Three-party *d*-level quantum secret sharing protocol

2008 J. Phys. A: Math. Theor. 41 255309

(http://iopscience.iop.org/1751-8121/41/25/255309)

J. Phys. A: Math. Theor. **41** (2008) 255309 (6pp) doi:10.1088/1751-8113/41/25/255309

Three-party *d*-level quantum secret sharing protocol

Dong Pyo Chi[1], **Jeong Woon Choi**[1], **Jeong San Kim**[2], **Taewan Kim**[1] **and Soojoon Lee**[3]

[1] Department of Mathematical Sciences, Seoul National University, Seoul 151-747, Korea
[2] Institute for Quantum Information Science, University of Calgary, Alberta T2N 1N4, Canada
[3] Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, Seoul 130-701, Korea

E-mail: dpchi@math.snu.ac.kr, cju@snu.ac.kr, jkim@qis.ucalgary.ca, april02@snu.ac.kr and level@khu.ac.kr

Received 16 January 2008, in final form 22 April 2008
Published 5 June 2008
Online at stacks.iop.org/JPhysA/41/255309

Abstract

We present a three-party quantum secret sharing protocol on arbitrary dimensional quantum systems, and derive mutually unbiased bases on three-qudit systems, which can guarantee the security of our protocol. In addition to the security, we show that our protocol is more efficient than any previous protocols since the number of discarding entangled states is minimized by controlling the sender's measurements according to other members' measurements, and also show that other members have no information about the sender's private key until knowing the hidden value.

PACS numbers: 03.67.Hk, 03.67.Dd

1. Introduction

In classical secret sharing [1, 2], one party, say Alice, wants to send her message to the other parties (Bob and Charlie) at a distance. However, Alice suspects that one of the others may be dishonest, and she does not know who is the dishonest one. She tries to divide the secret message into two pieces and give the proper relation between them so that Bob and Charlie can decode the message only if they cooperate in the same place.

Hillery *et al* [3] first proposed a quantum secret sharing scheme with a tripartite entangled state called the Greenberger–Horne–Zeilinger (GHZ) state [4], which was generalized into quantum secret sharing (QSS) protocols on any higher dimensional systems using a N-party N-level singlet state of total spin zero [5]. However, the protocols still have the restriction that the number of participants should be the same as the dimension of each particle.

In this paper we construct a QSS protocol which does not have such a limit, and which contains a hidden value controlling the correlation among outcomes of three parties. Moreover, we show that our protocol based on GHZ-like states can be more efficient than any previous

QSS protocols by allowing Alice to manage and to rotate the states locally according to the measurement directions of Bob and Charlie.

Most of quantum cryptographic protocols assure that a malicious eavesdropper cannot get the exact information about a private key and can be detected with a specific probability when she measures a given state in the wrong direction. Thus, in order for QSS protocols to be secure, Eve's wrong measurement should give rise to uncertainty as much as possible. On this account, two mutually unbiased basis (MUB) measurements [6–8] on d-dimensional quantum systems play an important role in our protocol.

In section 2 we consider the generalized Pauli operators acting on d-dimensional systems, and derive MUBs and the GHZ-like states. We provide our QSS protocol based on the GHZ-like states in section 3, and analyze the security of the protocol for two cases of attacks in section 4, where one is an eavesdropping by Eve, and the other is the intercept-and-resend attack by a dishonest person. We finally summarize our results in section 5.

2. GHZ-like states on d-dimensional quantum systems

In this section, we derive two MUBs and GHZ-like states on d-dimensional quantum systems, and investigate their properties related with the security of our protocol. First, we consider the generalized Pauli operators [9–11] acting on d-dimensional Hilbert space:

$$\tilde{X} = \sum_{j=0}^{d-1} |j+1\rangle\langle j|, \qquad \tilde{Z} = \sum_{j=0}^{d-1} \omega^j |j\rangle\langle j|, \tag{1}$$

$$\tilde{Y} = \tilde{X}\tilde{Z} = \sum_{j=0}^{d-1} \omega^j |j+1\rangle\langle j|, \tag{2}$$

where $\omega = \mathrm{e}^{2\pi i/d}$ is a primitive dth root of unity. Let

$$|k_x\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{-kj} |j\rangle. \tag{3}$$

Then $|k_x\rangle$ is an eigenstate of $\tilde{X}$ with eigenvalue ω^k. Let

$$|k_y\rangle = \begin{cases} \dfrac{1}{\sqrt{d}} \displaystyle\sum_{j=0}^{d-1} \omega^{\frac{j^2-2kj-j}{2}} |j\rangle & \text{if } d \text{ is odd,} \\ \dfrac{1}{\sqrt{d}} \displaystyle\sum_{j=0}^{d-1} \omega^{\frac{j^2-2kj-2j}{2}} |j\rangle & \text{if } d \text{ is even.} \end{cases} \tag{4}$$

Then $|k_y\rangle$ is an eigenstate of $\tilde{Y}$ with eigenvalue ω^k if d is odd and with eigenvalue $\omega^k\sqrt{w}$ if d is even.

