Secure delegated storage with quantum protocols

van der Vecht, B.

Award date:
2020

Technische Universiteit Eindhoven

Master's thesis

Secure delegated storage with quantum protocols

Bart van der Vecht

Supervised by

Boris Škorić

Assessment members and supporters

Stefan Wolf

Andreas Hülsing

Alexander Serebrenik

Xavier Coiteux-Roy

February, 2020

Abstract

In this thesis we consider quantum protocols for secure delegated storage of classical data. Specifically, we propose protocols that achieve information-theoretic security, and use a key that is shorter than the data itself. First we define our problem and security definitions, and give an overview of relevant work in the literature of quantum cryptography. Then, after explaining in detail the formalism that we use, we describe two protocols that achieve secure delegated storage. They each use a different approach, and we analyze their security in different ways. However, for both protocols we prove composable, information-theoretic security. We discuss the key lengths that can be achieved for both protocols, and proceed with a general discussion, pointing out directions for further research.

Acknowledgements

I would like to thank my supervisor, Boris Škorić, for the enthusiasm that he had for my project, for fruitful discussions and for detailed feedback on manuscripts. I would also like to thank Stefan Wolf for being a generous host at USI Lugano, and Xavier Coiteux-Roy for helpful discussions and ideas.

Contents

1 Introduction

1.1 Motivation

In this thesis we consider the problem of delegated storage: How to let an untrusted party keep your message for some time without that party managing to learn anything about it? One approach is to simply *encrypt* the whole message with a secret key, and sending the resulting ciphertext to the server. When you want access to the message again, ask back the ciphertext and decrypt it with the key. Such approaches are currently used for example by cloud based storage services using end-to-end encryption.

Typically, an encryption scheme is used that requires only a short key, which is easily stored locally. The security of such a scheme however relies on computational assumptions. While such security conditions are strong enough in most practical cases, and indeed widely considered acceptable, we are here interested in obtaining *information-theoretic* (or *unconditional*) security, meaning that the security cannot be compromised by potential technological or theoretical developments in the future.

Classically, information-theoretically secure encryption schemes require a key that is at least as long as the plaintext. Such a key is not practical for delegated storage, since it requires the client to store at least as many bits as the length of the message. Now the problem of storing your data is replaced by the problem of storing your keys. Information-theoretic security does hence not seem possible if keys are kept short.

Quantum information theory provides more flexibility. One of the properties that sets quantum information apart from classical information is that, in general, it cannot be cloned. This uncloneability provides, together with a suitable (secret) encoding of classical data in a quantum state, a way of tamper-detection: the ability to check whether someone interacted with a quantum state. This then opens up a new kind of security, which could be called *evident* security: If the state passes some tamper check, you *know* that the adversary has not learned anything about the data, but when the state fails the check, you cannot necesarily say anything about security. Perhaps surprisingly, this kind of approach can be achieved with information-theoretic guarantees, but with keys shorter than the data itself.

1.2 Problem statement

We will here make our goal more precise. We consider a client, hereafter called Alice, who has some data as a bitstring of length ℓ. We imagine protocols that allow Alice to transform her data (or message) into a ciphertext, which could be a quantum state. She then sends this ciphertext to a server called Eve, where it will be stored. At a later point in time, Alice should be able to ask back the ciphertext and transform it into her original data. In the box below we list the further requirements that the protocol should satisfy.

The protocol should

- require Alice to remember only a classical key, which is shorter than ℓ,
- allow Alice, when she has retrieved her ciphertext, to check whether Eve tampered with the ciphertext,
- guarantee unconditionally that if Alice verifies that Eve has not tampered too much, her data is authentic and Eve did not learn anything about the data,
- not have to guarantee anything about the authenticity or secrecy of the data if Alice determines that Eve tampered too much.

We stress that we do not require a full *encryption* protocol, which should hide the data from the server in all cases; we have the weaker requirement that the data should be secret only if we know that Eve did not significantly disturb the state.

It is now important to elaborate what we actually mean by information-theoretic security, and what we mean by it in the context of secure delegated storage. A cryptosystem or cryptographic protocol is meant to offer some kind of service, typically the hiding of information from an adversary. To *break* such a protocol could mean various things. In the context of delegated storage we use the following definition.

Definition 1. *An adversary can* ***break*** *a delegated-storage protocol if he can learn any information (apart from its length) about the message without causing noticeable disturbance.*

Note that the adversary might already have some information about the message before the protocol begins; he might know it contains natural language or that is always starts with the same pattern. In this case "breaking" or "learning information" then means that the adversary obtains *new* or *more* information about the message.

Now we can define information-theoretic security for delegated protocols.

Definition 2. *A delegated-storage protocol has* ***information-theoretic*** *or* ***unconditional*** *security if it is impossible to break even if the adversary has unlimited (quantum) computing power and memory.*

Furthermore, *composable* security of a protocol means that is can be safely used within another protocol. A common way to prove composable security is to bound the distance (typically the diamond norm, see Chapter 2) of the protocol to an ideal, perfect version of it. Such a distance represents the distinguishability between the real and the perfect protocol.

We note that the above requirements are impossible to meet using a fully classical protocol, since there is no way to classically detect any tampering by the adversary. In the following section, we give an introduction to *quantum* cryptography and results in the literature that are relevant for solving our problem.

1.3 Quantum cryptography

1.3.1 Overview

Although secure quantum (remote) storage has not had much research, and in practice is not yet feasible, the field of quantum cryptography has gotten quite some attention over the last couple of decades. Wiesner was one of the first to relate quantum mechanics to cryptography by proposing a scheme for quantum money [50]; however, the world was not yet ready for his ideas. In 1984 Bennett and Brassard really started the field of quantum cryptography by introducing the first algorithm for Quantum Key Distribution (QKD), later called BB84 after the inventors. Although QKD has been the flagship of the field as a whole, and has since been widely studied, other ways of exploiting quantum physics for cryptographic tasks include Quantum Key Recycling (QKR), uncloneable encryption, oblivious transfer, delegated computing, revocable commitment, proof-of-deletion, quantum readout of Physically Uncloneable Functions (PUFs) and one-time signatures. (For an overview of many of the non-QKD topics of quantum cryptography, see [8]).

A fundamental difference that sets quantum cryptography apart from the classical case is the ability to check if a malicious party has interacted or *tampered* with some quantum data. This works roughly as follows. The theory of quantum physics tells us that measuring a state that is in a superposition yields a non-deterministic result. Therefore, if a classical bit is *encoded* in a quantum state using an unknown basis (see Chapter 2), any interaction with this state—like measuring it, or entangling it with an ancilla—will likely disturb it. This then leads to disturbance of the classical information inside it, which is called *noise*. Furthermore, the *no-cloning principle* prevents an attacker to make copies of the quantum state. This means that to try and learn anything about the underlying classical data, the attacker must interact with (and disturb) the original quantum state. Using the noise level, or *bit error rate (BER)*, one can get an estimate of the amount of interaction by an attacker, and hence bound the attacker's knowledge. [1]

Tamper detection is indeed widely used in various quantum cryptographic protocols. In QKD for example, typically two honest parties—Alice and Bob—exchange secret classical information with each other by encoding it in quantum states. By checking how much a potential eavesdropper Eve has tampered with these quantum states, they obtain an estimate of how much information Eve might have gotten about the classical data. If the data is determined to still be sufficiently secret, Alice and Bob proceed with extracting a fully secret shared key from it [5, 30, 34].

QKR uses tamper detection to check whether keys can be used again after earlier uses, which might have been eavesdropped on [16, 17, 19, 41, 29]. This can lead to lower key consumption (or higher *rate*), which is not possible classically. Indeed, the well-known *one-time-pad* famously encrypts a message with information-theoretic-security, but is aptly named because there is no guarantee that is can be re-used safely. If, however, a quantum scheme is built around it, the amount of secrecy about the key can be established and parts of the key can safely be re-used.

Uncloneable Encryption has been studied first by Gottesman [22] and later (after having seen no attention for some time) by Broadbent et al [7]. Gottesman's ciphertexts are actually not uncloneable as such, but would merely reveal any tampering by an eavesdropper, which

[1] Such noise can also be introduced by imperfections of the physical channel. However, since the causes cannot be distinguished, all noise is assumed to come from a malicious eavesdropper.

is in fact much like what happens in QKD and QKR. Gottesman's main result is however that the message is still secure even if the keys leak afterwards. Broadbent relabelled the earlier work as *tamper-evident encryption* and herself considered quantum ciphertexts for which it is impossible to create two copies that are both decryptable.

In most of the protocols for one of the above topics, one can make a distinction between a quantum phase and a classical *post-processing* phase. In QKD and QKR, the classical result of the quantum phase is typically called a *raw key*. The honest parties (Alice and Bob) perform *parameter estimation* by calculating the noise of the communicated data; as explained above this is diretly related to an eavesdropper's tampering. If the noise level is too high, the protocol aborts. The reason for this is twofold. Firstly, Alice and Bob generally allow a certain amount of noise (be it due to physical imperfections or an attack), since otherwise, in practice they will abort almost all of the time. Therefore they perform *error-correction*, for example by exchanging a syndrome using a linear error correcting code, such that Alice and Bob end up with the exact same raw key. If the noise is too high, however, trying to correct all errors becomes infeasible if not impossible. Secondly, given a high error rate it cannot be ruled out that an eavesdropper has a considerable amount of information about the raw key. Depending on the subsequent classical *privacy amplification* scheme, it might become impossible to transform the raw key—now too unsecure—into a fully secret key. For a high noise level, the syndrome must be large as well; therefore its publication also decreases the raw key's secrecy considerably. The most common way of performing privacy amplification is to use a seeded *extractor* on the raw key. So-called *strong* extractors have the (perhaps surprising) property that the output is completely uniform to an attacker even if the seed is publicly announced, which is indeed what often happens in QKD or QKR protocols.

1.3.2 Proof techniques

The *correctness* of quantum cryptographic protocols is often defined in a straightforward way: for QKD, Alice and Bob must end up with the exact same key, and for any encryption protocol the message must be perfectly recoverable after encryption and decryption. Error correction, mentioned before, enables correct executions of the protocol even in the presence of noise.

The *security* of such protocols can be seen in multiple ways. For QKD for example, one way to reason about the security is to check the mutual information $I(K;E)$ between the generated key K and Eve's side information E [30, 31, 40]. In the context of *quantum side-information*, however, mutual information has been shown not to be a good security metric [26, 20]. *Universally composable security* of a protocol guarantees that it is still secure in any context, for example when it is used as a subprotocol in a bigger scheme. Universal composability is now the preferred goal for security proofs and has been proven for various QKD schemes [4, 10, 31, 36, 27, 33, 43].

Universally composable security can be proven in multiple ways. First, the (smooth) min-entropy, conditoned on (quantum) side-information, of the key or message could be bounded. More commonly, the concept of *distinguishablility* is used. If the actual scheme is distinguishable from an ideal scheme only with some arbitrarily small probability, the generated key, and its uses (composition) in any other scheme are likewise distinguishable from a perfect key only with small probability. Typically the diamond distance is used to measure the distance from the real protocol to some ideal version.

Over the last few decades, many different security proofs for QKD-like protocols have been produced in the literature. A major technique was introduced by Shor and Preskill [40] where they argued that the following two processes are equivalent:

- Alice generates a raw key uniformly at random, and encodes the bits as qubits in a random basis. She sends the qubits to Bob, who measures them in the correct bases and obtains a copy of Alice's raw key.
- Alice creates EPR pairs (entangled qubits), and sends half of each pair to Bob. Alice and Bob measure their halves in random (but the same) bases, and both obtain a copy of the raw key.

This reasoning implies that for any *prepare-and-measure* protocol (where the honest parties only need to prepare and measure quantum states, but not store them or apply operations on them), we can consider an equivalent *entanglement-based* protocol. In the latter, we consider the eavesdropper Eve preparing EPR pairs, and distributing them to Alice and Bob. Now we directly relate the bit error rate with the noisiness of the EPR pairs that Eve creates. In general, this gives more power to Eve than in the prepare-and-measure protocol, since normally she cannot influence Alice's state; however, security of the entanglement-based protocol—which is often easier to analyze—directly implies security of the prepare-and-measure protocol.

Apart from the above technique, which is widely used in many proofs, we identify two main routes of proving security of a quantum cryptographic protocol. One is based on so-called *entropic uncertainty relations*. These relations formalize the intuition that there is a certain duality between the correlations between Alice and Bob on the one hand and between Alice and Eve on the other: the lower the noise between Alice and Bob, the higher the uncertainty of an eavesdropper is about the raw key. By verifying whether this uncertainty is sufficiently high, one can proceed with privacy amplification. An advantage of this method is that it is *device-independent*, and proves security against *general* attacks (see Chapter 2). A disadvantage is that it is suitable only when using 4-state encoding, since generalizations do not appear to be easily made [6].

Another approach is due to Renner [36, 35, 34] and uses the fact that symmetrization of a quantum state drastically simplifies its analysis. By applying random permutations and Pauli operations on an n-partite quantum state, it becomes statistically equivalent to a factorized state consisting of n equivalent substates. This allows us to only consider a single subsystem for the security analysis. Furthermore, Skoric and others showed [29, 28] that using 8-state encoding and performing random Pauli operations on each such subsystem further simplifies the analysis, since only a single parameter remains: the noise.

The *rate* of QKD is typically written as the ratio ℓ/n between the length ℓ of the generated key and the number of quantum systems (qubits) n that were communicated over the quantum channel. Best known rates are of the form $1 - 2h(\beta)$, where β is the bit error rate (BER) of the quantum channel, and h is the binary entropy function. In practice, the number of qubits is desired to remain low, since they are expensive to use, and therefore the rate should be as high as possible. On the other hand, the amount of classical information that is to be stored or communicated during the protocol, such as the extractor seed or the basis encoding information, is generally deemed less important to minimize. However, research has been done on the topic of efficient QKD, where for example a bias in the basis encoding is used, which not only reduces the required number of qubits, but also decreases

the classical communication complexity for comparing the measurement bases [31].

1.3.3 Related work

Coiteux-Roy and Wolf considered the question of *proving erasure* [13], which can in fact be seen as an extension to our delegated storage. Their idea is to randomly place traps among some data to check for tampering upon retrieval. However, they also considered the task of erasing the data: the server should measure all data in the trap basis and prove that he did so by showing the measurement results of the trap bits.

1.4 Contributions

Inspired by the techniques and results explained above, we introduce two protocols for delegated storage, meeting the requirements as stated in Section 1.2. We prove information-theoretic security (according to Definition 2) for the first Protocol, and show that it is composable by bounding the distance between our protocol and a perfect one. For the second Protocol, we prove security in the Common Random String(CRS) model, without any further assumptions. Again we bound its distance to a perfect variant. The two protocols, Protocol 1 and Protocol 2, are explained in Chapters 3 and 4 respectively.

Both protocols can be seen as a form of Alice (the client) performing QKD with herself in the future, where the server is the quantum channel, and then using the generated key as a one-time pad (OTP) to encrypt her message. Tamper detection allows her to verify the security of the OTP and hence the message. Since the generated key is immediately used already, and since she only checks for tampering after this use, the protocols are in that sense similar to QKR.

Regardless of the similarities with QKD and QKR, there are two main subleties that we need to address for our use case.

- In most schemes for QKD or QKR, privacy amplification is achieved using a *pairwise-independent* (or *universal*) family of hash functions (see Chapter 2). For such families the well-known Leftover Hash Lemma can be used to bound the distance between the protocol and an ideal version of it. However, these families are relatively large; a seed to choose a function from this family needs to be at least as long as the raw key. For our approach to delegated storage, we need Alice to keep the seed herself, so we cannot let her keep such a long seed.
- Furthermore, QKD relies on the fact that first the key is established to be secure, and only then it is used for encryption. In our case, Eve already has access to the ciphertext at the moment when she is attacking the qubits, which might compromise security. Indeed, standard applications of the entropic uncertainty relation in proofs of QKD do not immediately carry over to our scenario, since the extractor output is now also part of Eve's side-information. In QKR, this scenario is handled, but often again with pairwise independent hashing, which is infeasible as explained above.

Protocol 1 solves the problem of long seeds by using a short-seeded quantum-proof extractor. The raw key is encoded with BB84 (4-state) encoding, and we analyze its security using entropic uncertainty relations. We deal with the problem of having the ciphertext already available to the adversary as follows. First we simply assume that the message is completely uniform, in which case the ciphertext does not provide any information about

the OTP (one could see the message as a key hiding the OTP). The resulting security (in terms of diamond distance) is given in Theorem 1. Then, we lift the restriction on the entropy of the message. In the analysis we use the weak bound that the adversary now has an extra ℓ bits of information in the worst case, since we do not necesarily know the exact amount of information she has. This leads to the number of qubits needing to be roughly twice as large. The corresponding security is given in Theorem 2.

Protocol 2 instead depends on the assumption that we are in the Common Random String (CRS) model, which allows us to perform perfect pseudo-random generation of longer keys. With these longer keys we can perform pairwise-independent hashing. Our proof holds for uniform messages. The raw key is encoded with 8-state[41]. Furthermore, we apply symmetrization to simplify our proof. The result (again the diamond distance between the protocol and an ideal one) is given in Theorem 3.

For both Protocols, the security error can be made exponentially small in the message length, by simply making the key material longer, which is commonplace—and indeed intuitive—in cryptographic protocols. However, our restriction that the key length should not exceed the message length must be taken into account. Sections 3.5 and 4.5 discuss attainable key lengths for Protocols 1 and 2 respectively.

2 Formalism

2.1 Mathematical representation of quantum systems

A quantum mechanical system can be described as a Hilbert space $\mathcal{H}$. The state of such a system is a vector in this space and is denoted using Dirac notation, like $|\psi\rangle$. Mixed states represent uncertainty: if a state has probability p_x of being the pure state $|x\rangle$, we write this as the density operator $\rho = \sum_x p_x |x\rangle\langle x|$. We denote by $\mathcal{D}(\mathcal{H}_A)$ the set of density operators on the space $\mathcal{H}_A$. We use the shorthand $\mathbb{E}_x$ to denote $\sum_x p_x$. Subnormalized states are density operators ρ with $\operatorname{tr} \rho < 1$.

Classical random variables are also denoted as density operators. A random variable X taking values in $\mathcal{X}$ is written as $\rho^X = \mathbb{E}_{x\in\mathcal{X}} |x\rangle\langle x|$ or simply $\mathbb{E}_x |x\rangle\langle x|$.

Classical-quantum states (*cq-states*) consist of a classical part and a quantum part, which can be correlated with each other, and often appear in quantum cryptographic settings. For example, there might be a quantum system E that is correlated to the classical variable X, in which case we can describe the whole system as the cq-state $\rho^{XE} = \mathbb{E}_x |x\rangle\langle x| \otimes \rho_x^E$ where ρ_x^E is the quantum state on E given that X takes the value x.

The *trace distance* between two density states ρ and σ is defined as

$$\|\rho - \sigma\|_{\mathrm{tr}} = \frac{1}{2}\|\rho - \sigma\|_1 = \frac{1}{2} \operatorname{tr}\left[\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}\right]. \tag{1}$$

We say that two states ρ and σ are ε-close if their trace distance $\|\rho-\sigma\|_{\mathrm{tr}}$ is at most ε.

A measurement on a quantum system is generally described as a *positive-operator valued measure (POVM)*, which is a set of measurement operators M_x that sum to the identity and are all positive semidefinite.

