Deterministic Key Distribution Scheme based on the Non-locality of Unentangled States

Xiaoyu Li*[1], Qiuyu Zhao[2]
[1]School of Information Engineering, Zhengzhou University, Zhengzhou City, 450001, the People's Republic of China
[2]Editorial Department of Journal of Xuchang University, Xuchang University, Xuchang City, 461000, the People's Republic of China
Corresponding author, e-mail: iexyli@zzu.edu.cn*, zqy@xuc.edu.cn

Abstract

In this paper we provide a deterministic key distribution scheme based on the non-locality of untangled states in which people can share a predeterministic string as the key. The fundamental Laws of quantum mechanics guarantee that the scheme is unconditionally secure. There are no entangled states or complex quantum operations needed in our scheme. We show that our scheme is easy to carry out in practice. Moreover our scheme is robust against possible noise and attacks.

Keywords*: deterministic key distribution, quantum cryptography, non-locality, untangled states, orthogonal product states*

1. Introduction

The aim of cryptography is to send secret information through an insecure channel. To keep the information secret, people often integrate the original information (called "plain text") with some auxiliary information (called "key") to produce the encrypted information (called "cipher text"). Only the cipher text is transmitted so anyone can get the cipher text. But no one can recover the plain text except the authenticated user who has the key. Then two users who share the key can perform secret communications. But how to distribute the key is the most important and most difficult problem. In fact there are no unconditionally secure key distribution schemes in classical cryptography.

Quantum key distribution (QKD) scheme is a good way to solve this problem. In QKD schemes we can achieve unconditional secure key distribution with an insecure quantum channel and an insecure but unjammed classical channel. The first quantum key distribution scheme is proposed by C. H. Bennett and G. Brassard in 1984 (so called BB84 scheme) [1]. Since then many quantum key distribution schemes have been established and their securities have been studied, such as the EPR schemes [2], B92 [3], the scheme of Lo-Chau [4], and so on [5-17]. On the other hand experimental work for OKD has also succeeded. In 1992 Bennett, Bessette and Brassard first realized BB84 scheme in laboratory [18]. Recently QKD in optical fiber has been achieved beyond 150 km [19] and in free space has been implemented over a distance of 1 km [20].

In most of the precious quantum key distribution schemes, the final key which is built between the two parties is a random string. It is produced by the random measurement results of a quantum system. But sometimes people may need to share a predeterministic string as the key. It's a realistic requirement which often appears in business and military affairs. Obviously the previous schemes can't help us to make it. A quantum deterministic key distribution key scheme using the Bell state measurement is present in [21]. The two parties can build a predeterministic string as the key with the help of entangled states and the Bell state measurement. But there are entangled states needed which makes the scheme difficult to fulfill in practice. In this paper we present a quantum deterministic key distribution scheme using orthogonal product states in which no entangled states and complex operations are needed. So it is easier to carry out and more robust in practice.

Received December 16, 2012; Revised March 17, 2013; Accepted April 13, 2013

2. Basic Idea

In quantum information science a two-state quantum system is often called a qubit while a three-state quantum system is called a qutrit. Once people thought that non-locality can only be found in entangled states system. But in [22] Bennett et al proved that a set of non-entangled orthogonal product states in a two-qutrit system can also show non-locality. There is a complete orthogonal set of states in this system:

$$|\varphi_1>=|1>|1> \ |\varphi_2>=|0>\frac{1}{\sqrt{2}}(|0>+|1>),\ |\varphi_3>=|0>\frac{1}{\sqrt{2}}(|0>-|1>)$$
$$|\varphi_4>=|2>\frac{1}{\sqrt{2}}(|1>+|2>), \qquad |\varphi_5>=|2>\frac{1}{\sqrt{2}}(|1>-|2>),$$
$$|\varphi_6>=\frac{1}{\sqrt{2}}(|1>+|2>)|0>, \qquad |\varphi_7>=\frac{1}{\sqrt{2}}(|1>-|2>)|0>,$$
$$|\varphi_8>=\frac{1}{\sqrt{2}}(|0>+|1>)|2>, \qquad |\varphi_9>=\frac{1}{\sqrt{2}}(|0>-|1>)|2> \qquad (1)$$

In which we can perform a collective measuremnt on a two-qutrit system. It is proved in [22] that these nine states can't be distinguished reliably by local operations and classical communications, that is to say, it's impossible to confirm the state uniquely in this vector set by local operations and classical communications. We can design a deterministic key distribution scheme based on this property as follows. First Alice and Bob agree to such coding rule.

