Narrow basis angle doubles secret key in the BB84 protocol

2010 J. Phys. A: Math. Theor. 43 145302

(http://iopscience.iop.org/1751-8121/43/14/145302)

IOP Publishing — Journal of Physics A: Mathematical and Theoretical

J. Phys. A: Math. Theor. **43** (2010) 145302 (6pp) doi:10.1088/1751-8113/43/14/145302

Narrow basis angle doubles secret key in the BB84 protocol

Ryutaroh Matsumoto[1] **and Shun Watanabe**[2]

[1] Department of Communications and Integrated Systems, Tokyo Institute of Technology,
Tokyo 152-8550, Japan
[2] Department of Information Science and Intelligent Systems, Tokushima University,
Tokushima 770-8506, Japan

E-mail: ryutaroh@rmatsumoto.org and shun-wata@is.tokushima-u.ac.jp

Received 29 May 2009
Published 16 March 2010
Online at stacks.iop.org/JPhysA/43/145302

Abstract

We consider a modified version of the BB84 quantum key distribution protocol in which the angle between two different bases is less than $\pi/4$. We show that the channel parameter estimate becomes the same as the original protocol with sufficiently transmitted qubits. On the other hand, the statistical correlation between bits transmitted in one basis and those received in the other basis becomes stronger as the angle between two bases becomes narrower. If the angle is very small, the statistical correlation between bits transmitted in one basis and those received in the other basis is as strong as those received in the same basis as the transmitting basis, which means that the modified protocol can generate almost twice as long secret key as in the original protocol, provided that Alice and Bob choose two different bases with almost the same probability. We also point out that the reverse reconciliation often gives a different amount of secret key to the direct reconciliation over Pauli channels with our modified protocol.

PACS number: 03.67.Dd

1. Introduction

The Bennett–Brassard 1984 protocol (BB84 protocol) [2] is one of the most known protocols for quantum key distribution (QKD). In this protocol, the sender, Alice, sends qubits in one of four quantum states, represented by the 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 them 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 belongs. Bob discards the measurement outcomes whose bases do not contain the transmitted states. We call such a measurement the *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 [15]. In this standard protocol, we have $|+\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$ and $|-\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle$ with $\theta = \pi/4$. In this paper we shall call θ the angle between the two bases.

As far as the authors know, there is no literature that shows the merit of using smaller values of θ in the BB84 protocol, while Tamaki *et al* [16] quantitatively demonstrated the merit of adjusting the angle between two different quantum states in the Bennett 1992 (B92) protocol [1]. A possible reason for the absence of the consideration of a narrower angle $\theta < \pi/4$ is that the narrower angle makes it difficult to obtain a meaningful lower bound on the amount of secret key by the conventional channel parameter estimation as described in section 2.2. This difficulty leads us to use the accurate channel parameter estimation method [17] for the BB84 protocol with narrower angle. We shall show that over any quantum channel between Alice and Bob, including Pauli channels, we can obtain almost the same amount of secret key from mismatched measurement outcomes when the angle between two bases is sufficiently narrow, while obtaining asymptotically the same amount of key per transmitted qubit from matched measurement outcomes, by using the accurate estimation method. We note that we have already considered obtaining secret key from mismatched measurement outcomes in [11]. However [11] was not so useful because we cannot obtain secret key if the channel is a Pauli one.

On the other hand, the amount of secret key is the same in the direct and reverse reconciliations in the standard BB84 protocol over Pauli channels [15], even if we use the accurate channel parameter estimation [17]. In contrast to this, we also point out that the reverse reconciliation [4, 12] often gives different amount of secret key to the direct reconciliation over Pauli channels with our modified protocol.

This paper is organized as follows. Section 2 presents a modified version of the BB84 protocol, its security and its performance analysis. Section 3 gives concluding remarks.

