Economical (k, m)-threshold controlled quantum teleportation

Akira SaiToh*[1], Robabeh Rahimi†[1], and Mikio Nakahara‡[1,2]
[1]Research Center for Quantum Computing, Interdisciplinary Graduate School of
Science and Engineering, Kinki University, 3-4-1 Kowakae, Higashi-Osaka, Osaka 577-8502, Japan
[2]Department of Physics, Kinki University, 3-4-1 Kowakae, Higashi-Osaka, Osaka 577-8502, Japan

Last modified: 14 June 2009

Abstract

We study a (k, m)-threshold controlling scheme for controlled quantum teleportation. A standard polynomial coding over GF(p) with prime $p > m - 1$ needs to distribute a d-dimensional qudit with $d \geq p$ to each controller for this purpose. We propose a scheme using m qubits (two-dimensional qudits) for the controllers' portion, following a discussion on the benefit of a quantum control in comparison to a classical control of a quantum teleportation.

Keywords: Quantum teleportation, Threshold scheme, Secret sharing
PACS: 03.67.Hk, 03.67.Mn

1 Introduction

Quantum teleportation [1] has been one of the leading discoveries followed by numerous quantum information processing technologies [2, 3]. Controlled quantum teleportation [4, 5, 6, 7, 8] is a variant in which a teleportation of a quantum state is performed under the supervision of controllers. Schemes using qubits as keys distributed among controllers [4, 5, 6, 7, 8] have been extensively studied and economization of required resources has been accomplished with respect to the number of qubits involved in an entangled qubit chain used in a scheme. The studies also include a security discussion on players' cheating controllers [9].

It is expected that a multifunctional quantum network is realized for a consumer market in future, presumably based on optical fibers. So far, simple quantum cryptosystems [10, 11] are highly developed [12, 13, 14, 15, 16, 17] toward the consumer use, which are mainly used to generate classical shared cryptographic keys. An advanced quantum network should be used not only for generating a classical key but for exchanging quantum states. A network with Einstein-Podolsky-Rosen (EPR) pairs as links [18] is a plausible form for this purpose; optical quantum teleportation has already become a well-established subject supported by many experimental demonstrations reported in, e.g., Refs. [19, 20, 21]. Considering an application for office networks, it is demanded that data transfers can be under the control of multiple supervisors. Controlled teleportation schemes have been developed to enable this feature. As the number of usable qubits and the quality of entanglement enhances, this function is approaching reality. A function like a vote to permit a transfer is also considered to be of public demand.

Qubit keys are commonly used in controlled quantum teleportation schemes for the basic control such that approvals of all the controllers are required to let the players transfer a quantum state. In such a control, use of qubit keys is sufficient and extending each dimension of a quantum system for a key causes a redundancy. Qudits (d-dimensional quantum systems) with $d > 2$ have been, in contrast, considered to be useful as keys when a vote for decision is in order.

It is easy to notice that such functions are enabled by using a threshold scheme [22, 23, 24, 25, 26]: controlling a transfer of a quantum state with a certain threshold in the number of controllers is implemented by secret sharing schemes (see, e.g., a discussion in Ref. [27]). This categorizes controlled quantum teleportation as a combination of quantum secret sharing and quantum teleportation. A well-known polynomial coding [23, 26] over GF(p) with prime p larger than the number m of participants (controllers in our context) is a quick solution[1]. A classical or quantum (k, m)-threshold scheme applied to a shared state of players and controllers enables a control such that a receiver can recover an original state when and only when k or more controllers among m provide their keys. There is a variant of quantum polynomial coding robust against a certain number of cheaters among participants [28].

A drawback to introduce a polynomial coding scheme in controlled quantum teleportation is that computation is conducted over the field GF(p). Thus each qudit distributed among controllers should have the dimension $d \geq p$. This also complicates a quantum circuit to compute a matrix equation for the coding. For a threshold scheme, i.e., a secret sharing without imposing access structure[2], the di-

*saitoh@alice.math.kindai.ac.jp
†rahimi@alice.math.kindai.ac.jp
‡nakahara@math.kindai.ac.jp

[1] Note that p can be equal to m if m is prime in the context of controlled quantum teleportation (See Sec. 3).

[2] See, e.g., Ref. [29] and citations therein for secret sharing schemes

mension of each key (share) using best known classical protocols [30, 31] is $O(2^m)$ (namely, $O(m)$ bits for each key) for a long secret. These protocols require the bit length of a secret $O(m)$ and that of a key at least as much as the length of a secret. For a short secret, a best known classical protocol is Shamir's one [23] in which each key has the dimension $\geq p > m$. It is thus not motivating to simply make a quantum extension of the classical protocols.

It was reported that an (m, m)-threshold secret sharing of a classical secret is achieved by a sort of key distribution without entanglement [32] and an (m, m)-threshold controlled quantum teleportation is achieved by using classical keys [33]. The latter one is easily extended to a (k, m)-threshold controlling scheme. Nevertheless, schemes using qudits for controllers' portion are more secure than the one using only classical keys as we will discuss in Sec. 4.1. There is a recently-proposed graph-state formalism [34] to produce quantum secret sharing systems using only qubits. This approach has achieved the systems for several particular (k, m) and not for general (k, m). We will construct a scheme which is not a direct extension of these approaches.

In this paper, we introduce a (k, m)-threshold controlled quantum teleportation scheme over GF(p) with prime $p > m - 1$ using m qubits for the controllers' portion in addition to classical information distributed to the controllers. This is achieved by a hybrid of classical and quantum protocols. It enables a reduction in the dimension of each qudit to two for general (k, m), which is a significant improvement for realizing the scheme. In contrast to classical systems, the dimension of a quantum system is limited and usually a large-dimensional qudit is implemented by multiple qubits. The size of a qudit register is also very limited in the present technology. The number of available qubits is, so far, twelve or less [35].

To begin with, a standard controlled quantum teleportation scheme is briefly described in Sec. 2. On the basis of the scheme, a (k, m)-threshold controlled quantum teleportation using a polynomial coding is briefly explained in Sec. 3. A reduction in required resources for the threshold-control scheme is accomplished in Sec. 4: First, a classical control of a quantum teleportation is discussed in Sec. 4.1. Second, a control of a quantum teleportation using m qubits for the controllers' portion is introduced in Sec. 4.2. Third, an economization of Bob's operations is accomplished in Sec. 4.3. An explicit preparation of an initial state for this economized scheme is shown in Sec. 5 together with the operational complexity of the whole process. We discuss advantages and disadvantages of the scheme in Sec. 6. Section 7 summarizes our results.

involving access structures.

