9-17-2001

Improving Quantum Secret-Sharing Schemes

Anderson C. Nascimento
University of Washington Tacoma, andclay@uw.edu

Joern Mueller-Quade

Hideki Imai

Improving quantum secret-sharing schemes

Anderson C. A. Nascimento, Joern Mueller-Quade, and Hideki Imai
Third Department, Institute of Industrial Science, The University of Tokyo, Tokyo 153-8505, Japan
(Received 21 February 2001; published 17 September 2001)

We propose a protocol that enables a dealer to share a quantum secret with n players using less than n quantum shares for several access structures. For threshold schemes we derived an expression that shows how many quantum shares can be saved in this scheme. Also, several features that are available for classical secret-sharing schemes (and previously not known to be possible for quantum secret-sharing) become available with this protocol.

DOI: 10.1103/PhysRevA.64.042311 PACS number(s): 03.67.Dd

I. INTRODUCTION

Secret-sharing schemes were independently introduced by Shamir [1] and Blakley [2] in 1979. They are fundamental building blocks of multiparty computation protocols [3], unconditionally secure key distribution [4], digital signature schemes [5], as well as of key management schemes [6]. In a classical secret-sharing scheme, a dealer shares a secret by distributing pieces of information among a set of players in a way, that only authorized subsets of the players' set will be able to recover the secret. Recently, this concept was generalized to the quantum scenario. In [7] Hillery *et al.* proposed a scheme where an unknown qubit can be shared with two players, such that to recover the original qubit the players have to put their pieces of quantum information together. In [8] Cleve, Gottesman, and Lo presented a more general scheme where a dealer can share an unknown quantum state with a set of players in a way that only authorized groups of players can recover the original secret and collusions of unauthorized players cannot get any information about it. The construction in [8] was based on quantum error-correcting codes. A construction for general access structures based on monotone span programs was presented in [9] by Smith.

Differently than quantum key exchange and other quantum cryptographic protocols such as quantum bit commitment, the main aim of quantum secret sharing is not to achieve a level of security that is impossible in the classical world. Rather, the aim is to share a different kind of data: an unknown quantum state. If quantum computers become a reality, quantum secret sharing could possibly play an important role in distributed quantum secure computations.

In classical secure multiparty computations, several computers interconnected by a network want to compute the value of a function, which depends on secret inputs of all the players. Some users might collude to cheat in the protocol as to obtain information about the secret inputs of other players or to modify the result of the computation. In a quantum version of a secure multiparty computation, a group of users would like to compute a quantum state by inputting quantum as well as classical data in a way that no allowed collusion of cheaters can get any information about the inputs of other players or alter the result of the computation.

A fundamental issue when dealing with secret-sharing schemes is the amount of data that must be given to the set of players. The smaller the amount of data given to the set of players the better. This issue becomes even more important when dealing with quantum secret sharing. As quantum data is expansive and hard to deal with, it would be desirable to use as little quantum data as possible in order to share an unknown quantum state. In this paper we show that quantum data and classical data can be used together in a hybrid quantum secret-sharing scheme in order to reduce the amount of quantum data that has to be distributed to the players. As classical data is much easier to store, transmit, and receive, this result significantly improves the viability of quantum secret-sharing schemes.

It is interesting to note that, in this case, classical data help one to perform a completely quantum task. This is not the case with data compression [10] or with the quantum capacity of a quantum channel [11]. In [11] Adami and Cerf proved that a classical forward channel connecting two parties cannot increase the capacity of a quantum channel between them. In [10] Barnum *et al.* proved that no part of the quantum-information content of a quantum source can be faithfully replaced by classical information.

This paper is organized as follows. In Sec. II we introduce our notations and give some preliminaries. In Sec. III we state our main results and in Sec. IV we introduce features of quantum secret-sharing schemes that become available with our results. Finally, in Sec. V we give our conclusions.

