PROTOCOL AND APPLICATIONS FOR SHARING QUANTUM PRIVATE KEYS

Han-Wei Wang[1], *Tien-Sheng Lin*[1,2], *I-Ming Tsai*[1], *and Sy-Yen Kuo*[1]

[1]Department of Electrical Engineering, National Taiwan University
No.1, Sec. 4, Roosevelt Road, Taipei, Taiwan, 106
[2]Department of International Trade, Lan Yang Institute of Technology
No.79, Fu Shin Road, Tou Chen, I Lan, Taiwan, 261

ABSTRACT

Transmitting message in secret is getting more and more important nowadays. In the classical world, the message we sent run the risk of being intercepted by an attacker. As a result, we have to encrypt the message, or send it using a private channel. However, if we transmit messages via such methods, there are still some ways to decipher the information. For example, a powerful computer can be used to decrypt the message or try to steal the message from the private channel.

In quantum cryptography, entanglement can be used as a secure channel to transmit information with absolute secrecy. From this perspective, quantum entanglement pairs are equivalent to a quantum private key. However, like the classical key distribution problem, the entanglement has to be shared before it can be used. In this paper, we propose a protocol that can be used to distribute such entanglement pairs securely, so they can be subsequently used to transmit messages with perfect security. The security of this protocol is based on the laws of nature, instead of unproven mathematical hard problems.

1. INTRODUCTION

In classical cryptography, there are some one-way functions that are easy to calculate in one direction but difficult in the other direction. This property can be used to derive many encryption protocols. Notice that the security of these algorithms depends on the assumption that there is no fast algorithm to find out the answer of the one-way function. However, there are some efficient quantum algorithms have been found to break these classical encryption algorithms. For instance, Shor's quantum algorithm [1] can be used to solve factoring problem in polynomial time, and RSA will be no more secure. Moreover, Grover's algorithm [2] can be used to do an exhaustive key search for DES or AES.

Recent study shows that quantum cryptography provides an option to perform secret communication. The most straightforward application of quantum cryptography is quantum key distribution [3][4]. Even in the presence of an eavesdropper with unlimited computing power, the laws of physics (instead of mathematical conjectures) guarantee that the secret key exchange will be secure. For example, BB84 [3] is one of the protocols to perform key distribution. It is a simple 'prepare-and-measure' protocol, and can easily make up a secret key securely using current technology. Once this secret key is established, it can be used with classical cryptographic techniques (such as one-time-pad) to allow two parties to exchange messages in absolute secrecy. In this paper, we propose a protocol to distribute entanglement pairs that can be subsequently used as private keys. Unlike classical key distribution protocols, its security is based on the laws of nature, instead of unproven mathematical hard problems [5][6].

2. PRELIMINARIES ON ENTANGLEMENT

There are some tiny particles that have discrete energy level. If they have quantum properties, we call them quantum bits, or briefed the name as qubits. Each qubit has its quantum state, we can measure $|0\rangle$ or $|1\rangle$ if the quantum state of qubit is two state particle. Moreover, we can apply some operations onto the qubit to change their quantum state. For example, σ_x rotate quantum state up to 90 degrees along the x axis, so is σ_y or σ_z.

In quantum mechanics, the state of a single two-level quantum bit (qubit) can be written as a linear combination in a two-dimensional complex vector space

0-7803-9245-0/05/$20.00

as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (1)$$

where α and β are complex numbers and $|\alpha|^2 + |\beta|^2 = 1$. The two orthonormal states $|0\rangle$ and $|1\rangle$ forms a computational basis of the system and the contribution of each basis state to the overall state (in this case $|\alpha|$ and $|\beta|$) is called the probability amplitude.

According to quantum mechanics, when the system is measured, the state *collapses* to one of the basis states ($|0\rangle$ or $|1\rangle$). The probability of collapsing to a particular basis state is directly proportional to the square of the amplitude associated with it.