2 A Standard Controlled Quantum Teleportation

Consider a controlled quantum teleportation using $(n-1)$ EPR pairs shared by Alice and Bob, and a single quantum system shared by Alice, Bob, and m controllers. Alice tries to send an n-qubit state

$$\sum_{x_1 \ldots x_n = 0\ldots 0}^{1\ldots 1} p_{x_1 \ldots x_n} |x_1 \ldots x_n\rangle_{\mathrm{A'}_1 \ldots \mathrm{A'}_n}$$

of the system A$'$ to Bob. A standard quantum teleportation protocol works fine for the $(n-1)$-EPR-pair channel consisting of $(n-1)$ pairs $\mathrm{A}_1\mathrm{B}_1, \ldots, \mathrm{A}_{n-1}\mathrm{B}_{n-1}$. The remaining channel, $\mathrm{A}_n\mathrm{B}_n$, is under the control of m controllers $\mathrm{C}_1, \ldots, \mathrm{C}_m$. The setup of the quantum system is illustrated in Fig. 1. Here it should be noted that, although we consider the control of a single channel here, it is straightforward to attach controllers to each channel. Thus let us limit setups to the illustrated one in the following. The initial state of the illustrated system is given by

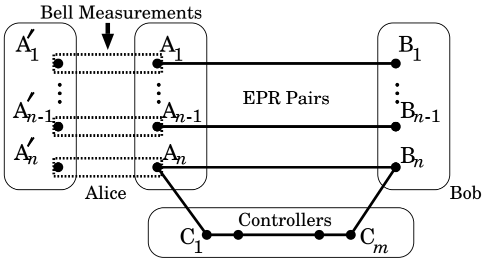

Figure 1: Illustration of qudit sharing for a controlled quantum teleportation.

$$|\mathrm{A'ABC}\rangle = \left(\sum_{x_1 \ldots x_n = 0\ldots 0}^{1\ldots 1} p_{x_1 \ldots x_n} |x_1 \ldots x_n\rangle_{\mathrm{A'}_1 \ldots \mathrm{A'}_n} \right) \otimes \left(\bigotimes_{l=1}^{n-1} \frac{1}{\sqrt{2}} \sum_{y_l = 0}^{1} |y_l\rangle_{\mathrm{A}_l} |y_l\rangle_{\mathrm{B}_l} \right) \otimes |\xi\rangle_{\mathrm{A}_n\mathrm{B}_n\mathrm{C}_1\ldots\mathrm{C}_m}$$

with

$$|\xi\rangle_{\mathrm{A}_n\mathrm{B}_n\mathrm{C}_1\ldots\mathrm{C}_m} = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} |yy\rangle_{\mathrm{A}_n\mathrm{B}_n} |\kappa(y)\rangle_{\mathrm{C}_1\ldots\mathrm{C}_m} \qquad (1)$$

a shared state involving the controllers' portion $|\kappa(y)\rangle_{\mathrm{C}_1\ldots\mathrm{C}_m}$ to be engineered for a tailored controlling scheme.

Let us recall the well-known relation

$$|x, y\rangle = \frac{1}{\sqrt{2}} \sum_{i=0}^{1} (-1)^{x \cdot i} |B_{i, x\oplus y}\rangle,$$

where $|x, y\rangle$ is a computational basis vector and $|B_{i,j}\rangle = (1/\sqrt{2}) \sum_{x=0}^{1} (-1)^{x \cdot i} |x, j \oplus x\rangle$ is the (i, j)th Bell basis vector (here, $j = x \oplus y$, i.e., $y = j \oplus x$). With this relation, we can rewrite the initial state as

$$\begin{aligned} &|\mathrm{A}'\mathrm{ABC}\rangle \\ &= \frac{1}{2^n} \sum_{x_1 \ldots x_n} p_{x_1 \ldots x_n} \Bigg[\Bigg(\bigotimes_{l=1}^{n-1} \sum_{i_l=0}^{1} \sum_{j_l=0}^{1} (-1)^{x_l \cdot i_l} \\ &\times |B_{i_l, j_l}\rangle_{\mathrm{A'}_l \mathrm{A}_l} |j_l \oplus x_l\rangle_{\mathrm{B}_l} \Bigg) \otimes \Bigg(\sum_{i_n=0}^{1} \sum_{j_n=0}^{1} (-1)^{x_n \cdot i_n} \\ &\times |B_{i_n, j_n}\rangle_{\mathrm{A'}_n \mathrm{A}_n} |j_n \oplus x_n\rangle_{\mathrm{B}_n} |\kappa(j_n \oplus x_n)\rangle_{\mathrm{C}_1 \ldots \mathrm{C}_m} \Bigg) \Bigg]. \end{aligned} \tag{2}$$

As is usual for a standard quantum teleportation, Alice makes Bell measurement on each $(\mathrm{A'}_l \mathrm{A}_l)$ pair and obtains an outcome (i_l, j_l).

Bob receives information $\{(i_l, j_l)\}$ from Alice and applies $\bigotimes_{l=1}^{n-1} Z^{i_l} X^{j_l}$ to $\mathrm{B}_1 \ldots \mathrm{B}_{n-1}$. This changes the state of each B_l (of each term in the summation) from $(-1)^{x_l \cdot i_l} |j_l \oplus x_l\rangle_{\mathrm{B}_l}$ to $|x_l\rangle_{\mathrm{B}_l}$ and hence the teleportation process for the original state of A' is completed up to $l = n-1$.

To complete the recovery of the original state of A' at Bob's side, he has to apply a certain operation to B_n. This requires Bob to know the effect of controllers' measurements on $|\kappa(j_n \oplus x_n)\rangle_{\mathrm{C}_1 \ldots \mathrm{C}_m}$. Operations Bob has to apply to B_n depend on the controlling scheme.

A popular controlled quantum teleportation scheme is the case where $|\kappa(y)\rangle_{\mathrm{C}_1 \ldots \mathrm{C}_m}$ is set to $|y \ldots y\rangle_{\mathrm{C}_1 \ldots \mathrm{C}_m}$, i.e., $|\xi\rangle_{\mathrm{A}_n \mathrm{B}_n \mathrm{C}_1 \ldots \mathrm{C}_m}$ is set to a Greenberger-Horne-Zeilinger (GHZ) state, and each controller makes a measurement in the X basis. Measuring C_s in the X basis results in the phase factor $(-1)^{y \cdot (h_s == -1)}$ depending on the outcome h_s (here, $s \in \{1, \ldots, m\}$; the operation "$==$" returns one if its two arguments are equal and zero otherwise)[3]. In this case, Bob first applies $Z^{i_n} X^{j_n}$ to B_n. In addition, he applies a single Z gate to B_n for recovery if the number of $-$'s in the controllers' outcomes ($\in \pm$) is odd. The final state of Bob after these operations becomes $\sum_{x_1 \ldots x_n} p_{x_1 \ldots x_n} \bigotimes_{l=1}^{n} |x_l\rangle_{\mathrm{B}_l}$. The teleportation is successful in this way.

In this contribution, we aim to introduce a threshold-control scheme in which the shared state $|\xi\rangle_{\mathrm{A}_n \mathrm{B}_n \mathrm{C}_1 \ldots \mathrm{C}_m}$ is engineered to be different from the GHZ state. We continue to concentrate on the case where only a single qubit of Bob is under the control, as illustrated in Fig. 1; this is because it is straightforward to extend the scheme so that multiple qubits are under the control. Such an extension will be considered only in Sec. 4.3.

