Quantum key recycling and unclonable encryption

Quantum key recycling and unclonable encryption

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de Technische Universiteit Eindhoven,
op gezag van de rector magnificus prof.dr.ir. F.P.T. Baaijens, voor een commissie
aangewezen door het College voor Promoties, in het openbaar te verdedigen
op maandag 19 April 2021 om 16:00 uur

door

Daan Leermakers

geboren te Wageningen

Dit proefschrift is goedgekeurd door de promotoren en de samenstelling van de promotiecommissie is als volgt:

voorzitter:	prof. dr. J.J. Lukkien
1e promotor:	dr. B. Škorić
2e promotor:	prof. dr. S. Etalle
leden:	prof. dr. S. Fehr (CWI & Universiteit Leiden)
	prof. dr. H. Zbinden (Université de Genève)
	dr. ir. L.A.M. Schoenmakers
adviseur:	dr. A.T. Hülsing

Het onderzoek of ontwerp dat in dit proefschrift wordt beschreven is uitgevoerd in overeenstemming met de TU/e Gedragscode Wetenschapsbeoefening.

ISBN: 978-90-386-5235-1
Cover design: Rosalie Dudink & Daan Leermakers

Thanks

If you are reading this it is highly likely that you are among those whom I would like to thank for supporting me during my PhD studies these past four years. In any case, thanks for taking the time to read this.

First off, I would like to thank my promotor Boris Škorić. Boris, bedankt voor al het enthousiasme dat een samenwerking met jou met zich meebrengt. De beste herinneringen heb ik aan de willekeurige momenten waarop je mijn kantoor binnenstapte met een creatief idee om een nieuwe eigenschap te bereiken, een plan om een probleem op te lossen of gewoon om iets grappigs te delen. Jouw deur stond ook altijd open waardoor ik op eenzelfde manier mijn enthousiasme met jou kon delen (al bleek mijn intuïtie niet altijd even realistisch). De afgelopen vier jaar heb ik veel van je kunnen en moeten leren. Toch gaf je mij het gevoel dat we op gelijke voet de wereld van de quantum crypto onderzochten. Dank voor deze fijne manier van begeleiden. Ook ben ik mijn dank verschuldigd voor de uitleg van allerlei cryptografische dan wel natuurkundige fenomenen. Keer op keer nam je hiervoor alle tijd. Ik ben me bewust van het geluk dat ik heb gehad dat je mij hebt weten te beschermen van de bureaucratische verplichtingen die een onderzoeksproject met zich meebrengt. Dit was voor mij een hele prettige samenwerking, ontzettend bedankt!

Thanks to the members of my doctoral committee. It seems to me there are not enough hours in a day for someone in your positions. This makes me truly appreciative of the time you took to read this thesis and provide me with valuable feedback.

A big thanks to all my colleagues and friends at the TU/e and in Eindhoven that have made the past four years so very pleasurable. I remember meeting my officemate Alessandro on my first day and thinking: whatever else happens, at least I have a nice officemate. I am grateful for having met some of the nicest nerds of Eindhoven since then. I am sure there will come a time when I will look back at the lunches, after lunch coffee, Friday drinks, PhD council meetings and events, swimming, judo, Simon en de Giganten games and general atmosphere, being incredibly envious of my past self. In fact it is happening in these strange times already.

Thank you to the friends that have managed to stay in contact with me even though I deserted them by moving away. I realize that I'm not very good at ensuring frequent contact which makes me all the more thankful for the people who managed to keep me around.

Thanks to my parents. Bedankt voor het doorgeven van jullie positieve, vrije en open kijk op het leven. Voor de ondersteuning in mijn keuzes en het soms kritische meedenken over mijn toekomst. Ook wil ik jullie bedanken voor jullie inspirerende levenswijze. Tijdens mijn PhD hebben jullie onder andere een master afgerond en voor het eerst een marathon gelopen. Ik vind dat heel stoer en inspirerend en schrijf dat hier graag op. Dank ook aan mijn zussen waar ik in de toekomst hoop dichtbij te wonen.

Roos, bedankt voor je steun en vertrouwen in tijden dat mijn eigen vertrouwen ver te zoeken was. Zeker het afgelopen jaar heb je mij ontzettend geholpen met je

optimisme en aanstekelijke vrolijkheid. Lief ook dat je me van een Id_IoT tot een zachte idioot hebt hernoemd. Je maakt me gelukkig.

Finally, to my officemates: sluitingstijd!

Contents

Meet Alice, Bob and Eve

This thesis tells the story of three characters. First there is Alice. Alice likes to talk to her friend Bob. Bob does not say much himself but loves to listen and always lets Alice know that she is being heard. Alice and Bob trust each other 100%. If anything goes wrong during their communication, they know it's not due to them but due to Eve. Eve's life goal is to eavesdrop on Alice and Bob. She will do everything in her power to do so.

Luckily for Alice and Bob there exist many ways to communicate securely using classical cryptography. The protocols they use every day take the fastest computers using the best known algorithms thousands of years to break. Alice and Bob simply use the Signal app on their smartphones to communicate as securely as they want.

One day, Alice reads an article about quantum computers [Mim19], "The Day When Computers Can Break All Encryption Is Coming". She realizes that when these quantum computers become reality they will be able to decipher all messages she sent in the past of which the ciphertext is stored somewhere, even when she switches to quantum-resilient encryption[a]. Alice wants to share the article with Bob, but she hesitates. Meanwhile Bob is trying his luck on a mathy puzzle he's been trying to solve forever, and finally comes up with the solution. He wants to tell Alice, but then he realizes their secure communication channel relies on the hardness of math problems. If he can solve his problem, how can he be sure Eve won't solve the math problem used by the Signal protocol?

Not communicating for a while, Alice and Bob slowly become more and more anxious. One day their fears get to the point where they decide to leave all classical cryptography behind. Both Alice and Bob build a lab with the latest and greatest lasers, lenses, beam splitters, single photon sources and detectors and locks on the doors to keep Eve out. Their new setup allows them to communicate securely without relying on the hardness of mathematical problems, but rather on the laws of quantum physics.

Alice and Bob used to meet up all the time. But ever since the pandemic, they have become averse to in person meetups. Luckily, during the last time they met, they shared just enough key material to authenticate some initial messages. They start out by using quantum key distribution protocols to extend their shared key into a longer key which they use for information-theoretically secure classical communication. Over time they develop more efficient ways of communication with lower round complexity, less classical communication and even achieve security notions beyond what is possible classically.

[a]Known as post-quantum cryptography. A name that seems to imply there is an era after the quantum computer. Quantum-safe cryptography seems like a better name.

Chapter 1
Introduction

Getting started
Every chapter in this thesis starts with a little update on the situation of Alice, Bob and Eve, the characters that we just met in the first story box. We hear about the concerns or problems they might have and what solutions they envision. In the protocols discussed in the chapters, the names Alice and Bob double as the names of the honest users and the name Eve represents any possible eavesdropper. These little stories serve as informal motivations for the chapters and can be skipped if you don't care for them. Right now, Alice and Bob are busy setting up their respective labs while Eve is a bit bored as they are not communicating a lot. Let's use this time for an introduction.

1.1 Quantum cryptography

Quantum Physics
When looking at the world at very small scales, we see that it behaves very different from what we have come to expect from everyday life. We can not simply speak of the position of a particle, but should consider the probability of a position, observing a state will change the state, and particles that are far away from each other can instantly influence each other. These counter-intuitive properties of the microscopic world are described by quantum physics. Despite its counter-intuitive nature, quantum physics is perhaps the most accurate and well tested scientific theory in modern times. Its predictions are so reliable that in 2019, the kilogram was the last SI unit to be defined in terms of constants of nature by fixing the numerical value of the Planck constant to be $h = 6.62607015 \times 10^{-34}\mathrm{J}\cdot\mathrm{s}$ [NIS]. The Planck constant relates the energy of a light quantum (a photon) to its frequency. The quantum physical measurements of h are much more precise than the very precise method of weighing a cylinder of platinum-iridium, which was the previous definition of the kilogram.

Rather than describing the state of a system, e.g. the position of a particle, quantum physics describes the *probability* of observing the system in that state. For large systems in our daily lives, the probability of finding an everyday object somewhere is one or zero for all practical purposes. In general however, each particle has a complex probability amplitude α related to every state. The probability of measuring the particle in that state is $|\alpha|^2$. Directly after the measurement, a quantum system is

no longer in a 'superposition' but the state of the measured system is equal to the measurement outcome.

The phase of α is unimportant for the measurement probabilities until systems interact. The probability distributions interact much like two waves that meet on a water surface. They can interfere constructively producing an extra big probability of finding a particle, or destructively leaving no probability amplitude at all. Interestingly, a single quantum state can interfere with itself when multiple parts of the superposition interact as we will see in Section 1.2.2 and Chapter 7.

Perhaps the strangest property of quantum physics is called entanglement. When two particles at the same location interact with each other, their probability distributions can become entangled. Afterwards, the probability of measuring one of the two particles in a specific state is linked to the measurement outcome of the other particle, independent of the distance between the particles! We call a pair of entangled particles an EPR pair, after a paper by Einstein, Podolsky and Rosen, who were so amazed by this property that they questioned the completeness of quantum physics. [EPR35].

Using quantum physics for cryptography

The three properties of quantum physics discussed above

1. inherent nondeterminism
2. destructive measurements
3. entanglement

can be used for cryptographic purposes.

Our main reason for studying quantum protocols is scientific curiosity. But an additional benefit of quantum protocols is that they don't require any computational assumptions. They achieve information-theoretic security, i.e. the security is guaranteed by an adversary's lack of information regardless of their computational capabilities. This means that the secrecy of all messages is guaranteed regardless of the future computational gains of the adversary.

There exist classical symmetric cryptographic schemes that achieve information-theoretic security while using up key material. The one-time pad is one that we will encounter a lot. Often times quantum protocols are only used as a secure way to distribute keys after which information-theoretically secure classical schemes are used to perform a cryptographic task.

Classical and quantum cryptographic protocols alike almost always use random numbers. The probabilistic nature of quantum physics allows for a straightforward way of generating good random numbers. A simple example is the setup shown in Figure 1.1. The probability of finding a single photon at Detector A is $\frac{1}{2}$. As is the probability of finding it at Detector B. Crucially this process is unpredictable. It can be used to generate random numbers. We will not be explicit about the way Alice and Bob obtain random numbers in the described protocols.

The destructive measurement property of quantum physics allows Alice and Bob to detect any measurement performed by Eve. If Alice sends an unpredictable state to Bob and Eve tries to measure it, she can not do so without influencing Bob's measurement result. Unlike for classical messages, she can not keep a copy of the

message and forward the original message to Bob. In fact, it is impossible to make a copy of an unknown quantum state [WZ82]. Intuitively it is clear that compared to classical ways of sending information, Alice and Bob gain extra information about the actions of Eve when using quantum states. This gives them an advantage over Eve that they can exploit to communicate confidentially.

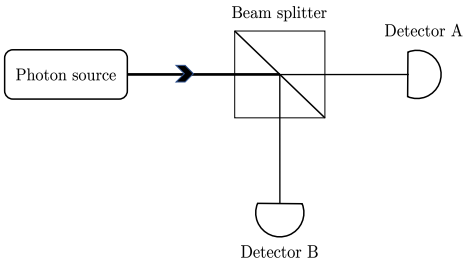

Figure 1.1: Simple setup to generate a random bit value from a quantum measurement.

We won't use stored EPR pairs in our protocols as it is very hard to store a quantum state for a long time. All the protocols we consider work with (an idealized version of) technology that is widely available today. There is however an equivalence between 'preparing a quantum state' and 'preparing an EPR pair and measuring one half' that allows us to construct equivalent protocols that we will use in our security proofs.

Although quantum cryptography, like classical cryptography, includes much more than confidential and authenticated communication between two parties, we will only be discussing six protocols that can achieve these 'simple' goals. For each protocol we will give a motivation, a protocol description and a proof of the security of the protocol. The proof recipe for the security of the quantum protocols that we will be using is given in Chapter 2. The remainder of this chapter introduces the six protocols that will be discussed and their specific aims.

1.2 Quantum key distribution

The most famous use of a quantum channel in the context of cryptography is Quantum Key Distribution (QKD). First proposed in 1984 [BB84], QKD allows two honest parties, Alice and Bob, to extend a small key, used for authentication, to a longer key in an information-theoretically secure way. Combined with classical one-time pad encryption, QKD Alice and Bob exchange messages with information-theoretic security.

The QKD field has received a large amount of attention, resulting in QKD schemes that discard fewer qubits, various advanced proof techniques, improved noise tolerance, improved rates, use of EPR pairs, higher-dimensional quantum systems etc. [Eke91, Bru98, GP01, SP00, LCA05, Ren05, KGR05, BOHL$^+$05, SYK14, TL17].

To explain the workings of our proof technique, we will discuss the security of six-state QKD as an example in Chapter 2. In Chapter 7, we will discuss an inter-

esting version of QKD that uses high-dimensional quantum states called round robin differential phase shift (RRDPS) QKD. It can deal with more noise than six state QKD while still being easy to implement.

1.2.1 BB84 and six-state QKD

The first quantum key distribution protocol was described in a famous paper by Charles Bennett and Gilles Brassard [BB84]. In BB84, Alice encodes a random bit x in the polarization of a photon. The way she encodes the bit x depends on her random basis bit b. Alice and Bob agree that when the encoding basis is zero ($b = 0$), a vertically polarized photon means $x = 0$ and a horizontally polarized photon means $x = 1$. When the other basis ($b = 1$) is used, the polarizations corresponding to $x = 0$ and $x = 1$ are rotated 45 degrees with respect to $b = 0$. The resulting photon represents a qubit with payload x in basis b which we write here as $|x\rangle_{b=...}$, see Figure 1.2 for a visualization of the encoding.

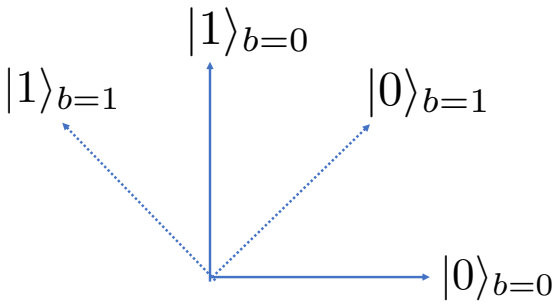

Figure 1.2: Encoding choice of the polarization of BB84 photons.

We denote the measurement result of Bob as y. The encoding has the following property. If Bob measures the qubit in the encoding basis, he will always measure the correct payload $y = x$. However, if he chooses the wrong basis (e.g. $b = 1$ while $b = 0$ was used to encode) he has equal probability to measure $y = 0$ or $y = 1$. Since in general the state changes after a measurement, the information is lost when measuring in the wrong basis. This property is not unique to the photon polarization, non-orthogonal bases of any quantum system have this property. In this thesis, we describe the protocols independent of the physical implementation of the quantum state.

Alice randomly sends one of these four states to Bob, who performs a measurement in the x- or z-basis chosen randomly. When using a uniform random basis choice, approximately half the time Bob uses the correct measurement basis and their payload bits should agree. By only keeping those bits where their bases agree, they end with what should be the same secret string. By comparing part of their measurement results publicly, Alice and Bob can estimate the noise on the channel. To deal with this noise, Alice and Bob have to perform two additional steps. They use an error correcting code to obtain the same string, followed by a cryptographic hash function

(privacy amplification) to make sure Eve doesn't know anything about their shared string. Information-theoretically secure authentication codes are typically used to authenticate the classical communication required by the protocol.

The same protocol can be executed using three instead of two encoding bases. In the polarization implementation, the extra encoding uses circular polarization as an extra orthogonal basis. Due to the larger uncertainty of the encoding bases it is harder for Eve to obtain information about the payload and to remain unnoticed in this six-state encoding. As a result, six-state QKD achieves a higher communication rate than BB84. In Section 2.6, we will consider a version of six-state QKD that works for any probability distribution on the basis choice. Using non-uniform basis choices further increases the obtainable rate [LCA05].

1.2.2 Round robin differential phase shift QKD

Round robin differential phase shift (RRDPS) QKD [SYK14] exchanges a key using the same principles as BB84 and six-state QKD. A random classical string is encoded in a quantum state, a random measurement is performed, Alice and Bob communicate classically about their preparation and measurement to determine their key and use error correction and privacy amplification to deal with noise. The main difference is the way RRDPS encodes information into the quantum states.

Alice generates a string of d random bits that we call a. The number d is the dimension of the qudit (a qubit of higher dimension). The bigger d is chosen the more information is encoded into the qudit. Alice prepares a photon in a uniform superposition of arrival times such that the phase corresponding to time bin t is given by a_t. Bob lets the photon interfere with itself. The difference between the arrival times that he lets interfere is determined by a random number Bob picks called r. Bob then measures the random arrival time k and the phase difference between times k and $k + r$. This measured phase difference is then $s = a_k \oplus a_{k+r}$. Bob tells Alice what r he picked and what k he measured so that she can compute s from her string a as well. The described protocol can be implemented practically with a a phase modulator on Alice's side, and a variable delay interferometer on Bob's side. The setup is shown in figure 1.3.

Repeating this process for many qudits gives Alice and Bob a shared string on which they can perform the same error correction and privacy amplification steps as in BB84. Since only one bit is extracted from the d random bits encoded in the photon, it is very hard for Eve to gain a lot of information about the relevant bit. It turns out that when Eve causes noise all the way up to 50%, which corresponds to Bob receiving random bits, Eve still can not learn a lot about s. Usually the amount of information Eve can gather increases as she causes more noise on the channel. For RRDPS QKD however, the amount of information she can obtain stops raising with the noise level at some saturation noise, e.g for $d = 10$ saturation occurs at $\sim$20% This incredible noise resilience is the main advantage of the RRDPS scheme.

1.3 Quantum key recycling

In BB84 and six-state QKD, after the measurements are done, Alice and Bob communicate classically about a number of things. i) Their basis choices; ii) their measure-

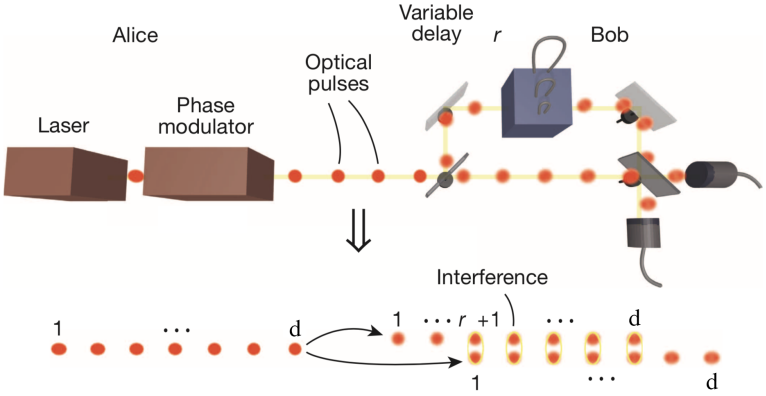

Figure 1.3: Round robin differential phase shift QKD setup [SYK14]. The interference of the different parts of the pulse train is visualized at the bottom of the figure.

ment results in some positions to check the noise; iii) the error correction redundancy information and iv) a random hash seed for privacy amplification. That seems like a lot of classical communication for a quantum protocol and they haven't even used their key for anything yet. In addition, they need to discard the measurement results of the qubit positions where their bases do not match, although this number can be kept low when using a heavily skewed probability distribution for the basis choice [LCA05].

Quantum Key Recycling (QKR) achieves the task of sending a classical message from Alice to Bob using the same principles as BB84 but without the large amount of classical communication back and forth and the waste of qubits. The only communication required in QKR is a single communication from Alice to Bob, and a single feedback bit from Bob to Alice indicating whether the communication was received alright. Since the waste of qubits is asymptotically negligible for skewed basis choices [LCA05], the reduced round complexity (number of times Alice and Bob communicate back and forth) is considered the main advantage of QKR.

In quantum key recycling, Alice and Bob share a secret encoding basis at the start of the protocol. As the name suggests, QKR will not use up this key material, but recycle (or re-use) the key material in subsequent rounds. The same properties that protect the qubit payload also protect the secret encoding basis, i.e. Eve can not learn the basis choice without being detected. If Bob received Alice's communication without too much noise, he is able to reconstruct the message without additional communication.

1.4 Unclonable encryption

In 2003, Daniel Gottesman considered the following attack on the one-time pad encryption.

1. Alice sends an encrypted message to Bob.

2. Eve makes a copy of the encrypted message.
3. Eve passes on the original message to Bob, who can not detect her copy.
4. Eve somehow obtains a copy of the secret key and decodes the message.

This attack illustrates that in addition to using the key only once, one-time pad encryption requires the users to keep the key secret forever, e.g. by destroying it. However, destroying information that has been kept for a longer time, e.g. on a hard disk memory, is hard in practice. To protect against this attack, Gottesman introduced a scheme he called unclonable encryption[1] [Got03]. By encoding the classical message directly into a quantum state, one can ensure that after measurement of the quantum state no ciphertext remains that could link the key to the message. If the noise on the quantum channel was not too high, the encoding guarantees Eve can never learn anything about the message in the future. Even when all used key material leaks, the message is secure. This notion of encryption is even stronger than information-theoretic security. Not only does Eve have too little information to decrypt Alice and Bob's ciphertext, she is guaranteed not to have gained the ciphertext, if the noise is sufficiently low. Therefore Eve can never learn the message independent of what she learns in the future (excluding the possibility where Alice and Bob leak the message itself). If Eve does cause a lot of noise on the channel, Alice and Bob should be careful with their key material since Eve might have intercepted and stored the quantum states. Although unclonable encryption protects against an attack where Eve uses quantum storage, Alice and Bob need only prepare and measure quantum states as is the case for QKD and QKR.

1.5 Desiderata for quantum encryption protocols

The BB84 and six-state quantum key distribution protocols facilitate the information-theoretically confidential communication between two parties. It achieves this using only simple operations on simple quantum states that are practically feasible with widely available current technology. We will consider protocols that aim to improve upon the performance of BB84 and six-state QKD without the need for additional technological requirements. The different chapters of this thesis focus on different desired functionalities. All chapters aim to answer the following research question:

"***How can two-party prepare-and-meaure quantum encryption protocols for communicating confidential classical information be improved beyond the state of the art?***"

To specify what is meant by *improved* we list the desiderata of a quantum encryption protocol. In addition to providing information-theoretic security, a good quantum encryption protocol has:

- Only simple operations on easily prepared states.
- Noise resilience (maximum noise that the scheme can tolerate).
- High communication rate (few quantum states per classical bit).

[1] Actually he called the property *uncloneable* encryption. Both spellings are used.

- Low round complexity (number of interactions between the parties).
- No redundant classical communication.
- Efficient use of key material.
- Small key sizes.
- Confidentiality guarantees in the case of key leakage.

1.6 Contributions

Each upcoming chapter of this thesis proves the security of a quantum key distribution, quantum key recycling or unclonable encryption protocol that achieves a number of our desiderata.

Chapter 2 describes the framework we use to prove the security of the protocols. The framework uses some crucial elements from the proof method developed by Renato Renner [Ren05] to give proofs that are *composable* with other protocols. An EPR version of the protocols is given. Eve is given a purification of the state shared by Alice and Bob (a description of everything their state interacted with). The post-selection technique [RK05] is used to extend attacks on single qubits or qudits to general attacks. Symmetries in the protocol are exploited to obtain a simple description of Eve's state: (i) it has factorized form, i.e. the tensor product of contributions from individual qubit positions, (ii) in each qubit position the density matrix depends only on the noise parameter(s) that are used in the monitoring procedure. We compare the real scenario to an ideal scenario in which the same protocol is executed but Eve can not learn anything. If the state that Eve can obtain in reality is statistically exponentially close to the ideal state, Eve has an exponentially low probability of successfully attacking the protocol.

As an example of the proof recipe, we prove the security of six-state QKD. The versatility of the proof method is demonstrated in the subsequent chapters where we apply the same recipe to a variety of protocols and settings. In particular, we will use it to prove the security of key material and messages by bounding a single quantity. We'll show that unclonability can be proven using the same method. And we will show that sharp results are obtained for protocols with high dimensional states and multiple passes over a quantum channel.

Chapter 3 introduces a quantum key recycling (QKR) protocol. QKR aims to lower the round complexity compared to QKD. Although QKR was proposed in 1982 [BBB82], two years before BB84, no qubit-based scheme was proven secure until 2017 [FS17]. Our protocol is similar to the protocol of [FS17], which in turn is similar to [BBB82]. The differences introduced in our protocol allow us the prove the security of the recycled keys and the message in a single expression. While [FS17] has low rate when used as an encryption, our protocol achieves the same communication rate (message bits per qubit sent) as QKD. In our protocol one can choose between the BB84 encoding and the six-state encoding [Bru98]. The six-state encoding yields a

higher rate, as known from QKD. This chapter is based on [LŠ19a].

Chapter 4 describes and proves the security of a quantum key recycling scheme. The scheme encodes all the information directly into the qubits without the need to send any classical information alongside the quantum states. The only classical communication remaining is a single feedback bit from Bob to Alice. This fully embedded scheme achieves the same communication rate as QKR and QKD. When the noise on the quantum channel is too high, QKR protocols yield a reject message indicating the communication was unsuccessful. For messages of size ℓ, the key update procedure in the reject case needs ℓ bits fresh key material in the noiseless case, which is the minimum possible [DPS05]. This chapter is based on [LŠ21].

Chapter 5 combines key recycling and unclonable encryption in a single protocol. Unclonable encryption provides security guarantees even if the key material used in the protocol leaks after the protocol is finished. The unclonable encryption scheme as introduced by Gottesman [Got03] achieves the unclonability property but is not very efficient. Asymptotically, it uses up one bit of key material for every message bit sent. By constructing an unclonable encryption scheme in which the key material can be recycled, we construct an efficient scheme in terms of communication rate as well as round complexity. By composing our protocol with a QKD or QKR scheme, we can refresh key material in an efficient manner as well. Like the fully embedded protocol of Chapter 4, we keep the classical communication to a minimum by encoding all information from Alice to Bob directly into the quantum states. We find a close relation between key recycling schemes and unclonable encryption schemes. This chapter is based on [LŠ20a]

Chapter 6 describes a quantum protocol in which a quantum state is sent in two directions, first from Bob to Alice and then back from Alice to Bob. It aims to improve the reject behavior of unclonable encryption for Alice (the sender of the message). Both the scheme by Gottesman [Got03] and the scheme of Chapter 5 require Alice and Bob to permanently keep their key material secret when the protocol outputs a reject message. By having Alice encode the message into a quantum state without holding the key material needed to perform the decoding, Alice can safely leak all the key material she holds after the protocol is finished. Bob, who has the key material to decode, is in the same situation as before, and has to keep the keys secure forever but only in the reject case. The described functionality is achieved by letting Bob prepare the qubit in a random basis. Alice, without knowing the encoding basis, can flip the qubit payload depending on her message. The result is a qubit going from Alice to Bob encoding Alice's message padded by Bob's initial payload in a basis that only Bob knows. Measuring the qubit in the correct basis lets Bob receive Alice's message.

We define a security notation we call vulnerable-sender unclonable encryption. This security property guarantees the security of an encoded message even when the shared key material of the two parties leaks afterward. Alice holds only shared key material and can safely leak it all.

The security proof of the protocol requires the description of a 16-dimensional quantum state held by Eve that is closely related to the state Eve obtains in six-state

QKD and QKR. We can modify our protocol to do QKD and find it achieves a better rate than other two-way QKD schemes [BLMR13]. This chapter is based on [LŠ20b].

Chapter 7 describes the round robin differential phase shift (RRDPS) quantum key distribution protocol introduced in 2014 by Sasaki, Yamamoto and Koashi [SYK14]. It aims to improve the noise resilience of quantum key distribution. We add noise monitoring to the RRDPS protocol and prove its security. Our proof method, detailed in Chapter 2, yields a sharper result than other results [SYK14, SK17] based on equivalence of the protocol to quantum error correction codes [SP00]. The proof requires the description of a d^2 dimensional state held by Eve which, after exploiting symmetries, has three degrees of freedom left. Optimizing these parameters as a function of noise yields a saturation noise. Introducing more noise than the saturation noise no longer helps Eve.

In addition to proving its security, we will gain insight in the gap between what we can prove using our proof method and how much Eve can learn with an attack where she directly performs a measurement characterized by the accessible information. The accessible information shows the same saturation behavior. This chapter is based on [LŠ19c].

Chapter 2
Proof technique

Quantum protocols require proofs
Alice and Bob learn all there is to know about quantum cryptographic protocols. They come across many very promising claims of "unconditional security" that is "guaranteed by the laws of physics". However, anxious about cryptography as they are, they decide it might be too good to be true and they first want to get a grip on the underlying assumptions. Once they know all about the notation and jargon, the classical tools and the quantum encodings, the attacker model and assumptions, they are ready to speak confidently about the security of a quantum protocol. They develop a proof framework that allows them to prove the security of a protocol before trusting that they perform exactly as expected. As their first protocol Alice and Bob decide on six-state quantum key distribution. Its security is already well understood and it achieves good performance in terms of communication rate.

2.1 Attacker model and assumptions

We will consider the security of our protocols in the following setting. Alice and Bob perform all their actions in their private labs. Eve has no access to their labs and no information about Alice and Bob's actions leaks from their labs. No sounds, (unintended) electromagnetic radiation, power usage information etc. are available to or can be influenced by Eve, i.e. there are no side-channel attacks. We do not consider the effects of imperfections in the devices used by Alice and Bob. Alice and Bob have access to a quantum channel for transmitting quantum states, as well as to a classical channel for transmitting classical bits.

Eve can read, copy and alter any and all messages sent over the classical channel as well as insert messages of her own. In our protocols, Alice and Bob use classical authentication methods to make sure they can detect the latter two classes of actions by Eve. Eve can perform any computation instantly, there are no computational assumptions. On the quantum channel, Eve can perform any action allowed by the laws of physics. She can apply arbitrary unitary operations to any state, she has access to unlimited quantum memory, she can create arbitrary quantum states and perform noiseless measurements. Independent of the expected noise of the quantum

channel, Eve always receives the sent states unaltered and can send any state in noiseless fashion. All noise on the quantum channel is assumed to be caused by Eve.

Initially, we will take the conventional view that Alice and Bob can forget or delete classical information. In later chapters, we will also consider situations in which classical information that is stored long-term will eventually leak to Eve.

2.2 Classical tools

In our protocols we will make repeated use of a number of useful classical tools. Note that the properties of all these tools are independent of the capabilities of the attacker. An overview of the notation introduced is given in Table 2.1.

2.2.1 Notation for classical tools

Classical random variables are denoted with capital letters, and their realizations with lowercase letters. The probability that a random variable X takes value x is written as $\Pr[X = x]$. Sets are denoted in calligraphic font. The space of probability distributions on $\mathcal{X}$ is written as $S(\mathcal{X})$. We write $[n]$ for the set $\{1, \ldots, n\}$. For a string x and a set of indices $\mathcal{I}$ the notation $x_{\mathcal{I}}$ means the restriction of x to the indices in $\mathcal{I}$. Bitwise XOR of binary strings is written as $\oplus$. The inverse of a bit $b \in \{0, 1\}$ is written as $\bar{b} = b \oplus 1$. The size of a string x and set $\mathcal{X}$ is written as $|x|$ and $|\mathcal{X}|$ respectively. The Hamming weight of a string x is denoted as $\texttt{Hamm}(x)$. The bit-wise logical *and* of two bit strings x, y is denoted as $x \wedge y$. A substring is denoted with square brackets, the first ℓ bits of a string x is denoted as $x[:\ell]$. The notation log stands for the logarithm with base 2. The binary entropy is written as $h(p) = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}$ with $p \in [0, 1]$ and $0 \log 0$ taken to be 0. We sometimes write $h(p_1, \ldots, p_n)$ meaning $\sum_i p_i \log \frac{1}{p_i}$. The Kronecker delta of variables x and x' is denoted as

$$\delta_{x,x'} = \begin{cases} 1 & \text{if } x = x' \\ 0 & \text{otherwise} \end{cases} \tag{2.1}$$

2.2.2 One-time pad encryption

Classically, the best confidentiality guarantee is provided by One-Time Pad encryption. If Alice and Bob share a uniform n-bit secret key k, they can exchange an n-bit message m with information-theoretic security. Alice adds the key and the message bit-wise to obtain a ciphertext $c = m \oplus k$. She sends the ciphertext to Bob over a classical channel. Without k, Eve can not learn anything about m since k completely decouples m and c. Eve can save a copy of c. Once Eve has c, Alice and Bob can not use k to pad another message safely, hence the name one-time pad encryption.

We will be using one-time pad encryption when we want to confidentially send a message over the classical channel. We don't explicitly speak about the security of the encrypted message or the key. We consider the encrypted message unknown to Eve when the key is kept secret, and known to Eve if the key becomes public at a later time.

Notation	Meaning
$\Pr[X = x]$	Probability that random variable X takes value x.
$\mathcal{X}$	Set of possible x values.
$S(\mathcal{X})$	Space of probability distributions on $\mathcal{X}$
$\bar{b}$	The inverse of a bit: $b \oplus 1$.
$\oplus$	Bit-wise XOR.
$\lvert x \rvert$	Length of a string x.
$\lvert \mathcal{X} \rvert$	Size of the set $\mathcal{X}$.
$\wedge$	Bitwise logical 'and'.
log	Logarithm base 2.
$h(p)$	Binary entropy $p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}$.
$h(p_1, \ldots p_n)$	Entropy $\sum_i p_i \log \frac{1}{p_i}$.
$\delta_{x,y}$	Kronecker delta. Equals 0 except when $x = y$ then equals 1.
λ	Security parameter.
$\mathbb{1}_\ell$	Identity matrix of dimension ℓ.
β	Bit error rate (bit flip probability)
`Enc`, `Dec`	Encoding and decoding functions.
`Syn`, `SynDec`	Syndrome and syndrome decoding functions.
$\hat{x}$	Reconstructed x by the decoding function.
tr	Trace
$A^\dagger$	Hermitian conjugate of an operator A.
x^*	Complex conjugate of x.
$\otimes$	Tensor product.
χ^A	Fully mixed state on the A space.
$\mathcal{B}$	Set of bases.
σ_i	i'th Pauli operator.
$S(\mathcal{H})$	Space of density matrices on $\mathcal{H}$
$S(\rho)$	Von Neumann entropy of the density matrix ρ
$S_\alpha(\rho)$	Rényi entropy of order α
$S_\alpha^\varepsilon(\rho)$	Smooth Rényi entropy of order α with smoothing parameter ε

Table 2.1: Notation introduced in this chapter

2.2.3 Pairwise independent hashing

A family of hash functions $H = \{h : \mathcal{X} \to \mathcal{Y}\}$ is called pairwise independent (a.k.a. 2–independent or strongly universal) [CW79] if for all distinct pairs $x, x' \in \mathcal{X}$ and all pairs $y, y' \in \mathcal{Y}$ it holds that $\Pr_{h\in H}[h(x) = y \wedge h(x') = y'] = |\mathcal{Y}|^{-2}$. For $|\mathcal{X}| \geq |\mathcal{Y}|$ there are known constructions for pairwise independent hash functions that have $|H| = |\mathcal{X}||\mathcal{Y}|$.

We will be using families of pairwise independent hash functions h_u where the function is specified by a random hash seed $u \in \mathcal{U}$. Let the probability distribution of U be uniform. The defining property of pairwise-independent hash functions gives

$$\mathop{\mathbb{E}}_{u} \delta_{h_u(x),y}\delta_{h_u(x'),y} \quad = \quad \delta_{x,x'}|\mathcal{Y}|^{-1} + (1 - \delta_{x,x'})|\mathcal{Y}|^{-2}. \tag{2.2}$$

An example of a hash function that achieves $|H| = |\mathcal{X}||\mathcal{Y}|$ uses an affine function in $GF(2^k)$ [LW99]. Let $u = (u_1, u_2)$ with $u_1, u_2 \in GF(2^\ell)$ be randomly chosen. Define $F_u(x) = u_1 \cdot x + u_2$, where the operations are in $GF(2^k)$. By taking the ℓ least significant bits of $F_u(x)$ we get a pairwise independent hash function $F : \{0,1\}^k \to \{0,1\}^\ell$. Note that since the $k - \ell$ most significant bits of $F_u(x)$ are dropped, the size of u_2 can be reduced by $k - \ell$ as well. Also note that the input of the hash function is decoupled from the output as long u is unknown.

Unless specified otherwise, this example can be used as the pairwise independent hash function in all protocol of this thesis.

2.2.4 Information-theoretically secure message authentication codes

Pairwise independent hash function can be used to construct single-use information-theoretically secure message authentication codes (MACs) [WC81]. A message m can be authenticated using a pairwise-independent hash function h_u with seed $u \in \mathcal{U}$ by computing a tag $\tau = h_u(m)$ and communicating τ alongside m. The defining property of the pairwise-independent hash function then guarantees that Eve can not alter the message undetected without knowing the hash seed u. If the verification $\tau' = h_u(m')$ holds for the received message m' and tag τ', Bob can be confident that $m = m'$ because the probability of successfully forging τ is $\Pr[\tau = h_u(m')|m \neq m'] = 2^{-\min(|\tau|, \log|\mathcal{U}|)}$.

Instead of using pairwise independent hash functions, single-use MACs can be built from easier to achieve primitives like universal hash functions and almost pairwise-independent hash functions [Sti94]. This allows for a smaller hash seed. For our MACs we assume $|\tau| = \log|\mathcal{U}| = 2\lambda$, with λ the security parameter.

We use single-use information-theoretically secure MACs (one-time MACs) to authenticate messages sent over the classical channel. Sometimes we will speak about an authenticated channel. It should then be understood that every use of this channel costs λ bits of key material and increases the failure probability of the protocol by $2^{-\lambda}$. In addition we will use MACs to authenticate messages encoded in quantum states.

2.2.5 Error correcting codes

The bit error rate β on a quantum channel is the probability that a classical bit x encoded into a quantum state by Alice arrives at Bob as the flipped value $\bar{x}$. We use β and γ to denote the noise (bit error rate). The combined noise of two subsequent channels is written as $\beta \star \gamma = \beta(1-\gamma) + (1-\beta)\gamma$.

An error correcting code (ECC) adds redundancy to a transmitted message to form a codeword. The original message can be recovered from a noisy version of this codeword. We will be using linear error-correcting codes that encode a message of size κ into a codeword of size n. They consist of an encoding function $\texttt{Enc} : \{0,1\}^\kappa \to \{0,1\}^n$ and a decoding function $\texttt{Dec} : \{0,1\}^n \to \{0,1\}^\kappa$. For linear codes, Alice encodes a message m into a codeword using a generator matrix G, $x = \texttt{Enc}(m) = xG$ where x is represented as a row vector. The matrix G can always be written in systematic form, $G = (\mathbb{1}_\kappa|\Gamma)$, where the $\kappa \times (n-\kappa)$ matrix Γ contains the checksum relations. The codewords will then have the original string as first κ bits followed by $n-\kappa$ redundancy bits. When Bob receives the noisy string x' with βn errors or less, he can reconstruct x with certainty. When there are more than βn bit flips the code will output the wrong message or an error $\perp$. We will use the 'hat' notation to refer to the reconstructed string. For $x = \texttt{Enc}(s)$ we write $\hat{s} = \texttt{Dec}(x')$ and $\hat{x} = \texttt{Enc}(\hat{s})$.

When Alice and Bob have access to a noisy channel (e.g. a quantum channel) and a robust channel (e.g. a classical channel), Alice can send an n-bit message over the noisy channel and send the redundancy bits over the robust channel. Alice and Bob agree on a syndrome function $\texttt{Syn} : \{0,1\}^n \to \{0,1\}^{n-\kappa}$ and decoder $\texttt{SynDec}$: $\{0,1\}^{n-\kappa} \to \{0,1\}^n$. Alice sends a string $x \in \{0,1\}^n$ to Bob over the noisy channel. In addition she sends a syndrome containing the error correction information, $e = \texttt{Syn}\, x$ over the robust channel. Bob can compare the syndromes of x and x' to find the noise vector $\eta = \texttt{SynDec}(\texttt{Syn}\, x' \oplus e)$ which he uses to reconstruct $\hat{x} = x' \oplus \eta$.

Without specifying the particular code used, we assume the performance of the code is independent of the location of the bit flips. Asymptotically, linear error correcting codes can reach channel capacity $\frac{\kappa}{n} = 1 - h(\beta)$. Non-asymptotically this limit can be approached as $n - \kappa = nh(\beta) + \sqrt{n}\Phi^{-1}(\varepsilon)\sqrt{\beta(1-\beta)}\log\frac{1-\beta}{\beta}$ (see [BKB04]), where ε is the probability of decoding error and $\Phi(z) \stackrel{\text{def}}{=} \int_z^\infty (2\pi)^{-1/2}\exp[-x^2/2]\mathrm{d}x$.[1]

2.3 Quantum toolbox

We will briefly describe the relevant aspects of quantum theory used for our proofs. We only need to understand a little for the simple systems we use.

2.3.1 Notation for quantum tools

The vector space in which quantum states exist is called the Hilbert space denoted as $\mathcal{H}$. Quantum states are denoted as kets $|\psi\rangle$. The Hermitian transpose of a ket is called a bra and is written as $\langle\psi|$. The notation 'tr' stands for trace[2]. The Hermitian conjugate of an operator A is written as $A^\dagger$. The complex conjugate of z is denoted

[1] For $\varepsilon = 10^{-6}$ we have $\Phi^{-1}(10^{-6}) \approx 4.75$.

[2] It is understood to be a linear operator acting to the right.

as z^*. Let A be a matrix with eigenvalues λ_i. The 1-norm of A is written as $\|A\|_1 = \mathrm{tr}\sqrt{A^\dagger A} = \sum_i |\lambda_i|$. We describe the system consisting of two states $|\psi\rangle$ and $|\phi\rangle$ as $|\psi\rangle \otimes |\phi\rangle = |\psi\rangle|\phi\rangle = |\psi\phi\rangle$. Here $\otimes$ denotes the tensor product.

2.3.2 Qubit Encodings

We consider the most common way to encode a bit $x \in \{0, 1\}$ into a qubit state. We denote the encoding of the zero and one bit in the standard basis as $|0\rangle, |1\rangle$ with $|0\rangle$ called the positive z-direction. The set of bases used is denoted as $\mathcal{B}$, and a basis choice as $b \in \mathcal{B}$. The encoding of bit value x in basis b is written as $|\psi_x^b\rangle$. We refer to x as the payload. In the BB84 encoding we write $\mathcal{B} = \{0, 1\}$ which we refer to as the z-basis ($b = 0$) and the x-basis ($b = 1$), with $|\psi_0^0\rangle = |0\rangle$, $|\psi_1^0\rangle = |1\rangle$, $|\psi_0^1\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|\psi_1^1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. In six-state encoding we additionally utilize the y-basis ($b = 2$), $\mathcal{B} = \{0, 1, 2\}$ with $|\psi_0^2\rangle = \frac{|0\rangle+i|1\rangle}{\sqrt{2}}$, $|\psi_1^2\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}$. We will also encounter the eight-state encoding [ŠdV17] consisting of non-orthogonal vectors, see Section 3.1.3.

The probability of getting outcome x when measuring a state $|\phi\rangle$ in the b basis is $|\langle\psi_x^b|\phi\rangle|^2$. For example, the probability of finding zero when measuring the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in the z-basis is $|\langle 0|\psi\rangle|^2 = |\alpha|^2$. For any basis, the measurement probabilities of a quantum state should add up to one. We then say the state is normalized. For $|\psi\rangle$ this means that $|\alpha|^2 + |\beta|^2 = 1$. The states $|\psi_0^0\rangle, |\psi_0^1\rangle, |\psi_0^2\rangle$ can be visualized as unit vectors spanning a three-dimensional space. Due to the normalization constraint, every qubit state exists on a sphere with radius one in this three-dimensional space. This sphere is known as the Bloch sphere.

2.3.3 Bell states

The smallest system with quantum entanglement consists of two qubits whose bit values are completely (anti)correlated. In any basis, the maximally entangled two-qubit states are represented by the four Bell states. The Bell states with respect to the z-basis are:

$$|\Phi^+\rangle = |\Phi_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad ; \quad |\Psi^+\rangle = |\Phi_{10}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}; \tag{2.3}$$

$$|\Phi^-\rangle = |\Phi_{01}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \quad ; \quad |\Psi^-\rangle = |\Phi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{2.4}$$

The subscript notations allow us to write the simple notation $|\Phi_{uv}\rangle = (\mathbb{1} \otimes \sigma_x^u \sigma_z^v)|\Phi_{00}\rangle$ (see Section 2.3.5 for the definitions of σ_x, σ_z). The $\pm$ notation is more memorable and common. In general we will refer to maximally entangled states as EPR pairs [EPR35]. Notice that the Bell states describe the state of both qubits together. This description is independent of the distance between the two qubits. This gives rise to the non-intuitive phenomenon in which a local action can have a remote effect. Consider for example the state $|\Phi^+\rangle$ where Alice holds the first qubit and Bob holds the second. When Alice measures her qubit in the z-basis she will measure a random bit. Depending on her measurement result Bob's state changes to the same bit encoded in the z-basis. This means that the net result of preparing one of the Bell states and measuring in the z-basis is equivalent to preparing a random bit in

the z-basis. Similarly, measuring in the x- or y-basis results in a random bit being encoded in that basis. Note that this instantaneous action at a distance can not be used to send information from Alice to Bob without an additional transmission after the measurement. The Bell states guarantee that a measurement of one half of the pair yields a random value rather than a chosen value.

The $|\Psi^-\rangle$ state is known as the singlet state. It is often used since it holds that $|\Psi^-\rangle \propto |\psi_0^b\rangle|\psi_1^b\rangle - |\psi_1^b\rangle|\psi_0^b\rangle$ for any basis b. The Bell states form a basis for the two-qubit space.

2.3.4 Mixed states

So far we have been considering pure quantum states. For a pure state we know exactly in which state the system is. An example of a pure state is the superposition discussed in Section 1.1 which we will write as $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ (where we have replaced position A by bit 0 and position B by bit 1). This so called ket $|\psi\rangle$ can be represented by a vector by taking $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ giving $|\psi\rangle = \begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix}$. The conjugate transpose (bra) is written as $\langle\psi| = (1/\sqrt{2}\ 1/\sqrt{2})$. Even though we have a probability of $\frac{1}{2}$ of measuring zero and probability of $\frac{1}{2}$ of measuring one, we know these probabilities exactly.

Imagine instead of preparing a pure state, Alice flips a coin and depending on the outcome prepares $|0\rangle$ or $|1\rangle$. Eve, who does not know the outcome of the coin flip, describes the state as a classical mixture of $|0\rangle$ and $|1\rangle$ each with probability $\frac{1}{2}$. The state can no longer be written as a ket or vector but is written as a matrix called a density matrix: $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. States that consist of a classical mixture of pure states are called mixed states. In general, when the probability of being in state $|\psi_x\rangle$ is $\Pr[X = x]$, we write $\rho_x = \sum_x \Pr[X = x]|\psi_x\rangle\langle\psi_x|$. We will encounter mixed states a lot. The values encoded into the quantum states are unknown to Bob and Eve, otherwise there would be no point in communicating. We write $\mathcal{S}(\mathcal{H})$ to denote the space of normalized ($\operatorname{tr}\rho = 1$) density matrices on Hilbert space $\mathcal{H}$, i.e. normalized positive semi-definite operators acting on $\mathcal{H}$.

To denote the combination of classical and quantum states, we represent classical variables in the bracket notation as well. The density operator describing a classical variable x is written as $\mathbb{E}_x |x\rangle\langle x|$. This allows us to describe the combination of classical variables and quantum states (classical-quantum states) as one density matrix. We use capitalized superscripts to label subsystems of a Hilbert space. Non-italic labels 'A', 'B' and 'E' indicate the subsystem of Alice/Bob/Eve. Consider classical variables X, Y and a quantum system in Eve's possession that depends on X and Y. The combined classical-quantum state is $\rho^{XY\mathrm{E}} = \mathbb{E}_{xy} |xy\rangle\langle xy| \otimes \rho^{\mathrm{E}}_{xy}$. The state of a sub-system is obtained by tracing out all the other subspaces, e.g. $\rho^{Y\mathrm{E}} = \operatorname{tr}_X \rho^{XY\mathrm{E}} = \mathbb{E}_y |y\rangle\langle y| \otimes \rho^{\mathrm{E}}_y$, with $\rho^{\mathrm{E}}_y = \mathbb{E}_{x|y}\, \rho^{\mathrm{E}}_{xy}$. When X is unknown to Eve, $\rho^{Y\mathrm{E}}$ is the relevant description of the state from Eve's perspective. The fully mixed state is denoted as $\chi^A = \sum_a \frac{1}{|\mathcal{A}|}|a\rangle\langle a|$.

2.3.5 Evolution of a quantum state

The change of a closed quantum system, i.e. a quantum system that is not interacting with other quantum systems, over time is described by a unitary transformation.

$$|\psi'\rangle = U|\psi\rangle \tag{2.5}$$

where it holds that $UU^\dagger = U^\dagger U = \mathbb{1}$. A unitary U describes a reversible operation. When we are not dealing with a closed system, e.g. Eve lets a qubit interact with a ancillary system of her own, we also make use of unitary operators by describing the combination of the qubit and the ancilla as a closed system. An important example of unitary operators working on qubits are the Pauli operators. We define the Pauli operators with respect to the z-basis as:

$$\sigma_0 = \mathbb{1}_2; \quad \sigma_1 = |0\rangle\langle 1| + |1\rangle\langle 0|; \quad \sigma_2 = -i|0\rangle\langle 1| + i|1\rangle\langle 0|; \quad \sigma_3 = |0\rangle\langle 0| - |1\rangle\langle 1|. \tag{2.6}$$

We also use the notation $\sigma_x \stackrel{\text{def}}{=} \sigma_1$, $\sigma_y \stackrel{\text{def}}{=} \sigma_2$, $\sigma_z \stackrel{\text{def}}{=} \sigma_3$. Acting on a qubit in an eigenstate of σ_z, e.g. $|x\rangle$, the Pauli operators can flip the payload and change the phase.

$$\sigma_0|x\rangle = |x\rangle \quad ; \quad \sigma_1|x\rangle = |\bar{x}\rangle; \quad \sigma_2|x\rangle = (-1)^x i|\bar{x}\rangle \quad ; \quad \sigma_3|x\rangle = (-1)^x|x\rangle. \tag{2.7}$$

The effect on the qubit encodings in the x- and y-basis discussed in Section 2.3.2 is given by

$$\sigma_0|\psi_x^1\rangle = |\psi_x^1\rangle \ ; \ \sigma_1|\psi_x^1\rangle = (-1)^x|\psi_x^1\rangle \ ; \ \sigma_2|\psi_x^1\rangle = (-1)^x i|\psi_{\bar{x}}^1\rangle \ ; \ \sigma_3|\psi_x^1\rangle = |\psi_{\bar{x}}^1\rangle, \tag{2.8}$$

$$\sigma_0|\psi_x^2\rangle = |\psi_x^2\rangle \ ; \ \sigma_1|\psi_x^2\rangle = (-1)^x i|\psi_{\bar{x}}^2\rangle \ ; \ \sigma_2|\psi_x^2\rangle = (-1)^x|\psi_x^2\rangle \ ; \ \sigma_3|\psi_x^2\rangle = |\psi_{\bar{x}}^2\rangle. \tag{2.9}$$

The evolution of a mixed state ρ is obtained by sandwiching the density matrix between the operator and its conjugate transpose $U\rho U^\dagger$.

2.3.6 Quantum measurements

We use the Positive Operator Valued Measure (POVM) formalism to describe quantum measurements. A POVM $\mathcal{M}$ consists of positive semidefinite operators, $\mathcal{M} = (M_x)_{x\in\mathcal{X}}$, $M_x \geq 0$ where x is the measurement outcome. A set of POVMs has to satisfy the condition $\sum_x M_x = \mathbb{1}$, which guarantees the total probability of getting some measurement result is one. POVMs are the most general kind of measurement in quantum physics. Applying a POVM is equivalent to coupling an ancilla state to a system then performing a unitary operation of the entire system and finally performing a projective measurement. The probability of measuring state ρ yielding outcome x is given by $\operatorname{tr} M_x\rho$.

2.3.7 Quantum maps and the diamond norm

Any quantum channel can be described by a completely positive trace-preserving (CPTP) map $\mathcal{E} : \mathcal{S}(\mathcal{H}_\mathrm{A}) \to \mathcal{S}(\mathcal{H}_\mathrm{B})$ that transforms a mixed state ρ^A to ρ^B: $\mathcal{E}(\rho^\mathrm{A}) = \rho^\mathrm{B}$. For a map $\mathcal{E} : S(\mathcal{H}_\mathrm{A}) \to S(\mathcal{H}_\mathrm{B})$, the notation $\mathcal{E}(\rho^\mathrm{AC})$ stands for $(\mathcal{E} \otimes \mathbb{1}_C)(\rho^\mathrm{AC})$, i.e. $\mathcal{E}$ acts only on the 'A' subsystem.

Quantum maps describe a variety of transformations a quantum state can undergo, including creation, time evolution, interaction, measurement and destruction. The protocols described in this thesis form a virtual quantum channel from Alice to Bob and can be described by a CPTP map.

The diamond norm of a quantum map is defined as the supremum of the 1-norm between the outputs of the maps, where the supremum is taken over the density matrices in $\mathcal{H}_\mathrm{A}$ with an auxiliary system $\mathcal{H}_\mathrm{C}$ that can be considered of the same dimension as $\mathcal{H}_\mathrm{A}$ [TL17]. The diamond norm of the map $\mathcal{E}$ is

$$\|\mathcal{E}\|_\diamond = \frac{1}{2} \sup_{\rho^{\mathrm{AC}} \in \mathcal{S}(\mathcal{H}_{\mathrm{AC}})} \|\mathcal{E}(\rho^{\mathrm{AC}})\|_1. \tag{2.10}$$

The diamond norm $\|\mathcal{E} - \mathcal{E}'\|_\diamond$ can be used to bound the probability of distinguishing two CPTP maps $\mathcal{E}$ and $\mathcal{E}'$ given that the process is observed once. The maximum probability of a correct guess is $\frac{1}{2} + \frac{1}{4}\|\mathcal{E} - \mathcal{E}'\|_\diamond$. We refer to $\|\mathcal{E} - \mathcal{E}'\|_\diamond$ as the diamond distance between $\mathcal{E}$ and $\mathcal{E}'$.

2.3.8 Entropy of quantum states

For a classical discrete random variable X, the amount of uncertainty on the variable can be quantified by the Shannon entropy: $\mathrm{H}(X) = \sum_x \Pr[X = x] \log \frac{1}{\Pr[X=x]}$. It can be thought of as the minimum number of binary questions one has to ask to learn x. A more conservative way of defining the uncertainty is through the min-entropy: $\mathrm{H}_{\min}(X) = -\log \max_{x \in \mathcal{X}} \Pr[X = x]$. It is related to the probability that one guesses x in a single try.

A natural way of extending these measures to quantum states is to consider the measurement on a quantum state ρ that minimizes the entropy of the resulting classical random variable. For the Shannon entropy this gives the accessible information $\mathrm{H}(X|\rho_x) = \min_{\mathcal{M}} \mathsf{H}(X|\mathcal{M}(\rho_x))$. However, the accessible information is not sufficient to bound Eve's potential knowledge about a classical variable in a cryptographic setting [KRBM07]. The min-entropy of the classical random variable X given the system ρ_x is $\mathrm{H}_{\min}(X|\rho_X) = -\log \max_{\mathcal{M}} \mathbb{E}_{x \in \mathcal{X}} \operatorname{tr}[M_x \rho_x]$ [KRS09]. For the min-entropy a test exists to find the POVM that satisfies the maximum. Let $\Lambda \stackrel{\mathrm{def}}{=} \sum_x \rho_x M_x$. If a POVM can be found that satisfies the condition[3] [Hol73]

$$\forall_{x \in \mathcal{X}} : \ \Lambda - \rho_x \geq 0, \tag{2.11}$$

then there can be no better POVM for guessing X (but equally good POVMs may exist). When X is a binary variable the min-entropy is directly related to the 1-norm. Let $X \in \{0, 1\}$ with probability p_0 that $X = 0$ and $p_1 = 1 - p_0$. Then

$$\mathsf{H}_{\min}(X|\rho_X) \quad = \quad -\log\left(\frac{1}{2} + \frac{1}{2}\operatorname{tr}\left\|p_0\rho_0 - p_1\rho_1\right\|_1\right). \tag{2.12}$$

Our attacker model allows Eve to store a quantum state until there is a more useful moment to perform her measurement, potentially even in a subsequent protocol. It

[3] Reference [Hol73] specifies a second condition, namely $\Lambda^\dagger = \Lambda$. However, the hermiticity of Λ already follows from the condition (2.11).

is therefore useful to consider the uncertainty about a quantum state ρ itself. The von Neumann entropy is the natural extension of the Shannon entropy for quantum states $S(\rho) = -\mathrm{tr}\,\rho\log\rho$. For our *composable* security definitions, it turns out the relevant uncertainty measures are Rényi entropies which are asymptotically related to the von Neumann entropy for factorized states.

The Rényi entropy of a mixed state ρ is defined as

$$\text{For } \alpha \in (0,1)\cup(1,\infty): \quad S_\alpha(\rho) \stackrel{\text{def}}{=} \frac{1}{1-\alpha}\log \mathrm{tr}\,\rho^\alpha, \tag{2.13}$$

where $\alpha = 0$ and $\alpha = \infty$ are defined as the limit behavior $S_0(\rho) = \lim_{\alpha\to 0} S_\alpha(\rho) = \log \mathrm{rank}(\rho)$ and $S_\infty(\rho) = \lim_{\alpha\to\infty} S_\alpha(\rho)$. In the limit $\alpha \to 1$, the Rényi entropy yields the von Neumann entropy.

By allowing states $\bar\rho$ that are ε close to the state ρ in terms of 1-norm, we obtain the ε-smooth Rényi entropy of order α [RK05].

$$\text{For } \alpha \in (0,1)\cup(1,\infty): \qquad S^\varepsilon_\alpha(\rho) \stackrel{\text{def}}{=} \frac{1}{1-\alpha}\log \inf_{\bar\rho:\,\|\bar\rho-\rho\|_1\le\varepsilon} \mathrm{tr}\,\bar\rho^\alpha, \tag{2.14}$$

where the density operator $\bar\rho$ may be sub-normalized.[4] Furthermore we have $S^\varepsilon_0(\rho) = \lim_{\alpha\to 0} S^\varepsilon_\alpha(\rho) = \inf_{\bar\rho:\,\|\bar\rho-\rho\|_1\le\varepsilon} \log\mathrm{rank}(\bar\rho)$ and $S^\varepsilon_\infty(\rho) = \lim_{\alpha\to\infty} S^\varepsilon_\alpha(\rho)$. It has been shown that the smooth Rényi entropy of factor states $\rho^{\otimes n}$ asymptotically approaches the von Neumann entropy.

Lemma 2.1. *Let ρ be a density matrix.*

$$S^\varepsilon_2(\rho^{\otimes n}) \;\ge\; nS(\rho) - (2\log\mathrm{rank}(\rho)+3)\sqrt{n\log\tfrac{2}{\varepsilon}}. \tag{2.15}$$

$$S^\varepsilon_0(\rho^{\otimes n}) \;\le\; nS(\rho) + \mathcal{O}(\sqrt{n\log\tfrac{1}{\varepsilon}}). \tag{2.16}$$

This lemma follows from [Ren05] (Corollary 3.3.7 and the comment above Theorem 3.3.6), combined with $S^\varepsilon_2 \ge S^\varepsilon_\infty$.

2.4 Security notions

Alice and Bob want to communicate confidentially and verifiably authentic. In this thesis we will focus on the secrecy since it relies on the quantum physical properties of our protocols. We rely on a classical tool for the authentication and integrity which we will capture in a single term: correctness. We consider the secrecy of the message by defining encryption. The confidentiallity of the future key material is captured by key recycling and key re-use. For protocols that use updated keys we will define forward secrecy as the confidentiallity of the message when future keys leak. We consider the confidentiallity of the message when all key material becomes public by defining unclonable encryption. All security notations used are composable with other (sub-)protocols.

[4] For finite-dimensional Hilbert spaces, the infimum becomes a minimum.

2.4.1 Encryption

To define the security of a quantum encryption scheme we first define what a quantum encryption scheme is. For simple prepare-and-measure schemes, like the ones presented in this thesis, the classical definition of a private key encryption scheme is a sufficient definition if we allow the ciphertext to be (partially) quantum.

Definition 2.2. *A private key encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$ is a triplet of algorithms (*Gen, Enc, Dec*), where*

1. Gen *is a probabilistic algorithm that generates a key $k = \mathsf{Gen}(1^\lambda)$, $k \in \mathcal{K}$. Here λ is the security parameter.*
2. Enc *is a (possibly randomized) encryption algorithm that takes as input a message $m \in \mathcal{M}$ and outputs a ciphertext $c = \mathsf{Enc}_k(m)$.*
3. Dec *is a decryption algorithm that takes as input a ciphertext c and a key k, and outputs a plaintext $\mathsf{Dec}_k(c)$.*
4. *It holds that $\forall_{m\in\mathcal{M},k\in\mathcal{K}} : \mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$.*

The aim of this chapter is to provide a systematic technique that allows us to prove the security of the protocols presented in Chapters 3 and 4, Chapter 5, Chapter 6 and Chapter 7, which differ from each other quite strongly. We describe the presented schemes as CPTP maps and prove the security in terms of a diamond distance between this map $\mathcal{E}$ and its idealized[5] counterpart $\mathcal{F}$. We will work with a more explicit description of a quantum encryption scheme than Definition 2.2. Our description is general enough to cover all schemes in this thesis. This includes quantum key distribution followed by a one-time pad and a two-way scheme with explicit key leakage. As a result, the description is less elegant than Definition 2.2.

- Instead of describing three algorithms (Gen, Enc, Dec) we describe four CPTP maps (Gen, Enc, Meas, Post). By making the entire scheme a CPTP map, a single diamond distance defines security. CPTP maps are sometimes used to definite quantum encryption schemes [ABW09, AM17, BL20].
- The post-processing is part of the description. Post behaves differently in different security models, e.g. in unclonable encryption keys become public as part of the scheme.
- The encryption can be a shared operation by Alice and Bob (and can depend on their respective random variables) so that two-way schemes are included in the description.
- The message and random variables are generated as part of the scheme. This allows the entire protocol to be described as working on a quantum state only.[6] In addition it forces us to be explicit about the role of random variables. This is important in unclonable encryption.

[5] The form of the idealized map depends on the security property and the attacker model.
[6] This makes it easy to use the post-selection technique, see Section 2.5.5.

- The classical variables that become public during and after the transfer of the quantum states are explicitly distinguished.
- We include the possibility of adversarial actions in our definition of correctness as is the standard in quantum key distribution [PR14].

We distinguish between five types of *classical* variables.

- Random variables that only Alice has access to: $r \in \mathcal{R}_A$.
- Random variables that only Bob has access to: $r' \in \mathcal{R}_B$.
- Shared random keys: $k \in \mathcal{K}$.
- A ciphertext that is available to Eve when attacking the quantum state: $c \in \mathcal{C}$.
- A transcript that is available to Eve after attacking the quantum state: $t \in \mathcal{T}$.

We will work with the following description.

Definition 2.3. *We describe a quantum encryption scheme* QE *with message space* $\mathcal{M}$*, measured payload space* $\mathcal{P}$*, key space* $\mathcal{K}$*, local random variable space at Alice and Bob* $\mathcal{R}_A, \mathcal{R}_B$*, ciphertext space* $\mathcal{C}$*, transcript space* $\mathcal{T}$ *and Hilbert spaces* $\mathcal{H}$ *and* $\mathcal{H}'$ *by the following components working on* $S(\mathcal{H})$*:*

1. *A CPTP map* $\mathsf{QE.Gen}$*:* $1^\lambda \to \mathcal{M} \times \mathcal{K} \times \mathcal{R}_A \times \mathcal{R}_B$*, that generates a message* $m \in \mathcal{M}$*, the shared key material* $k \in \mathcal{K}$ *and local random variables* $r \in \mathcal{R}_A$ *and* $r \in \mathcal{R}_B$ *(the initial quantum state remains untouched),* λ *is the security parameter.*
2. *A CPTP map* $\mathsf{QE.Enc}$*:* $\mathcal{M}\times\mathcal{K}\times\mathcal{R}_A\times\mathcal{R}_B\times\mathcal{S}(\mathcal{H}) \to \mathcal{M}\times\mathcal{K}\times\mathcal{R}_A\times\mathcal{R}_B\times\mathcal{C}\times\mathcal{S}(\mathcal{H}')$ *that takes as input a message* $m \in \mathcal{M}$*, a key* $k \in \mathcal{K}$ *and local random variables* $r \in \mathcal{R}_A$*,* $r' \in \mathcal{R}_B$*, acts on an initial quantum state* $\pi^0 \in \mathcal{S}(\mathcal{H})$*, and outputs a classical ciphertext* $c \in \mathcal{C}$ *and a quantum cipherstate* $\pi_{mkrr'} \in \mathcal{S}(\mathcal{H}')$*. (In addition to* m*,* k*,* r *and* r'*.) We write* $\mathsf{QE.Enc}\Big(|m\rangle\langle m|\otimes|k\rangle\langle k|\otimes|r\rangle\langle r|\otimes|r'\rangle\langle r'|\otimes \pi^0\Big) = |m\rangle\langle m| \otimes |k\rangle\langle k| \otimes |r\rangle\langle r| \otimes |r'\rangle\langle r'| \otimes |c\rangle\langle c| \otimes \pi_{mkrr'}$*.*
3. *A CPTP map* $\mathsf{QE.Meas}$*:* $\mathcal{K} \times \mathcal{R}_B \times \mathcal{C} \times \mathcal{S}(\mathcal{H}') \to \mathcal{K} \times \mathcal{R}_B \times \mathcal{C} \times \mathcal{P}$ *that takes as input a key* $k \in \mathcal{K}$*, local randomness* $r' \in \mathcal{R}_B$*, a classical ciphertext* $c \in \mathcal{C}$ *and a quantum cipherstate* $\pi_{mkrr'} \in \mathcal{S}(\mathcal{H}')$*, and outputs a received payload* $p \in \mathcal{P}$*. (The* k, r' *and* c *are not modified.) The POVM operators at given* k, r' *are written as* $D_p^{kr'}$*, with* $\forall_{k,r'} \sum_{p\in\mathcal{S}(\mathcal{P})} D_p^{kr'} = \mathbb{1}$*.*
4. *A CPTP map* $\mathsf{QE.Post}$*:* $\mathcal{M} \times \mathcal{K} \times \mathcal{R}_A \times \mathcal{R}_B \times \mathcal{C} \times \mathcal{P} \to \mathcal{M} \times \mathcal{M}' \times \mathcal{K} \times \mathcal{C} \times \mathcal{T}$ *that takes the message* $m \in \mathcal{M}$*, key* $k \in \mathcal{K}$*, local randomness* $r \in \mathcal{R}_A$ *and* $r' \in \mathcal{R}_B$*, classical ciphertext* $c \in \mathcal{C}$ *and received payload* $p \in \mathcal{P}$ *as input and outputs a message* $m' \in \mathcal{M}'$ *and a classical transcript* $t \in \mathcal{T}$ *(*m, c *are not modified,* k, r, r' *can be deleted, output or made public,* p *is deleted). Here we have defined* $\mathcal{M}' = \mathcal{M} \cup \{\perp\}$*.*

The initial Hilbert space $\mathcal{H}$ can be used by Alice to prepare a state to sent to Bob. It can also be an EPR pair on which Alice performs a measurement while the remaining half is sent to Bob. Without loss of generality we write $\pi^0 = |0\rangle\langle 0|$. The actions of Alice, Eve and Bob are described as follows. In $\mathsf{QE.Gen}$, Alice and Bob generate a shared key k. They generate uniform randomness r and r' locally (independent of k). Alice draws a plaintext message m from a distribution that is not necessarily uniform, and not necessarily known to Alice.[7] Alice applies $\mathsf{QE.Enc}$[8], yielding cipherstate $|c\rangle\langle c| \otimes \pi_{mkrr'}$ which she sends to Bob.

Eve intercepts $|c\rangle\langle c| \otimes \pi_{mkrr'}$. Eve entangles a quantum state of her own with $\pi_{mkrr'}$, resulting in a state $|c\rangle\langle c| \otimes \rho^{\mathrm{BE}}_{mkrr'c} = U(|c\rangle\langle c| \otimes \pi_{mkrr'} \otimes |e\rangle\langle e|)$, where $|e\rangle$ is the initial state of Eve's quantum system and U is a unitary operation[9]. The label 'B' and 'E' stand for the subsystems of Bob and Eve respectively. The above procedure, with postponed measurement on the E system, is the most general action possible for Eve, and comprises options like e.g. copying classical information, or completely keeping $\pi_{mkrr'c}$. Eve's overall action can be written as a CPTP map $\mathcal{A}$ which acts as $(\mathcal{A} \circ \mathsf{QE.Enc})\Big(|mkrr'0e\rangle\langle mkrr'0e|\Big) = |mkrr'c\rangle\langle mkrr'c| \otimes \rho^{\mathrm{BE}}_{mkrr'c}$. Bob acts on the 'B' part of $\rho^{\mathrm{BE}}_{mkrr'c}$ with $\mathsf{QE.Meas}$ yielding $p \in \mathcal{P}$ which we refer to as the received payload. Note that the payload Alice encodes (depending on r, m, k) can be different from the received payload p measured by Bob.

In the post-processing $\mathsf{QE.Post}$, Alice and Bob can communicate over a classical channel or publish some of their local randomness or keys. In this process Eve obtains the transcript T consisting of these classical variables. Bob outputs his attempt to recover m by computing m'. We treat T as an additional output of the protocol. Alice and Bob delete all other variables.

This whole sequence of events results in a final state that we refer to as the *output* of the scheme, $(\mathsf{QE.Post}\circ\mathsf{QE.Meas}\circ\mathcal{A}\circ\mathsf{QE.Enc})\big(\sum_{mm'kct} \frac{\Pr[M=m]}{|\mathcal{K}||\mathcal{R}_A||\mathcal{R}_B|}|mkrr'0e\rangle\langle\cdots|\big) = \mathbb{E}_{mm'kctrr'}\,|mm'kt\rangle\langle\cdots| \otimes \sum_p \mathrm{tr}_B(D_p^{krr'}|c\rangle\langle c| \otimes \rho^{\mathrm{BE}}_{mkrr'c}) \stackrel{\mathrm{def}}{=} \mathbb{E}_{mm'kctrr'}\,|mm'kt\rangle\langle\cdots| \otimes \sum_p (\mathrm{tr}\, D_p^{krr'}|c\rangle\langle c| \otimes \rho^{\mathrm{BE}}_{mkrr'c})\rho^{\mathrm{E}}_{mkrr'cp} = \rho^{MM'KCTE}$. Where we write m, m', k, c, t as subsystems of a large classical-quantum state. A general quantum encryption protocol is shown in Figure 2.1. The timing is flexible, it might happen that Alice's post-precessing already happens before Bob performed his measurement.

Correctness of quantum encryption

At the end of the protocol Alice holds her message m and Bob holds his received message m'. A protocol is ε-correct when the probability that m and m' differ and Alice and Bob believe their communication was successful is smaller than ε: $\Pr[m \neq m', \mathrm{accept}] \leq \varepsilon$. All our protocols use a classical MAC to guarantee the authenticity of the plaintext message. Let the message m consist of a plaintext μ and a tag $\tau = \Gamma(k_{\mathrm{MAC}}, \mu)$, where Γ is the MAC function and k_{MAC} a key of size 2λ. Bob's

[7] This includes a probability distribution that is peaked around a single m. Potentially it is known to Eve and it can obtained from a outside source.

[8] As we will see in Chapter 6, the encryption step can also include a preparation step by Bob. In that case, Eve can already be entangled to the initial state π^0.

[9] In general Eve could modify c. We don't explicitly describe Eve's actions on the classical variables c, t. We rely on classical authentication tags to guarantee they remain unmodified.

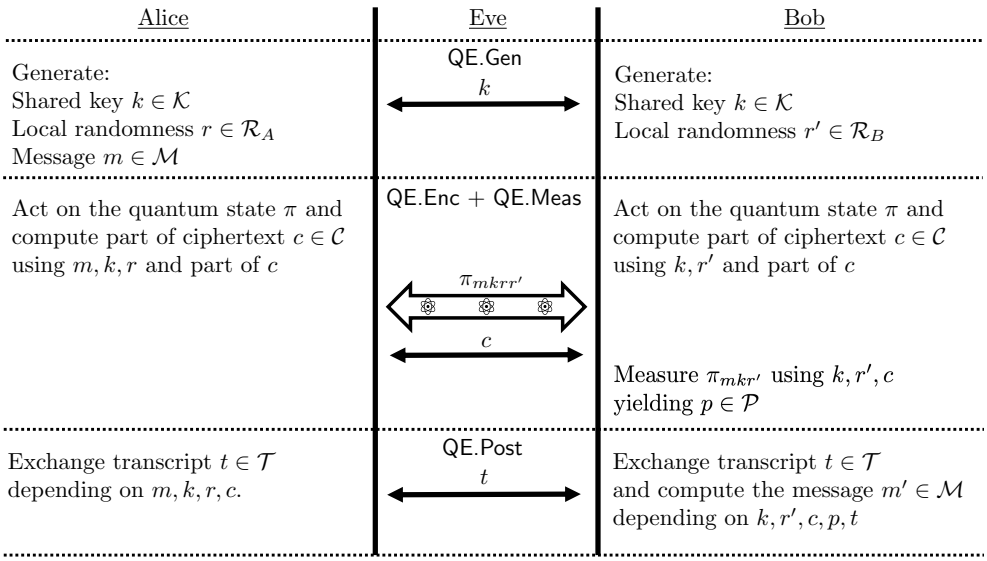

Figure 2.1: A general quantum encryption protocol.

reconstructed message is then $\hat{m} = \hat{\mu} \| \hat{\tau}$. Bob only accepts when his reconstructed tag successfully authenticates the reconstructed plaintext $\hat{\tau} == \Gamma(k_{\mathrm{MAC}}, \hat{\mu})$. The property of the information-theoretically secure MAC and Eve's ignorance of the MAC key then guarantees $\Pr[m \neq \hat{m}, \mathrm{accept}] \leq 2^{-\lambda}$ (see Section 2.2.4). The protocol is $2^{-\lambda}$-correct due to a classical MAC, we say the correctness is guaranteed by the classical authentication.

Let Ω denote the success of the protocol as determined by Bob. We refer to $\Omega = 1$ as the accept case and $\Omega = 0$ as the reject case. We define $\rho^{\mathrm{E}}_{\mathtt{accept}}$ and $\rho^{\mathrm{E}}_{\mathtt{reject}}$ by $\rho^{\Omega \mathrm{E}} = |\omega = 1\rangle\langle\omega = 1| \otimes \rho^{\mathrm{E}}_{\mathtt{accept}} + |\omega = 0\rangle\langle\omega = 0| \otimes \rho^{\mathrm{E}}_{\mathtt{reject}}$. It holds that $\operatorname{tr} \rho^{\mathrm{E}}_{\mathtt{accept}} = \Pr[\Omega = 1 | \rho^{\mathrm{E}}]$ and $\operatorname{tr} \rho^{\mathrm{E}}_{\mathtt{reject}} = \Pr[\Omega = 0 | \rho^{\mathrm{E}}]$. The transcript often contains the 'feedback bit' Ω.

A quantum encryption scheme according to Definition 2.3 with output $\rho^{MM'KC\mathrm{T}\mathrm{E}}$ then has $\| \rho^{MM'KC\mathrm{T}\mathrm{E}}_{\mathtt{accept}} - \rho^{MMKC\mathrm{T}\mathrm{E}}_{\mathtt{accept}} \|_1 \leq 2^{-\lambda}$. We will not write the double M space anymore. Instead we just write $\rho^{MKC\mathrm{T}\mathrm{E}}_{\mathtt{accept}}$. When Bob rejects he knows $m' \neq m$ so he might as well delete m'. We can then trace out M' and write $\rho^{MKC\mathrm{T}\mathrm{E}}_{\mathtt{reject}}$.

In our security definitions, we do not consider m' as separate output. This is allowed at the cost of a factor $2^{-\lambda}$ to the overall error of the protocol. Similarly, we do not consider Eve modifying authenticated classical messages. She could do so, but the probability that this goes unnoticed is $2^{-\lambda}$. It is understood that each time we ignore the failure probability of the classical MAC, this adds a term $2^{-\lambda}$ to the security parameter in the sense discussed in Section 2.4.4.

Security definition of encryption

We define confidentiallity as the inability of the attacker to determine the message m when observing the protocol once without having access to the shared key material k and local randomness r, r'. From Section 2.3.7, we know that the maximum probability of distinguishing two CPTP maps is directly related to the diamond distance between them. We define the security of encryption as the diamond distance between a protocol $\mathcal{E}_{\mathrm{ENC}}$ and an idealized version of the protocol $\mathcal{F}_{\mathrm{ENC}}$, where the message M is decoupled from Eve's state.

Let $\mathcal{E}_{\mathrm{ENC}}$ describe a quantum encryption protocol as in Definition 2.3 where as a final step Alice and Bob delete their key material k. The output of the CPTP map is then[10] $\mathcal{E}_{\mathrm{ENC}}(|0e\rangle\langle 0e|) = \rho^{MCT\mathrm{E}}$. Ideally the output is completely decoupled from the message. The corresponding ideal map $\mathcal{F}_{\mathrm{ENC}}$ has output $\mathcal{F}_{\mathrm{ENC}}(|0e\rangle\langle 0e|) = \rho^{\mathrm{M}} \otimes \rho^{CT\mathrm{E}}$. The diamond distance $\|\mathcal{E}_{\mathrm{ENC}} - \mathcal{F}_{\mathrm{ENC}}\|_\diamond$ motivates our security definition for encryption.

Definition 2.4. *Let* QE *be a quantum encryption scheme according to Definition 2.3 with output state* $\rho^{MM'KCT\mathrm{E}} = (\mathsf{QE.Post} \circ \mathsf{QE.Meas} \circ \mathcal{A} \circ \mathsf{QE.Enc})(\sum_{mkr} \frac{\Pr[M=m]}{|\mathcal{K}||\mathcal{R}|} |mkr0e\rangle\langle mkr0e|)$ *as described above.* QE *is called* ε*-encrypting (*ε*-ENC) if the output satisfies*

$$\|\rho^{MCT\mathrm{E}} - \rho^{M} \otimes \rho^{CT\mathrm{E}}\|_1 \leq \varepsilon \tag{2.17}$$

for all adversarial actions $\mathcal{A}$ *and all distributions of* M*.*

Note that Definition 2.4 demands that (2.17) holds for all distributions of M; hence it implies other security definitions used in the literature which work with '$\forall_m$' conditions. Security definitions in terms of diamond norms are the state of the art for QKD protocols [PR14]. In QKD, the definition of encryption only needs to consider the accept case [Ren05, TL17] since there is no chance of leaking the message in the reject case. For protocols that send the message and the quantum states in a single pass, message confidentiality in case of reject needs to be guaranteed as well. Quantum key recycling and unclonable encryption protocols typically send the message and the quantum states together.

2.4.2 Key recycling and re-use

A quantum key recycling scheme (QKR) not only encrypts a message, but also protects some of the key material for future use. Mathematically, it is a quantum encryption scheme that additionally outputs some key material. We will use the following description.

Definition 2.5. *We describe a quantum key recycling scheme (QKR) with message space* $\mathcal{M}$*, received payload space* $\mathcal{P}$*, key spaces* $\mathcal{K}$*,* $\tilde{\mathcal{K}}$*, local random variable space at Alice and Bob* $\mathcal{R}_A, \mathcal{R}_B$*, ciphertext space* $\mathcal{C}$*, transcript space* $\mathcal{T}$ *and Hilbert spaces* $\mathcal{H}$ *and* $\mathcal{H}'$ *by the following components working on* $S(\mathcal{H})$*:*

[10] Recall that $\pi^0 = |0\rangle\langle 0|$ and Eve's initial quantum state is $|e\rangle\langle e|$.

1. *A CPTP map* $\mathsf{QKR.Gen}\colon 1^\lambda \to \mathcal{M}\times\mathcal{K}\times\mathcal{R}_A\times\mathcal{R}_B$*, that generates a message* $m\in\mathcal{M}$*, the shared key material* $k\in\mathcal{K}$ *and local random variables* $r\in\mathcal{R}_A$ *and* $r\in\mathcal{R}_B$*,* λ *is the security parameter.*

2. *A CPTP map* $\mathsf{QKR.Enc}\colon \mathcal{M}\times\mathcal{K}\times\mathcal{R}_A\times\mathcal{R}_B\times\mathcal{S}(\mathcal{H})\to\mathcal{M}\times\mathcal{K}\times\mathcal{R}_A\times\mathcal{R}_B\times\mathcal{C}\times\mathcal{S}(\mathcal{H}')$ *that takes as input a message* $m\in\mathcal{M}$*, a key* $k\in\mathcal{K}$ *and local random variables* $r\in\mathcal{R}_A$*,* $r'\in\mathcal{R}_B$*, acts on an initial quantum state* $\pi^0\in\mathcal{S}(\mathcal{H})$*, and outputs a classical ciphertext* $c\in\mathcal{C}$ *and a quantum cipherstate* $\pi_{mkrr'}\in\mathcal{S}(\mathcal{H}')$*. (In addition to* m*,* k*,* r *and* r'*.) We write* $\mathsf{QKR.Enc}\Big(|m\rangle\langle m|\otimes|k\rangle\langle k|\otimes|r\rangle\langle r|\otimes|r'\rangle\langle r'|\otimes\pi^0\Big)=|m\rangle\langle m|\otimes|k\rangle\langle k|\otimes|r\rangle\langle r|\otimes|r'\rangle\langle r'|\otimes|c\rangle\langle c|\otimes\pi_{mkrr'}$.

