International Journal of Quantum Information
Vol. 4, No. 6 (2006) 935–946

World Scientific
www.worldscientific.com

NOISE TOLERANCE OF THE BB84 PROTOCOL WITH RANDOM PRIVACY AMPLIFICATION*

SHUN WATANABE†, RYUTAROH MATSUMOTO‡ and TOMOHIKO UYEMATSU§

Department of Communications and Integrated Systems,
Tokyo Institute of Technology,
Tokyo 152-8552, Japan
†*shun-wata@it.ss.titech.ac.jp*
‡*ryutaroh@it.ss.titech.ac.jp*
§*uyematsu@ieee.org*

Received 2 February 2006

This paper shows that the random privacy amplification is secure with a higher key rate than Mayers' evaluation at the same error rate in the BB84 protocol with one-way or two-way classical communications. There exists only Mayers' evaluation on the secure key rate with random privacy amplification that is applicable to the BB84 protocol with two-way classical communications. Our result improves the secure key rate of the random privacy amplification in the BB84 protocol with two-way classical communications.

Keywords: BB84 protocol; CSS code; quantum key distribution; random privacy amplification; two-way protocol.

1. Introduction

The BB84 protocol is the first quantum key distribution (QKD) protocol, which was proposed by Bennett and Brassard in 1984.[1] Unlike conventional cryptographies that rely on the conjectured difficulty of computing certain functions, the security of QKD is guaranteed by the postulate of quantum mechanics. In the BB84 protocol, the participants (Alice and Bob) agree on a secret key about which any eavesdropper (Eve) can obtain little information. The security proof of this protocol against arbitrary eavesdropping strategies was first proved by Mayers,[21] later another proof was shown by Biham *et al.*,[3] and a simple proof was later shown by Shor and Preskill.[23] After them, many security analyses are studied.[12,16,18,24] The proof method of Ref. 23 is also extended to the BB84 protocol with two-way classical communication[13]. It is known that the BB84 protocol with two-way classical communications can tolerate higher error rate than the BB84 protocol with one-way classical communication. The tolerable error rates are 18.9% in Ref. 13 and 20% in Ref. 5.

*Part of this paper was presented in the 2005 IEEE International Symposium on Information Theory, Adelaide Convention Centre, Adelaide, Australia, 4–9 September, 2005.

Roughly speaking, the BB84 protocol is divided into a quantum part and a classical part. In the quantum part, the transmitter Alice sends qubits to the receiver Bob to share a raw key (random binary sequence), which may be partially known to the eavesdropper, Eve. In the classical part, first Alice and Bob optionally perform two-way preprocessing. Then, the receiver Bob corrects his raw key so that his final key will be identical to Alice's final key. Finally, Alice and Bob perform the privacy amplification to extract a shorter but secret key from the raw key, about which Eve knows little information.

For the key distribution protocol to be practical, we have to perform the error correction and the privacy amplification efficiently. Based on the security proof of the BB84 protocol in Refs. 21 and 23, we use a pair of linear codes C_1 and C_2 with $C_2 \subset C_1$. The linear code C_1 is used for error correction, and the linear code C_2 is used for the privacy amplification. In order that the BB84 protocol is secure, the decoding error probability of C_1 and $C_2^\perp$ regarded as a Calderbank–Shor–Stean (CSS) code have to be small. As a practical requirement, the linear code C_1 have to be efficiently decodeable, while the linear code C_2 need not to be efficiently decodeable. It is difficult to find a pair of linear codes C_1 and C_2 that satisfy the above conditions. Mayers showed that if one arbitrarily fixes C_1 and chooses C_2 with rate $\mathrm{h}(2p)$ at random from subcodes of C_1, the minimum Hamming weight of $C_2^\perp \backslash C_1^\perp$ is greater than pn with high probability (Lemma 4 in Ref. 21), where p is estimated error rate and $\mathrm{h}(\cdot)$ is the binary entropy function. Consequently, the decoding error probability of $C_2^\perp$ regarded as a CSS code is small. When we use a linear code C_1 with rate close to $1-\mathrm{h}(p)$, Mayers' evaluation guarantees the secure key rate $1-\mathrm{h}(p)-\mathrm{h}(2p)$, which is lower than the achievable rate $1-2\mathrm{h}(p)$ given in Ref. 23. In this paper, we call the random privacy amplification as the method such that one chooses C_2 at random from subcodes of a fixed code C_1 and performs the privacy amplification by C_2.

By evaluating directly the decoding error probability of $C_2^\perp$ instead of the minimum Hamming weight, we can decrease the rate of C_2 while maintaining the security of the protocol. This paper shows that when one chooses C_2 with rate $\mathrm{h}(p)$ at random from subcodes of C_1, the decoding error probability of $C_2^\perp$ regarded as a CSS code is exponentially small with high probability.

It should be noted that the random privacy amplification (without two-way preprocessing) is known to be secure with rate $\mathrm{h}(p)$ according to Refs. 8 and 22. However, the proof method in Refs. 8 and 22 relies on the result in Ref. 17, which is only applicable to the QKD with one-way classical communication (Footnote 6 in Ref. 22), and it is not known how to extend that method to the QKD with two-way classical communications. On the other hand, the proof method of Ref. 23 is extended to the security proof of QKD with two-way classical communications,[13] and our result is valid for the BB84 protocol with two-way classical communications.