3 (k, m)-Threshold Controlled Quantum Teleportation

The functionality of threshold control is achieved by engineering the initial setup of the shared state given by Eq. (1). Let us begin with a rather expensive scheme that is a straightforward extension of a classical secret sharing. In this scheme, the state of the controllers' portion is assumed to be in the following form

$$\begin{aligned} &|\kappa(y)\rangle_{\mathrm{C}_1 \ldots \mathrm{C}_m} \\ &= \frac{1}{\sqrt{\#\mathcal{S}}} \sum_{c_1 \ldots c_m \in \mathcal{S}} e^{iy\theta(c_1 \ldots c_m)} |c_1 \ldots c_m\rangle_{\mathrm{C}_1 \ldots \mathrm{C}_m}, \end{aligned} \tag{3}$$

where $y = j_n \oplus x_n$, $c_s \in \{0, \ldots, d-1\}$ ($s \in \{1, \ldots, m\}$ and d is a positive integer), and $\mathcal{S}$ is a certain set of m-digit strings; the computational basis for each C_s is chosen arbitrarily and known by the sth controller. There are two conditions for the state appropriate for a (k, m)-threshold scheme:
(i) $\theta(c_1 \ldots c_m)$ cannot be uniquely determined unless the sequence $c_1 \ldots c_m$ is completely specified (i.e., unless the variables $c_1, \ldots, c_m$ are all specified).
(ii) A string $c_1 \ldots c_m$ is uniquely determined in $\mathcal{S}$ by fixing any k digits of $c_1, \ldots, c_m$.
Under these conditions, k controllers' measurements result in a single surviving vector $|c_1 \ldots c_m\rangle$. Thus Bob can recover the original state by the following process (in addition to the usual process for the original quantum teleportation for $l = 1, \ldots, n-1$). First Bob changes the phase factor $e^{iy\theta(c_1 \ldots c_m)}$ to unity by applying

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{-i\theta(c_1 \ldots c_m)} \end{pmatrix}$$

to the qubit B_n. Second Bob applies $Z^{i_n} X^{j_n}$ to B_n as is usual for a quantum teleportation. In these steps, Alice's Bell measurement on $\mathrm{A'}_n \mathrm{A}_n$ prior to controllers' measurements does not affect Bob's operation to recover the phase appearing as a result of controllers' measurements. This is clear from the initial state described in Eq. (2); the parameter $y = j_n \oplus x_n$ is common in the states of B_n and controllers' portion.

Let us turn to a system construction for satisfying the conditions. Condition (i) is satisfied by setting $\theta(c_1 \ldots c_m) = \sum_{s=1}^{m} c_s \pi / d$. Such $\theta(c_1 \ldots c_m)$ cannot be uniquely determined unless the variables $c_1, \ldots, c_m$ are completely specified. A quantum circuit to attach the phase factors is easily realized: from $s = 1$ to m, applying an A_n-controlled C_s-controlled phase gate with the phase $c_s \pi / d$, acting on a work qubit accomplishes this task. For the condition (ii), we will find a proper set $\mathcal{S}$ of m-digit vectors $c_1 \ldots c_m$ by a certain coding scheme. This is the main concern as the resource for quantum information processing is limited in the current technologies; a coding with a small resource is desirable.

We revisit the theory of Karnin *et al.* [24], which describes a sufficient condition for coding in a threshold scheme, and evaluate a polynomial-coding scheme [23, 26] as a typical example.

We begin with a well-known property of a linear matrix equation.

Proposition: A solvable matrix equation over

[3] This is because a computational basis state $|c\rangle$ of a qubit can be written as $|c\rangle = \frac{1}{\sqrt{2}} \sum_{h=+1,-1} (-1)^{c \cdot (h == -1)} |h\rangle$ using the X-basis states $|h\rangle$.

GF(p),

$$A\mathbf{x} = \mathbf{b}$$

with p a prime number, $A \in \mathrm{GF}(p)^{f\times g}$, $\mathbf{x} \in \mathrm{GF}(p)^g$, and $\mathbf{b} \in \mathrm{GF}(p)^f$ has a unique solution $\mathbf{x}$ if and only if $f \geq g$ and A has a full rank.

The proof is similar to the case of a real number field (see, e.g., Ref. [36, pages 96,103]).
Proof— (i) First we prove that the solution $\mathbf{x}$ is unique if $f \geq g$ and A has a full rank. Assume that there are two solutions $\mathbf{x}_1$ and $\mathbf{x}_2$. Then, $A\mathbf{x}_1 = A\mathbf{x}_2$. Let us pick up g rows of A appropriately to generate $\tilde{A}$ so that $\tilde{A}$ has a full rank. This is possible because otherwise the number of linearly independent row vectors of A should be less than g, which is a contradiction. We have thus $\tilde{A}\mathbf{x}_1 = \tilde{A}\mathbf{x}_2$ with the square full-rank matrix $\tilde{A}$. The matrix $\tilde{A}$ can be reduced to a diagonal matrix with nonzero diagonal elements by basic operations; thus $\det\tilde{A} \neq 0$. Consequently, $\mathbf{x}_1 = \mathbf{x}_2$ because $\tilde{A}^{-1}$ exists. This is a contradiction. (ii) Second we prove that $f \geq g$ and A has a full rank if $\mathbf{x}$ is a unique solution. The contraposition of this statement is that solution $\mathbf{x}$ is not unique if $f < g$ or rank A is less than $\min(f, g)$. This is easily shown to be true. □

On the basis of this proposition, a coding of our interest is achieved by a matrix equation for $(f, g) = (m, k)$ with a full-rank matrix A such that striking any $(m-k)$ rows keeps the rank full [24]. Given a matrix equation

$$A\mathbf{x} = (c_1, \ldots, c_m)^t \tag{4}$$

with such A which is notified to Bob, we prepare $|\kappa(y)\rangle_{\mathrm{C}_1\ldots\mathrm{C}_m}$ as

$$|\kappa(y)\rangle_{\mathrm{C}_1\ldots\mathrm{C}_m} = \frac{1}{\sqrt{\#\mathcal{S}_\mathbf{x}}} \sum_{c_1\ldots c_m \in \mathcal{S}_\mathbf{x}} e^{iy\theta(c_1\ldots c_m)} |c_1 \ldots c_m\rangle_{\mathrm{C}_1\ldots\mathrm{C}_m}$$

where $\mathcal{S}_\mathbf{x}$ is a set of $c_1 \ldots c_m$ corresponding to $\mathbf{x} \in \mathrm{GF}(p)^k$ (hence $\#\mathcal{S}_\mathbf{x} \leq p^k$). Suppose that at least k controllers measure their qudits in the computational basis. Then $\mathbf{x}$ is fixed uniquely because the matrix equation becomes solvable by using the rows corresponding to the fixed c_s's. This implies that the superposition is then resolved. Bob can determine the phase factor that he should modify by receiving at least k outcomes from controllers.

We have seen a common construction of a threshold scheme. Required resources for the threshold scheme are mostly dependent on the choice of the matrix A. There are two practical ways among many [24, 25]. One is the matrix in the form

$$A_{(\mathrm{i})} = (\ I \mid T\ )^t$$

with I the $k \times k$ identity matrix and T a $k \times (m-k)$ strictly totally positive matrix [37, 38]. Any minor of T is nonzero positive from the definition of strict total positivity; hence any k rows of A build up a square matrix with nonzero determinant. Thus a matrix equation with $A_{(\mathrm{i})}$ can be used for the threshold scheme. A drawback is the difficulty to find a strictly totally positive matrix T for sufficiently small prime p. A known systematic construction [39] for strictly totally positive matrices uses the largest element of T growing exponentially in dim T. Thus p also grows exponentially if we follow the construction. A manual optimization is indispensable.