The state described above exhibits an unique phenomenon called quantum *superposition* which means the particle has a part corresponding to $|0\rangle$ and a part corresponding to $|1\rangle$, at the same time. However, when a measurement is performed, it collapses to one of the states in the basis (eigenstates). An interesting phenomenon in measurement of a multi-particle state is called *entanglement*. Imagine that Alice and Bob share a two-qubit system in the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{ab}, \quad (2)$$

where a and b denote Alice and Bob respectively. According to quantum mechanics, if Alice takes a measurement on qubit a, the state of the qubit will collapse to $|0\rangle$ with a probability of $1/2$.

Moreover, in this case Alice immediately knows that the state of the other qubit (qubit b) must be $|0\rangle$. In other words, once the measurement result of one qubit is decided, the state of the other one is perfectly correlated and can be instantaneously decided, no matter how far away Alice and Bob are separated. A similar result happens if the result of Alice's measurement is $|1\rangle$. This non-classical correlation among multiple quantum systems is called quantum entanglement, because they can not be written as separable states and are considered to be entangled.

Entanglement can be used to perform, for example, secure communication (an example of doing this will be given in section 4). However, like the classical key distribution problem, the entanglement has to be securely shared first. One possible way to do this is to directly transmit one qubit in Eq.(2) to the receiver, but this is vulnerable to the coherent attack.

In this chapter, we present a protocol to accomplish this securely. The protocol is presented in the next section.

When the quantum state represents two or more qubits, there are some quantum states that can't be further decomposed by tensor product, which is called as entanglement. We take the advantage of entangled state during information transmission, because the qubits become relational, and they can affect the others jump to the special quantum state after measurement.

Therefore, if the quantum state of one qubit of the quantum EPR pair has been measured, then the other qubit will also be determined according the result of the former qubit. And no other people will be aware of that variance, let alone to steal the changed quantum information. This and so we can make up some communication protocol according to these special properties.

3. THE PROTOCOL

There are four steps in our entanglement sharing protocol. The resources and assumptions used in this protocol include a quantum channel between Alice and Bob and a classical public channel that can be used by Alice and Bob to exchange the transmission status. The classical channel does not have to be private. The only requirement of this channel is that all the messages transferred can be received by the recipient without being modified.

For example, a reliable radio broadcast in a non-jamming environment serves as the channel we require. The protocol is described as below.

In our protocol, if Alice and Bob want to share N entanglement pairs, then Alice must prepare $N + M$ quantum EPR pairs (which equals a total number of $2 \times (N + M)$ qubits). And the M entanglement pairs are used for verification. Beneath are the four steps to share N entanglement pairs securely. Notice that if M increases, then the success probability to be attacked will decrease exponentially. And it is a trade-off between security and the number of qubits we send.

STEP 1:
Alice prepares $N+M$ entanglement pairs that are chosen randomly from the following three types of entanglement states. Type I is the entanglement as described above:

$$T_1 = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{ab}. \quad (3)$$

Type II is to rotate qubit b for $\pi/4$ along the $\hat{y}$ axis. It can be written as

$$T_2 = \frac{1}{2}(|0\rangle(|0\rangle + |1\rangle) + |1\rangle(|0\rangle - |1\rangle))_{ab}. \quad (4)$$

Type III is to rotate qubit b for $\pi/4$ along the $\hat{x}$ axis. It can be written as

$$T_3 = \frac{1}{2}(|0\rangle(|0\rangle + i|1\rangle) + |1\rangle(|0\rangle - i|1\rangle))_{ab}. \quad (5)$$

By defining $|z^+\rangle = |0\rangle$ and $|z^-\rangle = |1\rangle$, we have $|x^\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and $|y^\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$. Hence, these entanglement pairs can be written as

$$T_1 = \frac{1}{\sqrt{2}}(|0\rangle|z^+\rangle + |1\rangle|z^-\rangle)_{ab} \quad (6)$$

$$T_2 = \frac{1}{\sqrt{2}}(|0\rangle|x^+\rangle + |1\rangle|x^-\rangle)_{ab} \quad (7)$$

$$T_3 = \frac{1}{\sqrt{2}}(|0\rangle|y^+\rangle + |1\rangle|y^-\rangle)_{ab} \quad (8)$$

STEP 2:
Alice sends Bob qubit b from each entanglement pair via the quantum channel and Bob informs Alice via the classical public channel after he receives these qubits.