2. Protocol

2.1. *Outline of the protocol*

In this section, we shall show a variant of the BB84 protocol that tries to extract secret key from mismatched measurement outcomes. Section 2.1 describes an outline of the protocol, section 2.2 derives the amount of secret key, and section 2.3 considers the reverse reconciliation. We define the matrices X and Z representing the bit error and the phase error, respectively, as

$$\begin{aligned} X|0\rangle &= |1\rangle, & X|1\rangle &= |0\rangle, \\ Z|+\rangle &= |-\rangle, & Z|-\rangle &= |+\rangle, \end{aligned}$$

and $Y = \mathrm{i}XZ$. We also fix $0 < \theta \leqslant \pi/4$ and define

$$\begin{aligned} |+_\theta\rangle &= \cos\theta|0\rangle + \sin\theta|1\rangle, \\ |-_\theta\rangle &= -\sin\theta|0\rangle + \cos\theta|1\rangle. \end{aligned}$$

(1) Alice makes a random qubit sequence according to the i.i.d. uniform distribution on $\{|0\rangle, |1\rangle, |+_\theta\rangle, |-_\theta\rangle\}$ and sends it to Bob.

(2) Bob chooses the $\{|0\rangle, |1\rangle\}$ basis or the $\{|+_\theta\rangle, |-_\theta\rangle\}$ basis uniformly randomly for each received qubit and measures it by the chosen basis.

(3) Alice publicly announces which basis $\{|0\rangle, |1\rangle\}$ or $\{|+_\theta\rangle, |-_\theta\rangle\}$ each transmitted qubit belongs to. Bob also publicly announces which basis was used for measurement of each qubit.

(4) Suppose that there are $2n$ qubits transmitted in the $\{|0\rangle, |1\rangle\}$ basis and measured with the $\{|+_\theta\rangle, |-_\theta\rangle\}$ basis by Bob. Index those qubits by $1, \ldots, 2n$. Define the bit $x_i = 0$ if Alice's ith qubit was $|0\rangle$, and $x_i = 1$ otherwise. Define the bit $y_i = 0$ if Bob's measurement outcome for ith qubit was $|+_\theta\rangle$, and $y_i = 1$ otherwise.

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

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

(7) For each combination of the transmission and the reception bases, Alice and Bob publicly announce the half of transmitted qubits and measurement outcomes. They conduct the channel parameter estimation described in section 2.2. We also define

$$q_1 = \frac{|\{i \in S \mid x_i \neq y_i\}|}{|S|}, \qquad q_2 = \frac{|\{i \in S' \mid a_i \neq b_i\}|}{|S'|},$$

where S and S' are the set of indices that are announced for the channel parameter estimation.

(8) Alice and Bob decide[3] 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_1. Let H_1 be a parity check matrix for C_1, $\vec{x}$ be Alice's remaining (not announced) bits among x_i's, and $\vec{y}$ be Bob's remaining bits among y_i's.

(9) Alice publicly announces the syndrome $H_1\vec{x}$.

(10) Bob computes the error vector $\vec{e}$ such that $H_1\vec{e} = H_1\vec{y} - H_1\vec{x}$ by the decoding algorithm for C_1. With a high probability $\vec{y} - \vec{e} = \vec{x}$.

(11) Alice chooses a subspace $C_2 \subset C_1$ with $\dim C_2 = n(1 - S(X|E) + \epsilon)$ uniformly and randomly, where $\epsilon > 0$ and $S(X|E)$ denotes the conditional von Neumann entropy of Alice's bit x_i given the quantum state of the environment E as defined in [13, 14], which can be regarded as Eve's ambiguity on Alice's bit x_i. After that she publicly announces her choice of C_2. The final shared secret key is the coset $\vec{x} + C_2$.

Provided that $\epsilon > 0$, the privacy amplification theorem with quantum eavesdropper's memory [13, 14] guarantees that the final key $\vec{x} + C_2$ becomes secure in the sense of [13, 14] as $n \to \infty$, which roughly means that the final key and the quantum state of the environment becomes statistically independent and that the final key has an almost uniform distribution on the set C_1/C_2. We shall consider the amount of secret key obtained by the above protocol in section 2.2.