The other is a Vandermonde matrix used in the well-known Shamir's scheme [23],

$$A_{(\mathrm{ii})} = V_{m,k} = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_m & x_m^2 & \cdots & x_m^{k-1} \end{pmatrix} \mod p \tag{5}$$

with mutually different x_i's with prime $p > m-1$. ($p > m-1$ is necessary to set x_i's mutually different.) Striking $(m-k)$ rows generates a square Vandermonde matrix and it is nonsingular when x_i's are mutually different (see, e.g., pages 43 and 219 of Ref. [40]). Hence a matrix equation with $A_{(\mathrm{ii})}$ can be used for the threshold scheme. This matrix has been known to be economical because p increases linearly in m. Each qudit distributed to a controller should have the dimension $d \geq p$, consequently. Nevertheless, one may need to further reduce the dimension considering the poor resources of presently available qudit systems [35, 41].

4 Economizing the Threshold Control Scheme

The dimension of each digit distributed to a party (a controller in the present context) is often evaluated by using the scale of "bit length" in conventional secret sharing schemes. Each key is $O(\log m)$-bit long [23] ($O(m)$-bit long [30, 31]) in the best known protocols for a short secret with the bit length $O(\log m)$ (for a long secret with the bit length $O(m)$) although this has not been taken as a drawback at all since classical bits are very cheap. Nevertheless, in quantum protocols one should not consume many qubits for individual quantum systems. It is of our concern to find a smaller dimension for each controller's qudit facing a limited resource of a quantum system.

One way is to abandon the use of quantum systems for controllers' portion and instead use a classical threshold scheme to control a quantum teleportation. A controlled teleportation proposed by Zhang and Man [33], in the context of (m, m) threshold, uses classical keys shared by Alice and controllers for encoding Alice's messages, which can be easily extended to a general threshold-control scheme. Here, we introduce a different scheme where controllers' qudits are simply replaced by classical digits. We will face the fact that classical control schemes are indeed economical but their security is based on classical keys. Using qudits is found to be more robust against Bob's physical-access attack.

Our interest is to find such a robust scheme with a simple quantum state for the controllers' portion. It is shown to be constructed by using the matrix equation with the Vandermonde matrix (5) and qubit states distributed to the controllers. We further perform an economization in the number of Bob's operations, which is useful for an extension in which multiple EPR channels are under controllers' control.

4.1 Classically-Controlled Quantum Teleportation

As we mentioned, the simplest way of economization is to use classical control digits instead of quantum ones. This is easily achieved by setting the state (not a state, actually) of the controllers' portion to be a scalar

$$|\kappa(y)\rangle_{\mathrm{C}_1\dots\mathrm{C}_m} = e^{iy\theta(c_1,\dots,c_m)}$$

with phase θ dependent on integers $c_1, ..., c_m$, the classical keys of a certain classical threshold scheme. Bob can modify this scalar factor by applying $\mathrm{diag}[1, e^{-i\theta(c_1,\dots,c_m)}]$ to his nth qubit B_n if he can gather at least k of the keys.

The security of the scheme is dependent on the classical scheme. Indeed, classical keys can be securely distributed by using a quantum key distribution (see Ref. [42] and references therein) and the risk of an interception during the key distribution is negligible. Classical keys are, however, easily copied by careless controllers. A possible drawback of the scheme is that controllers cannot stop Bob from recovering Alice's original state if Bob manages to obtain at least k of the keys without consent of the controllers. In contrast, in a threshold scheme using qudits, the operations for a recovery of the original state are unfixed until k controllers make measurements. This fact makes the quantum one more robust: Recall that the computational basis for C_s in Eq. (3) is not necessarily known in public. The correct basis for a measurement can be left unknown to Bob. Then, Bob cannot obtain c_s by a physical access to C_s unless he also has an access to the information on the measurement basis. Thus the cost for Bob to steal c_s's in the scheme is more than that in the classically controlled one. This logic is similar to the one utilized for keeping the security of dealer-player communications in some quantum threshold schemes [32, 34].

It should be mentioned that robustness depends on the type of protocol violations. Let us discuss a different type of violation that can be made by Bob. It is a common occasion that controllers do not want Bob to process further with a teleported state before they officially vote for their decision. A violation in this regard occurs when k or more controllers are friendly to Bob and they measure their qudits or digits and send the outcomes before the voting starts officially. This violation in the schedule of the procedure cannot be prevented even if qudits are distributed.

In the following, an economical quantum control scheme is introduced in order to reduce the resource for controllers' quantum system as we have mentioned. It is now our additional motivation to resolve the schedule violation problem due to friendly controllers.

4.2 Economical Quantum Threshold-Controlled Quantum Teleportation

As is discussed above, a quantum threshold scheme has a classically unachievable property, namely that the operations for a recovery of the original state are unfixed until controllers make measurements and the measurement bases can be left unnotified to Bob. As we have mentioned, our aim is to achieve such a scheme using small-dimensional systems for controllers' portions. Here, we propose a quantum protocol for the (k, m)-threshold controlled quantum teleportation with m qubits distributed to the controllers. It also resolves the problem of the possible violation in the voting schedule.

It is implemented with the following state for the controllers' portion:

$$\begin{aligned}&|\kappa(y)\rangle_{\mathrm{C}_1\dots\mathrm{C}_m}\\ &= \frac{1}{\sqrt{2^m}}\bigotimes_{s=1}^{m}[e^{i2\pi y c_s/p}|\tilde{0}_s\rangle + e^{i2\pi\neg y c_s/p}|\tilde{1}_s\rangle]_{\mathrm{C}_s},\end{aligned} \qquad (6)$$

where $|\tilde{0}_s\rangle$ and $|\tilde{1}_s\rangle$ are the basis vectors of the sth controller's chosen basis; $\neg y$ is a logical negation of y and c_s's are the keys of the following common classical polynomial-coding threshold scheme. The keys are generated from Eq. (4) using a Vandermonde matrix for A and a certain fixed vector for $\mathbf{x}$ [all the matrix and vector elements are in $\mathrm{GF}(p)$]. The matrix A is notified to Bob and $\mathbf{x}$ is hidden. Thus k or more keys are required for Bob to determine the remaining keys from Eq. (4).

The protocol imposed to controllers is as follows.
(I) Each controller $\mathrm{C}_{s,\mathrm{agree}}$ who agrees to allow Bob to recover Alice's original state measures her/his qubit in the basis $\{|\tilde{0}_s\rangle, |\tilde{1}_s\rangle\}$ and sends its outcome $r_s \in \{0, 1\}$ to Bob.
(II) $\mathrm{C}_{s,\mathrm{agree}}$ also sends her/his key c_s to Bob.
(III) Each controller $\mathrm{C}_{s,\mathrm{disagree}}$ who disagrees to allow Bob to recover Alice's original state does not make any action until she/he receives a contact from Bob.
(IV) When a solicit is sent from Bob, $\mathrm{C}_{s,\mathrm{disagree}}$ must measure her/his qubit in the basis $\{|\tilde{0}_s\rangle, |\tilde{1}_s\rangle\}$ and send its outcome $r_s \in \{0, 1\}$ to Bob.