Coding Rule:

$$|\varphi_2>\rightarrow 0 \quad |\varphi_3>\rightarrow 1 \quad |\varphi_4>\rightarrow 0 \quad |\varphi_5>\rightarrow 1 \qquad (2)$$

Alice creates a two-qutrit system in one of the nine states $\{|\varphi_1>,|\varphi_2>,....,|\varphi_9>\}$ at random and records her choices. Then Alice sends the second qutrit to Bob and keeps the first qutrit at her hands. To discriminate the two qutrits, we mark them qutrit 1 and qutrit 2 respectively. When Bob receives qutrit 2, Alice declares the state of qutrit 1 while she still keeps the state of the two-qutrit system secret. If the state of qutrit 1 is $|\varphi_1>,|\varphi_6>,|\varphi_7>,|\varphi_8>$ or $|\varphi_9>$, Alice and Bob abandon it and turn to the first step, that is to say Alice creates a new two-qutrit system again and repeat the following steps. If the state of qutrit 1 is $|\varphi_2>,|\varphi_3>,|\varphi_4>,$ or $|\varphi_5>$, Bob creates an auxiliary qutrit named qutrit E in the same state as qutrit 1. Then Bob perform collective measurement on the composed two-qutrit system of qutri E and qutrit 2 in basis $\{|\varphi_1>,|\varphi_2>,....,|\varphi_9>\}$. So Bob will get the state of the new two-qutrit system of qutri E and qutrit 1 which is just the same as the state of composed two-qutrit system of qutrit 1 and qutrit 2. Finally Alice and Bob get a bit respectively according to the Coding Rule. If Alice wants to share a bit “0” with Bob, she only needs to do according to the following Rule 1.

Rule 1:

If the state of the composed system of qutrit 1 and qutrit 2 is $|\varphi_2>,$ or $|\varphi_4>$, Alice asks Bob nothing to do but keep the bit he gets; If the state of the composed system of qutrit 1 and qutrit 2 is $|\varphi_3>,$ or $|\varphi_5>$, Alice asks Bo to reverse the bit he gets.

On the other hand, if Alice wants to share a bit “1” with Bob, she does according to Rule 2.

Rule 2:

If the state of the composed system of qutrit 1 and qutrit 2 is $|\varphi_2>,$ or $|\varphi_4>$, Alice asks Bob to reverse the bit he gets. If the state of the composed system of qutrit 1 and qutrit 2 is $|\varphi_3>,$ or $|\varphi_5>$, Alice asks Bob nothing to do but keep the bit he gets.

Finally Bob is sure to get the bit which Alice wants to share with him. The process of the key rules can be summarized as following tables.

Table 1. Key Rule 1. ...

String (Alice)	Origin state (Alice)	Dictate (Alice to Bob)	Measurement result (Bob)	String (Bob)
0	$\|\varphi_2>$	Nothing to do	$\|\varphi_2>$	0
	$\|\varphi_4>$	Nothing to fo	$\|\varphi_4>$	0
	$\|\varphi_3>$	Reverse the bit	$\|\varphi_3>$	0
	$\|\varphi_5>$	Reverse the bit	$\|\varphi_5>$	0

Table 2. Key Rule 2. ...

String (Alice)	Origin state (Alice)	Dictate (Alice to Bob)	Measurement result (Bob)	String (Bob)
1	$\|\varphi_2>$	Reverse the bit	$\|\varphi_2>$	1
	$\|\varphi_4>$	Reverse the bit	$\|\varphi_4>$	1
	$\|\varphi_3>$	Reverse the bit	$\|\varphi_3>$	1
	$\|\varphi_5>$	Reverse the bit	$\|\varphi_5>$	1

In section 4 we will prove that by a well-designed error-checking process we can prevent anyone except Alice and Bob from getting the bit. So we can develop a deterministic key distribution scheme based on these facts above.

3. Deterministic Key Distribution using Orthogonal Product Quantum State

Now we present our deterministic key distribution scheme.

