Quantum secret sharing based on quantum error-correcting codes*

Zhang Zu-Rong(张祖荣)†, Liu Wei-Tao(刘伟涛), and Li Cheng-Zu(李承祖)

Department of Physics, School of Science, National University of Defense Technology, Changsha 410073, *China*

(Received 7 November 2010; revised manuscript received 27 December 2010)

Quantum secret sharing(QSS) is a procedure of sharing classical information or quantum information by using quantum states. This paper presents how to use a $[2k-1,1,k]$ quantum error-correcting code (QECC) to implement a quantum $(k,2k-1)$ threshold scheme. It also takes advantage of classical enhancement of the $[2k-1,1,k]$ QECC to establish a QSS scheme which can share classical information and quantum information simultaneously. Because information is encoded into QECC, these schemes can prevent intercept-resend attacks and be implemented on some noisy channels.

Keywords: quantum secret sharing, quantum error-correcting code, classically enhanced quantum error-correcting code

PACS: 03.67.Dd, 03.67.Pp **DOI:** 10.1088/1674-1056/20/5/050309

1. Introduction

Alice wants to send a secret to two users, Bob and Charlie, in such a way that the two users must collaborate to acquire the secret, whereas any one of them acquires nothing about the secret, whatever he does. In classical cryptography, this technique is termed secret sharing.[1] In 1979, this technique was generalized to a (k,n) threshold scheme.[2] In the (k,n) threshold scheme with $n \geq k$, a secret is divided into n shares, any k or more shares of which can combine to reconstruct the secret, but any $k-1$ or fewer shares of which does not contain any information about the secret.

Now, this idea has been generalized to a quantum scenario. In 1999, Hillery *et al.*[3] first proposed a scheme sharing classical messages and a scheme sharing an arbitrary secret quantum state by using GHZ states. Schemes sharing secrets (classical secrets or quantum secrets) by using quantum states have been termed quantum secret sharing (QSS),[3−5] which are quantum-mechanical version of classical secret sharing schemes. After this, Cleve *et al.*[4] defined a quantum (k, n) threshold scheme with $k \leq n$, in which a secret quantum state is divided into n shares and can only be perfectly reconstructed from any k or more shares. Cleve *et al.*[4] and Gottesman[5] also gave the following results about a (k,n) threshold scheme based on quantum mechanics. A (k,n) threshold scheme of classical secrets exists for every value of $n \geq k$, but a quantum (k,n) threshold scheme, which shares an unknown quantum state, only exists for $k \leq n < 2k$. If $n \geq 2k$, no quantum (k,n) threshold scheme exists, due to the 'no-cloning theorem'. In 2004, the QSS of Hillery *et al.* was generalized by Xiao *et al.* into an (n,n) scheme and was reformulated in simple mathematical terms.[6] Until now, many schemes have been proposed to realize QSS. Besides GHZ states,[3,6−8] single photons,[9−11] Bell-states[12−15] and W-states[16,17] are used to realize QSS. All these schemes either deal with QSS of classical messages[3,6,9−15] or deal with QSS of quantum information.[3,7,8,16,17]

In this paper, we will describe a quantum (k,n) threshold scheme based on a quantum error-correcting code (QECC). On the other hand, we exploit redundancy in QECC to encode classical information so that we can establish a QSS scheme sharing both classical information and quantum information at the same time. The paper is organized as follows. First, we give a brief introduction of QECCs and classically enhanced quantum-error-correcting codes (CQECCs) in Section 2. In Section 3, we give a concrete description on how to use a QECC to share quantum information. In Section 4, we demonstrate a scheme that shares classical information and quantum information simultaneously based on a CQECC. We discuss security and properties of our schemes in Section 5.

*Project supported by the National Natural Science Foundation of China (Grant No. 61072071).

†Corresponding author. E-mail: graceshuai@yahoo.com.cn

© 2011 Chinese Physical Society and IOP Publishing Ltd

2. The QECC and CQECC

In order to fight against decoherence in quantum computers and quantum communication systems, QECCs[18−21] were established. Since Shor proposed the first QECC,[18] research in this field has made rapid progress. Gottesman established the theory of stabilizer codes,[22,23] which told us that QECCs are simultaneous eigenspaces of a group S of commuting operators. The group S of commuting operators is called the stabilizer of the code and the code is called the stabilizer code. A code with a code distance d which encodes q logical qubits into n physical qubits, is described as an $[n, q, d]$ code. Encoding operations of the $[n, q, d]$ code consist of first appending $n-q$ ancilla states $|0\rangle^{\otimes(n-q)}$, then performing unitary operations on the q qubits and the $n-q$ ancilla states. Thus, the data are no longer stored in the q qubits, but spread out among n qubits, which makes it possible for the information to be recovered, even if some of them are affected by environment. For example, the Shor code[18] encodes the data of a qubit into nine qubits and its encoding operations consist of appending eight ancilla states $|0\rangle^{\otimes 8}$ followed by performing two C-NOT operations, three Hadamard operations and six C-NOT operations in turn. The Shor code's codewords are given as follows:

