社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30（47）
2005／7／22

不正者を識別可能な量子秘密分散法

村上ユミコ[†,††]　中西　正樹[†]　山下　茂[†]　渡邊　勝正[†]

† 奈良先端科学技術大学院大学 情報科学研究科
奈良県生駒市高山町 8916-5
†† 科学技術振興機構 ERATO
E-mail: †{yumiko-m,m-naka,ger,watanabe}@is.naist.jp

あらまし　不正者を識別することのできる (k,n) 閾値量子秘密分散法を提案する。これは、不正者が高々t 人存在するとすると、$k \geqq 3t+1$ であれば、k 人以上の協力で誰が詐称行為を行っているか特定することができるものである。直交配列とスタビライザ符号を用いた、無条件安全な認証システムを利用しているのが特徴である。n と t の関係についても考察する。

キーワード　量子秘密分散法、量子認証、スタビライザ符号

Cheater Identifiable Quantum Secret Sharing Schemes

Yumiko MURAKAMI[†,††], Masaki NAKANISHI[†], Shigeru YAMASHITA[†], and Katsumasa WATANABE[†]

† Nara Institute of Science and Technology, graduate school of information scienece
8916-5,Takayama-cho, Ikoma, Nara
†† JST-ERATO
E-mail: †{yumiko-m,m-naka,ger,watanabe}@is.naist.jp

Abstract　In this paper, we show that there exists a cheater identifiable (k,n) threshold secret sharing scheme for a quantum secret. Suppose that there are at most t cheaters $(k \geqq 3t+1)$, k or more participants can identify who are cheating. Our scheme utilizes authentication codes based on an orthogonal array and stabilizer codes, which are unconditionally secure. Moreover, we discuss the relation between n and t.

Key words　quantum secret sharing, quantum authentication, stabilizer codes

1. Introduction

Suppose that the president of a bank needs to leave a significant information (e.g., the combination of a vault) with two vice presidents and he knows that one of them is dishonest, but does not know which is. He may well desire to distribute the secret to them such that no single person can read it, but two together can. How should he implement this? In classical cryptography, the answer is known as a secret sharing scheme. In 1979, Shamir [10] addressed a more generalized setting and showed how to construct schemes that divide a secret into n shares such that any subset of k or more shares can be reconstruct the secret and no subset of k or fewer cannot be obtain some information about the secret.

Such efficient threshold schemes can be very helpful in the management of cryptographic keys and in other applications which have a tradeoff between safety and convenience of management.

Recently, many researchers studied various quantum secret sharing schemes [2]～[4], [6]～[8]. Most of those proposals basically focus on the detection of eavesdropping or the efficiency in the use of quantum state [6]～[8].

From the aspect of fault tolerance, we focus on the cheater identifiability of the quantum secret sharing in this paper. In the classical setting, the cheater identifiable secret sharing scheme is proposed by Kurosawa et al. [9]. Basically, our scheme is based on thier scheme. Kurosawa's method successfully uses the message authentication based on an orthogonal array to identify which share is tampered, however, it is inconvenient to adapt to a quantum secret. Then, we interlock the quantum message authentication [1] which utilizes stabilizer codes [5], which is unconditionally secure.

Our scheme is a threshold scheme in which a secret is divided into n shares such that just k shares are enough to retrieve the secret and any subset of $k-1$ or fewer shares contain no information about the secret at all. This is called a k-out-of-n or (k,n) threshold secret sharing scheme. Some papers [2], [8] propose such a threshold scheme. In particular, Cleve et al. [2] showed the theorem that a stabilizer $[2k-1,1,k]$, if any, can be used as a $(k,2k-1)$ threshold scheme.

In this paper, we consider a threshold quantum secret sharing model in which there are at most t cheaters and show that there exists a t-cheater identifiable (k,n) threshold scheme, where $k \geqq 3t+1$, with high probability.

2. Cheater identifiable threshold secret sharing

2.1 Formulation

Informally, (k,n) threshold secret sharing schemes for quantum secret with cheaters are described as follows.

