How to share a Quantum Secret

Richard Cleve*, Daniel Gottesman†, Hoi-Kwong Lo
Extended Enterprise Laboratory
HP Laboratories Bristol
HPL-98-205
December, 1998

E-mail: cleve@cpsc.ucalgary.ca
gottesma@t6-serv.lanl.gov
hkl@hplb.hpl.hp.com

quantum information, secret sharing, quantum cryptography, quantum computation

We investigate the concept of quantum secret sharing, where a secret quantum state is distributed between n parties in such a way that certain subsets of the parties can jointly recover the secret, while other subsets of the parties can acquire absolutely no information about it. In a $((k,n))$ threshold scheme, any subset of k or more parties can reconstruct the secret, while any subset of $k-1$ or fewer parties can obtain no information. 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, in all such cases, we give an efficient construction of a $((k,n))$ threshold scheme. We also explore similarities and differences between quantum secret sharing schemes and quantum error-correcting codes. One remarkable difference is that, while most existing quantum codes encode pure states as pure states, quantum secret sharing schemes must use mixed states in some cases. For example, if $k \leq n < 2k-1$ then any $((k,n))$ threshold scheme must distribute information that is globally in a mixed state.

Internal Accession Date Only

*Department of Computer Science, University of Calgary, Calgary, Alberta, Canada
†T-6 Group, Los Alamos National Lab, Los Alamos, NM

How to Share a Quantum Secret

Richard Cleve*, Daniel Gottesman†, and Hoi-Kwong Lo‡

December 8, 1998

Abstract

We investigate the concept of quantum secret sharing, where a secret quantum state is distributed between n parties in such a way that certain subsets of the parties can jointly recover the secret, while other subsets of the parties can acquire absolutely no information about it. In a $((k,n))$ threshold scheme, any subset of k or more parties can reconstruct the secret, while any subset of $k-1$ or fewer parties can obtain no information. 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, in all such cases, we give an efficient construction of a $((k,n))$ threshold scheme. We also explore similarities and differences between quantum secret sharing schemes and quantum error-correcting codes. One remarkable difference is that, while most existing quantum codes encode pure states as pure states, quantum secret sharing schemes must use mixed states in some cases. For example, if $k \leq n < 2k-1$ then any $((k,n))$ threshold scheme *must* distribute information that is globally in a mixed state.

Suppose that a bank wants to give access to its main 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 designing cryptographic key management systems.

Now, consider a generalization of such schemes 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,

*Department of Computer Science, University of Calgary, Calgary, Alberta, Canada T2N 1N4. Email: cleve@cpsc.ucalgary.ca

†T-6 Group, Los Alamos National Lab, Los Alamos, NM 87545, USA. Email: gottesma@t6-serv.lanl.gov

‡Hewlett-Packard Labs, Bristol, UK BS34 8QZ. Email: hkl@hplb.hpl.hp.com

each of which individually contains no information about the qubit, but which jointly can be used to reconstruct the qubit. Hillery, Bužek, and Berthiaume [4] proposed a method for implementing some *classical* threshold schemes that uses quantum information to transmit the shares securely in the presence of eavesdroppers.

Define a $((k,n))$ *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. In this paper we do not consider the problem of securely creating and distributing the shared secret, and simply assume that it can be done when necessary.

Quantum secret sharing schemes might be used in the context of sharing quantum keys, such as those proposed by Weisner [7] for uncounterfeitable "quantum money." 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,[1] 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. More generally, 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. Finally, by definition, quantum secret sharing distributes trust between various parties and prevents a small coalition of malicious parties from learning a quantum secret.

Let us give 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

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

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

$$(\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle)(|00\rangle + |12\rangle + |21\rangle). \tag{2}$$

[1] Bob has no information about Alice's state, so there cannot be any entanglement or classical correlation between his and Alice's states. It can be shown that their state can therefore be written as a product of mixed states, i.e., $\rho_{AB} = \rho_A \otimes \rho_B$.

The first qutrit is now disentangled from the other two, and contains the secret. The reconstruction procedure for the other cases is similar, by the symmetry of mapping (1) with respect to cyclic permutations of the three qutrits.

