Trends in Mathematics
Information Center for Mathematical Sciences
Volume 8, Number 1, June, 2005, Pages 189–195

QUANTUM KEY DISTRIBUTION BASED ON CONFERENCE KEY AGREEMENT

DONG PYO CHI, SORA CHOI, AND SOOJOON LEE

Abstract. Applying multipartite entanglement purification protocol, we present a quantum key distribution protocol between two parties based on conference key agreement (or quantum secret sharing of classical secrets) as a generalization of quantum key distribution between two persons. We analyze the security of the protocol against an external eavesdropper and some dishonest members in two parties.

1. Introduction

Quantum mechanics provides us with new cryptosystems, quantum key distribution (QKD), which makes two parties share secret key strings. In 1984, the first protocol, called BB84, was introduced by Bennett and Brassard [1], and then Ekert presented the protocol using entangled particles in 1991 [7]. Ekert's protocol was modified by Bennett, Brassard, and Mermin and we call the modified protocol EPR protocol [2]. Hillery, Bužek, and Berthiaume provided a protocol for classical secret sharing schemes [8]. Using the secret sharing protocol, the QKD protocol between two parties that consist of several members, was constructed by Choi, Kim and Chi as a generalization of EPR protocol [5]. This protocol exploits n-particle entangled states, and in order to restore secret keys distributed among all members and in order to obtain secret key in each party, the whole members' approval are absolutely necessary.

On the other hand, being unconnected with development of QKD schemes, the analysis of the security has been advanced. In General, it has been spread widely that the security of QKD schemes have been guaranteed from the fundamental laws of quantum mechanics. However, in these years, the unconditional security of the modified BB84 was proved by Mayer [10], and Lo and Chau [11]. This unconditional security means that the protocol is secure for all kinds of attacks allowed by quantum mechanics. Since then, Shor and Preskill [12] gave the succinct and elegant proof of the BB84 scheme, using the Calderbank-Shor-Steane code [6]. Furthermore, in several aspects of QKD schemes, the security has been analyzed

2000 *Mathematics Subject Classification.* Primary 81P68; Secondary 94A05 .

Key words and phrases. Quantum key distribution, conference key agreement, entanglement.

The first author was supported in part by a KIAS Research Project (No. M1-0326-08-0002-03-B51-08-002-12) funded by the Korean Ministry of Science and Technology, the second author by the Korean Ministry of Planning and Budget.

©2005 Information Center for Mathematical Sciences

[13]. As such a flow, in order to present a QKD scheme, its security analysis should be required as an essential part. However, the protocol presented by Choi *et. al* was analyzed only for an intercept/resend strategy.

In this paper, we use the entanglement distillation of two particles state and make n-particle entangled state shared among all members. By means of the process, we construct a modification of the protocol of Choi *et. al*, show the unconditional security against an external eavesdropper, and analyze some dishonest members in two parties.

This paper is organized as follows: In Section 2, we review some properties of several cat states and the entanglement distillation of two particles entangled state. The modified QKD protocol is presented in Section 3. We analyze the security for the protocol in Section 4.

2. Properties of entanglement states

For a positive integer j, we define $\left|\Phi_j^{\pm}\right\rangle$ and $\left|\Psi_j^{\pm}\right\rangle$ by

$$\begin{aligned}\left|\Phi_j^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|0^j\right\rangle \pm \left|1^j\right\rangle\right),\\ \left|\Psi_j^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|0^j\right\rangle \pm \iota\left|1^j\right\rangle\right),\end{aligned} \tag{1}$$

where $|0\rangle$ and $|1\rangle$ are the spin-up and spin-down in the z-direction respectively, and $\iota = \sqrt{-1}$. Then we can readily obtain the following decomposition relations [5]: For positive integers n and m satisfying $n > m$,

