Optimal attacks on qubit-based Quantum Key Recycling

Optimal attacks on qubit-based Quantum Key Recycling

Daan Leermakers and Boris Škorić
d.leermakers.1@.tue.nl, b.skoric@tue.nl

Abstract

Quantum Key Recycling (QKR) is a quantum-cryptographic primitive that allows one to re-use keys in an unconditionally secure way. By removing the need to repeatedly generate new keys it improves communication efficiency. Škorić and de Vries recently proposed a QKR scheme based on 8-state encoding (four bases). It does not require quantum computers for encryption/decryption but only single-qubit operations. We provide a missing ingredient in the security analysis of this scheme in the case of noisy channels: accurate bounds on the privacy amplification. We determine optimal attacks against the message and against the key, for 8-state encoding as well as 4-state and 6-state conjugate coding. We show that the Shannon entropy analysis for 8-state encoding reduces to the analysis of Quantum Key Distribution, whereas 4-state and 6-state suffer from additional leaks that make them less effective. We also provide results in terms of the min-entropy. Overall, 8-state encoding yields the highest capacity.

1 Introduction

1.1 Quantum Key Recycling

Quantum communication differs significantly from classical communication. On a classical channel it is trivial to read and copy all messages. On a quantum channel, on the other hand, any form of eavesdropping is detectable. This fact has been exploited by cryptographers since the 1980s, most notably by the introduction of Quantum Key Distribution (QKD). However, even before the invention of BB84 another concept was studied: information-theoretically secure re-use of encryption keys. If Bob detects no disturbance on the quantum channel, it may be safe to re-use the encryption key, in stark contrast to e.g. One Time Pad (OTP) encryption on a classical channel. This idea was proposed in the paper *"Quantum Cryptography II: How to re-use a one-time pad safely even if P = NP"* [1] by Bennett, Brassard and Breidbart in 1982. However, after the discovery of QKD the idea of Quantum Key Recycling (QKR) received very little attention for several decades. The thread was picked up again in 2003 by Gottesman [2] and in 2005 by Damgård, Pedersen and Salvail [3, 4]. Gottesman's Unclonable Encryption offers a limited re-usability of key material. Damgård et al introduced a full key re-use scheme based on mutually unbiased bases in high-dimensional Hilbert space. A drawback of their scheme is that it requires a quantum computer to perform encryption and decryption. In 2016 Fehr and Salvail [5] and Škorić and de Vries [6] returned to qubit-based schemes that do not require a quantum computer. Fehr and Salvail [5] used BB84 states and introduced a new proof technique. Their scheme is provably secure when there is very little channel noise. Škorić and de Vries [6] showed that it is advantageous to switch from 4-state conjugate coding to 8-state encoding, and that 8-state encoding is equivalent to applying the Quantum One Time Pad (QOTP) [7, 8, 9]. Their scheme is designed to work at similar noise levels as QKD. The proof technique of [5] can be directly applied to it, but needs an accurate bound on the required amount of privacy amplification, which was provided only for the noiseless case.

The long neglect of QKR is undeserved. In a QKD-equipped world, QKR has an important role to play. The process of repeatedly generating new QKD keys and then using them up with classical OTP encryption is very wasteful of bandwidth. One QKD instance followed by repeated QKR runs is more communication-efficient.

1.2 Contributions and outline

- We determine optimal attacks against individual qubits in qubit-based QKR, such that Eve introduces channel noise parametrised by the bit error rate β. We apply the standard Shor-Preskill technique [10] to reformulate state preparation as a measurement on an EPR state. We apply noise symmetrisation [11] to Alice and Bob's noisy EPR state, followed by purification to obtain a worst-case description of Eve's ancilla state. We find optimal POVM measurements by which Eve extracts from her ancilla information about the plaintext, as well as POVMs for attacking the key in the known-plaintext setting. We obtain POVMs for Shannon entropy as well as min-entropy.
- From the optimal POVMs we determine how much privacy amplification is needed: this is dictated by the most powerful attack. We find that it depends on β which attack 'wins'.
  - **Shannon entropy**. For 4-state and 6-state encoding, the winning attack at low β is Eve stealing all qubits and performing a measurement to estimate the plaintext.[1] At larger β, Eve collects ancillas from many QKR rounds and then performs a measurement on all the ancillas that are protected by the same basis key; we show that this attack is (asymptotically) as powerful as the optimal qubit-wise attack on QKD [12]. For 8-state encoding, the QKD-like attack is always the winning one.
    The QKR channel capacity of 4-state encoding is always below 6-state. 8-state has higher capacity than 6-state at $\beta \in [0, 0.1061]$, after which they are the same and equal to the QKD capacity.
  - **Min-entropy**. For 4-state and 6-state, the winning attacks are as for the Shannon entropy case. For 8-state, however, the winning attack is an ancilla attack on the key. If capacity is computed using min-entropy loss as the measure of Eve's knowledge, then the QKR capacity of 8-state is higher than 6-state on the range $\beta \in [0, 0.0612]$. There is a tiny interval $\beta \in (0.0612, 0.0638)$ where 6-state outperforms 8-state; at $\beta > 0.0638$ all capacities are zero. 4-state is always worse than 6-state.

  Overall, 8-state encoding requires the least privacy amplification.
- We notice a duality relation in the optimal POVMs for the known-plaintext attack on the key. It turns out that the POVMs which minimise Eve's Shannon entropy are in a sense 'dual' to the POVMs associated with the min-entropy: The min-entropy-POVM for plaintext x is the Shannon-entropy-POVM for plaintext $1-x$. It would be very useful if such dualities hold more generally. While there exists a simple test [13] to check if a POVM is optimal for min-entropy, there is no such test for Shannon entropy.
- As a byproduct of our analysis we find a particularly easy and insightful way to derive the QKD capacity in a scenario where Alice adds artificial preprocessing noise. By identifying conditional channels in Eve's mixed state we are able to simplify the results of [14]. The noise-adding trick can be applied in QKR in exactly the same way as in QKD.

In Section 2 we introduce notation, and briefly recap 8-state QKR. In Section 3 we go to the EPR version of the protocol, apply noise symmetrisation and obtain Eve's state by purification. Attacks on the plaintext are described in Section 4, and known-plaintext attacks on the key in Section 5. We aggregate all the results in Section 6 and we determine the QKR capacities. Insertion of artificial noise is discussed in Section 7.

2 Preliminaries

2.1 Notation and terminology

Classical Random Variables (RVs) are denoted with capital letters, and their realisations with lowercase letters. The probability that a RV X takes value x is written as $\Pr[X = x]$. The expec-

[1] This is due to the fact that conjugate coding is not a particularly good encryption.

tation with respect to RV X is denoted as $\mathbb{E}_x f(x) = \sum_{x\in\mathcal{X}} \Pr[X=x]f(x)$. The Shannon entropy of an RV X is written as $\mathsf{H}(X)$. Sets are denoted in calligraphic font. The notation 'log' stands for the logarithm with base 2. The min-entropy of $X \in \mathcal{X}$ is $\mathsf{H}_{\min}(X) = -\log\max_{x\in\mathcal{X}} \Pr[X=x]$, and the conditional min-entropy is $\mathsf{H}_{\min}(X|Y) = -\log \mathbb{E}_y \max_{x\in\mathcal{X}} \Pr[X=x|Y=y]$. The notation h stands for the binary entropy function $h(p) = p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}$. Sometimes we will write $h(\{p_1,\ldots,p_n\})$ meaning $\sum_i p_i \log\frac{1}{p_i}$. Bitwise XOR of binary strings is written as '$\oplus$'. The inverse of a bit $b \in \{0,1\}$ is written as $\bar{b} = 1-b$.

For quantum states we use Dirac notation, with the standard qubit basis states $|0\rangle$ and $|1\rangle$ represented as $\binom{1}{0}$ and $\binom{0}{1}$ respectively. The Pauli matrices are denoted as $\sigma_x, \sigma_y, \sigma_z$, and we write $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. The standard basis is the eigenbasis of σ_z, with $|0\rangle$ in the positive z-direction. We write $\mathbb{1}$ for the identity matrix. The notation 'tr' stands for trace. The Hermitian conjugate of an operator A is written as $A^\dagger$. When A is a complicated expression, we sometimes write $(A+\text{h.c.})$ instead of $A + A^\dagger$. The complex conjugate of z is denoted as z^*.

We use the Positive Operator Valued Measure (POVM) formalism. A POVM $\mathcal{M}$ consists of positive semidefinite operators, $\mathcal{M} = (M_x)_{x\in\mathcal{X}}$, $M_x \geq 0$, and satisfies the condition $\sum_x M_x = \mathbb{1}$. The notation $\mathcal{M}(\rho)$ stands for the classical RV resulting when $\mathcal{M}$ is applied to mixed state ρ. Consider a bipartite system 'AB' where the 'A' part is classical, i.e. the state is of the form $\rho^{\text{AB}} = \mathbb{E}_{x\in\mathcal{X}} |x\rangle\langle x| \otimes \rho_x$ with the $|x\rangle$ forming an orthonormal basis. The min-entropy of the classical RV X given part 'B' of the system is [15]

$$\mathsf{H}_{\min}(X|\rho_X) = -\log\max_{\mathcal{M}} \mathbb{E}_{x\in\mathcal{X}} \text{tr}\,[M_x\rho_x]. \tag{1}$$

Here $\mathcal{M}$ denotes a POVM. Let $\Lambda \stackrel{\text{def}}{=} \sum_x \rho_x M_x$. If a POVM can be found that satisfies the condition[2] [13]

$$\forall_{x\in\mathcal{X}} :\ \Lambda - \rho_x \geq 0, \tag{2}$$

then there can be no better POVM (but equally good ones may exist).

For states that also depend on a classical RV $Y \in \mathcal{Y}$, the min-entropy of X given the quantum state and Y is

$$\mathsf{H}_{\min}(X|Y, \rho_X(Y)) = -\log \mathbb{E}_{y\in\mathcal{Y}} \max_{\mathcal{M}} \mathbb{E}_{x\in\mathcal{X}} \text{tr}\,[M_x\rho_x(y)]. \tag{3}$$

A simple expression can be obtained when X is a binary variable. Let $X \in \{0,1\}$. Then

$$X \sim (p_0, p_1): \qquad \mathsf{H}_{\min}(X|Y, \rho_X(Y)) = 1 - \log\left(1 + \mathbb{E}_y \text{tr}\left| p_0\rho_0(y) - p_1\rho_1(y)\right|\right). \tag{4}$$

For the Shannon entropy of a classical RV given a quantum system we have

$$\mathsf{H}(X|\rho_X) \stackrel{\text{def}}{=} \min_{\mathcal{M}} \mathsf{H}(X|\mathcal{M}(\rho_X)). \tag{5}$$

If the ensemble $(\rho_x)_{x\in\mathcal{X}}$ has a symmetry, i.e. $\forall_{x\in\mathcal{X}, g\in G} :\ U_g\rho_x U_g^\dagger = \rho_{g(x)}$ for some group G acting on $\mathcal{X}$, and unitary representation U of G, then it suffices [13] to consider only POVMs that obey the same symmetry, $U_g M_x U_g^\dagger = M_{g(x)}$.

