IEICE TRANS. FUNDAMENTALS, VOL.E91–A, NO.10 OCTOBER 2008

LETTER *Special Section on Information Theory and Its Applications*

Key Rate Available from Mismatched Measurements in the BB84 Protocol and the Uncertainty Principle

Ryutaroh MATSUMOTO[†a)], ***Member and*** **Shun WATANABE**[†], ***Student Member***

SUMMARY We consider the mismatched measurements in the BB84 quantum key distribution protocol, in which measuring bases are different from transmitting bases. We give a lower bound on the amount of a secret key that can be extracted from the mismatched measurements. Our lower bound shows that we can extract a secret key from the mismatched measurements with certain quantum channels, such as the channel over which the Hadamard matrix is applied to each qubit with high probability. Moreover, the entropic uncertainty principle implies that one cannot extract the secret key from both matched measurements and mismatched ones simultaneously, when we use the standard information reconciliation and privacy amplification procedure.

key words: *BB84, mismatched measurement, quantum key distribution*

1. Introduction

The BB84 protocol [1] is one of the most-known protocols for quantum key distribution. In this protocol, the sender, Alice, sends qubits in one of four quantum state vectors $|0\rangle$, $|1\rangle$, $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, where $\{|0\rangle, |1\rangle\}$ forms an orthonormal basis. Then the receiver, Bob, measures the received qubits with either $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ basis. After that, Alice publicly announces to which $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ basis each qubit belong. Bob discard the measurement outcomes whose bases do not contain the transmitted qubit. We call such measurement *mismatched measurement* in this paper. After that, Alice and Bob perform the information reconciliation and the privacy amplification to obtain the same secret key as described in [12].

As far as the authors know, there is no literature that clarifies the amount of key that can be extracted from mismatched measurements in the BB84 protocol, though Pawlowski [10] studied the same problem with a protocol completely different from the BB84. The efficiency of a quantum key distribution (QKD) protocol is measured by the ratio of extracted bits of secret key per remaining bits not disclosed nor discarded, which is called key rate. We shall show a lower bound on the key rate that can be extracted from mismatched measurements in the BB84 protocol. Moreover, we shall show that, when we use the standard information reconciliation and privacy amplification in [12] and the well-known lower bound on the key rate [4], the entropic uncertainty principle [8] implies that one cannot extract the secret key from both matched measurements and mismatched ones simultaneously.

The reader may think that the probability of getting the measurement outcome $|+\rangle$ is always 0.5 when the transmitted qubit is $|0\rangle$, and considering mismatched measurement outcomes is useless and nonsense. We cannot extract a secret key from mismatched measurement outcomes when such a probability is 0.5. However, consider the quantum channel over which the Hadamard matrix is applied to each qubit with high probability. With such a quantum channel the above probability is close to 0 or 1. The lower bound obtained in this paper shows that we can extract a secret key from mismatched measurement outcomes with such a quantum channel.

This paper is organized as follows: Section 2 presents a variant of the BB84 protocol. Section 3 verifies its unconditional security and shows a lower bound on its key rate. Section 4 shows that the lower bounds on the key rates available from matched measurements and mismatched ones cannot be simultaneously positive, by using the entropic uncertainty principle [8]. Section 5 gives concluding remarks and lists several open research questions.

2. Protocol

In this section, we shall show a variant of the BB84 protocol that tries to extract secret key from mismatched measurement outcomes. We define the matrices X and Z representing the bit error and the phase error, respectively, as

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle,$$
$$Z|+\rangle = |-\rangle, \quad Z|-\rangle = |+\rangle.$$

1. Alice makes a random qubit sequence according to the i.i.d. uniform distribution on $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sends it to Bob.
2. Bob chooses the $\{|0\rangle, |1\rangle\}$ basis or $\{|+\rangle, |-\rangle\}$ basis uniformly randomly for each received qubit and measure it by the chosen basis.
3. Alice publicly announces which basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ each transmitted qubit belongs to. Bob also publicly announces which basis was used for measurement of each qubit. In the following steps they will only consider qubits with which transmission basis and measuring bases *do not* coincide between Alice and Bob.
4. Suppose that there are $2n$ qubits transmitted in the $\{|0\rangle, |1\rangle\}$ basis and measured with the $\{|+\rangle, |-\rangle\}$ basis by Bob.