3. *A CPTP map* $\mathsf{QKR.Meas}\colon \mathcal{K}\times\mathcal{R}_B\times\mathcal{C}\times\mathcal{S}(\mathcal{H}')\to\mathcal{K}\times\mathcal{R}_B\times\mathcal{C}\times\mathcal{P}$ *that takes as input a key* $k\in\mathcal{K}$*, local randomness* $r'\in\mathcal{R}_B$*, a classical ciphertext* $c\in\mathcal{C}$ *and a quantum cipherstate* $\pi_{mkrr'}\in\mathcal{S}(\mathcal{H}')$*, and outputs a received payload* $p\in\mathcal{P}$*. (The* k, r' *and* c *are not modified.) The POVM operators at given* k, r' *are written as* $D_p^{kr'}$*, with* $\forall_{k,r'}\sum_{p\in\mathcal{S}(\mathcal{P})}D_p^{kr'}=\mathbb{1}$.

4. *A CPTP map* $\mathsf{QKR.Post}\colon \mathcal{M}\times\mathcal{K}\times\mathcal{R}_A\times\mathcal{R}_B\times\mathcal{C}\times\mathcal{P}\to\mathcal{M}\times\mathcal{M}'\times\mathcal{K}\times\tilde{\mathcal{K}}\times\tilde{\mathcal{K}}\times\mathcal{C}\times\mathcal{T}$ *that takes the message* $m\in\mathcal{M}$*, key* $k\in\mathcal{K}$*, local randomness* $r\in\mathcal{R}_A$ *and* $r'\in\mathcal{R}_B$*, classical ciphertext* $c\in\mathcal{C}$ *and received payload* $p\in\mathcal{P}$ *as input and outputs a message* $m'\in\mathcal{M}'$*, a new key at Alice and Bob* $\tilde{k}\in\tilde{\mathcal{K}}$*,* $\tilde{k}'\in\tilde{\mathcal{K}}$ *and a transcript* $t\in\mathcal{T}$ *(*m, c *are not modified,* k, r, r' *can be deleted, output or made public,* p *is deleted). Here we have defined* $\mathcal{M}'=\mathcal{M}\cup\{\perp\}$.

Quantum key recycling differs from quantum encryption in the output of a new key $\tilde{k}\in\tilde{\mathcal{K}}$ at Alice and one at Bob's lab $\tilde{k}'\in\tilde{\mathcal{K}}$ in the post-processing phase. Similar to the quantum encryption procedure the output is given by $\rho^{MM'K\tilde{K}\tilde{K}'CTE}=(\mathsf{QKR.Post}\circ\mathsf{QKR.Meas}\circ\mathcal{A}\circ\mathsf{QKR.Enc})(\sum_{mkr}\frac{\Pr[M=m]}{|\mathcal{K}||\mathcal{R}|}|mkr0e\rangle\langle mkr0e|)$. Usually the key update depends on a flag ω that is set to $\omega=0$ (reject) if $m'=\perp$ and to $\omega=1$ (accept) if $m'\in\mathcal{M}$ and a channel noise test is passed. When the protocol yields reject because there was too much noise on the quantum channel, at least $\log|\mathcal{M}|$ bit of key material need to be refreshed [DPS05]. In the accept case there is no such minimum. The flag ω is usually part of the transcript. The general quantum key recycling protocol is shown in Figure 2.2.

Definition 2.6. *Let* QKR *be a quantum key recycling scheme according to Definition 2.5 that uses key material* K*. Let* $\tilde{K}_{\mathtt{accept}}, \tilde{K}'_{\mathtt{accept}}$ *be the future keys at Alice and Bob's labs respectively after a successful instance of* QKR*.* QKR *is called a quantum key re-use scheme if* $\tilde{K}_{\mathtt{accept}}=\tilde{K}'_{\mathtt{accept}}=K$.

Correctness of key recycling

Correctness in the context of quantum key recycling means that we have $\Pr[m\neq m', \text{accept}]\leq\varepsilon$ and that there is no discrepancy between the future keys of Alice and Bob $\tilde{k}=\tilde{k}'$. The correctness of the message is guaranteed by the tag as discussed in Section 2.4.1. In general the future keys can be a function of old keys K, the public information C, T the messages M, M' and the qubit payload which is part of Alice's

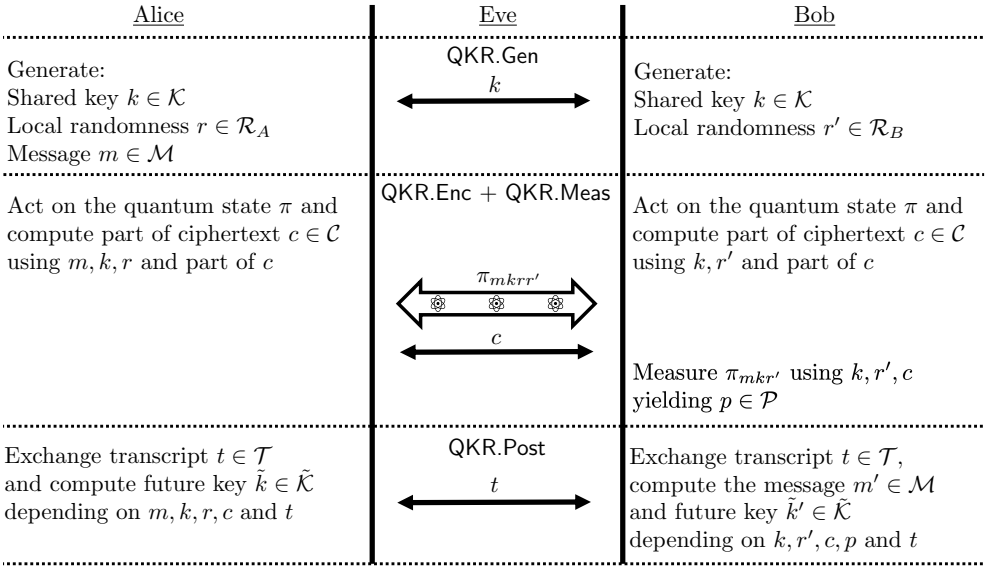

Figure 2.2: A general quantum key recycling protocol.

local randomness R and Bob's measurement result P. The key update procedures considered in this thesis will always update K such that the probability that $\tilde{k} \neq \tilde{k}'$ is bounded by $2^{-\lambda}$. Either Alice and Bob only use their previous key K or they use strings which are equal with a probability of at least $1 - 2^{-\lambda}$ (indirectly) guaranteed by an information theoretically secure MAC function. We use a simplified output with $\tilde{k} = \tilde{k}'$ so that $\tilde{k}'$ can be left out of the expression.

Security definition of key recycling

Let $\mathcal{E}_{\mathrm{KR}}$ describe a quantum key recycling protocol according to Definition 2.5, where in the final step Alice and Bob delete their old key material K. The output of the protocol is given by $\mathcal{E}_{\mathrm{KR}}(|0e\rangle\langle 0e|) = \rho^{M\tilde{K}CT\mathrm{E}}$. The ideal key recycling mapping has the future key $\tilde{K}$ completely decoupled from the state held by Eve. The $\tilde{k}$ has to be secure even if Eve has (partial or complete) knowledge of the message M. We leave the coupling of Eve's state to the message in tact. The corresponding map is $\mathcal{F}_{\mathrm{KR}}(|0e\rangle\langle 0e|) = \rho^{\tilde{K}} \otimes \rho^{MCT\mathrm{E}}$. The diamond distance $\|\mathcal{E}_{\mathrm{KR}} - \mathcal{F}_{\mathrm{KR}}\|_\diamond$ motivates the following definition.

Definition 2.7. *Let* QKR *be a quantum key recycling scheme according to Definition 2.5 with output state* $\rho^{MM'K\tilde{K}\tilde{K}'CT\mathrm{E}} =$ $(\mathsf{QKR.Post} \circ \mathsf{QKR.Meas} \circ \mathcal{A} \circ \mathsf{QKR.Enc})(\sum_{mkr} \frac{\Pr[M=m]}{|\mathcal{K}||\mathcal{R}|} |mkr0e\rangle\langle mkr0e|)$ *as described above.* QKR *is called* ε*-recycling (*ε*-KR) if it satisfies*

$$\|\rho^{M\tilde{K}CT\mathrm{E}} - \rho^{\tilde{K}} \otimes \rho^{MCT\mathrm{E}}\|_1 \leq \varepsilon \tag{2.18}$$

for all adversarial actions $\mathcal{A}$ and all distributions of M.

Note that other definitions of key recycling exist than the one given in Definition 2.7. For instance, [FS17] has a recycling definition that allows Eve to obtain some information about part of the key (the measurement basis), as long as the min-entropy is high enough. Our definitions of encryption and key recycling allow us to treat all keys as well as the message in the same way.

Communication rate

A protocol is more efficient, in the sense described below, if Alice and Bob do not use up a lot of key material. The number of expended key bits is $\Delta K = |K| - |\tilde{K}|$. One way to achieve $\Delta K = 0$ is by sending new key material as part of the message. On the other extreme, all key material can be used to send a larger message by using all key material as a one-time pad such that $|\tilde{K}| = 0$. We will speak of the (communication) rate of a protocol. The rate is positive when more bits of information are communicated than used up. We use the following definition of rate:

Definition 2.8 (Rate)**.** *Let* QKR *be a quantum key recycling scheme that uses n quantum states, is ε-encrypting and ε'-recycling with message space $\mathcal{M}$ and key spaces $\mathcal{K}$ and $\tilde{\mathcal{K}}$. Let λ be the security parameter and let $\Delta K = \log|\mathcal{K}| - \log|\tilde{\mathcal{K}}|$ be the expended amount of key material in the accept case. For $|\mathcal{M}|$ and $|\tilde{\mathcal{K}}|$ such that $\varepsilon + \varepsilon' \leq 2^{-\lambda}$, the rate of* QKR *is*

$$\text{rate} = \frac{\log|\mathcal{M}| - \Delta K}{n}. \tag{2.19}$$

We consider $|\mathcal{M}|$ and ΔK for which $\varepsilon, \varepsilon'$ become exponentially small. For asymptotic results we do not explicitly consider the value of λ.

Security definition of forward secrecy

The security of a given round of a QKR scheme should not be compromised by potential key leakage in future rounds. A protocol in which a compromise of future keys does not affect the security of the message of previous rounds is said to have (perfect) forward secrecy[11] [DVOW92]. Let $\mathcal{E}_{\text{FS}} = \mathcal{E}_{\text{KR}}$ be the same map as before. The ideal behavior of a scheme with forward secrecy decouples the message without decoupling the future keys $\mathcal{F}_{\text{FS}}(|0e\rangle\langle 0e|) = \rho^M \otimes \rho^{\tilde{K}CTE}$. The diamond distance $\|\mathcal{E}_{\text{FS}} - \mathcal{F}_{\text{FS}}\|_\diamond$ motivates the following definition of forward secrecy.

Definition 2.9. *Let* QKR *be a quantum key recycling scheme according to Definition 2.5 with output state $\rho^{MM'K\tilde{K}\tilde{K}'CTE} =$*
$(\mathsf{QKR.Post} \circ \mathsf{QKR.Meas} \circ \mathcal{A} \circ \mathsf{QKR.Enc})(\sum_{mkr} \frac{\Pr[M=m]}{|\mathcal{K}||\mathcal{R}|} |mkr0e\rangle\langle mkr0e|)$ as described above. QKR *is called forward secret with error ε (ε-FS) if it satisfies*

$$\|\rho^{M\tilde{K}CTE} - \rho^M \otimes \rho^{\tilde{K}CTE}\|_1 \leq \varepsilon \tag{2.20}$$

for all adversarial actions $\mathcal{A}$ and all distributions of M.

[11] The name forward secrecy refers to the secrecy of past messages, backward secrecy would arguably be more intuitive name.

The following lemma allows us to prove encryption, key recycling and forward secrecy by bounding a single 1-norm.

Lemma 2.10. *A* QKR *scheme with output state* $\rho^{MM'K\tilde{K}\tilde{K}'CTE}$ *is* ε*-encrypting,* 2ε*-recycling and forward secret with error* 2ε *if it satisfies*

$$\|\rho^{M\tilde{K}CTE} - \rho^{M} \otimes \rho^{\tilde{K}} \otimes \rho^{CTE}\|_1 \leq \varepsilon. \tag{2.21}$$

Proof: Taking the lhs of (2.21) and tracing over $\tilde{K}$ yields ε-ENC. Furthermore, using the triangle inequality we write $\|\rho^{M\tilde{K}CTE} - \rho^{\tilde{K}} \otimes \rho^{MCTE}\|_1 \leq \|\rho^{M\tilde{K}CTE} - \rho^{M} \otimes \rho^{\tilde{K}} \otimes \rho^{CTE}\|_1 + \|\rho^{M} \otimes \rho^{\tilde{K}} \otimes \rho^{CTE} - \rho^{\tilde{K}} \otimes \rho^{MCTE}\|_1$. Both terms individually are bounded by ε due to (2.21); the first term directly, the second term after taking the $\tilde{K}$-trace of both density matrices and using that the partial trace like any CPTP map can not increase trace distance [NC11]. This proves 2ε-KR. Similarly, we can write $\|\rho^{M\tilde{K}CTE} - \rho^{M} \otimes \rho^{\tilde{K}CTE}\|_1 \leq \|\rho^{M\tilde{K}CTE} - \rho^{M} \otimes \rho^{\tilde{K}} \otimes \rho^{CTE}\|_1 + \|\rho^{M} \otimes \rho^{\tilde{K}} \otimes \rho^{CTE} - \rho^{M} \otimes \rho^{\tilde{K}CTE}\|_1$ and bound both terms by the lhs of (2.21), directly and by taking the trace over M. This proves 2ε-FS. □

2.4.3 Unclonable encryption

A stronger notion of encryption was first considered by Gottesman in 2003 [Got03]. This notion aims to guarantee the security of the message M when the key material K leaks after the protocol is finished. Protocols that provide this functionality when the message is transferred successfully are called unclonable encryption protocols. In the reject case, leaking all key material will always compromise the encryption of the message.

Let the map $\mathcal{E}_{\text{uncl}}$ describe a QE scheme with output state $\mathcal{E}_{\text{uncl}}(|0e\rangle\langle 0e|) = \rho^{MKCTE} = \rho^{MKCTE}_{\texttt{accept}} + \rho^{MKCTE}_{\texttt{reject}}$. Where $\rho^{MKCTE}_{\texttt{accept}}$ and $\rho^{MKCTE}_{\texttt{reject}}$ denote the states corresponding to accept and reject respectively. The ideal behavior of an unclonable encryption protocol decouples the message in the accept case. In the corresponding ideal map we leave the reject part unchanged with respect to $\mathcal{E}_{\text{uncl}}$. This ideal map is $\mathcal{F}_{\text{uncl}}(|0e\rangle\langle 0e|) = \rho^{M} \otimes \rho^{KCTE}_{\texttt{accept}} + \rho^{MKCTE}_{\texttt{reject}}$. The diamond norm $\|\mathcal{E}_{\text{uncl}} - \mathcal{F}_{\text{uncl}}\|_\diamond$ motivates our definition of unclonable encryption.

Definition 2.11. *Let* QE *be a quantum encryption scheme according to Definition 2.3 with output state*
$\rho^{MM'KCTE} = (\mathsf{QE.Post} \circ \mathsf{QE.Meas} \circ \mathcal{A} \circ \mathsf{QE.Enc})(\sum_{mkr} \frac{\Pr[M=m]}{|\mathcal{K}||\mathcal{R}|} |mkr0e\rangle\langle mkr0e|)$. QE *is called* ε*-unclonable (*ε*-UE) if it satisfies*

$$\|\rho^{MKCTE}_{\texttt{accept}} - \rho^{M} \otimes \rho^{KCTE}_{\texttt{accept}}\|_1 \leq \varepsilon \tag{2.22}$$

for all adversarial actions $\mathcal{A}$ *and all distributions of* M*.*

The definition of unclonable encryption for a quantum key recycling scheme has the same requirement as (2.22) for the output of the key recycling scheme.

Intuitively, Definition 2.11 states that either the accept probability is low due to Eve's interference, or else Eve's posterior distribution of M, given that k leaks after completion of an accepted protocol run, is hardly distinguishable from the prior

distribution. This UE definition specifies no requirement for the reject case, since the ENC property already exists to keep M safe in case of reject (even if Eve keeps the whole cipherstate).

Gottesman's original definition of unclonable encryption [Got03] states that for a fraction $\geq 1-\varepsilon$ of keys $k \in \mathcal{K}$ and for all pairs $m, m' \in \mathcal{M}$, $m' \neq m$ it holds that $\|\rho^{\mathrm{E}}_{mkt,\mathtt{accept}} - \rho^{\mathrm{E}}_{m'kt,\mathtt{accept}}\|_1 \leq \varepsilon$. This property is implied by Definition 2.11.[12]

Our preference for our KR and UE definitions stems from (i) the fact that they allow for a unified treatment of all the components[13] of k; (ii) compatibility with the technique of [Ren05], which makes it possible to prove security of high-rate schemes; (iii) having the same type of definition for UE and KR. Furthermore our KR definition is compatible with [DPS05].

An alternative definition of unclonable encryption exists [BL20], with two collaborating adversaries who attempt to both recover the plaintext. In addition to the difference in definition, they consider the use of quantum pseudorandom functions to improve their bound while we remain information-theoretic. What Gottesman called unclonable encryption they re-label to Tamper-Evident Encryption. The precise relationship between the two definitions of unclonable encryption unknown.

2.4.4 Composability

Our security notions based on diamond distances guarantee composability [Ren05, PR14]. Two protocols that are secure according to our security notions will also be secure when executed in succession. The failure probability of the two protocols in succession is bounded by the sum of their individual failure probabilities. Composability is crucial for key recycling as well as for key distribution. A future protocol using a recycled key relies on the composable security of the previous protocol. Similar the secure use of an established key using QKD relies on the composable security of QKD. In general composability allows protocols to be useful as a part in a larger system. The following lemma shows composability holds for diamond norms in general.

Lemma 2.12. *For any CPTP maps $\mathcal{A}, \mathcal{A}', \mathcal{B}, \mathcal{B}'$, it holds that*

$$\|\mathcal{A}\circ\mathcal{B} - \mathcal{A}'\circ\mathcal{B}'\|_\diamond \quad\leq\quad \|\mathcal{A}-\mathcal{A}'\|_\diamond + \|\mathcal{B}-\mathcal{B}'\|_\diamond. \tag{2.23}$$

Proof:

$$\begin{aligned}
\|\mathcal{A}\circ\mathcal{B} - \mathcal{A}'\circ\mathcal{B}'\|_\diamond &= \|\mathcal{A}\circ\mathcal{B} - \mathcal{A}'\circ\mathcal{B}' + \mathcal{A}'\circ\mathcal{B} - \mathcal{A}'\circ\mathcal{B}\|_\diamond && (2.24)\\
&\leq \|(\mathcal{A}-\mathcal{A}')\circ\mathcal{B}\|_\diamond + \|\mathcal{A}'\circ(\mathcal{B}-\mathcal{B}')\|_\diamond && (2.25)\\
&\leq \|\mathcal{A}-\mathcal{A}'\|_\diamond + \|\mathcal{B}-\mathcal{B}'\|_\diamond && (2.26)
\end{aligned}$$

where the last inequality holds because a CPTP map can never increase the trace distance (Theorem 9.2 in [NC11]). □

Composability is also used to deal with imperfection of the MAC function used by Alice and Bob. An elegant way to avoid computational complications is to describe

[12] (i) For the specific values m, m' the same reasoning applies as with Definition 2.4. (ii) Our definition works with an average over k, and hence the desired $\|\cdots\|_1 \leq \varepsilon$ property may fail to hold for a fraction ε of all values $k \in \mathcal{K}$. This is the same fraction as in Gottesman's definition.

[13] e.g. measurement basis, MAC key, and seeds for hash functions.

the classical channel as a channel that is perfectly authenticated (Eve only listens) except with probability $2^{-\lambda}$, where $2^{-\lambda}$ is the failure probability of the MAC. If the protocol has security ε in case of a perfectly authenticated classical channel, then the real-life security is $\varepsilon + 2^{-\lambda}$. It was shown in Appendix D of [PR14] that this is true for parallel classical authentication and quantum encoding.

2.5 Proof recipe

The general proof structure described in this section is the one used for all protocols discussed in this thesis. This technique applies many aspects from the proof method of Renner [Ren05, RK05] in such a way that they are applicable to many types of scenarios such as quantum key recycling and unclonable encryption. The aim is always to bound the diamond norm between the CPTP map describing the protocol and its ideal counterpart. The bound on the diamond norm implies the security properties introduced in Section 2.4. The recipe consists of 6 steps:

1. Construct an EPR version of the protocol.
2. Construct an equivalent protocol that exploits the symmetries present in the scheme, including a permutation of the quantum states.
3. Describe the functionality of the protocol and its ideal counterpart in terms of CPTP maps $\mathcal{E}$ and $\mathcal{F}$ and derive the relevant 1-norms from their diamond distance $\|\mathcal{E} - \mathcal{F}\|_\diamond$.
4. Introduce smooth states and bound the 1-norms in terms of quantum entropies or simple expressions.
5. Use the post-selection technique to describe Eve's state in factorized form.
6. Use the symmetrization operations, introduced in step 2. Find a simple description of Eve's most general factorized state satisfying the constraints enforced by the protocol and compute the relevant expressions or entropies.

In the explanation of the steps we will often consider the example of Alice sending qubits to Bob. The same proof recipe applies more generally, e.g for high dimensional qudit or for multiple passes over the quantum channel.

2.5.1 Step 1: equivalent EPR protocol

As discussed in Section 2.3.3, preparation of an EPR pair and measuring one half is equivalent to preparing a random quantum state. Let Alice create n EPR pairs described by ρ^{AB}. She measures the subsystem A, consisting of half of each pair, and sends the remaining subsystem B to Bob. Bob receives the same state and performs the same actions as in the original protocol. If Alice wished to send a *specific value* x, she sends along a ciphertext that is a function of x and her measurement result. For qubits, she measures the bit s and sends along $a = s \oplus x$. Because s is random, a does not tell Eve anything about x.

Eve can create an auxiliary system of her own. Eve's subsystem E can be taken to be, without loss of generality, a Hilbert space of dimension d^{2n} where d is the dimension of the quantum states sent to Bob (d=2 for qubits). Eve can entangle her ancilla with the ρ^{AB} system with a unitary operation forming the state ρ^{ABE}. The protocol executed by Alice and Bob is then described by actions on the AB part of ρ^{ABE}.

The equivalence between prepare-and-measure on the one hand and the EPR mechanism on the other hand has been exploited in many works e.g. [SP00, Ren05].

2.5.2 Step 2: security-equivalent protocol using symmetrization

We construct an equivalent protocol to the EPR version by adding operations that do not affect the security of the protocol and that emphasize the symmetries present in the protocol. The output of the CPTP map describing the EPR version and the equivalent protocol is (almost[14]) the same. Most common are permutation invariance and the invariance to random Pauli operators. These invariances allow us to give a simpler description of the state held by Eve in steps 5 and 6. As the last modification, we let Eve instead of Alice create the EPR pairs.

Permutation invariance

We will be working with protocols that are invariant under permutation of the EPR pairs that were introduced in step 1. On Alice's side the invariance is obvious since she creates n EPR pairs independently. On Bob's side the effect of a permutation is a reordering of the noise in the quantum states. However, in all the protocols that we study Bob performs an error correction step. The error correcting codes used in our protocols are always invariant to the position of the errors. The output variables computed after the error correction step are independent of the noise position and therefore independent of the random permutation. In order to make the permutation invariance obvious, we explicitly add the permutation to the protocol. This symmetry will be exploited in step 5.

Pauli invariance

The 4- and 6-state encodings discussed in Section 2.3.2 are replaced by measurements in the x-, y- and z-basis in the EPR setting. Before applying this measurement, let Alice and Bob generate a public random number $\alpha \in \{0, 1, 2, 3\}$ and apply the corresponding Pauli operator σ_α. From Section 2.3.5 we know the effect on a qubit is a phase and/or bit flip. Hence, the random Pauli causes a random bit flip in Alice's measurement outcome, and the same flip at Bob's side. Applying the random Pauli operator on the qubits has the same effect as flipping every bit in Alice and Bob's measurement strings with probability $\frac{1}{2}$ while preserving the correlation. Since Alice's measurement result was already uniform, the output variables have the same statistics as before.

[14] We sometimes ignore the failure probability of a MAC yielding a $2^{-\lambda}$ difference. Sometimes a uniform random variable is output. In that case the output is equivalent to the original protocol where in addition a random uniform variable is created.

For the qudits in Chapter 7, we will exploit similar symmetries for higher dimensional states. Like the effect of the random Pauli operators in qubits, we will show the invariance to random phase flips and random permutations in the d-dimensional space. Symmetries on single quantum states are exploited in step 6.

Note that even though the modified protocol might be less practical than the original protocol, e.g. it might need quantum memory while the original protocol can be carried out with technology available today, this is not an issue. The modified protocol is a theoretical construct to prove the security, while the original protocol is the one used in practice.

Eve creates the EPR pairs

Instead of letting Eve attack the quantum state sent from Alice to Bob, we allow her to attack the entire EPR pairs. Clearly, if there is no successful attack in the scenario where Eve can attack the entire Alice-Bob system, there is no successful attack in the original protocol either. Since Eve has control over the entire system, we will allow Eve to prepare an arbitrary tripartite state ρ^{ABE}. Crucially, Eve knowing the plaintext should not influence the uniformity of Alice's measurement result.

We will consider the initial state of Alice, Bob and Eve to be some general density matrix $\rho^{\mathrm{ABE}} \in S(\mathcal{H}_{\mathrm{ABE}}^{\otimes n})$. As we will argue in step 6, Eve's state does not depend on the symmetrization variables. The protocol will only be successful if ρ^{AB} is close to n EPR pairs with a small coupling to the E-space. The random Pauli operator guarantees the outcome of Alice is still uniform when Eve creates the EPR pairs.

2.5.3 Step 3: CPTP maps

We describe the protocol of step 2 as a completely positive trace preserving map acting on a state shared by Alice, Bob and Eve ρ^{ABE}. The explicit values and relations between the message M, the keys K, the new keys $\tilde{K}$, the ciphertext C, the transcript T and the dependence of Eve's state ρ^{E}_{mkct} is given as a combined classical-quantum state: $\mathcal{E}(\rho^{\mathrm{ABE}}) = \rho^{MK\tilde{K}CT\mathrm{E}} = \mathbb{E}_{mk\tilde{k}ct} \left|mk\tilde{k}ct\right\rangle\!\left\langle mk\tilde{k}ct\right| \otimes \rho^{\mathrm{E}}_{mkct}$.

The coupling of ρ^{E} to m, k, c, t can be indirect. For example, say Alice and Bob both measure EPR pairs in the same shared basis given by b yielding x, y for Alice and Bob respectively. Eve's state is then coupled to b, x, y as $\mathbb{E}_{bxy} \left|bxy\right\rangle\!\left\langle bxy\right| \otimes \rho^{\mathrm{E}}_{bxy}$. Typically the message is then related to x and some additional variable $z = f(m, x)$ for some function f. For each classical variable that is computed, the probability distribution is peaked around the computed value and is described by a Kronecker delta. The output of $\mathcal{E}(\rho^{\mathrm{ABE}})$ can be obtained systematically.

1. Each generated classical variable is written as an expectation value of a register, e.g. $\mathbb{E}_m \left|m\right\rangle\!\left\langle m\right|$.

2. The measurements introduce a coupling between Eve's ancilla on the one hand and the measurement basis and the outcomes on the other hand, e.g. ρ^{E}_{bxy}.

3. The classical variables that are computed from other variables are added to the classical quantum-state with a Kronecker delta indicating its relations to the other variables, e.g $\sum_z \left|z\right\rangle\!\left\langle z\right| \delta_{z,f(m,x)}$.

4. The intermediate variables that only existed in the labs of Alice and Bob and do not become part of the transcript are traced out of the expression. We end up with $\rho^{MK\tilde{K}CT\mathrm{E}}$.

In the simple example described above, Alice and Bob measure in a shared secret basis b yielding measurement outcomes x, y. Alice computes the string $z = f(m, x)$ and sends it to Bob over a public channel. We have $K = B$, $T = Z$ and no $\tilde{K}$ and C. The variables x, y that are not output are traced out. Following the systematic approach, we write $\mathcal{E}(\rho^{\mathrm{ABE}}) = \rho^{MKT\mathrm{E}} = \mathrm{tr}_{XY}\, \mathbb{E}_{mbxy} \sum_z |mbxyz\rangle\langle mbxyz| \delta_{z,f(m,x)} \otimes \rho^{\mathrm{E}}_{bxy}$.

This systematic approach tends to give us lengthy expressions which may be harder to read, but it also gives us confidence our description of Eve's state is complete.

Depending on the desired security property, the corresponding ideal map $\mathcal{F}$ is described. In our systematic approach we describe $\mathcal{F}$ by taking the output of $\mathcal{E}$ and tracing out the variable that is to be protected. For example, if the message M is to be protected we write $\mathcal{F}(\rho^{\mathrm{ABE}}) = \rho^M \otimes \mathrm{tr}_M \mathcal{E}(\rho^{\mathrm{ABE}})$. In general there is some freedom in the choice of $\mathcal{F}$ as long as the diamond distance $\|\mathcal{E} - \mathcal{F}\|_\diamond$ bounds the desired properties e.g. ε-ENC.

2.5.4 Step 4: smoothing and entropies

The 1-norms of step 3 include the quantum state held by Eve ρ^E. In order the use the properties of smooth Rényi entropies (Section 2.3.8), we introduce smoothing as in [RK05, Ren05, TSSR11]. We consider states $\bar{\rho}^{\mathrm{E}}$ that are ε-close to ρ^{E} in terms of trace distance, $\|\rho^{\mathrm{E}} - \bar{\rho}^{\mathrm{E}}\|_1 \leq \varepsilon$. The smoothing introduces some freedom to modify states so as to get a more favorable diamond distance. For finite size results, where we can't use the asymptotic behavior of the Rényi entropy, smooth states are not considered.

The following lemma is Lemma 9 in [RK05].

Lemma 2.13. *Let $\rho^{X\mathrm{E}}$ be a normalized classical-quantum state with classical random variable X. Then for any $\varepsilon \geq 0$, there exists a state $\bar{\rho}^{X\mathrm{E}}$ with $\|\rho^{X\mathrm{E}} - \bar{\rho}^{X\mathrm{E}}\|_1 \leq \sqrt{\varepsilon}$ such that for any $\alpha > 1$*

$$S_\alpha(\bar{\rho}^{X\mathrm{E}}) - S_0(\bar{\rho}^{\mathrm{E}}) \geq S^\varepsilon_\alpha(\rho^{X\mathrm{E}}) - S^\varepsilon_0(\rho^{\mathrm{E}}). \tag{2.27}$$

In order to use the defining property of a two-wise independent hash function as in Equation 2.2, we need an average over the hashing seed. We will use Jensen's trace inequality to obtain expressions in which this average can be carried out. The following lemma follows from Theorem 2.4 of [HP02].

Lemma 2.14 (Jensen's Trace Inequality)**.** *Let $\rho_x \in S(\mathcal{H})$ be a density matrix. Let $f : S(\mathcal{H}) \to S(\mathcal{H})$ be a concave continuous function. It holds that*

$$\mathrm{tr} \mathop{\mathbb{E}}_x f(\rho_x) \leq \mathrm{tr}\, f(\mathop{\mathbb{E}}_x \rho_x). \tag{2.28}$$

In addition we will use the following lemma to 'pull' the trace into the square root.

Lemma 2.15. *Let ρ^{XE} be a classical-quantum state with classical random variable X. It holds that*

$$\mathrm{tr}_E \sqrt{\mathrm{tr}_X(\rho^{XE})^2} \leq \sqrt{\mathrm{rank}\big(\rho^E\big)} \sqrt{\mathrm{tr}\,(\rho^{XE})^2}. \tag{2.29}$$

Proof: We write the spectral decomposition of $\mathrm{tr}_X(\rho^{XE})^2 = \sum_i s_i |w_i\rangle\langle w_i|$ where w_i are eigenvectors in E space and $s_i > 0$. It then holds that $\mathrm{tr}_E \sqrt{\mathrm{tr}_X(\rho^{XE})^2} = \sum_i \sqrt{s_i} = \mathrm{rank}(\mathrm{tr}_X(\rho^{XE})^2)\, \mathbb{E}_i \sqrt{s_i}$, where we defined $\mathbb{E}_i(\cdot) \stackrel{\mathrm{def}}{=} \frac{1}{\mathrm{rank}(\mathrm{tr}_X(\rho^{XE})^2)} \sum_j (\cdot)$. Using Jensen's inequality to write $\mathbb{E}_i \sqrt{s_i} \leq \sqrt{\mathbb{E}_i\, s_i}$ we get

$$\mathrm{tr}_E \sqrt{\mathrm{tr}_X(\rho^{XE})^2} \leq \sqrt{\mathrm{rank}\big(\mathrm{tr}_X(\rho^{XE})^2\big)} \sqrt{\mathrm{tr}_{XE}(\rho^{XE})^2}. \tag{2.30}$$

We write ρ^{XE} in its spectral decomposition, $\rho^{XE} = \sum_j r_j |v_j\rangle\langle v_j|$, where the v_j are the eigenvectors in the XE space, and $r_j > 0$. It holds that $\mathrm{rank}(\mathrm{tr}_X(\rho^{XE})^2) = \mathrm{rank}(\rho^E)$. We have $\rho^E = \mathrm{tr}_X \rho^{XE} = \sum_j r_j V_j$, with $V_j \stackrel{\mathrm{def}}{=} \mathrm{tr}_X |v_j\rangle\langle v_j|$. Similarly, we write $\mathrm{tr}_X(\rho^{XE})^2 = \sum_j r_j^2 V_j$. Since $V_j > 0$ we can write $V_j = A_j^\dagger A_j$. We construct a matrix $A = [\sqrt{r_1}A_1; \sqrt{r_2}A_2; \sqrt{r_3}A_3; \cdots]$ by concatenating the matrices A_j under each other. It holds that $\sum_j r_j V_j = A^\dagger A$. Similarly we construct $Q = [r_1 A_1; r_2 A_2; r_3 A_3; \cdots]$, so that $\sum_j r_j^2 V_j = Q^\dagger Q$. We use the fact that $\mathrm{rank}(A^\dagger A) = \mathrm{rank}(A)$ and $\mathrm{rank}(Q^\dagger Q) = \mathrm{rank}(Q)$. By the construction of A and Q, the rows of A span the same space as the rows of Q. □

Together with the property of pairwise-independent hashing (2.2) this leads up to an expression in terms of (smooth-)Rényi entropies (see Section 2.3.8).

2.5.5 Step 5: post-selection

For a protocol that is invariant under permutations of the qubits, it has been shown in [CKR09] that security against collective attacks (same attack applied to each qubit individually) implies security against general attacks, at the cost of extra privacy amplification.

Lemma 2.16. *Let $\mathcal{E}$ be a protocol that acts on $S(\mathcal{H}_{AB}^{\otimes n})$ and let $\mathcal{F}$ be the ideal functionality of that protocol. If for all input permutations π there exists a map $\mathcal{K}_\pi$ on the output such that $(\mathcal{E} - \mathcal{F}) \circ \pi = \mathcal{K}_\pi \circ (\mathcal{E} - \mathcal{F})$, then*

$$\|\mathcal{E} - \mathcal{F}\|_\diamond \;\leq\; (n+1)^{d^2-1} \max_{\sigma \in S(\mathcal{H}_{ABE})} \Big\| (\mathcal{E} - \mathcal{F})(\sigma^{\otimes n}) \Big\|_1 \tag{2.31}$$

where d is the dimension of the $\mathcal{H}_{AB}$ space.

Step 2 of the recipe has introduced a random permuation as the first step of the protocol. Often the new protocol then trivially satisfies the requirement $(\mathcal{E} - \mathcal{F}) \circ \pi = \mathcal{K}_\pi \circ (\mathcal{E} - \mathcal{F})$ with $\mathcal{K}_\pi = \mathbb{1}$.

The product form $\sigma^{\otimes n}$ greatly simplifies the security analysis: now it suffices to prove security against 'collective' attacks, and to pay a price $2(d^2 - 1)\log(n+1)$ in the amount of privacy amplification, which is often negligible compared to n. We use the term 'privacy amplification' for the act of hashing to a smaller message size in order to obtain a better security parameter.

Using post-selection the relevant description of the quantum part of Eve's state is the purification of Alice and Bob's shared factorized state $\rho^{ABE} = (\sigma^{ABE})^{\otimes n}$. Eve having access to the purification of Alice and Bob's state ensures that we can describe her state explicitly without ignoring any other relevant state she could hold. For a protocol that sends quantum states of dimension d over a channel t times, the dimension of Eve's quantum state is $d^{\mathrm{Eve}} = d^{2t}$. So for simple qubit ($d = 2$) protocols with a single pass over the quantum channel ($t = 1$) we have $d^{Eve} = 4$. The factorized form allows us to use Lemma 2.1 and replace the Rényi entropies by von Neumann entropies in the asymptotic limit.

2.5.6 Step 6: Eve's simplified state

The invariances in the protocol that are described in step 2 are used to simplify the state held by Alice and Bob and therefore the purification held by Eve. Consider a shared state of Alice, Bob and Eve: ρ^{ABE}. Let Alice and Bob pick a random variable Σ according to which they apply their symmetrization. After their symmetrization the spaces of Alice and Bob are modified. The state is then $\rho^{\mathrm{A'B'\Sigma E}}$. After Σ has been applied, Alice and Bob entirely discard (or "forget") Σ. The rest of the protocol acts on A'B' without needing Σ. The state held by Alice and Bob is then $\rho^{\mathrm{A'B'}} = \mathrm{tr}_{\Sigma\mathrm{E}}\rho^{\mathrm{A'B'\Sigma E}}$. The strongest attack performed by Eve is such that she holds a purification of the state $\rho^{\mathrm{A'B'}}$. Since none of the subsequent steps involve Σ we do not explicitly write down Eve's coupling to Σ in step 3 as it will do her no good.

The addition of the random Pauli operators of step 2 greatly reduces the degrees of freedom in Alice and Bob's shared state.

Lemma 2.17. *Let $\tilde{\sigma}^{AB}$ be the 4-dimensional state shared by Alice and Bob after applying a random Pauli operator and forgetting the result. $\tilde{\sigma}^{\mathrm{AB}}$ is diagonal in the basis of Bell States $|\Phi_{ab}\rangle$.*

Proof: We can write an arbitrary 4-dimensional density matrix in the Bell basis as $\sigma^{\mathrm{AB}} = \sum_{ab}\sum_{a'b'}\nu^{ab}_{a'b'}|\Phi_{ab}\rangle\langle\Phi_{a'b'}|$. The effect of the random Pauli's is $\sum_\alpha(\sigma_\alpha \otimes \sigma_\alpha)|\Phi_{ab}\rangle\langle\Phi_{a'b'}|(\sigma_\alpha \otimes \sigma_\alpha) = (1 + (-1)^{b+b'} + (-1)^{a+a'+b+b'} + (-1)^{a+a'})|\Phi_{ab}\rangle\langle\Phi_{a'b'}| = 4\delta_{aa'}\delta_{bb'}|\Phi_{ab}\rangle\langle\Phi_{a'b'}|$. □

When Alice and Bob perform a measurement in the same basis, they expect their results to be fully correlated. They monitor the noise caused by Eve for each basis individually. By aborting the protocol when the noise constraints are not met, they can make sure that Eve's state satisfies the constraints.

The resulting states are simple enough that we can usually compute the eigenvalues of the state. When there is freedom left in the state of Eve, an optimization over the degrees of freedom is performed.

2.6 Example: six-state QKD

Using the recipe described in Section 2.5, we will prove the security of a version of six-state QKD [BPG99] in the limit of asymptotically many qubits. We consider a version of the six-state protocol that is very similar to the original BB84 protocol [BB84], but does not assume a specific probability distribution of the basis choice. The security and optimal rate of QKD is studied a lot. Thus, proving the security of 6-state QKD shows how the proof technique works in detail as well as showing it can yield tight bounds and high rates. In subsequent chapters we will consider protocols that use the same encoding. Hence, a lot of steps used in future proofs will be similar to the proof steps presented here. We will start by giving a protocol intuition, a description of the protocol, followed by the step by step proof.

Our proof uses techniques from [Ren05] in which 6-state QKD was treated as well. In [Ren05], Eve's knowledge is bounded by smooth Rényi entropies and we find the same result. The main way our proof technique distinguishes itself is that the same steps that are used here to prove the security of a QKD scheme, in which only one variable must be kept secure, can be used to prove different protocols with different goals as well, e.g. multiple variables must be secure. This is due to our systematic approach in terms of CPTP maps and diamond distances which is not used in [Ren05].

2.6.1 Protocol intuition

Alice and Bob's goal is to share a uniform random key that has the same length as the message that they want to one-time-pad encrypt. To start with, Alice and Bob only have a small shared key, long enough to authenticate their classical communication. Alice will encode random payload bits in qubits, exploiting Eve's inability to copy, measure or steal the qubits without being detected. These properties only hold when Eve does not know the encoding basis Alice uses. Alice randomly chooses the z-, x- or the y-basis. Since Bob, like Eve, doesn't know which basis Alice selected, he picks a random basis (z, x or y) for his measurement. When, by chance, Alice and Bob choose the same basis, Bob recovers Alice's payload. When their basis choices don't match, Bob measures a random bit. To achieve a shared string, Alice and Bob publicly tell each other which basis they used and only keep those bits that correspond to the qubits where they used the same basis. The rest they discard.

Alice and Bob perform error correction and check that the noise on the channel is sufficiently low. They can then perform privacy amplification corresponding to the measured noise level. The resulting shorter string can safely be used as a one-time pad to encrypt a message.

When Eve has access to the qubits, she does not know the encoding basis. There is no action she can perform on the qubits that has zero probability of causing noise. When Bob has performed his measurement and Alice and Bob sift out the qubits in which their bases match, they have an advantage over Eve, who will not have guessed the right basis each time. Thus we can bound Eve's knowledge on the payload by describing the most general state she can obtain. This state can not contain more information than the purification of the state shared by Alice and Bob. Due to the symmetries in the protocol the only useful degree of freedom is the bit error probability γ that she causes. Depending on the noise, we can tune the amount of

privacy amplification by tuning the size of the final message $m \in \{0,1\}^\ell$. Our final security parameter will be a function of the noise γ and the message size ℓ.

2.6.2 The six-state protocol with one-time pad encryption

We give a brief description of our version of the six-state protocol with a noisy quantum channel followed by a one-time pad. Alice and Bob have agreed on a security parameter λ, a noise threshold β, a family of pairwise independent hash functions $\Phi_u : \{0,1\}^n \to \{0,1\}^\ell$ with $u \in \mathcal{U}$, a set $\mathcal{B} = \{0,1,2\}$ of basis choices[15], a one-time MAC function $\Gamma : \{0,1\}^{2\lambda} \times \{0,1\}^* \to \{0,1\}^\lambda$ and a linear error-correcting code with syndrome function $\mathtt{Syn} : \{0,1\}^n \to \{0,1\}^{n-\kappa}$ and decoder $\mathtt{SynDec}$: $\{0,1\}^{n-\kappa} \to \{0,1\}^n$. They adopt the channel monitoring procedure shown below.

Definition 2.18. *Let x' be a noisy version of x resulting from n measurements in bases $b \in \mathcal{B}^n$. Let $\mathcal{I}_c$ be the positions where basis $c \in \mathcal{B}$ is used, $\mathcal{I}_c = \{i \in \mathbb{N} | b_i = c\}$. Let $x(c) \stackrel{\text{def}}{=} x_{\mathcal{I}_c}$ denote the part of x that is encoded in basis c and likewise $x'(c)$.*

$$\mathtt{NoiseCheck}(b,x,x') = \begin{cases} 1 & \text{if } \forall_{c\in\mathcal{B}} \ \frac{\mathtt{Hamm}(x(c)\oplus x'(c))}{|\mathcal{I}_c|} \le \beta \\ 0 & \text{otherwise.} \end{cases} \tag{2.32}$$

Definition 2.18 says the noise check yields 1 only when the noise is lower than the threshold β for each basis.

Alice and Bob perform the following actions, see Figure 2.3.

QKD.Gen:

Alice and Bob generate shared secret keys $k_1^{\mathrm{MAC}}, k_2^{\mathrm{MAC}}, k_3^{\mathrm{MAC}}, k_4^{\mathrm{MAC}}$.

Alice generates local random strings $x^{\mathrm{raw}} \in \{0,1\}^\nu$, $b^{\mathrm{raw}} \in \mathcal{B}^\nu$ and $u \in \mathcal{U}$.[16] She generates a message $m \in \{0,1\}^\ell$. Here b^{raw} and m do not have to be uniform.

Bob generates a local random string $b^{\mathrm{raw}\prime} \in \mathcal{B}^\nu$ that is not necessarily uniform.

QKD.Enc:

Alice prepares $|\Psi\rangle = \bigotimes_{i=1}^{\nu} |\psi^{b_i^{\mathrm{raw}}}_{x_i^{\mathrm{raw}}}\rangle$ and sends it to Bob.

QKD.Meas:

Bob receives $|\Psi\rangle'$ and measures in the $b^{\mathrm{raw}\prime}$ basis yielding $x^{\mathrm{raw}\prime}$.

QKD.Post:

Bob computes the tag $\tau_1 = \Gamma(k^1_{\mathrm{MAC}}, b^{\mathrm{raw}\prime})$. He sends $b^{\mathrm{raw}\prime}$ and the tag τ_1 to Alice.

Alice checks that $\tau_1 == \Gamma(k^1_{\mathrm{MAC}}, b^{\mathrm{raw}\prime})$. She compares $b^{\mathrm{raw}\prime}$ to b^{raw}. On the n indices where they agree $\mathcal{I} = \{i \in \mathbb{N} | b_i^{\mathrm{raw}} = b_i^{\mathrm{raw}\prime}\}$ she computes $x = x^{\mathrm{raw}}_{\mathcal{I}}$ and $e = \mathtt{Syn}\, x$. She authenticates e and $\mathcal{I}$, $\tau_2 = \Gamma(k_2^{\mathrm{MAC}}, e \| \mathcal{I})$ and sends $e, \mathcal{I}, \tau_2$ to Bob.

Bob checks $\tau_2 == \Gamma(k_2^{\mathrm{MAC}}, e\|\mathcal{I})$. Then he computes $x' = x^{\mathrm{raw}\prime}_{\mathcal{I}}$ and $b = b^{\mathrm{raw}\prime}_{\mathcal{I}}$ and performs the error correction $\hat{x} = x' \oplus \mathtt{SynDec}(e \oplus \mathtt{Syn}\, x')$ and the channel monitoring $\omega = \mathtt{NoiseCheck}(b, \hat{x}, x')$. He authenticates ω, $\tau_3 = \Gamma(k_3^{\mathrm{MAC}}, \omega)$ and sends ω, τ_3 to Alice.

Alice checks the authentication of ω. If $\omega = 1$, she computes $z = \Phi_u(x)$ and $c =$

[15] The same protocol can be performed with a different basis set. In particular using two possible bases yields the [BB84] protocol.

[16] The hash seed only needs to be generated in the accept case.

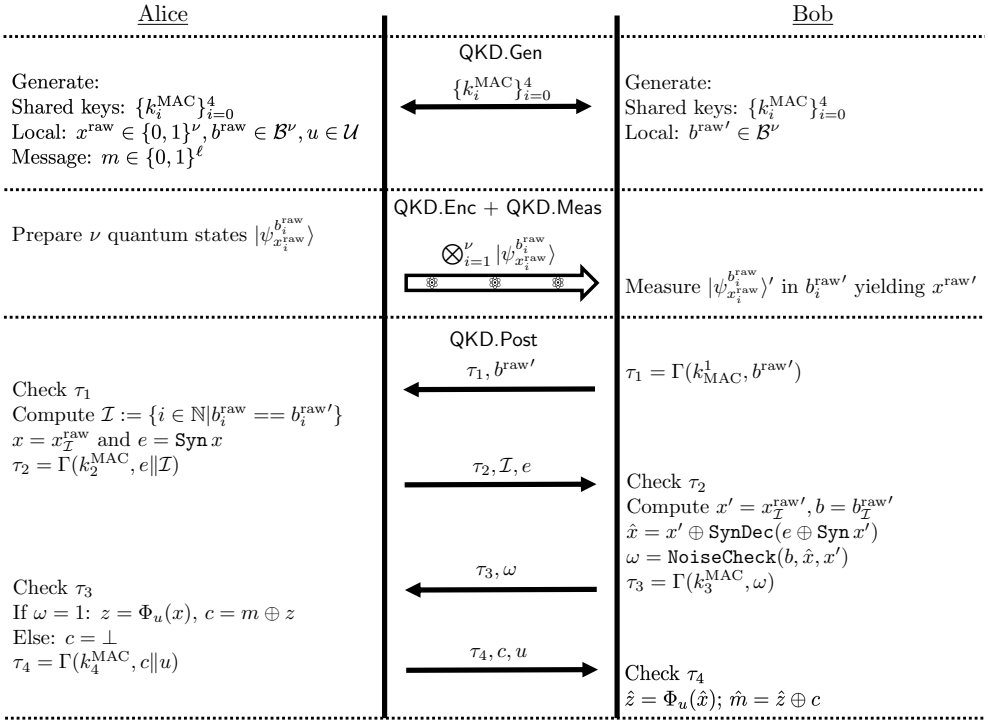

Figure 2.3: The six-state protocol together with a one-time pad encryption. The `NoiseCheck` function is defined in Definition 2.18.

$m \oplus z$. She aborts otherwise. She authenticates c, u with k_4^{MAC}, $\tau_4 = \Gamma(k_4^{\mathrm{MAC}}, c \| u)$ and sends the c, u and τ_4 to Bob.
Bob checks $\tau_4 == \Gamma(k_4^{\mathrm{MAC}}, c \| u)$. He computes $\hat{z} = \Phi_u(\hat{x})$ and $\hat{m} = \hat{z} \oplus c$.

2.6.3 Step 1: EPR version of six-state QKD

In the EPR version of the protocol, Alice generates ν EPR pairs in the singlet state $(|\Psi^-\rangle)$. Of this 4^ν-dimensional quantum system ρ^{AB} she sends the 2^ν-dimensional subsystem B to Bob. The QKD.Enc step is replaced by a measurement by Alice. For each half of an EPR pair, Alice measures the qubit in the b_i^{raw} basis yielding a bit s_i^{raw}. She computes $a^{\mathrm{raw}} = s^{\mathrm{raw}} \oplus x^{\mathrm{raw}}$ and sends a^{raw} to Bob classically. Effectively, the qubits at Bob's side are now a noisy encoding of s^{raw} in basis b^{raw}. To obtain x', Bob measures his qubit as before, yielding t^{raw}. He adds a^{raw} to his measurement outcome and flips the bit because of the anti-correlation in the singlet state: $x^{\mathrm{raw}\prime} = \bar{t}^{\mathrm{raw}} \oplus a^{\mathrm{raw}}$. By construction, the equivalence holds when Eve does not have access to a^{raw} when attacking the quantum states. Her ancilla doesn't depend on a^{raw}.

2.6.4 Step 2: equivalent protocol

We describe a protocol QKD' that is equivalent to the EPR version of six-state QKD adding a random permutation and a random Pauli as described in Section 2.5.2. In addition we let the creation of the EPR pairs be done by Eve. The random permutation and random Pauli operator are selected by Alice and communicated to Bob over a public channel. In QKD', we assume perfect authenticated classical channels, i.e. we no longer explicitly write down the classical MAC functions and authentication tags. The mappings of Section 2.6.2 are replaced by the mappings of QKD'.

The equivalence of applying random Pauli operators is discussed in Section 2.5.2. Eve's quantum state does not depend on α. The permutation invariance of the six-state protocol can be seen as follows. In the original prepare-and-measure protocol the basis sequence B and the payload X are uniform; therefore it does not matter if Alice performs a random permutation $b \mapsto \pi(b), x \mapsto \pi(x)$ (and Bob the corresponding permutation). The effect is still a uniform payload encoded in a uniform basis. The above action is identical to keeping b, x untouched but permuting the qubits: Alice applies π, and Bob π^{-1}. In the EPR version Alice and Bob both apply the same permutation, i.e. the EPR pairs get permuted and as a result so do s, t. The only difference in x, x' is the location of the errors which is undetectable after the error correction step.

Instead of letting Alice generate the EPR pairs, Eve generates an arbitrary 16^ν-dimensional system ρ^{ABE} and send the 2^ν-dimensional subsystem A to Alice and the 2^ν-dimensional subsystem B to Bob. Alice and Bob interpret their shared state as ν noisy EPR pairs in the singlet state. Due to the random Pauli operators applied by Alice, her measurement result s remains uniform. The steps of QKD' are also shown in Figure 2.4.

QKD'.Gen:
Alice generates the message $m \in \{0,1\}^\ell$ and local random strings $x^{\mathrm{raw}} \in \{0,1\}^\nu$, $b^{\mathrm{raw}} \in \mathcal{B}^\nu$ and $u \in \{0,1\}^n$. She generates a random permutation π of the ν qubits positions and random indices $\alpha \in \{0,1,2,3\}^\nu$ for the random Pauli.
Bob generates a local random string $b^{\mathrm{raw}\prime} \in \mathcal{B}^\nu$.

QKD'.Enc:
Eve prepares ν noisy EPR pairs in the $|\tilde{\Psi}^-\rangle$ state and sends half of each pair to Alice and half to Bob.
Alice applies the random permutation π to her qubits and applies σ_{α_i} to the ith qubit. She measures her half of the ith EPR pair in the b_i^{raw} basis yielding s_i^{raw}. She sends π, α and $a^{\mathrm{raw}} = x^{\mathrm{raw}} \oplus s^{\mathrm{raw}}$ to Bob over authenticated channel and forgets π, α.

QKD'.Meas:
Bob applies π and σ_a to his qubits and measures in the $b^{\mathrm{raw}\prime}$ basis yielding t^{raw}. He computes $x^{\mathrm{raw}\prime} = \bar{t}^{\mathrm{raw}} \oplus a^{\mathrm{raw}}$. He forget π, α.

QKD'.Post:
Bob sends $b^{\mathrm{raw}\prime}$ to Alice.
Alice compares $b^{\mathrm{raw}\prime}$ to b^{raw}. On the indices where they agree $\mathcal{I} = \{i \in \mathbb{N} | b_i^{\mathrm{raw}} = b_i^{\mathrm{raw}\prime}\}$ she computes $x = x_{\mathcal{I}}^{\mathrm{raw}}$ and $e = \mathtt{Syn}\, x$. She sends $e, \mathcal{I}$ to Bob.

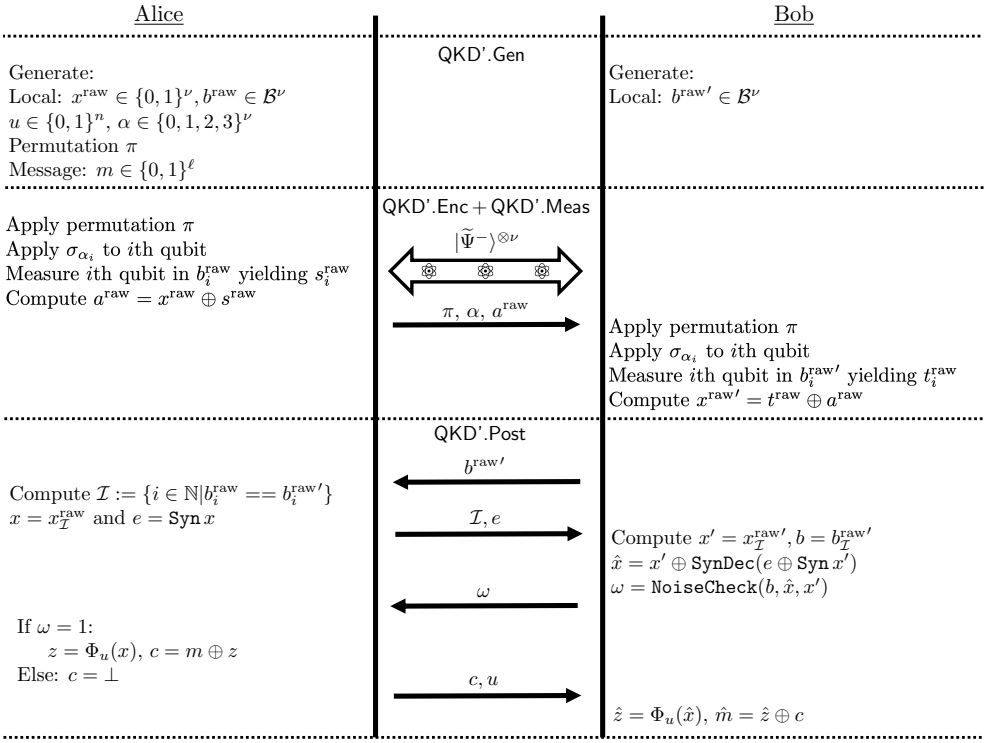

Figure 2.4: The equivalent six-state protocol together with a one-time pad encryption. The `NoiseCheck` function is defined in Definition 2.18.

Bob computes $x' = x_{\mathcal{I}}^{\text{raw}\prime}$ and $b = b_{\mathcal{I}}^{\text{raw}\prime}$ and performs the error correction $\hat{x} = x' \oplus \mathtt{SynDec}(e \oplus \mathtt{Syn}\, x')$ and the channel monitoring $\omega = \mathtt{NoiseCheck}(b, \hat{x}, x')$. He sends ω to Alice.
If $\omega = 1$, Alice computes $z = \Phi_u(x)$ and $c = m \oplus z$. She aborts otherwise. She sends the c, u to Bob.
Bob computes $\hat{z} = \Phi_u(\hat{x})$ and $\hat{m} = \hat{z} \oplus c$.

2.6.5 Step 3: CPTP mappings

Eve creates some state ρ^{ABE} on which the actions of Alice and Bob work. To simplify the notation, we only write down spaces and strings corresponding to the qubit positions Alice and Bob don't discard i.e. we consider s, t, x, x', b rather than $s^{\text{raw}}, t^{\text{raw}}, x^{\text{raw}}, x^{\text{raw}\prime}, b^{\text{raw}}, b^{\text{raw}\prime}$. In QKD′.Gen, QKD′.Enc and QKD′.Meas, the random variables m, u, x and b are generated, and the measurement of Alice and Bob has created a coupling between b, s, t, a, x'. Let $\mathcal{M}$ be shorthand notation for the first three QKD′ maps QKD′.Meas ∘ QKD′.Enc ∘ QKD′.Gen.

$$\mathcal{M}(\rho^{\text{ABE}}) = \mathop{\mathbb{E}}_{mbstxu} \sum_{ax'} |mbstaxx'u\rangle\langle mbstaxx'u| \delta_{a,x\oplus s}\delta_{x',a\oplus\bar{t}} \otimes \rho^{\text{E}}_{bst} \tag{2.33}$$

where the expectation values over b, u, x are uniform. The notation $\mathbb{E}_{st}(\cdot)$ means $\sum_s 2^{-n} \sum_t p_{t|s}(\cdot)$, where $p_{t|s}$ depends on ρ^{ABE}. In step 5, we will see that these probabilities have a simple form.

The post-processing step introduces the variables e, c, z. In addition a bit ω is output that indicates the success of the noise check. Let $\mathcal{P}$ be the map describing the protocol up to the point where Alice and Bob delete the variables that are not output.

$$\begin{aligned}\mathcal{P}(\rho^{\mathrm{ABE}}) &= \mathop{\mathbb{E}}_{bst} |bst\rangle\langle bst| \otimes \sum_{x' aecz\omega} \mathop{\mathbb{E}}_{mux} |muxx' aecz\omega\rangle\langle \cdots | \delta_{a,x\oplus s}\delta_{x',a\oplus \bar{t}} \\ &\quad \delta_{e,\mathtt{Syn(x)}}\delta_{\omega,\theta_{bst}}\left[\omega\delta_{c,m\oplus z}\delta_{z,\Phi_u(x)} + \bar{\omega}2^{-\ell}\delta_{c,\perp}\right] \otimes \rho^{\mathrm{E}}_{bst}. \end{aligned} \tag{2.34}$$

The θ_{bst} indicates whether the noise check of Definition 2.18 is passed (taking into account the anti-correlation of s, t due to the singlet state)

$$\theta_{bst} = \mathtt{NoiseCheck}(b, s, \bar{t}). \tag{2.35}$$

The variables that are not part of the output or the transcript are traced out, s, t, z, x, x'. The entire map $\mathcal{E}_{\mathrm{QKD}}$ corresponding to the modified six-state protocol followed by a one-time pad is given by

$$\begin{aligned}\mathcal{E}_{\mathrm{QKD}}(\rho^{\mathrm{ABE}}) &= \mathop{\mathbb{E}}_{mubcae} \sum_{\omega} |mbucae\omega\rangle\langle \cdots | \mathop{\mathbb{E}}_{st|b} \left[\omega 2^{\ell}\delta_{\Phi_u(s\oplus a),m\oplus c} + \bar{\omega}2^{\ell}\delta_{c,\perp}\right] \\ &\quad 2^{n-\kappa}\delta_{e,\mathtt{Syn}(s\oplus a)}\delta_{\omega,\theta_{bst}} \otimes \rho^{\mathrm{E}}_{bst} = \rho^{MBUCAE\Omega\mathrm{E}} \end{aligned} \tag{2.36}$$

where we write $\mathbb{E}_c(\cdot) = 2^{-n}\sum_c(\cdot)$, $\mathbb{E}_a(\cdot) = 2^{-n}\sum_a(\cdot)$ and $\mathbb{E}_e = 2^{\kappa-n}\sum_e(\cdot)$.

The only key material used in the six-state protocol is for authentication purposes which does not show up in (2.36). In the language of the security definitions of Section 2.4, the message is M, there is no key, the ciphertext[17] is A and the transcript is B, U, C, E, Ω.

The ideal behavior of the combination of quantum key distribution and one-time pad encryption outputs a quantum state held by Eve that is not coupled to the message. The rest of the ideal map $\mathcal{F}_{\mathrm{QKD}}$ should be as close to $\mathcal{E}_{\mathrm{QKD}}$ as possible. We trace out the message from the output of the real map and introduce a new decoupled message $\mathcal{F}_{\mathrm{QKD}}(\rho^{\mathrm{ABE}}) = \mathbb{E}_m |m\rangle\langle m| \otimes \mathrm{tr}_M \mathcal{E}_{\mathrm{QKD}}(\rho^{\mathrm{ABE}})$.

$$\begin{aligned}\mathcal{F}_{\mathrm{QKD}}(\rho^{\mathrm{ABE}}) &= \mathop{\mathbb{E}}_{mubcae} \sum_{\omega} |mbucae\omega\rangle\langle \cdots | \mathop{\mathbb{E}}_{st|b} \left[\omega 2^{\ell} \mathop{\mathbb{E}}_{m'} \delta_{\Phi_u(s\oplus a),m'\oplus c} + \bar{\omega}2^{\ell}\delta_{c,\perp}\right] \\ &\quad 2^{n-\kappa}\delta_{e,\mathtt{Syn}(s\oplus a)}\delta_{\omega,\theta_{bst}} \otimes \rho^{\mathrm{E}}_{bst} = \rho^{M} \otimes \rho^{BUCAE\Omega\mathrm{E}}. \end{aligned} \tag{2.37}$$

The diamond distance between $\mathcal{E}_{\mathrm{QKD}}$ and $\mathcal{F}_{\mathrm{QKD}}$ corresponds to the definition of encryption in Section 2.4.1.

$$\|\mathcal{E}_{\mathrm{QKD}} - \mathcal{F}_{\mathrm{QKD}}\|_{\diamond} = \frac{1}{2}\|\rho^{MBUCAE\Omega\mathrm{E}} - \rho^{M} \otimes \rho^{BUCAE\Omega\mathrm{E}}\|_1 \stackrel{\mathrm{def}}{=} D. \tag{2.38}$$

[17] The ciphertext in Section 2.4 is defined as the classical information sent at the same time as the qubit. This is different from the ciphertext that is part of the transcript.

In (2.38), the states held by Eve are optimal. The states $\rho^{MBUCAE\Omega E}$ and $\rho^{M}\otimes\rho^{BUCAE\Omega E}$ only differ in the accept case. Expression (2.38) can be seen as the difference between two sub-normalized states which both have norm $\mathbb{E}_{bst}\,\theta_{bst}$ which is the probability that the noise check is passed. Hence an upper bound $D\leq\mathbb{E}_{bst}\,\theta_{bst}$ immediately follows.

2.6.6 Step 4: smoothing

By allowing state $\bar{\rho}$ that are $\sqrt{\varepsilon}$-close to ρ in terms of trace distance we can bound the distance in (2.38) as $D\leq 2\sqrt{\varepsilon}+\bar{D}$ with $\bar{D}\stackrel{\text{def}}{=}\|\bar{\rho}^{MBUCAE\Omega E}-\rho^{M}\otimes\bar{\rho}^{BUCAE\Omega E}\|_1$.

$$\begin{aligned}\bar{D} \;=\; & \Big\| \mathop{\mathbb{E}}_{mbuace} |mbuace,\omega=1\rangle\langle mbuace,\omega=1| 2^{n-\kappa}2^{\ell}\delta_{e,\mathtt{Syn}(s\oplus a)} \\ & \otimes \mathop{\mathbb{E}}_{st|b}\bar{\rho}^{\mathrm{E}}_{bst}\theta_{bst}[\delta_{m\oplus c,\Phi_u(s\oplus a)}-\mathop{\mathbb{E}}_{m'}\delta_{m'\oplus c,\Phi_u(s\oplus a)}]\Big\|_1. \end{aligned} \tag{2.39}$$

The spaces corresponding to the classical variables are the same for the real and ideal state and give the overall matrix a block structure. This structure allows us to write:

$$\bar{D}\leq\tfrac{1}{2}\mathop{\mathbb{E}}_{mbuace}2^{n-\kappa}\Big\|\mathop{\mathbb{E}}_{st|b}\delta_{e,\mathtt{Syn}(s\oplus a)}\bar{\rho}^{\mathrm{E}}_{bst}\theta_{bst}2^{\ell}[\delta_{m\oplus c,\Phi_u(s\oplus a)}-\mathop{\mathbb{E}}_{m'}\delta_{m'\oplus c,\Phi_u(s\oplus a)}]\Big\|_1. \tag{2.40}$$

Expanding the 1-norm as $\|A\|_1=\operatorname{tr}\sqrt{A^{\dagger}A}$ we write the right hand side of (2.40) as

$$\begin{aligned}\bar{D} \;\leq\; & \tfrac{1}{2}\mathop{\mathbb{E}}_{mbuace}\operatorname{tr}\Big\{\mathop{\mathbb{E}}_{ss'tt'|b}\theta_{bst}\theta_{bs't'}2^{2n-2\kappa}\delta_{e,\mathtt{Syn}(s\oplus a)}\delta_{e,\mathtt{Syn}(s'\oplus a)}\bar{\rho}^{\mathrm{E}}_{bst}\bar{\rho}^{\mathrm{E}}_{bs't'} \\ & 2^{2\ell}[\delta_{\Phi_u(a\oplus s),m\oplus c}-\mathop{\mathbb{E}}_{m'}\delta_{\Phi_u(a\oplus s),m'\oplus c}][\delta_{\Phi_u(a\oplus s'),m\oplus c}-\mathop{\mathbb{E}}_{m''}\delta_{\Phi_u(a\oplus s'),m''\oplus c}]\Big\}^{\frac{1}{2}}. \end{aligned} \tag{2.41}$$

Using Jensen's inequality (Lemma 2.14), we 'pull' $\mathbb{E}_u$ and $\mathbb{E}_m$ under the square root and then make use of the pairwise-independent properties of Φ_u when acted upon with $\mathbb{E}_u$ (using Equation 2.2). This yields

$$\begin{aligned}& 2^{2\ell}\mathop{\mathbb{E}}_{mu}[\delta_{\Phi_u(a\oplus s),m\oplus c}-\mathop{\mathbb{E}}_{m'}\delta_{\Phi_u(a\oplus s),m'\oplus c}][\delta_{\Phi_u(a\oplus s'),m\oplus c}-\mathop{\mathbb{E}}_{m''}\delta_{\Phi_u(a\oplus s'),m''\oplus c}] \\ & \qquad = 2^{\ell}\delta_{ss'}(1-\mathop{\mathbb{E}}_{mm'}\delta_{mm'})<2^{\ell}\delta_{ss'} \end{aligned} \tag{2.42}$$

which leads to

$$\bar{D} \;<\; \tfrac{1}{2}\mathop{\mathbb{E}}_{bae}\operatorname{tr}\sqrt{2^{\ell}\mathop{\mathbb{E}}_{ss'tt'|b}\theta_{bst}\theta_{bs't'}2^{2n-2\kappa}\delta_{e,\mathtt{Syn}(s\oplus a)}\delta_{e,\mathtt{Syn}(s'\oplus a)}\bar{\rho}^{\mathrm{E}}_{bst}\bar{\rho}^{\mathrm{E}}_{bs't'}\delta_{ss'}} \tag{2.43}$$

$$\leq\; \tfrac{1}{2}\mathop{\mathbb{E}}_{b}\operatorname{tr}\sqrt{2^{\ell}2^{n-\kappa}\mathop{\mathbb{E}}_{ss'tt'|b}\theta_{bst}\theta_{bs't'}\bar{\rho}^{\mathrm{E}}_{bst}\bar{\rho}^{\mathrm{E}}_{bs't'}\delta_{ss'}} \tag{2.44}$$

where we used Jensen's inequality for e as well. Next we use $\theta_{bst}\leq 1$ and $\mathbb{E}_{t|bs}\,\bar{\rho}^{\mathrm{E}}_{bst}=\bar{\rho}^{\mathrm{E}}_{bs}$, yielding $\bar{D}<\frac{1}{2}\,\mathbb{E}_b\operatorname{tr}\sqrt{2^{n-\kappa+\ell}\,\mathbb{E}_{ss'|b}\,\bar{\rho}^{\mathrm{E}}_{bs}\bar{\rho}^{\mathrm{E}}_{bs'}\delta_{ss'}}$. Combining the two obtained bounds gives

$$\bar{D}\leq\min\Big(\mathop{\mathbb{E}}_{bst}\theta_{bst},\tfrac{1}{2}\mathop{\mathbb{E}}_{b}\operatorname{tr}\sqrt{2^{n-\kappa+\ell}\mathop{\mathbb{E}}_{ss'|b}\bar{\rho}^{\mathrm{E}}_{bs}\bar{\rho}^{\mathrm{E}}_{bs'}\delta_{ss'}}\Big). \tag{2.45}$$

The expression of the form $\mathbb{E}_b \operatorname{tr} \sqrt{\mathbb{E}_{ss'|b} \bar{\rho}^{\mathrm{E}}_{bs} \bar{\rho}^{\mathrm{E}}_{bs'} \delta_{ss'}}$ can be bounded by an expression in terms of smooth Rényi entropies. The following lemma holds independent of the interpretation or probability distributions of X and Y.

Lemma 2.19. *Let ρ^{E}_x be a density matrix describing Eve's state coupled to $x \in \mathcal{X}$. There exists a state $\bar{\rho}^{X\mathrm{E}}$ that is $\sqrt{\bar{\varepsilon}}$-close to $\rho^{X\mathrm{E}}$ in terms of trace distance such that*

$$\operatorname{tr} \sqrt{\mathop{\mathbb{E}}_{xx'} \bar{\rho}^{\mathrm{E}}_x \bar{\rho}^{\mathrm{E}}_{x'} \delta_{xx'}} \leq \sqrt{2^{S^{\varepsilon}_0(\rho^{\mathrm{E}}) - S^{\varepsilon}_2(\rho^{X\mathrm{E}})}}. \tag{2.46}$$

Proof: We use Lemma 2.15 to 'pull' the trace into the square root

$$\operatorname{tr} \sqrt{\mathop{\mathbb{E}}_{xx'} \bar{\rho}^{\mathrm{E}}_x \bar{\rho}^{\mathrm{E}}_{x'} \delta_{xx'}} = \operatorname{tr}_{\mathrm{E}} \sqrt{\operatorname{tr}_X (\bar{\rho}^{X\mathrm{E}})^2} \tag{2.47}$$

$$\overset{\text{Lemma 2.15}}{\leq} \sqrt{\operatorname{rank}\big(\bar{\rho}^{\mathrm{E}}\big)} \sqrt{\operatorname{tr}_{X\mathrm{E}} (\bar{\rho}^{X\mathrm{E}})^2}. \tag{2.48}$$

From the definition of the Rényi entropies (2.13) and smooth Rényi entropies (2.14) it then holds

$$\sqrt{\operatorname{rank}\big(\bar{\rho}^{\mathrm{E}}\big)} \sqrt{\operatorname{tr}_{X\mathrm{E}} (\bar{\rho}^{X\mathrm{E}})^2} = \sqrt{2^{S_0(\bar{\rho}^{\mathrm{E}}) - S_2(\bar{\rho}^{X\mathrm{E}})}} \tag{2.49}$$

$$\overset{\text{Lemma 2.13}}{\leq} \sqrt{2^{S^{\varepsilon}_0(\rho^{\mathrm{E}}) - S^{\varepsilon}_2(\rho^{X\mathrm{E}})}}. \tag{2.50}$$

□

We apply Lemma 2.19 to (2.45) with $\mathcal{X} = \mathcal{S}$. Our bound becomes

$$\bar{D} \leq \min \Big(\mathop{\mathbb{E}}_{bst} \theta_{bst}, \tfrac{1}{2} \sqrt{2^{n-\kappa+\ell}} \mathop{\mathbb{E}}_{b} \sqrt{2^{S^{\varepsilon}_0(\rho^{\mathrm{E}}_b) - S^{\varepsilon}_2(\rho^{S\mathrm{E}}_b)}} \Big). \tag{2.51}$$

2.6.7 Step 5: post-selection

The bound (2.51) depends on the form of ρ^{E}_{bs}. We use the post-selection technique to write $\rho^{\mathrm{ABE}} = (\sigma^{\mathrm{ABE}})^{\otimes n}$. This allows us to write $\rho^{\mathrm{E}}_{bs} = \bigotimes_{i=1}^n \sigma^{\mathrm{E}}_{b_i s_i} = \bigotimes_{i=1}^n \mathbb{E}_{t_i|b_i s_i} \sigma^{\mathrm{E}}_{b_i s_i t_i}$. In principle, the noise Eve causes can be different for each basis choice. However, the more noise is caused on the channel, the more information leaks about the classical variables encoded in the quantum state. By giving Eve access to the purification of the state in which the noise is maximal (equal to γ) for each basis, Eve has access to the maximum amount of information. For the factorized form of ρ^{ABE} and an equal noise level γ in each position it holds that $p_{t|bs} = \gamma^{\mathtt{Hamm}(s \oplus \tilde{t})} (1-\gamma)^{\mathtt{Hamm}(s \oplus t)}$.

Regarding the probability that the noise checks are passed, it can be advantageous for Eve to cause a different noise level in each basis choice. We denote the noise caused by Eve in basis b as γ_b. The accept probability is then defined as follows.

$$P_{\mathrm{acc}} \overset{\mathrm{def}}{=} \mathop{\mathbb{E}}_{bst} \theta_{bst} = \mathop{\mathbb{E}}_{\{n_b\}: \sum_b n_b = n} \prod_{b \in \mathcal{B}} \sum_{c=0}^{\lfloor n_b \beta \rfloor} \binom{n_b}{c} \gamma_b^c (1-\gamma_b)^{n_b - c} \tag{2.52}$$

where n_b denotes the number of times the basis b is used for encoding. From the Chernoff or Hoeffding inequality it follows that (2.52) becomes asymptotically small when $\gamma_b > \beta$ for any $b \in \mathcal{B}$.

Going forward we write $b \in \mathcal{B}$ and $s \in \{0,1\}$ to denote the value of a basis choice of bit value rather than strings length n. Using post-selection to simplify (2.51) and including the penalty term we get

$$\begin{aligned} \|\mathcal{E}_{\mathrm{QKD}} - \mathcal{F}_{\mathrm{QKD}}\|_\diamond \quad &\leq \quad \tfrac{1}{2}(n+1)^{15} \min\Big\{ P_{\mathrm{acc}}, \sqrt{\varepsilon} + \\ &\qquad \sqrt{2^{n-\kappa+\ell}} \mathop{\mathbb{E}}_b \sqrt{2^{S_0^\varepsilon([\sigma_b^{\mathrm{E}}]^{\otimes n}) - S_2^\varepsilon([\sigma_b^{\mathrm{SE}}]^{\otimes n})}} \Big\}. \end{aligned} \tag{2.53}$$

Asymptotically, the second term in the minimum can be simplified using Lemma 2.1

$$\sqrt{2^{S_0^\varepsilon([\sigma_b^{\mathrm{E}}]^{\otimes n}) - S_2^\varepsilon([\sigma_b^{\mathrm{SE}}]^{\otimes n})}} \overset{\text{Lemma 2.1}}{\leq} \sqrt{2^{nS(\sigma_b^{\mathrm{E}}) - nS(\sigma_b^{\mathrm{SE}}) + \mathcal{O}(\sqrt{n})}} \tag{2.54}$$

$$= \sqrt{2^{-n} 2^{nS(\mathbb{E}_{s|b}\, \sigma_{bs}^{\mathrm{E}}) - n\, \mathbb{E}_{s|b}\, S(\sigma_{bs}^{\mathrm{E}}) + \mathcal{O}(\sqrt{n})}}. \tag{2.55}$$

2.6.8 Step 6: Eve's state

To bound (2.55), we need the explicit form of $\sigma_{bst}^{\mathrm{E}}$ for the variables b, s, t. Let $\tilde{\sigma}^{\mathrm{AB}}$ be the state of the Alice-Bob system before they perform their measurements. We know from Lemma 2.17 that the state is diagonal in the basis of Bell states. By assuming the noise for every basis choice is maximal, which is optimal for Eve, we know the following constraints hold.

$$\forall_{b \in \mathcal{B}} \sum_{x=0}^{1} \langle \psi_x^b \psi_x^b | \tilde{\sigma}^{\mathrm{AB}} | \psi_x^b \psi_x^b \rangle = \gamma \tag{2.56}$$

where $\tilde{\sigma}^{\mathrm{AB}} = \lambda_1 |\Psi^-\rangle\langle\Psi^-| + \lambda_2 |\Phi^-\rangle\langle\Phi^-| + \lambda_3 |\Psi^+\rangle\langle\Psi^+| + \lambda_4 |\Phi^-\rangle\langle\Phi^-|$ is diagonal with respect to the Bell basis. The noise check introduces three constraints on the values of the λ_i's. Together with the normalization we have four constraints in total: $\lambda_2 + \lambda_3 = \lambda_2 + \lambda_4 = \lambda_3 + \lambda_4 = \gamma$ and $\sum_i \lambda_i = 1$. As a result the state held by Alice and Bob only depends on the noise parameter γ: $\tilde{\sigma}^{AB} = \mathrm{Diag}(1 - \frac{3}{2}\gamma, \frac{1}{2}\gamma, \frac{1}{2}\gamma, \frac{1}{2}\gamma)$. Because of the assumption that all noise is caused by Eve, we consider that Eve holds the purification of $\tilde{\sigma}^{\mathrm{AB}}$. We write

$$|\Psi^{\mathrm{ABE}}\rangle \;=\; \sqrt{1 - \tfrac{3}{2}\gamma} |\Psi^-\rangle |m_0\rangle + \sqrt{\tfrac{\gamma}{2}} \Big(- |\Phi^-\rangle |m_1\rangle + i |\Psi^+\rangle |m_2\rangle + |\Phi^+\rangle |m_3\rangle \Big) \tag{2.57}$$

where $|m_i\rangle$ is an orthonormal basis in Eve's four-dimensional ancilla space. The phases are chosen to make Eve's state after Alice and Bob's measurements simple. For the following, we don't restrict ourselves to the 6-state encoding to make the description of Eve's state as widely applicable to different encodings as possible.

Alice and Bob both do a projective measurement on their own subsystem. Describing their measurements in the Bloch sphere they measure the component in the direction $\boldsymbol{v} = (v_x, v_y, v_z) = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$. The eigenstates of this measurement are $|\boldsymbol{v}\rangle = e^{-i\varphi/2}\cos\frac{\theta}{2}|0\rangle + e^{i\varphi/2}\sin\frac{\theta}{2}|1\rangle$ (with eigenvalue '0') and $|\overline{\boldsymbol{v}}\rangle = -e^{-i\varphi/2}\sin\frac{\theta}{2}|0\rangle + e^{i\varphi/2}\cos\frac{\theta}{2}|1\rangle$ (with eigenvalue '1').

We rewrite the state (2.57) using $|\boldsymbol{v}\rangle, |\overline{\boldsymbol{v}}\rangle$ as the basis of the A and B subsystem,

$$\begin{aligned}
|\Psi^{\mathrm{ABE}}\rangle &= \sqrt{\tfrac{1-\gamma}{2}}|\boldsymbol{v}\overline{\boldsymbol{v}}\rangle|E^{\boldsymbol{v}}_{01}\rangle - \sqrt{\tfrac{1-\gamma}{2}}|\overline{\boldsymbol{v}}\boldsymbol{v}\rangle|E^{\boldsymbol{v}}_{10}\rangle + \sqrt{\tfrac{\gamma}{2}}|\boldsymbol{v}\boldsymbol{v}\rangle|E^{\boldsymbol{v}}_{00}\rangle - \sqrt{\tfrac{\gamma}{2}}|\overline{\boldsymbol{v}}\,\overline{\boldsymbol{v}}\rangle|E^{\boldsymbol{v}}_{11}\rangle \\
|E^{\boldsymbol{v}}_{01}\rangle &= \frac{1}{\sqrt{1-\gamma}}\left[\sqrt{1-\tfrac{3}{2}\gamma}|m_0\rangle + \sqrt{\tfrac{\gamma}{2}}\left(v_x|m_1\rangle + v_y|m_2\rangle + v_z|m_3\rangle\right)\right] \\
|E^{\boldsymbol{v}}_{10}\rangle &= \frac{1}{\sqrt{1-\gamma}}\left[\sqrt{1-\tfrac{3}{2}\gamma}|m_0\rangle - \sqrt{\tfrac{\gamma}{2}}\left(v_x|m_1\rangle + v_y|m_2\rangle + v_z|m_3\rangle\right)\right] \qquad (2.58) \\
|E^{\boldsymbol{v}}_{00}\rangle &= \frac{1}{\sqrt{2(1-v_z^2)}}\left[(-v_xv_z - iv_y)|m_1\rangle + (-v_yv_z + iv_x)|m_2\rangle + (1-v_z^2)|m_3\rangle\right] \\
|E^{\boldsymbol{v}}_{11}\rangle &= \frac{1}{\sqrt{2(1-v_z^2)}}\left[(-v_xv_z + iv_y)|m_1\rangle + (-v_yv_z - iv_x)|m_2\rangle + (1-v_z^2)|m_3\rangle\right].
\end{aligned}$$

A number of things are worth noting about this representation of the purification.

