A Kind of (n, t)Threshold Quantum State Sharing Scheme Based on Chinese Reminder Theorem

Yanchang Li

BEIJING 101 middle school, Beijing, 100091, China

craigliii@outlook.com

Abstract. Secret sharing is a key technology of data confidentiality, where one can distribute a secret among agents, and only the authorized agents can recover the original secret. Quantum information technology, including quantum communication, quantum computing can break through the bottlenecks of classical technology in information security and computing speed, based on quantum mechanics, such as quantum superposition, quantum uncertainty, quantum no-cloning and quantum entanglement. By combining quantum technology with classic secret sharing, the concept of quantum state sharing was presented. In this manuscript, a novel kind of (n,t) threshold quantum state sharing scheme is proposed, where the selected t agents among n agents can cooperate to reconstruct the target secret state. For implementing this scheme, the Chinese reminder theorem is introduced during the processing of the secret key distribution. In addition, to show the proposed scheme clearly, a concrete (5,3) example is given. Furthermore, the proof of the correctness of the scheme is shown. Our scheme will improve the development the quantum secret sharing and open up exploring the application of quantum information technology

Keywords: Secret sharing, quantum, (n,t).

1. Introduction

The emergence of quantum physics has revolutionized all scientific fields, especially computer science. The new Quantum information technology, inspired by quantum physics, allows us to make further progress beyond traditional computer science and promise great potential of application in various of fields, including economy, engineering and so on. In this paper, the development of quantum information technology will be explained and a novel information cyphering method based on Quantum physics will be introduced.

Quantum information technology [1] can break through the bottlenecks of classical technology in information security. For example, the first quantum key distribution protocol can establish an encryption key between two remote network nodes [2]. Relying on the laws of quantum mechanics, it can achieve theoretical unconditional security which can't be performed by the classic encryption. For another example, Shor's algorithm [3] allows computer to complete the factorization of large composite numbers in polynomial time, however, such task has an exponential complexity for traditional computers. Such advantages bring quantum-based information encryption its distinctive value in fields of commercial fields and military fields, thus, quantum cyphering was highly regarded by scientists and governments among the world.

The laws of quantum mechanics lay the theoretical foundation for the development of quantum information technology. The principle of quantum uncertainty and non-cloning ensures the security of quantum communication protocols. The superposition characteristics of quantum states and quantum entanglement of many-body systems are one of the important features that distinguish quantum mechanics from classical physics, which can realize many astonishing applications.

With the development of computing, the classical cryptography, which security based on computational complexity is being challenged. Stronger computing power could enhance the efficiency of brute-force attacks, which brings menace to traditional cryptography. Unlike the classical cryptography, quantum cryptography is based on the theory of quantum mechanics instead of computational complexity. The security of quantum cypher is guaranteed by quantum law such as such as Uncertainty Principle and Non-cloning Theorem, which can be proved security in theory. As an important research interest in quantum cryptography, Quantum Secure Communication Protocol theory combines quantum mechanics and classical communication theory, and its confidentiality can be proved through the theory of quantum physical mechanics.

Quantum Secure Communication includes Quantum Key Distribution (QKD), Quantum Secure Direct Communication (QSDC) [4-5], Quantum Teleportation (QT) [6], Quantum Secret Sharing (QSS), Quantum Dense Coding (QDC). Based on the idea of "quantum banknotes", C.H. Bennett and others proposed the first QKD protocol in 1984. This protocol is often called the quantum BB84 protocol. The quantum BB84 protocol proposed the idea of using quantum channels to transmit quantum states and traditional channels to openly transmit information related to quantum measurements. This idea had a profound impact on subsequent QKD protocol design and experiments.

The quantum key distribution protocol has become the most outstanding direction in the research of quantum secure communication protocols, which has greatly promoted the development of quantum communications. The information determined by the traditional QKD protocol is random, that is, the sender Alice cannot transmit the information to Bob with certainty. For example, in the original quantum BB84 protocol, if Alice sends a classical bit 0 without any discarding operation, the probability of Bob receiving 0 is only 75%, so Alice and Bob must go through some methods after the quantum information transmission is completed. Determine the information transmitted by both parties. Although the combination of QKD and OTP can achieve theoretical security, the overhead caused by using quantum channels to transmit keys that are as long as the ciphertext is huge.