$$\begin{aligned}\left|\Phi_n^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|\Phi_m^{+}\right\rangle\left|\Phi_{n-m}^{\pm}\right\rangle + \left|\Phi_m^{-}\right\rangle\left|\Phi_{n-m}^{\mp}\right\rangle\right)\\ &= \frac{1}{\sqrt{2}}\left(\left|\Psi_m^{+}\right\rangle\left|\Psi_{n-m}^{\mp}\right\rangle + \left|\Psi_m^{-}\right\rangle\left|\Psi_{n-m}^{\pm}\right\rangle\right),\\ \left|\Psi_n^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|\Phi_m^{+}\right\rangle\left|\Psi_{n-m}^{\pm}\right\rangle + \left|\Phi_m^{-}\right\rangle\left|\Psi_{n-m}^{\mp}\right\rangle\right)\\ &= \frac{1}{\sqrt{2}}\left(\left|\Psi_m^{+}\right\rangle\left|\Phi_{n-m}^{\pm}\right\rangle + \left|\Psi_m^{-}\right\rangle\left|\Phi_{n-m}^{\mp}\right\rangle\right).\end{aligned} \tag{2}$$

We consider the case that each member of two parties A and B, consisting of m and $n-m$ users respectively, possesses one particle of an n-particle state $|\Phi_n^{\pm}\rangle$, and that each member measures one's own particle in the x- or y-direction. For a party P (with l members), let $\mathcal{N}_P$ be the number (modulo 4) of members of P who measure in the y-direction, $\bar{\mathcal{N}}_P = \lfloor \mathcal{N}_P/2 \rfloor$, and $\mathcal{M}_P$ the sum (modulo 2) of the measurement outcomes of all members in P. It is then straightforward to obtain the following properties from Eq. (2): If $\mathcal{N}_P$ is even, then $\mathcal{M}_P \oplus \bar{\mathcal{N}}_P$ is zero (or one) when they share $\left|\Phi_l^{+}\right\rangle$ (or $\left|\Phi_l^{-}\right\rangle$), where $\oplus$ is the addition modulo 2. If $\mathcal{N}_P$ is odd, then $\mathcal{M}_P \oplus \bar{\mathcal{N}}_P$ is zero (or one) when P has the state $\left|\Psi_l^{+}\right\rangle$ (or $\left|\Psi_l^{-}\right\rangle$). Hence, we get the relations between outcomes of two parties as in the Table 1, respectively. It follows from these relations that the QKD between any kinds of two parties is feasible if they share the multi-particle entangled states such as $|\Phi_n^{+}\rangle$ [5].

		A		B	
	$\mathcal{N}_A \oplus \mathcal{N}_B$	$\mathcal{N}_A$	$\bar{\mathcal{N}}_A \oplus \mathcal{M}_A$	$\mathcal{N}_B$	$\bar{\mathcal{N}}_B \oplus \mathcal{M}_B$
$\lvert\Phi_n^+\rangle$	even	even	0	even	0
			1		1
		odd	0	odd	1
			1		0

TABLE 1. The relations between the measurement outcomes of two parties A and B.

From now we review the entanglement distillation protocol presented by Bennett, Divincenzo, Smolin, and Wootters [4]. General two-particle mixed state M has a property to be turned into the Werner state W_F by irreversible preprocessing operators, called random bilateral rotation [3] or twirl, and the Werner state can be regarded as classical mixture of four Bell states. Utilizing this properties, they presented a couple of methods. Here, we introduce a one-way hashing method to distill m states from n states. This method uses Bilateral XOR operation and several local operation on the corresponding pair, and starts from the assumption that all states have the type of the Werner state. Before the first round, the Bell sequence x_0 is distributed according to a a priori probability distribution P_{x_0}, being a product of n identical independent distribution. In $k+1$ round Alice and Bob obtain $n-k$ impure pairs of unknown Bell states represented by $2(n-k)$ bit string x_k. Alice then chooses $2(n-k)$ bit string s_k and let Bob know it. Alice and Bob take local unitary operations and measure one pair to determine $s_k \cdot x_k$. The unmeasured $n-k-1$ pairs consist of the Bell states represented by $2(n-k)-2$ bit string $x_{k+1} = f_{s_k}(x_k)$. From the repetition of this step, we can share the states to be very close to maximally entangled state.