$$\begin{aligned} &|0\rangle \to |0_{\rm L}\rangle \\ \equiv\ &\frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}, \\ &|1\rangle \to |1_{\rm L}\rangle \\ \equiv\ &\frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}. \end{aligned}$$

Stabilizer of the $[n, q, d]$ code has $n-q$ generators. We can diagnose errors and then correct errors by measuring these $n-q$ generators. The $[n, q, d]$ code can correct $(d-1)/2$ arbitrary single qubit errors and $d-1$ qubits erasure errors. It can correct an error set ε if for all $E_{\rm a}, E_{\rm b} \in \varepsilon$, $E_{\rm a}^{+}E_{\rm b} \in S \cup (g_n - N(S))$, where $N(S)$ is the normalizer of the group S.[23]

The code space of the $[n, q, d]$ code is a 2^q-dimensional subspace of the full 2^n-dimensional Hilbert space. Generally, n is much larger than q. For example, the smallest code encoding a logical qubit and able to correct an arbitrary error on a single qubit must satisfy $n \geq 5$.[24] Therefore, the $[n, q, d]$ code is an overly redundant quantum code, so we can exploit that redundancy to encode classical information. Suppose our classical information contains c bits, with $c < n-q$. The codes that encode both quantum information and classical information are called CQECCs.[25] An $[n, q : c, d']$ CQECC is defined as a code that encodes q logical qubits and c classical bits into n physical qubits with a code distance d'. The stabilizer of CQECC is described by $(S_{\rm Q}, S_{\rm C})$, where $S_{\rm Q}$ is the quantum stabilizer and $S_{\rm C}$ is the classical stabilizer. The group $(S_{\rm Q}, S_{\rm C})$ is the same as the stabilizer S of the $[n, q, d]$ code. Our code word is denoted by $|\Psi\rangle$.

Theorem 1[25] The quantum stabilizer $S_{\rm Q}$ of the $[n, q : c, d']$ code is generated by $n-q-c$ elements. The classical stabilizer $S_{\rm C}$ of the $[n, q : c, d']$ code is generated by c elements, such that $\forall g_j \in S_{\rm Q}$

$$g_j |\Psi\rangle = |\Psi\rangle,$$

and

$$g_i' |\Psi\rangle = (-1)^{x_i} |\Psi\rangle,$$

where g_i' is the ith element of the generator set of $S_{\rm C}$ and x_i is the ith bit of the c classical bits. If the measured result of the ith generator of $S_{\rm C}$ is 1, then $x_i = 0$, if -1, then $x_i = 1$.

Theorem 1 tells us that an $[n, q : c, d']$ CQECC is simultaneous eigenspaces of the quantum stabilizer $S_{\rm Q}$. We can diagnose errors by measuring the generators of the quantum stabilizer $S_{\rm Q}$. The $[n, q : c, d']$ code can correct $(d'-1)/2$ arbitrary single qubit errors and $d'-1$ qubits erasure errors. It can correct an error set ε if for all $E_{\rm a}, E_{\rm b} \in \varepsilon$, $E_{\rm a}^{+}E_{\rm b} \in (S_{\rm Q}, S_{\rm C}) \cup (g_n - N(S_{\rm Q}))$. Let ε_1 be the error set which can be corrected by the $[n, q, d]$ QECC and let ε_2 be the error set which can be corrected by the $[n, q : c, d']$ CQECC. Obviously, $\varepsilon_2 \subset \varepsilon_1$. After encoding classical messages, the $[n, q : c, d']$ CQECC can correct less errors than the $[n, q, d]$ QECC. Therefore $d' \leq d$.

3. Sharing quantum information by using a QECC

In this section, we will present how to use a QECC to share a secret quantum state, so that we realize a quantum (k, n) threshold scheme.