STEP 3:
Alice announces the types of all the entanglement pairs she had prepared via the classical public channel. Bob chooses M entanglement pairs randomly for further verification. Then Bob measures these qubits according to the bases that Alice had announced (*i.e.* along $\hat{z}$ for T_1, along $\hat{x}$ for T_2, along $\hat{y}$ for T_3). Then he announces the results of his measurements via the classical public channel.

STEP 4:
Alice measures the corresponding qubits to see if they are correct. Because of the entanglement between qubit a and b, when Alice measures her qubit of the same entanglement pair, her result should be correlated with Bob's measurement. More specifically, Alice's results of $|z^+\rangle$ should appear with Bob's result of $|x^+\rangle$, $|y^+\rangle$, or $|z^+\rangle$, depending on the entanglement type prepared by Alice.

If these results are correct, then the remaining entanglement pairs are shared securely between Alice and Bob. If Bob's results are different from Alice's results, then they can either abort the protocol or redo these steps, because there might be eavesdroppers in the channel.

4. APPLICATIONS

After the establishment of these entanglement pairs, they can be used to transmit classical or quantum information secretly. Here we give an example of transmitting classical messages using these entanglement pairs. It takes one entanglement pair and one classical bit to transmit a classical bit secretly, and one entanglement pair and two classical bits to transmit a quantum state secretly. Now we show these two applications using the following examples.

4.1. Transmit classical information using entanglement pairs

Assuming Bob is to transmit a classical bit p ($p \in \{0,1\}$) to Alice and the entanglement they have shared is T_2.

First, Bob takes a measurement on qubit b along the basis Alice had announced (*i.e.* the $\hat{x}$ axis), and Alice takes a measurement on the other qubit along the $\hat{z}$ axis. The result is that Alice and Bob should share either $|0\rangle|x^+\rangle$ or $|1\rangle|x^-\rangle$ and no one else knows about it. In other words, if Bob interprets $|x^+\rangle$ as 0 and $|x^-\rangle$ as 1, actually they share a classical secret bit r ($r \in \{0,1\}$). To send the classical bit p to Alice secretly, Bob can simply send $m = r \oplus p$ to Alice in public, Alice can then perform an exclusive-or to recover the message bit p. They can change the presentation of basis whenever they want, and the frequently change of protocol also makes it hard to attack.

For example, assuming the quantum state after their measurement is $|0\rangle_A|X^+\rangle_B$, if Bob wants to send classical bit 0, then he should encrypt this bit as $0 \oplus 0 = 0$ on the public classical channel. On the other hand, if Bob wants to send classical bit 1, then he should encrypt this bit as $1 \oplus 0 = 1$. After Alice receives this bit, she can decrypt the classical bit Bob sent using the quantum state of her qubit. This encryption/decryption process applies identically if Alice is the sender.

4.2. Transmit quantum information using entanglement pairs

If the information Alice wants to transmit to Bob is the state of a qubit, then they have to set up their entanglement pair to type $T1$. This can be done by Bob via a local operation. If the entanglement they shared is type $T1$, then Bob does not have to do anything.

On the other hand, if their entanglement pair is type $T2$ or $T3$, Bob has to do a σ_y rotation operation or a σ_x rotation operation on his qubit to make their quantum state become type $T1$, and make the quantum state of their qubits to $|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B$.

