

IMPROVED ONE-WAY RATES FOR BB84 AND 6-STATE PROTOCOLS

OLIVER KERN JOSEPH M. RENES

*Institut für Angewandte Physik, Technische Universität Darmstadt
64289 Darmstadt, Germany*

Received December 21, 2007

Revised March 4, 2008

We study the advantages to be gained in quantum key distribution (QKD) protocols by combining the techniques of local randomization, or noisy preprocessing, and structured (nonrandom) block codes. Extending the results of [Smith, Renes, and Smolin, *Physical Review Letters*, 100:170502] pertaining to BB84, we improve the best-known lower bound on the error rate for the 6-state protocol from 14.11% for local randomization alone to at least 14.59%. Additionally, we also study the effects of iterating the combined preprocessing scheme and find further improvements to the BB84 protocol already at small block lengths.

Keywords:

Communicated by: H-K Lo & H Zbinden

1 Introduction

Using a quantum channel to create a secret key between two parties is closely related to using the channel to send quantum information, with many results found in one area applicable in the other. For instance, by treating the steps in a quantum key distribution (QKD) protocol coherently and viewing the entire process as an entanglement distillation scheme, one can use properties of random quantum error-correcting codes to prove the security of the BB84 [1] and 6-state [2] protocols up to bit error rates of $p_{max} = 11.0028\%$ [3] and $p_{max} = 12.6193\%$ [4], respectively. Conversely, the formula for the quantum channel capacity can be obtained by importing the key rate resulting from a general approach to secret key generation over a known channel [5, 6, 7].

One of the surprising results related to quantum capacity is the non-optimality of random codes, in contrast to the classical case. The classical capacity of a channel can be achieved by using randomly-constructed block codes, and the independence of one input to the channel from the next results in a so-called single-letter formula for the capacity. Random coding can be used to create quantum error-correcting codes as well, but these do not always achieve the capacity. Better performance can be achieved by structured codes which exploit the ability of quantum error-correcting codes to correct errors without precisely identifying them, a property called degeneracy. Initial results on rates achievable with degenerate codes displayed only modest gains [8, 9], but recent analysis shows that degeneracy is crucial to the behavior of optimal codes [10].

By appealing to the coherent formulation of the protocol, degenerate codes should also

be useful in QKD. This was shown to be the case in the original security proof of the 6-state protocol [4], as the results of [9] were used to improve the error rate threshold to $p_{max} = 12.6904\%$. More striking threshold improvements are possible, if counterintuitive, by simply adding noise to the raw key bits before they are processed into the final key, a procedure known as local randomization [11, 12]. This improves the error rate thresholds for the two protocols to $p_{max} = 12.4120\%$ and $p_{max} = 14.1119\%$, respectively. At first glance, these results make no sense in the coherent picture of QKD, since adding more noise to already noisy entangled pairs only decreases the amount of pure entanglement which can be extracted. The entanglement/secret-key analogy does not hold perfectly, however; entangled states are sufficient, but not necessary, for creation of secret keys. A broader class of states, called private states, lead to secret keys when measured [13], and these should properly be the target output of the coherent version of the QKD protocol. Indeed, the exact error thresholds are recovered in the coherent picture when the QKD protocols with local randomization are analyzed in these terms [14].

With a systematic understanding of how degenerate codes and local randomization boost the key rate, it becomes sensible to combine the two methods to look for even higher thresholds. Recently it was shown in [15] that doing so improves the error threshold of the BB84 protocol up to at least $p_{max} \approx 12.92\%$ by using the same type of structured code studied in [8, 9, 10]. These specific codes consist of the concatenation of two codes, the first a simple repetition code and the second a random code. The repetition code, sometimes called a cat code in the context of quantum information theory since the codewords are $|0\rangle^{\otimes m}$ and $|1\rangle^{\otimes m}$, induces degeneracy in the overall code since a phase flip on any of the physical qubits leads to the same logical error, and is corrected in the same way. In particular, blocklength $m = 400$ corresponds to the threshold stated above. Since the random code portion of the protocol corresponds to information reconciliation and privacy amplification in the classical view, the local randomization and the repetition code together become a type of *preprocessing* performed before these “usual” steps. In this paper we show that the same preprocessing protocol as used in [15] can also be used to improve the maximum tolerable bit error rate for the 6-state protocol, up to at least $p_{max} = 14.5930\%$ for a blocksize of $m = 300$. This is already quite close to the upper bound of 14.6447% [16, 11, 17] on the tolerable error rate for the BB84 protocol, and since the error threshold grows with blocklength, the bound is presumably exceeded at larger blocklengths, indicating the higher robustness of the 6-state protocol. In addition we investigate iterating the preprocessing scheme in the BB84 protocol, and show an improvement both in rate and error threshold over single-round preprocessing for even modest blocklengths. Our calculations are facilitated by a closer look at the representation theory relevant to describing the quantum states resulting from the preprocessing, enabling us to continue the investigation started in [15] to the 6-state protocol and iterated versions of the preprocessing for BB84.

To begin, section II describes the preprocessing scheme in more depth and then derives secret key rate expressions for the BB84 and the 6-state protocols. Numerical calculations for blocklengths into the hundreds are then presented for the two protocols. Section III examines the advantages of iterating the preprocessing protocol to achieve higher rates and thresholds for the same amount of effort in noise addition and block coding. The appendix explains how representation theory is helpful for the numerical evaluation of such key rates in both cases.

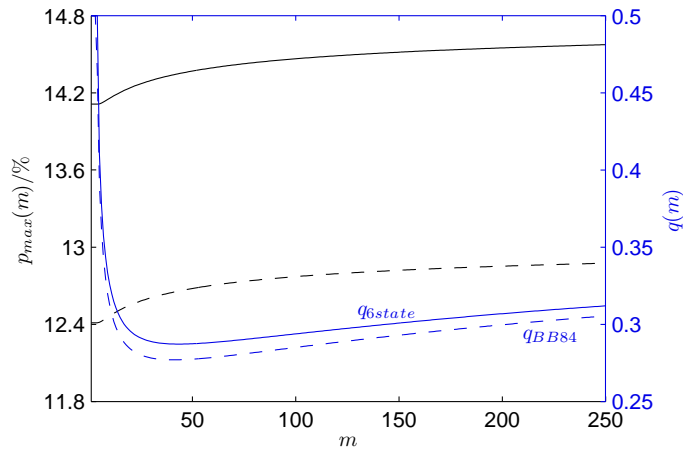


Fig. 1. Maximum tolerable bit error rate p_{max} (left y-axis, black) and the corresponding rate q of the added noise for which it is achieved (right y-axis, blue) versus block length m . Dashed lines correspond to the BB84 protocol, solid lines to the 6-state protocol.

2 Secure key rates using the preprocessing protocol

The preprocessing protocol proposed in [15] begins after Bob has received the quantum signals from Alice and they have sifted their raw keys to throw out mismatches between the preparation and measurement basis. Alice then flips each of her sifted key bits (x_1, \dots, x_n) with probability q , resulting in new bits $(\tilde{x}_1, \dots, \tilde{x}_n)$. These are partitioned into blocks of size m , and for each block she computes the syndrome $(\tilde{x}_1 \oplus \tilde{x}_2, \tilde{x}_1 \oplus \tilde{x}_3, \dots, \tilde{x}_1 \oplus \tilde{x}_m)$ and sends this information to Bob. He computes the *relative* syndrome of their blocks by adding his corresponding syndrome to Alice's, modulo two. Alice's message is public knowledge, but the first bit of each block is still secret, so it is kept as a potential key bit. The protocol then proceeds with the usual error correction and privacy amplification steps to transform these kept bits into a secret key, now aided by the relative syndrome of each block and knowledge of the probability q of local randomization. Without local randomization, it turns out that $m = 5$ is the optimal blocklength for improving the error threshold in the 6-state protocol—longer blocklengths have worse thresholds [4]. However, the results in [15] indicate that with the addition of noise, the highest tolerable bit error rate of BB84 grows with the blocksize m , and we find a similar result in the 6-state case (see figure 1).