In Ref. [4], Cleve *et al.* pointed out the relationship between QSS schemes and QECCs. Concretely, every QSS scheme is a QECC; but not all QECCs are QSS schemes. Cleve *et al.* gave a theorem as follows.

Theorem 2[4] If a $[2k-1, 1, k]$ code exists, a (k, n) threshold scheme exists for any $n < 2k$. For a pure state (k, n) scheme, $n = 2k-1$ and for a mixed state (k, n) scheme, $n < 2k-1$.

In Theorem 2, the pure state scheme encodes pure state secrets as pure states and the mixed state scheme encodes pure state secrets as mixed states.[4,5] The validity of the theory is obvious for a pure state $(k, 2k-1)$ scheme. The $[2k-1, 1, k]$ code spreads out the information of a qubit among $2k-1$ qubits. Of course, the $2k-1$ qubits together can extract the information. However, a code with the code distance k can correct any $k-1$ erasures, which means that we can compensate for the absence of any $k-1$ qubits and construct the secret in the absence of them. In other words, any k qubits are enough to recover the information. Thus a pure state $(k, 2k-1)$ scheme exists. A mixed state scheme can be realized by a pure state scheme along with discarding qubits. Therefore, for a mixed (k, n) threshold scheme, $n < 2k-1$.

Let us give a concrete description about a quantum $(k, 2k-1)$ threshold scheme based on the $[2k-1, 1, k]$ QECC. Suppose Alice wants to send an arbitrary quantum state $|\varphi\rangle$ in a qubit to $2k-1$ users at a distance in such a way that only any k or more users can infer the state $|\varphi\rangle$ by their mutual assistance. This goal can be achieved by following steps.

1) Alice performs a unitary operation U to encode $|\varphi\rangle$ into $2k-1$ physical qubits. In order to prevent eavesdropping and the dishonest guys among the $2k-1$ receivers from cheating, for example, their intercept-resend attacks, Alice also prepares a checking quantum state $|\varphi'\rangle$ and encodes $|\varphi'\rangle$ into another $2k-1$ physical qubits by performing a different unitary operation U'. We denote the code stabilizers of the information sequence and the checking sequence by S, S', respectively. Alice sends the two $2k-1$ physical qubits sequences to $2k-1$ receivers, so that each receiver has two qubits, respectively from two sequences. Of course, the larger the number of checking sequences is, the more secure our $(k, 2k-1)$ threshold scheme is.

2) After Alice makes certain that each of the $2k-1$ receivers has two qubits in hand, she announces the position of the checking sequence and her encoding operation U' on the checking quantum state $|\varphi'\rangle$ publicly.

3) According to Alice's announcement, the $2k-1$ receivers collaborate to measure generators of the code stabilizer S' to diagnose errors on the checking sequence. If the error rate is high, the process is abandoned. Otherwise the process continues.

4) If the error rate is low, Alice announces the unitary operation U on the quantum state $|\varphi\rangle$ publicly.

5) According to Alice's encoding operation, the $2k-1$ receivers measure generators of the stabilizer S jointly in order to correct errors resulting from noisy channel. Note that the receivers can correct any set of errors $\{E_i\}$ if $E_{\rm a}^{+}E_{\rm b} \in S \cup (g_{2k-1} - N(S))$, $\forall E_{\rm a}, E_{\rm b}$.

6) After assuring that no error happened during transmitting from Alice to the $2k-1$ receivers, arbitrary k receivers of the $2k-1$ receivers combine to reconstruct the code state in the absence of the other $k-1$ receivers. Concretely, the k receivers fill the other $k-1$ qubits with standard states, such as $|0\rangle$s and then collaborate to measure the generators of the code stabilizer S to diagnose which type of error this filling will result in. The k receivers perform error-correcting operation to recover the code state and then decode the state $|\varphi\rangle$.

So far, we have explained in detail how to use a $[2k-1, 1, k]$ QECC to realize a quantum $(k, 2k-1)$ threshold scheme.

4. Sharing classical information and quantum information simultaneously based on a CQECC

In this section, we will present a QSS scheme that can share both a classical message and an unknown quantum state simultaneously.

