How to Share a Quantum Secret

Richard Cleve,[1,*] Daniel Gottesman,[2,†] and Hoi-Kwong Lo[3,‡]

[1]*Department of Computer Science, University of Calgary, Calgary, Alberta, Canada T2N 1N4*
[2]*T-6 Group, Los Alamos National Laboratory, Los Alamos, New Mexico 87545*
[3]*Hewlett-Packard Labs, Bristol BS34 8QZ, United Kingdom*

(Received 11 January 1999)

We investigate the concept of quantum secret sharing. In a (k, n) threshold scheme, a secret quantum state is divided into n shares such that any k of those shares can be used to reconstruct the secret, but any set of $k - 1$ or fewer shares contains absolutely no information about the secret. We show that the only constraint on the existence of threshold schemes comes from the quantum "no-cloning theorem," which requires that $n < 2k$, and we give efficient constructions of all threshold schemes. We also show that, for $k \leq n < 2k - 1$, then any (k, n) threshold scheme *must* distribute information that is globally in a mixed state.

PACS numbers: 03.67.Dd, 03.67.–a

Suppose that the president of a bank wants to give access to a vault to three vice presidents who are not entirely trusted. Instead of giving the combination to any one individual, it may be desirable to distribute information in such a way that no vice president alone has any knowledge of the combination, but any two of them can jointly determine the combination. In 1979, Blakely [1] and Shamir [2] addressed a generalization of this problem, by showing how to construct schemes that divide a secret into n shares such that any k of those shares can be used to reconstruct the secret, but any set of $k - 1$ or fewer shares contains absolutely no information about the secret. This is called a (k, n) *threshold scheme,* and is a useful tool for cryptographic key management.

Now, consider a generalization to the setting of *quantum* information, where the secret is an arbitrary unknown quantum state. Salvail [3] (see also [4]) obtained a method to divide an unknown qubit into two shares, each of which individually contains no information about the qubit, but which jointly can be used to reconstruct the qubit. Hillery *et al.* [4] and Karlsson *et al.* [5] proposed methods for implementing some *classical* threshold schemes that use quantum information to transmit the shares securely in the presence of eavesdroppers. These papers also considered the possibility of splitting quantum information without keeping it completely secret.

Define a *quantum* (k, n) *threshold scheme,* with $k \leq n$, as a method to encode and divide an arbitrary *secret* quantum state (which is given but not, in general, explicitly known) into n *shares* with the following two properties. First, from any k or more shares, the secret quantum state can be perfectly reconstructed. Second, from any $k - 1$ or fewer shares, no information *at all* can be deduced about the secret quantum state. Each share can consist of any number of qubits (or higher-dimensional states), and not all shares need to be of the same size.

Quantum secret sharing schemes might be used in the context of sharing quantum keys, such as "quantum money" [6]. They can also be used to provide interesting ways of distributing quantum entanglement and nonlocality. For example, suppose that Alice has one qubit of an EPR pair and a $(2, 2)$ threshold scheme is applied to the other qubit to produce a share for Bob and a share for Carol. Then Alice and Bob together have a product state (i.e., $\rho_{AB} = \rho_A \otimes \rho_B$), as do Alice and Carol; however, Bob and Carol can jointly construct a qubit from their shares that is in an EPR state with Alice's qubit. Also, for quantum storage or quantum computations to be robust in the worst-case situation where a component or a group of components fail (due to sabotage by malicious parties or due to defects), quantum secret sharing may prove to be a useful concept.

Let us begin with an example of a $(2, 3)$ threshold scheme. The secret here is an arbitrary three-dimensional quantum state (a quantum trit or *qutrit*). The encoding maps the secret qutrit to three qutrits as

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

and each resulting qutrit is taken as a share. Note that, from a single share, absolutely no information can be deduced about the secret, since each individual share is always in the totally mixed state (an equal mixture of $|0\rangle$, $|1\rangle$, and $|2\rangle$). On the other hand, the secret can be reconstructed from any two of the three shares as follows. If we are given the first two shares (for instance), add the value of the first share to the second (modulo three), and then add the value of the second share to the first, to obtain the state

$$(\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle)(|00\rangle + |12\rangle + |21\rangle)\,. \quad (2)$$

The first qutrit now contains the secret.

