Optimal attacks on qubit-based Quantum Key Recycling

Daan Leermakers¹ · Boris Škorić¹

Received: 16 August 2017 / Accepted: 10 January 2018 / Published online: 29 January 2018
© The Author(s) 2018. This article is an open access publication

Abstract Quantum Key Recycling (QKR) is a quantum cryptographic primitive that allows one to reuse 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 upper bounds on the required amount of 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 provide results in terms of min-entropy loss as well as accessible (Shannon) information. 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. From the optimal attacks we compute the required amount of privacy amplification and hence the achievable communication rate (useful information per qubit) of qubit-based QKR. Overall, 8-state encoding yields the highest communication rates.

Keywords Quantum cryptography · Quantum Key Recycling · Quantum information

✉ Boris Škorić
b.skoric@tue.nl

Daan Leermakers
d.leermakers.1@tue.nl

¹ Eindhoven University of Technology (TU/e), Eindhoven, The Netherlands

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 reuse of encryption keys. If Bob detects no disturbance on the quantum channel, it may be safe to reuse 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 reuse 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 et al. [3, 4]. Gottesman’s Unclonable Encryption offers a limited reusability of key material. Damgård et al. introduced a full key reuse 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 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) [7–9]. 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 seems undeserved. In a QKD-equipped world, QKR can play an important role. The process of repeatedly generating new QKD keys and then using them up with classical OTP encryption is wasteful of bandwidth. One QKD instance followed by repeated QKR runs is more communication efficient.

1.2 Contributions and outline

- We consider four classes of attack against individual qubits in qubit-based QKR, such that Eve introduces channel noise parametrised by the bit error rate β . Two of these attacks are aimed against the message, and two against the basis key. We argue that these classes capture Eve’s strongest possible attack.
- 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 optimal

POVMs for attacking the key in the known-plaintext setting. We obtain POVMs for min-entropy as well as Shannon entropy. The min-entropy loss is a pessimistic bound on the required privacy amplification. The Shannon entropy loss ('accessible information') is relevant for a restricted class of attacks where Eve is forced (e.g. by lack of quantum memory) to immediately perform a measurement.

- From the optimal POVMs we determine how much privacy amplification is needed: this is dictated by the most powerful of the attacks. 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 rate 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 rate.
 - **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 the QKR message rate is computed using min-entropy loss as the measure of Eve's knowledge, then the rate 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 by-product 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 Sect. 2, we introduce notation and briefly recap 4-state QKR, QKR security notions, and 8-state QKR. In Sect. 3, we explain our approach. In Sect. 4, we introduce the EPR version of the protocol, apply noise symmetrisation and obtain Eve's state by purification. Attacks on the plaintext are described in Sect. 5, and known-plaintext

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

attacks on the key in Sect. 6. We aggregate all the results in Sect. 7, and we determine the QKR rates. Insertion of artificial noise is discussed in Sect. 8.

2 Preliminaries

2.1 Notation and terminology

Classical random variables (RVs) are written with capital letters. Their realisations are written in lowercase. The probability for an RV X to take value x is written as $\Pr[X = x]$. The expectation is denoted as $\mathbb{E}_x f(x) = \sum_{x \in \mathcal{X}} \Pr[X = x] f(x)$. The Shannon entropy of X is written as $H(X)$. Sets are written in calligraphic font. The notation ‘log’ stands for the base 2 logarithm. The min-entropy of $X \in \mathcal{X}$ is $H_{\min}(X) = -\log \max_{x \in \mathcal{X}} \Pr[X = x]$. The conditional min-entropy is $H_{\min}(X|Y) = -\log \mathbb{E}_y \max_{x \in \mathcal{X}} \Pr[X = x|Y = y]$. The notation h denotes the binary entropy function $h(p) = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}$. Sometimes we will write $h(\{p_1, \dots, p_n\})$ instead of $\sum_i p_i \log \frac{1}{p_i}$. Bitwise XOR of binary strings is written as ‘ $\oplus$ ’. The Kronecker delta is denoted as δ_{ab} . The inverse of a bit $b \in \{0, 1\}$ is written as $\bar{b} = 1 - b$.

We use Dirac notation of quantum states, with the standard qubit basis states $|0\rangle$ and $|1\rangle$ represented as $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. The Pauli matrices are $\sigma_x, \sigma_y, \sigma_z$. We write $\sigma = (\sigma_x, \sigma_y, \sigma_z)$. The standard basis is the eigenbasis of σ_z , with $|0\rangle$ in the positive z -direction. The identity matrix is denoted as $\mathbb{1}$. 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 z^* . Let A have eigenvalues λ_i . The 1-norm of A is written as $\|A\|_1 = \text{tr} \sqrt{A^\dagger A} = \sum_i |\lambda_i|$.

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 $\mathcal{M}$ applied to mixed state ρ . The $\mathcal{M}(\rho)$ is a classical RV. 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 $|x\rangle$ being an orthonormal basis. The min-entropy of the classical RV X given part ‘B’ of the system is [15]

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

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 condition² [13]

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

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

then there can be no better POVM (but equally good ones may exist). For states that furthermore depend on a classical RV $Y \in \mathcal{Y}$, the min-entropy of X given Y and the quantum state is

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

A simplification occurs when X is a binary variable. Let $X \in \{0, 1\}$.

Then

$$X \sim (p_0, p_1) : H_{\min}(X|Y, \rho_X(Y)) = 1 - \log \left(1 + \mathbb{E}_y \left\| p_0 \rho_0(y) - p_1 \rho_1(y) \right\|_1 \right). \quad (4)$$

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

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

The mutual information $H(X) - H(X|\rho_X)$ is called ‘accessible information’. 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, $U_g M_x U_g^\dagger = M_{g(x)}$.

We will speak about ‘the bit error rate β of a quantum channel’. This is defined as the probability that a classical bit g , sent by Alice embedded in a qubit, arrives at Bob’s side as $\bar{g}$.

2.2 Four-state QKR and its security

We briefly summarise the QKR construction by Fehr and Salvail (‘QENC*’ in [5], but using slightly different notation) and its security properties.

The message is $\mu \in \{0, 1\}^\ell$. The key material consists of a MAC key k_M , a Secure Sketch key k_{SS} , an extractor key k_{ext} and a basis key $\theta \in \mathcal{C}$, where $\mathcal{C}$ is a classical error-correcting code with codewords of length n and minimal distance d . The scheme makes use of a message-independent, key-private³ MAC function M that produces a tag of length λ . The probability that a message modification is not detected is $\varepsilon_{\text{MAC}} = 2^{-\lambda}$. Furthermore, the scheme needs a *secure sketch* [16]. The secure sketch consists of an algorithm SS that creates a ‘sketch’ $SS(k_{SS}, x) \in \{0, 1\}^a$, and a reconstruction algorithm Rec that is able to reconstruct x from a noisy value x' and the sketch. The secure sketch must have the message independence and key privacy property. Such secure sketches exist for very small β [17]. The probability of reconstruction failure is denoted as ε_{SS} .

Finally, there is a strong extractor Ext which too has message independence and key privacy.

³ For the definition of these concepts we refer to [5].

QENC* Encryption Alice performs the following steps. Choose a uniformly random $g \in \{0, 1\}^n$. Compute $s = \text{SS}(k_{\text{SS}}, g)$ and $z = \text{Ext}(k_{\text{ext}}, g) \in \{0, 1\}^\ell$. Compute the ciphertext $c = \mu \oplus z$ and authentication tag $T = M(k_{\text{M}}, g || c || s)$. Prepare n qubits in BB84 states such that the i 'th qubit contains payload g_i encoded in basis θ_i . Send the qubits to Bob as well as s, c, T .