We determine the secure key rates of the BB84 and 6-state one-way key distillation protocols involving the preprocessing protocol described above using the security proof of Renner [18]. This proof states that the key rate of such a protocol is given by

$$r = \frac{1}{m} \min_{\sigma_{AB} \in \Gamma} (S(X|E) - S(X|Y)) \quad (1)$$

where the minimum ranges over the set of states Γ of all density operators on the 2×2 dimensional Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ such that the measurement performed during the parameter estimation phase of the protocol leads to a certain bit error rate p . The conditional von

Neumann entropies in (1) are calculated for the states

$$\sigma_{XY\bar{E}} = \mathcal{E}_{XY\bar{E} \leftarrow A^m B^m E^m}(\sigma_{ABE}^{\otimes m}) \tag{2}$$

which describe the processing of each block, including local randomization and syndrome calculation, and eventual measurement of the output qubits of the repetition code. That is, the preprocessing is treated quantum-mechanically or coherently, but the usual processing classically. Here X denotes Alice’s key outcome when measuring the output bits and Y Bob’s key and syndrome outcomes.

For the BB84 protocol the set Γ contains the states

$$\sigma_{AB} = \sum_{u,v} p_{uv} X_B^u Z_B^v |\Phi^+\rangle\langle\Phi^+| Z_B^v X_B^u, \tag{3}$$

where $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}} \sum_k |kk\rangle_{AB}$ and $\{p_{uv}\} \equiv \{p_{00}, p_{10}, p_{11}, p_{01}\} = \{1 - 2p + t, p - t, t, p - t\}$, $t \in [0, p]$. In the 6-state protocol, meanwhile, parameter estimation assures us that Γ contains only the single state σ_{AB} with $\{p_{uv}\} = \{1 - \frac{3}{2}p, \frac{p}{2}, \frac{p}{2}, \frac{p}{2}\}$.

Using Renner’s proof allows us to include the preprocessing but still only minimize over the quantum states σ corresponding to individual signals. The crucial simplification is that the quantum state of the block can be taken to be the product $\sigma^{\otimes m}$ without loss of generality. Other proof techniques would require minimization over all possible (potentially-entangled) block states, or an additional step in the parameter estimation procedure to ensure that the state does have this power form.

2.1 Computation of the secure key rate

To compute the secure key rates we make use of the fact that the difference of entropies in (1) can also be written as difference of corresponding quantum mutual informations, i. e. $S(X|E) - S(X|Y) = I(X : Y) - I(X : E)$. In order to calculate these quantities, we need to determine the states $\sigma_{XY\bar{E}}$ defined in (2). Start with an m -fold tensor product of a purification of σ_{AB} ,

$$|\sigma\rangle_{ABE} \equiv |\sigma\rangle_{ABE_1 E_2}^{\otimes m} = \sum_{\vec{u}, \vec{v}} \sqrt{p_{\vec{u}, \vec{v}}} X_B^{\vec{u}} Z_B^{\vec{v}} |\Phi^+\rangle_{AB}^{\otimes m} |\vec{u}\rangle_{E_1} |\vec{v}\rangle_{E_2}, \tag{4}$$

where $\vec{u}, \vec{v} \in \{0, 1\}^m = \mathbb{F}^m$ so that $X^{\vec{u}} = X^{u_1} \otimes X^{u_2} \otimes \dots$, and similarly for $Z^{\vec{v}}$ and $p_{\vec{u}, \vec{v}}$. We now need to calculate the state resulting from noisy preprocessing followed by a blockwise stabilizer code measurement in which the stabilizers contain Pauli $\mathbb{1}$ and Z operators only.

The first step, local randomization, can be described in a coherent way by adding a classical register \mathbf{A}' (such systems will be denoted with boldface type) in the state $((1 - q)|0\rangle\langle 0| + q|1\rangle\langle 1|)^{\otimes m}$ and then applying controlled not gates from the individual register states to the bits A . This leads to

$$|\sigma'\rangle_{ABE} = \sum_{\vec{u}, \vec{v}, \vec{f}} \sqrt{p_{\vec{u}, \vec{v}} q_{\vec{f}}} X_B^{\vec{u} + \vec{f}} Z_B^{\vec{v}} |\Phi^+\rangle_{AB}^{\otimes m} |\vec{f}\rangle_{\mathbf{A}'} |\vec{u}\rangle_{E_1} Z_{E_2}^{\vec{f}} |\vec{v}\rangle_{E_2}, \tag{5}$$

where $\vec{f} \in \mathbb{F}^m$ and $q_{\vec{f}} = q^f (1 - q)^{m-f}$ for $f = |\vec{f}|$, the number of 1s in \vec{f} , a notation we shall use throughout. Here we have used the fact that $X_A |\Phi^+\rangle_{AB} = X_B |\Phi^+\rangle_{AB}$ to simplify the expression; this move is responsible for the $Z^{\vec{f}}$ operation applied to E_2 .

In the second step, Alice and Bob both measure the $m - 1$ (generators of the) stabilizers of a $\mathbb{1}/Z$ -only stabilizer code which encodes one logical qubit into m physical qubits. Using a public (authenticated) channel, Alice sends her syndrome to Bob who calculates the relative syndrome \vec{s} by adding Alice's string to his measurement outcome modulo two. Afterwards both decode their encoded state. Such a stabilizer code together with an encoding $U_{\text{enc}}|\vec{e}, c\rangle = |\theta(\vec{e}, c)\rangle$, where

$$|\theta(\vec{e}, c)\rangle = |c \cdot \vec{\eta}_m + \sum_{j=1}^{m-1} e_j \cdot \vec{\eta}_j\rangle, \quad (6)$$

can be fully specified by defining two bases $\{\vec{\xi}_i\}_{i=1\dots m}$ and $\{\vec{\eta}_j\}_{j=1\dots m}$ both spanning \mathbb{F}^m with the property that $\vec{\xi}_i \cdot \vec{\eta}_j = \delta_{ij}$ (see e. g. [19]). In this case the stabilizers are given by $Z(\vec{\xi}_i) = Z^{\vec{\xi}_i}$, $i = 1 \dots m - 1$, and a measurement of these stabilizers on the encoded state (6) will give the syndrome \vec{e} . Measurement of the logical Z operator $Z(\vec{\xi}_m)$ gives the value of the encoded bit c . Applying one of the $X(\vec{\eta}_i) = X^{\vec{\eta}_i}$, $i = 1 \dots m - 1$, operators on an encoded state results in a flip of the i -th bit of the syndrome, while applying the logical X operator $X(\vec{\eta}_m)$ flips the encoded bit, $c \mapsto c \oplus 1$. Both the set of all $Z(\vec{\xi}_i)$ and the set of all $X(\vec{\eta}_j)$ are complete sets of commuting observables. Note that (i)

$$|\Phi^+\rangle_{AB}^{\otimes m} = \frac{1}{\sqrt{2^{m-1}}} \sum_{\vec{e}} \frac{1}{\sqrt{2}} \sum_c |\bar{\theta}(\vec{e}, c)\rangle_A |\theta(\vec{e}, c)\rangle_B, \quad (7)$$

and (ii) that any m fold Pauli operator can be decomposed as

$$X^{\vec{u}} Z^{\vec{v}} = X^{\vec{\xi}_m \cdot \vec{u}}(\vec{\eta}_m) Z^{\vec{\eta}_m \cdot \vec{v}}(\vec{\xi}_m) \prod_{i=1}^{m-1} X^{\vec{\xi}_i \cdot \vec{u}}(\vec{\eta}_i) Z^{\vec{\eta}_i \cdot \vec{v}}(\vec{\xi}_i), \quad (8)$$