The $[2k-1, 1, k]$ code encodes a logic qubit into $2k-1$ physical qubit and the code space is a 2-dimensional subspace of the full 2^{2k-1}-dimensional Hilbert space. The stabilizer S of the code is generated by $2k-2$ elements. Our encoding operation for the $[2k-1, 1, k]$ code imports $2k-2$ redundant qubits. We can exploit some of these $2k-2$ redundant qubits to encode a c-bit classical message, with $c < 2k-2$. Our c-bit classical message is denoted by $\{x_i\}$, where $x_i \in \{0,1\}$ and $i = 0, 1, \ldots, c$. The $[2k-1, 1, k]$ code encoding c-bit classical information is described as a $[2k-1, 1 : c, k']$ CQECC, which is classical enhancement of the $[2k-1, 1, k]$ QECC. The value of the code distance k' depends on the number of the classical bits. Because of encoding the classical information additionally, the code distance of this CQECC decreases if it is compared with its corresponding QECC, i.e. $k' \leq k$. The $[2k-1, 1 : c, k']$ CQECC can correct $(k'-1)/2$ arbitrary single qubit errors and $k'-1$ erasure errors.

Now we use the $[2k-1, 1 : c, k']$ CQECC to complete a QSS scheme sharing c-bit classical information and a quantum state simultaneously. Suppose Alice wants to transmit a secret quantum state and a classical message to the $2k-1$ receivers in such a way that only any $2k-k'$ or more receivers can collaborate to retrieve the information, but fewer receivers acquire nothing about the information. She can achieve the goal as follows.

1) first Alice performs a unitary operation U to encode a state $|\varphi\rangle$ into $2k-1$ physical qubits sequence, then selects c physical qubits randomly from $2k-2$ ancillas of the sequence to encode the classical message $\{x_i\}$ by using operation $X^{x_1} \otimes X^{x_2} \otimes \cdots \otimes X^{x_c}$. Thus our encoded state is

$$|\Psi\rangle \equiv X^{x_1} \otimes X^{x_2} \cdots \otimes X^{x_3} U(|0\rangle^{\otimes(2k-2)} |\varphi\rangle).$$

At the same time, Alice also performs a unitary operation U' to encode a checking state $|\varphi'\rangle$ into another $2k-1$ physical qubits sequence.

2) Alice sends the two $2k-1$ physical qubits sequences to $2k-1$ receivers, each receiver has two qubits, each from one sequence.

3) After Alice makes certain that each of the $2k-1$ receivers has two qubits in hand, she announces her encoding operation U' on the checking state and the position of the checking sequence. The $2k-1$ receivers jointly measure the generators of the checking sequence stabilizer S' to determine the error rate. If the error rate is high, the process is cancelled. Otherwise the process continues.

4) If the error rate is low, Alice announces what her encoding operation U on the state $|\varphi\rangle$ is and which qubits the classical message is encoded on publicly, so that the receivers can obtain the quantum stabilizer $S_{\rm Q}$ and the classical stabilizer $S_{\rm C}$ of the $[2k-1, 1 : c, k']$ CQECC.

5) According to Alice's encoding operation, the $2k-1$ receivers collaborate to measure the generators of the code stabilizer $S_{\rm Q}$ to correct errors from noisy channel. They can correct an error set ε if $E_{\rm a}^{+} E_{\rm b} \in (S_{\rm Q}, S_{\rm C}) \cup (g_{2k-1} - N(S_{\rm Q}))$ for all $E_{\rm a}, E_{\rm b} \in \varepsilon$. After error recovery, the state that the receivers possess will be $\pm|\Psi\rangle$, where '–' results from some errors of $S_{\rm C}$.

6) After errors are corrected, we begin to implement a $(2k-k', 2k-1)$ QSS scheme of both the quantum information and the classical information, where $k' \leq k$. Because the $[2k-1, 1 : c, k']$ CQECC can correct fewer erasure errors than the $[2k-1, 1, k]$ QECC, more than k receivers are necessary to recover the code state. The scheme can be implemented as follows: any $2k-k'$ of the $2k-1$ receivers fill other $k'-1$ qubits with standard states and then they measure the generators of the quantum stabilizer $S_{\rm Q}$ so that they can correct the errors from the filling and recover the code state to $\pm|\Psi\rangle$.

7) The $2k-k'$ receivers measure the generator set of $S_{\rm C}$ on $\pm|\Psi\rangle$ to decode the classical message $\{x_i\}$, then perform the operation $X^{x_1} \otimes X^{x_2} \otimes \cdots \otimes X^{x_c}$ and U on $\pm|\Psi\rangle$ to decode the original qubit state $|\varphi\rangle$.

So far a QSS scheme has been established to realize simultaneous quantum information and classical information sharing.

