Multiparty quantum-key-distribution protocol without use of entanglement

Ryutaroh Matsumoto[*]

Department of Communications and Integrated Systems, Tokyo Institute of Technology, Tokyo 152-8550, Japan

(Received 7 August 2007; published 20 December 2007)

We propose a quantum-key-distribution protocol that enables three parties to agree at once on a shared common random bit string in the presence of an eavesdropper without use of entanglement. We prove its unconditional security and analyze the key rate.

DOI: 10.1103/PhysRevA.76.062316 PACS number(s): 03.67.Dd, 03.67.Pp

I. INTRODUCTION

When a sender, Alice, wants to send a confidential message to single receiver, Bob, over a public communication channel in an unconditionally secure way, they must share a secret common random bit string, which is usually called a secret key. Such a secret key can be shared by a quantum-key-distribution (QKD) protocol, such as the Bennett-Brassard 1984 (BB84) protocol [1,2] even when there is an eavesdropper, Eve, with unlimited computational power.

When Alice sends a confidential message by broadcast to two receivers, Bob and Charlie, these three parties must share a common secret key. We propose a protocol enabling them to share such a secret key under the assumption that there are point-to-point quantum channels from Alice to Bob and Charlie whose message can be eavesdropped and modified by Eve and three point-to-point classical channels among Alice, Bob, and Charlie whose message can be eavesdropped but cannot be modified by Eve. Eve is assumed to do whatever manipulation on quantum systems transmitted over the quantum channels allowed by the quantum mechanics. This assumption is the same as Ref. [3] and is a multiparty generalization of that in Ref. [2]. This problem is called the multiparty key distribution or conference key agreement. Under this assumption we prove the unconditional security and give a lower bound on the key rate.

As a prior relevant research, it was pointed out in Ref. [4] that Alice can secretly send a key after two different secret keys are shared between Alice and Bob and between Alice and Charlie by a conventional two-party QKD protocol such as Ref. [1]. The difference of our proposed protocol to Ref. [4] is that our protocol allows three parties to share a secret key at once.

As another prior relevant research, Chen and Lo [3] proposed a protocol for the same goal as our proposed protocol. In their protocol, Alice must prepare the Bell state while in our protocol she does not need an entangled quantum state, which makes our protocol easier to implement with current technology than theirs [3]. Our protocol is the first multiparty QKD protocol that does not use entangled state. It is also worth noting that the security proof for our protocol does not use multipartite entanglement distillation [5], while Chen and Lo [3] use it.

This paper is organized as follows: Section II presents the proposed protocol. Section III shows an unconditional security proof and a lower bound on its key rate. Section IV gives concluding remarks.

II. PROTOCOL

In this section we describe our proposed protocol. Let $|0\rangle$, $|1\rangle$ be an orthonormal basis for the qubit state space, and $|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$, $|-\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$. We also 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. Alice also sends the same qubit sequence to Charlie.

(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) Charlie does the same thing as step (2).

(4) Alice publicly announces which basis $\{|0\rangle,|1\rangle\}$ or $\{|+\rangle,|-\rangle\}$ each transmitted qubit belongs to. Bob and Charlie also publicly announce which bases were used for measurement of each qubit. In the following steps they will only consider qubits with which transmission basis and measuring bases coincide among all of them.

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

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

For the simplicity of the presentation, we shall describe the procedure extracting the secret key from a_i, b_i, and c_i.

[*] ryutaroh@rmatsumoto.org; URL: http://www.rmatsumoto.org/research.html

(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, Bob, and Charlie publicly announce a_i, b_i, and c_i for $i \in S$ and compute the error rate

$$q_1 = \max\left\{ \frac{|\{ i \in S | a_i \neq b_i\}|}{|S|}, \frac{|\{ i \in S | a_i \neq c_i\}|}{|S|} \right\}.$$

(8) 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, Bob, and Charlie publicly announce α_i, β_i, and γ_i for $i \in S'$ and compute the error rate

$$q_2 = \frac{|\{ i \in S' | \alpha_i = \gamma_i \neq \beta_i \text{ or } \alpha_i = \beta_i \neq \gamma_i\}|}{|S'|}. \tag{1}$$

Observe the difference between the definitions for q_1 and q_2.

(9) Alice, Bob, and Charlie decide a linear code C_1 of length n such that its decoding error probability is sufficiently small over all of the binary symmetric channel whose crossover probability is close to q_1. Let H_1 be a parity check matrix for C_1, $\vec{a}$ be Alice's remaining (not announced) bits among a_i's, $\vec{b}$ be Bob's remaining bits among b_i's, and $\vec{c}$ be Charlie's remaining bits among c_i's.

(10) Alice publicly announces the syndrome $H_1\vec{a}$.

(11) Bob computes 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) Charlie computes the error vector $\vec{f}'$ such that $H_1\vec{f}' = H_1\vec{c} - H_1\vec{a}$ by the decoding algorithm for C_1. With high probability $\vec{c} - \vec{f}' = \vec{a}$.

