Quantum secret sharing and quantum operations

Heling Xiao, Wangmei Guo and Xiao Wang

**State key Laboratory of Integrated Service Networks, Xidian University,
Xi'an, 710071, China**

Abstract

In this paper, we investigate the notion of quantum secret sharing (QSS) schemes based on quantum operations. We present the information theoretical model for QSS schemes using reversible operations and erase operations at first. We show that in pure state schemes, the recoverability requirement and the secrecy requirement are equivalent, which is regarded as a variant of no-cloning theorem. By establishing a relation between the quantum information quantity--coherent information and QSS schemes, the upper bound of quantum information rate is given. Finally, we propose a pure state threshold scheme with the form of quantum operations. The operations formalism of quantum secret sharing generalizes the theorey of QSS, and provides a unifying framework for the study of these schemes.

Keywords: *Quantum Secret Sharing, Quantum Operation, Quantum Information Theory, Information Security.*

1. Introduction

A secret sharing scheme [1] is a cryptographic protocol to distribute shares of a secret s among a set of participants $\mathcal{P}=\{P_1,...,P_n\}$, such that only authorized subsets of $\mathcal{P}$ are able to reconstruct the value of s. Subsets of $\mathcal{P}$ which cannot reconstruct the secret are called unauthorized sets. The connection of authorized sets, denoted by Γ ($\Gamma \subseteq 2^{\mathcal{P}}$), is called the access structure and the connection of unauthorized sets, denoted by $\mathcal{A}$ ($\mathcal{A} \subseteq 2^{\mathcal{P}} \backslash \Gamma$), is called the adversary structure.

Quantum secret sharing scheme is a secret sharing protocol based on quantum physics, and the security with the objective law of quantum physics. QSS was first introduced by Hillery, Buźek, and Berthiaume with three-particle and four-particle GHZ states [2]. Subsequently, the connection between QSS schemes and quantum error-correcting codes was made explicit in the work of Cleve et al. [3,4], and in greater depth by Rietjens et al. [5]. Since Imai et al. [6] defined the quantum information theoretical model of QSS schemes, a few of literature have succeeded in employing information theoretic tools, such as Holevo information [7], matroids [8,9], and entropic inequalities [10], for QSS schemes.

In this paper, we revisit QSS schemes in an information theoretical manner. We treat the authorized and unauthorized condition of QSS schemes as the reversible and erased condition for the corresponding quantum operation. A fundamental relation between the reversibility and erasability of quantum operations, and the coherent information is established.

This paper is organized as follows: in section 2, the definition of quantum operations formalism of QSS schemes is given, and show that recoverability requirement of pure state QSS schemes implies the secrecy one. In section 3, by using coherent information, we present a new proof that the lower bound dimension of each share in a QSS schemes. In section 5, we reformulate the $((k,n))$-threshold QSS scheme [3] for quantum operations formalism.

2. Operations formalism of QSS schemes

2.1 Definitions

Let $\mathcal{H}$ be finite dimensional Hilbert spaces, $\mathcal{B}(\mathcal{H})$ and $\mathcal{S}(\mathcal{H})$ be the totalities of density operators and linear operators on $\mathcal{H}$, respectively. Suppose a dealer, Alice, wants to share a quantum secret S with a set of players $\mathcal{P}=\{P_1,...,P_n\}$ according to a given access structure Γ. The quantum secret S is assumed to be an element of a q-dimension Hilbert space $\mathcal{H}_S$, where q usually is a prime power. The encryption/encoding operation of a QSS scheme is described as

$$O_{\mathcal{P}} : \mathcal{S}(\mathcal{H}_S) \to \mathcal{S}(\mathcal{H}_{P_1} \otimes ... \otimes \mathcal{H}_{P_n})$$

For any subset $X \subseteq \mathcal{P}$, let $\mathcal{H}_X = \otimes_{P_i \in X} \mathcal{H}_{P_i}$ be the Hilbert space that describes the shares of players in X. The map $O_X : \mathcal{S}(\mathcal{H}_S) \to \mathcal{S}(\mathcal{H}_X)$ is then denoted by $O_X = Tr_{\mathcal{P}\backslash X} O_{\mathcal{P}}$, where $Tr_{\mathcal{P}\backslash X}$ is the partial trace of the complement $\mathcal{P} \backslash X$.

