Quantum secret sharing schemes and reversibility of quantum operations

Tomohiro Ogawa,[1,*] Akira Sasaki,[2,†] Mitsugu Iwamoto,[3,‡] and Hirosuke Yamamoto[4,§]
[1]*Graduate School of Information Science and Technology, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, 113-8656 Japan*
[2]*Sumitomo Mitsui Banking Corporation, 1–3–2, Marunouchi, Chiyoda-ku, Tokyo 100-0005 Japan*
[3]*Graduate School of Information Systems, University of Electro-Communications, 1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182-8585 Japan*
[4]*Graduate School of Frontier Sciences, University of Tokyo, 5-1-5 Kashiwanoha, Kashiwa-shi, Chiba, 277-8561 Japan*
(Received 30 April 2005; published 14 September 2005)

Quantum secret sharing schemes encrypting a quantum state into a multipartite entangled state are treated. The lower bound on the dimension of each share given by Gottesman [Phys. Rev. A **61**, 042311 (2000)] is revisited based on a relation between the reversibility of quantum operations and the Holevo information. We also propose a threshold ramp quantum secret sharing scheme and evaluate its coding efficiency.

DOI: 10.1103/PhysRevA.72.032318 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum secret sharing (QSS) schemes were studied by several authors [1–5] as quantum counterparts of classical secret sharing (SS) schemes [6,7]. QSS schemes are methods to encrypt an arbitrary quantum state or classical message into a multipartite entangled state among several quantum systems—namely, *shares*—in the following way: each of shares has no information about the original state or message while it can be reproduced by collecting several shares. QSS schemes can be classified into two categories based on what is encrypted—i.e., quantum states [3–5] or classical messages [1,2]. In this paper, we treat only the QSS schemes encrypting quantum states, which we call just QSS schemes for simplicity.

In the literature on QSS schemes in this sense, the (k,n)-*threshold QSS scheme* was proposed by Cleve *et al.* [3]. In the (k,n)-threshold QSS scheme, an arbitrary quantum state is encoded into n shares so that any k out of n shares can reproduce the original state while any $k-1$ or less shares have no information about it. Recently, experimental demonstrations [8,9] of the threshold scheme were reported. After the work of Cleve *et al.*, Gottesman [4] demonstrated that any *general access structure* consistent with the *monotonicity* [10] and the no cloning theorem [11–15] can be realized by a QSS scheme. The same result was shown by Smith [5] independently by using monotone span programs. Gottesman [4] also analyzed the coding efficiency of QSS schemes and showed that the dimension of each share must be the same or larger than that of the original system.

In this paper, we revisit the coding efficiency of QSS schemes in an information theoretical manner. First, we establish a relation between the *reversibility* of quantum operations and the Holevo information [16] in a general setting rather than QSS schemes. This relation is a natural extension of the idea in the classical information theory that the *sufficient statistic* is characterized by the preservation of the mutual information [17]. In classical statistical inferences, the sufficient statistic has several equivalent characterizations [18]: the existence of reverse channels, the preservation of information quantities such as the relative entropy, and the factorization theorem. On the other hand, the reversibility of quantum operations was studied by several authors [19–21] related to the quantum error correcting code [22,23], while it was also studied in terms of *sufficiency* in the field of the operator algebra [24–30] (see also Refs. [31,32]).

Recently, Petz and his colleagues [33,34] have established a theory of sufficiency in the quantum setting that is characterized by the reversibility of quantum operations (or coarse-grainings), the preservation of information quantities, and the quantum version [35,36] of the factorization theorem. Our characterization of the reversibility falls into a natural variant of theirs. However, we rather use the term reversibility in this paper for the reasons that the characterization is closely related to the literature in the quantum error correcting code and that the notion of sufficiency is not yet so clear in quantum statistical inferences such as the quantum estimation theory [37–39] and quantum hypothesis testing [37,39–42].

Second, returning to QSS schemes, we utilize the characterization of the reversibility to evaluate a kind of information that each share has about the original quantum state, and then the evaluation leads to the lower bound on the dimension of each share given by Gottesman [4]. It should be noted[1] that a similar result on the dimension of each share has been given in Ref. [43] by a different method using the reference system relevant to the coherent information [21].

As mentioned above, it is impossible to reduce the dimension of each share than that of the original system in QSS schemes which have perfect security conditions. Here, the perfect security conditions mean that any set of shares can either reproduce the original state or obtain no information about it, and such schemes are called *perfect QSS schemes*. On the other hand, in classical ramp SS schemes [44,45], the

*Electronic address: ogawa@mist.i.u-tokyo.ac.jp
†Electronic address: Sasaki_Akira@dn.smbc.co.jp
‡Electronic address: mitsugu@hn.is.uec.ac.jp
§Electronic address: Hirosuke@ieee.org

[1]After the prototype [54] of this work was presented at SITA2003 in Japan, we were informed by an author of [43] that they had established a similar result on the dimension of each share.

size of each share can be decreased by the sacrifice of security conditions admitting the intermediate property for some sets of shares. Following these classical counterparts, we propose a *ramp QSS scheme* and analyze the coding efficiency of it. Then, it is shown that the dimension of each share can be reduced than that of the original system by the sacrifice of security conditions like the classical ramp schemes. Finally, we also demonstrate an optimal construction of the ramp QSS scheme.

II. DEFINITIONS

Let $\mathcal{H},\mathcal{J},\mathcal{K}$ be finite-dimensional Hilbert spaces, and let $\mathcal{L}(\mathcal{H})$ and $\mathcal{S}(\mathcal{H})$ be the totalities of linear operators and density operators on a Hilbert space $\mathcal{H}$, respectively. We will treat QSS schemes encrypting a quantum state on $\mathcal{H}$ into a composite system of Hilbert spaces $\mathcal{H}_1,\ldots,\mathcal{H}_n$, each of which is called a *share*. Let $N\overset{\text{def}}{=}\{1,\ldots,n\}$ be the entire set of shares and $\mathcal{H}_N\overset{\text{def}}{=}\otimes_{i\in N}\mathcal{H}_i$ be the corresponding Hilbert space. For a subset $X\subseteq N$ of shares, let $\mathcal{H}_X\overset{\text{def}}{=}\otimes_{i\in X}\mathcal{H}_i$ as well. The encoding operation of a QSS scheme is described by a quantum operation $W_N:\mathcal{S}(\mathcal{H})\to\mathcal{S}(\mathcal{H}_N)$, which is a completely positive and trace preserving map. For a subset $X\subseteq N$, the composition map of the encoder W_N and the partial trace of the complement $N\backslash X$ is denoted by $W_X\overset{\text{def}}{=}\mathrm{Tr}_{N\backslash X}\cdot W_N$.