Note that, because the data is quantum, one must be careful not to individually measure the shares while performing the reconstruction, since this will collapse any superposition of the basis states. The same considerations arise when considering quantum error-correcting codes [5, 6]. In fact, the above example 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 [8, 9] that corrects one erasure. A possible encoding is

$$\alpha|0\rangle + \beta|1\rangle \mapsto \alpha(|0000\rangle + |1111\rangle) + \beta(|0011\rangle + |1100\rangle) \tag{3}$$

(the code can actually be extended to encode two qubits, but we do not need this for our illustration). 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 $|1\rangle$. More generally, from these two qubits, statistical information about the relative values of $|\alpha|$ and $|\beta|$ can be obtained. 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 qu*bit* 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 [9].

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. The encoding procedure can be defined by the following linear map on density matrices

$$\begin{aligned} |0\rangle\langle 0| &\mapsto |00\rangle\langle 00| + |11\rangle\langle 11| + |22\rangle\langle 22| \\ |1\rangle\langle 1| &\mapsto |01\rangle\langle 01| + |12\rangle\langle 12| + |20\rangle\langle 20| \\ |2\rangle\langle 2| &\mapsto |02\rangle\langle 02| + |10\rangle\langle 10| + |21\rangle\langle 21|. \end{aligned} \tag{4}$$

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

$$\alpha|0\rangle + \beta|1\rangle \mapsto \alpha(|00\rangle - |11\rangle) + \beta(|01\rangle + |10\rangle). \tag{5}$$

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 [10] 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 quantum "no-cloning theorem" [11, 12], which states that no operation can produce multiple copies of an unknown arbitrary quantum state.

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 could 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" [11, 12]. □

The five-qubit quantum code proposed in [13, 14] 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. Moreover, 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 codewords of length $2k-1$ corrects $k-1$ erasure errors (which, in the language of quantum coding theory, is a $[[2k-1,1,k]]_q$ code[2], 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 [17]. 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. □

[2] Actually, the notation $[[2k-1,1,k]]_q$ only refers to a stabilizer code [15, 16]. However, Theorem 3 and Corollary 4 both apply to more general codes as well.

Note that, combining Theorem 3 with Theorem 1, we obtain

Corollary 4. *From a $[[2k-1,1,k]]_q$ code, a $((k,n))$ threshold scheme can be constructed 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, each share can be chosen to consist of at most $\max(\lceil \log_2(2k-1) \rceil, \lceil \log_2(s) \rceil)$ qubits, where s is the dimension of the quantum secret.*

Proof. The proof is based on a class of *quantum polynomial codes*, which are similar to those defined by Aharonov and Ben-Or [18], who used them in the context of fault-tolerant quantum computation. We will show that if $m < 2k$ then, for such a quantum polynomial code of degree $k-1$ and length m, the data that it encodes can always be recovered from any k of its m components. Then, by setting $m = 2k-1$, 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 power $q = p^r$ such that $\max(m,s) \leq \max(2k-1,s) \leq q$, and let $\mathbf{F} = GF(q)$, the finite field of size q. For example, when q is prime, $GF(q) = \mathbf{Z}_q$. On the other hand, by taking p to be 2, one obtains the bound stated in the theorem. 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

$$|s\rangle \mapsto \sum_{\substack{c \in \mathbf{F}^k \\ c_{k-1}=s}} |p_c(x_0), \ldots, p_c(x_{m-1})\rangle \,. \tag{6}$$

As an example, it turns out that mapping (1) (for the $((2,3))$ threshold scheme given at the beginning of this paper) is a quantum polynomial code with $k = 2$, $m = 3$, and $q = 3$.

To prove the theorem, it suffices to show that, given an encoding (6) 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 CSS codes [19, 20], noting that this code is formed from the two classical codes

$$C_1 = \{(p_c(x_0), \ldots, p_c(x_{m-1})) \,|\, c \in \mathbf{F}^k\} \tag{7}$$

$$C_2 = \{(p_c(x_0), \ldots, p_c(x_{m-1})) \,|\, c \in \mathbf{F}^k, c_{k-1} = 0\} \tag{8}$$

and that $\min(\text{dist } C_1, \text{dist } C_2^{\perp}) = m - k + 1$. Thus, when $m = 2k-1$, the minimal distance of the code is k, and Corollary 4 applies to prove the theorem.