2.2 Entropies

In cryptographic settings, we often want to reason about the uncertainty about some random variable ρ. Uncertainty can be modelled using entropies. The *Rényi entropy* of order α of a random variable ρ is defined as

$$H_\alpha(\rho) = \frac{1}{1-\alpha} \log \operatorname{tr}(\rho^\alpha) \tag{2}$$

for $\alpha \in (0,1)\cup(1,\infty)$. For a classical variable X with distribution p_x, the above expression evaluates to $\frac{1}{1-\alpha}\log\sum_x p_x^\alpha$, and we will simply write $H_\alpha(X)$ instead of $H_\alpha(\rho^X)$. Taking the limit $\alpha \to 1$ results in the von Neumann entropy $H(\rho) = -\rho \operatorname{tr} \rho$ (or Shannon entropy for classical variables). Other widely-used values are $\alpha = \infty$ resulting in the *min-entropy* and $\alpha = 1/2$ for the *max-entropy*[2].

Often, we want to bound the uncertainty of a variable in the case that an attacker has some side-information about it. This side-information could be a quantum ancillary state that is correlated to the classical variable. For example, in QKD a raw key X is generated, about which an eavesdropper E might have some (quantum) side-information. Eve might do

[2]Sometimes the max-entropy is instead defined as the Rényi entropy of order 0. However, their smooth versions (see Defintition 6) are equivalent up to terms that are logarithmic in the smoothing parameter [25].

some arbitrary operation on her quantum state to obtain information about X. To describe the uncertainty of the eavesdropper about X, given that she has the quantum state ρ^E, *conditional* entropies are used. In general, one can define the conditional Rényi entropy $H_\alpha(A|B)$ for quantum states A and B. Setting $\alpha = 1$ gives the conditional von Neumann entropy

$$H(A|B) = H(A) - H(AB) \tag{3}$$

where $H(AB)$ is the von Neumann entropy of the combined system ρ^{AB}.

Generally, given a state ρ^{AB}, the min-entropy of A conditioned on B is given by

$$H_{\min}(A|B) = -\inf_{\sigma_B} D_\infty(\rho_{AB} \| I_A \otimes \sigma_B) \tag{4}$$

where the infimum ranges over the space B and where the relative entropy D_∞ is defined as $D_\infty(\rho\|\sigma) = \inf\{\lambda \in \mathbf{R} : \rho \leq 2^\lambda \sigma\}$.

We will in the following only consider conditional entropies of a *classical* variable X given an arbitrary (quantum) state E. For these, it is much simpler to define the conditional min-entropy in terms of its operational meaning of the guessing probability[25]:

Definition 3 (See for example [25])**.** *The conditional min-entropy of a classical variable X given arbitrary side-information E is*

$$H_{\min}(X|E) = -\log P_{\text{guess}}(X|E) \tag{5}$$

where P_{guess} is the maximum probability that some party Eve holding the quantum side-information E can guess the values of X, regardless of how clever her attack is.

The conditonal max-entropy can also be written using relative entropies. However, the max-entropy turns out to be the *dual* of the min-entropy [25], which can be seen by the following definition.

Definition 4 (See for example [25])**.** *For a state ρ^{AB}, the max-entropy of A conditioned on B is*

$$H_{\max}(A|B) = -H_{\min}(A|C) \tag{6}$$

for a purification ρ^{ABC} of ρ^{AB}.

The max-entropy also has a simple operational meaning in the context of classical variables. For a classical variable X and a party Bob holding side-information B, $H_{\max}(X|B)$ is the number of extra bits that Bob would need to reconstruct X, given the information he can already get from B.

Renner introduced *smoothed* versions of the min- and max-entropies [37, 34].

Definition 5. *For a state ρ^{XE}, the ε-smooth min-entropy of X conditioned on E is defined as*

$$H^\varepsilon_{\min}(X|E)_\rho = \sup_{\rho'} H_{\min}(X|E)_{\rho'} \tag{7}$$

where the supremum ranges over states ρ' that are ε-close to ρ.

Definition 6. *For a state ρ^{XB}, the ε-smooth max-entropy of X conditioned on B is defined as*

$$H_{\max}^{\varepsilon}(X|B)_{\rho} = \inf_{\rho'} H_{\max}(X|B)_{\rho'} \tag{8}$$

where the infimum ranges over states ρ' that are ε-close to ρ.

2.3 Quantum operations

An operation on a quantum system is modelled as a *completely positive trace-preserving map (CPTP map)*. The following Lemma states that it is impossible to better distinguish two quantum states after processing them in some way.

Lemma 7. *For any CPTP map $\mathcal{E}$ and any states ρ, σ, [32]*

$$\|\mathcal{E}(\rho) - \mathcal{E}(\sigma)\|_{\mathrm{tr}} \leq \|\rho - \sigma\|_{\mathrm{tr}} \ . \tag{9}$$

Furthermore, processing side-information about a random variable cannot decrease the conditional entropy about it.

Lemma 8 (Data-processing inequality [14])**.** *Let X be a classical random variable. For any CPTP map $\mathcal{E}$ that acts on some state Y, and for any $\varepsilon \geq 0$, the following inequalities hold:*

$$H_{\max}^{\varepsilon}(X|Y) \leq H_{\max}^{\varepsilon}(X|\mathcal{E}(Y)) \ , \tag{10}$$
$$H_{\min}^{\varepsilon}(X|Y) \leq H_{\min}^{\varepsilon}(X|\mathcal{E}(Y)) \ . \tag{11}$$

The *diamond distance* is a common way to express the distance between some protocol (expressed as the CPTP map $\mathcal{E}$) and an ideal version $\mathcal{F}$.

Definition 9. *The diamond distance between two CPTP maps $\mathcal{E}$ and $\mathcal{F}$ that both act on a space $\mathcal{H}_A$ is*

$$\|\mathcal{E} - \mathcal{F}\|_{\diamond} = \sup_{\rho^{AC} \in \mathcal{D}(\mathcal{H}_{AC})} \|\mathcal{E}(\rho^{AC}) - \mathcal{F}(\rho^{AC})\|_{\mathrm{tr}} \ . \tag{12}$$

where $\mathcal{H}_C$ is some auxiliary system that can be considered to have the same dimension as $\mathcal{H}_A$ [29].

Definition 10. *The operator norm $\|\cdot\|_{\infty}$ is defined as*

$$\|A\|_{\infty} = \sup\{\sqrt{\langle v| A^{\dagger} A |v\rangle} : v \in \mathcal{H}_A, \langle v|v\rangle \leq 1\} \ . \tag{13}$$

If A has a complete set of eigenvalues $\{\lambda_i\}_i$, the above expression simplifies to $\max_i |\lambda_i|$.

Lemma 11. *For projectors P and Q, $\|PQ\|_{\infty}^2$ is given by*

$$\|PQ\|_{\infty}^2 = \sup\{\langle v| P |v\rangle : v \in \mathcal{H}_A, \langle v|v\rangle \leq 1, |v\rangle \in span\{Q\}\} \ . \tag{14}$$

Proof. First note that $(PQ)^{\dagger} PQ = QPQ$ since P is a projector. We are now interested in which $|v\rangle$ results in the largets value for $\langle v| QPQ |v\rangle$. Let $|w\rangle$ be a vector with $\langle w|w\rangle = 1$ that

is not completely within the subspace spanned by Q. Then Q projects $|w\rangle$ onto $Q|w\rangle = a|u\rangle$ with $|a|^2 < 1$ where $|u\rangle$ is in the subspace spanned by Q. Then we have

$$\langle w| QPQ |w\rangle = |a|^2 \langle u| P |u\rangle \ . \tag{15}$$

However, we could then have chosen $|u\rangle$ to start with, resulting instead in

$$\langle u| QPQ |u\rangle = \langle u| P |u\rangle > \langle w| QPQ |w\rangle \ . \tag{16}$$

So, for any $|w\rangle$ not completely in the subspace spanned by Q we can choose a $|u\rangle$ that is in that subspace such that $\langle u| QPQ |u\rangle > \langle w| QPQ |w\rangle$. This concludes the proof. □

2.4 Entropic uncertainty relations

Entropic uncertainty relations can be seen as generalizations to Heisenberg's uncertainty principle: the more information you have about one measurement outcome, the less information you have about the outcome of an incompatible measurement. Such relations also work for tripartite settings where various parties have different side-information about some random variable, and are useful in security proofs [46, 14, 43].

Definition 12. *The overlap of two POVMs $M = \{M^x\}_x$ and $N = \{N^y\}_y$ is given by*

$$c(M,N) = \max_{x,y} \left\| \sqrt{M^x}\sqrt{N^y} \right\|_\infty^2 \ . \tag{17}$$

We note that other, slightly different, definitions exist for the overlap [14].

Lemma 13 (Entropic uncertainty relation [44], [15])**.** *Let $\varepsilon \geq 0$. Given any tripartite state ρ^{ABE}, for any two POVMs M and M' acting on system A with outcomes X and X' respectively,*

$$H_{\min}^{\varepsilon}(X|E) + H_{\max}^{\varepsilon}(X'|B) \geq \log \frac{1}{c(M,M')} \ . \tag{18}$$

Corollary 14 (See for example [46])**.** *Let ρ^{ABE} be quantum state where $\rho^A \in \mathcal{H}^{\otimes n}$. Let X be the n-bit classical outcome of a measurment of each subsystem of A in the standard basis. Let X' be the n-bit classical outcome of a measurement of each subsystem of A in the Hadamard basis. Then, for any ε, we have*

$$H_{\min}^{\varepsilon}(X|E) + H_{\max}^{\varepsilon}(X'|B) \geq n \ . \tag{19}$$

Proof. A measurement in the standard basis can be written as the POVM

$$M = \{|x\rangle\langle x|\}_{x\in\{0,1\}^n} \ , \tag{20}$$

and a measurement in the Hadamard basis can be written as the POVM

$$M' = \{H|y\rangle\langle y|H\}_{y\in\{0,1\}^n} \ , \tag{21}$$

where H is to be understood as the n-partite operator $H^{\otimes n}$. Then,

$$c(M,M') = \max_{x,y} \left\| |x\rangle\langle x| H |y\rangle\langle y| H \right\|_\infty^2 \ . \tag{22}$$

By Definition 10,

$$c(M, M') = \max_{x,y} \sup\{\langle v| |x\rangle \langle x| H |y\rangle \langle y| H |v\rangle : v \in \mathcal{H}_A, \langle v|v\rangle \leq 1\} . \tag{23}$$

By Lemma 11 we know that the $|v\rangle$ that maximizes the above expression must be in the space spanned by $H|y\rangle\langle y|H$. So for each y, set $|v\rangle = H|y\rangle$. Then,

$$c(M, M') = \max_{x,y} \langle y| H |x\rangle \langle x| H |y\rangle \tag{24}$$

$$= 2^{-n/2} \cdot 2^{-n/2} . \tag{25}$$

Substituting this c into Lemma 13 concludes the proof. □

The following Lemmas are useful for smoothing out an unlikely event.

Lemma 15 (Lemma 6 from [43])**.** *Let $B = (B_1, \ldots B_{n+r})$ be boolean random variables, where $B_i \in \{0,1\}$ for each i, and let $\mathcal{S}$ be a subset of B that is chosen uniformly at random where $|\mathcal{S}| = r$. Then, for any distribution on the B_i, and for any $Q, q \geq 0$,*

$$\Pr_{B,\mathcal{S}}\Big[\sum_{i\in\mathcal{S}} b_i \leq rQ \ \wedge \ \sum_{i\notin\mathcal{S}} b_i \geq n(Q+q)\Big] \leq e^{\frac{-2q^2nr^2}{(n+r)(r+1)}} . \tag{26}$$

Definition 16. *For a classical random variable X taking values in $\mathcal{X}$, an event on X is a function $\Omega : \mathcal{X} \to \{0,1\}$. This allows us to write $\Pr[\Omega]_X = \mathbb{E}_x p_x \Omega(x)$.*

Lemma 17 (Lemma 7 in [43])**.** *Let ρ^{XE} be a (possibly subnormalized) state where X is classical, and let Ω be an event on X with probability $\Pr[\Omega]_\rho = \varepsilon < \text{tr}(\rho^{XE})$. Then there exists a (possibly subnormalized) state σ^{XE} with $\Pr[\Omega]_\sigma = 0$ and $\|\rho^{XE} - \sigma^{XE}\|_{\text{tr}} \leq \sqrt{\varepsilon}$.*

2.5 Hash functions and extractors

Hash functions are typically functions that map long strings to shorter ones, and which are hard to reverse [49]. They can be used for authentication: send a tag containing the hash of your message along with the message itself, and the receiver can check for authenticity by calculating the hash of the received message and comparing it to the tag. Hashing is a form of compression, and can hence also be seen as a form of privacy amplification. Indeed, hashing is often used to transform a partially secret string into a fully secret string.

One property of hash functions is its collision probability, defined as the probability that the hash of two different inputs are equal. In the literature, different terms are used to express various such properties, including *universality, two-universality, strong two-universality* and *pairwise independence*. Here, we use the following definitions.

Definition 18. *A family of functions $\mathcal{F} = \{f : \{0,1\}^n \to \{0,1\}^\ell\}$ is said to be **two-universal** if and only if for a function f chosen uniformly at random from $\mathcal{F}$, and every two $x, x' \in \{0,1\}^n$ such that $x \neq x'$,*

$$\Pr_f[f(x) = f(x')] = 2^{-\ell} . \tag{27}$$

Definition 19. *A family of functions $\mathcal{F} = \{f : \{0,1\}^n \to \{0,1\}^\ell\}$ is said to be* ***strongly two-universal*** *or* ***pairwise independent*** *if and only if for a function f chosen uniformly at random from $\mathcal{F}$, every two $x, x' \in \{0,1\}^n$ such that $x \neq x'$, and for every $z, z' \in \{0,1\}^\ell$ the following two conditions hold:*

$$\Pr\left[f(x) = z\right] = 2^{-\ell} \ , \tag{28}$$

$$\Pr\left[f(x) = z \wedge f(x') = z'\right] = 2^{-2\ell} \ . \tag{29}$$

The following two corollaries will be useful when analyzing Protocol 2. The Kronecker delta $\delta_{x,y}$ is equal to 1 if $x = y$ and 0 otherwise.

Corollary 20. *Consider a pairwise-independent family of hash functions $\mathcal{F}$ of size 2^d. Let f_u be the function in $\mathcal{F}$ indexed by some key $u \in \{0,1\}^d$. Then for every $x \in \{0,1\}^n$ and $z \in \{0,1\}^\ell$,*

$$\frac{1}{2^d} \sum_u \delta_{z, f_u(x)} = 2^{-\ell} \ . \tag{30}$$

Corollary 21. *Consider a pairwise-independent family of hash functions $\mathcal{F}$ of size 2^d. Let f_u be the function in $\mathcal{F}$ indexed by some key $u \in \{0,1\}^d$. Then for every two $x, x' \in \{0,1\}^n$ with $x \neq x'$ and every $z \in \{0,1\}^\ell$,*

$$\frac{1}{2^d} \sum_u \delta_{z, f_u(x)} \delta_{z, f_u(x')} = 2^{-2\ell} \ . \tag{31}$$

Corollary 21 is also a major ingredient in the proof of the Leftover Hash Lemma [23, 45, 2].

Lemma 22 (Leftover Hash Lemma (LHL), see for example [45])**.** *Let $\mathcal{F}$ be a pairwise independent family of functions and let ρ^{XE} be a state where X is classical. Let $Z \in \{0,1\}^\ell$ be the output of $f(X)$ where f is chosen uniformly at random from $\mathcal{F}$ and where μ^Z is the uniform distribution over Z. Then,*

$$\|\rho^{ZE} - \mu^Z \otimes \rho^E\|_{\mathrm{tr}} \leq \frac{1}{2} \sqrt{2^{\ell - H_{\min}(X|E)}} \ . \tag{32}$$

The LHL is often used to directly relate $H_{\min}(X|E)$ (the min-entropy of some raw key X given side-information E) to the number of securely extractable bits ℓ. In general there is an error parameter ε involved, and we can at best achieve roughly $\ell \approx H_{\min}(X|E) - 2\log(1/\varepsilon)$.

In QKD and QKR, choosing a function at random means generating a seed u that indexes the family. This seed, which has length $\log|\mathcal{F}|$, then needs to be communicated or stored. Pairwise-independent families need to have a size of at least 2^n [47], meaning that the seed must be at least as long as the input.

There are also *almost* (strong) 2-universal families. They are defined similary, but with some δ instead of $2^{-\ell}$. The seed lengths are however hardly shorter [42, 21].

Extractors are seeded functions that transform an input X that has a min-entropy of at least k into an (almost-) uniform output Z. Much work has been done on classical extractors (see [38] for an overview). The best known parameters are $d = \log(n-k)+2\log(1/\varepsilon)+O(1)$ and $\ell = k + d - 2\log(1/\varepsilon) - O(1)$ [47]. Pairwise independent families of hash functions are often used to construct extractors, and actually do not have a restriction on the min-entropy of the input.

Definition 23. *A (k,ε)-extractor is a function $Ext : \{0,1\}^d \times \{0,1\}^n \to \{0,1\}^\ell$ with the following property. Given an input $X \in \{0,1\}^n$ with $H_{\min}(X) \geq k$ and a uniform seed $U \in \{0,1\}^d$, the output $Z = Ext(U,X)$ is ε-close to uniform.*

With the introduction of QKD, extractors were needed in the context of *quantum* side-information. Pairwise independent hash functions still work because they do not rely on the min-entropy of the input. For some time it was not clear whether extractors that worked in the presence of classical side-information still worked in the presence of quantum side-information. The first such extractor that proved to be secure was based on Trevisan extractors [18, 39]. Recently, more quantum-proof extractors have been studied [3, 11] and it turns out that quantum-proof extractors exist with virtually optimal paramters [11].

Definition 24. *A (k,ε) quantum-proof extractor is a function $Ext : \{0,1\}^d \times \{0,1\}^n \to \{0,1\}^\ell$ with the following property. Let ρ^{XE} be state where $X \in \{0,1\}^n$ is classical, and E is any quantum state such that $H_{\min}(X|E) \geq k$, and let $U \in \{0,1\}^d$ be chosen uniformly at random and independently of X and E. Let $Z = Ext(U,X)$ be the output of the extractor. Then*

$$\|\rho^{ZE} - \mu^Z \otimes \rho^E\|_{\mathrm{tr}} \leq \varepsilon \ . \tag{33}$$

Lemma 25 (Theorem 1.5 from [11])**.** *For any $\alpha \in (0,1), \varepsilon > 0$, and for any integers n, k with $k \geq \log(n) + \log^{1+\alpha}(1/\varepsilon)$, there exists a (k,ε)-extractor Ext that gives an output of length $\ell = (1-\alpha)k$ and that needs a seed of length $d = O(\log(n/\varepsilon))$.*

Finally, we note that there are also exists the notion of *non-malleable* extractors [12]. These are extractors that are secure even when the attacker knows the seed *and* the extractor output given another seed. However, these are not relevant for delegated storage.

2.6 Encodings

A classical bit $x \in \{0,1\}$ can be encoded in a qubit in multiple ways. Here we consider 4-state (or BB84, or conjugate), 6-state, and 8-state encoding. The encoding of a bit depends on an encoding key, which is an index into a certain basis set. In the following, we call $|0\rangle$ and $|1\rangle$ the basis states of the standard basis.