Now the notion of the reversible operations and erase operations are defined. When we talk about reversing a quantum operation $\mathcal{E} : \mathcal{S}(L) \to \mathcal{S}(L')$, we generally do not mean that $\mathcal{E}$ can be reversed for all $\rho \in \mathcal{S}(L)$, but rather only that for $\forall \rho \in \mathcal{S}(M)$, $M \subseteq L$, there exist a deterministic quantum operation $\mathcal{R} : \mathcal{S}(L') \to \mathcal{S}(L)$ such

that $\mathcal{R}\circ\mathcal{E}(\rho)=\rho$. We say that a quantum operation $\mathcal{E}:\mathcal{S}(L)\to\mathcal{S}(L')$ is erased if there exists a density operator $\rho_0\in\mathcal{S}(L')$ such that $\mathcal{E}(\rho)=\rho_0$ for all ρ whose support lies in a subspace M of the total state space L.

2.2 QSS schemes

Definition 1: A QSS scheme realizing an access structure Γ is described by $O_{\mathcal{P}}:\mathcal{S}(\mathcal{H}_S)\to\mathcal{S}(\mathcal{H}_{\mathcal{P}})$ such that:

(1) Recoverability requirement: for all $X\in\Gamma$, we have that $O_X=Tr_{\mathcal{P}\setminus X}O_{\mathcal{P}}$ is reversible;

(2) Secrecy requirement: for all $Y\in\mathcal{A}$ ($\mathcal{A}\subseteq 2^{\mathcal{P}}\setminus\Gamma$), we have that $O_Y=Tr_{\mathcal{P}\setminus Y}O_{\mathcal{P}}$ is erased.

Remark: (1) If any set $X\subseteq\mathcal{P}$ is either a authorized set or a unauthorized set, i.e., $2^{\mathcal{P}}\setminus\Gamma=\mathcal{A}$, we call the scheme $O_{\mathcal{P}}$ as a perfect scheme. A QSS scheme $O_{\mathcal{P}}$ is called a non-perfect scheme if $\mathcal{A}\subset 2^{\mathcal{P}}\setminus\Gamma$, that is, there exists a set $X'\subset\mathcal{P}$ such that $X'\notin\Gamma$ and $X'\notin\mathcal{A}$. This paper focuses on perfect schemes only. (2) The access structure Γ of $O_{\mathcal{P}}$ satisfies the monotonicity, which means that the access structure Γ is upward-closed under inclusion, that is,

$$(X\subseteq N\subseteq\mathcal{P} \text{ and } X\in\Gamma)\Rightarrow N\in\Gamma$$

The operation $O_N:\mathcal{S}(\mathcal{H}_S)\to\mathcal{S}(\mathcal{H}_N)$ is then reversible. The adversary structure $\mathcal{A}$ of $O_{\mathcal{P}}$ satisfies the anti-monotonicity, which means that the adversary structure $\mathcal{A}$ is downward-closed under inclusion, that is,

$$(X\subseteq N\subseteq\mathcal{P} \text{ and } N\in\mathcal{A})\Rightarrow X\in\mathcal{A}$$

The operation O_X is then erased.

A quantum operation $\mathcal{E}$ is called a pure state operation if $\mathcal{E}(\rho)$ is a pure state for any pure state ρ. A QSS scheme $O_{\mathcal{P}}$ is called a pure state scheme if operation $O_{\mathcal{P}}:\mathcal{S}(\mathcal{H}_S)\to\mathcal{S}(\mathcal{H}_{\mathcal{P}})$ is a pure state operation. Otherwise, it is called a mixed state scheme. For pure state schemes, we have the following variant of no-cloning theorem.

Theorem 2 [6]: In a pure state QSS scheme $O_{\mathcal{P}}$, the recoverability requirement and the secrecy requirement are equivalent.

Proof: Suppose the QSS scheme $O_{\mathcal{P}=XY}:\mathcal{S}(\mathcal{H}_S)\to\mathcal{S}(\mathcal{H}_X\otimes\mathcal{H}_Y)$ realize an access structure Γ. Let $O_X=Tr_Y O_{XY}$, $O_Y=Tr_X O_{XY}$, and $X\in\Gamma$. By the Stinespring dilatation theorem, pure state operation $O_{XY}(\rho)$ can be represented as $O_{XY}(\rho)=U\rho U^{\dagger}$, where U is a unitary operator. Let $\{|i\rangle\}$ be an orthonormal basis on $\mathcal{H}_Y$. It follows from the fact that O_X is reversible, then $\forall i,j\in\{|i\rangle\}$ [12]