It should be also noted that our result is different from previously known results based on security proof method in Ref. 23. In Lemma 4 of Ref. 21, it is proved that if we fix C_1 of rate $1-\mathrm{h}(p)$ and choose its subcode C_2 of rate $\mathrm{h}(2p)$ at random, the

BB84 protocol is secure. In Ref. 23, they also cite Lemma 4 of Ref. 21 to show that we can securely choose a random subcode C_2 of an efficiently decodeable code C_1. However, it is not clarified in Ref. 23 that we can securely choose C_2 at random with rate $\mathrm{h}(p)$. Other previous papers[12,13,16,18,24] are based on the result in Ref. 23. We also stress that the random hashing method cannot be directly applied to the security proof of the BB84 protocol with random privacy amplification as used in Ref. 19, because a fixed C_1 and the condition $C_2 \subset C_1$ decrease the randomness of hashing. Application of the random hashing to a security proof of the random privacy amplification requires a careful argument similar to Sec. 3 of this paper. Although an idea to decouple the error correction and the privacy amplification in the random hashing was proposed in Ref. 25, a rigorous proof was not shown.

This paper is organized as follows. In Sec. 2, we review the Calderbank–Shor–Stean (CSS) code and the BB84 protocol. In Sec. 3, we show our main result. In Sec. 4, the secure key rate of the protocol is discussed.

2. Calderbank–Shor–Stean Code and BB84 Protocol

2.1. *Calderbank–Shor–Steane code*

In this section, we review the CSS code,[4] which is relevant to the security of the BB84 protocol.[23] Let $\mathcal{H}$ be the two-dimensional complex linear space (qubit) with an orthonormal basis $\{|0\rangle, |1\rangle\}$. We use another orthonormal basis $\{|+\rangle, |-\rangle\}$ of $\mathcal{H}$, where $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Let $\mathbf{F}_2$ be a finite field of order 2, and $\mathbf{F}_2^n$ be the n-dimensional vector space on $\mathbf{F}_2$. For a vector $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbf{F}_2^n$, define the quantum state

$$|\boldsymbol{x}\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle.$$

Define unitary matrices σ_x and σ_z on $\mathcal{H}$ by

$$\sigma_x|i\rangle = |i+1\rangle, \qquad \sigma_z|i\rangle = (-1)^i|i\rangle, \quad i \in \mathbf{F}_2.$$

For a vector $\boldsymbol{e} = (e_1, \ldots, e_n) \in \mathbf{F}_2^n$, define the unitary matrix

$$\sigma_a^{[\boldsymbol{e}]} = \sigma_a^{e_1} \otimes \cdots \otimes \sigma_a^{e_n},$$

where $a \in \{x, z\}$ and σ_a^0 is the identity matrix on $\mathcal{H}$.

A CSS code $\mathcal{Q} \subset \mathcal{H}^{\otimes n}$ is constructed from two linear codes C_1 and C_2 that satisfy $C_2 \subset C_1 \subset \mathbf{F}_2^n$, where $\dim C_1 = m_1$ and $\dim C_2 = m_2$. Let $C_1^\perp$ and $C_2^\perp$ be dual spaces of C_1 and C_2, respectively. A CSS code $\mathcal{Q} \subset \mathcal{H}^{\otimes n}$ is spanned by

$$|\phi_{\boldsymbol{u}}\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{\boldsymbol{w} \in C_2} |\boldsymbol{u} + \boldsymbol{w}\rangle \quad \boldsymbol{u} \in C_1.$$

For vectors $\boldsymbol{x}, \boldsymbol{z} \in \mathbf{F}_2^n$, a subspace $\mathcal{Q}_{\boldsymbol{xz}} \subset \mathcal{H}^{\otimes n}$ is spanned by

$$|\phi_{\boldsymbol{uxz}}\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{\boldsymbol{w} \in C_2} (-1)^{\boldsymbol{z}\cdot\boldsymbol{w}} |\boldsymbol{u} + \boldsymbol{w} + \boldsymbol{x}\rangle \quad \boldsymbol{u} \in C_1,$$

and $\mathcal{Q}_{\boldsymbol{xz}}$ is also called a CSS code.

In the recovery process of the CSS code, bit flip error correction and phase flip error correction is decoupled from each other. The linear code C_1 is related to the bit flip error correction and the linear code $C_2^\perp$ is related to the phase flip error correction. Let $\mathcal{E}_x \subset \mathbf{F}_2^n$ be the set such that the set $\{\sigma_x^{[\boldsymbol{e}]} \mid \boldsymbol{e} \in \mathcal{E}_x\}$ is the set of uncorrectable bit flip errors of the CSS code, and $\mathcal{E}_z \subset \mathbf{F}_2^n$ be the set such that the set $\{\sigma_z^{[\boldsymbol{e}]} \mid \boldsymbol{e} \in \mathcal{E}_z\}$ is the set of uncorrectable phase flip errors of the CSS code.