Definition 26. *4-state encoding uses a basis key $b \in \{0,1\}$. The encoding of bit x with key b is $H^b|x\rangle$. In other words, x is encoded in the standard basis if $b = 0$, and in the Hadamard basis otherwise.*

Definition 27. *6-state encoding uses a basis key $b \in \{0,1,2\}$. The encoding of bit x with*

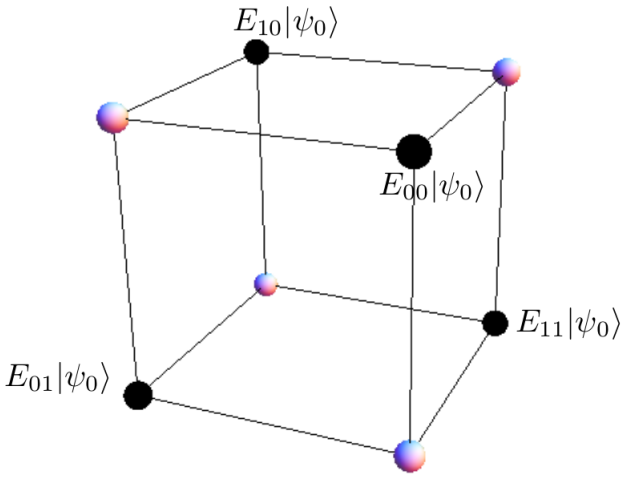

Figure 1: Figure from [41]. The center of the cube is at the center of the Bloch sphere. The labeled (black) points are the locations of the 4 possible encodings (35) of a bit $x = 0$. For each b, the encoding of the bit $x = 1$ is the unlabelled (colored) point opposite it.

key b is

$$\begin{cases} |x\rangle & \text{if } b = 0 \\ \big(\,|0\rangle + (-1)^x\,|1\rangle\,\big)/\sqrt{2} & \text{if } b = 1 \\ \big(\,|0\rangle + (-1)^x i\,|1\rangle\,\big)/\sqrt{2} & \text{if } b = 2 \end{cases} \tag{34}$$

In other words, the three bases correspond to the three axes of the Bloch sphere.

Definition 28. *8-state encoding uses a basis key $b \in \{0,1,2,3\}$ written as $b = 2u + v$ for $u, v \in \{0,1\}$. Let α such that $\cos\alpha = 1/\sqrt{3}$. The encoding of bit x with key b is [28]*

$$\begin{cases} (-\sqrt{i})^x \cos\frac{\alpha}{2}\,|x\rangle + \sqrt{i}^{\,1-x} \sin\frac{\alpha}{2}\,|1-x\rangle & \text{if } b = 0 \\ (-\sqrt{i})^x \cos\frac{\alpha}{2}\,|1-x\rangle + \sqrt{i}^{\,1-x} \sin\frac{\alpha}{2}\,|x\rangle & \text{if } b = 1 \\ \sqrt{i}^{\,x} \cos\frac{\alpha}{2}\,|x\rangle - \sqrt{i}^{\,1-x} \sin\frac{\alpha}{2}\,|1-x\rangle & \text{if } b = 2 \\ \sqrt{i}^{\,x} \cos\frac{\alpha}{2}\,|1-x\rangle - \sqrt{i}^{\,1-x} \sin\frac{\alpha}{2}\,|x\rangle & \text{if } b = 3 \end{cases} \tag{35}$$

In other words, the bases correspond to the 4 diagonals of a cube on the Bloch sphere. The points are visualized in Figure 1.

We can speak of an *encryption* of the classical bit if the qubit does not give any information about the classical value. In other words, without knowing the encoding key, the mixed state representing the encoding is equal for all classical values. In that sense, 8-state encoding is an encryption scheme, but 4-state and 6-state are not.

2.7 Symmetrisation

A *coherent* attack is one where we allow the attacker to perform any quantum operation. In entanglement-based schemes, this could for example mean that the n qubits that Alice receives are (partly) entangled with each other and not independent. A *collective* attack is an attack where the attacker is restricted to treat each qubit individually and equally. Security against collective attacks is much easier to prove. Renner showed that an n-fold quantum state that is invariant under permutations can be written as a factorized state [24, 35]. That is, their subsystems are independent. This has applications in the security analysis of a protocol and has been further developed as the *post-selection* argument [35].

Definition 29. *A quantum map $\mathcal{E}$ acting on a space $\mathcal{H}^{\otimes n}$ is called permutation-symmetric if for all permutations π on the n subsystems of $\mathcal{H}^{\otimes n}$ there exists a map K_π such that $\mathcal{E} \circ \pi = K_\pi \circ \mathcal{E}$.*

Lemma 30 (Post-selection [9])**.** *Let $\mathcal{H}_{ABE}$ be a tripartite quantum state, and let d be the dimension of the AB subsystem. Then for any two permutation-symmetric maps $\mathcal{E}$ and $\mathcal{F}$ acting on $\mathcal{D}(\mathcal{H}_{ABE}^{\otimes n})$,*

$$\|\mathcal{E} - \mathcal{F}\|_\diamond \leq (n+1)^{d^2-1} \max_{\sigma \in \mathcal{D}(\mathcal{H}_{ABE})} \|\mathcal{E}(\sigma^{\otimes n}) - \mathcal{F}(\sigma^{\otimes n})\|_1 \ . \tag{36}$$

We can further simplify the σ states themselves. The singlet state is written as $|\Psi^-\rangle = \frac{1}{\sqrt{2}} |0\rangle_A |1\rangle_B - \frac{1}{\sqrt{2}} |1\rangle_A |0\rangle_B$. Consider giving the A subsystem of this state to Alice and the B subsystem to Bob. For any basis b they both measure in, the outcomes x for Alice and y for Bob will always be anticorrelated. Consider now a *noisy* singlet state, which is a state σ^{AB} such that the probability that Alice and Bob's measurement outcomes do *not* anticorrelate is γ. We state the following Lemma from [36], where $|\Phi^\pm\rangle$ and $|\Psi^\pm\rangle$ are the Bell states.

Lemma 31. *Consider a noisy singlet state σ^{AB} with error rate γ. If both Alice and Bob apply a random (the same) Pauli operator to their subsystems, the resulting state can be written as [36]*

$$\sigma^{AB} = \Big(1 - \frac{3}{2}\gamma\Big) |\Psi^-\rangle \langle\Psi^-| + \frac{\gamma}{2}\Big(|\Phi^-\rangle \langle\Phi^-| + |\Psi^+\rangle \langle\Psi^+| + |\Phi^+\rangle \langle\Phi^+| \Big) \ . \tag{37}$$

We will write the purification E (held by Eve) of a noisy singlet state σ^{AB} as

$$|\Psi^{ABE}\rangle = \sqrt{1 - \frac{3}{2}\gamma}\, |\Psi^-\rangle \otimes |m_0\rangle - \sqrt{\frac{\gamma}{2}}\Big(|\Phi^-\rangle \otimes |m_1\rangle + i\, |\Psi^+\rangle \otimes |m_2\rangle + |\Phi^+\rangle \otimes |m_3\rangle \Big) \tag{38}$$

where the $|m_i\rangle$ form some orthonormal basis in Eve's space.

Now we consider Alice and Bob measuring such a noisy singlet state in one of the bases b of 8-state encoding. After a measurement in basis b, giving outcomes x for Alice and y for Bob, we write Eve's auxiliary state as σ^E_{bxy}.

Define

$$v(b) = \begin{cases} \frac{1}{\sqrt{3}}(1,1,1) & \text{if } b = 0 \\ \frac{1}{\sqrt{3}}(1,-1,-1) & \text{if } b = 1 \\ \frac{1}{\sqrt{3}}(-1,-1,1) & \text{if } b = 2 \\ \frac{1}{\sqrt{3}}(-1,1,-1) & \text{if } b = 3 \end{cases} \tag{39}$$

In [29], expressions are given for Eve's state after a measurment by Alice and Bob, for any measurement defined as two orthogonal vectors in the Bloch sphere.

Lemma 32 ([29])**.** *Let* $\mathbf{v} = (v_1, v_2, v_3)$ *be a vector on the Bloch sphere, and let* $|v \cdot m\rangle$ *be the notation for* $v_1 |m_1\rangle + v_2 |m_2\rangle + v_3 |m_3\rangle$*. By a measurment in the* v*-basis we mean that* $|v\rangle$ *stands for 0 and* $|-v\rangle$ *stands for 1. After Alice and Bob measure in the* v*-basis and obtain results* x *and* y*, Eve's state can be written as* $\sigma^E_{bxy} = |E^{v(b)}_{xy}\rangle \langle E^{v(b)}_{xy}|$ *where*

$$|E^v_{01}\rangle = \frac{1}{\sqrt{1-\gamma}} \left[\sqrt{1 - \frac{3}{2}\gamma}\, |m_0\rangle + \sqrt{\frac{\gamma}{2}}\, |v \cdot m\rangle \right] , \tag{40}$$

$$|E^v_{10}\rangle = \frac{1}{\sqrt{1-\gamma}} \left[\sqrt{1 - \frac{3}{2}\gamma}\, |m_0\rangle - \sqrt{\frac{\gamma}{2}}\, |v \cdot m\rangle \right] , \tag{41}$$

$$|E^v_{00}\rangle = \frac{1}{\sqrt{2(1-v_3^2)}} \Big[(-v_1 v_3 - i v_2)\, |m_1\rangle + (-v_2 v_3 + i v_1)\, |m_2\rangle + (1 - v_3^2)\, |m_3\rangle \Big] , \tag{42}$$

$$|E^v_{11}\rangle = \frac{1}{\sqrt{2(1-v_3^2)}} \Big[(-v_1 v_3 + i v_2)\, |m_1\rangle + (-v_2 v_3 - i v_1)\, |m_2\rangle + (1 - v_3^2)\, |m_3\rangle \Big] . \tag{43}$$

We write $\bar{x}$ for the opposite value of a bit x. We have

$$\sigma^E_{bx} = \gamma \sigma^E_{bxx} + (1-\gamma) \sigma^E_{bx\bar{x}} . \tag{44}$$

The following Lemmas will be useful in the proof of Protocol 2. Their proofs can be found in Appendix B.

Lemma 33. *For* $x \in \{0,1\}$*,*

$$\mathbb{E}_b \sigma^E_{bx} = \left(1 - \frac{3}{2}\gamma\right) |m_0\rangle \langle m_0| + \frac{\gamma}{2} \sum_{i=1}^{3} |m_i\rangle \langle m_i| . \tag{45}$$

Lemma 34. *For* $x \in \{0,1\}$*,*

$$\mathbb{E}_b (\sigma^E_{bx})^2 = (1 - \frac{5}{2}\gamma + \frac{3}{2}\gamma^2)\, |m_0\rangle \langle m_0| + \frac{2\gamma^2 + \gamma}{6} \sum_{i=1}^{3} |m_i\rangle \langle m_i| . \tag{46}$$

Lemma 35. *For* $x \in \{0,1\}$*,*

$$\mathbb{E}_b \sigma^E_{bx} \sigma^E_{b\bar{x}} = \left(1 - \frac{7}{2}\gamma + 3\gamma^2\right) |m_0\rangle \langle m_0| + \frac{2\gamma^2 - \gamma}{6} \sum_{i=1}^{3} |m_i\rangle \langle m_i| . \tag{47}$$

3 Protocol 1

We propose a protocol for delegated storage that roughly goes as follows. Alice one-time-pads her message with a secret key that she extracts from a random raw key. She stores the resulting classical ciphertext on the server. Furthermore, she encodes the raw key as a quantum state in which she randomly places additional 'trap' states, and stores the quantum state on the server as well. When retrieving the message, she checks the trap bits for tampering, and extracts again the one-time-pad for decrypting her message. Below follows a formal description.

3.1 Parameters

The protocol has the following parameters, which are publicly known:

- message length ℓ'
- augmented message length ℓ
- authentication key length κ
- authentication function $\mathrm{MAC} : \{0,1\}^{\ell'} \times \{0,1\}^{\kappa} \to \{0,1\}^{\ell-\ell'}$
- raw key length n
- number of trap bits r
- extractor seed length d
- quantum-proof extractor $\mathrm{Ext} : \{0,1\}^{d} \times \{0,1\}^{n} \to \{0,1\}^{\ell}$
- maximum tolerated trap bit error rate Q
- smoothing parameter q for error rate estimation, $0 < q < 1/2$
- error correcting code $\mathcal{C}$ using a syndrome function $\mathrm{Syn} : \{0,1\}^{n} \to \{0,1\}^{\lambda}$, where $\lambda \approx nh(Q+q)$, so that it can correct up to $n(Q+q)$ bit errors. We write SynDec for the corresponding syndrome decoding function.

The number of qubits stored on the server is $n + r$.

Alice's key consists of the following parts:

- trap location key $t \in \{0,1\}^{n+r}$ stored efficiently as a string of length $\log \binom{n+r}{r} \approx p = (n+r) \cdot h(r/(n+r))$
- extractor seed $u \in \{0,1\}^{d}$
- MAC key $k \in \{0,1\}^{\kappa}$

As long as the message is stored on the server, Alice needs to keep the key above, as well as the following values obtained during the protocol:

- trap value key $v \in \{0,1\}^{r}$ [3]
- raw key syndrome $s \in \{0,1\}^{\lambda}$

[3] Alice could also forget v and instead remember the syndrome of v and an authentication tag of v, which need less storage space. When retrieving the message from the server, she should then try to error-correct v and check the authentication tag. If she does not succeed she should abort.

3.2 Protocol description

To store (and later retrieve) a message $m_{\text{orig}} \in \{0,1\}^{\ell'}$, Alice performs the following steps:

- Generate uniformly at random a raw key $x \in \{0,1\}^n$, a trap value key $v \in \{0,1\}^r$ and a trap location key $t \in \{0,1\}^{n+r}$ such that $\text{Hamm}(t) = r$.
- Prepare the quantum state $|\Psi\rangle = \otimes_{i=1}^{n+r} |\psi_i\rangle$ where for j ranging over all t_j that are 0, $|\psi_j\rangle = |x_j\rangle$ and for j ranging over all t_j that are 1, $|\psi_j\rangle = H|v_j\rangle$. In other words, the traps are encoded in the Hadamard basis at locations i where $t_i = 1$, and the raw key is encoded in the other locations and in the standard basis.
- Generate a seed $u \in \{0,1\}^d$ uniformly at random and compute $z = \text{Ext}(u, x)$. Generate a MAC key $k \in \{0,1\}^\kappa$ and compute authentication tag $m_{\text{tag}} = \text{MAC}(k, m_{\text{orig}})$. Set $m = m_{\text{orig}}||m_{\text{tag}}$, such that $m \in \{0,1\}^\ell$.[4] Compute the ciphertext $c = m \oplus z$. Also, compute $s = \text{Syn}(x)$.
- Send $|\Psi\rangle$ and c to the server. Keep v, t, s, k and u as key.
- Retrieve $|\Psi'\rangle$ and c' from the server.
- Measure the qubits i of $|\Psi'\rangle$ where $t_i = 0$ in the standard basis to obtain $y \in \{0,1\}^n$ and measure the other qubits in the Hadamard basis to obtain $w \in \{0,1\}^r$.
- Abort if $\text{Hamm}(v \oplus w) > Qr$.
- Perform error correction to obtain an estimator $\hat{x} = y \oplus \text{SynDec}(s \oplus \text{Syn}(y))$.
- Compute $z' = \text{Ext}(u, \hat{x})$ and compute $m' = c' \oplus z'$. Parse $m' = m'_{\text{orig}}||m'_{\text{tag}}$ and abort if $\text{MAC}(k, m'_{\text{orig}}) \neq m'_{\text{tag}}$.

For the analysis we consider an entanglement-based version of the protocol. In the following, we address "future Alice" with "Bob". We let Eve create an arbitrary quantum state $\rho^{ABE} \in \mathcal{D}(\mathcal{H}_{ABE}^{\otimes(n+r)})$, and send the A subspace to Alice and the B subspace to Bob. Note that unlike QKD or QKR protocols, Bob receives his quantum state later than Alice, namely when the ciphertext is retrieved from the server.

Since Bob is the same person as Alice, 'communication' of the private key material is implicitly done by just remembering it. The steps of the entanglement-based protocol are visualized in Figure 2.

[4] From now on, we will simply use ℓ for the 'normal' message length, since we imagine κ to be a small constant value.

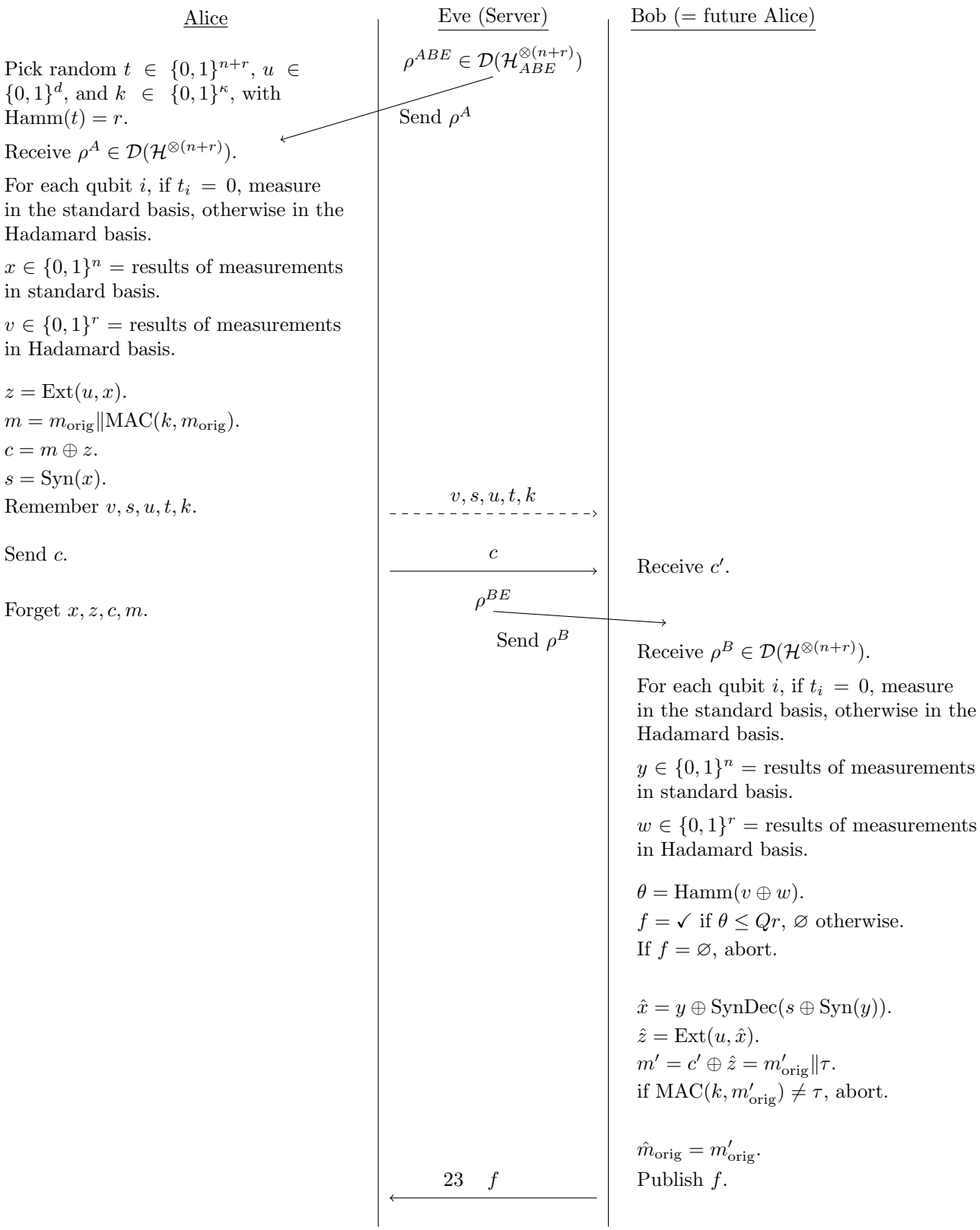

Figure 2: Schematic description of the entanglement-based version of Protocol 1.