Based on the fact that the theoretical security of quantum communication can be proven through the properties of quantum physics and mechanics, experts and scholars have proposed the idea of using quantum communication to directly transmit information to replace the traditional cryptography system. Based on this idea, a new quantum secure communication protocol was born, the quantum secure direct communication (QSDC) protocol. In the QSDC protocol, the quantum channel will directly and deterministically transmit information instead of keys. The biggest feature of the QSDC protocol is that the receiver Bob can immediately and definitely read the deterministic information transmitted by the sender Alice after obtaining the transmitted quantum state, without the need for other redundant information to assist.

Quantum teleportation (QT) [6] was first proposed by Bennett et al. in 1993 and later it was realized experimentally for the first time. It can teleport an unknown quantum state from the sender Alice to the receiver Bob without transferring the quantum state, which is done by using quantum entanglement, that is one of the most astonishing features of quantum mechanics.

In order to realize multifunctional quantum networks, diverse quantum state transfer protocols have been proposed and studied [7-12]. By introducing agents, quantum state sharing protocols have been proposed, which can realize the sharing of quantum states among multiple agents. By using this protocol, unless all agents cooperate, it is impossible for any agent to reconstruct the quantum state to be shared. The initial quantum state sharing protocol used GHZ states as entanglement channels. Later, a variety of quantum entangled states were used to achieve state sharing, such as Bell states, W states and cluster states and so on are used to realize quantum qubit state sharing.

Both QT and QSTS play an important role in quantum information processing technologies, such as quantum network, quantum network coding and long-distance quantum communications [13-14].

For the majority of the current QSTS schemes, only all the n participants cooperate together, the secret can be recovered. However, any one or any group of the participants cannot reconstruct the key. There are some (n,t) structure, but these schemes are very complicated. Therefore, it is more and more meaningful to try to search for a novel and effective way to construct (n,t) a kind of threshold structure.

In this manuscript, a new and effective way is proposed, where the Chinese Reminder Theorem is utilized to construct the (n,t) threshold structure. The core of the proposed protocol is based on the solutions of the Chinese Reminder Theorem and the quantum unitary transformations. In our proposed scheme, not only the private keys of the dealer and n agents can be easily generated, but also the process can be easily fulfilled.

The rest of this paper is organized as follows. In Section II, the basic knowledge is given, including the Chinese Reminder Theorem, quantum basis concept. In Section III and IV, the procedure of our scheme is given and an example is shown clearly. Section V shows the proof of the correctness of the scheme and Section V contains the conclusion.

2. The Basic Knowledge

2.1 The basic knowledge of quantum state

Bits, as the basic concept of classical computing and information, are represented by 0 and 1 and they are also the basis of the classical computers. Qubits, as a generalization of classical bits, are referred to as qubits. In physics, quantum state qubit describes discrete two-level physical systems, such as photons, atoms, etc. Mathematically, qubits can be described as mathematical objects with certain specific properties, which enables the free construction of quantum computing and quantum information theory that do not rely on specific physical systems.

Specifically, an arbitrary qubit is a unit vector in the two-dimensional Hilbert space C^2. Similar to the classical bits 0 and 1, two qubits can be represented by $|0\rangle$ and$|1\rangle$, where$|0\rangle = (1,0)^T$ and $|1\rangle = (0,1)^T$.$|0\rangle$ and $|1\rangle$are two mutually orthogonal vectors, so they can be expanded to the entire two-dimensional vector space. Different from classical bits, in addition to being in$|0\rangle$ and$|1\rangle$, qubits can also be a linear superposition of these two states, which is called a superposition state and is expressed as follows

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

where α and $\beta$are complex numbers and satisfy $||\alpha|^2 + |\beta|^2 = 1$. Therefore, a quantum state is a vector in a two-dimensional complex number space, where $|0\rangle$ and $|1\rangle$ are also called computational ground states. For a classical bit, you can easily tell whether it is 0 or 1. But for qubit, we cannot accurately obtain the values of α and β. Based on the laws of quantum mechanics, we can only obtain limited information about the quantum state. For example, if you use the measurement basis $\{|0\rangle, |1\rangle\}$ to measure $|\Psi\rangle$, then the measurement result is either the $|0\rangle$ state with probability $|\alpha|^2$, or $|1\rangle$ state with probability $|\beta|^2$.