3. PROTOCOLS

3.1. **Protocol.**

(1) The i-th member in each group transmits a particle of Bell state $\left|\Phi_2^+\right\rangle$ to the $(i+1)$-member. They share sufficiently many states.
(2) They performs entanglement purification protocol to obtain the state $\rho_{i',i+1}$ sufficiently close to Bell state $(1' \equiv 1)$.

For each i they get performance of the above steps.

(3) The second member in each group performs CNOT operation on states $\rho_{1,2}$ and $\rho_{2',3}$ as source system $2'$ and target system 2. After measurement on system $2'$, the second member takes suitable local operator according to the measurement result so that first, second, and third member share the state $\rho_{1,2,3}$ to be close to cat state $\left|\Phi_3^+\right\rangle$. And than the third member carries out on state $\rho_{1,2,3}$ and $\rho_{3',4}$ as source system $3'$ and target system 3 to obtain the state close to $\left|\Phi_4^+\right\rangle$. From these performance continuously all members in each group get the state close to $|\Phi_n^+\rangle$.

(4) Each members in each group randomly takes a measurement on his own particle either in the x- or y-direction, respectively.
(5) Each member in the two groups announces the basis he used through the public channel, but not the result he obtained. The two groups, A and B, obtain $\mathcal{N}_A$ and $\mathcal{N}_B$, respectively. We call the member who finally announces the basis in each group the 'last member'.
(6) Two groups, A and B, collect the outcomes to obtain $\mathcal{M}_A$ and $\mathcal{M}_B$, respectively, and then obtain the shared bit $\mathcal{M}_A \oplus \bar{\mathcal{N}}_A$ and $\mathcal{M}_B \oplus \bar{\mathcal{N}}_B$, respectively.

    In order to obtain the key bit strings, the two groups should repeat the above steps a sufficient number of times.
(7) The two groups have a public discussion on a set of bits used to detect existence of dishonest members. For the test bits, the collectors announce $\mathcal{M}_A$ or $\mathcal{M}_B$, respectively.

    With a set of test bits, the two groups make independently a test so that honest members get correct key string and if they cannot do it, they notice such thing.

    If errors is not enough small, all shared keys should be discarded, and the two groups should go back to Step 1. Otherwise, they obtain secret key strings.

We suggest a method of obtaining $\mathcal{M}_A$ (or $\mathcal{M}_B$). Here, we consider the first member as a collector and all operations are module 2. The collector chooses a random bit 'R', adds it to his outcome, and sends the result to the second member. The second member adds his own outcome to the received one, and then gives it to the next member. This procedure is continued until the collector receives $\mathcal{M}_A$ (or $\mathcal{M}_B$) $\oplus R$. After that, the collector finally takes $\mathcal{M}_A$ (or $\mathcal{M}_B$), which is $\mathcal{M}_A$ (or $\mathcal{M}_B$) $\oplus R \oplus R$.

If each member plays a role of the collector in rotation, all secret key string should be divided among all members with the same portion. If without rotation just one member always plays the collector, the protocol may be similar to the EPR protocol. However, even in such a case it is not the same as the EPR protocol in the aspect of requiring all members' approval. For instance, a message from another group is never decrypted without all members' agreement.

4. Analysis of Security

Firstly, we discuss that when there are some members who behave wrong if two groups, particularly the collectors, have the faulty key strings then they can notice it from the test.

We think over all members' behavior except the collector's one. Because $\mathcal{M}_A$ (or $\mathcal{M}_B$) is possessed by just a collector, any member except the collector cannot know it and hence cannot notice the shared bit. While some members are having behavior wrong, they cannot perceive what is the key bit made by their actions. Moreover, before the test step they cannot perceive if errors will be detected in the test step and what are the bit stings used to test. Hence, if the honest members have key

string wrong then they can certainly notice it by finding errors from sufficiently many test bits.

Let us consider the security of the protocol against eavesdropper. After Step 3 the state to be shared by all members is close to cat state $|\Phi_n^+\rangle$ as shown, i.e the fidelity of the state and $|\Phi_n^+\rangle$ is more than $1-\varepsilon$ for sufficiently small ε. Here we use the Lo-Chau result [11] that if every members share a state having a fidelity exponentially close to 1 with $|\Phi_n^+\rangle^{\otimes t}$ then Eve's mutual information with the key is at most exponentially small. From this fact we can obtain that Eve's mutual information about the secret key of group A and B is sufficiently small. Hence the protocol is secure against eavesdropper.

