Review of How to Share a Quantum Secret [1]

Haobei Song (20629096)
CO 481/CS 467/ **PHY 467**
University of Waterloo

March 30 2017

Abstract

Secret sharing also known as secret splitting has been developed considerably ever since its invention in 1979. With the emerging of quantum computing, study of secret sharing protocols implemented by quantum physics has become an active area filled with interest and intrigue due to the eccentric properties from quantum mechanics such as entanglement and interference between quantum states. In a (k, n) threshold scheme, a secret quantum state could be transformed into n shares and kept by different participants among whom only k or more shares combined can reconstruct the secret, with another restriction that any set of shares fewer than k contains no information at all about the secret and thus cannot be used to reconstruct the secret. This paper then shows that it is the "no-cloning theorem" solely that places the restriction on the existence of the threshold schemes (k, n) where $n < 2k$, along with the algorithms for constructiong all of the threshold schemes belonging to this category efficiently. In addition, it also explains the reason why the shares distributed by a (k, n) threshold scheme with $k \leq n < 2k - 1$ must be in a global mixed state.

1 Introductionn and Preliminaries

Since the first time the concept of secret sharing was proposed independently by Adi Shamir[2] and George Blakley[3] in 1979, it has gained appreciable attention and has been studied extensively in quantum computing. Secret sharing also known as secret splitting is refered to as protocols or methods for secret dstribution among a gathering of parties each of whom is provided with a share of the secret. Secret sharing is widely employed in cryptographic key management within information industries and considered of more and more importance as the concept of sharing information on internet has become extensively accepted by more and more people.

Suppose the secret is distributed into n shares, then a (k, n) scheme is defined as a method or protocol such that any set of k or more shares can be used to reconstruct the secret, but any set of less than k shares carry absolutely no information at all about the secret divided. For example, three keys to the vault are assigned to three clerks in a bank. They can open the vault with whichever two clerks present, but no one could open the vault by himself. Besides, one alone has no idea at all about the structure of the locker on the vault at all. This method or protocol of dividing the

keys (shares of the secret) is a $(2, 3)$ threshold scheme. Another interesting potential application of quantum secret is, proposed by Wiesner[4] in 1983, quantum bank which resembles the previous example. We first build a EPR pair which is in an entangled state. Alice owns one of the two qubits. Bob and Carol each has a share of qubit divided from the other qubit of that EPR pair. As Bob and Carol jointly can reconstruct one qubit with which Alice could then reconstruct the original EPR pair. This process does not leak any information about the secret to any potential eavesdropper as it is easy for them to detect the state collapse whenever the eavesdropeer gains any information about the secret.

As quantum secret sharing was still a relative strange area combining both frontier physics and cryptography, Cleve, Gottesman and Lo studies from the fundamental building blocks of quantum secret sharing and explained the only restraint the "no-cloning theorem" laid on the existence of all the threshold schemes where $n < 2k$ [1]. They also proposed an algorithm to effectively construct all the possible threshold schemes. Besides, they showed heuristically any (k, n) threshold scheme with $k \leq n < 2k - 1$ condition satisfied inevitablly give away some information to the shares which form a globally mixed state. Their work contributed considerablly to the later development of quantum secret sharing and encouraged plenty of profound discoveries in both physics and computer science.

This review paper is written carefully to present readers from various domains with heuristic understanding of the basis upon which quantum sharing is built. I will first introduce the setting up of quantum threshold schemes and some insights about its difference from classical shcemes. Then I will explain the rigorous proofs in their original talented paper. Different from the original work, I will show the proof in great detail to give general readers understanding of some nontrivial math along with it.

2 Quantum Threshold Scheme

A secret sharing protocol with respect to quantum states starts with a random states with no beforehand knowledge about the state. Salvail[5] invented a protocol to transform one unknown secret qubit into two shares, either of which by itself hold no information about that original qubit and therefore cannot be used to reconstruct the secret qubit, but those two dis-

tributed qubits together can be used to reconstruct the original secret qubit. Hillery[6] and Karlsson[7] described the methods they adopted to make use of quantum states to achieve classical threshold schemes while an eavesdropper is present. Other researchers took into consideration the possibility of dividing quantum information into different parts each of which shares a certain information about the secret bit.

2.1 Quantum Threshold Scheme

Here, we define a (k, n) quantum threshold scheme such that the secret quantum state is divided into n shares and any $k(k < n)$ or more shares can recover the original quantum state, but any set of less than k shares contains absolutely no information at all about the original secret state. However, there is no limitation for how many qubits the shares can have.
The following is a $(2, 3)$ quantum threshold scheme which divide a secret qutrit (three dimensional quantum state) into three qutrits any two or more of which could be used to reconstruct the original qutrit.