$$U^{\dagger}I_X\otimes|i\rangle\langle j|O_{XY}(\rho)I_X\otimes|j\rangle\langle i|U=c_{ij}^2\rho \quad (1)$$

where c_{ij} is a Hemitian matrix of complex numbers. We perform the local measurement described by the POVM $\{E_m\}$ on the state $O_Y(\rho)$ such that $\forall\rho\in\mathcal{S}(\mathcal{H}_S)$,

$$\begin{aligned} Tr(O_Y(\rho)E_m) &= Tr_{YX}(O_{XY}(\rho)(I_X\otimes E_m)) \\ &= Tr(U^{\dagger}O_{XY}(\rho)(I_X\otimes E_m)U) \\ &= Tr(\rho U^{\dagger}(I_X\otimes E_m)U) \\ &= c_m \end{aligned} \quad (2)$$

where the last equality follows from Eq.(1), and c_m is a constant depending on subscript m of measurement operators $\{E_m\}$. Therefore, there is no information about the input state ρ can be gained by performing arbitrary measurement on the state $O_Y(\rho)$. This is also implies that in a pure state QSS scheme $O_{\mathcal{P}}$ if O_X is reversible, then $O_{Y=\mathcal{P}\setminus X}$ is erased, which is a variant of no-cloning theorem.

Gottesman [4] showed that a mixed state QSS scheme can be described as a pure state scheme with one share discarded. Therefore, it actually suffices to only consider pure state schemes. In next section, we will establish a relation between the coherent information and pure state QSS schemes.

3. Coherent information and QSS schemes

Let A,B are two quantum system, and given a quantum operation $\varphi\in\mathcal{B}(\mathcal{H}_B)$ and a state $\rho\in\mathcal{S}(\mathcal{H}_B)$. The coherent information is defined as

$$I_c(\rho,\varphi)=S(\varphi(\rho))-S((I_A\otimes\varphi)\Phi_\rho) \quad (3)$$

where Φ_ρ is any purification of ρ into system AB, and $S(\rho,\varphi)\equiv S((I_A\otimes\varphi)\Phi_\rho)$ is the entropy exchange of the operation φ upon input of ρ. In fact, the entropy exchange $S(\rho,\varphi)$ may also be identified with the amount of entropy introduced by the operation φ into an environment C, initially in a pure state $|\phi\rangle\langle\phi|$. The reason is because from the Stinespring dilatation theorem, every quantum operation $\varphi\in\mathcal{B}(\mathcal{H}_B)$ can be represented as

$$\varphi(\rho)=Tr_{C'}(U_{BC}(\rho\otimes|\phi\rangle\langle\phi|)U_{BC}^{\dagger}) \quad (4)$$

where U_{BC} is a unitary acting on $\mathcal{H}_B\otimes\mathcal{H}_C$. The state on $\mathcal{H}_{A'}\otimes\mathcal{H}_{B'}\otimes\mathcal{H}_{C'}$ after the interaction is a pure state

$$|\omega\rangle\langle\omega|=I_A\otimes U_{BC}(\Phi_\rho\otimes|\phi\rangle\langle\phi|)I_A\otimes U_{BC}^{\dagger} \quad (5)$$

Let $\sigma=Tr_{A'B'}(|\omega\rangle\langle\omega|)$ be the state of environment C', and thus $S(\sigma)=S(\rho,\varphi)$. Particularly, if φ is a pure state operation, there is no interaction between the principal system AB and the environment C, i.e., φ is a unitary

operator. In this case, the entropy exchange $S(\rho,\varphi)$ equals zero.

With respect to the state $|\omega\rangle\langle\omega|$, we have $S(\rho)=S(Tr_{A'}(|\omega\rangle\langle\omega|))$, $S(\varphi(\rho))=S(Tr_{C'A'}(|\omega\rangle\langle\omega|))$, and $S(\sigma)=S(Tr_{B'A'}(|\omega\rangle\langle\omega|))$. Applying Araki-Lieb inequality [14], we get

$$0\le|S(\varphi(\rho))-S(\sigma)|\le S(\rho) \tag{6}$$

and in fact, $S(\varphi(\rho))-S(\sigma)=I_c(\rho,\varphi)$, so

$$0\le|I_c(\rho,\varphi)|\le S(\rho) \tag{7}$$

In [15] it was shown that there exists a quantum operation $\hat{\varphi}$ such that

$$(I_A\otimes\hat{\varphi}\varphi)\Phi_\rho=\Phi_\rho \tag{8}$$

if and only if the right-hand side of Eq. (7) holds, that is $I_c(\rho,\varphi)=S(\rho)$. On the other hand, when the left-hand side of Eq. (7) holds, that is $I_c(\rho,\varphi)=0$, which means that the entropy exchange is greater than the output entropy [16, 17]. Correspondingly, the noise introduced by the channel completely nullifies the input information. Thus, for any $\rho\in\mathcal{S}(\mathcal{H}_B)$, operation φ with the same output.