Now we will define the notion of the reversibility for general quantum operations. A quantum operation $\mathcal{E}:\mathcal{S}(\mathcal{J})\to\mathcal{S}(\mathcal{K})$ is called *reversible* with respect to (w.r.t.) a subset $\mathcal{S}\subseteq\mathcal{S}(\mathcal{J})$ of density operators if there exists a quantum operation $\mathcal{R}:\mathcal{S}(\mathcal{K})\to\mathcal{S}(\mathcal{J})$ such that $\forall\rho\in\mathcal{S},\mathcal{R}\cdot\mathcal{E}(\rho)=\rho$. A quantum operation $\mathcal{E}:\mathcal{S}(\mathcal{J})\to\mathcal{S}(\mathcal{K})$ is called *vanishing* w.r.t. $\mathcal{S}\subseteq\mathcal{S}(\mathcal{J})$ if there exists a density operator $\rho_0\in\mathcal{S}(\mathcal{K})$ such that $\forall\rho\in\mathcal{S},\mathcal{E}(\rho)=\rho_0$.

Remark 1. It should be noted here that a quantum operation is reversible (vanishing) w.r.t. $\mathcal{S}\subseteq\mathcal{S}(\mathcal{J})$ iff it is reversible (vanishing) w.r.t. the extreme points of the convex hull of $\mathcal{S}$. Therefore, letting $\mathcal{S}_1(\mathcal{J})$ be the totality of pure states on $\mathcal{J}$, a quantum operation is reversible (vanishing) w.r.t. $\mathcal{S}(\mathcal{J})$ iff it is reversible (vanishing) w.r.t. $\mathcal{S}_1(\mathcal{J})$.

A QSS scheme is defined by a quantum operation $W_N:\mathcal{S}(\mathcal{H})\to\mathcal{S}(\mathcal{H}_N)$ which is reversible w.r.t. $\mathcal{S}(\mathcal{H})$. For a QSS scheme W_N, a set $X\subseteq N$ is called *qualified* (*forbidden*) if W_X is reversible (vanishing) w.r.t. $\mathcal{S}(\mathcal{H})$, and, in addition, a set $X\subseteq N$ is called *intermediate* if W_X is neither reversible nor vanishing w.r.t. $\mathcal{S}(\mathcal{H})$. A QSS scheme W_N is called a *perfect scheme* if any set $X\subseteq N$ is either qualified or forbidden. Otherwise, W_N is called a *ramp scheme*. Although the terms "authorized" and "unauthorized" are used in the previous works [3,4] on perfect QSS schemes, we use the terms "qualified" and "forbidden" in this paper because we must divide "unauthorized" sets between "intermediate" sets and "forbidden" sets in ramp QSS schemes.

III. ACCESS STRUCTURE

The access structure of a QSS scheme is the list of forbidden, intermediate, and qualified sets. In classical ramp secret sharing schemes [44,45], intermediate sets are classified further into multilevel categories based on the conditional entropy. In ramp QSS schemes, however, we do not classify the intermediate sets for simplicity in this paper. Formally, the access structure of the set N is defined by a map $f:2^N\to\{0,1,2\}$, where 0, 1, and 2 indicate forbidden, intermediate, and qualified sets, respectively. For a QSS scheme W_N, the access structure of N is determined naturally and hence, is called the access structure of W_N. It is clear that the access structure of W_N satisfies the *monotonicity*—i.e., $X\subseteq Y\Rightarrow f(X)\leqslant f(Y)$. In addition to this relation, the restriction due to the no cloning theorem [11–15] (see also proposition 3 in the appendix) is imposed on QSS schemes; that is, the complement of a qualified set is necessarily forbidden. Conversely, it was shown in Refs. [4,5] that any perfect access structure, consistent with the monotonicity and the no-cloning theorem, can be realized by a perfect QSS scheme.

A quantum operation $\mathcal{E}$ is called a *pure state channel* if $\mathcal{E}(\rho)$ is a pure state for any pure state ρ. A QSS scheme W_N is called a *pure state scheme* if it is a pure state channel. Otherwise, it is called a *mixed state scheme*. Gottesman [4] showed that any perfect QSS scheme is regarded as a subsystem of a pure state QSS scheme. The following lemma is a slight extension of his result including ramp QSS schemes.

Lemma 1. Any mixed state QSS scheme W_N is realized by discarding one share from a pure state QSS scheme $W_{N'}$. Moreover, the access structure of $W_{N'}$ is determined uniquely by that of W_N.

Proof. From the Stinespring dilation theorem [46], there exists a Hilbert space $\mathcal{H}_Z$ and an isometry $V:\mathcal{H}\mapsto\mathcal{H}_N\otimes\mathcal{H}_Z$ such that

$$W_N(\rho)=\mathrm{Tr}_Z[V\rho V^*]. \tag{1}$$

Let $N'=N\cup Z$; then W_N is realized from the pure state QSS scheme $W_{N'}(\rho)=V\rho V^*$ by discarding one share Z. We note that the access structure of $W_{N'}$ for a set $X\subseteq N$ not including Z is the same as that of W_N. Hence we will consider the access structure of $W_{N'}$ for $X\subseteq N'$ which includes Z. It follows from proposition 3 in the appendix that X is qualified iff $N'\backslash X$ is forbidden and, equivalently, that X is forbidden iff $N'\backslash X$ is qualified. Furthermore, we can also see that X is intermediate iff $N'\backslash X$ is intermediate. Therefore, the access structure $f(X)$ is determined uniquely by the complement $N'\backslash X\subseteq N$.□

IV. REVERSIBILITY AND HOLEVO INFORMATION

In this section, turning to a general setting, we will demonstrate that the Holevo information [16] is closely related to the reversibility of quantum operations.