Threshold secret sharing

Let S be the set of quantum secrets. Dealer D produces n shares $(v_1,\ldots,v_n)$ on a given quantum secret in S and distributes them to n participants $P_1,\ldots,P_n$ respectively, such that any k or more shares can be used to retreive the secret, but any set of $k-1$ or fewer shares contains no information about the secret at all. We assume that (i) the dealer is honest, that is, if the shares produced by him are not tampered, any subset of more than k shares always reconstruct the original secret, and (ii) there are at most t cheaters in n participants and they may collude.

In other words, a t-cheater identifiable (k,n) threshold secret sharing scheme is summarized as follows.

-Completeness: Any set of participants containing at least k honest participants can reveal the original secret with high probability.

-Soundness: No subset of less than k participants can determine any partial information on the secret.

-Identifiability: There exists a Turing machine M which detects who are cheating with high probability if k or more participants open their shares.

Cheater identifiability

Suppose that $P_1,\ldots,P_t$ are cheaters without loss of generality and they open $\hat{v_1},\ldots,\hat{v_t}$. Successful cheating occurs if either one of the following two cases is satisfied;

(Case 1:) M cannot detect *who* are cheaters while the fact of cheating are detected, and the reconstruction of the secret fails.

(Case 2:) Participants reconstruct an incorrect secret from $(\hat{v_1},\ldots,\hat{v_t},v_{t+1},\ldots,v_m)$, where $m \geqq k$.

[Definition 1] We say that a (k,n) threshold secret sharing scheme is t-cheater identifiable if there exists a deterministic Turing machine which identifies t cheaters in any set of m $(\geqq k)$ participants, where the cheating fails with high probability.

2.2 Proposed scheme

Our scheme is outlined as follows. A dealer randomly chooses a secret sharing scheme, Q, for a quantum secret. He devides the secret into n shares by a quantum (k,n) threshold secret sharing scheme Q and then each share is authenticated by a quantum message authentication code (QMAC) in order to detect tampering. This is the quantization of the scheme proposed by Kurosawa et al. [9]. In [2], it is shown that a stabilizer code $[n,1,n-k+1]$, where $n<2(n-k+1)$, can be used as a threshold secret sharing scheme for a quantum secret. We use their scheme as Q. A stabilizer code can also be used as a QMAC [1]. Participants share additional secrets, the keys of QMACs and "which scheme is used as Q from a given set", which are classical information. The keys of QMACs are shared in the way that they are reconstructed by k or more participants even if they contains at most t cheaters. A linear code implements this. Q is shared by a classical (k,n) threshold secret sharing scheme, which identifies cheaters by the authentication based on an *orthogonal array*, as in [9]. Finding of Q needs at least k honest shares.

[Definition 2] An orthgonal array $OA(t+1,np,q)$ is a $q^{t+1} \times np$ array of q symbols such that, in any $t+1$ columns of the array, every one of the possible q^{t+1} ordered tuples of symbols occurs in exactly one row.

Let us start the concrete explanation of our scheme. Let $C=\{C_1,C_2,\ldots\}$ be a finite set of stabilizer codes $[n,1,n-k+1]$. The orthogonal array OA and the set C are publicly known. Let $|s_0\rangle$ be a quantum secret of single-qubit state. For each participant P_i, dealer D produces a share $\boldsymbol{v_i}=(|\boldsymbol{\alpha_i}\rangle, \boldsymbol{\beta_i}, \boldsymbol{\gamma_i}, \boldsymbol{\delta_i}, (\boldsymbol{g_{i,1}},\ldots,\boldsymbol{g_{i,n}}), (\boldsymbol{h_{i,1}},\ldots,\boldsymbol{h_{i,n}}))$ as follows. (Note that only ket-notation denotes a quantum data.)

(P1) D randomly chooses a stabilizer code C_{l_0} from C and encodes $|s_0\rangle$ to an n-qubit codeword $|\omega\rangle$ according to C_{l_0}.