2.2. *Amount of secret key*

We shall use the accurate channel parameter estimation [17], which gives asymptotically more secret key than the conventional estimation. This procedure is as follows. We do not make any assumption on the quantum channel between Alice and Bob, so the channel is specified by 12 real parameters. For 16 pairs $(|u\rangle, |v\rangle) \in \{|0\rangle, |1\rangle, |+_\theta\rangle, |-_\theta\rangle\}^2$, we record the 16 relative frequencies of the events in which $|u\rangle$ is transmitted and $|v\rangle$ is observed as the measurement outcome, which enable us to estimate 6 out of 12 channel parameters. After estimating the

[3] One can also use the Slepian–Wolf code used in [17].

part of parameters, we use the minimum of $S(X|E)$ over all the possible quantum channel, that is, we use the worst case estimate of $S(X|E)$ of quantum channels giving the 16 recorded relative frequencies, as done in the conventional estimation [7, 13, 14]. The set of estimable parameters with $0 < \theta < \pi/4$ is the same as $\theta = \pi/4$. The reason is as follows. Since the linear space spanned by $\{|0\rangle\langle 0|, |1\rangle\langle 1|, |+_\theta\rangle\langle +_\theta|, |-_\theta\rangle\langle -_\theta|\}$ is the same for all $0 < \theta \leqslant \pi/4$ and the expectation of the relative frequency of sending $|u\rangle$ and observing $|v\rangle$ is proportional to $\mathrm{Tr}[\Lambda(|u\rangle\langle u|)|v\rangle\langle v|]$ for any quantum channel Λ, there always exists a one-to-one linear relation that translates the set of 16 relative frequencies with $\theta < \pi/4$ to that with $\theta = \pi/4$. Therefore, the estimate of the worst case $S(X|E)$ does not depend on the value of θ. This means that the amount of secret key from matched measurement outcomes remains asymptotically the same even if we use θ narrower than $\pi/4$.

We cannot use a straightforward generalization of the conventional channel parameter estimation, that is to record two relative frequencies of event (a) in which $|0\rangle$ is sent and $|1\rangle$ is observed or $|1\rangle$ is sent and $|0\rangle$ is observed, and event (b) in which $|+_\theta\rangle$ is sent and $|-_\theta\rangle$ is observed or $|-_\theta\rangle$ is sent and $|+_\theta\rangle$ is observed. The reason of unavailability of the conventional channel parameter estimation is as follows. We cannot estimate the parameters of the Pauli channel that is obtained as the partial twirling [3][4] of the actual quantum channel because the relative frequency of event (b) also depends[5] on the non-diagonal elements in the Choi matrix [6] of the actual quantum channel with respect to the Bell basis as well as the diagonal elements unless $\theta = \pi/4$, and the four diagonal elements in the Choi matrix specify the Pauli channel obtained by the partial twirling. Since the standard technique is to bound the required dimension of C_2 in step 11 over the actual channel from above by the required $\dim C_2$ over its partially twirled channel, the inability to estimate the partially twirled channel prevents us from obtaining a useful upper bound on $\dim C_2$ of the actual channel. Thus, it is difficult to ensure that the worst case estimate of $\dim C_2$ is independent of θ by the above generalization of the conventional channel parameter estimation, and we have to use 16 relative frequencies to bound $\dim C_2$ from above.

The amount of secret key is [13, 14]

$$S(X|E) - h(q_1)$$

from single bit x_i not announced for the channel parameter estimation, while this amount is

$$S(X|E) - h(q_2) \tag{1}$$

from a_i, where $h(\,)$ denotes the binary entropy function. Since $q_1 \to q_2$ as $\theta \to 0$ and $h(\,)$ is a continuous function, we conclude that we can obtain almost the same amount of secret key from x_i as a_i.

