Generalized quantum secret sharing

Sudhir Kumar Singh*
Department of Electrical Engineering, University of California, Los Angeles, California 90095, USA

R. Srikanth†
Optics Group, Raman Research Institute, Bangalore-560080, India
(Received 20 July 2004; published 19 January 2005)

We explore a generalization of quantum secret sharing (QSS) in which classical shares play a complementary role to quantum shares, exploring further consequences of an idea first studied by Nascimento, Mueller-Quade, and Imai [Phys. Rev. A **64**, 042311 (2001)]. We examine three ways, termed inflation, compression, and twin thresholding, by which the proportion of classical shares can be augmented. This has the important application that it reduces quantum (information processing) players by replacing them with their classical counterparts, thereby making quantum secret sharing considerably easier and less expensive to implement in a practical setting. In compression, a QSS scheme is turned into an equivalent scheme with fewer quantum players, compensated for by suitable classical shares. In inflation, a QSS scheme is enlarged by adding only classical shares and players. In a twin-threshold scheme, we invoke two separate thresholds for classical and quantum shares based on the idea of information dilution.

DOI: 10.1103/PhysRevA.71.012328 PACS number(s): 03.67.Dd

I. INTRODUCTION

Suppose the president of a bank, Alice, wants to give access to a vault to two vice-presidents, Bob and Charlie, whom she does not entirely trust. Instead of giving the combination to any one of them, she may desire to distribute the information in such a way that no vice-president alone has any knowledge of the combination, but both of them can jointly determine the combination. Cryptography provides the answer to this question in the form of *secret sharing* [1,2]. In this scheme, some sensitive data are distributed among a number of parties such that certain authorized sets of parties can access the data, but no other combination of players. A particularly symmetric variety of secret splitting (sharing) is called a *threshold scheme*: in a (k,n) classical threshold scheme (CTS), the secret is split up into n pieces (shares), of which any k shares form a set *authorized* to reconstruct the secret, while any set of $k-1$ or fewer shares has no information about the secret. Blakely [3] and Shamir [4] showed that CTS's exist for all values of k and n with $n \geqslant k$. By concatenating threshold schemes, one can construct arbitrary access structures, subject only to the condition of monotonicity (i.e., sets containing authorized sets should also be authorized) [5]. Hillery *et al.* [6] and Karlsson *et al.* [7] proposed methods for implementing CTS's that use *quantum* information to transmit shares securely in the presence of eavesdroppers.

Subsequently, extending the above idea to the quantum case, Cleve, Gottesman, and Lo [8] proposed a (k,n) *quantum* threshold scheme (QTS) as a method to split up an unknown secret quantum state $|S\rangle$ into n pieces (shares) with the restriction that $k>n/2$ (for if this inequality were violated, two disjoint sets of players can reconstruct the secret, in violation of the quantum no-cloning theorem [9,10]). The notion of the QTS is based on quantum erasure correction [11,12]. Quantum secret sharing (QSS) has been extended beyond QTS to general access structures [13,14], but here the no-cloning theorem implies that none of the authorized sets shall be mutually disjoint. Potential applications of QSS include creating joint checking accounts containing quantum money [15], or sharing hard-to-create ancilla states [13], or performing secure distributed quantum computation [16]. Implementing QSS is well within current technology [17], and has been demonstrated by a recent experiment [18].

In conventional QSS schemes, it is often implicitly assumed that all shareholders carry and process quantum information. Given the fragile nature of quantum information, this can often be difficult and expensive from a practical viewpoint. Fortunately, it turns out to be possible sometimes to construct an equivalent scheme in which some shareholders carry only classical information and no quantum information, an idea first studied by Nascimeto *et al.* [19]. Our work is dedicated to exploring further consequences of this idea. It is of considerable importance to consider ways in which the proportion of classical shares and classical information processing can be increased in realizing a QSS scheme. Furthermore, hybrid (classical-quantum) QSS can potentially make use of features available to classical secret sharing such as share renewal [20], secret sharing with prevention [21], and disenrollment [22].

In particular, our work is aimed at studying ways to augment the proportion of classical shares in different ways for various situations in QSS. As pointed out above, the main purpose of this exercise is to render practical implementation easier and less expensive. In Sec. II, we present some basic ways to introduce a classical information component into QSS. In Sec. III, we discuss how this can be used to "compress" a QSS scheme, that is, reduce the proportion of quantum-information-carrying players. In Sec. IV, we show how a QSS scheme can be "inflated" by adding only classical shares. In Sec. V, we invoke two separate thresholds for

*Electronic address: suds@ee.ucla.edu
†Electronic address: srik@rri.res.in

classical and quantum shares based on the idea of information dilution. This generalizes the idea of conventional single-threshold QSS schemes and is again shown to lead to savings of quantum players.