II. PRELIMINARIES

A. Classical secret-sharing schemes

As stated in Sec. I, a secret-sharing scheme is a protocol that enables a dealer $\mathcal{D}$ to share a secret S with a set of players $\mathcal{P}$ so that the members of an authorized group will be able to recover S, but no other members can get any information about the secret S. The authorized groups will be defined by an access structure Γ, a family where each element is an authorized group. The secret-sharing scheme will be called *perfect* if (1) each set listed in Γ can recover the secret S with absolute certainty, and (2) none of the subsets not listed in Γ can get any information about the secret S.

When $|\mathcal{P}|=w$ and $\Gamma=\{B\subseteq\mathcal{P}:|B|\geqslant t\}$ we say we have a (t,w)-threshold scheme.

B. Quantum error-correction codes and quantum secret sharing

In [8] Cleve, Gottesman, and Lo introduced the notion of quantum threshold schemes. It was based on quantum erasure correction [12–15]. In an $[n,k]$ quantum error-correcting code, a quantum state $|X\rangle \in \mathcal{H}^k$ (where $\mathcal{H}^k$ is the k-dimensional Hilbert space) is associated with another vector $|\psi\rangle \in \mathcal{H}^n$ called a codeword, where $n \geqslant k$. The set of all codewords is a linear subspace $\mathcal{X} \subseteq \mathcal{H}^n$ with dim $\mathcal{X}=k$. Let U be a unitary transformation that represents the action of the environment introducing errors in a quantum state $|\phi\rangle \in \mathcal{H}^n$. If these errors are local errors, the action of this unitary operator U on the quantum state $|\phi\rangle \in \mathcal{H}^n$ can be expanded in terms of $\{I,X,Y,Z\}^{\otimes n}$, where X,Y and Z are the three Pauli operators.

Therefore, we have that in $\mathcal{H}^n$ the errors can be represented by tensor-products operators, $E_\alpha = \otimes_{1 \leqslant j \leqslant n} \alpha_j$, where $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_n)$, $\alpha_j \in \{I,X,Y,Z\}$. The number of $\alpha_j \neq I$ in a word α will denote the weight of α and will be represented by $w(\alpha)$. A quantum code $\mathcal{X}$ is called E-error correcting if $\forall\ \alpha,\beta$ with $w(\alpha),w(\beta) \leqslant E$ and for $\forall\, \phi,\psi \in \mathcal{X}$,

$$\langle \psi E_\alpha | E_\beta \phi \rangle = \langle \psi | E_\alpha E_\beta | \phi \rangle = b_{\alpha,\beta} \langle \psi | \phi \rangle, \quad b_{\alpha,\beta} \in \mathbb{C}$$

if additionally, $b_{\alpha,\beta}=0$, unless $\alpha=\beta$, the code is said to be nondegenerate. It is important to remark that α and β are independent of $\langle \psi|\phi\rangle$. It is a well-known result that an E-error-correcting quantum code can correct $2E$ erasures.

The minimum distance of a code can be defined as the minimum number of undetected errors. An $[n,k]$ code with minimum distance d is referred as an $[n,k,d]$ code. Cleve, Gottesman, and Lo exploited the fact that if we trace over any $n-t$ subset of qubits of a codeword $|\psi\rangle \in \mathcal{H}^n$ in an $[n,k,d]$ code with $d=t-1$, we have that

$$\rho^{(t)} = \mathrm{tr}_{(n-t)} |\psi\rangle\langle\psi| = \frac{1}{2^t} I$$

is the complete mixture. Therefore, by measuring any subset of dimension smaller or equal to $t-1$, it is impossible to get any information about the complete state $|\psi\rangle$. This is a consequence of the fact that any information extracted out of a quantum state implies disturbance of the state. Therefore, if we want to protect a quantum state composed of n qubits from errors in any subset of k qubits, we have to ensure that any measurement performed (maybe by the environment) on any subset of k qubits will get no information about the state. It follows that in order to implement a (t,w) quantum threshold secret-sharing scheme, we must have a $[2t-1,1,t]$ quantum code [8].

