Trends in Mathematics
Information Center for Mathematical Sciences
Volume 8, Number 1, June, 2005, Pages 145–154

# SECURE QUANTUM COMMUNICATION FOR SECRET SHARING

DONG PYO CHI, SORA CHOI, JAEWAN KIM, AND SOOJOON LEE

Abstract. In this paper, we present a protocol in which two or more parties can share multipartite entanglement over noisy quantum channels. Applying this protocol to the quantum communication between several partners, we prove that the quantum communication for secret sharing is secure against all kinds of exterior eavesdropping.

## 1. Introduction

During the last two decades, the theories on quantum communication protocols, such as quantum key distribution (QKD) [1, 2, 9] and quantum teleportation [3], have considerably been developed, and have improved quantum information sciences. Furthermore, quantum communication has almost attained to the practical stage.

A lot of quantum communication protocols [1, 2, 3, 9, 10] require perfect quantum channels, which can conventionally be obtained from entangled particles shared between two or more parties, even though quantum channels are typically noisy. Thus, in order to succeed in a faithful quantum communication via a noisy channel, first of all we should find a process to share a nearly perfect entangled state in a given situation by means of local quantum operations and classical communication (LOCC), which are allowed to perform in quantum communication. The process is called the *entanglement purification*, which have been studied in several ways [4, 5, 6, 12, 16, 18]. In particular, quantum error correcting codes are closely related with entanglement purification protocols [5, 6, 16].

The entanglement purification protocols can provide us with the proofs of the security for quantum communications as well as faithful quantum communications. In this paper, we show that multipartite entanglements can faithfully be shared between two or more parties by the entanglement purification [15], and also show that the quantum communication for secret sharing, proposed by Hillery *et al.* [10],

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

*Key words and phrases.* Quantum cryptography, secret sharing, 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, the third author by a Korea Research Foundation Grant (KRF-2002-070-C00029).

TABLE 1. The effects of Alice's and Bob's measurements on Charlie's state: Alice's and Bob's measurements are given in the columns and in the rows, respectively. Charlie's state, up to normalization, appears in the boxes.

| | | Alice | | | |
|---|---|---|---|---|---|
| | | $+x$ | $-x$ | $+y$ | $-y$ |
| Bob | $+x$ | $\|0\rangle + \|1\rangle$ | $\|0\rangle - \|1\rangle$ | $\|0\rangle - \iota\|1\rangle$ | $\|0\rangle + \iota\|1\rangle$ |
| | $-x$ | $\|0\rangle - \|1\rangle$ | $\|0\rangle + \|1\rangle$ | $\|0\rangle + \iota\|1\rangle$ | $\|0\rangle - \iota\|1\rangle$ |
| | $+y$ | $\|0\rangle - \iota\|1\rangle$ | $\|0\rangle + \iota\|1\rangle$ | $\|0\rangle - \|1\rangle$ | $\|0\rangle + \|1\rangle$ |
| | $-y$ | $\|0\rangle + \iota\|1\rangle$ | $\|0\rangle - \iota\|1\rangle$ | $\|0\rangle + \|1\rangle$ | $\|0\rangle - \|1\rangle$ |

is secure against all kinds of exterior eavesdropping by the faithful sharing of multipartite entanglement.

## 2. Quantum communication protocol for secret sharing

In this section, we briefly review the quantum communication protocol for secret sharing suggested by Hillery *et al.* [10]. Since the three-party quantum communication can easily be generalized to the multiparty case, we consider only the three-party case in this paper.

Let us suppose that Alice, Bob, and Charlie each have one particle from a Greenberger-Horne-Zeilinger(GHZ) triplet [11] which is in the state

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \tag{2.1}$$

They randomly measure their particles in the $x$ or $y$ direction, respectively. Then they publicly announce the direction of their own measurement, but not their results. If the number of measurements in the $y$ direction is even, then they can share bit strings with some kinds of correlations.