2.2 The basic knowledge of quantum unitary transformation

In quantum information science, a quantum transformation corresponds to a quantum operation, which is a quantum logic gate. Any quantum transformation can be represented by a unitary matrix. Performing a unitary operation on a quantum state is equivalent to matrix multiplication of the unitary matrix and the state vector. That is, for any two quantum states $|\Phi\rangle$ and $|\Psi\rangle$, the former is the input. state, the latter is the output state, then a quantum transformation U is defined as:

$$|\Psi\rangle = U|\Phi\rangle \tag{2}$$

The unitary operation U is a linear operation that satisfies $UU^* = I$, where U^* is the conjugate transpose of U and I is the identity transformation. The only restriction condition for quantum transformation U is that it satisfies the unitary matrix. The unitary operation does not change the inner product. Since unitary operations always have inverse operations, logical operations in quantum information processing are all reversible, which is also different from classical calculations.

For two-dimensional quantum state qubit, it can be divided into single-bit quantum logic gates and multi-bit quantum logic gates. Common single-bit quantum gates include Pauli gates and Hadamard gates. The unit gate, as a kind of Pauli gate, is an identity gate, that is, it does not perform any operations on the quantum state. The other Pauli gates are σ_x, σ_y and σ_z gates, which are represented by the following matrix:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{3}$$

where i is the imaginary unit. In addition, a generalized phase gate is defined by

$$U_z = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \tag{4}$$

2.3 The basic knowledge and the application of quantum entanglement

Quantum entanglement is a unique phenomenon in quantum mechanics that is different from classical physics. It is an important resource in quantum communication and quantum computing, and plays a very important role in quantum information science, such as quantum teleportation and quantum state sharing, quantum network coding, etc. Quantum entanglement originated from the EPR paradox proposed by Einstein, Podolsky and Rosen in the 1930s to prove the incompleteness of quantum mechanics. In 1935, Schrodinger introduced the concept of quantum entanglement into quantum mechanics for the first time.

A typical entangled state of two particles is the Bell state, which has the following form:

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \qquad |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle. \tag{5}$$

In the quantum Ping-pong protocol, the Bell entangled state is prepared by the receiver Bob. Bob sends one of the two-particle entangled states to Alice. Alice performs corresponding operations based on the information to be sent and then sends it back to Bob. Bob regains the entanglement. Measure the two particles in the state, and infer the operation performed by Alice based on the measurement results, thereby obtaining the information Alice wants to send. In the quantum Ping-pong protocol, the transmission of information between Alice and Bob requires the same particle to be transmitted twice in the channel, so the quantum Ping-pong protocol is a two-way protocol, also called two-step protocol.

Assume that the quantum Bell state prepared by Bob is $|\psi^{+}\rangle$, and define two operators *Z* and *I*: When Alice wants to transmit a classical bit 1, she performs Z operation on the obtained quantum state. when she wants to transmit a classical bit 0, she performs *I* operation on the obtained quantum state.

When Bob receives the particles sent back by Alice, he performs the Bell measurements on the two particles. If the measurement result is $|\psi^{-}\rangle$, it means that Alice has performed the *Z* operation, and the classic bit sent by Alice is 1, otherwise Alice sends a result of 0.