II. HYBRIDIZING QUANTUM SECRET-SHARING SCHEMES

The essential method to hybridize (i.e., to introduce classical shares into) QSS is to somehow incorporate classical information that is needed to decrypt or prepare the quantum secret as classical shares. Use of classical shares can sometimes obviate and thus lead to savings in quantum shares, or, at any rate, quantum players. A simple instance of such classical information is the ordering information of the shares. In QTS, it is implicity assumed that the shareholders know the coordinates of the shares in the secret, i.e., they know who is holding the first qubit, who the second, and so on. This ordering information is necessary to reconstruct the secret, without which successful reconstruction of the secret is not guaranteed. If we wish to make use of this ordering information in the above sense, then only quantum-error-correction-based secret sharing, where lack of ordering information leads to maximal ignorance, can be used. In particular, the scheme should be sensitive to the interchange of two or more qubits. For example, let us consider a (2,3) QTS. The secret here is an arbitrary qutrit and the encoding maps the secret qutrit to three qutrits as

$$\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \mapsto \alpha(|000\rangle + |111\rangle + |222\rangle) + \beta(|012\rangle + |120\rangle + |201\rangle) + \gamma(|021\rangle + |210\rangle + |102\rangle), \tag{1}$$

and each qutrit is taken as a share. While from a single share no information can be obtained, two shares, with ordering information, suffice to reconstruct the encoded state [8]. However, the lack of ordering information does not always lead to maximal ignorance about the secret. Note that the structure of the above code is such that any interchange of two qubits leaves an encoded $|0\rangle$ intact but interchanges $|1\rangle$ and $|2\rangle$. Thus, a secret like $|0\rangle$ or $(1/\sqrt{2})(|1\rangle+|2\rangle)$ can be entirely reconstructed without the ordering information. Therefore, only the subset of quantum error correction codes admissible in QSS that do not possess such symmetry properties can be used if the scheme is to be sensitive to ordering information.

Another scheme relevant here is due to Nascimento *et al.* [19], based on qubit encryption [23]. We adopt this method to generate the relevant encrypting classical information. However, in principle any classical data whose suppression leads to maximal ignorance of the secret are also good. Elsewhere, in Sec. V, we consider another way. Quantum encryption works as follows. Suppose we have an n-qubit quantum state $|\psi\rangle$ and random sequence K of $2n$ classical bits. Each sequential pair of classical bits is associated with a qubit and determines which transformation $\hat{\sigma}\in\{\hat{I},\hat{\sigma}_x,\hat{\sigma}_y,\hat{\sigma}_z\}$ is applied to the respective qubit. If the pair is 00, $\hat{I}$ is applied, if it is 01, $\hat{\sigma}_x$ is applied, and so on. To one not knowing K, the resulting $|\tilde{\psi}\rangle$ is a complete mixture and no information can be extracted out of it because the encryption leaves any pure state in a maximally mixed state, that is, $(1/4)(\hat{I}|S\rangle\langle S|\hat{I} + \hat{\sigma}_x|S\rangle\langle S|\hat{\sigma}_x + \hat{\sigma}_y|S\rangle\langle S|\hat{\sigma}_y + \hat{\sigma}_z|S\rangle\langle S|\hat{\sigma}_z) = (1/2)\hat{I}$. However, with knowledge of K the sequence of operations can be reversed and $|\psi\rangle$ recovered. Therefore, classical data can be used to encrypt quantum data. In general, given d-dimensional objects, quantum encryption requires d^2 operators and a key of $2\log(d)$ bits per object to randomize perfectly. In practice, such quantum operations may prove costly, and only near-perfect security may be sufficient. In this case, there exists a set of roughly $d\log(d)$ unitary operators whose average effect on every input pure state is almost perfectly randomizing, so that the size of the key can be reduced by about a factor of 2 [10,24].

III. COMPRESSING QUANTUM SECRET-SHARING SCHEMES

In hybrid QSS, the quantum secret is split up into quantum and classical shares of information. We call the former q-shares, and the latter c-shares. A player holding only c-shares is called a c-player or c-member. Otherwise, she or he is a q-player or q-member.

Definition 1. A QSS scheme realizing an access structure $\Gamma=\{\alpha_1,\alpha_2,\ldots,\alpha_r\}$ among a set of players $\mathcal{P}=\{P_1,P_2,\ldots,P_n\}$ is said to be compressible if fewer than n q-players are sufficient to implement it.