It is interesting to note that not all access structures can be implemented by quantum secret-sharing schemes. This restriction comes from the no-cloning theorem [16]. This theorem states that it is impossible to clone with perfect fidelity an unknown quantum state. Therefore, any access structure that has two disjoints subsets cannot be implemented. In another paper [17], Gottesman generalized the results obtained for threshold schemes to general access structures. It was stated in [17] that in a quantum secret-sharing scheme, the size of the shares must be at least that of the secret to be shared and all the important players must receive one quantum share.

C. Encryption of qubits

In the next section we show how to overcome this limitation by use of an interesting tool proposed in [18]: the encryption of quantum bits, which is briefly reviewed in this section. The encryption scheme works as follows: suppose we have a quantum state $|\psi\rangle$ composed of n qubits and a random sequence of $2n$ classical bits, each pair of classical bits is associated with a qubit and it determines which transformation $\sigma \in \{I,X,Y,Z\}$ is applied to the respective qubit. If the pair is 00, I is applied, if it is 01, X is applied, and so on. It is easy to see that if σ is chosen at random from $\{I,X,Y,Z\}$ the resulting state $|\tilde{\psi}\rangle$ is the complete mixture and no information can be extracted out of it. However, if someone knows the classical sequence of bits, the sequence of operators that were applied to $|\psi\rangle$ is known and, as they are unitary transformations, they can be reversed and $|\psi\rangle$ can be recovered. Therefore, classical data can be used to encrypt quantum data.

III. IMPROVING QUANTUM SECRET-SHARING SCHEMES

In this section we show how to improve quantum secret-sharing schemes, in terms of reducing the number of necessary quantum shares, by using quantum encryption. First, we give an example: suppose we want to share a quantum secret $|S\rangle$ with a set of players $\mathcal{P}=\{A,B,C,D,E\}$ realizing an access structure $\Gamma=\{(A,B,C),(A,D),(A,E)\}$. If we encrypt the quantum state $|S\rangle$ (using a classical key K) into another quantum state $|\tilde{S}\rangle$ using the method described in Sec. II C and give $|\tilde{S}\rangle$ to the player A, we can share the classical key by a classical secret-sharing scheme that realizes Γ. The player A cannot recover $|S\rangle$ from $|\tilde{S}\rangle$ because he does not have the key. Only the subsets present in Γ can recover the classical key and the encrypted state together. By using this hybrid (classic-quantum) secret-sharing scheme, we can realize the access structure Γ by giving quantum data plus some classical data to the player A, and only classical data to all the other players. This has some advantageous features; for example, classical data is much easier to store, transmit, and receive than quantum data. However, not all the access structures can be improved in this way. For example, if we analyze a (2,3)-secret-sharing scheme, we realize that there is no way to distribute quantum data to only some members of the set of players. We now give a definition of improvable secret-sharing schemes.

Definition 1. A quantum secret-sharing scheme realizing an access structure $\Gamma=\{A_1,A_2,\ldots,A_r\}$ among a set of players $\mathcal{P}=\{P_1,P_2,\ldots,P_n\}$ is improvable if less than n quantum shares are sufficient to implement it.

The following theorem answers the question of when a

quantum secret-sharing scheme realizing a given access structure can be improved.

Theorem 1. For a conventional quantum secret-sharing scheme realizing an access structure $\Gamma=\{A_1,A_2,\ldots,A_r\}$ among a set of players $\mathcal{P}=\{P_1,P_2,\ldots,P_n\}$, it is "improvable" if there exists at least one $P_i\in A_j\in\Gamma$, $1\leqslant j\leqslant r$ such that $\Gamma|_{\mathcal{P}-P_i}$ does not violate the no-cloning theorem, where $\Gamma|_{\mathcal{P}-P_i}$ denotes the restriction of Γ to $\mathcal{P}-P_i$.