Definition 1. We define the decoding error probability of C_1 regarded as a CSS code over a BSC (binary symmetric channel) whose crossover probability is q as

$$P_{\mathrm{err}}(C_1, q) = \sum_{\boldsymbol{e} \in \mathcal{E}_x} Q^n(\boldsymbol{e}),$$

where $Q(0) = 1-q,\ Q(1) = q$, and $Q^n(\boldsymbol{e}) = Q(e_1) \times \cdots \times Q(e_n)$ for $\boldsymbol{e} = (e_1, \ldots, e_n)$. Similarly, we define the decoding error probability of $C_2^\perp$ regarded as a CSS code over a BSC whose crossover probability is q as

$$P_{\mathrm{err}}(C_2^\perp, q) = \sum_{\boldsymbol{e} \in \mathcal{E}_z} Q^n(\boldsymbol{e}).$$

The decoding error probability $P_{\mathrm{err}}(C_1, q)$ represents the decoding error probability of bit flip errors, and the decoding error probability $P_{\mathrm{err}}(C_2^\perp, q)$ represents the decoding error probability of phase flip errors. See Ref. 16 for the formal definition of $\mathcal{E}_x$ and $\mathcal{E}_z$. We discuss $P_{\mathrm{err}}(C_2^\perp, q)$ and $\mathcal{E}_z$ in Sec. 3 of this paper. $P_{\mathrm{err}}(C_1, q)$ and $P_{\mathrm{err}}(C_2^\perp, q)$ are used to lower bound the fidelity of the transmitted state suffered by the noise and the recovery operation (Eq. (27) in Ref. 16). These facts follow from the theory of symplectic codes (stabilizer code).[6,7,11,15]

2.2. *BB84 protocol*

In this section, we review the BB84 protocol with one-way or two-way classical communications. The idea of the BB84 protocol with two-way classical communications is first proposed in Ref. 13 by extending the result of Ref. 23 to the two-way entanglement purification protocol (EPP).[2] The protocol consists of transmission of raw key (Steps i–iv), estimation about eavesdropper (Steps v–vii), two-way preprocessing (Step viii), error correction (Steps ix and x), and privacy amplification (Step xi). The protocol without two-way preprocessing (Step viii) is exactly the BB84 protocol with one-way classical communication. For a sequence $\boldsymbol{k} \in \mathbf{F}_2^N$ and a subset $\mathsf{T} \subset \{1, \ldots, N\}$, we denote the subsequence of $\boldsymbol{k}$ that consist of ith bit with $i \in \mathsf{T}$ by $\boldsymbol{k}_{\mathsf{T}}$.

(i) Alice chooses a binary vector $\boldsymbol{a} \in \mathbf{F}_2^N$, where $\Pr\{a_i = 1\} = 1/2$. Alice chooses a random binary vector $\boldsymbol{k} \in \mathbf{F}_2^N$.

(ii) Alice repeats the following procedures for $1 \le i \le N$. If $a_i = 0$, Alice sends either state $|0\rangle$ for $k_i = 0$ or $|1\rangle$ for $k_i = 1$. If $a_i = 1$, Alice sends either state $|+\rangle$ for $k_i = 0$ or $|-\rangle$ for $k_i = 1$.

(iii) Bob chooses a binary vector $\boldsymbol{b} \in \mathbf{F}_2^N$, where $\Pr\{b_i = 1\} = 1/2$.

(iv) Bob repeats the following procedures for $1 \leq i \leq N$. If $b_i = 0$, he measures ith received qubit with σ_z. If $b_i = 1$, he measures ith received qubit with σ_x. If the measurement result of ith received qubit is $+1$ (-1), then Bob sets $\tilde{k}_i = 0$ $(\tilde{k}_i = 1)$. After these procedures Bob will obtain $\tilde{\boldsymbol{k}} = (\tilde{k}_1, \ldots, \tilde{k}_N)$.

(v) Alice announces $\boldsymbol{a}$.

(vi) If $a_i \neq b_i$, Alice and Bob discard ith bit of $\boldsymbol{k}$, and $\tilde{\boldsymbol{k}}$, respectively. Let $\mathsf{R}_0 = \{i \mid a_i = b_i = 0\} \subset \{1, \ldots, N\}$ and $\mathsf{R}_1 = \{i \mid a_i = b_i = 1\} \subset \{1, \ldots, N\}$. $\mathsf{R} = \mathsf{R}_0 \cup \mathsf{R}_1$ are the remaining positions. Alice and Bob randomly divide R_0 into S_0 and T_0, and R_1 into S_1 and T_1. $\mathsf{S} = \mathsf{S}_0 \cup \mathsf{S}_1$ are the positions for generating a final key, and $\mathsf{T} = \mathsf{T}_0 \cup \mathsf{T}_1$ are the positions for estimating error rates. We assume $|\mathsf{S}_0| = |\mathsf{S}_1| = |\mathsf{T}_0| = |\mathsf{T}_1| = N'$.

(vii) Alice and Bob compare $\boldsymbol{k}_\mathsf{T}$ and $\tilde{\boldsymbol{k}}_\mathsf{T}$, and estimate error rates from $\boldsymbol{t}_x = \boldsymbol{k}_{\mathsf{T}_0} - \tilde{\boldsymbol{k}}_{\mathsf{T}_0}$ and $\boldsymbol{t}_z = \boldsymbol{k}_{\mathsf{T}_1} - \tilde{\boldsymbol{k}}_{\mathsf{T}_1}$. Alice and Bob choose a random permutation π on $\{1, \ldots, N'\}$.

(viii) Let $\boldsymbol{l} = \pi(\boldsymbol{k}_{\mathsf{S}_0})$ and $\tilde{\boldsymbol{l}} = \pi(\tilde{\boldsymbol{k}}_{\mathsf{S}_0})$. Alice and Bob perform the two-way preprocessing (see Sec. 7 of Ref. 13) appropriate times.