- With probability $1-\gamma$, Alice and Bob's measurement outcomes are opposite. With probability γ they are equal.
- We have $|E^{\boldsymbol{v}}_{10}\rangle = |E^{-\boldsymbol{v}}_{01}\rangle$ and $|E^{\boldsymbol{v}}_{11}\rangle = |E^{-\boldsymbol{v}}_{00}\rangle$. Furthermore $\langle E^{\boldsymbol{v}}_{00}|E^{\boldsymbol{v}}_{11}\rangle = 0$, and $|E^{\boldsymbol{v}}_{00}\rangle$, $|E^{\boldsymbol{v}}_{11}\rangle$ span a subspace orthogonal to $|E^{\boldsymbol{v}}_{01}\rangle$, $|E^{\boldsymbol{v}}_{10}\rangle$. Furthermore, $\langle E^{\boldsymbol{v}}_{01}|E^{\boldsymbol{v}}_{10}\rangle = \frac{1-2\gamma}{1-\gamma}$.
- It holds that $|\frac{-v_xv_z - iv_y}{\sqrt{1-v_z^2}}|^2 = 1 - v_x^2$ and $|\frac{-v_yv_z + iv_x}{\sqrt{1-v_z^2}}|^2 = 1 - v_y^2$.

After Alice and Bob performed a measurement in the same basis, Eve's auxiliary system is in state $\sigma^{\boldsymbol{v}}_{xy}$, given by

$$\sigma^{\boldsymbol{v}}_{xy} \stackrel{\mathrm{def}}{=} |E^{\boldsymbol{v}}_{xy}\rangle\langle E^{\boldsymbol{v}}_{xy}|. \qquad (2.59)$$

For a given basis set $\mathcal{B}$ and $b \in \mathcal{B}$, we will write σ^b_{st} instead of $\sigma^{\boldsymbol{v}}_{st}$, as the vector $\boldsymbol{v}$ is implicitly defined by the pair $(\mathcal{B}, b)$. Eve's state averaged over the measurement outcomes of Alice and Bob follows directly from (2.59)

$$\mathop{\mathbb{E}}_{st|b}\sigma^b_{st} = (1-\tfrac{3}{2}\gamma)|m_0\rangle\langle m_0| + \tfrac{\gamma}{2}\sum_{j=1}^{3}|m_j\rangle\langle m_j|. \qquad (2.60)$$

Notice that averaging over the measurement results yields a state that is independent of the encoding basis. This holds more generally.

Lemma 2.20. *Let ρ^{ABE} denote the purification of a 4^n-dimensional state ρ^{AB}. Let $b \in \mathcal{B}^n$ be a qubit-wise orthonormal basis. It holds that $\rho^{\mathrm{E}}_b = \rho^{\mathrm{E}}$.*

Proof: Let P^{A}_{bs} denote a projection operator on subsystem 'A' corresponding to a measurement in basis b with outcome $s \in \{0,1\}^n$. We have $\rho^{\mathrm{E}}_b \stackrel{\mathrm{def}}{=} \mathbb{E}_{st|b}\,\rho^{\mathrm{E}}_{bst} = \sum_{st}\mathrm{tr}_{\,\mathrm{AB}}(P^{\mathrm{A}}_{bs}\otimes P^{\mathrm{B}}_{bt}\otimes\mathbb{1})\rho^{\mathrm{ABE}} = \mathrm{tr}_{\,\mathrm{AB}}([\sum_s P^{\mathrm{A}}_{bs}]\otimes[\sum_t P^{\mathrm{B}}_{bt}]\otimes\mathbb{1})\rho^{\mathrm{ABE}} = \rho^{\mathrm{E}}$. We use the fact that $\sum_s P^{\mathrm{A}}_{bs} = \mathbb{1}$ and $\sum_t P^{\mathrm{B}}_{bt} = \mathbb{1}$ for any b. □

Von Neumann entropy

We use the description (2.59) to compute the relevant Von Neumann entropies in (2.55). From (2.60) we have

$$S(\mathop{\mathbb{E}}_{st|b}\sigma^b_{st}) = h(1-\frac{3}{2}\gamma,\frac{\gamma}{2},\frac{\gamma}{2},\frac{\gamma}{2}) = -(1-\tfrac{3}{2}\gamma)\log(1-\tfrac{3}{2}\gamma) - 3\tfrac{\gamma}{2}\log\tfrac{\gamma}{2}. \tag{2.61}$$

Using the fact that σ^b_{ss} and $\sigma^b_{s\bar{s}}$ are orthogonal we find

$$\mathop{\mathbb{E}}_{s} S(\mathop{\mathbb{E}}_{t|bs}\sigma^b_{st}) = S\big((1-\gamma)\sigma^b_{s\bar{s}} + \gamma\sigma^b_{ss}\big) = h(\gamma). \tag{2.62}$$

2.6.9 Rate of quantum key distribution

Using the von Neumann entropies we can write down our asymptotic bound on the security of six-state QKD.

$$\|\mathcal{E}_{\mathrm{QKD}} - \mathcal{F}_{\mathrm{QKD}}\|_\diamond < \tfrac{1}{2}(n+1)^{15}\min\Big(P_{\mathrm{acc}}, \sqrt{\varepsilon} + \sqrt{2^{\ell-\kappa-nh(\beta)+nh(1-\frac{3}{2}\gamma,\frac{\gamma}{2},\frac{\gamma}{2},\frac{\gamma}{2})+\mathcal{O}(\sqrt{n})}}\Big) + 4\cdot 2^{-\lambda} \tag{2.63}$$

where the term $4\cdot 2^{-\lambda}$ is a bound on the probability that (at least) one of the four classical MACs is forged. For small enough message sizes ℓ and noise thresholds β, (2.63) is exponentially small for every noise level γ. For $\gamma > \beta$ we have $\gamma_b > \beta$ for some γ_b and the accept probability (2.52) can be bounded by the Chernoff bound. For $\gamma \leq \beta$, ℓ can be chosen such that the square root in the min of (2.63) is exponentially small. The asymptotic rate of the protocol is computed from the greatest value of ℓ for which $\|\mathcal{E}_{\mathrm{QKD}} - \mathcal{F}_{\mathrm{QKD}}\|_\diamond$ is exponentially small at $\gamma = \beta$.

Error correcting codes exist that achieve the Shannon bound $\kappa = n - nh(\beta)$ asymptotically. Substituting this into (2.65) we find that we have to set ℓ slightly below $n - nh(1-\frac{3}{2}\beta,\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})$. When using a uniformly distributed basis B, the number of useful qubits n is approximately $\frac{1}{3}\nu$. By not using uniform, but rather very skewed probability distributions for the basis choice [LCA05], we get $\nu \approx n$ and we obtain the asymptotic rate of 6-state QKD

$$r_{6state} = \frac{\ell}{\nu} \approx \frac{\ell}{n} = 1 - h(1-\frac{3}{2}\beta,\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2}). \tag{2.64}$$

The six-state QKD protocol as depicted in Figure 2.3 has a higher round complexity than required. The round complexity can be reduced to two passes by Alice when Alice and Bob perform the channel monitoring on a random subset of the qubits. Bob generates a random subset $\mathcal{J}$ and sends it to Alice together with $b^{\mathrm{raw}\prime}$ and $x^{\mathrm{raw}\prime}_{\mathcal{J}}$. Alice can now do the noise check for the subset $\mathcal{J}$ and discard $x_{\mathcal{J}}$. When $\omega = 1$ she sends $\mathcal{I}, e, \omega, u, c$ all together. The downside of this approach is that if $\Pr[B = b] \approx 1$ for some basis choice b, the subset $\mathcal{J}$ might not include enough checks in every basis. The fraction of bases $b' \neq b$ needs to be high enough to be confident about the noise level in that basis. In the coming chapters, when we make comparisons to "6-state QKD". We will understand this as a highly optimized form of 6-state QKD which has the rate given in (2.64) and where Alice needs only two passes.

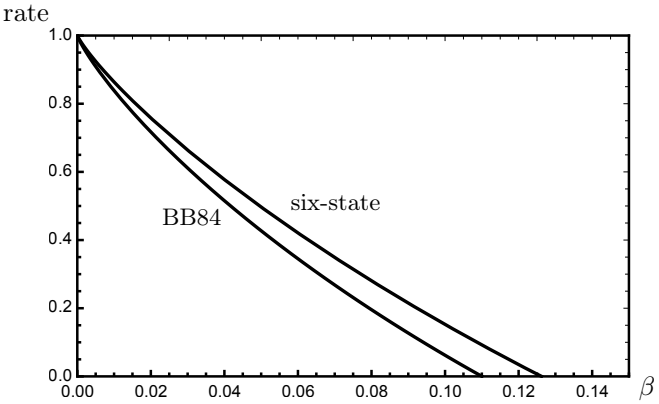

Figure 2.5: *Asymptotic QKD rates for the BB84 and six-state encodings as a function of the noise with one-way post-processing.*

A version of BB84 that follows exactly the steps of Section 2.6.2, but uses a 4-state encoding, e.g. only the x- and z-basis, can be proven secure using the same derivation. The only difference is that the y-basis constraint (2.56) does not exist. This leaves an extra degree of freedom in the state of Eve that she can use to maximize $S(\mathbb{E}_{bs}\,\sigma_{bs}) - \mathbb{E}_{s|b}\,S(\sigma_{bs})$. The outcome is the well known asymptotic BB84 rate [Ren05, SP00, TL17].

$$r_{4state} = 1 - 2h(\beta). \tag{2.65}$$

The rates of 4- and 6-state QKD are plotted as a function of the noise Alice and Bob tolerate in Figure 2.5.

The QKD rates given are with one-way post-processing i.e. without increasing the round complexity. In his thesis [Ren05], Renato Renner discussed advantage distillation and noisy preprocessing. In six-state QKD, noisy preprocessing increases the maximal error rate Alice and Bob can tolerate from $\approx$12.6% to $\approx$14.1% without increasing the round complexity. Advantage distillation requires an increase in the round complexity. Combined with noisy preprocessing an error rate of $\approx$ 27.6% can be achieved. We will consider the QKD rates given in (2.64) and (2.65) as the 'QKD rate with one-way post-processing'. Advantage distillation is not considered. Noisy preprocessing may also increase the maximal rate of protocols in future chapters, but this will not be the focus of this thesis.

This proof of the security of QKD does not yield new results but is meant to demonstrate how the proof method works. We already saw that the method allows us to prove the security of BB84, six-state QKD and QKD with non-uniform bases alike [BB84, BPG99, LCA05]. The versatility of the method is used to prove the security for different types of protocols and in different security models in the following chapters.

Chapter 3
High rate quantum key recycling

Why all the back and forth?
After a long struggle to get all their equipment set up and working correctly, Alice and Bob finally manage to shake off Murphy's law and get their QKD scheme up and running. They are happy to have seen a security proof and are confident that as long as they keep Eve out of their labs, there is no way Eve gets to listen in on any of their conversations. However, they are not yet all that satisfied about the efficiency of their communication. They are still discarding a fraction of the qubits they send and looking at Figure 2.3 they feel there is too much communication back and forth going on. The first problem can in principle be solved by using non-uniform basis choices, but the second is an inherent property of QKD. If only Bob knew Alice's encoding basis, he could just measure and compute her message directly without throwing away any qubits or needing to tell Alice what basis he used. But wouldn't this waste a lot of their shared key material? They dive back into literature and it turns out that very recently a *quantum key recycling scheme* was proven secure [BBB82, FS17]. This scheme allows users to exchange quantum states with a pre-shared basis choice and to re-use their basis choices so no keys will be wasted! Unfortunately, the proof of this scheme results in a low rate even when there is little noise on the quantum channel. To achieve a good rate, a new security proof and maybe an updated scheme is required.

3.1 Introduction

3.1.1 Quantum Key Recycling

The idea of quantum key recycling (QKR) is not new. Two years before the invention of quantum key distribution (QKD), the possibility of QKR was considered [BBB82]. Let Alice and Bob encrypt classical data as quantum states, using a classical key to determine the basis in which the data is encoded. If they do not detect any manipulation of the quantum states, then Eve has learned almost nothing about the encryption

This chapter is based on [LŠ19a]. The comparison with the literature has changed with respect to the publication.

key, and hence it is safe for Alice and Bob to re-use the key. A QKR protocol can achieve better round complexity than QKD, since communication about basis choices is avoided. After the discovery of QKD, interest in QKR was practically nonexistent for a long time. QKR received some attention again in 2003 when Gottesman [Got03] proposed an Unclonable Encryption scheme with partially re-usable keys. In 2005 Damgård, Pedersen and Salvail introduced a scheme that allows for complete key recycling, based on mutually unbiased bases in a high-dimensional Hilbert space [DPS05]. Though elegant, their scheme unfortunately needs a quantum computer for encryption and decryption. In 2017 Fehr and Salvail [FS17] introduced a qubit-based QKR scheme (similar to [BBB82]) that does not need a quantum computer. They were able to prove its security but achieve low rates even at low noise levels. Škorić and de Vries [ŠdV17] proposed a variant with 8-state encoding, aiming for high rate, but the security was not proven. Attacks on the qubit-based QKR schemes of [FS17, ŠdV17] were studied in [LŠ18], but that did not yield a security proof.

3.1.2 Rate of [FS17]

Fehr and Salvail [FS17] constructed a qubit-based authentication scheme similar to [BBB82]. They proved the security using entanglement monogamy. It is the first rigorously proven qubit-based prepare-and-measure QKR scheme. When adding encryption to the authentication scheme, the rate suffers a penalty. A term $3\log|\mathcal{M}|$ is added to the number of qubits n to send a message $m \in \mathcal{M}$. Their asymptotically achievable rate is $r = \frac{1}{3} - h(\beta)$ with β the noise parameter. The rate is positive up to a noise of $\beta \approx 6\%$ on the quantum channel. We would expect to achieve a rate of 1 in the noiseless case, at least for the 8-state encoding, see Section 3.1.3.

Our aim is to obtain a tighter bound on the rate, for all encoding schemes. We will allow the key to be modified in the recycling step while [FS17] is able to re-use the key in unmodified form. We believe this is unimportant in a practical setting, although it can provide benefits in the setting of unclonable encryption, see Chapter 5.

3.1.3 Eight state encoding

As discussed in Section 2.3.2, the BB84 encoding uses the $\pm z$ and $\pm x$ directions of the Bloch sphere and the six-state encoding uses $\pm z, \pm x$ and the $\pm y$ directions. When encoding a qubit using the BB84 or six-state encoding, there exists a measurement that yields some information about the payload. Although this will cause noise on the channel, which is detectable by Alice and Bob, it shows that 4- or 6-state encoding is not a true encryption.

In the 8-state encoding [ŠdV17] we have $\mathcal{B} = \{0,1,2,3\}$ and the eight states are the corner points of a cube on the Bloch sphere. We write $b = 2u + w$, with $u, w \in \{0,1\}$. The states are

$$|\psi_{uwg}\rangle = (-1)^{gu}\left[(-\sqrt{i})^g \cos\tfrac{\alpha}{2}|g \oplus w\rangle + (-1)^u(\sqrt{i})^{1-g}\sin\tfrac{\alpha}{2}|\overline{g \oplus w}\rangle\right]. \tag{3.1}$$

The angle α is defined as $\cos\alpha = 1/\sqrt{3}$. For given databit $g \in \{0,1\}$, the four states $|\psi_{uwg}\rangle$ are the Quantum One-Time Pad (QOTP) encryptions [AMTdW00,

Leu02, BR03] of $|\psi_{00g}\rangle$. The 'plaintext' states $|\psi_{000}\rangle$, $|\psi_{001}\rangle$ correspond to the vectors $\pm(1,1,1)/\sqrt{3}$ on the Bloch sphere. The 8-state encoding does provide a true encryption. When the basis is unknown, there exists no measurement that yields any information about the qubit payload. In QKD this is not a useful property since in Eve's strongest attack, she waits for the basis to be revealed before measuring. When the basis is not revealed however, the 8-state encoding is a true encryption while the BB84 and six-state encodings leak partial information on the payload.

In [ŠdV17] a QKR protocol was constructed that attempts to leverage the encryption property of the 8-state encoding but a security proof was not provided. In [LŠ18] optimal attacks on 4-, 6- and 8-state encodings are discussed in terms of accessible information and min-entropy. It was shown that the strongest collective attacks on the plaintext as well as the strongest collective attacks on the basis at known plaintext reveal more information for the 4- and 6-state encoding than for the 8-state encoding. This is true for both the accessible information and the min-entropy. Although the leakage of the payload and the basis is lower for the 8-state encoding than the 6-state encoding, when considering the combined leakage of the payload and the basis this advantage disappears. In the QKR protocol presented in the chapter we always care about the *combined* leakage. We will see that this removes the need to use the 8-state encoding. The 6-state and 8-state encodings will yield the same rate because Eve can obtain the same state, see the following lemma.

Lemma 3.1. *The Bell diagonal form of Eve's state given by* $\tilde{\sigma}^{\mathrm{AB}} = \lambda_0|\Psi^-\rangle\langle\Psi^-| + \lambda_1|\Phi^-\rangle\langle\Phi^-| + \lambda_2|\Psi^+\rangle\langle\Psi^+| + \lambda_3|\Phi^+\rangle\langle\Phi^+|$ *has the same values of* λ_i *for the noise checks in 6-state encoding (2.57) as for the noise checks in the 8-state encoding.*

Proof: Without loss of generality we take the 0-basis to be the z-basis. For the 6-state encoding the state $\tilde{\sigma}^{\mathrm{AB}}$ was subject to the constraints of (2.56). For the 8-state encoding, the constraints are for the 8-state encodings. We have $\langle 0|\tilde{\sigma}^{\mathrm{AB}}|0\rangle = \frac{1}{2}\lambda_2 + \frac{1}{2}\lambda_3 = \frac{\gamma}{2}$. The $b = 1$ and $b = 3$ constraints each give, after some algebra, $\frac{1}{18}(7\lambda_1 + 8\lambda_2 + 3\lambda_3) = \frac{\gamma}{2}$. The $b = 2$ constraint gives $\frac{1}{18}(\lambda_1 + 8\lambda_2 + 9\lambda_3) = \frac{\gamma}{2}$. Solving for the λ-parameters yields $\lambda_1 = \lambda_2 = \lambda_3 = \frac{\gamma}{2}$. □
The simple form of the averaged $\mathbb{E}_{st}\,\sigma^b_{st}$ (2.60) holds for the 8-state encoding as well.

3.1.4 Quantum key recycling with key update

Quantum key recycling has the potential to send information-theoretically secure message with a lower round complexity than QKD. The only qubit-based QKR scheme that is proven to be secure [FS17] has a rate $< \frac{1}{3}$. For the 8-state encoding especially it is clear that there is a gap between the rate that is proven secure and the actual secure rate.

We aim to construct a QKR protocol that is secure for a large noise regime and prove it achieves high rate secure communication. We don't require the unaltered re-use of key material, but instead allow new keys to be derived for each new round. Naturally, our protocol should have forward secrecy. It will work with different (4-state, 6-state, 8-state) encodings such that the rate can be increased by utilizing the entire Bloch sphere. The security of our QKR scheme should be composable with other protocols including multiple instances of itself.

We construct such a protocol in Section 3.3.2 and prove its security following the recipe of Section 2.5. The security proof differs from [FS17]. We treat all keys on the same footing. We find that for asymptotically large messages, the rate equals the rate of QKD with one-way postprocessing (i.e. without two-way advantage distillation). This means that whenever it is possible to do one-way-postprocessing-QKD, it is also possible to do QKR at the same asymptotic rate and hence get the benefit of reduced communication complexity. For finite n, our approach without smoothing yields a rate $\approx 1-h(\gamma)-2\log[\sqrt{(1-\frac{3}{2}\gamma)(1-\gamma)}+\sqrt{\frac{3}{2}\gamma(1+\gamma)}]$, where h is the binary entropy function. Both these results are more favorable than what one would expect based on the min-entropy analysis in [LŠ18] and than the entanglement monogamy analysis in [FS17].

3.2 QKR security notions and proof structure

A secure quantum key recycling protocol has to satisfy four requirements:

- Encryption: Eve learns nothing about the encrypted message.
- Key Recycling: it must be safe to use the future keys, even if Eve knows the plaintext.
- Forward secrecy: a compromise of future keys shouldn't impact past messages.
- Correctness: Alice and Bob hold the same future keys and when the round is successful the same message.

The first three properties are covered by ε-ENC, ε-KR and ε-FS in Definitions 2.4, 2.7 and 2.9. Using Lemma 2.10 we know that all these properties are guaranteed by a single condition $\|\rho^{M\tilde{K}CT\mathrm{E}}-\rho^{M}\otimes\rho^{\tilde{K}}\otimes\rho^{CT\mathrm{E}}\|_1$. We will follow the steps laid out in Section 2.5. We prove the security in the asymptotic limit of many qubits as well as for a finite number of qubits. The asymptotic proof will be very similar to the QKD example of Section 2.6. Moving to an EPR version of the protocol, the same invariance to permutation and random Paulis is used in the equivalent protocol (step 1 and 2). Next the CPTP maps corresponding to the equivalent protocol are obtained systematically (step 3). The smoothing step (step 4) is used in the asymptotic case. The finite size analysis follows the same recipe, except the optional smoothing of step 4 is skipped. Step 5 and 6 use post-selection and Eve's simple 4-dimensional state to arrive at smooth Rényi entropies in the asymptotic case. In the finite size analysis, the operator square root can than be computed explicitly thanks to the diagonal form of the operator.

The correctness of the message and future keys is guaranteed by authentication tags that authenticate the classical communication as well as the qubit payload. From these authenticated variables, Bob reconstructs the message and the future keys.

3.3 Protocol

3.3.1 Protocol intuition

When Eve gets hold of a quantum state encoding of an unknown bit x in an unknown basis b, she can attempt to learn about x, about b or more generally about the combination of x and b. For a given noise level on the quantum channel, we can bound the total amount of information she can gather. Typically, a quantum protocol protects the payload x with privacy amplification and either publishes b (QKD) or re-uses b ([BBB82, FS17, ŠdV17]). We allow the next round basis to be a function of the initial basis rather than an exact copy of it. We can then exploit Eve's ignorance about the combination of the payload and the basis to construct a one-time pad *and* the next round basis using a single instance of the privacy amplification function. The same principles that guarantee the security of the one-time pad in QKD, then guarantee the security of the one-time pad and the future basis in QKR. Due to the similar structure, a proof similar to the proof of QKD should hold. In the proof Eve's uncertainty about x holding her ancilla and b should be replaced by her knowledge on the combination of b and x holding only her ancilla. It turns that these uncertainties are bound by the same expression.

Like in QKD, a ciphertext is sent over a classical channel. However, since the basis choice is part of the initial key material, the ciphertext is known and can be sent at the same time as the quantum states. Together with the error correction information and a shared hash seed, this allows Bob to decrypt and reconstruct the classical message without the need for communication back and forth. The security of the future key depends on the noise on the channel. When Bob detects too much noise, he needs to inform Alice to not use the future key. Therefore a single authenticated feedback bit is required from Bob to Alice.

3.3.2 A single round of the QKR protocol

The protocol introduced has many similarities with the QKR scheme #2 proposed in [ŠdV17] and the QEMC* scheme of Fehr and Salvail [FS17]. The most important differences are:

- Some key refreshment of the basis key occurs even in case of an accept.
- We derive the one time pad not only from the qubits' payload but also from the basis key. With this construction it becomes evident that rate 1 (at zero noise) can be achieved not only using 8-state encoding but also using 4- and 6-state encodings.
- We combine the privacy amplification and the key refreshment into a single hashing operation. This simplifies the security proof.
- Part of the message is used to communicate keys for the next round. Consequently the scheme does not consume existing key material.

Alice and Bob have agreed on a family of pairwise independent hash functions $\Phi_u : \{0,1\}^n \times \mathcal{B}^n \to \{0,1\}^\ell \times \mathcal{B}^n$ with $u \in \mathcal{U}$, a MAC function $\Gamma : \{0,1\}^{2\lambda} \times \{0,1\}^{n+\ell+a} \to$

$\{0,1\}^\lambda$, and a linear error-correcting code with syndrome function $\texttt{Syn} : \{0,1\}^n \to \{0,1\}^{n-\kappa}$ and decoder $\texttt{SynDec}$: $\{0,1\}^{n-\kappa} \to \{0,1\}^n$. They adopt the channel monitoring procedure of Definition 2.18: the $\texttt{NoiseCheck}$ function outputs 1 only if the noise for every basis is smaller than the threshold β. Let **QKR** be a single round the quantum key recycling protocol. It consists of the following steps, also see Figure 3.1.

QKR.Gen:

Alice and Bob generate shared key material consisting of several parts: a basis sequence $b \in \mathcal{B}^n$, two MAC keys $k^1_{\text{MAC}}, k^2_{\text{MAC}} \in \{0,1\}^{2\lambda}$, an extractor key $u \in \mathcal{U}$, and a classical one-time pad $k_{\text{syn}} \in \{0,1\}^{n-\kappa}$ for protecting the syndrome. In addition Alice and Bob share a reservoir of key material to refresh their shared keys.

Alice generates the plaintext $m_{\text{bare}} \in \{0,1\}^{\ell'}$, with $\ell' \stackrel{\text{def}}{=} \ell - 2\lambda - n + \kappa$. She generates local randomness $x \in \{0,1\}^n$ and $k \in \{0,1\}^{2\lambda+n-\kappa}$. She concatenates m_{bare} and k to form augmented message $m = m_{\text{bare}} \| k \in \{0,1\}^\ell$.

QKR.Enc:

Alice performs the following steps. Compute $e = k_{\text{syn}} \oplus \texttt{Syn}(x)$ and $z||b' = \Phi_u(x||b)$. Compute the ciphertext $c = m \oplus z$ and the authentication tag $\tau = \Gamma(k_{\text{MAC}}, x||c||e)$. Prepare the quantum state $|\Psi\rangle = \bigotimes_{i=1}^n |\psi^{b_i}_{x_i}\rangle$. Send $|\Psi\rangle$, e, c, τ to Bob.

QKR.Meas:

Bob measures $|\Psi\rangle'$ in the b-basis yielding $x' \in \{0,1\}^n$.

QKR.Post:

Bob recovers $\hat{x} = x' \oplus \texttt{SynDec}(k_{\text{syn}} \oplus e \oplus \texttt{Syn}\, x')$. Computes $\hat{z}||\hat{b}' = \Phi_u(\hat{x}||b)$ and $\hat{m} = c \oplus \hat{z}$. He performs the channel monitoring $\omega = \texttt{NoiseCheck}(b, \hat{x}, x')$. He accepts only if $\tau == \Gamma(k^1_{\text{MAC}}, \hat{x}||c||e)$ holds and $\omega == 1$. He communicates the feedback bit (accept/reject) to Alice (publicly but with authentication using k^2_{MAC}). If the tag authenticated successfully, he parses $\hat{m}$ as $\hat{m}_{\text{bare}}||\hat{k}$.
Alice and Bob perform the following updates for the next round.

- In case of reject: Take completely new keys $k^1_{\text{MAC}}, k^2_{\text{MAC}}, k_{\text{syn}}, b, u$.
- In case of accept: Set $b \leftarrow b'$, $(k^1_{\text{MAC}}||k^2_{\text{MAC}}||k_{\text{syn}}) \leftarrow k$. The key u is re-used.

The protocol uses up $2\lambda + n - \kappa$ bits of key material (the two single-use MAC keys[1] and the one-time pad k_{syn}) but also delivers the same amount in the augmented message m; hence the net effect in case of accept is that Alice and Bob expend no key material. The size of the syndrome $n-\kappa$ depends on the noise level and on the choice of error-correcting code. See Section 3.4.7 for a discussion of the balance between message length and syndrome length.

[1] Only λ bits have to be used up per MAC, e.g. the tag can be one-time padded and only the pad can be refreshed in every round.

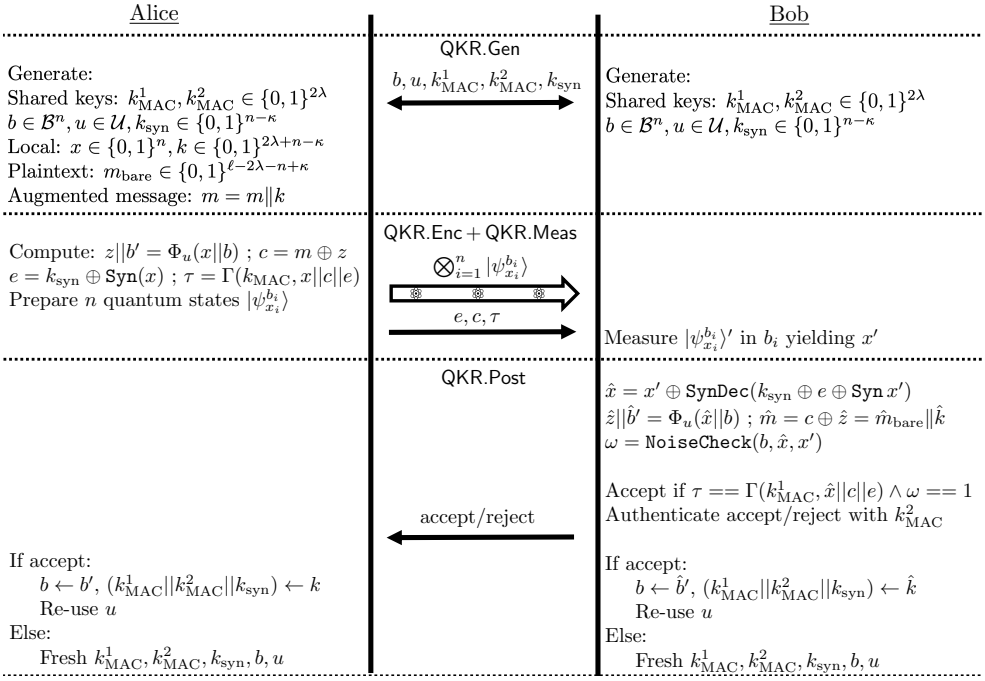

Figure 3.1: The procedure of the quantum key recycling protocol. The $\texttt{NoiseCheck}(b, x, x')$ function is defined in Definition 2.18.

3.4 Security proof

3.4.1 Multiple rounds of quantum key recycling

As discussed in Section 2.4.4, two protocols that are proven secure using our security definitions based on diamond distances, are also secure when executed in succession. This property can be used on multiple instances of the same protocol. We will prove the security of a single round of the QKR protocol and rely on composability to guarantee the security of the repeated use of QKR. Let $\mathcal{E}$ be the CPTP map that describes one round of the QKR protocol. Let $\mathcal{F}$ denote an 'ideal', perfectly secure version of $\mathcal{E}$ such that $\|\mathcal{E} - \mathcal{F}\|_\diamond \leq \varepsilon$ implies 2ε-encryption and 4ε-recycling. We say that one round of the QKR protocol is ε-secure when $\|\mathcal{E} - \mathcal{F}\|_\diamond \leq \varepsilon$. Lemma 2.12 then implies two round of the protocol are then 2ε-secure. By induction the scheme is then $N\varepsilon$-secure after N rounds.

3.4.2 Correctness

In the QKR protocol of Section 3.3.2, the correctness of the final message $\hat{m}$ is guaranteed by the authentication tag that authenticates x, c, e. The probability that this tag is forged is at most $2^{-\lambda}$. An additional tag is used to authenticate the feedback

bit form Alice to Bob, this adds an additional failure probability of $2^{-\lambda}$. When the two tags successfully authenticate the classical bits, both the future keys and the plaintext held by Alice and Bob are the same with a probability of at least $1 - 2^{1-\lambda}$. The failure probability is part of the final diamond distance.

3.4.3 Equivalent EPR protocol (step 1 and 2)

We work with the EPR version of the protocol. Alice preparing the state $|\psi_x^b\rangle$ is replaced by the following. Eve creates a noisy version the singlet state $|\Psi^-\rangle$ and sends half the state to Alice and the other half to Bob. Alice performs a measurement in the b-basis on her half of the EPR pair yielding s. The remaining half of the pair, held by Bob, then encodes a random payload $\bar{s}$ in the b basis. Bob measures in the b basis yielding t. Alice computes $a = x \oplus s$ and sends a to Bob over an authenticated channel. Bob then recovers x' a noisy version of x by computing $x' = a \oplus \bar{t}$. Both measurements act on the 16-dimensional quantum state ρ^{ABE}. If Eve is to have any hope of being undetected the ρ^{AB} subsystem should be close to $(|\Psi^-\rangle\langle\Psi^-|)^{\otimes n}$. In principle ρ^{ABE} could depend on e, c and m.[2] The syndrome is perfectly protected by k_{syn} so e is no help and Eve's ancilla does not depend on it in our analysis. The c, m dependence is not explicitly written out in our proof method. The relevant quantum state held by Eve is simplified by the randomization as argued in Section 2.5.6. For this description to hold, c, m must be decoupled from x so that x is uniform even in the known-plaintext scenario. This is guaranteed by the pairwise-independent hash function that decouples z from x when u is unknown[3] (as will be explicitly visible in Step 4 of the proof). Security of the EPR version of the protocol implies security of the original protocol by the argument in Section 2.5.1.

Like in the QKD proof, we apply a random permutation and a random Pauli operator. Since we are again working with uniform b, x, x', identical arguments to Sections 2.5.2 and 2.6.4 demonstrate the equivalence. In short, the uniformity of b, x, x' guarantees that the statistics of the output of the protocol are invariant to permutations of the input. Applying a random Pauli matrix to the qubits is equivalent to flipping the classical measurement outcomes publicly with probability $\frac{1}{2}$. In addition we replace the classical channels with authenticated classical channels. The steps in a single round of the modified protocol QKR' are described below and shown in Figure 3.2.

QKR'.Gen:

Alice and Bob generate shared key material consisting of several parts: a basis sequence $b \in \mathcal{B}^n$, an extractor key $u \in \mathcal{U}$, a classical one-time pad $k_{\mathrm{syn}} \in \{0,1\}^{n-\kappa}$ for protecting the syndrome and two MAC keys $k^1_{\mathrm{MAC}}, k^2_{\mathrm{MAC}} \in \{0,1\}^{2\lambda}$. In addition Alice and Bob share a reservoir of key material to refresh their shared keys.

Alice generates the plaintext $m_{\mathrm{bare}} \in \{0,1\}^{\ell'}$, with $\ell' \stackrel{\mathrm{def}}{=} \ell - 2\lambda - n + \kappa$. She generates local randomness $x \in \{0,1\}^n$ and $k \in \{0,1\}^{2\lambda+n-\kappa}$. She concatenates m_{bare} and k to form augmented message $m = m_{\mathrm{bare}} \| k \in \{0,1\}^{\ell}$. She generates a ran-

[2] Independence of a is by construction as argued in Section 2.6.3.

[3] Pairwise independence can be viewed as padding m with part of the hash seed and applying a universal hash function on the result, see the example in Section 2.2.3.

dom permutation π of the n qubits positions and random indices $\alpha \in \{0,1,2,3\}^\nu$ for the random Pauli.

QKR'.Enc:

Eve prepares n noisy EPR pairs in the $|\tilde{\Psi}^-\rangle$ state and sends half of each pair to Alice and the other half to Bob.

Alice applies the permutation π to her n qubits and applies α_i to the ith qubit. She measures the ith half EPR pair in b_i yielding s_i. She performs the following steps. She computes $a = s \oplus x$, $e = k_{\text{syn}} \oplus \texttt{Syn}(x)$, $z||b' = \Phi_u(x||b)$ and the ciphertext $c = m \oplus z$. Send a, e, c, π, α to Bob.

QKR'.Meas:

Bob applies the permutation π to his n qubits, and applies α_i to the ith qubit. He measures the ith half in b_i yielding $t \in \{0,1\}^n$. He computes $x' = \bar{t} \oplus a$.

QKR'.Post:

Bob recovers $\hat{x} = x' \oplus \texttt{SynDec}(k_{\text{syn}} \oplus e \oplus \texttt{Syn}\, x')$. Computes $\hat{z}||\hat{b}' = \Phi_u(\hat{x}||b)$ and $\hat{m} = c \oplus \hat{z}$. He performs the channel monitoring $\omega = \texttt{NoiseCheck}(b, x, x')$. He accepts only if $\omega == 1$. He sends the feedback bit ω to Alice. In case of accept he parses $\hat{m}$ as $\hat{m}_{\text{bare}}||\hat{k}$.

Alice and Bob perform the following updates for the next round.

- In case of reject: Take completely new keys $k^1_{\text{MAC}}, k^2_{\text{MAC}}, k_{\text{syn}}, b, u$.
- In case of accept: Set $b \leftarrow b'$, $(k^1_{\text{MAC}}, k^2_{\text{MAC}}, k_{\text{syn}}) \leftarrow k$. The key u is re-used.

3.4.4 The CPTP maps (step 3)

The action of one QKR' round on the n noisy EPR states is denoted as $\mathcal{E}_{\text{QKR}}$. The $\mathcal{E}_{\text{QKR}}$ comprises generation $\mathsf{QKR'.Gen}$, measurements by Alice and Bob $\mathsf{QKR'.Enc}$ and $\mathsf{QKR'.Meas}$ and post-processing $\mathsf{QKR'.Post}$,

$$\mathcal{E}_{\text{QKR}} = \mathsf{QKR'.Post} \circ \mathsf{QKR'.Meas} \circ \mathsf{QKR'.Enc} \circ \mathsf{QKR'.Gen} \tag{3.2}$$

In the generation step the message and all the keys are fetched and put in working memory. The exact procedure for the generation of shared keys in the first round if left open. The generation process has to be composably secure.

In $\mathsf{QKR'.Enc}$ and $\mathsf{QKR'.Meas}$, Eve creates the state ρ^{ABE} on which Alice and Bob perform their measurement (the permutation and random Pauli are treated in step 6 of the proof). They read out the state of the basis key register b and then perform a measurement in this basis, resulting in values s, t held by Alice and Bob respectively. Alice computes $a = x \oplus s$, $e = k_{\text{syn}} \oplus \texttt{Syn}(x)$, $z||b' = \Phi_u(x||b)$ and $c = m \oplus z$, Bob computes $x' = a \oplus \bar{t}$. Let $\mathcal{M}$ be a shorthand notation for $\mathsf{QKR'.Meas} \circ \mathsf{QKR'.Enc} \circ \mathsf{QKR'.Gen}$.

$$\begin{aligned}\mathcal{M}(\rho^{\text{ABE}}) \quad = \quad & \mathop{\mathbb{E}}_{mubk_{\text{syn}}} |mubk_{\text{syn}}\rangle\langle mubk_{\text{syn}}| \mathop{\mathbb{E}}_{stx} \sum_{ax'zb'c} |staxx'ezb'c\rangle\langle staxx'ezb'c| \\ & \delta_{a,x\oplus s}\delta_{x',a\oplus\bar{t}}\delta_{e,k_{\text{syn}}\oplus\texttt{Syn}\,x}\delta_{z\|b',\Phi_u(x\|b)}\delta_{c,m\oplus z} \otimes \rho^{\text{E}}_{bst}. \end{aligned} \tag{3.3}$$

Here the expectations over u, b, k_{syn}, x are uniform. The $\mathbb{E}_m$ is not necessarily uniform because m contains the plaintext message m_{bare}. The notation $\mathbb{E}_{st}(\cdot)$ stands for

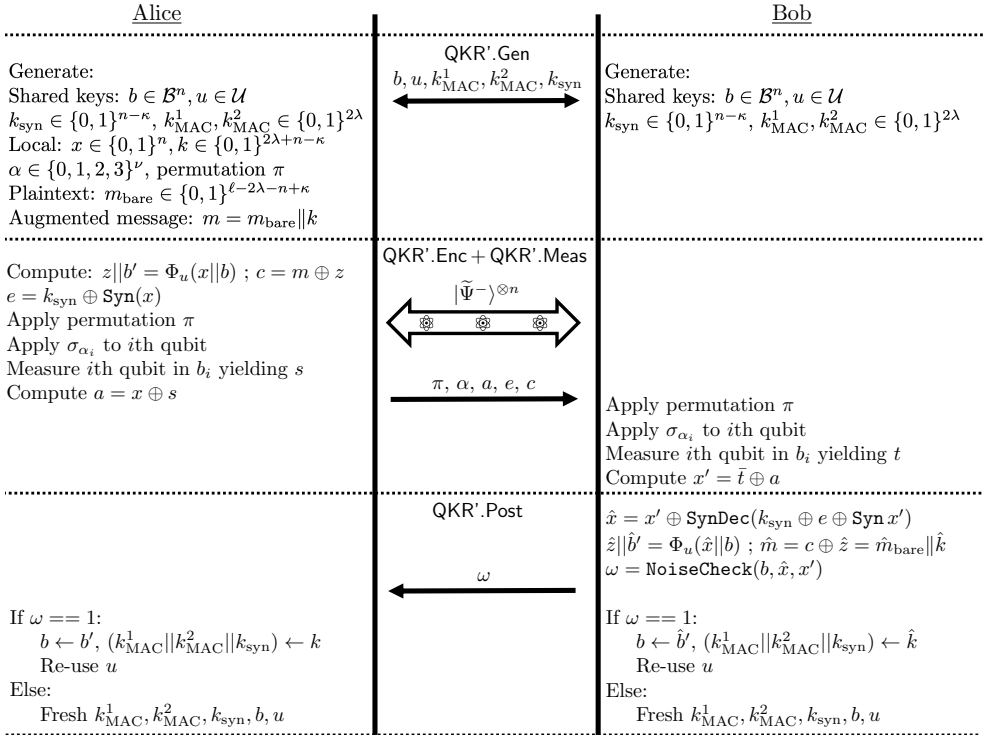

Figure 3.2: The procedure of QKR'. The $\mathtt{NoiseCheck}(b, x, x')$ function is defined in Definition 2.18.

$\sum_s 2^{-n} \sum_t p_{t|s}(\cdot)$, where $p_{t|s}$ depends on ρ^{ABE}. We will see in step 5 that when ρ^{ABE} is in factorized form $p_{t|s}$ is simple.

In the post-processing step the feedback bit ω as well as the next round keys $\tilde{u}, \tilde{b}$ are computed. We distinguish between *output variables* and *internal variables*. The list of output variables comprises the plaintext m_{bare}, the keys for the next round $(\tilde{u}, \tilde{b}, k)$ and the transcript e, c, τ, ω visible to Eve. The internal variables are traced over in the computation of the output.

We will ignore the authentication tags since we handle the possibility of each MAC failure by adding $2^{-\lambda}$ to the trace distance. We introduce the indicator variable $\theta_{bst} \in \{0,1\}$ which denotes the success of the protocol $\theta_{bst} = \mathtt{NoiseCheck}(b, s, \bar{t})$. When $\omega = 1$ each 'hatted' variable equals the variable without hat.

We write down the intermediate state including internal variables and then trace

them out. We have

$$\rho^{\overbrace{STXX'UBZB'K_{\rm syn}}^{\text{internal}}\overbrace{\tilde{B}\tilde{U}MAEC\Omega E}^{\text{output}}} \tag{3.4}$$
$$= \mathop{\mathbb{E}}_{stxubk_{\rm syn}} \sum_{x'zb'e} |stxx'ubzb'k_{\rm syn}\rangle\langle xyubzb'k_{\rm syn}| \otimes \mathop{\mathbb{E}}_{m} \sum_{\tilde{b}\tilde{u}aec\omega} |\tilde{b}\tilde{u}maec\omega\rangle\langle\cdots| \otimes \rho^{\rm E}_{bst}$$
$$\delta_{a,x\oplus s}\delta_{x',a\oplus\bar{t}}\delta_{e,k_{\rm syn}\oplus {\tt Syn}\, x}\ \delta_{z||b',\Phi_u(x||b)}\ \delta_{c,m\oplus z}\ \left\{\omega\theta_{bst}\delta_{\tilde{u}u}\delta_{\tilde{b}b'} + \bar{\omega}\overline{\theta_{bst}}\frac{1}{|B||U|}\right\}.$$

The protocol output is given by
$\mathcal{E}_{\rm QKR}(\rho^{\rm ABE}) = {\rm tr}_{\,STXX'UBZB'K_{\rm syn}}\rho^{STXX'UBZB'K_{\rm syn}\tilde{B}\tilde{U}MAEC\Omega E} = \rho^{\tilde{B}\tilde{U}MAEC\Omega E}$.

$$\rho^{\tilde{B}\tilde{U}MAEC\Omega E} = \mathop{\mathbb{E}}_{\tilde{b}\tilde{u}mae} \sum_{c\omega} 2^{-\ell} |\tilde{b}\tilde{u}maec\omega\rangle\langle\cdots| \otimes [\omega\rho^{E}_{\tilde{b}\tilde{u}mac,[\omega=1]} + \bar{\omega}\rho^{E}_{\tilde{b}\tilde{u}mac,[\omega=0]}] \tag{3.5}$$

$$\rho^{\rm E}_{\tilde{b}\tilde{u}mac,[\omega=1]} = \mathop{\mathbb{E}}_{st} \sum_{b} \theta_{bst} 2^{\ell} \delta_{(m\oplus c)||\tilde{b},\Phi_{\tilde{u}}(s\oplus a||b)} \rho^{\rm E}_{bst} \tag{3.6}$$

$$\rho^{E}_{\tilde{b}\tilde{u}mac,[\omega=0]} = \mathop{\mathbb{E}}_{bst} \overline{\theta_{bst}} \rho^{\rm E}_{bst}. \tag{3.7}$$

Where we write $\mathbb{E}_a = 2^{-n}\sum_a$. The states with subscript $[\omega = 1]$ are sub-normalized and their trace is the accept probability. The trace of states with subscript $[\omega = 0]$ is the reject probability. Note that the error correction information E is completely decoupled from the rest, since it is a one-time-pad encryption.

Next we describe the action of the ideal protocol $\mathcal{F}_{\rm QKR}$ systematically as described in step 3 of the proof method, i.e. we trace out the message and future keys from the output of $\mathcal{E}_{\rm QKR}$ and replace them by decoupled variables. We write $\mathcal{F}_{\rm QKR} = \mathcal{R}\circ\mathcal{E}_{\rm QKR}$, where $\mathcal{R}$ replaces $\tilde{b}\tilde{u}m$ with random[4] values that have no coupling to Eve's state[5]

$$\mathcal{F}_{\rm QKR}(\rho^{\rm ABE}) = \mathcal{R}(\rho^{\tilde{B}\tilde{U}MAEC\Omega E}) = \mathop{\mathbb{E}}_{\tilde{b}\tilde{u}m} |\tilde{b}\tilde{u}m\rangle\langle\tilde{b}\tilde{u}m| \otimes \rho^{AEC\Omega E}. \tag{3.8}$$

We will derive an upper bound on $\|\mathcal{E}_{\rm QKR} - \mathcal{F}_{\rm QKR}\|_\diamond$. By taking a partial trace of (3.5) we find $\rho^{AEC\Omega E}$.

$$\rho^{AEC\Omega E} = \mathop{\mathbb{E}}_{m} |m\rangle\langle m| \otimes \chi^{EC} \otimes \sum_{\omega} |\omega\rangle\langle\omega| \otimes [\omega\rho^{\rm E}_{[\omega=1]} + \bar{\omega}\rho^{\rm E}_{[\omega=0]}] \tag{3.9}$$

$$\rho^{E}_{[\omega=1]} = \mathop{\mathbb{E}}_{bst} \theta_{bst}\rho^{\rm E}_{bst} \tag{3.10}$$

$$\rho^{E}_{[\omega=0]} = \mathop{\mathbb{E}}_{bst} \overline{\theta_{bst}}\rho^{\rm E}_{bst}. \tag{3.11}$$

Where χ^A denotes the fully mixed state of A. The quantity that we now have to bound is

$$\|\mathcal{E}_{\rm QKR} - \mathcal{F}_{\rm QKR}\|_\diamond = \frac{1}{2}\,\|\rho^{\tilde{B}\tilde{U}MAC\Omega E} - \mathop{\mathbb{E}}_{m} |m\rangle\langle m| \otimes \chi^{\tilde{B}\tilde{U}} \otimes \rho^{AC\Omega E}\|_1. \tag{3.12}$$

[4] Again, m is not necessarily uniform because it contains $m_{\rm bare}$.

[5] Note that if Eve has (partial) knowledge of the plaintext, the same $\mathcal{F}_{\rm QKR}$ applies. If m is known and we only want to protect the key, we can take an $\mathcal{R}'$ that replaces $\tilde{b}\tilde{u}k$ ($m = m_{\rm bare}||k$). Then $\mathcal{F}'_{\rm QKR}(\rho^{\rm ABE}) = \mathcal{R}'(\rho^{\tilde{B}\tilde{U}MAEC\Omega E}) = \mathbb{E}_{\tilde{b}\tilde{u}k} |\tilde{b}\tilde{u}k\rangle\langle\tilde{b}\tilde{u}k| \otimes \rho^{M_{\rm bare}AEC\Omega E}$. Due to the partial trace over $\tilde{U}$, M will be decoupled from Eve's auxiliary state and we have $\mathcal{F}_{\rm QKR} = \mathcal{F}'_{\rm QKR}$.

The E has dropped out of this expression since E is completely decoupled. The expression (3.12) makes intuitive sense; we are interested in the security of all the next-round keys given the data and auxiliaries in the hands of Eve.

We will first derive bounds as a function of γ and then study the implications at a given bit error rate β tolerated by the error-correcting code. Asymptotically the optimal value of γ equals β. It is important to remark that the two reject case expressions (3.7) and (3.11) are identical. In the difference $\rho^{\tilde{B}\tilde{U}MCA\Omega\mathrm{E}} - \mathbb{E}_m |m\rangle\langle m| \otimes \chi^{\tilde{B}\tilde{U}} \otimes \rho^{AC\Omega\mathrm{E}}$ we see that the $\omega = 0$ part vanishes.

Note that since $\mathbb{E}_m |m\rangle\langle m| \otimes \chi^{\tilde{B}\tilde{U}} \rho^{AC\Omega\mathrm{E}}$ has the message and the next round keys decoupled from Eve's state as well as from each other, we can invoke Lemma 2.10 to conclude that $\|\mathcal{E}_{\mathrm{QKR}} - \mathcal{F}_{\mathrm{QKR}}\|_\diamond \leq \varepsilon$ implies 2ε-ENC, 4ε-KR and 4ε-FR as desired.

3.4.5 Asymptotic result

Theorem 3.2. *Consider one round of the QKR protocol (Section 3.3.2) with 6-state or 8-state encoding. Let $\gamma_b \in [0, \frac{1}{2}]$ be a noise parameter corresponding to basis b. Let $\gamma = \max_b \gamma_b$, let β be the noise threshold and let n_b denote the number qubits Alice measures in basis b. Let λ be the security parameter of the MAC. It holds that*

$$\|\mathcal{E}_{\mathrm{QKR}} - \mathcal{F}_{\mathrm{QKR}}\|_\diamond \leq \min\left(P_{\mathrm{acc}},\ \sqrt{2^{\ell - n + nh(\{1-\frac{3}{2}\gamma, \frac{\gamma}{2}, \frac{\gamma}{2}, \frac{\gamma}{2}\}) - nh(\gamma) + \mathcal{O}(\sqrt{n})}}\right) + 2^{1-\lambda} \tag{3.13}$$

with

$$P_{\mathrm{acc}} = \mathop{\mathbb{E}}_{\{n_b\}: \sum_b n_b = n} \prod_{b \in \mathcal{B}} \sum_{c=0}^{\lfloor n_b \beta \rfloor} \binom{n_b}{c} \gamma_b^c (1-\gamma_b)^{n_b - c}. \tag{3.14}$$

Proof of Theorem 3.2

The proof is obtained by following step 4 till 6 of the proof recipe. We write $D \stackrel{\mathrm{def}}{=} \|\rho^{\tilde{B}\tilde{U}MAC\Omega E} - \mathbb{E}_m |m\rangle\langle m| \otimes \chi^{\tilde{B}\tilde{U}} \otimes \rho^{AC\Omega E}\|_1 = \mathbb{E}_{\tilde{b}\tilde{u}mac} \|\rho^E_{\tilde{b}\tilde{u}mac,[\omega=1]} - \rho^E_{[\omega=1]}\|_1$. The $\rho^E_{\tilde{b}\tilde{u}mac,[\omega=1]}$ and $\rho^E_{[\omega=1]}$ are both sub-normalized states with trace $\mathbb{E}_{bst}\, \theta_{bst}$. Hence it holds that $D \leq 2\, \mathbb{E}_{bst}\, \theta_{bst}$. From (3.12) we know $\|\mathcal{E}_{\mathrm{QKR}} - \mathcal{F}_{\mathrm{QKR}}\|_\diamond \leq \frac{1}{2} D$.
Step 4: We introduce smoothing as in [RK05, Ren05, TSSR11] by allowing states $\bar{\rho}$ that are $\sqrt{\varepsilon}$-close to ρ in terms of trace distance. This yields $D \leq 2\sqrt{\varepsilon} + \bar{D}$, with $\bar{D} \stackrel{\mathrm{def}}{=} \|\bar{\rho}^{\tilde{B}\tilde{U}MAC\Omega E} - \mathbb{E}_m |m\rangle\langle m| \otimes \chi^{\tilde{B}\tilde{U}} \otimes \bar{\rho}^{AC\Omega E}\|_1$. Substituting (3.5, 3.9) into this expression gives

$$\bar{D} \quad = \quad \mathop{\mathbb{E}}_{\tilde{b}\tilde{u}mac} \|\bar{\rho}^E_{\tilde{b}\tilde{u}mac,[\omega=1]} - \bar{\rho}^E_{[\omega=1]}\|_1. \tag{3.15}$$

In slight abuse of notation we have written $\mathbb{E}_c(\cdot) \stackrel{\text{def}}{=} \sum_c 2^{-\ell}(\cdot)$. In addition we have

$$\begin{aligned}
\bar{D} &= \mathop{\mathbb{E}}_{\tilde{b}\tilde{u}mac} \operatorname{tr} \sqrt{(\bar{\rho}^{\mathrm{E}}_{\tilde{b}\tilde{u}mac,[\omega=1]} - \bar{\rho}^{\mathrm{E}}_{[\omega=1]})^2} && (3.16)\\
&\stackrel{\text{Jensen}}{\leq} \mathop{\mathbb{E}}_{\tilde{b}mac} \operatorname{tr} \sqrt{\mathop{\mathbb{E}}_{\tilde{u}}(\bar{\rho}^{\mathrm{E}}_{\tilde{b}\tilde{u}mac,[\omega=1]} - \bar{\rho}^{\mathrm{E}}_{[\omega=1]})^2} && (3.17)\\
&= \mathop{\mathbb{E}}_{\tilde{b}mac} \operatorname{tr} \sqrt{\mathop{\mathbb{E}}_{\tilde{u}}(\bar{\rho}^{\mathrm{E}}_{\tilde{b}\tilde{u}mac,[\omega=1]})^2 - (\bar{\rho}^{\mathrm{E}}_{[\omega=1]})^2}. && (3.18)
\end{aligned}$$

Here we used $\mathbb{E}_{\tilde{u}}\, \delta_{(m\oplus c)||\tilde{b},\Phi_{\tilde{u}}(s\oplus a||b)} = \frac{1}{2^\ell|B|}$ to see that $\mathbb{E}_{\tilde{u}}\, \bar{\rho}^{\mathrm{E}}_{\tilde{b}\tilde{u}mac,[\omega=1]} = \bar{\rho}^{\mathrm{E}}_{[\omega=1]}$. From the properties of two-universal hash functions we get

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\tilde{u}}(\bar{\rho}^{\mathrm{E}}_{\tilde{b}\tilde{u}mac,[\omega=1]})^2 - (\bar{\rho}^{\mathrm{E}}_{[\omega=1]})^2 && (3.19)\\
&= \mathop{\mathbb{E}}_{ss'} \sum_{bb'} [2^{2\ell} \mathop{\mathbb{E}}_{\tilde{u}} \delta_{m\oplus c||\tilde{b},\Phi_{\tilde{u}}(s\oplus a||b)} \delta_{m\oplus c||\tilde{b},\Phi_{\tilde{u}}(s'\oplus a||b')}] \bar{\rho}^{\mathrm{E}}_{bs,[\omega=1]} \bar{\rho}^{\mathrm{E}}_{b's',[\omega=1]} - (\bar{\rho}^{E}_{[\omega=1]})^2 && \\
&= \mathop{\mathbb{E}}_{ss'} \sum_{bb'} [|\mathcal{B}|^{-2n} + \delta_{bb'}\delta_{ss'}(2^\ell|\mathcal{B}|^{-n} - |\mathcal{B}|^{-2n})] \bar{\rho}^{\mathrm{E}}_{bs,[\omega=1]} \bar{\rho}^{\mathrm{E}}_{b's',[\omega=1]} - (\bar{\rho}^{\mathrm{E}}_{[\omega=1]})^2 && (3.20)\\
&= (2^\ell|\mathcal{B}|^n - 1) \mathop{\mathbb{E}}_{ss'} \mathop{\mathbb{E}}_{bb'} \delta_{bb'}\delta_{ss'} \bar{\rho}^{\mathrm{E}}_{bs,[\omega=1]} \bar{\rho}^{E}_{b's',[\omega=1]} && (3.21)\\
&\leq (2^\ell|\mathcal{B}|^n - 1) \mathop{\mathbb{E}}_{ss'} \mathop{\mathbb{E}}_{bb'} \delta_{bb'}\delta_{ss'} \bar{\rho}^{\mathrm{E}}_{bs} \bar{\rho}^{\mathrm{E}}_{b's'}. && (3.22)
\end{aligned}$$

Line (3.22) should be read as an operator inequality for a sum of positive semidefinite matrices; we used $\theta_{bst} \leq 1$. Substituting (3.22) into (3.18), we can use Lemma 2.19 with $\mathcal{X} = \mathcal{B} \cup \mathcal{S}$.

$$\begin{aligned}
\bar{D} &< \operatorname{tr} \sqrt{2^\ell|\mathcal{B}|^n \mathop{\mathbb{E}}_{ss'} \mathop{\mathbb{E}}_{bb'} \delta_{bb'}\delta_{ss'} \bar{\rho}^{\mathrm{E}}_{bs} \bar{\rho}^{\mathrm{E}}_{b's'}} && (3.23)\\
&\stackrel{\text{Lemma 2.19}}{\leq} \sqrt{2^\ell|\mathcal{B}|^n 2^{S^\varepsilon_0(\rho^E) - S^\varepsilon_2(\rho^{BSE})}}. && (3.24)
\end{aligned}$$

Step 5: We use the post selection technique in the same way as in the QKD example. The factorized form of ρ^{ABE} allows us to set $\mathbb{E}_{bst}\, \theta_{bst} = P_{\mathrm{acc}}$ as in (3.14) yielding the first term in the minimum of (3.13). For (3.24) we write $p_{t|s} = \gamma^{\mathtt{Hamm}(s\oplus t)}(1-\gamma)^{\mathtt{Hamm}(s\oplus t)}$. Here we assume the noise in each basis is the maximal value Eve causes (γ) since this gives Eve access to a purification containing the most information. Substituting the factorized state into (3.24) we get

$$\begin{aligned}
\bar{D} &< \sqrt{2^\ell|\mathcal{B}|^n 2^{S^\varepsilon_0([\mathbb{E}_{bst}\, \sigma^b_{st}]^{\otimes n}) - S^\varepsilon_2([\mathbb{E}_{bst}\, |bs\rangle\langle bs| \otimes \sigma^b_{st}]^{\otimes n})}} && (3.25)\\
&\stackrel{\text{Lemma 2.1}}{\to} \sqrt{2^\ell|\mathcal{B}|^n 2^{nS(\mathbb{E}_{bst}\, \sigma^b_{st}) - nS(\mathbb{E}_{bst}\, |bs\rangle\langle bs| \otimes \sigma^b_{st}) + \mathcal{O}(\sqrt{n})}}. && (3.26)
\end{aligned}$$

(In the last two lines we have $s, t \in \{0,1\}$ and $b \in \mathcal{B}$ in contrast to the previous lines.) Step 6: For the 6-state encoding exactly the same noise check is performed in our QKR protocol as in the 6-state QKD protocol. We can apply the same constraints. For the 8-state encoding, Lemma 3.1 tells us the same simple state (2.59) holds. For

both encodings (2.60) allows us to write $S(\mathbb{E}_{bst}\,\sigma^b_{st}) = h(1-\frac{3}{2}\gamma,\frac{\gamma}{2},\frac{\gamma}{2},\frac{\gamma}{2}) = -(1-\frac{3}{2}\gamma)\log(1-\frac{3}{2}\gamma) - 3\frac{\gamma}{2}\log\frac{\gamma}{2}$ and

$$\begin{aligned} S(\mathop{\mathbb{E}}_{bst}|bs\rangle\langle bs|\otimes\sigma^b_{bx}) &= S(BS) + \mathop{\mathbb{E}}_{bs} S(\mathop{\mathbb{E}}_{t|bs}\sigma^b_{st}) && (3.27)\\ &= \log|\mathcal{B}| + 1 + \mathop{\mathbb{E}}_{bs} S([1-\gamma]\sigma^b_{s\bar{s}} + \gamma\sigma^b_{ss}) && (3.28)\\ &= \log|\mathcal{B}| + 1 + h(\gamma). && (3.29)\end{aligned}$$

In the last line we used that the projectors $\sigma^b_{s\bar{s}}$ and σ^b_{ss} are orthogonal to each other. Substituting these entropies into (3.26) yields the second term of the 'min' in (3.13). The factor $2^{1-\lambda}$ is due to the use of two MAC functions. □

For $\gamma > \beta$ the probability P_{acc} is exponentially small. For $\gamma \leq \beta$, the second expression can be made exponentially small by setting the message size $\ell < n + nh(\gamma) - nh(\{1-\frac{3}{2}\gamma,\frac{\gamma}{2},\frac{\gamma}{2},\frac{\gamma}{2}\})$. Asymptotically the length of the syndrome is $n-\kappa = nh(\beta)$, and the $\mathcal{O}(\log n)$ contribution from post-selection (Lemma 2.16) becomes negligible compared to n. The QKR rate $\frac{\ell'-\mathcal{O}(\log n)}{n}$ goes to

$$\text{asymptotic rate} = 1 - h(1-\tfrac{3}{2}\beta,\tfrac{\beta}{2},\tfrac{\beta}{2},\tfrac{\beta}{2}), \tag{3.30}$$

which is exactly the asymptotic rate of 6-state QKD (2.64).

Step 4 of the proof closely resembles the leftover hashing lemma against quantum side information [Ren05, TSSR11], but with the difference that we do not concentrate on proving that the hash output z, b' is almost-uniform but instead focus on the decoupling of $\tilde{b}, \tilde{u}, m$ from Eve; here m is non-uniform, which necessitates the use of pairwise independent hashing instead of universal hashing. In (3.20) the decoupling between (m, c) and x is visible which was already argued in Section 3.4.3.

Note that the description of Eve's ancilla state (2.59) is valid for the 6-state encoding and 8-state encodings. In case of the BB84 encoding only the xz-plane of the Bloch sphere are involved in the protocol and specifically in the noise check, then (3.26) still holds, but with different σ^b_{xy} matrices, yielding a QKR rate equal to the BB84 QKD rate (2.65).

3.4.6 Non-asymptotic result without smoothing

We want to have a security proof also for finite n. One approach would be to start from (3.25) and analyse the smooth entropies S^ε_0 and S^ε_2 for finite n and ε, and minimise over ε. However, that is a cumbersome procedure. Below we present a less tight but easier to derive bound, obtained by setting ε to zero.

Theorem 3.3. *Consider one round of the QKR protocol (Section 3.3.2) with 6-state or 8-state encoding. Let $\gamma \in [0, \frac{1}{2}]$ be a noise parameter, let β be the noise threshold and let P_{acc} be defined by (3.14). Let the function f be defined as*

$$f(\gamma) \stackrel{\text{def}}{=} \sqrt{(1-\tfrac{3}{2}\gamma)(1-\gamma)} + \sqrt{\tfrac{3}{2}\gamma(1+\gamma)}. \tag{3.31}$$

The diamond distance between the actual protocol and the ideal protocol can be bounded as

$$\|\mathcal{E}_{\text{QKR}} - \mathcal{F}_{\text{QKR}}\|_\diamond \leq (n+1)^{15} \min\left\{P_{\text{acc}},\ \tfrac{1}{2}\sqrt{2^{\ell-n+2n\log f(\gamma)}}\right\} + 2^{1-\lambda}. \tag{3.32}$$

Proof of Theorem 3.3:

We follow step 4 of proof of Theorem 3.2 up to (3.23) but without smoothing ($\varepsilon = 0$). Step 5 is identical but now the factor $(n+1)^{15}$ is not ignored. We have

$$D \quad < \quad (n+1)^{15} \min\Big(P_{\rm acc}, \sqrt{2^{\ell-n}} {\rm tr} \sqrt{\mathop{\mathbb{E}}_{bs} (\rho^E_{bs})^2}\Big). \tag{3.33}$$

Step 6 uses the same simple state held by Eve of (2.59) for the 6- and 8-state encodings. Instead of computing entropies we show that the expression under the square root is diagonal in the m-basis. Using $\rho^{\rm E}_{bs} = \bigotimes_i \{(1-\gamma)\sigma^{b_i}_{s_i \overline{s_i}} + \gamma \sigma^{b_i}_{s_i s_i}\}$ and the orthogonality $\sigma^b_{s\bar{s}}\sigma^b_{ss} = 0$ we get

$$\mathop{\mathbb{E}}_{bs}(\rho^{\rm E}_{bs})^2 = \bigotimes_{i=1}^n \Big\{(1-\gamma)^2 \mathop{\mathbb{E}}_{b_i} \frac{\sigma^{b_i}_{01} + \sigma^{b_i}_{10}}{2} + \gamma^2 \mathop{\mathbb{E}}_{b_i} \frac{\sigma^{b_i}_{00} + \sigma^{b_i}_{11}}{2}\Big\} \tag{3.34}$$

$$= \Big\{(1-\gamma)\Big[(1-\tfrac{3}{2}\gamma)|m_0\rangle\langle m_0| + \tfrac{\gamma}{6}\sum_{j=1}^3 |m_j\rangle\langle m_j|\Big] + \tfrac{\gamma^2}{3}\sum_{j=1}^3 |m_j\rangle\langle m_j|\Big\}^{\otimes n} \tag{3.35}$$

$$= \Big\{(1-\gamma)(1-\tfrac{3}{2}\gamma)|m_0\rangle\langle m_0| + \tfrac{\gamma(1+\gamma)}{6}\sum_{j=1}^3 |m_j\rangle\langle m_j|\Big\}^{\otimes n} \tag{3.36}$$

from which it follows that

$${\rm tr}\sqrt{\mathop{\mathbb{E}}_{bs}(\rho^E_{bs})^2} = \Big\{\sqrt{(1-\gamma)(1-\tfrac{3}{2}\gamma)} + \sqrt{\tfrac{3}{2}\gamma(1+\gamma)}\Big\}^n. \tag{3.37}$$

The term $2^{1-\lambda}$ is due to the use of two MAC functions. □

For $\gamma > \beta$ the probability $P_{\rm acc}$ is exponentially small in n. Note that $2\log f(\gamma) \in [0,1)$ for $\gamma \in [0, \frac{1}{2})$. For any $\gamma < \frac{1}{2}$ it is possible to choose $\ell < n - n \cdot 2\log f(\gamma)$, so that the $\sqrt{\cdots}$ in (3.32) becomes exponentially small in n.

Theorem 3.4. *Consider the context of Theorem 3.3. Let β be the noise threshold. Let ν be a security parameter. Let ℓ be chosen as*

$$\ell \quad \leq \quad n - 2n\log f(\beta) - 2\xi\sqrt{\nu n} - 2\nu - 1 - 30\log(n+1) \tag{3.38}$$

$$\xi \quad \stackrel{\rm def}{=} \quad \min\left\{\frac{f'(\beta)}{f(\beta)}\left[\sqrt{\frac{2\beta}{\ln 2} + \frac{\nu}{n}} + \sqrt{\frac{\nu}{n}}\right], \quad \frac{\sqrt{3}}{\ln 2}\right\}. \tag{3.39}$$

Then

$$\|\mathcal{E}_{\rm QKR} - \mathcal{F}_{\rm QKR}\|_\diamond \leq 2^{-\nu} + 2^{1-\lambda}. \tag{3.40}$$

Proof of Theorem 3.4

Decreasing the size of ℓ by $30\log(n+1)$ compensates for the penalty term due to post-selection. We define the bound $P_{\rm acc} \leq P_{\rm glob} \stackrel{\rm def}{=} \sum_{c=0}^{\lfloor n\beta \rfloor} \binom{n}{c} \gamma^c (1-\gamma)^{n-c}$ where we have replaced n_b by n and γ_b by γ. This is allowed since the noise check is

only passed if the overall noise is sufficiently low. We (implicitly) define a function $\gamma_{\max}$ as $P_{\text{glob}}(\gamma = \gamma_{\max}) = 2^{-\nu}$. For $\gamma \geq \gamma_{\max}$ eq. (3.40) clearly holds. Next we need to bound the expression $\log f(\gamma)$ for $\gamma \leq \gamma_{\max}$. Taking the Chernoff bound $P_{\text{glob}} \leq \exp[-\frac{n}{2\gamma}(\gamma - \beta)^2]$ and solving for γ we get

$$\gamma_{\max} \leq \gamma_0 \stackrel{\text{def}}{=} \beta + \frac{\nu \ln 2}{n} + \sqrt{2\beta \frac{\nu \ln 2}{n} + (\frac{\nu \ln 2}{n})^2}. \tag{3.41}$$

We will bound the expression $\log f(\gamma_0)$ in two different ways: for 'large' β and for 'small' β.

- As f is a concave function we have $f(\gamma_0) \leq f(\beta) + (\gamma_0 - \beta) f'(\beta)$. This yields

$$\begin{aligned} \log f(\gamma_0) &\leq \log f(\beta) + \log[1 + \frac{f'(\beta)}{f(\beta)}(\gamma_0 - \beta)] \leq \log f(\beta) + \frac{f'(\beta)}{f(\beta)} \frac{\gamma_0 - \beta}{\ln 2} \\ &= \log f(\beta) + \frac{\nu}{n} + \sqrt{2\beta \frac{\nu}{n \ln 2} + (\frac{\nu}{n})^2}. \end{aligned} \tag{3.42}$$

- We write $\log f(\gamma_0) = \log f(\beta) + \log \frac{f(\gamma_0)}{f(\beta)} \leq \log f(\beta) + \log \frac{f(\gamma_0)}{f(\beta)}\Big|_{\beta=0}$. The inequality follows from the fact that $f(\gamma_0)/f(\beta)$ is a decreasing function of β. This yields

$$\log f(\gamma_0) \leq \log f(\beta) + \log f(\frac{2\nu}{n}) \leq \log f(\beta) + \log[1 + \sqrt{\tfrac{3}{2}(\tfrac{2\nu}{n})}] \leq \log f(\beta) + \tfrac{1}{\ln 2}\sqrt{\tfrac{3\nu}{n}}. \tag{3.43}$$

From (3.42) and (3.43) we conclude $n \log f(\gamma_{\max}) \leq n \log f(\beta) + \xi\sqrt{\nu n}$ with ξ as defined in (3.39). With ℓ chosen according to (3.38), the term $\sqrt{2^{\ell - n + 2n \log f(\gamma_{\max})}}$ in (3.32) is upper bounded by $2^{-\nu}/\sqrt{2}$. Hence the second expression in the $\min\{\cdot,\cdot\}$ of (3.32) is upper bounded by $\frac{2^{-\nu}}{2\sqrt{2}} + \frac{2^{-\nu}}{2} + \frac{2^{-2\nu}}{2\sqrt{2}} < 2^{-\nu}$. □

If according to (3.38) we have to set the length ℓ smaller than $2\lambda + n - \kappa$ (negative size of the message m_{bare}) then the desired security level ν cannot be achieved.

A typical choice for the tag length would be $\lambda = \nu$, yielding security $\|\mathcal{E}_{\text{QKR}} - \mathcal{F}_{\text{QKR}}\|_\diamond \leq 2^{1-\lambda} + 2^{-\nu} = 3 \cdot 2^{-\nu}$. Several things are worth noting.

- The ξ is of order 1. Hence the term $\xi\sqrt{\nu n}$ scales as $\sqrt{n}$.

- Analysis of QKD instead of QKR using the same technique yields a result similar to Theorem 3.3, but with a slightly more favorable function instead of $f(\gamma)$, namely $\sqrt{(1-\gamma)(1-\frac{3}{2}\gamma)} + \sqrt{\frac{1}{2}\gamma(1-\gamma)} + \gamma\sqrt{2}$. (We mention this without showing the proof.) Nevertheless, the asymptotics of QKD and QKR are the same.

3.4.7 Non-asymptotic QKR rate; Choosing the parameter values

We want to characterize the non-asymptotic performance of our QKR scheme under ideal circumstances. Consider a sequence of QKR rounds with a large number of consecutive accepts. Let $\eta = 2 \cdot 2^{-\lambda} + 2^{-\nu}$ be the 'imperfection' induced by one round of QKR. Let θ be the maximum distance that Alice and Bob are willing to tolerate between reality and the ideal state. After $N = \lfloor \theta/\eta \rfloor$ rounds they have to refresh *all* their key material. We define the amortized QKR rate as

$$A \stackrel{\text{def}}{=} \frac{\text{total message data sent in } N \text{ rounds} - \text{expended key material}}{N \cdot n} \tag{3.44}$$

$$= \frac{\ell'}{n} - \frac{\log |\mathcal{U} \times \mathcal{B}^n|}{N \cdot n}, \tag{3.45}$$

namely the usual definition of rate ($\frac{\ell'}{n}$) minus the amortized cost of completely replacing u and b after N rounds. A is an operational quantity that measures how much useful classical payload is sent per qubit. The subtraction can be understood as the cost of putting enough key material into m_{bare} to compensate for the eventual replacement of u, b after N rounds.

The total message size is $N\ell' = N(\ell - 2\lambda - n + \kappa)$, with ℓ specified in (3.38). The total key expenditure consists of $\log |\mathcal{B}^n|$ bits of basis key b, and $\log |\mathcal{U}| = \log |\{0,1\}^{n+\ell} \times \mathcal{B}^{2n}|$ bits of extractor key u. This gives

$$\begin{aligned} A &= \frac{\kappa}{n} - 2\log f(\beta) - \frac{2\xi\sqrt{\nu}}{\sqrt{n}} - \frac{30\log(n+1)}{n} - \frac{2\lambda + 2\nu + 1}{n} \\ &\quad - \frac{2 + 3\log|\mathcal{B}| - 2\log\, f(\beta)}{N} + \frac{2\xi\sqrt{\nu}}{\sqrt{n}N} + \frac{2\nu + 1 + 30\log(n+1)}{nN}. \end{aligned} \tag{3.46}$$

Note that η can be made exponentially small (N exponentially large) by increasing λ and ν.

For large n and N the rate (3.47) tends to $1 - h(\beta) - 2\log f(\beta)$, which is lower than the asymptotic result of Section 3.4.5. The discrepancy is of course caused by the fact that we did not use smoothing for Theorem 3.3. Figure 3.3 shows the asymptotic (QKR=QKD) rate (3.30) as well as the $\varepsilon = 0$ rate (3.47) in the limit $n \to \infty, N \to \infty$ and the rate obtained from the Entanglement Monogamy approach (Section 3.1.2). Obviously smoothing improves the tightness of the provable bounds significantly. Furthermore it is also clear that the Entanglement Monogamy bound is far from tight.

Instead of pairwise independent hashing one may use 'almost pairwise independent' hash functions. The length of the extractor key u is reduced from $n+\ell+2n\log|\mathcal{B}|$ to potentially $2\ell + 2n\log|B|$ [Sti94].

Typically θ is fixed. Then it remains to tune N (which via $\eta = \theta/N$ fixes ν) and n for fixed (θ, β) so as to optimise the rate. In Figure 3.4 the non-asymptotic rate is plotted for $\theta = 2^{-256}$ and various values of β, N and n. We see that the asymptotic rate can be approached well for realistic values of N and n.

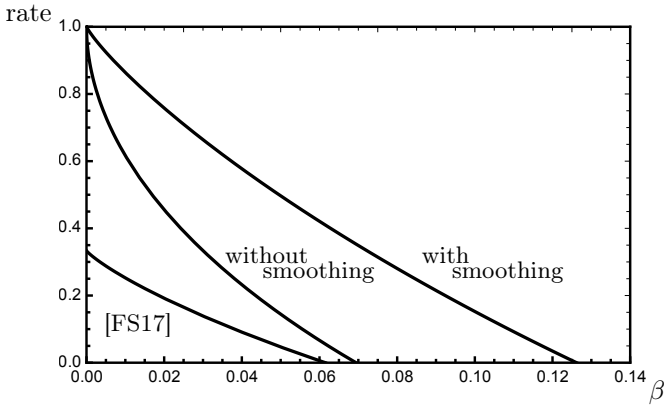

Figure 3.3: *Asymptotic QKR rates. The 'with smoothing' curve is the result (3.30). The 'without smoothing' curve is the result* $1 - h(\beta) - 2\log f(\beta)$ *obtained without smoothing. The rate of [FS17] is for the BB84 encoding (see Section 3.1.2).*

3.5 Discussion

3.5.1 Comparison to existing results

The proof technique of [FS17] requires a special 'key privacy' property of the MAC function, and has to keep track of the security of the MAC key. We avoid this requirement at the cost of shortening ℓ'. An interesting difference with respect to [FS17] is that we capture the security of the basis key B and the extractor key U in a single quantity (a single trace distance), whereas [FS17] uses a min-entropy result for B and a trace distance for U.

We compare our result to the min-entropy analysis of attacks in [LŠ18]. For the 'K2 attack' (a known-plaintext attack on b) a min-entropy loss of $\log(1+\sqrt{6\beta(1-\frac{3}{2}\beta)})$ bits per qubit was found for 8-state encoding; that is more than our leakage result $2\log f(\beta)$. We conclude that non-smooth min-entropy is too pessimistic as a measure of security in this context.

It was pointed out in [ŠdV17, LŠ18] that with 8-state encoding there is no leakage about the qubit payload X, whereas 6-state and BB84 encoding allow Eve to learn a lot about X in case of a reject. One may conclude that more privacy amplification is needed for 6-state and BB84 encoding than for 8-state. However, for our protocol it turns out that the situation is the same for all encoding schemes: the privacy amplification key U adequately masks Z and gets replaced upon reject.

Upon accept, our protocol does not *reduce* the stack of shared key material that Alice and Bob have. A difference with respect to [FS17] is that the 'top' keys on the stack are *modified* upon accept. We do not see this as a significant drawback; the key modification is just some additional data processing.

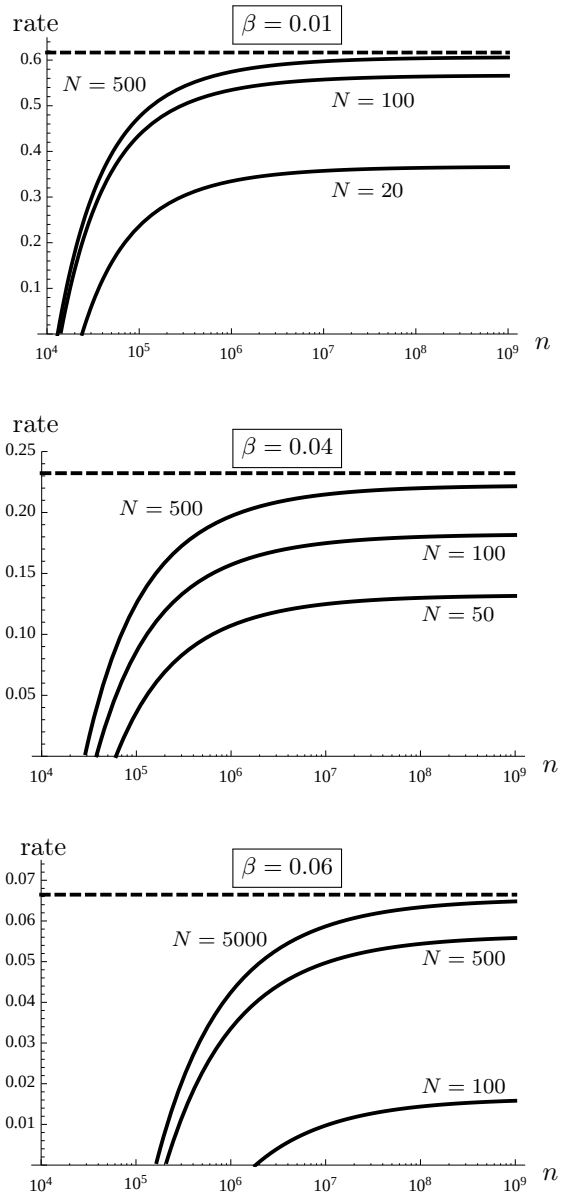

Figure 3.4: *Non-asymptotic bound on the amortized QKR rate as a function of the number of qubits (n), for various values of the design parameter N and tolerated noise β. The dashed lines indicate the $\varepsilon = 0$ limit $1 - h(\beta) - 2\log f(\beta)$. $\lambda = \nu$; $\theta = 2^{-256}$; the syndrome length $n - \kappa$ is set to $nh(\beta) + \sqrt{n}\Phi^{\mathrm{inv}}(10^{-6})\sqrt{\beta(1-\beta)}\log\frac{1-\beta}{\beta}$ (see e.g. [BKB04]), where Φ is defined as $\Phi(z) \stackrel{\mathrm{def}}{=} \int_z^\infty (2\pi)^{-1/2}\exp[-x^2/2]\mathrm{d}x$.*

3.5.2 Dealing with erasures

Our analysis has not taken into account quantum channels with erasures. (Particles failing to arrive.) Consider a channel with erasure rate η and bit error rate β for the non-erased states. The Alice-to-Bob channel capacity is $(1-\eta)(1-h(\beta))$. A capacity-achieving linear error-correcting code that is able to deal with such a channel has a syndrome of size $nh(\beta) + n\eta[1 - h(\beta)]$. Imagine the QKR scheme of Section 3.3.2 employing such an error-correcting code. On the one hand, the parameter a increases from $nh(\beta)$ to $nh(\beta) + n\eta[1 - h(\beta)]$. On the other hand, the leakage increases. Every qubit not arriving at Bob's side must be considered to be in Eve's possession; since an erasure can be parametrized as a qubit with $\beta = \frac{1}{2}$, the leakage is 1 bit per erased qubit. Hence the leakage term $n \cdot 2 \log f(\beta)$ changes to $n(1 - \eta)2 \log f(\beta) + n\eta$. The combined effect of the syndrome size and the leakage increase has a serious effect on the QKR rate. The asymptotic rate becomes $1-h(\beta)-\eta[1-h(\beta)]-(1-\eta)2 \log f(\beta)-\eta$. For $\beta = 0$ this is $1 - 2\eta$; at zero bit error rate no more than 50% erasures can be accommodated by the scheme. In long fiber optic cables the erasure rate is often larger than 90%. Under such circumstances the QKR scheme of Section 3.3.2 simply does not work. (Note that continuous-variable schemes do not have erasures but instead have large β.)