For each d, the set of eigenstates $\{|k_x\rangle : k \in \mathbb{Z}_d\}$ of $\tilde{X}$ forms an orthonormal basis for a d-dimensional quantum system, and so does $\{|k_y\rangle : k \in \mathbb{Z}_d\}$ of $\tilde{Y}$. Furthermore, they are mutually unbiased to each other, that is, for any $k, k' \in \mathbb{Z}_d$

$$|\langle k_x | k'_y \rangle| = \frac{1}{\sqrt{d}}.$$

In our protocol, two MUB measurements, $X = \{|k_x\rangle\langle k_x| : k \in \mathbb{Z}_d\}$ and $Y = \{|k_y\rangle\langle k_y| : k \in \mathbb{Z}_d\}$, are alternatively used.

Let us construct a three-party entangled state

$$|\Psi(\alpha)\rangle_{XYY} = \frac{1}{d} \sum_{s+t+u=\alpha \pmod d} |s_x\rangle|t_y\rangle|u_y\rangle, \tag{5}$$

where $\alpha \in \mathbb{Z}_d$. Then we can readily obtain

$$|\Psi(\alpha)\rangle_{XYY} = \begin{cases} \dfrac{1}{\sqrt{d}} \displaystyle\sum_{j=0}^{d-1} \omega^{j(j-1-\alpha)} |jjj\rangle & \text{if } d \text{ is odd,} \\ \dfrac{1}{\sqrt{d}} \displaystyle\sum_{j=0}^{d-1} \omega^{j(j-2-\alpha)} |jjj\rangle & \text{if } d \text{ is even.} \end{cases} \tag{6}$$

Similarly we can derive an entangled state $|\Psi(\alpha)\rangle_{XXX}$ as follows:

$$\begin{aligned} |\Psi(\alpha)\rangle_{XXX} &= \frac{1}{d} \sum_{s+t+u=\alpha \pmod d} |s_x\rangle|t_x\rangle|u_x\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{-j\alpha} |jjj\rangle. \end{aligned} \tag{7}$$

It is easy to check that $|\Psi(1)\rangle_{XYY}$ and $|\Psi(0)\rangle_{XXX}$ are the same for $d = 2$, and furthermore both $|\Psi(\alpha)\rangle_{XYY}$ and $|\Psi(\alpha)\rangle_{XXX}$ are essentially equivalent to the standard d-dimensional GHZ state up to local unitary operations. In particular, it follows from equations (6) and (7) that

$$\begin{aligned} |\Psi(\alpha)\rangle_{XYY} &= (U \otimes I \otimes I)|\Psi(\alpha)\rangle_{XXX} \\ &= \frac{1}{d} \sum_{s+t+u=\alpha \pmod d} U|s_x\rangle|t_x\rangle|u_x\rangle, \end{aligned} \tag{8}$$

where

$$U = \begin{cases} \displaystyle\sum_{j=0}^{d-1} \omega^{j(j-1)} |j\rangle\langle j| & \text{if } d \text{ is odd,} \\ \displaystyle\sum_{j=0}^{d-1} \omega^{j(j-2)} |j\rangle\langle j| & \text{if } d \text{ is even.} \end{cases} \tag{9}$$

From this point of view, we call these states the *GHZ-like* states.

We now show that $|\Psi(\alpha)\rangle_{XYY}$ is the uniquely determined common eigenstate of XYY, YXY and YYX with respect to eigenvalue ω^α if d is odd ($\omega^{\alpha+1}$ if d is even). Let d be odd and assume that an arbitrary 3-qudit pure state $|\phi\rangle = \sum_{j,k,l} a_{jkl}|jkl\rangle$ satisfies

$$XYY|\phi\rangle = YXY|\phi\rangle = YYX|\phi\rangle = \omega^\alpha|\phi\rangle. \tag{10}$$

It follows from straightforward calculations that

$$|\phi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{j(j-1-\alpha)} |jjj\rangle = |\Psi(\alpha)\rangle_{XYY}. \tag{11}$$

Similarly, if d is even, we also have

$$|\phi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{j(j-2-\alpha)} |jjj\rangle = |\Psi(\alpha)\rangle_{XYY}. \tag{12}$$

Moreover, we can see that $|\Psi(\alpha)\rangle_{XYY} = |\Psi(\alpha)\rangle_{YXY} = |\Psi(\alpha)\rangle_{YYX}$. Hence, if Alice, Bob and Charlie measure $|\Psi(\alpha)\rangle_{XYY}$ by XYY, YXY or YYX, then they obtain outcomes s, t and u satisfying that $s + t + u = \alpha \pmod d$, respectively.