Manuscript received January 15, 2008.
Manuscript revised March 31, 2008.

[†]The authors are with the Department of Communications and Integrated Systems, Tokyo Institute of Technology, Tokyo, 152-8550 Japan.
a) E-mail: ryutaroh@rmatsumoto.org

DOI: 10.1093/ietfec/e91–a.10.2870

Copyright © 2008 The Institute of Electronics, Information and Communication Engineers

Index those qubits by $1, \ldots, 2n$. Define the bit $a_i = 0$ if Alice's i-th qubit was $|0\rangle$, and $a_i = 1$ otherwise. Define the bit $b_i = 0$ if Bob's measurement outcome for i-th qubit was $|+\rangle$, and $b_i = 1$ otherwise.

5. Suppose also that there are $2n'$ qubits transmitted in the $\{|+\rangle, |-\rangle\}$ basis and measured with the $\{|0\rangle, |1\rangle\}$ basis by Bob. Index those qubits by $1, \ldots, 2n'$. Define the bit $\alpha_i = 0$ if Alice's i-th qubit was $|+\rangle$, and $\alpha_i = 1$ otherwise. Define the bit $\beta_i = 0$ if Bob's measurement outcome for i-th qubit was $|0\rangle$, and $\beta_i = 1$ otherwise.

For the simplicity of the presentation, we shall describe the procedure extracting the secret key from a_i and b_i. The key rate for α_i, β_i will turn out to be the same as that for a_i, b_i at the end of Sect. 3.2. In the following steps, the half of measurement outcomes will be disclosed and used for estimation of error rates q_X and q_Z. The amount of disclosure can be arbitrarily chosen provided that the estimation of error rates can be done sufficiently accurately.

6. Alice chooses a subset $S \subset \{1, \ldots, 2n\}$ with size $|S| = n$ uniformly randomly from subsets of $\{1, \ldots, 2n\}$, and publicly announces the choice of S. Alice and Bob publicly announce a_i and b_i for $i \in S$ and compute the error rate
$$q_X = \frac{|\{i \in S \mid a_i \neq b_i\}|}{|S|}. \tag{1}$$
7. Alice chooses a subset $S' \subset \{1, \ldots, 2n'\}$ with size $|S'| = n'$ uniformly randomly from subsets of $\{1, \ldots, 2n'\}$, and publicly announces the choice of S'. Alice and Bob publicly announce α_i and β_i for $i \in S'$ and compute the error rate
$$q_Z = \frac{|\{i \in S' \mid \alpha_i \neq \beta_i\}|}{|S'|}. \tag{2}$$
8. Alice and Bob decide a linear code C_1 of length n such that its decoding error probability is sufficiently small over all the binary symmetric channel whose crossover probability is close to q_X. Let H_1 be a parity check matrix for C_1, $\vec{a}$ be Alice's remaining (not announced) bits among a_i's, and $\vec{b}$ be Bob's remaining bits among b_i's.
9. Alice publicly announces the syndrome $H_1\vec{a}$.
10. If $q_X > 0.5$ then Bob negates every bit in $\vec{b}$ before executing the following steps.
11. Bob compute the error vector $\vec{f}$ such that $H_1\vec{f} = H_1\vec{b} - H_1\vec{a}$ by the decoding algorithm for C_1. With high probability $\vec{b} - \vec{f} = \vec{a}$.
12. Alice chooses a subspace $C_2 \subset C_1$ with $\dim C_2 = nh(q_Z)$ uniformly randomly, where h denotes the binary entropy function, and publicly announces her choice of C_2. The final shared secret key is the coset $\vec{a} + C_2$.

When measuring bases are the same as the transmitting bases, we can use the standard BB84 protocol. Thus, we discard no measurement outcome when we combine the above protocol with the standard BB84.