If Alice wants to share a predeterministic n-bit string named K with Bob as the key. They do as the following steps.

Step 1: Alice creates N two-qutrit system (N>>n) in one state in the set $\{|\varphi_1>,|\varphi_2>,....,|\varphi_9>\}$ at random and records her choices.

Step 2: Alice sends qutrit 2 of each two-qutrit system to Bob.

Step 3: After Bob receives the qutrits, to each two-qutrit system Alice chooses it out and declares its state if it is in the state $|\varphi_1>,|\varphi_6>,|\varphi_7>,|\varphi_8>$ or $|\varphi_9>$ while Alice keep its state secret if it is in the state $|\varphi_2>,|\varphi_3>,|\varphi_4>,$ or $|\varphi_5>$. Let's assume that there are m two-qutrit systems chosen out. So there are N-m two-qutrit systems left whose states are still secret.

Step 4: To each of the m two-qutrit system, Bob creates an auxiliary qutrit (qutrit E) in the same state as the qutrit 1 whose state is now public. Then Bob performs collective measurement on the composed system consisting of the qutrit E and qutrit 2 in basis $\{|\varphi_1>,|\varphi_2>,....,|\varphi_9>\}$.

step 5(error-checking): To each composed system consisting of qutrit E and qutrit 2 Bob compares his measurement result with the state of corresponding two-qutrit system consisting of qutrit 1 and qutrit 2 which Alice has declared. If there are too many disagreements, Alice and Bob abandon the scheme and turn back into step 1. Else they continue to step 6.

Step 6: Alice and Bob choose m two-qutrit systems out at random and discard the others. Because N>>n, so they can always accomplish it.

Step 7: To each one of the left n two-qutrit systems, Alice declares the state of qutrit 1 of every two-qutrit system and send dictates to Bob according to K as Rule 1 and Rule 2 ask.

Step 8: To each one of these two-qutrit systems Bob creates an auxiliary qutrit (qutrit E) in the same state as the qutrit 1. Then Bob performs collective measurements on the composed systems consisting of qutrit E and qutrit 2 in basis $\{|\varphi_1>,|\varphi_2>,....,|\varphi_9>\}$ and records his measurement results. Next Bob does as Alice's dictates ask. Finally he will get an n-bit string named K1.

Step 9: Obviously we have K1=K. It is just the key that Alice and Bob want to share in our deterministic key distribution scheme.

Now Alice and Bob have established a shared key using a predeterministic string.

4. Security of the Scheme

Our scheme is secure. No one except Alice and Bob can get the key. We prove it as follows.

Let's assume that an eavesdropper, for example, Eve, wants to get the key. She may catch the qutrits sent from Alice to Bob and try to get some information about the key. We can prove that it’s impossible. From Equation (1) we can notice that the possible states set of qutrit 2 is $\{|0>,|1>,|2>,\frac{1}{\sqrt{2}}(|0>+|1>),\frac{1}{\sqrt{2}}(|0>-|1>),\frac{1}{\sqrt{2}}(|1>+|2>),\frac{1}{\sqrt{2}}(|1>-|2>)\}$ Which contains seven states. These states aren’t nonorthogonal to each other. As known nonorthogonal quantum states are indistinguishable. So Eve can’t know the state of qutrit 2 with certainty whatever she does, or in other words, she can’t get the key just as Bob. We can estimate the probability she fortunately get a bit. Notice that if Eve chooses exact the correct basis to measure qutrit 2 she catched, she may know the state of qutrit with certain and get a bit of the key at last. But to the qutrit, Eve can get its state with certainty only when she choose the correct basis to measure. It’s easy to find that there are three possible basises.

$$\begin{aligned}
&B1=\{|0>,|1>,|2>\},\\
&B2=\{\frac{1}{\sqrt{2}}(|0>+|1>),\frac{1}{\sqrt{2}}(|0>-|1>),|2>\}\\
&B3=\{|0>,\frac{1}{\sqrt{2}}(|1>+|2>),\frac{1}{\sqrt{2}}(|1>-|2>)\}
\end{aligned} \tag{3}$$

If Eve choose the incorrect basis, she only get the state with a probability p(p<1). It can be summarized as the following table.