(ix) Let $\boldsymbol{m} \in \mathbf{F}_2^n$ and $\tilde{\boldsymbol{m}} \in \mathbf{F}_2^n$ be Alice and Bobs' remaining sequences in Step viii respectively. Alice chooses a random codeword $\boldsymbol{u} \in C_1$, and announces $\boldsymbol{u} + \boldsymbol{m}$.

(x) Bob subtracts $\tilde{\boldsymbol{m}}$ from $\boldsymbol{u} + \boldsymbol{m}$ and corrects $\boldsymbol{u} + \boldsymbol{e}$ to a code word $\tilde{\boldsymbol{u}} \in C_1$, where $\boldsymbol{e} = \boldsymbol{m} + \tilde{\boldsymbol{m}}$.

(xi) Alice uses the coset $\boldsymbol{u} + C_2$ as the final key, and Bob uses the coset $\tilde{\boldsymbol{u}} + C_2$ as the final key.

We can generate the final key from $\boldsymbol{k}_{\mathsf{S}_1}$ and $\tilde{\boldsymbol{k}}_{\mathsf{S}_1}$ in the same way, where $\boldsymbol{k}_{\mathsf{S}_1}$ and $\tilde{\boldsymbol{k}}_{\mathsf{S}_1}$ are the raw keys transmitted in the $\{|+\rangle, |-\rangle\}$ basis. Before Steps ix–xi, Alice and Bob decide a pair of linear codes C_1 and C_2 according to estimated error rates and the result of two-way preprocessing.

Let p_x and p_z be $p_x = P_{\boldsymbol{t}_x}(1) + \delta$ and $p_z = P_{\boldsymbol{t}_z}(1) + \delta$, where $P_{\boldsymbol{t}_x}$ and $P_{\boldsymbol{t}_z}$ are the types[10] of $\boldsymbol{t}_x$ and $\boldsymbol{t}_z$, respectively, and $\delta > 0$ is a sufficiently small constant. Then, the bit error rate $\hat{p}_x$ and phase error rate $\hat{p}_z$ after two-way preprocessing are calculated from p_x, p_z (see Ref. 13). The conditions for the protocol to be secure is given as follows.

(i) If C_1 is used over a BSC whose crossover probability is smaller than $\hat{p}_x$, then the decoding error probability of C_1 regarded as a CSS code is smaller than or equal to ε, i.e. $P_{\mathrm{err}}(C_1, q) \leq \varepsilon \ \forall q \leq \hat{p}_x$.

(ii) If $C_2^\perp$ is used over a BSC whose crossover probability is smaller than $\hat{p}_z$, then the decoding error probability of $C_2^\perp$ regarded as a CSS code is smaller than or equal to ε, i.e. $P_{\mathrm{err}}(C_2^\perp, q) \leq \varepsilon \ \forall q \leq \hat{p}_z$.

Note that δ is required due to the deviation of estimated error rate from the error rate on the raw key bits (Lemma 3 in Ref. 13). Note also that ε is a small positive number decided from the acceptable level of Eve's information about the final key.

Although Eve's eavesdropping on each qubit is not independently identical, the use of random permutation π in the protocol enables us to securely use linear codes C_1 and C_2 whose decoding error probability regarded as a CSS code is small over the BSC[13,16,23]. We stress that the decoding error probabilities of C_1 and $C_2^\perp$ have to be small over any BSCs with crossover probabilities below $\hat{p}_x$ and $\hat{p}_z$, instead of a single pair of BSCs with crossover probabilities $\hat{p}_x$ and $\hat{p}_z$ in the conditions (i) and (ii), respectively. The necessity of such a requirement on decoding error probability is already observed in the proof of Lemma 3 in Ref. 13 or in Ref. 16.

3. Random Privacy Amplification

To implement the BB84 protocol, we need a linear code C_1 to be efficiently decodeable, which is used for error correction in Step x. Under the conditions (i) and (ii) of Sec. 2.2 and the condition $C_2 \subset C_1$, it is difficult to find a pair of linear codes C_1 and C_2 of which C_1 is efficiently decodeable. On the other hand, since we do not decode $C_2^\perp$ in the BB84 protocol, we can evaluate the condition (ii) with an arbitrary decoding method. Therefore, first we choose a code C_1 that satisfies the condition (i) and is efficiently decodeable. Then we will find a code C_2 that satisfies the conditions (ii) and $C_2 \subset C_1$. Given a code C_1, choosing a code C_2 with the condition $C_2 \subset C_1$ is same as choosing a code $C_2^\perp$ that satisfies $C_1^\perp \subset C_2^\perp$.

If we fix a rate R lower than $1 - \mathrm{h}(2\hat{p}_z)$ and choose a code $C_2^\perp$ of rate R at random with the condition $C_1^\perp \subset C_2^\perp$, then with high probability the condition (ii) is satisfied (Lemma 4 in Ref. 21). In this section, we will prove that if we fix a rate R lower than $1 - \mathrm{h}(\hat{p}_z)$ and choose a code $C_2^\perp$ of rate R at random with the condition $C_1^\perp \subset C_2^\perp$, with high probability the condition (ii) will be satisfied. Some ideas used in the proof are borrowed from Refs. 14 and 20.

3.1. *The code for privacy amplification*

Given a code $C_1^\perp$ of dimension $n - m_1$, fix a rate $R = \frac{n-m_2}{n} < 1 - \mathrm{h}(\hat{p}_z)$, and let

$$\mathsf{A} = \left\{ C_2^\perp \subset \mathbf{F}_2^n \mid C_2^\perp \text{ is a linear space}, \dim C_2^\perp = n - m_2,\ C_1^\perp \subset C_2^\perp \right\}$$

be the set from which we choose a code $C_2^\perp$.