2.2 Eight-state Quantum Key Recycling

We briefly review the main properties of the 8-state QKR scheme ("scheme #2" in [6]). A classical bit $g \in \{0,1\}$ is encoded into a qubit state using one of four possible bases. The basis is labeled $b \in \{0,1,2,3\}$, and for convenience the notation $b = 2u + w$ is introduced, with $u, w \in \{0,1\}$. The labels b and (u,w) are used interchangeably. The encoding of g in basis (u,w) is expressed on the Bloch sphere as a unit vector

$$\boldsymbol{n}_{uwg} = \frac{(-1)^g}{\sqrt{3}} \begin{pmatrix} (-1)^u \\ (-1)^{u+w} \\ (-1)^w \end{pmatrix}, \tag{6}$$

[2] Ref. [13] specifies a second condition, namely $\Lambda^\dagger = \Lambda$. However, the hermiticity of Λ already follows from the condition (2).

i.e. the eight corner points of a cube. The corresponding states in Hilbert space are

$$|\psi_{uwg}\rangle = (-1)^{gu}\left[(-\sqrt{i})^g \cos\tfrac{\alpha}{2}|g\oplus w\rangle + (-1)^u(\sqrt{i})^{1-g}\sin\tfrac{\alpha}{2}|\overline{g\oplus w}\rangle\right] \tag{7}$$

in the z-basis. The angle α is defined as $\cos\alpha = 1/\sqrt{3}$. The four states $|\psi_{uwg}\rangle$, for fixed g, are the Quantum One-Time Pad (QOTP) encryptions of $|\psi_{00g}\rangle$.

The bit error rate (BER) on the quantum channel is denoted as $\beta \in [0, \frac{1}{2}]$. The key recycling scheme makes use of a Secure Sketch $S : \{0,1\}^n \to \{0,1\}^a$, with $a > nh(\beta)$. (Asymptotically a approaches $nh(\beta)$). Furthermore the scheme uses an extractor $\texttt{Ext} : \{0,1\}^n \to \{0,1\}^\ell$ and a message-independent, key-private [5] MAC function that produces a tag of length λ. The message is $\mu \in \{0,1\}^\ell$. The key material shared between Alice and Bob consists of three parts: a basis sequence $b \in \{0,1,2,3\}^n$, a MAC key K_M and a classical OTP $K_\text{SS} \in \{0,1\}^a$ for protecting the secure sketch.

Encryption

Alice performs the following steps. Generate random $g \in \{0,1\}^n$. Compute $s = K_\text{SS} \oplus S(g)$ and $z = \texttt{Ext}\, g$. Compute the ciphertext $c = \mu \oplus z$ and authentication tag $T = M(K_\text{M}, g||c||s)$. Prepare the quantum state $|\Psi\rangle = \bigotimes_{i=1}^n |\psi_{b_i g_i}\rangle$. Send $|\Psi\rangle$, s, c, T.

Decryption

(Bob gets $|\Psi'\rangle$, s', c', T'). Bob performs the following steps. Measure $|\Psi'\rangle$ in the b-basis. This yields $g' \in \{0,1\}^n$. Recover $\hat{g}$ from g' and $K_\text{SS} \oplus s'$ (by the syndrome decoding procedure of the Secure Sketch primitive). Compute $\hat{z} = \texttt{Ext}\,\hat{g}$ and $\hat{\mu} = c' \oplus \hat{z}$. Accept the message $\hat{\mu}$ if the syndrome decoding succeeded and $T' = M(K_\text{M}, \hat{g}||c'||s')$. Communicate Accept/Reject to Alice.

Key update

Alice and Bob perform the following actions. If Bob Accepts, replace K_SS. If Bob Rejects, replace K_SS and compute the updated key b' as a function of b and n fresh secret bits.

In case of Bob accepting the transmission, an ℓ-bit message has been communicated while only $a \approx nh(\beta)$ bits of key material have been spent.[3] The aim of the current paper is to find out how large ℓ is allowed to be as a function of the noise parameter β.

3 EPR formulation, noise symmetrisation, and purification

Apart from QKR employing the 8-state (QOTP) encoding as described above, we also investigate 4-state (BB84) and 6-state conjugate coding. For the security analysis of qubit-based QKR we piggyback on (i) proof techniques [16] that use e.g. quantum de Finetti [17] to reduce the analysis to individual-qubit attacks; (ii) the proof technique for qubit-based QKR introduced in [5], which can directly be applied to the scheme of [6] provided that correct values are known for the required amount of privacy amplification as a function of the noise parameter β.

We study optimal attacks against individual qubits, making use of the standard Shor-Preskill technique [10] and the noise symmetrisation technique introduced by [11].

3.1 EPR version of the QKR protocol

We follow the standard Shor-Preskill technique [10] and re-formulate the QKR protocol (Section 2.2) using EPR pairs. The step where Alice prepares the state $|\Psi\rangle$ and sends it to Bob is replaced by the following procedure.

Alice prepares a two-qubit singlet state. She keeps one qubit ('A') and sends the other qubit ('B') to Bob. Eve is allowed to manipulate the whole 'AB' system[4] in any way, including coupling to ancillas. Then Alice and Bob perform their projective measurements in the correct basis (basis b_i for the i'th bit). Let the outcome of Alice's measurement be $x \in \{0,1\}$, and Bob's outcome $y \in \{0,1\}$. Alice sends $e = x \oplus g$ to Bob. Bob computes $\hat{g} = \bar{y} \oplus e$, which is guaranteed to equal g

[3] "Scheme #3" in [6] greatly reduces the key material expenditure.

[4] Note that this attacker model gives Eve more power than she can actually have in real life. Realistically, she would be able to manipulate only the 'B' subsystem.

if Eve has done nothing ($\beta = 0$).[5] Security of this EPR-version of the protocol implies security of the original protocol.

Note that the above description is agnostic of the number of bases used in the encoding. We will use the notation $\mathcal{B}$ to denote the set of bases in an encoding scheme. For 4-state encoding we write $\mathcal{B} = \{0, 1\}$, and the states are the spin states $|\pm z\rangle$ (at $b = 0$) and $|\pm x\rangle$ (at $b = 1$). For 6-state we write $\mathcal{B} = \{1, 2, 3\}$, with spin states $|\pm x\rangle$ (at $b = 1$), $|\pm y\rangle$ (at $b = 2$) and $|\pm z\rangle$ (at $b = 3$). For 8-state we have $\mathcal{B} = \{00, 01, 10, 11\}$, and the states are defined in (7). The number of bases is $|\mathcal{B}|$.

3.2 Noise symmetrisation

After Eve's interference, the bipartite system held by Alice and Bob is no longer a pure singlet state but a general mixed state ρ^{AB}. As the singlet state is invariant under unitary transformations of the form $\rho^{\mathrm{AB}} \mapsto U \otimes U \rho^{\mathrm{AB}} U^\dagger \otimes U^\dagger$ (where U acts on a single qubit), Alice and Bob are 'allowed' to perform the following sequence of actions.

Preparation phase, before the protocol

Alice and Bob agree on a single basis $b^* \in \mathcal{B}$.

During the protocol

For each bit, just before they execute their measurement

- Alice and Bob publicly draw a random number $\gamma \in \{0, 1, 2, 3\}$.
- They both apply to their own qubit the Pauli operator σ_γ, defined with respect to the b^* basis. Here σ_0 is the identity matrix.
- They forget γ.

These actions have no effect on the original state (the desired singlet) but they dramatically simplify the noise in ρ^{AB}.

Lemma 3.1 *Consider 6-state or 8-state encoding. Let* $|\Psi^\pm\rangle = \frac{|01\rangle_* \pm |10\rangle_*}{\sqrt{2}}$ *and* $|\Phi^\pm\rangle = \frac{|00\rangle_* \pm |11\rangle_*}{\sqrt{2}}$ *denote the Bell basis states with respect to the* b^* *basis. Let Eve introduce a bit error rate of* exactly β *between Alice and Bob's measurement results. Then the mixed state of the 'AB' system after the above described symmetrisation procedure is given by*

$$\tilde{\rho}^{\mathrm{AB}} = (1 - \frac{3}{2}\beta)|\Psi^-\rangle\langle\Psi^-| + \frac{\beta}{2}\left(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Phi^+\rangle\langle\Phi^+|\right). \tag{8}$$

Proof: In [18] it was shown that the AB state reduces to the form $\tilde{\rho} = \lambda_0|\Psi^-\rangle\langle\Psi^-| + \lambda_1|\Phi^-\rangle\langle\Phi^-| + \lambda_2|\Psi^+\rangle\langle\Psi^+| + \lambda_3|\Phi^+\rangle\langle\Phi^+|$, with $\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = 1$. We impose the constraint $(|\psi_{bg}\rangle \otimes |\psi_{bg}\rangle)^\dagger \tilde{\rho} |\psi_{bg}\rangle \otimes |\psi_{bg}\rangle = \beta/2$ for all $b \in \mathcal{B}$, $g \in \{0, 1\}$.[6] For the 6-state case it was shown in [11] that these constraints yield (8). We next study the 8-state case. Taking $b = b^*$, the above constraints yield $\frac{1}{2}\lambda_2 + \frac{1}{2}\lambda_3 = \frac{\beta}{2}$. The case $b \neq b^*$ is more complicated. Without loss of generality we take $b^* = 00$. Then the $b = 01$ and $b = 11$ constraints each give, after some algebra, $\frac{1}{18}(7\lambda_1 + 8\lambda_2 + 3\lambda_3) = \frac{\beta}{2}$. The $b = 10$ constraint gives $\frac{1}{18}(\lambda_1 + 8\lambda_2 + 9\lambda_3) = \frac{\beta}{2}$. Solving for the λ-parameters finally yields $\lambda_1 = \lambda_2 = \lambda_3 = \frac{\beta}{2}$. □

Note that setting $b^* \in \mathcal{B}$ is important: if the Pauli operators $\sigma_\gamma \otimes \sigma_\gamma$ are chosen with respect to a different basis, then Lemma 3.1 does not necessarily hold.

Also note that Lemma 3.1 usually does not hold for 4-state (BB84) conjugate coding. 4-state encoding has fewer noise-related constraints, and hence Eve has more freedom. However, one can imagine a protocol variant where Alice and Bob spend some extra key material[7] in order to agree on qubit positions which they sacrifice for noise testing purposes. With Lemma 3.1 holding for

[5] In the singlet state the x and y are anti-correlated, i.e. $y = \bar{x}$.

[6] From the above constraints and $\operatorname{tr}\tilde{\rho} = 1$ it follows that $(|\psi_{bg}\rangle \otimes |\psi_{b\bar{g}}\rangle)^\dagger \tilde{\rho} |\psi_{bg}\rangle \otimes |\psi_{b\bar{g}}\rangle = \frac{1-\beta}{2}$.

[7] This key has to be refreshed every time, otherwise Eve may find out which positions are test positions.