2.3. *Reverse reconciliation*

The reverse reconciliation [4, 12] is the method of reconciliation in which Bob publicly announces the syndrome $H_1\vec{y}$ in step 9 instead of Alice, Alice computes $\vec{y}$ in step 10 instead of Bob, and the final key is generated from $\vec{y}$. The standard way of reconciliation [15] is called the direct reconciliation. In order to give a simpler exposition of the main contribution, we have restricted ourselves to the direct reconciliation up to this point. In this subsection we shall consider the reverse reconciliation and point out that the amount of secret key is often different in the reverse reconciliation to the direct one over a Pauli channel.

We can also use the same parity check matrix H_1 in step 8 since $\vec{x}$ can be regarded as the output of the binary symmetric channel with crossover probability q_1 with input $\vec{y}$. We

[4] See also equation (12) of [8], in which the partial twirling is called the discrete twirling.

[5] The relative frequency of event (a) is independent of the non-diagonal elements in the Choi matrix.

have to change $\dim C_2$ in step 11 to $\dim C_2 = n(1 - S(Y|E) + \epsilon)$, where $S(Y|E)$ denotes the conditional von Neumann entropy of Bob's bit y_i given the quantum state of the environment E. We have to compute the minimum value of $S(Y|E)$ over quantum channels that give the recorded relative frequencies.

Hereafter we assume that the channel between Alice and Bob is a Pauli channel that sends a qubit density matrix ρ to

$$\Gamma(\rho) = (1 - r_X - r_Y - r_Z)\rho + r_X X\rho X + r_Y Y\rho Y + r_Z Z\rho Z,$$

instead of a general qubit channel that is not necessarily a Pauli one. We define

$$p_X = r_X + r_Y, \qquad p_Z = r_Z + r_Y.$$

It is well known that the worst case $S(X|E)$ is $1 - h(p_Z)$ [7, 13, 14].

In the evaluation of the worst case $S(Y|E)$, Bob's bit Y can be regarded as the measurement outcome in the $\{|0\rangle, |1\rangle\}$ basis on the output of the unitary channel rotating $|+_\theta\rangle$ to $|0\rangle$ and $|-_\theta\rangle$ to $|1\rangle$, connected to the actual channel. The Pauli channel followed by a rotation is a unital channel, which outputs the completely mixed state if the input is completely mixed. This observation enables us to apply the formula for the worst case $S(Y|E)$ over unital channels given in proposition 2 and remark 6 of [17], which gives

$$S(Y|E) = 1 - h(p_X) - h(p_Z) + h\left(\frac{1 + \sqrt{(1-2p_X)^2\cos^2 2\theta + (1-2p_Z)^2\sin^2 2\theta}}{2}\right).$$

We can see that $S(Y|E) \to 1 - h(p_Z)$ as $\theta \to 0$ and $S(Y|E) \to 1 - h(p_X)$ as $\theta \to \pi/4$, which confirms our intuition. Observe also that generally $S(X|E) \neq S(Y|E)$ when $p_X \neq p_Z$.

By using a similar idea, we can obtain Eve's ambiguity on Alice's bit α_i that is transmitted in the $\{|+_\theta\rangle, |-_\theta\rangle\}$ basis. By the continuity of the von Neumann entropy, we can also see that the amount of secret key from α_i converges to equation (1) obtained from a_i as $n \to \infty$ and $\theta \to 0$. Therefore, the conclusion in section 2.2 also holds for qubits transmitted by the $\{|+_\theta\rangle, |-_\theta\rangle\}$ basis.

3. Concluding remarks

We have shown that from mismatched measurement outcomes we can obtain as much secret key per transmitted qubit as matched measurement outcomes over any channels if we make the angle between two bases sufficiently narrow. The same conclusion holds for the six-state protocol [5] and the variants of the standard BB84 protocols with the noisy preprocessing [13, 14], and the advantage distillation [7, 18]. We have also pointed out that the reverse reconciliation often gives different amount of secret key to the direct reconciliation over Pauli channels with our modified protocol, which is in contrast to the standard BB84 protocol [15], and that there is difficulty to use the conventional channel parameter estimation if the angle between two bases is narrower than $\pi/4$.