3. Security Proof and a Lower Bound on the Key Rate

We shall verify the unconditional security of our proposed protocol by directly relating it to the quantum error correction by the quantum CSS (Calderbank-Shor-Steane) codes [2], [13]. To make this paper self-contained, we shall briefly review the CSS code. After that we shall relate our variant of the BB84 protocol to the CSS code in a similar way to Shor and Preskill [12].

3.1 Review of the CSS Code

For a binary vector $\vec{v} = (v_1, \ldots, v_n) \in \mathbf{F}_2^n$, where $\mathbf{F}_2$ is the Galois field with two elements, we define the quantum state vector $|\vec{v}\rangle$ by
$$|\vec{v}\rangle = |v_1\rangle \otimes \cdots \otimes |v_n\rangle.$$
For two binary linear codes $C_2 \subset C_1 \subset \mathbf{F}_2^n$, the CSS code is the complex linear space spanned by the vectors
$$\frac{1}{\sqrt{|C_2|}} \sum_{\vec{w} \in C_2} |\vec{v} + \vec{w}\rangle,$$
for all $\vec{v} \in C_1$. We also need parameterized CSS codes introduced in [12]. The parameterized CSS code for $\vec{x}, \vec{z} \in \mathbf{F}_2^n$ is defined as the linear space spanned by
$$\frac{1}{\sqrt{|C_2|}} \sum_{\vec{w} \in C_2} (-1)^{(\vec{z},\vec{w})} |\vec{x} + \vec{v} + \vec{w}\rangle, \tag{3}$$
for all $\vec{v} \in C_1$, where $(\cdot, \cdot)$ denotes the inner product.

3.2 Security Proof and Analysis of the Key Rate

We shall first show that our protocol is equivalent to sending a parameterized CSS codeword with the parameter $\vec{z}$ randomly chosen. If we fix $\vec{v}$ and $\vec{x}$ and choose $\vec{z}$ uniformly randomly in Eq. (3), then the resulting density operator is
$$\frac{1}{2^n|C_2|} \sum_{\vec{z} \in \mathbf{F}_2^n} \left(\sum_{\vec{w_1} \in C_2} (-1)^{(\vec{z},\vec{w_1})} |\vec{x} + \vec{v} + \vec{w_1}\rangle \right) \left(\sum_{\vec{w_2} \in C_2} (-1)^{(\vec{z},\vec{w_2})} \langle \vec{x} + \vec{v} + \vec{w_2}| \right) = \frac{1}{|C_2|} \sum_{\vec{w} \in C_2} |\vec{x} + \vec{v} + \vec{w}\rangle\langle \vec{x} + \vec{v} + \vec{w}|, \tag{4}$$
by the exactly same argument as [12].

Denote the right hand side of Eq. (4) by $\rho(\vec{x}, \vec{v})$. By a straightforward computation we can see
$$\frac{1}{2^n|C_1|} \sum_{\vec{x} \in \mathbf{F}_2^n} \sum_{\vec{v} \in C_1} \rho(\vec{x}, \vec{v}) = \frac{1}{2^n} \sum_{\vec{a} \in \mathbf{F}_2^n} |\vec{a}\rangle\langle\vec{a}|. \tag{5}$$
The right hand side of Eq. (5) means sending $|0\rangle$ or $|1\rangle$ n times with equal probability, which is exactly what Alice is

doing in our protocol. Announcing the syndrome $H_1\vec{a}$ in Step 9 is equivalent to announcing which $\vec{x}$ is chosen.

Consider the Hadamard matrix H defined by $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$. Consider the memoryless quantum channel Γ over which the error HX occurs with probability r_X, HZ occurs with probability r_Z, HXZ occurs with probability r_{XZ}, and H occurs with probability $1-r_X-r_Z-r_{XZ}$, with $q_X = r_X + r_{XZ}$ and $q_Z = r_Z + r_{XZ}$. The qubits received by Bob can be regarded as the output of Γ when Alice sends $|0\rangle$ and $|1\rangle$ with equal probability, which is equivalent to sending a quantum codeword in the CSS code as described above.