Proof. If $\Gamma|_{\mathcal{P}-P_i}$ does not violate the no-cloning theorem, there exists a quantum secret-sharing scheme that realizes $\Gamma|_{\mathcal{P}-P_i}$. We can implement a hybrid scheme realizing Γ in the following way: we encrypt the shares of $\Gamma|_{\mathcal{P}-P_i}$ with a classical key K and share it using a classical secret-sharing scheme realizing Γ. As Γ is a monotone access structure, the existence of a classical secret-sharing scheme implementing Γ is easily proved by using any of the well-known construction techniques for monotone access structures present in the literature (such as [19]). All the sets in $\Gamma|_{\mathcal{P}-P_i}$ can recover the encrypted shares, but only the sets in Γ can recover the encrypted shares and the classical key together. ■

Now we formalize the notion of minimal and optimal restricted-access structure.

Definition 2. A realizable restriction of an access structure $\Gamma=\{A_1,A_2,\ldots,A_r\}$ to a subset $B\subseteq\mathcal{P}=\{P_1,P_2,\ldots,P_n\}$ is a family $\Gamma|_B=\{\{A_i\cap B\}:A_i\in\Gamma\}$ that satisfies the no-cloning theorem, and $B\cap A_i\neq\varnothing$, $\forall A_i\in\Gamma$. $\Gamma|_B$ is called minimal if it is not improvable, and it is optimal if there is no other $D\subseteq\mathcal{P}$ such that $\Gamma|_D$ is minimal and $|D|<|B|$.

We now give a protocol that implements an improved quantum secret-sharing scheme among a set of players $\mathcal{P}=\{P_1,P_2,\ldots,P_n\}$, realizing an access structure Γ when its realizable minimal restriction $\Gamma|_B$ is known. In this improved scheme only $|B|$ quantum shares are needed, instead of $|\mathcal{P}|$.

Distribution phase. (1) Choose a random classical encryption K. Encrypt the quantum secret $|S\rangle$ using the encryption algorithm described in Sec. II C. The encrypted state will be denoted $|\tilde{S}\rangle$. (2) Using a normal quantum secret-sharing scheme, share $|\tilde{S}\rangle$ with the set of players realizing $\Gamma|_B$. Each member of B will receive a quantum share $|Q_i\rangle$, $1\leqslant i\leqslant|B|$. (3) Using a classical secret-sharing scheme share K with the set of players realizing Γ. Each member of $\mathcal{P}=\{P_1,P_2,\ldots,P_n\}$ will receive a classical share C_j, $1\leqslant j\leqslant n$.

Reconstruction phase. (1) Collect the quantum shares from the members of B. (2) Collect the classical shares from the members of $\mathcal{P}$. (3) Reconstruct the encrypted quantum secret $|\tilde{S}\rangle$ and the classical key K. (4) Decrypt $|\tilde{S}\rangle$ by using K.

It is easy to see that the protocol described above shares a quantum secret with a set of players so that only the groups of players specified by Γ will have access to the quantum secret. However, we have to note that it is not easy to compute the minimal access structure for a general access structure Γ. This task can be made easier if Γ has certain symmetry. This is the case of an important class of access structures: the so-called threshold schemes.

A. Threshold schemes

In order to find out this expression, we first state the following lemma.

Lemma 1. A restriction of a threshold scheme is always a threshold scheme.

Proof. The proof of this lemma follows from the definition of threshold schemes.

The following lemma gives us the expression for the optimal restriction of a threshold scheme.

Lemma 2. If a (k,n)-threshold scheme does not violate the no-cloning theorem, its minimal access structure is equal to the optimal one. Moreover it is given by the expression $(k-\gamma,n-\gamma)$ where $\gamma=2k-n-1$.