Theorem 3: Suppose a quantum secret sharing scheme $O_\mathcal{P}$ realize an access structure Γ,

(1) $\forall X\subseteq\mathcal{P}$, $X\in\Gamma$ iff $\forall\rho\in\mathcal{S}(\mathcal{H}_S)$, $I_c(\rho,O_X)=S(\rho)$.

(2) $\forall Y\subseteq\mathcal{P}$, $Y\in\mathcal{A}(\mathcal{A}=2^\mathcal{P}\backslash\Gamma)$ iff $\forall\rho\in\mathcal{S}(\mathcal{H}_S)$, $I_c(\rho,O_Y)=0$.

Proof: From [15], the necessity and sufficiency of the condition (1) is obvious. From [16, 17], we have that O_Y is erased with respect to $\mathcal{S}(\mathcal{H}_S)$ and $Y\in\mathcal{A}$ when $I_c(\rho,O_Y)=0$. On the other hand, if $Y\in\mathcal{A}$, then the quantum operation O_Y is erased with respect to $\mathcal{S}(\mathcal{H}_S)$, that is, $\forall\rho\in\mathcal{S}(\mathcal{H}_S)$, $O_Y(\rho)=\rho_0$, here $\rho_0\in\mathcal{S}(\mathcal{H}_Y)$. Therefore, there is no quantum information survives the transmission through the channel, i.e., $I_c(\rho,O_Y)=0$, this completes the proof.

The efficiency of quantum secret sharing schemes is quantified by its information rate, which is given by the following expression $r=\frac{S(\mathrm{S})}{\max_{X\in\mathcal{P}}S(X)}$. Smaller the rate, the sizes of the shares are larger and overhead costs of storage and communication. As the shares are to be kept secret, the security of the protocol can be undermined by large shares. For these reasons, it is beneficial to design schemes with high information rate. In the following proposition, we give the upper bound of quantum information rate.

Theorem 4: Suppose QSS scheme $O_\mathcal{P}$ realize an access structure Γ. The dimension of share of any participant $X\in\mathcal{P}$ must be at least as large as the dimension of the secret, and quantum information rate $r\le1$.

Proof: $O_\mathcal{P}$ is supposed to be a pure sate scheme without loss of generality. For any participant X, suppose we can choose a unauthorized set $Y\in\mathcal{A}(\mathcal{A}=2^\mathcal{P}\backslash\Gamma)$ such that $(Y\bigcup X)\in\Gamma$. From theorem 3, it holds that $I_c(\rho,O_Y)=0$ and $I_c(\rho,O_{XY})=S(\rho)$ for any $\rho\in\mathcal{S}(\mathcal{H}_S)$. Thus, we have

$$\begin{aligned}S(\rho)&=I_c(\rho,O_{XY})-I_c(\rho,O_Y)\\&=S(O_{XY}(\rho))-S(\rho,O_{XY})-S(O_Y(\rho))+S(\rho,O_Y)\\&\le S(O_X(\rho))-S(\rho,O_{XY})+S(\rho,O_Y)\end{aligned} \tag{9}$$

where the last inequality follows from the subadditivity of the von Neumann entropy. Let $Z=\mathcal{P}/(X\bigcup Y)$, then it follows from theorem 2 that the set Z is unauthorized, and $(X\bigcup Z)\in\Gamma$. Similarly to Eq. (9), we have

$$S(\rho)\le S(O_X(\rho))-S(\rho,O_{XZ})+S(\rho,O_Z) \tag{10}$$

Adding the Eq. (9) and Eq. (10) to obtain

$$\begin{aligned}S(\rho)\le S(O_X(\rho))+\frac{1}{2}(&-S(\rho,O_{XY})+S(\rho,O_Y)\\&-S(\rho,O_{XZ})+S(\rho,O_Z))\end{aligned} \tag{11}$$