If we apply H^{-1} to each qubit, then the quantum channel can be regarded as causing the X error with probability r_X, the Z error with probability r_Z, and the XZ error with probability r_{XZ}. Therefore, if we use the standard decoding procedure of the CSS code after applying H^{-1} to each qubit in the received codeword, then the transmitted CSS codeword is recovered with high fidelity provided that $q_X < 0.5$ and $q_Z < 0.5$. Observe also that this imaginary quantum decoding process is equivalent to what is actually performed in our variant of the BB84 protocol described in Sect. 2 by the almost same argument as [12].

When $q_X > 0.5$ and $q_Z < 0.5$, applying X to each qubit in the received codeword after H^{-1} makes q_X to $1 - q_X$ and leaves q_Z unchanged. When $q_X < 0.5$ and $q_Z > 0.5$, apply Z to each qubit, and when $q_X > 0.5$ and $q_Z > 0.5$, apply XZ. By the above operations we can regard both q_X and q_Z being less than 0.5 provided that $q_X \neq 0.5$ and $q_Z \neq 0.5$. Observe that application of Z is purely imaginary and does not correspond to the actual operations in the protocol in Sect. 2. On the other hand, application of X corresponds to flipping each bit in Step 10 in our protocol. Application of XZ is equivalent to that of X in the actual protocol.

We have shown that the procedure in Sect. 2 can be regarded as the quantum error correction of the CSS code over a peculiar quantum channel Γ. It was shown in Corollary 2 of [3] that there exists a linear code C_1 of information rate $1 - h(q_X)$ satisfying the condition in Step 8. If we use such C_1 then we can correct HX errors on Γ with high probability.

It is stated in [12] and proved in [14] that random choice of $[n - nh(q_Z)]$-dimensional subspace C_2 in C_1 almost always gives the low phase error decoding probability in the standard CSS decoding procedure. This implies that randomly chosen $[n - nh(q_Z)]$-dimensional subspace C_2 in C_1 can almost always correct HZ errors on Γ. Therefore, if the choice of C_1 is appropriate, then the fidelity of quantum error correction in the imaginary transmission of the CSS codeword (3) over the channel Γ is close to 1, which implies that the eavesdropper Eve can obtain little information by the same argument as [5], which shows the security of the BB84 protocol directly relating it to the quantum error correction without use of entanglement distillation argument.

Therefore, we can extract $1-h(q_X)-h(q_Z)$ bit of secret key from one bit of the raw bits $\vec{a}$. With a similar argument, we can also see that the key rate available from α_i's is $1 - h(q_X) - h(q_Z)$. Because with the key rate from α_i's the roles of q_X and q_Z are interchanged, which does not change the key rate $1 - h(q_X) - h(q_Z)$.

4. Implication by the Uncertainty Principle

At the end of Sect. 2, we stated that we try to extract a secret key from both matched measurement outcomes and mismatched ones. In this section, we shall consider the relation between the amount of secret key extracted from matched measurement outcomes and that from mismatched ones. We shall show that we cannot extract secret key from both matched and mismatched measurement outcomes by the entropic version [8] of the uncertainty principle, when we use the information reconciliation and privacy amplification in [12] and the lower bound on its key rate in [4]. Note that Koashi already used the uncertainty principle for security analysis of QKD protocols [6].

Maassen and Uffink [8] (see also Box 11.1 of [9]) proved the following version of uncertainty principle in terms of the Shannon entropy. Let ρ be a density operator of a qubit. Let P_{01} (resp. P_{+-}) be the probability distribution of the measurement outcome by measuring ρ by $\{|0\rangle, |1\rangle\}$ (resp. $\{|+\rangle, |-\rangle\}$). Let $H(\cdot)$ denotes the Shannon entropy. Then we have $H(P_{01}) + H(P_{+-}) \geq 1$ as described at Eq. (11.3) in [9], where the entropy is counted in the unit of bits.