Proof. From lemma 1 we know that a restriction of a threshold scheme is always a threshold scheme. Therefore, a restriction of a (k,n)-threshold scheme must be of the form $(k-\gamma,n-\gamma)$ for an integer γ. From the no-cloning theorem we know that $k-\gamma>(n-\gamma)/2\Rightarrow 2k-n>\gamma$, so the minimal restriction has $\gamma=2k-n-1$. ■

Example 1. Suppose a threshold scheme (99,100). In a conventional quantum secret-sharing realization of this access structure, all the 100 players must receive a quantum share that is as large as the secret to be shared. However, from lemma 5 we know that its minimal restriction is a (2,3)-threshold scheme. Therefore, we just need three quantum shares in order to implement a hybrid quantum secret-sharing scheme realizing a quantum (99,100)-threshold scheme. Following the same logic, we see that an (n,n)-threshold scheme can be realized with only one quantum share.

B. General access structures

The analysis for general access structures is more complicated. We just improve a construction technique that was presented in [17]. First, we remember a construction of general access structures from threshold secret-sharing schemes proposed in [19] by Benaloh and Leichter. It is based on monotonic circuits. With each general access structure, Benaloh associated a special kind of boolean circuit called monotonic circuit. Suppose we have a boolean circuit with Boolean inputs, which represent the players, and one output y. The basic idea is to have a circuit that recognizes an authorized group of users. It means that the output y will be 1 if an authorized group of players is used as the input of the circuit. As the circuit is monotonic, changing one input from 1 to 0 does not change the output from 0 to 1 (excluding members of an unauthorized group will not change it into an authorized one). Afterwards, we could build up a secret-sharing scheme from the description of the circuit. To ensure the monotonicity of the circuit we will use only AND ($\wedge$) and OR ($\vee$) gates.

Example 2. Following Benaloh's representation, an access structure $\Gamma=\{(A,B,C),(A,D)\}$ would be represented by the circuit $y=(A\wedge B\wedge C)\vee(A\wedge D)$.

In a classical secret-sharing scheme, an access structure can be realized by associating the AND gates with a (q,q)-threshold scheme and the OR gates with a $(1,r)$-threshold scheme. In the given example, $(A\wedge B\wedge C)$

would be realized by a (3,3)-threshold scheme and the OR would be realized by a (1,2)-threshold scheme. This construction does not directly apply to the quantum scenario because $(1,r)$ quantum threshold schemes do not exist for $r \geqslant 2$ due to the no-cloning theorem.

In [17], Gottesman proved that the $(1,r)$-threshold scheme can be substituted by an $(r,2r-1)$-threshold scheme (a majority function). We earlier saw that an $(r,2r-1)$-threshold scheme cannot be improved. However, all the (q,q)-threshold schemes used to implement the logical AND can be substituted by a (1,1)-quantum secret-sharing scheme plus a (q,q)-classical secret-sharing scheme. Therefore, we see that a large group of general access structures can also be improved. However, it is clear that the improved access structure achieved by this construction is not minimal in general.

IV. FEATURES

Besides reducing the amount of quantum data that must be given to the set of players in order to share a quantum secret, another advantage of the hybrid quantum secret-sharing schemes is that they make possible a straightforward application of several features that are available for classical secret-sharing schemes and are not yet known to be valid in the quantum scenario. We briefly explain these features in this section.

The security of an (k,n)-threshold scheme is ensured iff an adversary is restricted to compromise less than k players during the whole lifetime of the secret. This is a quite strong assumption for long-term secrets. In order to cope with this problem, Herzberg *et al.* proposed in [20] a scheme where the shares are periodically renewed without changing the secret. It is easy to see that this construction applies to our hybrid secret-sharing scheme, therefore creating a proactive quantum secret-sharing scheme. To do so, we just use a proactive secret-sharing scheme to share the classical key K, and we periodically change the classical shares among the players. It is important to note that we still do not know whether such a protocol exists or not in a pure quantum secret-sharing scheme.