Theorem 1. If we choose a code $C_2^\perp$ at random from A, for arbitrary $\mu > 0$, we have

$$\begin{aligned} &\Pr\left\{ P_{\mathrm{err}}(C_2^\perp, q) \le (n+1)^2 \exp\{-n(E(R,\hat{p}_z) - \mu)\} \ \ \forall\, q \le \hat{p}_z \right\} \\ &\qquad \ge 1 - (n+1)\exp\{-\mu n\}, \end{aligned}$$

where

$$E(R,\hat{p}_z) = \min_p \left[\mathrm{D}(p\|\hat{p}_z) + |1 - R - \mathrm{h}(p)|^+ \right],$$

the base of $\exp(\cdot)$ is 2, $|x|^+ = \max\{x, 0\}$, and $\mathrm{D}(\cdot\|\cdot)$ is the Kullback–Leibler information.[9] Note that $\min_p$ is taken over $0 \le p \le 1$. Since $\mathrm{D}(p\|\hat{p}_z) = 0$ if and only if $p = \hat{p}_z$, and $R < 1 - \mathrm{h}(\hat{p}_z)$, we have $E(R, \hat{p}_z) > 0$.

Consequently, we can obtain a code $C_2^\perp$ that satisfies the condition (ii) with high probability by choosing a code at random from A.

3.2. *Proof of the theorem*

Refer to Ref. 10 for the method of type used in this section. The type of a vector $\boldsymbol{e} \in \mathbf{F}_2^n$ is denoted by $P_{\boldsymbol{e}}$, the set of all types of vectors in $\mathbf{F}_2^n$ is denoted by P_n, and for $Q \in P_n$ the set of all vectors of type Q is denoted by T_Q^n. We use the following bounds

$$\begin{aligned} |P_n| &\le (n+1), \\ |T_Q^n| &\le \exp\{n\mathrm{h}(Q)\} \quad \forall\, Q \in P_n, \\ p^n(T_Q^n) &\le \exp\{-n\mathrm{D}(Q\|p)\}, \end{aligned}$$

where $\mathrm{h}(Q)$ is the entropy of the distribution $Q(a)$ over $\mathbf{F}_2$.

To evaluate the decoding error probability, we employ the minimum entropy decoding. In the minimum entropy decoding, we choose a coset representative $\boldsymbol{z}$ from each coset of $\mathbf{F}_2/C_2^\perp$ such that $\mathrm{h}(P_{\boldsymbol{z}})$ is the minimum in the coset $\boldsymbol{z} + C_2^\perp$. Let

$$\mathcal{E}(C_2^\perp) = \left\{ \boldsymbol{e} \in \mathbf{F}_2^n \mid \exists \boldsymbol{e}'\ \mathrm{h}(P_{\boldsymbol{e}'}) \le \mathrm{h}(P_{\boldsymbol{e}}),\ \boldsymbol{e} + \boldsymbol{e}' \in C_2^\perp \backslash C_1^\perp \right\}.$$

From the general theory of symplectic codes and the property of the minimum entropy decoding,[14] we have $\mathcal{E}_z \subset \mathcal{E}(C_2^\perp)$. Thus, we evaluate the probability

$$P'_{\mathrm{err}}(C_2^\perp, q) = \sum_{\boldsymbol{e} \in \mathcal{E}(C_2^\perp)} Q^n(\boldsymbol{e}).$$

Observe that $P_{\mathrm{err}}(C_2^\perp, q) \le P'_{\mathrm{err}}(C_2^\perp, q)$.

We classify $\mathcal{E}(C_2^\perp)$ by the types in P_n as

$$\mathcal{E}(C_2^\perp) = \cup_{P \in P_n} \mathcal{E}_P(C_2^\perp),$$

where $\mathcal{E}_P(C_2^\perp) = \mathcal{E}(C_2^\perp) \cap T_P^n$. First, we prove the following lemma.

Lemma 1. *If we choose a code $C_2^\perp$ at random from A, for arbitrary $\mu > 0$, we have*

$$\begin{aligned} &\Pr\left\{ \frac{|\mathcal{E}_P(C_2^\perp)|}{|T_P^n|} \le \exp\{-n(|1 - \mathrm{h}(P) - R|^+ - \mu)\} \quad \forall\, P \in P_n \right\} \\ &\qquad \ge 1 - (n+1)\exp\{-\mu n\}. \end{aligned}$$

Proof. We evaluate the average of $\frac{|\mathcal{E}_P(C_2^\perp)|}{|T_P^n|}$ over $C_2^\perp \in \mathsf{A}$. Define the set of codes that cannot correct $\boldsymbol{e}$ as

$$\mathsf{B}(\boldsymbol{e}) = \left\{C_2^\perp \in \mathsf{A} \mid \boldsymbol{e} \in \mathcal{E}(C_2^\perp)\right\}.$$