where $\vec{\xi}_m \cdot \vec{u}$ and $\vec{\eta}_m \cdot \vec{v}$ are the logical bit and phase flip errors resulting when this Pauli operator is applied to an encoded state like (6). In other words, the maximally-entangled state of m physical qubits is the equal superposition of a logical maximally-entangled state in all the possible encodings, which can be seen using the completeness of $\vec{\eta}_i$. Meanwhile, the formulation of physical X and Z operators in terms of their logical versions follows from using the orthogonality of the $\vec{\eta}_i$ and $\vec{\xi}_j$. Using these two facts we find that, after Bob's calculation of the relative syndrome \vec{s} , the tripartite state can be expressed as (up to a local unitary acting only on Eve's systems)

$$|\sigma''\rangle_{ABE} = \sum_{\vec{u}, \vec{v}, \vec{f}} \sqrt{p_{\vec{u}, \vec{v}} q_{\vec{f}}} X_B^{\vec{\xi}_m \cdot (\vec{u} + \vec{f})} Z_B^{\vec{\eta}_m \cdot \vec{v}} |\Phi^+\rangle_{AB} |\vec{f}\rangle_{\mathbf{A}} |\vec{u}\rangle_{E_1} Z_{E_2}^{\vec{f}} |\vec{v}\rangle_{E_2} |\vec{s}\rangle_{\mathbf{B}'}, \quad (9)$$

where $\vec{s} = (\vec{\xi}_1 \cdot (\vec{u} + \vec{f}), \dots, \vec{\xi}_{m-1} \cdot (\vec{u} + \vec{f}))$. While the registers A and B in equation (5) have been m -qubit registers, here they contain only a single qubit each. Alice's missing $(m - 1)$ -qubits have been traced out since they contained only classical information about her absolute syndrome (accessible to all parties). The rest of Bob's m -qubit register now contains classical information about the relative syndrome \vec{s} and is labeled \mathbf{B}' . We now restrict ourselves to the cat code, which is given by $(\vec{\xi}_i)_j = \delta_{1j} + \delta_{i+1,j}$ for $i = 1 \dots m - 1$, $(\vec{\xi}_m)_j = \delta_{1j}$ and $(\vec{\eta}_i)_j = \delta_{i+1,j}$ for $i = 1 \dots m - 1$, $(\vec{\eta}_m)_j = 1$ (see figure 2). The name comes from the fact that $\alpha|\theta(\vec{0}, 0)\rangle + \beta|\theta(\vec{0}, 1)\rangle = \alpha|00\dots 0\rangle + \beta|11\dots 1\rangle$, a Schrödinger cat state when $\alpha = \beta = \frac{1}{\sqrt{2}}$.

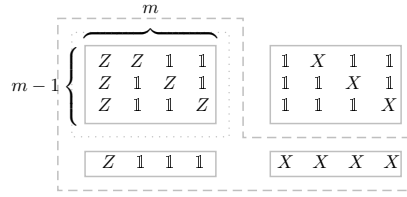


Fig. 2. Cat code encoding one qubit into $m = 4$. The operators on the left hand side are the $Z(\vec{\xi}_i) = Z^{\xi_i}$ ($i = 1 \dots m$ from top to bottom), those on the right hand side the $X(\vec{\eta}_i) = X^{\eta_i}$. The (generators of the) stabilizers are within the dotted line, the (generators of the) normalizers within the dashed one.

Finally, Alice and Bob both measure their key bit. Alice forgets about which bits she flipped by tracing out the A' register. The correlations between Alice, Bob, and Eve are described by the following semiclassical state:

$$\sigma_{XYE} = \frac{1}{2} \sum_x [x]_A \otimes \sum_{\vec{u}, \vec{f}} \sum_{\vec{v}_1, \vec{v}_2} \sqrt{p_{\vec{u}, \vec{v}_1} p_{\vec{u}, \vec{v}_2} q_{\vec{f}}} [x + \vec{\xi}_m \cdot (\vec{u} + \vec{f})]_B \otimes [\vec{s}]_{B'} \otimes [\vec{u}]_{E_1} \otimes (Z^{\vec{\eta}_m})_{E_2}^x Z_{E_2}^{\vec{f}} |\vec{v}_1\rangle\langle\vec{v}_2| Z_{E_2}^{\vec{f}} (Z^{\vec{\eta}_m})_{E_2}^x, \quad (10)$$

where $[x]_B = |x\rangle\langle x|_B$, etc. Note that the state is diagonal in E_1 since the quantities $\vec{\xi}_i \cdot (\vec{u} + \vec{f})$ are all classical: $i = 1, \dots, m - 1$ is already classical in (9), $i = m$ became classical after the key bit measurements by Alice and Bob. The $\{\vec{\xi}_i\}_{i=1, \dots, m}$ span \mathbb{F}^m thereby completely fixing the string $\vec{u} + \vec{f}$.

To calculate the quantum mutual information between Alice and Bob we trace out Eve and obtain

$$\begin{aligned} \sigma_{XY} &= \frac{1}{2} \sum_x [x]_A \otimes \sum_{\vec{u}, \vec{f}} p_{\vec{u}} q_{\vec{f}} [x + \vec{\xi}_m \cdot (\vec{u} + \vec{f})]_B \otimes [(\vec{\xi}_1 \cdot (\vec{u} + \vec{f}), \dots)]_{B'} \\ &= \frac{1}{2} \sum_x [x]_A \otimes \sum_{\vec{u}} \tilde{p}_{\vec{u}} [x + \vec{\xi}_m \cdot \vec{u}]_B \otimes [(\vec{\xi}_1 \cdot \vec{u}, \vec{\xi}_2 \cdot \vec{u}, \dots)]_{B'} \\ &= \frac{1}{2} \sum_x [x]_A \otimes \sum_{l_x, \vec{s}} \tilde{P}(l_x, \vec{s}) [x + l_x]_B \otimes [\vec{s}]_{B'}, \end{aligned} \quad (11)$$

where $\tilde{p} = p(1 - q) + (1 - p)q$, $\tilde{p}_{\vec{u}}$ is defined as $\tilde{p}_{\vec{u}} = \tilde{p}^u (1 - \tilde{p})^{m-u}$, and $\tilde{P}(l_x, \vec{s}) = (\tilde{p}^s (1 - \tilde{p})^{m-s})^{1-l_x} (\tilde{p}^{m-s} (1 - \tilde{p})^s)^{l_x}$. In the last step we used $\vec{u} = l_x \vec{\eta}_m + \sum_i s_i \vec{\eta}_i$ to write the sum over \vec{u} as a sum over l_x and \vec{s} , where l_x is the logical X error, i.e. X error on the first qubit in the block. This immediately yields

$$I(X : Y) = 1 - \sum_{\vec{s}} \tilde{P}(\vec{s}) H_2(\tilde{P}(l_x | \vec{s})), \quad (12)$$

using the binary entropy $H_2(x) = -x \log x - (1 - x) \log(1 - x)$. Note that $I(X : Y)$ does not depend on the particular values $\{p_{uv}\}$ in σ_{AB} (see (3)), but only depends on the bit error rate $p = p_{10} + p_{11}$. The form of the mutual information indicates the advantage provided by the syndrome. If Alice did not send any information, Bob's state would be averaged over the

possible syndromes, and the mutual information would involve the entropy of the average of the $\tilde{P}(l_x|\bar{s})$ rather than the average of the entropies. By concavity of entropy, the latter rate is larger.