For $\rho,\sigma\in\mathcal{S}(\mathcal{J})$, let

$$D(\rho\,\|\,\sigma)\overset{\text{def}}{=}\mathrm{Tr}[\rho(\log\rho-\log\sigma)] \tag{2}$$

be the quantum relative entropy. Then, for any quantum operation $\mathcal{E}:\mathcal{S}(\mathcal{J})\to\mathcal{S}(\mathcal{K})$, it yields the monotonicity [47–49], i.e.,

$$D(\rho\,\|\,\sigma)\geqslant D(\mathcal{E}(\rho)\,\|\,\mathcal{E}(\sigma)), \tag{3}$$

and the equality holds iff $\mathcal{E}$ is reversible w.r.t. $\{\rho,\sigma\}$ [29] (see also Refs. [31,32]). Furthermore, in the case of equality, there is a canonical reverse operation depending only on σ, which is given by

$$\mathcal{R}_\sigma(\tau) \stackrel{\text{def}}{=} \sigma^{1/2}\mathcal{E}^*(\mathcal{E}(\sigma)^{-1/2}\tau\mathcal{E}(\sigma)^{-1/2})\sigma^{1/2}. \tag{4}$$

Here $\mathcal{E}^*:\mathcal{L}(\mathcal{K})\to\mathcal{L}(\mathcal{J})$ is the dual of $\mathcal{E}$ satisfying

$$\forall\rho\in\mathcal{S}(\mathcal{J}),\ \forall\, Y\in\mathcal{L}(\mathcal{K}),\quad \mathrm{Tr}[\mathcal{E}(\rho)Y]=\mathrm{Tr}[\rho\mathcal{E}^*(Y)].$$

The above fact is summarized as the following proposition.

Proposition 1 (Petz [29]; see also Refs. [31,32]). Given a quantum operation $\mathcal{E}:\mathcal{S}(\mathcal{J})\to S(\mathcal{K})$ and $\rho,\sigma\in\mathcal{S}(\mathcal{J})$, let $\mathcal{R}_\sigma$ be the quantum operation defined by Eq. (4). Then the following three conditions are equivalent.

(a) $D(\rho\|\sigma)=D(\mathcal{E}(\rho)\|\mathcal{E}(\sigma))$.

(b) $\mathcal{R}_\sigma\cdot\mathcal{E}(\rho)=\rho$.

(c) $\mathcal{E}$ is reversible w.r.t. $\{\rho,\sigma\}$.

This fact can be easily extended to a general relation between the Holevo information and the reversibility of a quantum operation w.r.t. a subset $\mathcal{S}\subseteq\mathcal{S}(\mathcal{J})$. Let $\mathcal{P}(\mathcal{S})$ be the set of probability measures on $\mathcal{S}\subseteq\mathcal{S}(\mathcal{J})$, and let

$$\mathrm{E}_\mu[\cdot]=\int_{\mathcal{S}}\cdot\,\mu(\mathrm{d}\rho) \tag{5}$$

be the expectation by a probability measure $\mu\in\mathcal{P}(\mathcal{S})$. Given an ensemble $\mu\in\mathcal{P}(\mathcal{S})$ and a quantum operation $\mathcal{E}$, the Holevo information is defined by

$$I(\mu;\mathcal{E}) \stackrel{\text{def}}{=} \mathrm{E}_\mu[D(\mathcal{E}(\rho)\,\|\,\mathcal{E}(\sigma_\mu))]=H(\mathcal{E}(\sigma_\mu))-\mathrm{E}_\mu[H(\mathcal{E}(\rho))], \tag{6}$$

where $\sigma_\mu \stackrel{\text{def}}{=} \mathrm{E}_\mu[\rho]$ and $H(\rho)\stackrel{\text{def}}{=}-\mathrm{Tr}[\rho\log\rho]$ is the von Neumann entropy. Moreover, let $\mathcal{P}_+(\mathcal{S})$ be the set of probability measures on $\mathcal{S}\subseteq\mathcal{S}(\mathcal{J})$ which are positive almost everywhere on $\mathcal{S}$. More specifically,

$$\mathcal{P}_+(\mathcal{S})\stackrel{\text{def}}{=}\{\mu\in\mathcal{P}(\mathcal{S})\,|\,\forall\, O\subseteq\mathcal{O}(\mathcal{S}),\mu(O)>0\}, \tag{7}$$

where $\mathcal{O}(\mathcal{S})$ is the totality of open sets on $\mathcal{S}$ and is defined in terms of the relative topology induced by the inclusion $\mathcal{S}\subseteq\mathcal{S}(\mathcal{J})$. Then we have the following theorem.

Theorem 1. Let $\mathcal{I}:\mathcal{S}(\mathcal{J})\to\mathcal{S}(\mathcal{J})$ be the identity map. Given a quantum operation $\mathcal{E}:\mathcal{S}(\mathcal{J})\to\mathcal{S}(\mathcal{K})$ and $\mathcal{S}\subseteq\mathcal{S}(\mathcal{J})$, the following three conditions are equivalent.

(a) $\mathcal{E}$ is reversible (vanishing) w.r.t. $\mathcal{S}$.

(b) $\forall\mu\in\mathcal{P}_+(\mathcal{S}),I(\mu;\mathcal{E})=I(\mu;\mathcal{I})(=0)$.

(c) $\exists\mu\in\mathcal{P}_+(\mathcal{S}),I(\mu;\mathcal{E})=I(\mu;\mathcal{I})(=0)$.

Proof.(a) ⇒ (b): From the definition of the reversibility, there exists a quantum operation $\mathcal{R}$ such that $\forall\rho\in\mathcal{S},\mathcal{R}\cdot\mathcal{E}(\rho)=\rho$. Taking the expectation of ρ by an arbitrary $\mu\in\mathcal{P}_+(\mathcal{S})$, we have $\mathcal{R}\cdot\mathcal{E}(\sigma_\mu)=\sigma_\mu$. Then it follows from "(c) ⇒ (a)" of proposition 1 that

$$\forall\rho\in\mathcal{S},D(\rho\,\|\,\sigma_\mu)=D(\mathcal{E}(\rho)\,\|\,\mathcal{E}(\sigma_\mu)). \tag{8}$$

Taking the expectation of the above equality by μ leads to (b).

(b) ⇒ (c): Obvious.