4-state too, we can now treat all three encoding methods on an equal footing. We will see in Section 6 that even with this advantage given to Alice and Bob for 4-state, the 4-state encoding still performs worst.

3.3 Purification

The $\tilde{\rho}^{\rm AB}$ can be purified as follows, under the worst-case assumption that all noise is caused by Eve. Denoting Eve's four-dimensional subsystem as 'E', with orthonormal basis $|m_i\rangle$, we can write

$$|\Psi^{\rm ABE}\rangle = \sqrt{1-\tfrac{3}{2}\beta}|\Psi^-\rangle \otimes |m_0\rangle + \sqrt{\tfrac{\beta}{2}}\Big(-|\Phi^-\rangle \otimes |m_1\rangle + i|\Psi^+\rangle \otimes |m_2\rangle + |\Phi^+\rangle \otimes |m_3\rangle\Big). \qquad (9)$$

Alice and Bob know in which basis to measure. They both do a projective measurement on their own subsystem. They measure the spin component in the direction $\boldsymbol{v} = (v_x, v_y, v_z) = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$. The eigenstates of this measurement are $|\boldsymbol{v}\rangle = e^{-i\varphi/2}\cos\frac{\theta}{2}|0\rangle + e^{i\varphi/2}\sin\frac{\theta}{2}|1\rangle$ (with eigenvalue '0') and $|\overline{\boldsymbol{v}}\rangle = -e^{-i\varphi/2}\sin\frac{\theta}{2}|0\rangle + e^{i\varphi/2}\cos\frac{\theta}{2}|1\rangle$ (with eigenvalue '1'). We rewrite the state (9) using $|\boldsymbol{v}\rangle, |\overline{\boldsymbol{v}}\rangle$ as the basis of the A and B subsystem,

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

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

- With probability $1-\beta$, Alice and Bob's measurement outcomes are opposite. With probability β they are equal.
- $|E^{\boldsymbol{v}}_{10}\rangle = |E^{-\boldsymbol{v}}_{01}\rangle$ and $|E^{\boldsymbol{v}}_{11}\rangle = |E^{-\boldsymbol{v}}_{00}\rangle$. Furthermore $\langle E^{\boldsymbol{v}}_{00}|E^{\boldsymbol{v}}_{11}\rangle = 0$, and $|E^{\boldsymbol{v}}_{00}\rangle$, $|E^{\boldsymbol{v}}_{11}\rangle$ span a subspace orthogonal to $|E^{\boldsymbol{v}}_{01}\rangle$, $|E^{\boldsymbol{v}}_{10}\rangle$. Furthermore, $\langle E^{\boldsymbol{v}}_{01}|E^{\boldsymbol{v}}_{10}\rangle = \frac{1-2\beta}{1-\beta}$. This structure makes it particularly easy to analyse QKD. See Section 4.4.1.
- $|\frac{-v_xv_z - iv_y}{\sqrt{1-v_z^2}}|^2 = 1 - v_x^2$ and $|\frac{-v_yv_z + iv_x}{\sqrt{1-v_z^2}}|^2 = 1 - v_y^2$.

In the analysis of QKD schemes, it suffices to express (10) only for a single choice of $\boldsymbol{v}$, because the basis is eventually revealed to Eve. In QKR the basis is not revealed. In our treatment of known plaintext attacks (Section 5) we will need to evaluate (10) for different bases.

3.4 Eve's mixed state

After Alice and Bob have performed their measurement, Eve possesses one of the $4|\mathcal{B}|$ pure states $\rho^{\boldsymbol{v}(b)}_{xy}$, with $x, y \in \{0,1\}$, $b \in \mathcal{B}$

$$\rho^{\boldsymbol{v}}_{xy} \stackrel{\rm def}{=} |E^{\boldsymbol{v}}_{xy}\rangle\langle E^{\boldsymbol{v}}_{xy}|, \qquad (11)$$

coupled to the unknown (to her) classical random variables B, X, Y. The whole system of B, X, Y and E can be represented as a four-part system in the following mixed state,

$$\Omega^{BXYE} = \frac{1}{|\mathcal{B}|}\sum_{b\in\mathcal{B}} \mathbb{E}_{x\in\{0,1\}}\mathbb{E}_{y|x}|b\rangle\langle b| \otimes |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho^{\boldsymbol{v}(b)}_{xy}. \qquad (12)$$

At given x, the probability of $y \neq x$ is $1-\beta$. (Before the introduction of noise, the x and y were perfectly anti-correlated.)
In Section 5 we will study known plaintext attacks, i.e. Eve knows g and wants to learn the basis b. If Eve knows that $x=0$, then she has to distinguish between the following $|\mathcal{B}|$ states,

$$\zeta_b \overset{\text{def}}{=} (1-\beta)\rho_{01}^{\boldsymbol{v}(b)} + \beta\rho_{00}^{\boldsymbol{v}(b)}, \qquad b \in \mathcal{B}. \tag{13}$$

The case $x=1$ will not be treated separately as it is analogous to $x=0$.

4 Security of the message

4.1 Attacks targeting the message

We consider attacks by which Eve tries to gain information about Alice's plaintext x.

M1 Eve steals one whole transmission $|\Psi\rangle$ and performs a measurement. (No matter what Eve sends to Bob, Bob rejects with overwhelming probability.)

M2 Eve couples each qubit individually to an ancilla, and transfers information into the ancilla in such a way that the bit error rate is exactly β. She does this for N transmissions ($N \gg 1$) before finally performing a measurement on her ancillas.

Attack M1 is the worst case scenario given that Bob does not accept. M2 is the worst case given that Bob accepts N times in a row.
Attack M1 has no effect against 8-state encoding (since it is a QOTP), but is important in the case of 4-state and 6-state encoding. Below we briefly recap the results of [6]. In Section 4.4 we will see that the analysis of M2 reduces to the analysis of QKD.

4.2 Attack M1 on 4-state encoding

Eve intercepts the whole n-qubit state $|\Psi\rangle$ and immediately does a measurement. She subjects each qubit i individually to the spin measurement $(\sigma_x+\sigma_z)/\sqrt{2}$. The probability distribution of X_i given the outcome always consists of the numbers $(\cos\frac{\pi}{8})^2$ and $(\sin\frac{\pi}{8})^2$. In terms of Shannon entropy this corresponds to the following mutual information per qubit,

$$I_{\text{AE}}^{\text{M1,4state}} = 1 - h([\sin\tfrac{\pi}{8}]^2) \approx 0.399. \tag{14}$$

The min-entropy loss per qubit is

$$\triangle \mathsf{H}_{\text{min}}^{\text{M1,4state}} = 1 - \log\frac{1}{(\cos\frac{\pi}{8})^2} \approx 0.772. \tag{15}$$

4.3 Attack M1 on 6-state encoding

Eve's spin measurement is $(\sigma_x+\sigma_y+\sigma_z)/\sqrt{3}$. The probability distribution for X_i given the outcome always consists of the numbers $(\cos\frac{\alpha}{2})^2$ and $(\sin\frac{\alpha}{2})^2$. This yields

$$I_{\text{AE}}^{\text{M1,6state}} = 1 - h([\sin\tfrac{\alpha}{2}]^2) \approx 0.256 \tag{16}$$

$$\triangle \mathsf{H}_{\text{min}}^{\text{M1,6state}} = 1 - \log\frac{1}{(\cos\frac{\alpha}{2})^2} \approx 0.658. \tag{17}$$

4.4 Attack M2: All Your Basis Are Belong To Us.

Attack M2 is effective because Eve is attacking N qubits that are encrypted *with the same key b*. Eve collects N ancillas containing partial information about the message bits; these message bits are protected by a total of $\log|\mathcal{B}|$ key bits. Hence, for large N the key b offers essentially no protection of the information drawn into the ancillas. (On the other hand, the key prevents Eve from absorbing full information into her ancillas. And the key itself does not become known to Eve.)

Lemma 4.1 *Let Alice and Bob take fresh keys and then run the EPR version of the QKR protocol N times, with Bob Accepting each time. Let $X_i^{(j)}$, with $j \in \{1,\dots,N\}$, be Alice's measurement result in qubit position $i \in \{1,\dots,n\}$ in the j'th run of the protocol and B_i the basis key used to encode all the $X_i^{(j)}$. Let $E_i^{(j)}$ denote Eve's corresponding ancilla system, created without knowledge of B_i. Then*

$$\frac{1}{N}\mathsf{H}(X_i^{(1)},\dots,X_i^{(N)}|\, E_i^{(1)},\dots,E_i^{(N)}) \geq \mathsf{H}(X_i^{(j)}|B_i E_i^{(j)}) \qquad j \text{ arbitrary.} \tag{18}$$

Proof: Let $\mathcal{M}$ denote a POVM. We have $\mathsf{H}(\boldsymbol{X}_i|\boldsymbol{E}_i) = \min_{\mathcal{M}} \mathsf{H}(\boldsymbol{X}_i|\mathcal{M}(\boldsymbol{E}_i)) \geq \min_{\mathcal{M}} \mathsf{H}(\boldsymbol{X}_i|B_i\mathcal{M}(\boldsymbol{E}_i))$ $= N\min_{\mathcal{M}} \mathsf{H}(X_i^{(j)}|B_i\mathcal{M}(E_i^{(j)})) = N\mathsf{H}(X_i^{(j)}|B_iE_i^{(j)})$ for arbitrary j. □

For $N \gg 1$ the bound is tight. The left hand side of (18) is the leakage per qubit. The right hand side is precisely the quantity that determines the security of QKD: the uncertainty about X given a noise-constrained ancilla and the basis B revealed to Eve *after she has created the ancilla states.* Lemma 4.1 allows us to obtain a tight lower bound on the QKR capacity, namely the QKD capacity, whenever M2 is the dominant attack.

4.4.1 QKD, Shannon entropy

The computation of $\mathsf{H}(X|BE)$ for BB84 and 6-state (or more) QKD is well known. Here we combine the two standard approaches: (i) the simplest possible description of the noise, i.e. noise symmetrisation, (ii) specifying optimal measurements instead of bounds based on von Neumann entropy. The results are of course not new, but we present the matter in a particularly clean way which helps when protocol embellishments are considered (e.g. addition of artificial noise, see Section 7).