Here the α_i's are the minimal authorized sets of players. Knowledge of compressibility helps us decide how to minimize valuable quantum resources needed for implementing a given QSS scheme. As an example of compression by means of hybrid QSS, suppose we want to split a quantum secret $|S\rangle$ among a set of players $\mathcal{P}=\{A,B,C,D,E,F\}$ realizing the access structure $\Gamma=\{ABC,AD,AEF\}$. That is, the only sets authorized to reconstruct the secret are $\{A,B,C\}$, $\{A,D\}$, and $\{A,E,F\}$ and sets containing them, while any other set is unauthorized to do so. For distributing the secret, we encrypt $|S\rangle$ using the quantum encryption method (described above) with classical key K into a new state $|\tilde{S}\rangle$ and give $|\tilde{S}\rangle$ to A. We then split up K using a CSS scheme that realizes Γ. Player A cannot recover $|S\rangle$ from $|\tilde{S}\rangle$ because he cannot unscramble it without K. Only the α_j's, and sets containing them, can recover the classical key K, and thence decrypt the secret state. In this way, by means of a hybrid (classical-quantum) secret-sharing scheme, we can compress the original QSS scheme into an equivalent one in which fewer players need to handle quantum information.

We use the notation of single parentheses (double parantheses) to indicate a CTS (a QTS). In a conventional $((k,n))$ scheme, a compression is known to be possible if $2k>n+1$, in which case, the scheme can be compressed into a $((k-\gamma,n-\gamma))$ scheme combined with a (k,n) scheme, where $\gamma\equiv 2k-n-1$ [18]. A general access structure $\Gamma=\{\alpha_1,\alpha_2,\ldots,\alpha_r\}$ can be realized by a first layer of a $(1,r)$-threshold scheme. In the quantum case, since this violates the no-cloning theorem, it is replaced by the majority function $((r,2r-1))$ scheme [13]. This, again, is incompressible. However, in the second layer of the construction, the $((|\alpha_i|,|\alpha_i|))$ schemes can be replaced with a ((1,1)) scheme combined with $(|\alpha_i|,|\alpha_i|)$ schemes [19].

In the above, the degree of compression is determined by $\Gamma=\{\alpha_1,\ldots,\alpha_r\}$ and the requirement to minimize q-players, *no matter who they are*. This can be distorted if the information-processing capabilities of individual players are known to be different. In particular, suppose we are given a set $\mathbb{Q}$, such that players from this set are able to process quantum information reliably. The set of remaining players $\bar{\mathbb{Q}}=\mathcal{P}-\mathbb{Q}$ are best designated to be c-players. A "hitting set" $\mathcal{H}(\Gamma)$ for the collection of sets Γ is a set of players such that $\mathcal{H}\cap\alpha_i\neq\emptyset\,\forall\, i(1\leqslant i\leqslant r)$. Let $\mathcal{M}(\Gamma)$ be the smallest hitting set for Γ such that $\mathcal{M}(\Gamma)\subset\mathbb{Q}$. $\mathcal{M}(\Gamma)$ may or may not be unique. We denote $M\equiv|\mathcal{M}(\Gamma)|$. Under compression, only M q-players are needed. First a majority function $((r,2r-1))$ is employed, r of the shares being encrypted and deposited with the M q-players. In the second layer of the construction, the $((|\alpha_i|,|\alpha_i|))$ schemes can be compressed to ((1,1)) schemes combined with $(|\alpha_i|,|\alpha_i|)$ schemes, the q-shares of each α_i being deposited with the respective q-player. The remaining $M-1$ shares are split-shared according to a maximal scheme that contains Γ. The maximal scheme is obtained by adding authorized sets to Γ until authorized and unauthorized sets form exact complements [13]. Thus we require only $M\leqslant|\mathcal{P}|$ q-players to implement the protocol, which represents a compression by $|\mathcal{P}|-M$ q-players. We note that if $\mathcal{M}(\Gamma)=\emptyset$, then compression is impossible. We can observe that for a general access structure involving a large number of players, computing $\mathcal{M}$ is a provably hard problem (in fact its decision version can be shown to be *NP*-complete [25,26]).