State	|0>	|1>	|2>	$\frac{1}{\sqrt{2}}(\|0>+\|1>)$	$\frac{1}{\sqrt{2}}(\|0>-\|1>)$	$\frac{1}{\sqrt{2}}(\|1>+\|2>)$	$\frac{1}{\sqrt{2}}(\|1>-\|2>)$
B1	1	1	1	0	0	0	0
B2	0	0	1	1	1	0	0
B3	1	0	0	0	0	1	1

Because no information can help Eve to choose correct basis, she has to meaosure qutrit 2 in one basis at random, or in other words, the probability that Eve choose any basis is 1/3. So from table 1 we can deduce that theprobability that to the seven states Eve chooses the correct basis and get the bit are:

$$\begin{aligned}
&p_1=1/3\times 2=2/3,\ p_2=1/3\times 1=1/3,\ p_3=1/3\times 2=2/3,\ p_4=1/3\times 1=1/3\\
&p_5=1/3\times 1=1/3,\ p_6=1/3\times 1=1/3,\ \ p_7=1/3\times 1=1/3
\end{aligned} \tag{4}$$

According to our ptrotocol, Alice creates the two-qutrit systems in one state of the set $\{|\varphi_1>,|\varphi_2>,....,|\varphi_9>\}$ at random. So for each state the probability is 1/9. From Equation (1) and Equation (4), the average probability which Eve get a bit witout being found by Alice and Bob is:

$$P=\frac{1}{9}\times(p_1\times 2+p_2+p_3\times 2+p_4+p_5+p_6+p_7)=\frac{13}{27}\ . \tag{5}$$

The length of the key is n. So the probability for Eve to get the key is:

$$P_{error} = p^n = \left(\frac{13}{27}\right)^n \tag{6}$$

If n=1000, we have:

$$P_{error} = p^n = \left(\frac{13}{27}\right)^{1000} \approx 10^{-300} \tag{7}$$

It’s a number too small to image. So Eve’s attack can’t succeed.

Since attacks by catching the qutrits fails, all that Eve can do is to listen to the public classical channel in which Alice sends her dictates to Bob. But she can just get the dictates that Alice tells Bob to perform operation on his strings from measurement results. The key is determined by not only Alice’s dictates, but also Bob's measurement results which are kept secret by Bob. Eve can’t get them. It’s easy to prove that Eve could obtain no information about the key as follows. First the measurement results Alice gets is random, or in other words, Alice will get measurement results $|\varphi_2>, |\varphi_3>, |\varphi_4>,$ or $|\varphi_5>$ with equal probability 1/4 no matter what string Alice wants to send to Bob. Then Alice sends dictates to Bob according to her measurement results as the two key rules ask. We can easily deduct from the four tables in section 2 as follows. If Eve gets a dictate from Alice to Bob, for example, “nothing to do”, she can’t get any information about the string which Alice sends to Bob because it may be 0 or 1 with equal probability 1/2. The same result does she get if the dictate is “reverse the bit”. So Eve has no way to get any more information about the key than random guessing. The probability she gets a correct two-bit string is:

$$p_e = \frac{1}{2}. \tag{8}$$

Then the probability she gets the n-bit key is:

$$P_{error} = p_e{}^n = \left(\frac{1}{2}\right)^n. \tag{9}$$

Let n=100 which is a common length of a key. We have:

$$P_{error} = \left(\frac{1}{2}\right)^{100} \approx 10^{-30}. \tag{10}$$

It’s also a number too small to image. So it’s impossible foe Eve to get the key in fact, or in other words, Eve’s attack fails.

Let’s consider resend attack. Eve may catch all the qutrits sent from Alice to Bob and send fake qutrit to let Bob get a fake key. But in step 5 of our scheme Alice and Bob perform error-checking. Because Eve doesn’t know the states of the original two-qutrit systems created by Alice, she can only create two-qutrit systems in one state of $\{|\varphi_1>, |\varphi_2>, ..., |\varphi_9>\}$ and send the second qutrit to Bob. So when Bob gets these qutrits and performs error-checking with Alice, they are sure to find many disagreements.The probability that Eve succeedds in cheating is equals to the probability that she just choose the same state as Alice’s two-qutrit system, which is 1/9. There are m two-qutrit system for error-checking. So the probability for Eve to escape from being found by Alice and Bob is:

$$P_{error} = \left(\frac{1}{9}\right)^m \tag{11}$$

If m=100, we have:

$$P_{error} = \left(\frac{1}{9}\right)^{100} \approx 10^{-95} \tag{12}$$

So Alice and Bob abandon the scheme and turn back into step 1. That is to say, Eve’s attack fails. So we have proved that our scheme is unconditionally secure.