5. Discussion

In this paper, we have presented a detailed procedure of sharing a secret quantum state based on a $[2k-1, 1, k]$ QECC. We have also taken advantage of a $[2k-1, 1 : c, k']$ CQECC, which is a unification of both quantum and classical coding theory,[25] to establish a QSS scheme which can share a secret quantum state and a classical message at the same time. In our schemes, we add a checking sequence to prevent eavesdroppers or the dishonest receivers from acquiring the secrets by their intercept- resend attacks. If Alice only sends the secret sequence, once all qubits were intercepted, the interceptors would gain the secrets after Alice announces her encoding operation publicly. However, if Alice adds the checking sequence and first announces her encoding operation on it, the interceptors' behaviour will import some errors into the checking sequence which can be detected when all the receivers measure the stabilizer generators of the checking sequence. According to the error rate, Alice decides whether she continues to announce her encoding operation on the secrets. Under these circumstances, even if all qubits encoding the secrets were intercepted, the interceptors would not acquire any information about the secrets because they did not know Alice's operation on the secrets.

On the other hand, because our quantum information and classical information are encoded on QECC, we can depend on properties of QECC to correct some errors from noisy channel, including errors on the classical information. After assuring no error happened during transmission, we implement the QSS schemes, which improves the success possibility of the schemes.

Thus the above schemes can be implemented on some particular noisy channels.

In our schemes, the secrets are shared by encoding and decoding operations. In 2003, Hsu[26] proposed a (2,2) threshold scheme in which Grover algorithm operation was used to encode and decode classical secret. Recently Hao *et al.*[27] proved that the Hsu-protocol is completely unsecure and proposed an improved protocol with large information capacity and better security. Compared with the improved Hsu-protocol, our schemes encode and decode both quantum secret and classical secret and are not limited to some encoding operations. If a concrete encoding operation is given, our schemes can be experimentally implemented. Of course, whether a (k, n) threshold scheme can be experimentally realized depends on the development of quantum information networks. Recently, some progress has been made in this direction,[28] which provides an experimental base for our schemes.

References

[1] Schneier B 1996 *Applied Cryptography* (New York: Wiley) p. 70

[2] Shamir A 1979 *Commun. ACM* **22** 612

[3] Hillery M, Buzk V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[4] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **82** 648

[5] Gottesman D 2000 *Phys. Rev.* A **61** 042311

[6] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev.* A 69 052307

[7] Wang C, Zhang Y and Jin G S 2010 *Sci. Chin.* Ser. G **53** 2064

[8] Hu M L, Qin M, Tao Y J and Tian D P 2008 *Chin. Phys.* B **17** 624

[9] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev.* A **71** 044301

[10] Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329

[11] Gao T, Yan F L and Li Y C 2009 *Sci. Chin.* Ser. G **52** 1191

[12] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162

[13] Zhang Z J and Man Z X 2005 *Phys. Rev.* A **72** 022303

[14] Chen P, Deng F G and Long G L 2006 *Chin. Phys.* **15** 2228

[15] Shi R H, Huang L S, Yang W and Zhong H 2010 *Sci. Chin.* Ser. G **53** 2238

[16] Wang Y H and Song H S 2009 *Chin. Sci. Bull.* **54** 2599

[17] Gu Y J, Ma L Z, Yu X M and Zhou B A 2008 *Chin. Phys.* B **17** 462

[18] Shor P W 1995 *Phys. Rev.* A **52** R2493

[19] Knill E and Laflamme R 1997 *Phys. Rev.* A **55** 900

[20] Steane A 1996 *Phys. Rev. Lett.* **77** 793

[21] Calderbank A R and Shor P W 1996 *Phys. Rev.* A **54** 1098

[22] Gottesman D 1998 *Phys. Rev.* A **57** 127

[23] Gottesman D *Stabilizer Codes and Quantum Error Correction* (Ph. D. thesis) California Institute of Technology

[24] Nielsen M A and Chuang I L 2003 *Quantum Computation and Quantum Information* (Bejing: Higher Education Press) p. 445

[25] Kremsky I, Hsieh M H and Brun T A 2008 *Phys. Rev.* A **78** 012341

[26] Hsu L Y 2003 *Phys. Rev.* A **68** 022306

[27] Hao L, Li J L and Long G L 2010 *Sci. Chin.* Ser. G **53** 491

[28] Xu F X, Chen W, Wang S, Yin Z Q, Zhang Y, Liu Y, Zhou Z, Zhao Y B, Li H W, Liu D, Han Z F and Guo G C 2009 *Chin. Sci. Bull.* **54** 2991