As an example, let us consider the access structure $\Gamma=\{ABCD,ADF,CDE\}$ among six players $\mathcal{P}=\{A,B,C,D,E,F\}$. Suppose $\mathbb{Q}=\{A,C,E\}$. We can choose $\mathcal{M}=\{A,C\}$ or $\mathcal{M}=\{A,E\}$, representing the two required q-players (instead of six q-players, required in the uncompressed version). Suppose we choose the latter. The first layer will employ a (3,5) QTS to split secret $|S\rangle$. At the second layer, the shares on the top two rows are encrypted using K_1, K_2 and given to A, the last using K_3 and given to E. The K_j's are classically shared on each row, though the q-shares remains with A or E. The last share $|S'\rangle$ is shared using a pure state scheme that implements $\Gamma_{\max}$, the maximal scheme obtained from Γ. The resultant q-shares for each authorized set α_j are deposited with $\alpha_j\cap\mathcal{M}(\Gamma)$. This scheme is depicted in Eq. (2):

$$((3,5))\begin{cases} A & \to(4,4){:}A,B,C,D,\\ A & \to(3,3){:}A,D,F,\\ E & \to(3,3){:}C,D,E,\\ |S'\rangle. & \end{cases} \tag{2}$$

We note that if $D\in\mathbb{Q}$ then $\mathcal{M}(\Gamma)=\{D\}$, and only one q-player, namely, D, would have sufficed to implement compression. And if $\mathbb{Q}=\{E,F\}$, then $\mathcal{M}=\emptyset$ because there is an authorized set with no q-player. Hence no compression would be possible.

IV. INFLATING QUANTUM SECRET SHARING SCHEMES

The question of how to augment or "inflate" a given QSS scheme keeping the quantum component fixed is considered below. This is of practical relevance if we wish to expand a given QSS scheme by including new players who do not have (reliable) quantum information processing capacity. To this end, we now define an inflatable QSS.

Definition 2. A QSS (Γ) scheme realizing an access structure $\Gamma=\{\alpha_1,\alpha_2,\ldots,\alpha_r\}$ among a set of players $\mathcal{P}=\{P_1,P_2,\ldots,P_n\}$ is inflatable if n can be increased for fixed number of q-players to form a new QSS (Γ') such that $\Gamma'|_{\mathcal{P}}=\Gamma$, where $\Gamma'|_{\mathcal{P}}$ denotes the restriction of Γ' to $\mathcal{P}$.

Clearly, inflation involves the addition of classical-information-carrying c-players. The additional shares required for them will be c-shares, so that q-shares may remain fixed at m. The following theorem answers the question when a QSS scheme can be inflated.

Theorem 1. A QSS scheme realizing an access structure $\Gamma=\{\alpha_1,\alpha_2,\ldots,\alpha_r\}$ among a set of players $\mathcal{P}=\{P_1,P_2,\ldots,P_n\}$ can always be inflated.

Proof. Consider the addition of m new players $P_{n+1},\ldots,P_{n+m}$, where $m\geqslant 1$. The new set of all players are $\mathcal{P}'\equiv\{P_1,P_2,\ldots,P_{n+m}\}$. A new access structure $\Gamma'=\{\alpha_1',\ldots,\alpha_r'\}$ can be obtained by arbitrarily adding the new players to any of the α_j's. Clearly, Γ' will not violate the no-cloning theorem, since Γ does not. The secret $|S\rangle$ is encrypted using classical string K to obtain $|\tilde{S}\rangle$. This encrypted secret is split-shared according to the original scheme implementing Γ, while K is split-shared among all $n+m$ players according to the classical scheme implementing Γ'. To reconstruct the secret, members of any α_j' combine the q-shares of $\alpha_j\subseteq\alpha_j'$ to reconstruct $|\tilde{S}\rangle$, and the c-shares with all members of α_j' to reconstruct K, using which the encrypted secret $|\tilde{S}\rangle$ is decrypted to $|S\rangle$. The new scheme is such that $\Gamma=\Gamma'|_{\mathcal{P}}$ and $\mathcal{P}'-\mathcal{P}$ are c-players. Therefore, the new scheme QSS(Γ') is an inflation of the given scheme QSS(Γ). ■

The above theorem only says that any QSS scheme can be inflated in *some* way. A specific problem is whether a given (k,n) QTS can be inflated to another QTS. This is considered in the following theorem and corollary.

Theorem 2. A (k,n) QTS can be inflated only conformally, i.e., to threshold schemes having the form $(k+\gamma,n+\gamma)$, where γ $(\geqslant 0)$ is an integer.