Now we show how this works in more detail. Define the $x$ and $y$ eigenstates

$$\begin{aligned} |+x\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); & |+y\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + \iota|1\rangle); \\ |-x\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle); & |-y\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - \iota|1\rangle), \end{aligned} \tag{2.2}$$

where $\iota = \sqrt{-1}$. Since $|0\rangle = (|+x\rangle + |-x\rangle)/\sqrt{2}$ and $|1\rangle = (|+x\rangle - |-x\rangle)/\sqrt{2}$, we can write

$$\begin{aligned} |GHZ\rangle =& \frac{1}{2\sqrt{2}}\left[(|+x\rangle_A|+x\rangle_B + |-x\rangle_A|-x\rangle_B)(|0\rangle_C + |1\rangle_C)\right. \\ &\left. + (|+x\rangle_A|-x\rangle_B + |-x\rangle_A|+x\rangle_B)(|0\rangle_C - |1\rangle_C)\right]. \end{aligned} \tag{2.3}$$

From the decompositions of $|GHZ\rangle$ such as Eq. (2.3), we can obtain the correlations in Table 1.

As seen in Table 1, it can readily be shown that if the number of measurements in the $y$ direction is totally even then the measurement results of any two of them and the other one are correlated or anti-correlated, and hence, any two of them

can obtain the other one's result from their own results. Therefore, Alice, Bob, and Charlie can perform a classical secret sharing, using their bit strings shared by means of the above protocol.

## 3. Three lemmas

3.1. **Shor-Preskill's entanglement purification protocol.** We now review the entanglement purification protocol presented by Shor and Preskill [16]. The protocol exploits the Calderbank-Shor-Steane (CSS) code [7], one of the representative quantum error-correcting codes, and has a merit that one can check the fidelity of the finally shared channel with a perfect quantum channel before completing the protocol, since the protocol was originally constructed in order to prove the security of the QKD protocol proposed by Bennett and Brassard [1]. Thus, if two parties successfully pass the checking procedure in the protocol, then they can share nearly perfect bipartite entanglements with high probability.

We consider the CSS code of $C_1$ over $C_2$, which encodes $m$-qubits in $n$-qubits and can correct up to $t$ errors, where $C_1$ and $C_2$ are classical linear codes such that

$$\{0\} \subset C_2 \subset C_1 \subset \mathbb{Z}_2^n. \tag{3.1}$$

The entanglement purification protocol based on the CSS code is as follows: (1) Alice creates $2n$ Einstein-Podolski-Rosen (EPR) pairs in the state $(|\phi^+\rangle\langle\phi^+|)^{\otimes 2n}$, where

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right) \tag{3.2}$$

is one of Bell states. (2) Alice selects a random $2n$-bit string $b$, and performs a Hadamard transform on the second qubit of each EPR pair for which $b$ is 1. (3) Alice sends the second qubit of each EPR pair to Bob. (4) Bob receives the qubits and publicly announces this fact. (5) Alice selects $n$ of the $2n$ encoded EPR pairs to serve as check bits to test for noises. (6) Alice announces the bit string $b$, and which $n$ EPR pairs are to be check bits. (7) Bob performs Hadamards on the qubits where $b$ is 1. (8) Alice and Bob each measure their qubits of the $n$ check EPR pairs in the $|0\rangle$, $|1\rangle$ basis and share the results. If more than $t$ of these measurements disagree, they abort the protocol. (9) Alice and Bob make the measurements on their code qubits of $\sigma_z^{[r]}$ for each row $r \in H_1$ and $\sigma_x^{[r]}$ for each row $r \in H_2$. Alice and Bob share the results, compute the syndromes for bit and phase flips, and then transform their state so as to obtain $m$ nearly perfect EPR pairs.

Here, $\sigma_a^{[r]}$ is defined by

$$\sigma_a^{[r]} = \sigma_a^{r_1} \otimes \sigma_a^{r_2} \otimes \cdots \sigma_a^{r_n} \tag{3.3}$$

for a Pauli matrix $\sigma_a$, $a \in \{x, z\}$ and a binary vector $r = (r_1, r_2, \ldots, r_n)$, and $H_1$ and $H_2$ are parity check matrices for $C_1$ and $C_2^{\perp}$ respectively. We then obtain the following lemma.