Informal treatment

Eve knows $\boldsymbol{v}$. Eve does a projective measurement $|E^{\boldsymbol{v}}_{00}\rangle\langle E^{\boldsymbol{v}}_{00}| + |E^{\boldsymbol{v}}_{11}\rangle\langle E^{\boldsymbol{v}}_{11}|$. This measurement does not destroy any information. With probability β the outcome is '1'; next Eve can perfectly distinguish between the orthogonal states $|E^{\boldsymbol{v}}_{00}\rangle$, $|E^{\boldsymbol{v}}_{11}\rangle$ and hence learns X with 100% accuracy. With probability $1-\beta$ the outcome is '0'; now Eve has to handle the trickier task of distinguishing between the non-orthogonal $|E^{\boldsymbol{v}}_{01}\rangle$ and $|E^{\boldsymbol{v}}_{10}\rangle$, which have inner product $c \stackrel{\text{def}}{=} \langle E^{\boldsymbol{v}}_{01}|E^{\boldsymbol{v}}_{10}\rangle = \frac{1-2\beta}{1-\beta}$. This is done optimally using a projective measurement in the following orthonormal basis,

$$\begin{aligned} |\mu_{01}\rangle &= \gamma_+|E^{\boldsymbol{v}}_{01}\rangle + \gamma_-|E^{\boldsymbol{v}}_{10}\rangle \\ |\mu_{10}\rangle &= \gamma_+|E^{\boldsymbol{v}}_{10}\rangle + \gamma_-|E^{\boldsymbol{v}}_{01}\rangle \\ \gamma_\pm &= \frac{1}{2\sqrt{1+c}} \pm \frac{1}{2\sqrt{1-c}} \end{aligned} \tag{19}$$

and has error probability

$$p_\beta = |\langle E^{\boldsymbol{v}}_{01}|\mu_{10}\rangle|^2 = |\langle E^{\boldsymbol{v}}_{10}|\mu_{01}\rangle|^2 = \tfrac{1}{2} - \tfrac{1}{2}\sqrt{1-c^2} = \tfrac{1}{2} - (1-\beta)^{-1}\sqrt{\tfrac{\beta}{2}(1-\tfrac{3}{2}\beta)}. \tag{20}$$

The channel capacity from Alice to Eve is

$$I_{\text{AE}}(\beta) = \beta\cdot[1-h(0)] + (1-\beta)[1-h(p_\beta)]. \tag{21}$$

The secrecy capacity is

$$C(\beta) = I_{\text{AB}}(\beta) - I_{\text{AE}}(\beta) = 1 - h(\beta) - I_{\text{AE}}(\beta). \tag{22}$$

Formal treatment

Eve has to guess X from a state $\rho^{\boldsymbol{v}}_{XY} = |E^{\boldsymbol{v}}_{XY}\rangle\langle E^{\boldsymbol{v}}_{XY}|$. We write $Y = \bar{X}\oplus R$, with $R \in \{0,1\}$ the noise. Eve does not know R. Let $\mathcal{Q} = (Q_x)_{x\in\{0,1\}}$ be a POVM applied by Eve, and let $\mathcal{Q}(\rho^{\boldsymbol{v}}_{XY}) \in \{0,1\}$ be the outcome of the measurement. The main quantity to compute is

$$\begin{aligned} \mathsf{H}(X|\rho^{\boldsymbol{v}}_{X,\bar{X}\oplus R}) &= \min_{\mathcal{Q}} \mathsf{H}(X|\mathcal{Q}(\rho^{\boldsymbol{v}}_{X,\bar{X}\oplus R})) = \min_{\mathcal{Q}} \mathbb{E}_r \mathsf{H}(X|\mathcal{Q}(\rho^{\boldsymbol{v}}_{X,\bar{X}\oplus r})) \\ &= \min_{\mathcal{Q}} \Big[(1-\beta)\mathsf{H}(X|\mathcal{Q}(\rho^{\boldsymbol{v}}_{X\overline{X}})) + \beta\mathsf{H}(X|\mathcal{Q}(\rho^{\boldsymbol{v}}_{XX}))\Big]. \end{aligned} \tag{23}$$

The optimal POVM is given by $Q_0 = |E^{\boldsymbol{v}}_{00}\rangle\langle E^{\boldsymbol{v}}_{00}| + |\mu_{01}\rangle\langle\mu_{01}|$, $Q_1 = |E^{\boldsymbol{v}}_{11}\rangle\langle E^{\boldsymbol{v}}_{11}| + |\mu_{10}\rangle\langle\mu_{10}|$. This is equivalent to the two-step procedure detailed in the informal treatment above, and yields

$$\mathsf{H}(X|\rho^{\boldsymbol{v}}_{XY}) = (1-\beta)h(p_\beta) + \beta\cdot 0. \tag{24}$$

Eve's knowledge about X is $I_{\rm AE} = \mathsf{H}(X) - \mathsf{H}(X|\rho^{\boldsymbol{v}}_{XY})$, which precisely equals (21).

4.4.2 QKD, min-entropy

Expressed as min-entropy loss, Eve's knowledge is $\mathsf{H}_{\min}(X) - \mathsf{H}_{\min}(X|\rho^{\boldsymbol{v}}_{X,\bar{X}\oplus R})$ for known $\boldsymbol{v}$ and unknown noise $R\in\{0,1\}$. We have

$$\begin{aligned}
\mathsf{H}_{\min}(X|\rho^{\boldsymbol{v}}_{X,\overline{X}\oplus R}) &= -\log p_{\rm guess}(X|\mathcal{Q}(\mathbb{E}_r\rho^{\boldsymbol{v}}_{X,\overline{X}\oplus r}))\\
&= -\log \mathbb{E}_r p_{\rm guess}(X|\mathcal{Q}(\rho^{\boldsymbol{v}}_{X,\overline{X}\oplus r}))\\
&= -\log\left[\beta p_{\rm guess}(X|\mathcal{Q}(\rho^{\boldsymbol{v}}_{XX})) + (1-\beta)p_{\rm guess}(X|\mathcal{Q}(\rho^{\boldsymbol{v}}_{X\overline{X}}))\right]\\
&= -\log\left[\beta\cdot 1 + (1-\beta)(1-p_\beta)\right]\\
&= \mathsf{H}_{\min}(X) - \log[1+\sqrt{2}\sqrt{\beta(1-\tfrac{3}{2}\beta)}+\beta].
\end{aligned}\tag{25}$$

5 Security of the key

5.1 Known plaintext attacks on the key

We have to take into account the possibility that Eve knows the plaintext μ. Then Ψ may give Eve information on the (basis) key b. We focus on attacks that lead Bob to Accept. (A Reject causes Alice and Bob to refresh their keys.) We look at the two types of attack available to Eve,

K1 Eve intercepts a fraction 3β of the qubits, does a measurement on them, and sends the resulting states on to Bob.

K2 Eve lets every qubit individually interact with an ancilla. She forwards the qubits to Bob.

In attack K1 Eve receives a state

$$\omega_{Bx} = |\psi_{Bx}\rangle\langle\psi_{Bx}| \tag{26}$$

for known x and unknown B. For attack K2 Eve's view is the mixed state ζ_B as defined in (13), for unknown B.

Lemma 5.1 *The Shannon entropy of B given ζ_B can be written as*

$$\mathsf{H}(B|\zeta_B) = \log|\mathcal{B}| - \max_{\mathcal{M}}\left[h(\{{\rm tr}\, M_m\frac{\sum_b\zeta_b}{|\mathcal{B}|}\}_{m\in\mathcal{B}}) - \frac{1}{|\mathcal{B}|}\sum_{b\in\mathcal{B}}h(\{{\rm tr}\, M_m\zeta_b\}_{m\in\mathcal{B}})\right] \tag{27}$$

where $\max_{\mathcal{M}}$ *is maximisation over POVMs $(M_m)_{m\in\mathcal{B}}$. If we impose the symmetry relations $\forall_{b\in\mathcal{B}}$: ${\rm tr}\, M_b\zeta_b = p_{\rm OK}$ and $\forall_{m,b\in\mathcal{B},m\neq b}$: ${\rm tr}\, M_m\zeta_b = \frac{1-p_{\rm OK}}{|\mathcal{B}|-1}$ then the expression for the entropy reduces to*

$$\mathsf{H}(B|\zeta_B) = \min_{\text{symmetric}\,\mathcal{M}}\left[h(p_{\rm OK}) + (1-p_{\rm OK})\log(|\mathcal{B}|-1)\right]. \tag{28}$$

<u>Proof</u>: Let $\mathcal{M}(\zeta_B)$ be the classical random variable describing the outcome of the POVM measurement $\mathcal{M}$ on state ζ_B. We have $\mathsf{H}(B|\zeta_B) = \min_{\mathcal{M}}\mathsf{H}(B|\mathcal{M}(\zeta_B))$, with $\mathsf{H}(B|\mathcal{M}(\zeta_B)) = \sum_m \Pr[\mathcal{M}(\zeta_B) = m]\mathsf{H}(B|\mathcal{M}(\zeta_B) = m)$. We write $\Pr[B=b|\mathcal{M}(\zeta_B)=m] = \frac{1}{|\mathcal{B}|}[{\rm tr}\, M_m\zeta_b]/\Pr[\mathcal{M}(\zeta_B)=m]$ and $\Pr[\mathcal{M}(\zeta_B)=m] = \frac{1}{|\mathcal{B}|}\sum_b {\rm tr}\, M_m\zeta_b$. After some manipulation (27) follows. In the first $h(\cdots)$ of (27) we then write $\frac{1}{|\mathcal{B}|}\sum_b{\rm tr}\,\zeta_b M_m = \frac{1}{|\mathcal{B}|}[p_{\rm OK} + (|\mathcal{B}|-1)\frac{1-p_{\rm OK}}{|\mathcal{B}|-1}] = \frac{1}{|\mathcal{B}|}$. The $h(\frac{1}{|\mathcal{B}|})$ cancels the $\log|\mathcal{B}|$. The second $h(\cdots)$ in (27) is the same for all $b\in\mathcal{B}$, namely $h(\{p_{\rm OK}, \frac{1-p_{\rm OK}}{|\mathcal{B}|-1},\ldots,\frac{1-p_{\rm OK}}{|\mathcal{B}|-1}\})$ $= -p_{\rm OK}\log p_{\rm OK} - (|\mathcal{B}|-1)\cdot\frac{1-p_{\rm OK}}{|\mathcal{B}|-1}\log\frac{1-p_{\rm OK}}{|\mathcal{B}|-1} = h(p_{\rm OK}) + (1-p_{\rm OK})\log(|\mathcal{B}|-1)$. □

5.2 Attack K1, 4-state

Eve scrutinises ω_{Bx}. If $x=0$ then the state is either the $+x$ or $+z$ spin state. If $x=1$ then the state is either $-x$ or $-z$. In both cases, the optimal way to distinguish between the states is to measure the spin $(\sigma_x-\sigma_z)/\sqrt{2}$. Given the measurement outcome, the probabilities for the two key values are $(\cos\frac{\pi}{8})^2$ and $(\sin\frac{\pi}{8})^2$. This holds for $x=0$ as well as $x=1$. Eve's knowledge about B is

$$\begin{aligned} \mathsf{H}(B)-\mathsf{H}(B|X,\omega_{BX}) &= 1-h([\sin\tfrac{\pi}{8}]^2)\approx 0.399 && (29)\\ \mathsf{H}_{\min}(B)-\mathsf{H}_{\min}(B|X,\omega_{BX}) &= 1-\log\frac{1}{(\cos\frac{\pi}{8})^2}\approx 0.772. && (30)\end{aligned}$$

The effect on the whole n-bit string is obtained by multiplying (29,30) times $3\beta n$.