3.3 Security definition

In this section we write out in detail the states that appear during the protocol, and state the security definition which we then evaluate in the next sections. The intermediate states written here will in fact not be used in the later analysis, but are shown for completeness. For these intermediate states we assume that the message is uniform, so that Eve's state is independent of the ciphertext. The analyses in Sections 3.4 and 3.6 will make a distinction between a uniform message and a non-uniform one, respectively.

We model the variables and quantum states during the protocol as density operators. All classical variables occurring in the protocol are denoted by the capitalization of their letters as used in the protocol description above. The input state of the protocol consists of the quantum state ρ^{ABE}, the message (including the authentication tag) and Alice's key material:

$$\rho^{ABEMTU} = \rho^{ABE} \otimes \mathbb{E}_m \left|m\right\rangle \left\langle m\right| \otimes \mathbb{E}_t \left|t\right\rangle \left\langle t\right| \otimes \mathbb{E}_u \left|u\right\rangle \left\langle u\right| \tag{48}$$

where the expectation over U is uniform, T is uniform over all choices of t such that $\mathrm{Hamm}(t) = r$, and where M can have any distribution. (We leave out the MAC key as we directly work with the augmented message m.)

The protocol can be seen as a CPTP map $\mathcal{E}$ that acts on the initial state ρ and outputs a state ω. This output state is obtained as follows.

The quantum measurements leave ρ^{ABE} in a state than can be written as

$$\mathbb{E}_{txyvwc} \left|xyvw\right\rangle \left\langle xyvw\right| \otimes \rho^E_{txyvwc} \tag{49}$$

where the expectations on X, Y, V and W depend on the exact state that Eve prepared. In particular, they do not have to be uniform, and the correlation between X and Y and the correlation between V and W are given by an arbitrary amount of noise introduced by Eve. Eve's state depends on the ciphertext C. However, in the following we treat C as being independent of Eve's state, as discussed above.

We introduce the variable θ_{vw} indicating whether the error rate of the traps is low enough or not:

$$\theta_{vw} = \begin{cases} 1 & \text{if } \mathrm{Hamm}(v \oplus w) \leq Qr \ , \\ 0 & \text{otherwise} \ . \end{cases} \tag{50}$$

After the classical post-processing the full state is

$$\begin{aligned} \omega^{MTUXYVWEZCSF} &= \mathbb{E}_{mtu} \left|mtu\right\rangle \left\langle mtu\right| \otimes \mathbb{E}_{xyvw} \left|xyvw\right\rangle \left\langle xyvw\right| \otimes \rho^E_{txyvw} \\ &\otimes \sum_z \left|z\right\rangle \left\langle z\right| \delta_{z,\mathrm{Ext}(u,x)} \otimes \sum_c \left|c\right\rangle \left\langle c\right| \delta_{c,m\oplus z} \otimes \sum_s \left|s\right\rangle \left\langle s\right| \delta_{s,\mathrm{Syn}(x)} \otimes \sum_f \left|f\right\rangle \left\langle f\right| \delta_{f,\theta_{vw}} \ . \end{aligned} \tag{51}$$

We make a distinction between intermediate variables and output variables. The output variables are the information that Eve has (C, E, and F), as well as M, which Alice wants to keep secret. We trace out all the intermediate variables and obtain

$$\omega^{MCEF} = \mathbb{E}_m \left|m\right\rangle \left\langle m\right| \otimes \mathbb{E}_{txyvw} \rho^E_{txyvw} \otimes \mathbb{E}_u \sum_c \left|c\right\rangle \left\langle c\right| \delta_{m\oplus c,\mathrm{Ext}(u,x)} \otimes \sum_f \left|f\right\rangle \left\langle f\right| \delta_{f,\theta_{vw}} \ . \tag{52}$$

Furthermore we define the subnormalized state representing the output conditioned on Alice not aborting:

$$\omega^{MCEF}_{F=\checkmark} = \mathbb{E}_m \left|m\right\rangle \left\langle m\right| \otimes \mathbb{E}_{txyvw} \theta_{vw} \rho^E_{txyvw} \otimes \mathbb{E}_u \sum_c \left|c\right\rangle \left\langle c\right| \delta_{m\oplus c,\mathrm{Ext}(u,x)} \otimes \left|F=\checkmark\right\rangle \left\langle F=\checkmark\right| \ . \tag{53}$$

We will now define the security of the protocol $\mathcal{E}$ by comparing it to an ideal protocol $\mathcal{F}$. We define $\mathcal{F}$ in terms of its output state given the same input state ρ as defined above: if $\mathcal{E}$ would abort, the output state of $\mathcal{F}$ is equal to that of $\mathcal{E}$; if the protocol does not abort, the output state of $\mathcal{F}$ is

$$\omega^{MCEF}_{\mathrm{ideal},F=\checkmark} = \mathbb{E}_m \left|m\right\rangle \left\langle m\right| \otimes \omega^{CEF} \ , \tag{54}$$

where

$$\omega^{CEF} = \mathrm{tr}_M \left(\omega^{MCEF}_{F=\checkmark} \right) \tag{55}$$

$$= \mathbb{E}_m \mathbb{E}_{tuxyvw} \theta_{vw} \rho^E_{txyvw} \otimes \sum_c \left|c\right\rangle \left\langle c\right| \delta_{m\oplus c,\mathrm{Ext}(u,x)} \otimes \left|F=\checkmark\right\rangle \left\langle F=\checkmark\right| \ . \tag{56}$$

In other words, $\omega^{MCEF}_{\mathrm{ideal},F=\checkmark}$ is a state where the message is independent of Eve's side-information. The distribution of M must be the same as in the beginning: Eve must not learn any new information about it, regardless of whether she already had some information.

Finally we define the security of our protocol as the diamond distance between $\mathcal{E}$ and $\mathcal{F}$. This is given by

$$\left\| \mathcal{E} - \mathcal{F} \right\|_\diamond = \left\| \omega^{MCEF}_{F=\checkmark} - \omega^{MCEF}_{\mathrm{ideal},F=\checkmark} \right\|_{\mathrm{tr}} \tag{57}$$

since the output states in case of abort are the same.

Towards the end of the protocol, Bob checks the authentication tag of the retrieved message. If the tag is correct, he assumes the message is authentic and does not abort. There is however a small probability that Eve replaced the message with another and still managed to append a valid tag. Since the length of the MAC key is κ, this probability is $2^{-\kappa}$. For the analysis, we simply consider a protocol $\mathcal{E}'$ in which the MAC verification always unerringly detects if Eve has manipulated the state. This protocol is then $2^{-\kappa}$-close to the actual protocol. Using the triangle inequality,

$$\begin{aligned} \left\| \mathcal{E} - \mathcal{F} \right\|_\diamond &\leq \left\| \mathcal{E} - \mathcal{E}' \right\|_\diamond + \left\| \mathcal{E}' - \mathcal{F} \right\|_\diamond \\ &= 2^{-\kappa} + \left\| \mathcal{E}' - \mathcal{F} \right\|_\diamond \ . \end{aligned} \tag{58}$$

The following section shows the analysis of the second term.

3.4 Security analysis

Here we analyze the case where the message is uniform. In that case the ciphertext c, which gets revealed to Eve before she performs an attack using her quantum side-information, is completely independent of the other variables. In Section 3.6 we consider arbitrary message distributions.

We write the quantum state ρ^{ABE} as $\rho^{A_x A_v B_y B_w E}$ where A_x is the subspace of A that Alice measures in the standard basis (to obtain X), and where A_v is the subspace of A that Alice measures in the Hadamard basis (to obtain V). B_y and B_w are defined similarly. Note that the actual locations of these subsystems depend on the random variable T denoting the trap location key.

For the analysis we will also consider the hypothetical action of Alice and Bob where they measure A_x and B_y in the Hadamard basis instead of the standard basis, obtaining classical outcomes X' and Y'. In Table 1 we summarize the names of the classical outcomes that are the results of measuring in a certain basis. (We do not consider measuring A_v and B_w in the standard basis.)

	A_x	B_y	A_v	B_w
Standard basis	X	Y	-	-
Hadamard basis	X'	Y'	V	W

Table 1: Classical variables resulting from different measurements.

Consider the state $\rho^{A_x EFY'}_{F=\checkmark}$. This state corresponds to the situation where A_v, B_w, and B_y were all measured in the Hadamard basis, and such that $\mathrm{Hamm}(V \oplus W) \leq Qr$, but where the measurement on A_x has still not been performed. We apply Corollary 14 to this state, giving us the following entropic uncertainty relation:

$$H^{\varepsilon}_{\min}(X|E, F=\checkmark) + H^{\varepsilon}_{\max}(X'|Y', F=\checkmark) \geq n \ . \tag{59}$$

In the protocol, only output X is generated, not X'. We can however consider the two different states σ and τ that would be the result of generating X or X' respectively. Let $\sigma = \rho^{XYVWEF}_{F=\checkmark}$ be the state (observed during the protocol) resulting from measuring A_x and B_y in the standard basis, conditioned on $F = \checkmark$, and let $\tau = \rho^{X'Y'VWEF}_{F=\checkmark}$ be the (hypothetical) state resulting from measuring A_x and B_y in the Hadamard basis, conditioned on $F = \checkmark$.

We now prove the following bound on the smooth min-entropy of X given Eve's side-information, closely following the approach of [43].

Lemma 36. *Let* $\eta(q) = e^{\frac{-q^2 nr^2}{(n+r)(r+1)}}$. *Then,*

$$H^{\eta(q)}_{\min}(X|E, F=\checkmark) \geq n\big[1 - h(Q+q)\big] \ . \tag{60}$$

Proof. Consider scenario τ, that is, both Alice and Bob measure all their $n+r$ qubits in the Hadamard basis, resulting in classical variables X', Y', V and W. We can also write all Alice's outcomes as binary random variables $O^A_1, \ldots O^A_{n+r}$ where each $O^A_i \in \{0,1\}$ is

the measurement outcome of the ith qubit. Note that $O^A \in \{0,1\}^{n+r}$ consists exactly of X' and V, where the bits of V are at the locations $\mathcal{T} = \{i \mid t_i = 1\}$. Similarly we define $O_1^B, \dots O_{n+r}^B$ as Bob's measurement outcomes, comprising Y' and W.

We now introduce binary random variables $B_1, \dots B_{n+r}$ defined as $B_i = O_i^A \oplus O_i^B$.

Note that $\mathrm{Hamm}(V \oplus W) = \sum_{i \in \mathcal{T}} B_i$ and $\mathrm{Hamm}(X' \oplus Y') = \sum_{i \notin \mathcal{T}} B_i$. Finally, since $\mathcal{T}$ is an index subset that was chosen uniformly and independently of the B_i, we can apply Lemma 15 and obtain

$$\Pr\Big[\mathrm{Hamm}(V \oplus W) \leq rQ \wedge \mathrm{Hamm}(X' \oplus Y') \geq n(Q+q)\Big] \leq \eta(q)^2 \ . \tag{61}$$

Remember that in our scenario we already conditioned on the fact that $F = \checkmark$, meaning that $\mathrm{Hamm}(V \oplus W)_\tau \leq rQ$. We denote by Ω the event that $\mathrm{Hamm}(X' \oplus Y')_\tau > n(Q+q)$. Then his event has probability $\Pr[\Omega]_\tau \leq \eta(q)^2$.

By Lemma 17, there exists a state τ' that is $\eta(q)$-close to τ with $\Pr[\Omega]_{\tau'} = 0$. Now we show a derivation similar to that in [43], where in the last step we use an inequality that is shown in [48].

$$\begin{aligned}
H_{\max}(X'|Y', F = \checkmark)_{\tau'} &= H_{\max}(X'|Y')_{\tau'} && (62)\\
&\leq \max_{y' \in \{0,1\}^n} \log |\{x' \in \{0,1\}^n : \Pr\left[X' = x' \wedge Y' = y'\right]_{\tau'} > 0\}| && (63)\\
&\leq \log \sum_{i=0}^{n(Q+q)} \binom{n}{i} && (64)\\
&\leq nh(Q+q) \ . && (65)
\end{aligned}$$

When going from (63) to (64) we use that for a given y', the possible x' in the corresponding set are restricted in having at most $n(Q+q)$ different bits.

Since τ' is $\eta(q)$-close to τ, by definition of the smooth max-entropy (Definition 6),

$$H_{\max}^{\eta(q)}(X'|Y', F = \checkmark)_\tau \leq H_{\max}(X'|Y', F = \checkmark)_{\tau'} \leq nh(Q+q) \ . \tag{66}$$

Using the entropic uncertainty relation (59) we obtain the bound

$$H_{\min}^{\eta(q)}(X|E, F = \checkmark)_\sigma \geq n - nh(Q+q) \tag{67}$$

for the state $\sigma_{F=\checkmark}^{XYVWEF}$ occuring during the protocol if it does not abort. □

As noted above, we assume that the message is uniform, and hence the ciphertext C is independent of the extractor output. So,

$$H_{\min}^{\eta(q)}(X|EC, F=\checkmark)_\sigma = H_{\min}^{\eta(q)}(X|E, F=\checkmark)_\sigma \geq n - nh(Q+q) \ . \tag{68}$$

Now we are ready to bound the trace distance of (57).

Lemma 37. *For a suitably chosen (k, ε)-quantum-proof extractor Ext with $k = n - nh(Q+q)$, and for any $0 < \alpha < 1$ and $\varepsilon > 0$ such that $n - nh(Q+q) \geq \log n + \log^{1+\alpha}(1/\varepsilon)$, the output Z of Ext(X, U) has length $(1-\alpha)(n - nh(Q+q))$ and we have*

$$\|\sigma_{F=\checkmark}^{ZCEF} - \mu^Z \otimes \sigma_{F=\checkmark}^{CEF}\|_{\mathrm{tr}} \leq \eta(q) + 2^{-d+\log n} \ . \tag{69}$$

Proof. By definition of the smooth entropy (Definition 5), there exists a state σ' that is $\eta(q)$-close to σ and for which $H_{\min}(X|EC, F=\checkmark)_{\sigma'} \geq n - nh(Q+q)$. By Lemma 25, there exists a $(n - nh\left[Q+q\right], \varepsilon)$ quantum-proof extractor Ext such that for the state σ', for any $0 < \alpha < 1$ and $\varepsilon > 0$ such that $n - nh(Q+q) \geq \log n + \log^{1+\alpha}(1/\varepsilon)$,

$$\|\sigma'^{ZCEF}_{F=\checkmark} - \mu^Z \otimes \sigma'^{CEF}_{F=\checkmark}\|_{\mathrm{tr}} \leq \varepsilon \tag{70}$$

and such that the output Z has length $(1-\alpha)(n - nh(Q+q))$.

Since $d = O(\log(n/\varepsilon))$, we can set $\varepsilon = 2^{-d+\log n}$. Then, since σ' is $\eta(q)$-close to σ, we obtain

$$\begin{aligned}
\|\sigma_{F=\checkmark}^{ZCEF} - \mu^Z \otimes \sigma_{F=\checkmark}^{CEF}\|_{\mathrm{tr}} &\leq \|\sigma_{F=\checkmark}^{ZCEF} - \sigma'^{ZCEF}_{F=\checkmark}\|_{\mathrm{tr}} + \|\sigma'^{ZCEF}_{F=\checkmark} - \mu^Z \otimes \sigma'^{CEF}_{F=\checkmark}\|_{\mathrm{tr}} && (71)\\
&\leq \|\sigma_{F=\checkmark}^{XCEF} - \sigma'^{XCEF}_{F=\checkmark}\|_{\mathrm{tr}} + \|\sigma'^{ZCEF}_{F=\checkmark} - \mu^Z \otimes \sigma'^{CEF}_{F=\checkmark}\|_{\mathrm{tr}} && (72)\\
&\leq \eta(q) + \varepsilon && (73)
\end{aligned}$$

where we used the triangle inequality for the first inequality and Lemma 7 for the second one.

□

Finally we state the security of Protocol 1 for a uniform message.

Theorem 1. *Let M be a **uniform** message with length ℓ. Let $Q+q$ be the maximum tolerated bit error rate, d the extractor seed length, r the number of traps, and κ the length of the authentication tag. Furthermore, let n be the length of the raw key and $\alpha > 0$ such that $n - nh(Q+q) \geq \log n + (d - \log n)^{1+\alpha}$. Let $\mathcal{E}$ be the CPTP map modeling Protocol 1 and $\mathcal{F}$ the ideal version of Protocol 1, as described above.*

Then, as long as $\ell \leq (1-\alpha)(n - nh(Q+q))$,

$$\|\mathcal{E} - \mathcal{F}\|_\diamond \leq e^{\frac{-q^2 nr^2}{(n+r)(r+1)}} + 2^{-d+\log n} + 2^{-\kappa} \ . \tag{74}$$

Proof. We have $M = Z \oplus C$. Since M is uniform, and using Lemma 37, we obtain

$$\|\sigma_{F=\checkmark}^{MCEF} - \mu^M \otimes \sigma_{F=\checkmark}^{CEF}\|_{\mathrm{tr}} \leq \eta(q) + 2^{-d+\log n} \tag{75}$$

Combining this with our security definition in (58) proves the theorem. □

3.5 Key length

In this section we consider what values for the key lengths we can use and what they mean for the security value in Theorem 1. We cannot simply make the diamond distance arbitrarily small by increasing the key lengths, since we do not want these lengths to exceed the message length.

Recall that the data that Alice needs to remember consists of

- trap location key $t \in \{0,1\}^{n+r}$ stored efficiently as a key of length $\log \binom{n+r}{r} \approx p = (n+r) \cdot h(r/(n+r))$,
- extractor seed $u \in \{0,1\}^d$
- MAC key $k \in \{0,1\}^\kappa$
- trap value key $v \in \{0,1\}^r$,
- raw key syndrome $s \in \{0,1\}^\lambda$, where $\lambda \approx nh(Q+q)$

and that we want their total length to be at most that of the message, that is,

$$p + d + \kappa + r + \lambda < \ell \ . \tag{76}$$

Since there are so many variables that all contribute somehow to the key length and the security, it is difficult to get an optimal set of values. However, the dominating term in Theorem 1 is $\eta(q) = e^{\frac{-q^2 n r^2}{(n+r)(r+1)}}$. Indeed, we can simply set for example $\kappa = 100$ and $d = 100 + \log n$, in which case the authentication tag and seed only contribute an (almost) constant value in the total key length.

To bound $\eta(q)$, we need to find suitable values for r and q. A higher value for q implies a larger λ and higher r implies a higher value for p as well. It turns out the bottleneck in terms of key length is the syndrome length, that is, λ. Indeed, $h(Q+q)$ shrinks very slowly when decreasing Q and q: to get $\lambda = n/1000$ for example, we need $Q + q \lesssim 6.5 \cdot 10^{-5}$. Having such low values for q however also impacts the security due to its presence in $\eta(q)$.

Below we give an example set of parameters to achieve reasonable key length and security. Firstly, we set $r = \gamma n$ for some $\gamma \in (0,1)$.