5. Feasibility Analysis of the Scheme

Notice that there are no entangled states and complex quantum operation needed in our scheme. All that people need to do is performing measurement on a qutrit and performing collective measurement on a two-qutrit system which have been mature technology in laboratory. So it's easier to carry out in practice. On the other hand without producing and controlling entangled states, without complex quantum operations make our scheme to have less fragility from noise, decoherence effects and possible attacks. So our scheme is more robust.

Second as known in quantum cryptographic schemes to keep quantum coherence is the most important and most difficult task. Especially in schemes using entangled states, the scheme is sure to fail if the entangled qubits lose coherence, or in other words, lose correlations between them. In practice quantum systems often undergo decoherence over time which make them lose quantum coherence and turn into classical systems inevitably. So the more work to handle and control quantum systems does a quantum cryptographic scheme need, the more difficult to accomplish it is. In our scheme the qutrits need to be tansfered for one time. To Alice, she won’t handle quantum at all after step 2, which means decoherence no onger affect Alice’s work. It will reduce the risk of decoherence much for our scheme. Onthe other hand Alice and Bob don’t exchange quantum information after step 2. What they need is only to exchange classical information. Or in other words, the quantum channel is no longer needed, which reduce the risk of decoheren of the quantum channel, too. So our scheme is easier to carry out in practice. This is a significant advantage of our scheme.

All that above discussions are based on that Alice and Bob always using noiseless channels to build a key in our scheme. If there are no noiseless channels, can this scheme work? In our scheme they need an unjamed classical channel and a quantum channel. The quantum channel can be insecure. An eavesdropper can control it, which we have discussed in section 4. At the same time it can be a noisy channel in which occasional mistakes may occur at random. When a qutrit is affected by channel noise and changes its state, it seems that such accident will threaten our scheme. We can prove that such error can’t cause our scheme fail. In step 4 of our scheme Alice and Bob do error-checking by comparing omeasurement results of m qutrits. If the error qutrit is in the m chosen qutrits, it will be found in the error-cheking and doesn’t affect the process of key building. Only when the error qutrit isn’t in the m chosen qubits, it may be left to contribute a mistaken bit to the key. On the other hand we can estimate the maximum probability that qutrit errors cause to the failure of the scheme. Let’s assume that the error rate of the channel is e. Alice and Bob choose m two-qutrit systems to do error-checking from N two-qutrit system. So the probability that an error qubit is chosen out for error-checking is m/N. We can conclude that a qutrit error is from being found is:

$$p = \frac{m}{N} \tag{13}$$

Then the probability that all error qubit escapes from being found is:

$$P_{error} = (1 - \frac{m}{N})^{Ne} \tag{14}$$

Let e=0.1, m=200, N=2000, which is a reasonable assumption, we have:

$$P_{error} = (1 - 0.1)^{200} \approx 0.000035 \tag{15}$$

It's an acceptable error rate for a noisy channel. If we need lower error-rate, we can use quantum error-correcting coding scheme which will be discussed in future work. So we can say our scheme works in a noisy quantum channel. However how about a noisy classical channel in our scheme? We can study it, too. In the step 2 in which Alice send qutrits with Bob, the classical channel must be unjamed and error-free because Alice and Bob's error-checking needs to exchange classical information. On a noisy classical channel, it can't be accomplish to build shared the two-qutrit systems between Alice and Bob. Fortunately classical error-correcting coding technology has been a mature and powerful now. We can fulfill information transmission through a noisy classical channel with very low error rate by error-correcting coding. On the other hand in step 7 in which Alice sends dictates to Bob, we also need a classical channel. This channel can be unsecure. Eavesdroppers can control it and catch the dictates form Alice to Bob. They can even sends fake dictates to Bob. All this doesn't prevent Alice and Bob from establishing a shared key, which we have proved in section 4. But if there are noise in this channel which make a dictate error, Bob will be unable to get the correct key. So we need try to avoid the error caused by the channel noise. The solution to it is still error-correcting coding. We can guarantee that Bob get the correct dictates by transmitting them using error-correcting coding.