(P2) As in Shamir's scheme, D chooses a $(k-1)$-th order random polynomial over $GF(p)$, where $p=|C|$ and p is a prime power:

$$F_1(x) = l_0 + a_{(1,1)}x + a_{(1,2)}x^2 + \cdots + a_{(1,k-1)}x^{k-1}.$$

Let $\beta_i = F_1(i)$ for $i = 1, \ldots, n$.

(P3) Let $OA(t+1, np, q)$ be an orthogonal array such that q is a prime power. D chooses a random number c, where $1 \leqq c \leqq q^{t+1}$. Let γ_i be the c-th row and the $(i-1)p + \beta_i$ th column element of $OA(t+1, np, q)$.

(P4) D chooses a t-th order random polynomial over $GF(q^{t+1})$:

$$F_2(x) = c + a_{(2,1)}x + a_{(2,2)}x^2 + \cdots + a_{(2,t)}x^t.$$

Let $\delta_i = F_2(i)$ for $i = 1, 2, \ldots, n$.

(P5) D randomly chooses n pairs $(C_{l_1}, e_1), \ldots, (C_{l_n}, e_n)$ such that C_{l_i} is a stabilizer code in C and e_i is an error in E_i, where E_i is the set of correctable errors of C_{l_i} and $|E_i|$ is a prime power. Without loss of generality, e_i can be substituted with a number, e.g., an error syndrome. For $j = 1, \ldots, n$, D chooses t-th order random polynomials G_j over $GF(p)$ and t-th order random polynomials H_j over $GF(|E_j|)$:

$$G_j(x) = l_j + a_{(l_j,1)}x + a_{(l_j,2)}x^2 + \cdots + a_{(l_j,t)}x^t.$$
$$H_j(x) = e_j + a_{(e_j,1)}x + a_{(e_j,2)}x^2 + \cdots + a_{(e_j,t)}x^t.$$

Let $g_{i,j} = G_j(i)$ and $h_{i,j} = H_j(i)$ for $i, j = 1, \ldots, n$.

(P6) Let $|s\rangle_i$ be the i-th qubit state of $|s\rangle$. D encodes $|s\rangle_i$ to an n-qubit codeword $|\alpha_i\rangle$ according to C_{l_i} with error syndrome e_i.

Put simply, v_i consists of the shares of the secret and the authenticators for it. $|\alpha_i\rangle$ is a share of the very secret, and authenticators of $|\alpha_i\rangle$ are reconstructed from $g_{i,j}$ and $h_{i,j}$. β_i is also a share of the secret in the sense that l_0, which can be retrieved from β_i's, is an immediate key to obtain the original secret. γ_i and δ_i are the authenticators of β_i.

[Theorem 1] The above scheme is a t-cheater identifiable (k, n) threshold secret sharing scheme for a quantum secret if $k \geqq 3t + 1$.

[Proof 1] Consider that $P_1, \ldots, P_m$ open their holding shares $v_1, \ldots, v_m$, where $m \geq k$. Without loss of generality, we suppose that $P_1, \ldots, P_t$ are cheaters and they open $\hat{v}_1, \ldots, \hat{v}_t$. We show that there exists a deterministic Turing machine M which detects who are cheaters on $\hat{v} = (\hat{v}_1, \ldots, \hat{v}_t, v_{t+1}, \ldots, v_m)$ which does not satisfy (P2),...,(P6). (Clearly, if $\hat{v}$ satisfies (P2),...,(P6), the original secret is reconstructed deterministically.)