One can think of a number of straightforward ways to make the QKR protocol erasure-resistant. Below we sketch a protocol variant in which Alice sends qubits, and Bob returns an authenticated and encrypted message.

1. Alice sends a random string $x \in \{0, 1\}^q$ encoded in q qubits, with $q(1 - \eta) > n$.

2. Bob receives qubits in positions $i \in \mathcal{I}, \mathcal{I} \subseteq [q]$ and measures x'_i in those positions. He aborts the protocol if $|\mathcal{I}| < n$. Bob selects a random subset $\mathcal{J}' \subset \mathcal{I}$, with $|\mathcal{J}'| = n$. He constructs a string $y' = x'_{\mathcal{J}'}$. He computes $e' = k_{\text{syn}} \oplus \texttt{Syn}\, y'$, $z'||b' = \Phi_u(y'||b)$, $c' = m \oplus z'$, $t' = \Gamma(k^1_{\text{MAC}}, \mathcal{J}'||y'||c'||e')$. He sends $\mathcal{J}', e', c', t'$.

3. Alice receives this data as $\mathcal{J}, e, c, t$. She computes y by doing error correction on $x_{\mathcal{J}}$ aided by the syndrome $k_{\text{syn}} \oplus e$. Then she computes $z||b'' = \texttt{Ext}(u, y||b)$, $\hat{m} = z \oplus c$ and $\tau = \Gamma(k^1_{\text{MAC}}, \mathcal{J}||y||c||e)$. Alice accepts the message $\hat{m}$ if $\tau = t$ and rejects otherwise.[6] Key refreshment is as in the original protocol.

The security is not negatively affected by the existence of erasures. Assume that Eve holds all the qubits that have not reached Bob. Since the data in the qubits is random, and does not contribute to the computation of z', it holds that (i) it is not important if Eve learns the content of these bits, (ii) known plaintext does not translate to partial knowledge of the data content of these qubits, which would endanger the basis key b and the extractor key u.

3.5.3 Potential improvements

It is possible to evaluate or bound $S^\varepsilon_0(\rho^E)$ and $S^\varepsilon_2(\rho^{BXE})$ in (3.24) for finite n and ε 'by hand', i.e. specifically for $\rho^E_{bxy} = \otimes^n_{i=1}\sigma^{b_i}_{x_i y_i}$. That would yield a non-asymptotic result for ℓ that is more favorable than Theorem 3.4.

[6] Alice may send the accept/reject bit along with the next batch of qubits; then the protocol has only two rounds.

It is interesting to note that QKR protocols which derive an OTP z from the qubit payload and then use z for encryption look a lot like Quantum Key Distribution, but with reduced communication complexity. This changes when the message is put directly into the qubits, e.g. as is done in Gottesman's Unclonable Encryption [Got03].

The QKR scheme of Section 3.3.2 can be improved and embellished in various ways. For instance, the λ-bit space in m reserved for the new k^1_{MAC} may not be necessary. Alice's authentication tag may simply be generated as part of the Φ_u function's output, and then the security of the MAC key can be proven just by proving the security of the extractor key u (similar to what is done in [FS17]).

Another interesting option is to deploy the Quantum One Time Pad with approximately half the key length, which still yields information-theoretic security. This would reduce the cost of refreshing b from $2n$ bits to n bits.

Finally, various tricks known from QKD may be applied to improve the noise tolerance of QKR, e.g. artificial noise added by Alice.

3.6 What's next?

We have shown that quantum key recycling can provide the same security guarantees as QKD with a lower round complexity without sacrificing the asymptotic rate. In addition we have shown a composable secure QKR protocol can be realized with reasonable parameters in the finite size regime. By applying privacy amplification to the basis as well as the payload, we find that the 6-state encoding achieves the same efficiency as the 8-state encoding while the basis enjoys the same level of security as the message.

From the potential improvements to the QKR protocol, the most fundamental seems to be the embedding of the message directly into the qubits. First, the question of whether this is possible securely without sacrificing the rate is an interesting one. Second, there might be advantages in terms of security since there is no ciphertext linking the message to the key material remaining after the quantum states are measured. Third, although QKR does not seem to increase the potential rate beyond that of QKD (except for the gain due to no qubits being discarded), the amount of classical communication can in principle still be decreased significantly. The next chapter will discuss a protocol that embeds the message directly into the qubits.

Chapter 4
Quantum Key Recycling with almost no classical communication

Do we need all these classical messages?
Having made the switch from quantum key distribution to quantum key recycling, Alice and Bob realize the main improvement is the reduction in classical communication back and forth. Especially Bob is happy. When Alice tells him one of her long stories, he only has to indicate everything is fine every ones in a while without interrupting her story. Alice still feels like all the classical strings she has to send are a waste. Can't she just send quantum states and be done?
During their transition of protocols, Alice and Bob of course experienced a number of hiccups. In the first attempts of running the protocol, the communication was often unsuccessful. Since the QKR scheme demanded the complete refresh of all key material when the protocol aborted, Alice and Bob used a lot of their shared key material and had to use part of their qubits to extend their shared key again. Alice and Bob decide they want the wasted key material in the reject case to be as low as possible.
By encoding the message directly into the quantum state while still only having a single authenticated bit as feedback, and by improving the key expenditure in the reject case, Alice and Bob feel they can improve their efficiency. Hopefully this won't result in the need to send too many extra qubits. Let's find out.

4.1 Introduction

4.1.1 Quantum Key Recycling

Quantum key recycling (QKR) achieves information-theoretically secure communication in such a way that no key material is used up as long as the quantum channel is undisturbed. Compared to QKD followed by classical one-time-pad message encryption, QKR's main advantage is *reduced round complexity*: QKR needs only one message from Alice to Bob, and one authenticated bit from Bob to Alice. QKD needs

This chapter is based on [LŠ21].

at least two messages from Alice to Bob. Furthermore, a minor advantage is that QKR does not discard any qubits, whereas QKD does.

A prepare-and-measure QKR scheme based on qubits was proposed already in 1982 [BBB82]. Then QKR received little attention for a long time. A security proof[1] for qubit-based[2] QKR was given only in 2017 by Fehr and Salvail [FS17]. In Chapter 3 we showed (for a scheme similar to [FS17]) that the communication rate in case of a noisy quantum channel is asymptotically the same as for QKD with one-way postprocessing.

4.1.2 Related work; putting the message in the quantum states

Different from the classical setting, in the quantum cryptographic setting authentication implies encryption [BCG$^+$02]. Portmann [Por17] showed that quantum authentication is possible with re-use of all the encryption keys, but stated as an open problem to find a *prepare-and-measure* QKR scheme for classical messages.

The QKR scheme of Fehr and Salvail [FS17] provides a solution to this problem. The drawback of their scheme is that when it's used for encryption, the communication rate does not exceed 1/3. A variant of their scheme allows for full embedding of the classical message in the quantum states.

In 2003 Gottesman [Got03] proposed a scheme called 'Unclonable Encryption' which encodes a message directly into qubit states. Although some of the keys in his scheme can be re-used, still n key bits are discarded when sending an n-bit message. His scheme does achieve an extra security feature in the case of future key leakage.

The high-dimensional QKR of Damgård, Pedersen and Salvail [DPS05] has full recycling of keys. The amount of key material that needs to be refreshed when the communication of a message $m \in \mathcal{M}$ is unsuccessful asymptotically equals $\log|\mathcal{M}|$ and they showed this is optimal. Their scheme does however require a quantum computation for encryption and decryption.

4.1.3 Brief summary of results from Chapter 3

Recall that in Chapter 3 Alice encodes random bits into the qubits; over a classical channel she sends a ciphertext; one-time pad-encrypted information for error-correction and an authentication tag. The ciphertext is the message padded with the pairwise independent hash of the qubit payload. The recycled keys are a basis sequence and the pairwise independent hash seed. Let the CPTP map $\mathcal{E}_{\mathrm{QKR}}$ be the protocol of Chapter 3, and $\mathcal{F}_{\mathrm{QKR}}$ its idealized version where the message and the next round's keys are completely unknown to Eve. Using Lemma 2.10 this is sufficient to show encryption, key recycling and forward secrecy as defined in definitions 2.4, 2.7 and 2.9. It was shown that

$$\|\mathcal{E}_{\mathrm{QKR}}-\mathcal{F}_{\mathrm{QKR}}\|_\diamond \leq 2^{-\lambda+1}+(n+1)^{15}\min\left(\varepsilon+\frac{1}{2}\mathrm{tr}_E\sqrt{|\mathcal{B}|^n 2^\ell \mathrm{tr}_{BS}\left(\bar{\rho}^{BS\mathrm{E}}\right)^2}, P_{\mathrm{acc}}\right), \quad (4.1)$$

[1] For a scheme slightly different from [BBB82].

[2] As opposed to schemes that work with higher-dimensional spaces, e.g. using mutually unbiased bases [DPS05].

where λ is the length of the authentication keys, n the number of qubits, $\mathcal{B}$ the alphabet of the qubit basis choice, ℓ the message length, B the basis sequence, S the random data encoded in the qubits, and P_{acc} the probability that the noise checks are passed. Let $\rho^{BS\text{E}}$ be the state $\mathcal{E}_{\text{QKR}}(\rho^{\text{ABE}})$ with everything traced out except the B, S and E subsystems, then $\bar{\rho}^{BS\text{E}}$ is a state ε-close to $\rho^{BS\text{E}}$ in terms of trace distance; ε is the amount of state 'smoothing' [RK05]. If 6-state encoding[3] of bits is used then the 4×4 matrix σ is completely determined [Ren05] by a single parameter: the bit error probability γ on the quantum channel. Smoothing allows us to write (4.1) as smooth min- and max entropies which are asymptotically equal to von Neumann entropies. Asymptotically for large n, the bound (4.1) reduces to

$$\|\mathcal{E}_{\text{QKR}} - \mathcal{F}_{\text{QKR}}\|_\diamond \leq 2^{-\lambda+1} + n^{15} \min\left(\sqrt{2^{\ell - n + nh(\{1-\frac{3}{2}\gamma, \frac{\gamma}{2}, \frac{\gamma}{2}, \frac{\gamma}{2}\}) - nh(\gamma) + \mathcal{O}(\sqrt{n})}}, P_{\text{acc}}\right), \tag{4.2}$$

which yields exactly the same rate[4] $1 - h(\{1 - \frac{3}{2}\gamma, \frac{\gamma}{2}, \frac{\gamma}{2}, \frac{\gamma}{2}\})$ as 6-state QKD with one-way post-processing.[5] The security of N QKR rounds follows from $\|\mathcal{E}_N \circ \cdots \circ \mathcal{E}_1 - \mathcal{F}_N \circ \cdots \circ \mathcal{F}_1\|_\diamond \leq N\|\mathcal{E}_{\text{QKR}} - \mathcal{F}_{\text{QKR}}\|_\diamond$.

4.1.4 Improving the QKR scheme of Chapter 3

We answer the open question of whether it is possible to have a prepare-and-measure qubit-based QKR scheme with the message entirely contained in the qubits, without increasing the number of qubits compared to QKD schemes with one-way post-processing. The answer is affirmative. We achieve two improvements over the QKR scheme of Chapter 3.

- We present a scheme called 'Embedded Quantum Key Recycling' (EQKR) which has the message embedded directly into the qubits and Alice's classical messages removed entirely. EQKR achieves the same asymptotic rate the scheme of Chapter 3.
- In the reject case, we implement the key update by hashing fresh key material into the old keys. This reduces the key expenditure in the reject case. For $\beta = 0$ it is reduced to the message size, which, as mentioned in Section 4.1.2, is optimal.

We prove the security of EQKR against general attacks using the proof recipe of Chapter 2. At an early stage the accept case of the proof reduces exactly to the derivation in Chapter 3. Notably, this proof asymptotically achieves optimal rates for 6-state as well as 4-state encodings. The finite-size effects are the same as Chapter 3, but with an additional small term due to the new key refresh procedure in the reject case.

Although classical communication may be considered 'cheap' compared to the communication over the quantum channel in most practical settings, we find that

[3] For 4-state (BB84) 'conjugate' coding Eve has two degrees of freedom, i.e. a more powerful attack.

[4] The term $nh(\gamma)$ gets cancelled because Alice and Bob expend $nh(\gamma)$ bits of key material to OTP the redundancy bits.

[5] For 4-state encoding the result is different from (4.2) and yields the BB84 rate.

reducing the overall communication to the bare minimum is of theoretical interest. In addition, the complete removal of classical communication removes the need to synchronize the classical and quantum channel.

4.1.5 Protocol aims

Current QKR schemes all have some drawback. They require a quantum computer for their implementation, only re-use a small amount of key material resulting in poor rate or they have classical ciphertext. In this work we aim for a QKR protocol that is efficient in the sense of minimal communication and optimal key consumption while still being simple to implement. This comes down to the following desiderata:

- All actions on quantum states should be simple single-qubit actions like state preparation and measurement.
- Alice should send only qubits, so that no bandwidth is wasted.
- Bob should send only an authenticated accept/reject bit.
- No key material should be consumed in case of accept, and the bare minimum should be consumed in case of reject.
- The communication rate should equal that of QKD.

4.2 The Embedded Quantum Key Recycling protocol

4.2.1 Protocol design considerations

In the transformation from QKR of Chapter 3 to EQKR, there are several proof-technical issues. Most importantly, the qubit payload $X \in \{0,1\}^n$ needs to be uniformly random. (See Section 4.4.3. In the proof the X acts as a uniform mask.) This has to be reconciled with the fact that (i) the message is typically not uniform; (ii) the error-correction encoding step introduces redundancy. Our solution to these issues is shown in Figure 4.1, which depicts most of the variables in the protocol. Alice first appends randomness k' and an authentication tag τ to her plaintext μ to construct the message m. She then appends a random string $r \in \{0,1\}^\varrho$ to the message, which will serve for privacy amplification. Then she does the error correction encoding, resulting in a codeword $c \in \{0,1\}^n$. The c is then masked with a one-time pad z; this masks any structure present in c. A similar construction was proposed by Gottesman [Got03]. However, instead of discarding z we re-use most of the entropy in z. After every round, the pad z and the basis choice b are hashed together with the randomness r resulting in the next round pad $\tilde{z}$ and next round basis $\tilde{b}$. In a sense this corresponds to the privacy amplification step of QKD and QKR except it happens in between the rounds of the protocol.

4.2.2 Protocol intuition

Since the codeword c is padded (xor'ed) with the uniform shared key z to compute the qubit payload, the security of the message is somewhat obvious. No knowledge of

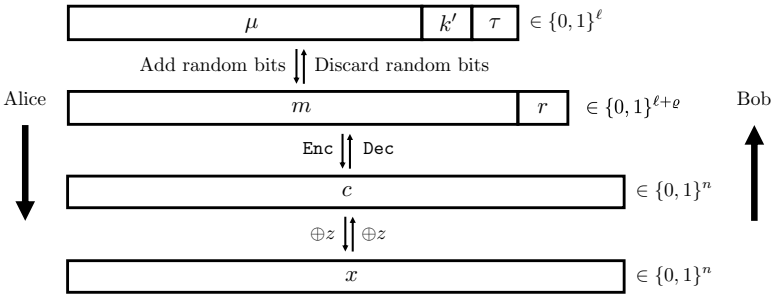

Figure 4.1: *Classical processing performed by Alice, and in reverse by Bob.*

c implies no knowledge on m. However, for the scheme to be efficient in terms of rate, most of the entropy in z and basis choice b needs to be re-used. Intuitively it is clear that in the accept case the leakage on x bounds the leakage on z by the same bound as in QKD and QKR when the same encoding is used. Similar to the QKR scheme of Chapter 3, we can bound the leakage on z and b together to determine the amount of privacy amplification done on both strings together. The privacy amplification guarantees the security of the keys for the next round, while the security of the message in a given round is obvious for secure keys.

In the reject case there might be a lot of leakage on the combination of z and b. We choose to discard z. This leaves the entropy of b largely intact since Eve's remaining task is to learn the encoding basis without knowing the payload. Depending on Eve's actions, the feedback bit indicating the success of the protocol can potentially leak information on the basis choice. In addition to refreshing z it is therefore needed to add a little bit of new entropy to b. This is done by hashing some shared randomness into b with a pairwise-independent hash.

4.2.3 Setup and protocol steps

Alice and Bob have agreed on a linear error-correcting code with encoding and decoding functions $\texttt{Enc} : \{0,1\}^{\ell+\varrho} \to \{0,1\}^{n}$ and $\texttt{Dec} : \{0,1\}^{n} \to \{0,1\}^{\ell+\varrho}$. The choice of ϱ and n depends on the bit error rate of the quantum channel and on the required amount of privacy amplification. Furthermore Alice and Bob have agreed on a one-time MAC function $\Gamma : \{0,1\}^{2\lambda} \times \{0,1\}^{*} \to \{0,1\}^{\lambda}$, and two pairwise independent hash functions $F_u : \{0,1\}^{n} \times \mathcal{B}^{n} \times \{0,1\}^{\varrho} \to \{0,1\}^{n} \times \mathcal{B}^{n}$ $(u \in \mathcal{U})$ and $G_v : \mathcal{B}^{n} \times \mathcal{Q} \to \mathcal{B}^{n}$ $(v \in \mathcal{V})$. The space $\mathcal{Q}$ contains the shared randomness that Alice and Bob hash into their shared basis sequence after a failed round. The λ is a security parameter for the MAC function and is constant with respect to n. They agree on the channel monitoring procedure of Definition 2.18 in which the `NoiseCheck` function outputs 1 only if the noise for every basis is smaller than the threshold β. Let EQKR denote a single round of the protocol, it consists of the following steps (see Figure 4.2):

EQKR.Gen:
Alice and Bob generate shared key material consisting of a mask $z \in \{0,1\}^n$, a MAC key $\xi \in \{0,1\}^{2\lambda}$ for Alice's message, a basis sequence $b \in \mathcal{B}^n$, a MAC key $k \in \{0,1\}^{2\lambda}$ for Bob's feedback bit, and seeds $u \in \mathcal{U}$, $v \in \mathcal{V}$ for pairwise independent hashing.[6] Furthermore Alice and Bob share a 'reservoir' of additional spare key material.
Alice generates random strings $r \in \{0,1\}^{\varrho}$, $k' \in \{0,1\}^{\lambda}$ and the plaintext $\mu \in \{0,1\}^{\ell-2\lambda}$. She computes the authentication tag $\tau = \Gamma(\xi, \mu\|k'\|r)$ and the 'augmented message' $m = \mu\|k'\|\tau$ (with $m \in \{0,1\}^{\ell}$).

EQKR.Enc
Alice computes the encoding $c = \texttt{Enc}(m\|r) \in \{0,1\}^n$, and the padded qubit payload $x = c \oplus z$. She prepares $|\Psi\rangle = \bigotimes_{i=1}^{n} |\psi_{x_i}^{b_i}\rangle$ and sends $|\Psi\rangle$ to Bob.

EQKR.Meas:
Bob receives $|\Psi'\rangle$. He measures $|\Psi'\rangle$ in the basis b. The result is $x' \in \{0,1\}^n$.

EQKR.Post
Bob computes $c' = x' \oplus z$. He tries to recover $\hat{m}\|\hat{r} = \texttt{Dec}(c')$. If decoding is successful, he parses $\hat{m}$ as $\hat{m} = \hat{\mu}\|\hat{k}'\|\hat{\tau}$. He computes $\hat{c} = \texttt{Enc}(\hat{m}\|\hat{r})$ and $\hat{x} = \hat{c} \oplus z$. He performs the channel monitoring $\omega = \texttt{NoiseCheck}(b, \hat{x}, x')$.
Feedback:
Bob checks if $\Gamma(\xi, \hat{\mu}\|\hat{k}'\|\hat{r}) == \hat{\tau}$. He accepts only if $\omega == 1$ and the MAC $\hat{\tau}$ is correct; he rejects otherwise. He authenticates the feedback bit (accept/reject) with k and sends it to Alice. Alice checks the MAC on the feedback.
Key Update:
The keys/seeds ξ, u, v are always re-used. The updated version of the z, b, k in the next round is denoted as $\tilde{z}, \tilde{b}, \tilde{k}$.

- In case of accept:
  Alice sets[7] $\tilde{k} \leftarrow k'$ and $\tilde{z}||\tilde{b} \leftarrow F_u(x\|b\|r)$.
  Bob sets $\tilde{k} \leftarrow \hat{k}'$ and $\tilde{z}||\tilde{b} \leftarrow F_u(\hat{x}\|b\|\hat{r})$.
- In case of reject:
  Alice and Bob take new $\tilde{z}$ and $\tilde{k}$ from their reservoir.
  They take $q \in \mathcal{Q}$ from the reservoir and set $\tilde{b} \leftarrow G_v(b\|q)$.

4.3 Security notions and proof structure

4.3.1 Secrecy

We demand the secrecy of the message ε-ENC as in Definition 2.4, secrecy of the future keys ε-KR as in Definition 2.7 and forward secrecy ε-FS as in Definition 2.9. We take advantage of Lemma 2.10 to guarantee all three properties by bounding a single norm: $\|\rho^{M\tilde{K}CT\mathrm{E}} - \rho^{M} \otimes \rho^{\tilde{K}} \otimes \rho^{CT\mathrm{E}}\|_1$. We prove the ε-ENC of the augmented message. Since k' and τ are part of m, this implies that the future key k' is secure when the message

[6] The strings u and v are never both used in the same round. We describe them independently since they have a different length, but the shorter (v) may as well be a substring of the longer (u).

[7] The size difference between k and k' is justified since only λ fresh bits are needed, e.g. the tags can be protected by a one-time pad.

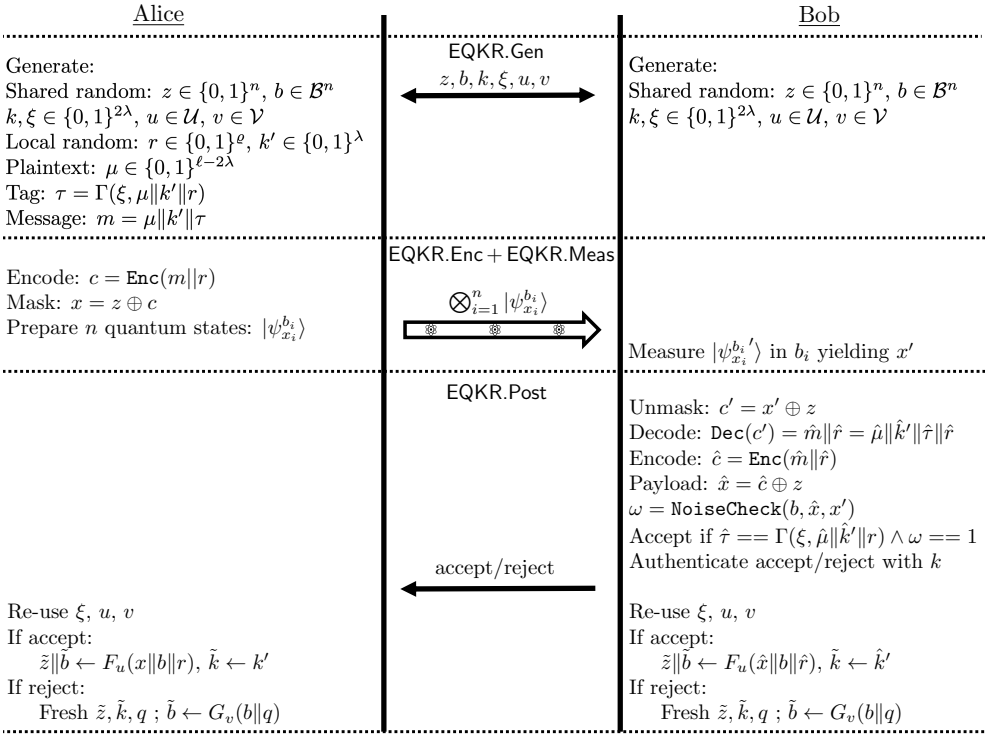

Figure 4.2: *Protocol steps of* EQKR.

is secure, and that the MAC key ξ used for τ can be re-used securely. We start with steps 1 and 2 of the proof recipe, describing an equivalent EPR version of the protocol including random permutations and random Pauli operators. We describe the CPTP maps (step 3) and obtain a 1-norm on which we can apply Lemma 2.10. Then we bound this norm in steps 4 and 5 until we reach exactly the expression in (4.1). We refer back to the bounds of Chapter 3 for an expression in the asymptotic as well as the finite size regime. Due to the difference in the key update procedure, we make note of a small extra term in the reject case.

4.3.2 Correctness

The authentication tag that is part of the augmented message guarantees authenticity of the reconstructed message. In the accept case we have $\hat{m} = m$ except with probability at most $2^{-\lambda}$. This guarantees the correctness of the plaintext as well as $\tilde{k}$. In the accept case, the future keys $\tilde{z}$ and $\tilde{b}$ are a function of x, b and r for Alice and $\hat{x}, b$ and $\hat{r}$ for Bob. When the authentication tag τ successfully authenticates $\hat{m}$ and $\hat{r}$ this also guarantees that $x = \hat{x} = \mathtt{Enc}(\hat{m} \| \hat{r}) \oplus z$, so that $\tilde{z}$ and $\tilde{b}$ are the same for Alice and Bob with probability $2^{-\lambda}$ as well. In the reject case, $\tilde{z}, \tilde{b}$ are only a function of shared key material.

In addition an authentication tag is used for the feedback bit. If this tag is forged Alice and Bob could also end up with different $\tilde{z}, \tilde{b}$. This adds another factor of $2^{-\lambda}$ to the failure probability. The total probability that Alice and Bob have the same output message and future keys is at least $1 - 2^{1-\lambda}$.

4.4 Protocol reformulation for the security proof

We introduce a sequence of small modifications to the protocol of Section 4.2. Before moving to the EPR version we introduce an intermediate step. Before encoding into qubits, we apply a random mask. Next we introduce the same actions as in the previous chapter, allowing us to achieve a very similar proof.

- We mask the qubit payload with public randomness.
- We go to an EPR version.
- We add random permutation of the qubits.
- We add random Pauli transforms.
- We pretend that the two authentication tags cannot be forged.

4.4.1 Masking the qubit payload with public randomness

Alice picks a random string $a \in \{0,1\}^n$. She computes $s = x \oplus a$. Instead of qubit states $|\psi^{b_i}_{x_i}\rangle$ she prepares $|\psi^{b_i}_{s_i}\rangle$. We denote Bob's measurement result as $t \in \{0,1\}^n$. After Bob's measurement, Alice publishes a over an authenticated channel.[8] Bob computes $x' = t \oplus a$. Note that the qubit payload is completely randomized by a without affecting the computations of Alice and Bob. Eve's ancilla does not depend on a, see Section 2.6.3.

4.4.2 EPR version of the protocol (proof step 1)

Instead of having Alice prepare a qubit, she prepares an EPR pair and sends half to Bob. Alice and Bob measure their i'th qubit in basis b_i; this yields s_i for Alice and t_i for Bob, where t_i equals $\overline{s_i}$ plus noise. Alice computes $a = s \oplus x$ and publishes a in an authenticated way. Bob computes $x' = \bar{t} \oplus a$. As in Section 2.6, the statistics of the variables a, x, x', s, t is unchanged by this modification.

4.4.3 Adding a random permutation

The protocol of Section 4.4.2 is permutation invariant. To make this obvious we add a random permutation to the protocol. Alice and Bob publicly agree on a random permutation π. Before performing any measurement they both apply π to their own set of n qubits. Then they forget π. The remainder of the protocol is as in Section 4.4.2.

[8] This is a tamper-proof channel with perfect authentication.

As in Section 2.5.2, the effect of the permutation on the noise positions is undone by the error correction. Hence all the classical variables that are processed/computed after the error correction step are unaffected by π. We can use Lemma 2.16. The new protocol is equivalent to the one in Section 4.4.2.

4.4.4 Adding random Pauli transforms

For each individual EPR pair, Alice and Bob publicly agree on a random $\alpha_i \in \{0,1,2,3\}$. They both apply the Pauli transform σ_{α_i} to their own qubit states, and then forget α. This happens before they do their measurement. The rest of the protocol is as in Section 4.4.3.

As argued in Section 2.5.2, Alice's measurement result is now uniform even when Eve makes the (noisy) EPR pairs. The padding z ensures this equivalence holds in the case of known plaintext as well. The random-Paulis trick yields a major simplification, see Section 2.6.8.

4.4.5 Pretending that the authentication tags are unforgeable

We pretend that Eve is unable to forge the authentication tag τ used to authenticate the message and the authentication tag for the feedback bit. This pretense is true except with probability $\leq 2^{1-\lambda}$. This has two benefits: (i) We get rid of complicated case-by-case analyses that would allow events where the error correction yields a wrong $\hat{m}, \hat{r}$ without warning, while $\hat{\tau}$ looks correct; (ii) In the accept case Bob's reconstructed variables $\hat{m}, \hat{r}$ automatically equal Alice's m, r, thus reducing the number of variables. As argued in 2.4.4 the difference in diamond distance between the original and the modified protocol is at most $2^{1-\lambda}$.

4.4.6 Modified protocol procedure

Alice and Bob have agreed on a linear error-correcting code with encoding and decoding functions $\texttt{Enc} : \{0,1\}^{\ell+\varrho} \to \{0,1\}^n$ and $\texttt{Dec} : \{0,1\}^n \to \{0,1\}^{\ell+\varrho}$. Furthermore Alice and Bob have agreed on two pairwise independent hash functions $F_u : \{0,1\}^n \times \mathcal{B}^n \times \{0,1\}^\varrho \to \{0,1\}^n \times \mathcal{B}^n$ $(u \in \mathcal{U})$ and $G_v : \mathcal{B}^n \times \mathcal{Q} \to \mathcal{B}^n$ $(v \in \mathcal{V})$. They agree on the channel monitoring procedure of Definition 2.18. Let EQKR' denote a single round of the modified protocol, it consists of the following steps (see Figure 4.3):

EQKR'.Gen:

Alice and Bob generate shared key material consisting of a mask $z \in \{0,1\}^n$, a basis sequence $b \in \mathcal{B}^n$, and seeds $u \in \mathcal{U}$, $v \in \mathcal{V}$ for pairwise independent hashing. Furthermore Alice and Bob have a 'reservoir' of additional spare key material.

Alice generates random strings $r \in \{0,1\}^\varrho$, $k' \in \{0,1\}^\lambda$ and the plaintext $\mu \in \{0,1\}^{\ell-2\lambda}$. She generates a random permutation π of the n qubit positions and random indices $\alpha \in \{0,1,2,3\}^\nu$ for the random Pauli operator. She computes a tag τ that perfectly authenticates μ, k' and r. She computes the augmented message $m = \mu \| k' \| \tau$ (with $m \in \{0,1\}^\ell$).

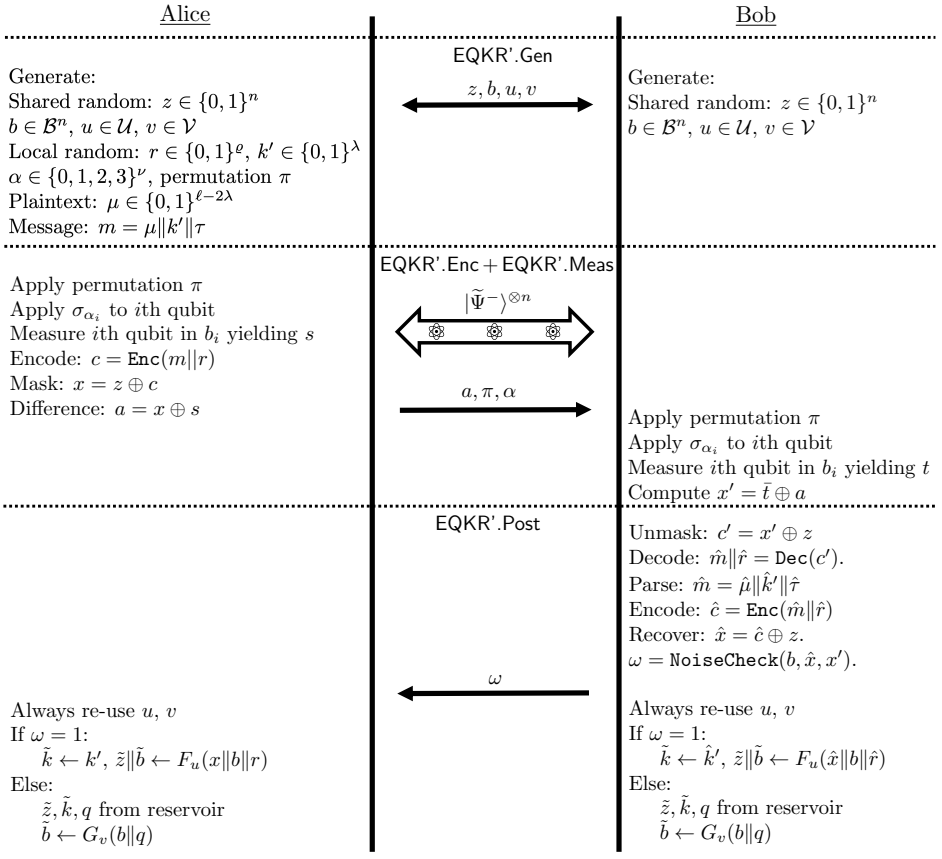

Figure 4.3: *The procedure of the* EQKR' *protocol.*

EQKR'.Enc

Eve generates n noisy EPR pairs $|\widetilde{\Psi}^-\rangle^{\otimes n}$. She sends half of each pair to Alice and half to Bob.

Alice applies the permutation π to her n qubits and applies α_i to the ith qubit. She measures her half of the ith EPR pair in b_i yielding s_i. She computes the encoding $c = \mathtt{Enc}(m \| r) \in \{0,1\}^n$, $x = c \oplus z$ and $a = x \oplus s$. She sends a to Bob over an authenticated channel.

EQKR'.Meas

Bob applies the permutation π to his n qubits, and applies α_i to the ith qubit. He measures the ith qubit in b_i yielding t_i. He computes $x' = \overline{t} \oplus a$.

EQKR'.Post

Bob computes $c' = x' \oplus z$. He tries to recover $\hat{m} \| \hat{r} = \mathtt{Dec}(c')$. If decoding is successful, he parses $\hat{m}$ as $\hat{m} = \hat{\mu} \| \hat{k}' \| \hat{\tau}$. He computes $\hat{c} = \mathtt{Enc}(\hat{m} \| \hat{r})$ and $\hat{x} = \hat{c} \oplus z$. He performs the channel monitoring $\omega = \mathtt{NoiseCheck}(b, \hat{x}, x')$.

Feedback:

Bob sends ω to Alice.
Key Update:
The seeds u, v are always re-used. The updated version of the z, b, k in the next round is denoted as $\tilde{z}, \tilde{b}, \tilde{k}$.

- In case of accept:
  Alice sets $\tilde{k} \leftarrow k'$ and $\tilde{z}||\tilde{b} \leftarrow F_u(x\|b\|r)$.
  Bob sets $\tilde{k} \leftarrow \hat{k}'$ and $\tilde{z}||\tilde{b} \leftarrow F_u(\hat{x}\|b\|\hat{r})$.
- In case of reject:
  Alice and Bob take new $\tilde{z}$ and $\tilde{k}$ from their reservoir.
  They take $q \in \mathcal{Q}$ from the reservoir and set $\tilde{b} \leftarrow G_v(b\|q)$.

4.5 The output state

We move on to step 3 of the proof recipe. Let $\mathcal{E}_{\mathrm{EQKR}}$ be the CPTP map describing EQKR'. It consists of four consecutive mappings

$$\mathcal{E}_{\mathrm{EQKR}} = \mathsf{EQKR'.Post} \circ \mathsf{EQKR'.Meas} \circ \mathsf{EQKR'.Enc} \circ \mathsf{EQKR'.Gen} \tag{4.3}$$

The map $\mathcal{E}_{\mathrm{EQKR}}$ works on the 16^n-dimensional state ρ^{ABE} created by Eve. We follow the systematic approach of Section 2.5.3 to describe the output of $\mathcal{E}_{\mathrm{EQKR}}(\rho^{\mathrm{ABE}})$.

The map EQKR'.Gen fetches the classical input variables and generates the local randomness. The exact procedure for obtaining shared keys is left open as long as its security is composable.

$$\mathsf{EQKR'.Gen}(\rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{mzbuvr} |mzbuvr\rangle\langle mzbuvr| \otimes \rho^{\mathrm{ABE}}. \tag{4.4}$$

Note that all input variables except m are uniform. Let $\mathcal{M}$ denote $\mathsf{EQKR'.Meas} \circ \mathsf{EQKR'.Enc} \circ \mathsf{EQKR'.Gen}$. The measurements introduce a coupling between the classical b register and the quantum state. It destroys the AB subsystem and creates new classical registers $s, t \in \{0,1\}^n$. In addition, Alice computes $c = \mathtt{Enc}(m\|r) \in \{0,1\}^n$, $x = c \oplus z$ and $a = x \oplus s$. Bob computes $x' = \bar{t} \oplus a$.

$$\begin{aligned}\mathcal{M}\big(\rho^{\mathrm{ABE}}\big) \quad = \quad & \mathop{\mathbb{E}}_{mzbuvr} |mzbuvr\rangle\langle mzbuvr| \otimes \mathop{\mathbb{E}}_{st} |st\rangle\langle st| \otimes \rho^{\mathrm{E}}_{bst} \otimes \\ & \sum_{caxx'} |caxx'\rangle\langle caxx'| \delta_{c,\mathtt{Enc}(m\|r)} \delta_{x,c\oplus z} \delta_{a,x\oplus s} \delta_{x',\bar{t}\oplus a}\end{aligned} \tag{4.5}$$

where $\mathbb{E}_{st}(\cdot) = \sum_{st} 2^{-n} P_{t|s}(\cdot)$, with $P_{t|s}$ depending on the form of ρ^{ABE}. In step 5 we will use a simple form of $P_{t|s}$ due to the factorized form of ρ^{ABE}.

The post-processing step introduces $\omega, \tilde{z}$, $\tilde{b}$ and q is fetched from the reservoir. Let $\theta_{bst} = \mathtt{NoiseCheck}(b, x, x')$ indicate whether the noise check of Definition 2.18 was passed. Let $\mathcal{P}$ denote the map that describes the protocol before the variables

are traced out.

$$\begin{aligned}\mathcal{P}(\rho^{\mathrm{ABE}}) &= \mathop{\mathbb{E}}_{mzbuvrq} |mzbruvq\rangle\langle mzbuvrq| \otimes \mathop{\mathbb{E}}_{st} |st\rangle\langle st| \otimes \rho^{\mathrm{E}}_{bst} \otimes \\ &\quad \sum_{cxay\omega\tilde{z}\tilde{b}} |caxx'\omega\tilde{z}\tilde{b}\rangle\langle cxay\omega\tilde{z}\tilde{b}| \delta_{c,\mathtt{Enc}(m\|r)} \delta_{x,c\oplus z} \delta_{a,x\oplus s} \delta_{x',\bar{t}\oplus a} \\ &\quad \delta_{\omega,\theta_{st}} \left[\theta_{bst} \delta_{\tilde{z}\|\tilde{b},F_u(x\|b\|r)} + \overline{\theta_{bst}} 2^{-n} \delta_{\tilde{b},G_v(b\|q)} \right]. \end{aligned} \tag{4.6}$$

In addition EQKR'.Post traces out the variables $zbrqstcxx'$ that are not part of the output, ciphertext or transcript.

$$\begin{aligned}\mathcal{E}_{\mathrm{EQKR}}(\rho^{\mathrm{ABE}}) &= \rho^{UV\tilde{Z}\tilde{B}MA\Omega\mathrm{E}} \\ &= \mathop{\mathbb{E}}_{uvm\tilde{z}\tilde{b}a} \sum_{\omega} |uv\tilde{z}\tilde{b}ma\omega\rangle\langle uv\tilde{z}\tilde{b}ma\omega| \otimes [\omega\rho^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a} + \overline{\omega}\rho^{\mathrm{E}[\omega=0]}_{v\tilde{b}a}] \qquad (4.7) \\ \rho^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a} &= \mathop{\mathbb{E}}_{bst} \rho^{\mathrm{E}}_{bst} \theta_{bst} 2^n |\mathcal{B}|^n \mathop{\mathbb{E}}_{r} \delta_{\tilde{z}\|\tilde{b},F_u[(s\oplus a)\|b\|r]} \qquad (4.8) \\ \rho^{\mathrm{E}[\omega=0]}_{v\tilde{b}a} &= \mathop{\mathbb{E}}_{bst} \rho^{\mathrm{E}}_{bst} \overline{\theta_{bst}} |\mathcal{B}|^n \mathop{\mathbb{E}}_{q} \delta_{\tilde{b},G_v(b\|q)}. \qquad (4.9) \end{aligned}$$

In slight abuse of notation we have written $2^{-n}\sum_a = \mathbb{E}_a$, $2^{-n}\sum_{\tilde{z}} = \mathbb{E}_{\tilde{z}}$, $|\mathcal{B}|^{-n}\sum_{\tilde{b}} = \mathbb{E}_{\tilde{b}}$. In (4.7,4.8,4.9) we would systematically have written $\rho^{\mathrm{E}[\omega=1]}_{uv\tilde{b}\tilde{z}ma}$ and $\rho^{\mathrm{E}[\omega=0]}_{uv\tilde{b}\tilde{z}ma}$, but in the subscript we have kept only the variables on which the state actually has dependence.

The idealized version $\mathcal{F}_{\mathrm{EQKR}}$ of the protocol is obtained by first executing $\mathcal{E}_{\mathrm{EQKR}}$, then tracing away the message m and the keys $uv\tilde{z}\tilde{b}$, and finally replacing them with completely random values.[9]

$$\begin{aligned}\mathcal{F}_{\mathrm{EQKR}}(\rho^{\mathrm{ABE}}) &= \chi^{UV\tilde{Z}\tilde{B}A} \otimes \mathop{\mathbb{E}}_{m} \sum_{\omega} |m\omega\rangle\langle m\omega| \otimes \left(\omega\rho^{\mathrm{E}[\omega=1]} + \overline{\omega}\rho^{\mathrm{E}[\omega=0]} \right) \qquad (4.10) \\ \rho^{\mathrm{E}[\omega=1]} &= \mathop{\mathbb{E}}_{bst} \rho^{\mathrm{E}}_{bst} \theta_{bst} \qquad (4.11) \\ \rho^{\mathrm{E}[\omega=0]} &= \mathop{\mathbb{E}}_{bst} \rho^{\mathrm{E}}_{bst} \overline{\theta_{bst}}. \qquad (4.12) \end{aligned}$$

The states with label '$[\omega = 1]$' are sub-normalized; we have $\operatorname{tr}\rho^{\mathrm{E}[\omega=1]} = \mathbb{E}_{bst}\,\theta_{bst}$ and $\mathbb{E}_u \operatorname{tr}\rho^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a} = \mathbb{E}_{bst}\,\theta_{bst}$, where $\mathbb{E}_{bst}\,\theta_{bst}$ is the probability that the noise check of Definition 2.18 yields one. Similarly $\operatorname{tr}\rho^{\mathrm{E}[\omega=0]} = 1 - \mathbb{E}_{bst}\,\theta_{bst}$ and $\mathbb{E}_v \operatorname{tr}\rho^{\mathrm{E}[\omega=0]}_{v\tilde{b}\tilde{z}a} = 1 - \mathbb{E}_{bst}\,\theta_{bst}$.

Note that when m is uniform, the trace distance of the actual versus the ideal output state has an intuitive meaning as the distance of the keys/seeds from uniformity given Eve's side information,

$$\left\| (\mathcal{E}_{\mathrm{EQKR}} - \mathcal{F}_{\mathrm{EQKR}})(\rho^{\mathrm{ABE}}) \right\|_1 = \left\| \rho^{UV\tilde{Z}\tilde{B}MA\Omega\mathrm{E}} - \chi^{MUV\tilde{Z}\tilde{B}} \otimes \rho^{A\Omega\mathrm{E}} \right\|_1. \tag{4.13}$$

Note that (4.13) allows us to use Lemma 2.10 such that a small diamond norm implies encryption, key recycling and forward secrecy.

[9] The distribution of m does not have to be uniform.

4.6 Main result: upper bound on the diamond norm

Theorem 4.1. *Let $\bar{\rho}^{\mathrm{E}}$ denote a smoothed state satisfying $\|\rho^{\mathrm{E}} - \bar{\rho}^{\mathrm{E}}\|_1 \leq \varepsilon$. Let $\gamma_b \in [0, \frac{1}{2}]$ be a noise parameter corresponding to basis b. Let $\gamma = \max_b \gamma_b$, let β be the noise threshold and let n_b denote the number qubits Alice measures in basis b. Then*

$$\Big\| \mathcal{E}_{\mathrm{EQKR}} - \mathcal{F}_{\mathrm{EQKR}} \Big\|_\diamond < (n+1)^{15} \left[\frac{1}{2\sqrt{|Q|}} + \min\left(P_{\mathrm{acc}}, \varepsilon + \frac{1}{2} \mathrm{tr}_{\mathrm{E}} \sqrt{2^{n-\varrho} |\mathcal{B}|^n \mathrm{tr}_{BS}(\bar{\rho}^{BSE})^2} \right) \right]. \quad (4.14)$$

with

$$P_{\mathrm{acc}} = \mathop{\mathbb{E}}_{n_b : \sum_b n_b = n} \prod_{b \in \mathcal{B}} \sum_{c=0}^{\lfloor n_b \beta \rfloor} \binom{n_b}{c} \gamma_b^c (1-\gamma_b)^{n_b - c}. \quad (4.15)$$

The $\min\{\cdots\}$ term is the same as in (4.1) with ℓ replaced by $n - \varrho$. Since the same symmetrization is used, ρ^{BSE} has the same description for QKR of Chapter 3 and EQKR. This implies the asymptotic result (4.2) with ℓ replaced by $n - \varrho$. Asymptotically it holds that the error correction redundancy has size $n - (\ell + \varrho) \to nh(\beta)$. This then yields an expression $\frac{1}{2}\sqrt{2^{\ell - n + nh(\{1-\frac{3}{2}\gamma, \frac{\gamma}{2}, \frac{\gamma}{2}, \frac{\gamma}{2}\}) + \mathcal{O}(\sqrt{n})}}$. We conclude that the asymptotic rate (ℓ/n) equals $1 - h(\{1 - \frac{3}{2}\gamma, \frac{\gamma}{2}, \frac{\gamma}{2}, \frac{\gamma}{2}\})$, as mentioned in Section 4.1.3. The factor $2^{1-\lambda}$ in (4.1) comes from the transition from the original to the modified protocol and is part of the final security parameter for EQKR as well.

The term $\frac{1}{2\sqrt{|Q|}}$ dictates that, in order to have α bits of security, we have to set $\log|\mathcal{Q}| > 30\log(n+1) - 2 + 2\alpha$. Hence in case of reject the amount of expended key material is $n - 1 + 30\log(n+1) + \lambda + 2\alpha$. Asymptotically this is $n[1 + \mathcal{O}(\frac{\log n}{n})]$.

Proof of Theorem 4.1: For bounding the trace norm $\|(\mathcal{E}_{\mathrm{EQKR}} - \mathcal{F}_{\mathrm{EQKR}})(\rho^{\mathrm{ABE}})\|_1$, we start from (4.7), (4.10) and use the fact that the eigenvalue problem reduces to an individual eigenvalue problem for each value of the classical variables, orthogonal to the other values. We get

$$\begin{aligned} \|(\mathcal{E}_{\mathrm{EQKR}} - \mathcal{F}_{\mathrm{EQKR}})(\rho^{\mathrm{ABE}})\|_1 &= D_{\mathtt{acc}} + D_{\mathtt{rej}} && (4.16) \\ D_{\mathtt{acc}} &= \mathop{\mathbb{E}}_{um\tilde{z}\tilde{b}a} \Big\| \rho^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a} - \rho^{\mathrm{E}[\omega=1]} \Big\|_1 && (4.17) \\ D_{\mathtt{rej}} &= \mathop{\mathbb{E}}_{vm\tilde{z}\tilde{b}a} \Big\| \rho^{\mathrm{E}[\omega=0]}_{v\tilde{b}\tilde{z}a} - \rho^{\mathrm{E}[\omega=0]} \Big\|_1. && (4.18) \end{aligned}$$

First we provide two upper bounds on $D_{\mathtt{acc}}$. The first one simply follows from the triangle inequality,

$$\begin{aligned} \mathop{\mathbb{E}}_{u} \Big\| \rho^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a} - \rho^{\mathrm{E}[\omega=1]} \Big\|_1 &\leq \mathop{\mathbb{E}}_{u} \|\rho^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a}\|_1 + \mathop{\mathbb{E}}_{u} \|\rho^{\mathrm{E}[\omega=1]}\|_1 && (4.19) \\ &= \mathop{\mathbb{E}}_{u} \mathrm{tr}\, \rho^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a} + \mathrm{tr}\, \rho^{\mathrm{E}[\omega=1]} = 2 \mathop{\mathbb{E}}_{bst} \theta_{bst}. && (4.20) \end{aligned}$$

For the second bound on $D_{\mathtt{acc}}$ we follow the remaining steps of the proof recipe of Section 2.5. Step 4: we introduce smoothing of ρ as in [Ren05, RK05, TSSR11], allowing states $\bar{\rho}$ that are ε-close to ρ in the sense of trace distance. The smoothing has no effect on the classical part of the classical-quantum states. We have $D_{\mathtt{acc}} \leq 2\varepsilon + \overline{D}_{\mathtt{acc}}$, with $\overline{D}_{\mathtt{acc}} = \mathbb{E}_{uvm\tilde{z}\tilde{b}a} \|\bar{\rho}^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a} - \bar{\rho}^{\mathrm{E}[\omega=1]}\|_1$. We write

$$\overline{D}_{\mathtt{acc}} = \mathop{\mathbb{E}}_{mu\tilde{z}\tilde{b}a} \operatorname{tr}\sqrt{(\bar{\rho}^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a} - \bar{\rho}^{\mathrm{E}[\omega=1]})^2} \tag{4.21}$$

$$\overset{\text{Jensen}}{\leq} \mathop{\mathbb{E}}_{m\tilde{z}\tilde{b}a} \operatorname{tr}\sqrt{\mathop{\mathbb{E}}_{u}(\bar{\rho}^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a} - \bar{\rho}^{\mathrm{E}[\omega=1]})^2} \tag{4.22}$$

$$= \mathop{\mathbb{E}}_{m\tilde{z}\tilde{b}a} \operatorname{tr}\sqrt{\mathop{\mathbb{E}}_{u}(\bar{\rho}^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a})^2 - (\bar{\rho}^{\mathrm{E}[\omega=1]})^2}. \tag{4.23}$$

In (4.22) we used Jensen's inequality (Lemma 2.14). In (4.23) we used $\mathbb{E}_u\, \bar{\rho}^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a} = \bar{\rho}^{\mathrm{E}[\omega=1]}$. Next we evaluate the expression under the square root, making use of the properties of the pairwise independent hash function F. Squaring (4.8) yields

$$\begin{aligned}
&\mathop{\mathbb{E}}_{u}(\bar{\rho}^{\mathrm{E}[\omega=1]}_{u\tilde{b}\tilde{z}a})^2 - (\bar{\rho}^{\mathrm{E}[\omega=1]})^2 \\
&\quad= \mathop{\mathbb{E}}_{bb'ss'tt'} \bar{\rho}^{\mathrm{E}}_{bst}\bar{\rho}^{\mathrm{E}}_{b's't'}\theta_{bst}\theta_{b's't'}2^{2n}|\mathcal{B}|^{2n} && (4.24)\\
&\quad\mathop{\mathbb{E}}_{urr'} \delta_{\tilde{z}\|\tilde{b},F_u[(s\oplus a)\|b\|r]}\delta_{\tilde{z}\|\tilde{b},F_u[(s'\oplus a)\|b'\|r']} - (\bar{\rho}^{\mathrm{E}[\omega=1]})^2 \\
&\quad= \mathop{\mathbb{E}}_{bb'ss'tt'} \bar{\rho}^{\mathrm{E}}_{bst}\bar{\rho}^{\mathrm{E}}_{b's't'}\theta_{bst}\theta_{b's't'} \mathop{\mathbb{E}}_{rr'}[1+(2^n|\mathcal{B}|^n-1)\delta_{ss'}\delta_{bb'}\delta_{rr'}] - (\bar{\rho}^{\mathrm{E}[\omega=1]})^2 && (4.25)\\
&\quad= (2^n|\mathcal{B}|^n-1)2^{-\varrho} \mathop{\mathbb{E}}_{bb'ss'tt'} \delta_{bb'}\delta_{ss'}\bar{\rho}^{\mathrm{E}}_{bst}\bar{\rho}^{\mathrm{E}}_{b's't'}\theta_{bst}\theta_{b's't'} && (4.26)\\
&\quad< 2^{n-\varrho}|\mathcal{B}|^n \mathop{\mathbb{E}}_{bb'ss'tt'} \delta_{bb'}\delta_{ss'}\bar{\rho}^{\mathrm{E}}_{bst}\bar{\rho}^{\mathrm{E}}_{b's't'} && (4.27)\\
&\quad= 2^{n-\varrho}|\mathcal{B}|^n \mathop{\mathbb{E}}_{bb'ss'} \delta_{bb'}\delta_{ss'}\bar{\rho}^{\mathrm{E}}_{bs}\bar{\rho}^{\mathrm{E}}_{b's'} = 2^{n-\varrho}|\mathcal{B}|^n \mathrm{tr}_{BS}(\bar{\rho}^{BSE})^2. && (4.28)
\end{aligned}$$

In (4.25) we use the pairwise independent property of F_u. In (4.27) we used $\theta_{bst} \leq 1$. We have obtained the bound $\overline{D}_{\mathtt{acc}} < \sqrt{2^{n-\varrho}|\mathcal{B}|^n}\cdot \operatorname{tr}_{\mathrm{E}}\sqrt{\mathrm{tr}_{BS}(\bar{\rho}^{BSE})^2}$. We derive a bound on $D_{\mathtt{rej}}$ using similar steps, but without the smoothing. Squaring (4.9) and taking the expectation $\mathbb{E}_v$ we get

$$\begin{aligned}
&\mathop{\mathbb{E}}_{v}(\rho^{\mathrm{E}[\omega=0]}_{v\tilde{b}\tilde{z}a})^2 - (\rho^{\mathrm{E}[\omega=0]})^2 \\
&\quad= \mathop{\mathbb{E}}_{bb'ss'tt'} \rho^{\mathrm{E}}_{bst}\rho^{\mathrm{E}}_{b's't'}\overline{\theta_{bst}}\,\overline{\theta_{b's't'}} \mathop{\mathbb{E}}_{qq'} |\mathcal{B}|^{2n} \mathop{\mathbb{E}}_{v}\left[\delta_{\tilde{b},G_v(b\|q)}\delta_{\tilde{b},G_v(b'\|q')}\right] - (\rho^{\mathrm{E}[\omega=0]})^2 && (4.29)\\
&\quad= \mathop{\mathbb{E}}_{bb'ss'tt'} \rho^{\mathrm{E}}_{bst}\rho^{\mathrm{E}}_{b's't'}\overline{\theta_{bst}}\,\overline{\theta_{b's't'}} \mathop{\mathbb{E}}_{qq'}\left\{1+(|\mathcal{B}|^n-1)\delta_{bb'}\delta_{qq'}\right\} - (\rho^{\mathrm{E}[\omega=0]})^2 && (4.30)\\
&\quad= \frac{|\mathcal{B}|^n-1}{|\mathcal{Q}|} \mathop{\mathbb{E}}_{bb'ss'tt'} \delta_{bb'}\rho^{\mathrm{E}}_{bst}\rho^{\mathrm{E}}_{b's't'}\overline{\theta_{bst}}\,\overline{\theta_{b's't'}} && (4.31)\\
&\quad< \frac{|\mathcal{B}|^n}{|\mathcal{Q}|} \mathop{\mathbb{E}}_{bb'ss'tt'} \delta_{bb'}\rho^{\mathrm{E}}_{bst}\rho^{\mathrm{E}}_{b's't'} = \frac{|\mathcal{B}|^n}{|\mathcal{Q}|} \mathop{\mathbb{E}}_{bb'} \delta_{bb'}\rho^{\mathrm{E}}_{b}\rho^{\mathrm{E}}_{b'}. && (4.32)
\end{aligned}$$

Step 5: we use Lemma 2.16 to write ρ^{ABE} in factorized form $\rho^{\mathrm{ABE}} = (\sigma^{\mathrm{ABE}})^{\otimes n}$. This allows us to write $p_{t|s} = \gamma^{\mathtt{Hamm}(s\oplus\bar{t})}(1-\gamma)^{\mathtt{Hamm}(s\oplus t)}$ where we assume the noise in each

basis is the same maximal value γ for the second term in the $\min(\cdot)$ of (4.14). For the first term in the $\min(\cdot)$ we allow for different noise levels γ_b and find $\mathbb{E}_{bst}\,\theta_{bst} = P_{\text{acc}}$. Finally, we can use Lemma 2.20 to write $\rho_b^{\text{E}} = \rho^{\text{E}}$ yielding the bound $D_{\texttt{rej}} < 1/\sqrt{|Q|}$. □

4.7 Discussion

We have shown that the protocol QKR of Chapter 3 can be modified in a way that *eliminates all classical communication from Alice to Bob, without increasing the number of qubits.* Essentially we have moved the classical OTP of QKR to the next round. Furthermore the error correction and authentication are happening 'inside' the quantum state. The asymptotic communication rate is not affected and is equal to the rate of QKD with one-way postprocessing. Our protocol has forward secrecy. The size of the keys shared by Alice and Bob is $n + n\log|\mathcal{B}| + \log|\mathcal{U}| + 4\lambda$, (namely $z \in \{0,1\}^n$, $b \in \mathcal{B}^n$, $u \in \mathcal{U}$, $\xi \in \{0,1\}^\lambda$, $k \in \{0,1\}^\lambda$), with $\log|\mathcal{U}| = 2n + 2n\log|\mathcal{B}| + \varrho$. The size of $\mathcal{U}$ could be reduced by switching from pairwise independent hash functions to universal hash functions or almost-univeral hashing. While the proof of QKR in the previous chapters relies on the hash seed u for the decoupling of m and x, the pad z has that role in EQKR. Another way of reducing the size of the initial key material is reducing the size of z by ϱ. In the encoding step we can choose to write c in systematic form. Then a part of c literally equals r, which is already uniform. Reducing the size of z by ϱ then still yields a uniform string allowing us to use the same proof technique while reducing the initial key material is reduced. Furthermore, the length of the seeds u, v is reduced by 2ϱ. The effect of this modification to the rate is to be determined.

In the accept case the reservoir of shared key material remains untouched. In the reject case the number of bits expended from the reservoir is $n + \mathcal{O}(\log n)$. This can again be reduced by shortening z by ϱ. Asymptotically, in the noiseless case ($n \to \ell + \varrho$, $\varrho \to 0$), this expenditure is very close to the optimum value ℓ [DPS05]. (It is not possible to protect an ℓ-bit message information-theoretically with less than ℓ bits of key expenditure.)

It is possible to take the seed u from public randomness that is drawn in every QKR round. This would not affect the security, and it would reduce the amount of shared key material. However, it would require either (a) a source of public randomness that is not known by Eve beforehand, e.g. a broadcast; or (b) communication of u from Alice to Bob or the other way round. The former involves nontrivial logistics, while the latter violates the aims of this chapter.

We have not done anything about the classical feedback from Bob to Alice. It cannot be removed, because Alice needs to know if Bob correctly received her message. On the other hand, one can consider a scenario where Alice and Bob are both senders, in an alternating way. Then the feedback bit can be placed inside the next message, resulting in a fully quantum conversation.

There is one drawback to the EQKR protocol described in this chapter. It is bad at dealing with erasures. As the actual message (as opposed to a random string) is encoded in the quantum state, absorption of qubits in the quantum channel has to be

compensated in the error-correcting code. The effect of erasures on the rate is severe. A solution as proposed in Section 3.5.2 would imply that the message is no longer encoded directly in the qubits; instead Alice sends a random string to Bob, part of which survives the channel and gets used to derive an OTP. Such a solution does not satisfy the aims of this chapter.

4.8 Can full embedding add to the security of QKR?

The EQKR protocol achieves very efficient communication in terms of round complexity, classical communication, rate and key expenditure, especially in the noiseless case. This leaves little to be desired in terms of efficiency. Besides efficiency encoding the message directly into the qubits can increase the security of the protocol in the following sense. When Alice and Bob are certain that the qubits have not been attacked, the qubits no longer exists after the protocol ends. This seems to imply that, as in unclonable encryption as introduced by Gottesman [Got03], it is safe to leak the key material after the protocol is finished. However, since the privacy amplification step in EQKR happens in between rounds, a single qubit can leak one bit of plaintext when the keys become public. Since Alice and Bob can in no way guarantee not a single qubit is kept in Eve's quantum memory, EQKR has no unclonable encryption.

Can a quantum key recycling protocol have unclonable encryption? Is it possible to have an unclonable encryption protocol that does not use up key material? How does modifying a QKR scheme to have unclonable encryption affect its efficiency? These questions will be answered in the next chapter.

Chapter 5
Qubit-based Unclonable Encryption with Key Recycling

A stronger notion of encryption
As Alice and Bob's relationship matures, their desire for an unbreakable encryption scheme becomes stronger. Having used quantum key distribution combined with one-time pad encryption and quantum key recycling with and without classical side-information, they already communicate with information-theoretical security. One crucial assumption for the security of their messages is that the keys used for encryption never leak to the outside world. Eve should never get to know them.
One day Bob reads an article that revises his anxiousness about secure communication. There are many cases of governments, hospitals, schools, lawyers, etc. not properly erasing sensitive data from their computers when throwing them away [GS03]. If Alice or Bob fails to properly destroy the secret keys used in their protocol, all their past communication could still fall into Eve's hands! The protocol is not the problem, they are the problem. Maybe there's a protocol that can help though. They need a protocol that protects their messages from human errors. They want to communicate in such a way that after the messages are read by Bob, nothing they do in the future (except leak the message itself) will compromise the security of the message. They want to be able to safely give Eve all the keys used in their protocol without consequences. They want unclonable encryption. Of course they want to sacrifice as little of their so recently gained communication efficiency as possible.

5.1 Introduction

5.1.1 Doing better than One-Time Pad encryption

Classically, the best confidentiality guarantee is provided by One-Time Pad (OTP) encryption. If Alice and Bob share a uniform n-bit secret key, they can exchange an n-bit message with information-theoretic security. In the classical setting Eve is able

This chapter is based on [LŠ20a].

to save a copy of the ciphertext. For the message to remain secure in the future, two conditions must be met:

1. The key is used only once.
2. The key is never revealed.

If a quantum channel is available, these conditions can both be relaxed. (i) Quantum Key Recycling (QKR) [BBB82, FS17, LŠ19a, LŠ21] schemes provide a way of re-using encryption keys. (ii) Unclonable Encryption (UE) [Got03] guarantees that a message remains secure even if the keys leak at some time in the future.

In this chapter we introduce a scheme that achieves both the key recycling and UE properties, and we explicitly prove that this can be achieved with low communication complexity. Our scheme acts only on individual qubits with simple prepare-and-measure operations.

5.1.2 Quantum Key Recycling

Quantum key distribution allows Alice and Bob to extend a small key, used for authentication, to a longer key in an information-theoretically secure way. Combined with classical one-time pad encryption this lets Alice and Bob exchange messages with information-theoretic security. The security of both QKD and the one-time pad is composable. The security of the combination of the two schemes is guaranteed by the security of both schemes separately. In quantum key recycling, a classical message is encrypted into a quantum 'cipherstate' using basis choices that are a shared secret between Alice and Bob, and allows for the re-use of this secret when no disturbance is detected. QKD and QKR have a lot in common. (i) They both encode classical data in quantum states, in a basis that is not a priori known to Eve. (ii) They rely on the no-cloning theorem [WZ82] to guarantee that without disturbing the quantum state, Eve can not gain information about the classical payload or about the basis.

The main advantage of QKR over QKD+OTP is reduced round complexity: QKR needs only two rounds. After the communication from Alice to Bob, only a single bit of authenticated information needs to be sent back from Bob to Alice. In the previous chapters we showed that QKR over a noisy quantum channel can achieve the same communication rate as QKD (Chapter 3) even if Alice sends only qubits (Chapter 4); a further reduction of the total amount of communicated data.

5.1.3 Unclonable Encryption

In 2003, D. Gottesman introduced a scheme called *Unclonable Encryption*[1] (UE) [Got03] where the message remains secure even if the encryption keys leak at a later time (provided that not too much disturbance is detected). His work was motivated by the fact that on the one hand many protocols require keys to be deleted, but on the other hand permanent deletion of data from nonvolatile memory is a nontrivial task. In this light it is prudent to assume that all key material which is not *immediately*

[1] This is different from the unclonability notion of Broadbent and Lord [BL20] which considers two collaborating parties who both wish to recover the plaintext.

discarded is in danger of becoming public in the future; hence the UE security notion demands that the message stays safe even if all this key material is made public after Alice and Bob decide that they didn't detected too much disturbance. (In case too much disturbance is detected, the keys have to remain secret forever or permanently destroyed.)

It is interesting to note that Gottesman's UE construction allows partial re-use of keys. However, it still expends one bit of key material per qubit sent. In this chapter we introduce qubit-based UE without key expenditure. Gottesman remarked on the close relationship between UE and QKD, and in fact constructed a QKD variant from UE. The revealing of the basis choices in QKD is equivalent to revealing keys in UE.

Since QKR sends a message directly instead of establishing a key for later use, QKR protocols are natural candidates to have the UE property. In the case of noiseless quantum channels, the high-dimensional encryption scheme [DPS05] and the qubit-based scheme [FS17] seem to have UE. The QKR protocol of Chapter 3 also seems to have UE for noiseless channels as well as for noisy channels although the parameters would need to be modified, i.e. more privacy amplification is needed, reducing the efficiency. However, none of these conjectures have been explicitly stated or proven, which is a shame since resilience against key leakage is an interesting security feature. The QKR of Chapter 4 where Alice sends only qubits is clearly not unclonable, due to the fact that single-use keys are stored at the end of each round.

5.2 Combining unclonable encryption and key recycling

We construct an Unclonable Encryption scheme with recyclable keys, while aiming for low communication complexity and high rate. We consider the following setting. Alice and Bob have a reservoir of shared key material. Alice sends data to Bob in N chunks. Each chunk individually is tested by Bob for consistency (sufficiently low noise and valid MAC). In case of reject they have to access new key material from the reservoir. In case of accept, Alice and Bob re-use their key material; this may be done either by keeping keys unchanged or by re-computing keys without accessing the reservoir. If the N'th round was an accept, all keys of round N are assumed to become public.

- For our definitions of key recycling (Definition 2.7) and unclonable encryption (Defnition 2.11) we show a relation between KR and UE: If a KR scheme re-uses all its long-term secrets in unchanged form upon accept, then it also has the UE property.
- We introduce KRUE, a qubit-based prepare-and-measure scheme that satisfies KR and UE. Alice sends a single transmission, which consists entirely of qubits. Bob responds with an authenticated classical feedback bit. We apply the proof recipe of Section 2.5 and find that it reduces to the diamond distance found in the proof of 6-state QKD (Section 2.6). In the case of a noiseless channel this reduction is almost immediate, without involving any inequalities.
- KRUE by itself expends key material. To become 'key neutral', it relies on an external mechanism to securely transport some key material for the key update.

We propose to employ the efficient EQKR scheme of Chapter 4 as the external mechanism. The advantage of using a QKR scheme is that it can be combined efficiently with KRUE to yield a two-pass protocol, i.e. its advantage is low round complexity. We derive the asymptotic rate of the combined KRUE+EQKR scheme for BB84 encoding and 6-state encoding. In the case of BB84 encoding the asymptotic rate of KRUE+EQKR is $\frac{[1-2h(\beta)]^2}{1-h(\beta)}$, Here h is the binary entropy function, and β is the tolerated bit error rate in the quantum channel.[2]

We present a rate comparison between various constructions that achieve UE and KR simultaneously. KRUE+EQKR has the highest rate.

5.3 Pairwise independent hashing with easy inversion

To achieve unclonable encryption, security of the message needs to be guaranteed by output of the performed privacy amplification on the qubit payload. This is different from Chapter 4 where the privacy amplification was done in between rounds. To achieve this without the need for classical communication, we will need a privacy amplification function that is easily computable in two directions. Unfortunately the code-based construction due to Gottesman [Got03] does not work with the proof technique of Chapter 2 and [Ren05], which requires a family of universal hash functions. We will be using a family of pairwise independent hash functions $F : \{0,1\}^k \to \{0,1\}^k$ that are easy to invert. An easy way to construct such a family is to use an affine function in $GF(2^k)$ [LW99]. Let $u = (u_1, u_2)$ with $u_1, u_2 \in GF(2^k)$ randomly chosen such that u_1 is invertible. Define $F_u(x) = u_1 \cdot x + u_2$, where the operations are in $GF(2^k)$. Likewise $F_u^{\text{inv}}(z) = u_1^{-1} \cdot (z + u_2)$. A pairwise independent family of hash functions Φ from $\{0,1\}^k$ to $\{0,1\}^\ell$, with $\ell < k$, can be obtained by taking the ℓ most significant bits of $F_u(x)$.[3] We denote this as

$$\Phi_u(x) \stackrel{\text{def}}{=} F_u(x)[:\ell]. \tag{5.1}$$

The inverse operation is as follows. Given $c \in \{0,1\}^\ell$, generate random $r \in \{0,1\}^{k-\ell}$ and output $F_u^{\text{inv}}(c||r)$. It obviously holds that $\Phi_u(F_u^{\text{inv}}(c||r)) = c$. Computing an inverse in $GF(2^k)$ costs $O(k \log^2 k)$ operations [Moe73].

5.4 Attacker model and security definitions

5.4.1 Attacker model of unclonable encryption

For the setting of unclonable encryption, the attacker model needs to be altered compared to the attacker model of Section 2.1 used thus far. When Alice and Bob need to store information, the attacker model of unclonable encryption considers the difficulty of deleting this information.

[2] For comparison, the key generation rate of 4-state QKD (BB84) is $1 - 2h(\beta)$ see (2.65).

[3] The proof is straightforward. Write $F_u(x) = c\|r$, with $c \in \{0,1\}^\ell$. Let $x' \neq x$. Then $\Pr_u[\Phi_u(x) = c \wedge \Phi_u(x') = c'] = \sum_{r,r' \in \{0,1\}^{k-\ell}} \Pr_u[F_u(x) = c\|r \wedge F_u(x') = c'\|r']$. By the pairwise independence of F this gives $\sum_{r,r' \in \{0,1\}^{k-\ell}} 2^{-2k} = 2^{-2\ell}$.

We work in the same setting as Gottesman [Got03], as discussed in Section 5.1.3. We distinguish between on the one hand long-term secrets and on the other hand short-term secrets. A variable is considered short-term only if it is created[4] and immediately operated upon locally (without waiting for incoming communication), and then deleted. All other variables are long-term. (An example of a short-term variable is a nonce that is generated, immediately used in a function evaluation and then deleted. On the other hand, all keys that are stored between protocol rounds are long-term.)

We consider two world views.

- **World1**. All secrets can be kept confidential indefinitely or are destroyed.
- **World2**. Long-term secrets are in danger of leaking at some point in time.

There are several motivations for entertaining the second world view. (a) It is difficult to permanently erase data from nonvolatile memory. (b) Whereas everyone understands the necessity of keeping message content confidential, it is not easy to guarantee that protocol implementations (and users) handle the keys with the same care as the messages.

QKR protocols are typically designed to be secure in world1. In this chapter we prove security guarantees that additionally hold in world2. One way of phrasing this is to say that we add 'user-proofness' to QKR.

Alice sends data to Bob in N chunks. We refer to the sending of one chunk as a 'round'.[5] In each round Bob tells Alice if he noticed a disturbance (reject) or not (accept). In case of reject they are *alarmed* and they know that they must take special care to protect the keys of this round indefinitely (i.e. a fallback to *World1* security). Crucially, *we assume that a key theft occurring before the end of round N is immediately noticed by Alice and/or Bob.* Without this assumption it would be impossible to do Key Recycling in a meaningful way. We allow all keys to become public after round N.

The rest of the attacker model consists of the attacker model of Section 2.1: no information, other than specified above, leaks from the labs of Alice and Bob; there are no side-channel attacks; Eve has unlimited (quantum) resources; all noise on the quantum channel is considered to be caused by Eve.

5.4.2 Security notions

The proof recipe laid out in Section 2.5 is general enough to handle the altered attacking model relevant for unclonable encryption. A protocol that achieves unclonable encryption as well as key recycling has four security requirements.

- Encryption: The message is confidential in the accept as well as in the reject case. Recall from Definition 2.4 that we require a small norm $\|\rho^{MCT\mathrm{E}} - \rho^{M} \otimes \rho^{CT\mathrm{E}}\|_1$.

[4] Performing a measurement on a quantum state is also considered to 'create' a classical variable.
[5] One data transmission will be called a *pass*. A round consists of multiple passes.

- Unclonable encryption: The message is confidential in the accept case, even when all key material leaks. Recall from Definition 2.11 that we require a small norm $\|\rho^{MK\tilde{K}CT\mathrm{E}}_{\mathtt{accept}} - \rho^{M} \otimes \rho^{K\tilde{K}CT\mathrm{E}}_{\mathtt{accept}}\|_1$.
- Key recycling: The keys remain confidential in the accept and reject case, also when the plaintext leaks. Recall from Definition 2.7 that we require a small norm $\|\rho^{M\tilde{K}CT\mathrm{E}} - \rho^{\tilde{K}} \otimes \rho^{MCT\mathrm{E}}\|_1$.
- Correctness: Alice and Bob hold the same future keys and in the accept case hold the same message.

Note that our KR and UE do not automatically imply ENC. The ENC property has to be considered as a separate requirement. For the combination of ENC and KR can be proven using Lemma 2.10. For protocols that re-use rather than recycle keys, unclonable encryption is implied by encryption and key recycling. The following lemma holds.

Lemma 5.1.

$$(\tilde{K}_{\mathtt{accept}} = K) \ \wedge \ \varepsilon_1\text{-}ENC \ \wedge \ \varepsilon_2\text{-}KR \quad \Longrightarrow \quad (\varepsilon_1+\varepsilon_2)\text{-}UE. \tag{5.2}$$

Proof. With $\tilde{K}_{\mathtt{accept}} = K$ we have $\|\rho^{MK\tilde{K}CT\mathrm{E}}_{\mathtt{accept}} - \rho^{M} \otimes \rho^{K\tilde{K}CTE\mathrm{E}}_{\mathtt{accept}}\|_1 \leq \|\rho^{MKCT\mathrm{E}}_{\mathtt{accept}} - \rho^{M} \otimes \rho^{K} \otimes \rho^{CT\mathrm{E}}_{\mathtt{accept}}\|_1 + \|\rho^{M} \otimes \rho^{K} \otimes \rho^{CT\mathrm{E}}_{\mathtt{accept}} - \rho^{M} \otimes \rho^{KCT\mathrm{E}}_{\mathtt{accept}}\|_1$. The first term is bounded by taking the trace over K and using ε_1-ENC. For the second we take the trace over M, yielding $\|\rho^{KCT\mathrm{E}}_{\mathtt{accept}} - \rho^{K} \otimes \rho^{CT\mathrm{E}}_{\mathtt{accept}}\|_1$. This expression is bounded by ε_2, which is seen by taking the M-trace of (2.7). □

Lemma 5.1 is an important statement: any ENC scheme that upon accept re-uses its keys *in unmodified form* and satisfies KR is automatically a UE scheme. It is interesting to note that [FS17] has $\tilde{K}_{\mathtt{accept}} = K$ but does not satisfy our KR definition, whereas Chapters 3 and 4 satisfy our KR definition but do not have $\tilde{K}_{\mathtt{accept}} = K$. By Theorem 4 in [DPS05] and Lemma 5.1, the *high-dimensional* scheme of Damgård et al. [DPS05] has the UE property.

5.5 The proposed scheme

We propose a qubit-based prepare-and-measure scheme for Unclonable Encryption with Key Recycling. It consists of two components: (i) a core part that we call KRUE, which protects the message, and (ii) a quantum key recycling scheme EQKR for refreshing some of the keys.

KRUE involves two passes: one from Alice to Bob, followed by a short feedback message from Bob to Alice. We use the EQKR scheme of Chapter 4. A different QKR scheme would also suffice as long as it is likewise a two-pass scheme. EQKR is chosen because of its efficiency. The scheme of Chapter 3 will yield the same rate.

We denote the composition of KRUE and EQKR as "KRUE+EQKR". This composition is a two-pass protocol, defined as follows.

1. Alice sends the first pass of KRUE and the first pass of EQKR together.

2. Bob sends the second pass of KRUE and the second pass of EQKR together.
3. Alice and Bob both execute EQKR.Post and then KRUE.Post.

If KRUE has accept but EQKR has reject then EQKR is re-run again on its own until it succeeds. This is safe since EQKR serves only to transport random keys for the next round.

5.5.1 KRUE building blocks

KRUE consists of publicly known algorithms Gen, Enc, Dec and Post. It works with bit-lengths λ, ℓ, k, and n which are publicly known. KRUE needs the following ingredients, which Alice and Bob have agreed on beforehand.

- A set $\mathcal{B}$ of measurement bases. In particular the BB84 set consisting of the standard basis and the Hadamard basis, or the 6-state set consisting of the bases in the $\pm x$, $\pm y$, $\pm z$ direction.
- An information-theoretically secure MAC function $\Gamma : \{0,1\}^{2\lambda} \times \{0,1\}^{\ell-\lambda} \to \{0,1\}^{\lambda}$, outputting a tag τ of length λ, where λ is the security parameter. For an adversary who does not know the key, the probability of forgery is $2^{-\lambda}$.
- The pairwise independent hash families $\{F_u\} : \{0,1\}^{\kappa} \to \{0,1\}^{\kappa}$ and $\{\Phi_u\} : \{0,1\}^{\kappa} \to \{0,1\}^{\ell}$ as discussed in Section 5.3. We use the $\{\Phi_u\}$ for privacy amplification in the 'standard' way, except that Alice is now able to choose the outcome of the hashing.
- A binary linear error correcting code which has encoding function $\mathrm{Enc} : \{0,1\}^{\kappa} \to \{0,1\}^{n}$ in systematic form and decoding function $\mathrm{Dec} : \{0,1\}^{n} \to \{0,1\}^{\kappa}$. The code is built to correct bit error rate β with certainty. (The distance of the code is $2\beta n$.) Asymptotically the codeword length n as a function of κ and β is given by $n \to \frac{\kappa}{1-h(\beta)}$.
- The channel monitoring procedure of Definition 2.18 that checks that the noise does not exceed β seperatly for each basis.

5.5.2 KRUE protocol steps

In round j, Alice wants to send a message $\mu_j \in \{0,1\}^{\ell-\lambda}$. We will often drop the index j for notational brevity. The protocol steps are described below. We use the notation $\vec{0}^{\kappa}$ for the all zero's string of length κ. Section 5.5.3 lists some of the considerations that lie at the basis of this protocol design.

KRUE.Gen:

Alice and Bob generate the shared key material consisting of a mask $z \in \{0,1\}^{\ell}$, a MAC key $k_{\mathrm{MAC}} \in \{0,1\}^{2\lambda}$, a basis sequence $b \in \mathcal{B}^n$, keys $\varphi_0, \varphi_1 \in \{0,1\}^{\lambda}$ for authenticating the feedback bit, a key $u \in \{0,1\}^{2\kappa}$ for universal hashing and a key $e \in \{0,1\}^{n-\kappa}$ to mask the redundancy bits. Alice and Bob furthermore share a reservoir of spare key material (k_{rej}) from which to refresh key material in case of reject.

Alice generates the plaintext $\mu \in \{0,1\}^{\ell-\lambda}$ and a random string $r \in \{0,1\}^{\kappa-\ell}$.

She computes the authentication tag $\tau = \Gamma(k_{\mathrm{MAC}}, \mu)$ and the augmented message $m = \mu \| \tau$.