 0031-9007/99/83(3)/648(4)$15.00

Note that the above example is similar to a quantum error-correcting code [7,8]. In fact, it is a three-qutrit quantum code that can correct one erasure error. Every quantum secret sharing scheme is, in some sense, a quantum error-correcting code; however, some error-correcting codes are not secret sharing schemes, since they may contain sets of shares from which *partial* information about the secret can be obtained. For example, consider a four-qubit code [9,10] that corrects one erasure by the encoding

$$\alpha|0\rangle + \beta|1\rangle \mapsto \alpha(|0000\rangle + |1111\rangle) + \beta(|0011\rangle + |1100\rangle).$$

While it is true that any three qubits suffice to reconstruct the secret, it is *not* true that two qubits provide no information. For instance, given the first and third qubits, one can distinguish between the secrets $|0\rangle$ and $|1\rangle$. Later, we shall show how to obtain a $(3,4)$ threshold scheme with four qubits using a different approach.

Returning to the $(2,3)$ threshold scheme using qutrits, note that it can be used to share a secret that is a *qubit* by simply not using the third dimension of the input space (though the resulting shares are still full qutrits). It turns out that there does not exist a $(2,3)$ threshold scheme for qubits in which each share is also a qubit. This is because such a scheme would also be a three-qubit code that corrects single qubit erasure errors, which has been shown not to exist [10].

The $(2,3)$ qutrit threshold scheme can be used to construct a $(2,2)$ threshold scheme, by simply discarding (i.e., tracing out) one of the three shares. Note that the resulting $(2,2)$ scheme produces a mixed state encoding even when the secret is a pure state. Call a scheme that encodes pure state secrets using global pure states a *pure state scheme*, and a scheme for which the encodings of pure states are sometimes in global mixed states a *mixed state scheme*. We shall show later that there does not exist a pure state $(2,2)$ threshold scheme.

On the other hand, if we do not insist on protecting an arbitrary secret, we could use the encoding

$$\alpha|0\rangle + \beta|1\rangle \mapsto \alpha(|00\rangle - |11\rangle) + \beta(|01\rangle + |10\rangle). \quad (3)$$

For the restricted set of secrets where $\alpha \cdot \beta^*$ is real valued, it functions as a $(2,2)$ threshold scheme. However, without this restriction, this is not a secret sharing scheme, since (for example) it can be verified that a single share can completely distinguish between the secrets $|0\rangle + i|1\rangle$ and $|0\rangle - i|1\rangle$. Although such a scheme may be useful in some contexts, we shall henceforth consider only "unrestricted" secret sharing schemes.

Note that the previously mentioned technique of discarding a share from a $(2,3)$ threshold scheme to obtain a $(2,2)$ threshold scheme (suggested by [11] in the context of a different scheme) generalizes considerably.

Theorem 1.—From any (k,n) threshold scheme with $n > k$, a $(k, n-1)$ threshold scheme can be constructed by discarding one share.

In the classical case, a (k,n) threshold scheme exists for every value of $n \geq k$. However, this does not hold in the quantum case, due to the "no-cloning theorem" [12,13].

Theorem 2.—If $n \geq 2k$ then no (k,n) threshold scheme exists.

Proof.—If a (k,n) threshold scheme exists with $n \geq 2k$ then the following procedure can be used to make two independent copies of an arbitrary quantum state (that is, to clone). First, apply the (k,n) scheme to the state to produce n shares. Then, taking two disjoint sets of k shares, reconstruct two independent copies of the state. This contradicts the no-cloning theorem [12,13].

The five-qubit quantum code proposed in [14,15] immediately yields a $(3,5)$ threshold scheme. First, since it corrects any two erasure errors, it enables the secret to be reconstructed from any three shares. Also, any pair of qubits provides no information about the data. This is a consequence of the following more general theorem.

Theorem 3.—If a quantum code with code words of length $2k-1$ corrects $k-1$ erasure errors (which, for stabilizer codes [16,17], is a $[[2k-1,1,k]]_q$ code, where q is the dimensionality of each coordinate and of the encoded state) then it is also a $(k, 2k-1)$ threshold scheme.

Proof.—First, suppose that we are given a set of k shares. Since this set excludes precisely $k-1$ shares and the code corrects any $k-1$ erasures, the secret can be reconstructed from these k shares. On the other hand, suppose that we are given a set of $k-1$ shares. This subset excludes a set of k shares, from which we know that the secret can be perfectly reconstructed. Now, in quantum mechanics, it is well known that any information gain on an unknown quantum state necessarily leads to its disturbance [18]. Therefore, if a measurement on the given $k-1$ shares provided any information about the secret, then this measurement would disturb the information that the remaining k qubits contain about the secret. This leads to a contradiction.