We will show that after Step 3 the state to be shared by all members is close to cat state $|\Phi_n^+\rangle$.

We consider the operation $CNOT_{s,t}(\otimes_{i=1}^n|\alpha_i\rangle) = \otimes_{i=1}^n|\beta_i\rangle$ defined in the following: $|\beta_i\rangle = |\alpha_s \oplus \alpha_t\rangle$ if $i = s$, and $|\beta_i\rangle = |\alpha_i\rangle$ if $i \neq s$ where α_i and β_i stand for the binary variable in {0,1}.

We assume $\rho_{i',i+1} = \rho_{j',j+1}$, called ρ, for each i and j, because in Step 2 we can do it using LOCC (local operation and classical communication). For the state, called ρ_n, to be shared among all members after Step 3 we show if $F(\rho_{ij}, |\Phi_2^+\rangle\langle\Phi_2^+|) \geq 1-\varepsilon$ than the fidelity $F(\rho_n, |\Phi_n^+\rangle\langle\Phi_n^+|)$ is not less than $1-(n-1)^2\varepsilon$, where the fidelity F of X and Y is defined by

$$F(X,Y) = \mathrm{tr}\left(\sqrt{X^{1/2}YX^{1/2}}\right)^2. \tag{3}$$

In Step 3, we consider the ith member obtains the state $|a_i\rangle$ after measurement on system i' where a_i is the binary variable in {0,1}. In the case, ρ_n can be expressed as following:

$$\rho_n = \sum_{a_2,a_3,\cdots,a_{n-1}} P(a_2,a_3,\cdots,a_{n-1}) \\ (I_1 \otimes \sigma_x^{a_2} \otimes \cdots \otimes \sigma_x^{a_{n-1}})\sigma(a_2,\cdots,a_{n-1})(I_1 \otimes \sigma_x^{a_2} \otimes \cdots \otimes \sigma_x^{a_{n-1}}),$$

where $P(a_2,a_3,\cdots,a_{n-1})$ is the probability that all members except the first member and the nth member obtain the states $|a_2\rangle_{2'}$, $|a_3\rangle_{3'}$, $\cdots$, $|a_{n-1}\rangle_{n-1'}$, respectively, as the result of measurement, and the state $\sigma(a_2,\cdots,a_{n-1})$ is the state shared among all members in the same case.

First of all, we define $|\phi_i\rangle$ in the following:

$$|\phi_0\rangle \equiv |\phi^+\rangle \equiv \tfrac{1}{2}(|00\rangle + |11\rangle)$$
$$|\phi_1\rangle \equiv (I\otimes\sigma_1)|\phi^+\rangle \equiv |\psi^+\rangle \equiv \tfrac{1}{2}(|01\rangle + |10\rangle)$$
$$|\phi_2\rangle \equiv (I\otimes\sigma_2)|\phi^+\rangle \equiv i|\psi^-\rangle \equiv \tfrac{1}{2}(|01\rangle - |10\rangle)$$
$$|\phi_3\rangle \equiv (I\otimes\sigma_3)|\phi^+\rangle \equiv |\phi^-\rangle \equiv \tfrac{1}{2}(|00\rangle + |11\rangle),$$

where $\sigma_0 \equiv I$, $\sigma_1 \equiv \sigma_x$, $\sigma_2 \equiv \sigma_y$, and $\sigma_3 \equiv \sigma_z$.

We use the induction on n ($n \leq 3$). For $n = 3$, each state ρ is represented as $\sum_{i,j=0}^3 a_{ij}|\phi_i\rangle\langle\phi_j|$ where $a_{00} = 1-\varepsilon$, $\sum_{i,j} a_{ij} = 1$, and $a_{ij} = a_{ji}^*$ for each i, j. Then $\rho = \sum_{i,j=0}^3 a_{ij}(I\otimes\sigma_i)|\phi^+\rangle\langle\phi^+|(I\otimes\sigma_j)$. We can describe $\rho_{2,1}$ and $\rho_{2',3}$ by the same expression of ρ.