KRUE.Enc:

Alice computes the ciphertext $c = z \oplus m$, the reversed privacy amplification $p = F_u^{\mathrm{inv}}(c\|r) \in \{0,1\}^\kappa$ and the qubit payload $x = \mathrm{Enc}(p) \oplus (\vec{0}^\kappa \| e) \in \{0,1\}^n$. She deletes r. She prepares $|\Psi\rangle = \bigotimes_{i=1}^n |\psi_{x_i}^{b_i}\rangle$ and sends it to Bob. Alice deletes x, p, c, r.

KRUE.Meas:

Bob receives $|\Psi\rangle'$ and measures in the basis b, yielding $x' \in \{0,1\}^n$.

KRUE.Post

Bob decodes $\hat{p} = \mathrm{Dec}(x' \oplus (\vec{0}^\kappa \| e))$. He computes $\hat{c} = \Phi_u(\hat{p})$, $\hat{x} = \mathrm{Enc}(\hat{p}) \oplus (\vec{0}^\kappa \| e)$ and $\hat{\mu} \| \hat{\tau} = \hat{c} \oplus z$. He performs the channel monitoring and checks the MAC. He computes $\omega = \texttt{NoiseCheck}(b, \hat{x}, x') \wedge \Gamma(k_{\mathrm{MAC}}, \hat{\mu}) == \hat{\tau}$. He sends φ_ω to Alice. Bob deletes $x', \hat{x}, \hat{p}, \hat{c}$.

Alice deduces ω from Bob's feedback, or aborts if she does not receive either φ_0 or φ_1.

Alice and Bob perform the following actions (a tilde denotes the key for the next round):

— Re-use $b, u, k_{\mathrm{MAC}}, \varphi_{\overline{\omega}}$.

— Refresh φ_ω, e to entirely new $\tilde{\varphi}_\omega, \tilde{e}$ using an external mechanism.

— In case of accept re-use z. In case of reject take fresh $\tilde{z}$ from k_{rej}.

After round N, according to the attacker model, all keys from all rounds leak[6] except for masks z associated with reject events. I.e. what leaks is: b, u, k_{MAC}, $\{\varphi_0^{(j)}, \varphi_1^{(j)}, e^{(j)}\}_{j=1}^N$, and if round N was accept also $z^{(N)}$. Note that although r is generated in KRUE.Gen and deleted in KRUE.Enc it is a short term variable as Alice can perform these actions without waiting for Bob. The protocol is also shown in Figure 5.1.

5.5.3 Design rationale

The rationale behind the various design choices in our scheme is as follows.

- The payload $x \in \{0,1\}^n$ needs to be uniform (as seen by Eve), otherwise Eve can get information about the basis b from the qubit states $|\psi_{x_i}^{b_i}\rangle$. Uniformity is most difficult to achieve in the case of known plaintext μ. We make x uniform in three steps. The z masks the ℓ bits of $m \in \{0,1\}^\ell$; then appending r increases that to κ bits; finally the e masks the $n-\kappa$ redundancy bits. Here we need that the error-correcting code is in systematic form.

- The tag τ allows Bob to verify that the received string m has not been manipulated.

- The UE property holds for the following reason. After the keys have been revealed, Eve extracts partial information about x from her quantum system. If x itself were a ciphertext, she would be able to perform decryption and thus

[6] Optionally this leakage can be made part of the protocol, i.e. Alice and Bob publish the keys.

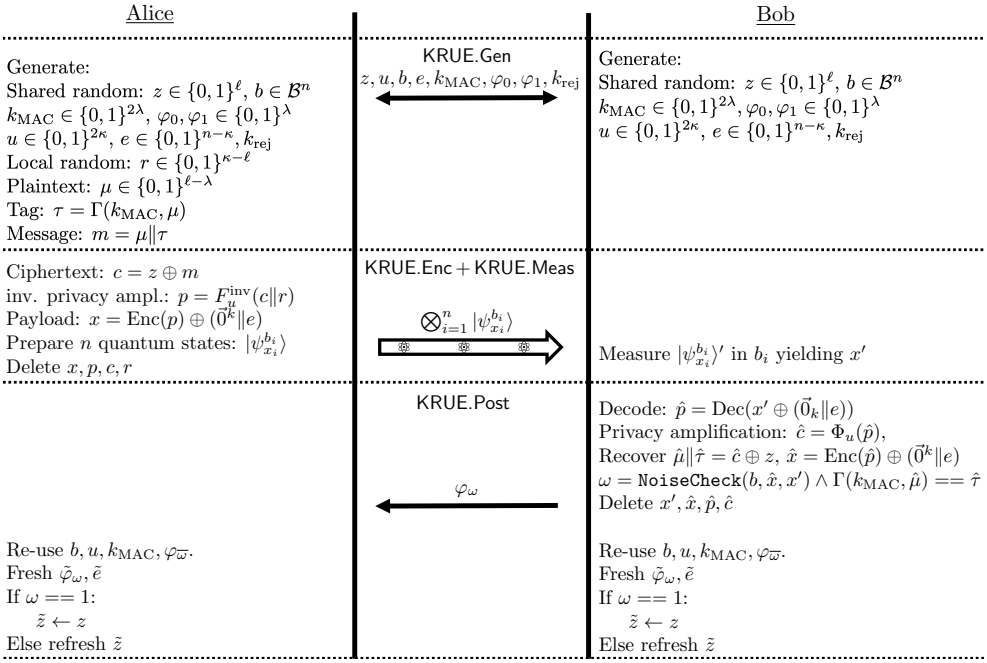

Figure 5.1: *A single round of* KRUE.

obtain some non-negligible amount of information about the plaintext. However, the actual ciphertext c is obtained from x by a privacy amplification step (similar to QKD), and hence Eve knows almost nothing about the ciphertext.

- The usual steps of information reconciliation (error correction Enc,Dec) and privacy amplification (Φ_u) are performed. What is special here is that we do not want the outcome of the hash Φ_u to be random, but equal to some target value c. For this reason we are applying the construction of Section 5.3 with the truncation of the invertible F_u.

- We want to re-use the basis b in unmodified form. Our definition of the KR property (Definition 2.7) demands that Eve learns next to nothing about b, with a formulation in terms of a trace distance, until we let b leak after round N. This requirement is impossible to satisfy if Eve has access to the feedback bit ω. She may make a guess for b in a small number of qubit positions, just small enough to be on the edge of the ECC's error-correction capability, measure those qubits in the guessed bases and forward the resulting state to Bob. Observing ω then yields non-negligible information about b. In order to avoid this problem we encrypt ω temporarily. Bob's feedback φ_ω simultaneously encrypts and authenticates ω. (Note that all ω's are revealed after round N, because all keys leak eventually.) The keys φ_0, φ_1 essentially form a single-use random codebook.

- It is always safe to re-use the key k_{MAC} and the seed u. Intuitively this is clear from the fact that z, e, r together entirely mask the relation between the payload x and the augmented message m. Since the tag is part of m, the k_{MAC} can safely be re-used when m is secure.

- The reason for doing the refreshment of φ_ω, e via an *external* mechanism is that it would be inefficient to send them via Unclonable Encryption. These keys are revealed after round N, so they do not need the extra level of protection. In Section 5.8.5 we study the case where $\tilde{\varphi}_\omega, \tilde{e}$ are sent as part of μ; it turns out that this causes a severe penalty on the rate.

Remark. It is possible to send the *current*-round e via QKR instead of the next-round key $\tilde{e}$. This would make e into a short-term variable instead of a long-term key, and would make it possible to elegantly use Lemma 5.1 in the security proof of KRUE. However, it would also complicate the security analysis of the *combined* scheme. We will not pursue this possibility.

5.6 Proof structure

We prove the security properties laid out in Section 5.4.2. We distinguish between secrecy and correctness. We apply the proof recipe of Section 2.5. We first describe a modified protocol that simplifies the security proof (steps 1 and 2). Next we systematically obtain the CPTP maps describing the modified protocol (step 3). In step 4 we consider smooth states and find a bound on the diamond norms that directly relates the the QKD bound of Section 2.6. Since the same qubit invariances are used, steps 5 and 6 can follow identical steps to the QKD proof and yield very similar bounds. Note that the UE and KR properties follow from slightly different maps since in UE the key is assumed to leak while key recycling only makes sense as long as the keys didn't leak yet.

5.6.1 Secrecy

The notation $\mathcal{E}(\rho^{\mathrm{ABE}})$ stands for the CPTP map $\mathsf{KRUE.Post} \circ \mathsf{KRUE.Dec} \circ \mathsf{KRUE.Enc} \circ \mathsf{KRUE.Gen}$ acting on the AB part of ρ^{ABE}. The output is $\mathcal{E}(\rho^{\mathrm{ABE}}) = \rho^{MKM'\tilde{K}T\Omega\mathrm{E}}$. The different nature of the KR and UE property forces us to introduce additional notations. On the one hand, we write $\mathcal{E}_{\mathrm{UE}} = \mathrm{tr}_{M'} \circ \mathcal{E}$, so that $\mathcal{E}_{\mathrm{UE}}(\rho^{\mathrm{ABE}}) = \rho^{MK\tilde{K}T\Omega\mathrm{E}}$. On the other hand we write $\mathcal{E}_{\mathrm{KR}} = \mathrm{tr}_{KM'} \circ \mathcal{E}$, with $\mathcal{E}_{\mathrm{KR}}(\rho^{\mathrm{ABE}}) = \rho^{M\tilde{K}T\Omega\mathrm{E}}$. Furthermore we introduce the notation $\mathcal{E}_{\mathrm{UE}}^{\mathtt{accept}}$ for $\mathcal{E}_{\mathrm{UE}}$ followed by selecting the $\Omega = 1$ part of the state, and similarly $\mathcal{E}_{\mathrm{UE}}^{\mathtt{reject}}$.[7]

The 'ideal' version of $\mathcal{E}$ is denoted as $\mathcal{F}$, with notations $\mathcal{F}_{\mathrm{UE}}$, $\mathcal{F}_{\mathrm{UE}}^{\mathtt{accept}}$ and $\mathcal{F}_{\mathrm{KR}}$ defined as for $\mathcal{E}$. The $\mathcal{F}$ is 0-ENC, 0-KR and 0-UE. The $\mathcal{F}$ satisfies $\mathcal{F}_{\mathrm{KR}}(\rho^{\mathrm{ABE}}) = \sum_{m\in\mathcal{M}} \Pr[M = m] \sum_{\tilde{k}\in\mathcal{K}} \frac{1}{|\mathcal{K}|} |m\tilde{k}\rangle\langle m\tilde{k}| \otimes \mathrm{tr}_{M\tilde{K}} \mathcal{E}_{\mathrm{KR}}(\rho^{\mathrm{ABE}})$, $\mathcal{F}_{\mathrm{UE}}^{\mathtt{reject}} = \mathcal{E}_{\mathrm{UE}}^{\mathtt{reject}}$, and $\mathcal{F}_{\mathrm{UE}}^{\mathtt{accept}}(\rho^{\mathrm{ABE}}) = \sum_{m\in\mathcal{M}} \Pr[M = m] |m\rangle\langle m| \otimes \mathrm{tr}_M \mathcal{E}_{\mathrm{UE}}^{\mathtt{accept}}(\rho^{\mathrm{ABE}})$.[8]

[7] $\mathcal{E}_{\mathrm{UE}}^{\mathrm{accept}}$ and $\mathcal{E}_{\mathrm{UE}}^{\mathrm{reject}}$ are not trace-preserving.

[8] 0-ENC and 0-KR follow from Lemma 2.10. Given 0-ENC the behavior of $\mathcal{E}_{\mathrm{UE}}$ in case of reject is already ideal.

We consider again the sequence of N chunks. The KR property must hold in the first $N-1$ rounds. The ENC and UE property must hold in all rounds. The following condition implies ε-KR and ε-UE properties hold

$$\forall_{j\in\{1,\ldots,N\}} \quad \left\| \mathcal{E}_{\mathrm{UE}}^{(j)} \circ \mathcal{E}_{\mathrm{KR}}^{(j-1)} \circ \cdots \circ \mathcal{E}_{\mathrm{KR}}^{(1)} \;-\; \mathcal{F}_{\mathrm{UE}}^{(j)} \circ \mathcal{F}_{\mathrm{KR}}^{(j-1)} \circ \cdots \circ \mathcal{F}_{\mathrm{KR}}^{(1)} \right\|_{\diamond} \leq \varepsilon, \quad (5.3)$$

where the superscript is the round index.

Using Lemma 2.12 it is easily seen that the following condition implies (5.3),

$$(N-1)\|\mathcal{E}_{\mathrm{KR}} - \mathcal{F}_{\mathrm{KR}}\|_{\diamond} + \|\mathcal{E}_{\mathrm{UE}} - \mathcal{F}_{\mathrm{UE}}\|_{\diamond} \leq \varepsilon. \quad (5.4)$$

It is therefore sufficient to upper bound the single-round quantities $\|\mathcal{E}_{\mathrm{KR}} - \mathcal{F}_{\mathrm{KR}}\|_{\diamond}$ and $\|\mathcal{E}_{\mathrm{UE}} - \mathcal{F}_{\mathrm{UE}}\|_{\diamond}$,

$$\|\mathcal{E}_{\mathrm{KR}} - \mathcal{F}_{\mathrm{KR}}\|_{\diamond} = \frac{1}{2} \sup_{\rho^{\mathrm{ABE}}} \left\| \mathcal{E}_{\mathrm{KR}}(\rho^{\mathrm{ABE}}) - \mathop{\mathbb{E}}_{m\tilde{k}} |m\tilde{k}\rangle\langle m\tilde{k}| \otimes \mathrm{tr}_{M\tilde{K}}\, \mathcal{E}_{\mathrm{KR}}(\rho^{\mathrm{ABE}}) \right\|_1 \quad (5.5)$$

$$\|\mathcal{E}_{\mathrm{UE}} - \mathcal{F}_{\mathrm{UE}}\|_{\diamond} = \frac{1}{2} \sup_{\rho^{\mathrm{ABE}}} \left\| \mathcal{E}_{\mathrm{UE}}^{\mathtt{accept}}(\rho^{\mathrm{ABE}}) - \mathop{\mathbb{E}}_{m} |m\rangle\langle m| \otimes \mathrm{tr}_{M}\, \mathcal{E}_{\mathrm{UE}}^{\mathtt{accept}}(\rho^{\mathrm{ABE}}) \right\|_1. \quad (5.6)$$

5.6.2 Correctness

It is straightforward to see that KRUE satisfies Correctness. Bob only accepts (sets $\omega = 1$) when the reconstructed tag successfully authenticates the reconstructed plaintext $\hat{\tau} == \Gamma(k_{\mathrm{MAC}}, \hat{\mu})$. The property of the information-theoretically secure MAC and Eve's ignorance of k_{MAC} then guarantees $\Pr[m \neq \hat{m} | \omega = 1] \leq 2^{-\lambda}$. The future keys are either fresh or re-used in unaltered form.

5.7 EPR version of KRUE (step 1 and 2)

The security proof (Section 5.8) will be based on the EPR variant of the scheme. Here we first present the EPR version of KRUE and its description in terms of CPTP maps.

5.7.1 Protocol steps in the EPR version

In the EPR version of the protocol n noisy singlet states are produced by an untrusted source, e.g. Eve. One half of each EPR pair is sent to Alice, the other half to Bob. Before Alice and Bob perform their measurements, they perform the same public random permutation π on their qubits. On their ith qubit, they apply a random Pauli operator σ_{α_i}. The protocol is invariant to the random permutation since a uniform string is encoded in a uniform basis. A permutation re-arranges the noise in the measured strings over the bit positions $\{1,\ldots,n\}$, which could potentially break the symmetry; however, the error correction step is insensitive to such a change.

Alice measures her halves of the EPR pairs in the basis $b \in \mathcal{B}^n$, resulting in a string $s \in \{0,1\}^n$. Bob too measures his qubits in basis b, which yields $t \in \{0,1\}^n$.[9] After they compute x and x' respectively, Alice and Bob delete s, t.

[9] If the EPR pairs are noiseless then $t = \bar{s}$; the inversion occurs because we work with singlet states.

Alice computes x as specified in Section 5.5.2, then computes $a = x \oplus s$ and sends a to Bob over an authenticated classical channel. Bob receives a, computes $x' = \bar{t} \oplus a$ and performs the decryption steps specified in Section 5.5.2. KRUE.Post is performed as before. The protocol steps are shown in Figure 5.2. We ignore the fact that the two authentication tags (τ and φ_ω) can each be forged by Eve with probability $2^{-\lambda}$; the price for this omission is paid elsewhere, namely a term $2 \cdot 2^{-\lambda}$ in the overall error of the scheme.

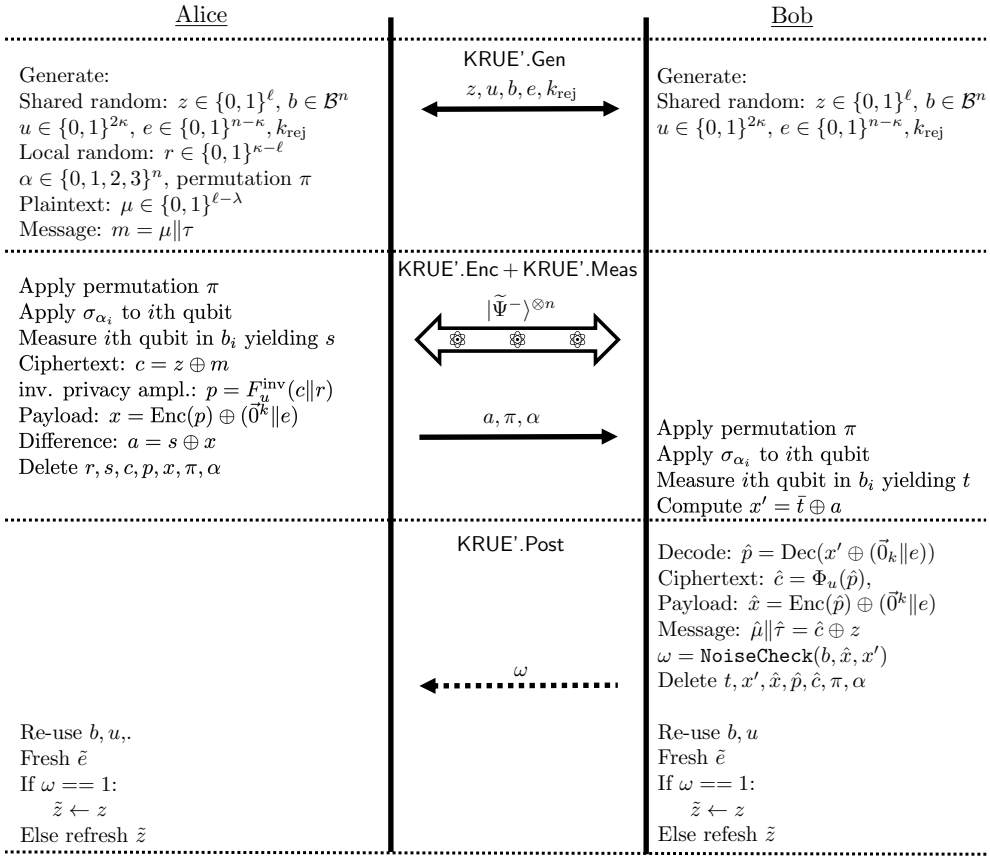

Figure 5.2: *EPR version of* KRUE. *The dashed line represents a confidential channel.*

5.7.2 CPTP maps for the EPR version of KRUE (step 3)

We specify the CPTP maps which represent the actions of Alice and Bob executed on the noisy EPR pairs in the modified protocol KRUE'. The $\mathcal{E}_{\text{UE}}$ is defined as the four consecutive maps

$$\mathcal{E}_{\text{UE}} = \text{KRUE}'.\text{Post} \circ \text{KRUE}'.\text{Meas} \circ \text{KRUE}'.\text{Enc} \circ \text{KRUE}'.\text{Gen}. \tag{5.7}$$

The generation step initializes the variables $mbzuer$,

$$\mathsf{KRUE}'.\mathsf{Gen}(\rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{mbzuer} |mbzuer\rangle\langle mbzuer| \otimes \rho^{\mathrm{ABE}}. \tag{5.8}$$

Here b, z, u, e, r are uniform, but m is not necessarily. The measurements of Alice and Bob described by $\mathsf{KRUE}'.\mathsf{Meas} \circ \mathsf{KRUE}'.\mathsf{Enc}$ use the classical b-register and ρ^{ABE}, outputting the strings s, t and Eve's state ρ^{E}_{bst}, which is correlated to the measurement basis b and the outcomes s, t,

$$\mathsf{KRUE}'.\mathsf{Meas} \circ \mathsf{KRUE}'.\mathsf{Enc}\left(|b\rangle\langle b| \otimes \rho^{\mathrm{ABE}}\right) = \mathop{\mathbb{E}}_{st|b} |bst\rangle\langle bst| \otimes \rho^{\mathrm{E}}_{bst}. \tag{5.9}$$

Here the distribution of s and t is governed by the precise details of the ρ^{ABE} created by Eve. Anticipating the post-selection and random-Paulis technique applied in steps 5 and 6 we write the effect of Eve's actions as i.i.d. noise with noise parameter γ. The marginals of s and t are uniform, while for all $j \in \{1, \ldots, n\}$ it holds that $\Pr[s_j = t_j] = \gamma$.

The flag ω is computed as a function of b, s and t, which we will denote as $\omega = \theta_{bst} = \mathtt{NoiseCheck}(\mathsf{b}, \mathsf{s}, \bar{\mathsf{t}})$. We will use the notation P_{acc} for the probability that the noise check has a positive outcome $\theta_{bst} = 1$. Recall that for the noise check of Definition 2.18 it holds that

$$P_{\mathrm{acc}} \stackrel{\mathrm{def}}{=} \mathop{\mathbb{E}}_{bst} \theta_{bst} = \mathop{\mathbb{E}}_{n_b : \sum_b n_b = n} \prod_{b \in \mathcal{B}} \sum_{c=0}^{\lfloor n_b \beta \rfloor} \binom{n_b}{c} \gamma_b^c (1-\gamma_b)^{n-c}. \tag{5.10}$$

where n_b denotes the number of times the basis b is used for encoding. Let the map $\mathcal{P}$ describe the protocol before all variables are traced out.

$$\begin{aligned} \mathcal{P}(\rho^{\mathrm{ABE}}) \;=\; & \mathop{\mathbb{E}}_{mbzuest} |mbzuest\rangle\langle mbzuest| \otimes \rho^{\mathrm{E}}_{bst} \otimes \sum_{capxx'\omega\tilde{z}} \mathop{\mathbb{E}}_{r} |capxx'\omega\tilde{z}r\rangle\langle capxx'\omega\tilde{z}r| \\ & \delta_{a,s\oplus x}\delta_{c,m\oplus z}\delta_{p,F_u^{\mathrm{inv}}(c\|r)}\delta_{x,p\|[\mathrm{Red}(p)\oplus e]}\delta_{x',\bar{t}\oplus a}\delta_{\omega,\theta_{bst}}\left[\omega\delta_{\tilde{z}z} + \frac{\overline{\omega}}{2^\ell}\right]. \end{aligned} \tag{5.11}$$

Here '$\mathrm{Red}(p)$' stands for the redundancy bits appended to p in the systematic-form ECC encoding $\mathrm{Enc}(p)$. Finally we trace away all variables that are not part of the transcript or the output: s, t, c, p, x, x', r. These variables exist only temporarily and can be quickly discarded by Alice and Bob; they are never stored in nonvolatile memory. The a and ω are observed by Eve as part of the communication. (The ω initially in encrypted form, but the keys φ_0, φ_1 are assumed to leak in the future.) The b, z, u, e are assumed to leak in the future and thus they have to be kept as part of the state. We obtain[10]

$$\begin{aligned} \mathcal{E}_{\mathrm{UE}}(\rho^{\mathrm{ABE}}) \;=\; & \mathop{\mathbb{E}}_{mbzue} \sum_{a\tilde{z}\omega} |mbzuea\tilde{z}\omega\rangle\langle mbzuea\tilde{z}\omega| \otimes \mathop{\mathbb{E}}_{st|b} \rho^{\mathrm{E}}_{bst} \sum_p 2^\ell \delta_{\Phi_u(p),m\oplus z} \\ & 2^{-k}\delta_{s\oplus a,p\|[\mathrm{Red}(p)\oplus e]}\delta_{\omega,\theta_{bst}}\Big[\omega\delta_{\tilde{z}z} + \overline{\omega}2^{-\ell}\Big]. \end{aligned} \tag{5.12}$$

[10] Note that tracing out u or $z\tilde{z}$ in (5.12) yields a state in which the M-subspace is completely decoupled from the rest of the Hilbert space. This shows that the scheme, when merely viewed as an encryption scheme, protects m unconditionally as soon as the adversary does not know u or $z\tilde{z}$.

As discussed in Section 5.6, only the accept part (the $\omega = 1$ part) of the idealized $\mathcal{F}_{\mathrm{UE}}$ is relevant. This is obtained as $\mathcal{F}_{\mathrm{UE}}^{\mathtt{accept}}(\rho^{\mathrm{ABE}}) = \mathbb{E}_m |m\rangle\langle m| \otimes \mathrm{tr}_M \mathcal{E}_{\mathrm{UE}}^{\mathrm{accept}}(\rho^{\mathrm{ABE}})$. We get

$$\begin{aligned}\mathcal{F}_{\mathrm{UE}}^{\mathtt{accept}}(\rho^{\mathrm{ABE}}) \;&=\; \mathop{\mathbb{E}}_{mbzue} \sum_{a\tilde{z}} |mbzuea\tilde{z}\rangle\langle mbzuea\tilde{z}|\delta_{\tilde{z}z} \\ &\quad \otimes \mathop{\mathbb{E}}_{st|b} \rho^{\mathrm{E}}_{bst}\theta_{bst} \sum_p 2^{\ell-k}\delta_{s\oplus a,p\|[\mathrm{Red}(p)\oplus e]} \mathop{\mathbb{E}}_{m'} \delta_{\Phi_u(p),m'\oplus z}. \quad (5.13)\end{aligned}$$

Note that this expression is sub-normalized; its trace equals $\mathbb{E}_{bst}\,\theta_{bst}$. We write

$$\begin{aligned}(\mathcal{E}_{\mathrm{UE}}^{\mathrm{accept}} - \mathcal{F}_{\mathrm{UE}}^{\mathrm{accept}})(\rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{mbzue} \sum_{a\tilde{z}} |mbzuea\tilde{z}\rangle\langle mbzuea\tilde{z}|\delta_{\tilde{z}z} \otimes \mathop{\mathbb{E}}_{st|b} \rho^{\mathrm{E}}_{bst}\theta_{bst} \\ \sum_p 2^{\ell-k}\delta_{s\oplus a,p\|[\mathrm{Red}(p)\oplus e]}\big[\delta_{\Phi_u(p),m\oplus z} - \mathop{\mathbb{E}}_{m'} \delta_{\Phi_u(p),m'\oplus z}\big]. \quad (5.14)\end{aligned}$$

For the description of $\mathcal{E}_{\mathrm{KR}}$ we have to take (5.12) and trace out z, e, ω.

$$\mathcal{E}_{\mathrm{KR}}(\rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{mbu} 2^{-n} \sum_{a\tilde{z}} |mbua\tilde{z}\rangle\langle\cdots| \otimes \mathop{\mathbb{E}}_{st|b} \rho^{\mathrm{E}}_{bst}\Big[\theta_{bst}\delta_{\Phi_u((s\oplus a)[:\kappa]),m\oplus\tilde{z}} + 2^{-\ell}\overline{\theta_{bst}}\Big] \quad (5.15)$$

The ideal functionality $\mathcal{F}_{\mathrm{KR}}$ has $m, b, u, \tilde{z}$ decoupled from the rest of the system. We have $\mathcal{F}_{\mathrm{KR}}(\rho^{\mathrm{ABE}}) = \mathbb{E}_{mbu}\, 2^{-\ell} \sum_{\tilde{z}} |mbu\tilde{z}\rangle\langle mbu\tilde{z}| \otimes \mathrm{tr}_{MBU\tilde{Z}} \mathcal{E}_{\mathrm{KR}}(\rho^{\mathrm{ABE}})$, which yields

$$\mathcal{F}_{\mathrm{KR}}(\rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{mbu} 2^{-n-\ell} \sum_{a\tilde{z}} |mbua\tilde{z}\rangle\langle mbua\tilde{z}| \otimes \mathop{\mathbb{E}}_{stb'} \rho^{\mathrm{E}}_{b'st}. \quad (5.16)$$

Note that $\mathbb{E}_{stb'}\,\rho^{\mathrm{E}}_{b'st} = \rho^{\mathrm{E}}$. From Lemma 2.20 we know that $\mathbb{E}_{st|b}\,\rho^{\mathrm{E}}_{bst} = \rho^{\mathrm{E}}$. This allows us to write

$$(\mathcal{E}_{\mathrm{KR}} - \mathcal{F}_{\mathrm{KR}})(\rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{mbu} 2^{-n-\ell} \sum_{a\tilde{z}} |mbua\tilde{z}\rangle\langle\cdots| \otimes \mathop{\mathbb{E}}_{st|b} \rho^{\mathrm{E}}_{bst}\theta_{bst}[2^{\ell}\delta_{\Phi_u((s\oplus a)[:\kappa]),m\oplus\tilde{z}} - 1]. \quad (5.17)$$

5.8 Security proof

In our analysis we will use λ as the security parameter, i.e. we will strive to make all diamond distances smaller than $2^{-\lambda}$. In the asymptotics this will not always be explicitly visible, as λ drops out of the expressions for the asymptotic rate.

5.8.1 Intermezzo: QKD with protected syndrome

In Chapter 2 we considered a QKD protocol that sends the syndrome over a public authenticated channel. If instead we protect the syndrome with a one-time pad, we end up with the same rate. The output can be obtained by tracing out the syndrome e from (2.36) so that the output of the modified map $\mathcal{E}'_{\mathrm{QKD}}$ is

$$\mathcal{E}'_{\mathrm{QKD}}(\rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{mbu} 2^{-n} \sum_{ac\omega} |mbuac\omega\rangle\langle mbuac\omega| \otimes \mathop{\mathbb{E}}_{st|b} \rho^{\mathrm{E}}_{bst}\delta_{\omega,\theta_{bst}}[\omega\delta_{c,m\oplus\Phi_u(a\oplus s)} + \overline{\omega}\delta_{c\perp}]. \quad (5.18)$$

The idealized output state is obtained as $\mathbb{E}_m |m\rangle\langle m| \otimes \mathrm{tr}_M \mathcal{E}_{\mathrm{QKD}}(\rho^{\mathrm{ABE}})$, which yields

$$\mathcal{F}'_{\mathrm{QKD}}(\rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{mbu} 2^{-n} \sum_{ac\omega} |mbuac\omega\rangle\langle\cdots| \otimes \mathop{\mathbb{E}}_{st|b} \rho^{\mathrm{E}}_{bst} \delta_{\omega,\theta_{bst}} [\omega \mathop{\mathbb{E}}_{m'} \delta_{c,m'\oplus\Phi_u(a\oplus s)} + \overline{\omega}\delta_{c\perp}]. \tag{5.19}$$

The diamond difference is given by

$$\|\mathcal{E}'_{\mathrm{QKD}} - \mathcal{F}'_{\mathrm{QKD}}\|_\diamond = \tfrac{1}{2} \mathop{\mathbb{E}}_{mbu} \frac{1}{2^{n+\ell}} \sum_{ac} \left\| \mathop{\mathbb{E}}_{st|b} \rho^{\mathrm{E}}_{bst} \theta_{bst} 2^{\ell} [\delta_{c,m\oplus\Phi_u(a\oplus s)} - \mathop{\mathbb{E}}_{m'} \delta_{c,m'\oplus\Phi_u(a\oplus s)}] \right\|_1 . \tag{5.20}$$

When considering smooth density matrices ε-close to the real states (step 4), we can apply identical steps (expect for the Jensen of e) as from (2.39) till (2.45). We find

$$\|\mathcal{E}'_{\mathrm{QKD}} - \mathcal{F}'_{\mathrm{QKD}}\|_\diamond \leq \min\Big(\mathop{\mathbb{E}}_{bst} \theta_{bst}, \frac{1}{2} \mathop{\mathbb{E}}_{b} \mathrm{tr} \sqrt{2^{\ell} \mathop{\mathbb{E}}_{ss'|b} \delta_{ss'} \bar{\rho}^{\mathrm{E}}_{bs} \bar{\rho}^{\mathrm{E}}_{bs'}} \Big), \tag{5.21}$$

which is identical to (2.45) except for a factor $2^{n-\kappa}$ which is the size of the extra key used to protect the syndrome. The remainder of the proof of Section 2.6 holds so that the well known asymptotic QKD rate is obtained: $1-2h(\beta)$ for BB84 (Equation 2.65) and $1 - h(1 - \frac{3\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})$ for 6-state QKD (Equation 2.64).

5.8.2 How many qubits are used by KRUE

We are interested in the asymptotic rate that the composed scheme KRUE+EQKR, as defined in Section 5.5, can achieve. We first show that the fraction ℓ/n in KRUE approaches the asymptotic key generation rate of QKD with one-way post-processing.[11] In Section 5.1.2 we analyze the reduction of the rate due to the use of EQKR as external mechanism.

Since our analysis focuses on the asymptotics, it is not necessary to specify security parameters in detail. It suffices to state that KRUE has to satisfy the ENC, KR, and UE properties with some arbitrary 'epsilon' error values that are small but constant, i.e. do not increase when ℓ is sent to infinity. Similarly, for the composition with EQKR we only have to show that the error of the combined scheme is still constant. That being said, our results allow for a non-asymptotic analysis as well, but we leave this for future work.

In KRUE there are two authentication tags. Each of these has forgery probability $2^{-\lambda}$. In the diamond norm formalism we can say that we are at trace distance $2 \cdot 2^{-\lambda}$ away from ideality. Thus we can pretend that the two tags cannot be forged and simply add a constant penalty $2 \cdot 2^{-\lambda}$ to the error. The penalty term does not affect the asymptotics. This procedure allows us to write the CPTP maps for the protocol in a simplified form as in Section 5.7.2, i.e. not needing various case distinctions due to accidentally successful forgeries.

Theorem 5.2. *Asymptotically, the* KRUE *protocol can satisfy the ENC, KR and UE properties as defined in Section 2.4 with any fixed security parameter while achieving the following ratio* $r = \ell/n$,

$$r^{\mathsf{KRUE}}_{4\mathrm{state}} = r^{\mathrm{QKD}}_{4\mathrm{state}} = 1 - 2h(\beta) \quad ; \quad r^{\mathsf{KRUE}}_{6\mathrm{state}} = r^{\mathrm{QKD}}_{6\mathrm{state}} = 1 - h(1 - \tfrac{3\beta}{2}, \tfrac{\beta}{2}, \tfrac{\beta}{2}, \tfrac{\beta}{2}). \tag{5.22}$$

[11] As opposed to QKD protocols with more passes that allow Alice and Bob to perform advantage distillation, which yields a higher rate.

Proof of Theorem 5.2: We denote the maximally achievable value of ℓ, at given n and security parameter, as $\ell_{\max}$. We need to determine $\ell_{\max}$ for both the UE and the KR property individually and take the smaller of the two. From (5.5) and (5.6) in Section 5.6 we know the ENC, KR and UE properties follow from the upper bounds on the diamond distances $\|\mathcal{E}_{\rm KR}-\mathcal{F}_{\rm KR}\|_\diamond$ and $\|\mathcal{E}_{\rm UE}-\mathcal{F}_{\rm UE}\|_\diamond$. We bound UE-distance starting from (5.14) (part 1) and the KR-distance starting from (5.17) (part 2).

Part 1. First we note that (5.14) is the difference of two sub-normalized states that both have trace equal to $\mathbb{E}_{bst}\,\theta_{bst}$. This immediately yields the bound $\|\mathcal{E}_{\rm UE}-\mathcal{F}_{\rm UE}\|_\diamond \leq \mathbb{E}_{bst}\,\theta_{bst}$. Furthermore, from (5.14) we get, by using the orthogonality of the eigenspaces of the classical subsystems,

$$\|\mathcal{E}_{\rm UE}-\mathcal{F}_{\rm UE}\|_\diamond = \mathop{\mathbb{E}}_{mbzuea}\left\|\mathop{\mathbb{E}}_{st|b}\rho^{\rm E}_{bst}\theta_{bst}\sum_p 2^{\ell+n-\kappa}\delta_{s\oplus a,p\|[{\rm Red}(p)\oplus e]}[\delta_{\Phi_u(p),m\oplus z}-\mathop{\mathbb{E}}_{m'}\delta_{\Phi_u(p),m'\oplus z}]\right\|_1 \quad (5.23)$$

which resembles (5.20). The main difference is the $2^{n-\kappa}\sum_p\delta_{s\oplus a,p\|[{\rm Red}(p)\oplus e]}$. In step 4 in the QKD derivation as shown in Section 2.6, upon doubling as in (2.41), applying the $\mathbb{E}_u$ then yields instead of $\delta_{ss'}$ the following expression,

$$\sum_{pp'}\delta_{pp'}\delta_{s\oplus a,p||(e\oplus{\rm Red}p)}\delta_{s'\oplus a,p'||(e\oplus{\rm Red}p')}=\delta_{ss'}\delta_{e,(s\oplus a)[\kappa+1:n]\oplus{\rm Red}((s\oplus a)[:\kappa])}. \quad (5.24)$$

The factor $(2^{n-\kappa})^2\delta_{e,\ldots}$, together with the $\mathbb{E}_e$ outside the trace norm, together have the same effect as having the plaintext syndrome in the QKD derivation: a factor $2^{n-\kappa}$ under the square root in (5.21). Asymptotically this yields $\ell^{\rm UE,4state}_{\max}=n-2nh(\beta)$ and $\ell^{\rm UE,6state}_{\max}=n-nh(1-\frac{3\beta}{2},\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})$.

Part 2. First we note that (5.17) is the difference of two sub-normalized states that both have trace equal to $\mathbb{E}_{bst}\,\theta_{bst}$. This immediately yields the bound $\|\mathcal{E}_{\rm KR}-\mathcal{F}_{\rm KR}\|_\diamond \leq \mathbb{E}_{bst}\,\theta_{bst}$. Furthermore, from (5.17) we find

$$\|\mathcal{E}_{\rm KR}-\mathcal{F}_{\rm KR}\|_\diamond=\tfrac{1}{2}\mathop{\mathbb{E}}_{mbu}\frac{1}{2^{n+\ell}}\sum_{a\tilde{z}}\left\|\mathop{\mathbb{E}}_{st|b}\rho^{\rm E}_{bst}\theta_{bst}[2^\ell\delta_{\Phi_u((s\oplus a)[:\kappa]),m\oplus\tilde{z}}-1]\right\|_1. \quad (5.25)$$

This expression very closely resembles (5.20), with $\tilde{z}$ precisely playing the role of c, and the term $\mathbb{E}_{m'}\,\delta_{c,m'\oplus\Phi_u(a\oplus s)}$ replaced by the constant '1'. Carrying the '1' through steps (2.41) and (2.42) yields the same result as the QKD derivation, except for one important difference: the $(s+a)[:\kappa]$ restriction to the first κ bits yields a modification of $\delta_{ss'}$ to the first κ bits only. In the end result the parameter n is entirely replaced by κ. Hence we obtain asymptotically $\ell^{\rm KR,4state}_{\max}=k-kh(\beta)=n(1-h(\beta))^2$ and $\ell^{\rm KR,6state}_{\max}=\kappa+\kappa h(\beta)-\kappa h(1-\frac{3\beta}{2},\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})=n[1-h(\beta)][1+h(\beta)-h(1-\frac{3\beta}{2},\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})]$.

It is easily seen that $\ell^{\rm UE}_{\max}\leq\ell^{\rm KR}_{\max}$. For brevity we use shorthand notation $h=h(\beta)$ and $H=h(1-\frac{3\beta}{2},\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})$, noting that $H>h$ and $H<2h$. For BB84 encoding we see $\ell^{\rm KR}_{\max}/\ell^{\rm UE}_{\max}=\frac{(1-h)^2}{1-2h}\geq 1$. For 6-state we see $\ell^{\rm KR}_{\max}/\ell^{\rm UE}_{\max}=\frac{(1-h)(1+h-H)}{1-H}=\frac{1-H+h(H-h)}{1-H}\geq 1$. □

Remark: In the zero-noise case ($\beta=0$) there is no mask e. Then we have, without the use of inequalities, $\|\mathcal{E}_{\rm UE}-\mathcal{F}_{\rm UE}\|_\diamond=\|\mathcal{E}_{\rm KR}-\mathcal{F}_{\rm KR}\|_\diamond=\|\mathcal{E}_{\rm QKD}-\mathcal{F}_{\rm QKD}\|_\diamond=$

$\mathbb{E}_{mubza} \| \mathbb{E}_{st}\, \theta_{bst} \rho^{\mathrm{E}}_{bst} \big[2^{\ell} \delta_{\Phi_u(s\oplus a), m\oplus z} - 1 \big] \|_1$, i.e. the KR and UE properties reduce to QKD security.

Also note that for $\beta = 0$ we could invoke Lemma 5.1 to prove UE, by viewing the constant-length keys φ_0, φ_1 as 'external' to the proof.

For $\beta > 0$ we are not allowed to invoke Lemma 5.1, since not all the key material is carried to the next round in unmodified form: upon accept the e is updated. The e plays an integral role in the bounding of the diamond norm (5.23) and cannot be moved outside that part of the proof.

5.8.3 Security and rate of the composition KRUE+EQKR

We consider the composition of KRUE with the EQKR scheme of Chapter 4.EQKR is a two-pass protocol with the following properties: (i) its asymptotic rate equals the QKD rate; (ii) Alice's pass comprises only qubits and no classical communication.

First we show that security-wise the effect of the composition is that the errors simply add up or remain unchanged. Hence, the composition does not complicate the asymptotic analysis.

Theorem 5.3. *Let* QKR *be a ε_1-KR scheme in which Alice makes one pass. Let P be a ε_2-KR, ε_3-UE scheme in which Alice makes one pass. Let Q be the composition of* QKR *and P such that Alice sends her messages in parallel, and the message of* QKR *contains all key material for P. Then Q is $(\varepsilon_1 + \varepsilon_2)$-KR, and it is ε_3-UE with respect to the message of P.*

Proof: See Appendix 5.A. □

Next, we determine the asymptotic rate of KRUE+EQKR. Due to the additional qubits spent in EQKR, the rate is lower than the $\frac{\ell}{n}$ fraction of KRUE (and therefore lower than the QKD rate).

Theorem 5.4. *The asymptotic rate of the composed scheme* KRUE+EQKR *in the case of 4-state and 6-state encoding is given by*

$$r^{\mathsf{KRUE+EQKR}}_{\text{4state}} = \frac{[1-2h(\beta)]^2}{1-h(\beta)} \quad ; \quad r^{\mathsf{KRUE+QKR}}_{\text{6state}} = \frac{[1-h(1-\frac{3\beta}{2},\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})]^2}{1-h(1-\frac{3\beta}{2},\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})+h(\beta)}. \tag{5.26}$$

Proof: Let $\mu \in \{0,1\}^L$. Sending μ via KRUE needs $n = L/r^{\mathsf{KRUE}}$ qubits. Asymptotically, the size of $\tilde{k}_{\mathrm{OTP}}$ and $\tilde{k}_{\mathrm{fb}}$ is negligible compared to $\tilde{e}$. The size of $\tilde{e}$ is $nh(\beta)$. Sending $\tilde{e}$ via EQKR takes $nh(\beta)/r^{\mathsf{EQKR}} = Lh(\beta)/(r^{\mathsf{QKR}} r^{\mathsf{KRUE}})$ qubits. The total number of qubits spent is $q = L/r^{\mathsf{KRUE}} + Lh(\beta)/(r^{\mathsf{EQKR}} r^{\mathsf{KRUE}})$. Using $r^{\mathsf{KRUE}} = r^{\mathrm{EQKD}}$ and $r^{\mathsf{EQKR}} = r^{\mathrm{QKD}}$ this can be written as $q = L(r^{\mathrm{QKD}} + h(\beta))/(r^{\mathrm{QKD}})^2$. Finally the overall rate is $\frac{L}{q} = \frac{(r^{\mathrm{QKD}})^2}{r^{\mathrm{QKD}}+h(\beta)}$, with r^{QKD} as given in (5.22). □

Interestingly, the rate $r^{\mathsf{KRUE+EQKR}}_{\text{4state}}$ that we achieve here is twice the rate of the composition {QKD followed by Gottesman's Unclonable Encryption scheme [Got03]}.[12]

[12] The rate for that combination is obtained as follows. The UE step needs $n_{\mathrm{UE}} = L/[1-2h(\beta)]$ qubits. Then n_{UE} bits of key need to be refreshed using QKD; this takes $n_{\mathrm{QKD}} = n_{\mathrm{UE}}/[1-2h(\beta)]$ qubits. The rate is $L/(n_{\mathrm{UE}} + n_{\mathrm{QKD}}) = \frac{1}{2} \cdot \frac{[1-2h(\beta)]^2}{1-h(\beta)}$.

5.8.4 Combining KRUE with QKD

We briefly comment on the option of combining KRUE with a QKD scheme instead of a QKR scheme as the external mechanism. QKD spends as many qubits as QKR; hence KRUE combined with QKD achieves the rate given in Theorem 5.4. However, the drawback of QKD is that it is not a two-pass protocol. When allowing more passes, two-way post-processing techniques can increase the rate of QKD beyond the proven rates in Chapter 2 [Ren05]. This would increase the rate of KRUE + QKD a bit as well.

5.8.5 KRUE*: sending key updates via KRUE itself

In order to get a more 'self-contained' scheme, we study the option of *not* using an external mechanism to transport the next-round keys $\tilde{\varphi}_\omega, \tilde{e}$. Instead we reserve space in the message μ for this purpose. We refer to the resulting scheme as KRUE*. The security of KRUE* is the same as for KRUE. The ratio ℓ/n, however, is seriously reduced, since the effective message size is now smaller by an amount $\lambda + n - \kappa$, which asymptotically goes to $nh(\beta)$. This causes a reduction of ℓ/n by an amount $h(\beta)$, i.e. $r^{\mathsf{KRUE}^*} = r^{\mathsf{KRUE}} - h(\beta)$. Since $\tilde{e}$ is already refreshed, no external mechanism is needed, the rate of KRUE* is $1 - 3h(\beta)$.

5.9 Comparison to other schemes

We briefly comment on the round complexity and the asymptotic rate of the protocols proposed in this chapter as compared to other schemes. The word 'round complexity' here is not to be confused with the N rounds in our protocol. For a given message chunk μ_j we count *the number of times Alice has to send something*, and refer to this number as Alice's number of *passes*.

We compare against other information-theoretically secure schemes which also do not use up[13] key material,

- **QKD+OTP**. Key establishment using Quantum Key Distribution, followed by One Time Pad classical encryption. We consider efficient QKD with negligible waste of qubits [LCA05] and the smallest possible number of communication rounds: only 2 passes by Alice.
- **QKR**. Qubit-wise prepare-and-measure Quantum Key Recycling as described in Chapter 3 and 4. Only a single pass by Alice is needed, since Alice and Bob already share key material.
- **QKD+[Got03]**. Key establishment using QKD, followed by Gottesman's Unclonable Encryption [Got03]. At least two passes by Alice are needed.
- **QKR+[Got03]**. Key establishment using QKR, followed by Gottesman's Unclonable Encryption. Only a single pass by Alice is needed when the two are performed in parallel.[14]

[13] Our schemes use up key material, but this is amortised over N rounds. We neglect this expenditure for the purpose of the comparison.

[14] We don't give a proof for this combination as [Got03] uses a different proof technique.

Protocol	Alice #passes	Asymptotic rate (4-state)	Unclonability
QKD + OTP	2	$1 - 2h(\beta)$	no
QKR [LŠ19a, LŠ21]	1	$1 - 2h(\beta)$	no
QKD + [Got03]	2	$\frac{1}{2} \cdot \frac{[1-2h(\beta)]^2}{1-h(\beta)}$	yes
QKR + [Got03]	1	$\frac{1}{2} \cdot \frac{[1-2h(\beta)]^2}{1-h(\beta)}$	yes
KRUE*	1	$1 - 3h(\beta)$	yes
KRUE+QKD	2	$\frac{[1-2h(\beta)]^2}{1-h(\beta)}$	yes
KRUE+QKR	1	$\frac{[1-2h(\beta)]^2}{1-h(\beta)}$	yes

Table 5.1: *Comparison of schemes that have no net expenditure of key material upon accept.*

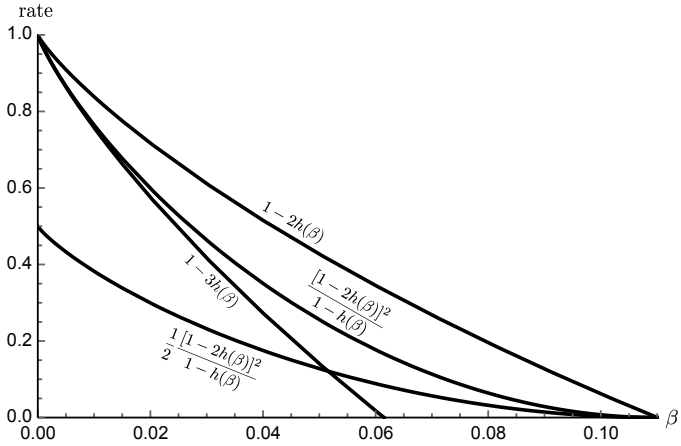

Figure 5.3: *Asymptotic communication rates (4-state) as a function of the noise parameter β.*

The scheme properties are summarised in Table 5.1, and the rates are plotted in Figure 5.3. (We only show 4-state encoding. The comparison holds qualitatively for 6-state encoding as well, but with slightly higher rates.) QKR is an improvement over QKD in terms of round complexity, while achieving the same rate. However, QKD and QKR over a noisy channel do not have the Unclonable Encryption property.

To our knowledge, the only existing scheme with an explicit proof of the UE property before our work was Gottesman's construction [Got03]. (And thus "QKD/QKR + [Got03]" was the only known way to have UE without net expenditure of key material.) Our best performing scheme is KRUE+EQKR, with one pass from Alice and double the rate of QKR + [Got03]. Our sub-optimal scheme KRUE* has a better rate than QKD/QKR + [Got03] at noise levels below $\beta \approx 0.052$.

The above comparison does not contain the key recycling schemes [DPS05, FS17], because [DPS05] is defined only for the noiseless case $\beta = 0$, while [FS17] has low rate ($\leq \frac{1}{3}$) and limited noise tolerance. Note that [DPS05] has the UE property by Lemma 5.1, and we suspect that [FS17] satisfies a version of unclonability with a somewhat modified definition that allows for a reduction of the min-entropy of some of the keys. We believe that the QKR scheme QKR of Chapter 3 can be tweaked to have the UE property by doing more privacy amplification; this would probably lead to the same rate as KRUE^*.

We briefly comment on the key sizes as a function of the message length L. The keys in KRUE are the OTP $z \in \{0,1\}^\ell$, the hash seed $u \in \{0,1\}^{2k}$, the basis choice $B \in \mathcal{B}^n$, the redundancy mask $e \in \{0,1\}^{n-\kappa}$, the authentication key $k_{\mathrm{MAC}} \in \{0,1\}^{2\lambda}$ and the random codebook $(\varphi_0, \varphi_1) \in \{0,1\}^{2\lambda}$. Counting only contributions proportional to n, the total size in bits is $\ell + k + n + n \log \mathcal{B} + \mathcal{O}(1)$. With $L \approx \ell$, $\ell \approx r^{\mathrm{QKD}} n$, $k \approx n[1-h(\beta)]$, the key size of KRUE (in the case of 4-state encoding) is approximately $L\frac{4-3h(\beta)}{1-2h(\beta)} \geq 4L$.

Furthermore, sending $nh(\beta)$ bits via the QKR scheme EQKR takes a further $4\frac{nh(\beta)}{1-2h(\beta)}$ key bits. This adds up to $L\frac{4-7h(\beta)+6[h(\beta)]^2}{[1-2h(\beta)]^2}$ as the total key size for the combination KRUE+EQKR.

The keys are expended over a block of N rounds (or $\leq N$ in case of reject). If there are no rejects, the 'amortized' key expenditure per round equals the above key size divided by N, which can be made much smaller than L.

Gottesman's scheme has somewhat shorter keys, total length $L\frac{2-h(\beta)}{1-2h(\beta)} + \mathcal{O}(1)$, but it needs to refresh $\approx L/[1-2h(\beta)]$ bits every round.

5.10 Discussion

We have proven, in the proof framework of Chapter 2, that quantum encryption over noisy channels can have Unclonability (as defined by Gottesman) as well as Key Recycling. The rate of KRUE, when disregarding the external mechanism, equals the QKD rate. The rate of KRUE+QKR is lower ($\frac{[1-2h(\beta)]^2}{1-h(\beta)}$ in the case of 4-state encoding), but (i) positive on the same β-interval as QKD and (ii) better than alternative schemes that achieve both UE and KR. It is an open question whether the low rate of UE schemes compared to QKD is unavoidable. The error-correction redundancy data has to be somehow protected; this requirement does not exist in QKD. Yet, the UE requirement makes it difficult to protect the redundancy, as long-term keys will leak eventually. Perhaps an error-correcting scheme like [DS05], which was used in [FS17], can help here.

One attempt to increase the rate of KRUE+EQKR is the following involving two modifications. i) Send the current round e with EQKR; ii) choose x such that $\Phi_u(x) = m \oplus z$. We remark in Section 5.5.3 that the *current round* error correction pad e could be sent by the QKR protocol. This would make e a short term variable so that it doesn't leak entirely. This reduces the amount of privacy amplification needed to achieve the UE property. The second modification is aimed to decrease the privacy amplification needed for the key recycling property. When Alice can choose x such that Bob's privacy amplification step works on the entire string, i.e. $\Phi_u(x) = m \oplus z$

instead of $\Phi_u(x[:\kappa]) = m \oplus z$, the rate for the KR property equals the QKD rate. Unfortunately, computing such a qubit payload x is computationally infeasible for Alice using the current way of performing privacy amplification and error correction. How to make this operation feasible is an open question.

Our scheme was designed by starting from QKR and making the privacy amplification a step in the computation of the qubit payload. Gottesman's construction [Got03] does something very similar, and hence one might try to construct a variant of KRUE that is closer to [Got03]. This would have the advantage that there is no longer a seed u that needs to be stored as part of the keys, as [Got03] employs ECC-based privacy amplification. In addition allows the entire payload to be an input to the privacy amplification which seems to be a requirement to reach the QKD rate. However, the proof technique that we use, with its reliance on hash families, does not work for ECC-based privacy amplification.

Our protocols (temporarily) hide the accept/reject feedback bit ω. This is a technicality that allows us to re-use b in un-altered form. The alternative would be to send ω in the clear and then either (i) partially refresh b as in QKR and EQKR, or (ii) find a way to cope with a reduced entropy of b as in [FS17]. Note that it is not realistic to hide a *large* accumulation of ω-feedbacks from Eve. Alice and Bob would have to act for a long time in a way that, to an external observer, does not depend on the ω's. For a *small* accumulation (e.g. size N) we expect that it *is* realistic to hide the feedbacks temporarily.

It is of course possible to tweak KRUE in various ways to make it more efficient. It may be possible to improve on the length of the hash seed, or the length of the MAC key, or the entropy of b. We did not pursue such optimizations as our focus was on the rate.

The downside associated with encoding a message directly into qubits, just as in QKR and EQKR, is the vulnerability to erasures (particle loss) on the quantum channel. Whereas QKD can just ignore erasures, in QKR they have to be compensated by the error-correcting code, which incurs a serious rate penalty.

5.11 Beyond unclonable encryption

Having seen the properties of the protocol QKR in Chapter 3, one of the remaining questions tackled in Chapter 4 was whether it is possible to improve the behavior of the protocol in the reject case. It turned out the key re-use could be made more efficient. In this chapter we have again constructed a protocol that has fine behavior in the accept case, but is not very ambitious in the reject case. The key update is as efficient as in Chapter 4, but the unclonable encryption property only improves security in the accept case. In the reject case, we have the same confidentiality guarantee the classical one-time pad provides. It might seem impossible to have any guarantees on the security of the message when the quantum states don't arrive at Bob's lab intact and the encryption keys leak. Nevertheless, the next chapter aims to improve the reject behavior of unclonable encryption.

Appendix

5.A Proof of Theorem 5.3

We consider the EPR version of Q. Eve creates a state that can be written as $\rho^{\mathrm{A}_1\mathrm{B}_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}}$, where the labels '1' and '2' refer to the EPR pairs intended for QKR and P respectively, and A,B refers to the EPR parts going to Alice and Bob. As in Section 5.6 we introduce different notation for the same CPTP map depending on the property that we are looking at (KR or UE). Thus we have CPTP maps $\mathcal{Q}_{1\mathrm{KR}}$, $\mathcal{Q}_{1\mathrm{UE}}$, $\mathcal{Q}_{2\mathrm{KR}}$, $\mathcal{Q}_{2\mathrm{UE}}$, with

$$\begin{aligned}(\mathcal{Q}_{2\mathrm{KR}}\circ\mathcal{Q}_{1\mathrm{KR}})(\rho^{\mathrm{A}_1\mathrm{B}_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}}) &= \mathcal{Q}_{2\mathrm{KR}}(\rho^{M_1\tilde{K}_1T_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}}) = \rho^{\tilde{K}_1T_1M_2\tilde{K}_2T_2\mathrm{E}} \quad (5.27)\\ (\mathcal{Q}^{\mathsf{acc}}_{2\mathrm{UE}}\circ\mathcal{Q}_{1\mathrm{UE}})(\rho^{\mathrm{A}_1\mathrm{B}_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}}) &= \mathcal{Q}^{\mathsf{acc}}_{2\mathrm{UE}}(\rho^{M_1K_1\tilde{K}_1T_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}})\\ &= \rho^{M_1K_1\tilde{K}_1T_1M_2K_2\tilde{K}_2T_2\mathrm{E}}_{[\Omega=1]}. \quad (5.28)\end{aligned}$$

With respect to the KR property, the ideal functionality is $\mathcal{Q}^{\mathrm{ideal}}_{2\mathrm{KR}}\circ\mathcal{Q}^{\mathrm{ideal}}_{1\mathrm{KR}}$. With respect to UE the ideal functionality is as follows. In case of reject there are no requirements. In case of accept the M_2 is protected by $\mathcal{Q}^{\mathsf{acc},\mathrm{ideal}}_{2\mathrm{UE}}$ even if $\mathcal{Q}_{1\mathrm{UE}}$ does not behave ideally; hence the ideal functionality is described by the mapping $\mathcal{Q}^{\mathsf{acc},\mathrm{ideal}}_{2\mathrm{UE}}\circ\mathcal{Q}_{1\mathrm{UE}}$. We have

$$\begin{aligned}(\mathcal{Q}^{\mathrm{ideal}}_{2\mathrm{KR}}\circ\mathcal{Q}^{\mathrm{ideal}}_{1\mathrm{KR}})(\rho^{\mathrm{A}_1\mathrm{B}_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}}) &= \mathcal{Q}^{\mathrm{ideal}}_{2\mathrm{KR}}(\rho^{M_1\tilde{K}_1}\otimes\rho^{T_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}})\\ &= \rho^{\tilde{K}_1M_2\tilde{K}_2}\otimes\rho^{T_1T_2\mathrm{E}} \quad (5.29)\\ (\mathcal{Q}^{\mathsf{acc},\mathrm{ideal}}_{2\mathrm{UE}}\circ\mathcal{Q}_{1\mathrm{UE}})(\rho^{\mathrm{A}_1\mathrm{B}_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}}) &= \mathcal{Q}^{\mathsf{acc},\mathrm{ideal}}_{2\mathrm{UE}}(\rho^{M_1K_1\tilde{K}_1T_1\mathrm{A}_2\mathrm{B}_2\mathrm{E}})\\ &= \rho^{M_2}\otimes\rho^{M_1K_1\tilde{K}_1T_1K_2\tilde{K}_2T_2\mathrm{E}}_{[\Omega=1]}. \quad (5.30)\end{aligned}$$

It is given that $\|\mathcal{Q}_{1\mathrm{KR}}-\mathcal{Q}^{\mathrm{ideal}}_{1\mathrm{KR}}\|_\diamond\le\varepsilon_1$, and $\|\mathcal{Q}_{2\mathrm{KR}}-\mathcal{Q}^{\mathrm{ideal}}_{2\mathrm{KR}}\|_\diamond\le\varepsilon_2$, and $\|\mathcal{Q}_{2\mathrm{UE}}-\mathcal{Q}^{\mathrm{ideal}}_{2\mathrm{UE}}\|_\diamond\le\varepsilon_3$. The KR property of Q follows trivially from

$$\left\|\mathcal{Q}_{2\mathrm{KR}}\circ\mathcal{Q}_{1\mathrm{KR}}-\mathcal{Q}^{\mathrm{ideal}}_{2\mathrm{KR}}\circ\mathcal{Q}^{\mathrm{ideal}}_{1\mathrm{KR}}\right\|_\diamond\le\left\|\mathcal{Q}_{1\mathrm{KR}}-\mathcal{Q}^{\mathrm{ideal}}_{1\mathrm{KR}}\right\|_\diamond+\left\|\mathcal{Q}_{2\mathrm{KR}}-\mathcal{Q}^{\mathrm{ideal}}_{2\mathrm{KR}}\right\|_\diamond\le\varepsilon_1+\varepsilon_2. \quad (5.31)$$

Finally, the UE property with regard to M_2 follows from

$$\left\|\mathcal{Q}_{2\mathrm{UE}}\circ\mathcal{Q}_{1\mathrm{UE}}-\mathcal{Q}^{\mathrm{ideal}}_{2\mathrm{UE}}\circ\mathcal{Q}_{1\mathrm{UE}}\right\|_\diamond\le\left\|\mathcal{Q}_{2\mathrm{UE}}-\mathcal{Q}^{\mathrm{ideal}}_{2\mathrm{UE}}\right\|_\diamond\le\varepsilon_3. \quad (5.32)$$

Chapter 6
Two-way Unclonable Encryption with a vulnerable sender

Vulnerable Alice
Alice and Bob have been communicating for a long time. During this time, their relationship has evolved. Things are now being said of which the confidentiality is absolutely paramount. But a new thread to their confidentiality is forming. The surroundings of Alice's lab are changing. Robberies are at an all time high, and break-ins occur regularly. To combat the crime, the local government is more inclined to confiscate communication devices of citizens in the hope to catch criminals. Meanwhile Bob's neighborhood is its boring, safe self.
Thanks to the unclonable encryption scheme Alice and Bob use, the messages that are successfully communicated will remain secure even if either Alice or Bob somehow leaks the keys used in the protocol. In the reject case however, it is crucial that the keys don't fall into Eve's hands.
With Alice's increasingly unsafe environment, Alice and Bob would like some sort of guarantee on the security of the messages sent by Alice, even when they don't arrive and her keys eventually leak. For this to be possible, only Bob should hold the keys to perform the decryption. Bob could initialize the communication so that qubits are sent both from Bob to Alice and from Alice to Bob. However, this would means Eve will have two opportunities to learn something about their qubits.
Unfortunately, Alice and Bob can't find a quantum protocol that achieves their desired functionality. There do exist protocols that employ two-way use of a quantum channel. Maybe a similar protocol will do the trick.

6.1 Introduction

6.1.1 Motivation

In unclonable encryption (UE) as introduced by Gottesman [Got03] and also achieved in Chapter 5, Alice directly encodes the message into the quantum states. Bob

This chapter is based on [LŠ20b].

responds with a feedback bit accepting or rejecting the communication depending on how much disturbance he detects. UE provides information-theoretic security even when all key material becomes public after an accept[1]. This relieves Alice and Bob of the burden of eternal confidential storage or perfect deletion. In the reject case, however, the burden is still there.

The combination of Quantum Key Recycling and UE was studied in Chapter 5. Our aim in this chapter is to allow for even more leakage than Gottesman's UE. In particular, we want a scheme that allows one party to leak all its keys even in the reject case. Here it is important to remark on a fundamental impossibility for a prepare-and-measure scheme. The leaking party cannot be the *receiver* of the message (Bob). Bob's keys are by definition sufficient for decrypting the cipherstate; if the reject was caused by Eve intercepting the complete cipherstate, and she gets Bob's keys, then she can decrypt. Hence, the most we can aim for is a scheme that allows leakage at Alice's side.[2] Such a thing is possible only if Alice's keys are not the same as Bob's.

We achieve the asymmetry between Alice and Bob by using a quantum channel in two directions, in a way similar to Quantum Secure Direct Communication (QSDC) and two-way QKD schemes [LM05, BF02, BLMR13]. Bob creates qubit states that are not fully known to Alice and 'bounces' them off Alice, who modifies them in a message-dependent way. Alice does not possess the secrets needed to read out the qubit states.

By relieving Alice of the burden of protecting or wiping her keys after a protocol run, we reduce the number of ways in which the security of an UE scheme can be compromised by an attacker. A full break of the sender's device may now be allowed regardless of the accept/reject outcome. We will call this the *Vulnerable-Sender* (VS) property, and refer to our scheme as a VSUE scheme. VSUE is useful especially in scenarios where the sender is a resource-constrained device, or located in a hostile environment.

An additional motivation for allowing more leakage than UE is that Alice and Bob's shared keys may have been derived via some mechanism that does not have the UE property. Then the keys that are shared between them are more vulnerable than keys that exist only at Alice's or Bob's side. In scenarios where Alice holds shared keys only, the situation is equivalent to the Vulnerable Sender setting sketched above.

6.1.2 Two-way channels

The back-and-forth use of a quantum channel has been studied mainly because it enables *passive* correction of polarization drift in fibers.[3] Several schemes have been proposed, most notably the ping-pong protocol [BF02] and LM05 [LM05]. Ping-pong uses entanglement and a two-qubit measurement at Bob's side. LM05 achieves the same communication but with single-qubit operations. In LM05, Bob sends qubits to

[1] An alternative definition of unclonable encryption exists [BL20], with two collaborating parties who attempt to both recover the plaintext. We will not use this definition.

[2] Of course it is then allowed for Bob to leak keys that Alice too possesses.

[3] Another motivation is a reduction of the number of qubits that have to be discarded because of basis mismatch between Alice and Bob in typical QKD. However, the gain is minor given that there are highly efficient biased-basis QKD schemes [LCA05] that need to discard only $\mathcal{O}(\log n)$ qubits.

Alice in BB84 states (x-basis or z-basis on the Bloch sphere). Alice may choose to flip the state independent of the encoding basis by applying the Pauli operation σ_y. Bob measures in the correct basis to see if a flip occurred. This creates the communication channel from Alice to Bob. The same channel will be used in our two-way protocol.

Variants of ping-pong and LM05 have been used to construct QKD protocols. A QKD version of LM05 was proven secure against general attacks in [LFMC11]. A proof technique based on an entropic uncertainty relation improved the communication rate [BLMR13].

6.1.3 Vulnerable-sender unclonable encryption

We propose and study a two-way protocol that achieves unclonable encryption with improved reject behavior. The sender's key material is allowed to leak independent of the accept/reject outcome.

- We introduce a security notion for quantum protocols that we call Vulnerable-Sender Unclonable Encryption (VSUE). Ordinary UE guarantees that all keys may be leaked after an accept without jeopardizing the message. VSUE in addition guarantees that all Alice's keys are allowed to leak even upon reject. We formulate VSUE in terms of trace distance as we did for the definitions in Section 2.4.

- We introduce a protocol for the Vulnerable Sender setting. It makes two-way use of the quantum channel, to make sure that Alice does not have to know all of Bob's keys. We prove that our protocol satisfies VSUE and furthermore allows for partial key re-use.

- We prove the security of the protocol, including the VSUE property using the recipe laid out in Chapter 2. Due to the bi-directional use of the quantum channel, the EPR version of the protocol involves two Bell states rather than one. The permutation invariance holds for permutation of pairs of qubits, the two EPR pairs together, rather than permutation of single qubits. This allows us the use of post-selection (step 5) to describe Eve's optimal attack as an attack on each pair of Bell states. Random Pauli operator equivalence of each of the qubits is exploited for each EPR pair individually. In step 6, this results in a four-qubit mixed state shared by Alice and Bob with only two degrees of freedom in the accept case, namely the bit error probabilities in the individual EPR pairs. Eve holds the purification of this state.

- Asymptotically our scheme achieves rate $(1-2J)(1-J)/(1-J+h(2\beta-2\beta^2))$, where β is the tolerable bit error rate on both quantum channels, h is the binary entropy function and J stands for $-(1-\frac{3}{2}\beta)\log(1-\frac{3}{2}\beta) - 3\cdot\frac{\beta}{2}\log\frac{\beta}{2}$.

- We present a side result of our work. From our protocol we construct a two-way QKD variant. We show that it has a slightly higher key rate than [BLMR13] in the case of identical channels with independent channel noise.

6.2 Security notions

We are concerned with protocols in which a classically authenticated classical message m is communicated over a quantum channel. Due to the asymmetry between Alice and Bob our attacker model is different from the attacker model of Chapter 2 and Chapter 5. We will consider the security notions of Chapter 2 in the vulnerable-sender attacker model and in the context of two-way quantum protocols. We define the vulnerable-sender unclonable encryption (VSUE) property.

6.2.1 Vulnerable-sender attacker model

Like in Chapter 5, we distinguish between two kinds of secret data. (i) Secrets which, upon being generated or received, are used 'on the fly' and are immediately discarded. They are needed for a short time, and in volatile memory only; thus they are easy to delete entirely. We will refer to these secrets as *volatile*. (ii) Secrets which are kept, at some point in time, in nonvolatile memory. We take a very conservative approach and assume that the act of waiting for a communication to arrive causes such a long delay that data gets stored in nonvolatile memory. We will refer to these secrets as *nonvolatile keys* or simply *keys*.

We assume that volatile secrets will never leak to the adversary. Nonvolatile keys are harder to protect, however, and we adopt a particular model that describes whose keys can leak and when. The attacker model used for unclonable encryption with a vulnerable sender differs from Section 5.4.1 in two ways.

1. Upon reject only Bob is able to permanently destroy nonvolatile secrets, Alice is not.

2. The number of rounds Alice and Bob communicate is not fixed to N. Instead key recycling is safe as long as Alice and Bob are confident no nonvolatile keys leaked.

During a certain time window, which depends on the context, Alice and Bob are confident that their keys have not yet leaked, and are re-using keys upon accept. The assumption is that there is indeed no leakage during this time window. Apart from Bob's keys in the reject case, all nonvolatile keys are assumed to leak after the time window.

The rest of the attacker model consists of the standard assumptions of Chapter 2: No information, other than specified above, leaks from the labs of Alice and Bob; there are no side-channels; Eve has unlimited quantum storage and computing resources; all noise on the quantum channel is considered to be caused by Eve.

We do not consider automatic polarization drift correction by double use of the channel. The noise in the two uses of the quantum channel is assumed to be entirely independent.

We will not explicitly write out the message authentication steps. Instead we give Alice and Bob access to an authenticated classical channel. It is understood that every use of this classical channels adds an error term $2^{-\lambda}$ to the final diamond distance (with λ the security parameter of the MAC), and that Alice and Bob need shared MAC keys.

6.2.2 Security definitions for two-way schemes

Recall the definition of encryption of Chapter 2. For a quantum encryption scheme QE, the output state of the scheme $\rho^{MM'KCT\mathrm{E}} = (\mathsf{QE.Post} \circ \mathsf{QE.Meas} \circ \mathcal{A} \circ \mathsf{QE.Enc})$ $(\sum_{mkr} \frac{\Pr[M=m]}{|\mathcal{K}||\mathcal{R}|} |mkr0e\rangle\langle mkr0e|)$ is defined for all adversarial actions $\mathcal{A}$. In a two-way scheme, the encoding ($\mathsf{QE.Enc}$) is done by Alice and Bob together. Bob initially prepares a state, sends it to Alice who does something two it and sends it back to Bob. Compared to one-way protocols, Eve has an additional attacking opportunity when the quantum state is sent from Bob to Alice. We therefore have two adversarial actions $\mathcal{A}$, $\mathcal{A}'$. We view the encoding map as a shared operation by Alice, Bob and Eve that depends on the Eve's action $\mathcal{A}'$. We denote the encoding in a two-way quantum encryption scheme as $\mathsf{QE.Enc}_{\mathcal{A}'}$. We adapt the definition of encryption (Definition 2.4) to include the adversarial actions $\mathcal{A}'$.

Definition 6.1. *Let* QE *be a quantum encryption scheme according to Definition 2.3 with output state*
$\rho^{MM'KCT\mathrm{E}} = (\mathsf{QE.Post} \circ \mathsf{QE.Decr} \circ \mathcal{A} \circ \mathsf{QE.Enc}_{\mathcal{A}'})(\sum_{mkr} \frac{\Pr[M=m]}{|\mathcal{K}||\mathcal{R}|} |mkr0e\rangle\langle mkr0e|)$.
QE *is called* ε**-encrypting (**ε**-ENC)** *if the output satisfies*

$$\|\rho^{MCT\mathrm{E}} - \rho^{M} \otimes \rho^{CT\mathrm{E}}\|_1 \leq \varepsilon \tag{6.1}$$

for all adversarial actions $\mathcal{A}, \mathcal{A}'$ *and all distributions of* M*.*

(The ε is referred to as the *error*). Let Ω denote the success of the protocol such that $\Omega = 1$ when Bob outputs accept and $\Omega = 0$ otherwise. The output state of QE can be written as $\rho^{MM'KCT\mathrm{E}} = \rho^{MM'KCT\mathrm{E}}_{\mathrm{accept}} + \rho^{MM'KCT\mathrm{E}}_{\mathrm{reject}}$, where the two states in the right hand side are sub-normalized, with $\operatorname{tr} \rho^{MM'KCT\mathrm{E}}_{\mathrm{accept}} = \Pr[\Omega = 1]$ and $\operatorname{tr} \rho^{MM'KCT\mathrm{E}}_{\mathrm{reject}} = \Pr[\Omega = 0]$. We adapt the definition of unclonable encryption (Definition 2.11) to include all adversarial actions $\mathcal{A}'$.

Definition 6.2. *Let* QE *be a quantum key recycling scheme according to Definition 2.3 with output state*
$\rho^{MM'KCT\mathrm{E}} = (\mathsf{QE.Post} \circ \mathsf{QE.Meas} \circ \mathcal{A} \circ \mathsf{QE.Enc}_{\mathcal{A}'})(\sum_{mkr} \frac{\Pr[M=m]}{|\mathcal{K}||\mathcal{R}|} |mkr0e\rangle\langle mkr0e|)$.
QE *is called* ε*-unclonable (*ε*-UE) if it satisfies*

$$\|\rho^{MKCT\mathrm{E}}_{\mathtt{accept}} - \rho^{M} \otimes \rho^{KCT\mathrm{E}}_{\mathtt{accept}}\|_1 \leq \varepsilon \tag{6.2}$$

for all adversarial actions $\mathcal{A}$,$\mathcal{A}'$ *and all distributions of* M*.*

In order to write down the definition of VSUE we need to distinguish between *shared* keys 'S', which Alice and Bob both have, and keys that are uniquely in Bob's possession, 'P'. (Here we assume that Alice possesses shared keys only.)

Definition 6.3. *Let* QE *be a quantum encryption scheme according to Definition 2.3 with output state*
$\rho^{MM'KCT\mathrm{E}} = (\mathsf{QE.Post} \circ \mathsf{QE.Meas} \circ \mathcal{A} \circ \mathsf{QE.Enc}_{\mathcal{A}'})(\sum_{mkr} \frac{\Pr[M=m]}{|\mathcal{K}||\mathcal{R}|} |mkr0e\rangle\langle mkr0e|)$,
where $K = (S, P)$*, with* S *shared keys.* QE *is called* **Vulnerable-Sender Unclonable** *with error* ε **(**ε**-VSUE)** *if it is* ε*-UE and also satisfies*

$$\left\| \rho^{MSCT\mathrm{E}}_{\mathtt{reject}} - \rho^{M} \otimes \rho^{SCT\mathrm{E}}_{\mathtt{reject}} \right\|_1 \leq \varepsilon \tag{6.3}$$

for all adversarial actions $\mathcal{A}$, $\mathcal{A}'$ and all distributions of M.

Definition 6.3 states that, on top of the UE property, M is secure also if the shared keys leak after a reject. Since we will restrict ourselves to schemes where Alice possesses shared keys only, this leak represents a full compromise of Alice's keys. Note that ε-VSUE implies ε-ENC and ε-UE.

Finally, we are also interested in (partial) key re-use. The P, the one-sided keys, can be randomly re-generated 'for free' after each protocol run, because no communication is needed for such a refresh. Hence the question of key re-use is relevant only for the shared keys S.

Definition 6.4. *Let* QE *be a quantum encryption scheme according to Definition 2.3 with output state* $\rho^{MM'KCT\mathrm{E}} = (\mathsf{QE.Post} \circ \mathsf{QE.Meas} \circ \mathcal{A} \circ \mathsf{QE.Enc}_{\mathcal{A}'})(\sum_{mkr} \frac{\Pr[M=m]}{|\mathcal{K}||\mathcal{R}|} |mkr0e\rangle\langle mkr0e|)$*, where* $K = (S_{\mathrm{re}}, S_{\mathrm{once}}, P)$*, with* $S_{\mathrm{re}}, S_{\mathrm{once}}$ *shared keys.* QE *is called* ε**-Key-Reusing (**ε**-KR)** *if*

$$\left\| \rho^{MS_{\mathrm{re}}S_{\mathrm{once}}PCT\mathrm{E}} - \rho^{S_{\mathrm{re}}} \otimes \rho^{MS_{\mathrm{once}}PCT\mathrm{E}} \right\|_1 \leq \varepsilon \tag{6.4}$$

for all adversarial actions $\mathcal{A}$ and all distributions of M.

Remark 1. In Definition 6.4 Eve potentially gets access to part of the key material. Thus Definition 6.4 imposes requirements that are much more demanding than other definitions of key recycling or key re-use.
Remark 2. In order for a scheme to satisfy VSUE, Eve must not have access to P. The reject-case output state of a VSUE scheme is of the form $\rho^{MS_{\mathrm{re}}S_{\mathrm{once}}P\Omega T\mathrm{E}}_{\mathrm{reject}} = \rho^{P} \otimes \rho^{MS_{\mathrm{re}}S_{\mathrm{once}}\Omega T\mathrm{E}}_{\mathrm{reject}}$.

Correctness

For protocols like ours (Section 6.3), where the message is authenticated with a classical MAC and the re-used keys are unaltered, correctness of the message is guaranteed except with probability $2^{-\lambda}$, the probability of forging the MAC. The correctness of the next round keys that are not modified or obtained using a secure protocol is obvious.

6.3 The protocol

6.3.1 Protocol intuition

As mentioned in Section 6.1.1, we create the knowledge asymmetry between Alice and Bob by making use of a two-way protocol. Bob 'bounces' random qubit states off Alice, which Alice is able to flip without knowing the states. A message from Alice to Bob is encoded in these flips. Only Bob knows how to interpret the states coming back from Alice.

Channel monitoring has to occur on both the Bob-to-Alice channel ('Channel 1') and the Alice-to-Bob channel ('Channel 2'). This monitoring is done by sending, interspersed in between the ordinary states, *test qubits* whose states are known to the

receiver; the locations and the states are part of the a priori shared key material. In contrast to the data carrying qubits, which are in BB84 states (on the xz-circle on the Bloch sphere), we let the test bit states cover both dimensions of the Bloch sphere (by using the same six states as six-state QKD [BPG99, Bru98]). The advantage of this larger test space is that the noise symmetrization technique of Renner et al. [RGK05, Ren05] then yields a higher rate than BB84 test states would.

Alice is willing to send meaningful data to Bob only if Channel 1 is sufficiently noiseless. However, she already has to send data before she can assess the noise level. The solution is to first send a random string and later decide to use that string as an encryption mask for useful data.

Error correction and privacy amplification are done in a fairly straightforward way, except for one technicality: The privacy amplification must be computable in both directions. We implement this with the hash functions discussed in Section 5.3.

The shared secret hash seed can be re-used as is the case in the QKR schemes of Chapters 3 and 4 where it plays a similar role.

6.3.2 Preparation

Alice holds a classical message $m \in \{0,1\}^\ell$ which contains an authentication tag created with a one-time MAC. The security parameter of the MAC is a constant that we will ignore in our analysis since we are mainly interested in the asymptotics.

There are $n + \nu$ qubits sent back and forth, n for communication and ν for channel monitoring. $\nu = \mathcal{O}(\log n)$. Alice and Bob generate shared key material $k = (u, k_{\text{syn}}, k_{\text{test}}, \mathcal{I}_{\text{test}}, b^1_{\text{test}}, b^2_{\text{test}}, \xi, \eta)$. Here $u \in \{0,1\}^{2n}$ is the random seed used for privacy amplification; the $k_{\text{syn}} \in \{0,1\}^{n-\kappa}, k_{\text{test}} \in \{0,1\}^\nu$ are used as one-time pads protecting the syndrome and Alice's test measurement outcome respectively; $\mathcal{I}_{\text{test}} \subset \{1, \ldots, n+\nu\}$, with $|\mathcal{I}_{\text{test}}| = \nu$, describes the positions of the test qubits; $b^{1,2}_{\text{test}} \in \{0,1,2\}^\nu$ are the bases in which the test qubits are prepared, and $\xi, \eta \in \{0,1\}^\nu$ are the payloads of the test qubits in Channel 1 and 2 respectively. In addition, not named explicitly, Alice and Bob share two authentication keys, one for the plaintext message m and one for the classical channel.

Alice and Bob agree on a efficiently invertible paiwise independent hash $\Phi_u : \{0,1\}^n \to \{0,1\}^\ell$, see Section 5.3. They agree on an error correcting code with syndrome function `Syn`: $\{0,1\}^n \to \{0,1\}^{n-\kappa}$ and decoding function `SynDec`: $\{0,1\}^{n-\kappa} \to \{0,1\}^n$. They agree on noise thresholds β^*, γ^* for quantum Channels 1 and 2 respectively. They adopt the channel monitoring procedure shown below, which accepts only if the bit error rates in the test states are sufficiently low and independent of the bases.