The protocol imposed to Bob is as follows.
(i) Bob receives (i_l, j_l)'s from Alice. Bob applies $\bigotimes_{l=1}^{n-1} Z^{i_l}X^{j_l}$ to $\mathrm{B}_1 ... \mathrm{B}_{n-1}$.
(ii) Bob waits for at least k pairs of (r_s, c_s)'s sent from the controllers.
(iii) Bob calculates the remaining c_s's by substituting the obtained c_s's into Eq. (4) if at least k pairs are obtained; aborts otherwise.
(iv) Bob sends solicits to the controllers who did not send information to him.
Note: it is possible to count his solicits. Therefore, he cannot cheat by sending more than $(m-k)$ solicits in this stage

even when he succeeds in stealing k or more c_s's beforehand.
(v) Bob receives the remaining r_s's.
(vi) Bob modifies the phase factor due to controllers' measurements in his phase recovery process described below.
(vii) Bob applies $Z^{i_n} X^{j_n}$ to B_n.

Bob's phase recovery process corresponding to the controllers' measurements— The m controllers' measurements (of course, after Alice's Bell measurements) make the component state for $\mathrm{A'}_n\mathrm{A}_n\mathrm{B}_n\mathrm{C}_1...\mathrm{C}_m$ in Eq. (2), with the controllers' state (6) in the present context, evolve into the state

$$\sum_{y=j_n\oplus x_n=0}^{1} (-1)^{x_n\cdot i_n} |B_{i_n,j_n}\rangle_{\mathrm{A'}_n\mathrm{A}_n} |y\rangle_{\mathrm{B}_n} |\widetilde{\kappa}(y)\rangle_{\mathrm{C}_1...\mathrm{C}_m}$$

with

$$|\widetilde{\kappa}(y)\rangle_{\mathrm{C}_1...\mathrm{C}_m} = \frac{1}{\sqrt{2^m}} \bigotimes_{s=1}^{m} \exp[i2\pi(\neg)^{r_s} y c_s/p] |r_s\rangle_{\mathrm{C}_s}.$$

The phase factor

$$\prod_s \exp[i2\pi(\neg)^{r_s} y c_s/p]$$

should be canceled by Bob before the normal recovery operation is performed in step (vii). The cancellation of the factor with probability one is possible if and only if all the controllers follow the protocol and at least k of them send c_s's to Bob (otherwise he will get an uncertain state as his operations become a guesswork). Since c_s's are classical keys of a (k,m) threshold scheme, k or more of them are necessary and sufficient to find out all of them. Bob can eliminate the phase by applying

$$\prod_s \mathrm{diag}[\exp(-i2\pi r_s c_s/p), \exp(-i2\pi\neg r_s c_s/p)] \qquad (7)$$

to his nth qubit B_n. This operation is unaffected by Alice's Bell measurement on $\mathrm{A'}_n\mathrm{A}_n$ as is clear from the initial state described in Eq. (2).

In this way, the (k,m)-threshold control is realized by using only qubit systems for individual portions. One may notice that it is a hybrid scheme in the sense that the (k,m) threshold is realized by a classical threshold scheme. Although classical keys are used, we claim that this scheme possesses a property thanks to a quantum control; the recovery operations are unfixed unless all the controllers make measurements, and the measurement bases are unknown to Bob. The measurements are not completely performed unless there are at least k $\mathrm{C}_{s,\mathrm{agree}}$'s and Bob sends at most $(m-k)$ solicits to $\mathrm{C}_{s,\mathrm{disagree}}$'s. Hence, in order to cheat under the protocol, Bob needs to collect c_s's, qubits, and measurement bases of at least k controllers.

The scheme has an advantage over the previously-introduced quantum scheme in the sense that it is secure against the possible schedule violation due to friendly controllers. Owing to step (IV), Bob has to wait for an official voting time to obtain Alice's original state unless the controllers violate the voting schedule all together.

4.3 Economization in Bob's Operations

We have shown an economized quantum (or hybrid) controlled quantum teleportation using the state (6) for the controllers' portion, in which the dimension of each distributed qudit has been reduced to two. As two is the minimal dimension for a nontrivial quantum system, it is optimized with respect to the dimension of a Hilbert space of each portion. Here we consider an economization of Bob's operations to eliminate the phase factor coming from controllers' measurements.

The number of Bob's single-qubit operations for the recovery is not important as far as a single EPR channel is under the controllers' control because Eq. (7) reduces to a single operation. It is, however, not negligible in case we extend the setup to the one illustrated in Fig. 2, in which we may have multiple shared states. Each controller is assigned to a single $\mathrm{A}_l\mathrm{B}_l$ pair and the total number of controllers is m.

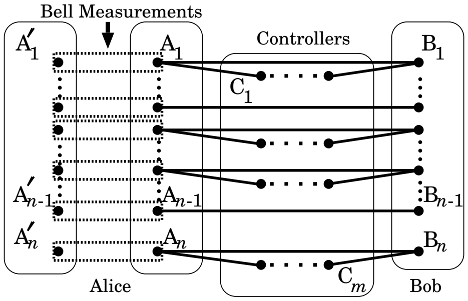

Figure 2: A straightforward extension of the system setup shown in Fig. 1, such that controllers are assigned to multiple channels. Each $\mathrm{A}_l\mathrm{B}_l$ pair is not necessarily under the supervision of controllers.

Let us use the same state as in Eq. (6), except the labels of controllers, for each of the controllers' portions (represented by dotted lines inside the square of "Controllers" in Fig. 2). We change the protocol for controllers in the following way.
(A) A controller who Agrees to allow Bob to recover the original state makes a measurement on her/his qubit in the basis $\{|\tilde{+}_s\rangle, |\tilde{-}_s\rangle\}$ with $|\tilde{\pm}_s\rangle = |\tilde{0}_s\rangle \pm |\tilde{1}_s\rangle$. She/he sends Bob the outcome $u_s \in \{\tilde{+}, \tilde{-}\}$ together with c_s.
(D) A controller who Disagrees does not make any action. However when a solicit is sent from Bob, a controller who Disagrees must make a measurement on her/his qubit in the basis $\{|\tilde{0}_s\rangle, |\tilde{1}_s\rangle\}$ and send Bob the outcome $v_s \in \{0, 1\}$.

To understand the effect of a measurement, let us decompose each component of the state (6) in the following way:

$$\begin{aligned}\frac{1}{\sqrt{2}}&[e^{i2\pi y c_s/p}|\tilde{0}_s\rangle + e^{i2\pi\neg y c_s/p}|\tilde{1}_s\rangle]\\ &= \frac{1}{2\sqrt{2}}\Big[(e^{i2\pi y c_s/p} + e^{i2\pi\neg y c_s/p})|\tilde{+}_s\rangle\\ &\qquad + (e^{i2\pi y c_s/p} - e^{i2\pi\neg y c_s/p})|\tilde{-}_s\rangle\Big].\end{aligned}$$

First consider the case (A).
(A-i) Suppose that the outcome of a measurement by the sth controller is $\tilde{+}$. Then, the unnormalized phase factor owing to this measurement is

$$e^{i2\pi y c_s/p} + e^{i2\pi\neg y c_s/p} = 1 + e^{i2\pi c_s/p},$$

which is a global phase uncorrelated with y. Thus Bob does not have to modify it.
(A-ii) Suppose that the outcome of a measurement by the sth controller is $\tilde{-}$. Then, the unnormalized phase factor owing to this measurement is $e^{i2\pi y c_s/p} - e^{i2\pi\neg y c_s/p}$, which can be regarded as

$$\begin{cases} \alpha & (y=0)\\ -\alpha & (y=1)\end{cases}$$

with $\alpha = 1 - e^{i2\pi c_s/p}$. Thus Bob can modify the factor by applying Z to some B_l for which the controller's qubit is originally connected in Fig. 2.