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

$$|(y_0, \ldots, y_{d-1})\rangle \mapsto |(y_0, \ldots, y_{d-1})M\rangle \tag{9}$$

(where we are equating $|(y_0, \ldots, y_{d-1})\rangle$ with $|y_0, \ldots, y_{d-1}\rangle$). Also, for any $z_0, \ldots, z_{d-1} \in \mathbf{F}$, define the $d \times d$ Vandermonde matrix

$$V_d(z_0, \ldots, z_{d-1}) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ z_0 & z_1 & \cdots & z_{d-1} \\ \vdots & \vdots & \ddots & \vdots \\ z_0^{d-1} & z_1^{d-1} & \cdots & z_{d-1}^{d-1} \end{pmatrix}. \tag{10}$$

This matrix is invertible whenever $z_0, \ldots, z_{d-1}$ are distinct. 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, $R_0, \ldots, R_{k-1}$).

1. Apply $V_k(x_0, \ldots, x_{k-1})^{-1}$ to $R_0, \ldots, R_{k-1}$.
2. Cyclically shift the first k registers by one to the right by setting $(R_0, R_1 \ldots, R_{k-1})$ to $(R_{k-1}, R_0, \ldots, R_{k-2})$.
3. Apply $V_{k-1}(x_k, \ldots, x_{m-1})$ to $R_1, \ldots, R_{k-1}$.
4. For each $i \in \{1, \ldots, k-1\}$, 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 (6) on a basis state $|s\rangle$. After steps 1 and 2, the state of the n registers is

$$\begin{aligned} & \sum_{\substack{c \in \mathbf{F}^k \\ c_{k-1} = s}} |c_{k-1}, c_0, \ldots, c_{k-2}\rangle \, |p_c(x_k), \ldots, p_c(x_{m-1})\rangle \\ = \; & |s\rangle \sum_{\substack{c \in \mathbf{F}^k \\ c_{k-1} = s}} |c_0, \ldots, c_{k-2}\rangle \, |p_c(x_k), \ldots, p_c(x_{m-1})\rangle \, . \end{aligned} \tag{11}$$

If the data is a basis state $|s\rangle$ (for some $s \in \mathbf{F}$) then, at this point, its recovery is complete. However, for a general secret, which is a superposition of $|s\rangle$ states, register R_0 is entangled with the other registers. The entanglement is due to the fact that, in (11), the value of s can be determined by the value of any of the kets $|c_0, \ldots, c_{k-2}\rangle \, |p_c(x_k), \ldots, p_c(x_{m-1})\rangle$. In fact, if we had $m \geq 2k$ then s could be determined from just the state of the last $m - k$ registers, so it would be impossible to perform the necessary disentanglement by accessing only the first k registers. Since $m = 2k - 1$, this is not a problem and the remaining steps correctly extract the data in the following manner.

After step 3, the state of the m registers is

$$|s\rangle \sum_{\substack{c\in\mathbf{F}^k \\ c_{k-1}=s}} |p'_c(x_k),\ldots,p'_c(x_{m-1})\rangle\,|p_c(x_k),\ldots,p_c(x_{m-1})\rangle\,, \tag{12}$$

where $p'_c(t) = c_0 + c_1 t + \cdots + c_{k-2}t^{k-2} = p_c(t) - c_{k-1}t^{k-1}$. Finally, after step 4, the state is

$$\begin{aligned} & |s\rangle \sum_{\substack{c\in\mathbf{F}^k \\ c_{k-1}=s}} |p_c(x_k),\ldots,p_c(x_{m-1})\rangle\,|p_c(x_k),\ldots,p_c(x_{m-1})\rangle \\ = \;& |s\rangle \sum_{y\in\mathbf{F}^{k-1}} |y_1,\ldots,y_{k-1}\rangle\,|y_1,\ldots,y_{k-1}\rangle\,, \end{aligned} \tag{13}$$

where the last equality holds because, for any $s \in \mathbf{F}$ and $y_1,\ldots,y_{k-1} \in \mathbf{F}$, there exists a unique $c \in \mathbf{F}^k$ with $c_{k-1} = s$ such that $p_c(x_{k+i-1}) = y_i$, for all $i \in \{1,\ldots,k-1\}$. Since the state of $R_1,\ldots,R_{m-1}$ is now independent of s, the decoding procedure is now correct for arbitrary data. □