Definition 6.5. *Let ξ' be the noisy version of the test string ξ as received by Alice through Channel 1, and likewise let η' be the noisy version of η received by Bob. For $b \in \{0,1,2\}$ let $\xi(b)$ denote the part of ξ that is encoded in basis b, and likewise for ξ', η, η'. Let $\triangle_1(b) = \xi(b) \oplus \xi'(b)$ and $\triangle_2(b) = \eta(b) \oplus \eta'(b)$ be error vectors. Let $\nu(b)$ denote the number of test qubits encoded in basis b. For $b, b' \in \{0,1,2\}$ let $\xi(b,b')$ denote ξ restricted to those positions where the encoding basis is b in Channel 1 and b' in Channel 2. Let $d_1(b,b') = \xi(b,b') \oplus \xi'(b,b')$ and $d_2(b,b') = \eta(b,b') \oplus \eta'(b,b')$ be the corresponding error vectors. Let $\nu(b,b')$ denote the number of positions where the*

qubit on Channel 1 is encoded in basis b and the qubit in Channel 2 in basis b'. The channel monitoring consists of two verifications,

$$\mathsf{CheckA}(b, \triangle_1) = \begin{cases} 1 & \text{if } \forall_{b\in\{0,1,2\}} \frac{\mathtt{Hamm}(\triangle_1(b))}{\nu(b)} \leq \beta^* \\ 0 & \text{otherwise.} \end{cases} \tag{6.5}$$

$$\mathsf{CheckB}(b, b', \triangle_1, \triangle_2, d_1, d_2) = \begin{cases} 1 & \text{if } \forall_{b,b'\in\{0,1,2\}} \left\{ \frac{\mathtt{Hamm}(d_1(b,b')\wedge d_2(b,b'))}{\nu(b,b')} \leq \beta^*\gamma^* \right. \\ & \text{and } \frac{\mathtt{Hamm}(\triangle_1(b))}{\nu(b)} \leq \beta^* \\ & \left. \text{and } \frac{\mathtt{Hamm}(\triangle_2(b'))}{\nu(b')} \leq \gamma^* \right\} \\ 0 & \text{otherwise.} \end{cases} \tag{6.6}$$

Our motivation for including a separate test for each (b, b') combination is that it imposes symmetry, which simplifies the noise symmetrization step (Section 6.4.1).

6.3.3 Protocol steps

Let VSUE denote the vulnerable-sender unclonable encryption protocol. In our attacker model it is crucial that Alice does not generate her private randomness at the start of the protocol. We describe Alice and Bob's actions chronologically by splitting up VSUE.Gen, VSUE.Enc and VSUE.Post. Alice and Bob perform the following actions (See Figure 6.1).

Alice and Bob:

VSUE.Gen: Alice and Bob generate shared key material $k = (u, k_{\text{syn}}, k_{\text{test}}, \mathcal{I}_{\text{test}}, b^1_{\text{test}}, b^2_{\text{test}}, \xi, \eta)$. The hash seed u can be re-used from the previous round.

Bob:

VSUE.Gen: Bob generates random $x, b \in \{0,1\}^n$.

VSUE.Enc: Bob prepares $n + \nu$ qubits. At locations $\mathcal{I}_{\text{test}}$ he encodes ξ in basis b^1_{test}. In the other positions he encodes x in basis b. He sends the qubits to Alice and stores x, b as private keys.

Alice:

VSUE.Gen: Alice generates her authenticated message $m \in \{0,1\}^\ell$. She generates local random strings $t \in \{0,1\}^n$ and $r \in \{0,1\}^{n-\ell}$.

VSUE.Enc: At the i'th non-test position Alice applies the Pauli operation $(\sigma_x\sigma_z)^{t_i}$ to the qubit,[4] and sends the resulting state back to Bob. In the test positions, she measures the qubits in basis b^1_{test}, yielding measurement outcomes that form a string $\xi' \in \{0,1\}^\nu$. In the j'th test position she prepares state $|\psi^{b^2_{\text{test}}[j]}_{\eta[j]}\rangle$ and sends it to Bob.

VSUE.Post: Alice computes $\triangle_1(0), \triangle_1(1), \triangle_1(2)$ from $\xi, \xi', b^1_{\text{test}}$ and performs $\mathsf{CheckA}(b^1_{\text{test}}, \triangle_1)$. If the result is 0 she sets $\mu = \perp$. Otherwise she {computes $z = F^{\text{inv}}_u(m\|r)$, $c = z \oplus t$ and $s = \mathtt{Syn}\, z$. She sets $\mu = (\xi' \oplus k_{\text{test}}, s \oplus k_{\text{syn}}, c)$ and deletes z, c, s}. She sends μ over the authenticated classical channel and deletes t, r.

[4] This operation has the effect that a BB84 state $|\psi^b_x\rangle$ is changed to $|\psi^b_{x\oplus t_i}\rangle$.

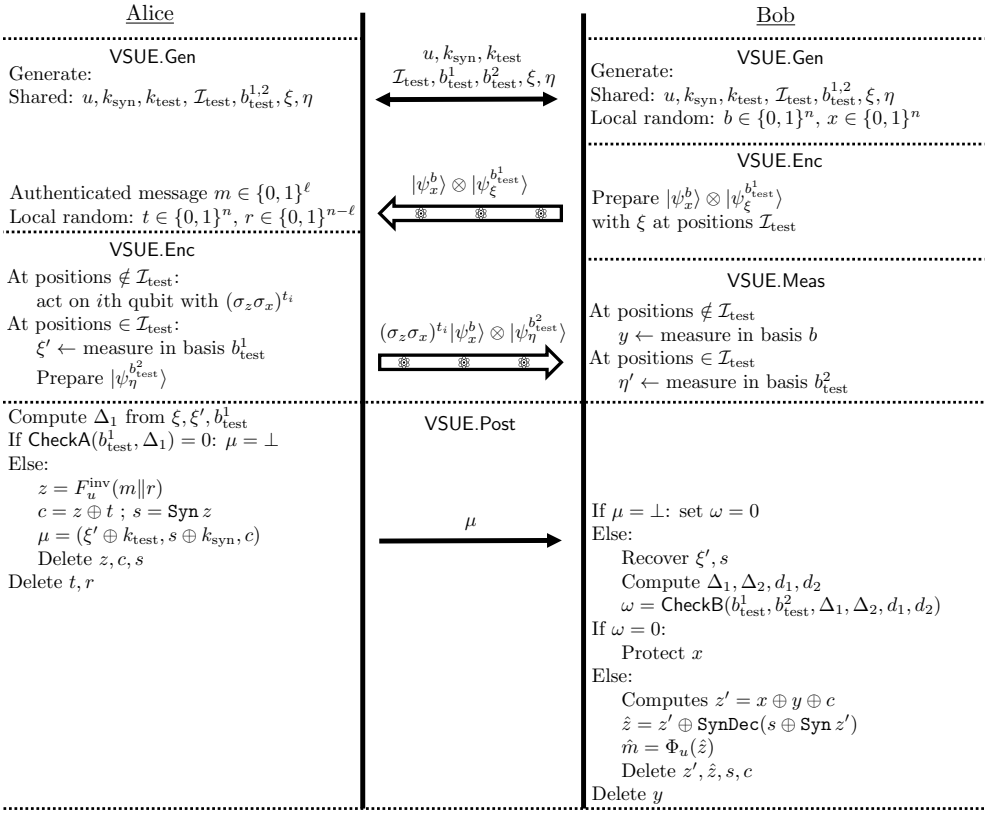

Figure 6.1: VSUE *protocol steps.*

Bob:

VSUE.Meas: At the non-test positions, Bob measures the qubits in basis b, yielding $y \in \{0,1\}^n$. At the test positions, he measures in basis $b^2_{\rm test}$, yielding $\eta' \in \{0,1\}^\nu$.
VSUE.Post: If Alice's classical message is $\perp$ he sets $\omega = 0$. Otherwise he {recovers ξ' from $\xi' \oplus k_{\rm test}$ and compute $\triangle_1, \triangle_2, d_1, d_2$ from $\xi, \xi'\eta, \eta', b^1_{\rm test}, b^2_{\rm test}$. He performs the channel monitoring $\omega = \mathsf{CheckB}(b^1_{\rm test}, b^2_{\rm test}, \triangle_1, \triangle_2, d_1, d_2)$.} If $\omega = 0$ he takes effort to protect x. If $\omega = 1$ he {computes $z' = x \oplus y \oplus c$, recovers s from $s \oplus k_{\rm syn}$, performs error correction as $\hat{z} = z' \oplus \mathtt{SynDec}(s \oplus \mathtt{Syn}\, z')$, reconstructs the message $\hat{m} = \Phi_u(\hat{z})$ and deletes $s, z', \hat{z}, c$.}
He deletes y. (Depending on the context he can send ω over the authenticated channel.)

Alice's nonvolatile keys are the shared keys. Her volatile secrets are t, r, z, c, s. Bob's nonvolatile keys are the shared keys and in addition b, x. His volatile secrets are $s, z', \hat{z}, y$. The deletion of volatile secrets is explicitly indicated in the protocol.

6.4 Modified protocol for the security proof

6.4.1 List of modifications

We will prove the security using the proof recipe of Section 2.5. We introduce protocol modifications step by step. At each step we indicate why the newly obtained scheme is equivalent, security-wise, to the previous. Security of the modified scheme implies security of the original scheme.

The main modifications are (i) EPR re-formulation of Bob's state preparation and Alice's state manipulation; (ii) EPR re-formulation of the channel monitoring; (iii) A random permutation of the EPR pairs, which makes the existing permutation symmetry explicitly visible. Permutation symmetry is needed in order to apply Post-selection (Lemma 2.16); (iv) Noise symmetrization using random Pauli operators.

Furthermore, the use of the one-time pads k_{test} and k_{syn} is replaced by a confidential channel, invisible to Eve, through which ξ' and s respectively are transported. The length of $k_{\text{test}}, k_{\text{syn}}$ is still taken into account when we compute communication efficiency. Similarly, the existence of the shared keys ξ, η is replaced by a confidential channel over which to transport data of the same size.

Note that the modified scheme requires Alice and Bob to have quantum memory. This does not affect the practical implementability of the original scheme, since the EPR-based scheme serves as a proof-technical construct only.

In Section 6.4.2 we give the full details of the modified scheme.

EPR variant of the 'bounce'

We replace Alice's operation $(\sigma_x\sigma_z)^t$ on the qubit state $|\psi_x^b\rangle$ (and Bob's recovery of t) by the following steps. Let $\mathcal{A}_0 = \{\mathbb{1}, \sigma_y\}$, $\mathcal{A}_1 = \{\sigma_z, \sigma_x\}$. First Alice flips a coin $a \in \{0,1\}$ which decides whether she will pick $\mathcal{A}_0$ or $\mathcal{A}_1$. Then she applies $\mathcal{A}_a[t]$ to $|\psi_x^b\rangle$.[5] She sends the resulting qubit state and a to Bob. Bob measures in basis b, yielding $y \in \{0,1\}$. In case $a = 0$, Bob recovers t as $t = y \oplus x$ as before. In case $a = 1$, a flip in basis $b = 0$ results from the σ_x while a flip in basis $b = 1$ results from σ_z; hence $t = x \oplus y \oplus b$. Overall $t = x \oplus y \oplus ab$.

Note that Eve learns nothing about t by observing a. Obviously, if this protocol variant with the additional parameter a is secure then the original protocol is secure.

Next we make one more change. Let $|\Phi_{vw}\rangle$ be the Bell states on the two-qubit space. Recall from Section 2.3.3 that we can write the Bell states and their relations as: $|\Phi_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, $|\Phi_{vw}\rangle = (\mathbb{1} \otimes \sigma_x^v\sigma_z^w)|\Phi_{00}\rangle = \frac{|0,v\rangle+(-1)^w|1,\bar{v}\rangle}{\sqrt{2}}$. We replace the sending of a random bit $t \in \{0,1\}$ by the following steps. Eve prepares two (noisy) EPR pairs, nominally in the state $|\Phi_{00}\rangle$, and sends one half to Alice, one half to Bob. Alice measures her two qubits in the Bell basis $|\Phi_{vw}\rangle$, yielding outcome $(v,w) \in \{0,1\}^2$. She sets $t = v$, $a = v \oplus w$. She sends a. Bob generates random $b \in \{0,1\}$ and measures both his qubits in basis b, yielding $x, y \in \{0,1\}$. He recovers t as

[5] I.e. $(a,t) = (0,0)$ corresponds to $\mathbb{1}$, $(0,1)$ to σ_y, $(1,0)$ to σ_z and $(1,1)$ to σ_x. Alice's action can be seen as a Quantum One Time Pad encryption $\sigma_x^t\sigma_z^{a\oplus t}$.

$t = x \oplus y \oplus ab$.[6] Security of the EPR variant implies security of the protocol variant described above. The same equivalence is used in [BLMR13].

EPR variant of the channel monitoring

The monitoring procedure of sending a state $|\psi_\xi^b\rangle$ (with shared $b \in \{0,1,2\}, \xi \in \{0,1\}$) to the other side, where it is measured in basis b, is now replaced by the following procedure. The basis b is still a shared secret. Eve prepares two (noisy) EPR pairs, nominally in the state $|\Phi_{00}\rangle$, and sends one half to Alice, one half to Bob. Alice measures her qubit in basis b, obtaining outcome ξ^{A}. Bob measures his qubit in basis b, obtaining outcome ξ^{B}. One party sends its measurement outcome to the other side, in plaintext. There the noise bit $\triangle$ is computed as $\triangle = \xi^{\mathrm{A}} \oplus \xi^{\mathrm{B}} \oplus \delta_{b2}$. (The contribution δ_{b2} comes from the fact that the $|\Phi_{00}\rangle$ state[7] causes $\xi^{\mathrm{B}} = 1 - \xi^{\mathrm{A}}$ when $b = 2$.) This procedure is followed in all test positions $\mathcal{I}_{\mathrm{test}}$ and allows for the computation of the strings $\triangle_1(b), \triangle_2(b), d_1(b,b'), d_2(b,b')$ as in the original protocol.

Random permutation

To make the permutation invariance of the modified protocol explicitly visible, we introduce a permutation that is applied to the pairs of EPR states corresponding to a qubit moving back and forth in the original protocol before anything else is done. Of course we have to justify why this addition has no impact on the security analysis. A permutation of the EPR positions re-distributes the noise. First, this has no impact on the statistics of the error counts $\mathtt{Hamm}(\triangle_1(b))$, $\mathtt{Hamm}(\triangle_2(b))$, $\mathtt{Hamm}(d_1(b,b'))$, $\mathtt{Hamm}(d_2(b,b'))$ (since $\mathcal{I}_{\mathrm{test}}$ is random and unknown to Eve) and hence the monitoring is not affected. Second, the error correction of z' is not sensitive to permutation of the bit flips.

Let $\mathcal{E}_{\mathrm{perm}}$ denote the CPTP map describing the new protocol, which has the random permutation as its first step. Permutation invariance is evident since we have $\mathcal{E}_{\mathrm{perm}} \circ \pi = \mathcal{E}_{\mathrm{perm}}$ for any permutation π. This allows us to use post-selection (Lemma 2.16) and focus on collective attacks. Crucially, this means that *the noise level caused by Eve is the same in the non-test locations as in the test locations*, and has to be such that the monitoring tests are passed.

Noise symmetrisation with random Pauli operators

We apply the noise symmetrization trick as introduced in [Ren05]. Alice and Bob publicly draw random strings $\alpha_1, \alpha_2 \in \{0,1,2,3\}^{n+\nu}$. Before they do any measurement, they each apply the Pauli operation $\Sigma(\alpha_1) = \bigotimes_{i=1}^{n+\nu} \sigma_{\alpha_1[i]}$ on their own EPR qubits in Channel 1, and $\Sigma(\alpha_2)$ in Channel 2. Then they forget α_1, α_2. This results

[6] This procedure can be interpreted as entanglement swapping by Alice, so that Bob's qubits become entangled, but with one difference: Bob receives only one classical bit ($a = v \oplus w$) instead of the two 'key' bits v, w. Alternatively, it can be viewed as an incomplete teleport. First, Bob's measurement in basis b, yielding x, is equivalent to sending $|\psi_x^b\rangle$. Alice's Bell measurement is a teleport, turning the state of Bob's second qubit into a random encryption $\sigma_x^v \sigma_z^w |\psi_x^b\rangle$. For a full teleport Alice would send v and w.

[7] If we had chosen the singlet state $\propto |01\rangle - |10\rangle$ there would be no asymmetry between the bases.

in a huge simplification of Alice and Bob's state: only 15 global parameters are left to describe the whole state.

Of course we have to justify why adding this operation does not affect the correctness and the security of the protocol. All measurements in the protocol (with outcomes x, y, a, t) are done in either the x, y or z basis. For $b \in \{0, 1, 2\}$ the effect of a Pauli on a qubit state $|\psi_x^b\rangle$ is at most a bit flip to $|\psi_{\bar{x}}^b\rangle$. Thus, the effect on the outcomes x, y, a, t is at most a number of bit flips; but since Alice and Bob apply the same Paulis, the flips do not prevent Bob from reconstructing the correct t. Furthermore, Eve knows α_1, α_2, so for her the statistics of x, y, a, t have not changed.

6.4.2 The modified protocol

Let VSUE' be the modified protocol. The steps are shown in Figure 6.2 and listed below. An untrusted source creates $2(n+\nu)$ noisy EPR pairs in the $|\widetilde{\Phi}_{00}\rangle$ state, sends half of each pair to Alice and half to Bob. They perform the following actions:

Alice and Bob:

VSUE.Gen: Alice and Bob generate shared key material $k = (u, \mathcal{I}_{\text{test}}, b^1_{\text{test}}, b^2_{\text{test}})$.

Bob:

VSUE.Gen: Bob generates random $b \in \{0,1\}^n$, a random permutation π and random $\alpha_1, \alpha_2 \in \{0, 1, 2, 3\}^{n+\nu}$.

VSUE.Enc: He permutes the qubits according to π and applies $\Sigma(\alpha_1)$ on his first qubits and $\Sigma(\alpha_2)$ on his second qubits. He measures the qubits of Channel 1. At the test positions $\mathcal{I}_{\text{test}}$, he measures in basis b^1_{test}. This yields outcome $\xi \in \{0,1\}^\nu$. At the non-test positions he measures in basis b, yielding outcome $x \in \{0,1\}^n$. He sends ξ through the confidential channel and stores b, x as private keys.

Alice:

VSUE.Gen: Alice generates her authenticated message $m \in \{0,1\}^\ell$. She generates local random string $r \in \{0,1\}^{n-\ell}$.

VSUE.Enc: She permutes the qubits according to π and applies $\Sigma(\alpha_1)$ on her first qubits and $\Sigma(\alpha_2)$ on her second qubits. In the test positions $\mathcal{I}_{\text{test}}$, she measures the Channel 1 qubits in basis b^1_{test}, and the Channel 2 qubits in basis b^2_{test}. This yields strings ξ' and η respectively. In each non-test position she measures the pair of qubits in the Bell basis $(|\Phi_{tw}\rangle)_{t,w\in\{0,1\}}$. This yields outcome $t, w \in \{0,1\}^n$. She compute $\triangle_1$ from $\xi, \xi', b^1_{\text{test}}$ and perform $\mathsf{CheckA}(b^1_{\text{test}}, \triangle_1)$. If the result is 0, she sets $\mu = \perp$. Otherwise she {sets $a = t \oplus w$, computes $z = F_u^{\text{inv}}(m\|r)$, $s = \mathtt{Syn}\, z$, $c = t \oplus z$, $\mu = (a, c)$. She sends ξ', η, s over the confidential channel; She deletes r, z, s, c.} She sends μ over the authenticated channel and deletes t, w.

Bob:

VSUE.Meas: Bob measure the qubits of Channel 2. In the test positions $\mathcal{I}_{\text{test}}$ he measures in basis b^2_{test}, yielding $\eta' \in \{0,1\}^\nu$. In the non-test positions he measures in basis b, yielding $y \in \{0,1\}^n$.

VSUE.Post: If $\mu = \perp$ he sets $\omega = 0$. Else he computes $\triangle_1, \triangle_2, d_1, d_2$ from $\xi, \xi', \eta, \eta', b^1_{\text{test}}, b^2_{\text{test}}$ and sets $\omega = \mathsf{CheckB}(b^1_{\text{test}}, b^2_{\text{test}}, \triangle_1, \triangle_2, d_1, d_2)$. If $\omega = 0$ he protects x. Otherwise he compute $z' = x \oplus y \oplus c \oplus (b \wedge a)$, $\hat{z} = z' \oplus \mathtt{SynDec}(s \oplus \mathtt{Syn}\, z')$, $\hat{m} = \Phi_u(\hat{z})$ and deletes $y, z', \hat{z}$.}

Depending on the context he sends ω to Alice.

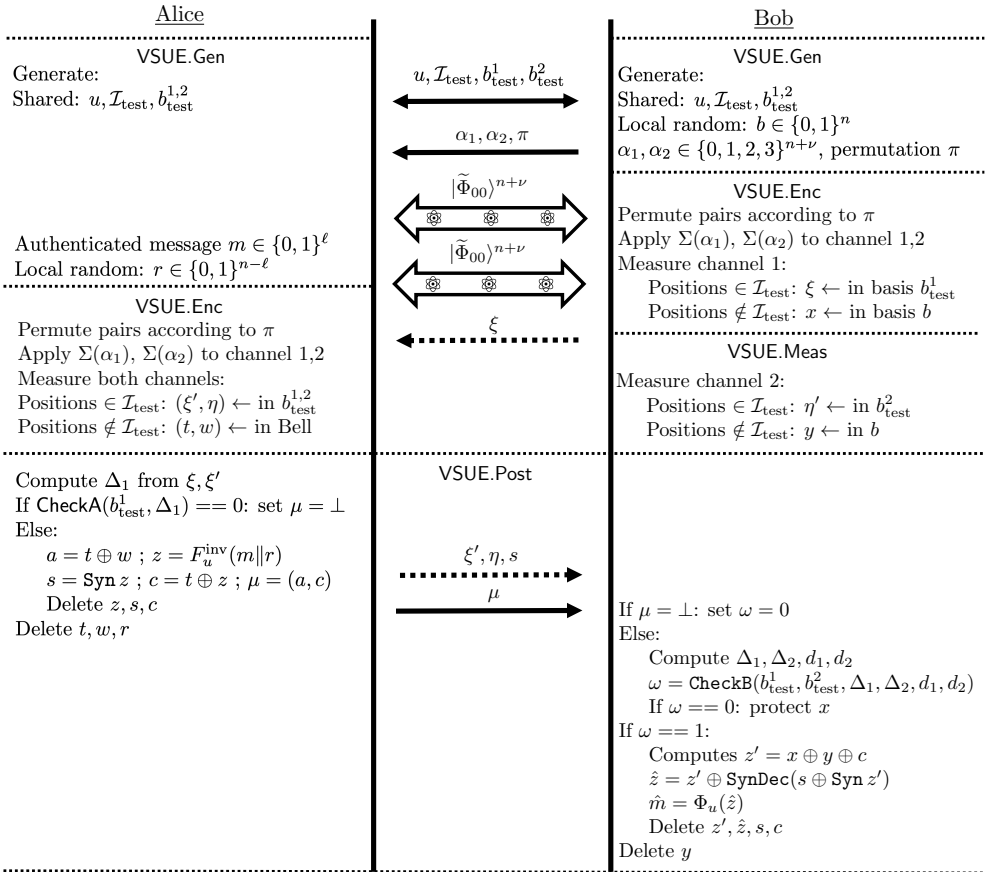

Figure 6.2: VSUE' *protocol steps. A dashed arrow represents a confidential classical channel.*

6.5 Eve's state

In step 6 of the proof recipe we will need a simplified form of the factorized state held by Eve. Here we derive that simple form. This will be used at the end of Section 6.6.3.

6.5.1 Effect of symmetrisation

We consider the (noisy) state of the EPR particles received by Alice and Bob. Without post-selection we would have had to consider a general $2^{4(n+\nu)}$-dimensional state. Post-selection instead allows us to restrict the analysis to collective attacks, which lead to a factorised state which we write as $(\sigma^{A_1B_1A_2B_2})^{\otimes(n+\nu)}$. Here 'A' and 'B' denote the subsystems of Alice and Bob, and the indices 1,2 denote the channel. Note that $\sigma^{A_1B_1A_2B_2}$ is 16-dimensional.

Next we look at the effect of the noise symmetrization as discussed in Section 6.4.1. Averaging over the random Pauli operators yields a new state $\tilde{\sigma}$ given by

$$\tilde{\sigma}^{A_1B_1A_2B_2} = \frac{1}{16}\sum_{\alpha_1,\alpha_2=0}^{3}(\sigma_{\alpha_1}\otimes\sigma_{\alpha_1}\otimes\sigma_{\alpha_2}\otimes\sigma_{\alpha_2})\sigma^{A_1B_1A_2B_2}(\sigma_{\alpha_1}\otimes\sigma_{\alpha_1}\otimes\sigma_{\alpha_2}\otimes\sigma_{\alpha_2}). \quad (6.7)$$

Lemma 6.6. *$\tilde{\sigma}^{A_1B_1A_2B_2}$ is diagonal in the basis $\left(|\Phi_{a_1b_1}\rangle\otimes|\Phi_{a_2b_2}\rangle\right)_{a_1,b_1,a_2,b_2\in\{0,1\}}$, where $|\Phi_{ab}\rangle$ stands for the Bell states as defined in Section 2.3.3.*

Proof: For a general 16-dimensional mixed state we can write

$$\sigma^{\mathrm{A_1B_1A_2B_2}} = \sum_{a_1b_1a_2b_2}\sum_{a_1'b_1'a_2'b_2'}\nu^{a_1b_1a_2b_2}_{a_1'b_1'a_2'b_2'}|\Phi_{a_1b_1}\rangle\langle\Phi_{a_1'b_1'}|\otimes|\Phi_{a_2b_2}\rangle\langle\Phi_{a_2'b_2'}|. \quad (6.8)$$

The randomization happens in each channel separately. The effect of the randomization is $\frac{1}{4}\sum_\alpha(\sigma_\alpha\otimes\sigma_\alpha)|\Phi_{ab}\rangle\langle\Phi_{a'b'}|(\sigma_\alpha\otimes\sigma_\alpha) = \delta_{aa'}\delta_{bb'}|\Phi_{ab}\rangle\langle\Phi_{a'b'}|$. This yields $\tilde{\sigma}^{A_1B_1A_2B_2} = \sum_{a_1b_1a_2b_2}\nu^{a_1b_1a_2b_2}_{a_1b_1a_2b_2}|\Phi_{a_1b_1}\rangle\langle\Phi_{a_1b_1}|\otimes|\Phi_{a_2b_2}\rangle\langle\Phi_{a_2b_2}|$. □

We denote the diagonal elements of $\tilde{\sigma}^{A_1B_1A_2B_2}$ as $\nu^{a_1b_1}_{a_2b_2}$ with $a_1,b_1,a_2,b_2\in\{0,1\}$. Eve holds the purification of $\tilde{\sigma}^{A_1B_1A_2B_2}$. The joint state of Alice Bob and Eve is described by a pure state $|\psi^{\mathrm{ABE}}\rangle$,

$$|\psi^{\mathrm{ABE}}\rangle \quad = \quad \sum_{a_1b_1a_2b_2}\sqrt{\nu^{a_1b_1}_{a_2b_2}}|\Phi_{a_1b_1}\rangle\otimes|\Phi_{a_2b_2}\rangle\otimes|e^{a_1b_1}_{a_2b_2}\rangle. \quad (6.9)$$

Here $|e^{a_1b_1}_{a_2b_2}\rangle$ is an orthonormal basis in Eve's 16-dimensional Hilbert space.

6.5.2 Effect of channel monitoring

There are 15 degrees of freedom in $\tilde{\sigma}^{A_1B_1A_2B_2}$. However, the channel monitoring CheckA, CheckB imposes a large number of constraints. For the bit error probability in Channel i, as a function of the monitoring basis $b\in\{0,1,2\}$, we write

$$r_i(b) \stackrel{\mathrm{def}}{=} \sum_{x\in\{0,1\}}\langle\psi^b_x|\otimes\langle\psi^b_{\overline{x}\oplus\delta_{b2}}|\tilde{\sigma}^{\mathrm{A_iB_i}}|\psi^b_x\rangle\otimes|\psi^b_{\overline{x}\oplus\delta_{b2}}\rangle \quad (6.10)$$

where the δ_{b2} occurs because the $|\Phi_{00}\rangle$ Bell state has a bit flip in the $b=2$ basis (y basis). Similarly, by $s(b,b')$ we denote the probability that a flip is detected *both* Channels, as a function of the monitoring basis b in Channel 1 and b' in Channel 2,

$$s(b,b') \stackrel{\mathrm{def}}{=} \sum_{p,q\in\{0,1\}}\langle\psi^b_p|\langle\psi^b_{\overline{p}\oplus\delta_{b2}}|\langle\psi^{b'}_q|\langle\psi^{b'}_{\overline{q}\oplus\delta_{b'2}}|\tilde{\sigma}^{\mathrm{A_1B_1A_2B_2}}|\psi^b_p\rangle|\psi^b_{\overline{p}\oplus\delta_{b2}}\rangle|\psi^{b'}_q\rangle|\psi^{b'}_{\overline{q}\oplus\delta_{b'2}}\rangle. \quad (6.11)$$

If only CheckA is passed, the monitoring imposes that $\forall_{b\in\{0,1,2\}}\quad r_1(b)\le\beta^*$. If CheckB is passed, the channel monitoring imposes 15 constraints,

$$\forall_{b,b'\in\{0,1,2\}}\quad r_1(b)\le\beta^*\ \wedge\ r_2(b')\le\gamma^*\ \wedge\ s(b,b')\le\beta^*\gamma^*. \quad (6.12)$$

Since we give Eve access to the purification of the state shared by Alice and Bob, it is always to her advantage to have more noise on Alice and Bob's state so that the purification holds more information. We therefore set the noise she causes (β, γ) asymptotically equal to the noise thresholds β^*, γ^* if the checks are passed.

Lemma 6.7. *If* $\mathsf{CheckA} = 1$ *then it holds that* $\sum_{a_2b_2} \nu_{a_2b_2}^{a_1b_1} = \frac{\beta}{2} + \delta_{a_1,0}\delta_{b_1,0}(1-2\beta)$.

Proof: We have $\tilde{\sigma}^{\mathrm{A_1B_1}} = \mathrm{tr}_{\mathrm{A_2B_2}}\tilde{\sigma}^{\mathrm{A_1B_1A_2B_2}} = \sum_{a_1b_1}(\sum_{a_2b_2}\nu_{a_2b_2}^{a_1b_1})|\Phi_{a_1b_1}\rangle\langle\Phi_{a_1b_1}|$. We introduce abbreviated notation $c^{a_1b_1} = \sum_{a_2b_2}\nu_{a_2b_2}^{a_1b_1}$. The $b=0$ constraint (6.12) in Channel 1 gives $\sum_{b_1} c^{1,b_1} = \beta$. Similarly, the $b=1$ constraint gives $\sum_{a_1} c^{a_1,1} = \beta$, and the $b=2$ constraint gives $\sum_{a_1} c^{a_1\overline{a_1}} = \beta$. Furthermore, normalisation of $\tilde{\sigma}$ requires $\sum_{a_1b_1} c^{a_1b_1} = 1$. Together this uniquely fixes $c^{a_1b_1} = \frac{\beta}{2} + \overline{a_1}\overline{b_1}(1-2\beta)$. □

Lemma 6.8. *If* $\mathsf{CheckB} = 1$ *then* $\nu_{a_2b_2}^{a_1b_1} = \left[\frac{\beta}{2} + \delta_{0,0}^{a_1b_1}(1-2\beta)\right]\left[\frac{\gamma}{2} + \delta_{0,0}^{a_2b_2}(1-2\gamma)\right]$.

Proof: CheckB comprises CheckA. Hence we can use the result of Lemma 6.7. Also, we get the equivalent of Lemma 6.7 for Channel 2, $\sum_{a_1b_1}\nu_{a_2b_2}^{a_1b_1} = \frac{\gamma}{2} + \delta_{0,0}^{a_2b_2}(1-2\gamma)$. The $s(b,b')$ constraints in (6.12) yield $\sum_{a_1a_2}\nu_{a_21}^{a_11} = \sum_{a_1a_2}\nu_{a_2\bar{a}_2}^{a_11} = \sum_{a_1b_2}\nu_{1b_2}^{a_11} = \sum_{a_1a_2}\nu_{a_21}^{a_1\bar{a}_1} = \sum_{a_1a_2}\nu_{a_2\bar{a}_2}^{a_1\bar{a}_1} = \sum_{a_1b_2}\nu_{1b_2}^{a_1\bar{a}_1} = \sum_{b_1a_2}\nu_{a_21}^{1b_1} = \sum_{b_1a_2}\nu_{a_2\bar{a}_2}^{1b_1} = \sum_{b_1b_2}\nu_{1b_2}^{1b_1} = \beta\gamma$. Solving this system of equations yields the claim. □

Lemma 6.8 tells us that in the accept case ($\omega = \mathsf{CheckB} = 1$), Alice and Bob's state reduces to the tensor product of two states known from the 6-state analysis in Chapter 2 and in [Ren05]. The state depends only on the noise parameters β and γ.

$$\begin{aligned}\tilde{\sigma}_{\mathsf{accept}}^{\mathrm{A_1B_1A_2B_2}} &= \Big[(1-\frac{3}{2}\beta)|\Phi_{00}\rangle\langle\Phi_{00}| + \frac{\beta}{2}\big(|\Phi_{01}\rangle\langle\Phi_{01}| + |\Phi_{10}\rangle\langle\Phi_{10}| + |\Phi_{11}\rangle\langle\Phi_{11}|\big)\Big] \otimes \\ &\quad \Big[(1-\frac{3}{2}\gamma)|\Phi_{00}\rangle\langle\Phi_{00}| + \frac{\gamma}{2}\big(|\Phi_{01}\rangle\langle\Phi_{01}| + |\Phi_{10}\rangle\langle\Phi_{10}| + |\Phi_{11}\rangle\langle\Phi_{11}|\big)\Big]. \quad (6.13)\end{aligned}$$

6.5.3 Conditioning on measurement outcomes

Next we look at the effect of Alice and Bob's measurements in the non-test positions. Alice performs a Bell measurement and Bob measures both his qubits in basis b. Using the definition of the Bell states $|\Phi_{t,a\oplus t}\rangle_{A_1A_2} = \sum_{p\in\{0,1\}}|p\rangle_{A_1}\sigma_x^t\sigma_z^{a\oplus t}|p\rangle_{A_2}$ the measurements of Alice and Bob can be described by a single POVM. At given $b \in \{0,1\}$ the joint measurement yields $x, y, a, t \in \{0,1\}$,

$$\mathcal{M}_{xyat}^b = |\phi_{xyat}^b\rangle\langle\phi_{xyat}^b| \quad (6.14)$$

$$|\phi_{xyat}^b\rangle = \frac{1}{\sqrt{2}}\sum_p |p\rangle|\psi_x^b\rangle\sigma_x^t\sigma_z^{a\oplus t}|p\rangle|\psi_y^b\rangle. \quad (6.15)$$

Here $\forall_b \sum_{xyat}\mathcal{M}_{xyat}^b = \mathbb{1}$. Having a description of $|\psi^{\mathrm{ABE}}\rangle$ and $|\phi_{xyat}^b\rangle$ allows us to write down Eve's state after the A and B subsystems have been measured, i.e. conditioned on the measurement outcomes. At fixed $b \in \{0,1\}$ we write

$$P_{xyat|b} \stackrel{\mathrm{def}}{=} \Pr[xyat|b] \quad (6.16)$$

$$P_{xyat|b}\cdot\sigma_{bxyat}^{\mathrm{E}} = \mathrm{tr}_{\mathrm{AB}}\left(|\Psi^{\mathrm{ABE}}\rangle\langle\Psi^{\mathrm{ABE}}|\mathcal{M}_{xyat}^b\right) = |\bar{\psi}_{bxyat}^{\mathrm{E}}\rangle\langle\bar{\psi}_{bxyat}^{\mathrm{E}}| \quad (6.17)$$

$$|\bar{\psi}_{bxyat}^{\mathrm{E}}\rangle \stackrel{\mathrm{def}}{=} \langle\phi_{xyat}^b|\Psi^{\mathrm{ABE}}\rangle. \quad (6.18)$$

Here $|\bar{\psi}^{\mathrm{E}}_{bxyat}\rangle$ is a sub-normalized state with squared norm $P_{xyat|b}$. We will write $|\bar{\psi}^{\mathrm{E}}_{bxyat}\rangle = \sqrt{P_{xyat|b}}|\psi^{\mathrm{E}}_{bxyat}\rangle$.

Lemma 6.9. *Eve's (sub-normalized) pure state conditioned on Alice and Bob's measurement outcomes is given by*

$$|\bar{\psi}^{\mathrm{E}}_{bxyat}\rangle = \frac{1}{2\sqrt{2}}\sum_{a_1b_1a_2b_2}\sqrt{\nu^{a_1b_1}_{a_2b_2}}(-1)^{b_2t}\Big[\bar{b}\delta_{x\oplus y\oplus t,a_1\oplus a_2}(-1)^{(b_1+b_2+a+t)(a_1+x)} + b(-1)^{xa_1+y(t+a_2)}\delta_{b_1\oplus b_2,x\oplus y\oplus a\oplus t}\Big]|e^{a_1b_1}_{a_2b_2}\rangle \tag{6.19}$$

Proof: see Appendix 6.A. □

From Lemma 6.9 we obtain

$$P_{xyat|b} = \langle\bar{\psi}^{\mathrm{E}}_{bxyat}|\bar{\psi}^{\mathrm{E}}_{bxyat}\rangle = \frac{1}{8}\Big(\bar{b}\sum_{a_1b_1b_2}\nu^{a_1b_1}_{a_1\oplus x\oplus y\oplus t,b_2} + b\sum_{a_1b_1a_2}\nu^{a_1b_1}_{a_2,b_1\oplus x\oplus y\oplus a\oplus t}\Big). \tag{6.20}$$

Note: substituting the ν's corresponding to an accept (Lemma 6.8) gives

$$P^{[\omega=1]}_{xyat|b} = \frac{1}{8}\big[\delta_{x\oplus y\oplus t\oplus ab,0}(1-\beta\star\gamma) + \delta_{x\oplus y\oplus t\oplus ab,1}\beta\star\gamma\big] \tag{6.21}$$

with the '$\star$' notation defined as $\beta\star\gamma = \beta(1-\gamma)+(1-\beta)\gamma$. This is as expected, since the bit error probability between x and y results from the concatenation of Channels 1 and 2.

Corollary 6.10. *It holds that* $P_{xat|b} = \frac{1}{8}$.

Proof: $P_{xat|b} = \sum_y P_{xyat|b}$. In (6.20) the summation over y gives rise to a full summation over all 16 components of ν. The Corollary follows from the normalization $\sum_{a_1b_1a_2b_2}\nu^{a_1b_1}_{a_2b_2} = 1$. □

The 16 states $|\psi^{\mathrm{E}}_{bxyat}\rangle$ (at fixed b) are *not* all mutually orthogonal, though a subset is.

Lemma 6.11.

$$\langle\psi^{\mathrm{E}}_{bxyat}|\psi^{\mathrm{E}}_{b\bar{x}yat}\rangle = \langle\psi^{\mathrm{E}}_{bxyat}|\psi^{\mathrm{E}}_{bx\bar{y}at}\rangle = \langle\psi^{\mathrm{E}}_{bxyat}|\psi^{\mathrm{E}}_{bxya\bar{t}}\rangle = \langle\psi^{\mathrm{E}}_{bxyat}|\psi^{\mathrm{E}}_{b\bar{x}\,\bar{y}a\bar{t}}\rangle = 0. \tag{6.22}$$

Proof: We take the inner product of two states of the form (6.19). The cross terms contain $b\bar{b}$ and vanish. The Kronecker deltas ensure that the inner product vanishes when an odd number out of the variables $\{x, y, t\}$ flip. □

Remark. Eve's overall state $\sigma^{\mathrm{E}}_b = \mathbb{E}_{xyat|b}\,\sigma^{\mathrm{E}}_{bxyat}$ (at fixed b) is the purification of $\tilde{\sigma}^{\mathrm{A_1B_1A_2B_2}}$ and is therefore diagonal in the basis $|e^{a_1b_1}_{a_2b_2}\rangle$ and has eigenvalues $\nu^{a_1b_1}_{a_2b_2}$. By way of consistency check we verify this by expanding $\mathbb{E}_{xyat|b}\,\sigma^{\mathrm{E}}_{bxyat} = \sum_{xyat}P_{xyat|b}|\psi^{\mathrm{E}}_{bxyat}\rangle\langle\psi^{\mathrm{E}}_{bxyat}| = \sum_{xyat}\mathrm{tr}_{\mathrm{AB}}|\psi^{\mathrm{ABE}}\rangle\langle\psi^{\mathrm{ABE}}|\mathcal{M}^b_{xyat} = \mathrm{tr}_{\mathrm{AB}}|\psi^{\mathrm{ABE}}\rangle\langle\psi^{\mathrm{ABE}}|(\sum_{xyat}\mathcal{M}^b_{xyat}) = \mathrm{tr}_{\mathrm{AB}}|\psi^{\mathrm{ABE}}\rangle\langle\psi^{\mathrm{ABE}}|$, which indeed produces the correct result.

Eve's state conditioned on the measurement outcomes and acceptance is denoted as $\sigma^{\mathrm{E}}_{bxyat,\omega=1}$.

Lemma 6.12. *Consider* $\sigma^{\mathrm{E}}_{bxat,\omega=1} = \mathbb{E}_{y|bxat,\omega=1}\, \sigma^{\mathrm{E}}_{bxyat,\omega=1}$. *The eigenvalues of* $\sigma^{\mathrm{E}}_{bxat,\omega=1}$ *are* $\beta \star \gamma, 1-\beta\star\gamma$ *and fourteen times zero.*

Proof: We have $\sigma^{\mathrm{E}}_{bxat,\omega=1} = \sum_y \frac{\Pr[xyat|b,\omega=1]}{\Pr[xat|b,\omega=1]} \sigma^{\mathrm{E}}_{bxyat,\omega=1} = \sum_y 8 P^{[\omega=1]}_{xyat|b} \sigma^{\mathrm{E}}_{bxyat,\omega=1}$. Here we have used (6.21). From Lemma 6.11 we know that $\sigma^{\mathrm{E}}_{bxyat,\omega=1}\sigma^{\mathrm{E}}_{bx\overline{y}at,\omega=1} = 0$. Thus $\sigma^{\mathrm{E}}_{bxat,\omega=1}$ is the weighted sum of two orthogonal projectors, with weights $\beta\star\gamma$ and $1-\beta\star\gamma$. □

Lemma 6.13. *Consider* $\sigma^{\mathrm{E}}_{bat} = \mathbb{E}_{xy|bat}\, \sigma^{\mathrm{E}}_{bxyat}$. *The spectral decomposition of* $\sigma^{\mathrm{E}}_{bat}$ *is*

$$\sigma^{\mathrm{E}}_{bat} = \sum_{u,v\in\{0,1\}} \Lambda_{uv} |V^{at}_{uv}\rangle\langle V^{at}_{uv}| \tag{6.23}$$

$$\Lambda_{uv} = \sum_{k,\ell\in\{0,1\}} \nu^{k,\ell}_{k\oplus u,\ell\oplus v} \tag{6.24}$$

$$|V^{at}_{uv}\rangle = \sum_{k,\ell\in\{0,1\}} \sqrt{\lambda^{k\ell}_{k\oplus u,\ell\oplus v}} |e^{k\ell}_{k\oplus u,\ell\oplus v}\rangle (-1)^{(a+v)\bar{k}} (-1)^{t(k+\ell)}. \tag{6.25}$$

It holds that $\langle V^{at}_{uv}|V^{at}_{u'v'}\rangle = \delta_{uu'}\delta_{vv'}$.

Proof: See Appendix 6.B. □

6.6 Security proof

We prove the security of the modified protocol as presented in Section 6.4.2. We show that the protocol is ε-VSUE (Definition 6.3) and ε-KR (Definition 6.4), where ε decreases exponentially in n if the message length ℓ is chosen appropriately. In Section 6.6.4 we derive an expression for the asymptotic rate. We first describe the CPTP maps related to the ideal protocol and the security definitions (step 3). We consider smooth states (step 4) and use the post-selection technique (step 5) to allow the use of the simplified state of Section 6.5 in step 6.

6.6.1 CPTP maps

The identification between the abstract quantities in the security definitions on the one hand and the protocol variables on the other hand is shown in Table 6.1.

Here b and s are counted as part of the transcript because they eventually leak.[8] The random Paulis α_1, α_2 will not appear explicitly in the analysis below because their symmetrising effect has already been accounted for. Similarly, the $\mathcal{I}_{\mathrm{test}}, b^{1,2}_{\mathrm{test}}$ do not feature in the analysis because the channel monitoring has been accounted for in Section 6.5.2.

We denote the overall action of Alice and Bob running the whole protocol as a CPTP map $\mathcal{E}_{\mathrm{VSUE}}$ acting on the 'AB' subsystem of the noisy EPR state ρ^{ABE}. We have

$$\mathcal{E}_{\mathrm{VSUE}} = \mathsf{VSUE'.Post} \circ \mathsf{VSUE'.Meas} \circ \mathsf{VSUE'.Enc} \circ \mathsf{VSUE'.Enc} \tag{6.26}$$

[8] s leaks because its one-time pad eventually leaks.

Definitions Section 6.2.2	EPR protocol Section 6.4.2
m, ω	m, ω
transcript t	$b, s, a, c, \alpha_1, \alpha_2$
S_{re}	u
S_{once}	$\mathcal{I}_{\text{test}}, b^{1,2}_{\text{test}}$
P	x

Table 6.1: Relation between variable names in Section 6.2.2 and Section 6.4.2.

Note that this order of maps commutes with the order of maps in the protocol description 6.4.2. It holds that

$$\mathcal{E}_{\text{VSUE}}(\rho^{\text{ABE}}) = \rho^{XMUBSACE}_{\texttt{accept}} + \rho^{X} \otimes \rho^{MUBSACE}_{\texttt{reject}}. \tag{6.27}$$

In the 'output' state we have traced out all variables except those in the table above. Note that we have isolated ρ^X in the Reject case, since the attacker model states that x does not leak upon reject. The coupling between Eve's subsystem 'E' and all the other variables occurs through the measurement variables $b, x, y, a, t \in \{0,1\}^n$. We write ρ^{E}_{bxyat} for Eve's state conditioned on b, x, y, a, t.

We derive an expression for (6.27) starting from the state that additionally contains the variables r, ω, t, y and the channel monitoring variables 'D', which we then trace out. We have $\rho^{XMUBSACRD\Omega TY\text{E}} = \mathbb{E}_{mubr}\, \mathbb{E}_{xyat|b}\, \mathbb{E}_d \sum_{sc\omega} |xmubsacrd\omega ty\rangle\langle\cdots| \otimes \rho^{\text{E}}_{bxyat}\ \delta_{s,\texttt{Syn}(c\oplus t)}\ \delta_{c,t\oplus F^{\text{inv}}_u(m||r)}\ \delta_{\omega,\texttt{CheckB}(d)}$. Here the u, b, r are uniform. The distribution of x, y, a, t, d is determined by the noise that Eve is causing. We trace out r, t, y, d. The expectation $\mathbb{E}_d$ then acts only on the Kronecker delta that contains d, which yields a factor $\mathbb{E}_d\, \delta_{\omega,\texttt{CheckB}(d)} = \Pr[\Omega = \omega]$; similarly, from $\mathbb{E}_r$ we get a factor $\mathbb{E}_r\, \delta_{c,t\oplus F^{\text{inv}}_u(m||r)} = 2^{\ell-n}\delta_{m,\Phi_u(c\oplus t)}$. The expectation $\mathbb{E}_{y|bxat}$ acting on ρ^{E}_{bxyat} gives ρ^{E}_{bxat} by definition. The result is

$$\begin{aligned}
\rho^{XMUBSACE}_{\texttt{accept}} \;=\;& \Pr[\Omega = 1] \mathop{\mathbb{E}}_{mubxa} \sum_{sc} |xmubsac\omega = 1\rangle\langle xmubsac\omega = 1| \\
& \otimes \mathop{\mathbb{E}}_{t|bxa} \rho^{\text{E}}_{bxat} \delta_{s,\texttt{Syn}(c\oplus t)} 2^{\ell-n} \delta_{m,\Phi_u(c\oplus t)} \qquad (6.28) \\
\rho^{MUBSACE}_{\texttt{reject}} \;=\;& \Pr[\Omega = 0] \mathop{\mathbb{E}}_{muba} \sum_{sc} |mubsac\omega = 0\rangle\langle mubsac\omega = 0| \\
& \otimes \mathop{\mathbb{E}}_{t|ba} \rho^{\text{E}}_{bat} \delta_{s,\texttt{Syn}(c\oplus t)} 2^{\ell-n} \delta_{m,\Phi_u(c\oplus t)} \qquad (6.29)
\end{aligned}$$

Next we determine the CPTP map $\mathcal{F}_{\text{VSUE}}$ that corresponds to the 'ideal' functionality. First, in order to achieve 0-KR according to Def. 6.4 the re-used key u must decouple from all the other variables. I.e. $\mathcal{F}_{\text{VSUE}}$ must be such that $\mathcal{F}_{\text{VSUE}}(\rho^{\text{ABE}}) = \rho^U \otimes \text{tr}_U\, \mathcal{E}(\rho^{\text{ABE}})$. If we apply tr_U to (6.28,6.29) we see the expression $\mathbb{E}_u\, \delta_{m,\Phi_u(c\oplus t)}$

appearing, which evaluates to $2^{-\ell}$ due to the fact that Φ is a pairwise independent hash. This causes $\mathbb{E}_m |m\rangle\langle m|$ to decouple from the rest of the state; hence 0-VSUE (Definition 6.3) is also satisfied. We get

$$\begin{aligned}
\mathcal{F}_{\mathrm{VSUE}}(\rho^{\mathrm{ABE}}) &= \rho^{MU} \otimes (\rho^{XBSAC\mathrm{E}}_{\texttt{accept}} + \rho^{X} \otimes \rho^{BSAC\mathrm{E}}_{\texttt{reject}}) && (6.30)\\
\rho^{XBSAC\mathrm{E}}_{\texttt{accept}} &= \Pr[\Omega=1] \mathop{\mathbb{E}}_{bxa} \sum_{sc} 2^{-n} |xbsac\omega=1\rangle\langle xbsac\omega=1| \\
&\quad \otimes \mathop{\mathbb{E}}_{t|bxa} \rho^{\mathrm{E}}_{bxat} \delta_{s,\texttt{Syn}(c\oplus t)} && (6.31)\\
\rho^{BSAC\mathrm{E}}_{\texttt{reject}} &= \Pr[\Omega=0] \mathop{\mathbb{E}}_{ba} \sum_{sc} 2^{-n} |bsac\omega=0\rangle\langle bsac\omega=0| \\
&\quad \otimes \mathop{\mathbb{E}}_{t|ba} \rho^{\mathrm{E}}_{bat} \delta_{s,\texttt{Syn}(c\oplus t)}. && (6.32)
\end{aligned}$$

Finally we obtain an expression for $\|\mathcal{E}_{\mathrm{VSUE}} - \mathcal{F}_{\mathrm{VSUE}}\|_\diamond$ by taking the trace distance between (6.27) and (6.30). Using the triangle inequality to separate the accept and reject contribution, we get

$$\begin{aligned}
&\|\mathcal{E}_{\mathrm{VSUE}} - \mathcal{F}_{\mathrm{VSUE}}\|_\diamond \leq D_{\mathrm{acc}} + D_{\mathrm{rej}} && (6.33)\\
D_{\mathrm{acc}} &= \Pr[\Omega=1] \mathop{\mathbb{E}}_{mu} \mathop{\mathbb{E}}_{bxa} \sum_{sc} 2^{-n} \Big\| \mathop{\mathbb{E}}_{t|bxa} \rho^{\mathrm{E}}_{bxat} \delta_{s,\texttt{Syn}(c\oplus t)} (2^{\ell} \delta_{m,\Phi_u(c\oplus t)} - 1) \Big\|_1 && (6.34)\\
D_{\mathrm{rej}} &= \Pr[\Omega=0] \mathop{\mathbb{E}}_{mu} \mathop{\mathbb{E}}_{ba} \sum_{sc} 2^{-n} \Big\| \mathop{\mathbb{E}}_{t|ba} \rho^{\mathrm{E}}_{bat} \delta_{s,\texttt{Syn}(c\oplus t)} (2^{\ell} \delta_{m,\Phi_u(c\oplus t)} - 1) \Big\|_1. && (6.35)
\end{aligned}$$

Note that a bound $\|\mathcal{E}_{\mathrm{VSUE}} - \mathcal{F}_{\mathrm{VSUE}}\|_\diamond \leq \varepsilon$ implies ε-VSUE and ε-KR.

6.6.2 Main result: distance to ideal

Theorem 6.14. *Let $\mathcal{E}_{\mathrm{VSUE}}$ be the CPTP map according to the protocol of Section 6.4.2, and let $\mathcal{F}_{\mathrm{VSUE}}$ be its idealized version that satisfies 0-VSUE and 0-KR as defined in Defs. 6.3 and 6.4. It holds asymptotically that*

$$\begin{aligned}
&\|\mathcal{E}_{\mathrm{VSUE}} - \mathcal{F}_{\mathrm{VSUE}}\|_\diamond \leq \varepsilon_{\mathrm{acc}} + \varepsilon_{\mathrm{rej}} && (6.36)\\
&\varepsilon_{\mathrm{acc}} = \Pr[\Omega=1] \cdot \min\left[1, \sqrt{2^{\ell-n+nh(1-\frac{3}{2}\beta^*,\frac{\beta^*}{2},\frac{\beta^*}{2},\frac{\beta^*}{2})+nh(1-\frac{3}{2}\gamma^*,\frac{\gamma^*}{2},\frac{\gamma^*}{2},\frac{\gamma^*}{2})+\mathcal{O}(\sqrt{n})}}\right] \\
&\varepsilon_{\mathrm{rej}} = \Pr[\Omega=0] \cdot \min\left[(1, \sqrt{2^{\ell-n+nh(1-\frac{3}{2}\beta^*,\frac{\beta^*}{2},\frac{\beta^*}{2},\frac{\beta^*}{2})+nh(\beta^*\star\gamma^*)+\mathcal{O}(\sqrt{n})}}\right].
\end{aligned}$$

Note that $\Pr[\Omega=1]$ is exponentially small in n when $\beta > \beta*$ and/or $\gamma > \gamma*$. (This follows from e.g. Hoeffding's inequality).

6.6.3 Proof of Theorem 6.14

We start from (6.33) and apply steps 4 till 6 of the proof recipe of Section 2.5. Since D_{acc} and D_{rej} are both defined as a distance between sub-normalized states, we have $D_{\mathrm{acc}} \leq \Pr[\Omega=1]$ and $D_{\mathrm{rej}} \leq \Pr[\Omega=0]$. We note that D_{acc} and D_{rej} are very similar expressions. In order to treat them in one go we introduce the notation 'q' which stands for (b,x,a) in the accept case and for (b,a) in the reject case.

Step 4: we introduce smoothing as in [Ren05], i.e. we consider states $\bar{\rho}$ that are $\sqrt{\varepsilon}$-close to ρ in terms of trace distance. Doing this incurs a penalty $\propto \sqrt{\varepsilon}$ in the diamond norm, but this penalty vanishes asymptotically. After these steps we can write the smoothened version of D_{acc},D_{rej} both in the form $\Pr[\Omega = 0/1]\bar{D}$.

$$\bar{D} \stackrel{\text{def}}{=} \mathop{\mathbb{E}}_{muscq} 2^{n-\kappa} \Big\| \mathop{\mathbb{E}}_{t|q} \bar{\rho}^{\text{E}}_{qt} \delta_{s,\texttt{Syn}(c\oplus t)} (2^{\ell}\delta_{m,\Phi_u(c\oplus t)} - 1) \Big\|_1 . \tag{6.37}$$

Here we have written, in slight abuse of notation, $\mathbb{E}_s(\cdots) = 2^{\kappa-n}\sum_s(\cdots)$ and $\mathbb{E}_c(\cdots) = 2^{-n}\sum_c(\cdots)$. We derive an upper bound on $\bar{D}$ using steps that are very similar to the derivation in 6-state QKD of Section 2.6 and the Leftover Hash Lemma [TSSR11]. We rewrite the 1-norm as the trace over a square root. Then we use Jensen's inequality to 'pull' the $\mathbb{E}_u$, $\mathbb{E}_q$ and $\mathbb{E}_s$ expectation into the square root. Next we exploit the pairwise independence property of the hash function Φ, yielding a result that can be formulated in terms of smooth Rényi entropies S_0^{ε} and S_2^{ε} using Lemma 2.19. Finally we substitute the factorised form of Eve's state due to Postselection (step 5) and make use of the limiting behavior of Lemma 2.1 to obtain von Neumann entropies.

$$\begin{aligned}
\bar{D} &= \mathop{\mathbb{E}}_{muscq} 2^{n-\kappa} \text{tr} \Big\{ \mathop{\mathbb{E}}_{t|q} \mathop{\mathbb{E}}_{t'|q} \bar{\rho}^{\text{E}}_{qt} \bar{\rho}^{\text{E}}_{qt'} \delta_{s,\texttt{Syn}(c\oplus t)} \delta_{s,\texttt{Syn}(c\oplus t')} && (6.38)\\
&\quad (2^{\ell}\delta_{m,\Phi_u(c\oplus t)} - 1)(2^{\ell}\delta_{m,\Phi_u(c\oplus t')} - 1) \Big\}^{\frac{1}{2}} \\
&\overset{\text{Jensen}}{\leq} \mathop{\mathbb{E}}_{mcq} 2^{n-\kappa} \text{tr} \Big\{ \mathop{\mathbb{E}}_{us} \mathop{\mathbb{E}}_{tt'|q} \bar{\rho}^{\text{E}}_{qt} \bar{\rho}^{\text{E}}_{qt'} \delta_{s,\texttt{Syn}(c\oplus t)} \delta_{s,\texttt{Syn}(c\oplus t')} && (6.39)\\
&\quad \big[2^{2\ell}\delta_{m,\Phi_u(c\oplus t)}\delta_{m,\Phi_u(c\oplus t')} - 2^{\ell}\delta_{m,\Phi_u(c\oplus t)} - 2^{\ell}\delta_{m,\Phi_u(c\oplus t')} + 1 \big] \Big\}^{\frac{1}{2}} \\
&\overset{\text{pair.indep.}}{=} \mathop{\mathbb{E}}_{mcq} 2^{n-\kappa} \text{tr} \sqrt{ \mathop{\mathbb{E}}_{tt'|q} \bar{\rho}_{qt}\bar{\rho}_{qt'} [\mathop{\mathbb{E}}_{s} \delta_{s,\texttt{Syn}(c\oplus t)}\delta_{s,\texttt{Syn}(c\oplus t')}] 2^{\ell}\delta_{tt'} } && (6.40)\\
&= \sqrt{2^{n-\kappa}} \mathop{\mathbb{E}}_{q} \text{tr} \sqrt{ \mathop{\mathbb{E}}_{tt'|q} \bar{\rho}^{\text{E}}_{qt}\bar{\rho}^{\text{E}}_{qt'} 2^{\ell}\delta_{tt'} } && (6.41)\\
&\overset{\text{Jensen}}{\leq} \sqrt{ |\mathcal{Q}|\, 2^{n-\kappa+\ell} \mathop{\mathbb{E}}_{qq'tt'} \delta_{qq'}\delta_{tt'} \bar{\rho}^{\text{E}}_{qt}\bar{\rho}^{\text{E}}_{q't'} } && (6.42)\\
&\overset{\text{Lemma 2.19}}{\leq} \sqrt{ |\mathcal{Q}|\, 2^{n-\kappa+\ell} 2^{S_0^{\varepsilon}(\rho^E) - S_2^{\varepsilon}(\rho^{QTE})} } && (6.43)\\
&\overset{\text{postselection}}{=} \sqrt{ |\mathcal{Q}|\, 2^{n-\kappa+\ell} 2^{S_0^{\varepsilon}([\sigma^{\text{E}}]^{\otimes n}) - S_2^{\varepsilon}([\sigma^{QTE}]^{\otimes n})} } && (6.44)\\
&\overset{\text{Lemma 2.1}}{\to} \sqrt{ |\mathcal{Q}|\, 2^{n-\kappa+\ell}\, 2^{nS(\sigma^{\text{E}}) - nS(\sigma^{QTE}) + \mathcal{O}(\sqrt{n})} }. && (6.45)
\end{aligned}$$

In (6.40) we used $\mathbb{E}_u\, \delta_{m,\Phi_u(\cdots)} = 2^{-\ell}$ and $\mathbb{E}_u\, 2^{2\ell}\delta_{m,\Phi_u(c\oplus t)}\delta_{m,\Phi_u(c\oplus t')} = 2^{\ell}\delta_{tt'} + (1 - \delta_{tt'})$. We used Lemma 2.19 with $\mathcal{X} = \mathcal{Q}$. In (6.45) the σ^{E} and σ^{QTE} are given by

$$\sigma^{\text{E}} = \mathop{\mathbb{E}}_{bxyat} \sigma^{\text{E}}_{bxyat} \quad ; \quad \sigma^{QTE} = \mathop{\mathbb{E}}_{qt} |qt\rangle\langle qt| \otimes \sigma^{\text{E}}_{qt}, \tag{6.46}$$

with $\sigma^{\text{E}}_{bxat} = \mathbb{E}_{y|bxat}\, \sigma^{\text{E}}_{bxyat}$ and $\sigma^{\text{E}}_{bat} = \mathbb{E}_{xy|bat}\, \sigma^{\text{E}}_{bxyat}$. We have $S(\sigma^{QTE}) = \mathsf{H}(QT) + \mathbb{E}_{qt}\, S(\sigma^{\text{E}}_{qt})$. Step 6: we use the simple form of Eve's state discussed in Section 6.5 to

compute the relevant entropies. From Lemma 6.12 we know that the eigenvalues of $\sigma^{\mathrm{E}}_{bxat}$ do not depend on $bxat$ in the accept case (which is exactly the case at hand). Similarly, from Lemma 6.13 we see that the eigenvalues of $\sigma^{\mathrm{E}}_{bat}$ do not depend on bat. Hence we can write $\mathbb{E}_{qt}\, S(\sigma^{\mathrm{E}}_{qt}) = S(\sigma^{\mathrm{E}}_{qt})$ where in the last expression the q and t have arbitrary values. Furthermore, from Corollary 6.10 we get $\mathsf{H}(BXAT) = 4$ and $\mathsf{H}(BAT) = 3$. Asymptotically it holds that $n - \kappa \to nh(\beta^* \star \gamma^*)$, since the error correcting code is designed to deal with bit error rate $\beta^* \star \gamma^*$, which results from the serial concatenation of noisy channels with error probability β^* and γ^*. Substitution into (6.45) gives the following asymptotic result

$$D_{\mathrm{acc}} \leq \Pr[\Omega = 1]\sqrt{2^{\ell - n + nh(\beta^* \star \gamma^*)} 2^{nS(\sigma^{\mathrm{E}}_{\omega=1}) - nS(\sigma^{\mathrm{E}}_{bxat,\omega=1}) + \mathcal{O}(\sqrt{n})}} \tag{6.47}$$

$$D_{\mathrm{rej}} \leq \Pr[\Omega = 0]\sqrt{2^{\ell - n + nh(\beta^* \star \gamma^*)} 2^{nS(\sigma^{\mathrm{E}}) - nS(\sigma^{\mathrm{E}}_{bat}) + \mathcal{O}(\sqrt{n})}}. \tag{6.48}$$

Accept case. From Lemma 6.8 it follows that $S(\sigma^{\mathrm{E}}_{\omega=1}) = h(1 - \frac{3}{2}\beta, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}) + h(1 - \frac{3}{2}\gamma, \frac{\gamma}{2}, \frac{\gamma}{2}, \frac{\gamma}{2})$. From Lemma 6.12 we get $S(\sigma^{\mathrm{E}}_{bxat,\omega=1}) = h(\beta \star \gamma)$. In the accept case we know that $\beta \leq \beta^*$, $\gamma \leq \gamma^*$. Substitution of these von Neumann entropies into (6.47) yields (6.37).

Reject case. From Lemma 6.13 we have

$$S(\sigma^{\mathrm{E}}) - S(\sigma^{\mathrm{E}}_{bat}) = \sum_{a_1 b_1 a_2 b_2} \nu^{a_1 b_1}_{a_2 b_2} \log \frac{1}{\nu^{a_1 b_1}_{a_2 b_2}} + \sum_{uv} \Lambda_{uv} \log \Lambda_{uv}. \tag{6.49}$$

We need to upper bound this expression under the four constraints specified in Lemma 6.7. We use Lagrange optimization, with constraint multipliers $\mu_{a_1 b_1}$. The Lagrangian is

$$\mathcal{L} = \sum_{\substack{a_1 b_1 \\ a_2 b_2}} \nu^{a_1 b_1}_{a_2 b_2} \ln \frac{1}{\nu^{a_1 b_1}_{a_2 b_2}} + \sum_{uv} \Lambda_{uv} \ln \Lambda_{uv} + \sum_{a_1 b_1} \mu_{a_1 b_1} \Big(\sum_{a_2 b_2} \nu^{a_1 b_1}_{a_2 b_2} - \frac{\beta}{2} - \delta^{a_1, b_1}_{0,0}(1 - 2\beta) \Big). \tag{6.50}$$

Computing the derivatives with respect to the ν-parameters, and setting these derivatives to zero yields, after some algebra,

$$\nu^{a_1 b_1}_{a_2 b_2} = \Lambda_{a_1 \oplus a_2, b_1 \oplus b_2} \exp \mu_{a_1 b_1}. \tag{6.51}$$

Summing (6.51) over a_2, b_2 and using the constraints of Lemma 6.7 we solve for $\mu_{a_1 b_1}$ and find $\exp \mu_{a_1 b_1} = \frac{\beta}{2} + \delta^{a_1, b_1}_{0,0}(1 - 2\beta)$. Substituting this back into (6.51) and using the definition of Λ (6.24) we get a system of linear equations,

$$\nu^{a_1 b_1}_{a_2 b_2} = \left[\frac{\beta}{2} + \delta^{a_1, b_1}_{0,0}(1 - 2\beta) \right] \sum_{k\ell} \nu^{k\ell}_{k \oplus a_1 \oplus a_2, \ell \oplus b_1 \oplus b_2}. \tag{6.52}$$

The solution is $\nu^{01}_{u\bar{v}} = \nu^{10}_{\bar{u}v} = \nu^{11}_{\bar{u}\bar{v}} = \nu^{00}_{uv} \frac{\beta/2}{1 - 3\beta/2} \wedge \sum_{uv} \nu^{00}_{uv} = 1 - \frac{3}{2}\beta$. Then the simple relation $\Lambda_{uv} = (1 - \frac{3}{2}\beta)^{-1} \nu^{00}_{uv}$ holds. This solution does not entirely fix all the parameters (three degrees of freedom are still open), but it does entirely fix (6.49),

$$S(\sigma^{\mathrm{E}}) - S(\sigma^{\mathrm{E}}_{bat}) \leq h(1 - \frac{3}{2}\beta, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2}). \tag{6.53}$$

Because of the succeeded CheckA we have $\beta \leq \beta^*$. Finally, substitution of (6.53) with $\beta \leq \beta^*$ into (6.48) yields (6.37). □

Remark: An alternative way of deriving the reject case result (6.53) would have been to consider a modification to the original protocol where Eve receives the basis choice b just before Alice sends qubits. Eve can then measure $y = x \oplus t$ with perfect accuracy. What remains for Eve is get information about x from her 4-dimensional ancilla state. This is exactly the six-state QKD analysis.

6.6.4 Achievable asymptotic rate

Theorem 6.14 tells us how the length ℓ must be set so as to ensure an exponentially small diamond distance $\|\mathcal{E}_{\rm VSUE} - \mathcal{F}_{\rm VSUE}\|_\diamond$,

$$\ell \leq n - nh(1-\frac{3}{2}\beta^*, \frac{\beta^*}{2}, \frac{\beta^*}{2}, \frac{\beta^*}{2}) - n \max\Big(h(\beta^* \star \gamma^*),\ h(1-\frac{3}{2}\gamma^*, \frac{\gamma^*}{2}, \frac{\gamma^*}{2}, \frac{\gamma^*}{2})\Big). \quad (6.54)$$

When γ^* is close to β^*, the second term in the max() is dominant. From this point on we set $\gamma^* = \beta^*$. The requirement on ℓ becomes

$$\text{In case } \gamma^* = \beta^* : \quad \ell \leq n - 2nh(1 - \frac{3}{2}\beta^*, \frac{\beta^*}{2}, \frac{\beta^*}{2}, \frac{\beta^*}{2}). \quad (6.55)$$

The rate of a scheme is the length of the actual message sent, divided by the expended number of qubits. Our scheme transmits a string of length ℓ while expending $n + \nu$ qubits, with $\nu \ll n$. However, that is not the whole story, since the single-use keys $k_{\rm syn}, k_{\rm test}, \mathcal{I}_{\rm test}, b^{1,2}_{\rm test}, \xi, \eta$ need to be refreshed somehow. Of these keys, $k_{\rm syn}$ has length $nh(\beta^* \star \beta^*)$ while the others are at most of order $\log n$. One way of refreshing the keys is to send them as part of the message m. This reduces the actual message size from ℓ to $\ell - nh(\beta^* \star \beta^*)$, which results in the following rate,

$$\text{Refresh through VSUE : rate} = 1 - 2h(1 - \frac{3}{2}\beta^*, \frac{\beta^*}{2}, \frac{\beta^*}{2}, \frac{\beta^*}{2}) - h(\beta^* \star \beta^*). \quad (6.56)$$

As we saw in Chapter 5, using an unclonable scheme like VSUE to transport the single-use keys is overkill, since they are assumed to leak afterward. It is much more efficient to do the refresh via QKD (or QKR). The rate of six-state QKD is $R_{\rm QKD} = 1 - h(1 - \frac{3}{2}\beta^*, \frac{\beta^*}{2}, \frac{\beta^*}{2}, \frac{\beta^*}{2})$; the number of qubits spent on transporting $nh(\beta^* \star \beta^*)$ bits is $N_{\rm QKD} = nh(\beta^* \star \beta^*)/R_{\rm QKD}$; the rate is $\ell/(n + N_{\rm QKD})$,

$$\text{Refresh by 6-state QKD : rate} = \frac{(1-2J)(1-J)}{1 - J + h(\beta^* \star \beta^*)},\ J \stackrel{\rm def}{=} h(1 - \frac{3}{2}\beta^*, \frac{\beta^*}{2}, \frac{\beta^*}{2}, \frac{\beta^*}{2}). \quad (6.57)$$

The rates (6.56,6.57) are plotted in Figure 6.3. Key update via QKD is clearly the best option. Note that these rates are significantly lower than what can be achieved with a UE scheme that uses the quantum channel in a single direction (see Chapter 5). In UE a positive rate is possible up to $\beta \approx 0.12$.

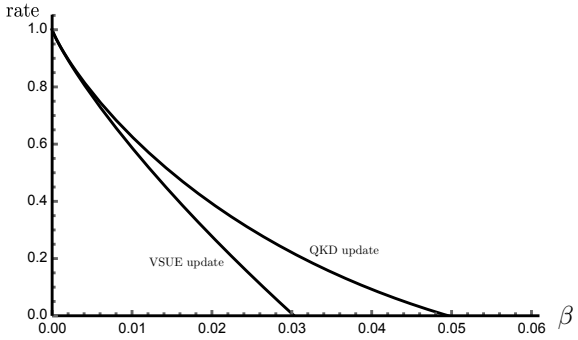

Figure 6.3: *Communication rate of our scheme with two different ways to update the single-use keys: through VSUE itself and via 6-state QKD. The bit error rate on all channels is taken to be β.*

6.7 Two-way Quantum Key Distribution

Our VSUE scheme can be modified such that it becomes a QKD scheme with two-way use of the quantum channel, like [BLMR13]. The modifications with respect to Section 6.3.3 are as follows.
(i) The message m is replaced by a uniform random string, which serves as the QKD key.
(ii) Alice chooses u. (It is no longer a shared key). Bob confirms that he has received the qubits. Then Alice reveals u.
(iii) The syndrome s is sent in the clear, together with u. k_{syn} does not exist.
(iv) The keys $b, k_{\text{test}}, \mathcal{I}_{\text{test}}, b^1_{\text{test}}, b^2_{\text{test}}, \xi, \eta$ are kept secret forever.

The quantity to be upperbounded is $D_{\text{QKD}} = \|\rho^{MUSACE}_{\texttt{accept}} - \rho^M \otimes \rho^{USACE}_{\texttt{accept}}\|_1$, since only the message needs to be kept safe, and it is only endangered in case of accept. Following the same steps as in Section 6.6.3 we find

$$D_{\text{QKD}} = \Pr[\Omega=1] 2^{-n} \mathop{\mathbb{E}}_{mua} \sum_{sc} \Big\| \mathop{\mathbb{E}}_{t|a} \rho^{\text{E}}_{at} \delta_{s,\texttt{syn}(c\oplus t)} (2^\ell \delta_{m,\Phi_u(c\oplus t)} - 1) \Big\|_1 \tag{6.58}$$

$$\leq \Pr[\Omega=1] \cdot \min\left(1, \sqrt{2^{\ell-n+nh(\beta\star\gamma)} 2^{nS(\sigma^{\text{E}}_{\omega=1}) - nS(\sigma^{\text{E}}_{at,\omega=1}) + \mathcal{O}(\sqrt{n})}}\right). \tag{6.59}$$

From Lemma 6.8 we get $S(\sigma^{\text{E}}_{\omega=1}) = J_\beta + J_\gamma$, where we use shorthand notation $J_\beta \stackrel{\text{def}}{=} h(1-\frac{3}{2}\beta, \frac{\beta}{2}, \frac{\beta}{2}, \frac{\beta}{2})$. Furthermore, substitution of Lemma 6.8 into Lemma 6.13 shows that the eigenvalues of $\sigma^{\text{E}}_{at,\omega=1}$ are $\Lambda_{01} = \Lambda_{10} = \Lambda_{11} = \frac{1}{2}\beta \star \gamma$ and $\Lambda_{00} = 1 - \frac{3}{2}\beta \star \gamma$, which yields $S(\sigma^{\text{E}}_{at,\omega=1}) = J_{\beta\star\gamma}$. Hence we obtain

$$D_{\text{QKD}} \leq \Pr[\Omega=1] \cdot \min\left(1, \sqrt{2^{\ell-n+nh(\beta\star\gamma)} 2^{nJ_\beta + nJ_\gamma - nJ_{\beta\star\gamma} + \mathcal{O}(\sqrt{n})}}\right). \tag{6.60}$$

From (6.60) we see that ℓ has to be chosen as $\ell \leq n - nh(\beta\star\gamma) - nJ_\beta - nJ_\gamma + nJ_{\beta\star\gamma}$. The corresponding rate is

$$\text{Key rate} = 1 - h(\beta\star\gamma) - J_\beta - J_\gamma + J_{\beta\star\gamma}. \tag{6.61}$$

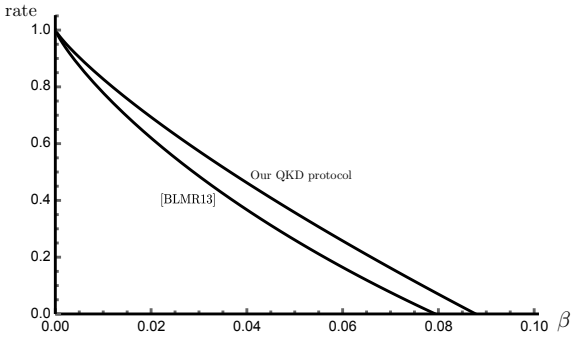

Figure 6.4: *Asymptotic key rate of two-way QKD as a function of the bit error rate β on the quantum channels. (The error rate of the two channels is set to be equal.) Upper curve: our result (6.61). Lower curve: [BLMR13].*

Note that now there is no additional penalty from a syndrome mask, since the syndrome is sent in the clear.

The authors of [BLMR13] used an entropic uncertainty relation to prove achievable rate $1-h(\beta\star\gamma)-\min\big(h(\beta),h(\gamma)\big)$ for LM05, in the case of independent channel noise. To our knowledge that is the best known rate so far for a two-way version of QKD. Our proof yields a higher rate (6.61) when γ is close to β. Figure 6.4 shows a comparison of the rates for $\beta=\gamma$. This rate improvement could be due to the 6-state channel monitoring in combination with a proof technique similar to [Ren05] which is able to exploit that kind of monitoring.

6.8 Discussion

We have constructed an Unclonable Encryption scheme with the additional property that even after a reject Alice is allowed to leak all her keys. The price we pay for having VSUE, as compared to merely UE, is a lower rate when there is channel noise; this is due to the accumulation of noise from two channel uses instead of one.

The size of the shared keys is $2n+nh(\beta\star\gamma)+\mathcal{O}(\log n)$, where $u\in\{0,1\}^{2n}$ is re-usable and all the other keys have to be refreshed. The optimal way to refresh is to use 6-state QKD. The key $k_{\text{syn}}\in\{0,1\}^{nh(\beta\star\gamma)}$ causes the main burden here. It would be interesting to see if alternative ways of handling the leakage from error correction, such as [DPS05], can help to improve the rate. This is left for future work.

We have used a proof technique with post-selection and random Pauli operators because this technique allows us to prove a higher rate than techniques based on entropic inequalities. A slight disadvantage of this technique is that three-basis channel monitoring must become part of the protocol.

Our attacker model assumes that the noise on Channels 1 and 2 is independent. In some circumstances it may be argued that the noise is *dependent* [BLMR13], making it possible to achieve higher rates. This is left as a topic for future work.

Finally we mention that schemes in which a message is encoded directly into qubits are very sensitive to particle loss (erasures). In our protocol, erasures in Channel 1 are harmless since Alice can ignore the erased positions. Erasures in Channel 2 however are problematic; they force Alice and Bob to adapt their error-correcting code to cope with erasures, which is costly. A naive attempt to fix the problem would be to let Bob report erasure locations before Alice computes μ. However, that would force Alice as well as Bob to wait for a response from the other party. According to the attacker model, some of their variables would then become long-term secrets and the VSUE property would be lost.

6.9 From qubits to qudits

In this chapter we have seen that two passes over a quantum channel allows security in the scenario where one of the two communicating parties is in a sense vulnerable compared to the other. Due to the double-pass of the qubits involved, Eve has a stronger attack compared to single-pass protocols. This causes us to pay a price in the rate of the protocol as a function of noise compared to single-pass protocols, see Chapters 2 till 5. If the noise exceeds a threshold, these protocols no longer have a positive rate, i.e. it becomes impossible to use them.

In the next chapter we will consider a protocol that is particularly useful for communication over very noisy channels. So far we have been using qubits, i.e. 2-dimensional quantum states. We will see that by sending higher dimensional quantum states, called qudits, it becomes harder for Eve to learn all the details of the quantum state. This increased difficulty can be exploited to construct QKD schemes that have a positive rate over a larger interval of the noise parameter β.