QENC* Decryption (Bob receives the classical information s', c', T' and n qubits that have possibly been interfered with). Bob performs the following steps. For $i \in \{1, \dots, n\}$ measure the i 'th qubit in the θ_i -basis. This yields $g' \in \{0, 1\}^n$. Recover an estimator $\hat{g}$ from g' and s' using the reconstruction procedure Rec of the secure sketch. Compute $\hat{z} = \text{Ext}(k_{\text{ext}}, \hat{g})$ and $\hat{\mu} = c' \oplus \hat{z}$. Accept the message $\hat{\mu}$ if Rec succeeded and $T' = M(k_{\text{M}}, \hat{g} || c' || s')$. Communicate Accept/Reject to Alice.

QENC* Key update In case of Reject, Alice and Bob pick a uniformly random $\theta' \in \mathcal{C}$.

Theorem 1 (Theorem 2 in [5], with encryption made explicit) *Let $K_{\text{MAC}}, K_{\text{SS}}, K_{\text{ext}}$ be completely unknown to Eve before the execution of QENC*. Let Eve's state be labelled as E before execution, and E' after one execution of QENC*. Let Θ' be the (possibly updated) basis key after execution. Let δ denote statistical distance. Let γ denote guessing probability. Then it holds that*

$$\gamma(\Theta' | E') \leq \gamma(\Theta | E) + \frac{1}{|\mathcal{C}|} \quad (6)$$

$$\delta(U, K_{\text{MAC}} K_{\text{SS}} K_{\text{ext}} | \Theta' E') \leq \varepsilon_{\text{MAC}} + \varepsilon_{\text{SS}} + \sqrt{\gamma(\Theta | E) \left(1 + \frac{|\mathcal{C}| 2^{nh(\beta)}}{2^{d/2}}\right)} 2^{\lambda+a+\ell} \quad (7)$$

where U is a uniform variable on the space of $K_{\text{MAC}}, K_{\text{SS}}, K_{\text{ext}}$.

From this theorem it was shown that after repeated executions of QENC* all keys are still secure. This holds even in the case of known plaintext. The security of the keys implies the confidentiality of the messages.

It is possible to use a basis key θ chosen at random from $\{0, 1\}^n$ instead of from $\mathcal{C}$. Then the term $1/|\mathcal{C}|$ in (6) becomes 2^{-n} and (7) takes the form [18]

$$\delta(U, K_{\text{MAC}} K_{\text{SS}} K_{\text{ext}} | \Theta' E') \leq \varepsilon_{\text{MAC}} + \varepsilon_{\text{SS}} + \sqrt{\gamma(\Theta | E) (2Z)^n 2^{\lambda+a+\ell}} \quad (8)$$

where in the noiseless case Z is given by $Z_0 = \left(\cos \frac{\pi}{8}\right)^2 = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.854$.

2.3 Eight-state encoding

We briefly summarise 8-state encoding as treated in [6]. A classical bit $g \in \{0, 1\}$ is encoded into a qubit state using one of four possible bases. The basis is labelled $b \in \{0, 1, 2, 3\}$, 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

$$\mathbf{n}_{uwg} = \frac{(-1)^g}{\sqrt{3}} \begin{pmatrix} (-1)^u \\ (-1)^{u+w} \\ (-1)^w \end{pmatrix}, \quad (9)$$

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

$$|\psi_{uwg}\rangle = (-1)^{gu} \left[(-\sqrt{i})^g \cos \frac{\alpha}{2} |g \oplus w\rangle + (-1)^u (\sqrt{i})^{1-g} \sin \frac{\alpha}{2} |\overline{g \oplus w}\rangle \right] \quad (10)$$

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 $|\psi_{00g}\rangle$.

2.4 QKR with eight-state encoding

We briefly review QKR based on 8-state encoding, in particular ‘scheme #2’ in [6]. This scheme is given by QENC* with the following modifications.

- The encoding is not the BB84 conjugate coding but the four-basis encoding as discussed above.
- The basis key is not chosen from a code $\mathcal{C}$, but each qubit $i \in \{1, \dots, n\}$ has its own basis key $b_i \in \{0, 1, 2, 3\}$.
- The scheme makes use of an *ordinary* Secure Sketch $S : \{0, 1\}^n \rightarrow \{0, 1\}^a$ instead of a special one. This ensures that a large amount of noise can be handled. (Asymptotically a approaches $nh(\beta)$ from above). In order to guarantee the message independence and key privacy, the sketch is protected by a one-time pad (OTP).
- The key updating procedure is slightly different. (1) The OTP protecting the sketch must always be refreshed, even if Bob Accepts. (2) In case Bob Rejects, Alice and Bob do not discard the whole basis key ($2n$ bits). Discarding n bits (in a proper way) suffices to eliminate Eve’s potential knowledge.

The key material shared between Alice and Bob consists of three parts: the basis sequence $b \in \{0, 1, 2, 3\}^n$, the MAC key k_{MAC} , the extractor key k_{ext} ⁴ 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 $z = \text{Ext}(k_{\text{ext}}, g)$. Compute the ciphertext $c = \mu \oplus z$ and authentication tag $T = M(k_{\text{MAC}}, g || c || s)$. 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

⁴ The extractor key was not mentioned explicitly in [6].

the Rec procedure of the Secure Sketch primitive). Compute $\hat{z} = \text{Ext}(k_{\text{ext}}, \hat{g})$ and $\hat{\mu} = c' \oplus \hat{z}$. Accept the message $\hat{\mu}$ if Rec succeeded and $T' = M(k_{\text{MAC}}, \hat{g} || c' || s')$. 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.⁵ 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 Our approach

Let us consider (8) with $\gamma(\Theta|E) = 2^{-n}$ and look at the $n \gg 1$ asymptotics. Asymptotically it holds that $a \rightarrow nh(\beta)$. The square root in (8) then reads $\sqrt{2^{-n} 2^{n+n \log Z} 2^{\lambda+nh(\beta)+\ell}}$. Note that Z is Eve's guessing probability in an entanglement monogamy game [18]; hence $-\log Z$ represents a min-entropy, and $1 + \log Z$ is a min-entropy loss which we will denote as $\Delta H_{\min}(\beta)$. The expression in the square root can be made arbitrarily small (by increasing n) if the following inequality is satisfied,

$$\frac{\ell}{n} < 1 - \frac{\lambda}{n} - h(\beta) - \Delta H_{\min}(\beta). \quad (11)$$

As λ is a constant, the term λ/n vanishes asymptotically. The bound (11) on the message length has a form that is of course familiar from QKD analyses: the maximum possible rate⁶ ℓ/n equals 1 minus the loss $h(\beta)$ from error correction minus the loss $\Delta H_{\min}(\beta)$ from Eve's knowledge.

The min-entropy $-\log Z_0 = -\log(\cos \frac{\pi}{8})^2$ represents Eve's ignorance about the data bit in the BB84 qubit encoding, given that Bob's measurement outcome is exactly the same as Alice's. (Noiseless case $\beta = 0$.) It also equals Eve's ignorance *about the key bit*.

Our goal is to determine the entropy loss term under more general circumstances: (1) nonzero noise; (2) six-state and eight-state encoding.

We are helped by the fact that, in this kind of analysis, it suffices to look at individual qubits instead of the whole n -qubit ensemble. The entanglement monogamy game of [18] factorises into individual qubits. Similarly, powerful proof techniques for QKD, e.g. based on quantum de Finetti [19, 20], reduce the full security analysis to an analysis of attacks on individual qubits.

A complicating factor for analysing QKR is that there is leakage not only about the message *but also about the basis key*; these two are not the same in general, and the

⁵ 'Scheme #3' in [6] greatly reduces the key material expenditure.