5.3 Attack K1, 6-state

Consider $x=0$. (The analysis for $x=1$ is analogous). Eve has to distinguish between the spin states $+x$, $+y$, $+z$ using a POVM $\mathcal{M}=(M_b)_{b\in\{1,2,3\}}$. For the min-entropy the best POVM is given by $M_b=\frac{1}{3}\mathbb{1}-\frac{1}{3}\boldsymbol{n}_b\cdot\boldsymbol{\sigma}$, with $\boldsymbol{n}_1=(-2,1,1)^{\mathrm{T}}/\sqrt{6}$, $\boldsymbol{n}_2=(1,-2,1)^{\mathrm{T}}/\sqrt{6}$, $\boldsymbol{n}_3=(1,1,-2)^{\mathrm{T}}/\sqrt{6}$. It yields the following probability distribution for B: $\{\frac{1}{3}+\frac{2}{3\sqrt{6}},\ \frac{1}{3}-\frac{1}{3\sqrt{6}},\ \frac{1}{3}-\frac{1}{3\sqrt{6}}\}$.

$$\mathsf{H}_{\min}(B)-\mathsf{H}_{\min}(B|X,\omega_{BX})=\log 3+\log(\tfrac{1}{3}+\tfrac{2}{3\sqrt{6}})\approx 0.861. \qquad (31)$$

For the Shannon entropy the best POVM is of the same form as above but with $\boldsymbol{n}_b\to-\boldsymbol{n}_b$. The probability distribution for B is $\{\frac{1}{3}+\frac{1}{3\sqrt{6}},\ \frac{1}{3}+\frac{1}{3\sqrt{6}},\ \frac{1}{3}-\frac{2}{3\sqrt{6}}\}$.

$$\mathsf{H}(B)-\mathsf{H}(B|X,\omega_{BX})=\log 3-h(\{\tfrac{1}{3}+\tfrac{1}{3\sqrt{6}},\tfrac{1}{3}+\tfrac{1}{3\sqrt{6}},\tfrac{1}{3}-\tfrac{2}{3\sqrt{6}}\})\approx 0.314. \qquad (32)$$

The effect on the whole n-bit string is obtained by multiplying (31,32) times $3\beta n$.

5.4 Attack K1, 8-state

Consider $x=0$. (The analysis for $x=1$ is analogous). Eve has to distinguish between the four states $|\psi_{b0}\rangle$ with a POVM $\mathcal{M}=(M_b)_{b\in\mathcal{B}}$. For the min-entropy the optimal POVM is $M_b=\frac{1}{2}|\psi_{b0}\rangle\langle\psi_{b0}|$, yielding probability distribution $\{\frac{1}{2},\frac{1}{6},\frac{1}{6},\frac{1}{6}\}$. For the Shannon entropy the optimum is $M_b=\frac{1}{2}|\psi_{b1}\rangle\langle\psi_{b1}|$, yielding distribution $\{0,\frac{1}{3},\frac{1}{3},\frac{1}{3}\}$.

$$\begin{aligned} \mathsf{H}_{\min}(B)-\mathsf{H}_{\min}(B|X,\omega_{BX}) &= 2-1=1 && (33)\\ \mathsf{H}(B)-\mathsf{H}(B|X,\omega_{BX}) &= 2-\log 3\approx 0.415. && (34)\end{aligned}$$

The effect on the whole n-bit string is obtained by multiplying (33,34) times $3\beta n$.

5.5 Attack K2, 4-state

Eve has to distinguish between $B=0$ (z-basis) and $B=1$ (x-basis) by inspecting her ancilla state ζ_B.

Theorem 5.2 *In the case of 4-state encoding, the min-entropy of the basis B given the mixed state ζ_B is*

$$\mathsf{H}_{\min}(B|\zeta_B)=\mathsf{H}_{\min}(B)-\log(1+\sqrt{\beta(1-\tfrac{3}{2}\beta)}+\frac{\beta}{\sqrt{2}}). \qquad (35)$$

The corresponding POVM $\mathcal{M}=(M_b)_{b\in\{0,1\}}$ is given by

$$\begin{aligned} M_0=|\gamma_1\rangle\langle\gamma_1|+|\gamma_2\rangle\langle\gamma_2| \quad &; \quad M_1=|\gamma_3\rangle\langle\gamma_3|+|\gamma_4\rangle\langle\gamma_4| && (36)\\ |\gamma_1\rangle=\frac{|m_0\rangle}{\sqrt{2}}+\frac{|m_3\rangle-|m_1\rangle}{2} \quad &; \quad |\gamma_3\rangle=\frac{|m_0\rangle}{\sqrt{2}}-\frac{|m_3\rangle-|m_1\rangle}{2} &&\\ |\gamma_2\rangle=\frac{|m_2\rangle}{\sqrt{2}}+i\frac{|m_1\rangle+|m_3\rangle}{2} \quad &; \quad |\gamma_4\rangle=\frac{|m_2\rangle}{\sqrt{2}}-i\frac{|m_1\rangle+|m_3\rangle}{2}. && (37)\end{aligned}$$

Proof:

$$
|E_{01}^{(0,0,1)}\rangle = \frac{\sqrt{1-\frac{3}{2}\beta}|m_0\rangle + \sqrt{\frac{\beta}{2}}|m_3\rangle}{\sqrt{1-\beta}} \quad ; \quad |E_{01}^{(1,0,0)}\rangle = \frac{\sqrt{1-\frac{3}{2}\beta}|m_0\rangle + \sqrt{\frac{\beta}{2}}|m_1\rangle}{\sqrt{1-\beta}}
$$

$$
|E_{00}^{(0,0,1)}\rangle \propto \frac{|m_1\rangle - i|m_2\rangle}{\sqrt{2}} \quad ; \quad |E_{00}^{(1,0,0)}\rangle = \frac{i|m_2\rangle + |m_3\rangle}{\sqrt{2}} \tag{38}
$$

$$
\zeta_0 - \zeta_1 = \sqrt{\beta(1-\tfrac{3}{2}\beta)}\left[|m_0\rangle\frac{\langle m_3| - \langle m_1|}{\sqrt{2}} + \text{h.c.}\right] + \frac{\beta}{\sqrt{2}}\left[-i|m_2\rangle\frac{\langle m_1| + \langle m_3|}{\sqrt{2}} + \text{h.c.}\right]. \tag{39}
$$

The two expressions between square brackets act on orthogonal two-dimensional subspaces and both have the form of a Pauli operator. It directly follows that the eigenvalues are $\pm\sqrt{\beta(1-\frac{3}{2}\beta)}$ and $\pm\beta/\sqrt{2}$. Finally we apply (4) with $p_0 = p_1 = \frac{1}{2}$. □

Theorem 5.3 *In the case of 4-state encoding, the Shannon entropy of the basis B given the mixed state ζ_B is*

$$
\mathsf{H}(B|\zeta_B) = h(\frac{1}{2} + \frac{1}{2}\sqrt{\beta(1-\tfrac{3}{2}\beta)} + \frac{\beta}{2\sqrt{2}}). \tag{40}
$$

Proof: For binary B, the POVM associated with the min-entropy maximises $\text{tr}\, M_0(\zeta_0 - \zeta_1)$ (see Section 2.1). If we impose the symmetry $\text{tr}\, M_0\zeta_1 = \text{tr}\, M_1\zeta_0$ then this expression becomes $\text{tr}\, M_0\zeta_0 - (1 - \text{tr}\, M_0\zeta_0) = 2\text{tr}\, M_0\zeta_0 - 1$. (Imposing this symmetry is allowed, see Section 2.1). Hence the optimisation in the min-entropy-POVM is the same as the optimisation in the Shannon-POVM, and we conclude that the POVM associated with the min-entropy also minimises the Shannon entropy. Applying the POVM from Theorem 5.2 to (28) yields (40). □

5.6 Attack K2, 6-state

Eve has to distinguish between $B = 1$ (x-basis), $B = 2$ (y-basis), and $B = 3$ (z-basis). We define the permutation matrix S as

$$
S \stackrel{\text{def}}{=} |m_0\rangle\langle m_0| + |m_2\rangle\langle m_1| + |m_3\rangle\langle m_2| + |m_1\rangle\langle m_3|. \tag{41}
$$

Theorem 5.4 *In the case of 6-state encoding, the min-entropy of the basis B given the mixed state ζ_B is*

$$
\mathsf{H}_{\min}(B|\zeta_B) = \mathsf{H}_{\min}(B) - \log\left(1 + \frac{2\sqrt{2}}{\sqrt{3}}\sqrt{\beta(1-\beta)}\right). \tag{42}
$$

The associated POVM is

$$
M_3 \;=\; \frac{3-4\beta}{3(1-\beta)}|q\rangle\langle q| + \frac{1}{3(1-\beta)}|r\rangle\langle r| \tag{43}
$$

$$
|q\rangle \;=\; -\sqrt{\frac{1-\beta}{3-4\beta}}|m_0\rangle + \frac{\sqrt{2-3\beta}}{\sqrt{3-4\beta}}\frac{|m_1\rangle + |m_2\rangle - 2|m_3\rangle}{\sqrt{6}} \tag{44}
$$

$$
|r\rangle \;=\; \sqrt{1-\beta}\frac{|m_1\rangle + |m_2\rangle + |m_3\rangle}{\sqrt{3}} + i\sqrt{\beta}\frac{|m_1\rangle - |m_2\rangle}{\sqrt{2}} \tag{45}
$$

and $M_1 = SM_3S^\dagger$, $M_2 = SM_1S^\dagger$.

Proof: For $b \in \{1, 2, 3\}$ we have

$$
\begin{aligned}
\zeta_b \;=\; & (1-\tfrac{3}{2}\beta)|m_0\rangle\langle m_0| + \tfrac{\beta}{2}(|m_1\rangle\langle m_1| + |m_2\rangle\langle m_2| + |m_3\rangle\langle m_3|) \\
& + \sqrt{\tfrac{\beta}{2}(1-\tfrac{3}{2}\beta)}(|m_0\rangle\langle m_b| + \text{h.c.}) + \tfrac{\beta}{2}(i|m_{b+1}\rangle\langle m_{b+2}| + \text{h.c.})
\end{aligned} \tag{46}
$$

where $b+1$ should be read as $b+1 \bmod 3 \in \{1,2,3\}$.
The matrix Λ as defined in Section 2.1 is given by

$$\begin{aligned}\Lambda &= \sum_b \zeta_b M_b = (1-\tfrac{3}{2}\beta)(1+\frac{2\sqrt{\beta}}{\sqrt{6}\sqrt{1-\beta}})|m_0\rangle\langle m_0| + (\frac{1}{2}+\frac{(2-\beta)\sqrt{\beta}}{3\sqrt{6}\sqrt{1-\beta}})\sum_{j=1}^{3}|m_j\rangle\langle m_j| \qquad (47)\\ &\quad +\frac{\sqrt{2}}{6}\sqrt{\beta(1-\beta)}\left[\sum_{j=1}^{3}|m_0\rangle\langle m_j| + \text{h.c.}\right] + [(\frac{-i\beta}{2}-\frac{(1-2\beta)\sqrt{\beta}}{3\sqrt{6}\sqrt{1-\beta}})\sum_{j=1}^{3}|m_{j+1}\rangle\langle m_j| + \text{h.c.}].\end{aligned}$$

With some effort it is verified that indeed $\Lambda - \zeta_b \geq 0$ for $b \in \{1,2,3\}$ and $\beta \in [0, \frac{1}{2}]$. □

Conjecture 5.5 *Consider 6-state encoding. In terms of Shannon entropy, Eve's optimal POVM* $\mathcal{Q} = (Q_b)_{b\in\mathcal{B}}$ *for learning as much as possible about* B *from* ζ_B *is given by*

$$Q_3 = \frac{3-4\beta}{3(1-\beta)}|q'\rangle\langle q'| + \frac{1}{3(1-\beta)}|r'\rangle\langle r'| \qquad (48)$$

$$|q'\rangle = \sqrt{\frac{1-\beta}{3-4\beta}}|m_0\rangle + \frac{\sqrt{2-3\beta}}{\sqrt{3-4\beta}}\frac{|m_1\rangle+|m_2\rangle-2|m_3\rangle}{\sqrt{6}} \qquad (49)$$

$$|r'\rangle = |r\rangle^* \qquad (50)$$

with $|r\rangle$ *as defined by (45), and* $Q_1 = SQ_3S^\dagger$, $Q_2 = SQ_1S^\dagger$.