Then,

$$e^{\frac{-q^2 n r^2}{(n+r)(r+1)}} \approx e^{\frac{-q^2 \gamma^2 n^3}{(n+\gamma n)\cdot \gamma n}} \tag{77}$$

$$= e^{-q^2 \frac{\gamma}{1+\gamma} n}. \tag{78}$$

If we set q and γ to small values (one could for example set $q = \log^{-1} n$ and γ to a small constant), the expression is exponentially small in the number of qubits n, and hence disappears for large n. Furthermore, we can set $d = \log n + \log(1/\varepsilon)$, and set κ to a small constant. Then the whole security error disappears for large n.

Meanwhile, with these values the key length becomes

$$\kappa + d + r + p + \lambda = \kappa + \log n + \log(1/\varepsilon) + n\big[\gamma + (1+\gamma) h(\frac{\gamma}{1+\gamma}) + h(Q+q)\big]. \tag{79}$$

For large n, the dominating term is $nh(Q+q)$, and the other terms disappear (for suitable values for ε, γ and κ). Using $\ell = (1-\alpha)n\big[1-h(Q+q)\big]$ and setting α close to 0, the short-key requirement becomes roughly $nh(Q+q) < n\big[1-h(Q+q)\big]$ or

$$1 - 2h(Q+q) > 0 \ . \tag{80}$$

We could hence state that the rate of our protocol is $1-2h(Q+q)$, similar to that of QKD. However, note that in this context the *rate* has a slightly different interpretation than for QKD: the result here is that as long as $1-2h(Q+q) > 0$, we can keep our key shorter than the message.

3.6 Non-uniform message

In the analysis of Section 3.4 we assumed that the message was completely uniform. Therefore, the fact that Eve already has access to the ciphertext while performing her attack was not relevant in the security proof. Here we consider the case where Eve does have some information about the message. In fact, the security proof does not change much, except that we need longer keys.

In Section 3.4, we bounded the min-entropy of X given Eve's side-information by showing that $H_{\min}^{\eta(q)}(X|E, F=\checkmark) \geq n - nh(Q+q)$. For a known message, we cannot simply add C without penalty. In the worst case we obtain

$$H_{\min}^{\eta(q)}(X|EC, F=\checkmark) \geq n - nh(Q+q) - \ell \tag{81}$$

since C could give at most ℓ bits of extra information about X.[5]

This means that now we would need a (k,ε) quantum-proof extractor with $k = n - nh(Q+q) - \ell$ and $k \geq \log n + \log^{1+\alpha}(1/\varepsilon)$. Furthermore, the output length is now $(1-\alpha)(n - nh(Q+q) - \ell)$. In other words, n must now be roughly ℓ longer than in the case of a uniform message.

Theorem 2. *Let M be a message with **any** distribution and length ℓ. Let $Q+q$ be the maximum tolerated bit error rate, d the extractor seed length, r the number of traps, and κ the length of the authentication tag. Furthermore, let n be the length of the raw key and $\alpha > 0$ such that $n - nh(Q+q) - \ell \geq \log n + (d - \log n)^{1+\alpha}$. Let $\mathcal{E}$ be the CPTP map modeling Protocol 1 and $\mathcal{F}$ the ideal version of Protocol 1, as described above.*

Then, as long as $\ell \leq \frac{1-\alpha}{2+\alpha}(n - nh(Q+q))$,

$$\|\mathcal{E} - \mathcal{F}\|_\diamond \leq e^{\frac{-q^2 n r^2}{(n+r)(r+1)}} + 2^{-d+\log n} + 2^{-\kappa} \ . \tag{82}$$

Proof. The same proof as for Theorem 1 applies, except the following values in Lemma 37 need to be updated: k must be $n - nh(Q+q) - \ell$ and the output length ℓ of Z is $(1-\alpha)(n - nh(Q+q) - \ell)$. Therefore we now need

$$\ell \leq (1-\alpha)(n - nh(Q+q) - \ell) \tag{83}$$

[5] If we somehow know that Eve can only have $s < \ell$ bits of information about the message, than we only need to substract s.

which can be written as

$$\ell \leq \frac{1-\alpha}{2+\alpha}(n - nh(Q+q)) \ . \tag{84}$$

□

Typically we would like to keep α very small, resulting in a rate $\ell/n \approx \frac{1}{2}(1-h(Q+q))$, that is, half that of the uniform-message case. Furthermore, since n roughly doubles, λ doubles as well, but $p+r$ increases slower than doubly. So, compared to the uniform-message case, the key length is at most twice as long.

The weak bound that we used—that C gives Eve ℓ bits of information—does not seem very satisfying, since it represents the extreme situation that Eve completely knows the message, in which case storage is not relevant anymore in the first place. However, it turns out to be difficult to reason about how much extra information about X Eve can get out of C. Knowledge about M gives Eve (by seeing C) knowledge about Z, which in turn could give information about X. This last step depends on the working on the extractor: given the output, can one say something about the input? Pairwise-independent hash functions have the property that we can directly say something about the number of inputs x that map to a particular output z. However, for our goal to keep keys short, we need short-seeded extractors, and in general they do not possess this property.

We mention that we also considered applying the entropic uncertainty relation already on the state ρ^{ABCEU}, that is, trying to directly bound the min-entropy of the extractor output Z given EC. For this we model the quantum measurements followed by the classical extractor application as one POVM, and try to calculate the overlap (according to Definition 12) between this POVM and one where the quantum states are measured in the opposite bases. These calculations can be found in Appendix A. Unfortunately, we were only able to obtain a result of pairwise independent hash functions, but not for short-seeded extractors. This is exactly due to the fact mentioned above, that we cannot bound the number of inputs x that give a particular output z.

4 Protocol 2

We propose another protocol for delegated storage. In this case we prove security in the Common Random String (CRS) model[6]. It assumes that there is public uniform randomness available to all parties. In our scenario we imagine this randomness to be a large table (in fact, two tables, see below) that has relatively few, long, rows. This allows us to index the table with a 'seed' that has low entropy, resulting in a long uniform string. Essentially, with this model we assume that we have access to a *perfect* pseudo-random generator (PRNG), meaning a PRNG that cannot be attacked in a smarter way than by brute-forcing the seed.

The protocol is almost equal to Protocol 1, except for two differences:

- Both the raw key and the traps are encoded using 8-state encoding. The basis key (now consisting of $2(n+r)$ bits, 2 bits for each qubit), is obtained by indexing a large common *basis table* ϕ (a common random string) that consists of 2^b rows of length $2(n+r)$. Alice only remembers a uniformly chosen short index key $g \in \{0,1\}^b$, but uses the long key $\phi(g)$ for encoding her raw key.
- The extractor is now based on a two-universal hash function. The seed has length $2n$, but is sampled from a large public *seed table* ξ (another common random string), which consists of 2^d rows of length $2n$. Alice only remembers a uniformly chosen short index key $u \in \{0,1\}^d$, but uses the long seed $\xi(u)$ for the extractor.

Below follows a formal description of the protocol. Then, in Sections 4.3 and 4.4 we do the security analysis, which is quite different from that of Protocol 1.

4.1 Parameters

The protocol has the following parameters, which are publicly known:

- message length ℓ'
- augmented message length ℓ
- authentication key length κ
- authentication function $\mathrm{MAC} : \{0,1\}^{\ell'} \times \{0,1\}^{\kappa} \to \{0,1\}^{\ell-\ell'}$
- raw key length n
- number of trap bits r
- length b of the basis encoding key, (to sample a $2(n+r)$-length encoding key from the public table ϕ)
- length d of the extractor key (to sample a seed of length $2n$ from the public table ξ)
- pairwise indepedent hash function $\mathrm{Ext} : \{0,1\}^{2n} \times \{0,1\}^{n} \to \{0,1\}^{\ell}$
- maximum tolerated trap bit error rate Q
- smoothing parameter q for error rate estimation, $0 < q < 1/2$

[6] CRS could also stand for Common Reference String model, where the common string has an arbitrary distribution. The Common Random String model that we use here is then a special case of the CRS where the distribution is uniform.

- error correction scheme $\mathcal{C}$ using a syndrome function $\mathrm{Syn} : \{0,1\}^n \to \{0,1\}^\lambda$, where $\lambda \approx nh(Q+q)$, so that it can correct up to $n(Q+q)$ bit errors. We write SynDec for the corresponding syndrome decoding function.

The number of qubits stored on the server is $n + r$.

Alice's key consists of the following parts:

- basis encoding key $g \in \{0,1\}^b$
- trap location key $t \in \{0,1\}^{n+r}$ stored efficiently as a key of length $\log \binom{n+r}{r} \approx p = (n+r) \cdot h(r/(n+r))$
- extractor seed $u \in \{0,1\}^d$
- MAC key $k \in \{0,1\}^\kappa$

As long as the message is stored on the server, Alice needs to keep the key above, as well as the following values obtained during the protocol:

- trap data key $v \in \{0,1\}^r$
- raw key syndrome $s \in \{0,1\}^\lambda$

4.2 Protocol description

To store (and later retrieve) a message $m_{\mathrm{orig}} \in \{0,1\}^{\ell'}$, Alice performs the following steps. We assume that there are public tables ϕ and ξ available as described above.

- Generate uniformly at random a raw key $x \in \{0,1\}^n$, a trap key $v \in \{0,1\}^r$, a trap location key $t \in \{0,1\}^{n+r}$ such that $\mathrm{Hamm}(t) = r$ and a basis encoding key $g \in \{0,1\}^b$.
- Compute $g' = \phi(g)$. Let $a_1, \ldots a_{n+r}$ be the string where the traps are placed between the raw key bit according to t. Prepare the quantum state $|\Psi\rangle$ where the ith qubit is the 8-state encoding of a_i according to basis g'_i.
- Generate a seed $u \in \{0,1\}^d$ uniformly at random and compute $z = \mathrm{Ext}(\xi(u), x)$. Generate a MAC key $k \in \{0,1\}^\kappa$ and compute authentication tag $m_{\mathrm{tag}} = \mathrm{MAC}(k, m_{\mathrm{orig}})$. Set $m = m_{\mathrm{orig}} || m_{\mathrm{tag}}$, such that $m \in \{0,1\}^\ell$.[7] Compute the ciphertext $c = m \oplus z$. Also, compute $s = \mathrm{Syn}(x)$.
- Send $|\Psi\rangle$ and c to the server. Keep v, t, s, k, g and u as key.
- Retrieve $|\Psi'\rangle$ and c' from the server.
- Measure each qubit i in basis $\phi(g)_i$ to obtain the raw key $y \in \{0,1\}^n$ and trap values $w \in \{0,1\}^r$.
- Abort if $\mathrm{Hamm}(v \oplus w) > Qr$.
- Perform error correction to obtain an estimator $\hat{x} = y \oplus \mathrm{SynDec}(s \oplus \mathrm{Syn}(y))$.
- Compute $z' = \mathrm{Ext}(\xi(u), \hat{x})$ and $m' = c' \oplus z'$. Parse $m' = m'_{\mathrm{orig}} || m'_{\mathrm{tag}}$ and abort if and only if $\mathrm{MAC}(k, m'_{\mathrm{orig}}) \neq m'_{\mathrm{tag}}$.

[7] Like for Protocol 1, we will from now on simply use ℓ for the 'normal' message length, since we imagine κ to be a small constant value.

For the analysis we consider again an entanglement-based version of the protocol. For this case, however, we assume Eve prepares *singlet* states, which means that 'no noise' means *anticorrelated* values for Alice and Bob. This allows us to use the symmetrization techniques from Chapter 2. 'Communication' between Alice and Bob of the private key material is implicitly done by just remembering it. The steps of the entanglement-based protocol are visualized in Figure 3.

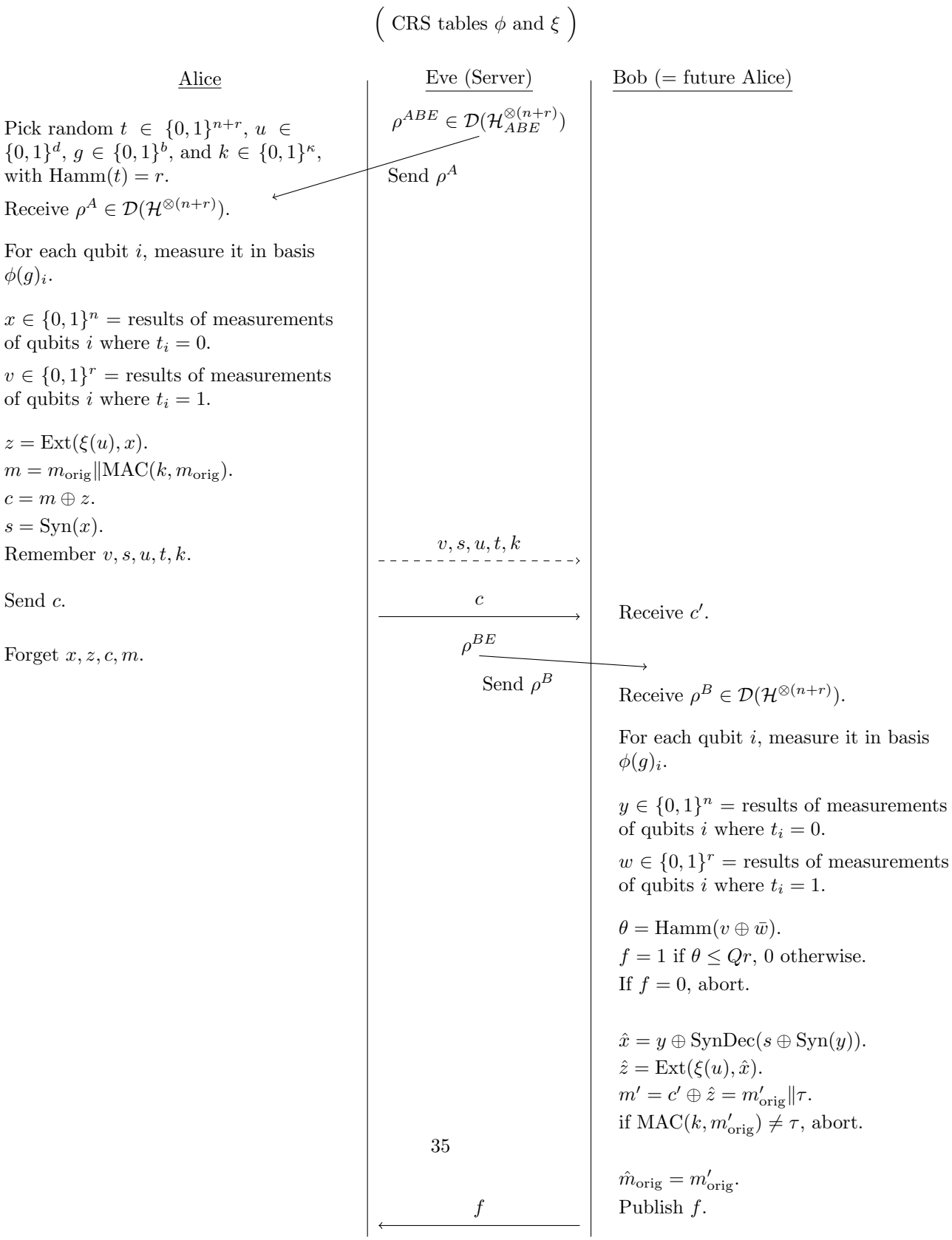

Figure 3: Schematic description of the entanglement-based version of Protocol 2. The CRS tables are assumed to be accessable for all parties.

4.3 Security definition

Like for Protocol 1, we first write out the states that occur during the protocol, and define the security in terms of the diamond distance between the real protocol and an ideal version. In Section 4.4 we then proceed to calculate this distance. We assume the message to be uniform. This means that the ciphertext does not give Eve any information, so it can be decoupled from the rest.

We treat the protocol as a map $\mathcal{E}$ that acts on a state $\rho^{ABE} \in \mathcal{D}(\mathcal{H}_{ABE}^{\otimes n})$ and outputs a state ω^{MCEF} comprising the message M, together with Eve's side information consisting of C (the ciphertext), E (her ancilla quantum state) and F (the flag indicating whether the protocl aborted or not). We will define an ideal protocol $\mathcal{F}$, and calculate the diamond distance $\|\mathcal{E} - \mathcal{F}\|_\diamond$.

The input state of the protocol consists of the quantum state ρ^{ABE}, the message (including the authentication tag), Alice's key material, and the public tables:

$$\rho^{ABEMGTUK\Phi\Xi} \tag{85}$$

$$= \rho^{ABE} \otimes \mathbb{E}_m |m\rangle\langle m| \otimes \mathbb{E}_g |g\rangle\langle g| \otimes \mathbb{E}_t |t\rangle\langle t| \otimes \mathbb{E}_u |u\rangle\langle u| \otimes \mathbb{E}_\phi |\phi\rangle\langle\phi| \otimes \mathbb{E}_\xi |\xi\rangle\langle\xi| \tag{86}$$

where all expectations are uniform.

We use post-selection and noise symmetrization to simplify the state ρ^{ABE}. First we argue that the protocol $\mathcal{E}$ is permutation-symmetric.

Lemma 38. *$\mathcal{E}$ is permutation-symmetric.*

Proof. Consider a variant $\mathcal{E}' = \mathcal{E} \circ \pi$ where Alice and Bob both apply the same random permutation π on their input qubits. Note that in the prepare-and-measure protocol, the variables x, v, t, g and ϕ are all chosen uniformly at random. Therefore, Alice and Bob could also apply a permutation π' on all these variables, because they will still be uniform. However, this is the same as keeping the variables the same but permuting the qubits. Therefore, $\mathcal{E}'$ is the same as $\mathcal{E}$, so according to Definition 29 $\mathcal{E}$ is permutation-symmetric (using K_π equal to the identity). □

This allows us to treat ρ^{ABE} as a factorized state $\sigma^{\otimes n}$ where σ is an element of $\mathcal{H}_{ABE}$ and has dimension $d = 4$ (Eve holds the purification of the 2-dimensional subspace AB). Using Lemma 30 we obtain

$$\|\mathcal{E} - \mathcal{F}\|_\diamond \leq (n+1)^{15} \max_{\sigma \in \mathcal{D}(\mathcal{H}_{ABE})} \|\mathcal{E}(\sigma^{\otimes n}) - \mathcal{F}(\sigma^{\otimes n})\|_1 \tag{87}$$

for the ideal version $\mathcal{F}$ that we define later.

We can also simplify the state σ itself. Indeed, the protocol does not behave differently if Alice and Bob would apply random Pauli's to their qubits before measuring them. This is because the measurement bases that they use are chosen uniformly at random. This then means that we can write $\sigma = |\Psi^{ABE}\rangle\langle\Psi^{ABE}|$ as defined in (38). Note that in general, Eve's state also depends on the ciphertext C. However, since we assume the message to be uniform, C is completely independent of Eve's state, and hence we do not need a subscript c in Eve' state.

Now we show how the output state ω^{MCEF} is obtained. Define

$$\rho^E_{\phi(g)xy} = \bigotimes_{i:t_i=0} \sigma^E_{\phi(g)_i x_i y_i} \ , \tag{88}$$

$$\rho^E_{\phi(g)vw} = \bigotimes_{i:t_i=1} \sigma^E_{\phi(g)_i v_i w_i} \ . \tag{89}$$

where $\sigma^E_{\phi(g)_i x_i y_i}$ is defined as in Lemma 32.