6. Conclusion

A deterministic key distribution scheme using orthogonal product states is present. People can share a predeterministic string as the key. We prove that the scheme is unconditionally secure. There are no entangled states or complex quantum operations needed in our scheme. So it's easy to carry out in practice and robust against possible noise and attacks.

Acknowledgement

This work is supported by Natural Science Foundation of China (Grants 61073023); We would thank Ruqian Lu for directing us into this research.

References

[1] Bennet C, Brassard G. *Quantum cryptography: Public-key distribution and tossing*. Proceedings of IEEE International conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE Press. 1984: 175.

[2] Ekert A. Quantum cryptography based on Bell's theorem. *Physical Review Letters*. 1991; 67: 661-663.

[3] CH Bennett, G Brassard G, Mermin N. Quantum cryptography without Bell's theorem. *Physical Review Letters*. 1992; 68: 557-559.

[4] Lo H, Chau H Science. *Unconditional Security of Quantum Key Distribution over arbitrarily long distances*.Science. 1999; 283: 2050-2056.

[5] Cabello A. *Quantum Key Distribution in the Holevo Limit*. Physical Review Letters. 2000; 85: 5635-5638.

[6] Xue P, Li CF, Guo GC. Efficient quantum-key-distribution scheme with non-maximally entangled states. *Physical Review A*. 2001; 64: 032305.

[7] Li XY. Efficient Quantum Key Distribution Scheme using the Bell State Measurement. *International Journal of Modern Physics C*. 2003; 14(6): 757-763.

[8] Deng FG, Long GL. Bidirectional quantum key distribution protocol with practical faint laser pulses. *Physical Review A*. 2004; 70: 012311.

[9] Namiki R, Hirano T. Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection. *Physical Review A.* 2006; 74: 032301.

[10] Qi B, Zhao X, Ma XF, Lo H-K, Qian L. Quantum key distribution with dual detectors. *Physical Review A*. 2007; 75: 052304.

[11] Adachi Y, Yamamoto T, Koashi M, Imoto N. Simple and efficient quantum key distribution with parametric down-conversion. *Physical Review Letters.* 2007; 99: 180503.

[12] Yin ZQ, Han ZF, Sun FW, Guo GC. Decoy State Quantum Key Distribution with Modified Coherent State. *Physical Review A*. 2007; 76: 014304.

[13] Matsumoto R. Quantum multiparty key distribution protocol without use of entanglement. *Physical Review A*. 2007; 76: 062316.

[14] Ahonen A, Mottonen M, O'Brien J. Entanglement-enhanced quantum key distribution. *Physical Review A*. 2008; 78: 032314.

[15] Zhao Y, Qi B, Lo H-K. Quantum key distribution with an unknown and untrusted source. *Physical Review A*. 2008; 77: 052327.

[16] Choi T, Choi M. Quantum Key Distribution Using Quantum Faraday Rotators. *Journal of Physics: Condensed Matter.* 2008; 20: 275242.

[17] Horodecki K, Horodecki P, Leung D, Oppenheim J. Quantum key distribution based on private states: unconditional security over untrusted channels with zero quantum capacity. *IEEE Transaction Information Theory.* 2008; 54(6): 2604-2620.

[18] Bennett C, Bessette F, Brassard G, Salvail L, Smolin J. Experimental quantum cryptography. *Journal of Cryptology.* 1992; 5(1): 3-28.

[19] Kimura T, Y Nambu Y, Hatanaka T, Tomita A, Kosaka H, Nakamura K. Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography. *Eprints: quant-ph/0403104.*

[20] Buttler W, et al. Practical Free-Space Quantum Key Distribution over 1 km. *Physical Review Letters.* 1998; 81: 3283-3286.

[21] Li XY, Zhang DX. *Quantum determined key distribution scheme using Bell measurement*. International Conference on Networking and Digital Society, Guiyang. 2009; 1: 25-28.

[22] Bennett C, Divicenzo D, Fuchs C, et al. Quantum nonlocality without entanglement. *Physical Review A.* 1999; 59: 1070-1091.