Combining Theorem 3 with Theorem 1, we obtain the following.

Corollary 4.—If a $[[2k-1,1,k]]_q$ code exists, a (k,n) threshold scheme exists for any $n < 2k$.

For example, from the aforementioned five-qubit code, a $(3,4)$ threshold scheme and $(3,3)$ threshold scheme can be obtained (by discarding shares).

Next, we prove the converse of Theorem 2.

Theorem 5.—If $n < 2k$, then a (k,n) threshold scheme exists. Moreover, the dimension of each share can be bounded above by $2\,max(2k-1, s)$, where s is the dimension of the quantum secret.

Proof.—We will use a class of *quantum polynomial codes*, which are based on those defined by Aharonov and Ben-Or [19] in the context of fault-tolerant quantum

computation. Our goal is to show how to construct such a code of length m and degree $k-1$ whenever $m < 2k$, and that the data that it encodes can always be recovered from any k of its m coordinates. Then, considering the special case where $m = 2k-1$, we obtain a $[[2k-1, 1, k]]_q$ code, for which Corollary 4 applies to prove the theorem.

Let k and m be given with $m < 2k$, and let s be the dimension of the quantum state to be encoded. Choose a prime q such that $\max(m, s) \le q \le 2\max(m, s)$ (which is always possible [20]) and let $\mathbf{F} = \mathbf{Z}_q$. For $c = (c_0, c_1, \ldots, c_{k-1}) \in \mathbf{F}^k$, define the polynomial $p_c(t) = c_0 + c_1 t + \cdots + c_{k-1} t^{k-1}$. Let $x_0, \ldots, x_{m-1}$ be m distinct elements of $\mathbf{F}$. Encode a q-ary quantum state by the linear mapping which is defined on basis states $|s\rangle$ (for $s \in \mathbf{F}$) as

$$|s\rangle \mapsto \sum_{\substack{c\in\mathbf{F}^k \\ c_{k-1}=s}} |p_c(x_0), \ldots, p_c(x_{m-1})\rangle . \tag{4}$$

As an example, it turns out that mapping (1) [for the $(2,3)$ threshold scheme] is a quantum polynomial code with $k = 2$, $m = 3$, and $q = 3$.

It now suffices to show that, given an encoding (4) of a quantum state, the state can be recovered from any k of the m coordinates. One way to show this is to apply the theory of Calderbank-Shor-Steane codes [21,22], noting that this code is formed from the two classical codes

$$C_1 = \{(p_c(x_0), \ldots, p_c(x_{m-1})) \,|\, c \in \mathbf{F}^k\}, \tag{5}$$

$$C_2 = \{(p_c(x_0), \ldots, p_c(x_{m-1})) \,|\, c \in \mathbf{F}^k, c_{k-1} = 0\}, \tag{6}$$

and that $\min(\mathrm{dist}C_1, \mathrm{dist}C_2^{\perp}) = m - k + 1$. From this it follows that the code corrects $m-k$ erasure errors.

For completeness, we also give an explicit decoding procedure for the case of interest, where $m = 2k-1$. We begin with some preliminary definitions. For an invertible $d \times d$ matrix M, define the operation *apply* M to a sequence of d quantum registers as applying the mapping

$$|(y_0, \ldots, y_{d-1})\rangle \mapsto |(y_0, \ldots, y_{d-1})M\rangle . \tag{7}$$

For $z_0, \ldots, z_{d-1} \in \mathbf{F}$, define the $d \times d$ Vandermonde matrix $[V_d(z_0, \ldots, z_{d-1})]_{ij} = z_j^i$ (for $i, j \in \{0, \ldots, d-1\}$). Also, note that applying $V_d(z_0, \ldots, z_{d-1})$ to registers in state $|c_0, \ldots, c_{d-1}\rangle$ yields the state $|p_c(z_0), \ldots, p_c(z_{d-1})\rangle$, where $c = (c_0, \ldots, c_{d-1})$.