The measurement results of ρ^{ABE} can be written as

$$\mathbb{E}_{\phi g} \left|\phi g\right\rangle \left\langle \phi g\right| \otimes \mathbb{E}_{xy} \left|xy\right\rangle \left\langle xy\right| \otimes \rho^E_{\phi(g)xy} \otimes \mathbb{E}_{vw} \left|vw\right\rangle \left\langle vw\right| \otimes \rho^E_{\phi(g)vw} \tag{90}$$

where the expectations depend on the exact state that Eve prepared. In particular, they do not have to be uniform, and the correlation between X and Y and the correlation between V and W are given by an arbitrary amount of noise introduced by Eve.

Note that we were able to split Eve's side information about xy from her side-information about vw, because of the factorization of the state ρ^{ABE}.

Next, define[8]

$$\theta_{xy} = \begin{cases} 1 \text{ if } \mathrm{Hamm}(x \oplus \bar{y}) \leq Qn \\ 0 \text{ otherwise} \end{cases} . \tag{91}$$

This θ_{xy} is never explicitly calculated during the protocol. Instead, Bob calculates $\mathrm{Hamm}(v \oplus w)$ and sets $f = \theta_{vw}$. Since the symmetrization made sure that all singlet states σ are identical, $\mathrm{Hamm}(v \oplus w)$ should be a good estimator of $\mathrm{Hamm}(x \oplus y)$. To be precise, the probability that it is not a good estimator is

$$\Pr\left[\mathrm{Hamm}(v \oplus \bar{w}) \leq Qr \ \wedge \ \mathrm{Hamm}(x \oplus \bar{y}) > (Q+q)n\right] \leq \eta(q) \tag{92}$$

by Lemma 15, and where $\eta(q)$ is the same as in Lemma 36.

In the following we analyze the security of a protocol $\mathcal{E}'$ where estimation is always correct, so we have $f = \theta_{xy}$, which will allow us to ignore $\rho^E_{\phi(g)vw}$. Furthermore, as we did in Protocol 1, we simply assume that authentication is always correct, by adding the term $2^{-\kappa}$ in the security expression. We have

$$\|\mathcal{E} - \mathcal{F}\|_\diamond \leq \|\mathcal{E} - \mathcal{E}'\|_\diamond + \|\mathcal{E}' - \mathcal{F}\|_\diamond \tag{93}$$

$$= 2^{-\kappa} + \eta(q) + \|\mathcal{E}' - \mathcal{F}\|_\diamond \ . \tag{94}$$

After the classical post-processing the full state is

[8] Remember that in case of no noise, we expect anticorrelated outcomes x and y, that is, $x = \bar{y}$.

$$
\begin{aligned}
&\omega^{M\Phi GXYE\Xi UZCFVW} \\
&= \mathbb{E}_m \left|m\right\rangle \left\langle m\right| \otimes \mathbb{E}_{\phi gxy} \left|\phi gxy\right\rangle \left\langle \phi gxy\right| \otimes \rho^E_{\phi(g)xy} \otimes \mathbb{E}_{\xi u} \left|\xi u\right\rangle \left\langle \xi u\right| \otimes \sum_z \left|z\right\rangle \left\langle z\right| \delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)} \\
&\otimes \sum_c \left|c\right\rangle \left\langle c\right| \delta_{c,m\oplus z} \otimes \sum_f \left|f\right\rangle \left\langle f\right| \delta_{f,\theta_{xy}} \otimes \mathbb{E}_{vw} \left|vw\right\rangle \left\langle vw\right| \otimes \rho^E_{\phi(g)vw} \ . \qquad (95)
\end{aligned}
$$

We make a distinction between intermediate variables and output variables. The output variables are the information that Eve has (C, E, and F), as well as M, which Alice wants to keep secret.

We trace out the internal variables $\phi, g, \xi, u, z, x, y, v, w$, and leave out $\rho^E_{\phi(g)vw}$ since it is independent of the rest:

$$
\begin{aligned}
\omega^{MCEF} &= \mathbb{E}_m \left|m\right\rangle \left\langle m\right| \otimes \mathbb{E}_{\phi gxy} \rho^E_{\phi(g)xy} \otimes \sum_f \left|f\right\rangle \left\langle f\right| \delta_{f,\theta_{xy}} \mathbb{E}_{\xi u} \sum_z \delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)} \\
&\quad \otimes 2^{-\ell} \sum_c 2^\ell \left|c\right\rangle \left\langle c\right| \delta_{c,z} \qquad (96) \\
&= \mathbb{E}_{mc} \left|mc\right\rangle \left\langle mc\right| \otimes \mathbb{E}_{\phi gxy} \rho^E_{\phi(g)xy} \otimes \sum_f \otimes \left|f\right\rangle \left\langle f\right| \delta_{f,\theta_{xy}} \otimes \mathbb{E}_{\xi u} 2^\ell \delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)} \qquad (97)
\end{aligned}
$$

where in the last expression the expectation over c is uniform.

Now we split the state in a part where Bob does not abort, and one where he does abort.

$$
\omega^{MCEF} = \mathbb{E}_{mc} \left|mc\right\rangle \left\langle mc\right| \otimes \sum_f \left|f\right\rangle \left\langle f\right| \left[f \rho^E_{mc,f=1} + (1-f) \rho^E_{mc,f=0} \right] \qquad (98)
$$

where

$$
\begin{aligned}
\rho^E_{mc,f=1} &= \mathbb{E}_{\phi gxy\xi u} \theta_{xy} \rho^E_{\phi(g)xy} 2^\ell \delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)} \qquad (99) \\
\rho^E_{mc,f=0} &= \mathbb{E}_{\phi gxy\xi u} (1-\theta_{xy}) \rho^E_{\phi(g)xy} 2^\ell \delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)} \ . \qquad (100)
\end{aligned}
$$

We define the ideal protocol $\mathcal{F}$ as follows. If the input is such that $\mathcal{E}$ would abort, output the same state as $\mathcal{E}$. If $\mathcal{E}$ does not abort, let the output state be

$$
\omega^{MCEF}_{\mathrm{ideal},f=1} = \mathbb{E}_{mc} \left|mc\right\rangle \left\langle mc\right| \otimes \rho^E_{f=1} \qquad (101)
$$

where

$$\rho^E_{f=1} = \mathbb{E}_{mc}\rho^E_{mc,f=1} \tag{102}$$
$$= \mathbb{E}_{mc}\mathbb{E}_{\phi gxy\xi u}\theta_{xy}\rho^E_{\phi(g)xy}2^\ell\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)} \tag{103}$$
$$= \mathbb{E}_{\phi gxy\xi u}\theta_{xy}\rho^E_{\phi(g)xy}\sum_{m\oplus c}\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)} \tag{104}$$
$$= \mathbb{E}_{\phi gxy}\theta_{xy}\rho^E_{\phi(g)xy}\ . \tag{105}$$

We have $\mathbb{E}_{xy} = \sum_x 2^{-\ell}\sum_y \gamma^{\mathrm{Hamm}(x\oplus\bar{y})}(1-\gamma)^{\mathrm{Hamm}(x\oplus y)}$, where γ is the bit error rate (which is at most $Q+q$ in case of no abort).

We use the notation

$$\rho^E_{\phi(g)x} = \sum_y \gamma^{\mathrm{Hamm}(x\oplus\bar{y})}(1-\gamma)^{\mathrm{Hamm}(x\oplus y)}\rho^E_{\phi(g)xy} \tag{106}$$
$$\tag{107}$$

so we can write

$$\rho^E_{mc,f=1} = \mathbb{E}_{\phi gx}\rho^E_{\phi(g)x}\mathbb{E}_{\xi u}2^\ell\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)}\ , \tag{108}$$
$$\rho^E_{f=1} = \mathbb{E}_{\phi gx}\rho^E_{\phi(g)x}\ . \tag{109}$$

In case of abort, the ideal protocol is the same as the real one. For the security it is therefore only needed to consider the distance between the output states in case of no abort.

Using (93) we hence define the security of Protocol 2 as

$$\|\mathcal{E}-\mathcal{F}\|_\diamond = \|\mathcal{E}(\sigma^{\otimes n}) - \mathcal{F}(\sigma^{\otimes n})\|_1 \tag{110}$$
$$\leq 2^{-\kappa} + \eta(q) + \|\mathcal{E}'(\sigma^{\otimes n}) - \mathcal{F}(\sigma^{\otimes n})\|_1 \tag{111}$$
$$= 2^{-\kappa} + \eta(q) + \|\omega^{MCEF}_{f=1} - \omega^{MCEF}_{ideal,f=1}\|_1 \tag{112}$$
$$= 2^{-\kappa} + \eta(q) + \|\mathbb{E}_{mc}\left|mc\right\rangle\left\langle mc\right| \otimes \rho^E_{mc,f=1} - \mathbb{E}_{mc}\left|mc\right\rangle\left\langle mc\right| \otimes \rho^E_{f=1}\|_1 \tag{113}$$
$$= 2^{-\kappa} + \eta(q) + \mathbb{E}_{mc}\|\rho^E_{mc,f=1} - \rho^E_{f=1}\|_1 \tag{114}$$

where in the last step we used the fact that the mc form an orthonormal basis.

The following section shows the calculation of the last term.

4.4 Security analysis

$$D = \mathbb{E}_{mc}\|\rho^E_{mc,f=1} - \rho^E_{f=1}\|_1 \tag{115}$$

$$= \mathbb{E}_{mc}\|\mathbb{E}_{\phi gx}\rho^E_{\phi(g)x}\left[\mathbb{E}_{\xi u}2^\ell\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)} - 1\right]\|_1 \tag{116}$$

$$= \mathbb{E}_{mc\phi\xi}\|\mathbb{E}_{gx}\rho^E_{\phi(g)x}\left[\mathbb{E}_{u}2^\ell\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)} - 1\right]\|_1 \tag{117}$$

$$= \mathbb{E}_{mc\phi\xi}\mathrm{tr}\sqrt{\left(\mathbb{E}_{gx}\rho^E_{\phi(g)x}\left[\mathbb{E}_{u}2^\ell\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)} - 1\right]\right)^2} \tag{118}$$

$$= \mathbb{E}_{mc\phi\xi}\mathrm{tr}\sqrt{\mathbb{E}_{gg'}\mathbb{E}_{xx'}\rho^E_{\phi(g)x}\rho^E_{\phi(g')x'}\mathbb{E}_{uu'}(2^\ell\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)} - 1)(2^\ell\delta_{m\oplus c,\mathrm{Ext}(\xi(u'),x')} - 1)} \tag{119}$$

$$\leq \mathbb{E}_{mc}\mathrm{tr}\sqrt{\mathbb{E}_{gg'}\mathbb{E}_{xx'}\mathbb{E}_{\phi}\rho^E_{\phi(g)x}\rho^E_{\phi(g')x'}\Lambda} \tag{120}$$

where $\Lambda = \mathbb{E}_{\xi}\mathbb{E}_{uu'}(2^\ell\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)} - 1)(2^\ell\delta_{m\oplus c,\mathrm{Ext}(\xi(u'),x')} - 1)$.

Let us first simplify Λ. We have

$$\begin{aligned}\Lambda &= \mathbb{E}_{\xi}\mathbb{E}_{uu'}2^{2\ell}\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)}\delta_{m\oplus c,\mathrm{Ext}(\xi(u'),x')} \\ &\quad - \mathbb{E}_{\xi}\mathbb{E}_{u}2^{\ell}\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)} - \mathbb{E}_{\xi}\mathbb{E}_{u'}2^{\ell}\delta_{m\oplus c,\mathrm{Ext}(\xi(u'),x')} + 1 \qquad (121)\\ &= \mathbb{E}_{\xi}\mathbb{E}_{uu'}2^{2\ell}\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)}\delta_{m\oplus c,\mathrm{Ext}(\xi(u'),x')} - 1 - 1 + 1 \qquad (122)\end{aligned}$$

where in the last line we used that for any x,

$$\mathbb{E}_{\xi u}\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)} = 2^{-\ell} \tag{123}$$

because of the properties of pairwise independent hash functions (Definition 19).

Then, using $\delta_{xx'}$ which is 1 if $x = x'$ and 0 otherwise,

$$\Lambda = -1 + 2^{2\ell-2d}\mathbb{E}_\xi\left[\sum_u \delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)}\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x')} + \sum_{uu',u\neq u} \delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)}\delta_{m\oplus c,\mathrm{Ext}(\xi(u'),x')}\right] \tag{124}$$

$$= -1 + 2^{2\ell-2d}\left[\mathbb{E}_\xi \sum_u \delta_{xx'}(\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)})^2 + \mathbb{E}_\xi \sum_u (1-\delta_{xx'})\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)}\delta_{m\oplus c,\mathrm{Ext}(\xi(u),x')}\right.$$

$$\left. + \mathbb{E}_\xi \sum_{uu',u\neq u} \delta_{m\oplus c,\mathrm{Ext}(\xi(u),x)}\delta_{m\oplus c,\mathrm{Ext}(\xi(u'),x')}\right] \tag{125}$$

$$= -1 + 2^{2\ell-2d}\left[\sum_u 2^{-\ell}\delta_{xx'} + \sum_u 2^{-2\ell}(1-\delta_{xx'}) + \sum_{uu',u\neq u} 2^{-2\ell}\right] \tag{126}$$

$$= -1 + 2^{\ell-d}\delta_{xx'} + 2^{-d}(1-\delta_{xx'}) + 2^{-2d}(2^{2d}-2^d) \tag{127}$$

$$= -1 + 2^{-d}(2^\ell - 1)\delta_{xx'} + 2^{-d} + 1 - 2^{-d} \tag{128}$$

$$= \frac{2^\ell - 1}{2^d}\delta_{xx'}\ . \tag{129}$$

In (126) we used the fact that for any u, the uniform expectation over ξ allows us to apply Corollaries 20 and 21.

Substituting this back into the main formula yields

$$D \leq \sqrt{\frac{2^\ell - 1}{2^d}} \cdot \mathbb{E}_{mc}\mathrm{tr}\sqrt{\mathbb{E}_{gg'}\mathbb{E}_{xx'}\delta_{xx'}\mathbb{E}_\phi \rho^E_{\phi(g)x}\rho^E_{\phi(g')x'}} \tag{130}$$

$$= \sqrt{\frac{2^\ell - 1}{2^d}} \cdot \mathrm{tr}\sqrt{\mathbb{E}_{gg'}\mathbb{E}_{xx'}\delta_{xx'}\mathbb{E}_\phi \rho^E_{\phi(g)x}\rho^E_{\phi(g')x'}}\ . \tag{131}$$

We will now rewrite $\mathbb{E}_{gg'}\mathbb{E}_{xx'}\delta_{xx'}\mathbb{E}_{\phi}\rho^E_{\phi(g)x}\rho^E_{\phi(g')x'}$. Define

$$M = (1-\frac{3}{2}\gamma)\left|m_0\right\rangle\left\langle m_0\right| + \frac{\gamma}{2}\sum_{i=1}^{3}\left|m_j\right\rangle\left\langle m_j\right| \ , \tag{132}$$

$$A = c_1\left|m_0\right\rangle\left\langle m_0\right| + c_2\sum_{i=1}^{3}\left|m_i\right\rangle\left\langle m_i\right| \tag{133}$$

$$\tag{134}$$

where $c_1 = (1-\frac{3}{2}\gamma)(1-\gamma)$ and $c_2 = \frac{2\gamma+\gamma^2}{6}$.

Then,

$$\begin{aligned}
&\mathbb{E}_{gg'}\mathbb{E}_{xx'}\delta_{xx'}\mathbb{E}_{\phi}\rho^E_{\phi(g)x}\rho^E_{\phi(g')x'} && (135)\\
&= 2^{-2b}\sum_{gg',g\neq g'}\mathbb{E}_{xx'}\delta_{xx'}\mathbb{E}_{\phi}\rho^E_{\phi(g)x}\rho^E_{\phi(g')x'} + 2^{-2b}\sum_{g}\mathbb{E}_{xx'}\delta_{xx'}\mathbb{E}_{\phi}\rho^E_{\phi(g)x}\rho^E_{\phi(g)x'} && (136)\\
&= 2^{-2b}\sum_{gg',g\neq g'}2^{-2n}\sum_{x}\mathbb{E}_{\phi}\rho^E_{\phi(g)x}\rho^E_{\phi(g')x} + 2^{-2b}\sum_{g}2^{-2n}\sum_{x}\mathbb{E}_{\phi}\rho^E_{\phi(g)x}\rho^E_{\phi(g)x} && (137)\\
&= 2^{-2b}(2^{2b}-2^b)\cdot 2^{-2n}\sum_{x}(M^{\otimes n})^2 + 2^{-b}\cdot 2^{-2n}\sum_{x}A^{\otimes n} && (138)\\
&= 2^{-n}\Big[(1-2^{-b})(M^{\otimes n})^2 + 2^{-b}A^{\otimes n}\Big] \ . && (139)
\end{aligned}$$

In (138) we used Lemmas 33 and 34.

Finally, we obtain

$$\begin{aligned}
D &\leq \sqrt{\frac{2^{-n+\ell}-2^{-n})}{2^d}}\mathrm{tr}\sqrt{(1-2^{-b})(M^{\otimes n})^2 + 2^{-b}A^{\otimes n}} && (140)\\
&\leq \sqrt{\frac{2^{-n+\ell}-2^{-n})}{2^d}}\left[\big(1-2^{-b}\big)\mathrm{tr}\sqrt{(M^{\otimes n})^2} + 2^{-b}\mathrm{tr}\sqrt{A^{\otimes n}}\right] && (141)\\
&= \sqrt{\frac{2^{-n+\ell}-2^{-n})}{2^d}}\left[\big(1-2^{-b}\big) + 2^{-b}(\sqrt{c_1}+3\sqrt{c_2})^n\right] \ . && (142)
\end{aligned}$$

We use the bound $\sqrt{c_1}+3\sqrt{c_2} \leq 1+\gamma^{1/3}$. Then, as long as $d < \ell/2$,

$$\begin{aligned}
D &\leq \sqrt{2^{\ell-n-d}-2^{d-n}}\cdot\big[(1-2^{-b}) + 2^{-b}\cdot(1+\gamma^{1/3})^n\big] && (143)\\
&\leq \sqrt{2^{\ell-n-d}}\cdot\big[1+2^{-b+n\log(1+\gamma^{1/3})}\big] && (144)\\
&= 2^{\frac{1}{2}(\ell-n-d)} + 2^{\frac{1}{2}(\ell-\left[1-2\log(1+\gamma^{1/3})\right]n-d-2b)} \ . && (145)
\end{aligned}$$

Finally we state the security of the actual protocol.

Theorem 3. *Let M be a **uniform** message with length ℓ. Let d be the extractor seed length, b be the basis key length, r the number of traps, and κ the length of the authentication tag. Furthermore, let $\gamma = Q + q$ be the tolerated bit error rate. Let $\mathcal{E}$ be the CPTP map modeling Protocol 2 and $\mathcal{F}$ the ideal version of Protocol 2, as described above. Then,*

$$\|\mathcal{E} - \mathcal{F}\|_\diamond \leq 2^{-\kappa} + e^{\frac{-q^2 nr^2}{(n+r)(r+1)}} + 2^{\frac{1}{2}(\ell - n - d)} + 2^{\frac{1}{2}(\ell - \left[1 - 2\log(1+\gamma^{1/3})\right] n - d - 2b)} \ . \quad (146)$$

Proof. The distance $\mathbb{E}_{mc}\|\rho^E_{mc,f=1} - \rho^E_{f=1}\|_1$ is given by (145). Combining this with (114) proves the theorem.

□

4.5 Key length

In this section we consider what values for the key lengths we can use and what they mean for the security.