(c) ⇒ (a): First, note that

$$I(\mu;\mathcal{I})-I(\mu;\mathcal{E})=\mathrm{E}_\mu[D(\rho\,\|\,\sigma_\mu)-D(\mathcal{E}(\rho)\,\|\,\mathcal{E}(\sigma_\mu))]\geqslant 0, \tag{9}$$

since the monotonicity of the quantum relative entropy leads to

$$D(\rho\,\|\,\sigma_\mu)-D(\mathcal{E}(\rho)\,\|\,\mathcal{E}(\sigma_\mu))\geqslant 0 \tag{10}$$

for each term in the expectation of (9). Therefore we can see from the definition of $\mathcal{P}_+(\mathcal{S})$, along with the continuity of $\mathcal{E}$ and the quantum relative entropy that Eq. (8) is a necessary condition for $I(\mu;\mathcal{I})-I(\mu;\mathcal{E})=0$. Using "(a) ⇒ (b)" of proposition 1, we have that $\forall\rho\in\mathcal{S},\mathcal{R}_{\sigma_\mu}\cdot\mathcal{E}(\rho)=\rho$, which implies (a).

As for the vanishing property, we can show the assertion in the same way as the reversibility by using $D(\rho\|\sigma)\geqslant 0$ and $D(\rho\|\sigma)=0\Leftrightarrow\rho=\sigma$. □

V. CODING EFFICIENCY OF QSS SCHEMES

Let $\mathcal{S}_1(\mathcal{H})$ be the totality of pure states on $\mathcal{H}$, and note that a quantum operation is reversible (resp. vanishing) w.r.t. $\mathcal{S}(\mathcal{H})$ iff it is reversible (vanishing) w.r.t. $\mathcal{S}_1(\mathcal{H})$. Therefore it suffices to treat the reversibility of a QSS scheme W_N w.r.t. $\mathcal{S}_1(\mathcal{H})$. For a pure state ensemble $\mu\in\mathcal{P}_+(\mathcal{S}_1(\mathcal{H}))$, the Holevo information is given by $I(\mu;\mathcal{I})=H(\sigma_\mu)$, since $H(\rho)=0$ for any pure state $\rho\in\mathcal{S}_1(\mathcal{H})$, and hence, the following theorem immediately follows from theorem 1.

Theorem 2. For any QSS scheme W_N, the following three conditions are equivalent.

(a) X is qualified (forbidden).

(b) $\forall\mu\in\mathcal{P}_+(\mathcal{S}_1(\mathcal{H})),I(\mu;W_X)=H(\sigma_\mu)(=0)$.

(c) $\exists\mu\in\mathcal{P}_+(\mathcal{S}_1(\mathcal{H})),I(\mu;W_X)=H(\sigma_\mu)(=0)$.

Remark 2. Theorem 2 can be regarded as a variant of the perfect error correcting condition [21] without using reference systems, while theorem 1 is an extension of these conditions to the reversibility condition w.r.t. general subsets of $\mathcal{S}(\mathcal{H})$.

Remark 3. As is clear by definition, it is also interesting to observe from theorem 2 that the access structure of QSS schemes does not depend on μ in $\mathcal{P}_+(\mathcal{S}_1(\mathcal{H}))$. We note that this fact holds in classical perfect SS schemes. Actually, corresponding statements are given by a different approach in Ref. [50].

Now we consider the coding efficiency of QSS schemes. A set $X\subseteq N$ is called *significant* if there exists a forbidden set $Y\subseteq N$ such that $X\cup Y$ is qualified.

Theorem 3. For any significant set $X\subseteq N$ of any QSS scheme W_N, it holds that

$$\forall\mu\in\mathcal{P}_+(\mathcal{S}_1(\mathcal{H})),H(\sigma_\mu)\leqslant H(W_X(\sigma_\mu)). \tag{11}$$

Proof. From lemma 1, W_N is supposed to be a pure state scheme without loss of generality. Moreover, for any significant set $X\subseteq N$ we can choose a forbidden sets $Y\subseteq N$ such that $X\cup Y$ is qualified and $X\cap Y=\emptyset$. Then it holds that $I(\mu;W_{XY})=H(\sigma_\mu)$ and $I(\mu;W_Y)=0$ for any $\mu\in\mathcal{P}_+(\mathcal{S}_1(\mathcal{H}))$ from theorem 2, and hence, we have

$$
\begin{aligned}
H(\sigma_\mu) &= I(\mu;W_{XY}) - I(\mu;W_Y) \\
&= H(W_{XY}(\sigma_\mu)) - \mathrm{E}_\mu[H(W_{XY}(\rho))] \\
&\quad - H(W_Y(\sigma_\mu)) + \mathrm{E}_\mu[H(W_Y(\rho))] \\
&\leqslant H(W_X(\sigma_\mu)) - \mathrm{E}_\mu[H_\rho(W_X|W_Y)], \qquad (12)
\end{aligned}
$$

where the last inequality follows from the subadditivity of the von Neumann entropy and we have written the conditional entropy as

$$H_\rho(W_X|W_Y) \stackrel{\mathrm{def}}{=} H(W_{XY}(\rho)) - H(W_Y(\rho)). \qquad (13)$$

Now let $Z=N\backslash(X\cup Y)$ and note that $W_N=W_{XYZ}$ is a pure state channel. Then it follows from proposition 3 in the Appendix that qualified $X\cup Y$ implies forbidden Z and forbidden Y implies qualified $X\cup Z$. Hence, since Z has the same property as Y, Z also satisfies the same inequality as (12)—i.e.,

$$H(\sigma_\mu) \leqslant H(W_X(\sigma_\mu)) - \mathrm{E}_\mu[H_\rho(W_X|W_Z)]. \qquad (14)$$

Since $W_{XYZ}(\rho)$ is a pure state, we have $H(W_{XY}(\rho)) = H(W_Z(\rho))$ and $H(W_{XZ}(\rho))=H(W_Y(\rho))$. Consequently, it follows from Eqs. (12) and (14) that

$$
\begin{aligned}
H(\sigma_\mu) &\leqslant H(W_X(\sigma_\mu)) - \frac{1}{2}\mathrm{E}_\mu[H_\rho(W_X|W_Y) + H_\rho(W_X|W_Z)] \\
&= H(W_X(\sigma_\mu)), \qquad (15)
\end{aligned}
$$

which has been asserted. □

Corollary 1 (Gottesman [4]). For any significant share $i \in N$ of any QSS scheme W_N, we have

$$\dim \mathcal{H} \leqslant \dim \mathcal{H}_i. \qquad (16)$$

Proof. Let μ be the uniform distribution on $\mathcal{S}_1(\mathcal{H})$ in theorem 3—namely, the invariant measure with respect to the special unitary group. Then we have $\sigma_\mu = I/\dim \mathcal{H}$ and the dimension of each share is bounded below as

$$\log \dim \mathcal{H} = H(\sigma_\mu) \leqslant H(W_i(\sigma_\mu)) \leqslant \log \dim \mathcal{H}_i. \qquad (17)$$