Suppose that $\hat{v}$ does not satisfy (P5) or (P6). That is,

$$\exists i, j, \quad \hat{g}_{i,j} \neq G_j(i) \text{ or } \hat{h}_{i,j} \neq H_j(i).$$

$\{(G_j(1), \ldots, G_j(m))\}$ is a linear code with the Hamming distance $d = m - t$. In our case,

$$m \geqq k \geqq 3t + 1$$
$$\therefore d \geqq 2t + 1$$

There is a deterministic algorithm which identifies t or fewer errors (i.e., cheaters) in $\hat{g}_{1,j}, \ldots, \hat{g}_{m,j}$ and $\hat{h}_{1,j}, \ldots, \hat{h}_{m,j}$ for every j. Therefore, the algorithm recovers $G_j(x)$ and $H_j(x)$. Note that cheaters obtain no information about $G_j(x)$ and $H_j(x)$ at all, even if they collude. Once l_j and e_j is retrieved, the result of the error syndrome measurement on the disclosed $|\hat{\alpha}_i\rangle$ decides whether falsification occurs with high probability.

Suppose that $\hat{v}$ does not satisfy (P2), (P3), or (P4). By the same token, if $\hat{\delta}_i$ does not satisfy (P4), the falsification is detected deterministically. Once c is recovered, it is easy to detect which set of β_i and γ_i violates (P3) from the nature of orthogonal array. If it is confirmed that there is k or more β_i's which are not tampered, l_0 is reconstructed. It is obvious that the recovery of $F_1(x)$ needs at least k honest β_i's, and thus this quantum secret sharing is a (k, n) threshold scheme. □

Our scheme uses a stabilizer $[n, 1, K]$, where $K = n - k + 1$, to split a secret of single-qubit state into n shares. The code is tolerant of at most $K - 1 = n - k$ located errors, namely, just k shares are enough to correct the erasure errors and retrieve the original state, and $k - 1$ or fewer shares obtain no information about the secret at all [2]. In our case,

$$k \geqq 3t + 1$$
$$\Rightarrow n - K \geqq 3t$$

Here, let $K = an$ $(0 < a < 1)$.

$$\Rightarrow \frac{(1-a)}{3} n \geqq t \qquad (1)$$

If, in the model of cheater identifiable threshold quantum secret sharing, the upper bound of a number of cheaters becomes clear, equation (1) may give a lead for the relation between K and n on a stabilizer code $[n, 1, K]$. This is challenging and requires further investigation. Calculating the cheating success probability is also a future work.

Acknowledgement This work was supported in part by Grants-in-Aid for Scientific Research (no. 15700014 and no. 16092218).

References

[1] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, "Authentication of Quantum Messages," Proc. 43rd Annual IEEE Symposium on the Foundations of Computer Science, pp. 449-458, IEEE Press, 2002.

[2] R. Cleve, D. Gottesman, and H. L. Lo, "How to Share a Quamtum Secret," Phys. Rev. Lett., 83, 648, 1999.

[3] C. Crepeau, D. Gottesman, and A. Smith, "Secure Multiparty Quantum Computation," Proc. 34th Annual ACM

Symposium on Theory of computing, pp.643–652, 2002.

[4] C. Crepeau, D. Gottesman, and A. Smith, "Approximate Quantum Error-Correcting Codes and Secret Sharing Schemes," EUROCRYPT 2005, May, 2005.

[5] D. Gottesman, "Stabilizer Codes and Quantum Correction," quant-ph/9705052.

[6] G. P. Guo and G. C. Guo, "Quantum Secret Sharing without Entanglement," Phys. Lett. A, vol. 310/4, pp.247–251, 2003.

[7] M. Hillery, C. Buzek, and A. Berthiaume, "Quantum Secret Sharing," Phys. Rev. A., 59, 1829, 1999.

[8] A. Karlsson, M. Koashi, and N. Imoto, "Quantum Entanglement for Secret Sharing and Secret Splitting," Phys. Rev. A., 59, 162, 1999.

[9] K. Kurosawa, S. Obana, and W. Ogata, "t-Cheater Identifiable (k, n) Threshold Secret Sharing Schemes," Proc. of CRYPTO'95, LNCS, 963, pp.410–423, 1995.

[10] A. Shamir, "How to Share a Secret," Commun. ACM 22, 612, 1979.