Proof. If the given (k,n) QTS satisfies the no-cloning theorem, then clearly so will the $(k+\gamma_k,n+\gamma_n)$ QTS, where $\gamma_k\geqslant\gamma_n\geqslant 0$ and $k+\gamma_k\leqslant n+\gamma_n$. Further, according to Lemma 1 of Ref. [19], a restriction of the $(k+\gamma_k,n+\gamma_n)$ QTS by γ players necessarily yields a conformally reduced, $(k+\gamma_k-\gamma,n+\gamma_n-\gamma)$ QTS. The restricted scheme has a different access structure from (k,n) QTS unless $\gamma_k=\gamma_n=\gamma$. Therefore, only a conformal inflation of (k,n) QTS is possible, whereby it is inflated to a $(k+\gamma,n+\gamma)$ QTS by the addition of γ c-players. ■

In an implementation of Theorem 2, the quantum secret $|S\rangle$ is encrypted to $|\tilde{S}\rangle$ using a classical string K which is split-shared among all $n+\gamma$ players according to a $(k+\gamma,n+\gamma)$ CTS. State $|\tilde{S}\rangle$ is then quantally split-shared among the n q-players according to a (k,n) QTS. As a consequence of Theorem 2, we have the following negative result.

Corollary 1. A (k,n) QTS cannot be inflated at constant threshold. ■

V. TWIN-THRESHOLD QUANTUM SECRET SHARING SCHEMES

In a conventional or compressed (k,n) QTS, the threshold k applies to all members taken together. Now suppose that we have *separate* thresholds for c-members and q-members, namely, k_c and k_q, with $k=k_c+k_q$. We now extend the definition of a conventional QTS to a (k_c,k_q,n) *quantum twin-threshold scheme* (Q2TS) and a $(k_c,k_q,n,\mathbb{C})$ *quantum twin-threshold scheme with common set* (Q2TS+C), where a quantum secret $|S\rangle$ is split into n pieces (shares) according to some preagreed procedure and distributed among n players. These n shareholders consist of members of set $\mathbb{Q}$ of q-players and set $\overline{\mathbb{Q}}$ of c-players. We denote $q\equiv|\mathbb{Q}|$, so that $|\overline{\mathbb{Q}}|=n-q$. Obviously, in a quantum scheme, $\mathbb{Q}\neq\varnothing$.

Definition 3. A QSS scheme is a (k_c,k_q,n) quantum twin-threshold scheme among n players, of which q are q-players and the remaining are c-players, if at least k_c c-players and at least k_q q-players are necessary to reconstruct the secret.

Definition 4. A QSS scheme is a $(k_c,k_q,n,\mathbb{C})$ quantum twin-threshold scheme with common set among n players, of which q are q-players and the remaining are c-players, if: (a) at least k_c c-players and at least k_q q-players are necessary to reconstruct the secret; (b) all members of the set $\mathbb{C}$ are necessary to reconstruct the secret.

The idea behind distinguishing between the classical threshold k_c and the quantum threshold k_q is to obtain a simple generalization that combines the properties of the CTS and QTS. Practically speaking, it is best to minimize k_q, at fixed k. However, one can in principle consider situations of potential use for a twin-threshold scheme, when a sufficiently large number of members are able to process quantum information safely. Further, some of the shareholders, while not entirely trustworthy, may yet be more trustworthy than others. The share dealer (say Alice) may prefer to include all such shareholders during any reconstruction of the secret. This is the requirement that motivates the introduction of set $\mathbb{C}$. In general, $\mathbb{C}$ can contain members drawn from $\mathbb{Q}$ and/or $\overline{\mathbb{Q}}$ or may be a null set. By definition, Q2TS+C with $\mathbb{C}=\varnothing$ is Q2TS.

In the following sections we present two methods to realize in varying degrees the generalized quantum secret splitting scheme. The first of these is the general version of Q2TS+C. The second, while more restricted, is interesting because it is not directly based on quantum erasure correction, but on information dilution via homogenization, in contrast to current proposals of QSS.

A. Quantum error correction and quantum encryption

We now give protocols that realizes the twin-threshold scheme based on quantum encryption.

Scheme 1. Protocol to realize (k_c,k_q,n) Q2TS.

Distribution phase. (1) Choose a random classical encryption K. Encrypt the quantum secret $|S\rangle$ using the encryption algorithm described in Sec. I. The encrypted state is denoted $|\tilde{S}\rangle$. (2) Using a conventional (k_q,q) QTS, split-share $|\tilde{S}\rangle$ among the members of $\mathbb{Q}$; to not violate no-cloning, q should satisfy $k_q>(q/2)$. (3) Using a $(k_c,n-q)$ CTS, split-share K among the members of $\overline{\mathbb{Q}}$.

Reconstruction phase. (1) Collect any k_q q-shares from members of $\mathbb{Q}$ and reconstruct $|\tilde{S}\rangle$. (2) Collect any k_c shares from members of $\overline{\mathbb{Q}}$ and reconstruct K. (3) Reconstruct $|S\rangle$ using $|\tilde{S}\rangle$ and K.