□

Remark 4. The arguments and the theorems so far are valid even in the classical cases. That is verified by replacing the corresponding notions with the classical ones. For example, quantum operations, the Holevo information, and pure states are replaced with channels, the mutual information, and δ distributions, respectively. In this case, it should be noted that the proof of theorem 3 is already finished in (12), since the conditional entropy is nonnegative in the classical cases.

VI. RAMP QSS SCHEMES

From corollary 1, it is impossible to reduce the dimension of each share than that of the original system in perfect QSS schemes, since any share except useless ones should be significant in perfect QSS schemes. On the other hand, in classical ramp SS schemes such as (k,L,n)-threshold ramp SS schemes [44,45], the size of each share can be decreased by taking into account the trade-off between the security condition and the coding efficiency. We utilize this idea in the quantum setting to propose (k,L,n)-*threshold ramp QSS schemes* in the following sense.

Definition 1. A QSS scheme W_N is called a (k,L,n)-threshold ramp QSS scheme if the following conditions are fulfilled.

(a) $X\subseteq N$ is forbidden iff $|X|\leqslant k-L$.

(b) $X\subseteq N$ is qualified iff $|X|\geqslant k$.

Note that the above conditions imply

(c) $X\subseteq N$ is intermediate iff $k-L<|X|<k$,

and the (k,L,n)-threshold ramp QSS scheme reduces to the (k,n)-threshold QSS scheme [3] if $L=1$.

Cleve *et al.* [3] showed that the condition $n\leqslant 2k-1$ must be satisfied for the (k,n)-threshold QSS scheme to exist. As an extension of this condition, we have the following lemma.

Lemma 2. For a (k,L,n)-threshold ramp QSS scheme, it holds that $n\leqslant 2k-L$. Especially, we have $n=2k-L$ if it is a pure state QSS scheme.

Proof. From definition 1, X is a qualified set if $|X|=k$. In this case, it follows from proposition 3 in the Appendix that the complement $N\backslash X$ is forbidden, which implies $|N\backslash X|=n-k\leqslant k-L$. In the case of a pure state QSS scheme, we can also show that $n\geqslant 2k-L$ in the same way.

Similarly to theorem 3 and corollary 1, we can evaluate the coding efficiency of the ramp scheme as follows.

Theorem 4. For (k,L,n)-threshold ramp QSS schemes, it holds that

$$\forall \mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H})), \quad \frac{1}{L}H(\sigma_\mu) \leqslant \frac{1}{n}\sum_{i\in N} H(W_i(\sigma_\mu)). \qquad (18)$$

Proof. For any set $X\subseteq N$ with the cardinality $|X|=L$, there exists $Y\subseteq N$ such that $X\cap Y=\emptyset$ and $|Y|=k-L$. Then $X\cup Y$ is qualified while Y is forbidden. Therefore it follows from theorem 3 that

$$H(\sigma_\mu) \leqslant H(W_X(\sigma_\mu)) \leqslant \sum_{i\in X} H(W_i(\sigma_\mu)), \qquad (19)$$

where we used the subadditivity of the von Neumann entropy. Finally we can show (18) by taking the arithmetic mean of (19) for all $X\subseteq N$ satisfying $|X|=L$. □

Corollary 2. For (k,L,n)-threshold ramp QSS schemes, we have

$$\frac{1}{L}\dim \mathcal{H} \leqslant \frac{1}{n}\sum_{i\in N} \dim \mathcal{H}_i. \qquad (20)$$

The above corollary implies that the dimension of each share can be decreased by the factor $1/L$ in the average sense than that of the original system.

VII. CONSTRUCTION OF RAMP SCHEMES

In this section, we will show a method to realize (k,L,n)-threshold ramp QSS schemes which has the optimal coding efficiency in the sense of corollary 2. The encoding and reverse operations used here are regarded as extensions of Ref. [3] to the ramp QSS scheme.

Let $\mathbb{F}$ be a finite field with $q \stackrel{\mathrm{def}}{=} |\mathbb{F}| \geqslant n$, and let $\mathcal{J}_j(j=1,\ldots,L)$ and $\mathcal{H}_i(i\in N=\{1,\ldots,n\})$ be isomorphic Hilbert spaces with dimension $\dim \mathcal{J}_j = \dim \mathcal{H}_i = q$ and an orthonormal basis $\{|s\rangle\}_{s\in\mathbb{F}}$ indexed by $\mathbb{F}$. We will construct a pure state QSS scheme W_N which maps a quantum state on $\mathcal{H} \overset{\text{def}}{=} \otimes_{j=1}^{L} \mathcal{J}_j$ into the composite system of shares $\mathcal{H}_N \overset{\text{def}}{=} \otimes_{i\in N}\mathcal{H}_i$. Note that $n=2k-L$ holds from lemma 2. Since the pure state QSS scheme W_N is represented by an isometry $V:\mathcal{H}\to\mathcal{H}_N$ as

$$W_N(\rho) = V\rho V^*, \tag{21}$$

it suffices to specify the images $V|s^L\rangle$ of the basis

$$|s^L\rangle = |s_1\rangle \otimes \cdots \otimes |s_L\rangle, \quad s^L = (s_1,\cdots,s_L) \in \mathbb{F}^L,$$

on $\mathcal{H}$. For this purpose, we utilize the polynomial of degree $k-1$ on $\mathbb{F}$ specified by coefficients $c=(c_1,\ldots,c_k)\in\mathbb{F}^k$—i.e.,

$$p_c(x) = \sum_{i=1}^{k} c_i x^{i-1}. \tag{22}$$

By providing publicly revealed constants $x_1,\ldots,x_n \in \mathbb{F}$ which are different from each other, define the isometry V by