⁶ The *rate* is defined as the amount of message information conveyed per qubit. Classical communication is not counted. Rate larger than zero is needed in order for the quantum cryptographic scheme to be possible.

largest one determines the achievable rate ℓ/n . For attacks on the basis key, it has to be assumed that the plaintext is known to Eve.

A bound on the entropy loss can be obtained from the entanglement monogamy game applied in a noisy setting [18]. However, such results are based on a Schatten norm inequality (Lemma 2 in [18]) which is not tight. It yields an upper bound on the leakage that is independent of β , namely $1 + \log \left[\frac{1}{|\Theta|} + \frac{|\Theta|-1}{|\Theta|} \sqrt{c} \right]$, where $|\Theta|$ is the number of bases and c is a constant, where $c = \frac{1}{2}$ for 4-state and 6-state encoding, and $c = \frac{2}{3}$ for 8-state encoding. At small β , it is especially clear that this bound is far from tight, as it gives a large value for the 8-state case, while we know the 8-state leakage to be zero at $\beta = 0$.

In this paper, we determine the worst-case leakage, as a function of β , by identifying worst-case attacks. We consider the QKR scheme described in Sect. 2.4, with either 4-state, 6-state or 8-state encoding. We consider the attack categories listed below. A label ‘M’ indicates an attack on the message, and ‘K’ a known-plaintext attack on the basis key.

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 Alice–Bob bit error rate is exactly β . She does this for N transmissions ($N \gg 1$) before finally performing a joint measurement on the N ancillas associated with one qubit.

K1 Eve intercepts a fraction 3β of the qubits,⁷ does a measurement on individual qubits, and sends the resulting states on to Bob.

K2 As M2, but with a measurement that aims to get information about the basis key.

We argue that the above categories cover Eve’s most powerful attack, for the following reasons.

- In the attacks on the message, M1 represents the worst-case scenario given that Bob Rejects. M2 is the worst case given that Bob Accepts N times in a row.
- K1 and K2 are attacks that lead Bob to Accept. (Attacks that cause a Reject are not relevant, since they cause Alice and Bob to refresh the basis key.) They represent extreme cases. On the one hand, K1 performs a measurement *immediately*, with the advantage that Alice’s full quantum state is available. (But only a fraction 3β of the qubits can be scrutinised because of the noise constraint.) On the other hand, K2 maximally *postpones* measurement by drawing information into ancillas, with the advantage that information is tapped from every qubit, even in multiple rounds. (But only a limited amount of information per qubit because of the noise constraint.) Any intermediate form of POVM, e.g. using an ancilla and causing noise between β and $1/3$, interpolates between K1 and K2 in terms of information gain.
- Mixing ‘M’ and ‘K’ attacks does not give an advantage to Eve. The ‘K’ attacks assume that the plaintext is already known.

⁷ This causes overall bit error rate β .

- Applying M1 to some qubits and M2 to other qubits does not give an advantage to Eve. The effect is the average of the two. (The same applies to K1 and K2.)

Remark 1 M1 has no effect against 8-state encoding (since this encoding is a QOTP), but it will turn out to be crucially important in the case of 4-state and 6-state encoding.

Remark 2 Because of symmetry, we assume that the N -ancilla measurement in K2 can not yield more information to Eve than measurements on the N individual ancillas.

Remark 3 As we are working under assumptions, and the above arguments are informal, the analysis that follows is not a full security proof.

Our analysis contains the following steps. We take the QKR protocol with independent basis keys in each individual qubit and formulate an EPR version of the protocol (Sect. 4.1). Then we apply noise symmetrisation (Sect. 4.2), which considerably simplifies the Alice–Bob mixed two-qubit state. We purify the Alice–Bob mixed state (Sect. 4.3); the whole purification space is considered to be owned by Eve. From this purified state, we derive the mixed state ρ of Eve’s subsystem (which is coupled to the basis key and to Alice and Bob’s measurement outcome), and then we apply attacks M1, M2, K1, K2 on ρ (Sects. 5 and 6). Here the trick is to determine which POVM measurement Eve has to apply in order to maximise the leakage. We refer to these POVMs as *optimal*. (Hence the title of this paper.) Finally we determine which of the attacks M1/M2/K1/K2 causes the worst leakage and from that derive the rate ℓ/n (Sect. 7).

The security proof in [5, 18] yields a statement where leakage is expressed in terms of min-entropy loss. We too compute the min-entropy loss. In addition, we present results on the accessible information, which is of interest for a restricted class of attacks where Eve is forced (e.g. by lack of quantum memory) to immediately perform a measurement.

4 EPR formulation; noise symmetrisation; purification

Apart from QKR employing the 8-state (QOTP) encoding, we also investigate 4-state (BB84) and 6-state conjugate coding. We study optimal attacks against individual qubits, making use of the standard Shor–Preskill technique [10] and the noise symmetrisation technique introduced by Renner et al. [11].

4.1 EPR version of the QKR protocol

We follow the standard Shor–Preskill technique [10] and reformulate the QKR protocol (Sect. 2.4) 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’ system⁸ in any way,

⁸ 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.

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 if Eve has done nothing ($\beta = 0$).⁹ 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 (10). The number of bases is $|\mathcal{B}|$.

4.2 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 $\rho^{AB} \mapsto U \otimes U \rho^{AB} U^\dagger \otimes U^\dagger$ (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 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

$$\tilde{\rho}^{AB} = \left(1 - \frac{3}{2}\beta\right) |\Psi^-\rangle\langle\Psi^-| + \frac{\beta}{2} \left(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Phi^+\rangle\langle\Phi^+| \right). \quad (12)$$

Proof In [21] 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

⁹ In the singlet state the x and y are anti-correlated, i.e. $y = \bar{x}$.

the constraint $(|\psi_{bg}\rangle \otimes |\psi_{bg}\rangle)^\dagger \tilde{\rho} |\psi_{bg}\rangle \otimes |\psi_{bg}\rangle = \beta/2$ for all $b \in \mathcal{B}$, $g \in \{0, 1\}$.¹⁰ For the 6-state case, it was shown in [11] that these constraints yield (12). 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 $\lambda_1 = \lambda_2 = \lambda_3 = \frac{\beta}{2}$. $\square$

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 1 does not necessarily hold.

Also note that Lemma 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 material¹¹ in order to agree on qubit positions which they sacrifice for noise testing purposes. With Lemma 1 holding for 4-state too, we can now treat all three encoding methods on an equal footing. We will see in Sect. 7 that even with this advantage given to Alice and Bob for 4-state, the 4-state encoding still performs worst.

4.3 Purification

The $\tilde{\rho}^{AB}$ 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

$$|\Psi^{ABE}\rangle = \sqrt{1 - \frac{3}{2}\beta} |\Psi^-\rangle \otimes |m_0\rangle + \sqrt{\frac{\beta}{2}} \left(-|\Phi^-\rangle \otimes |m_1\rangle + i|\Psi^+\rangle \otimes |m_2\rangle + |\Phi^+\rangle \otimes |m_3\rangle \right). \quad (13)$$

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 $\mathbf{v} = (v_x, v_y, v_z) = (\sin \theta \cos \varphi, \sin \theta \sin \varphi, \cos \theta)$. The eigenstates of this measurement are $|\mathbf{v}\rangle = e^{-i\varphi/2} \cos \frac{\theta}{2} |0\rangle + e^{i\varphi/2} \sin \frac{\theta}{2} |1\rangle$ (with eigenvalue '0') and $|\bar{\mathbf{v}}\rangle = -e^{-i\varphi/2} \sin \frac{\theta}{2} |0\rangle + e^{i\varphi/2} \cos \frac{\theta}{2} |1\rangle$ (with eigenvalue '1').