**Lemma 3.1** (Shor-Preskill)**.** *There exists an entanglement purification protocol between two parties, Alice and Bob, in which if they have greater than an exponentially small probability of passing the test then the fidelity of Alice and Bob's state* $\rho_{AB}$ *with* $(|\phi^+\rangle\langle\phi^+|)^{\otimes m}$ *is exponentially close to 1.*

Here, the fidelity $F$ of $\sigma$ with $\tau$ is defined by

$$F(\sigma,\tau)=\mathrm{tr}\left(\sqrt{\sigma^{1/2}\tau\sigma^{1/2}}\right)^2, \tag{3.4}$$

and we then note that

$$F\left(\rho_{AB},\left(\left|\phi^+\right\rangle\left\langle\phi^+\right|\right)^{\otimes m}\right)=\left\langle\phi^+\right|^{\otimes m}\rho_{AB}\left|\phi^+\right\rangle^{\otimes m}. \tag{3.5}$$

3.2. **Isotropic states.** In this paper, we are going to prove the following theorem by exploiting some appropriate LOCC and nearly perfect bipartite entangled states obtained from the entanglement purification protocol in Lemma 3.1.

Let

$$\left|\Phi_d^+\right\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle|j\rangle \tag{3.6}$$

be one of $d$-dimensional generalized Bell states. We remark that $\left|\Phi_2^+\right\rangle=|\phi^+\rangle$ and that when $d=2^m$

$$\left|\Phi_d^+\right\rangle_{AB}=\frac{1}{\sqrt{2^m}}\sum_{j\in\mathbb{Z}_2^m}|j\rangle_A|j\rangle_B=\left|\phi^+\right\rangle_{AB}^{\otimes m}. \tag{3.7}$$

We now consider a one-parameter class of states in $d\otimes d$ quantum systems, called the *isotropic states* [12],

$$\begin{aligned}\rho_F=&\frac{1-F}{d^2-1}\left(I\otimes I-\left|\Phi_d^+\right\rangle\left\langle\Phi_d^+\right|\right)+F\left|\Phi_d^+\right\rangle\left\langle\Phi_d^+\right|\\ =&\frac{d^2(1-F)}{d^2-1}\frac{I\otimes I}{d^2}+\frac{d^2F-1}{d^2-1}\left|\Phi_d^+\right\rangle\left\langle\Phi_d^+\right|,\end{aligned} \tag{3.8}$$

with $F=\langle\Phi_d^+|\rho_F|\Phi_d^+\rangle$. The isotropic states $\rho_F$ have an important property that $\rho_F$ is separable if and only if $\rho_F$ has positive partial transposition if and only if $0\le F\le 1/d$ [12], and furthermore several measures of entanglement for the isotropic states can be calculated by the explicit formulas [17]. Let $\mathcal{T}_{\mathrm{iso}}$ be the $(U\otimes U^*)$-twirling operator defined by

$$\mathcal{T}_{\mathrm{iso}}(\rho)=\int dU(U\otimes U^*)\rho(U\otimes U^*)^\dagger, \tag{3.9}$$

where $dU$ denotes the standard Haar measure on the group of all $d\times d$ unitary operations. Then the operator satisfies the following two properties: $\mathcal{T}_{\mathrm{iso}}(\rho)=\rho_{F(\rho)}$ with $F(\rho)=\left\langle\Phi_d^+\right|\rho\left|\Phi_d^+\right\rangle$ for any state $\rho$ in a $d\otimes d$ quantum system, and $\mathcal{T}_{\mathrm{iso}}(\rho_F)=\rho_F$. We note that $\mathcal{T}_{\mathrm{iso}}$ can be implemented by means of LOCC [8]. Employing the isotropic states $\rho_F$ and the twirling operator $\mathcal{T}_{\mathrm{iso}}$, we readily obtain the following lemma which has essentially originated from the results in [12].

**Lemma 3.2.** *Suppose that Alice and Bob share a state $\rho_{AB}$ in $d \otimes d$ quantum system, $\mathcal{H}_A \otimes \mathcal{H}_B$, such that*

$$\left\langle \Phi_d^+ \middle| \rho_{AB} \middle| \Phi_d^+ \right\rangle \geq 1 - \varepsilon \tag{3.10}$$

*for some $\varepsilon > 0$. Then Alice can teleport any pure state $|\psi\rangle$ in $\mathcal{H}_A$ to Bob in the state $\rho_{|\psi\rangle}$ satisfying*

$$\langle \psi | \rho_{|\psi\rangle} | \psi \rangle \geq 1 - \frac{d}{d+1}\varepsilon, \tag{3.11}$$