$$V|s^L\rangle \overset{\text{def}}{=} \frac{1}{\sqrt{C}} \sum_{c\in D(s^L)} |p_c(x_1),\ldots,p_c(x_n)\rangle, \tag{23}$$

where

$$D(s^L) \overset{\text{def}}{=} \{(c_1,\ldots,c_k) \in \mathbb{F}^k | c_i = s_i (i=1,\ldots,L)\},$$

and C is a normalization constant to be specified later. Now, in order to verify that V is actually an isometry, let us introduce the following notations for $X=\{i_1,\ldots,i_m\}\subseteq N$:

$$M_b^a(X) \overset{\text{def}}{=} \begin{pmatrix} x_{i_1}^a & \ldots & x_{i_m}^a \\ x_{i_1}^{a+1} & \ldots & x_{i_m}^{a+1} \\ \vdots & & \vdots \\ x_{i_1}^b & \ldots & x_{i_m}^b \end{pmatrix} \quad (a<b), \tag{24}$$

$$p_c(X) \overset{\text{def}}{=} (p_c(x_{i_1}),\ldots,p_c(x_{i_m})). \tag{25}$$

Then we have $p_c(X)=(c_1,\ldots,c_k)M_{k-1}^0(X)$, and the following lemma is useful for later discussions.

Lemma 3. For each $s^L\in\mathbb{F}^L$, the map $c\in D(s^L)\mapsto p_c(X)$ is injective if $|X|\geq k-L$. Especially, it is one-to-one if $|X|=k-L$. Similarly, the map $c\in\mathbb{F}^k\mapsto p_c(X)$ is injective if $|X|\geq k$, and it is one-to-one if $|X|=k$.

Proof. The injective property is verified by the following relation:

$$p_c(X) = (s_1,\ldots,s_L,c_{L+1},\ldots,c_k)\begin{pmatrix} M_{L-1}^0(X) \\ M_{k-1}^L(X) \end{pmatrix}, \tag{26}$$

since $M_{k-1}^L(X)$ has the full column rank if $|X|\geq k-L$. In addition, it is one-to-one if $|X|=k-L$, since $|D(s^L)|=|\mathbb{F}^{k-L}|$. In the same way, we can show the remaining part of the lemma. □

From the above lemma, we can see that $|p_c(N)\rangle (c\in\mathbb{F}^k)$ are orthogonal to each other, and hence, $V|s^L\rangle (s^L\in\mathbb{F}^L)$ are also orthogonal to each other, which ensures that V is isometric. At the same time, the normalizing constant is determined as $C=q^{k-L}$.

Next, we will show that thus constructed QSS scheme W_N is actually a (k,L,n)-threshold ramp scheme.

a. Qualified sets. In order to verify that X is qualified for $|X|\geq k$, it suffices to show that $X=\{1,\ldots,k\}$ is qualified, because of the symmetrical way to construct W_N and the monotonicity of the access structure. The following local operations on X realize the reverse operation of W_X.

(i) Perform the unitary transformation on X corresponding to $p_c(X)M_{k-1}^0(X)^{-1}$, which turns the summation in (23) into

$$\sum_{c\in D(s^L)} |c_1,\ldots,c_k,p_c(x_{k+1}),\ldots,p_c(x_n)\rangle. \tag{27}$$

(ii) Noting that $n-k=k-L$, perform the unitary transformation on X corresponding to the linear transformation:

$$(c_1,\ldots,c_k)\begin{pmatrix} I & M_{L-1}^0(N\setminus X) \\ 0 & M_{k-1}^L(N\setminus X) \end{pmatrix}. \tag{28}$$

Then (27) yields

$$|s^L\rangle \sum_{c\in D(s^L)} |p_c(N\setminus X)\rangle |p_c(N\setminus X)\rangle, \tag{29}$$

which can be represented by lemma 3 as

$$|s^L\rangle \sum_{y^{k-L}\in\mathbb{F}^{k-L}} |y^{k-L}\rangle |y^{k-L}\rangle. \tag{30}$$

Thus, we have recovered $|s^L\rangle$ on $\{1,\ldots,L\}$ from $V|s^L\rangle$ by the local operations on X.

b. Forbidden sets. When $|X|\leq k-L, N\setminus X$ is qualified since $|N\setminus X|\geq k$. Therefore it follows from proposition 3 in the appendix that X is forbidden.

c. Intermediate sets. In the case $|X|=k-l (0<l<L)$, we show that X is intermediate. For this purpose, it is sufficient to show that for $X=\{1,\ldots,k-l\}, W_X$ is neither reversible nor vanishing w.r.t. a subset $\mathcal{S}=\{|s^L\rangle\langle s^L|\}_{s^L\in\mathbb{F}^L}$ included by $\mathcal{S}(\mathcal{H})$. Taking theorem 2 into account, let us calculate the Holevo information

$$I(\mu;W_X) = H(W_X(\sigma_\mu)) - E_\mu[H(W_X(|s^L\rangle\langle s^L|))]$$

and $H(\sigma_\mu)$ for the uniform distribution μ on $\mathcal{S}$. Then the von Neumann entropy is easily calculated as $H(\sigma_\mu)=L\log q$ since $\sigma_\mu=I/q^L$. On the other hand, from lemma 3 and

$$|N\setminus X| = n-(k-l) = (2k-L)-(k-l) > k-L,$$

we have

$$W_X(|s^L\rangle\langle s^L|) = \frac{1}{C}\sum_{c,d\in D(s^L)} \langle p_d(N\setminus X), p_c(N\setminus X)\rangle |p_c(X)\rangle\langle p_d(X)|$$
$$= \frac{1}{C}\sum_{c\in D(s^L)} |p_c(X)\rangle\langle p_c(X)|. \tag{31}$$