The advantage of the proposed protocol is that we can obtain $1 - h(p_X) - h(p_Z)$ bits of secret key per single qubit that is not used for channel parameter estimation. The same advantage is also realized when we decrease the ratio of the number of transmitted qubits in the $\{|+\rangle, |-\rangle\}$ basis to that in the $\{|0\rangle, |1\rangle\}$ basis [9, 10]. Although the proposed method, the method in [9, 10], and their combination have exactly the same performance in the asymptotic limit of infinitely many qubits, they may have different performances in the finite number of qubits. The identification of the best method among these three methods in the finite setting is a future research agenda. This identification might be analytically difficult as stated in the introduction of [9].

References

[1] Bennett C H 1992 Quantum cryptography using any two nonorthogonal states *Phys. Rev. Lett.* **68** 3121–4

[2] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing* pp 175–9

[3] Bennett C H, Di Vincenzo D P, Smolin J A and Wootters W K 1996 Mixed-state entanglement and quantum error correction *Phys. Rev.* A **54** 3824–51 (arXiv:quant-ph/9604024)

[4] Boileau J-C, Batuwantudawe J and Laflamme R 2005 Higher-security thresholds for quantum key distribution by improved analysis of dark counts *Phys. Rev.* A **72** 032321 (arXiv:quant-ph/0502140)

[5] Bruß D 1998 Optimal eavesdropping in quantum cryptography with six states *Phys. Rev. Lett.* **81** 3018–21 (arXiv:quant-ph/9805019)

[6] Choi M-D 1975 Completely positive linear maps on complex matrices *Linear Algebra and Appl.* **10** 285–90

[7] Gottesman D and Lo H-K 2003 Proof of security of quantum key distribution with two-way classical communications *IEEE Trans. Inf. Theory* **49** 457–75 (arXiv:quant-ph/0105121)

[8] Hamada M 2003 Notes on the fidelity of symplectic quantum error-correcting codes *Int. J. Quantum Inf.* **1** 443–63 (arXiv:quant-ph/0311003)

[9] Hayashi M 2009 Optimal ratio between phase basis and bit basis in quantum key distributions *Phys. Rev.* A **79** 020303 (arXiv:0805.3190)

[10] Lo H-K, Chau H F and Ardehali M 2004 Efficient quantum key distribution scheme and a proof of its unconditional security *J. Cryptol.* **18** 133–65 (arXiv:quant-ph/0011056)

[11] Matsumoto R and Watanabe S 2008 Key rate available from mismatched measurements in the BB84 protocol and the uncertainty principle *IEICE Trans. Fundam.* **E91-A** 2870–3 (arXiv:0711.1731)

[12] Maurer U 1993 Secret key agreement by public discussion from common information *IEEE Trans. Inf. Theory* **39** 733–42

[13] Renner R 2008 Security of quantum key distribution *Int. J. Quantum Inf.* **6** 1–127 (originally published as *PhD Thesis*, ETH Zürich, Switzerland, 2005) (arXiv:quant-ph/0512258)

[14] Renner R, Gisin N and Kraus B 2005 Information-theoretic security proof for quantum-key-distribution protocols *Phys. Rev.* A **72** 012332 (arXiv:quant-ph/0502064)

[15] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol *Phys. Rev. Lett.* **85** 441–4 (arXiv:quant-ph/0003004)

[16] Tamaki K, Koashi M and Imoto N 2003 Unconditionally secure key distribution based on two nonorthogonal states *Phys. Rev. Lett.* **90** 167904 (arXiv:quant-ph/0212162)

[17] Watanabe S, Matsumoto R and Uyematsu T 2008 Tomography increases key rates of quantum-key-distribution protocols *Phys. Rev.* A **78** 042316 (arXiv:0802.2419)

[18] Watanabe S, Matsumoto R, Uyematsu T and Kawano Y 2007 Key rate of quantum key distribution with hashed two-way classical communication *Phys. Rev.* A **76** 032312 (arXiv:0705.2904)