*by means of LOCC.*

*Proof.* First, Alice and Bob transform $\rho_{AB}$ to an isotropic state $\rho_F$ by employing the LOCC which can implement the $(U \otimes U^*)$-twirling operator $\mathcal{T}_{\text{iso}}$, where $F = \left\langle \Phi_d^+ \middle| \rho_{AB} \middle| \Phi_d^+ \right\rangle \geq 1 - \varepsilon$. Then Alice teleport a given state $|\psi\rangle$ to Bob via $\rho_F$, using the standard quantum teleportation scheme. Let $\rho_{|\psi\rangle}$ be Bob's final state. Since the scheme produces the fidelity 1 via a maximally entangled state $\left|\Phi_d^+\right\rangle\left\langle\Phi_d^+\right|$ and the fidelity $1/d$ via the maximally mixed state $I \otimes I/d^2$, it follows from Eq. (3.8) that

$$\langle \psi | \rho_{|\psi\rangle} | \psi \rangle = \frac{d(1-F)}{d^2-1} + \frac{d^2F-1}{d^2-1} = \frac{Fd+1}{d+1} \geq 1 - \frac{d}{d+1}\varepsilon. \tag{3.12}$$

This completes the proof. □

3.3. **Partial quantum operation.** The final lemma is a generalization of Theorem 5.3 in [13] into $d$-dimensional quantum systems.

**Lemma 3.3.** *Let $\mathcal{E}$ be a quantum operation on a $d$-dimensional quantum system $\mathcal{H}_A$, and $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_R$ a purification of a state $\rho_A$ on $\mathcal{H}_A$, where $\mathcal{H}_R$ is a reference system such that $\operatorname{tr}_R(|\Psi\rangle\langle\Psi|) = \rho_A$. Suppose that there is $\varepsilon > 0$ such that*

$$\langle \psi | \mathcal{E}(|\psi\rangle\langle\psi|) | \psi \rangle \geq 1 - \varepsilon \tag{3.13}$$

*for all $|\psi\rangle$ in the support of $\rho_A$. Then*

$$\langle \Psi | \left[ (\mathcal{E} \otimes \mathcal{I}_R)(|\Psi\rangle\langle\Psi|) \right] |\Psi\rangle \geq 1 - \left( 1 + d_0 \cdot \max_{j \neq k} \{ p_j p_k \} \right) \varepsilon, \tag{3.14}$$

*where $d_0$ is the Schmidt number of $|\Psi\rangle$ and $\sqrt{p_j}$ are the Schmidt coefficients of $|\Psi\rangle$ with respect to the bipartite quantum system $\mathcal{H}_A \otimes \mathcal{H}_R$.*

*Proof.* By the Schmidt decomposition theorem, $|\Psi\rangle$ can be written as

$$|\Psi\rangle = \sum_{j=0}^{d-1} \sqrt{p_j} |\psi_j\rangle \otimes |\phi_j\rangle \in \mathcal{H}_A \otimes \mathcal{H}_R \tag{3.15}$$

with $p_j \geq 0$ and mutually orthogonal $|\psi_j\rangle$'s in $\mathcal{H}_A$, and it clearly follows that

$$\rho_A = \sum_{j=0}^{d-1} p_j |\psi_j\rangle\langle\psi_j|. \tag{3.16}$$

Then the left-hand side in Eq. (3.14) becomes

$$\sum_{j,k=0}^{d-1}\sum_{\mu} p_j p_k \langle\psi_j|E_\mu|\psi_j\rangle\langle\psi_k|E_\mu^\dagger|\psi_k\rangle, \tag{3.17}$$

where $\mathcal{E}(\sigma)=\sum_\mu E_\mu \sigma E_\mu^\dagger$ is the Kraus operator-sum representation of $\mathcal{E}$ with

$$\sum_{\mu} E_\mu^\dagger E_\mu = I. \tag{3.18}$$

For $0\le\theta\le 2\pi$, we let

$$|\psi_\theta\rangle = \sum_{j=0}^{d-1} (e^{\iota\theta})^{q_j}\sqrt{p_j}|\psi_j\rangle \tag{3.19}$$

where $\iota=\sqrt{-1}$ and $q_j$ are inductively defined by $q_0=0$ and $q_j=\sum_{l=0}^{j-1} q_l+1$ for $j\ge 1$, that is, $q_j=2^{j-1}$ for $j\ge 1$. Then it follows from Eq. (3.13) that