To calculate the quantum mutual information between Alice and Eve, we trace out Bob's systems and obtain

$$\sigma_{X\bar{E}} = \frac{1}{2} \sum_x [x]_A \otimes \rho_{E_1 E_2}^{(x)}, \quad (13)$$

$$\rho_{E_1 E_2}^{(x)} = \sum_{\vec{u}} p_{\vec{u}} [\vec{u}]_{E_1} \otimes \rho_{E_2}^{(x), \vec{u}}, \quad \text{and} \quad (14)$$

$$\rho_{E_2}^{(x), \vec{u}} = (Z^{\vec{\eta}_m})^x \sum_{\vec{f}} q_{\vec{f}} Z^{\vec{f}} |\Psi_{|\vec{u}}\rangle \langle \Psi_{|\vec{u}}| Z^{\vec{f}} (Z^{\vec{\eta}_m})^x, \quad (15)$$

with

$$|\Psi_{|\vec{u}}\rangle = \sum_{\vec{v}} \sqrt{p_{\vec{v}|\vec{u}}} |\vec{v}\rangle. \quad (16)$$

We proceed with the computation of the secure key rate for the BB84 and the 6-state protocol separately in the following two subsections.

2.1.1 BB84

To calculate the secure key rate we must find the minimum over all σ_{AB} of the difference between the quantum mutual information between Alice and Bob and Alice and Eve. Since $I(X : Y)$ does not depend on the particular structure of $\{p_{uv}\} = \{1 - 2p + t, p - t, t, p - t\}$, $t \in [0, p]$, in σ_{AB} , but only depends on the bit error rate $p = p_{10} + p_{11}$, this corresponds to finding the maximum of $I(X : E)$.

Let us assume for a moment that this maximum is achieved for independent bit and phase errors, i. e. we consider the state σ_{AB} with $\{p_{uv}\} = \{1 - 2p + t, p - t, t, p - t\}$ and $t = p^2$. In this case $|\Psi_{|\vec{u}}\rangle$ does not depend on \vec{u} , and we get

$$\rho_{E_2}^{(x), \vec{u}} = (Z^{\vec{\eta}_m})^x \rho_{pq}^{\otimes m} (Z^{\vec{\eta}_m})^x \quad (17)$$

with $\rho_{pq} = (1 - q)|\varphi_+\rangle\langle\varphi_+| + q|\varphi_-\rangle\langle\varphi_-|$ and $|\varphi_{\pm}\rangle = \sqrt{1 - p}|0\rangle \pm \sqrt{p}|1\rangle$. Part E_1 and E_2 of the state $\rho_{E_1 E_2}^{(x)}$ in (14) are now completely decoupled. As it was shown in [15], the fact that E_1 is classical allows the corresponding state describing dependent errors to be reconstructed from this state: After tracing out the E_1 part, we add an ancilla $[0]_{E_3}$, apply the isometry $\sum_{\vec{u}, \vec{v}} \sqrt{p_{\vec{u}|\vec{v}}} |\vec{u}\rangle_{E_3} \langle 0| \otimes |\vec{v}\rangle_{E_2}$ and eventually dephase the ancilla. Since quantum mutual information never increases under local operations, the maximum of $I(X : E)$ is indeed achieved for independent errors and we get

$$I(X : E) = S\left(\frac{1}{2}\rho_{pq}^{\otimes m} + \frac{1}{2}(Z\rho_{pq}Z)^{\otimes m}\right) - mS(\rho_{pq}). \quad (18)$$

Subtraction of (18) from (12) gives the secure key rate for the BB84 protocol:

$$r(m, p) = \max_q \frac{1}{m} \left[1 - \sum_{s=0}^{m-1} \binom{m-1}{s} \tilde{P}(s) H_2(\tilde{P}(l_x|s)) \right. \\ \left. - S\left(\frac{1}{2}\rho_{pq}^{\otimes m} + \frac{1}{2}(Z\rho_{pq}Z)^{\otimes m}\right) + mH_2\left(\frac{1}{2}(1 + \sqrt{1 - 16p(1-p)q(1-q)})\right) \right]. \quad (19)$$

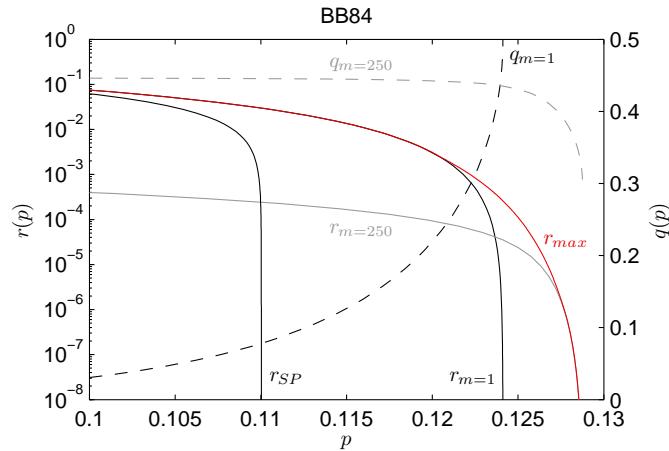


Fig. 3. Secure key rate r of BB84 for various types of preprocessing versus bit error rate p . No preprocessing corresponds to r_{SP} , noisy preprocessing to $r_{m=1}$, and the maximum over all block lengths $m \leq 250$ to r_{max} , shown in red. For the rates achieved by the blocklengths $m = 1$ and $m = 250$, the corresponding rate of the added noise is shown on the right y axis.

Omitting the maximization over q , the above formula gives the key rate $r_{m,q}(p)$ for some fixed values of m and q as a function of the bit error rate p . By setting $r_{m,q}(p)$ equal to zero, we find $p_{max}(m, q)$, the maximum tolerable bit error rate for given m and q . For very high levels of added noise, i. e. for $q = \frac{1}{2} - \epsilon$, we find that for all values of m , the key rate becomes zero at the bit error rate $p_{max}(m, q = \frac{1}{2} - \epsilon) = 12.4120\%$, but by adding less noise at higher values of m , secret keys can be generated for even larger bit error rates.

Without the use of the cat code (i. e. if we take $m = 1$) the rate reduces to [11, 12]

$$r(p) = \max_q \left[1 - H_2(\tilde{p}) - H_2(p) + H_2\left(\frac{1}{2}(1 + \sqrt{1 - 16p(1-p)q(1-q)})\right) \right]. \quad (20)$$

With neither local randomization ($q = 0$) nor use of the cat code ($m = 1$) the key rate (20) becomes even smaller [3],

$$r(p) = 1 - 2H_2(p), \quad (21)$$

and secure key generation becomes impossible for bit error rates higher than $p_{max} = 11.0028\%$.

Figure 3 shows plots of the key rates given by (21) and (20) (black) and the maximum over the key rates given by (19) (red) for values of m up to 250. The increase of the maximal tolerable bit error rate with the block length m is illustrated in figure 1. The highest value of m for which we maximized the tolerable bit error rate as function of the added noise q was $m = 500$ leading to $p_{max}(m = 500, q = 0.32656) = 12.9379\%$.

By far the most difficult part in the numerical evaluation of (19) is computing the von Neumann entropy, as it contains a sum of two m -fold tensor products of different one qubit density operators. Such an expression can be more efficiently calculated by taking into account its block diagonal structure which follows from permutation invariance, as detailed in the Appendix.