We rewrite the state (13) using $|\mathbf{v}\rangle$, $|\bar{\mathbf{v}}\rangle$ as the basis of the A and B subsystem,

$$|\Psi^{ABE}\rangle = \sqrt{\frac{1-\beta}{2}} |\mathbf{v}\bar{\mathbf{v}}\rangle \otimes |E_{01}^v\rangle - \sqrt{\frac{1-\beta}{2}} |\bar{\mathbf{v}}\mathbf{v}\rangle \otimes |E_{10}^v\rangle + \sqrt{\frac{\beta}{2}} |\mathbf{v}\mathbf{v}\rangle \otimes |E_{00}^v\rangle - \sqrt{\frac{\beta}{2}} |\bar{\mathbf{v}}\bar{\mathbf{v}}\rangle \otimes |E_{11}^v\rangle$$

$$|E_{01}^v\rangle = \frac{1}{\sqrt{1-\beta}} \left[\sqrt{1 - \frac{3}{2}\beta} |m_0\rangle + \sqrt{\frac{\beta}{2}} (v_x |m_1\rangle + v_y |m_2\rangle + v_z |m_3\rangle) \right]$$

$$|E_{10}^v\rangle = \frac{1}{\sqrt{1-\beta}} \left[\sqrt{1 - \frac{3}{2}\beta} |m_0\rangle - \sqrt{\frac{\beta}{2}} (v_x |m_1\rangle + v_y |m_2\rangle + v_z |m_3\rangle) \right] \quad (14)$$

¹⁰ From the above constraints and $\text{tr } \tilde{\rho} = 1$ it follows that $(|\psi_{bg}\rangle \otimes |\psi_{b\bar{g}}\rangle)^\dagger \tilde{\rho} |\psi_{bg}\rangle \otimes |\psi_{b\bar{g}}\rangle = \frac{1-\beta}{2}$.

¹¹ This key has to be refreshed every time, otherwise Eve may find out which positions are test positions.

$$|E_{00}^v\rangle = \frac{1}{\sqrt{2(1-v_z^2)}} [(-v_x v_z - i v_y)|m_1\rangle + (-v_y v_z + i v_x)|m_2\rangle + (1 - v_z^2)|m_3\rangle]$$

$$|E_{11}^v\rangle = \frac{1}{\sqrt{2(1-v_z^2)}} [(-v_x v_z + i v_y)|m_1\rangle + (-v_y v_z - i v_x)|m_2\rangle + (1 - v_z^2)|m_3\rangle].$$

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.
- We have $|E_{10}^v\rangle = |E_{01}^{-v}\rangle$ and $|E_{11}^v\rangle = |E_{00}^{-v}\rangle$. Furthermore $\langle E_{00}^v | E_{11}^v \rangle = 0$, and $|E_{00}^v\rangle, |E_{11}^v\rangle$ span a subspace orthogonal to $|E_{01}^v\rangle, |E_{10}^v\rangle$. Furthermore, $\langle E_{01}^v | E_{10}^v \rangle = \frac{1-2\beta}{1-\beta}$. This structure makes it particularly easy to analyse QKD. See Sect. 5.3.1.
- It holds that $|\frac{-v_x v_z - i v_y}{\sqrt{1-v_z^2}}|^2 = 1 - v_x^2$ and $|\frac{-v_y v_z + i v_x}{\sqrt{1-v_z^2}}|^2 = 1 - v_y^2$.

In the analysis of QKD schemes, it suffices to express (14) only for a single choice of $\mathbf{v}$, because the basis is eventually revealed to Eve. In QKR, the basis is not revealed. In our treatment of known-plaintext attacks (Sect. 6), we will need to evaluate (14) for different bases.

4.4 Eve's mixed state

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

$$\rho_{xy}^v \stackrel{\text{def}}{=} |E_{xy}^v\rangle\langle E_{xy}^v|, \quad (15)$$

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,

$$\Omega^{BXYE} = \frac{1}{|\mathcal{B}|} \sum_{b \in \mathcal{B}} \mathbb{E}_{x \in \{0,1\}} \mathbb{E}_{y|x} |b\rangle\langle b| \otimes |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_{xy}^{v(b)}. \quad (16)$$

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 Sect. 6, 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,

$$\zeta_b \stackrel{\text{def}}{=} (1 - \beta)\rho_{01}^{v(b)} + \beta\rho_{00}^{v(b)}, \quad b \in \mathcal{B}. \quad (17)$$

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

5 Security of the message

Below we briefly recap the results of [6]. In Sect. 5.3, we show that the analysis of M2 reduces to the analysis of QKD.

5.1 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,

$$I_{\text{AE}}^{\text{M1,4state}} = 1 - h\left(\left[\sin \frac{\pi}{8}\right]^2\right) \approx 0.399. \quad (18)$$

The min-entropy loss per qubit is

$$\Delta H_{\min}^{\text{M1,4state}} = 1 - \log \frac{1}{(\cos \frac{\pi}{8})^2} \approx 0.772. \quad (19)$$

5.2 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

$$I_{\text{AE}}^{\text{M1,6state}} = 1 - h\left(\left[\sin \frac{\alpha}{2}\right]^2\right) \approx 0.256 \quad (20)$$

$$\Delta H_{\min}^{\text{M1,6state}} = 1 - \log \frac{1}{(\cos \frac{\alpha}{2})^2} \approx 0.658. \quad (21)$$

5.3 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 2 *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 outcome 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

$$\frac{1}{N} H(X_i^{(1)}, \dots, X_i^{(N)} | E_i^{(1)}, \dots, E_i^{(N)}) \geq H(X_i^{(j)} | B_i E_i^{(j)}) \quad j \text{ arbitrary.} \quad (22)$$

Proof Let $\mathcal{M}$ denote a POVM. We have $H(X_i | E_i) = \min_{\mathcal{M}} H(X_i | \mathcal{M}(E_i)) \geq \min_{\mathcal{M}} H(X_i | B_i \mathcal{M}(E_i)) = N \min_{\mathcal{M}} H(X_i^{(j)} | B_i \mathcal{M}(E_i^{(j)})) = NH(X_i^{(j)} | B_i E_i^{(j)})$ for arbitrary j . $\square$

For $N \gg 1$ the bound is tight. The left hand side of (22) 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 2 allows us to obtain a tight lower bound on the QKR capacity, namely the QKD capacity, whenever M2 is the dominant attack.

5.3.1 QKD, Shannon entropy

The computation of $H(X|BE)$ for BB84 and 6-state (or more) QKD is well known. Here we combine the two standard approaches: (1) the simplest possible description of the noise, i.e. noise symmetrisation, (2) 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 Sect. 8).

Informal treatment Eve knows $\mathbf{v}$. Eve does a projective measurement $|E_{00}^{\mathbf{v}}\rangle\langle E_{00}^{\mathbf{v}}| + |E_{11}^{\mathbf{v}}\rangle\langle E_{11}^{\mathbf{v}}|$. This measurement does not destroy any information. With probability β the outcome is ‘1’; next Eve can perfectly distinguish between the orthogonal states $|E_{00}^{\mathbf{v}}\rangle$, $|E_{11}^{\mathbf{v}}\rangle$ 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 $|E_{01}^{\mathbf{v}}\rangle$ and $|E_{10}^{\mathbf{v}}\rangle$, which have inner product $c \stackrel{\text{def}}{=} \langle E_{01}^{\mathbf{v}} | E_{10}^{\mathbf{v}} \rangle = \frac{1-2\beta}{1-\beta}$. This is done optimally using a projective measurement in the following orthonormal basis,

$$\begin{aligned} |\mu_{01}\rangle &= \gamma_+ |E_{01}^{\mathbf{v}}\rangle + \gamma_- |E_{10}^{\mathbf{v}}\rangle \\ |\mu_{10}\rangle &= \gamma_+ |E_{10}^{\mathbf{v}}\rangle + \gamma_- |E_{01}^{\mathbf{v}}\rangle \\ \gamma_{\pm} &= \frac{1}{2\sqrt{1+c}} \pm \frac{1}{2\sqrt{1-c}} \end{aligned} \quad (23)$$

and has error probability

$$p_{\beta} = |\langle E_{01}^{\mathbf{v}} | \mu_{10} \rangle|^2 = |\langle E_{10}^{\mathbf{v}} | \mu_{01} \rangle|^2 = \frac{1}{2} - \frac{1}{2} \sqrt{1-c^2} = \frac{1}{2} - (1-\beta)^{-1} \sqrt{\frac{\beta}{2} \left(1 - \frac{3}{2}\beta\right)}. \quad (24)$$