$$\begin{aligned} 1-\varepsilon \le& \langle\psi_\theta|\mathcal{E}(|\psi_\theta\rangle\langle\psi_\theta|)|\psi_\theta\rangle \\ =& \sum_{j,j',k,k'=0}^{d-1}\sum_{\mu} (e^{\iota\theta})^{q_j-q_{j'}+q_k-q_{k'}}\sqrt{p_j p_{j'} p_k p_{k'}}\langle\psi_{j'}|E_\mu|\psi_k\rangle\langle\psi_{k'}|E_\mu^\dagger|\psi_j\rangle, \end{aligned} \tag{3.20}$$

for any $0\le\theta\le 2\pi$. Averaging uniformly the last equation in the inequality (3.20) over all values of $\theta$, from Eq. (3.17) we obtain the following inequality:

$$\begin{aligned} 1-\varepsilon \le& \sum_{j,k=0}^{d-1}\sum_{\mu} p_j p_k \langle\psi_j|E_\mu|\psi_j\rangle\langle\psi_k|E_\mu^\dagger|\psi_k\rangle + \sum_{j\ne k}\sum_{\mu} p_j p_k \langle\psi_j|E_\mu|\psi_k\rangle\langle\psi_k|E_\mu^\dagger|\psi_j\rangle \\ \le& \langle\Psi|\left[(\mathcal{E}\otimes\mathcal{I}_R)\left(|\Psi\rangle\langle\Psi|\right)\right]|\Psi\rangle + \max_{j\ne k}\{p_j p_k\}\sum_{j\ne k}\sum_{\mu}\langle\psi_j|E_\mu|\psi_k\rangle\langle\psi_k|E_\mu^\dagger|\psi_j\rangle. \end{aligned} \tag{3.21}$$

We note that

$$\sum_{\mu}\langle\psi_k|E_\mu|\psi_k\rangle\langle\psi_k|E_\mu^\dagger|\psi_k\rangle \ge 1-\varepsilon, \tag{3.22}$$

by Eq. (3.13) in the assumption of the lemma. Since it follows from Eq. (3.18) that for any $k$

$$\sum_{j=0}^{d-1}\sum_{\mu}\langle\psi_j|E_\mu|\psi_k\rangle\langle\psi_k|E_\mu^\dagger|\psi_j\rangle = 1, \tag{3.23}$$

we get the following inequality:

$$\sum_{j\ne k}\sum_{\mu}\langle\psi_j|E_\mu|\psi_k\rangle\langle\psi_k|E_\mu^\dagger|\psi_j\rangle \le d_0\varepsilon. \tag{3.24}$$

Hence, from the inequalities (3.21) and (3.24) we obtain the inequality (3.14). Therefore, the proof is completed. □

We remark that since $p_j p_k\le 1/4$ for all $j\ne k$

$$\langle\Psi|\left[(\mathcal{E}\otimes\mathcal{I}_R)\left(|\Psi\rangle\langle\Psi|\right)\right]|\Psi\rangle \ge 1-\frac{d_0+4}{4}\varepsilon, \tag{3.25}$$

and that if $\rho_A = I/d$, that is, $|\Psi\rangle$ is a pure maximally entangled state in a $d$-dimensional quantum system then the right-hand side in the inequality (3.14) becomes

$$1 - \frac{d+1}{d}\varepsilon, \tag{3.26}$$

and hence with the result of Lemma 3.2, we readily obtain the following corollary.

**Corollary 3.4.** *Suppose that Alice and Bob share a state $\rho_{AB}$ in $d \otimes d$ quantum system, $\mathcal{H}_A \otimes \mathcal{H}_B$, such that*

$$\left\langle \Phi_d^+ \middle| \rho_{AB} \middle| \Phi_d^+ \right\rangle \geq 1 - \varepsilon, \tag{3.27}$$

*that Alice prepares another state $\left|\Phi_d^+\right\rangle$, and that Alice teleport the second half of $\left|\Phi_d^+\right\rangle$ to Bob via $\rho_{AB}$. Then the state which they finally share has the fidelity not less than $1-\varepsilon$ with $\left|\Phi_d^+\right\rangle$.*

## 4. Main results

**Theorem 4.1.** *A given multipartite entanglement can faithfully be shared between two parties over noisy quantum channels.*

*Proof.* For $N > m$, we let $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_{A'}$ be an $N$-qubit state which Alice and Bob want to share in the way that Alice and Bob possess $N-m$ and $m$ particles, respectively, where $\mathcal{H}_A$ is an $m$-qubit system, and let $\rho_A = \mathrm{tr}_{A'}|\Psi\rangle\langle\Psi|$.