Let Γ be the memoryless quantum channel that represents Eve's manipulation and the channel noise between Alice and Bob. Γ is a map between density operators. Define

$$
\begin{aligned}
p_{X-} &= \langle +|\Gamma(|-\rangle\langle -|)|+\rangle,\\
p_{X+} &= \langle -|\Gamma(|+\rangle\langle +|)|-\rangle,\\
q_{X1} &= \langle +|\Gamma(|1\rangle\langle 1|)|+\rangle,\\
q_{X0} &= \langle -|\Gamma(|0\rangle\langle 0|)|-\rangle,\\
p_{Z1} &= \langle 0|\Gamma(|1\rangle\langle 1|)|0\rangle,\\
p_{Z0} &= \langle 1|\Gamma(|0\rangle\langle 0|)|1\rangle,\\
q_{Z-} &= \langle 0|\Gamma(|-\rangle\langle -|)|0\rangle,\\
q_{Z+} &= \langle 1|\Gamma(|+\rangle\langle +|)|1\rangle.
\end{aligned}
$$

Observe that $q_X = (q_{X0} + q_{X1})/2$ and $q_Z = (q_{Z+} + q_{Z-})/2$, where q_X and q_Z are as defined in Eqs. (1) and (2).

Define $p_X = (p_{X+} + p_{X-})/2$ and $p_Z = (p_{Z0} + p_{Z1})/2$. Observe that p_Z (resp. p_X) is the error rate of the matched measurement in the BB84 protocol when transmitting basis is $\{|0\rangle, |1\rangle\}$ (resp. $\{|+\rangle, |-\rangle\}$). The lower bound on key rate of the plain one-way postprocessing described in [12] is given by $1 - h(p_X) - h(p_Z)$ [4].

From the entropic uncertainty principle reviewed at the beginning of this section, we have

$$h(p_{X+}) + h(q_{Z+}) \geq 1, \tag{6}$$

$$h(p_{X-}) + h(q_{Z-}) \geq 1, \tag{7}$$

$$h(p_{Z0}) + h(q_{X0}) \geq 1, \tag{8}$$

$$h(p_{Z1}) + h(q_{X1}) \geq 1. \tag{9}$$

By the concavity of the entropy function

$$h(p_X) = h\left(\frac{p_{X+} + p_{X-}}{2}\right) \geq \frac{h(p_{X+}) + h(p_{X-})}{2}, \tag{10}$$

$$h(q_Z) = h\left(\frac{q_{Z+} + q_{Z-}}{2}\right) \geq \frac{h(q_{Z+}) + h(q_{Z-})}{2}, \quad (11)$$

$$h(p_Z) = h\left(\frac{p_{Z0} + p_{Z1}}{2}\right) \geq \frac{h(p_{Z0}) + h(p_{Z1})}{2}, \quad (12)$$

$$h(q_X) = h\left(\frac{q_{X0} + q_{X1}}{2}\right) \geq \frac{h(q_{X0}) + h(q_{X1})}{2}. \quad (13)$$

Applying Eqs. (10) and (11) to the sum of Eqs. (6) and (7) divided by two, we obtain

$$h(p_X) + h(q_Z) \geq 1. \quad (14)$$

From Eqs. (8, 9, 12, 13) in a similar manner we obtain

$$h(p_Z) + h(q_X) \geq 1. \quad (15)$$

Equations (14) and (15) imply

$$[1 - h(p_X) - h(p_Z)] + [1 - h(q_X) - h(q_Z)] \leq 0. \quad (16)$$

The first term in Eq. (16) is the lower bound on key rate of the matched measurement in the BB84 protocol, while the second term is that of the mismatched measurement. Equation (16) means that both lower bounds on key rates cannot be simultaneously positive.

5. Concluding Remarks

We proposed a variant of the BB84 protocol that extracts secret key from measurement outcomes with which measuring bases are different from transmitting bases, obtained a lower bound on the key rate which has a similar form to that of the standard BB84 protocol, and verified its unconditional security. After that, we showed that the lower bounds on the key rates available from matched and mismatched measurements cannot be simultaneously positive.