Appendix

6.A Proof of Lemma 6.9: Eve's sub-normalized pure state

We write out $|\bar{\psi}^{\mathrm{E}}_{bxyat}\rangle$ as follows,

$$
\begin{aligned}
|\bar{\psi}^{\mathrm{E}}_{bxyat}\rangle &= \langle\phi_{bxyat}|\psi^{\mathrm{ABE}}\rangle && (6.62)\\
&= \frac{1}{\sqrt{2}}\sum_{pa_1b_1a_2b_2}\langle p|\langle\psi^b_x|\langle p|\langle\psi^b_y|(\mathbb{1}_2\otimes\sigma_x^{a_1}\sigma_z^{b_1}\otimes\sigma_z^{t\oplus a}\sigma_x^t\otimes\sigma_x^{a_2}\sigma_z^{b_2}\otimes\mathbb{1}_{16})\\
&\quad\sqrt{\nu^{a_1b_1}_{a_2b_2}}|\Phi_{00}\rangle|\Phi_{00}\rangle|e^{a_1b_1}_{a_2b_2}\rangle && (6.63)\\
&= \frac{1}{2\sqrt{2}}\sum_{pqa_1b_1a_2b_2}\sqrt{\nu^{a_1b_1}_{a_2b_2}}\langle\psi^b_x|\sigma_x^{a_1}\sigma_z^{b_1}|p\rangle\langle p|\sigma_z^{t\oplus a}\sigma_x^t|q\rangle\langle\psi^b_y|\sigma_x^{a_2}\sigma_z^{b_2}|q\rangle|e^{a_1b_1}_{a_2b_2}\rangle && (6.64)\\
&= \frac{1}{2\sqrt{2}}\sum_{\substack{a_1b_1a_2b_2\\pq}}\sqrt{\nu^{a_1b_1}_{a_2b_2}}(-1)^{b_1p+b_2q}\big[\delta_{b0}\delta_{x,p\oplus a_1}\delta_{y,q\oplus a_2}+\\
&\quad\frac{\delta_{b1}}{2}(-1)^{x(p\oplus a_1)+y(q\oplus a_2)}\big]\big[\delta_{p0}\delta_{tq}+(-1)^{a\oplus t}\delta_{t\bar{q}}\delta_{p1}\big]|e^{a_1b_1}_{a_2b_2}\rangle && (6.65)\\
&= \frac{1}{2\sqrt{2}}\sum_{a_1b_1a_2b_2}\sqrt{\nu^{a_1b_1}_{a_2b_2}}(-1)^{b_2t}\Big[\delta_{b0}\big(\delta_{xa_1}\delta_{y\oplus t,a_2}+(-1)^{b_1+b_2+a+t}\delta_{x\bar{a}_1}\delta_{y\oplus t,\bar{a}_2}\big)\\
&\quad+\frac{\delta_{b1}}{2}(-1)^{xa_1+y(t+a_2)}\big(1+(-1)^{b_1+b_2+x+y+a+t}\big)\Big]|e^{a_1b_1}_{a_2b_2}\rangle && (6.66)\\
&= \frac{1}{2\sqrt{2}}\sum_{a_1b_1a_2b_2}\sqrt{\nu^{a_1b_1}_{a_2b_2}}(-1)^{b_2t}\Big[\bar{b}\delta_{x\oplus y\oplus t,a_1\oplus a_2}\\
&\quad(-1)^{(b_1+b_2+a+t)(a_1+x)}+b(-1)^{xa_1+y(t+a_2)}\delta_{b_1\oplus b_2,x\oplus y\oplus a\oplus t}\Big]|e^{a_1b_1}_{a_2b_2}\rangle && (6.67)
\end{aligned}
$$

where the last line is the claim. □

6.B Proof of Lemma 6.13

We have $\sigma^{\mathrm{E}}_{bat}=\sum_{xy}\Pr[xy|bat]\sigma^{\mathrm{E}}_{bxyat}=\sum_{xy}\frac{\Pr[xyat|b]}{\Pr[at|b]}\sigma^{\mathrm{E}}_{bxyat}=4\sum_{xy}|\bar{\psi}^{\mathrm{E}}_{bxyat}\rangle\langle\bar{\psi}^{\mathrm{E}}_{bxyat}|$. Next we check that the given $|V^{at}_{uv}\rangle$ are indeed eigenvectors. Keeping track of the phases we get:

$$
\begin{aligned}
\langle\bar{\psi}^{E}_{bxyat}|V^{at}_{uv}\rangle &= \frac{1}{2\sqrt{2}}\sum_{k\ell}\nu^{k,\ell}_{k\oplus u,\ell\oplus v}(-1)^{(a+v)\bar{k}+(k+v)t} && (6.68)\\
&\quad\big[\bar{b}\delta_{x\oplus y\oplus t,u}(-1)^{(v+a+t)(k+x)}+b\delta_{x\oplus y\oplus a\oplus t,v}(-1)^{xk+(t+k+u)y}\big]
\end{aligned}
$$

$$\sigma^E_{bat}|V^{at}_{uv}\rangle = \frac{1}{2}\sum_{xyk\ell}\sum_{a_1b_1a_2b_2} \nu^{k,\ell}_{k\oplus u,\ell\oplus v}\sqrt{\nu^{a_1b_1}_{a_2b_2}}|e^{a_1b_1}_{a_2b_2}\rangle(-1)^{(a+v)\bar{k}+(k+v+b_2)t}$$
$$\big[\bar{b}\delta_{x\oplus y\oplus t,u}\delta_{u,a_1\oplus a_2}(-1)^{(v+a+t)(k+x)+(b_1+b_2+a+t)(a_1+x)}$$
$$+b\delta_{x\oplus y\oplus a\oplus t,v}\delta_{v,b_1\oplus b_2}(-1)^{xk+(t+k+u)y+xa_1+(t+a_2)y}\big] \tag{6.69}$$
$$= \frac{1}{2}\sum_{k\ell}\sum_{a_1b_1a_2b_2} \nu^{k,\ell}_{k\oplus u,\ell\oplus v}\sqrt{\nu^{a_1b_1}_{a_2b_2}}|e^{a_1b_1}_{a_2b_2}\rangle(-1)^{(a+v)\bar{k}+(k+v+b_2)t}$$
$$\big[\bar{b}\delta_{u,a_1\oplus a_2}(-1)^{(v+a+t)k+(b_1+b_2+a+t)a_1}\sum_x(-1)^{(v+b_1+b_2)x}$$
$$+b\delta_{v,b_1\oplus b_2}(-1)^{(a+t+v)k+(a+t+v)a_1}\sum_y(-1)^{(a_1+a_2+u)y}\big] \tag{6.70}$$
$$= \sum_{k\ell}\sum_{a_1b_1} \nu^{k,\ell}_{k\oplus u,\ell\oplus v}\sqrt{\nu^{a_1b_1}_{a_1\oplus u,b_1\oplus v}}|e^{a_1b_1}_{a_1\oplus u,b_1\oplus v}\rangle(-1)^{(a+v)\bar{k}+(k+b_1)t}$$
$$\big[\bar{b}(-1)^{(v+a+t)k+(v+a+t)a_1}+b(-1)^{(a+t+v)k+(a+t+v)a_1}\big] \tag{6.71}$$
$$= \sum_{k\ell}\nu^{k,\ell}_{k\oplus u,\ell\oplus v}\sum_{a_1b_1}\sqrt{\nu^{a_1b_1}_{a_1\oplus u,b_1\oplus v}}|e^{a_1b_1}_{a_1\oplus u,b_1\oplus v}\rangle(-1)^{(a+v)\bar{a}_1+(a_1+b_1)t}. \tag{6.72}$$

We recognize $\Lambda_{uv}|V^{at}_{uv}\rangle$ with renamed summation variables.

Chapter 7
Round robin differential phase shift quantum key distribution

Dealing with more noise
Luckily for Alice, things start to cool down in the neighborhood of her lab. The nerable sender unclonable encryption scheme gave them confidence in their confidential communication during a tough time. For some reason though, after all the unrest, the amount of noise Alice and Bob detect on their quantum channel has increased. They decide that they need a protocol that can deal with more noise than the protocols used up to this point. Luckily such a scheme already exists. Round robin differential phase shift quantum key distribution uses higher dimensional quantum states than the qubits Alice and Bob used up to this point. This makes it harder for Eve to learn anything relevant from the states. In fact, the protocol does not even require channel monitoring. But Alice and Bob are interested in efficient communication. Can the rate of the protocol be increased by adding channel monitoring to the protocol and taking this into account in the security proof?

7.1 Introduction

7.1.1 Round robin differential phase shift quantum key distribution

In 2014, Sasaki, Yamamoto and Koashi introduced *Round-Robin Differential Phase-Shift* (RRDPS) [SYK14], a QKD scheme based on d-dimensional qudits. It has the advantage that it is very noise resilient while being easy to implement using photon pulse trains and interference measurements. One of the interesting aspects of RRDPS is that it is possible to omit the monitoring of signal disturbance. Even at high disturbance, Eve can obtain little information I_{AE} about Alice's secret bit. The value of I_{AE} determines how much privacy amplification is needed. The maximum possible QKD rate (the number of actual key bits conveyed per quantum state) is

This chapter is based on [LŠ19c]. A factor 2 omission in the paper, regarding the post-selection penalty, has been corrected (Figures 7.6 and 7.7).

$1 - h(\beta) - I_{\mathrm{AE}}$, where the binary entropy function is due to the error correction. Monitoring of signal disturbance induces a small penalty on the QKD rate. However, the number of qubits that needs to be discarded is only logarithmic in the length of the derived key [Lo05].

7.1.2 Prior work on the security of RRDPS

The security of RRDPS has been discussed in a number of papers [SYK14, ZYCM17, SK17, Ško17]. The original RRDPS paper gives an asymptotic upper bound for the leakage,

$$I_{\mathrm{AE}} \leq h(\frac{1}{d-1}) \tag{7.1}$$

(Eq. 5 in [SYK14] with photon number set to 1). The security analysis in [SYK14] is based on the Shor-Preskill proof technique [SP00] and an estimate of the phase error. It is not known how tight the bound (7.1) is. Reference [ZYCM17] follows [SYK14] and does a more accurate computation of phase error rate, tightening the $1/(d-1)$ in (7.1) to $1/d$. In [SK17] Sasaki and Koashi add noise-dependence to their analysis and claim a bound

$$I_{\mathrm{AE}} \leq h(\frac{2\beta}{d-2}) \qquad \text{for } \beta \leq \frac{1}{2} \cdot \frac{d-2}{d-1} \tag{7.2}$$

and $I_{\mathrm{AE}} \leq h(\frac{1}{d-1})$ for $\beta \in [\frac{1}{2} \cdot \frac{d-2}{d-1}, \frac{1}{2}]$. (See Section 7.14.2). The analysis in [Ško17] considers only intercept-resend attacks, and hence puts a *lower bound* on Eve's potential knowledge, $I_{\mathrm{AE}} \geq 1 - h(\frac{1}{2} + \frac{1}{d}) = \mathcal{O}(1/d^2)$.[1]

7.1.3 Contributions to round robin differential phase shift QKD

Using the proof method of Chapter 2, we will give a bound on the leakage I_{AE}, which leads to a bound on the achievable rate as a function of β. The result is composable, since the proof technique is based on the diamond norm. We consider the case where Alice and Bob *do monitor the channel* (i.e. they are able to tune the amount of privacy amplification as a function of the observed bit error rate) as well as the saturated regime where the leakage does not depend on the amount of noise.

- We describe a version of RRDPS that contains channel monitoring.
- We show that the RRDPS protocol is equivalent to a protocol that contains an additional randomisation step by Alice and Bob. The randomization consists of phase flips, a permutation of the basis states and permutation of the qudits. We construct an EPR variant of RRDPS-with-randomization. Different from the qubit case, Alice measures half of a d^2-dimensional quantum system, which is equivalent to preparing a d-dimensional qudit. The effect of the randomization is that Alice and Bob's entangled state is symmetrized and can be described using just three real degrees of freedom. Eve holds the purification of this state.

[1] Ref. [Ško17] gives a min-entropy of $-\log(\frac{1}{2} + \frac{1}{d})$, which translates to Shannon entropy $h(\frac{1}{2} + \frac{1}{d})$.

- We derive the required amount of privacy amplification in the *finite size* regime. Additionally we compute the relevant von Neumann entropies following from step 6 of the proof recipe of Chapter 2. This provides a bound on the leakage in the *asymptotic* (long key) regime. Our asymptotic result is tighter than [SYK14] for all values of d and β. Our non-asymptotic result is tighter than [SYK14] for low d.

- We provide a number of additional results by way of supplementary information. (i) We show that Eve's ancilla coupling can be written as a unitary operation on the Bob-Eve system. This shows how Eve's optimal attack can be executed even if she has no access to Alice's qudit. (ii) We compute the min-entropy of one secret bit given the corresponding ancilla. (iii) We compute the accessible information (mutual Shannon entropy) of one secret bit given the corresponding ancilla. The min-entropy and accessible-information results are relevant for collective attacks.

7.2 RRDPS QKD description and security intuition

7.2.1 The RRDPS scheme in a nutshell

The dimension of the qudit space is d. The basis states[2] are denoted as $|t\rangle$, with time indices $t \in \{0, \ldots, d-1\}$. Whenever we use notation "$t_1 + t_2$" it should be understood that the addition of time indices is modulo d. The RRDPS scheme consists of the following steps.

1. Alice generates a random bitstring $a \in \{0,1\}^d$. She prepares the single-photon state
$$|\mu_a\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} (-1)^{a_t} |t\rangle \tag{7.3}$$
and sends it to Bob.

2. Bob chooses a random integer $r \in \{1, \ldots, d-1\}$. Bob performs a POVM measurement $\mathcal{M}^{(r)}$ described by a set of $2d$ operators $(M_{ks}^{(r)})_{k \in \{0,\ldots,d-1\}, s \in \{0,1\}}$,
$$M_{ks}^{(r)} = \frac{1}{2} |\Psi_{ks}^{(r)}\rangle\langle\Psi_{ks}^{(r)}| \qquad\qquad |\Psi_{ks}^{(r)}\rangle = \frac{|k\rangle + (-1)^s |k+r\rangle}{\sqrt{2}}. \tag{7.4}$$
The result of the measurement $\mathcal{M}^{(r)}$ on $|\mu_a\rangle$ is an random integer $k \in \{0, \ldots, d-1\}$ and a bit $s = a_k \oplus a_{k+r}$.[3]

3. Bob announces k and r over a public but authenticated channel. Alice computes $s = a_k \oplus a_{k+r}$. Alice and Bob now have a shared secret bit s.

[2] The physical implementation [SYK14] is a *pulse train*: a photon is split into d coherent pieces which are released at different, equally spaced, points in time.

[3] The phase $(-1)^{a_k \oplus a_{k+r}}$ is the phase of the field oscillation in the $(k+r)$'th pulse relative to the k'th. The measurement $\mathcal{M}^{(r)}$ is an interference measurement where one path is delayed by r time units.

This procedure is repeated multiple times. Finally, on the remaining bits Alice and Bob carry out the standard procedures of information reconciliation and privacy amplification.

In the original scheme [SYK14], Alice and Bob do not monitor the noise on the channel. Instead they perform the amount of privacy amplification corresponding to the maximum noise on the channel ($\beta = \frac{1}{2}$). Note that Alice and Bob do require some bound on the channel noise in order to perform error correction. We will consider a modified version of the original RRDPS QKD scheme that includes channel noise monitoring. This allows us to give a relatively simple description of the d^2 dimensional state held by Eve.

7.2.2 Security intuition

The security of RRDPS is intuitively understood as follows. A measurement in a d-dimensional space cannot extract more than $\log d$ bits of information. The state $|\mu_a\rangle$, however, contains $d-1$ bits of information, which is a lot more than $\log d$. Eve can learn only a fraction of the string a embedded in the qudit. Furthermore, what information she has is of limited use, because she cannot force Bob to select specific phases. (i) She cannot force Bob to choose a specific r value. (ii) Even if she feeds Bob a state of the form $|\Psi_{\ell u}^{(r)}\rangle$, where r accidentally equals Bob's r, then there is a $\frac{1}{2}$ probability that Bob's measurement $\mathcal{M}^{(r)}$ yields $k \neq \ell$ *with random* s.

7.2.3 Attacker model

The attacker model is the basic attacker model introduced in Section 2.1. We allow Eve to attack the qudits in any way allowed by the laws of quantum physics, e.g. using unbounded quantum memory, entanglement, lossless operations, arbitrary POVMs, arbitrary unitary operators etc. All bit errors observed by Alice and Bob are assumed to be caused by Eve. Eve has no access to the labs of Alice and Bob, i.e. there are no side-channel attacks. In a quantum key distribution scheme, the final result is long-term key shared by Alice and Bob. Hence the attacker model relevant for unclonable encryption is not feasible for any QKD scheme. Alice and Bob are able to destroy classical variables. For simplicity we do not describe the classical authentication performed by Alice and Bob. Instead we give Alice and Bob access to an authenticated classical channel.

7.3 The RRDPS QKD protocol with channel monitoring

7.3.1 Protocol description

Alice and Bob have agreed on a noise threshold β, the number of qudits n, a family of pairwise independent hash functions $\Phi_u : \{0,1\}^n \to \{0,1\}^\ell$ with $u \in \mathcal{U}$ and a linear error-correcting code with syndrome function $\texttt{Syn} : \{0,1\}^n \to \{0,1\}^{n-\kappa}$ and decoder $\texttt{SynDec}$: $\{0,1\}^{n-\kappa} \to \{0,1\}^n$. Let $x^{(i)}$ denote the value of x in the ith qudit. The vector consisting of n strings $a^{(i)}$ is denoted in bold font: $\boldsymbol{a} = (a^{(i)})_{i=1}^n$. The notation $\boldsymbol{a}_k \in \{0,1\}^n$ denotes the string $(a_{k_i}^{(i)})_{i=1}^n$. Similarly $\boldsymbol{a}_{k+r}$ stands for $(a_{k_i+r_i}^{(i)})_{i=1}^n$. Alice and Bob adopt the channel monitoring procedure shown below.

Definition 7.1. *Let s' be a noisy version of s.*

$$\texttt{NoiseCheck}(s,s') = \begin{cases} 1 & \text{if } \frac{\texttt{Hamm}(s\oplus s')}{n} \leq \beta \\ 0 & \text{otherwise.} \end{cases} \tag{7.5}$$

Definition 7.1 states that the channel noise should not exceed the threshold β.

As we did for six-state QKD, we describe the RRDPS QKD protocol with channel monitoring followed by a one-time pad encryption. This ensures that it is a quantum encryption protocol according to Definition 2.3.

RR.Gen:

Alice generates n local random bitstrings of length d: $\boldsymbol{a} = (a^{(i)} \in \{0,1\}^d)_{i=1}^n$, a random hash seed $u \in \mathcal{U}$ and a message $m \in \{0,1\}^\ell$.

Bob generates a local random string $r \in \{1,\ldots,d-1\}^n$.

RR.Enc

Alice prepares n qudits in a joint state that we write as $|\mu_{\boldsymbol{a}}\rangle = \bigotimes_{i=1}^n |\mu_{a^{(i)}}\rangle$ with $|\mu_{a^{(i)}}\rangle = \frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} (-1)^{a_t^{(i)}} |t\rangle$.

RR.Meas

For all qudits $i \in [n]$, Bob applies the POVM $\mathcal{M}^{(r^{(i)})}$, which yields measurement outcomes $k \in \{0,\ldots,d-1\}^n$ and $s \in \{0,1\}^n$.

RR.Post

Bob sends r, k to Alice.

Alice computes $s' = \boldsymbol{a}_k \oplus \boldsymbol{a}_{k+r}$. She sends $e = \texttt{Syn}\, s'$ to Bob.

Bob performs the error correction $\hat{s}' = s \oplus \texttt{SynDec}(\texttt{Syn}\, s \oplus e)$ and the channel monitoring $\omega = \texttt{NoiseCheck}(s, \hat{s}')$. He sends ω to Alice.

If $\omega == 1$, Alice computes $z = \Phi_u(s')$ and $c = z \oplus m$ and sends u, c to Bob. If $\omega == 0$ she sends $\perp$.

Bob computes $\hat{z} = \Phi_u(\hat{s}')$ and $\hat{m} = c \oplus \hat{z}$.

7.4 Proof structure

We prove the secrecy of the message after an instance of the protocol. We bound the leakage for a finite number of qudits as well as for asymptotically many qudits. We apply the proof recipe of Section 2.5 to the RRDPS QKD scheme with channel monitoring. We start by formulating an EPR version of the protocol (step 1). In the EPR version, Eve prepares a d^2-dimensional noisy EPR state. Alice performs a measurements that ensures the state $|\mu_{\boldsymbol{a}}\rangle$ is held by Bob. In step 2 we show the EPR version is invariant to random permutations of qubit positions as well as permutations of time indices within a qudit. We also show an invariance to random phase flips. In step 3, we systematically describe the completely positive trace preserving maps that describe modified protocol $\mathcal{E}$ and its ideal counterpart $\mathcal{F}$ in which the message is completely decoupled from the state held by Eve. For the asymptotic result, we introduce smooth states in step 4. Finally in step 5 and 6 we exploit the symmetrized form of Eve's state and compute bounds on the leakage. The correctness of the message is guaranteed by the authenticated classical channels.

7.5 Symmetrized EPR version of the protocol

We construct an EPR version of the protocol. We show that the security of the EPR version is unaffected by permutation of the qudit positions as well as in the time indices within a qudit. In addition we show the protocol is security-equivalent to a protocol with added random phase flips within the qudits.

7.5.1 EPR version

Consider the following modifications to the protocol of Section 7.3. Alice does not generate the random string $\boldsymbol{a}$ in RR.Gen. We replace the map RR.Enc by the following. Alice prepares $(|\alpha_0\rangle)^{\otimes n}$ with

$$|\alpha_0\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} |tt\rangle \tag{7.6}$$

She sends half of each pair to Bob. Alice performs the POVM $\mathcal{Q} = (Q_z)_{z\in\{0,1\}^d}$ on each qudit, where

$$Q_z = \frac{d}{2^d} |\mu_z\rangle\langle\mu_z|. \tag{7.7}$$

This results in n measured strings $a^{(i)} \in \{0,1\}^d$. This procedure is equivalent to generating a random $\boldsymbol{a}$ and sending $|\mu_{\boldsymbol{a}}\rangle$ to Bob. The rest of the protocol remains unchanged.

Lemma 7.2. *The hermitian matrices Q_z as defined in (7.7) form a POVM, i.e. $\sum_{z\in\{0,1\}^d} Q_z = \mathbb{1}$.*

Proof:
$\sum_z |\mu_z\rangle\langle\mu_z| = \sum_z \frac{1}{d} \sum_{t,t'=0}^{d-1} (-1)^{z_{t'}+z_t} |t\rangle\langle t'| = \frac{1}{d} \sum_{t,t'=0}^{d-1} |t\rangle\langle t'| \sum_z (-1)^{z_{t'}+z_t}$.
Using $\sum_z (-1)^{z_{t'}+z_t} = 2^d \delta_{tt'}$ we get $\sum_z |\mu_z\rangle\langle\mu_z| = \frac{2^d}{d} \sum_t |t\rangle\langle t| = \frac{2^d}{d}\mathbb{1}$. □
It is not important whether $\mathcal{Q}$ is practical or not; it is a theoretical construct which allows us to build an EPR version of RRDPS.

7.5.2 Random permutation of qudits

We show the security of the protocol is not changed if random permutation of the qudits is added. Consider the following modifications to RR.Gen, RR.Enc and RR.Meas.

In RR.Gen, Alice generates a random permutation π_q of the n qudits. In RR.Enc she applies the permutation to the received qubits before measuring with $\mathcal{Q}$. She sends π_q to Bob. In RR.Meas Bob permutes his qubits according to π_q before measuring with $\mathcal{M}^{(r)}$. The remainder of the protocol remains unchanged.

The effect of the random permutation on Alice's side is a random permutation of her measurement results $a^{(i)}$ which were and stay uniform. At Bob's side his measurement outcomes are permuted. The potential non-uniformity of k caused by Eve occurs at different positions, causing an alteration of s, s' but with the same probability distribution as before. The noise on s is permuted as well, but this alteration is

undone by the error correction step which is indifferent to the noise positions. Overall, Alice and Bob's output variables have the same probability distributions with or without the random permutation. The only difference in output is a permutation of the indices of k. The permutation invariance of the protocol, in accordance with Lemma 2.16, allows for the use of post-selection.

7.5.3 Random permutation of time indices

We show the security of the protocol is unchanged under permutations of the orthonormal basis states $|t\rangle$, $t \in \{0, \ldots, d-1\}$ within each qudit. Consider the following modifications to the maps RR.Gen, RR.Enc and RR.Meas. In RR.Gen, Alice generates n random permutation of the d temporal positions: $\pi_T = \bigotimes_{i=1}^{n} \pi_T^{(i)}$. In RR.Enc Alice permutes the time indices of the ith qudit according to $\pi_T^{(i)}$ before performing her measurement $\mathcal{Q}$. Alice sends π_T to Bob. In RR.Meas, before measuring with $\mathcal{M}^{(r)}$, Bob applies the same permutation $\pi_T^{(i)}$ to his ith qudit. The remainder of the protocol is unchanged.

The security equivalence is seen as follows. Since $\boldsymbol{a}$ was already uniform, its statistics are unaffected by the permutation. Bob's measurement outcome k is modified according to the permutation. The statistics of s are unaffected since the distributions of $\boldsymbol{a}$ and r are unchanged. The permutation of the time indices by Alice and Bob has the same effect as a permutation of the classical string a by Alice and changing the value of k accordingly by Bob. Permuting these random classical strings does not affect the state held by Eve. The security of the protocol is not impacted.

7.5.4 Random phase flips

We show that the security of the protocol is unchanged when random phase flips are added as an extra step to the protocol. Consider the following modifications to the maps RR.Gen, RR.Enc and RR.Meas. In RR.Gen Alice generates n uniform random bit strings: $\boldsymbol{p} = (p^{(i)} \in \{0,1\}^d)_{i=1}^n$. In RR.Enc, before measuring with $\mathcal{Q}$, Alice performs phase flips on her ith qudit according to the rule $|t\rangle \to (-1)^{\boldsymbol{p}_t^{(i)}} |t\rangle$. She sends $\boldsymbol{p}$ to Bob. This random phase flip replaces Alice's check on the uniformity of a. In RR.Meas Bob performs the same phase flips according to $\boldsymbol{p}$ before measuring with $\mathcal{M}^{(r)}$. The remainder of the protocol remains unchanged.

Alice's measurement outcome a is randomized by the random phase flip. However, a was already uniform. Bob's measurement result s is changed according to the change in Alice's a, but the correlation with s' and noise distribution is unaffected. The measurement outcome k is unaffected. Alice and Bob's output variables which are a function of s', s are altered but have the same probability distribution as before. The phase flips on the qudits are equivalent to Alice and Bob flipping their classical strings a, s according to $\boldsymbol{p}$ and performing RR.Post as before.

Since the random phase flip guarantees Alice's measurement result is uniform, we allow Eve to create the EPR pairs. Giving Eve access to Alice's part of the state can never decrease her attacking possibilities. Security of the symmetrized EPR version implies security of the original protocol.

7.6 CPTP mappings

Let RR' be the modified protocol described in Section 7.5. Eve creates some d^{4n}-dimensional state ρ^{ABE}. Just as in the qubit analysis of the previous chapters, we don't explicitly write down the randomizations $\pi_q, \pi_T, \boldsymbol{p}$ but instead consider their effects on Eve's state. This is allowed since none of the further actions depend on $\pi_q, \pi_T, \boldsymbol{p}$.

Let $\mathcal{M}_{\mathrm{RR}}$ be shorthand notation for $\mathsf{RR'.Meas} \circ \mathsf{RR'.Enc} \circ \mathsf{RR'.Gen}$. The generated random variables are m, u, r where m is not necessarily uniform. The measurements of Alice and Bob introduce the vector of strings $\boldsymbol{a}$ and the strings k, s. The measurements introduce a coupling between Eve's state and the measurement variables $\boldsymbol{a}, k, s, r$.

$$\mathcal{M}_{\mathrm{RR}}(\rho^{\mathrm{ABE}}) = \mathop{\mathbb{E}}_{mur\boldsymbol{a}ks} |mur\boldsymbol{a}ks\rangle\langle mur\boldsymbol{a}ks| \otimes \rho^{\mathrm{E}}_{\boldsymbol{a}ksr}. \tag{7.8}$$

The variables u, r and a are uniform. The distributions of k and s depend on $\rho^{\mathrm{E}}_{\boldsymbol{a}ksr}$.

In RR'.Post Alice and Bob compute the variables s', ω, z, e, c. Let $\mathcal{P}_{\mathrm{RR}}$ denote the RR′ protocol up to the point where the variables are deleted (and therefore traced out). We introduce the notation $\theta_{ss'} = \mathtt{NoiseCheck}(s, s')$.

$$\begin{aligned}\mathcal{P}_{\mathrm{RR}}(\rho^{\mathrm{ABE}}) \;=\; & \mathop{\mathbb{E}}_{mur\boldsymbol{a}ks} \sum_{s'\omega zec} |umr\boldsymbol{a}kss'\omega zec\rangle\langle umr\boldsymbol{a}kss'\omega zec| \delta_{s',\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r}} \delta_{\omega,\theta_{ss'}} \\ & \left[\omega\delta_{z,\Phi_u(s')}\delta_{e,\mathtt{Syn}\,s'}\delta_{c,m\oplus z} + \bar{\omega}\delta_{z\|e\|c,\perp}\right] \otimes \rho^{\mathrm{E}}_{\boldsymbol{a}ksr}. \end{aligned} \tag{7.9}$$

The map that describes the entire protocol $\mathcal{E}_{\mathrm{RR}}$ follows by tracing out the variables $\boldsymbol{a}ss'z$ that are not part of the output m or the transcript k, r, c, e, u, ω. The result is the state $\rho^{MURKEC\Omega\mathrm{E}}$.

$$\mathcal{E}_{\mathrm{RR}}(\rho^{\mathrm{ABE}}) \;=\; \rho^{MURKEC\Omega\mathrm{E}} \tag{7.10}$$

$$\begin{aligned} \;=\; & \mathop{\mathbb{E}}_{murk} \sum_{\omega ec} |murkec\omega\rangle\langle\cdots| \mathop{\mathbb{E}}_{\boldsymbol{a}s|rk} \delta_{\omega,\theta_{s,\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r}}} \\ & \left[\omega\delta_{c,m\oplus\Phi_u(\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r})}\delta_{e,\mathtt{Syn}(\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r})} + \bar{\omega}\delta_{c\|e,\perp}\right] \otimes \rho^{\mathrm{E}}_{\boldsymbol{a}ksr}. \end{aligned} \tag{7.11}$$

The ideal behavior decouples the message M from the rest of Eve's state. We can obtain the ideal map $\mathcal{F}_{\mathrm{RR}}$ by tracing the message out of the output of $\mathcal{E}_{\mathrm{RR}}$. Notice that the reject part of $\rho^{MURKEC\Omega\mathrm{E}}$ is independent of m. Hence the output of $\mathcal{E}_{\mathrm{RR}}$ and $\mathcal{F}_{\mathrm{RR}}$ will only differ in the accept part.

$$\mathcal{F}_{\mathrm{RR}}(\rho^{\mathrm{ABE}}) \;=\; \rho^{M} \otimes \rho^{URKEC\Omega\mathrm{E}} \tag{7.12}$$

$$\begin{aligned} \;=\; & \mathop{\mathbb{E}}_{murk} \sum_{\omega ec} |murkec\omega\rangle\langle\cdots| \mathop{\mathbb{E}}_{\boldsymbol{a}s|rk} \delta_{\omega,\theta_{s,\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r}}} \\ & \left[\omega \mathop{\mathbb{E}}_{m'} \delta_{c,m'\oplus\Phi_u(\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r})}\delta_{e,\mathtt{Syn}(\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r})} + \bar{\omega}\delta_{c\|e,\perp}\right] \otimes \rho^{\mathrm{E}}_{\boldsymbol{a}ksr}. \end{aligned} \tag{7.13}$$

A small diamond norm between $\mathcal{E}_{\mathrm{RR}}$ and $\mathcal{F}_{\mathrm{RR}}$ implies that our definition of encryption is satisfied (Definition 2.4).

$$\|\mathcal{E}_{\mathrm{RR}} - \mathcal{F}_{\mathrm{RR}}\|_\diamond \quad = \quad \frac{1}{2}\Big\|\rho^{MURKEC\Omega=1\mathrm{E}} - \rho^M \otimes \rho^{URKEC\Omega=1\mathrm{E}}\Big\|_1 \stackrel{\mathrm{def}}{=} D. \tag{7.14}$$

Equation 7.14 is the difference between two sub-normalized states with trace $\mathbb{E}_{\boldsymbol{a}krs}\,\theta_{s,\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r}}$. It immediately follows that $D \leq \mathbb{E}_{\boldsymbol{a}krs}\,\theta_{s,\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r}}$.

7.7 Smooth states

We allow states $\bar\rho$ that are $\sqrt{\varepsilon}$-close to ρ in order to apply Lemma 2.19. We define $\bar D \stackrel{\mathrm{def}}{=} \frac{1}{2}\|\bar\rho^{MURKEC\Omega\mathrm{E}} - \rho^M \otimes \bar\rho^{URKEC\Omega\mathrm{E}}\|_1$. For the 1-norm in (7.14) it then holds that $D \leq \bar D + 2\sqrt{\varepsilon}$. Writing $\mathbb{E}_c(\cdot) = 2^{-\ell}\sum_c(\cdot)$ and $\mathbb{E}_e(\cdot) = 2^{\kappa-n}\sum_e(\cdot)$ and using Jensen's inequality on u, e, m we get

$$\begin{aligned}
\bar D \quad = \quad & \mathop{\mathbb{E}}_{murkec}\Big\|2^{\ell+n-\kappa}\mathop{\mathbb{E}}_{\boldsymbol{a}s|rk}\theta_{s,\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r}}\delta_{e,\mathtt{Syn}(\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r})} \\
& \qquad \big[\delta_{\Phi_u(\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r}),m\oplus c} - \mathop{\mathbb{E}}_{m'}\delta_{\Phi_u(\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r}),m'\oplus c}\big]\bar\rho^{\mathrm{E}}_{\boldsymbol{a}ksr}\Big\|_1 \qquad (7.15) \\
\stackrel{\text{Jensen}}{\leq} \quad & \mathop{\mathbb{E}}_{rkc}\mathrm{tr}\Big\{2^{2\ell+2n-2\kappa}\mathop{\mathbb{E}}_{mue}\mathop{\mathbb{E}}_{\boldsymbol{a}\boldsymbol{a}'ss'|rk}\theta_{s,\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r}}\theta_{s',\boldsymbol{a}'_k\oplus\boldsymbol{a}'_{k+r}}\delta_{e,\mathtt{Syn}(\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r})} \\
& \delta_{e,\mathtt{Syn}(\boldsymbol{a}'_k\oplus\boldsymbol{a}'_{k+r})}\big[\delta_{\Phi_u(\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r}),m\oplus c} - \mathop{\mathbb{E}}_{m'}\delta_{\Phi_u(\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r}),m'\oplus c}\big] \qquad (7.16) \\
& \big[\delta_{\Phi_u(\boldsymbol{a}'_k\oplus\boldsymbol{a}'_{k+r}),m\oplus c} - \mathop{\mathbb{E}}_{m''}\delta_{\Phi_u(\boldsymbol{a}'_k\oplus\boldsymbol{a}'_{k+r}),m''\oplus c}\big]\bar\rho^{\mathrm{E}}_{\boldsymbol{a}ksr}\bar\rho^{\mathrm{E}}_{\boldsymbol{a}'ks'r}\Big\}^{\frac{1}{2}}.
\end{aligned}$$

Using the defining property of the pairwise-independent hash function Φ_u and introducing the shorthand notation $x \stackrel{\mathrm{def}}{=} \boldsymbol{a}_k \oplus \boldsymbol{a}_{k+r}$ and $x' \stackrel{\mathrm{def}}{=} \boldsymbol{a}'_k \oplus \boldsymbol{a}'_{k+r}$ we write

$$\begin{aligned}
2^{2\ell}\mathop{\mathbb{E}}_{mu}\big[\delta_{\Phi_u(x),m\oplus c} - \mathop{\mathbb{E}}_{m'}\delta_{\Phi_u(x),m'\oplus c}\big]\big[\delta_{\Phi_u(x'),m\oplus c} - \mathop{\mathbb{E}}_{m''}\delta_{\Phi_u(x'),m''\oplus c}\big] \\
= 2^\ell\delta_{xx'}(1 - \mathop{\mathbb{E}}_{mm'}\delta_{mm'}) < 2^\ell\delta_{xx'}. \qquad (7.17)
\end{aligned}$$

Substituting (7.17) into (7.16) we get a factor $\delta_{xx'}\delta_{\mathtt{Syn}(x),\mathtt{Syn}(x')} = \delta_{xx'}$. We use the simple bound $\theta_{s,\boldsymbol{a}_k\oplus\boldsymbol{a}_{k+r}} \leq 1$ and write

$$\bar D \leq \mathop{\mathbb{E}}_{kr}\mathrm{tr}\sqrt{2^{\ell+n-\kappa}\mathop{\mathbb{E}}_{xx'|rk}\delta_{xx'}\bar\rho^{\mathrm{E}}_{xkr}\bar\rho^{\mathrm{E}}_{x'kr}} \tag{7.18}$$

where $\bar\rho^{\mathrm{E}}_{xkr}$ is averaged over s and over $\boldsymbol{a}$ except for the degree of freedom $\boldsymbol{a}_k \oplus \boldsymbol{a}_{k+r}$. Equation 7.18 has the appropriate form to use Lemma 2.19. This yields

$$\bar D \leq \sqrt{2^{\ell+n-\kappa}}\mathop{\mathbb{E}}_{kr}\sqrt{2^{S_0^\varepsilon(\rho^{\mathrm{E}}_{kr}) - S_2^\varepsilon(\rho^{X\mathrm{E}}_{kr})}}. \tag{7.19}$$

7.8 Post-selection

As argued in Section 7.5.2 the protocol is invariant to qudit permutations except for a permutation of the transcript variable k. The post-selection step of Lemma 2.16 is applicable when there exists a $\mathcal{K}_{\pi_q}$ that undoes the permutation of k. Which in this case is simply π_q^{-1} applied to k. We use the post-selection technique to consider factorized states of the form $\rho^{\mathrm{E}} = \bigotimes_{i=1}^{n} \sigma_i^{\mathrm{E}}$. This replacement introduces a penalty factor to the final diamond norm of size $(n+1)^{d^4-1}$, which becomes significant for large d and finite size n. Asymptotically for fixed d and $n \to \infty$ the penalty is negligible.

Recall the bound $D \leq \mathbb{E}_{\boldsymbol{a}krs}\, \theta_{s,\boldsymbol{a}_k \oplus \boldsymbol{a}_{k+r}}$. The factorization allows us to interpret this as the probability of passing the noise check when attacking each qudit in the same manner (with the same noise γ). We get a simple expression for $\Pr[s|\boldsymbol{a}kr]$ so we can write $\mathbb{E}_{s|\boldsymbol{a}kr}(\cdot) = \sum_s (\gamma^{\mathtt{Hamm}(s \oplus \boldsymbol{a}_k \oplus \boldsymbol{a}_{k+r})}(1-\gamma)^{\mathtt{Hamm}(\bar{s} \oplus \boldsymbol{a}_k \oplus \boldsymbol{a}_{k+r})})(\cdot)$. The accept probability is then

$$P_{\mathrm{acc}} \overset{\mathrm{def}}{=} \mathop{\mathbb{E}}_{\boldsymbol{a}krs} \theta_{s,\boldsymbol{a}_k \oplus \boldsymbol{a}_{k+r}} = \sum_{c=0}^{\lfloor \beta n \rfloor} \binom{n}{c} \gamma^c (1-\gamma)^{n-c}. \tag{7.20}$$

For the bound (7.19), the factorized state allows us to use Lemma 2.1 in the asymptotic regime and express our bound in terms of von Neumann entropies. The two bounds together give

$$\|\mathcal{E}_{\mathrm{RR}} - \mathcal{F}_{\mathrm{RR}}\|_\diamond \overset{\text{asymp.}}{\leq} (n+1)^{d^4-1} \min\left(P_{\mathrm{acc}}, \sqrt{\varepsilon} + \sqrt{2^{\ell+n-\kappa}} \mathop{\mathbb{E}}_{kr} \sqrt{2^{nS(\sigma^{\mathrm{E}}_{kr}) - nS(\sigma^{\mathrm{XE}}_{kr}) + \mathcal{O}(\sqrt{n})}}\right). \tag{7.21}$$

For our finite size result we don't perform smoothing. The relevant expression is (7.18) with ρ^{E} factorized and ε set to zero.

$$\|\mathcal{E}_{\mathrm{RR}} - \mathcal{F}_{\mathrm{RR}}\|_\diamond \leq (n+1)^{d^4-1} \min\left(P_{\mathrm{acc}}, \mathop{\mathbb{E}}_{rk} \operatorname{tr} \sqrt{2^{\ell+n-\kappa} \bigotimes_{i=1}^{n} \mathop{\mathbb{E}}_{x_i|r_i k_i} (\sigma^{\mathrm{E}}_{x_i k_i r_i})^2}\right). \tag{7.22}$$

7.9 Eve's factorized state

7.9.1 Effect of the random transforms: state symmetrization

The random permutation of the qudits allows us to use the post-selection technique [CKR09] to prove security against general attacks by only considering collective attacks. Let ρ^{AB} denote the mixed state Alice and Bob receive from Eve at a single qudit position. We write

$$\rho^{\mathrm{AB}} = \sum_{t,t',\tau,\tau' \in \{0,\ldots,d-1\}} \rho^{tt'}_{\tau\tau'} |t,t'\rangle\langle\tau,\tau'|, \tag{7.23}$$

with $\rho_{tt'}^{\tau\tau'} = (\rho_{\tau\tau'}^{tt'})^*$ and $\sum_{tt'} \rho_{tt'}^{tt'} = 1$. The effect of the random permutations of time indices is that the AB state gets averaged over all permutations, i.e. we get the following mapping

$$\rho^{\mathrm{AB}} \mapsto \tilde{\rho}^{\mathrm{AB}} \stackrel{\mathrm{def}}{=} \frac{1}{d!} \sum_{\pi} \sum_{t,t',\tau,\tau'} \rho_{\pi(\tau),\pi(\tau')}^{\pi(t),\pi(t')} |t,t'\rangle\langle\tau,\tau'| \tag{7.24}$$

$$\stackrel{\mathrm{def}}{=} \sum_{t,t',\tau,\tau'} \tilde{\rho}_{\tau\tau'}^{tt'} |t,t'\rangle\langle\tau,\tau'|. \tag{7.25}$$

Here the parameters $\tilde{\rho}_{\tau\tau'}^{tt'}$ are invariant under simultaneous permutation of the four indices, i.e. $\tilde{\rho}_{\pi(\tau),\pi(\tau')}^{\pi(t),\pi(t')} = \tilde{\rho}_{\tau\tau'}^{tt'}$ for all π,t,t',τ,τ'. The consequence is that $\tilde{\rho}^{\mathrm{AB}}$ contains only a few degrees of freedom, namely the constants $\tilde{\rho}_{ss}^{ss}$, $\tilde{\rho}_{st}^{ss}$, $\tilde{\rho}_{ts}^{ss}$, $\tilde{\rho}_{tt}^{ss}$, $\tilde{\rho}_{st}^{st}$, $\tilde{\rho}_{ts}^{st}$, $\tilde{\rho}_{tu}^{ss}$, $\tilde{\rho}_{su}^{st}$, $\tilde{\rho}_{us}^{ts}$, $\tilde{\rho}_{us}^{st}$, $\tilde{\rho}_{uv}^{st}$, where s,t,u,v are mutually distinct.

Next, the random phase flips reduce the degrees of freedom even further. Let F_p be the phase flip operator.

$$\hat{\rho}^{\mathrm{AB}} \stackrel{\mathrm{def}}{=} \mathop{\mathbb{E}}_{p\in\{0,1\}^d} F_p \tilde{\rho}^{\mathrm{AB}} F_p^\dagger \tag{7.26}$$

$$= \mathop{\mathbb{E}}_{p} \sum_{tt'\tau\tau'} \tilde{\rho}_{\tau\tau'}^{tt'} (-1)^{p_t+p_{t'}+p_\tau+p_{\tau'}} |t,t'\rangle\langle\tau,\tau'| \tag{7.27}$$

$$= \sum_{tt'\tau\tau'} |t,t'\rangle\langle\tau,\tau'| \tilde{\rho}_{\tau\tau'}^{tt'} \mathop{\mathbb{E}}_{p} (-1)^{p_t+p_{t'}+p_\tau+p_{\tau'}} \tag{7.28}$$

$$\stackrel{\mathrm{def}}{=} \sum_{tt'\tau\tau'} |t,t'\rangle\langle\tau,\tau'| \hat{\rho}_{\tau\tau'}^{tt'}. \tag{7.29}$$

From (7.28) we see that any time index that occurs an odd number of times will be wiped out, i.e. $\mathbb{E}_c (-1)^{c_t} = 0$. The only surviving degrees of freedom are the four constants $\hat{\rho}_{\bullet\bullet}^{\bullet\bullet}$, $\hat{\rho}_{\circ\circ}^{\bullet\bullet}$, $\hat{\rho}_{\bullet\circ}^{\bullet\circ}$, $\hat{\rho}_{\circ\bullet}^{\bullet\circ}$, where $\bullet$ and $\circ$ denote distinct arbitrary indices. Note that these constants are real-valued. We can now write

$$\hat{\rho}^{\mathrm{AB}} = \hat{\rho}_{\bullet\bullet}^{\bullet\bullet} \sum_{t} |tt\rangle\langle tt| + \hat{\rho}_{\circ\circ}^{\bullet\bullet} \sum_{[t\tau]} |tt\rangle\langle\tau\tau| + \hat{\rho}_{\bullet\circ}^{\bullet\circ} \sum_{[tt']} |tt'\rangle\langle tt'| + \hat{\rho}_{\circ\bullet}^{\bullet\circ} \sum_{[tt']} |tt'\rangle\langle t't|. \tag{7.30}$$

Furthermore, the requirement $\operatorname{tr} \hat{\rho}^{\mathrm{AB}} = 1$ imposes the constraint $d\hat{\rho}_{\bullet\bullet}^{\bullet\bullet} + d(d-1)\hat{\rho}_{\bullet\circ}^{\bullet\circ} = 1$, reducing the number of degrees of freedom to three.

7.9.2 Imposing the noise constraint

The channel monitoring restricts the ways in which Eve can alter the AB state. We will determine the most general allowed $\hat{\rho}^{\mathrm{AB}}$ that is compatible with bit error rate γ. We introduce the notation $P_{aks|r} = \Pr[A=a, K=k, S=s|R=r]$.

Lemma 7.3. *Let Alice and Bob's bipartite state be $\hat{\rho}^{\mathrm{AB}}$, and let them perform the measurements $\mathcal{Q}$ and $\mathcal{M}^{(r)}$ respectively. At given r, the joint probability of the outcomes a,k,s is given by*

$$P_{aks|r} = \frac{1}{2d2^d} + \frac{1}{2\cdot 2^d} (\hat{\rho}_{\circ\circ}^{\bullet\bullet} + \hat{\rho}_{\circ\bullet}^{\bullet\circ})(-1)^{s+a_k+a_{k+r}}. \tag{7.31}$$

Proof: $P_{aks|r} = \mathrm{tr}\,(Q_a \otimes M_{ks}^{(r)})\hat{\rho}^{\mathrm{AB}}$
$= \mathrm{tr}\,(\frac{1}{2^d}\sum_{\ell\ell'}(-1)^{a_\ell+a_{\ell'}}|\ell\rangle\langle\ell'|\otimes\frac{1}{2}\frac{|k\rangle+(-1)^s|k+r\rangle}{\sqrt{2}}\frac{\langle k|+(-1)^s\langle k+r|}{\sqrt{2}})\sum_{tt'\tau\tau'}\hat{\rho}^{tt'}_{\tau\tau'}|t\rangle\langle\tau|\otimes|t'\rangle\langle\tau'|$
$= \frac{1}{2^{d4}}\sum_{tt'\tau\tau'}\hat{\rho}^{tt'}_{\tau\tau'}(-1)^{a_t+a_\tau}[\delta_{t'k}+(-1)^s\delta_{t',k+r}][\delta_{\tau'k}+(-1)^s\delta_{\tau',k+r}]$
$= \frac{1}{2^{d4}}\sum_{t\tau}(-1)^{a_t+a_\tau}[\hat{\rho}^{tk}_{\tau k}+\hat{\rho}^{t,k+r}_{\tau,k+r}+(-1)^s\hat{\rho}^{tk}_{\tau,k+r}+(-1)^s\hat{\rho}^{t,k+r}_{\tau k}]$. We use $\hat{\rho}^{t\ell}_{\tau\ell} = \delta_{t\ell}\delta_{\tau\ell}\hat{\rho}^{\bullet\bullet}_{\bullet\bullet}$ $+\delta_{\tau t}(1-\delta_{t\ell})\hat{\rho}^{\bullet\circ}_{\bullet\circ}$ for the first two terms, setting $\ell = k$ and $\ell = k+r$. Since $k+r \neq k$ we write $\hat{\rho}^{tk}_{\tau,k+r} = \delta_{tk}\delta_{\tau,k+r}\hat{\rho}^{\bullet\bullet}_{\circ\circ} + \delta_{t,k+r}\delta_{\tau k}\hat{\rho}^{\bullet\circ}_{\circ\bullet}$, and similarly for $\hat{\rho}^{t,k+r}_{\tau k}$. Finally we use $\hat{\rho}^{\bullet\bullet}_{\bullet\bullet} + (d-1)\hat{\rho}^{\bullet\circ}_{\bullet\circ} = 1/d$. (See end of Section 7.9.1.) □

We now impose the constraint that a bit error occurs with probability γ,

$$\Pr[S = A_K \oplus A_{K+R}] = 1 - \gamma. \tag{7.32}$$

Here the random variables are A, R, K, and S.

Theorem 7.4. *Let $|\alpha_0\rangle$ be defined by (7.6). The constraint (7.32) can only be satisfied by a density function of the form*

$$\hat{\rho}^{\mathrm{AB}} = (1-2\gamma-V)|\alpha_0\rangle\langle\alpha_0| + V\frac{1}{d}\sum_{tt'}|tt'\rangle\langle t't| + (2\gamma-\mu)\frac{\mathbb{1}}{d^2} + \mu\frac{1}{d}\sum_{t}|tt\rangle\langle tt| \tag{7.33}$$

with $\mu, V \in \mathbb{R}$. Written componentwise,

$$\hat{\rho}^{tt'}_{\tau\tau'} = \frac{1-2\gamma-V}{d}\delta_{t't}\delta_{\tau'\tau} + \frac{V}{d}\delta_{\tau t'}\delta_{\tau' t} + \frac{2\gamma-\mu}{d^2}\delta_{\tau t}\delta_{\tau' t'} + \frac{\mu}{d}\delta_{t't}\delta_{\tau t}\delta_{\tau' t}. \tag{7.34}$$

Proof: We write $\Pr[S = A_K \oplus A_{K+R}] = \sum_{akrs}\frac{1}{d-1}P_{aks|r}\delta_{s,a_k\oplus a_{k+r}}$ and use Lemma 7.3. This yields $\Pr[S = A_K \oplus A_{K+R}] = \frac{1}{2} + \frac{d}{2}(\hat{\rho}^{\bullet\bullet}_{\circ\circ} + \hat{\rho}^{\bullet\circ}_{\circ\bullet})$. The constraint (7.32) can only be satisfied by setting $\hat{\rho}^{\bullet\bullet}_{\circ\circ} + \hat{\rho}^{\bullet\circ}_{\circ\bullet} = \frac{1-2\gamma}{d}$. We choose $\hat{\rho}^{\bullet\bullet}_{\circ\circ}, \hat{\rho}^{\bullet\circ}_{\bullet\circ}$ as the two independent degrees of freedom and re-parametrise them as $\hat{\rho}^{\bullet\bullet}_{\circ\circ} = (1-2\gamma-V)/d$ and $\hat{\rho}^{\bullet\circ}_{\bullet\circ} = (2\gamma-\mu)/d^2$, where $\mu, V \in \mathbb{R}$ are the new independent degrees of freedom. Substitution into (7.30) yields (7.33). □

Theorem 7.4 shows that (at fixed γ) there are only two degrees of freedom, μ and V, in Eve's manipulation of the EPR pair.

7.9.3 Purification

According to the attacker model we have to assume that Eve has the purification of the state $\hat{\rho}^{\mathrm{AB}}$. The purification contains all information that exists outside the AB system.

We introduce the following notation,

$$|\alpha_j\rangle \stackrel{\mathrm{def}}{=} \frac{1}{\sqrt{d}}\sum_t e^{i\frac{2\pi}{d}jt}|tt\rangle, \qquad j \in \{0,\ldots,d-1\} \tag{7.35}$$

$$|D^{\pm}_{tt'}\rangle \stackrel{\mathrm{def}}{=} \frac{|tt'\rangle \pm |t't\rangle}{\sqrt{2}} \qquad t < t'. \tag{7.36}$$

Lemma 7.5. *The $\hat{\rho}^{\rm AB}$ given in (7.33) has the following orthonormal eigensystem,*

$$\begin{array}{lll} |\alpha_0\rangle & \text{with eigenvalue } \lambda_0 \stackrel{\rm def}{=} \dfrac{2\gamma-\mu}{d^2}+\dfrac{\mu+V}{d}+1-2\gamma-V \\ |\alpha_j\rangle \quad j\in\{1,\ldots,d-1\} & \text{with eigenvalue } \lambda_1 \stackrel{\rm def}{=} \dfrac{2\gamma-\mu}{d^2}+\dfrac{\mu+V}{d}. \\ |D^{\pm}_{tt'}\rangle \quad (t<t') & \text{with eigenvalue } \lambda_{\pm} \stackrel{\rm def}{=} \dfrac{2\gamma-\mu}{d^2}\pm\dfrac{V}{d} \end{array} \tag{7.37}$$

Proof: The term proportional to $\mathbb{1}$ in (7.33) yields a contribution $(2\gamma-\mu)/d^2$ to each eigenvalue. First we look at $|\alpha_j\rangle$. We have $\langle\alpha_0|\alpha_j\rangle = \delta_{j0}$. Furthermore $\langle t't|\alpha_j\rangle = \delta_{t't}e^{i\frac{2\pi}{d}jt}/\sqrt{d}$, which gives $(\sum_{tt'}|tt'\rangle\langle t't|)|\alpha_j\rangle = |\alpha_j\rangle$. Similarly we have $(\sum_t |tt\rangle\langle tt|)|\alpha_j\rangle = |\alpha_j\rangle$. Next we look at $|D^{\pm}_{tt'}\rangle$. We have $\langle\alpha_0|D^{\pm}_{tt'}\rangle = 0$ and $\langle uu|D^{\pm}_{tt'}\rangle = 0$. Hence the $(1-2\gamma-V)$-term and the μ-term in (7.33) yield zero when acting on $|D^{\pm}_{tt'}\rangle$. Furthermore $\sum_{uu'}|uu'\rangle\langle u'u|D^{+}_{tt'}\rangle = \sum_{uu'}|uu'\rangle\frac{\delta_{ut}\delta_{u't'}+\delta_{ut'}\delta_{u't}}{\sqrt{2}}$ $= |D^{+}_{tt'}\rangle$. Similarly, $\sum_{uu'}|uu'\rangle\langle u'u|D^{-}_{tt'}\rangle = \sum_{uu'}|uu'\rangle\frac{\delta_{ut}\delta_{u't'}-\delta_{ut'}\delta_{u't}}{\sqrt{2}}\mathrm{sgn}(u-u') = -|D^{-}_{tt'}\rangle$. □

In diagonalized form the $\hat{\rho}^{\rm AB}$ is given by

$$\hat{\rho}^{\rm AB} = \lambda_0|\alpha_0\rangle\langle\alpha_0| + \lambda_1\sum_{j=1}^{d-1}|\alpha_j\rangle\langle\alpha_j| + \lambda_+\sum_{tt':t<t'}|D^{+}_{tt'}\rangle\langle D^{+}_{tt'}| + \lambda_-\sum_{tt':t<t'}|D^{-}_{tt'}\rangle\langle D^{-}_{tt'}|. \tag{7.38}$$

The purification is

$$\begin{aligned} |\Psi^{\rm ABE}\rangle \;=\; & \sqrt{\lambda_0}|\alpha_0\rangle\otimes|E_0\rangle + \sqrt{\lambda_1}\sum_{j=1}^{d-1}|\alpha_j\rangle\otimes|E_j\rangle \\ & + \sqrt{\lambda_+}\sum_{tt':t<t'}|D^{+}_{tt'}\rangle\otimes|E^{+}_{tt'}\rangle + \sqrt{\lambda_-}\sum_{tt':t<t'}|D^{-}_{tt'}\rangle\otimes|E^{-}_{tt'}\rangle. \end{aligned} \tag{7.39}$$

where we have introduced orthonormal basis states $|E_j\rangle$, $|E^{\pm}_{tt'}\rangle$ in Eve's Hilbert space. In Appendix 7.A we give more details on Eve's unitary operation.

7.9.4 Eve's state

Eve waits for Alice and Bob to perform their measurements and reveal k and r.

Lemma 7.6. *After Alice has measured $a\in\{0,1\}^d$ and Bob has measured $k\in\{0,\ldots,d-1\}$, $s\in\{0,1\}$, Eve's state is given by*

$$\sigma^{rk}_{as} = \mathrm{tr}_{\rm AB}\Big[|\Psi^{\rm ABE}\rangle\langle\Psi^{\rm ABE}|\frac{Q_a\otimes M^{(r)}_{ks}\otimes\mathbb{1}}{P_{aks|r}}\Big]. \tag{7.40}$$

Proof: The POVM elements Q_a and $M^{(r)}_{ks}$ are proportional to projection operators. Hence the tripartite ABE pure state after the measurement is proportional to $(Q_a\otimes M^{(r)}_{ks}\otimes\mathbb{1})|\Psi^{\rm ABE}\rangle$. It is easily verified that the normalisation in (7.40) is correct: taking

the trace in E-space yields $\mathrm{tr}_{\mathrm{AB}}\mathrm{tr}_{\mathrm{E}}|\Psi^{\mathrm{ABE}}\rangle\langle\Psi^{\mathrm{ABE}}|Q_a\otimes M_{ks}^{(r)}\otimes\mathbb{1} = \mathrm{tr}_{\mathrm{AB}}\ \hat{\rho}^{\mathrm{AB}}Q_a\otimes M_{ks}^{(r)}$ $= P_{aks|r}$. □

Lemma 7.7. *It holds that*

$$\frac{d}{2^d}\sum_{\substack{a_0\cdots a_{d-1}\\ \text{without } a_k,a_{k+r}}}|\mu_a\rangle\langle\mu_a| = \frac{1}{4}\mathbb{1}+\frac{1}{4}(-1)^{a_k+a_{k+r}}\Big(|k\rangle\langle k+r|+|k+r\rangle\langle k|\Big) \quad (7.41)$$

$$= M^{(r)}_{k,a_k\oplus a_{k+r}}+\frac{1}{4}\sum_{t:\ t\neq k,k+r}|t\rangle\langle t|. \quad (7.42)$$

Proof: We have $|\mu_a\rangle\langle\mu_a| = \frac{1}{d}\mathbb{1}+\frac{1}{d}\sum_{t\tau:t\neq\tau}|t\rangle\langle\tau|(-1)^{a_t+a_\tau}$. Summation of the $\frac{1}{d}\mathbb{1}$ term is trivial and yields $2^{d-2}\cdot\frac{1}{d}\mathbb{1}$. In the summation of the factor $(-1)^{a_t+a_\tau}$ in the second term, any summation $\sum_{a_t}(-1)^{a_t}$ yields zero. The only nonzero contribution arises when $t=k,\tau=k+r$ or $t=k+r,\tau=k$; the a-summation then yields a factor 2^{d-2}. □

Lemma 7.8. *It holds that*

$$\mathop{\mathbb{E}}_{a:a_k\oplus a_{k+r}=s'}|\mu_a\rangle\langle\mu_a| = \frac{\mathbb{1}}{d}+(-1)^{s'}\frac{|k\rangle\langle k+r|+|k+r\rangle\langle k|}{d}. \quad (7.43)$$

Proof: We have $\mathbb{E}_{a:a_k\oplus a_{k+r}=s'}|\mu_a\rangle\langle\mu_a| = 2^{-(d-1)}\sum_{a_k}\sum_{a_{k+r}}\delta_{a_k\oplus a_{k+r},s'}\cdot$ $\sum_{a\text{ without }a_k,a_{k+r}}|\mu_a\rangle\langle\mu_a|$. For the rightmost summation we use Lemma 7.7. Performing the $\sum_{a_k}$ and $\sum_{a_{k+r}}$ summations yields (7.43). □

The relevant states of Eve from (7.21) and (7.22) are σ^{E}_{kr} and $\sigma^{\mathrm{E}}_{a_k\oplus a_{k+r},kr}$. Eve's task is to guess Alice's bit[4] $s'=a_k\oplus a_{k+r}$ from the mixed state σ^{rk}_{as}, where Eve does not know a and s. We define

$$\sigma^{rk}_{s'} = \mathop{\mathbb{E}}_{s,a:a_k\oplus a_{k+r}=s'}[\sigma^{\mathrm{E}}_{aksr}]. \quad (7.44)$$

This represents Eve's ancilla state given some value of Alice's bit s'. Next we introduce notations that are useful for understanding the structure of $\sigma^{rk}_{s'}$. We define, for $t,t'\in\{0,\ldots,d-1\}$, non-normalised vectors $|w_{tt'}\rangle$ in Eve's Hilbert space as

$$|w_{tt'}\rangle \stackrel{\mathrm{def}}{=} \langle tt'|\Psi^{\mathrm{ABE}}\rangle. \quad (7.45)$$

Furthermore we define angles α and φ as

$$\cos 2\alpha \stackrel{\mathrm{def}}{=} \frac{\langle w_{kk}|w_{k+r,k+r}\rangle}{\langle w_{kk}|w_{kk}\rangle},\quad \cos 2\varphi \stackrel{\mathrm{def}}{=} \frac{\langle w_{k,k+r}|w_{k+r,k}\rangle}{\langle w_{k,k+r}|w_{k,k+r}\rangle} \quad (7.46)$$

[4] In (7.21) and (7.22) we used the notation x for s'.

and vectors $|A\rangle, |B\rangle, |C\rangle, |D\rangle$

$$\frac{|w_{kk}\rangle}{\sqrt{\langle w_{kk}|w_{kk}\rangle}} = \cos\alpha|A\rangle + \sin\alpha|B\rangle \tag{7.47}$$

$$\frac{|w_{k+r,k+r}\rangle}{\sqrt{\langle w_{k+r,k+r}|w_{k+r,k+r}\rangle}} = \cos\alpha|A\rangle - \sin\alpha|B\rangle \tag{7.48}$$

$$\frac{|w_{k,k+r}\rangle}{\sqrt{\langle w_{k,k+r}|w_{k,k+r}\rangle}} = \cos\varphi|C\rangle + \sin\varphi|D\rangle \tag{7.49}$$

$$\frac{|w_{k+r,k}\rangle}{\sqrt{\langle w_{k+r,k}|w_{k+r,k}\rangle}} = \cos\varphi|C\rangle - \sin\varphi|D\rangle. \tag{7.50}$$

The $|A\rangle$, $|B\rangle$, $|C\rangle$, $|D\rangle$ are mutually orthogonal, and also orthogonal to any vector $|w_{tt'}\rangle$ ($t' \neq t$) with $\{t, t'\} \neq \{k, k+r\}$.

Theorem 7.9. *The eigenvalues of $\sigma_{s'}^{rk}$ are given by*

$$\xi_0 \stackrel{\text{def}}{=} \frac{d}{2} \cdot \frac{\lambda_+ + \lambda_-}{2} \tag{7.51}$$

$$\xi_1 \stackrel{\text{def}}{=} \tfrac{d}{2}(\lambda_1 + \lambda_-) = \gamma - \tfrac{d}{2}(\tfrac{d}{2} - 1)(\lambda_+ + \lambda_-) \tag{7.52}$$

$$\xi_2 \stackrel{\text{def}}{=} \tfrac{d}{2}(\lambda_1 + 2\frac{\lambda_0 - \lambda_1}{d} + \lambda_+) = 1 - \gamma - \tfrac{d}{2}(\tfrac{d}{2} - 1)(\lambda_+ + \lambda_-) \tag{7.53}$$

and the diagonal representation of $\sigma_{s'}^{rk}$ is

$$\begin{aligned}\sigma_{s'}^{rk} = {} & \xi_0 \sum_{\substack{t\in\{0,\ldots,d-1\}\\ t\neq k, t\neq k+r}} \Big(\frac{|w_{tk}\rangle\langle w_{tk}|}{\langle w_{tk}|w_{tk}\rangle} + \frac{|w_{t,k+r}\rangle\langle w_{t,k+r}|}{\langle w_{t,k+r}|w_{t,k+r}\rangle}\Big) \\ & + \xi_2 \frac{[\sqrt{\xi_2 - \frac{d}{2}\lambda_+}|A\rangle + (-1)^{s'}\sqrt{\frac{d}{2}\lambda_+}|C\rangle][\cdots]^\dagger}{\xi_2} \\ & + \xi_1 \frac{[\sqrt{\xi_1 - \frac{d}{2}\lambda_-}|B\rangle - (-1)^{s'}\sqrt{\frac{d}{2}\lambda_-}|D\rangle][\cdots]^\dagger}{\xi_1}\end{aligned} \tag{7.54}$$

Proof: We have

$$\begin{aligned}\sigma_{s'}^{rk} &= \mathrm{tr}_{\mathrm{AB}}|\Psi^{\mathrm{ABE}}\rangle\langle\Psi^{\mathrm{ABE}}| \mathop{\mathbb{E}}_{a:a_k\oplus a_{k+r}=s'} Q_a \otimes \mathop{\mathbb{E}}_{s|s'} \frac{M_{ks}^{(r)}}{P_{aks|r}} \otimes \mathbb{1} \\ &= d2^d\, \mathrm{tr}_{\mathrm{AB}}|\Psi^{\mathrm{ABE}}\rangle\langle\Psi^{\mathrm{ABE}}|[\mathop{\mathbb{E}}_{a:a_k\oplus a_{k+r}=s'} Q_a] \otimes [\sum_s M_{ks}^{(r)}] \otimes \mathbb{1}.\end{aligned} \tag{7.55}$$

We use Lemma 7.8 to evaluate the $\mathbb{E}_a$ factor. We use $\sum_s M_{ks}^{(r)} = \frac{1}{2}|k\rangle\langle k| + \frac{1}{2}|k+r\rangle\langle k+r|$. This allows us to write everything in terms of $|w_{tt'}\rangle$ states. For $t = t'$ we have

$$|w_{tt}\rangle = \sqrt{\lambda_0/d}|E_0\rangle + \sqrt{\lambda_1/d}\sum_{j=1}^{d-1}(e^{i\frac{2\pi}{d}})^{jt}|E_j\rangle \tag{7.56}$$

$$\langle w_{tt}|w_{tt}\rangle = \lambda_1 + \frac{\lambda_0 - \lambda_1}{d}, \tag{7.57}$$

and for $t \neq t'$ we have

$$|w_{tt'}\rangle = \sqrt{\lambda_+/2}|E^+_{(tt')}\rangle + \mathrm{sgn}(t'-t)\sqrt{\lambda_-/2}|E^-_{(tt')}\rangle \quad (7.58)$$

$$\langle w_{tt'}|w_{tt'}\rangle = (\lambda_+ + \lambda_-)/2. \quad (7.59)$$

The following properties hold ($t \neq t'$)

$$\langle w_{tt}|w_{tt'}\rangle = 0 \quad , \quad \langle w_{tt}|w_{t't}\rangle = 0 \quad (7.60)$$

$$\langle w_{tt}|w_{t't'}\rangle = \frac{\lambda_0 - \lambda_1}{d} \quad , \quad \langle w_{tt'}|w_{t't}\rangle = \frac{\lambda_+ - \lambda_-}{2}. \quad (7.61)$$

We get

$$\cos 2\alpha = 1 - \frac{d\lambda_1}{\lambda_0 + (d-1)\lambda_1}, \quad \cos 2\varphi = 1 - \frac{2\lambda_-}{\lambda_+ + \lambda_-} \quad (7.62)$$

After some tedious algebra the result (7.54) follows. □

Note that the σ_0^{rk} and σ_1^{rk} have the same set of eigenvalues: $2(d-2)$ times ξ_0, and once ξ_1 and ξ_2.

Corollary 7.10. *It holds that*

$$\frac{\sigma_0^{rk} + \sigma_1^{rk}}{2} = \sum_{\substack{t\in\{0,\ldots,d-1\}\\ t\neq k, t\neq k+r}} \xi_0 \cdot \Big(\frac{|w_{tk}\rangle\langle w_{tk}|}{\langle w_{tk}|w_{tk}\rangle} + \frac{|w_{t,k+r}\rangle\langle w_{t,k+r}|}{\langle w_{t,k+r}|w_{t,k+r}\rangle}\Big)$$
$$+(\xi_2 - \tfrac{d}{2}\lambda_+)|A\rangle\langle A| + \tfrac{d}{2}\lambda_+|C\rangle\langle C| + (\xi_1 - \tfrac{d}{2}\lambda_-)|B\rangle\langle B| + \tfrac{d}{2}\lambda_-|D\rangle\langle D|.$$

Proof: Follows directly from Theorem 7.9 by discarding the terms in (7.54) that contain $(-1)^{s'}$ (the AC and BD crossterms). □

Corollary 7.11. *The difference between σ_0^{rk} and σ_1^{rk} can be written as*

$$\frac{\sigma_0^{rk} - \sigma_1^{rk}}{2} = \frac{1}{2}\sqrt{d\lambda_+}\sqrt{d\lambda_- + 2(1-\gamma) - \frac{d^2}{2}(\lambda_+ + \lambda_-)}\Big(|A\rangle\langle C| + |C\rangle\langle A|\Big)$$
$$-\frac{1}{2}\sqrt{d\lambda_-}\sqrt{d\lambda_+ + 2\gamma - \frac{d^2}{2}(\lambda_+ + \lambda_-)}\Big(|B\rangle\langle D| + |D\rangle\langle B|\Big). \quad (7.63)$$

Proof: Using Theorem 7.9, we see everything except the AC and BD crossterms cancel from (7.54). □

7.10 Main results

Our first result is a non-asymptotic bound on the secrecy of the message in the protocol described in Section 7.3.

Theorem 7.12. *Consider the RRDPS QKD protocol with channel monitoring as described in Section 7.3. Let $\gamma \in [0, \frac{1}{2}]$ be the noise parameter, let β be the noise threshold, let d be the dimensionality of the qudits and let P_{acc} be defined by (7.20).*

The distance between the real protocol described by $\mathcal{E}_{\rm RR}$ and the ideal protocol $\mathcal{F}_{\rm RR}$ (Section 7.6) is bounded as follows

$$\|\mathcal{E}_{\rm RR}-\mathcal{F}_{\rm RR}\|_\diamond < (n+1)^{d^4-1}\min\Big(P_{\rm acc}\,,\,\sqrt{2^{\ell+n-\kappa-n(1-2\log T)}}\Big) \tag{7.64}$$

where T is given by

$$\gamma\le\gamma_* \quad : \qquad T=2\gamma+\sqrt{1-2\gamma}\Big[\sqrt{1-2\gamma\frac{d-1}{d-2}}+\frac{\sqrt{2\gamma}}{\sqrt{d-2}}\Big] \tag{7.65}$$

$$\gamma\ge\gamma_* \quad : \qquad T=2\gamma_*+\sqrt{1-2\gamma_*}\Big[\sqrt{1-2\gamma_*\frac{d-1}{d-2}}+\frac{\sqrt{2\gamma_*}}{\sqrt{d-2}}\Big] \tag{7.66}$$

and γ_* is a saturation value that depends on d as

$$\gamma_*=\frac{x_d/2}{1+x_d}, \tag{7.67}$$

where x_d is the solution on $(0,1)$ of the equation

$$(1-\frac{x}{d-2})^{\frac12}+(1+\frac{1}{d-2})(1-\frac{x}{d-2})^{-\frac12}+\frac{1}{\sqrt{d-2}}(\sqrt{x}-\frac{1}{\sqrt{x}})-2=0. \tag{7.68}$$

For $\gamma>\beta$, $P_{\rm acc}$ is exponentially small, by e.g. Hoeffding's inequality. For $\gamma\le\beta$ the second term in the $\min(\cdot)$ can be made exponentially small by tuning ℓ. The upper bound on the amount of information that Eve has about S' is $2\log T$. This is a concave function of γ (see Figure 7.1). This confirms there is no advantage for Eve to cause different error rates in different qudit positions.

Our second result holds for asympotically large n.

Theorem 7.13. *Consider the RRDPS QKD protocol with channel monitoring of Section 7.3. Let $\gamma\in[0,\frac12]$ be the noise parameter, let β be the noise threshold, let d be the dimensionality of the qudits and let $P_{\rm acc}$ be defined by (7.20). The distance between the real protocol described by $\mathcal{E}_{\rm RR}$ and the ideal protocol $\mathcal{F}_{\rm RR}$ (Section 7.6) is bounded as follows*

$$\|\mathcal{E}_{\rm RR}-\mathcal{F}_{\rm RR}\|_\diamond < (n+1)^{d^4-1}\min\Big(P_{\rm acc}\,,\,\sqrt{2^{\ell+n-\kappa-n(1-I_{\rm AE})+\mathcal{O}(\sqrt{n})}}\Big) \tag{7.69}$$

$$\gamma\le\gamma_0 \quad : \qquad I_{\rm AE}=(1-2\gamma)h(\frac{1}{d-2}\cdot\frac{2\gamma}{1-2\gamma}) \tag{7.70}$$

$$\gamma\ge\gamma_0 \quad : \qquad I_{\rm AE}=(1-2\gamma_0)h(\frac{1}{d-2}\cdot\frac{2\gamma_0}{1-2\gamma_0}). \tag{7.71}$$

Here γ_0 is a saturation value (different from γ_*) given by

$$\gamma_0=\frac12\Big[1+\frac{1}{(d-2)(1-y_d)}\Big]^{-1} \tag{7.72}$$

where y_d is the unique positive root of the polynomial $y^{d-1}+y-1$.

The theorems are proven in Sections 7.11 and 7.12. In Section 7.12 we will see that Theorem 7.13 is sharper than (7.2) and hence allows for a higher QKD rate ℓ/n.

7.11 Proof of Theorem 7.12

We start from (7.22). The open problem is to bound $\operatorname{tr}\sqrt{(\mathbb{E}_{x|rk}\,(\sigma^{\mathrm{E}}_{xkr})^2)^{\otimes n}}$.

Lemma 7.14. *It holds that*

$$\frac{(\sigma_0^{rk})^2+(\sigma_1^{rk})^2}{2} = \sum_{\substack{t\in\{0,\ldots,d-1\}\\ t\neq k,t\neq \ell}} \xi_0^2\Big(\frac{|w_{tk}\rangle\langle w_{tk}|}{\langle w_{tk}|w_{tk}\rangle}+\frac{|w_{t,k+r}\rangle\langle w_{t,k+r}|}{\langle w_{t,k+r}|w_{t,k+r}\rangle}\Big)+\xi_1(\xi_1-\tfrac{d}{2}\lambda_-)|B\rangle\langle B| + \xi_1\tfrac{d}{2}\lambda_-|D\rangle\langle D|+\xi_2(\xi_2-\tfrac{d}{2}\lambda_+)|A\rangle\langle A|+\xi_2\tfrac{d}{2}\lambda_+|C\rangle\langle C|.$$

Proof: Follows directly from Theorem 7.9. □

Lemma 7.15.

$$\operatorname{tr}\sqrt{(\mathop{\mathbb{E}}_{x|rk}\,(\sigma^{\mathrm{E}}_{xkr})^2)^{\otimes n}} < T^n \tag{7.73}$$

$$T \stackrel{\mathrm{def}}{=} 2(d-2)\xi_0+\sqrt{\xi_2(\xi_2-\tfrac{d}{2}\lambda_+)}+\sqrt{\xi_2\tfrac{d}{2}\lambda_+}+\sqrt{\xi_1(\xi_1-\tfrac{d}{2}\lambda_-)}+\sqrt{\xi_1\tfrac{d}{2}\lambda_-}. \tag{7.74}$$

Proof: It holds that $\operatorname{tr}\sqrt{(\mathbb{E}_{x|rk}\,(\sigma^{\mathrm{E}}_{xkr})^2)^{\otimes n}} = \big(\operatorname{tr}\sqrt{\frac{(\sigma_0^{rk})^2+(\sigma_1^{rk})^2}{2}}\big)^n$ where the factor $\frac{1}{2}$ is due to the uniformity of a. We define $T=\operatorname{tr}\sqrt{(\sigma_0^{rk})^2+(\sigma_1^{rk})^2}/\sqrt{2}$ for arbitrary r,k. From Lemma 7.14 we obtain (7.74). □

Since Eve is still free to choose the parameters μ and V (or, equivalently, λ_+ and λ_-) she can choose them such that $\|\mathcal{E}_{\mathrm{RR}}-\mathcal{F}_{\mathrm{RR}}\|_\diamond$ is maximized.

Theorem 7.16. *Eve's choice of T that maximizes $\|\mathcal{E}_{\mathrm{RR}}-\mathcal{F}_{\mathrm{RR}}\|_\diamond$ is given by*

$$\gamma\le\gamma_* \quad : \quad T=2\gamma+\sqrt{1-2\gamma}\Big[\sqrt{1-2\gamma\frac{d-1}{d-2}}+\frac{\sqrt{2\gamma}}{\sqrt{d-2}}\Big] \tag{7.75}$$

$$\text{at } \lambda_-=0,\quad \lambda_+=\frac{4\gamma}{d(d-2)} \tag{7.76}$$

$$\gamma\ge\gamma_* \quad : \quad T=2\gamma_*+\sqrt{1-2\gamma_*}\Big[\sqrt{1-2\gamma_*\frac{d-1}{d-2}}+\frac{\sqrt{2\gamma_*}}{\sqrt{d-2}}\Big] \tag{7.77}$$

$$\text{at } \lambda_-=\frac{4\gamma_*(\gamma-\gamma_*)}{d(d-2)(1-2\gamma_*)},\quad \lambda_+=\frac{4\gamma_*(1-\gamma-\gamma_*)}{d(d-2)(1-2\gamma_*)}. \tag{7.78}$$

Here γ_* is a saturation value that depends on d as follows,

$$\gamma_*=\frac{x_d/2}{1+x_d}, \tag{7.79}$$

where x_d is the solution on $(0,1)$ of the equation

$$(1-\frac{x}{d-2})^{\frac{1}{2}}+\frac{d-1}{d-2}(1-\frac{x}{d-2})^{-\frac{1}{2}}+\frac{1}{\sqrt{d-2}}(\sqrt{x}-\frac{1}{\sqrt{x}})-2=0. \tag{7.80}$$

Proof: We start from (7.74). At $\gamma = \frac{1}{2}$ the expression for T is symmetric in λ_+ and λ_-. Hence the overall maximum achievable at any γ lies at $\lambda_+ = \lambda_- = \frac{q}{d(d-2)}$ for some as yet unknown q. We have

$$T_{\max}^{\gamma=\frac{1}{2}} = \zeta(q,d) \stackrel{\text{def}}{=} q + \sqrt{1-q}\Big(\sqrt{1-\frac{d-1}{d-2}q} + \frac{\sqrt{q}}{\sqrt{d-2}}\Big). \tag{7.81}$$

On the other hand, we note that substitution of (7.76) into (7.74) yields (7.75), which is precisely of the form $\zeta(q,d)$ if we identify $2\gamma \equiv q$. Hence, at some $\gamma < \frac{1}{2}$ it is already possible to achieve $T = T_{\max}^{\gamma=1/2}$, i.e. we have saturation. We note that substitution of (7.78) into (7.74) yields (7.77). The saturation value γ_* is found by solving $\partial\zeta(2\gamma,d)/\partial\gamma = 0$; after some simplification, this equation can be rewritten as (7.80) by setting $x = 2\gamma/(1-2\gamma)$.[5] □

This concludes the proof of Theorem 7.12.

The optimal λ_+,λ_- are plotted in Figure 7.3 (Section 7.13).

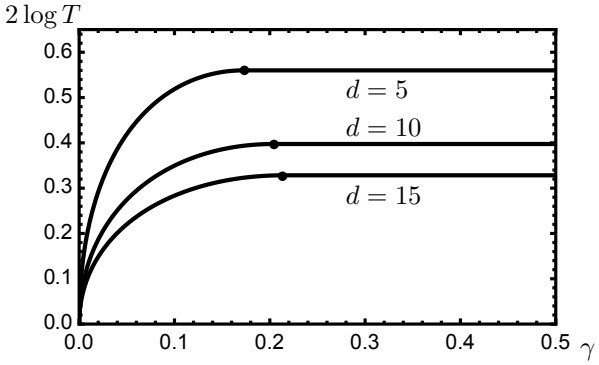

Figure 7.1: *Upper bound on the information leakage in the finite size regime as a function of the bit error rate for $d = 5$, $d = 10$ and $d = 15$ (Theorem 7.12). A dot indicates the saturation point γ_*.*

Lemma 7.17. *The large-d asymptotics of the saturation value γ_* is given by*

$$\gamma_* = \frac{1}{4} - \frac{1}{8\sqrt{d-2}} - \mathcal{O}(\frac{1}{(d-2)^{3/2}}), \tag{7.82}$$

which yields

$$T \quad = \quad 1 + \frac{1}{2\sqrt{d-2}} - \mathcal{O}(\frac{1}{d-2}). \tag{7.83}$$

[5] After some rewriting it can be seen that (7.80) is equivalent to a complicated 6th order polynomial equation. We have not yet been able to prove that the solution on $(0,1)$ is unique. Our numerical solutions however indicate that this is the case.

Proof: We set $x_d = 1 - 1/\sqrt{d-2} + a/(d-2)$, where a is supposedly of order 1, and substitute this into (7.80). This yields $a = \frac{1}{2} + \mathcal{O}(1/\sqrt{d-2})$, which is indeed of order 1. Substitution of x_d into (7.79) gives (7.82), and substitution of γ_* into (7.77) gives (7.83). □

7.12 Proof of Theorem 7.13

Here we prove Theorem 7.13. We inspect expression (7.21) and write the leakage from Alice to Eve, in terms of von Neumann entropy $I_{\rm AE} = S(\sigma^{\rm E}_{kr}) - S(\sigma^{X{\rm E}}_{kr})$. It is given by

$$I_{\rm AE} \;=\; S\Big(\frac{\sigma_0^{rk}+\sigma_1^{rk}}{2}\Big) - \frac{S(\sigma_0^{rk})+S(\sigma_1^{rk})}{2} \quad r,k \text{ arbitrary.} \tag{7.84}$$

The eigenvalues of σ_x^{rk} and $\sigma_0^{rk}+\sigma_1^{rk}$ do not actually depend on r and k. Again λ_+ and λ_- can be optimized to Eve's advantage.

Theorem 7.18. *Eve's choice that maximizes the von Neumann leakage is given by*

$$\gamma \le \gamma_0 \;:\quad I_{\rm AE} = (1-2\gamma)h\Big(\frac{1}{d-2}\cdot\frac{2\gamma}{1-2\gamma}\Big) \tag{7.85}$$

$$\text{at } \lambda_- = 0, \quad \lambda_+ = \frac{4\gamma}{d(d-2)} \tag{7.86}$$

$$\gamma \ge \gamma_0 \;:\quad I_{\rm AE} = (1-2\gamma_0)h\Big(\frac{1}{d-2}\cdot\frac{2\gamma_0}{1-2\gamma_0}\Big) \tag{7.87}$$

$$\text{at } \lambda_- = \frac{4\gamma_0(\gamma-\gamma_0)}{d(d-2)(1-2\gamma_0)}, \quad \lambda_+ = \frac{4\gamma_0(1-\gamma-\gamma_0)}{d(d-2)(1-2\gamma_0)}. \tag{7.88}$$

Here γ_0 is a saturation value that depends on d as follows,

$$\gamma_0 = \frac{1}{2}\Big[1+\frac{1}{(d-2)(1-y_d)}\Big]^{-1} \tag{7.89}$$

where y_d is the unique positive root of the polynomial $y^{d-1}+y-1$.