Lemma 3 with $|X|=k-l>k-L$ also enables us to see that $|p_c(X)\rangle$ in the summation in Eq. (31) are orthogonal to each other, and hence, we have $H(W_X(|s^L\rangle\langle s^L|))=(k-L)\log q$ for all $s^L\in\mathbb{F}^L$. Next, letting $Y=\{1,\ldots,k\}$, we have

$$W_Y(\sigma_\mu) = \frac{1}{q^L}\sum_{s^L\in\mathbb{F}^L} W_Y(|s^L\rangle\langle s^L|)$$
$$= \frac{1}{q^L C}\sum_{s^L\in\mathbb{F}^L}\sum_{c,d\in D(s^L)} \langle p_d(N\setminus Y), p_c(N\setminus Y)\rangle \times |p_c(Y)\rangle\langle p_d(Y)|$$
$$= \frac{1}{q^k}\sum_{s^L\in\mathbb{F}^L}\sum_{c\in D(s^L)} |p_c(Y)\rangle\langle p_c(Y)| = I/q^k, \quad (32)$$

where the third and last equalities follow from lemma 3. Then we have $W_X(\sigma_\mu)=I/q^{k-l}$ and $H(W_X(\sigma_\mu))=(k-l)\log q$. Consequently, it holds that

$$0 < I(\mu;W_X) = (L-l)\log q < L\log q = H(\sigma_\mu). \quad (33)$$

Therefore it follows from theorem 2 that W_X is neither reversible nor vanishing w.r.t. $\mathcal{S}$.

At last, it is confirmed that W_N actually realizes the (k,L,n)-threshold ramp scheme. It is clear from the construction of W_N that the coding efficiency of W_N is optimal in the sense of corollary 2.

VIII. CONCLUDING REMARKS

In this paper, we have revisited the lower bound on the dimension of each share in QSS schemes given by Gottesman [4] and gave a rigorous proof for the lower bound (theorem 3 and corollary 1). The key idea of the proof was as follows. First, we have established a fundamental relation between the reversibility of quantum operations and the Holevo information (theorem 1). Then, we have treated the qualified or forbidden condition as the reversible or vanishing condition for the corresponding quantum operation. These steps gave us clear insights into QSS schemes and even into classical SS schemes (see remark 4). For example, we can easily see from these pictures that the qualified or forbidden condition is independent of the probability of the source ensemble in both classical and quantum cases (remark 3).

We have also proposed a ramp QSS scheme called the (k,L,n)-threshold QSS ramp scheme so that the dimension of each share could be decreased than that of the original system by the sacrifice of security conditions. Finally, we have analyzed the coding efficiency of the (k,L,n)-threshold ramp scheme and shown an optimal construction to attain the lower bound on the efficiency.

One may wonder that a forbidden party with the forbidden set of shares could disturb the protocol in QSS schemes by using the property of the entanglement. In other words, what happens if the forbidden party would try to break the protocol to measure their particles and to announce the outcome publicly?

The answer of the question is as follows. Let $X\subseteq N$ be a qualified set for a QSS scheme W_N. Then, $Y\overset{\text{def}}{=}N\setminus X$ is forbidden and there exists a decoding operation $\mathcal{R}_X$ for X recovering any pure state ρ from $W_N(\rho)$:

$$(\mathcal{I}_Y\otimes\mathcal{R}_X)W_N(\rho) = W_Y(\rho)\otimes\rho = \rho_0\otimes\rho, \quad (34)$$

where $\mathcal{I}_Y$ is the identity map and $\rho_0\overset{\text{def}}{=}W_Y(\rho)$. Note that pure states have no entanglement with another systems and that ρ_0 does not depend on ρ. Then, we can see that Eq. (34) also holds for mixed states ρ and that any malicious operation $\mathcal{E}_Y$ by the forbidden party Y could not interfere with the qualified set of shares—i.e.,

$$(\mathcal{I}_Y\otimes\mathcal{R}_X)(\mathcal{E}_Y\otimes\mathcal{I}_X)W_N(\rho) = (\mathcal{E}_Y\otimes\mathcal{I}_X)(\mathcal{I}_Y\otimes\mathcal{R}_X)W_N(\rho) = \mathcal{E}_Y(\rho_0)\otimes\rho. \quad (35)$$

However, the above arguments are not valid for intermediate sets of shares; i.e., a measurement on an intermediate set of shares may affect the quantum state of another intermediate set through the effects of the entanglement. For this reason, it is a challenging problem to classify intermediate sets in ramp QSS schemes. We need to study security conditions for ramp QSS schemes and to develop tools to quantify the information that an intermediate set of share has. These developments are left to further studies.

APPENDIX: NO-CLONING AND NO-DELETING THEOREM

In this paper, we have used a fundamental result in QSS schemes shown by Cleve *et al.* [3]—that is, if a set of shares $X\subseteq N$ is qualified, the complement $N\setminus X$ is necessarily forbidden, and, in addition, the converse is also true in pure state QSS schemes. These properties are regarded as variants of the no cloning theorem [11–15] and the no deleting theorem [51,52]. Another proof of this property relevant to the no-cloning theorem is given by an information theoretical manner in Ref. [43]. In this appendix , we will review these results in our notations for readers' convenience following the original proof [3] which utilizes the perfect error correcting condition [19,20]. Here we introduce a notation $\mathcal{E}\sim\{E_a\}_a$ by which we mean that $\mathcal{E}$ is a quantum operation represented by the Kraus representation [53] $\mathcal{E}(\rho)=\sum_a E_a\rho E_a^*$.

Proposition 2 ([19,20]). Let $\mathcal{C}:\rho\in\mathcal{S}(\mathcal{H})\mapsto V\rho V^*\in\mathcal{S}(\mathcal{J})$ be a quantum operation defined by an isometry $V:\mathcal{H}\to\mathcal{J}$, and let $\mathcal{E}:\mathcal{S}(\mathcal{J})\to\mathcal{S}(\mathcal{K})$ be a quantum operation represented by $\mathcal{E}\sim\{E_a\}_a$. Then the following conditions are equivalent.

(a) $\mathcal{E}\cdot\mathcal{C}$ is reversible w.r.t. $\mathcal{S}(\mathcal{H})$.

(b) For each pair of indices a and b, there exists $C_{ab}\in\mathbb{C}$ such that $V^*E_a^*E_bV=C_{ab}I_{\mathcal{H}}$.

Proposition 3 (Cleve-Gottesman-Lo [3]). Given a quantum operation $W_{XY}:\mathcal{S}(\mathcal{H})\to\mathcal{S}(\mathcal{H}_X\otimes\mathcal{H}_Y)$, let $W_X\overset{\text{def}}{=}\mathrm{Tr}_Y\cdot W_{XY}$ and $W_Y\overset{\text{def}}{=}\mathrm{Tr}_X\cdot W_{XY}$. If W_{XY} is a pure state channel and reversible, then the following conditions are equivalent.