The protocol in which Alice and Bob can faithfully share $|\Psi\rangle$ is as follows: (1) Alice and Bob perform the entanglement purification protocol in Lemma 3.1, so that they can share nearly perfect states. (2) Alice and Bob transform the shared state to an isotropic state by means of LOCC. (3) Alice prepares the state $|\Psi\rangle$, and then they perform the standard teleportation scheme on $m$ particles of $|\Psi\rangle$ via the isotropic state.

We now show that the above protocol can guarantee the faithful sharing of $|\Psi\rangle$.

By Lemma 3.1, Alice and Bob can share $2m$-qubit state $\rho_{AB}$ such that

$$\left\langle \Phi_{2^m}^+ \middle| \rho_{AB} \middle| \Phi_{2^m}^+ \right\rangle \geq 1 - \varepsilon \tag{4.1}$$

for some sufficiently small $\varepsilon > 0$. Thus, it follows from Lemma 3.2 that Alice can teleport any $m$-qubit pure state $|\psi\rangle$ to Bob in the state $\rho_{|\psi\rangle}$ satisfying

$$\langle\psi|\rho_{|\psi\rangle}|\psi\rangle \geq 1 - \frac{2^m}{2^m+1}\varepsilon \tag{4.2}$$

by transforming $\rho_{AB}$ to an isotropic state $\rho_F$ with $F = \left\langle \Phi_{2^m}^+ \middle| \rho_{AB} \middle| \Phi_{2^m}^+ \right\rangle$.

Since all pure states in the support of $\rho_A$ clearly satisfy the inequality (4.2), by Lemma 3.2 and Lemma 3.3, we conclude that

$$\langle\Psi|\left[(\mathcal{E}\otimes\mathcal{I}_{A'})\left(|\Psi\rangle\langle\Psi|\right)\right]|\Psi\rangle \geq 1 - \frac{2^m}{2^m+1}\left(1 + d_0 \cdot \max_{j\neq k}\{p_j p_k\}\right)\varepsilon, \tag{4.3}$$

where $\mathcal{E}$ is the quantum operation representing the standard teleportation via $\rho_F$, and $d_0$ is the Schmidt number of $|\Psi\rangle$ and $\sqrt{p_j}$ the Schmidt coefficients of $|\Psi\rangle$ with respect to a given bipartite system $\mathcal{H}_A \otimes \mathcal{H}_{A'}$. Therefore, since $\varepsilon$ is sufficiently small, the proof of Theorem 4.1 is completed. □

We remark that the right-hand side in the inequality (4.3) is not less than

$$1 - \frac{2^m(d_0+4)}{4(2^m+1)}\varepsilon, \tag{4.4}$$

by the inequality (3.25).

Since more than two parties can share a multipartite entanglement by sequentially executing the protocol for two parties, we immediately obtain the following corollary.

**Corollary 4.2.** *Several parties can faithfully share a given multipartite entanglement over noisy quantum channels.*

We now need a result of Lo and Chau [14] as the following.

**Lemma 4.3** (Lo-Chau)**.** *If Alice and Bob share a state having a fidelity* $1-2^{-s}$ *with* $\left|\Phi_{2^m}^+\right\rangle = |\phi^+\rangle^{\otimes m}$*, then Eve's mutual information with the key is at most* $2^{-c} + 2^{\mathrm{O}(-2s)}$*, where* $c = s - \log_2(2m + s + \log_2 e)$*.*

We remark that $m$ copies of a GHZ state can be expressed as

$$|GHZ\rangle_{ABC}^{\otimes m} = \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} |j\rangle_A |j\rangle_B |j\rangle_C. \tag{4.5}$$

Thus, by Lemma 4.3, we can readily obtain the following lemma.