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

Each qutrit is a share which contains no information at all about the secret as these shares present a symetric structure with each qutrit having equal probability of being in $\left|0\right\rangle, \left|1\right\rangle, \left|2\right\rangle$. More detaied mathematical proof is as follows when we trace out the second and the third qutrits.

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

As all the three states are of equal probability to collapes into, there is no way eavesdroppers can obtain any useful information about the original qutrit. However, any two shares can recover the original qutrit perfectly if we add the first qutrit to the second and then add the modified second qutrit back to the first one. This can be easily implemented by three dimensional quantum

control gates.

$$\begin{aligned}
&\alpha(|000\rangle + |111\rangle + |222\rangle) + \beta(|012\rangle + |120\rangle + |201\rangle) + \gamma(|021\rangle + |102\rangle + |210\rangle) \\
\mapsto&\alpha(|000\rangle + |121\rangle + |212\rangle) + \beta(|012\rangle + |100\rangle + |221\rangle) + \gamma(|021\rangle + |112\rangle + |200\rangle) \\
\mapsto&\alpha(|000\rangle + |021\rangle + |012\rangle) + \beta(|112\rangle + |100\rangle + |121\rangle) + \gamma(|221\rangle + |212\rangle + |200\rangle) \\
=&(\alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle)(|00\rangle + |12\rangle + |21\rangle) \qquad (3)
\end{aligned}$$

As a result, the secret qutrit is reconstructed at the first qutrit after the transformation above.

Researchers from quantum computing would recognize the similarities of this protocol with quantum error-correctiong algorithms. Furthermore, it is actually a three-qutrit quantum correcting code which corrects one erasure error of the three intermidiate qutrits. Generally speaking, each quantum threshold scheme is in some sense an error-correcting code which can be implemented by quantum sharing, which I will show later with proofs. But the inverse is not that simple as some error-correcting code leaks partial information from the secret qubit (or qutrit). Here is a four-qubit error-correctiong code correcting one erasure error:

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

Any three qubits can be used to construct the original secret qubit by the same idea from previous example, but not all the sets of less than 3 qubits contain no information about the secret. Notice the asymmetry within the structure of the transformed qubits. Given any one of the first two qubits and one of the last two qubits, we can by a high probability distinguish between $|0\rangle$ and $|1\rangle$ since if we trace out, say the first and the last qubit, we end up with:

$$(\alpha^2, |00\rangle), (\alpha^2, |11\rangle), (\beta^2, |01\rangle), (\beta^2, |10\rangle) \qquad (4)$$

Whenever α differes from β, there would be a preference of being in first two of the four states $\|\alpha\| > \|\beta\|$ over the other two and vice versa. However, there are other protocols which could achieve the $(3, 4)$ threshold scheme theoretically and I will show how to come up with that protocol from a general consideration in the proof part of this paper.

3 Proof Chain

From now on, consider it possible to construct a $(3, 4)$ threshold scheme procotol, which I will return back later. We can always discard one qubit of the shared states (by tracing out that state to discard as shown by (2) and (3), and use the $(3, 4)$ threshold scheme to implement a $(3, 3)$ threshold scheme. The same is true to obtain a $(2, 2)$ threshold scheme from a $(2, 3)$ threshold scheme or more generally:

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

Drawn from the study of classical secret sharing, a (k, n) threshold scheme can be constructed as long as $n \geq k$. But this is not the case for quantum secret sharing as a result of the famous "no-cloning theorem". We could prove

Theorem 2. *There exits no threshold scheme form $n \geq 2k$.*

Proof: By contradiction, suppose there exists a threshold scheme $S : (k, n)$ with $n \geq 2k$ and an arbitrary secret state can be divided into n shares which we denote as set N. First, collect k shares from the n divided quantum states to form a set N_1 which is a subset of N, and the original arbitrary quantum state could be reconstructed by N_1. Then, collect another set N_2 of k shares from the set $N \setminus N_1$, and we can recover the original arbitrary secret state together with the one created before contradicting the no-cloning theorem as we could otherwise use this protocol to copy any arbitrary quantum state.

Theorem 3. *A quantum correction scheme which corrects $k-1$ erasure errors from the codewords of length $2k-1$ is also a $(k, 2k-1)$ threshold scheme.*

Proof: Given the codeword shares transformed from the original code, k bits of the codeword can then be used to reconstruct the original word as the error correction scheme can correct the rest $k-1$ erasure errors. These k bits are taken as the k shares in a threshold scheme context and can be used to recover the secret.

The key point is to show that the $k-1$ shares (corresponding to the $k-1$ bits to be corrected) contain absolute no information about the original secret (code). By the measurement theory in quantum mechanics, any measurement performed on a quantum state would make it collapse to its eigenstate. And whenever we gain some information about the secret from those $k-1$ shares, we inexorablly made an measurement on them and make the whole system collapse to a state which lost some information about the original secret.[8] As a result, the k bits among the codewords cannot theoretically reconstruct the original code. Therefore, those $k-1$ shares contains no information at all about the secret code if there exists such error-correction algorithm.