2.4 The Chinese Remainder Theorem

The Chinese Remainder Theorem is a theorem in number theory about a system of linear congruential equations of one variable, where it can explain the criteria and solution methods for a system of linear congruential equations of one variable. Assume x is the solution of the following equations:

$$\begin{cases} x \equiv a_1 \ (mod\ m_1) \\ x \equiv a_2 \ (mod\ m_2) \\ \qquad \vdots \\ x \equiv a_n \ (mod\ m_n) \end{cases} \tag{6}$$

where any two of these *n* numbers $m_1, m_2, \cdots, m_n$ are relatively prime. Base on the Chinese Reminder Theorem, the solution x has the following expression:

$$x = \sum_{i=1}^{n} a_i t_i M_i + kM \tag{7}$$

Where $M = m_1 m_2 \cdots m_n$, $M_i = M/m_i$, $k \in Z$ and $t_i M_i \equiv 1\ (mod\ m_i)$. Furthermore, by selecting the proper k_1, the solution will be

$$x = \sum_{i=1}^{n} a_i t_i M_i + k_1 M \tag{8}$$

which will be taken as the key to implement the scheme.

Based on CRT, the (n, t) threshold secret sharing can be realized as the following approach. Suppose the solution x is the key and $m_1 < m_2 < \cdots < m_n$, and two conditions need to be satisfied:

(i) The product of any t smallest m_i is greater than x;

(ii) The product of any $t-1$ biggest m_i is less than x; that is

$$\begin{cases} m_1 m_2 \cdots m_t > x \\ m_{n-t+2} m_{n-t+3} \cdots m_n < x \end{cases} \tag{9}$$

3. The Proposed Protocol

Suppose that Alice is the dealer who holds on the secret unknown quantum state as follows

$$|\phi_0\rangle = \alpha|0\rangle + \beta|1\rangle \tag{10}$$

where the complex amplitudes α and β satisfies the equation $|\alpha|^2 + |\beta|^2 = 1$.

The goal is to realize the initial secret state $|\phi_0\rangle$ sharing among *n* agents $\{Bob_1, Bob_2, \cdots, Bob_n\}$, where any *t* selected agents determined by Alice can reconstruct the initial state when they cooperate. Without loss of generality, denote *t* participants as $\{Bob_{i_1}, Bob_{i_2}, \cdots, Bob_{i_t}\}$. The proposed scheme is as follows.

Initially, Alice needs to encrypt the shared quantum state $|\phi_0\rangle$ to $|\phi_0'\rangle$ by the quantum unitary transform $U(k_1M - x)$ defined by

$$U(k_1M - x) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i(k_1M - x)} \end{pmatrix} \tag{11}$$

where $(k_1M - x)$ is the secret key chosen by Alice. For simplifying the expression, define $x' = k_1M - x$ Then, the new quantum state will become $|\phi_0'\rangle = U(x')|\phi_0\rangle$

(2) Then, by introducing Chinese Remainder Theorem, Alice distributes (a_i, M_i) to *i*-th agent. For improving the security, the classical information (a_i, M_i) can be sent by quantum secure direction communication.

(3) If it comes to the pinch, Alice randomly select t agents $(B_{i_1}, B_{i_2}, \cdots, B_{i_t})$ to cooperate to reconstruct the initial state $|\phi_0\rangle$, she transmits the classical information M' and the encrypted quantum state $|\phi_0'\rangle$ to B_{i_1}, where $M' = m_{i_1} m_{i_2 \ldots} m_{i_t}$. After B_{i_1} receiving the quantum state, he selects $x_{i_1} = a_{i_1} t_{i_1} M'/m_{i_1}$ and performs the unitary transform $U(x_{i_1})$. Then B_{i_1} obtains the quantum state $|\phi_1\rangle$, where $|\phi_1\rangle = U(x_{i_1})|\phi_0'\rangle$ and transmits it and the classical information M' to B_{i_2}.

(4) Similar to the steps as B_{i_1} does, after B_{i_2} receiving the quantum state, he selects $x_{i_2} = a_{i_2} t_{i_2} M'/m_{i_2}$ and performs the unitary transform $U(x_{i_2})$. Then B_{i_2} obtains the quantum state $|\phi_2\rangle$, where $|\phi_2\rangle = U(x_{i_2})|\phi_1\rangle$ and transmits it and the classical information M' to B_{i_3}.