Evidence: The POVM $\mathcal{Q}$ is the 'dual' of $\mathcal{M}$ in the sense that it has $\boldsymbol{v}$ replaced by $-\boldsymbol{v}$. (This fact is not immediately evident. One can also take $\mathcal{M}$ and apply it to the state ζ_B with $\boldsymbol{v} \to -\boldsymbol{v}$; this is equivalent). It was noticed in [6] that such a 'dual' is the optimal POVM in the case of the intercept attack K1. We have performed numerical POVM optimisations which find a local minimum of the Shannon entropy, starting from 3^{10} initial points in POVM space; all combinations of a positive/zero/negative value for each of the 10 degrees of freedom that are left in the POVM after imposing S-symmetry.[8] Furthermore we did a Monte Carlo sampling of 10^{11} random POVMs. We did not find a single POVM that performs better than $\mathcal{Q}$. The numerical search did find $\mathcal{M}$ and $\mathcal{Q}$, as well as 200 POVMs with Shannon entropy between that of $\mathcal{Q}$ and $\mathcal{M}$. □

Theorem 5.6 *In case of the measurement* $\mathcal{Q}$ *specified in Conjecture 5.5, the entropy of* B *is given by*

$$\mathsf{H}(B|\mathcal{Q}(\zeta_B)) = h(p_6) + 1 - p_6 \qquad (51)$$

$$p_6 \overset{\text{def}}{=} \frac{1}{3} - \frac{2\sqrt{2}}{3\sqrt{3}}\sqrt{\beta(1-\beta)}. \qquad (52)$$

Proof: After some algebra it can be seen that $\operatorname{tr}\zeta_3 Q_3 = p_6$. We apply (28) from Lemma 5.1. □
Some remarks on the case $\beta \geq \frac{1}{3}$ can be found in the Appendix.

5.7 Attack K2, 8-state

Theorem 5.7 *Let* $\beta \leq \frac{1}{3}$. *In the 8-state case, the min-entropy of* B *given the mixed state* ζ_B *is*

$$\mathsf{H}_{\min}(B|\zeta_B) = \mathsf{H}_{\min}(B) - \log\left(1+\sqrt{6}\sqrt{\beta(1-\tfrac{3}{2}\beta)}\right). \qquad (53)$$

The associated POVM $(M_{uw})_{u,w\in\{0,1\}}$ *is*

$$M_{00} = \frac{\sum_{a=0}^{3}|m_a\rangle}{2}\frac{\sum_{a'=0}^{3}\langle m_{a'}|}{2} \quad ; \quad M_{01} = (\sigma_z\otimes\mathbb{1})M_{00}(\sigma_z\otimes\mathbb{1}) \qquad (54)$$

$$M_{10} = (\sigma_z\otimes\sigma_z)M_{00}(\sigma_z\otimes\sigma_z) \quad ; \quad M_{11} = (\mathbb{1}\otimes\sigma_z)M_{00}(\mathbb{1}\otimes\sigma_z). \qquad (55)$$

[8] Imposing symmetry is allowed, see Section 2.1.

Proof: The states ζ_{uw} are given by

$$\begin{aligned}\zeta_{00} &= (1-\tfrac{3}{2}\beta)|m_0\rangle\langle m_0| + \frac{\beta}{2}\sum_{j=1}^{3}|m_j\rangle\langle m_j| + \sqrt{\tfrac{\beta}{2}(1-\tfrac{3}{2}\beta)}\left[|m_0\rangle\frac{\langle m_1|+\langle m_2|+\langle m_3|}{\sqrt{3}} + \text{h.c.}\right] \\ &\quad + \frac{\beta}{2\sqrt{3}}\left[i\sum_{j=1}^{3}|m_j\rangle\langle m_{j+1}| + \text{h.c.}\right] \qquad (56)\end{aligned}$$

and $\zeta_{01}=(\sigma_z\otimes\mathbb{1})\zeta_{00}(\sigma_z\otimes\mathbb{1})$, $\zeta_{10}=(\sigma_z\otimes\sigma_z)\zeta_{00}(\sigma_z\otimes\sigma_z)$, $\zeta_{11}=(\mathbb{1}\otimes\sigma_z)\zeta_{00}(\mathbb{1}\otimes\sigma_z)$. The matrix Λ has a simple diagonal form,

$$\Lambda = \sum_{uw}\zeta_{uw}M_{uw} = \left(1-\tfrac{3}{2}\beta+\sqrt{3}\sqrt{\tfrac{\beta}{2}(1-\tfrac{3}{2}\beta)}\right)|m_0\rangle\langle m_0| + (\frac{\beta}{2}+\frac{\sqrt{\frac{\beta}{2}(1-\frac{3}{2}\beta)}}{\sqrt{3}})\sum_{j=1}^{3}|m_j\rangle\langle m_j|. \qquad (57)$$

It is easily verified that $\Lambda-\zeta_{uw}\geq 0$ for all $\beta\in[0,\frac{1}{3}]$ and $u,w\in\{0,1\}$. Furthermore we have

$$\text{tr}\,\Lambda = 1+\sqrt{6}\sqrt{\beta(1-\tfrac{3}{2}\beta)}. \qquad (58)$$

□

Conjecture 5.8 *Consider 8-state encoding. Let $\beta\leq\frac{1}{3}$. In terms of Shannon entropy, Eve's optimal POVM $\mathcal{R}=(R_{uw})_{u,w\in\{0,1\}}$ for learning as much as possible about U,W from ζ_{UW} is given by*

$$R_{00}=|v\rangle\langle v|, \qquad |v\rangle = \frac{|m_0\rangle-|m_1\rangle-|m_2\rangle-|m_3\rangle}{2} \qquad (59)$$

and $R_{01}=(\sigma_z\otimes\mathbb{1})R_{00}(\sigma_z\otimes\mathbb{1}), R_{10}=(\sigma_z\otimes\sigma_z)R_{00}(\sigma_z\otimes\sigma_z), R_{11}=(\mathbb{1}\otimes\sigma_z)R_{00}(\mathbb{1}\otimes\sigma_z)$.

Evidence: Just as in the 6-state case, the POVM for the Shannon entropy is the 'dual' ($\boldsymbol{v}\to-\boldsymbol{v}$) of the POVM associated with the min-entropy. Numerical optimisations (from 3^{12} initial points) with imposed symmetry gave us no POVM that performs better than $\mathcal{R}$. The numerical search did find $\mathcal{R}$ and $\mathcal{M}$, as well as 168 POVMs with Shannon entropy between that of $\mathcal{R}$ and $\mathcal{M}$. □

Theorem 5.9 *In case of the measurement $\mathcal{R}$ specified in Conjecture 5.8, the entropy of B is given by*

$$\begin{aligned}\mathsf{H}(B|\mathcal{R}(\zeta_B)) &= h(p_8)+(1-p_8)\log 3 \qquad (60)\\ p_8 &\overset{\text{def}}{=} \frac{1}{4}-\frac{\sqrt{3}}{2\sqrt{2}}\sqrt{\beta(1-\tfrac{3}{2}\beta)}. \qquad (61)\end{aligned}$$

Proof: A brief calculation gives $\text{tr}\,\zeta_{uw}R_{uw}=p_8$ (for all u,w) with p_8 as defined in (61). Then we use (28). □

Some remarks on the case $\beta\geq\frac{1}{3}$ can be found in the Appendix.

6 Putting it all together

The amount of privacy amplification needed in the protocol (Section 2.2, `Ext` function) is determined by the *strongest* of the M1, M2, K1, K2 attacks. Below we combine all the results from Sections 4 and 5.

Shannon entropy leakage $I(\beta)$ per qubit			
	4-state	*6-state*	*8-state*
M1	0.399	0.256	0
M2	$\beta \cdot 1 + (1-\beta)[1-h(p_\beta)], \quad p_\beta = \frac{1}{2} - \frac{\sqrt{\frac{\beta}{2}(1-\frac{3}{2}\beta)}}{1-\beta}$		
K1	$3\beta \cdot 0.399$	$3\beta \cdot 0.314$	$3\beta \cdot 0.415$
K2	$1 - h(\frac{1}{2} + \frac{1}{2}\sqrt{\beta(1-\frac{3}{2}\beta)} + \frac{\beta}{2\sqrt{2}})$	$\log 3 - [h(p_6) + 1 - p_6]$ $p_6 = \frac{1}{3} - \frac{2\sqrt{2}}{3\sqrt{3}}\sqrt{\beta(1-\beta)}$	$2 - [h(p_8) + (1-p_8)\log 3]$ $p_8 = \frac{1}{4} - \frac{\sqrt{6}}{4}\sqrt{\beta(1-\frac{3}{2}\beta)}$

Table 1: *Shannon entropy loss $I(\beta)$ as a function of noise β, for the attacks M1,M2,K1,K2. The 6-state and 8-state K2 results are conjectures.*

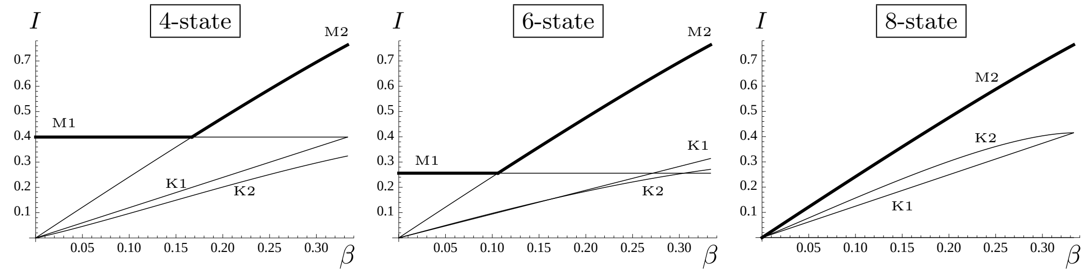

Figure 1: *Shannon leakage $I(\beta)$ per qubit as a function of the bit error rate β. The 6-state and 8-state K2 results are conjectures.*

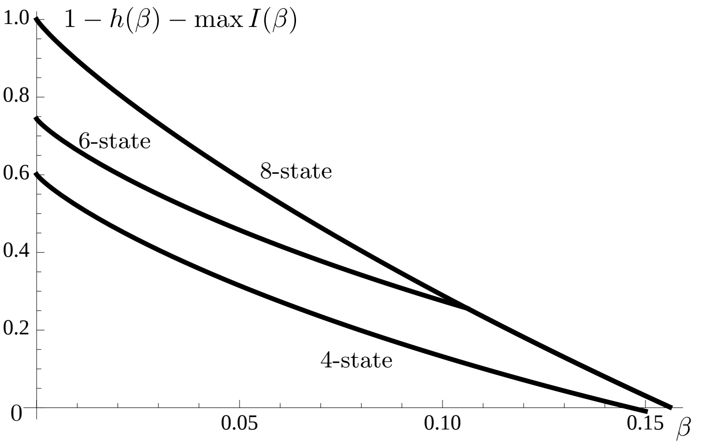

Figure 2: *QKR capacity* $1 - h(\beta) - \max_{\text{attacks}} I(\beta)$ *as a function of the bit error rate β. (Leakage is expressed as mutual information). The strongest attack determines $I(\beta)$.*

6.1 Combined results for Shannon entropy

Table 1 shows an overview of the Shannon entropy losses in all the attacks. The individual M1,M2,K1,K2 leakages (and the maximum) are plotted as a function of β in Fig. 1. Fig. 2 shows the QKR capacity $1 - h(\beta) - I(\beta)$.