Define $\mathsf{C}(\boldsymbol{e})$ as

$$\mathsf{C}(\boldsymbol{e}) = \left\{C_2^\perp \in \mathsf{A} \mid \boldsymbol{e} \in C_2^\perp \backslash C_1^\perp\right\}$$

and G as the set of bijective linear maps α on $\mathbf{F}_2^n$ that satisfies $\alpha(C_1^\perp) = C_1^\perp$. Then we have the following equalities:

$$\begin{aligned}
|\mathsf{C}(\boldsymbol{e})| &= \left|\left\{C_2^\perp \in \mathsf{A} \mid \boldsymbol{e} \in C_2^\perp \backslash C_1^\perp\right\}\right| \\
&= \left|\left\{\alpha(C_2^\perp) \mid \boldsymbol{e} \in \alpha(C_2^\perp \backslash C_1^\perp), \alpha \in G,\ C_2^\perp \text{ is fixed}\right\}\right| \\
&= \left|\left\{\beta\alpha(C_2^\perp) \mid \beta(\boldsymbol{e}) \in \beta\alpha(C_2^\perp \backslash C_1^\perp),\ \alpha, \beta \in G, \beta \text{ and } C_2^\perp \text{ are fixed}\right\}\right|.
\end{aligned}$$

Since there exists $\beta \in G$ such that $\boldsymbol{e}' = \beta(\boldsymbol{e})$ for arbitrary $\boldsymbol{e}$ and $\boldsymbol{e}' \in \mathbf{F}_2^n \backslash C_1^\perp$, $|\mathsf{C}(\boldsymbol{e})|$ does not depend on $\boldsymbol{e} \in \mathbf{F}_2^n \backslash C_1^\perp$ and

$$\begin{aligned}
|\mathsf{C}(\boldsymbol{e})| &= \frac{\sum_{\boldsymbol{e} \in \mathbf{F}_2^n \backslash C_1^\perp} |\mathsf{C}(\boldsymbol{e})|}{|\mathbf{F}_2^n \backslash C_1^\perp|} \\
&= \frac{\sum_{\boldsymbol{e} \in \mathbf{F}_2^n \backslash C_1^\perp} |\{C_2^\perp \in \mathsf{A} \mid \boldsymbol{e} \in C_2^\perp \backslash C_1^\perp\}|}{|\mathbf{F}_2^n \backslash C_1^\perp|} \\
&= \frac{\sum_{C_2^\perp \in \mathsf{A}} |\{\boldsymbol{e} \in \mathbf{F}_2^n \backslash C_1^\perp \mid \boldsymbol{e} \in C_2^\perp \backslash C_1^\perp\}|}{|\mathbf{F}_2^n \backslash C_1^\perp|} \\
&= \frac{|C_2^\perp \backslash C_1^\perp||\mathsf{A}|}{|\mathbf{F}_2^n \backslash C_1^\perp|}.
\end{aligned}$$

From the definition, it is obvious that $|\mathsf{C}(\boldsymbol{e})| = 0$ for $\boldsymbol{e} \in C_1^\perp$. Hence

$$\begin{aligned}
|\mathsf{C}(\boldsymbol{e})| &\le \frac{|C_2^\perp \backslash C_1^\perp||\mathsf{A}|}{|\mathbf{F}_2^n \backslash C_1^\perp|} \\
&= \frac{2^{n-m_2} - 2^{n-m_1}}{2^n - 2^{n-m_1}}|\mathsf{A}| \\
&= \frac{|\mathsf{A}|}{2^{m_2}} \frac{1 - 2^{m_2 - m_1}}{1 - 2^{-m_1}} \\
&\le \frac{|\mathsf{A}|}{2^{m_2}} \\
&= |\mathsf{A}| \exp\{-n(1-R)\}.
\end{aligned}$$

Because the condition for $C_2^{\perp} \in \mathsf{A}$ to belong to $\mathsf{B}(\boldsymbol{e})$ is $\exists \boldsymbol{e}',\ \mathrm{h}(P_{\boldsymbol{e}'}) \le \mathrm{h}(P_{\boldsymbol{e}}),\ \boldsymbol{e}+\boldsymbol{e}' \in C_2^{\perp} \backslash C_1^{\perp}$, we obtain

$$\begin{aligned}\frac{|\mathsf{B}(e)|}{|\mathsf{A}|} &\le \frac{1}{|\mathsf{A}|} \sum_{\substack{\boldsymbol{e}' \in \mathbf{F}_2^n \\ \mathrm{h}(P_{\boldsymbol{e}'}) \le \mathrm{h}(P_{\boldsymbol{e}})}} |\mathsf{C}(\boldsymbol{e}+\boldsymbol{e}')| \\ &\le \sum_{\substack{\boldsymbol{e}' \in \mathbf{F}_2^n \\ \mathrm{h}(P_{\boldsymbol{e}'}) \le \mathrm{h}(P_{\boldsymbol{e}})}} \exp\{-n(1-R)\}.\end{aligned}$$

We also have a trivial upper bound $\frac{|\mathsf{B}(e)|}{|\mathsf{A}|} \le 1$. Thus we have

$$\frac{|\mathsf{B}(e)|}{|\mathsf{A}|} \le \min\left\{ \sum_{\substack{\boldsymbol{e}' \in \mathbf{F}_2^n \\ \mathrm{h}(P_{\boldsymbol{e}'}) \le \mathrm{h}(P_{\boldsymbol{e}})}} \exp\{-n(1-R)\}, 1 \right\}.$$