Proof: We start from (7.84). We note that the eigenvalue set of $(\sigma_0^{rk}+\sigma_1^{rk})/2$ largely coincides with that of σ_0^{rk} and σ_1^{rk} (Theorem 7.9 and Corollary 7.10). What remains of (7.84) comes entirely from the $|A\rangle, |B\rangle, |C\rangle, |D\rangle$ subspace,

$$\begin{aligned} I_{\rm AE} \;&=\; \xi_1\log\xi_1 + \xi_2\log\xi_2 - (\xi_2 - \tfrac{d}{2}\lambda_+)\log(\xi_2-\tfrac{d}{2}\lambda_+) - \tfrac{d}{2}\lambda_+\log(\tfrac{d}{2}\lambda_+) \\ &\quad -(\xi_1-\tfrac{d}{2}\lambda_-)\log(\xi_1-\tfrac{d}{2}\lambda_-) - \tfrac{d}{2}\lambda_-\log(\tfrac{d}{2}\lambda_-) \\ &=\; \xi_1 h\Big(\frac{d}{2}\cdot\frac{\lambda_-}{\xi_1}\Big) + \xi_2 h\Big(\frac{d}{2}\cdot\frac{\lambda_+}{\xi_2}\Big). \end{aligned} \tag{7.90}$$

We note that (7.90) is invariant under the transformation $(\gamma \to 1-\gamma; \lambda_+ \leftrightarrow \lambda_-)$. At $\gamma = 1/2$ we must hence have $\lambda_+ = \lambda_- = \lambda$.

$$I_{\rm AE}^{\gamma=\frac{1}{2}} = g(d,\lambda) \stackrel{\rm def}{=} [1-d(d-2)\lambda]\cdot h\Big(\frac{d\lambda}{1-d(d-2)\lambda}\Big). \tag{7.91}$$

At $\gamma = \frac{1}{2}$, the largest leakage that Eve can cause is $\max_\lambda g(d,\lambda) = g(d,\lambda_*)$.[6] Next we note that substitution of (7.88) into (7.90) yields (7.87); this has the same form as $g(d,\lambda)$ (7.91) if we make the identification $\lambda d(d-2) = 2\gamma_0$. Moreover, by setting $\gamma_0 = \frac{1}{2}\lambda_* d(d-2)$, Eve achieves the overall maximum leakage $g(d,\lambda_*)$ already at a value of γ smaller than $\frac{1}{2}$. Since the maximum leakage cannot decrease with γ, this implies that the maximum leakage saturates at $\gamma = \gamma_0$ and stays constant at $I_{\rm AE}^{\max}(\gamma) = g(d,\lambda_*)$ on the interval $\gamma \in [\gamma_0, \frac{1}{2}]$. The value $g(d,\lambda_*)$ precisely equals (7.87). Next we determine the value of γ_0. Demanding $\partial g(d,\lambda)/\partial\lambda = 0$ at $\lambda = \lambda_*$ yields

$$\log \frac{[1-d(d-1)\lambda_*]^{d-1}}{[1-d(d-2)\lambda_*]^{d-2}\lambda_* d} = 0. \tag{7.92}$$

This is equivalent to the polynomial equation $y^{d-1} + y - 1 = 0$ with $y \in [0,1]$ if we make the identification $y = 1 - \frac{\lambda_* d}{1-\lambda_* d(d-2)} = \frac{1-\lambda_* d(d-1)}{1-\lambda_* d(d-2)}$. (It is readily seen that $\lambda_* \in [0, \frac{1}{d(d-1)}]$ implies $y \in [0,1]$.) This precisely matches (7.89), because of the optimal choice $\gamma_0 = \frac{1}{2}\lambda_* d(d-2)$. By Descartes' rule of signs, the function $y^{d-1}+y-1$ has exactly one positive root.

When γ is decreased below γ_0, the location (λ_-, λ_+) of the maximum of the stationary point of $I_{\rm AE}$ leaves the 'allowed' triangular region; this happens at a corner of the triangle, $\lambda_- = 0$, $\lambda_+ = \frac{4\gamma}{d(d-2)}$. For $\gamma < \gamma_0$ this corner yields the highest achievable leakage. Substitution of (7.86) into (7.90) yields (7.85). □

This concludes the proof of theorem 7.13.

Note that the leakage $I_{\rm AE}$ is again a concave function of γ.

Remark. From $y > 0$ and (7.89) it follows that $\gamma_0 < \frac{1}{2} \cdot \frac{d-2}{d-1}$.

Figure 7.2 shows the von Neumann mutual information for three values of d. The optimal λ_+,λ_- are plotted in Figure 7.3 (Section 7.13).

Lemma 7.19. *The large-d asymptotics of the $I_{\rm AE}$ is given by*

$$\gamma \le \gamma_0 \quad : \quad I_{\rm AE} = \frac{2\gamma}{d-2} \log \frac{(d-2)(1-2\gamma)e}{2\gamma} + \mathcal{O}(d^{-2}) \tag{7.93}$$

$$\gamma \ge \gamma_0 \quad : \quad I_{\rm AE} = \frac{\log d}{d} + \mathcal{O}(\frac{\log\log d}{d}). \tag{7.94}$$

Proof: The result for $\gamma < \gamma_0$ follows by doing a series expansion of (7.85) in the small parameter $1/(d-2)$. For $\gamma > \gamma_0$ we study the equation $y^{d-1} = 1 - y$. Let us try a solution of the form $y = 1 - \frac{\ln[(d-1)/\alpha]}{d-1}$ for some unknown α. This yields $\alpha \cdot \{(1 - \frac{\ln[(d-1)/\alpha]}{d-1})^{d-1} \frac{d-1}{\alpha}\} = \ln \frac{d-1}{\alpha}$. Using the fact that $\lim_{n\to\infty}(1-x/n)^n = e^{-x}$ we see that the expression $\{\cdots\}$ is close to 1 if it holds that $\ln \frac{d-1}{\alpha} \ll d-1$, and that the equation is then satisfied by $\alpha = \mathcal{O}(\ln d)$, which is indeed consistent with $\ln \frac{d-1}{\alpha} \ll d-1$. Substituting $\alpha = \mathcal{O}(\ln d)$ into the expression for y and then into (7.89) gives $1 - 2\gamma_0 = \frac{1}{\ln d} + \mathcal{O}(\frac{\ln\ln d}{[\ln d]^2})$. Substituting this result for $1-2\gamma_0$ into (7.87) finally yields (7.94). □

[6] $\frac{\partial^2 g(d,\lambda)}{\partial\lambda^2} = -\frac{d}{\lambda}[1-d(d-2)\lambda]^{-1}[1-d(d-1)\lambda]^{-1}$, hence g is a concave function of λ on the interval $\lambda \in [0, \frac{1}{d(d-1)}]$, which interval coincides with the region allowed by the constraints on μ, V. The function g has a single maximum at some point λ_*.

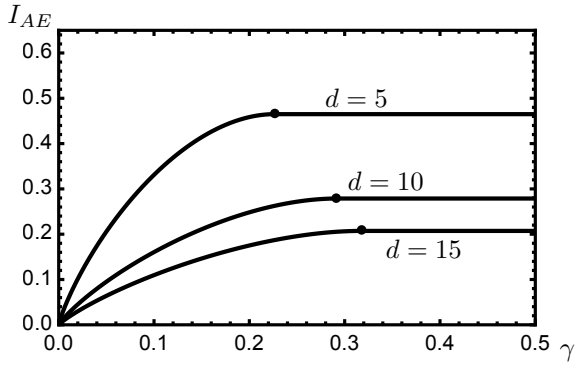

Figure 7.2: *Mutual information between Alice and Eve in terms of von Neumann entropy as a function of the bit error rate, for $d = 5$, $d = 10$ and $d = 15$ (Theorem 7.13). A dot indicates the saturation point γ_0.*

7.13 Collective attacks

By way of supplementary information we present a number of results about collective attacks. These are attacks on individual qudits where Eve performs the same measurement on every individual ancilla that she holds. First, this teaches us which kind of measurement is informative for Eve. Second, it quantifies the gap between what is provable for general attacks and what is provable for more restricted attacks. We compute leakage in terms of min-entropy loss and in terms of accessible (Shannon) information. Since min-entropy is a very conservative measure we will see that the min-entropy loss exceeds the leakage found in Theorems 7.12 and 7.13. The main interest is in Eve's measurement itself. The accessible information is the relevant quantity when Eve's quantum memory is short-lived, forcing her to perform a measurement on her ancillas before she has observed Alice and Bob's usage of the QKD key. As expected, the accessible information will turn out to be smaller than the leakage of Theorems 7.12 and 7.13.

7.13.1 Min-entropy

Eve's ability to distinguish between the cases $s' = 0$ and $s' = 1$ depends on the distance between σ_0^{rk} and σ_1^{rk} (see Section 2.3.8). Eq. (2.12) with $p_0 = \frac{1}{2}$, $p_1 = \frac{1}{2}$ tells us that the relevant quantity is $\|\sigma_0^{rk} - \sigma_1^{rk}\|_1$. For notational convenience we define the value γ_{sat},

$$\gamma_{\text{sat}} \stackrel{\text{def}}{=} \frac{1}{4} \cdot \frac{d-2}{d-1}. \tag{7.95}$$

Again we optimize λ_+ and λ_-.

Lemma 7.20. *For all r, k the choice for λ_+ and λ_- that maximizes the trace distance $\frac{1}{2}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1$ is*

$$\lambda_+ = \tfrac{4\gamma}{d(d-2)} \qquad \lambda_- = 0 \qquad \text{for } \gamma < \gamma_{\text{sat}} \tag{7.96}$$

$$\lambda_+ = \tfrac{4\gamma_{\text{sat}}}{d(d-2)} - \tfrac{2(\gamma-\gamma_{\text{sat}})}{d^2} \qquad \lambda_- = \tfrac{2(\gamma-\gamma_{\text{sat}})}{d^2} \qquad \text{for } \gamma \geq \gamma_{\text{sat}}. \tag{7.97}$$

which gives

$$\frac{1}{2}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1 = \begin{cases} \frac{1}{\sqrt{d-1}}\frac{\sqrt{\beta}}{\gamma_{\text{sat}}}\sqrt{2\gamma_{\text{sat}} - \beta} & \text{for} \quad \gamma < \gamma_{\text{sat}} \\ \\ \frac{1}{\sqrt{d-1}} & \text{for} \quad \gamma \geq \gamma_{\text{sat}}. \end{cases} \tag{7.98}$$

Proof: From Corollary 7.11 it is easy to see that

$$\begin{aligned} \frac{1}{2}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1 &= \sqrt{d\lambda_-}\sqrt{d\lambda_+ + 2\gamma - \frac{d^2}{2}(\lambda_+ + \lambda_-)} \\ &\quad + \sqrt{d\lambda_+}\sqrt{d\lambda_- + 2(1-\gamma) - \frac{d^2}{2}(\lambda_+ + \lambda_-)}. \end{aligned} \tag{7.99}$$

In Appendix 7.B we derive the λ_+, λ_- that maximize (7.99) while keeping all eigenvalues non-negative. □

Remark. The optimal choice for λ_+,λ_- has the same form for all three optimizations that we have performed. The only difference is the saturation value. Although (7.97) is shown in a simplified form one can manipulate it to the same form as (7.78) and (7.88) with γ_{sat} instead of γ_* or γ_0.

Figure 7.3 shows the optimal λ_+ and λ_- together with the constraints on the λ parameters for all three optimizations. The lower dots in the figure correspond to $\gamma = \frac{1}{2}$. For all three information measures the optimum moves towards the top corner of the triangle for decreasing γ. For γ values below the saturation point the optimum is the top corner, with $\lambda_- = 0$ and $\lambda_1 = 0$.

Knowing the optimal values for λ_+ and λ_-, we compute the min-entropy leakage.

Theorem 7.21. *The min-entropy of the bit S' given R, K and the state $\sigma_{S'}^{RK}$ is*

$$\gamma < \gamma_{\text{sat}}: \quad \mathrm{H}_{\min}(S'|\sigma_{S'}^{rk}) = -\log\left(\frac{1}{2} + \frac{1}{2\sqrt{d-1}}\frac{\sqrt{\beta}}{\gamma_{\text{sat}}}\sqrt{2\gamma_{\text{sat}} - \beta}\right) \tag{7.100}$$

$$\gamma \geq \gamma_{\text{sat}}: \quad \mathrm{H}_{\min}(S'|\sigma_{S'}^{rk}) = -\log\left(\frac{1}{2} + \frac{1}{2\sqrt{d-1}}\right). \tag{7.101}$$

Proof: Eq. (2.12) with X uniform becomes

$$\begin{aligned} \mathrm{H}_{\min}(S'|\sigma_{s'}^{rk}) &= -\log\left(\frac{1}{2} + \frac{1}{2}\mathop{\mathbb{E}}_{rk}\left\|\frac{1}{2}\sigma_0^{rk} - \frac{1}{2}\sigma_1^{rk}\right\|_1\right) \\ &= -\log\left(\frac{1}{2} + \frac{1}{4}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1\right) \qquad (r, k \text{ arbitrary}). \end{aligned} \tag{7.102}$$

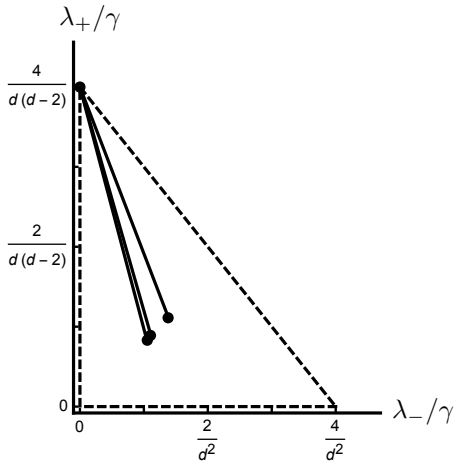

Figure 7.3: *Optimal choice of λ_+ and λ_- at $d = 10$ for the finite size leakage (left line), min-entropy (middle line) and von Neumann entropy (right line). The dashed triangle represents the region for which the eigenvalues λ_+, λ_- and λ_1 are non-negative. The black dots indicate the optimum at $\beta = \frac{1}{2}$ (dots inside the triangle) and $\gamma \leq \gamma_*, \gamma_{\rm sat}, \gamma_0$ (upper corner of the triangle). Not shown in this plot is the $\lambda_0 \geq 0$ constraint which cuts off the upper left corner of the triangle for $\gamma > 2\gamma_{\rm sat}$.*

In the last step we omitted the expectation over r and k since the trace distance does not depend on r, k. Substitution of (7.98) into (7.102) gives the end result. □

Corollary 7.22. *Eve's optimal POVM $\mathcal{T}^{rk} = (T_0^{rk}, T_1^{rk})$ for maximising the min-entropy leakage is given by*

$$T_0^{rk} = \frac{1}{2}\Big(\mathbb{1} + |A\rangle\langle C| + |C\rangle\langle A| - |B\rangle\langle D| - |D\rangle\langle B|\Big) \quad ; \quad T_1^{rk} = \mathbb{1} - T_0^{rk}. \tag{7.103}$$

Proof: The trace distance in Lemma 7.20 is the sum of the positive eigenvalues of $\sigma_0^{rk} - \sigma_1^{rk}$. In the space spanned by $|A\rangle, |B\rangle, |C\rangle, |D\rangle$, the optimal T_0 consists of the projection onto the space spanned by the eigenvectors corresponding to the positive eigenvalues. These eigenvectors are $|v_1\rangle = \frac{|A\rangle+|C\rangle}{\sqrt{2}}$ and $|v_2\rangle = \frac{|D\rangle-|B\rangle}{\sqrt{2}}$. The matrix that projects onto them is $|v_1\rangle\langle v_1| + |v_2\rangle\langle v_2| = \frac{1}{2}|A\rangle\langle A| + \frac{1}{2}|B\rangle\langle B| + \frac{1}{2}|C\rangle\langle C| + \frac{1}{2}|D\rangle\langle D| + |A\rangle\langle C| + |C\rangle\langle A| - |B\rangle\langle D| - |D\rangle\langle B|$. In order to satisfy the constraint $T_0 + T_1 = \mathbb{1}$ and symmetry, half the identity matrix in the remaining $d^2 - 4$ dimensions has to be added to T_0. We mention, without showing it, that (7.103) satisfies the test (2.11). □

As expected, the min-entropy loss decreases as the dimension of the Hilbert space grows. We see that the entropy loss saturates at $\gamma = \gamma_{\rm sat}$; hence RRDPS is secure up to arbitrarily high noise levels when the error correction leakage can be kept low. Figure 7.4 shows the min-entropy leakage as a function of γ.

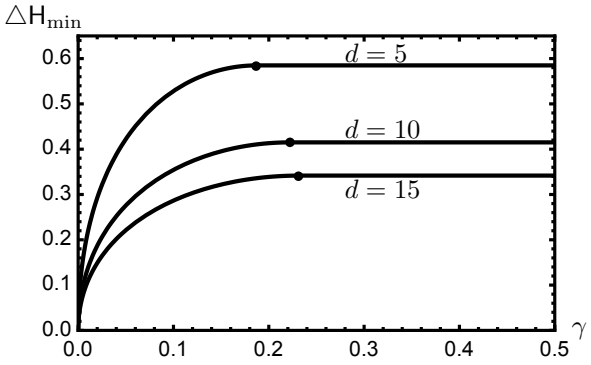

Figure 7.4: *Min-entropy leakage as a function of the bit error rate for $d = 5$, $d = 10$ and $d = 15$. A dot indicates the saturation point γ_{sat}.*

7.13.2 Accessible Shannon information

Lemma 7.23. *Let $X \in \mathcal{X}$ be a uniformly distributed random variable. Let $Y \in \mathcal{Y}$ be a random variable. Let ρ_{xy} be a quantum state coupled to the classical x, y. The Shannon entropy of X given a state ρ_{XY} that has to be measured (for unknown X and Y) is given by*

$$\mathsf{H}(X|\rho_{XY}) = \min_{POVM\ \mathcal{M}=(M_m)_{m\in\mathcal{X}}} \mathop{\mathbb{E}}_{x\in\mathcal{X}} \mathsf{H}\Big(\{\operatorname{tr} M_m \mathop{\mathbb{E}}_{y|x} \rho_{xy}\}_{m\in\mathcal{X}}\Big). \tag{7.104}$$

Proof: We have $\mathsf{H}(X|\rho_{XY}) = \min_{\mathcal{M}} \mathsf{H}(X|Z)$, where Z is the outcome of the POVM measurement $\mathcal{M}$. Z is a classical random variable that depends on X and Y. We can write $\mathsf{H}(X|Z) = \mathsf{H}(X) - \mathsf{H}(Z) + \mathsf{H}(Z|X)$. Since X is uniform, and Z is an estimator for X, the Z is uniform as well. Thus we have $\mathsf{H}(X) - \mathsf{H}(Z) = 0$, which yields $\mathsf{H}(X|\rho_{XY}) = \min_{\mathcal{M}} \mathsf{H}(Z|X) = \min_{\mathcal{M}} \mathbb{E}_x \mathsf{H}(Z|X = x)$. The probability $\Pr[z|x]$ is given by $\Pr[z|x] = \mathbb{E}_{y|x} \Pr[z|xy] = \mathbb{E}_{y|x} \operatorname{tr} M_z \rho_{xy}$. □

Corollary 7.24. *It holds that*

$$\mathsf{H}(S'|RK\sigma_{AS}^{RK}) = \mathop{\mathbb{E}}_{rk} \min_{\mathcal{G}^{rk}=(G_0^{rk},G_1^{rk})} \mathop{\mathbb{E}}_{s'} h(\operatorname{tr} G_m^{rk}\sigma_{s'}^{rk}), \quad m \in \{0,1\} \text{ arbitrary.} \tag{7.105}$$

Proof: Application of Lemma 7.23 yields

$$\begin{aligned} \mathsf{H}(S'|RK\sigma_{AS}^{RK}) &= \mathop{\mathbb{E}}_{rk} \min_{\mathcal{G}^{rk}=(G_0^{rk},G_1^{rk})} \mathop{\mathbb{E}}_{s'} H(\{\operatorname{tr} G_m^{rk} \mathop{\mathbb{E}}_{as|s'} \sigma_{as}^{rk}\}_{m\in\{0,1\}}) \\ &= \mathop{\mathbb{E}}_{rk} \min_{\mathcal{G}^{rk}=(G_0^{rk},G_1^{rk})} \mathop{\mathbb{E}}_{s'} H(\{\operatorname{tr} G_m^{rk}\sigma_{s'}^{rk}\}_{m\in\{0,1\}}) \end{aligned} \tag{7.106}$$

where in the last step we used the definition of $\sigma_{s'}^{rk}$. Finally, the Shannon entropy of a binary variable is given by the binary entropy function h, where $h(1-p) = h(p)$. □

From Corollary 7.24 we see that the POVM $\mathcal{T}^{rk}$ associated with the min-entropy also optimizes the Shannon entropy: maximizing the guessing probability $\operatorname{tr} G_{s'}^{rk}\sigma_{s'}^{rk}$ minimizes the Shannon entropy.

Theorem 7.25. *The Shannon entropy of Alice's bit S' given the state σ_{AS}^{RK}, R and K is:*

$$\gamma < \gamma_{\rm sat}: \qquad \mathsf{H}(S'|RK\sigma_{AS}^{RK}) = h\left(\frac{1}{2}+\frac{1}{2\sqrt{d-1}}\frac{\sqrt{\gamma}}{\gamma_{\rm sat}}\sqrt{2\gamma_{\rm sat}-\gamma}\right). \quad (7.107)$$

$$\gamma \geq \gamma_{\rm sat}: \qquad \mathsf{H}(S'|RK\sigma_{AS}^{RK}) = h\left(\frac{1}{2}+\frac{1}{2\sqrt{d-1}}\right). \quad (7.108)$$

Proof: The min-entropy result (7.100,7.101) can be written as $\mathrm{H}_{\min}(S'|RK\sigma_{S'}^{RK}) = -\log \mathrm{tr}\, T_{s'}^{rk}\sigma_{s'}^{rk}$, so we already have an expression for $\mathrm{tr}\, T_{s'}^{rk}\sigma_{s'}^{rk}$. Substitution of $\mathcal{T}^{rk}$ for $\mathcal{G}^{rk}$ in (7.105) yields the result. □

Since the optimal POVM for min- and Shannon entropy are the same, saturation occurs at the same point ($\gamma = \gamma_{\rm sat}$). Figure 7.5 shows the Shannon entropy leakage (mutual information) $I_{\rm AE} = 1 - \mathsf{H}(S'|RK\sigma_{AS}^{RK})$ as a function of γ.

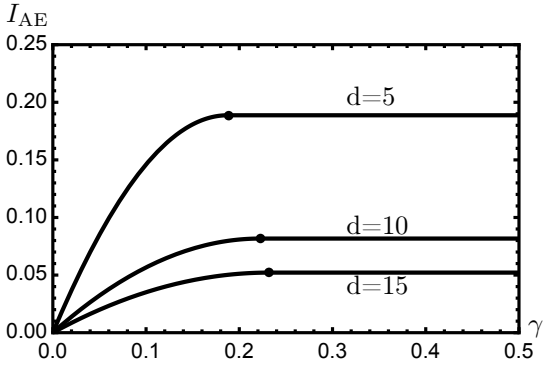

Figure 7.5: *Accessible Shannon entropy as a function of γ for $d = 5$, $d = 10$ and $d = 15$. A dot indicates the saturation point $\gamma_{\rm sat}$.*

7.14 Discussion

7.14.1 Phase error

Sasaki and Koashi [SK17] provided an upper bound on the privacy amplification equal to $h(e^{\rm ph})$, where $e^{\rm ph}$ is the phase error rate. They derived a relation between the phase error rate and the bit error rate, $e^{\rm ph} \leq \inf_{\lambda\geq 0}[\lambda\beta + \max\{\Omega_-(\nu,\lambda), \Omega_+(\nu,\lambda)\}]$, where ν is the photon number and $\Omega_\pm$ are functions which for $\nu = 1$ reduce to $\Omega_-(1,\lambda) = 0$ and $\Omega_+(1,\lambda) = \frac{1}{d-1} - \lambda\frac{d-2}{2(d-1)}$. At $\nu = 1$ the optimal λ is $\frac{2}{d-2}$, yielding $e^{\rm ph} \leq \frac{2\beta}{d-2}$ and thus an upper bound of $h(\frac{2\beta}{d-2})$ on the privacy amplification.

7.14.2 Comparison

We first compare our asymptotic result (Theorem 7.13) with the asymptotic $h(\frac{2\beta}{d-2})$ of [SK17]. For all $\beta \in [0, \beta_0]$ and $d > 2$ it holds that

$$(1-2\beta)h(\tfrac{2\beta}{(d-2)(1-2\beta)}) \leq h(\tfrac{2\beta}{d-2}). \quad (7.109)$$

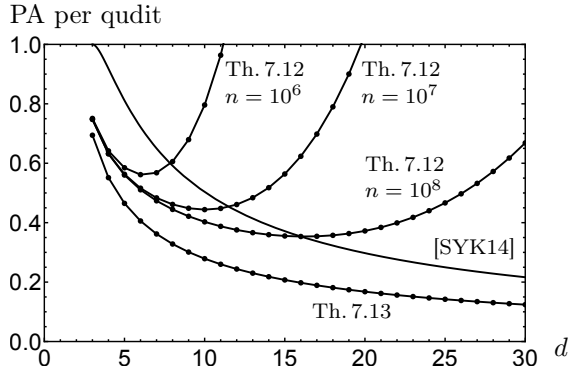

Figure 7.6: *Saturated privacy amplification (PA) per qudit as a function of d. Here we ignore the leakage due to the syndrome to compare with existing results. Comparison of [SYK14] and our finite size and asymptotic results (Theorem 7.12 and Theorem 7.13). Our non-asymptotic result is shown for several values of n.*

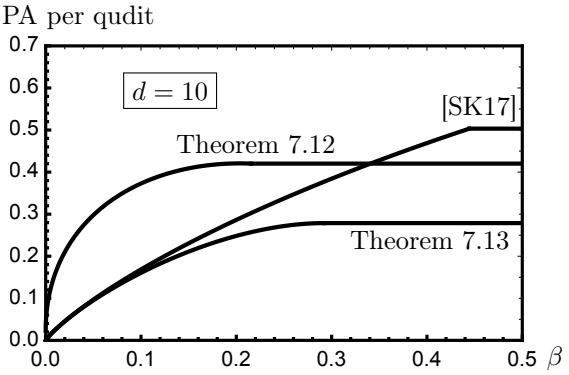

Figure 7.7: *Amount of privacy amplification (PA) per qudit as a function of β, for $d = 10$. Here we ignore the leakage due to the syndrome to compare with existing results. Comparison of our Theorem 7.12 ($n = 10^7$) and Theorem 7.13 versus the privacy amplification of [SK17], which equals $h(\frac{2\beta}{d-2})$ below saturation and $h(\frac{1}{d-1})$ above saturation.*

This is verified as follows. Let $p_0 = 2\beta$, $p_1 = 1 - 2\beta$, $x_0 = 0$, $x_1 = \frac{2\beta}{(d-2)(1-2\beta)}$. The left hand side of (7.109) can be expressed as $p_0 h(x_0) + p_1 h(x_1)$, and the right hand side as $h(p_0 x_0 + p_1 x_1)$. Because h is concave we have $\mathbb{E}\, h(\cdots) \leq h(\mathbb{E}\cdots)$. Thus our von Neumann result is sharper than [SK17].

Note too that our saturation occurs at lower β than in [SK17], especially for small d.

Our Theorem 7.12 is *non-asymptotic*; we cannot compare it to previous results since the previous results are for the asymptotic regime.

Figs. 7.6 and 7.7 show plots of the privacy amplification per qudit. In Fig. 7.6 the post-selection 'price' proportional to $d^4 \frac{\log n}{n}$ is clearly visible; for large d the cost is prohibitive. Interestingly, at small d our non-asymptotic result for the saturated

privacy amplification is sharper than the asymptotic $h(\frac{1}{d-1})$ [SYK14, SK17].

7.14.3 Remarks on the optimal attack

The $\hat{\rho}^{\mathrm{AB}}$ mixed state allowed by the noise constraint has two degrees of freedom, μ and V. While this is more than the zero degrees of freedom in the case of qubit-based QKD [RGK05], it is still a small number, given the dimension d^2 of the Hilbert space.

Eve's attack has an interesting structure. Eve entangles her ancilla with Bob's qudit. Bob's measurement affects Eve's state. When Bob reveals r, k, Eve knows which 4-dimensional subspace is relevant. However, the basis state $|k\rangle$ in Bob's qudit is coupled to $|A_k^a\rangle$ in Eve's space (see appendix 7.A), which is spanned by $d-1$ different basis vectors $|E^+_{(kt')}\rangle$ (Eq. 7.113 with $\lambda_1 = 0$, $\lambda_- = 0$), each carrying different phase information $a_k \oplus a_{t'}$. Only one out of $d-1$ carries the information she needs, and she cannot select which one to read out. Her problem is aggravated by the fact that the $|A_t^a\rangle$ vectors are not orthogonal (except at $\gamma = \frac{1}{2}$). Note that this entanglement-based attack is far more powerful than the intercept-resend attack studied in [Ško17].

7.14.4 Round complexity

The round complexity can be reduced by letting Bob send the syndrome of his measurement result s instead of Alice at the same time as k and r. Alice then performs the noise check. If she finds the noise is sufficiently low, she can send u, c one pass sooner. The bit from which the one-time pad is obtained is then Bob's measurement s instead of Alice's bit s'. This requires a different security proof. Intuitively this should yield the same results. The round complexity of RRRDPS QKD + one-time pad encryption is then equal with or without channel monitoring.

Appendix

7.A Details of Eve's unitary operation

In Theorem 7.26 below we show that Eve does not have to touch Alice's qudit. Hence the attacks that we are describing here can also be carried out in the original (non-EPR) protocol, where Eve gets access only to the qudit state sent to Bob.

Theorem 7.26. *The operation that maps the pure EPR state to $|\Psi^{\mathrm{ABE}}\rangle$ (7.39) can be represented as a unitary operation on Bob's subsystem and Eve's ancilla.*

Proof: Let Eve's ancilla have initial state $|E_0\rangle$. The transition from the pure EPR state to (7.39) can be written as the following mapping,

$$U\Big(|t\rangle_{\mathrm{B}} \otimes |E_0\rangle_{\mathrm{E}}\Big) = |\Omega_t\rangle, \tag{7.110}$$

where $|\Omega_t\rangle$ is a state in the BE system defined as

$$\begin{aligned} |\Omega_t\rangle \quad \stackrel{\mathrm{def}}{=} \quad & \sqrt{\lambda_0}|t\rangle|E_0\rangle + \sqrt{\lambda_1}|t\rangle \sum_{j=1}^{d-1} e^{i\frac{2\pi}{d}jt}|E_j\rangle + \sqrt{\frac{d\lambda_+}{2}} \sum_{t':t'\neq t} |t'\rangle|E^+_{(tt')}\rangle \\ & + \sqrt{\frac{d\lambda_-}{2}} \sum_{t':t'\neq t} |t'\rangle|E^-_{(tt')}\rangle \mathrm{sgn}(t'-t). \end{aligned} \tag{7.111}$$

The notation (tt') indicates ordering of t and t' such that the smallest index occurs first. It holds that $\langle\Omega_t|\Omega_\tau\rangle = \delta_{t\tau}$. Eqs. (7.110,7.111) show that the attack can be represented as an operation that does not touch Alice's subsystem. Next we have to prove that the mapping is unitary. The fact that $\langle\Omega_t|\Omega_\tau\rangle = \delta_{t\tau}$ shows that orthogonality in Bob's space is correctly preserved. In order to demonstrate full preservation of orthogonality we have to define the action of the operator U on states of the form $|t\rangle_{\mathrm{B}} \otimes |\varepsilon\rangle_{\mathrm{E}}$, where $|\varepsilon\rangle$ is one of Eve's basis vectors orthogonal to $|E_0\rangle$, in such a way that the resulting states are mutually orthogonal and orthogonal to all $|\Omega_t\rangle$, $t \in \{0, \ldots, d-1\}$. The dimension of the BE space is d^3 and allows us to make such a choice of $d(d^2-1)$ vectors. □

Theorem 7.27. *Let Alice send the state $|\mu_a\rangle$ to Bob. Let Eve apply the unitary operation U (specified in the proof of Theorem 7.26) to this state and her ancilla. The result can be written as*

$$U\Big(|\mu_a\rangle \otimes |E_0\rangle\Big) = \frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} (-1)^{a_t}|t\rangle \otimes |A^a_t\rangle, \tag{7.112}$$

$$\begin{aligned} |A^a_t\rangle \quad \stackrel{\mathrm{def}}{=} \quad & \sqrt{\lambda_0}|E_0\rangle + \sqrt{\lambda_1} \sum_{j=1}^{d-1} e^{i\frac{2\pi}{d}jt}|E_j\rangle + \sqrt{\frac{d}{2}} \sum_{t':t'\neq t} (-1)^{a_t + a_{t'}} \\ & \Big[\sqrt{\lambda_+}|E^+_{(tt')}\rangle + \sqrt{\lambda_-}\mathrm{sgn}(t'-t)|E^-_{(tt')}\rangle\Big]. \end{aligned} \tag{7.113}$$

The states $|A_t^a\rangle$ *are normalised and satisfy* $\forall_{t\tau:\tau\neq t}\ \langle A_\tau^a|A_t^a\rangle = (1-2\gamma)$.

Proof: We start from $U(|\mu_a\rangle|E_0\rangle) = (1/\sqrt{d})\sum_t(-1)^{a_t}|\Omega_t\rangle$ and we substitute (7.111). Re-labeling of summation variables yields (7.112,7.113). The norm $\langle A_t^a|A_t^a\rangle$ equals $\lambda_0 + (d-1)\lambda_1 + \frac{d(d-1)}{2}\lambda_+ + \frac{d(d-1)}{2}\lambda_-$, which equals 1 since this is also equal to the trace of $\tilde{\rho}^{\mathrm{AB}}$. For $\tau \neq t$ the inner product $\langle A_\tau^a|A_t^a\rangle$ yields

$$\lambda_0+\lambda_1\sum_{j=1}^{d-1}e^{i\frac{2\pi}{d}j(t-\tau)}+\frac{d}{2}\sum_{t'\neq t}\sum_{\tau'\neq\tau}(-1)^{a_t+a_{t'}+a_\tau+a_{\tau'}}\delta_{t'\tau}\delta_{\tau't}[\lambda_+ +\lambda_-\mathrm{sgn}(t'-t)\mathrm{sgn}(\tau'-\tau)]. \tag{7.114}$$

We use $\sum_{j=1}^{d-1}e^{i\frac{2\pi}{d}j(t-\tau)} = d\delta_{\tau t}-1 = -1$. Furthermore the Kronecker deltas in (7.114) set the phase $(-1)^{\cdots}$ to 1 and $\mathrm{sgn}(t'-t)\mathrm{sgn}(\tau'-\tau) = \mathrm{sgn}(\tau-t)\mathrm{sgn}(t-\tau) = -1$. Finally we use $\lambda_0 - \lambda_1 = 1-2\gamma-V$ and $\lambda_+ - \lambda_- = 2V/d$. □

Theorem 7.27 reveals an intuitive picture. In the noiseless case ($\gamma = 0$) it holds that $\forall_t\ |A_t^a\rangle = |E_0\rangle$, i.e. Eve does nothing, resulting in the factorised state $|\mu_a\rangle|E_0\rangle$. In the case of extreme noise ($\gamma = \frac{1}{2}$) we have $\langle A_t^a|A_\tau^a\rangle = \delta_{t\tau}$, which corresponds to a maximally entangled state between Bob and Eve.

Corollary 7.28. *The pure state (7.112) in Bob and Eve's space gives rise to the following mixed state* ρ_a^{B} *in Bob's subsystem,*

$$\rho_a^{\mathrm{B}} = (1-2\gamma)|\mu_a\rangle\langle\mu_a| + 2\gamma\frac{\mathbb{1}}{d}. \tag{7.115}$$

Proof: Follows directly from (7.112) by tracing out Eve's space and using the inner product $\langle A_\tau^a|A_t^a\rangle = (1-2\gamma)$ for $\tau \neq t$. □

From Bob's point of view, what he receives is a mixture of the $|\mu_a\rangle$ state and the fully mixed state. The interpolation between these two is linear in γ. Note that the parameters μ, V are not visible in ρ_a^{B}.

7.B Optimization for the min-entropy

Here we prove that (7.96,7.97) maximizes (7.99). We first show that (7.99) is concave and obtain the optimum for $\gamma \geq \gamma_{\mathrm{sat}}$. Then we take into account the constraints on the eigenvalues and derive the optimum for $\gamma < \gamma_{\mathrm{sat}}$.

Unconstrained optimization. For notational convenience we define

$$w_1 = \sqrt{d\lambda_+ + 2\gamma - \frac{d^2}{2}(\lambda_+ + \lambda_-)} \tag{7.116}$$

$$w_2 = \sqrt{d\lambda_- + 2(1-\gamma) - \frac{d^2}{2}(\lambda_+ + \lambda_-)}. \tag{7.117}$$

This allows us to formulate everything in terms of λ_+ and λ_-. Eq. (7.99) becomes

$$\frac{1}{2}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1 = \sqrt{d\lambda_-}w_1 + \sqrt{d\lambda_+}w_2. \tag{7.118}$$

Next we compute the derivatives,

$$\frac{\partial}{\partial\lambda_+}\left\|\sigma_0^{rk}-\sigma_1^{rk}\right\|_1 = -\frac{d^2}{2}\frac{\sqrt{\lambda_+}}{w_2}+\frac{w_2}{\sqrt{\lambda_+}}+(d-\frac{d^2}{2})\frac{\sqrt{\lambda_-}}{w_1}. \tag{7.119}$$

$$\frac{\partial}{\partial\lambda_-}\left\|\sigma_0^{rk}-\sigma_1^{rk}\right\|_1 = -\frac{d^2}{2}\frac{\sqrt{\lambda_-}}{w_1}+\frac{w_1}{\sqrt{\lambda_-}}+(d-\frac{d^2}{2})\frac{\sqrt{\lambda_+}}{w_2}. \tag{7.120}$$

Setting both these derivatives to zero yields a stationary point. Setting $w_1\sqrt{\lambda_+}\frac{\partial}{\partial\lambda_+}\left\|\sigma_0^{rk}-\sigma_1^{rk}\right\|_1 - w_2\sqrt{\lambda_-}\frac{\partial}{\partial\lambda_-}\left\|\sigma_0^{rk}-\sigma_1^{rk}\right\|_1$ to zero gives $\lambda_+w_1^2-\lambda_-w_2^2=0$, which describes a hyperbola

$$(\tfrac{1}{2}d^2-d)(\lambda_-^2-\lambda_+^2)+2\gamma\lambda_+-2(1-\gamma)\lambda_-=0. \tag{7.121}$$

Next, the equations $\sqrt{\lambda_+}w_1w_2\frac{\partial}{\partial\lambda_+}\left\|\sigma_0^{rk}-\sigma_1^{rk}\right\|_1=0$ and $\sqrt{\lambda_-}w_1w_2\frac{\partial}{\partial\lambda_-}\left\|\sigma_0^{rk}-\sigma_1^{rk}\right\|_1=0$ can both easily be written in the form $\frac{w_2}{w_1}=expression$. Equating these two expressions gives us another hyperbola,

$$\left(d^2\lambda_+ + \frac{d^2}{2}\lambda_- - d\lambda_- - 2(1-\gamma)\right)\left(d^2\lambda_- + \frac{d^2}{2}\lambda_+ - d\lambda_+ - 2\gamma\right) - \lambda_-\lambda_+(d-\frac{d^2}{2}) = 0. \tag{7.122}$$

The stationary point lies at the crossing of these two hyperbolas. There are four crossing points,

$$\lambda_+ = 0 \quad ; \qquad \lambda_- = \frac{4(1-\gamma)}{d(d-2)} \tag{7.123}$$

$$\lambda_+ = \frac{4\gamma}{d(d-2)} \qquad ; \qquad \lambda_- = 0 \tag{7.124}$$

$$\lambda_+ = \frac{1}{2d(d-1)}+\frac{1-2\gamma}{d^2} \qquad ; \qquad \lambda_- = \frac{1}{2d(d-1)}-\frac{1-2\gamma}{d^2} \tag{7.125}$$

$$\lambda_+ = \frac{2+d(1-2\gamma)}{2d^2} \qquad ; \qquad \lambda_- = \frac{2-d(1-2\gamma)}{2d^2}. \tag{7.126}$$

In the steps above, we have multiplied our derivatives by λ_+, λ_-, w_1 and w_2; this has introduced spurious zeros that now need to be removed. From (7.119,7.120) it is easily seen that $\lambda_+=0$ and $\lambda_-=0$ are never stationary points since the derivatives diverge near these values. Furthermore, we find that substitution of (7.126) into the derivatives does not yield two zeros. Expression (7.125) is the only stationary point. As the function value lies higher there than in other points, we conclude that $\left\|\sigma_0^{rk}-\sigma_1^{rk}\right\|_1$ is concave.

Constrained optimization. The optimization problem is constrained by the fact that the λ eigenvalues are non-negative. For $\gamma\geq\gamma_{\rm sat}$ the stationary point satisfies the constraints and hence is the optimal choice for $\gamma\geq\gamma_{\rm sat}$.

For $\gamma<\gamma_{\rm sat}$ the stationary point has $\lambda_-<0$, i.e. it lies outside the allowed region. Because of the concavity the highest function value which satisfies the constraints occurs at $\lambda_0=0$, $\lambda_1=0$, $\lambda_+=0$ or $\lambda_-=0$. It is easily seen that $\lambda_0\geq0$ implies $\lambda_+\leq\frac{1}{d-1}-\frac{2\gamma}{d}$ and $\lambda_1\geq0$ implies $\lambda_+\leq\frac{4\gamma}{d(d-2)}-\frac{d}{d-2}\lambda_-$ and $\lambda_-\leq\frac{4\gamma}{d^2}-\frac{d-2}{d}\lambda_+$.

In the range $\gamma < \gamma_{\text{sat}}$ it holds that $\frac{4\gamma}{d(d-2)} < \frac{1}{d-1} - \frac{2\gamma}{d}$; hence the λ_0-constraint is irrelevant in this region. We get $\lambda_1 = 0$ when $\lambda_+ = \frac{4\gamma}{d(d-2)} - \frac{d}{d-2}\lambda_-$. Substitution gives $\frac{1}{2}\left|\left|\sigma_0^{rk} - \sigma_1^{rk}\right|\right|_1 =$
$\frac{\sqrt{2}}{d-2}\sqrt{2(1-\gamma) + d(1-2\beta + d\,(1-2\gamma(d-1)\lambda_-))\,(d^2\lambda_- - 4\beta)}$ which has its maximum at $\lambda_- = 0$ for non-negative values of λ_-. So either $\lambda_- = 0$ or $\lambda_+ = 0$. This leaves two options for the maximum at low γ,

$$\lambda_+ = 0; \lambda_- = \frac{4\gamma}{d^2} \quad \Rightarrow \quad \frac{1}{2}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1 = 0. \tag{7.127}$$

$$\lambda_- = 0; \lambda_+ = \frac{4\gamma}{d(d-2)} \quad \Rightarrow \quad \frac{1}{2}\left\|\sigma_0^{rk} - \sigma_1^{rk}\right\|_1 = 2\sqrt{2}\frac{\sqrt{\gamma(d-2) - 2\beta^2(d-1)}}{d-2} \tag{7.128}$$

Clearly (7.128) is the larger of the two and therefore the optimal choice.

Chapter 8
General discussion

The end
Even in the presence of a lot of noise, Alice and Bob can communicate again. Yet, here we lose track of their story. They may have gotten into a fight and never said another word to each other. They may have fallen in love and may be living together at an undisclosed location. Unfortunately, for privacy reasons we can't discuss any of the details, except to say this: Alice and Bob live happily ever after.

8.1 The road traveled

We started out with a clear set of properties we would like a quantum encryption protocol to have. These desiderata from Section 1.5 are not always easy to achieve simultaneously. In each chapter we have focussed on one or a few of these goals.

Our first protocol (Chapter 3) is a quantum key recycling protocol that reduces the *round complexity* compared to QKD and at the same time tries to achieve a good *rate* and *noise resilience*. The resulting scheme QKR of Chapter 3 achieves the same asymptotic rate as quantum key distribution with one-way post-processing. This is $1 - h(1 - \frac{3}{2}\beta, \beta/2, \beta/2, \beta/2)$ when using the 6-state encoding and $1 - 2h(\beta)$ when using the BB84 encoding. The QKR scheme sends along a classical ciphertext as well as classical side-information for error correction and authentication. Compared to QKD the initial key material is increased. In scenarios where only a small amount of initial key material is available, six-state QKD might be the better option (initially), while QKR thrives when low round complexity is of importance.

In the EQKR scheme of Chapter 4 we construct a quantum key recycling protocol from which we have removed almost all the classical communication of QKR. The only classical communication remaining is a single authenticated feedback bit from Bob to Alice. We achieve this without compromising in terms of *round complexity*, *rate* and *noise resilience*. In addition, compared to QKR, EQKR has improved *key efficiency*; it requires less fresh key material in the reject case. For messages $m \in \mathcal{M}$ and an error correcting code that achieves channel capacity, $\log |\mathcal{M}| + nh(\beta)$ bits have to be refreshed after an unsuccessful communication. The advantages and disadvantages of quantum key recycling compared to quantum key distribution exist for the EQKR scheme as well.

The KRUE scheme of Chapter 5 provides additional *confidentiality guarantees* in the event of *key leakage*. It achieves unclonable encryption with high *rate*. Yet compared to QKR and EQKR the rate is reduced. The best efficiency is achieved when EQKR is used for the update of key material. The rate is $\frac{(1-2h(\beta))^2}{1-h(\beta)}$ for the BB84 encoding and $\frac{[1-h(1-\frac{3\beta}{2},\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})]^2}{1-h(1-\frac{3\beta}{2},\frac{\beta}{2},\frac{\beta}{2},\frac{\beta}{2})+h(\beta)}$ for the 6-state encoding. These rates are positive in the same β-interval as QKD. Like EQKR, KRUE has low *round complexity* and *no classical communication* from Alice to Bob. The confidentially guarantee in the event of key leakage is an advantage over QKD and QKR independent of communication efficiency.

The VSUE scheme of Chapter 6 achieves *confidentiallity guarantees* in the event of *key leakage* beyond KRUE and the unclonable encryption scheme by Gottesman. It achieves vulnerable-sender unclonable encryption. To achieve this, a compromise on the efficiency in terms of *round complexity*, *rate*, *classical communication* and *noise resilience* is made. Due to the two-way nature of the scheme, the *initial key material* is reduced which automatically limits the key material wasted in the reject case. Use of the VSUE scheme only makes sense in a vulnerable-sender setting or in a scenario where the shared key material has only temporary confidentiality. In those scenarios it does provide a unique security property.

The RRDPS QKD scheme of Chapter 7 achieves key distribution with improved noise resilience. Our contribution is the application of a different proof technique which yields a higher *rate* without significantly impacting the other aspects of the scheme. The rate achieved is $1 - h(\beta) - (1 - 2\beta)h(\frac{1}{d-2} \cdot \frac{2\beta}{1-2\beta})$ up to the noise saturation value β_0, after which β is replaced by β_0 in the last term of the rate formula. The RRDPS scheme is the only scheme discussed in this thesis that does not use qubit operations. However, the proposed implementation [SYK14] works with widely available current day technology and is a remarkably simple way to take advantage of high-dimensional quantum states.

Throughout the thesis we have not placed much emphasis on reducing initial key sizes. We list the achievements of the discussed protocols in terms of our desiderata in Table 8.1. The rates of the protocols are plotted in Figure 8.1. Some unexplored possibilities to improve upon the protocols presented in this thesis are presented in Section 8.2.

8.2 Roads untraveled

8.2.1 Quantum memory

All the protocols presented in this thesis can be implemented with currently widely available technology. Without speculation when quantum computers might start performing useful operations, one can imagine a time in the not so distant future when quantum memory becomes stable, cheap and widely available as well. Techniques like entanglement purification [BBPS96], then allow for protocols that first establish good EPR pairs before performing any measurements. In such a scenario, unclonable encryption is much easier to achieve. We may think of these quantum memories as being unclonable. In such a setting it is no longer true that vulnerable-receiver

Chapter	**2**	**3**	**4**	**5**	**6**	**7**
Name	QKD	QKR	EQKR	KRUE	VSUE	RRDPS
Rate	$1-J$	$1-J$	$1-J$	$\frac{(1-J)^2}{1-J+h(\beta)}$	$\frac{(1-2J)(1-J)}{1-J+h(2\beta-2\beta^2)}$	$1-h-(1-2\beta)h(\frac{1}{d-2}\frac{2\beta}{1-2\beta})$
Max noise	12.6%	12.6%	12.6%	12.6%	5.0%	50%
Alice # passes	≥ 2	1	1	1	1^*	≥ 2
Classical Alice	yes	yes	no	no	yes	yes
Key size	0	$n(2+h+3\log 3)$	$n(3+3\log 3+J-h)$	$n\big[3+\log 3+f(\beta)\big]$	$n(2+h)$	0
Unclonable	no	no	no	yes	yes + VSUE	no

Table 8.1: *Properties of the protocols discussed in this thesis. The number of quantum states is n. Asymptotic rates are shown for the 6-state encoding (except for RRDPS). $h \stackrel{\text{def}}{=} h(\beta)$ and $J \stackrel{\text{def}}{=} h(1-\frac{3}{2}\beta, \beta/2, \beta/2, \beta/2)$. The RRDPS rate holds up to the saturation point. The maximum noise of RRDPS is in the limit $d \to \infty$. Although the* VSUE *scheme only has one pass by Alice, a quantum channel is used in two directions. For* KRUE *and* VSUE *we give the parameters for the most efficient variant in which the protocol are combined with* EQKR*. Key size are computed with hash seeds with a size of twice the size of the input space. For the key size of* KRUE *we use the definition $f(\beta) \stackrel{\text{def}}{=} h(\beta)(\frac{4}{1-J}-1)-J$.*

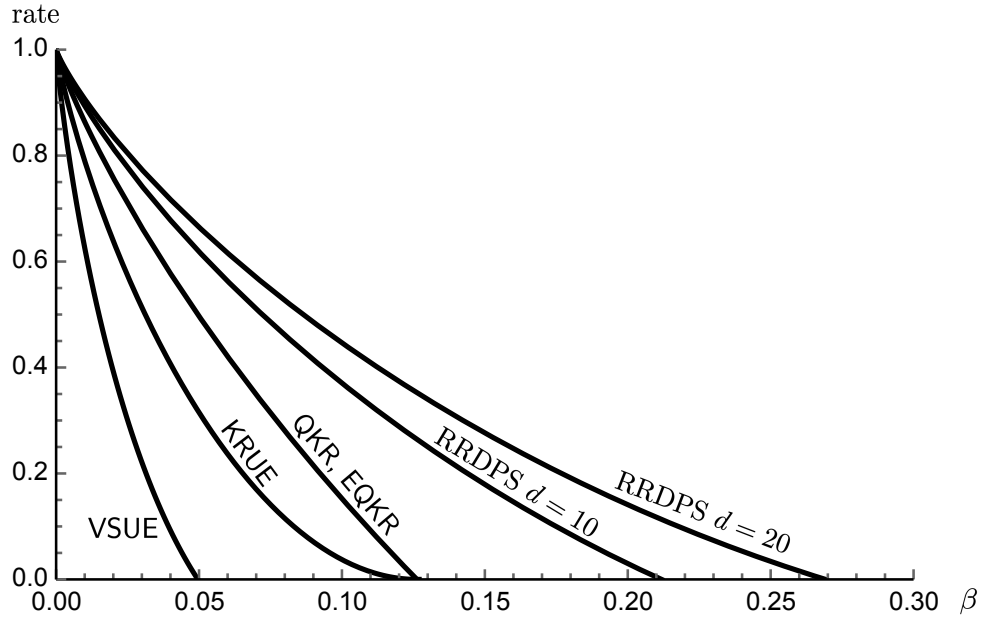

Figure 8.1: Asymptotic rates of the protocols discussed in this thesis. These are rates for the 6-state encoding, except for RRDPS where $d = 10$ and $d = 20$ are shown.

unclonable encryption is impossible. A scheme in which unclonable encryption holds independent of the success of the communication becomes feasible.

When quantum computers become widely available, the high-dimensional scheme of [DPS05] becomes feasible to send quantum states with near optimal key recycling. How to implement this scheme over a noisy channel using good quantum error-correcting codes is an interesting open question.

8.2.2 Communication rate and noise resilience

For QKD it has been worked out how the communication rate as a function of noise can be further increased by two-way post-processing techniques (advantage distillation) as well as noisy preprocessing [Ren05]. As mentioned in Section 2.6.9, this allows the maximum tolerable noise of six-state QKD to be extended from $\approx 12.6\%$ to $\approx 27.6\%$. This same increase can not be achieved by a scheme, like QKR, with low round complexity. The artificial-noise preprocessing technique alone is shown in [Ren05] to increase the maximally tolerable noise of six-state QKD to $\approx 14.1\%$ without requiring two-way post-processing. The analysis is based of the von Neumann entropies of the same states that are relevant for QKR. Thus the same noise resilience should directly translate to an increase in the rates of QKR and EQKR. In KRUE there is an extra penalty due to the leakage of the error correction redundancy which might amplify the negative effect of the noisy preprocessing. The effects of noisy preprocessing on the KRUE, VSUE and RRDPS schemes are an interesting

open question.

The rate reduction of KRUE compared to QKR, EQKR and QKD is caused by a double penalty due to the leakage and initial protection of the redundancy bits. Two modifications to increase the rate of KRUE are suggested in Section 5.10. However, the suggested computation by Alice is not computationally feasible. It remains an open question whether unclonable encryption can be achieved with QKD rate.

The post-selection technique introduces a penalty factor $(n+1)^{d^4-1}$ to the diamond distance where d is the dimension of the quantum states. While this penalty is small for qubit-based schemes (d=2), it becomes problematic (at finite n) for high-dimensional schemes like RRDPS QKD. For a finite number of qudits n and large qudit-dimensions d this term dominates the rate formula. A different way of moving from collective attacks to general attacks that scales better with the qudit-dimension could reduce this penalty. Finding a way to apply the entropy accumulation theorem [DFR20] would be a solution.

An open question mentioned in Chapter 3 is whether the finite size can be increased performing smoothing 'by hand', i.e. describing states that are ε-close to real state that yield a better bound. This option is not explored but has the potential to close the gap between the asymptotic and finite size results and to show how well the asymptotic result can be approximated as a function of n.

8.2.3 Round complexity and classical messages

Quantum key recycling allows Alice to send her message to Bob with minimal interaction. The only interaction required is a feedback bit indicating whether keys can be re-used. Since key material must always be updated in the case of a reject, this feedback is always required. In a scenario where Alice and Bob both have messages to send each other, the feedback bits can be made part of messages encoded in the quantum states and the single remaining classical bit in EQKR and KRUE no longer exists. In terms of round complexity and classical communication, such a 'quantum conversation' is optimal.

When quantum key recycling is used for key distribution on a robust channel, the feedback bit can be delayed until the distributed key is used. The potentially insecure re-use of key material then does not risk the leakage of important information. Alice and Bob would need to make sure no two qubits using the same key material are in transit at once, e.g. by keeping track of the timing. Such a scheme shows key recycling can be used for efficient key distribution as well.

Removing classical communication from the two-way scheme VSUE is non-trivial. Alice should avoid sending useful information until she is confident the noise on the first channel is sufficiently low. One can imagine a variant of VSUE where Alice, instead of checking the noise after responding to all the incoming qubits, keeps track of the error rate of the incoming qubits while she is responding. If the error rate ever exceeds the threshold (after a sufficient number of qubits) she aborts and ignores the remainder of the qubits. When the message is embedded into the qubits as in KRUE, the privacy amplification guarantees that the message doesn't leak if only a fraction of qubits is sent (and available to Eve). The error correction information and noise information can be encoded into the qubits to remove the remaining classical

communication. This modification potentially increases the amount of test qubits required in exchange for the abolishment of classical communication.

The noise resilience property of RRDPS would be a wonderful property for a QKR scheme. A QKR scheme with noise resilience up to 50% would imply the feedback bit is no longer required for confidentiality. However, as already argued above, this is known to be impossible since least some key material needs to be refreshed when the message fails to arrive. Nevertheless we have tried to construct (in unpublished work) a key recycling scheme inspired by RRDPS. It requires Alice and Bob to share a key $v \in \{0,1\}^{d-1}$. Either v or $\bar{v}$ is encoded into the qubits instead of the random string a. The key v is recycled for future rounds. Unfortunately, the noise resilience requires that most of the d-dimensional state encodes information that is useless to Eve. When the qudits sent from Alice to Bob contain information on the message as well as the key, it becomes increasingly easy for Eve to gain some useful information. Although we were able to construct a secure protocol in this fashion, we found that it does not yield any advantages over the qubit-based schemes QKR and EQKR. In particular its noise resilience is worse. For $d = 3$ the rate is positive up to $\approx 5\%$. This number drops for increasing d.

8.2.4 Key size

The focus of this thesis has not been the minimization of the key size. The key size increases when moving from QKD to QKR. Nevertheless, measures can be taken to try to minimize the key size in QKR schemes.

All protocols discussed use pairwise independent hash functions. For a hash $\Phi_u : \{0,1\}^n \to \{0,1\}^\ell$, the size of the seed u used can be decreased. from $\log |\mathcal{U}| = n+\ell$ to potentially $\log |\mathcal{U}| = 2\ell$ by switching from pairwise-independent to almost-pairwise independent hash functions [Sti94]. For protocols that mask the non-uniformity of the message, step 4 of the proof method works for universal hash functions and almost-universal hash functions as well, just like the leftover hashing lemma [Ren05, TSSR11]. Universal hash functions further reduce the size of the hash seed.

When using the six-state and eight-state encodings, the basis choice has more than one bit of entropy ($\log 3$ and 2 respectively). However, Eve can at most learn one bit of information from a qubit. It should therefore be possible for Alice and Bob to share the n bits of initial amount of key material when using the six-state or eight-state encodings like they do when using the BB84 encoding. They would need to extend their key of length n to $n \log 3$ or $2n$ without negatively impacting the security of the QKR scheme reducing their initial key material.

Another open question is whether it is possible to do unclonable encryption with low key sizes. Both KRUE and VSUE have quite large key sizes. A big contribution comes from the fact that our way of performing privacy amplification in a reversible manner uses a shared hash seed. Finding a way of doing privacy amplification without a shared hash seed could reduce the key material in both schemes significantly.

8.2.5 Unclonability

There is a close relation between unclonable encryption and quantum key recycling. In Lemma 5.1 we saw that our definition of key re-use implies unclonable encryption.

An open question is whether such a statement is also true for other proof techniques. In particular the one used in [FS17] in which the entropy of the basis key decreases after every use.

In Chapter 6 we comment on the impossibility of extending the unclonability property to a vulnerable-receiver scenario with a prepare-and-measure scheme. Extending the confidentiallity guarantees beyond vulnerable-sender unclonable encryption does not seem possible for a prepare-and-measure type protocol. Maybe different types of protocols can achieve unclonable encryption or related security properties.

8.3 Limitations

8.3.1 Communication speed

In this thesis we have focused on *rates* defined as message bits per qubit. We have not discussed communication speed in bits per second, which is of course an important real-life consideration. The quantity of interest to obtain high communication speed is the number of qubits per second that can be prepared, sent, measured and processed. In the most common implementation of quantum cryptographic schemes, single photons are sent over an optical fibre. Using good optical cables, single-photon sources and detectors and dedicated hardware for the classical communication, secure communication rates over 10 Mb/s at a distance of 10 km have been achieved in the lab [YPT$^+$18]. Commercial systems available today achieve speeds closer to one Kb/s for distances of about 50 km [idQ].

For the hypothetical chats in the stories of this thesis those speeds are sufficient. But if Alice and Bob want to send a picture of about a MB, this would take too long for modern people with little patience. They can forget about sending videos. This is why many implementations of QKD nowadays are combined with AES rather than one-time pad encryption. The security of the combined scheme is then no longer information-theoretic. This takes away the biggest advantage quantum cryptography has to offer.

8.3.2 Erasures

The biggest downside to the key recycling and unclonable encryption schemes described in this thesis is their bad handling of channel erasures (quantum states failing to arrive). There are two straightforward ways to deal with erasures. (i) Alice sends a random payload and Bob informs Alice where the erasures occurred. This has the drawback that the round complexity increases to the same level as highly-round-optimized QKD. (ii) The qubit payload consists of a codeword from an error correcting code that is able to deal with the expected number of erasures. This has the drawback that the rate of the code suffers dramatically, which simultaneously increases the leakage towards Eve. The end result is a very bad communication rate as a function of β.

An open question is whether the unclonable encryption property can be achieved when the number of erasures on the quantum channel is large. Under such conditions it is infeasible for Alice to know which part of the payload wlll be received by Bob. Any

attempt at error correction will just give more information to Eve, who is hoarding the lost qubits. This seems to be a fundamental problem.

An low-loss optical fibre with an attenuation of 0.15dB/km [BBR$^+$18, Ten16] would mean the errasure rate is < 0.5 at a maximum distance of $1/(0.015 \log 10)$ km $\approx$ 20 km, making QKR and unclonable encryption through optical fibre at larger distances infeasible.

Recently QKD distribution has been experimentally performed from a satellite to a ground station [LCL$^+$17]. In their implementation using weak coherent pulses rather than single photons, they estimate loss due to beam diffraction (22 dB), pointing error (3 dB), atmospheric turbulence and absorption (3-8 dB) to be about 30 dB over a distance of 1200 km. Although this is less loss per kilometer, distances in such an implementation are necessarily larger.

An interesting possibility is to construct a quantum key recycling scheme similar to continuous-variable QKD. This would greatly reduce the erasure rate of the optical channel, potentially opening the door to a more robust implementation. The provable security properties of a continuous-variable QKR scheme are an open question.

Course of life

June 1993	Born in Wageningen, Netherlands
2005 - 2011	Student at Pantarijn Wageningen
2011 - 2014	Bachelor's student in Physics and Astronomy at Utrecht University
2015	CERN Summerschool
2014 - 2016	Master's student in Experimental Physics at Utrecht University
2016 - 2021	PhD student at Eindhoven University of Technology

Summary

Quantum key recycling and unclonable encryption

Quantum cryptography uses the properties of quantum physics to achieve security feats that are impossible with only classical communication. An unknown quantum state cannot be copied or measured without influencing the state. This property is exploited in quantum key distribution (QKD) to establish a secret key between two parties, Alice and Bob, such that they are certain that an eavesdropper, Eve, does not gain any information about their key. Chapter 7 provides a security proof for round robin differential phase shift quantum key distribution, a QKD scheme that is extremely noise resilient. The resulting maximum key rate (key bits established per sent qubit) is higher than previously proven.

When executing a QKD protocol, Alice and Bob communicate classically in multiple rounds to establish their key, followed by the use of classical one-time pad encryption to send a message. In principle there is no need to interact multiple times. The same properties that protect the random key in QKD can be used to protect a message encoded directly into the quantum states. A shared secret key is then used as an encoding basis and is protected by these quantum physical properties as well. To achieve the same efficiency in terms of communication rate, the keys used to encode the qubits can be recycled. Protocols of this form are called quantum key recycling (QKR) schemes. In Chapter 3, a QKR protocol is introduced that for asymptotically many qubits achieves the same communication rate (message bits per qubit) as QKD with one-way postprocessing. A security proof is provided that is composable with other protocols.

QKD and QKR alike make use of information theoretically secure classical tools like one-time pad encryption, message authentication codes, universal hashing and error correcting codes. Often times these tools introduce strings of information that Alice and Bob share over a classical channel. However, since the information Eve can gather from the quantum states is limited and keys can be re-used, there is no fundamental need to communicate classical strings alongside the quantum states. In Chapter 4, a QKR scheme is introduced that removes the need for any classical communication from Alice to Bob without the need to send additional qubits. The only communication from Bob to Alice is a single authenticated feedback bit that indicates the success of the protocol. In the case of unsuccessful communication, only a small amount of fresh key material is required.

When sending a classically encrypted message, e.g. with one-time pad encryption, an attacker is able to intercept the classical ciphertext and keep a copy for a future attack. To keep their communication confidential, the users of the scheme have to make sure that their encryption key does not leak at a later time. The difficulty of deleting information from non-volatile memory makes this a non-trivial task. Unclonable encryption uses keys to encode a message in a quantum state such that the keys can safely become public after a successful instance of the protocol. Chapter 5

introduces an unclonable encryption scheme that also provides key recycling. It uses only simple qubit operations, only quantum states are sent from Alice to Bob and a single authenticated feedback bit is returned. The unclonable encryption and key recycling properties are proven in a composable way and it is shown that the two properties are closely related. The communication rate can be increased by using QKR to refresh some of the key material.

Although unclonable encryption provides an extra security property when it succeeds, in case of failure Alice and Bob have to forever protect their encryption keys, as in classical encryption. Two-way quantum protocols allow for the communication of classical information from Alice to Bob without the need for Alice to know the secret encoding basis. Chapter 6 introduces a two-way unclonable encryption scheme that allows Alice to safely leak her key material regardless of the success or failure of the message transfer. Vulnerable-sender unclonable encryption is defined to guarantee security of the message when all shared key material leaks after successful as well as unsuccessful communication. In the presented two-way scheme, Alice holds only shared key material. Vulnerable-sender unclonable encryption and secure partial key re-use are proven in a composable way. Again, the rate can be increased by combining the protocol with an instance of QKR.

Samenvatting

Sleutelhergebruik en onkloonbaarheid in kwantumcommunicatie

Kwantumfysica is de natuurkundige theorie die de wereld van de zeer kleine deeltjes beschrijft. Op deze kleine lengteschaal geldt een fundamentele wet die we ook kennen als een alledaagse wijsheid: het observeren van een fenomeen verandert het fenomeen. Deze kwantumfysische wet is niet alleen interessant voor de natuurkunde, maar kan ook gebruikt worden voor cryptografische doeleinden.

In dit proefschrift staan drie personages centraal: Alice, Bob en Eve. Alice wil een boodschap versturen naar Bob, zodanig dat Eve de boodschap onmogelijk kan afluisteren. In plaats van gebruik te maken van wiskundige algoritmes, net als de rest van de wereld, gaan Alice en Bob gebruik maken van kwantumfysische deeltjes zoals enkele lichtdeeltjes (fotonen).

Alice en Bob spreken van tevoren een sleutel af die ze gaan gebruiken om de geheime boodschap te versturen. Afhankelijk van de sleutel en de boodschap stuurt Alice de deeltjes naar Bob. Bob gebruikt de sleutel om de deeltjes op de juiste manier te meten en zo de boodschap van Alice te ontvangen. Een sleutel kan bijvoorbeeld bestaan uit de exacte tijdstippen waarop de deeltjes worden verstuurd. Bob leert dan de geheime boodschap uit een meting die de verschillende tijdstippen combineert (interferentie).

Om de communicatie tussen Alice en Bob af te luisteren moet Eve de deeltjes meten voordat Bob dat doet. Maar zonder de sleutel weet ze niet welke metingen ze moet doen om de geheime boodschap te achterhalen. Als ze toch probeert om de deeltjes te meten kan ze dat niet doen zonder iets aan de deeltjes te veranderen. Dit wordt gegarandeerd door de eerder genoemde wet van de kwantumfysica. Door deze verandering op te merken weten Alice en Bob wanneer Eve heeft geprobeerd af te luisteren en wanneer niet. Als Alice en Bob zeker zijn dat hun communicatie niet is afgeluisterd weten ze dat Eve de geheime boodschap niet kent én dat ze de sleutel niet heeft geleerd. De volgende keer dat Alice en Bob willen communiceren kunnen ze dezelfde sleutel veilig hergebruiken.

In Hoofdstuk 3 van dit proefschrift wordt een kwantumcommunicatie-protocol met herbruikbare sleutels voorgesteld dat enkel gebruik maakt van technieken die vandaag de dag beschikbaar zijn. Het voorgestelde protocol heeft minder deeltjes nodig om een gegeven boodschap te versturen dan eerder bekende protocollen met sleutelhergebruik.

Het protocol van Hoofdstuk 3 gebruikt naast het versturen van kwantumdeeltjes ook klassieke communicatie, bijvoorbeeld voor het corrigeren van fouten in de ontvangen boodschap van Bob. Hoofdstuk 4 introduceert een sleutelhergebruik protocol zonder klassieke communicatie waarbij dus enkel kwantumdeeltjes worden verstuurd. Ten opzichte van Hoofdstuk 3 blijft het aantal deeltjes en de technologische complexiteit gelijk.

Bij klassieke communicatie kan Eve alle berichten van Alice en Bob kopiëren. Ook nadat het protocol is beëindigd moet worden voorkomen dat Eve de sleutel in handen krijgt. De klassieke berichten en de sleutel zijn samen immers voldoende om de geheime boodschap ook achteraf te ontcijferen. Bij kwantumcommunicatie hoeft dit niet het geval te zijn. Als Alice en Bob weten dat Eve de deeltjes niet heeft gemeten dan is zij niet in staat om de boodschap te ontcijferen, zelfs niet als ze op een later moment de sleutel in handen krijgt. Deze eigenschap wordt wel onkloonbaarheid genoemd aangezien Eve niet in staat is om een kopie van communicatie tussen Alice en Bob te bewaren voor een toekomstige aanval (mits de boodschap succesvol overkomt).

Hoofdstuk 5 introduceert een protocol dat onkloonbaarheid heeft en veilig sleutels hergebruikt. Hierdoor wordt het mogelijk om onkloonbare versleuteling te bereiken met hedendaagse technologie zonder dat de sleutel wordt opgebruikt.

Hoofdstuk 6 introduceert een protocol dat onkloonbaarheid heeft bij succesvolle communicatie en bovendien extra veiligheid biedt als de communicatie onsuccesvol is. Bob initieert het protocol door deeltjes naar Alice te sturen. Alice stuurt dan haar geheime boodschap door de deeltjes terug te kaatsen naar Bob op een boodschapafhankelijke manier. Aangezien alleen Bob de initiële toestand van de deeltjes kent is het zo mogelijk om een boodschap van Alice naar Bob te sturen zonder dat Alice over de volledige sleutel beschikt. De veiligheid van de boodschap komt dan niet in gevaar als de kennis van Alice achteraf publiek wordt. Ook niet als de communicatie onsuccesvol blijkt. Deze nieuwe eigenschap krijgt de naam 'kwetsbare-zender onkloonbare versleuteling'.

Hoofdstuk 7 bespreekt de veiligheid van een bestaand protocol dat Alice en Bob in staat stelt om hun hoeveelheid sleutelmateriaal uit te breiden over een kwantumkanaal met veel ruis. Het aantal kwantumdeeltjes dat hiervoor nodig is blijkt lager dan eerder gedacht.

Van alle protocollen in dit proefschrift is de veiligheid bewezen. Het effect van een protocol wordt vergeleken met het effect van een geïdealiseerde versie van dat protocol. Er wordt bewezen dat de kans dat Eve het echte protocol en het ideale protocol van elkaar kan onderscheiden extreem klein is, ook al heeft ze alle mogelijkheden toegestaan door de wetten van de natuurkunde. De bewijzen zijn zodanig dat de sleutels en boodschappen veilig zijn voor ruizige kanalen en veilig blijven als ze worden gecombineerd met andere protocollen.

Bibliography

[ABW09] A. Ambainis, J. Bouda, and A. Winter. Nonmalleable encryption of quantum information. *Journal of Mathematical Physics*, 50(4):042106, 2009, https://doi.org/10.1063/1.3094756. doi:10.1063/1.3094756.

[AM17] G. Alagic and C. Majenz. Quantum non-malleability and authentication. In J. Katz and H. Shacham, editors, *Advances in Cryptology – CRYPTO 2017*, pages 310–341, Cham, 2017. Springer International Publishing.

[AMTdW00] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *Annual Symposium on Foundations of Computer Science*, pages 547–553, 2000.

[BB84] C. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[BBB82] C. Bennett, G. Brassard, and S. Breidbart. Quantum Cryptography II: How to re-use a one-time pad safely even if P=NP. *Natural Computing*, 13:453–458, 2014. Original manuscript 1982.

[BBPS96] C.H. Bennett, H.J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53:2046–2052, Apr 1996. doi:10.1103/PhysRevA.53.2046.

[BBR+18] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.J. Li, D. Nolan, A. Martin, and H. Zbinden. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.*, 121:190502, Nov 2018. doi:10.1103/PhysRevLett.121.190502.

[BCG+02] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In *IEEE Symposium on Foundations of Computer Science*, pages 449–458, 2002. Full version at `http://arxiv.org/abs/quant-ph/0205128`.

[BF02] K. Boström and T. Felbinger. Deterministic secure direct communication using entanglement. *PhysRevLett.89.187902*, 2002.

[BKB04] D. Baron, M. Khojastepour, and R. Baraniuk. How quickly can we approach channel capacity? In *Asilomar Conference on Signals, Systems and Computers*, pages 1096–1100. IEEE, 2004.

[BL20] A. Broadbent and S. Lord. Uncloneable quantum encryption via oracles. In *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, pages 4:1–4:22, 2020.

[BLMR13] N.J. Beaudry, M. Lucamarini, S. Mancini, and R. Renner. Security of two-way quantum key distribution. *Phys. Rev. A*, 88:062302, Dec 2013. URL `https://link.aps.org/doi/10.1103/PhysRevA.88.062302`.

[BOHL+05] M. Ben-Or, M. Horodecki, D. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography*, volume 3378 of *LNCS*, pages 386–406, 2005.

[BPG99] H. Bechmann-Pasquinucci and N. Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. A*, 59:4238–4248, Jun 1999. URL `https://link.aps.org/doi/10.1103/PhysRevA.59.4238`.

[BR03] P. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. *Phys. Rev. A*, 67(4):042317, 2003.

[Bru98] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):3018–3021, 1998.

[CKR09] M. Christandl, R. König, and R. Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys.Rev.Lett.*, 102:020504, 2009.

[CW79] J. Carter and M. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.

[DFR20] F. Dupuis, O. Fawzi, and R. Renner. Entropy accumulation. *Communications in Mathematical Physics*, 379(3):867–913, Sep 2020.

[DPS05] I. Damgård, T. Pedersen, and L. Salvail. A quantum cipher with near optimal key-recycling. In *CRYPTO*, pages 494–510, 2005.

[DS05] Y. Dodis and A. Smith. Correcting errors without leaking partial information. In *ACM STOC*, pages 654–663, 2005.

[DVOW92] W. Diffie, P.C. Van Oorschot, and M.J. Wiener. Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, 2(2):107–125, 1992. doi:10.1007/BF00124891.

[Eke91] A. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661 – 663, 1991.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935. URL `https://link.aps.org/doi/10.1103/PhysRev.47.777`.

[FS17] S. Fehr and L. Salvail. Quantum authentication and encryption with key recycling. In *Eurocrypt*, pages 311–338, 2017.

[Got03] D. Gottesman. Uncloneable encryption. *Quantum Information and Computation*, 3(6):581–602, 2003.

[GP01] D. Gottesman and J. Preskill. Secure quantum key distribution using squeezed states. *Phys. Rev. A*, 63:022309, 2001.

[GS03] S.L. Garfinkel and A. Shelat. Remembrance of data passed: a study of disk sanitization practices. *IEEE Security Privacy*, 1(1):17–27, Jan 2003. doi:10.1109/MSECP.2003.1176992.

[Hol73] A. Holevo. Statistical decision theory for quantum systems. *Journal of multivariate analysis*, 3:337–394, 1973.

[HP02] F. Hansen and G. Pedersen. Jensen's operator inequality. *Bulletin of the London Mathematical Society*, 35, 05 2002.

[idQ] `https://marketing.idquantique.com/acton/attachment/11868/f-021a/1/-/-/-/-/Cerberis%20QKD%20System_Brochure.pdf`.

[KGR05] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret key rate for quantum key distribution protocols using one-way classical communication. *Phys.Rev.Lett.*, 95:080501, 2005.

[KRBM07] R. König, R. Renner, A. Bariska, and U. Maurer. Small accessible quantum information does not imply security. *Phys. Rev. Lett.*, 98:140502, Apr 2007. URL `https://link.aps.org/doi/10.1103/PhysRevLett.98.140502`.

[KRS09] R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans.Inf.Th.*, 55(9):4337–4347, 2009.

[LCA05] H.K. Lo, H. Chau, and M. Ardehali. Efficient Quantum Key Distribution scheme and proof of its unconditional security. *Journal of Cryptology*, 18:133–165, 2005.

[LCL+17] S.K. Liao, W.Q. Cai, W.Y. Liu, L. Zhang, Y. Li, J.G. Ren, J. Yin, Q. Shen, Y. Cao, Z.P. Li, F.Z. Li, X.W. Chen, L.H. Sun, J.J. Jia, J.C. Wu, X.J. Jiang, J.F. Wang, Y.M. Huang, Q. Wang, Y.L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.A. Chen, N.L. Liu, X.B. Wang, Z.C. Zhu, C.Y. Lu, R. Shu, C.Z. Peng, J.Y. Wang, and J.W. Pan. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, 2017. doi:10.1038/nature23655.

[Leu02] D. Leung. Quantum Vernam cipher. *Quantum Information and Computation*, 2(1):14–34, 2002.

[LFMC11] H. Lu, C.H.F. Fung, X. Ma, and Q.y. Cai. Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel. *Phys. Rev. A*, 84:042344, Oct 2011. doi:10.1103/PhysRevA.84.042344.

[LM05] M. Lucamarini and S. Mancini. Secure deterministic communication without entanglement. *Phys. Rev. Lett.*, 94:140501, Apr 2005. doi:10.1103/PhysRevLett.94.140501.

[Lo05] H.K. Lo. Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology*, 2005.

[LŠ18] D. Leermakers and B. Škorić. Optimal attacks on qubit-based Quantum Key Recycling. *Quantum Information Processing*, 2018.

[LŠ19a] D. Leermakers and B. Škorić. Security proof for Quantum Key Recycling with noise. *Quantum Information and Computation*, 19, 2019.

[LŠ19c] D. Leermakers and B. Škorić. Security proof for round-robin differential phase shift QKD. *Quantum Information Processing*, 19(11&12):913–934, 2019.

[LŠ20a] D. Leermakers and B. Škorić. Qubit-based Unclonable Encryption with Key Recycling. 2020. `https://eprint.iacr.org/2020/172`.

[LŠ20b] D. Leermakers and B. Škorić. Two-way unclonable encryption with a vulnerable sender. `https://eprint.iacr.org/2020/172`, 2020.

[LŠ21] D. Leermakers and B. Škorić. Quantum Alice and silent Bob: Qubit-based Quantum Key Recycling with almost no classical communication. *Quantum Information and Computation*, 21(1+2):1–18, 2021.

[LW99] M. Luby and A. Wigderson. Pairwise independence and derandomization. *Foundations and Trends in Theoretical Computer Science*, 1, 1999. doi:10.1561/0400000009.

[Mim19] C. Mims. The day when computers can break all encryption is coming, June 2019. URL `www.wsj.com/articles/the-race-to-save-encryption-11559646737`.

[Moe73] R.T. Moenck. Fast Computation of GCDs. In *Proceedings of the fifth annual ACM Symposium on Theory of Computing*, STOC '73, pages 142–151, New York, NY, USA, 1973. ACM. URL `http://doi.acm.org/10.1145/800125.804045`.

[NC11] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.

[NIS] NIST. `https://www.nist.gov/pml/weights-and-measures/si-units-mass`.

[Por17] C. Portmann. Quantum authentication with key recycling. In J.S. Coron and J.B. Nielsen, editors, *Advances in Cryptology – Eurocrypt 2017*, pages 339–368, Cham, 2017. Springer International Publishing.

[PR14] C. Portmann and R. Renner. Cryptographic security of quantum key distribution. *https://arxiv.org/abs/1409.3525*, 2014.

[Ren05] R. Renner. *Security of quantum key distribution.* PhD thesis, ETH Zürich, 2005.

[RGK05] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys.Rev.A*, 72:012332, 2005.

[RK05] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography*, volume 3378 of *LNCS*, pages 407–425, 2005.

[ŠdV17] B. Škorić and M. de Vries. Quantum Key Recycling with eight-state encoding. (The Quantum One Time Pad is more interesting than we thought). *International Journal of Quantum Information*, 2017.

[SK17] T. Sasaki and M. Koashi. A security proof of the round-robin differential phase shift quantum key distribution protocol based on the signal disturbance. *Quantum Science and Technology*, 2(2):024006, 2017.

[Ško17] B. Škorić. A short note on the security of Round-Robin Differential Phase-Shift QKD, 2017. URL `https://eprint.iacr.org/2017/052.pdf`.

[SP00] P. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys.Rev.Lett.*, 85:441, 2000.

[Sti94] D. Stinson. Universal hashing and authentication codes. *Des. Codes Cryptogr.*, 4:369–380, 1994.

[SYK14] T. Sasaki, Y. Yamamoto, and M. Koashi. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature*, 509:475–478, 2014.

[Ten16] S. Ten. Ultra low-loss optical fiber technology. In *2016 Optical Fiber Communications Conference and Exhibition (OFC)*, pages 1–3, March 2016.

[TL17] M. Tomamichel and A. Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, 07 2017.

[TSSR11] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, 2011.

[WC81] M. Wegman and J. Carter. New hash functions and their use in authentication and set equality. *Journal of computer and system sciences*, 22:265–279, 1981.

[WZ82] W. Wootters and W. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[YPT+18] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A.W. Sharpe, A.R. Dixon, E. Lavelle, J.F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A.J. Shields. 10-mb/s quantum key distribution. *Journal of Lightwave Technology*, 36(16):3427–3433, Aug 2018. doi:10.1109/JLT.2018.2843136.

[ZYCM17] Z. Zhang, X. Yuan, Z. Cao, and X. Ma. Practical round-robin differential-phase-shift quantum key distribution. *New Journal of Physics*, 19:033013, 2017.