For 4-state and 6-state encoding, the strongest attack at low β is M1. At larger β it is the QKD-like attack M2. For 8-state encoding, M2 is always the strongest attack. The QKR channel capacity of 4-state encoding is always below 6-state. 8-state has higher capacity than 6-state at β up to ≈ 0.1061, after which they are the same and equal to the QKD capacity.

Our plots do not go beyond $\beta = \frac{1}{3}$ because intercept-resend attacks cause noise $\beta = \frac{1}{3}$. In attack K1 the fraction of qubits intercepted by Eve is 3β, which at $\beta > \frac{1}{3}$ would exceed 1. At $\beta > \frac{1}{3}$ we have to be careful how we interpret K1. A discussion can be found in the Appendix. Note that attacks K1 and K2 at $\beta = \frac{1}{3}$ are not necessarily the same thing. Attack K2 restricts Eve's options by forcing her to first perform a specific ancilla operation, whereas attack K1 allows any POVM on the intercepted qubit. Hence at $\beta = \frac{1}{3}$ the K2 leakage cannot exceed the K1 leakage.

6.2 Combined results for min-entropy

Table 2 shows an overview of the min-entropy entropy losses in all the attacks. The individual M1,M2,K1,K2 leakages (and the maximum) are plotted as a function of β in Fig. 3. Fig. 4 shows the QKR capacity $1 - h(\beta) - \triangle\mathsf{H}_{\min}(\beta)$. For 4-state and 6-state, the winning attacks are as for the Shannon entropy case. For 8-state, however, the winning attack is K2. If capacity is computed using min-entropy loss as the measure of Eve's knowledge, then the QKR capacity of 8-state is higher than 6-state on the range $\beta \in [0, 0.0612]$. There is a tiny interval $\beta \in (0.0612, 0.0638]$ where 6-state outperforms 8-state; at $\beta > 0.0638$ all capacities are zero. 4-state is always worse than 6-state.

Min-entropy leakage per qubit			
	4-state	6-state	8-state
M1	0.772	0.658	0
M2	$\log[1+\sqrt{2}\sqrt{\beta(1-\frac{3}{2}\beta)}+\beta]$		
K1	$3\beta \cdot 0.772$	$3\beta \cdot 0.861$	$3\beta \cdot 1$
K2	$\log(1+\sqrt{\beta(1-\frac{3}{2}\beta)}+\frac{\beta}{\sqrt{2}})$	$\log\left(1+\frac{2\sqrt{2}}{\sqrt{3}}\sqrt{\beta(1-\beta)}\right)$	$\log\left(1+\sqrt{6}\sqrt{\beta(1-\frac{3}{2}\beta)}\right)$

Table 2: *Min-entropy loss as a function of noise β, for the attacks M1,M2,K1,K2.*

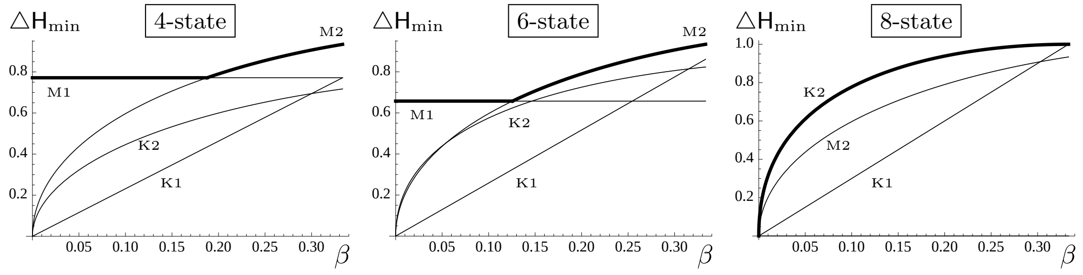

Figure 3: *Min-entropy leakage per qubit as a function of the bit error rate β.*

7 Addition of artificial noise

The structure evident in the $|E^{\boldsymbol{v}}_{xy}\rangle$ vectors (10) allows us to simplify the derivation of the capacity of 6-state/8-state QKD with added artificial noise. (This also applies to attack M2.) In [14] a derivation for 6-state QKD was given without noise symmetrisation, resulting in a lengthy analysis. Moreover, the end result was presented in a less than elegant way. Here we give a shorter derivation, and we present the end result in a very intuitive form.

Alice adds artificial noise to X. This is represented as a binary symmetric channel with bit error rate ε. Let $\varepsilon \star \beta \overset{\text{def}}{=} \varepsilon(1-\beta) + (1-\varepsilon)\beta$ be the bit error rate on the concatenated channel consisting of Alice's noise ε followed by the physical noise β introduced by Eve. The channel capacity from Alice to Bob becomes $I'_{\text{AB}}(\varepsilon, \beta) = 1 - h(\varepsilon \star \beta)$. Eve's task of distinguishing between the various $|E^{\boldsymbol{v}}\rangle$ states is not affected; the weights β and $1-\beta$ in (21) do not change. However, Eve's inference about X from her measurement outcomes has additional noise ε: the bit error rate of the 'easy' channel changes from 0 to $\varepsilon \star 0 = \varepsilon$, and the bit error rate of the 'difficult' channel changes from p_β to $\varepsilon \star p_\beta$.

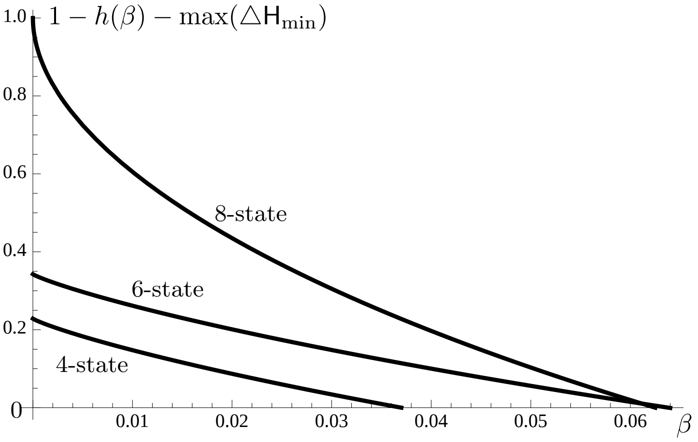

Figure 4: *QKR capacity as a function of the bit error rate β, if leakage is expressed as min-entropy loss.*

Thus the channel from Alice to Eve now has capacity $I'_{\rm AE}(\varepsilon,\beta)=\beta[1-h(\varepsilon)]+(1-\beta)[1-h(\varepsilon\star p_\beta)]$, with p_β as defined in (20). The secrecy capacity is

$$\begin{aligned} C'(\varepsilon,\beta)=I'_{AB}-I'_{AE} &= 1-h(\varepsilon\star\beta)-\Big\{\beta[1-h(\varepsilon)]+(1-\beta)[1-h(\varepsilon\star p_\beta)]\Big\} \\ &= (1-\beta)h(\varepsilon\star p_\beta)+\beta h(\varepsilon)-h(\varepsilon\star\beta) \qquad (62) \end{aligned}$$

which is precisely the result of [14] but in simplified form. Fig. 5 shows the optimal noise $\varepsilon_{\rm opt}(\beta)$ as a function of β, and the resulting capacity $C_{\rm opt}(\beta)=C'(\varepsilon_{\rm opt}(\beta),\beta)$. The original positive-capacity region $\beta\leq 0.156$ is extended to $\beta\leq 0.162$.

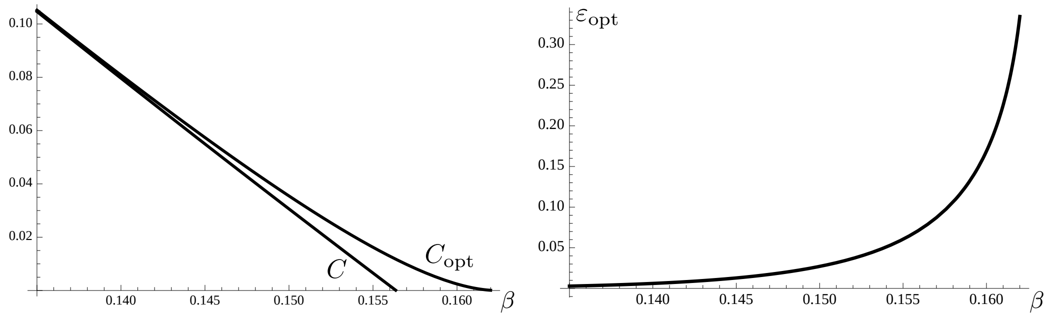

Figure 5: **Left:** *The capacity $C(\beta)$ without artificial noise and the capacity $C_{\rm opt}=C'(\varepsilon_{\rm opt}(\beta),\beta)$ for the best choice of artificial noise.* **Right:** *The optimal value of Alice's noise parameter ε as a function of the channel noise β. (Numerical optimisation.)*

8 Discussion

The fact that M1 is the dominant attack against 4-state and 6-state encoding at low bit error rate, and M2 at larger β, comes as no surprise. The vulnerability of the message is exactly the reason why 8-state encoding was introduced in [6]. And as 8-state protects the message better, it is also not surprising that an attack on the key dominates in the 8-state min-entropy analysis.

What we did not know a priori is the relative strength of the β-dependent attacks, and their strength (at large β) compared to M1. Figs. 1 and 3 show complicated behaviour with various intersections of curves.

We were surprised to see M2 'winning' in the 8-state Shannon entropy analysis. With M2 being the relevant attack, a large part of the security analysis becomes identical, or at least very similar, to well known QKD analysis. Hence the trick with Alice's artificial noise is as relevant to QKR as it is to QKD.