Let Φ_ρ is any purification of ρ into system RS. It follows from the definition of pure state schemes that the state $(I_R\otimes O_{XYZ})\Phi_\rho$ is a pure state. Hence, we have $S(Tr_Y((I_R\otimes O_{XYZ})\Phi_\rho))=S(Tr_{XZ}((I_R\otimes O_{XYZ})\Phi_\rho))$, that is,

$$S(\rho,O_{XZ})=S(\rho,O_Y) \tag{12}$$

and $S(Tr_Z((I_R\otimes O_{XYZ})\Phi_\rho))=S(Tr_{XY}((I_R\otimes O_{XYZ})\Phi_\rho))$, that is,

$$S(\rho,O_{XY})=S(\rho,O_Z) \tag{13}$$

Substituting Eqs. (12) and (13) into Eq. (11) yields that

$$S(\rho)\le S(O_X(\rho)) \tag{14}$$

which implies that

$$r=\frac{S(\mathrm{S})}{\max_{X\in\mathcal{P}}S(X)}\le1 \tag{15}$$

4. Threshold QSS schemes

In this section, we revisit the $((k,2k-1))$ -threshold QSS scheme [3] in quantum operations form.

Definition 5: A QSS scheme $O_\mathcal{P}$ is called a $((k,n))$ -threshold scheme if the following conditions are fulfilled.

(1) $\forall X\subseteq\mathcal{P}$, O_X is erased iff $|X|<k$.

(2) $\forall X \subseteq \mathcal{P}$, O_X is reversible iff $|X| \geq k$.

We will construct a pure state QSS scheme $O_{\mathcal{P}}$ which maps a quantum state on $\mathcal{H}_S$ into a entangled state on the composite system $\mathcal{H}_{\mathcal{P}} = \otimes_{P_i \in \mathcal{P}} \mathcal{H}_{P_i}$. Pure state operation $O_{\mathcal{P}}$ is represented by a unitary operator $U: \mathcal{S}(\mathcal{H}_S) \to \mathcal{S}(\mathcal{H}_{\mathcal{P}})$, that is, for any $\rho \in \mathcal{S}(\mathcal{H}_S)$, $O_{\mathcal{P}}(\rho) = U\rho U^{\dagger}$. Let $\{|s\rangle\}_{s \in \mathbb{F}_q}$ be an orthonormal basis on $\mathcal{H}_S$, it suffices only consider the encoding operation $U|s\rangle$ of the basis $|s\rangle$. The principle of our QSS scheme $O_{\mathcal{P}}$ in detail as follows: Alice defines firstly a polynomial on $\mathbb{F}$ $p_c(x) = \sum_{i=1}^{k} c_i x^{i-1}$ specified by an arbitrary set $c = (c_1, ..., c_k) \in \mathbb{F}_q^k$. Then, she provides publicly revealed constants $x_1, ..., x_n \in \mathbb{F}_q$ ($|\mathbb{F}_q| \geq n$), and performs the following operation on the secret basis states $|s\rangle$:

$$U|s\rangle = \frac{1}{\sqrt{H}} \sum_{\substack{c \in F_q^k \\ c_1 = s}} |p_c(x_1), ..., p_c(x_n)\rangle \tag{16}$$

where H is a normalization constant. Finally, the output particles of n registers are assigned to the participants set $\mathcal{P}=\{P_1, ..., P_n\}$.

We now show that constructed as above QSS scheme $O_{\mathcal{P}}$ is feasible. For convenience, let us introduce the following notations for any $X = \{P_{i_1}, ..., P_{i_{|X|}}\} \subseteq \mathcal{P}$,

$$|p_c(X)\rangle = \left|p_c(x_{P_{i_1}}), ..., p_c(x_{P_{i_{|X|}}})\right\rangle = |(c_1, ..., c_k)V^k(X)\rangle \tag{17}$$

where $V^k(X) = \begin{pmatrix} 1 & \cdots & 1 \\ x_{P_{i_1}}^1 & \cdots & x_{P_{i_{|X|}}}^1 \\ \vdots & \vdots & \vdots \\ x_{P_{i_1}}^{k-1} & \cdots & x_{P_{i_{|X|}}}^{k-1} \end{pmatrix}$.