Now consider the case $\mathbb{C}\neq\varnothing$ and the Q2TS scheme becomes the more general Q2TS+C scheme. We now give a protocol that realizes this more general twin-threshold scheme. We denote $\lambda_q\equiv|\mathbb{Q}\cap\mathbb{C}|$ and $\lambda_c\equiv|\overline{\mathbb{Q}}\cap\mathbb{C}|$. Clearly, $\lambda_c+\lambda_q=|\mathbb{C}|$. If there are no q-players in $\mathbb{C}$, set $\lambda_q=0$, and if there are no c-players in $\mathbb{C}$, set $\lambda_c=0$. Note that by definition, q-players may also carry classical information, but c-players do not carry quantum information.

Scheme 2. Protocol to realize $(k_c,k_q,n,\mathbb{C})$-Q2TS+C.

Distribution phase. (1) Choose a random classical encryption K. Encrypt the quantum secret $|S\rangle$ using the encryption algorithm described in Sec. I. The encrypted state is denoted $|\tilde{S}\rangle$. (2) Using a (2, 2) QTS, divide $|\tilde{S}\rangle$ into two pieces, say $|\tilde{S}_1\rangle$ and $|\tilde{S}_2\rangle$. (3) Using a (λ_q,λ_q) QTS, split $|\tilde{S}_1\rangle$ among the q-members in $\mathbb{C}$. (4) Using a conventional $(k_q-\lambda_q,q-\lambda_q)$ QTS, split $|\tilde{S}_2\rangle$ among the q-members not in $\mathbb{C}$; to not violate no-cloning, q should satisfy $(k_q-\lambda_q)>(q-\lambda_q)/2$. (5) Using a (2,2) CTS, divide K into two shares, say K_1 and K_2. (6) Part K_1 is split among the members of $\mathbb{C}$ using a $(|\mathbb{C}|,|\mathbb{C}|)$ CTS. Alternatively, it can be split using a (λ_c,λ_c) CTS among the c-players in $\mathbb{C}$. (7) Using a $(k_c-\lambda_c,n-q-\lambda_c)$ CTS, split K_2 among the members of $\overline{\mathbb{Q}}-\mathbb{C}$.

Reconstruction phase. (1) Collect all λ_q shares from all members of $\mathbb{Q}\cap\mathbb{C}$ and reconstruct $|\tilde{S}_1\rangle$. (2) Collect any $k_q-\lambda_q$ q-shares from $\mathbb{Q}-\mathbb{C}$ to reconstruct $|\tilde{S}_2\rangle$. (3) Combining $|\tilde{S}_1\rangle$ and $|\tilde{S}_2\rangle$, reconstruct $|\tilde{S}\rangle$. (4) Collect all $|\mathbb{C}|$ c-shares from members of $\mathbb{C}$ and reconstruct K_1. Alternatively, collect all λ_c c-shares from members of $\overline{\mathbb{Q}}\cap\mathbb{C}$ and reconstruct K_1. (5) Collect any $k_c-\lambda_c$ shares from $\overline{\mathbb{Q}}-\mathbb{C}$ and reconstruct K_2. (6) Combining K_1 and K_2, reconstruct K. (7) Reconstruct $|S\rangle$ using $|\tilde{S}\rangle$ and K.

B. Quantum twin-threshold scheme based on information dilution via homogenization

The second, more restrictive scheme, is based on the procedure for information dilution in a system-reservoir interaction, proposed by Ziman *et al.* [27]. The novelty of the scheme lies in the fact that it is not directly based on a quantum error-correction code. However, it is applicable only to QSS with $\mathbb{C} \neq \emptyset$. Reference [27] presents a *universal quantum homogenizer*, a machine that takes as input a system qubit initially in the state ρ and a set of N reservoir qubits initially prepared in the identical state ξ. In the homogenizer the system qubit sequentially interacts with the reservoir qubits via the partial swap operation so that the initial state $\rho_S^{(0)}$ of the system, after interacting with the N reservoir qubits, becomes

$$\rho^{(N)} = \mathrm{Tr}_R[U_N \cdots U_1(\rho_S^{(0)} \otimes \xi^{\otimes N})U_1^{\dagger} \cdots U_N^{\dagger}] \tag{3}$$

where $U_k \equiv U \otimes (\otimes_{j \neq k} \mathbb{I}_j)$ describes the interaction between the kth qubit of the reservoir and the system qubit. The homogenizer realizes, in the limit sense, the transformation such that at the output each qubit is in an arbitrarily small neighborhood of the state ξ irrespective of the initial states of the system and the reservoir qubits. Formally,