(a) W_X is reversible w.r.t. $\mathcal{S}(\mathcal{H})$.

(b) W_Y is vanishing w.r.t. $\mathcal{S}(\mathcal{H})$.

In the case of general quantum operations, (a) implies (b).

Proof. First, we show the equivalence when W_{XY} is a pure state channel and reversible. In this case, W_{XY} is written as $W_{XY}(\rho)=V\rho V^*$ by an isometry $V:\mathcal{H}\rightarrow\mathcal{H}_X\otimes\mathcal{H}_Y$. Let $\{|a\rangle\}_a$ be an orthonormal basis on $\mathcal{H}_Y$. Then it follows from proposition 2 with $\mathcal{E}=\mathrm{Tr}_Y\sim\{I_X\otimes\langle a|\}_a$ that (a) holds iff there exists $C_{ab}\in\mathbb{C}$ such that

$$\forall(a,b), V^*(I_X\otimes|a\rangle\langle b|)V=C_{ab}I_{\mathcal{H}}. \tag{A1}$$

Moreover, Eq. (A1) is equivalent to the existence of a linear functional $C:\mathcal{L}(\mathcal{H}_Y)\rightarrow\mathbb{C}$ such that

$$\forall A\in\mathcal{L}(\mathcal{H}_Y), V^*(I_X\otimes A)V=C(A)I_{\mathcal{H}}. \tag{A2}$$

Now we can easily see the equivalence of Eq. (A2) and (b) from the following equalities:

$$\mathrm{Tr}[W_Y(\rho)A]=\mathrm{Tr}[W_{XY}(\rho)(I_X\otimes A)]=\mathrm{Tr}[\rho V^*(I_X\otimes A)V]. \tag{A3}$$

In the general case, let $W_{XY}(\rho)=\mathrm{Tr}_Z[U\rho U^*]$ be the Stinespring representation [46], where $U:\mathcal{H}\rightarrow\mathcal{H}_X\otimes\mathcal{H}_Y\otimes\mathcal{H}_Z$ is an isometry. Then $W_{XYZ}(\rho)=U\rho U^*$ is a pure state channel and reversible. From the above argument, if W_X is reversible w.r.t. $\mathcal{S}(\mathcal{H})$, then W_{YZ} is vanishing, and hence W_Y is also vanishing w.r.t. $\mathcal{S}(\mathcal{H})$.□

[1] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[2] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[3] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[4] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).
[5] A. D. Smith, e-print quant-ph/0001087.
[6] A. Shamir, Commun. ACM **22**, 612 (1979).
[7] G. R. Blakley (unpublished).
[8] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[9] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
[10] J. C. Benaloh and J. Leichter (unpublished).
[11] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[12] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[13] H. P. Yuen, Phys. Lett. **113A**, 405 (1986).
[14] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).
[15] M. Koashi and N. Imoto, Phys. Rev. Lett. **81**, 4264 (1988).
[16] A. S. Holevo, Probl. Inf. Transm. **9**, 3 (1973).
[17] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
[18] H. Strasser, *Mathematical Theory of Statistics* (Walter de Gruyter, Berlin, 1985).
[19] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[20] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[21] B. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996).
[22] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[23] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[24] H. Umegaki, Kodai Math. Semin. Rep. **11**, 51 (1959).
[25] H. Umegaki, Kodai Math. Semin. Rep. **14**, 59 (1962).
[26] S. Gudder and J.-P. Marchand, J. Math. Phys. **13**, 799 (1972).
[27] F. Hiai, M. Ohya, and M. Tsukada, Pac. J. Math. **96**, 99 (1981).
[28] F. Hiai, M. Ohya, and M. Tsukada, Pac. J. Math. **107**, 117 (1983).
[29] D. Petz, Q. J. Math. **39**, 907 (1988).
[30] D. Petz, Commun. Math. Phys. **105**, 123 (1986).
[31] D. Petz, Rev. Math. Phys. **15**, 79 (2003).
[32] P. Hayden, R. Jozsa, D. Petz, and A. Winter, Commun. Math. Phys. **246**, 359 (2004).
[33] M. Mosonyi and D. Petz, e-print quant-ph/0312221.
[34] A. Jencova and D. Petz, e-print quant-ph/0412093.
[35] M. Koashi and N. Imoto, Phys. Rev. A **66**, 022318 (2002).
[36] G. Lindblad, Lett. Math. Phys. **47**, 189 (1999).
[37] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[38] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
[39] *Asymptotic Theory of Quantum Statistical Inference: Selected Papers* edited by M. Hayashi,(World Scientific, Singapore, 2005).
[40] A. S. Holevo, J. Multivariate Anal. **3**, 337 (1973).
[41] F. Hiai and D. Petz, Commun. Math. Phys. **143**, 99 (1991).
[42] T. Ogawa and H. Nagaoka, IEEE Trans. Inf. Theory **46**, 2428 (2000).
[43] H. Imai, J. Mueller-Quade, A. C. A. Nascimento, P. Tuyls, and A. Winter, e-print quant-ph/0311136.
[44] H. Yamamoto, Trans. Inst. Electron. Commun. Eng. Jpn., Sect. E **J68-A**, 945 (1985) (in Japanese); Electron. Commun. Jpn., Part 2: Electron. **69**, 46 (1986).
[45] G. R. Blakley and C. Meadows (unpublished).
[46] W. F. Stinespring, Proc. Am. Math. Soc. **6**, 211 (1955).
[47] G. Lindblad, Commun. Math. Phys. **40**, 147 (1975).
[48] H. Araki, Publ. RIMS Kyoto Univ. **11**, 809 (1976).
[49] A. Uhlmann, Commun. Math. Phys. **54**, 21 (1977).
[50] C. Blundo, A. D. Santis, and U. Vaccaro, Inf. Process. Lett. **65**, 25 (1998).
[51] A. K. Pati and S. L. Braunstein, Nature (London) **404**, 164 (2000).
[52] A. K. Pati and S. L. Braunstein, e-print quant-ph/0007121.
[53] K. Kraus, *States, Effects, and Operations* (Springer-Verlag, Berlin, 1983).
[54] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto (unpublished).