Let $|x|^+ = \max\{x, 0\}$ and note that if $a, b \ge 0$, then $\min\{a+b, 1\} \le \min\{a, 1\} + \min\{b, 1\}$. Using the above definitions, we have

$$\begin{aligned}&\frac{1}{|\mathsf{A}|} \sum_{C_2^{\perp} \in \mathsf{A}} \frac{|\mathcal{E}_P(C_2^{\perp})|}{|T_P^n|} \\ &\quad= \frac{1}{|T_P^n|} \sum_{\boldsymbol{e} \in T_P^n} \frac{|\mathsf{B}(\boldsymbol{e})|}{|\mathsf{A}|} \\ &\quad\le \frac{1}{|T_P^n|} \sum_{\boldsymbol{e} \in T_P^n} \min\left\{ \sum_{\substack{\boldsymbol{e}' \in \mathbf{F}_2^n \\ \mathrm{h}(P_{\boldsymbol{e}'}) \le \mathrm{h}(P_{\boldsymbol{e}})}} \exp\{-n(1-R)\}, 1 \right\} \\ &\quad= \min\left\{ \sum_{\substack{P' \in P_n \\ \mathrm{h}(P') \le \mathrm{h}(P)}} |T_{P'}^n| \exp\{-n(1-R)\}, 1 \right\} \\ &\quad\le \sum_{\substack{P' \in P_n \\ \mathrm{h}(P') \le \mathrm{h}(P)}} \exp\{-n|1-R-\mathrm{h}(P')|^+\} \\ &\quad\le |P_n| \max_{\substack{P' \in P_n \\ \mathrm{h}(P') \le \mathrm{h}(P)}} \exp\{-n|1-R-\mathrm{h}(P')|^+\} \\ &\quad\le (n+1) \exp\{-n|1-R-\mathrm{h}(P)|^+.\end{aligned}$$

Let A_P and A_g be

$$\begin{aligned}\mathsf{A}_P &= \left\{ C_2^{\perp} \in \mathsf{A} \mid \frac{|\mathcal{E}_P(C_2^{\perp})|}{|T_P^n|} > (n+1) \exp\{-n(|1-R-\mathrm{h}(P)|^+ - \mu)\} \right\}, \\ \mathsf{A}_g &= \mathsf{A} \backslash \cup_{P \in P_n} \mathsf{A}_P.\end{aligned}$$

From the union bound and the Chebychev inequality, we have

$$\begin{aligned}\frac{|\mathsf{A}_g|}{|\mathsf{A}|} &= 1 - \frac{|\cup_{P\in P_n} \mathsf{A}_P|}{|\mathsf{A}|} \\ &\geq 1 - \sum_{P\in P_n} \frac{|\mathsf{A}_P|}{|\mathsf{A}|} \\ &\geq 1 - \sum_{P\in P_n} \frac{(n+1)\exp\{-n|1-R-\mathrm{h}(P)|^+\}}{(n+1)\exp\{-n(|1-R-\mathrm{h}(P)|^+ - \mu)\}} \\ &\geq 1 - (n+1)\exp\{-\mu n\}.\end{aligned}$$

□

The probability $P'_{\mathrm{err}}(C_2^\perp, q)$ of $C_2^\perp \in \mathsf{A}_g$ is upper bounded as

$$\begin{aligned}P'_{\mathrm{err}}(C_2^\perp, q) &= \sum_{\boldsymbol{e}\in\mathcal{E}(C_2^\perp)} Q^n(\boldsymbol{e}) \\ &= \sum_{P\in P_n} \sum_{\boldsymbol{e}\in\mathcal{E}_P(C_2^\perp)} Q^n(\boldsymbol{e}) \\ &= \sum_{P\in P_n} \frac{|\mathcal{E}_P(C_2^\perp)|}{|T_P^n|} Q^n(T_P^n) \\ &\leq \sum_{P\in P_n} (n+1)\exp\{-n(|1-R-\mathrm{h}(P)|^+ - \mu)\} \quad \text{(by Lemma 1)} \\ &\quad \times \exp\{-n\mathrm{D}(P||q)\} \\ &\leq |P_n| \max_{P\in P_n} (n+1)\exp\{-n(|1-R-\mathrm{h}(P)|^+ - \mu)\} \\ &\quad \times \exp\{-n\mathrm{D}(P||q)\} \\ &\leq (n+1)^2 \exp\{-nE(R,q) - \mu\},\end{aligned}$$

where

$$E(R,q) = \min_p \left[\mathrm{D}(p||q) + |1-R-\mathrm{h}(p)|^+\right].$$

We can rewrite $E(R,q)$ into the form

$$E(R,q) = \begin{cases} -R + 1 - 2\log(\sqrt{q} + \sqrt{1-q}) & \text{if } 0 \leq R < R', \\ \mathrm{D}(q^*||q) & \text{if } R' \leq R < 1 - \mathrm{h}(q), \end{cases}$$

where $R' = 1 - \mathrm{h}(q')$, $q' = \sqrt{q}/(\sqrt{q} + \sqrt{1-q})$, and q^* satisfies $R = 1 - \mathrm{h}(q^*)$ (see p. 168, pp. 192–193 of Ref. 10). Thus $E(R,q)$ is an increasing function of q for a fixed R, and we have $\min_{0\leq q\leq p_z} E(R,q) = E(R,p_z)$ and

$$P'_{\mathrm{err}}(C_2^\perp, q) \leq (n+1)^2 \exp\{-n(E(R,p_z) - \mu)\} \quad \forall\ q \leq p_z.$$

4. Secure Key Rate

In this section, we discuss the secure key rate of the BB84 protocol. When we use a linear code C_1 of rate close to $1 - \mathrm{h}(\hat{p}_x)$ and choose a linear code C_2 at random from subcodes of C_1, according to Lemma 4 in Ref. 21, the secure key rate after two-way preprocessing $R_{\mathrm{key}} = \frac{\dim C_1 - \dim C_2}{n}$ is about

$$1 - \mathrm{h}(\hat{p}_x) - \mathrm{h}(2\hat{p}_z).$$

According to our result in Sec. 3, the secure key rate is about

$$1 - \mathrm{h}(\hat{p}_x) - \mathrm{h}(\hat{p}_z).$$

Note that the secure key rate $1-\mathrm{h}(p_x)-\mathrm{h}(p_z)$ with the random privacy amplification in the BB84 protocol with one-way classical communication is already shown in Refs. 8 and 22, where p_x and p_z are error rates without two-way preprocessing.