Recall the key material that Alice needs to remember. It is similar to that of Protocol 1, except that Alice now also needs to remember the basis encoding key:

- basis encoding key $g \in \{0,1\}^b$,
- trap location key $t \in \{0,1\}^{n+r}$ stored efficiently as a key of length $\log \binom{n+r}{r} \approx p = (n+r) \cdot h(r/(n+r))$,
- extractor seed $u \in \{0,1\}^d$
- MAC key $k \in \{0,1\}^\kappa$
- trap data key $v \in \{0,1\}^r$
- raw key syndrome $s \in \{0,1\}^\lambda$, where $\lambda \approx nh(Q+q)$

Again, we want their total length to remain smaller than ℓ:

$$b + p + d + \kappa + r + \lambda < \ell \ . \quad (147)$$

In the security error there are two terms that are the same as in Protocol 1: $2^{-\kappa}$ and $\eta(q) = e^{\frac{-q^2 nr^2}{(n+r)(r+1)}}$. The other two terms are different, and in fact look more like standard security expressions for QKD or QKR. Indeed, it is clear to see that larger values for n and the key length result in lower security errors, and that these values depend (partly) on the bit error rate γ. Assuming d and b are constants, the last term in Theorem 3 reveals a "rate" of $1 - 2\log(1+\gamma^{1/3})$. This means that the maximum tolerated error rate is roughly 0.07, since for higher values of γ this rate drops below zero. This is in contrast with Protocol 1, which does not have a hard bound on the maximum tolerated bit error rate. However, as we saw in Section 3.5, high tolerated BER values quickly lead to large key material (λ); for example when setting $\gamma = 0.07$, λ becomes $h(0.07) \approx 0.37$, meaning that Alice needs to remember at least a fraction 0.37 of the message length herself. Using a much lower tolerated γ we can get similar concrete values for key length and security as in Section 3.5.

We note that working in the CRS model might not be very useful; it is a somewhat strange assumption. However, we did show that our protocol is secure given such a perfect pseudo-random generator (PRG), if it exists. Therefore, the security of an instantiation of our protocol using a real-world PRG really depends on the security of that PRG. In other words, the security of our protocol is independent of how the PRG is actually implemented.

Furthermore, the pseudorandom generation of longer keys might seem like cheating, and one could ask if we could not simply use existing classical encryptions based on pseudorandom generation. We note however that our quantum protocol still has the special ability of checking Eve's tampering, which is classicaly not possible. Therefore, a classical protocol for delegated storage based on the CRS model is not possible, since Eve can brute-force the ciphertext without Alice noticing.

5 Discussion

5.1 Relevancy of the results

The results of the previous sections can be seen both from a theoretical and a practical viewpoint.

Theorem 2 (and Theorem 1 as a special case) is interesting from a theoretical viewpoint since it shows that we can have a form of information-theoretic security, while using keys that are shorter than the plaintext. In most cases, information-theoretic security is associated with longer keys. On the other hand, Theorem 3 states the same, but relies on the CRS model assumption. Therefore the result is perhaps somewhat less special, because CRS can be used to 'explain' the shorter keys.

Furthermore, Theorem 1 proves the possibility of information-theoretic security for unknown plaintexts. This has implications for QKD, as follows. For a uniform plaintext, the ciphertext in Protocol 1 is independent of the raw key quantum state. Therefore, ignoring the message completely, the protocol can really be seen as Alice performing QKD with 'herself in the future', where the server is the quantum channel that Eve listens on. If we swap out 'future Alice' for Bob, and let Eve be a 'normal' quantum channel again, Theorem 1 is now a result for QKD: namely that Alice and Bob can establish a key, while having to exchange ('remember' in delegated storage) *fewer* bits than the length of the established key.

Finally, the composability of our protocols implies that we can chain together a sequence of these protocols. A relatively short key can be used for secure delegated storage of a longer key, which is used for the delegated storage for an even longer key, and so on. Finally, the last key can be used to actually one-time pad the plaintext. In this way, it is in theory possible to securely store an arbitrarily long plaintext using a short key of fixed length.

Practically, one could argue that the results are not particularly relevant, at least not at the moment. Quantum memory is currently a very difficult technological challenge, with attainable storage times of typically fractions of a second. (Storage times of serveral hours have been shown in some circumstances [1].) Refreshing techniques—used for example with DRAM—where the memory value is periodically read and rewritten, cannot be used because of the uncloneable nature of the quantum memory. The act of reading it (before rewriting) will destroy the original value.

While the amount of key material is shorter than the message length, it is not significantly shorter, except when only very little noise is tolerated. We saw that the bottleneck here is the error correction syndrome. If we want to let the syndrome be at most 1% of the message length, we can only tolerate an error rate of roughly 0.00087 (since $h(0.00087) \approx 0.01$). If we tolerate 2% noise, the syndrome has length roughly $nh(0.02) \approx 0.14n$. If we want to store 1 TB, it is not clear if we are satisfied in having to store at least 140 GB of key material ourselves. In theory, we could use the chaining technique as mentioned above. However, this would require (many) more operations for storing and retrieving the data, namely wrapping and unwrapping each 'layer' of delegated storage.

5.2 Protocol design

The two protocols proposed in this thesis have the same structure. They rely on trap qubits distributed among the raw-key qubits. The idea is that checking the values of the traps after retrieval gives a straight-forward way to estimate the amount of tampering: simply count the number of bit flips. The use of trap qubits has its origin in earlier work on Provable Deletion by Coiteux-Roy [13], where deliberate measurement of the traps results in the destruction of the message qubits. Furthermore, the concept of additional qubits that are purely used for tamper checking, is well known in BB84. Therefore, we were comfortable in using traps for our protocols as well.

However, we can simplify their use somewhat compared to what we did in Protocols 1 and 2. First of all, as hinted in the description of Protocol 1, it it not necessary to remember the trap *values*. Instead we can simply rember a MAC of the trap values as well as their syndrome. After retrieval, we try to error correct the traps. By checking the MAC of the result, Alice knows whether error correction succeeded or not. If we assume that the error correcting code that we used can only correct up to, say, s bit flips (except with negligible probability), the correct MAC tag then means that there were at most s errors in the traps. Since a MAC tag is typically only of constant length, we reduce the total key length by roughly r (the number of traps).

So far we have considered traps that are *additional* qubits, separate from the raw-key qubits. We could also let the trap values themselves be part of the raw key. One could imagine a protocol that is similar to Protocol 1, with the following changes. Alice encodes most of her raw key bits in the standard basis, and the other bits in the Hadamard basis. She remembers separately the MAC and syndrome of the qubits in the standard basis and the MAC and syndrome of the qubits in the Hadamard basis. After retrieval, she tries to error correct both parts and checks their MAC tags. In this way she can bound the number of bit flips in each part. For both parts, we can apply the entropic uncertainty relation to estimate the min-entropy of the other part. The sums of these min-entropies then gives us a bound on Eve's knowledge about the full raw key.

We used 4-state (or BB84 encoding) for Protocol 1 and 8-state for Protocol 2. It is worth consdering how 6-state could be used for delegated storage, but we do not see immediate uses. The entropic relations that we use for the analysis of Protocol 1 make use of a certain duality between two incompatible bases; a third basis would not help much. Indeed, there exist entropic relations for more than two sets of bases, but their bounds are not tight enough [14]. In Protocol 2 we used the property of 8-state encoding that it is an encryption. Averaged over all basis keys, the quantum state is fully mixed. This allowed us to simplify the expression for the diamond distance. 6-state does not give us this property.

5.3 Further work

There are still directions in which one could invest more research.

One direction is to investigate how we can reduce the key length that Alice needs to remember. We mentioned the 'chaining' technique, where the key itself is also stored on a server, for which Alice only needs to remember even shorter keys, and so on. It is worth investigating the security that is lost at each such iteration and whether it is worth it compared to the key size that it saves.

It might also be worth investigating if we can just store parts of the key on the server. Perhaps it is possible to do a form of 'chaining' on only the syndrome: store the syndrome on the server, encoded in some way, and remember locally a *shorter* syndrome such that the orignal syndrome itself can be error-corrected. Furthermore, we argued that the extractor seed should not be stored on the server since Eve might use it to perform a better attack. It is not clear however *how much* her having the seed compromises the security, and indeed it might still be possible to store the seed on the server, perhaps with a suitable quantum encoding. Futhermore, it could be interesting to see whether it is useful to quantum-encode the ciphertext (the one-time pad of the message) as well.

We should also mention Gottesman's work about Uncloneable Encryption, in which he uses a form of privacy amplification in which the parties do not need to remember the seed. It is based on error correcting codes, and much different than extractor-based privacy amplification like we studied in this thesis. However, the fact that the generated seed can be forgotten by Alice after its use might make it suitable for delegated storage with short keys. It is not clear however if Gottesman's form of privacy amplification also yields composable security.

Apart from looking for ways to shorten the key, we can think about different techniques for analyzing the security.

For the analysis of Protocol 1 we tried, without result, to immediately bound the min-entropy of the extractor output by modeling measurement and post-processing as one POVM. Using this we could have bounded the min-entropy of the message, given Eve's side-information. Although such a result about the min-entropy is weaker than the diamond distance that we *did* use in this thesis, it is still a composable security measure, and worth investigating more. The problem that we faced was that short-seeded extractors typically do not have properties that allow us to calculate the number of inputs that give a certain output. It is worth investigating whether there are short-seeded extractors that do have these properties, to hopefully get better bounds when we try to model extraction as a POVM.

We faced the issue that a non-uniform message gives a ciphertext that Eve can use to her advantage while performing her attack. One idea to tackle this issue is to use a raw key x such that the message m is the output of applying an extractor on x with seed u. In this way, there is no ciphertext c needed and hence it is not observed by Eve. Alice would need to compute the inverse of the extractor to find a suitable such x.

Finally, it would be interesting to revisit the topic of Provable Deletion [13], and see if it can be incorporated with the protocols from this thesis.

6 Conlusion

In this thesis we set out to find quantum protocols for secure delegated storage of classical messages. These protocols should work with a key shorter than the message itself, but should still prevent an adversary to learn anything about the message without noticeable tampering of the quantum state, with information-theoretic guarantee. We proposed two protocols that achieve this. Protocol 1 uses BB84-encoding of a raw key, out of which a one-time pad for the message is extracted. Privacy amplification is done with a short-seeded quantum-proof extractor. The security analysis relies on entropic uncertainty relations. Protocol 2 is similar but uses 8-state encoding instead, and relies on the assumption of the CRS model. It uses a pairwise indepenent hash function for extraction. For both protocols, the bottleneck in terms of key length is the raw-key syndrome that needs to be remembered in order to perform error correction. Although the required key length in both cases is relatively long—roughly linear in the message length—the fact that we can still obtain information-theoretic security is an interesting result.

Appendices

A Quantum measurement and extraction as one POVM

Measure subsystem UCA of $\rho^{UCA,UCB,CE}$ with either POVM $P_0 = \{M_0^m \mid m \in \{0,1\}^\ell\}$ or POVM $P_1 = \{M_1^m \mid m \in \{0,1\}^\ell\}$ with

$$M_0^m = \sum_u |u\rangle\langle u| \otimes \sum_c |c\rangle\langle c| \otimes \sum_x |x\rangle\langle x| \, \delta_{mcux} \tag{148}$$

$$M_1^m = \sum_u |u\rangle\langle u| \otimes \sum_c |c\rangle\langle c| \otimes \sum_x H|x\rangle\langle x| H \delta_{mcux} \tag{149}$$

$$\tag{150}$$

for each m, and where δ_{mcux} is a shorthand for $\delta_{m\oplus c,\mathrm{Ext}(u,x)}$.

Then the overlap $c(P_0, P_1)$ is

$$c(P_0,P_1) = \max_{m,m'} \|M_0^m (M_1^{m'})^\dagger\|_\infty^2 = \max_v \{\langle v| M_0^m M_1^{m'} M_0^m |v\rangle : |v\rangle \in \mathcal{H}_U \otimes \mathcal{H}_C \otimes \mathcal{H}_A\} \tag{151}$$

To upper bound the overlap, we need to find the eigenvector $|v\rangle$ that has the largest eigenvalue. We note that this eigenvector must be in the subspace spanned by the projector M_0^m, according to Lemma 11.

Now we can evaluate $\|M_0^m (M_1^{m'})^\dagger\|_\infty^2$. Let $|v\rangle = \sum_{ucx} \delta_{mcux} \lambda_{ucx} |u\rangle\otimes|c\rangle\otimes|x\rangle$ for eigenvalues λ_{ucx}. Then

$$\begin{aligned}\max_v \{\langle v| M_0^m M_1^{m'} M_0^m |v\rangle : |v\rangle\} &= \max_v \{\langle v| M_0^m M_1^{m'} M_0^m |v\rangle : |v\rangle = \sum_{ucx} \delta_{mcux}\lambda_{ucx} |u\rangle\otimes|c\rangle\otimes|x\rangle\} \\ &= \max_v \{\langle v| M_1^{m'} |v\rangle : |v\rangle = \sum_{ucx} \delta_{mcux}\lambda_{ucx} |u\rangle\otimes|c\rangle\otimes|x\rangle\}\end{aligned} \tag{152}$$

We have

$$\begin{aligned} M_1^{m'} &= \sum_u |u\rangle\langle u| \otimes \sum_c |c\rangle\langle c| \otimes \sum_x H|x\rangle\langle x| H \delta_{m'cux} \\ &= \sum_u |u\rangle\langle u| \otimes \sum_c |c\rangle\langle c| \otimes \sum_x 2^{-n/2} \sum_{x'} (-1)^{x\cdot x'} |x'\rangle \cdot 2^{-n/2} \sum_{\hat{x}} (-1)^{x\cdot\hat{x}} \langle\hat{x}| \, \delta_{m'cux} \\ &= 2^{-n} \sum_{ucxx'\hat{x}} \delta_{m'cux} |uc\rangle\langle uc| \otimes (-1)^{x\cdot(x'\oplus\hat{x})} |x'\rangle\langle\hat{x}| \end{aligned} \tag{153}$$

Substituting this into (152) yields

$$\begin{aligned} c(P_0, P_1) &= \max_v 2^{-n} \sum_{ucxx'\hat{x}} \delta_{m'cux} (-1)^{x(x' \oplus \hat{x})} \langle v|ucx'\rangle \langle uc\hat{x}|v\rangle \\ &= \max_\lambda 2^{-n} \sum_{ucxx'\hat{x}} \delta_{m'cux} \delta_{mcux'} \delta_{mcu\hat{x}} (-1)^{x(x' \oplus \hat{x})} \lambda^*_{cux'} \lambda_{cu\hat{x}} \\ &\leq \max_\lambda 2^{-n} \sum_{ucxx'\hat{x}} \delta_{m'cux} \delta_{mcux'} \delta_{mcu\hat{x}} \lambda^*_{ucx'} \lambda_{uc\hat{x}} \end{aligned} \tag{154}$$

where the λ to maximize over is the vector of eigenvalues of $|v\rangle$.

A.1 Min-entropy bound for pairwise independent extractor

We will now calculate $c(P_0, P_1)$ for a pairwise independent extractor, and use it in an entropic uncertainty relation.

Let Γ_m be the number of (u, c, x)-combinations that give $\mathrm{Ext}(u, x) = m \oplus c$. That is, $\Gamma_m = \sum_{ucx} \delta_{mcux}$. We have for all x and for all z, $\sum_u \Pr[\mathrm{Ext}(u, x) = z] = 2^{d-\ell}$, so for all m, $\Gamma_m = \sum_c 2^{d+n-\ell} = 2^{d+n}$.

Let $\lambda_{ucx} = 2^{(-d-n)/2}$ for all u, c, x. Note that then

$$\langle v|v\rangle = \sum_{ucx} \delta_{mcux} 2^{-d-n} = \Gamma_m 2^{-d-n} = 1 \tag{155}$$

so $|v\rangle$ is a valid vector. We conjecture that these λ_{ucx}, an equal spread over all (u, c, x)-combinations, gives us the smallest value for $c(P_0, P_1)$. We do not prove this conjecture here.

Substituting this into (154) gives

$$\begin{aligned} c(P_0, P_1) &\leq 2^{-n} \sum_{xx'\hat{x}} \sum_{uc} \delta_{m'cux} \delta_{mcux'} \delta_{mcu\hat{x}} 2^{-d-n} \\ &= 2^{-2n-d} \Big[\sum_{xx'} \sum_{uc} \delta_{m'cux} \delta_{mcux'} + \sum_{xx'\hat{x}, x' \neq \hat{x}} \sum_{mc} \delta_{m'cux} \delta_{mcux'} \delta_{mcu\hat{x}} \Big] \\ &= 2^{-2n-d} \Big[\sum_{xx'} 2^{d+\ell} 2^{-2\ell} + \sum_{xx'\hat{x}, x' \neq \hat{x}} 2^{d+\ell} 2^{-3\ell} \Big] \\ &= 2^{-2n-d} \Big[2^{2n+d-2\ell} + (2^{3n} - 2^{2n}) 2^{d-3\ell} \Big] \\ &= 2^{-\ell} + 2^{n-2\ell} - 2^{-2\ell} \ . \end{aligned} \tag{156}$$

Consider now the output Z which is the result of POVM P_0 and Z' which is the result of POVM P_1. Combining the above result with Lemma 13, we can now state

$$H^\varepsilon_{\min}(Z|EC) + H^\varepsilon_{\max}(Z'|BU) \geq \log \frac{1}{c(P_0, P_1)} \tag{157}$$

which is non-negative only if $n < 2\ell$.

The result is hence that as long as $n < 2\ell$, we can use an entropic uncertainty relation on the POVM representing "measurement followed by pairwise independent hashing", which then gives us a non-negative lower bound on the min-entropy of the extractor output, given Eve's side-information (including the ciphertext).