2.1.2 6-state

Since the set Γ only contains the single state $\{p_{uv}\} = \{1 - \frac{3}{2}p, \frac{p}{2}, \frac{p}{2}, \frac{p}{2}\}$, minimization over σ_{AB} is unnecessary and the secure key rate is directly given by the difference of the quantum mutual informations between Alice and Bob (12) and Alice and Eve. Despite the simplicity of Γ , this calculation is more difficult than BB84 due to the correlation between bit and phase errors. The corresponding conditional probabilities are given by $p_{v=1|u=0} = \frac{p}{2(1-p)} = p'$, $p_{v=0|u=0} = 1 - p'$ and $p_{v|u=1} = \frac{1}{2}$. Therefore, denoting the number of ones in \vec{u} as u and by reordering the qubits in such a way that the first u qubits are the ones with $u_i = 1$, we get

$$|\Psi_{|\vec{u}}\rangle = \sum_{\vec{v}} \sqrt{p_{\vec{v}|\vec{u}}} |\vec{v}\rangle = |+\rangle^{\otimes u} \otimes |\varphi'_+\rangle^{\otimes m-u} = |\Psi_{|u}\rangle \quad (22)$$

with $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and $|\varphi'_{\pm}\rangle = \sqrt{p'}|0\rangle \pm \sqrt{1-p'}|1\rangle$, leading to

$$\begin{aligned} \rho_{E_2}^{(x),u} &= (Z^{\vec{\eta}_m})^x \sum_{\vec{f}} q_{\vec{f}} Z^{\vec{f}} [+]^{\otimes u} \otimes [\varphi'_+]^{\otimes m-u} Z^{\vec{f}} (Z^{\vec{\eta}_m})^x \\ &= (Z^{\vec{\eta}_m})^x \sigma^{\otimes u} \otimes \gamma^{\otimes m-u} (Z^{\vec{\eta}_m})^x \end{aligned} \quad (23)$$

with $\sigma = (1-q)[+] + q[-]$ and $\gamma = (1-q)[\varphi'_+] + q[\varphi'_-]$. Reordering the state in this manner does not change the entropy, and so will not alter the rate. Using these results the quantum mutual information between Alice and Eve can be expressed as

$$\begin{aligned} I(X : E) &= \sum_{u=0}^m \binom{m}{u} p^u (1-p)^{m-u} \left[S\left(\frac{1}{2}\sigma^{\otimes u} \otimes \gamma^{\otimes m-u} + \frac{1}{2}(Z\sigma Z)^{\otimes u} \otimes (Z\gamma Z)^{\otimes m-u}\right) \right. \\ &\quad \left. - uH_2(q) - (m-u)H_2\left(\frac{1}{2}(1 + \sqrt{1 - 16p'(1-p')q(1-q)})\right) \right]. \end{aligned} \quad (24)$$

Since σ and $Z\sigma Z$ are diagonal in the same basis we are able to write the von Neumann entropy as

$$\sum_{k=0}^u \binom{u}{k} S\left(\frac{(1-q)^k q^{u-k}}{2} \gamma^{\otimes m-u} + \frac{q^k (1-q)^{u-k}}{2} (Z\gamma Z)^{\otimes m-u}\right) \quad (25)$$

which is of the same form as the von Neumann entropy in (18). Therefore the same methods for evaluation can be applied; see the Appendix.

The secure key rate is given by subtracting (24) from (12),

$$r(m, p) = \max_q \frac{1}{m} \left[1 - \sum_{s=0}^{m-1} \binom{m-1}{s} \tilde{P}(s) H_2\left(\tilde{P}(l_x|s)\right) - I(X : E) \right]. \quad (26)$$

As it is the case for the BB84 protocol, the key rate becomes zero for all values of m for $q \rightarrow \frac{1}{2}$ (this time at bit error rate $p_{max}(m, q = \frac{1}{2} - \epsilon) = 14.1119\%$), but again adding less noise at higher values of m gives rise to secret keys for even higher bit error rates.

Two special cases emerge from (26), $m = 1$:

$$r(p) = \max_q \left[1 - H_2(\tilde{p}) - \sum_u p_u \left(H_2(p_{v|u}) - H_2\left(\frac{1}{2}(1 + \sqrt{1 - 16p_{1|u}(1-p_{1|u})q(1-q)})\right) \right) \right], \quad (27)$$

and $q = 0$, which leads to [8, 9, 4]:

$$r(p) = \frac{1}{m} \left[1 - \sum_{\vec{s}} P(\vec{s}) H(P(l^x, l^z | \vec{s})) \right] \tag{28}$$

(note the appearance of the usual entropy, not the binary entropy), with

$$P(l^x, l^z, \vec{s}) = \frac{1}{2} \left[p^{l^x(m-2s)+s} (1-p)^{(1-l^x)(m-2s)+s} + \delta_{0, l^x(m-2s)+s} (-1)^{l^z} (1-2p)^{(1-l^x)(m-2s)+s} \right] \tag{29}$$

which attains the highest robustness for $m = 5$ leading to $p_{max}(m = 5, q = 0) = 12.6904\%$ instead of $p_{max}(m = 1, q = 0) = 12.6193\%$.^a

In figure 4 we show the key rates in these special cases as well as the general case for optimal noise and blocklengths up to $m = 125$. Included are $q = 0, m = 1$ (black), $q = 0, m = 5$ (dotted), and $m = 1$ for the optimal q (black). The maximum over the key rates given by (26) for values of m up to 125 is shown in red, along with the specific case of $m = 125$. The increase of the maximal tolerable bit error rate with the block length m is illustrated in figure 1. The highest value of m for which we maximized the tolerable bit error rate as function of the added noise q was $m = 250$ leading to $p_{max}(m = 250, q = 0.31210) = 14.5741\%$. Since the computation for larger block sizes becomes rather slow, we extrapolated the value for the optimum noise leading to $q \approx 0.31650$ for $m = 300$. By calculating the highest tolerable bit error for this value of noise we get the best lower bound $p_{max}(m = 300, q = 0.31650) = 14.5930\%$.

3 Iterated Preprocessing

By combining local randomization with the cat-code of size m , Alice and Bob gain an advantage over Eve and intuitively it seems this advantage might be even bigger by performing the procedure twice. In this section we discuss such a twofold iterated protocol where Alice adds noise at a rate q to m_2 blocks of size m_1 each, and then after measuring the syndromes of these blocks, adds further noise at another rate Q to the m_2 'key' bits of these blocks. Then the syndrome of these m_2 bits is measured and the remainder of the protocol proceeds as usual. We restrict ourselves to the BB84 protocol for simplicity. Using essentially the same argument as in section 2.1.1, we find that we only need to consider independent bit and phase errors described by the state σ_{AB} with $\{p_{uv}\} = \{1 - 2p + t, p - t, t, p - t\}$ and $t = p^2$: (i) $I(X : Y)$ depends only on the bit error rate $p = p_{10} + p_{11}$, (ii) therefore we have to find the maximum of $I(X : E)$, (iii) which is achieved for independent errors. The proof of (iii) works as in section 2.1.1, since, as we will see, E_1 of $\sigma_{X\bar{E}}$ is again classical.

^aNote that in [8, 9] the quantity under consideration was the capacity of the quantum depolarizing channel with $\{p_{uv}\} = \{1 - p, \frac{p}{3}, \frac{p}{3}, \frac{p}{3}\}$ therefore leading to $p_{max} = \frac{3}{2} \times 12.6904\%$

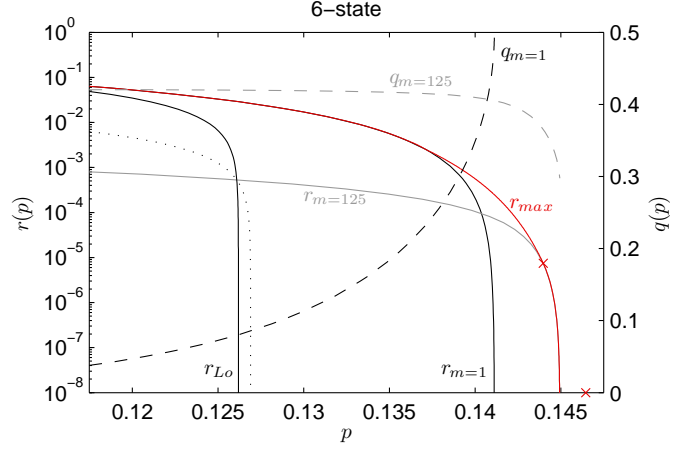


Fig. 4. Secure key rate r of the 6-state protocol for various types of preprocessing versus bit error rate p . No preprocessing corresponds to r_{Lo} , noisy preprocessing to $r_{m=1}$, and the maximum achievable rate over all blocklengths $m \leq 125$, to r_{max} , shown in red. For the rates achieved by the blocklengths $m = 1$ and $m = 125$, the corresponding rate of the added noise is shown on the right y -axis. The dotted rate with $p_{max} = 12.6904\%$ is due to Lo, corresponding to use of a repetition code of blocklength $m = 5$ and no noisy preprocessing.