From both **Theorem 3** and **Theorem 1**, we have the following corollary directly.

Corollary 4. A $[[2k-1,1,k]]_q$ error-correction code ensures the existence of a (k,n) quantum threshold schmeme for any $n<2k$.

Here let us catch up with the following definition in the rest of the proofs.

Definition 1. *A quantum threshold scheme that encodes pure state secrets into global pure state is called a* ***pure state scheme.*** *For a quantum threshold scheme by which if there exists any secret quantum pure state which is encoded to a global mixed state, such a threshold scheme is called a* ***mixed state scheme***

All the quantum threshold schemes shown previously are mixed state schemes by this definition.

We could actually move further from **Theorem 2**.

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

Proof: Let me sketch the whole proof where we first prove the existence of a $[[2k-1,1,k]]_q$ error-correction code when $n<2k$ and then by the

Corollary 4 shown earlier, the whole proof is completed.

Let $m < 2k$ and s be the dimension of the quantum state to be encoded. There then always exists a prime q which satisfies $\mathbf{max}(m, s) \leq q \leq 2\mathbf{max}(m, s)$ from number theory. For $c \in \mathbf{F}^k$, define the polynomial $p_c(x)$ to be $c_0 + c_1 x + \ldots c_{k-1} x^{k-1}$. We can then divide a q-ary quantum state by the following linear map:

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

The original state can then be reconstructed from any k of the m coordinates by applying CSS (Calderbank-Shor-Steane) code [9].

After cyclically shifting the coordinates and apply the Vandermonde matrix (see more detail on [1]), we recover the secret at the first coordinate

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

We then successfully obtain the $[[2k-1, 1, k]]_q$ error-correction code and thus the theorem is proved by ***Corollary 4***.

Quantum error-correction code and quantum threshold scheme are correlated cheek by jowl and their summary relationship is outlined as follows:

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,

$$\langle \phi_i | \, E \, | \phi_j \rangle = 0 \quad (i \neq j), \tag{7}$$

$$\langle \phi_i | \, E \, | \phi_j \rangle = c(E) \quad (i = j) \tag{8}$$

for all operators E acting on K.

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

$$\langle \phi | \, E \, | \phi \rangle = c(E) \tag{9}$$

To understand what this Proposition means in a quantum computing

context, we consider the subspace C as the shares within which the same number as the dimension of set K, of coordinates of the shares contain no information about the original quantum system at all and in light of this, the more rigorous proof is as follows.

Proof: (a) $\Leftrightarrow$ (b) is actually the standard quantum error-correction conditions correcting the erasure errors within the set K. (b) $\Rightarrow$ (c) is obvious and (c) $\Rightarrow$ (b) is also straightforward as we work in a computational basis. The proof for that (a) $\Leftrightarrow$ (c) is written by Knill[10]. These summary equivalence relation suggests that keeping the secret from noise is equivalent to keeping the secret from potential eavesdroppers.

Theorem 7. *An encoding $f : |\psi\rangle \mapsto |\phi\rangle$ is a pure state quantum secret sharing scheme iff (9) holds, where E is acting on the compliment of the authorized set of shares divided from the secret.*

The proof follows from the **Proposition 6**. The operator can E can be shown to act solely on the unauthorized set of coordinates. Thus, the encoding f is a pure state quantum secret sharing scheme.

There are two remarkable corollaries coming from this theorem which are:

Corollary 8. *For a pure state quantum secret sharing scheme, any authorized set of shares is the compliment of the unauthorized set and vice versa.*

Corollary 9 *Any (k, n) pure state threshold scheme must have $n = 2k-1$.*

For mixed state quantum threshold scheme we have

Corollary 10 *Any (k, n) threshold scheme satisfying $(n < 2k - 1)$ is a mixed quantum threshold scheme*

This completes the proof chain.

References

[1] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, pp. 648–651, Jul 1999. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.83.648

[2] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979. [Online]. Available: http://doi.acm.org/10.1145/359168.359176

[3] G. R. Blakley, "Safeguarding cryptographic keys," *Managing Requirements Knowledge, International Workshop on*, vol. 00, p. 313, 1899.

[4] Wiesner, "Conjugate coding," *SIGACT News*, pp. 15,77.

[5] L. S. (personal communication).

[6] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, pp. 1829–1834, Mar 1999. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.59.1829

[7] A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting," *Phys. Rev. A*, vol. 59, pp. 162–168, Jan 1999. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.59.162

[8] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, Feb 1992. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.68.557

[9] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, Aug 1996. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.54.1098

[10] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A*, vol. 55, pp. 900–911, Feb 1997. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.55.900