Another interesting scheme that becomes available in the hybrid scheme is secret sharing with prevention. In a (k,n,p)-secret sharing with prevention scheme, any group of p users can avoid all the other users to reconstructing the secret. Obviously, this scheme supposes that the players send their shares to a center in order to reconstruct it. This scheme was proposed in [21]. It becomes available in the quantum scenario in the same way as the proactive scheme, by applying it to the classical scheme used to share the key.

As a final example, we cite secret-sharing schemes with disenrollment [22]. In this scheme, a player can be excluded without setting a new scheme. We see that this scheme does not directly apply to our hybrid scheme. However, if we regard the players who will hold quantum shares as high reliable ones and that they will not be excluded of the scheme, it becomes implantable. However, only the players who hold only classical data can be excluded. Other variations, like nonperfect secret-sharing schemes, gradual disclosure of a secret, among others can be achieved in the same way.

V. CONCLUSIONS

We proposed a hybrid classical-quantum secret-sharing scheme that shares a quantum secret among a set of players such that only authorized groups can recover the secret and unauthorized groups have no information about it. We proved that for several access structures, this scheme can be implemented with less quantum shares than in a conventional quantum secret-sharing scheme. Additionally, some features of classical secret-sharing schemes, whose availability was not even known in the quantum domain, became available. We did not address the robustness against noise and/or cheating in the proposed protocol. Clearly, there is a trade-off between the improvability of an access structure and its robustness. If only one player holds the quantum shares and if anything happens to this state, the secret will be destroyed forever. We state the analysis of this problem as a future research topic.

ACKNOWLEDGMENTS

A.C.A.N. thanks Motohiko Isaka and Fabio Takada for valuable suggestions.

[1] A. Shamir, Commun. ACM **22**, 612 (1979).
[2] G. R. Blakley, in Safeguarding Cryptographic Keys, AFIPS Conf. Proc. No. 48, pp. 313–317.
[3] R. Cramer, I. Damgard, and U. Maurer, General Secure Multiparty Computation from any Linear Secret Sharing Scheme, most recent version available from http://www.inf.etzh.ch/personal/cramer (1998).
[4] R. Blom, Lect. Notes Comput. Sci. **209**, 335 (1985).
[5] G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai, *Lecture Notes in Computer Science* (Springer-Verlag, Berlin, 2000).
[6] A. Menezes, P. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography* (CRC Press, Boca Raton, FL, 1997), Chap. 13.
[7] M. Hillery, V. Bužek, and A. Berthiaume, e-print quant-ph/9806063.
[8] R. Cleve, D. Gottesman, and H-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[9] A. Smith, e-print quant-ph/0001087.
[10] H. Barnum, P. Hayden, R. Jozsa, and A. Winter, e-print quant-ph/0011072.
[11] C. Adami and N.J. Cerf, Phys. Rev. A **56**, 3470 (1997).
[12] M. Grassl, T. Beth, and T. Pellizzari, Phys. Rev. A **56**, 33 (1997).
[13] D. Gotttesman, e-print quant-ph/9705052.
[14] E. Knill and R. Laflamme, Phys. Rev. Lett. **84**, 2525 (2000).
[15] A.R. Calderbank and P.W. Shor, Phys. Rev. A **54**, 1098 (1996).

[16] W.K. Wooters and W.H. Zurek, Nature (London) **299**, 802 (1982).
[17] D. Gottesman, e-print quant-ph/9910067.
[18] M. Mosca, A. Tapp, and R. de Wolf, e-print quant-ph/0003101.
[19] J. Benaloh and J. Leichter, Lect. Notes Comput. Sci. **403**, 27 (1990).
[20] A. Herzberg, S. Jarecki, H. Krawczyk, 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, *Untrustworthy Participants in Perfect Secret Sharing Schemes*, edited by M. J. Gandley, Cryptography and Coding III (Oxford Clarendon Press, Oxford, 1993), pp. 255–264.