After performance of $CNOT_{2,2'}$ operation on $\rho_{21} \otimes \rho_{2',3}$ we obtain

$$\sigma(0)_{3,1,2} = \frac{1}{N_0} \sum_{i,j,k,l=0}^{3} a_{ij}a_{kl}(I \otimes \sigma_i \otimes \sigma_k)\big|\Phi_3^+\big\rangle\big\langle\Phi_3^+\big|(I \otimes \sigma_j \otimes \sigma_l),$$

and

$$(I \otimes I \otimes \sigma_1)\sigma(1)_{3,1,2}(I \otimes I \otimes \sigma_k)$$
$$= \frac{1}{N_1} \sum_{i,j,k,l=0}^{3} a_{ij}a_{kl}(I \otimes \sigma_i \otimes \sigma_1\sigma_k\sigma_1)\big|\Phi_3^+\big\rangle\big\langle\Phi_3^+\big|(I \otimes \sigma_j \otimes \sigma_1\sigma_l\sigma_1),$$

where N_0 and N_1 are normalization factors of $\sigma(0)$ and $\sigma(1)$, respectively. Hence,

$$\rho_{3,1,2} = \sum_{i,j,k,l=0}^{3} a_{ij}a_{kl}\left[(I \otimes \sigma_i \otimes \sigma_k)\big|\Phi_3^+\big\rangle\big\langle\Phi_3^+\big|(I \otimes \sigma_j \otimes \sigma_l)\right.$$
$$\left.+(I \otimes \sigma_i \otimes \sigma_1\sigma_k\sigma_1)\big|\Phi_3^+\big\rangle\big\langle\Phi_3^+\big|(I \otimes \sigma_j \otimes \sigma_1\sigma_l\sigma_1)\right].$$

Since $a_{11} + a_{22} + a_{33} = \varepsilon$, $|\Im(a_{03})| \le \sqrt{a_{00} \cdot a_{33'}}$, $|\Re(a_{03})| \le \sqrt{a_{00} \cdot a_{33'}}$, and $\Re(a_{03}^2) = \Re(a_{03})^2 - \Im(a_{03})^2$,

$$\big\langle\Phi_3^+\big|\rho_{2,1',3}\big|\Phi_3^+\big\rangle = \quad a_{00}^2 + a_{33}^2 - 2a_{00} \cdot a_{33} = (a_{00} - a_{03})^2 \ge 1 - 4\varepsilon$$

We suppose that the above fact is hold on $n-1$.

For each i $(0 \le i \le 2^n - 1)$, there is a binary expression $(i_1, \cdots, i_{n-1})$.

$$\rho_{n-1,1,\cdots,n-2} = \quad \textstyle\sum_{i,j} A_{ij}|\phi_i\rangle\langle\phi_i| = \sum_{i,j} A_{ij}(I \otimes S_i)\big|\Phi_{n-1}^+\big\rangle\big\langle\Phi_{n-1}^+\big|(I \otimes S_j)$$

where $A_{00} \ge 1-(n-2)^2\varepsilon$, and $A_{11}+\cdots+A_{(n-1)(n-1)} \le \varepsilon$. Here, $\big|\phi_0^{n-1}\big\rangle = \big|\Phi_{n-1}^+\big\rangle$, and S_i's are of the form $\sigma_x^{i_1} \otimes \sigma_x^{i_2} \otimes \cdots \otimes \sigma_x^{i_{n-2}} \otimes \sigma_z^{i_{n-1}}$. So $(I \otimes S_i)\big|\Phi_{n-1}^+\big\rangle$'s are orthonormal bases on $\mathbb{C}^{n-1}$.