It should be noted that, for a quantum polynomial code of degree $k-1$ and length $n < 2k-1$, even though the data can still be recovered from any k coordinates, such a code is not a valid $((k,n))$ threshold scheme. This is because, when $n < 2k-1$, it turns out that $k-1$ coordinates will yield partial information about the data.

Although we have focused on threshold schemes, it should be noted that 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 at all can be obtained about the secret. Those other sets are called *unauthorized sets*. For example, consider a scenario with four shares, A, B, C, D, where the authorized sets are $\{A,B\}$, $\{A,C\}$, $\{A,D\}$, $\{B,C,D\}$, and any superset of one of these sets. Such a secret sharing scheme can be easily implemented by starting with the $((3,5))$ threshold scheme and bundling the first two shares into the share A.

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

The following proposition follows naturally from the usual formulation of the conditions for a quantum error-correcting code.

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

a) $\mathcal{C}$ corrects erasures on a set K of coordinates.

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

$$\langle\phi_i|E|\phi_j\rangle = 0 \quad (i \neq j) \tag{14}$$

$$\langle\phi_i|E|\phi_i\rangle = c(E) \tag{15}$$

for all operators E acting on K.

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

$$\langle\phi|E|\phi\rangle = c(E). \tag{16}$$

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 [13, 22] applied to erasure errors [9]. b) $\Leftrightarrow$ c) is straightforward. Alternately, a) $\Leftrightarrow$ c) follows from the main theorem of [21]. □

Equation (14) says that in correcting errors, we will never confuse two different basis vectors. Equation (15) says that learning about the error will never give us any information about which basis vector we have. This is important, since that information would constitute a measurement, collapsing a superposition of basis vectors.

On the other hand, condition (16) 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 problem as preventing the environment from learning about the state.

Condition (16) 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.

In the theory of quantum error-correcting codes, we usually consider shares of the same dimension. In contrast, in quantum secret sharing, we would like to allow shares to live in Hilbert spaces of different sizes. Nevertheless, it is still true that conditions a), b), and c) in Proposition 6 are equivalent.

Theorem 7. *An encoding* $f : |\psi\rangle \mapsto |\phi\rangle$ *is a pure state quantum secret sharing scheme iff*

$$\langle\phi|E|\phi\rangle = c(E) \tag{17}$$

(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.*

For instance, for the three-qutrit scheme (1) and $E_j\,|y_1, y_2, y_3\rangle = \omega^{y_j}\,|y_1, y_2, y_3\rangle$, where $\omega = \exp(2\pi i/3)$, we have $\langle\phi|E_j|\phi\rangle = 0$ for all states $|\phi\rangle$ used in the scheme.

Proof. Let $\mathcal{C}$ be the image of f.

S is an authorized set iff the subspace $\mathcal{C}$ can correct for erasures on K, the complement of S. By Proposition 6, this means S is an authorized set iff (17) 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 $|\phi\rangle \in \mathcal{C}$ for any operator E we could choose to measure, which means it must act on T. Again, this is condition (17).

Therefore, f defines a quantum secret sharing scheme iff (17) holds for operators acting on unauthorized sets or on the complement of authorized sets. □

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 (17) 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 now show that *any* mixed state scheme can be derived by throwing away shares from a larger pure state scheme. Note that any mixed state scheme can be encoded via a unitary transformation on a larger quantum system in which part of the larger system is discarded (i.e. traced out). The following theorem shows that this larger system will always be a valid secret sharing scheme.