Assume Alice wants to transmit a quantum state of $|\phi\rangle$ to Bob. Then Alice should prepare a qubit which its quantum state is $|\phi\rangle$. Firstly Alice measures both the qubit she has and qubit C along the Bell basis. After the measurement, Alice transfers the two states into two classical bits $(00, 01, 10, 11)$ and sends these two classical bits to Bob via public classical channel. Then Bob can do Bell operation on his qubit according to the two classical bits Alice sent. Bob's qubit will change to the same quantum state with the original quantum state of qubit C. The quantum information transmission protocol is called teleportation, and it is

a well-done protocol.

5. ANALYSIS

An important issue to protect our entanglement against Eve is that we do not want these quantum EPR pairs to be intercepted or copied or even destroyed during the transmission. In the transmission phase, we take advantages of the uncertainty principle that allows Alice and Bob to perform security checking. Because the qubits that sent to Bob are based on three orthogonal bases.

If Eve measures the quantum state of the qubit using a wrong basis, the original state mapping (caused by the entanglement) between Alice and Bob will be destroyed, Alice and Bob can check this relation of some randomly chosen entanglement pairs to prevent the attack. Because Alice is using different orthogonal bases in the second qubit, if Eve measures or copies this qubit along a wrong basis, then she will be wrong with the probability of 1/2. Because of the basis is orthogonal, so that the value will be projected to the right or wrong state along the measured basis randomly. If Alice and Bob use more entanglement pairs for verification, then Eve has an exponentially small probability to steal or copy the qubit without being detected.

Some possible attacks for Eve are discussed as follows.

1. If Eve measures the qubit, then she may be detected. Because there are three orthogonal basis, if she measures along the wrong basis, she has the probability of 1/2 to make the quantum state of Alice and Bob different.

2. If Eve only copies some of the qubits Alice sent using control-not gate. If Eve copies n qubits, the number of the expected value of qubits used for verification is $n*[M/(N+M)]$, then She have the probability of $(2/3)^{n*[M/(N+M)]}$ to attack success and get the quantum state of the rest $n*[N/(N+M)]$ qubits. But if M is big enough, then the probability trends to be very small. Moreover, when n is very big, the probability trends to be zero, too. For example, if n is 20 and we take 10 entanglement pairs for verification, then the probability is $(2/3)^{10} = 0.01734$. That is, if Eve copies 20 qubits, then she has the probability of 0.01734 to get the quantum state of the rest 10 qubits.

3. If there is a man in the middle, Alice and Bob can do verification using half of the entanglement pairs via the public authenticated classical channel, and they can always get the status of each other. Because in an authenticated channel no one can modify the message between Alice and Bob, if they detect anything wrong, they can ask for retransmission via the classical channel to prevent the man-in-the-middle attack. And there is no way for Eve to use try and error attack method, because Alice and Bob are communicated by entanglement. She has no way to know the quantum state of the qubits they shared.

6. CONCLUSION

In this paper, quantum entanglement pairs are used as private keys. We present a quantum key distribution protocol which allows two parties to securely share entanglement pairs that can be subsequently used to perform private communication. Eavesdroppers are not able to deduce the message and will be detected if they do exist. The security of this protocol is based on the laws of physics, instead of unproven mathematical conjectures.

7. REFERENCES

[1] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proc. of the 35th Annual IEEE Symposium on the Foundations of Computer Science*, 1994, pp. 124-134.

[2] L. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. of the 28th Annual ACM Symposium on the Theory of Computing*, 1996, pp. 212-219.

[3] C. Bennett and G. Brassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, December 1984, pp. 175-179.

[4] C. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, pp. 3121 - 2124.

[5] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. (2) 21, pp. 120-126 (1978).

[6] W. Diffie, and M. E. Hellman, "Multiuser Cryptogrphic Techniques," in *Proceeding of AFIPS National Computer Conference*, pp. 644-654 (1976).