Second consider the case (D).
The phase factor due to the measurement, with the outcome $v_s \in \{0,1\}$, is $\exp[i2\pi(\neg)^{v_s} y c_s/p]$. This can be modified by applying

$$\mathrm{diag}[\exp(-i2\pi v_s c_s/p), \exp(-i2\pi\neg v_s c_s/p)]$$

to a proper B_l, which is possible if Bob knows c_s, namely, if k or more controllers follow (A).

In addition to the above recovery of the phase factors corresponding to controllers' measurements, Bob applies $Z^{i_l}X^{j_l}$ to each B_l, as usual, to recover the phase factors corresponding to Alice's Bell measurements.

Let us estimate the reduction in the number of operations that Bob has to apply to B_l's for eliminating the phase factors due to controllers' measurements. Let us consider the worst case where the m controllers are assigned to mutually different channels. In our previous protocol, the number of the operations is m. In the present protocol, it is, on average, $t/2 + (m-t) = m - t/2$ with t the number of controllers who agree to allow Bob to recover the original state. (Of course, Bob cannot recover the state when $t < k$.)

5 Operational Complexity

In the previous section, a quantum (or hybrid) (k, m)-threshold controlled quantum teleportation using qubits (without qudits whose dimension is more than two) has been constructed. We will count the number of single-qubit operations and that of two-qubit operations by following the whole process. Here, we consider the case where the controllers are attached to the nth EPR channel $\mathrm{A}_n\mathrm{B}_n$ and regard Bob's recovery operation corresponding to each controller's measurement as a single operation, for simplicity. The number of operations is unchanged by employing the setup illustrated in Fig. 2.

The process is the same as the original quantum teleportation [1] except for the measurements and operations acting on the shared state of $\mathrm{A}_n\mathrm{B}_n\mathrm{C}_1 ... \mathrm{C}_m$, as we have seen in Sec. 2.

For the part without controllers in Fig. 1, there are $(n-1)$ EPR pairs prepared between Alice and Bob. The quantum circuit for preparing the EPR states involves $(n-1)$ Hadamard gates and the same number of controlled-NOT (CNOT) gates. Alice makes $(n-1)$ Bell measurements between the system $\mathrm{A'}_1 ... \mathrm{A'}_{n-1}$ and the system $\mathrm{A}_1 ... \mathrm{A}_{n-1}$ and sends the outcomes (i_l, j_l) as classical information to Bob. Bob applies $2(n-1)$ single-qubit operations at most, namely, $\bigotimes_{l=1}^{n-1} Z^{i_l}X^{j_l}$, according to the classical information received from Alice.

For the portion of the shared state in the figure, the initial state

$$\frac{1}{\sqrt{2}}\sum_{y=0}^{1}|yy\rangle_{\mathrm{A}_n\mathrm{B}_n}|\kappa(y)\rangle_{\mathrm{C}_1...\mathrm{C}_m}$$

with $|\kappa(y)\rangle_{\mathrm{C}_1...\mathrm{C}_m}$ given by Eq. (6) should be prepared. It is prepared as follows. First we produce the state

$$\frac{1}{\sqrt{2}}\sum_{y=0}^{1}|yy\rangle_{\mathrm{A}_n\mathrm{B}_n} \otimes \bigotimes_{s=1}^{m}|\tilde{0}_s\rangle_{\mathrm{C}_s}.$$

This is easily prepared by a single Hadamard gate and a CNOT gate acting on $\mathrm{A}_n\mathrm{B}_n$. The state $|\tilde{0}_s\rangle_{\mathrm{C}_s}$ is a basis vector in the sth controller's favorite basis. Second, m Hadamard gates are applied to $\mathrm{C}_1 ... \mathrm{C}_m$ individually in their bases. In addition, the operation

$$\mathrm{diag}[1, \exp(i2\pi c_s/p), \exp(i2\pi c_s/p), 1]$$

is applied to $\mathrm{A}_n\mathrm{C}_s$ for all $s \in \{1, ..., m\}$ in the basis $\{|0\rangle, |1\rangle\}_{\mathrm{A}_n} \otimes \{|\tilde{0}_s\rangle, |\tilde{1}_s\rangle\}_{\mathrm{C}_s}$. The desired initial state for $\mathrm{A}_n\mathrm{B}_n\mathrm{C}_1 ... \mathrm{C}_m$ is now achieved. In the teleportation stage, Alice makes a Bell measurement on $\mathrm{A'}_n\mathrm{A}_n$ and sends Bob the outcome (i_n, j_n). The controllers and Bob follow the protocol as described in Sec. 4.2 or that in Sec. 4.3. In this process, Bob can eliminate the phase factors due to controllers' measurements if k or more controllers agree to allow Bob to obtain the original state. Finally, Bob applies $Z^{i_n}X^{j_n}$ to B_n. After all these steps, he obtains the original state of $\mathrm{A'}_1 ... \mathrm{A'}_n$ in $\mathrm{B}_1 ... \mathrm{B}_n$.

With the above description of the process, we find that the number of single-qubit operations and that of two-qubit operations for preparing the initial state of the whole system are $n + m$ for both operations. The teleportation process involves n Bell measurements performed by Alice and m single-qubit measurements performed by controllers. It also involves Bob's recovery operations: (i) at most $2n$ single-qubit operations corresponding to Alice's measurement outcomes; (ii) m single qubit operations [on average, $(m-t/2)$ single-qubit operations] corresponding to controllers' measurement outcomes when the protocol described in Sec. 4.2 is employed [when that in Sec. 4.3 is employed].

In addition, as we have mentioned in Sec. 4.3, the operations of (ii) reduce to a single operation in reality for the present setup while it does not for the setup of Fig. 2.

6 Discussions

We have proposed an economical scheme for a (k,m)-threshold control of a quantum teleportation. It uses a shared state of Alice, Bob, and controllers with the controllers' portion in the state of Eq. (6), which consists of qubits only. Thus a drawback of a usual polynomial coding, namely, the required dimension $d \geq p > m-1$ for each controller's qudit, has been resolved. In addition, it is straightforward to extend the scheme so that multiple qubits in Bob's portion are under the threshold control.

Our economical scheme can be seen as a hybrid of a standard (m,m)-threshold controlled quantum teleportation and a (k,m)-threshold classically-controlled quantum teleportation, as we have mentioned in Sec. 4.2. It should be noted that this has been realized by a nontrivial protocol using the state (6). The scheme has a good redundancy for the securement of the (k,m) threshold: (i) To modify the phase factors owing to controllers' measurements, k or more classical keys are required for Bob. (ii) To make disagreeing controllers perform measurements, at most $(m-k)$ solicits should be sent from Bob. In fact, the standard controlled teleportation in the context of (m,m) threshold can be used in the context of (k,m) threshold by stating only (ii) in its protocol. The advantage of our economical scheme over this simple extension is, thus, the redundant securement.