The channel capacity from Alice to Eve is

$$I_{AE}(\beta) = \beta \cdot [1 - h(0)] + (1 - \beta)[1 - h(p_\beta)]. \quad (25)$$

The resulting QKD rate is

$$C(\beta) = I_{AB}(\beta) - I_{AE}(\beta) = 1 - h(\beta) - I_{AE}(\beta). \quad (26)$$

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

$$\begin{aligned} H(X|\rho_{X,\bar{X} \oplus R}^v) &= \min_{\mathcal{Q}} H(X|\mathcal{Q}(\rho_{X,\bar{X} \oplus R}^v)) = \min_{\mathcal{Q}} \mathbb{E}_r H(X|\mathcal{Q}(\rho_{X,\bar{X} \oplus r}^v)) \\ &= \min_{\mathcal{Q}} \left[(1 - \beta)H(X|\mathcal{Q}(\rho_{X\bar{X}}^v)) + \beta H(X|\mathcal{Q}(\rho_{X\bar{X}}^v)) \right]. \end{aligned} \quad (27)$$

The optimal POVM is given by $\mathcal{Q}_0 = |E_{00}^v\rangle\langle E_{00}^v| + |\mu_{01}\rangle\langle\mu_{01}|$, $\mathcal{Q}_1 = |E_{11}^v\rangle\langle E_{11}^v| + |\mu_{10}\rangle\langle\mu_{10}|$. This is equivalent to the two-step procedure detailed in the informal treatment above and yields

$$H(X|\rho_{XY}^v) = (1 - \beta)h(p_\beta) + \beta \cdot 0. \quad (28)$$

Eve's knowledge about X is $I_{AE} = H(X) - H(X|\rho_{XY}^v)$, which precisely equals (25).

5.3.2 QKD, min-entropy

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

$$\begin{aligned} H_{\min}(X|\rho_{X,\bar{X} \oplus R}^v) &= -\log p_{\text{guess}}(X|\mathcal{Q}(\mathbb{E}_r \rho_{X,\bar{X} \oplus r}^v)) \\ &= -\log \mathbb{E}_r p_{\text{guess}}(X|\mathcal{Q}(\rho_{X,\bar{X} \oplus r}^v)) \\ &= -\log \left[\beta p_{\text{guess}}(X|\mathcal{Q}(\rho_{X\bar{X}}^v)) + (1 - \beta) p_{\text{guess}}(X|\mathcal{Q}(\rho_{X\bar{X}}^v)) \right] \\ &= -\log [\beta \cdot 1 + (1 - \beta)(1 - p_\beta)] \\ &= H_{\min}(X) - \log[1 + \sqrt{2}\sqrt{\beta(1 - \frac{3}{2}\beta)} + \beta]. \end{aligned} \quad (29)$$

6 Security of the key

6.1 Known-plaintext attacks on the key

In attack K1 Eve receives a state

$$\omega_{Bx} = |\psi_{Bx}\rangle\langle\psi_{Bx}| \quad (30)$$

for known x and unknown B . For attack K2 Eve's view is the mixed state ζ_B as defined in (17), for unknown B .

Lemma 3 *The Shannon entropy of B given ζ_B can be written as*

$$H(B|\zeta_B) = \log |\mathcal{B}| - \max_{\mathcal{M}} \left[h \left(\left\{ \text{tr } M_m \frac{\sum_b \zeta_b}{|\mathcal{B}|} \right\}_{m \in \mathcal{B}} \right) - \frac{1}{|\mathcal{B}|} \sum_{b \in \mathcal{B}} h(\{\text{tr } M_m \zeta_b\}_{m \in \mathcal{B}}) \right] \quad (31)$$

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

$$H(B|\zeta_B) = \min_{\text{symmetric } \mathcal{M}} \left[h(p_{\text{OK}}) + (1 - p_{\text{OK}}) \log(|\mathcal{B}| - 1) \right]. \quad (32)$$

Proof 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 $H(B|\zeta_B) = \min_{\mathcal{M}} H(B|\mathcal{M}(\zeta_B))$, with $H(B|\mathcal{M}(\zeta_B)) = \sum_m \Pr[\mathcal{M}(\zeta_B) = m] H(B|\mathcal{M}(\zeta_B) = m)$. We write $\Pr[B = b|\mathcal{M}(\zeta_B) = m] = \frac{1}{|\mathcal{B}|} [\text{tr } M_m \zeta_b] / \Pr[\mathcal{M}(\zeta_B) = m]$ and $\Pr[\mathcal{M}(\zeta_B) = m] = \frac{1}{|\mathcal{B}|} \sum_b \text{tr } M_m \zeta_b$. After some manipulation (31) follows. In the first $h(\dots)$ of (31) we then write $\frac{1}{|\mathcal{B}|} \sum_b \text{tr } \zeta_b M_m = \frac{1}{|\mathcal{B}|} [p_{\text{OK}} + (|\mathcal{B}| - 1) \frac{1-p_{\text{OK}}}{|\mathcal{B}|-1}] = \frac{1}{|\mathcal{B}|}$. The $h(\frac{1}{|\mathcal{B}|})$ cancels the $\log |\mathcal{B}|$. The second $h(\dots)$ in (31) is the same for all $b \in \mathcal{B}$, namely $h(\{p_{\text{OK}}, \frac{1-p_{\text{OK}}}{|\mathcal{B}|-1}, \dots, \frac{1-p_{\text{OK}}}{|\mathcal{B}|-1}\}) = -p_{\text{OK}} \log p_{\text{OK}} - (|\mathcal{B}| - 1) \cdot \frac{1-p_{\text{OK}}}{|\mathcal{B}|-1} \log \frac{1-p_{\text{OK}}}{|\mathcal{B}|-1} = h(p_{\text{OK}}) + (1 - p_{\text{OK}}) \log(|\mathcal{B}| - 1)$. $\square$

6.2 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

$$H(B) - H(B|X, \omega_{BX}) = 1 - h\left(\left[\sin \frac{\pi}{8}\right]^2\right) \approx 0.399 \quad (33)$$

$$H_{\min}(B) - H_{\min}(B|X, \omega_{BX}) = 1 - \log \frac{1}{\left(\cos \frac{\pi}{8}\right)^2} \approx 0.772. \quad (34)$$

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

6.3 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 $M_b = \frac{1}{3}\mathbb{1} - \frac{1}{3}\mathbf{n}_b \cdot \boldsymbol{\sigma}$, with $\mathbf{n}_1 = (-2, 1, 1)^T/\sqrt{6}$, $\mathbf{n}_2 = (1, -2, 1)^T/\sqrt{6}$, $\mathbf{n}_3 = (1, 1, -2)^T/\sqrt{6}$. It yields the following probability distribution for B : $\{\frac{1}{3} + \frac{2}{3\sqrt{6}}, \frac{1}{3} - \frac{1}{3\sqrt{6}}, \frac{1}{3} - \frac{1}{3\sqrt{6}}\}$.

$$H_{\min}(B) - H_{\min}(B|X, \omega_{BX}) = \log 3 + \log\left(\frac{1}{3} + \frac{2}{3\sqrt{6}}\right) \approx 0.861. \quad (35)$$

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

$$H(B) - H(B|X, \omega_{BX}) = \log 3 - h\left(\left\{\frac{1}{3} + \frac{1}{3\sqrt{6}}, \frac{1}{3} + \frac{1}{3\sqrt{6}}, \frac{1}{3} - \frac{2}{3\sqrt{6}}\right\}\right) \approx 0.314. \quad (36)$$

The effect on the whole n -bit string is obtained by multiplying (35,36) times $3\beta n$.