(1) Recoverability. In order to verify that any subset $X \subseteq \mathcal{P}$ is authorized set for $|X| \geq k$, it suffices to show that $|X| = k$, because of the monotonicity of the access structure. Let $X = \{P_{i_1}, ..., P_{i_k}\}$,

$$\begin{aligned} & O_X(|s\rangle\langle s|) \\ &= Tr_{\mathcal{P}\setminus X}(O_{\mathcal{P}}(|s\rangle\langle s|)) \\ &= \frac{1}{H} \sum_{\substack{c,c' \in F_q^k \\ c_1 = c_1' = s}} \langle p_{c'}(\mathcal{P}\setminus X)|p_c(\mathcal{P}\setminus X)\rangle \cdot |p_c(X)\rangle\langle p_{c'}(X)| \\ &= \frac{1}{H} \sum_{\substack{c,c' \in F_q^k \\ c_1 = c_1' = s}} \langle (s, ..., c_k')V^k(\mathcal{P}\setminus X)|(s, ..., c_k)V^k(\mathcal{P}\setminus X)\rangle \\ &\quad \cdot |p_c(X)\rangle\langle p_{c'}(X)| \\ &= \frac{1}{H} \sum_{c_1 = s} |p_c(X)\rangle\langle p_c(X)| \end{aligned} \tag{18}$$

where the fourth equality holds because when $(c_2, ..., c_k) \neq (c_2', ..., c_k')$ that $p_c(\mathcal{P}\setminus X) \neq p_{c'}(\mathcal{P}\setminus X)$ and $\langle p_c(\mathcal{P}\setminus X)|p_{c'}(\mathcal{P}\setminus X)\rangle = 0$. Furthermore, we can see the normalizing constant $H = q^{k-1}$. There exists a operation such that $\hat{O}_X = V^k(X)^{-1}$ (since $V^k(X)$ has full rank if $x_{P_{i_1}}, ..., x_{P_{i_k}}$ different from each other), then

$$\begin{aligned} & \hat{O}_X O_X(|s\rangle\langle s|)\hat{O}_X^{\dagger} \\ &= \frac{1}{H} \sum_{\substack{c \in F_q^k \\ c_1 = s}} |p_c(X)V^k(X)^{-1}\rangle\langle p_c(X)V^k(X)^{-1}| \\ &= \frac{1}{H} \sum_{c \setminus c_1 \in F_q^{k-1}} |s\rangle|c_2, ..., c_k\rangle\langle s|\langle c_2, ..., c_k| \\ &= |s\rangle\langle s| \otimes \frac{I}{q^{k-1}} \end{aligned} \tag{19}$$

Thus, we have recovered $|s\rangle$ from $O_{\mathcal{P}}|s\rangle$ by the local operation on X. In addition, from theorem 3, we have

$$\begin{aligned} & S(\frac{1}{q}\sum\nolimits_s |s\rangle\langle s|, O_X) \\ &= S(O_X(\frac{1}{q}\sum\nolimits_s |s\rangle\langle s|)) - S(\frac{1}{q}\sum\nolimits_s |s\rangle\langle s|) \\ &= k\log q - \log q \\ &= (k-1)\log q \end{aligned} \tag{20}$$

(2) Security. In order to verify that any subset $Y \subseteq \mathcal{P}$ is unauthorized set for $|Y| < k$, it suffices to show that $|Y| = k-1$, because of the anti-monotonicity of the adversary structure. Since O_{XY} is a pure state scheme, we naturally have

$$S(\frac{1}{q}\sum\nolimits_s |s\rangle\langle s|, O_Y) = S(\frac{1}{q}\sum\nolimits_s |s\rangle\langle s|, O_X) = (k-1)\log q \tag{21}$$

Let $Y = \{P_{i_1}, ..., P_{i_{k-1}}\} \subseteq \mathcal{P}$, then

$$\begin{aligned} O_Y(\frac{1}{q}\sum\nolimits_s |s\rangle\langle s|) &= Tr_{\mathcal{P}\setminus Y}(O_{\mathcal{P}}(\frac{1}{q}\sum\nolimits_s |s\rangle\langle s|)) \\ &= \frac{1}{qH} \sum\nolimits_s \sum_{\substack{c,c' \in F_q^k \\ c_1 = c_1' = s}} \langle p_{c'}(\mathcal{P}\setminus Y)|p_c(\mathcal{P}\setminus Y)\rangle \\ &\quad \cdot |p_c(Y)\rangle\langle p_{c'}(Y)| \\ &= \frac{1}{H} \sum_{c \in F_q^{k-1}} |p_c(Y)\rangle\langle p_c(Y)| = \frac{I}{q^{k-1}} \end{aligned} \tag{22}$$

where the third equality holds since, for any $s \in \mathbb{F}_q$ and $\{P_{i_1}, ..., P_{i_k}\} = \mathcal{P}\setminus Y$, there are q distinct $(c_1, c_2, ..., c_k)$ with