We take $CNOT_{n-1,n-1'}$ operation on $\rho_{n-1,1,\cdots,n-2} \otimes \rho_{n-1',n}$. Then

$$\rho_{n,1,\cdots,n-1} = \sum_{i,j,k,l=0}^{2^n-1} A_{ij}a_{kl}\left[(I \otimes S_i \otimes \sigma_k)\big|\Phi_3^+\big\rangle\big\langle\Phi_3^+\big|(I \otimes S_j \otimes \sigma_l)\right.$$
$$\left.+(I \otimes S_i \otimes \sigma_1\sigma_k\sigma_1)\big|\Phi_3^+\big\rangle\big\langle\Phi_3^+\big|(I \otimes S_j \otimes \sigma_1\sigma_l\sigma_1)\right],$$

and than

$$\begin{aligned}\big\langle\Phi_n^+\big|\rho_{n,1,\cdots,n-1}\big|\Phi_n^+\big\rangle &= A_{00}a_{00} + A_{11}a_{33} + A_{01}a_{03} + A_{10}a_{30} \\ &\ge ((A_{00}a_{00})^{\frac{1}{2}} - (A_{11}a_{33})^{\frac{1}{2}})^2 \\ &\ge 1 - (N-1)^2\varepsilon.\end{aligned}$$

References

[1] C.H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, in *Proceeding of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179; IBM Tech. Discl. Bull. **28** (1985), 3153.

[2] C.H. Bennett, G. Brassard and N.D. Mermin, *Quantum Cryptography without Bell's Theorem*, Phys. Rev. Lett. **68** (1992), 557–559.

[3] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, and W. K. Wooters, *Mixed-state entanglement and quantum error correction*, Phys. Rev. Lett. **76** (1996), 722–725.

[4] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, *Mixed-state entanglement and quantum error correction*, Phys. Rev. A **54** (1996), 3824–3851.

[5] S. Choi, J. Kim, and D.P. Chi, *Quantum key distribution between two groups using secret sharing*, quant-ph/0306067, 2003.

[6] A.R. Calderbank and P.W. Shor, *Good Quantum Error-Correcting Codes Exist*, Phys. Rev. A **54** (1996), 1098–1105; A.M. Steane, *Multiple-particle interference and quantum error correction*, Proc. R. Soc. London A **452** (1996), 2551–2577.

[7] A.K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, Phys. Rev. Lett. **67** (1991), 661–663.

[8] M. Hillery, V. Bužek, and A. Berthiaume, *Quantum secret sharing*, Phys. Rev. A **59** (1999), 1829–1834;

[9] M. Koashi and J. Preskill, *Secure Quantum Key Distribution with an Uncharacterized Source*, Phys. Rev. Lett. **90** (2003), 057902.

[10] D. Mayer, *Unconditional security in Quantum Cryptography*, in Advances in Cryptography.Proceedings of Crypto'96 (Springer-Verlag, New York, 1996), pp. 343–357; J. Assoc. Comput. Mach. **48**, (2001) 351.

[11] H.-K. Lo and H.F. Chau, *Unconditional Security of Quantum Key Distribution Over Arbitrary Long Distances*, Science **283** (1999), 2050–2056.

[12] P.W. Shor and J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Phys. Rev. Lett. **85** (2000), 441–444.

[13] V. Scarani and N. Gisin, *Quantum Communication between N partners and Bell's inequalities*, Phys. Rev. Lett. **87** (2001), 117901; D. Gottesman, H. Lo, N. Lütkenhaus, and J. Preskill, *Security of quantum key distribution with imperfect devices*, Quantum Information and Computation **4** (2004) 325–360; Z. Quan, and T. Chaojing, *Simple proof of the unconditional security of the Bennett 1992 quantum key distribution protocol*, Phys. Rev. A **65** (2002), 062301; M.Curty, and N. Lütkenhaus, *Practical quantum key distribution: On the security evaluation with inefficient single-photon detectors*, Phys. Rev. A **69** (2004), 042321.

(Dong Pyo Chi) School of Mathematical Sciences, Seoul National University, Seoul 151-747, Korea

(Sora Choi) Future Technology Research Division, Electronics and Telecommunications Research Institute, Daejeon 305-350, Korea

(Soojoon Lee) Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, Seoul 130-701, Korea

E-mail address: level@khu.ac.kr