6.4 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 $\{0, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}\}$.

$$H_{\min}(B) - H_{\min}(B|X, \omega_{BX}) = 2 - 1 = 1 \quad (37)$$

$$H(B) - H(B|X, \omega_{BX}) = 2 - \log 3 \approx 0.415. \quad (38)$$

The effect on the whole n -bit string is obtained by multiplying (37,38) times $3\beta n$.

6.5 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 2 *In the case of 4-state encoding, the min-entropy of the basis B given the mixed state ζ_B is*

$$H_{\min}(B|\zeta_B) = H_{\min}(B) - \log(1 + \sqrt{\beta(1 - \frac{3}{2}\beta)} + \frac{\beta}{\sqrt{2}}). \quad (39)$$

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

$$M_0 = |\gamma_1\rangle\langle\gamma_1| + |\gamma_2\rangle\langle\gamma_2| \quad ; \quad M_1 = |\gamma_3\rangle\langle\gamma_3| + |\gamma_4\rangle\langle\gamma_4| \quad (40)$$

$$\begin{aligned} |\gamma_1\rangle &= \frac{|m_0\rangle}{\sqrt{2}} + \frac{|m_3\rangle - |m_1\rangle}{2} \quad ; \quad |\gamma_3\rangle = \frac{|m_0\rangle}{\sqrt{2}} - \frac{|m_3\rangle - |m_1\rangle}{2} \\ |\gamma_2\rangle &= \frac{|m_2\rangle}{\sqrt{2}} + i \frac{|m_1\rangle + |m_3\rangle}{2} \quad ; \quad |\gamma_4\rangle = \frac{|m_2\rangle}{\sqrt{2}} - i \frac{|m_1\rangle + |m_3\rangle}{2}. \end{aligned} \quad (41)$$

Proof We have

$$\begin{aligned} |E_{01}^{(0,0,1)}\rangle &= \frac{\sqrt{1 - \frac{3}{2}\beta}|m_0\rangle + \sqrt{\frac{\beta}{2}}|m_3\rangle}{\sqrt{1 - \beta}} \quad ; \quad |E_{01}^{(1,0,0)}\rangle = \frac{\sqrt{1 - \frac{3}{2}\beta}|m_0\rangle + \sqrt{\frac{\beta}{2}}|m_1\rangle}{\sqrt{1 - \beta}} \\ |E_{00}^{(0,0,1)}\rangle &\propto \frac{|m_1\rangle - i|m_2\rangle}{\sqrt{2}} \quad ; \quad |E_{00}^{(1,0,0)}\rangle = \frac{i|m_2\rangle + |m_3\rangle}{\sqrt{2}} \end{aligned} \quad (42)$$

$$\zeta_0 - \zeta_1 = \sqrt{\beta(1 - \frac{3}{2}\beta)} \left[|m_0\rangle \frac{\langle m_3| - \langle m_1|}{\sqrt{2}} + \text{h.c.} \right] + \frac{\beta}{\sqrt{2}} \left[-i|m_2\rangle \frac{\langle m_1| + \langle m_3|}{\sqrt{2}} + \text{h.c.} \right]. \quad (43)$$

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 $p_0 = p_1 = \frac{1}{2}$. $\square$

Theorem 3 *In the case of 4-state encoding, the Shannon entropy of the basis B given the mixed state ζ_B is*

$$H(B|\zeta_B) = h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\beta(1 - \frac{3}{2}\beta)} + \frac{\beta}{2\sqrt{2}}\right). \quad (44)$$

Proof For binary B , the POVM associated with the min-entropy maximises $\text{tr } M_0(\zeta_0 - \zeta_1)$ (see Sect. 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 Sect. 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 2 to (32) yields (44). $\square$

6.6 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

$$S \stackrel{\text{def}}{=} |m_0\rangle\langle m_0| + |m_2\rangle\langle m_1| + |m_3\rangle\langle m_2| + |m_1\rangle\langle m_3|. \quad (45)$$

Theorem 4 *In the case of 6-state encoding, the min-entropy of the basis B given the mixed state ζ_B is*

$$H_{\min}(B|\zeta_B) = H_{\min}(B) - \log \left(1 + \frac{2\sqrt{2}}{\sqrt{3}} \sqrt{\beta(1-\beta)} \right). \quad (46)$$

The associated POVM is

$$M_3 = \frac{3-4\beta}{3(1-\beta)} |q\rangle\langle q| + \frac{1}{3(1-\beta)} |r\rangle\langle r| \quad (47)$$

$$|q\rangle = -\sqrt{\frac{1-\beta}{3-4\beta}} |m_0\rangle + \frac{\sqrt{2-3\beta}}{\sqrt{3-4\beta}} \frac{|m_1\rangle + |m_2\rangle - 2|m_3\rangle}{\sqrt{6}} \quad (48)$$

$$|r\rangle = \sqrt{1-\beta} \frac{|m_1\rangle + |m_2\rangle + |m_3\rangle}{\sqrt{3}} + i\sqrt{\beta} \frac{|m_1\rangle - |m_2\rangle}{\sqrt{2}} \quad (49)$$

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

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

$$\begin{aligned} \zeta_b = & (1 - \tfrac{3}{2}\beta) |m_0\rangle\langle m_0| + \tfrac{\beta}{2} (|m_1\rangle\langle m_1| + |m_2\rangle\langle m_2| + |m_3\rangle\langle m_3|) \\ & + \sqrt{\tfrac{\beta}{2} (1 - \tfrac{3}{2}\beta)} (|m_0\rangle\langle m_b| + \text{h.c.}) + \tfrac{\beta}{2} (i|m_{b+1}\rangle\langle m_{b+2}| + \text{h.c.}) \end{aligned} \quad (50)$$

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

$$\begin{aligned} \Lambda = \sum_b \zeta_b M_b = & (1 - \tfrac{3}{2}\beta) \left(1 + \frac{2\sqrt{\beta}}{\sqrt{6}\sqrt{1-\beta}} \right) |m_0\rangle\langle m_0| \\ & + \left(\frac{1}{2} + \frac{(2-\beta)\sqrt{\beta}}{3\sqrt{6}\sqrt{1-\beta}} \right) \sum_{j=1}^3 |m_j\rangle\langle m_j| + \frac{\sqrt{2}}{6} \sqrt{\beta(1-\beta)} \left[\sum_{j=1}^3 |m_0\rangle\langle m_j| + \text{h.c.} \right] \\ & + \left[\left(\frac{-i\beta}{2} - \frac{(1-2\beta)\sqrt{\beta}}{3\sqrt{6}\sqrt{1-\beta}} \right) \sum_{j=1}^3 |m_{j+1}\rangle\langle m_j| + \text{h.c.} \right]. \end{aligned} \quad (51)$$