3.1 Rate Calculation

We start with (9), now denoting m as m_1 . Adding additional noise at rate Q to the key bit the state is described as

$$|\sigma'\rangle_{ABE} = \sum_{\vec{f}, \vec{u}, \vec{v}} \sum_F \sqrt{p_{\vec{u}, \vec{v}} q_{\vec{f}}} Q_F X_B^{\vec{\xi}_{m_1} \cdot (\vec{u} + \vec{f}) + F} Z_B^{\vec{\eta}_{m_1} \cdot \vec{v}} |\Phi^+\rangle_{AB} \otimes |\vec{u}\rangle_{E_1} (Z^{\vec{\eta}_{m_1}})^F Z^{\vec{f}} |\vec{v}\rangle_{E_2} |\vec{s}\rangle_{\mathbf{B}} |\vec{f}\rangle_{\mathbf{A}'} |F\rangle_{\mathbf{A}''} \quad (30)$$

with classical registers \mathbf{B} , \mathbf{A}' and \mathbf{A}'' and the same relationship $\vec{s} = (\xi_1 \cdot (\vec{u} + \vec{f}), \dots, \xi_{m_1-1} \cdot (\vec{u} + \vec{f}))$ as before. Now we consider the m_2 -fold tensor product $|\sigma'\rangle_{ABE}^{\otimes m_2}$ and define the abbreviations $\vec{U} = (\xi_{m_1} \cdot (\vec{u}_1 + \vec{f}_1), \dots, \xi_{m_1} \cdot (\vec{u}_{m_2} + \vec{f}_{m_2}))$ and $\vec{V} = (\eta_{m_1} \cdot \vec{v}_1, \dots, \eta_{m_1} \cdot \vec{v}_{m_2})$. Again Alice and Bob both measure their stabilizers, Alice sends her result to Bob, who calculates the relative syndrome $\vec{S} = (\xi_1 \cdot (\vec{U} + \vec{F}), \dots, \xi_{m_2-1} \cdot (\vec{U} + \vec{F}))$. Both then measure their key bit. The tripartite semiclassical state describing the correlations is now given by

$$\begin{aligned} \sigma_{XY\bar{E}} = & \frac{1}{2} \sum_{\vec{F}} Q_{\vec{F}} \sum_{\vec{f}_1, \dots, \vec{f}_{m_2}} q_{\vec{f}_1} \cdots q_{\vec{f}_{m_2}} \sum_{\vec{u}_1, \dots, \vec{u}_{m_2}} p_{\vec{u}_1} \cdots p_{\vec{u}_{m_2}} \\ & \times \sum_x [x]_A \otimes [x + L_x]_B \otimes [\vec{s}_1, \dots, \vec{s}_{m_2}, \vec{S}]_{\mathbf{B}} \otimes [\vec{u}_1, \dots, \vec{u}_{m_2}]_{E_1} \\ & \otimes (Z^{\otimes m_1 m_2})^x \bigotimes_{i=1}^{m_2} ((Z^{\otimes m_1})^{F_i} Z^{\vec{f}_i} |\Psi\rangle \langle \Psi| Z^{\vec{f}_i} (Z^{\otimes m_1})^{F_i}) (Z^{\otimes m_1 m_2})^x, \quad (31) \end{aligned}$$

where $|\Psi\rangle = \sum_{\vec{v}} \sqrt{p_{\vec{v}}} |\vec{v}\rangle$ and $\vec{s}_i = (\xi_1 \cdot (\vec{u}_i + \vec{f}_i), \dots)$, $\vec{S} = (\xi_1 \cdot (\vec{U} + \vec{F}), \dots)$, and $L_x = \xi_{m_2} \cdot (\vec{U} + \vec{F})$.

To calculate the quantum mutual information between Alice and Bob we trace out Eve's systems and obtain

$$\sigma_{XY} = \frac{1}{2} \sum_{\vec{F}} Q_{\vec{F}} \sum_{\vec{u}_1 \dots \vec{u}_{m_2}} \tilde{p}_{\vec{u}_1} \dots \tilde{p}_{\vec{u}_{m_2}} \sum_x [x]_A \otimes [x + L_x]_B \otimes [\vec{s}_1 \dots \vec{s}_{m_2}, \vec{S}]_B, \quad (32)$$

using $\tilde{p} = p(1-q) + (1-p)q$. Since Alice's additional noise \vec{f} is now combined with Eve's noise \vec{u} , \vec{f} no longer appears in the syndromes \vec{s}_i and \vec{S} : $\vec{s}_i = (\xi_1 \cdot \vec{u}_i, \dots)$, $\vec{S} = (\xi_1 \cdot (\vec{U}' + \vec{F}), \dots)$. Additionally, L_x is now $L_x = \vec{\xi}_{m_2} \cdot (\vec{U}' + \vec{F})$, with $\vec{U}' = (\xi_{m_1} \cdot \vec{u}_1, \dots, \xi_{m_1} \cdot \vec{u}_{m_2})$. The mutual information can therefore be written as

$$I(X : Y) = 1 - \sum_{\vec{s}_1 \dots \vec{s}_{m_2}, \vec{S}} \tilde{P}'(\vec{s}_1 \dots \vec{s}_{m_2}, \vec{S}) H_2(\tilde{P}'(L_x | \vec{s}_1 \dots \vec{s}_{m_2}, \vec{S})), \quad (33)$$

where the probability distribution \tilde{P}' only depends on the number of ones in each of the syndromes \vec{s}_i and \vec{S} (we assume that the zeros and ones in \vec{S} are ordered such that the syndromes \vec{s}_i , $i \in \{1, \dots, m_2 - S\}$, correspond to $S_i = 0$):

$$\begin{aligned} \tilde{P}'(L_x = 0, s_1 \dots s_{m_2}, S) &= \prod_{i=1}^{m_2-S} [(1-\tilde{p})^{m_1-s_i} \tilde{p}^{s_i} (1-Q) + (1-\tilde{p})^{s_i} \tilde{p}^{m_1-s_i} Q] \times \\ &\quad \prod_{i=m_2-S+1}^{m_2} [(1-\tilde{p})^{s_i} \tilde{p}^{m_1-s_i} (1-Q) + (1-\tilde{p})^{m_1-s_i} \tilde{p}^{s_i} Q]. \end{aligned} \quad (34)$$

In addition we see from (34) that for a given value of S only the frequency distribution of the s_i , $i \in \{1, \dots, m_2 - S\}$, and the s_j , $j \in \{m_2 - S + 1, \dots, m_2\}$, matters. This fact can be used to speed up the calculation of the sum over the syndromes in (33).

Since $\rho_{E_2}^{(x), \vec{u}} = (Z^{\otimes m_1 m_2})^x [(1-Q)\rho_{pq}^{\otimes m_1} + Q(Z\rho_{pq}Z)^{\otimes m_1}]^{\otimes m_2} (Z^{\otimes m_1 m_2})^x$, the mutual information between Alice and Eve can be seen to be

$$\begin{aligned} I(X : E) &= S \left(\frac{1}{2} [(1-Q)\rho_{pq}^{\otimes m_1} + Q(Z\rho_{pq}Z)^{\otimes m_1}]^{\otimes m_2} + \frac{1}{2} [Q\rho_{pq}^{\otimes m_1} + (1-Q)(Z\rho_{pq}Z)^{\otimes m_1}]^{\otimes m_2} \right) \\ &\quad - m_2 S ((1-Q)\rho_{pq}^{\otimes m_1} + Q(Z\rho_{pq}Z)^{\otimes m_1}) \end{aligned} \quad (35)$$

Once more the secure key rate is given by the difference of these mutual informations,

$$r(m_1, m_2, p) = \max_{q, Q} \frac{1}{m_1 m_2} (I(X : Y) - I(X : E)). \quad (36)$$

Again the hardest part in the numerical evaluation of (36) comes from the von Neumann entropies. One contains a sum of two m_2 -fold tensor products of different density operators, but this time these density operators are m_1 -qubit density operators. Such an expression can also be calculated more efficiently by taking into account its permutation invariance. For more details see the Appendix.