(5) This procedure goes on until the participant B_{i_t}. Finally, B_{i_t} take the unitary matrix $U(x_{i_t})$ on the quantum state $|\phi_{t-1}\rangle$, which can reconstruct the initial quantum state $|\phi_0\rangle$ with $x_{i_t} = a_{i_t} t_{i_t} M'/m_{i_t}$.

4. Concrete Example of the Proposed Protocol

In this section, an example of quantum (5, 3) threshold is proposed. The example of quantum state sharing (5, 3) threshold, that is $n = 5$ and $t = 3$. The goal is to realize the initial secret state $|\phi_0\rangle$ sharing among 5 agents $\{Bob_1, Bob_2, \cdots, Bob_5\}$, where any 3 selected agents determined by Alice can reconstruct the initial state when they cooperate. Assume that $\{Bob_1, Bob_2, Bob_5\}$are chosen to cooperate to obtain the target state.

Correspondingly, taking $x = 117$ and $m_1 = 4,$ $m_2 = 5,$ $m_3 = 7,$ $m_4 = 9,$ and $m_5 = 11$ as the relatively primes. Therefore, one can obtain

$$\begin{cases} 117 \equiv 1 \ (mod\ 4) \\ 117 \equiv 2 \ (mod\ 5) \\ 117 \equiv 5 \ (mod\ 7) \\ 117 \equiv 0 \ (mod\ 9) \\ 117 \equiv 7 \ (mod\ 11) \end{cases} \tag{12}$$

where the values $a=(a_1,a_2,a_3,a_4,a_5)=(1,2,5,0,7)$. The proposed scheme is as follows in detail.

Initially, Alice needs to encrypt the shared quantum state $|\phi_0\rangle$ to $|\phi_0'\rangle$ by the quantum unitary transform $U(-337)$ defined by

$$U(-337)=\begin{pmatrix}1 & 0\\ 0 & e^{-i\,337}\end{pmatrix} \tag{13}$$

where $337=117+M$ is the secret key chosen by Alice.

Then, by introducing Chinese Remainder Theorem, Alice distributes $(1,2,5,0,7)$to the five agents separately. For improving the security, the classical secret information a_i can be sent by quantum key distribution.

As the three agents (B_1,B_2,B_5) are chosen to obtain the target quantum state $|\phi_0\rangle$, she transmits the classical information $M'=m_{i_1}m_{i_2}...m_{i_t}=220$ and the encrypted quantum state $|\phi_0'\rangle$ to B_1. After B_1 receiving the quantum state, he selects $x_1=\frac{a_1t_1M'}{m_1}=165$ and performs the unitary transform $U(165)$. Then B_1 obtains the quantum state $|\phi_1\rangle$, where $|\phi_1\rangle=U(165)|\phi_0'\rangle$ and transmits it and the classical information $M'=220$ to B_2.

After B_2 receiving the quantum state $|\phi_1\rangle$, he selects $x_2=\frac{a_2t_2M'}{m_2}=132$ and performs the unitary transform $U(132)$. Then B_2 obtains the quantum state $|\phi_2\rangle$, where $|\phi_2\rangle=U(132)|\phi_1\rangle$ and transmits it and the classical information $M'=220$to B_5.

Certainly, the order of the agent B_1 and B_2 can be exchange, that is, Alice firstly send the quantum state and classical information to B_2, and then B_2 transmits it to B_1. Finally, B_5 take the unitary matrix $U(x_5)$ with $x_5=40$ on the quantum state $|\phi_{t-1}\rangle$, which can reconstruct the initial quantum state $|\phi_0\rangle$. All of the unitary transformations are

$$U(40)U(132)U(165)U(-337)=U(0)=I \tag{14}$$

where I is the identify matrix.