Table 1. Alice's measurements corresponding to Bob's and Charlie's: U is the local unitary operation which transforms $|\Psi(\alpha)\rangle_{XXX}$ into $|\Psi(\alpha)\rangle_{XYY}$ in equation (9).

State	Bob	Charlie	Alice
$\|\Psi(\alpha)\rangle_{XYY}$	Y	Y	X
$\|\Psi(\alpha)\rangle_{XYY}$	Y	X	Y
$\|\Psi(\alpha)\rangle_{XYY}$	X	Y	Y
$\|\Psi(\alpha)\rangle_{XYY}$	X	X	$UXU^{\dagger}$

3. Our protocol

In QSS, Bob and Charlie obtain Alice's private key from the correlation of outcomes, given by measuring a three-party entangled quantum systems. In fact, Bob and Charlie can get Alice's information by a joint measurement such as Bell measurement if they are together at same place. This is the same situation as the quantum key distribution (QKD) like BB84 or EPR protocols [12, 13].

However, QSS protocol proceeds in the condition that they are far away from each other and measure their states locally. Non-locality and entanglement distributed between them are, after all, used to give a correlation between their classical outcomes by local measurements. Therefore, one of the most important problem in QSS is how Alice sends an entangled state to Bob and Charlie securely against eavesdropping by any exterior Eve and the intercept-and-resend attack by an interior dishonest person. In order to construct the QSS protocol satisfying the above conditions, we use two MUB measurements given in section 2.

(i) Alice prepares a GHZ-like state, $|\Psi(\alpha)\rangle_{XYY}$, and sends Bob and Charlie the last two particles, respectively. Alice repeats this step $2n$ times, and all participants store their particles in the order received.

(ii) Bob and Charlie publicly announce the fact that they have already received all $2n$ particles from Alice, and then they measure their own qudits after deciding one of measurement directions X and Y randomly.

(iii) Alice informs Bob and Charlie a randomly chosen $2n$ bit string $\mathbf{b}$, each entry of which is either 0 or 1. Then for ith particles corresponding to $\mathbf{b}_i = 1$ Alice requires Bob and Charlie to announce their measurement outcomes and directions in the order randomly determined as either [(1) Bob's outcome, (2) Charlie's outcome, (3) Charlie's direction, (4) Bob's direction] or [(1) Charlie's outcome, (2) Bob's outcome, (3) Bob's direction, (4) Charlie's direction].

(iv) Alice properly measures her ith particles corresponding to $\mathbf{b}_i = 1$ in the direction correlated with measurement of Bob and Charlie as in table 1.

(v) If Alice finds any error from all participants' measurement outcomes in step iv, then she aborts the protocol. Otherwise, they discard the particles for the test, and Alice lets Bob and Charlie announce their measurement directions for the particles left after the test.

(vi) Alice properly measures her particles in the direction perfectly correlated with measurement of Bob and Charlie as in table 1; this step tells us that since there is no loss of states except for particles discarding for the test, our protocol can be twice as efficient as the original QSS, on the average.

(vii) When Bob and Charlie collaborate to obtain Alice's information, Alice announces the hidden value α to Bob and Charlie. Then they can derive her private key string from the outcome correlation, $s + t + u = \alpha \pmod{d}$.

Here, Alice's private key s is determined by $t + u$ and the hidden value α. Thus, Bob and Charlie have no information about Alice's private key until knowing α.

We remark that it is possible to use a string consisting of different hidden values for GHZ-like states, instead of the fixed α, and also remark that only in the distribution and verification of desired quantum states, one needs to use different basis measurements, in other words, once they have verified that they have the desired states, the three participants only need to measure XYY for secret sharing [14].

4. Security

4.1. Eavesdropping by exterior Eve

In section 2, we have shown that $|\Psi(\alpha)\rangle_{XYY}$ is the unique pure three-party quantum state invariant under operators XYY, YXY and YYX simultaneously, with respect to an eigenvalue ω^{α} if d is odd ($\omega^{\alpha+1}$ if d is even).