Theorem 10. *Given any mixed state quantum secret sharing scheme, if we include the missing subsystem generated during the unitary encoding process as a single additional share, then a pure state quantum secret sharing scheme results. In other words, it satisfies the conditions of Theorem 7.*

Proof. Given any mixed state quantum secret sharing scheme, let us include the missing subsystem as a single additional share and consider the resulting scheme. If S is a set that includes the extra share, we do not know *a priori* that it is not possible to gain partial but incomplete information from S. However, K, the complement of S, is a set consisting of original shares. By the definition of a mixed state secret sharing scheme, either one can gain full information about the secret from the shares in K or none at all.

If K gives full information, then it follows from Proposition 6 that S yields no information. On the other hand, if K gives no information, then we can correct erasures on K, thereby obtaining full information on the original quantum secret from the shares in S. This shows that no set of shares will allow us to get partial information on the quantum secret. Therefore, we have a pure state secret sharing scheme. □

We would like to thank Alexei Ashikhmin, Charles Bennett, André Berthiaume, Vladimir Bužek, Mark Hillery, Brendan Lane, and Louis Salvail for helpful discussions. Part of this work was completed during the 1998 Elsag-Bailey – I.S.I. Foundation research meeting on quantum computation, and the 1998

meeting at the Benasque Center for Physics. R.C. is supported in part by Canada's NSERC. D.G. is supported by the Department of Energy under contract W-7405-ENG-36.

References

[1] G. Blakely, "Safeguarding cryptographic keys," Proc. AFIPS, Vol. 48, pp. 313-317 (1979).

[2] A. Shamir, "How to share a secret," Communications of the ACM, Vol. 22, No. 11, pp. 612-613 (1979).

[3] L. Salvail, private communication.

[4] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," quant-ph/9806063.

[5] P. Shor, "Scheme for reducing decoherence in quantum memory," Phys. Rev. A **52**, 2493 (1995).

[6] A. M. Steane, "Error correcting codes in quantum theory," Phys. Rev. Lett. **77**, 793 (1996).

[7] S. Wiesner, "Conjugate Coding," SIGACT News 15, p. 77 (1983).

[8] L. Vaidman, L. Goldenberg, and S. Wiesner, "Error prevention scheme with four particles," Phys. Rev. A **54**, R1745 (1996); quant-ph/9603031.

[9] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," Phys. Rev. A **56**, 33 (1997); quant-ph/9610042.

[10] B. Lane, personal communication (1997).

[11] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature **299**, 802 (1982).

[12] D. Dieks, "Communication by EPR devices," Phys. Lett. A **92**, 271 (1982).

[13] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, "Mixed state entanglement and quantum error correction," Phys. Rev. A **54**, 3824 (1996); quant-ph/9604024.

[14] R. Laflamme, C. Miquel, J. P. Paz, and W. Zurek, "Perfect quantum error correction code," Phys. Rev. Lett. **77**, 198 (1996); quant-ph/9602019.

[15] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," Phys. Rev. A **54**, 1862 (1996); quant-ph/9604038.

[16] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," Phys. Rev. Lett. **78**, 405 (1997); quant-ph/9605005.

[17] C. H. Bennett, G. Brassard and N. David Mermin, "Quantum Cryptography without Bell's Theorem," Phys. Rev. Lett. **68**, 557 (1992).

[18] D. Aharonov and M. Ben-Or, "Fault-tolerant quantum computation with constant error," *Proc. 29th Ann. ACM Symp. on Theory of Computing*, (ACM, New York, 1998), 176; quant-ph/9611025.

[19] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," Phys. Rev. A **54**, 1098 (1996); quant-ph/9512032.

[20] A. Steane, "Multiple particle interference and quantum error correction," Proc. Roy. Soc. Lond. A **452**, 2551 (1996); quant-ph/9601029.

[21] M. A. Nielsen and C. M. Caves, "Reversible quantum operations and their application to teleportation," Phys. Rev. A **55**, pp 2547-2556 (1997); quant-ph/9608001

[22] E. Knill and R. Laflamme, "A theory of quantum error-correcting codes," Phys. Rev. A **55**, 900 (1997); quant-ph/9604034.