5. The Analysis and Discussion

5.1 The Correctness of the Proposed Protocol

Firstly, one can obtain that $x_{i_1}+x_{i_2}+x_{x_{i_t}}+k_1M-x=0$ according to the Chinese reminder theorem, and therefore $x_{i_1}+x_{i_2}+x_{x_{i_t}}+x'=0$.

By utilizing $t+1$ times unitary quantum operators from Alice, B_{i_1}, B_{i_2},⋯, and B_{i_t} separately, the initial quantum state $|\phi_0\rangle$ will become

$$\begin{aligned}&U(x_{i_t})\cdots U(x_{i_2})U(x_{i_1})U(x')|\phi_0\rangle\\ &=U(x_{i_t}+x_{i_2}+\cdots+x_{i_1}+x'M)|\phi_0\rangle\\ &=U(0)|\phi_0\rangle\\ &=|\phi_0\rangle\end{aligned} \tag{15}$$

Therefore, the last selected agent B_{i_t} will reconstruct the target state $|\phi_0\rangle$, meaning that the proposed scheme is correct.

5.2 The analysis of the proposed protocol

In our work, the Chinese Reminder Theorem is introduced to implement the construction of the (*n*, *t*) structure. The idea is that taking the solution as the secret key and distribute all the remainders to the corresponding agents. In addition, the information obtain is encoded into the quantum unitary transformations, in particularly, the quantum phase Z gate is introduced. In our work, not only the private keys of the dealer and *n* agents can be easily generated, but also the procedure can be easily finished practically.

6. Conclusion

In this paper, a new kind of (*n*,*t*) threshold quantum state sharing scheme was proposed where the selected *t* agents among *n* agents can cooperate to reconstruct the target secret state, by utilizing the Chinese reminder theorem. Moreover, the proof of the correctness of the scheme was shown. Our scheme can improve the development the quantum secret sharing and open up exploring the application of quantum information technology.

References

[1] Hayashi, M., Ishizaka, S., Kawachi, A., et al. Introduction to Quantum Information Science [M]. Springer, 2014.

[2] Bennett, C. H., Bessette, F., Brassard, G., et al. Experimental quantum cryptography [J]. Journal of Cryptology, 1992, 5(1): 3-28.

[3] . Shor, P. W. Algorithms for quantum computation: Discrete logarithms and factoring [C]. in Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994: IEEE.

[4] Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme [J]. Physical Review A, 2002, 65(3): 032302.

[5] Boström K a F, Timo. Deterministic Secure Direct Communication Using Entanglement [J]. Physical review letters, 2002, 89(01): 187902.

[6] Bennett, C. H., Brassard, G., Crépeau, C., et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels [J]. Physical Review Letters, 1993, 70(13): 1895.

[7] Hillery, M., Bužek, V., and Berthiaume, A. Quantum secret sharing [J]. Physical Review A, 1999, 59(3): 1829.

[8] Karlsson, A., Koashi, M., and Imoto, N. Quantum entanglement for secret sharing and secret splitting [J]. Physical Review A, 1999, 59(1): 162.

[9] Yang, Y. G., Yang, J. J., Zhou, Y. H., et al. Quantum secret sharing among four players using multipartite bound entanglement of an optical field [J]. Physical Review Letters, 2018, 121(15): 150502.

[10] Ghosh, S., Kar, G., Roy, A., et al. Entanglement teleportation through GHZ-class states [J]. New Journal of Physics, 2002, 4(1): 48.

[11] Zhang, Q., Goebel, A., Wagenknecht, C., et al. Experimental quantum teleportation of a two-qubit composite system [J]. Nature Physics, 2006, 2(10): 678-682.

[12] Lee, S. M., Lee, S. W., Jeong, H., et al. Quantum teleportation of shared quantum secret [J]. Physical Review Letters, 2020, 124(6): 060501.

[13] Kimble, H. J. The quantum internet [J]. Nature, 2008, 453(7198): 1023-1030.

[14] Xia, X. X., Sun, Q. C., Zhang, Q., et al. Long-distance quantum teleportation [J]. Quantum Science and Technology, 2017, 3(1): 014012.