The scheme is, however, not as economical as a classically-controlled quantum teleportation, as we have discussed in Sec. 4.1. A quantum threshold-control scheme is certainly more expensive than a classical threshold-control scheme. It is thus recommended to assess the trade-off between the benefit and the economicalness to choose an appropriate scheme.

The benefit to distribute qudits (qubits in our scheme) among controllers is to make the recovery operation of Bob unfixed unless controllers make measurements. This makes the protocol robust against Bob's attack to the keys: In order for cheating, he needs both physical accesses to at least k controllers' qudits and information on their measurement bases. One may however claim that careless controllers tend to lose both of them at once in a real world. Our economical scheme possesses a clearer advantage also: it can prevent a violation of a voting schedule, i.e. it can prevent Bob from recovering the original state before an official voting time, unless controllers violate the schedule all together.

There is one drawback in our protocol. In case we use the scheme of Sec. 3, controllers who disagree to the teleportation do not have to measure their systems. In contrast, in our economical protocol, a disagreeing controller has to measure her/his qubit if a solicit is sent from Bob. Our protocol can be broken by a controller who does not follow this regulation. It seems an important drawback at a glance, but there is a quick solution: one can easily find out which controller cheats in the protocol. Any controller who does not send a measurement outcome despite a solicit sent from noncheating Bob is a cheater.

A clever cheater, however, may report an opposite measurement outcome and/or a wrong key instead of being quiet. It has been well-known that a basic secret sharing is not robust against dishonest participants who report wrong keys. There have been several proposals to remedy this drawback in classical secret sharing schemes [43, 44, 45, 46]. These classical schemes are easily combined into our scheme in order to find cheating in the keys c_s, as is clear from the protocol. Nevertheless, a protocol to find cheaters sending wrong messages as measurement outcomes should be newly constructed. One way to achieve this task is to add a supercontroller who grasps controllers' states by entangling her/his systems and their corresponding systems. Let the supercontroller know their measurement bases. Then the supercontroller can check the measurement outcomes afterward. It is hoped that a more sophisticated way will be developed.

Finally, we discuss a well-known strategy to use controlled quantum teleportation as a secret sharing to hide a quantum state as a secret [7]. Any (k,m)-threshold controlled quantum teleportation in the stage after Alice's Bell measurements is regarded as a (k,m)-threshold quantum secret sharing: Alice's original state to be recovered in Bob's side is regarded as a secret and the controllers are regarded as participants sharing the secret. A drawback of this approach is that the original state is recovered in the system of Bob's side; participants who try to cooperate for recovery should gather at this side or ask a dealer for proxy.

A solution to avoid this drawback is to construct m initially identical copies of the entire system K for the (k,m)-threshold controlled quantum teleportation, where $\mathrm{K} = \mathrm{A'}_1\mathrm{A}_1 ... \mathrm{A'}_n\mathrm{A}_n\mathrm{B}_1 ... \mathrm{B}_n\mathrm{C}_1 ... \mathrm{C}_m$. Let us write a copy as $\mathrm{K}^u = \mathrm{A'}^u_1\mathrm{A}^u_1 ... \mathrm{A'}^u_n\mathrm{A}^u_n\mathrm{B}^u_1 ... \mathrm{B}^u_n\mathrm{C}^u_1 ... \mathrm{C}^u_m$ with $u \in \{1,...,m\}$. We send the system $\mathrm{B}^v_1 ... \mathrm{B}^v_n$, together with classical information obtained by the Bell measurements on each of $\mathrm{A'}^v_1\mathrm{A}^v_1, ..., \mathrm{A'}^v_n\mathrm{A}^v_n$, to the vth participant ($v \in \{1,...,m\}$). The vth participant should also receive $\mathrm{C}^1_v, ..., \mathrm{C}^m_v$, namely the vth control systems of all K^u's. The vth participant can recover the original state in the system $\mathrm{B}^v_1 ... \mathrm{B}^v_n$ when she/he gets to know the measurement results on k or more among $\mathrm{C}^v_1, ..., \mathrm{C}^v_m$, including her/his own, and corresponding classical keys if they are used in the scheme.

This approach possesses the following benefit. The original quantum secret sharing is limited to $m < 2k-1$ due to the no-cloning theorem when an unknown quantum state is a secret [26]. A controlled quantum teleportation with a (k, m)-threshold control is not limited by the no-cloning theorem because the secret, namely, Alice's original state, is teleported to Bob's system. The approach is practical when we use classical keys for controlling a quantum teleportation. The resource required for this case is m classical keys and m copies of the system that consists of n EPR pairs and the n-qubit original state. Of course, the m copies of the system are reduced to one copy in case participants may gather in a particular place or may use a trusted dealer for proxy.

There seems to be no serious drawback of using classical control because the classical keys can be securely distributed and a scheduled vote is not interposed usually for a secret sharing. The robustness of our economical scheme is effective when an untrusted Bob exists. This is due to the fact that the measurement basis of each controller can be hidden. In this sense, our economical scheme might be used for a secret sharing to build in robustness against physical access attacks by malicious participants who try to cheat. Nevertheless, it is not attractive to spend many EPR pairs despite the reduction in the resource for controllers' portion. A choice of a proper scheme is dependent on the demand of participants when a controlled quantum teleportation is applied to a secret sharing.

We have discussed the advantage and disadvantage of our scheme in which the dimension of each controller's qudit is reduced to two. This reduction is indeed significant for physical realization of the threshold control of a quantum teleportation. Nevertheless, it is controversial as to which extent a controlled quantum teleportation should be performed with quantum resources. The answer depends on the application and as to which party is trusted, as is clear from the above discussions.

7 Summary

We have proposed an economical protocol for (k, m)-threshold controlled quantum teleportation. This protocol uses qubits distributed to controllers; hence we have achieved the reduction in the dimension of each qudit from a prime $p > m - 1$ to two. In addition, we have shown an economization in the number of Bob's recovery operations.

Acknowledgments

A.S. and M.N. are supported by "Open Research Center" Project for Private Universities: matching fund subsidy from MEXT. R.R. is supported by the Grant-in-Aid from JSPS (Grant No. 1907329). M.N. would like to thank a partial support of the Grant-in-Aid for Scientific Research from JSPS (Grant No. 19540422).

References

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", Phys. Rev. Lett., vol.70, pp.1895-1899, 1993.

[2] J. Gruska, Quantum Computing, McGraw-Hill, London, 1999.

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

[4] J. Zhou, G. Hou, S. Wu, and Y. Zhang, "Controlled Quantum Teleportation", LANL arXiv: quant-ph/0006030.

[5] N. B. An, "Teleportation of coherent-state superpositions within a network" Phys. Rev. A, vol.68, pp.022321-1-6, 2003.

[6] C.-P. Yang, S.-I. Chu, and S. Han, "Efficient many-party controlled teleportation of multiqubit quantum information via entanglement", Phys. Rev. A, vol.70, pp.022329-1-8, 2004.