**Lemma 4.4.** *If Alice, Bob, and Charlie share a state having a fidelity* $1-2^{-s}$ *with* $|GHZ\rangle^{\otimes m}$*, then Eve's mutual information with the key is at most* $2^{-c} + 2^{\mathrm{O}(-2s)}$*, where* $c = s - \log_2(2m + s + \log_2 e)$*.*

Furthermore, this result can easily be generalized to the multipartite case. Thus, we can directly notice that if every members share a state having a fidelity exponentially close to 1 with copies of generalized GHZ states, such as $(\left|0^N\right\rangle + \left|1^N\right\rangle)/\sqrt{2}$, then Eve's mutual information with the key is at most exponentially small. Therefore, by Corollary 4.2, we obtain the following theorem.

**Theorem 4.5.** *The quantum communication protocol for secret sharing is secure against all kinds of exterior eavesdropping.*

## 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, *Quantum Cryptography Using Any Two Nonorthogonal States*, Phys. Rev. Lett. **68** (1992), 3121–3124.

[3] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, *Teleporting an Unknown Quantum State via a Dual Classical and Einstein-Podolski-Rosen Channels*, Phys. Rev. Lett. **70** (1993), 1895–1899.

[4] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, and W.K. Wootters, *Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels*, Phys. Rev. Lett. **76** (1996), 722-725.

[5] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, *Authentication of Quantum Messages*, in *Proceeding of the 43rd Annual IEEE Symposium on the Foundations of Computer Science* (FOCS '02), pp. 449–458. IEEE Press, 2002.

[6] 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.

[7] 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.

[8] W. Dür, J.I. Cirac, M. Lewenstein, and D. Bruß, *Distillabillty and partial transposition in bipartite system*, Phys. Rev. A **61** (2000), 062313.

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

[10] M. Hillery, V. Bužek, and A. Berthiaume, *Quantum secret sharing*, Phys. Rev. A **59** (1999), 1829–1834; A. Karlsson, M. Koashi, and N. Imoto *Quantum entanglement for secret sharing and secret splitting*, Phys. Rev. A **59** (1999), 162–168; V. Scarani and N. Gisin, *Quantum Communication between N partners and Bell's inequalities*, Phys. Rev. Lett. **87** (2001), 117901; V. Scarani and N. Gisin, *Quantum Key Distribution between N partners: optimal eavesdropping and Bell's inequalities*, Phys. Rev. A **65** (2002), 012311; S. Choi, J. Kim, and D.P. Chi, *Quantum key distribution between two groups*, quant-ph/0306067, 2003.

[11] D. Greenberger, M. Horne, and A. Zeilinger in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kaftos (Kluwer Academic, Dordrecht, 1989).

[12] M. Horodecki and P. Horodecki, *Reduction criterion of separability and limits for a class of distillation protocols*, Phys. Rev. A **59** (1999), 4206–4216; M. Horodecki, P. Horodecki, and R. Horodecki, *General teleporation channel, singlet fraction, and quasidistillation*, Phys. Rev. A **60** (1999), 1888–1898; P. Badziąg, M. Horodecki, P. Horodecki, and R. Horodecki, *Local environment can enhance fidelity of quantum teleportation*, Phys. Rev. A **62** (2000), 012311.

[13] E. Knill and R. Laflamme, *Theory of quantum error-correcting codes*, Phys. Rev. A **55** (1997), 900–911.

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

[15] S. Lee, S. Choi, and D.P. Chi, *Faithful Sharing of Multipartite Entanglement over Noisy Quantum Channels*, J. Korean Phys. Soc. **45** (2004), 1119–1122.

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

[17] B.M. Terhal and K.G.H. Vollbrecht, *Entanglement of formation for isotopic states*, Phys. Rev. Lett. **85** (2000), 2625–2628; K.G.H. Vollbrecht and R.F. Werner, *Entanglement measures under symmetry*, Phys. Rev. A **64** (2001), 062307; P. Rungta and C.M. Caves, *Concurrence-based entanglement measures for isotropic states*, Phys. Rev. A **67** (2003), 012307; S. Lee, D.P. Chi, S.D. Oh, and J. Kim, *Convex-roof extended negativity as an entanglement measure for bipartite quantum systems*, Phys. Rev. A **68** (2003), 062304.

[18] V. Vedral and M.B. Plenio, *Entanglement measures and purification procedures*, Phys. Rev. A **57** (1998), 1619–1633.

(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

(Jaewan Kim) School of Computational Sciences, Korea Institute for Advanced Study, Seoul 130-722, 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