$$D(\rho_S^{(N)}, \xi) \leqslant \delta, \quad \forall\, N \geqslant N_\delta, \tag{4a}$$

$$D(\xi_k', \xi) \leqslant \delta, \quad \forall\, 1 \leqslant k \leqslant N, \tag{4b}$$

where $D(\cdot\,,\cdot)$ denotes some distance (e.g., a trace norm) between the states, $\delta > 0$ is a small parameter chosen a *priori*, and $\xi_k' \equiv \mathrm{Tr}_S[U\rho_S^{(k-1)} \otimes \xi U^{\dagger}]$.

The interaction between a reservoir qubit and the system qubit is given by the partial swap operation $P(\eta) = (\cos\eta)\mathbb{I} + i(\sin\eta)S$, where S, the *swap* operator acting on the state of two qubits, is defined by $S|\psi\rangle \otimes |\phi\rangle = |\phi\rangle \otimes |\psi\rangle$. It can be shown that η can be chosen to enforce Eq. (4a) according to the relation

$$\sin\eta \leqslant \sqrt{\delta/2}. \tag{5}$$

Thus the information contained in the unknown system state is distributed in the correlations among the system and the reservoir qubits, whose marginal states are close to ξ. As the authors point out, this process can be used as a *quantum safe with a classical combination*.

Now we show how this particular feature can be turned into a special case of the $(k_c, k_q, n, \mathbb{C})$ threshold scheme, subject to the restriction that $\mathbb{Q} \subseteq \mathbb{C}$, so that $k_q = q$, i.e., all q-players must be present to reconstruct the secret. The homogenization is reversible and the original state of the system and the reservoir qubits can be unwound. Perfect unwinding can be performed only when the system particle is correctly identified from among the $N+1$ output qubits, and it and the reservoir qubits interact via the inverse of the original partial swap operation. Therefore, in order to unwind the homogenized system, the classical information (denoted K) about the sequence of the qubit interactions is essential. Now, of the $(N+1)!$ possible orderings, only one will reverse the original process. The probability to choose the system qubit correctly is $1/(N+1)$. Even when the particle is chosen successfully, there are still $N!$ different possibilities in choosing the sequence of interaction with the reservoir qubits. Thus, without the knowledge of the correct ordering, the probability of successfully unwinding the homogenization transformation is $1/((N+1)!)$, which is exponentially small in N. Moreover, a particular order of trial unwinding and measurement will irrecoverably destroy the system. This is demonstrated in Figs. 4 and 5 of Ref. [27], where various wrong permutations of the ordering, chosen by trial-and-error strategy, are shown not to reproduce the state. So, for a sufficiently large value of N, no information about the system qubit can be deduced without this classical information. Nevertheless, it is worth noting that the above computational argument, while rendering security of the homogenizing procedure intuitively understandable and highly plausible, does not rigorously prove it, even in the $N \to \infty$ limit.

A secondary wall of security is provided by the smallness of δ. It is useful if players already have knowledge of ξ. In this case, because of conditions (4a), the homogenized state of the system or reservoir qubit cannot be distinguished from ξ.

If K is split up among the q members holding the system and reservoir qubits according to a (q, q) CTS, it is easy to observe that this realizes a (q, q) QTS not based directly on a quantum error-correction code. In terms of the generalized definition, this corresponds to a $(k_c, k_q, n, \mathbb{C})$ scheme in which $k_c = 0$, $\mathbb{Q} = \mathbb{C}$, and $n = k_q = q$. The classical layer of information sharing is necessary in order to strictly enforce the threshold: if prior ordering information were openly available, then, for example, the last $q-1$ participants could collude to obtain a state close to ρ. We now present the most general twin-threshold scheme possible based on homogenization. It will still be more restricted than that obtained via quantum encryption, requiring that $\mathbb{Q} \subseteq \mathbb{C}$, so that $k_q = q$. If n is not too large, it is preferable for prevention of partial information leakage to choose the number N of reservoir qubits such that $N \gg n$. The general protocol is executed recursively as follows.

Scheme 3. Protocol to realize a restricted $(k_c, k_q, n, \mathbb{C})$ Q2TS+C, with $k_q = q \leqslant n$. Alice takes N ($\geqslant 1$) reservoir qubits, where $N+1 = \Sigma_i m_i$ and integers $m_i \geqslant 1$ ($\forall i, 1 \leqslant i \leqslant n$), and performs the process of homogenization to obtain states $\xi_0, \xi_1, \ldots, \xi_N$ on the system qubit and the N reservoir qubits.