(13) Alice chooses a subspace $C_2 \subset C_1$ with $\dim C_2 = nh(q_2)$ 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 $\vec{a} + C_2$.

III. SECURITY PROOF AND A LOWER BOUND ON THE KEY RATE

We shall show the unconditional security of our proposed protocol by directly relating it to the quantum error correction by the quantum CSS (Calderbank-Shor-Steane) codes [6,7]. To make this paper self-contained, we shall briefly review the CSS code.

A. 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

$$|\vec{v}\rangle = |v_1\rangle \otimes |v_2\rangle \otimes \cdots \otimes |v_n\rangle.$$

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 parametrized CSS codes introduced in Ref. [2]. The parametrized CSS code for $\vec{x}, \vec{z} \in \mathbf{F}_2^n$ is defined as the linear space spanned by

$$\frac{1}{\sqrt{|C_2|}} \sum_{\vec{w} \in C_2} (-1)^{(\vec{z},\vec{w})} |\vec{x} + \vec{v} + \vec{w}\rangle,$$

for all $\vec{v} \in C_1$, where $(\cdots,\cdots)$ denotes the inner product.

For a linear code C of length n, define the linear code CC of length $2n$ and dimension $\dim C$ by

$$\{\vec{c}\vec{c} | \vec{c} \in C\},$$

where $\vec{c}\vec{c}$ is the concatenated vector of length $2n$. In the security proof of our protocol, we must consider the CSS code defined by the pair of linear codes $C_1C_1 \supset C_2C_2$, whose orthonormal basis is given by

$$\frac{1}{\sqrt{|C_2|}} \sum_{\vec{w} \in C_2} |\vec{v} + \vec{w}\rangle |\vec{v} + \vec{w}\rangle.$$

For vectors $\vec{x}$ and $\vec{z} \in \mathbf{F}_2^n$ of length n, we define the parametrized CSS code as the complex linear space spanned by

$$\frac{1}{\sqrt{|C_2|}} \sum_{\vec{w} \in C_2} (-1)^{(\vec{z},\vec{w})} |\vec{x} + \vec{v} + \vec{w}\rangle |\vec{x} + \vec{v} + \vec{w}\rangle, \tag{2}$$

for $\vec{v} \in C_1$. Using the parametrized CSS code defined in Eq. (2), we shall show a security proof of our protocol.

B. Security proof and analysis of the key rate

We shall first show that our protocol is equivalent to sending a parametrized CSS codeword with the parameters $\vec{x}$ and $\vec{z}$ randomly chosen. If we fix $\vec{v}$ and $\vec{x}$ and choose $\vec{z}$ uniformly randomly in Eq. (2), then the resulting density operator is

$$\begin{aligned} &\frac{1}{2^n|C_2|} \sum_{\vec{z} \in \mathbf{F}_2^n} \left(\sum_{\vec{w}_1 \in C_2} (-1)^{(\vec{z},\vec{w}_1)} |\vec{x} + \vec{v} + \vec{w}_1\rangle |\vec{x} + \vec{v} + \vec{w}_1\rangle \right) \\ &\quad \times \left(\sum_{\vec{w}_2 \in C_2} (-1)^{(\vec{z},\vec{w}_2)} \langle \vec{x} + \vec{v} + \vec{w}_2| \langle \vec{x} + \vec{v} + \vec{w}_2| \right) \\ &= \frac{1}{|C_2|} \sum_{\vec{w} \in C_2} |\vec{x} + \vec{v} + \vec{w}\rangle |\vec{x} + \vec{v} + \vec{w}\rangle \langle \vec{x} + \vec{v} + \vec{w}| \langle \vec{x} + \vec{v} + \vec{w}|, \end{aligned} \tag{3}$$

by the exact same argument as Ref. [2].

Denote the right-hand side of Eq. (3) by $\rho(\vec{x},\vec{v})$. By a straightforward computation we can see

$$\frac{1}{4^n} \sum_{\vec{x} \in \mathbf{F}_2^n} \sum_{\vec{v} \in \mathbf{F}_2^n} \rho(\vec{x},\vec{v}) = \frac{1}{2^n} \sum_{\vec{a} \in \mathbf{F}_2^n} |\vec{a}\vec{a}\rangle\langle\vec{a}\vec{a}|. \tag{4}$$

The right-hand side of Eq. (4) means sending $|00\rangle$ or $|11\rangle$ n times with equal probability, which is exactly what Alice is doing in our protocol. Announcing the syndrome $H_1\vec{a}$ in step (10) is equivalent to announcing which $\vec{x}$ is chosen.

We shall consider the decoding of the imaginary transmission of CSS code words. A good review of decoding of CSS codes is provided in Ref. [2]. We regard Bob and Charlie as a single receiver. The bit error correction is actually performed in our protocol, therefore we must ensure that it can be separately executed by Bob and Charlie. On the other hand, the phase error correction is not actually performed, so it does not need to be separately executable.