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

Conjecture 1 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

$$Q_3 = \frac{3-4\beta}{3(1-\beta)} |q'\rangle\langle q'| + \frac{1}{3(1-\beta)} |r'\rangle\langle r'| \quad (52)$$

$$|q'\rangle = \sqrt{\frac{1-\beta}{3-4\beta}} |m_0\rangle + \frac{\sqrt{2-3\beta}}{\sqrt{3-4\beta}} \frac{|m_1\rangle + |m_2\rangle - 2|m_3\rangle}{\sqrt{6}} \quad (53)$$

$$|r'\rangle = |r\rangle^* \quad (54)$$

with $|r\rangle$ as defined by (49), 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 $\mathbf{v}$ replaced by $-\mathbf{v}$. (This fact is not immediately evident. One can also take $\mathcal{M}$ and apply it to the state ζ_B with $\mathbf{v} \rightarrow -\mathbf{v}$; this is equivalent). It was noticed in [6] that such a ‘dual’ is the optimal POVM in the case of the intercept attack K1. Numerical optimisation by semidefinite programming [22, 23] confirms (52). We have performed additional numerics 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.¹² 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 $\mathcal{M}$. $\square$

Theorem 5 In case of the measurement $\mathcal{Q}$ specified in Conjecture 1, the entropy of B is

$$H(B|\mathcal{Q}(\zeta_B)) = h(p_6) + 1 - p_6 \quad (55)$$

$$p_6 \stackrel{\text{def}}{=} \frac{1}{3} - \frac{2\sqrt{2}}{3\sqrt{3}} \sqrt{\beta(1-\beta)}. \quad (56)$$

Proof After some algebra, it can be seen that $\text{tr } \zeta_3 Q_3 = p_6$. We apply (32) from Lemma 3. $\square$

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

6.7 Attack K2, 8-state

Theorem 6 Let $\beta \leq \frac{1}{3}$. In the 8-state case, the min-entropy of B given the mixed state ζ_B is

$$H_{\min}(B|\zeta_B) = H_{\min}(B) - \log \left(1 + \sqrt{6} \sqrt{\beta \left(1 - \frac{3}{2}\beta \right)} \right). \quad (57)$$

¹² Imposing symmetry is allowed, see Sect. 2.1.

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

$$M_{00} = \frac{\sum_{a=0}^3 |m_a\rangle \sum_{a'=0}^3 \langle m_{a'}|}{2} \quad ; \quad M_{01} = (\sigma_z \otimes \mathbb{1}) M_{00} (\sigma_z \otimes \mathbb{1}) \quad (58)$$

$$M_{10} = (\sigma_z \otimes \sigma_z) M_{00} (\sigma_z \otimes \sigma_z) \quad ; \quad M_{11} = (\mathbb{1} \otimes \sigma_z) M_{00} (\mathbb{1} \otimes \sigma_z). \quad (59)$$

Proof The states ζ_{uw} are given by

$$\begin{aligned} \zeta_{00} = & \left(1 - \frac{3}{2}\beta\right) |m_0\rangle \langle m_0| + \frac{\beta}{2} \sum_{j=1}^3 |m_j\rangle \langle m_j| \\ & + \sqrt{\frac{\beta}{2} \left(1 - \frac{3}{2}\beta\right)} \left[|m_0\rangle \frac{\langle m_1| + \langle m_2| + \langle m_3|}{\sqrt{3}} + \text{h.c.} \right] + \frac{\beta}{2\sqrt{3}} \left[i \sum_{j=1}^3 |m_j\rangle \langle m_{j+1}| + \text{h.c.} \right] \end{aligned} \quad (60)$$

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,

$$\begin{aligned} \Lambda = & \sum_{uw} \zeta_{uw} M_{uw} \\ = & \left(1 - \frac{3}{2}\beta + \sqrt{3} \sqrt{\frac{\beta}{2} \left(1 - \frac{3}{2}\beta\right)}\right) |m_0\rangle \langle m_0| + \left(\frac{\beta}{2} + \frac{\sqrt{\frac{\beta}{2} \left(1 - \frac{3}{2}\beta\right)}}{\sqrt{3}}\right) \sum_{j=1}^3 |m_j\rangle \langle m_j|. \end{aligned} \quad (61)$$

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

$$\text{tr } \Lambda = 1 + \sqrt{6} \sqrt{\beta \left(1 - \frac{3}{2}\beta\right)}. \quad (62)$$

□

Conjecture 2 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

$$R_{00} = |v\rangle \langle v|, \quad |v\rangle = \frac{|m_0\rangle - |m_1\rangle - |m_2\rangle - |m_3\rangle}{2} \quad (63)$$

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' ($v \rightarrow -v$) of the POVM associated with the min-entropy. Numerical solution by semidefinite programming confirms the above conjecture. Additional 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 7 *In case of the measurement $\mathcal{R}$ specified in Conjecture 2, the entropy of B is*

$$H(B|\mathcal{R}(\zeta_B)) = h(p_8) + (1 - p_8) \log 3 \quad (64)$$

$$p_8 \stackrel{\text{def}}{=} \frac{1}{4} - \frac{\sqrt{3}}{2\sqrt{2}} \sqrt{\beta \left(1 - \frac{3}{2}\beta\right)}. \quad (65)$$

Proof A brief calculation gives $\text{tr } \zeta_{uw} R_{uw} = p_8$ (for all u, w) with p_8 as defined in (65). Then we use (32). $\square$

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

7 Putting it all together

The amount of privacy amplification needed in the protocol is determined by the *strongest* of the M1, M2, K1, K2 attacks. Below we combine all the results from Sects. 5 and 6.

7.1 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. Figure 2 shows the QKR rate $1 - h(\beta) - I(\beta)$.

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 rate of 4-state encoding is always below 6-state. 8-state has higher rate 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 ‘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.

7.2 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. Figure 4 shows the QKR rate $1 - h(\beta) - \Delta H_{\min}(\beta)$. 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 rate is computed using min-entropy loss as the measure of Eve’s knowledge, then the QKR rate of 8-state is higher than 6-state on the range $\beta \in$

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

	4-State	6-State	8-State
<i>Shannon entropy leakage $I(\beta)$ per qubit</i>			
M1	0.399	0.256	0
M2	$\beta \cdot 1 + (1 - \beta)[1 - h(p\beta)]$, with $p\beta = \frac{1}{2} - \frac{\sqrt{\frac{\beta}{2}(1 - \frac{3}{2}\beta)}}{1 - \beta}$		
K1	$3\beta \cdot 0.399$	$3\beta \cdot 0.314$	$3\beta \cdot 0.415$
K2	$1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\beta\left(1 - \frac{3}{2}\beta\right) + \frac{\beta}{2\sqrt{2}}}\right)$	$\log 3 - [h(p_6) + 1 - p_6]$	$2 - [h(p_8) + (1 - p_8) \log 3]$
		$p_6 = \frac{1}{3} - \frac{2\sqrt{2}}{3\sqrt{3}}\sqrt{\beta(1 - \beta)}$	$p_8 = \frac{1}{4} - \frac{\sqrt{6}}{4}\sqrt{\beta\left(1 - \frac{3}{2}\beta\right)}$

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

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

$[0, 0.0612]$. There is a tiny interval $\beta \in (0.0612, 0.0638]$ where 6-state outperforms 8-state; at $\beta > 0.0638$ all rates are zero. 4-state is always worse than 6-state.

8 Addition of artificial noise

The structure evident in the $|E_{xy}^v\rangle$ vectors (14) allows us to simplify the derivation of the key rate 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,

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

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

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

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 $\varepsilon \star \beta \stackrel{\text{def}}{=} \varepsilon(1 - \beta) + (1 - \varepsilon)\beta$ 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 $I'_{AB}(\varepsilon, \beta) = 1 - h(\varepsilon \star \beta)$. Eve's task of distinguishing between the various $|E^v\rangle$ states is not affected; the weights β and $1 - \beta$ in (25) 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 $\varepsilon \star p_\beta$. Thus, the channel from Alice to Eve now has capacity

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

Fig. 5 Left: the capacity $C(\beta)$ without artificial noise and the capacity $C_{\text{opt}} = C'(\epsilon_{\text{opt}}(\beta), \beta)$ 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)

$I'_{\text{AE}}(\epsilon, \beta) = \beta[1 - h(\epsilon)] + (1 - \beta)[1 - h(\epsilon \star p_\beta)]$, with p_β as defined in (24). The rate is

$$\begin{aligned} C'(\epsilon, \beta) &= I'_{\text{AB}} - I'_{\text{AE}} = 1 - h(\epsilon \star \beta) - \left\{ \beta[1 - h(\epsilon)] + (1 - \beta)[1 - h(\epsilon \star p_\beta)] \right\} \\ &= (1 - \beta)h(\epsilon \star p_\beta) + \beta h(\epsilon) - h(\epsilon \star \beta) \end{aligned} \quad (66)$$

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

9 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. Figures 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.