The secret can be recovered from any k coordinates by the following procedure. Call the m registers containing the coordinates $R_0, \ldots, R_{m-1}$, and suppose that we are given, say, the first k registers (that is, $R_0, \ldots, R_{k-1}$). (i) Apply $V_k(x_0, \ldots, x_{k-1})^{-1}$ to $R_0, \ldots, R_{k-1}$. (ii) Cyclically shift the first k registers by one to the right by setting $(R_0, R_1, \ldots, R_{k-1})$ to $(R_{k-1}, R_0, \ldots, R_{k-2})$. (iii) Apply $V_{k-1}(x_k, \ldots, x_{m-1})$ to $R_1, \ldots, R_{k-1}$. (iv) For all $i \in \{1, \ldots, k-1\}$, add $R_0 \cdot (x_{k+i-1})^{k-1}$ to R_i.

Consider an execution of the above procedure on a state resulting from the encoding Eq. (4) on a basis state $|s\rangle$. After steps (i) and (ii), the state of the n registers is

$$\sum_{\substack{c\in\mathbf{F}^k \\ c_{k-1}=s}} |c_{k-1}, c_0, \ldots, c_{k-2}\rangle |p_c(x_k), \ldots, p_c(x_{m-1})\rangle$$
$$= |s\rangle \sum_{\substack{c\in\mathbf{F}^k \\ c_{k-1}=s}} |c_0, \ldots, c_{k-2}\rangle |p_c(x_k), \ldots, p_c(x_{m-1})\rangle . \tag{8}$$

If the datum is a basis state $|s\rangle$ (for some $s \in \mathbf{F}$), its recovery is already complete. However, for a general secret, which is a superposition of $|s\rangle$ states, register R_0 is entangled with the other registers. This is because, in (8), the value of s can be determined by the value of any of the kets $|c_0, \ldots, c_{k-2}\rangle |p_c(x_k), \ldots, p_c(x_{m-1})\rangle$. The remaining steps complete the decoding.

After steps (iii) and (iv), the state is

$$|s\rangle \sum_{\substack{c\in\mathbf{F}^k \\ c_{k-1}=s}} |p_c(x_k), \ldots, p_c(x_{m-1})\rangle |p_c(x_k), \ldots, p_c(x_{m-1})\rangle$$
$$= |s\rangle \sum_{y\in\mathbf{F}^{k-1}} |y_1, \ldots, y_{k-1}\rangle |y_1, \ldots, y_{k-1}\rangle , \tag{9}$$

where we use the fact that, for any $s \in \mathbf{F}$ and $y_1, \ldots, y_{k-1} \in \mathbf{F}$, there is a unique $c \in \mathbf{F}^k$ with $c_{k-1} = s$ such that $p_c(x_{k+i-1}) = y_i$, for all $i \in \{1, \ldots, k-1\}$. The decoding procedure is now correct for arbitrary data.

Although we have focused on threshold schemes, it is possible to consider more general *access structures.* In a general quantum secret sharing scheme, from certain *authorized sets* of shares, the secret can be reconstructed, while, from all other sets of shares, no information can be obtained about the secret. For example, consider a scenario with three shares, A, B, C, where the authorized sets are $\{A, B\}$, $\{A, C\}$, and any superset of one of these sets. Such an access structure can be easily implemented by starting with the $(3,4)$ threshold scheme and bundling the first two shares into the share A.

We have already seen relationships between quantum secret sharing schemes and quantum error-correcting codes. We now explore this connection more deeply.

The usual formulation of conditions for a quantum error-correcting code yields the following.

Proposition 6.—Let C be a subspace of a Hilbert space $\mathcal{H}$. The following conditions are equivalent.

(a) C corrects erasures on a set K of coordinates.

(b) For any orthonormal basis $\{|\phi_i\rangle\}$ of C,

$$\langle \phi_i | E | \phi_j \rangle = 0 \qquad (i \neq j), \tag{10}$$

$$\langle \phi_i | E | \phi_i \rangle = c(E), \tag{11}$$

for all operators E acting on K.

(c) For all (normalized) $|\phi\rangle \in C$ and all E acting on K,

$$\langle \phi | E | \phi \rangle = c(E). \tag{12}$$

Note that the same function $c(E)$ appears in conditions (b) and (c), and that it is independent of $|\phi\rangle$ or $|\phi_i\rangle$.

Proof.—(a) $\Leftrightarrow$ (b) is essentially the standard quantum error correction conditions [14,23] applied to erasure errors [10]. (b) $\Leftrightarrow$ (c) is straightforward. Alternately, (a) $\Leftrightarrow$ (c) follows from the main theorem of [24].

Equation (10) says that, in correcting errors, we will never confuse two different basis vectors. Equation (11) says that learning about the error will never give us any information about which basis vector we have.