Our result generates a number of interesting research questions. Firstly, the well-known upper bound (Table I in [4]) on the key rates of the BB84 protocol [12] is expressed in terms of error rates for matched measurements with which measuring bases are the same as the transmitting bases. If both error rates for the matched bases are 0.5, for example the Hadamard matrix is applied to every qubit, then those upper bounds state that we cannot extract secret key. However, our proposed variant of the BB84 protocol can extract secret key in such case. It is desirable to have an upper bound on the amount of available secret key taking into account mismatched measurement in the BB84 protocol.

Secondly, we could not disprove the possibility that we can extract secret key from both matched and mismatched measurements by more sophisticated postprocessing of the BB84 protocol such as Refs. [4], [7], [11], [15]. It is desirable to prove or disprove such possibility.

Thirdly, in the standard BB84 protocol, it is generally believed that we can postprocess bits transmitted by $\{|0\rangle, |1\rangle\}$ basis and $\{|+\rangle, |-\rangle\}$ basis separately without decreasing the key rate. The proposed variant of the BB84 protocol separately postprocess bits obtained by matched measurements and mismatched ones, because the matched measurement outcomes are processed with the standard BB84 protocol separately. It is not clear whether or not such separate processing of matched and mismatched measurement outcomes decreases the total amount of secret key. We leave these questions as future research agenda. Note added in proof: The second problem was recently solved in [16].

Acknowledgment

This research was partly supported by the Japan Society for the Promotion of Science under Grants-in-Aid No. 18760266 and No. 00197137.

References

[1] C.H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. IEEE Intl. Conf. on Computers, Systems, and Signal Processing, pp.175–179, 1984.

[2] A.R. Calderbank and P.W. Shor, "Good quantum error-correcting codes exist," Phys. Rev. A, vol.54, no.2, pp.1098–1105, Aug. 1996.

[3] I. Csizár, "Linear codes for sources and source networks: Error exponents, universal coding," IEEE Trans. Inf. Theory, vol.28, no.4, pp.585–592, July 1982.

[4] D. Gottesman and H.K. Lo, "Proof of security of quantum key distribution with two-way classical communications," IEEE Trans. Inf. Theory, vol.49, no.2, pp.457–475, Feb. 2003.

[5] M. Hamada, "Reliability of Calderbank-Shor-Steane codes and security of quantum key distribution," J. Phys. A, Math. Gen., vol.37, no.34, pp.8303–8328, Aug. 2004.

[6] M. Koashi, "Unconditional security of quantum key distribution and the uncertainty principle," J. Physics: Conference Series, vol.36, pp.98–102, 2006.

[7] X. Ma, C.H.F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.K. Lo, "Decoy-state quantum key distribution with two-way classical postprocessing," Phys. Rev. A, vol.74, no.3, 032330, Sept. 2006.

[8] H. Maassen and J.B.M. Uffink, "Generalized entropic uncertainty relations," Phys. Rev. Lett., vol.60, no.2, pp.1103–1106, March 1988.

[9] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, UK, 2000.

[10] M. Pawlowski, "How not to discard half of the cases in QKD," arXiv:0708.0933, Aug. 2007.

[11] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," Phys. Rev. A, vol.72, no.1, 012332, July 2005.

[12] P.W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett., vol.85, no.2, pp.441–444, July 2000.

[13] A.M. Steane, "Multiple particle interference and quantum error correction," Proc. Roy. Soc. London Ser. A, vol.452, no.1954, pp.2551–2577, Nov. 1996.

[14] S. Watanabe, R. Matsumoto, and T. Uyematsu, "Noise tolerance of the BB84 protocol with random privacy amplification," International Journal on Quantum Information, vol.4, no.6, pp.935–946, Dec. 2006.

[15] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, "Key rate of quantum key distribution with hashed two-way classical communication," Phys. Rev. A, vol.76, no.3, 032312, Sept. 2007.

[16] S. Watanabe, R. Matsumoto, and T. Uyematsu, "Tomography increases key rates of guantum-key-distribution protocols," to be published in Phys. Rev. A, arXiv: 0802.2419.