This means that if

$$|\Psi\rangle = \sum_{j,k,l=0}^{d-1} a_{jkl}|jkl\rangle_{ABC}|R_{jkl}\rangle_{E} \tag{13}$$

successfully passes the test of our protocol then $|\Psi\rangle$ should be a product state

$$|\Psi\rangle = |\Psi(\alpha)\rangle_{XYY} \otimes |R\rangle_{E}. \tag{14}$$

In other words, after the test of our protocol, Eve is perfectly separated and the perfect correlation, $s + t + u = \alpha \pmod d$, is securely preserved among all participants. Therefore, our protocol is secure against any exterior Eve's eavesdropping.

4.2. Intercept-and-resend attack by interior dishonest party

In this section, we consider the case that one of receivers Bob and Charlie changes his mind and tries to obtain Alice's private key alone. Suppose a dishonest person (Bob) performs the intercept-and-resend attack on Charlie's particles.

First, Bob can intercept, measure by predicting the measurement direction of Charlie, and resend the collapsed state to him. If Bob and Charlie measure Charlie's original states in the same directions, then Bob can obtain the information about Alice's private key alone after knowing the hidden value α. Although Bob performs measurements in the directions different from Charlie, his attacks can be unexposed with probability $1/d$. Therefore, the exposed probability is not less than $1 - \left(\frac{d+1}{2d}\right)^n$ during the test procedure and we can find out that the higher dimensional system provides us with the better security for QSS protocol. This is due to the fact that the number of eigenspaces of measurement linearly increases as the dimension of system gets higher, and that it is also difficult for Bob to obtain the same result as Charlie's when n is sufficiently large.

We now assume that Bob possesses all states Alice sent and gives Charlie one sides of d-dimensional bipartite (maximally entangled) states. In step iii of our protocol, the measurement directions and outcomes of Bob and Charlie are alternately announced in a specific way. As in [15], this procedure prevents dishonest Bob from cheating the other members. Therefore, our protocol is also secure against intercept-and-resend attacks by an interior dishonest member.

We remark here that although this security analysis is not about unconditional security, its unconditional security could be proved by modifying the proof of unconditional security of the QKD and applying it to our protocol.

5. Conclusions

We have presented a 3-party d-level QSS protocol. To construct a QSS protocol on arbitrary d-dimensional quantum systems, we have derived MUBs on Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$, which guarantees the security of our protocol. Especially, with the explicit formula for the exposed probability, we have shown that the higher dimensional system assures the better security for QSS protocol.

In addition to the security, our protocol is more efficient than any other protocols since the number of discarding entangled states is minimized in our protocol by controlling Alice's measurements according to measurements of Bob and Charlie. Furthermore, in contrast to the previously known QSS protocols, Bob and Charlie have no information about Alice's private key until knowing the hidden value or string α, although a dishonest member is not detected in the middle of test.

Our protocol requires perfect GHZ-like states. Applying several techniques in [14] to our protocol, quantum sharing of classical secrets could be also possible in a noisy quantum channel.

Acknowledgments

DPC was supported by the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MOST) (no R01-2006-000-10698-0), JSK was supported by Alberta's informatics Circle of Research Excellence (iCORE) and SL was supported by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD, Basic Research Promotion Fund) (KRF-2007-331-C00049).

References

[1] Shamir A 1979 *Commun. ACM* **22** 612
[2] Blakley G R 1979 *Proc. of the National Computer Conf.* vol 48 p 313
[3] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[4] Greenberger D M, Horne M A and Zeilinger A 1989 *Bell's Theorem, Quantum Theory, and Conceptions of the Universe* ed M Kafatos (Dordrecht: Kluwer) p 69
[5] Cabello A 2002 *Phys. Rev. Lett.* **89** 100402
[6] Wootters W K and Fields B D 1989 *Ann. Phys.* **191** 363
[7] Barnum H 2002 *Preprint* quant-ph/0205155
[8] Klappenecker A and Roetteler M 2004 *Proc. 7th Int. Conf. on Finite Fields and Applications (Toulouse, 2003) (Lecture Notes in Computer Science* vol 2948*)* (Berlin: Springer) pp 137–44 (*Preprint* quant-ph/0309120)
[9] Patera J and Zassenhaus H 1988 *J. Math. Phys.* **29** 665
[10] Gottesman D, Kitaev A and Preskill J 2001 *Phys. Rev.* A **64** 012310
[11] Bartlett S D, de Guise H and Sanders B C 2002 *Phys. Rev.* A **65** 052316
[12] Bennett C H and Brassard G 1984 *Conf. on Computers, Systems and Signal Processing (Bangalore, India)* (New York: IEEE) p 175
[13] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[14] Chen K and Lo H K 2007 *Quantum Inf. Comput.* **7** 689
[15] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162