We compare the resulting key rate of the $m_1 \times m_2 = 3 \times 3$ iterated code with the key rates of the non-iterated codes of block sizes $m \in \{9, 10, 11\}$ in figure 5.

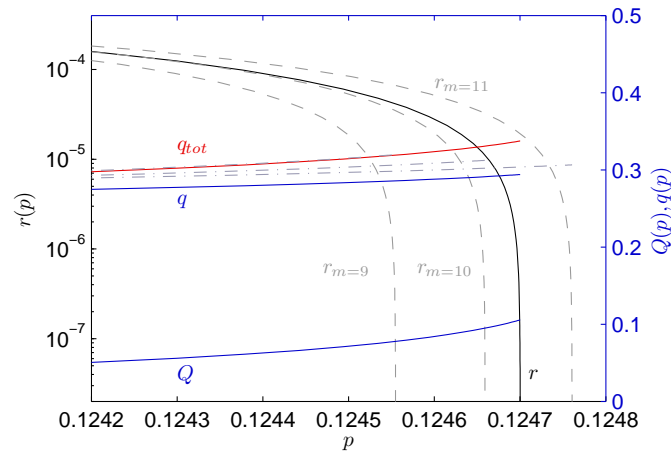


Fig. 5. Secure key rate r of BB84 with iterated preprocessing of size $m_1 \times m_2 = 3 \times 3$ versus bit error rate p . The right y-axis shows the corresponding values of added noise in the first (q) and second iteration (Q) as well as values of the total amount of added noise ($q_{tot} = q(1-Q) + (1-q)Q$, red). For comparison, the rates of the non-iterated protocol are shown for block sizes $m \in \{9, 10, 11\}$ (dashed lines). The corresponding values of added noise for these cases are also shown (dash-dot lines).

4 Conclusions

Although sending quantum information and establishing a secret key are not equivalent uses of a quantum channel, their similarities are enough to ensure a fruitful exchange of techniques between the two problems. Here we have extended the application of structured codes to the problem of QKD given in [15] to the 6-state protocol, showing how preprocessing based on both structured codes and local randomization leads to higher tolerable error rates. Having one more unbiased basis implies correlation between bit and phase errors of the estimated quantum state, leading to increased robustness of the protocol. Indeed, it seems likely that for large blocklength ($m \approx 500$) the threshold of the 6-state protocol exceeds the lowest known upper bound on the threshold for the BB84 protocol (14.6447%). This method of preprocessing does not close the gap between BB84 upper and lower bounds, however, as the available data suggests that the BB84 threshold never exceeds roughly 13% even for asymptotically-long blocks. For the 6-state protocol, more data is needed to draw even a partial conclusion on the asymptotic threshold.

Additionally, we have shown that further performance gains are possible when iterating the preprocessing step. Although our results are confined to two rounds with small block sizes, we can nevertheless already observe some general properties. The entire rate curve shifts to higher values, so this type of processing might be useful in increasing the efficiency of protocols running over noisy channels. Intriguingly, the total amount of noise added to the sifted key bits is essentially the same as in the case of one round, showing that the improvement comes from making better use of the same amount of noise. More sophisticated representation-theoretic methods, in particular a Clebsch-Gordon decomposition of the states input to the second preprocessing round, should make analysis of more rounds and larger block sizes tractable.

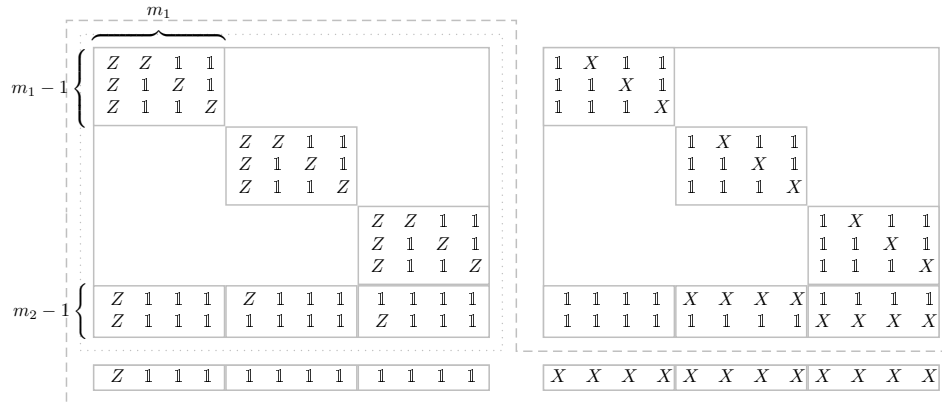


Fig. 6. The concatenated code of size $m_1 = 4$ and $m_2 = 3$ encoding one qubit into $n = m_1 \times m_2$. The operators on the left hand side are the $Z(\vec{\xi}_i) = Z^{\xi_i}$, those on the right hand side the $X(\vec{\eta}_i) = X^{\eta_i}$. The stabilizers are within the dotted line, the normalizers within the dashed one.

Acknowledgements

We thank Gernot Alber and Graeme Smith for helpful discussions. Financial support by the EC within the IP SECOQC is acknowledged. JMR acknowledges support from the Alexander von Humboldt Foundation.

References

1. Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *IEEE International Conference on Computers Systems and Signal Processing*, pages 175–179, Bangalore, India, 1984.
2. Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81:3018, October 1998.
3. Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85:441, July 2000.
4. Hoi-Kwong Lo. Proof of unconditional security of six-state quantum key distribution scheme. *Quantum Information and Computation*, 1:81–94, August 2001.
5. I. Devetak and A. Winter. Relating quantum privacy and quantum coherence: An operational approach. *Physical Review Letters*, 93:080501–4, 2004.
6. I. Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, 51:44– 55, 2005.
7. Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A*, 461:207–235, 2005.
8. Peter W Shor and John A Smolin. Quantum error-correcting codes need not completely reveal the error syndrome. *quant-ph/9604006v2*, April 1996.
9. David P. DiVincenzo, Peter W. Shor, and John A. Smolin. Quantum-channel capacity of very noisy channels. *Physical Review A*, 57:830, February 1998.
10. Graeme Smith and John A. Smolin. Degenerate quantum codes for pauli channels. *Physical Review Letters*, 98:030501–4, 2007.
11. B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Physical Review Letters*, 95:080501–4, 2005.
12. Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A*, 72:012332–17, July 2005.

13. Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. *Physical Review Letters*, 94:160502–4, April 2005.
14. Joseph M. Renes and Graeme Smith. Noisy processing and distillation of private quantum states. *Physical Review Letters*, 98:020502, 2007.
15. Graeme Smith, Joseph M Renes, and John A Smolin. Structured codes improve the bennett-brassard-84 quantum key rate. *Physical Review Letters*, 100:170502, April 2008.
16. Christopher A. Fuchs, Nicolas Gisin, Robert B. Griffiths, Chi-Sheng Niu, and Asher Peres. Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy. *Physical Review A*, 56:1163, 1997.
17. Tobias Moroder, Marcos Curty, and Norbert Lütkenhaus. One-way quantum key distribution: Simple upper bound on the secret key rate. *quant-ph/0603270*, March 2006.
18. Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zürich, 2006.
19. Mitsuru Hamada. Notes on the fidelity of symplectic quantum error-correcting codes. *International Journal of Quantum Information*, 1:443–463, December 2003.
20. Jin-Quan Chen, Jialun Ping, and Fan Wang. *Group Representation Theory for Physicists*. World Scientific Publishing Company, 2nd edition, September 2002.