5. Conclusion

In this paper, we have shown that for a fixed linear code C_1, if we choose a linear code $C_2 \subset C_1$ at random with rate $\mathrm{h}(\hat{p}_z)$, then C_2 satisfies the condition for the security with high probability. Consequently, when we use the random privacy amplification in the BB84 protocol with one-way or two-way classical communication, the secure key rate is increased and the protocol can tolerate more severe noise.

Acknowledgments

We appreciate the helpful comment by Dr. Masahito Hayashi on an earlier version of this paper. This research is partly supported by the Japan Society for the Promotion of Science under Grants–in–Aid for Young Scientists No. 16760289.

References

1. C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing*, Bangalore, India (1984), pp. 175–179.
2. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters, Mixed-state entanglement and quantum error correction, *Phys. Rev. A* **68**(5) (1996) 3824–3851. [quant-ph/9604024].
3. E. Biham, M. Boyer, P. O. Boykin, T. Mor and V. Ryoichowdhury, A proof of the security of quantum key distribution, in *Proc. 32nd Ann. ACM Symp. Theory of Computing*, New York (2000), pp. 715–724 [quant-ph/9912053].
4. A. R. Calderbank and P. W. Shor, Good quantum error correcting codes exist, *Phys. Rev. A* **54**(2) (1996) 1098–1105 [quant-ph/9512032].
5. H. F. Chau, Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate, *Phys. Rev. A* **66**(6) (2002) 060302 [quant-ph/0205060].
6. A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction and orthogonal geometry, *Phys. Rev. Lett.* **78**(3) (1997) 405–408 [quant-ph/9605005].

7. A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over $GF(4)$, *IEEE Trans. Inform. Theory* **44**(4) (1998) 1369–1387 [quant-ph/9608006].
8. M. Christandl, R. Renner and A. Ekert, A generic security proof for quantum key distribution, quant-ph/0402131v2.
9. T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
10. I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems* (Akademiai Kiado, 1981).
11. D. Gottesman, Class of quantum error-correcting codes saturating the quantum Hamming bound, *Phys. Rev. A* **54**(3) (1996) 1862–1868 [quant-ph/9604038].
12. D. Gottesman and J. Preskill, Secure quantum key distribution using squeezed states, *Phys. Rev. A* **63**(2) (2000) 022309 [quant-ph/0008046].
13. D. Gottesman and H.-K. Lo, Proof of security of quantum key distribution with two-way classical communications, *IEEE Trans. Inform. Theory* **49**(2) (2003) 457–475 [quant-ph/0105121].
14. M. Hamada, Exponential lower bound on the highest fidelity achievable by quantum error-correcting codes, *Phys. Rev. A* **65**(5) (2002) 052305 [quant-ph/0109114].
15. M. Hamada, Notes on the fidelity of symplectic quantum error-correcting codes, *Int. J. Quant. Inf.* **1**(4) (2003) 443–463 [quant-ph/0311003].
16. M. Hamada, Reliability of Calderbank-Shor-Steane codes and security of quantum key distribution, *J. Phys. A: Math. Gen.* **37**(34) (2004) 8303–8328 [quant-ph/0308029].
17. R. König, U. Maurer, and R. Renner, On the power of quantum memory, *IEEE Trans. Inform. Theory* **51**(7) (2005) 2391–2401 [quant-ph/0305154].
18. H.-K. Lo, H. F. Chau and M. Ardehali, Efficient quantum key distribution scheme and proof of its unconditional security, *J. Cyptol.* **18**(2) (2005) 133–165 [quant-ph/0011056].
19. H.-K. Lo, Proof of unconditional security of six-state quantum key distribution scheme, *Quant. Inform. Comput.* **1**(2) (2001) 81–94 [quant-ph/0102138].
20. R. Matsumoto and T. Uyematsu, Lower bound for the quantum capacity of a discrete memoryless quantum channel, *J. Math. Phys.* **43**(9) (2002) 4391–4403 [quant-ph/0105151].
21. D. Mayers, Unconditional security in quantum cryptography, *J. ACM* **48**(3) (2001) 351–406 [quant-ph/9802025].
22. R. Renner, N. Gisin and B. Kraus, Information-theoretic security proof for quantum-key-distribution protocols, *Phys. Rev. A* **72** (2005) 012332 [quant-ph/0502064].
23. P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, *Phys. Rev. Lett.* **85**(2) (2000) 441–444 [quant-ph/0003004].
24. X.-B. Wang, Quantum key distribution with asymmetric channel noise, *Phys. Rev. A* **71** (2005) 052328 [quant-ph/0406099].
25. X.-B. Wang, BDSW protocol revisited: an efficient method for the key distillation without classical computational complexity, quant-ph/0409099v2.