When the number of qubits (n) is very large, the relevant quantity to look at is Shannon entropy. For small n it is min-entropy. In intermediate cases it is something in between. From our results we conclude that 8-state encoding yields the highest QKR capacity under practically all circumstances.

As topics for future work we see (i) Adaptation of the protocol so that the n-qubit quantum state $|\Psi\rangle$ sent by Alice contains the message itself (in privacy-amplified form, as in [2]), instead of a random mask. This would further improve communication efficiency. (ii) Determine the effect of artificial noise on the min-entropy loss in the case of the K2 attack on 8-state encoding. (iii) Determine how tight the bound in Lemma 4.1 (M2 reduces to QKD analysis) is as a function of N.

Acknowledgments

We thank Serge Fehr for useful discussions. Part of this research was funded by NWO (CHIST-ERA project ID_IOT).

Appendix: Attack K2 at high noise levels

For the sake of completeness we present entropy results for the K2 attack at very high noise levels. As mentioned in Section 6.1, the K1 attack needs some interpreting at $\beta > \frac{1}{3}$: Eve does the the optimal K1-POVM on all n qubits but then forwards badly chosen states to Bob which cause $\beta > \frac{1}{3}$. Attack K2 is still defined as before: Eve couples her ancilla to the AB system in such a way that noise $\beta > \frac{1}{3}$ occurs. At $\beta = \frac{1}{2}$ the point is reached where Eve might as well send a completely random qubit state to Bob, and she extracts the maximum possible amount of information from the scrutinised qubit. Hence the K2-leakage at $\beta = \frac{1}{2}$ must equal the K1-leakage at $\beta = \frac{1}{3}$.

In the case of 4- and 6-state encoding we find that the POVMs (35) and (43,48) respectively are optimal on the whole range $\beta \in [0, \frac{1}{2}]$. In the 8-state case the situation is different: we find a different POVM in the range $\beta \in [\frac{1}{3}, \frac{1}{2}]$.

Theorem .1 *Let $\frac{1}{3} \leq \beta \leq \frac{1}{2}$. For 8-state encoding, the min-entropy of B given the mixed state ζ_B is*

$$\mathsf{H}_{\min}(B|\zeta_B) = \mathsf{H}_{\min}(B) - 1 = 1. \tag{63}$$

The associated POVM $(M_{uw})_{u,w\in\{0,1\}}$ is

$$\begin{aligned} M_{00} &= \frac{1-\beta}{2\beta}|a\rangle\langle a| + \frac{3\beta-1}{2\beta}|d\rangle\langle d| & (64)\\ |a\rangle &= \frac{\sqrt{\beta/2}}{\sqrt{1-\beta}}|m_0\rangle + \frac{\sqrt{1-\frac{3}{2}\beta}}{\sqrt{1-\beta}} \cdot \frac{|m_1\rangle + |m_2\rangle + |m_3\rangle}{\sqrt{3}} & (65)\\ |d\rangle &= \frac{e^{i\pi/3}|m_1\rangle + e^{-i\pi/3}|m_2\rangle - |m_3\rangle}{\sqrt{3}} & (66) \end{aligned}$$

$$M_{01} = (\sigma_z \otimes \mathbb{1})M_{00}(\sigma_z \otimes \mathbb{1}); M_{10} = (\sigma_z \otimes \sigma_z)M_{00}(\sigma_z \otimes \sigma_z); M_{11} = (\mathbb{1} \otimes \sigma_z)M_{00}(\mathbb{1} \otimes \sigma_z). \tag{67}$$

<u>Proof</u>: After some algebra it turns out that the matrix Λ has a simple diagonal form,

$$\Lambda = \sum_{uw} \zeta_{uw} M_{uw} = (2-3\beta)\,|m_0\rangle\langle m_0| + \beta \sum_{j=1}^{3} |m_j\rangle\langle m_j|. \tag{68}$$

It is easily verified that $\Lambda - \zeta_{uw} \geq 0$ for all $\beta \in [\frac{1}{3}, \frac{1}{2}]$ and $u, w \in \{0, 1\}$. □

Lemma .2 *Consider 8-state encoding. Let $\frac{1}{3} \leq \beta \leq \frac{1}{2}$. In terms of Shannon entropy, Eve's optimal POVM $\mathcal{R} = (R_{uw})_{u,w\in\{0,1\}}$ for learning as much as possible about U, W from ζ_{UW} is given by*

$$R_{00} \;=\; \frac{1-\beta}{2\beta}|a'\rangle\langle a'| + \frac{3\beta-1}{2\beta}|d'\rangle\langle d'| \tag{69}$$

$$|a'\rangle \;=\; -\frac{\sqrt{\beta/2}}{\sqrt{1-\beta}}|m_0\rangle + \frac{\sqrt{1-\frac{3}{2}\beta}}{\sqrt{1-\beta}} \cdot \frac{|m_1\rangle + |m_2\rangle + |m_3\rangle}{\sqrt{3}} \tag{70}$$

$$|d'\rangle \;=\; |d\rangle^* \tag{71}$$

and $R_{01} = (\sigma_z \otimes \mathbb{1})R_{00}(\sigma_z \otimes \mathbb{1}), R_{10} = (\sigma_z \otimes \sigma_z)R_{00}(\sigma_z \otimes \sigma_z), R_{11} = (\mathbb{1} \otimes \sigma_z)R_{00}(\mathbb{1} \otimes \sigma_z)$.

Proof: On the whole range $\beta \in [\frac{1}{3}, \frac{1}{2}]$ the POVM $\mathcal{R}$ gives $\mathsf{H}(B|\mathcal{R}(\zeta_B)) = \log 3$, which is the K1 result at $\beta = \frac{1}{3}$ and therefore the minimum possible value. □
Just as in the 6-state case and in the 8-state for $\beta \leq \frac{1}{3}$, the POVM $\mathcal{R}$ for the Shannon entropy is the 'dual' ($\boldsymbol{v} \to -\boldsymbol{v}$) of the POVM associated with the min-entropy.
Note that at $\beta = \frac{1}{3}$ the POVMs for $\beta \leq \frac{1}{3}$ and $\beta \geq \frac{1}{3}$ match, as they should. The leakages for the K1 and K2 attacks up to $\beta = \frac{1}{2}$ are plotted in Figs. 6 and 7.

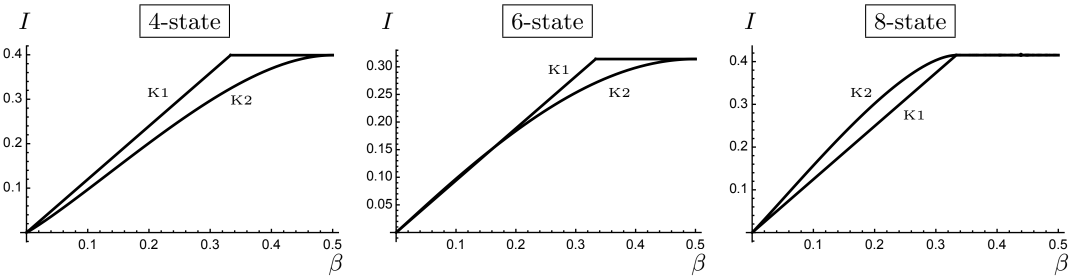

Figure 6: *Shannon leakage $I(\beta)$ per qubit as a function of the bit error rate β up to $\beta = \frac{1}{2}$. The K2 results for 6-state and 8-state encoding are conjectures.*

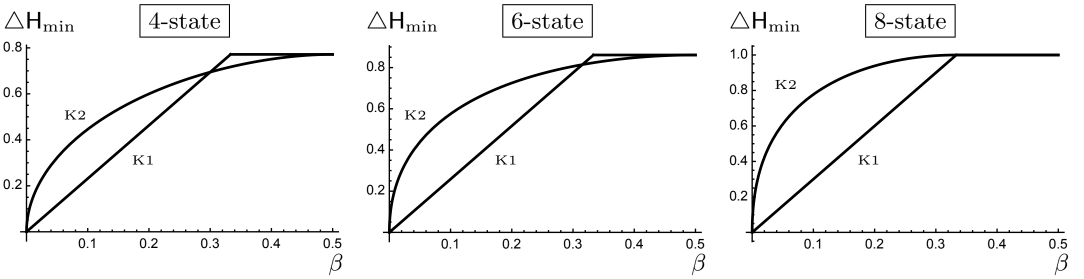

Figure 7: *Min-entropy leakage per qubit as a function of the bit error rate β up to $\beta = \frac{1}{2}$.*

For 4- and 6-state, K2 reaches it maximum at $\beta = \frac{1}{2}$, whereas in the 8-state case the maximum is reached already at $\beta = \frac{1}{3}$.

References

[1] C.H. Bennett, G. Brassard, and S. Breidbart. Quantum Cryptography II: How to re-use a one-time pad safely even if P=NP. *Natural Computing*, 13:453–458, 2014. Original manuscript 1982.

[2] D. Gottesman. Uncloneable encryption. *Quantum Information and Computation*, 3(6):581–602, 2003.

[3] I.B. Damgård, T.B. Pedersen, and L. Salvail. A quantum cipher with near optimal key-recycling. In *CRYPTO*, pages 494–510, 2005.

[4] I.B. Damgård, T.B. Pedersen, and L. Salvail. How to re-use a one-time pad safely and almost optimally even if P = NP. *Natural Computing*, 13(4):469–486, 2014.

[5] S. Fehr and L. Salvail. Quantum authentication and encryption with key recycling. In *Eurocrypt*, 2017. `https://arxiv.org/abs/1610.05614v1`.

[6] B. Škorić and M. de Vries. Quantum Key Recycling with eight-state encoding. (The Quantum One Time Pad is more interesting than we thought). *International Journal of Quantum Information*, 2017. `https://eprint.iacr.org/2016/1122`.

[7] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *Annual Symposium on Foundations of Computer Science*, pages 547–553, 2000.

[8] D.W. Leung. Quantum Vernam cipher. *Quantum Information and Computation*, 2(1):14–34, 2002.

[9] P.O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. *Phys. Rev. A*, 67(4):042317, 2003.

[10] P. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys.Rev.Lett.*, 85:441, 2000.

[11] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys.Rev.A*, 72:012332, 2005.

[12] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):3018–3021, 1998.

[13] A.S. Holevo. Statistical decision theory for quantum systems. *Journal of multivariate analysis*, 3:337–394, 1973.

[14] Z. Shadman, H. Kampermann, T. Meyer, and D. Bruß. Optimal eavesdropping on noisy states in quantum key distribution. *Int. J. of Quantum Information*, 07(01):297, 2009.

[15] R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans.Inf.Th.*, 55(9):4337–4347, 2009.

[16] R. Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3:645–649, 2007.

[17] M. Christandl, R. König, G. Mitchison, and R. Renner. One-and-a-half quantum de Finetti theorems. *Communications in Mathematical Physics*, 273(2):473–498, 2007.

[18] R. Renner. *Security of quantum key distribution.* PhD thesis, ETH Zürich, 2005.