Appendix A Efficient computation of the key rates

To evaluate the secure key rate of the BB84 and the 6-state quantum key distribution protocols involving our preprocessing protocol, we need to compute the von Neumann entropy of a linear combination of m -fold tensor products of different one-qubit density matrices, $S(\alpha\rho^{\otimes m} + \beta\sigma^{\otimes m})$. In the case of the iterated preprocessing protocol this expression becomes a sum over m_2 -fold tensor products of some qudit density matrices of dimension $d = 2^{m_1}$. In this appendix we discuss how such expressions can be evaluated efficiently by using the Schur transform, following the presentation in [20].

Considering m qudits of dimension d , the Schur transform is a unitary transformation relating the standard computational basis $\{|i_1, \dots, i_m\rangle\}$, $i_j = 0, 1, \dots, d-1$, to a basis associated with the representation theory of the symmetric and general linear groups,

$$|\lambda\rangle|p_\lambda\rangle|q_\lambda\rangle = \sum_{i_1 \dots i_m} [U_{Sch}]_{i_1 \dots i_m}^{\lambda p_\lambda q_\lambda} |i_1, \dots, i_m\rangle. \quad (\text{A.1})$$

The new basis $\{|\lambda\rangle|p_\lambda\rangle|q_\lambda\rangle\}$ is labeled by a Young diagram λ denoting the irreducible representations of both \mathcal{S}_m and GL_d , a Young tableau p_λ labeling the basis vectors spanning the representation spaces of \mathcal{S}_m , and a Weyl tableau q_λ labeling the the basis vectors spanning the representation spaces of GL_d . Elements $\sigma \in \text{GL}_d$ and $s \in \mathcal{S}_m$ transform the basis states according to

$$\sigma^{\otimes m} |\lambda\rangle|p_\lambda\rangle|q_\lambda\rangle = |\lambda\rangle|p_\lambda\rangle (\sigma_\lambda |q_\lambda\rangle), \quad (\text{A.2})$$

$$s |\lambda\rangle|p_\lambda\rangle|q_\lambda\rangle = |\lambda\rangle (s_\lambda |p_\lambda\rangle) |q_\lambda\rangle, \quad (\text{A.3})$$

whereas σ_λ denotes $\sigma^{\otimes m}$ in the irrep λ and s_λ denotes s in the irrep λ .

It then follows that states like $\rho^{\otimes m}$ are block-diagonal, with blocks labeled by a Young diagram and tableau (λ, p_λ) . Blocks with the same Young diagram are identical, and the number of Young tableaux $N_Y(\lambda)$ specifies degeneracy. Meanwhile, the dimension of the blocks is given by the corresponding number of Weyl tableaux $N_W(\lambda)$.

This structure is clearly helpful for the calculation of expressions like $S(\alpha\rho^{\otimes m} + \beta\sigma^{\otimes m})$. The entropy of the state reduces to the sum of entropies of the blocks, which itself factors

into the entropy for a block (λ, p_λ) with a fixed Young tableau p_λ , say the first one, times the corresponding degeneracy $N_Y(\lambda)$.

For $d > 2$ we explicitly calculate both the ρ_λ and the σ_λ blocks using (A.1), e. g.

$$(\rho_\lambda)_{Qq} = \langle Q_\lambda | \langle p_\lambda | \langle \lambda | \rho^{\otimes m} | \lambda \rangle | p_\lambda \rangle | q_\lambda \rangle = \sum_{j_1 \dots j_m} \sum_{i_1 \dots i_m} [U_{Sch}^*]_{j_1 \dots j_m}^{\lambda p_\lambda Q_\lambda} [U_{Sch}]_{i_1 \dots i_m}^{\lambda p_\lambda q_\lambda} \langle j_1, \dots, j_m | \rho^{\otimes m} | i_1, \dots, i_m \rangle.$$

The Schur transform itself can be obtained using e. g. the eigenfunction method [20]. For the iterated protocol it may be possible to further streamline the calculation by taking into account the fact that the qudit inputs to the second round are themselves block-diagonal. Computations for much larger blocksizes $m_1 \times m_2$ may then become feasible.

For $d = 2$ things are simpler, as Young diagrams λ consist of at most two rows and can be labeled by an index j , where $2j$ is the number of columns consisting of one row only ($j = 0 \dots \frac{m}{2}$ if m is even, $j = \frac{1}{2} \dots \frac{m}{2}$ if m is odd).

$$\lambda = \begin{array}{c} j \\ \downarrow \\ \begin{array}{cccc} \square & \square & \dots & \square \\ \square & \square & \dots & \square \end{array} \end{array}$$

$\overbrace{\hspace{2cm}}^{\frac{m}{2}-j} \quad \overbrace{\hspace{2cm}}^{2j}$

The dimension of an irreducible representation with label j is $N_W(j) = 2j + 1$ and the Weyl tableaux are now labeled $k = -j, \dots, j$, whereas $j + k$ denotes the number of ones in the first row of the Weyl tableaux:

$$\begin{array}{cccc} \overbrace{\hspace{2cm}}^{\frac{m}{2}-j} & & \overbrace{\hspace{2cm}}^{2j} & \\ \begin{array}{ccc} \boxed{0} \boxed{0} & \dots & \boxed{0} \boxed{0} \boxed{0} \boxed{0} \dots \boxed{1} \boxed{1} \\ \boxed{1} \boxed{1} & & \boxed{1} \boxed{1} \quad \underbrace{\hspace{1cm}}_{j-k} \quad \underbrace{\hspace{1cm}}_{j+k} \end{array} \end{array}$$

The corresponding degeneracy follows from Robinson's hook length formula, which in this case yields

$$N_Y(j) = \binom{m}{m/2-j} \frac{2j+1}{m/2+j+1}. \quad (\text{A.4})$$

We diagonalize ρ and σ , denoting the two eigenvalues of ρ [σ] as ρ_1 and ρ_2 [σ_1 and σ_2],

$$\begin{aligned} \rho &= U_\rho \varrho U_\rho^\dagger, & \varrho &= \text{diag}\{\rho_1, \rho_2\}, \\ \sigma &= U_\sigma \varsigma U_\sigma^\dagger, & \varsigma &= \text{diag}\{\sigma_1, \sigma_2\}, \end{aligned}$$

and note that diagonal density operators like ϱ and ς can easily be expressed in the j -th representation, since they are diagonal in all these representations, too. The action of $\varrho^{\otimes m}$ on basis states (A.1) of the Schur basis becomes simply a multiplication by powers of the two eigenvalues because of the symmetry properties of these basis states: Each basis state of the Schur basis labeled by a certain Young diagram j and Weyl tableaux k consists of a superposition of computational basis states which are permutations of $|01\rangle^{\otimes(m/2-j)} |0\rangle^{\otimes(j-k)} |1\rangle^{\otimes(j+k)}$ independently of the Young tableaux (specifying degeneracy). We obtain

$$\varrho_j = \text{diag}\{\rho_1^{j-k} \rho_2^{j+k} (\rho_1 \rho_2)^{m/2-j}\}_{k=-j \dots j}, \quad (\text{A.5})$$

and an analogous expression for ς_j . To get the non-diagonal original block ρ_j [σ_j] we have to apply the unitary U_ρ [U_σ] in the irrep j which is given by the Wigner rotation matrices $D_j(U_\rho)$

$[D_j(U_\sigma)]$. In our case these Wigner matrices are given simply by matrix exponentiation, $D_j(U_\rho) = \exp(-\frac{\theta(\rho)}{2}(J_+ - J_-))$, where $\theta(\rho)$ denotes a phase calculated from ρ , and J_\pm denotes the usual angular momentum ladder operators, $J_\pm|jm\rangle = \sqrt{j(j+1) + m(m\pm 1)}|jm\pm 1\rangle$. In this way it becomes feasible to calculate expressions like $S(\alpha\sigma^{\otimes m} + \beta\rho^{\otimes m})$ for values of m up to several hundreds.