[7] F. G. Deng, C.-Y. Li, Y.-S. Li, H.-Y. Zhou, and Y. Wang, "Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement", Phys. Rev. A, vol.72, pp.022338-1-8, 2005.

[8] Z.-X. Man, Y.-J. Xia, and N. B. An, "Economical and feasible controlled teleportation of an arbitrary unknown N-qubit entangled state", J. Phys. B: At. Mol. Opt. Phys., vol.40, pp.1767-1774, 2007.

[9] D. Kenigsberg and T. Mor, "Secure Controlled Teleportation", LANL arXiv: quant-ph/0609028.

[10] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography", J. Crypt., vol.5, pp.3-28, 1992.

[11] H.-K. Lo, X. Ma and K. Chen, "Decoy state quantum key distribution", Phys. Rev. Lett., vol.94, pp.230504-1-4, 2005.

[12] C. Marand and P. Townsend, "Quantum key distribution over distances as long as 30km", Opt. Lett., vol.20, pp.1695-1697, 1995.

[13] A. Muller, H. Zbinden, and N. Gisin, "Quantum cryptography over 23 km of installed under-lake telecom fibre", Europhys. Lett., vol.33, pp.335-339, 1996.

[14] T. Hasegawa, T. Nishioka, H. Ishizuka, J. Abe, K. Shimizu, M. Matsui and S. Takeuchi, "An Experimental Realization of Quantum Cryptosystem", IEICE Trans. Fund., vol.E85-A, no.1, pp.149-157, January 2002.

[15] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67km with a plug&play system", New J. Phys., vol.4, pp.41-1-8, 2002.

[16] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Free-space quantum key distribution with entangled photons", Appl. Phys. Lett., vol.89, pp.101122-1-3, 2006.

[17] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "Practical quantum key distribution over 60 hours at an optical fiber distance of 20km using weak and vacuum decoy pulses for enhanced security", Optics Express, vol.15, iss.13, pp.8465-8471, 2007.

[18] S. Bose, V. Vedral, and P. L. Knight, "Multiparticle generalization of entanglement swapping", Phys. Rev. A, vol.57, pp.822-829, 1998.

[19] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental Quantum Teleportation", Nature, vol.390, no.6660, pp.575-579, 1997.

[20] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, "Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual classical and Einstein-Podolsky-Rosen channels", Phys. Rev. Lett., vol.80, no.6, pp.1121-1125, 1998.

[21] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, "Long-Distance Teleportation of Qubits at Telecommunication Wavelengths", Nature, vol.421, no.6922, pp.509-513, 2003.

[22] G. R. Blakley, "Safeguarding cryptographic keys", in Proceedings of AFIPS 1979 National Computer Conference, New York, 1979, vol.48, pp.313-317, AFIPS Press, Arlington, Va., June 1979.

[23] A. Shamir, "How to Share a Secret", Commun. ACM, vol.22, no.11, pp.612-613, 1979.

[24] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On Secret Sharing Systems", IEEE Trans. Inf. Theory, vol.IT-29, no.1, pp.35-41, January 1983.

[25] S. C. Kothari, "Generalized linear threshold scheme", in Proceedings of Crypto'84, Santa Barbara, 1984, Edited by G. R. Blakley and D. Chaum, Springer-Verlag, New York, 1985, pp.231-241.

[26] R. Cleve, D. Gottesman, and H.-K. Lo, "How to Share a Quantum Secret", Phys. Rev. Lett., vol.83, pp.648-651, 1999.

[27] Z. Zhang, "Controlled teleportation of an arbitrary n-qubit quantum information using quantum secret sharing of classical message", Phys. Lett. A, vol.352, pp.55-58, 2006.

[28] Y. Murakami, M. Nakanishi, S. Yamashita, and K. Watanabe, "Cheater Identifiable Quantum Secret Sharing Schemes", IPSJ SIG Technical Reports, 2005-CSEC-30(47), pp.337-340, 2005.

[29] S. Iftene, "General Secret Sharing Based on the Chinese Remainder Theorem", Cryptology ePrint Archive: 2006/166, http://eprint.iacr.org/2006/166.

[30] H. Kunii and M. Tada, "A note on information rate for fast threshold schemes", in Proceedings of Computer Security Symposium 2006, Kyoto, Japan, October 2006, pp.101-106.

[31] J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "A fast (3,n)-threshold secret sharing scheme using exclusive-OR operations", IEICE Trans. Fund., vol.E91-A, no.1, pp.127-138, January 2008.

[32] G.-P. Guo and G.-C. Guo, "Quantum secret sharing without entanglement", Phys. Lett. A, vol.310, pp.247-251, 2003.

[33] Z.-J. Zhang and Z.-X. Man, "Many-agent controlled teleportation of multi-qubit quantum information", Phys. Lett. A, vol.341, pp.55-59, 2005.

[34] D. Markham and B. C. Sanders, "Graph states for quantum secret sharing", Phys. Rev. A, vol.78, pp.042309-1-17, 2008.

[35] C. Negrevergne, T. S. Mahesh, C. A. Ryan, M. Ditty, F. Cyr-Racine, W. Power, N. Boulant, T. Havel, D. G. Cory, and R. Laflamme, "Benchmarking Quantum Control Methods on a 12-Qubit System", Phys. Rev. Lett., vol.96, pp.170501-1-4, 2006.

[36] P. Lancaster and M. Tismenetsky, The Theory of Matrices, 2nd Ed., Academic Press, San Diego, 1985.

[37] S. Karlin, Total Positivity, Volume I, Stanford University Press, California, 1968.

[38] T. Ando, "Totally Positive Matrices", Linear Algebra Appl., vol.90, pp.165-219, 1987.

[39] T. Craven and G. Csordas, "A Sufficient Condition for Strict Total Positivity of a Matrix", Linear Multilinear Algebra, vol.45, pp.19-34, 1998.

[40] G. Pólya and G. Szegö, Problems and Theorems in Analysis, Volume II, Springer-Verlag, Berlin, 1976, 4th Ed.

[41] Proceedings of the symposium "Quantum Computation: Are the DiVincenzo Criteria Fulfilled in 2004?", Edited by M. Nakahara, S. Kanemitsu, M. M. Salomaa, and S. Takagi, published as "Physical Realizations of Quantum Computing", World Scientific, Singapore, 2006.

[42] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography”, Rev. Mod. Phys., vol.74, no.1, pp145-195, 2002.

[43] M. Tompa and H. Woll, “How to share a secret with cheaters”, J. Crypt., vol.1, pp.133-138, 1989.

[44] J. Rifà-Coma, “How to Avoid the Cheaters Succeeding in the Key Sharing Scheme”, Designs, Codes, and Crypt., vol.3, pp.221-228, 1993.

[45] R. S. Rees, D. R. Stinson, R. Wei, and G. H. J. van Rees, “An application of covering designs: determining the maximum consistent set of shares in a threshold scheme”, Ars Combin. vol.53, pp.225-247, 1999.

[46] R. Tso, Y. Miao, and E. Okamoto, “A new algorithm for searching a consistent set of shares in a threshold scheme with cheaters”, in Proceedings of the 6th Information Security and Cryptology Conference, Edited by J. I. Lim and D. H. Lee, Lecture Notes in Computer Science, vol.2971, pp.377-385, Springer-Verlag, Berlin, 2003.