$c_1=s$ such that $p_c(x_{P_{ij}})=y_j$ for all $j=1,...,k$. Consequently, it holds that

$$I_c(\frac{1}{q}\sum_s |s\rangle\langle s|, O_Y)$$
$$= S(O_Y(\frac{1}{q}\sum_s |s\rangle\langle s|)) - S(\frac{1}{q}\sum_s |s\rangle\langle s|, O_Y) \quad (23)$$
$$= 0$$

Therefore it follows from theorem 3 that O_Y is erased.

5. Conclusion

In this paper, we treated the authorized sets and unauthorized sets of QSS schemes as the reversible operations and erase operations respectively. By establishing a fundamental relation between the reversibility and erasability of quantum operations and the quantum coherent information, we revisited the lower bound on the dimension of each share in QSS schemes and gave a rigorous proof by using coherent information. We have also revisited $((k,2k-1))$ -threshold scheme in [3] by using quantum operation. This model of QSS schemes in the form of quantum operation provides new insights into the theory of quantum secret sharing.

Acknowledgments

This work was supported by the National Science Foundation (NSF) under grant Nos 60832001, 60902080, 61271174, and State Key Laboratory of Integrates Service Network (ISN) under grant Nos (ISN 0208002, ISN 090307).

References

[1] A. Shamir. Communications of the ACM. vol. 22, pp612-613, 1979
[2] M. Hillery, V. Buzek, A.Berthiaume. Phys.Rev.A. vol. 59, 1829, 1999
[3] R. Cleve, D. Gottesman, H. K. Lo. Physical Review Letters. vol. 83, pp648-651, 1999
[4] D. Gottesman. Physical Review A. vol. 61, 042311, 2000
[5] H. Imai, J. Muller-Quade, A. C. A. Nascimento, P. Tuyls, A. Winter. Quantum Information and Computation. vol. 5, pp69-80, 2005
[6] K. Rietjens, B. Schoenmakers, P. Tuyls. Int. Symp. Information Theorey. Adelaide, Australia, pp1598-1602, 2005
[7] T. Ogawa, A. Sasaki, M. Iwamoto, H. Yamamoto. Physical Review A. vol. 72, 032318, 2005
[8] P. Sarvepalli. Physical Review A. vol. 83, 042303, 2011
[9] P. Sarvepalli, R. Raussendorf. Physical Review A. vol. 81, 052333, 2010
[10] P. Sarvepalli. Physical Review A. vol. 83, 042324, 2011
[11] E. Knill, R. Laflamme. Physical Review A. vol. 55, pp900-911, 1997
[12] J. Preskill. [online] Available: www.theory.caltech.edu/people/preskill/ph219, 2001
[13] B. Schumacher, M. A. Nielsen . Phys. Rev. A. vol. 54, pp2629-2635, 1996
[14] H. Araki, E. H. Lieb. Comm. Math. Phys. vol.18, pp160-170, 1970
[15] M. A. Nielsen, C. M. Caves, B. Schumacher and H. Barnum. Proceedings of the Royal Society of London Series a-Mathematical Physical and Engineering Sciences. vol. 454, pp277-304, 1998
[16] S. Lloyd. Physical Review A. vol. 55, pp1613-1622, 1997
[17] B. A. Grishanin V. N. Zadkov. Physical Review A. vol. 62, 032303, 2000

Heling Xiao Received the B.S. degree in Information Secure from Xidian University, Xi'an, China in 2007. Now she is a Master-Docter combined program graduate student in class of 2008. Her research interests are quantum secret sharing schemes and quantum secure communication.

Wangmei Guo Received the B.S. degree in Information Secure and the Dr. degree in Communication and Information System from Xidian University, Xi'an, China in 2006 and 2012 respectively. Her research interests are Convolutional network coding and Convolutional quantum coding.

Xiao Wang Received the B.S. degree in Communication Engineering and M.S. degree in Communication and Information System from Xidian University, Xi'an, China in 2008 and 2011 respectively, where he is currently working toward the Ph.D. degree in Communication and Information System.