From our results, we conclude that 8-state encoding yields the highest QKR rate under practically all circumstances. As topics for future work we see (1) A more formal treatment of the security arguments in Sect. 3. (2) 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. (3) Determine the effect of artificial noise on the min-entropy loss in the case of the K2 attack on 8-state encoding. (4) Determine how tight the bound in Lemma 2 (M2 reduces to QKD analysis) is as a function of N .

Acknowledgements We thank Serge Fehr for useful discussions. Part of this research was funded by NWO (Grant No. 651.002.003) (CHIST-ERA Project ID_IOT).

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

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 Sect. 7.1, the K1 attack needs some interpreting at $\beta > \frac{1}{3}$: Eve does 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 (39) and (47,52), 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 8 *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*

$$H_{\min}(B|\zeta_B) = H_{\min}(B) - 1 = 1. \quad (67)$$

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

Fig. 6 Shannon leakage $I(\beta)$ (accessible information) 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

$$M_{00} = \frac{1-\beta}{2\beta} |a\rangle\langle a| + \frac{3\beta-1}{2\beta} |d\rangle\langle d| \quad (68)$$

$$|a\rangle = \frac{\sqrt{\beta/2}}{\sqrt{1-\beta}} |m_0\rangle + \frac{\sqrt{1-\frac{3}{2}\beta}}{\sqrt{1-\beta}} \cdot \frac{|m_1\rangle + |m_2\rangle + |m_3\rangle}{\sqrt{3}} \quad (69)$$

$$|d\rangle = \frac{e^{i\pi/3}|m_1\rangle + e^{-i\pi/3}|m_2\rangle - |m_3\rangle}{\sqrt{3}} \quad (70)$$

$$\begin{aligned} M_{01} &= (\sigma_z \otimes \mathbb{1}) M_{00} (\sigma_z \otimes \mathbb{1}) \quad ; \quad M_{10} = (\sigma_z \otimes \sigma_z) M_{00} (\sigma_z \otimes \sigma_z) ; \\ M_{11} &= (\mathbb{1} \otimes \sigma_z) M_{00} (\mathbb{1} \otimes \sigma_z). \end{aligned} \quad (71)$$

Proof After some algebra it turns out that the matrix Λ has a simple diagonal form,

$$\Lambda = \sum_{uw} \zeta_{uw} M_{uw} = (2-3\beta) |m_0\rangle\langle m_0| + \beta \sum_{j=1}^3 |m_j\rangle\langle m_j|. \quad (72)$$

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

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

Lemma 4 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

$$R_{00} = \frac{1-\beta}{2\beta} |a'\rangle\langle a'| + \frac{3\beta-1}{2\beta} |d'\rangle\langle d'| \quad (73)$$

$$|a'\rangle = -\frac{\sqrt{\beta/2}}{\sqrt{1-\beta}} |m_0\rangle + \frac{\sqrt{1-\frac{3}{2}\beta}}{\sqrt{1-\beta}} \cdot \frac{|m_1\rangle + |m_2\rangle + |m_3\rangle}{\sqrt{3}} \quad (74)$$

$$|d'\rangle = |d\rangle^* \quad (75)$$

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 $H(B|\mathcal{R}(\zeta_B)) = \log 3$, which is the K1 result at $\beta = \frac{1}{3}$ and therefore, the minimum possible value. $\square$

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' ($\mathbf{v} \rightarrow -\mathbf{v}$) 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.

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

References

1. Bennett, C.H., Brassard, G., Breidbart, S.: Quantum Cryptography II: How to re-use a one-time pad safely even if $P = NP$. *Nat. Comput.* **13**, 453–458, 2014 (**Original manuscript 1982**)
2. Gottesman, D.: Unccloneable encryption. *Quantum Inf. Comput.* **3**(6), 581–602 (2003)
3. Damgård, I.B., Pedersen, T.B., Salvail, L.: A quantum cipher with near optimal key-recycling. In: *CRYPTO*, pp. 494–510 (2005)
4. Damgård, I.B., Pedersen, T.B., Salvail, L.: How to re-use a one-time pad safely and almost optimally even if $P = NP$. *Nat. Comput.* **13**(4), 469–486 (2014)
5. Fehr, S., Salvail, L.: Quantum authentication and encryption with key recycling. In: *Eurocrypt* (2017). [arxiv:1610.05614v1](https://arxiv.org/abs/1610.05614v1)
6. Škorić, B., de Vries, M.: Quantum Key Recycling with eight-state encoding (The Quantum One Time Pad is more interesting than we thought). *Int. J. Quantum Inf.* (2017) <https://eprint.iacr.org/2016/1122>
7. Ambainis, A., Mosca, M., Tapp, A., de Wolf, R.: Private quantum channels. In: *Annual Symposium on Foundations of Computer Science*, pp. 547–553 (2000)
8. Leung, D.W.: Quantum Vernam cipher. *Quantum Inf. Comput.* **2**(1), 14–34 (2002)
9. Boykin, P.O., Roychowdhury, V.: Optimal encryption of quantum bits. *Phys. Rev. A* **67**(4), 042317 (2003)
10. Shor, P., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441 (2000)
11. Renner, R., Gisin, N., Kraus, B.: Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A* **72**, 012332 (2005)
12. Bruß, D.: Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **81**(14), 3018–3021 (1998)
13. Holevo, A.S.: Statistical decision theory for quantum systems. *J. Multivar. Anal.* **3**, 337–394 (1973)
14. Shadman, Z., Kampermann, H., Meyer, T., Bruß, D.: Optimal eavesdropping on noisy states in quantum key distribution. *Int. J. Quantum Inf.* **07**(01), 297 (2009)
15. König, R., Renner, R., Schaffner, C.: The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Theory* **55**(9), 4337–4347 (2009)
16. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.: Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.* **38**(1), 97–139 (2008)
17. Dodis, Y., Smith, A.: Correcting errors without leaking partial information. In: *ACM STOC*, pp. 654–663 (2005)
18. Tomamichel, M., Fehr, S., Kaniewski, J., Wehner, S.: One-sided device-independent QKD and position-based cryptography from monogamy games. In: *EUROCRYPT 2013*, volume 7881 of LNCS, pp. 609–625 (2013)
19. Renner, R.: Symmetry of large physical systems implies independence of subsystems. *Nat. Phys.* **3**, 645–649 (2007)
20. Christandl, M., König, R., Mitchison, G., Renner, R.: One-and-a-half quantum de Finetti theorems. *Commun. Math. Phys.* **273**(2), 473–498 (2007)
21. Renner, R.: Security of quantum key distribution. PhD thesis, ETH Zürich (2005)
22. Grant, M., Boyd, S.: CVX: Matlab software for disciplined convex programming, version 2.0 beta (2013). <http://cvxr.com/cvx>
23. Grant, M., Boyd, S.: Graph implementations for nonsmooth convex programs. *Recent Advances in Learning and Control (A Tribute to M. Vidyasagar)*, *Lecture Notes in Control and Information Sciences*, pp. 95–110. Springer, Berlin (2008)