Distribution phase. (1) Any m_i qubits from $N+1$ qubits are given to the ith member of $\mathbb{Q}$. (2) K is divided into two parts, K_1 and K_2, according to a (2,2) CTS. (3) Let $\lambda_c \equiv |\overline{\mathbb{Q}} \cap \mathbb{C}| \geqslant 0$. K_1 is further split among the members of $\mathbb{Q}$ and $\overline{\mathbb{Q}} \cap \mathbb{C}$ using a $(q+\lambda_c, q+\lambda_c)$ CTS. (4) K_2 is split among the members of $\overline{\mathbb{Q}} - \mathbb{C}$ using a $(k_c - \lambda_c, n - q - \lambda_c)$ CTS.

Reconstruction phase. (1) Collect all q-shares from members of $\mathbb{Q}$. (2) Collect all $|\mathbb{C}|$ c-shares from members of $\mathbb{C}$ and reconstruct K_1. (3) Collect any $k_c - \lambda_c$ shares from members of $\overline{\mathbb{Q}} - \mathbb{C}$ to reconstruct K_2. (4) Using K_1 and K_2, reconstruct K. (5) Using the q-shares and K, unwind the system state to restore the secret $|S\rangle$.

ACKNOWLEDGMENTS

We are grateful to Dr. Mueller-Quade for pointing out an important reference. We thank Professor Anil Kumar, Professor J. Pasupathy, and Ranabir Das for discussions. S.K.S. thanks Professor Anil Kumar for enabling his visit to IISc during which this work was done. R.S.'s work, begun at the Center for Theoretical Studies, was partially supported by DRDO Project No. 510 01PS-00356.

[1] B. Schneier, *Applied Cryptography* (Wiley, New York, 1996), p. 70.
[2] J. Gruska, *Foundations of Computing* (Thomson Computer Press, London, 1997), p. 504.
[3] G. Blakely, in Proc. National Comp. Conf., New York, New York, June 4–7, 1979 (AFIPS Press, Arlington, VA, 1979), Vol. 48, p. 313.
[4] A. Shamir, Commun. ACM **22**, 612 (1979).
[5] J. Benaloh and J. Leichter, Lect. Notes Comput. Sci. **403**, 27 (1990).
[6] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[7] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[8] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[9] W. K. Wooters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[10] H. Imai, J. Mueller-Quade, A. C. A. Nascimento, P. Tuyls, and A. Winter, e-print quant-ph/0311136.
[11] S. Calderbank and P. Shor, Phys. Rev. A **54**, 1098 (1996).
[12] M. Grassl, T. Beth, and T. Pellizzari, Phys. Rev. A **56**, 33 (1997).
[13] D. Gottesman, e-print quant-ph/9910067.
[14] A. Smith, e-print quant-ph/0001087.
[15] S. Wiesner, SIGACT News **15**, 78 (1983).
[16] C. Crépeau, D. Gottesman, and A. Smith, in Proceedings of the 34th Annual ACM Symposium on the Theory of Computing, 2002 (unpublished).
[17] A. M. Lance, T. Symul, W. P. Bowen, T. Tyc, B. C. Sanders, and P. K. Lam New J. Phys. **5**, 4.1 (2003).
[18] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
[19] A. C. A. Nascimento, J. Mueller-Quade, and H. Imai, Phys. Rev. A **64**, 042311 (2001).
[20] A. Herzberg, S. Jarecki, H. Krawszyk, and M. Yung, Lect. Notes Comput. Sci. **963**, 339 (1996).
[21] A. Beltelspacher, *Lecture Notes in Computer Science* (Springer-Verlag, Berlin, 1990), pp. 491–496.
[22] K. M. Martin, in *Cryptography and Coding III*, edited by M. J. Gandley (Clarendon Press, Oxford, 1993), pp. 255–264.
[23] M. Mosca, A. Tapp, and R. de Wolf, e-print quant-ph/0003101.
[24] P. Hayden, D. Leung, P. W. Shor, and A. Winter, e-print quant-ph/0307104.
[25] R. M. Karp, *Complexity of Computer Computations*, in Procedings of the Symposium at IBM Thomas J. Watson Research Center, Yorktown Heights, NY, 1972 (Plenum, New York, 1972), pp. 85–103.
[26] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP Completeness* (W. H. Freeman and Company, San Francisco, 1979).
[27] M. Ziman, P. Štelmachovič, V. Bužek, M. Hillery, V. Scarani, and N. Gisin, Phys. Rev. A **65**, 042105 (2002).