B Proof of Lemmas 33, 34 and 35

We repeat the expressions for Eve's state $|E^v_{xy}\rangle$ for outcomes x for Alice and y for Bob. Note that we are considering singlet states, meaning that no noise results in anticorrelated results.

$$|E^v_{01}\rangle = \frac{1}{\sqrt{1-\gamma}}\left[\sqrt{1-\frac{3}{2}\gamma}\,|m_0\rangle + \sqrt{\frac{\gamma}{2}}\,|v\cdot m\rangle\right] \tag{158}$$

$$|E^v_{10}\rangle = \frac{1}{\sqrt{1-\gamma}}\left[\sqrt{1-\frac{3}{2}\gamma}\,|m_0\rangle - \sqrt{\frac{\gamma}{2}}\,|v\cdot m\rangle\right] \tag{159}$$

$$|E^v_{00}\rangle = \frac{1}{\sqrt{2(1-v_3^2)}}\Big[(-v_1v_3 - iv_2)\,|m_1\rangle + (-v_2v_3 + iv_1)\,|m_2\rangle + (1-v_3^2)\,|m_3\rangle\Big] \tag{160}$$

$$|E^v_{11}\rangle = \frac{1}{\sqrt{2(1-v_3^2)}}\Big[(-v_1v_3 + iv_2)\,|m_1\rangle + (-v_2v_3 - iv_1)\,|m_2\rangle + (1-v_3^2)\,|m_3\rangle\Big] \tag{161}$$

$$\tag{162}$$

Below are given the expressions for the corresponding projectors.

$$|E^v_{01}\rangle\langle E^v_{01}| = \frac{1}{1-\gamma}\Bigg[(1-\frac{3}{2}\gamma)\,|m_0\rangle\langle m_0| + \sqrt{\frac{\gamma}{2}-\frac{3}{4}\gamma^2}\,|m_0\rangle\langle v\cdot m| + \sqrt{\frac{\gamma}{2}-\frac{3}{4}\gamma^2}\,|v\cdot m\rangle\langle m_0| + \frac{\gamma}{2}\,|v\cdot m\rangle\langle v\cdot m|\Bigg] \tag{163}$$

$$|E^v_{10}\rangle\langle E^v_{10}| = \frac{1}{1-\gamma}\Bigg[(1-\frac{3}{2}\gamma)\,|m_0\rangle\langle m_0| - \sqrt{\frac{\gamma}{2}-\frac{3}{4}\gamma^2}\,|m_0\rangle\langle v\cdot m| - \sqrt{\frac{\gamma}{2}-\frac{3}{4}\gamma^2}\,|v\cdot m\rangle\langle m_0| + \frac{\gamma}{2}\,|v\cdot m\rangle\langle v\cdot m|\Bigg] \tag{164}$$

$$|E^v_{00}\rangle\langle E^v_{00}| = \frac{1}{2}\sum_{i=1}^{3}|m_i\rangle\langle m_i| - \frac{1}{2}\,|v\cdot m\rangle\langle v\cdot m| + \frac{i}{2}\sum_{ijp=1}^{3}\varepsilon_{jkp}v_j\,|m_k\rangle\langle m_p| \tag{165}$$

$$|E^v_{11}\rangle\langle E^v_{11}| = |E^{-v}_{00}\rangle\langle E^{-v}_{00}| = \frac{1}{2}\sum_{i=1}^{3}|m_i\rangle\langle m_i| - \frac{1}{2}\,|-v\cdot m\rangle\langle -v\cdot m| - \frac{i}{2}\sum_{ijp=1}^{3}\varepsilon_{jkp}v_j\,|m_k\rangle\langle m_p| \tag{166}$$

Now we consider Eve's state given a certain outcome x for Alice. Bob's outcome depends on x according to the noise paramater γ.

We have

$$\rho^E_{v,x=0} = (1-\gamma)\,|E^v_{01}\rangle\langle E^v_{01}| + \gamma\,|E^v_{00}\rangle\langle E^v_{00}| \tag{167}$$

$$= (1-\frac{3}{2}\gamma)\,|m_0\rangle\langle m_0| + \frac{\gamma}{2}\sum_{i=1}^{3}|m_i\rangle\langle m_i| \tag{168}$$

$$+ \sqrt{\frac{\gamma}{2}-\frac{3}{4}\gamma^2}\,|m_0\rangle\langle v\cdot m| + \sqrt{\frac{\gamma}{2}-\frac{3}{4}\gamma^2}\,|v\cdot m\rangle\langle m_0| + \frac{i\gamma}{2}\sum_{ijp=1}^{3}\varepsilon_{jkp}v_j\,|m_k\rangle\langle m_p| \tag{169}$$

and

$$\rho^E_{v,x=1} = (1-\gamma)\,|E^v_{10}\rangle\langle E^v_{10}| + \gamma\,|E^v_{11}\rangle\langle E^v_{11}| \tag{170}$$

$$= (1-\frac{3}{2}\gamma)\,|m_0\rangle\langle m_0| + \frac{\gamma}{2}\sum_{i=1}^{3}|m_i\rangle\langle m_i| \tag{171}$$

$$- \sqrt{\frac{\gamma}{2}-\frac{3}{4}\gamma^2}\,|m_0\rangle\langle v\cdot m| - \sqrt{\frac{\gamma}{2}-\frac{3}{4}\gamma^2}\,|v\cdot m\rangle\langle m_0| - \frac{i\gamma}{2}\sum_{ijp=1}^{3}\varepsilon_{jkp}v_j\,|m_k\rangle\langle m_p|\ . \tag{172}$$

Proof of Lemma 33. Using the above expressions, we can take the uniform expectation over all 4 possible bases b of eight-state encoding. Let $v(b)$ be the corresponding vector according to (39).

$$\mathbb{E}_b\rho^E_{b,x=0} = \mathbb{E}_b\rho^E_{b,x=1} \tag{173}$$

$$= \frac{1}{4}\Big[\rho^E_{v(0),x=0} + \rho^E_{v(1),x=0} + \rho^E_{v(2),x=0} + \rho^E_{v(3),x=0}\Big] \tag{174}$$

$$= (1-\frac{3}{2}\gamma)\,|m_0\rangle\langle m_0| + \frac{\gamma}{2}\sum_{i=1}^{3}|m_i\rangle\langle m_i| \tag{175}$$

□

Now we will calculate $\mathbb{E}_b \rho_{v(b),x} \rho_{v(b),y}$ for all values x, y. We have

$$\rho_{v,x=0}\rho_{v,x=0} = (1-\gamma)^2 \left|E^v_{01}\right\rangle \left\langle E^v_{01}\right| + \gamma^2 \left|E^v_{00}\right\rangle \left\langle E^v_{00}\right| \tag{176}$$

$$= (1 - \frac{5}{2}\gamma + \frac{3}{2}\gamma^2) \left|m_0\right\rangle \left\langle m_0\right| + \frac{\gamma^2}{2} \sum_{i=1}^{3} \left|m_i\right\rangle \left\langle m_i\right| \tag{177}$$

$$+ \frac{\gamma - \gamma^2}{2} \left|v \cdot m\right\rangle \left\langle v \cdot m\right| \tag{178}$$

$$+ (1-\gamma)\sqrt{\frac{\gamma}{2} - \frac{3}{4}\gamma^2} \left|m_0\right\rangle \left\langle v \cdot m\right| + (1-\gamma)\sqrt{\frac{\gamma}{2} - \frac{3}{4}\gamma^2} \left|v \cdot m\right\rangle \left\langle m_0\right| \tag{179}$$

$$+ \frac{i\gamma^2}{2} \sum_{ijp=1}^{3} \varepsilon_{jkp} v_j \left|m_k\right\rangle \left\langle m_p\right| \ . \tag{180}$$

$$\rho_{v,x=1}\rho_{v,x=1} = (1-\gamma)^2 \left|E^v_{10}\right\rangle \left\langle E^v_{10}\right| + \gamma^2 \left|E^v_{11}\right\rangle \left\langle E^v_{11}\right| \tag{181}$$

$$= (1 - \frac{5}{2}\gamma + \frac{3}{2}\gamma^2) \left|m_0\right\rangle \left\langle m_0\right| + \frac{\gamma^2}{2} \sum_{i=1}^{3} \left|m_i\right\rangle \left\langle m_i\right| \tag{182}$$

$$+ \frac{\gamma - \gamma^2}{2} \left|v \cdot m\right\rangle \left\langle v \cdot m\right| \tag{183}$$

$$- (1-\gamma)\sqrt{\frac{\gamma}{2} - \frac{3}{4}\gamma^2} \left|m_0\right\rangle \left\langle v \cdot m\right| - (1-\gamma)\sqrt{\frac{\gamma}{2} - \frac{3}{4}\gamma^2} \left|v \cdot m\right\rangle \left\langle m_0\right| \tag{184}$$

$$- \frac{i\gamma^2}{2} \sum_{ijp=1}^{3} \varepsilon_{jkp} v_j \left|m_k\right\rangle \left\langle m_p\right| \tag{185}$$

$$\rho_{v,x=0}\rho_{v,x=1} = \Big[(1-\gamma)\left|E^v_{01}\right\rangle \left\langle E^v_{01}\right| + \gamma \left|E^v_{00}\right\rangle \left\langle E^v_{00}\right|\Big] \cdot \Big[(1-\gamma)\left|E^v_{10}\right\rangle \left\langle E^v_{10}\right| + \gamma \left|E^v_{11}\right\rangle \left\langle E^v_{11}\right|\Big] \tag{186}$$

$$= (1-\gamma)(1-2\gamma)\left|E^v_{01}\right\rangle \left\langle E^v_{10}\right| \tag{187}$$

$$\rho_{v,x=1}\rho_{v,x=0} = \Big[(1-\gamma)\left|E^v_{10}\right\rangle \left\langle E^v_{10}\right| + \gamma \left|E^v_{11}\right\rangle \left\langle E^v_{11}\right|\Big] \cdot \Big[(1-\gamma)\left|E^v_{01}\right\rangle \left\langle E^v_{01}\right| + \gamma \left|E^v_{00}\right\rangle \left\langle E^v_{00}\right|\Big] \tag{188}$$

$$= (1-\gamma)(1-2\gamma)\left|E^v_{10}\right\rangle \left\langle E^v_{01}\right| \tag{189}$$

Proof of Lemmas 34 and 35. Using the above expressions, we can again take the uniform expectation over all 4 possible bases b of eight-state encoding. Let $v(b)$ be the corresponding vector according to (39).

$$\mathbb{E}_b \rho_{b0} \rho_{b0} = \mathbb{E}_b \rho_{b1} \rho_{b1} \tag{190}$$

$$= \frac{1}{4}\Big[\rho^E_{v(0),x=0}\rho^E_{v(0),x=0} + \rho^E_{v(1),x=0}\rho^E_{v(1),x=0} + \rho^E_{v(2),x=0}\rho^E_{v(2),x=0} + \rho^E_{v(3),x=0}\rho^E_{v(3),x=0}\Big] \tag{191}$$

$$= (1 - \frac{5}{2}\gamma + \frac{3}{2}\gamma^2)\left|m_0\right\rangle\left\langle m_0\right| + \frac{2\gamma^2+\gamma}{6}\sum_{i=1}^{3}\left|m_i\right\rangle\left\langle m_i\right| \tag{192}$$

$$\mathbb{E}_b \rho_{b0} \rho_{b1} = \mathbb{E}_b \rho_{b1} \rho_{b0} \tag{193}$$

$$= \frac{1}{4}\Big[\rho^E_{v(0),x=0}\rho^E_{v(0),x=1} + \rho^E_{v(1),x=0}\rho^E_{v(1),x=1} + \rho^E_{v(2),x=0}\rho^E_{v(2),x=1} + \rho^E_{v(3),x=0}\rho^E_{v(3),x=1}\Big] \tag{194}$$

$$= \Big(1 - \frac{7}{2}\gamma + 3\gamma^2\Big)\left|m_0\right\rangle\left\langle m_0\right| + \frac{2\gamma^2-\gamma}{6}\sum_{i=1}^{3}\left|m_i\right\rangle\left\langle m_i\right| \tag{195}$$

□

References

[1] Thomas Astner et al. "Solid-state electron spin lifetime limited by phononic vacuum modes". In: *Nature materials* 17.4 (2018), pp. 313–317.

[2] Boaz Barak et al. "Leftover hash lemma, revisited". In: *Annual Cryptology Conference*. Springer. 2011, pp. 1–20.

[3] Avraham Ben-Aroya and Amnon Ta-Shma. "Better short-seed quantum-proof extractors". In: *Theoretical Computer Science* 419 (2012), pp. 17–25.

[4] Michael Ben-Or et al. "The universal composable security of quantum key distribution". In: *Theory of Cryptography Conference*. Springer. 2005, pp. 386–406.

[5] Charles H Bennett and Gilles Brassard. "Quantum cryptography: public key distribution and con Tos5". In: *Proceedings of the International Conference on Computers, Systems and Signal Processing*. 1984.

[6] Kamil Brádler et al. "Finite-key security analysis for multilevel quantum key distribution". In: *New Journal of Physics* 18.7 (2016), p. 073030.

[7] Anne Broadbent and Sébastien Lord. "Uncloneable Quantum Encryption via Random Oracles". In: *arXiv preprint arXiv:1903.00130* (2019).

[8] Anne Broadbent and Christian Schaffner. "Quantum cryptography beyond quantum key distribution". In: *Designs, Codes and Cryptography* 78.1 (2016), pp. 351–382.

[9] Matthias Christandl, Robert König, and Renato Renner. "Postselection technique for quantum channels with applications to quantum cryptography". In: *Physical review letters* 102.2 (2009), p. 020504.

[10] Matthias Christandl, Renato Renner, and Artur Ekert. "A generic security proof for quantum key distribution". In: *arXiv preprint quant-ph/0402131* (2004).

[11] Kai-Min Chung et al. "Quantum-Proof Extractors: Optimal up to Constant Factors". In: *arXiv* (2016).

[12] Gil Cohen, Ran Raz, and Gil Segev. "Nonmalleable extractors with short seeds and applications to privacy amplification". In: *SIAM Journal on Computing* 43.2 (2014), pp. 450–476.

[13] Xavier Coiteux-Roy and Stefan Wolf. "Proving Erasure". In: *arXiv preprint arXiv:1902.06656* (2019).

[14] Patrick J Coles et al. "Entropic uncertainty relations and their applications". In: *Reviews of Modern Physics* 89.1 (2017), p. 015002.

[15] Patrick J Coles et al. "Uncertainty relations from simple entropic properties". In: *Physical review letters* 108.21 (2012), p. 210405.

[16] Ivan Damgård, Thomas Brochmann Pedersen, and Louis Salvail. "A Quantum Cipher with Near Optimal Key-recycling". In: *Proceedings of the 25th Annual International Conference on Advances in Cryptology*. CRYPTO'05. Santa Barbara, California: Springer-Verlag, 2005, pp. 494–510. ISBN: 3-540-28114-2, 978-3-540-28114-6. DOI: 10.1007/11535218_30. URL: http://dx.doi.org/10.1007/11535218_30.

[17] Ivan Damgård, Thomas Brochmann Pedersen, and Louis Salvail. "How to Re-use a One-time Pad Safely and Almost Optimally Even if P = NP". In: 13.4 (Dec. 2014), pp. 469–486. ISSN: 1567-7818. DOI: 10.1007/s11047-014-9454-5. URL: http://dx.doi.org/10.1007/s11047-014-9454-5.

[18] Anindya De et al. "Trevisan's extractor in the presence of quantum side information". In: *SIAM Journal on Computing* 41.4 (2012), pp. 915–940.

[19] Serge Fehr and Louis Salvail. "Quantum authentication and encryption with key recycling". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2017, pp. 311–338.

[20] Dmitry Gavinsky et al. "Exponential separations for one-way quantum communication complexity, with applications to cryptography". In: *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*. 2007, pp. 516–525.

[21] Pete Gemmell and Moni Naor. "Codes for interactive authentication". In: *Annual International Cryptology Conference*. Springer. 1993, pp. 355–367.

[22] Daniel Gottesman. "Uncloneable encryption". In: *arXiv preprint quant-ph/0210062* (2002).

[23] Russell Impagliazzo, Leonid A Levin, and Michael Luby. "Pseudo-random generation from one-way functions". In: *Proceedings of the twenty-first annual ACM symposium on Theory of computing*. ACM. 1989, pp. 12–24.

[24] Robert König and Renato Renner. "A de Finetti representation for finite symmetric quantum states". In: *Journal of Mathematical physics* 46.12 (2005), p. 122108.

[25] Robert Konig, Renato Renner, and Christian Schaffner. "The operational meaning of min-and max-entropy". In: *IEEE Transactions on Information theory* 55.9 (2009), pp. 4337–4347.

[26] Robert König et al. "Small accessible quantum information does not imply security". In: *Physical Review Letters* 98.14 (2007), p. 140502.

[27] Barbara Kraus, Nicolas Gisin, and Renato Renner. "Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication". In: *Physical review letters* 95.8 (2005), p. 080501.

[28] Daan Leermakers and Boris Skoric. "Optimal Attacks on Qubit-based Quantum Key Recycling". In: *Quantum Information Processing* 17.3 (Mar. 2018), pp. 1–31. ISSN: 1570-0755. DOI: 10.1007/s11128-018-1819-8. URL: https://doi.org/10.1007/s11128-018-1819-8.

[29] Daan Leermakers and Boris Skoric. "Security proof for Quantum Key Recycling with noise." In: *IACR Cryptology ePrint Archive* 2018 (2018), p. 264.

[30] Hoi-Kwong Lo and Hoi Fung Chau. "Unconditional security of quantum key distribution over arbitrarily long distances". In: *science* 283.5410 (1999), pp. 2050–2056.

[31] Hoi-Kwong Lo, Hoi Fung Chau, and Mohammed Ardehali. "Efficient quantum key distribution scheme and a proof of its unconditional security". In: *Journal of Cryptology* 18.2 (2005), pp. 133–165.

[32] Michael A Nielsen and Isaac L Chuang. "Quantum information and quantum computation". In: *Cambridge: Cambridge University Press* 2.8 (2000), p. 23.

[33] Christopher Portmann and Renato Renner. "Cryptographic security of quantum key distribution". In: *arXiv preprint arXiv:1409.3525* (2014).

[34] Renato Renner. "Security of quantum key distribution". In: *International Journal of Quantum Information* 6.01 (2008), pp. 1–127.

[35] Renato Renner. "Symmetry of large physical systems implies independence of subsystems". In: *Nature Physics* 3.9 (2007), p. 645.

[36] Renato Renner, Nicolas Gisin, and Barbara Kraus. "Information-theoretic security proof for quantum-key-distribution protocols". In: *Physical Review A* 72.1 (2005), p. 012332.

[37] Renato Renner and Stefan Wolf. "Simple and tight bounds for information reconciliation and privacy amplification". In: *International conference on the theory and application of cryptology and information security*. Springer. 2005, pp. 199–216.

[38] Ronen Shaltiel. "Recent developments in explicit constructions of extractors". In: *Current Trends in Theoretical Computer Science: The Challenge of the New Century Vol 1: Algorithms and Complexity Vol 2: Formal Models and Semantics*. World Scientific, 2004, pp. 189–228.

[39] Amnon Ta-Shma. "Short Seed Extractors Against Quantum Storage". In: *SIAM J. Comput.* 40.3 (June 2011), pp. 664–677. ISSN: 0097-5397. DOI: 10.1137/09076787X. URL: http://dx.doi.org/10.1137/09076787X.

[40] Peter W Shor and John Preskill. "Simple proof of security of the BB84 quantum key distribution protocol". In: *Physical review letters* 85.2 (2000), p. 441.

[41] Boris Škorić and Manon de Vries. "Quantum Key Recycling with 8-state encoding (The Quantum One-Time Pad is more interesting than we thought)". In: *International Journal of Quantum Information* 15.03 (2017), p. 1750016.

[42] Douglas R. Stinson. "Universal hashing and authentication codes". In: *Designs, Codes and Cryptography* 4.3 (1994), pp. 369–380.

[43] Marco Tomamichel and Anthony Leverrier. "A largely self-contained and complete security proof for quantum key distribution". In: *Quantum* 1 (2017), p. 14.

[44] Marco Tomamichel and Renato Renner. "Uncertainty relation for smooth entropies". In: *Physical review letters* 106.11 (2011), p. 110506.

[45] Marco Tomamichel et al. "Leftover hashing against quantum side information". In: *IEEE Transactions on Information Theory* 57.8 (2011), pp. 5524–5535.

[46] Marco Tomamichel et al. "Tight finite-key analysis for quantum cryptography". In: *Nature communications* 3.1 (2012), pp. 1–6.

[47] Salil P Vadhan et al. "Pseudorandomness". In: *Foundations and Trends® in Theoretical Computer Science* 7.1–3 (2012), pp. 1–336.

[48] Jacobus Hendricus Van Lint. *Coding theory*. Vol. 201. Springer, 1971.

[49] Mark N Wegman and J Lawrence Carter. "New hash functions and their use in authentication and set equality". In: *Journal of computer and system sciences* 22.3 (1981), pp. 265–279.

[50] Stephen Wiesner. "Conjugate coding". In: *ACM Sigact News* 15.1 (1983), pp. 78–88.