Observe that the bit error correction for the leftmost n qubits in the CSS code defined in Eq. (2) can be done separately from the rightmost n qubits in Eq. (2), which means that Bob and Charlie can correct their bit flip errors with their local operations and that they do not need their cooperation for bit error correction.

We shall consider the phase error correction. Let Z_i be the phase error that occurred at ith qubit in Eq. (2). We can see that Z_i and Z_{n+i} have the same effect on the quantum codeword in Eq. (2), and that $Z_i \otimes Z_{n+i}$ does not change the quantum codeword in Eq. (2).

Let

$$H_2 = \begin{pmatrix} \vec{h}_1 \\ \vdots \\ \vec{h}_{n-\dim C_2} \end{pmatrix}$$

be a parity check matrix for $C_2^{\perp}$, then

$$H_2' = \begin{pmatrix} \vec{h}_1\vec{h}_1 \\ \vdots \\ \vec{h}_{n-\dim C_2}\vec{h}_{n-\dim C_2} \end{pmatrix}$$

is a parity check matrix for $(C_2C_2)^{\perp}$.

Suppose that a phase error

$$Z^{z_1} \otimes \cdots \otimes Z^{z_{2n}} \tag{5}$$

occurred with the quantum state (2), where $z_i \in \mathbf{F}_2$ for $i = 1, \ldots, 2n$. Let $\vec{e} = (z_1, \ldots, z_{2n}) \in \mathbf{F}_2^{2n}$. From the measurement outcomes in the phase error correction process, we can know

$$(\vec{h}_i\vec{h}_i, \vec{e}) \tag{6}$$

for $i = 1, \ldots, n - \dim C_2$. Observe that the error (5) and

$$Z^{z_1'} \otimes \cdots \otimes Z^{z_{2n}'}$$

has the same effect on the state (2) if $z_i + z_{n+i} = z_i' + z_{n+i}'$ for all i, where the addition is considered in $\mathbf{F}_2$. Thus, in order to correct phase errors, we must find the binary vector

$$\vec{e}' = (e_1 + e_{n+i}, \ldots, e_n + e_{2n}) \tag{7}$$

from the data given in Eq. (6). Also observe that

$$(\vec{h}_i\vec{h}_i, \vec{e}) = (\vec{h}_i, \vec{e}').$$

Finding $\vec{e}'$ from $(\vec{h}_i, \vec{e}')$ is exactly the ordinary decoding process for the classical linear code $C_2^{\perp}$. Also observe that the probability of $e_i + e_{n+i} = 1$ is given by q_2 in Eq. (1) in our situation.

It is proved in Ref. [8] that random choice of $[n - h(q_2)]$-dimensional subspace C_2 in C_1 almost always gives the low phase error decoding probability. This fact is also stated without proof in Ref. [2]. If the choice of C_1 is appropriate, then the fidelity of quantum error correction in the imaginary transmission of the CSS codeword (2) is close to 1, which implies that the eavesdropper Eve can obtain little information by the same argument as Ref. [9], which shows the security of the BB84 protocol directly relating it to the quantum error correction without use of entanglement distillation argument.

It was shown in Corollary 2 of Ref. [10] that there exists a linear code C_1 of information rate $1 - h(q_1)$ satisfying the condition in step (9). Therefore, we can extract $1 - h(q_1) - h(q_2)$ bit of secret key from one bit of the raw bits $\vec{a}$.

IV. CONCLUSION AND DISCUSSION

We have proposed a protocol that allows Alice, Bob, and Charlie to share a common secret key at once. This is the first such protocol without use of entangled states. However, the amount of extracted common secret key per single photon transmission is lower than the repeated use of the BB84 protocol and the well-known post-processing described in Ref. [4]. Finding a multiparty QKD protocol with higher efficiency is a future research agenda.

ACKNOWLEDGMENTS

The author would like to thank Shun Watanabe and Tomohiko Uyematsu for helpful discussions. This research was partly supported by the Japan Society for the Promotion of Science under Grants-in-Aid for Young Scientists Grant No. 18760266.

[1] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, 1984, pp. 175–179.

[2] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[3] K. Chen and H.-K. Lo, *Proceedings of the 2005 IEEE International Symposium on Information Theory* (IEEE, Adelaide, Australia, 2005), pp. 1607–1611.

[4] S. K. Singh and R. Srikanth, e-print arXiv:quant-ph/0306118.

[5] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, R4075 (1998).

[6] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).

[7] A. M. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).

[8] S. Watanabe, R. Matsumoto, and T. Uyematsu, Int. J. Quantum Inf. **4**, 935 (2006).

[9] M. Hamada, J. Phys. A **37**, 8303 (2004).

[10] I. Csiszár, IEEE Trans. Inf. Theory **28**, 585 (1982).