On the other hand, condition (12) simply says that the environment can never gain any information about the state. In other words, the proposition tells us that protecting a state from noise is exactly the same as preventing the environment from learning about it.

Condition (12) is also very convenient for our purposes, since the two constraints that arise on a quantum secret sharing scheme are the ability to correct erasures and the requirement that no information be gained by unauthorized sets of shares.

Theorem 7.—An encoding $f : |\psi\rangle \mapsto |\phi\rangle$ is a pure state quantum secret sharing scheme iff Eq. (12) holds (independent of $|\phi\rangle$) whenever E is an operator acting on the complement of an authorized set or when E is an operator acting on an unauthorized set.

Proof.—Let C be the image of f. S is an authorized set iff the subspace C can correct for erasures on K, the complement of S. By Proposition 6, this means S is an authorized set iff (12) holds for all E acting on K. T is an unauthorized set whenever we can gain no information about the state $|\psi\rangle$ from any measurement on T. That is, the expectation value $\langle \phi | E | \phi \rangle$ is independent of $|\phi\rangle \in C$ for any operator E we could choose to measure, which means it must act on T. Again, this is condition (12).

Theorem 7 has at least one remarkable consequence.

Corollary 8.—For a pure state quantum secret sharing scheme, every unauthorized set of shares is the complement of an authorized set and vice versa.

Proof.—If the complement of an authorized set of shares S_1 were another authorized set S_2 then we could create two copies of the secret from S_1 and S_2, violating the no-cloning theorem. Therefore, the complement of an authorized set is always an unauthorized set.

On the other hand, by Proposition 6, if condition (12) holds on an unauthorized set T, we can correct erasures on T, and therefore reconstruct the secret on the complement of T. Therefore, the complement of an unauthorized set is always an authorized set.

For a pure state (k, n) threshold scheme, this condition implies that $n - k = k - 1$. Therefore,

Corollary 9.—Any (k, n) pure state threshold scheme satisfies $n = 2k - 1$.

Clearly, this corollary does not apply to mixed state schemes, since we have constructed (k, n) threshold schemes with $n < 2k - 1$.

We thank A. Ashikhmin, C. H. Bennett, A. Berthiaume, V. Bužek, H. F. Chau, M. Hillery, B. Lane, D. Leung, and L. Salvail for helpful discussions. Part of this work was completed at the 1998 Elsag-Bailey–I. S. I. Foundation research meeting on quantum computation, and the 1998 meeting at the Benasque Center for Physics. This work is supported in part by Canada's NSERC and by the Department of Energy under Contract No. W-7405-ENG-36.

*Email address: cleve@cpsc.ucalgary.ca
†Email address: gottesma@t6-serv.lanl.gov
‡Email address: hkl@hplb.hpl.hp.com

[1] G. Blakely, in *Proceedings of the National Computer Conference, New York, 1979* (AFIPS, Montvale, NJ, 1979), Vol. 48, pp. 313–317.
[2] A. Shamir, Commun. ACM **22**, 612 (1979).
[3] L. Salvail (private communication).
[4] M. Hillery, V. Bužek, and A. Berthiaume, quant-ph/9806063.
[5] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[6] S. Wiesner, SIGACT News **15**, 77 (1983).
[7] P. Shor, Phys. Rev. A **52**, 2493 (1995).
[8] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[9] L. Vaidman, L. Goldenberg, and S. Wiesner, Phys. Rev. A **54**, R1745 (1996).
[10] M. Grassl, T. Beth, and T. Pellizzari, Phys. Rev. A **56**, 33 (1997).
[11] B. Lane (private communication).
[12] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[13] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[14] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, Phys. Rev. A **54**, 3824 (1996); quant-ph/9604024.
[15] R. Laflamme, C. Miquel, J. P. Paz, and W. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[16] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[17] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
[18] C. H. Bennett, G. Brassard, and N. David Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[19] D. Aharonov and M. Ben-Or, in *Proceedings of the 29th ACM Symposium on Theory of Computing* (ACM, New York, 1998), p. 176.
[20] M. Aigner and G. M. Ziegler, *Proofs from The Book* (Springer, Berlin, 1998), p. 7.
[21] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[22] A. Steane, Proc. R. Soc. London A **452**, 2551 (1996).
[23] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[24] M. A. Nielsen and C. M. Caves, Phys. Rev. A **55**, 2547 (1997).