Vol 15 No 8, August 2006
1009-1963/2006/15(08)/1690-05

Chinese Physics

© 2006 Chin. Phys. Soc.
and IOP Publishing Ltd

A quantum encryption scheme using d-level systems*

Guo Fen-Zhuo(郭奋卓)[a)b)], Gao Fei(高 飞)[a)], Wen Qiao-Yan(温巧燕)[a)], and Zhu Fu-Chen(朱甫臣)[c)]

[a)] *School of Science, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*
[b)] *State Key Laboratory of Integrated Services Network, Xidian University, Xi'an* 710071, *China*
[c)] *National Laboratory for Modern Communications, P.O. Box 810, Chengdu* 610041, *China*

(Received 20 May 2005; revised manuscript received 2 March 2006)

Using the generalized Bell states and quantum gates, we introduce a quantum encryption scheme of d-level states (qudits). The scheme can detect and correct arbitrary transmission errors using only local operations and classical communications between the communicators. In addition, the entanglement key used to encrypt can be recycled. The protocol is informationally secure, because the output state is a totally mixed one for every input state ρ.

Keywords: quantum encryption, d-level, quantum cryptography, quantum information
PACC: 0365, 4230, 4250

1. Introduction

The role of cryptography is to keep the data transmitted between the communicators unintelligible to a third party, and to prove that the message has not been changed in transmission. In a classical situation, one-time-pad[1] is the only known scheme that has unconditional security, and it requests a random bit string to encrypt, whose length is equal to the length of message. Therefore, how Alice and Bob can possess a secret key, while being sure that Eve does not have even partial information about it, becomes one of the main tasks of cryptography. Quantum key distribution (QKD) based on the quantum mechanics principle comes into being just for this work,[2−5] and it is the best one that can implement the above task up to now. Since the first QKD protocol[2] was proposed, quantum cryptography, as one branch of quantum information, has become more and more popular and mature in both theory and experiment. However, the study on the quantum analogue of the two well-known encryption schemes, which we call private-key and public-key schemes respectively, is insufficient compared with their classical counterparts. In Refs.[6,7], some results about quantum public-key cryptography were given, the algorithm of which may be practical only after a certain quantum algorithm (e.g. Shor's discrete logarithm problem) is efficiently realized on a quantum machine. In Refs.[8–14], some protocols about quantum private-key encryption were proposed, and the algorithms of them are relatively easy to implement. In this paper, we focus our interest on quantum private-key cryptography. That is, Alice and Bob share some secret key K, which can be classical bits or quantum states. Alice uses her half part of K to encrypt the message M into the cipher C through some quantum operations, and Bob uses his half part of K to recover M from C using the reversible operations. In particular, we use entanglement as the key in this paper.

In Ref.[14], Leung proposed a kind of quantum Vernam cipher for two-level systems, which is looked upon as the quantum analogue of the classical one-time-pad. Furthermore, it is shown that this scheme has two intriguing properties: (i) the quantum key can be recycled; (ii) any transmission error can be detected and corrected.

Generally speaking, two-level systems are competent for almost all quantum cryptography protocols. However, as far as quantum hardware is concerned, a bigger Hilbert space becomes indispensable. Therefore, the d-level system has significant advantage over the two-level one, because it is well known that coupling qubits becomes more difficult with the number of qubits increasing,[15] and bigger Hilbert spaces can

*Project supported by the National Natural Science Foundation of China (Grant No 60373059), the Special Research Fund for the Doctoral Program of Higher Education of China (Grant No 20040013007), the Major Research plan of the National Natural Science Foundation of China(Grant No 90604023), the National Laboratory for Modern Communications Science Foundation of China, the National Key Laboratory on Theory and Chief Technology of Integrated Services Networks (ISN) Open Foundation, and the Graduate Students Innovation Foundation of Beijing University of Posts and Telecommunications.

be made by coupling fewer d-level systems than the two-level ones. In addition, in most situations, Eve's eavesdropping introduces a higher error rate in d-level protocol than in the corresponding two-level one.[10,16] Moreover, the scheme in a dimension-free context is universal. The aim of this paper is to implement the quantum Vernam cipher in d-level systems, and maintain the above two properties at the same time.

The rest of this paper is organized as follows. In Section 2, we review the generalized Bell states and some of the basic gates, which have been given independently in Refs.[16–18]. In Section 3, we present the d-level quantum encryption scheme and show it is informationally secure. We show how the scheme can correct arbitrary transmission errors as well as recycle the key used to encrypt with semantically security in Section 4. And we give our conclusions in Section 5.

2. States and gates for d-level systems

For qudits, the computational basis is $\{|k\rangle\}$, with $k = 0, 1, ..., d-1$, and its dual under Fourier transform is $\{|\bar{l}\rangle\}$ with $|\bar{l}\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \zeta^{kl} |k\rangle$, where $\zeta = \mathrm{e}^{2\pi \mathrm{i}/d}$. A general state in a d-level system can be expressed as $|\varphi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle$, where $\sum_{i=0}^{d-1} |\alpha_i|^2 = 1$. The generalization of the familiar Bell states, which is a set of d^2 maximally entangled states, forms an orthonormal basis for the space of two qudits. Their explicit forms are $|\psi(m,n)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \zeta^{jn} |j, j+m\rangle$, where m and n both run from 0 to $d-1$. Note that all the computation in the kets must take modulo d here. The unitary operators $U_{m,n}$, defined as $U_{m,n} = \sum_{k=0}^{d-1} \zeta^{kn} |k+m\rangle\langle k|$, form a group of qudit error operators generalizing the Pauli errors for a two-level system, where m labels the shift error and n labels the phase error. That is, $U_{m,0} = \sum_{k=0}^{d-1} |k+m\rangle\langle k|$ refers to the shift error alone, and $U_{0,n} = \sum_{k=0}^{d-1} \zeta^{kn} |k\rangle\langle k|$ refers to the phase error alone. In particular, $R \equiv U_{1,0} = \sum_{k=0}^{d-1} |k+1\rangle\langle k|$ and $P \equiv U_{0,1} = \sum_{k=0}^{d-1} \zeta^{k} |k\rangle\langle k|$ are the generalized X gate and Z gate for the two-level system, respectively. Note that the operators $U_{m,n}$ are not necessarily Hermitian. For example, according to the definition $R|j\rangle = |j+1\rangle$ and $P|j\rangle = \zeta^j |j\rangle$, while $R^{-1}|j\rangle \equiv L|j\rangle = |j-1\rangle$ and $P^{-1}|j\rangle \equiv N|j\rangle = \zeta^{-j}|j\rangle$. The generalized Hadamard gate is

$$H \equiv \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \zeta^{ij} |i\rangle\langle j| \,,$$

which can change any computational basis into its dual basis.

For any unitary operator U, the controlled gate U_{c} that acts on the second qudit conditioned on the first qudit is $U_{\mathrm{c}}(|i\rangle \otimes |j\rangle) = |i\rangle \otimes U^i |j\rangle$, For example, $R_{\mathrm{c}}(|i\rangle \otimes |j\rangle) = |i\rangle \otimes |j+i\rangle$, $L_{\mathrm{c}}(|i\rangle \otimes |j\rangle) = |i\rangle \otimes |j-i\rangle$, $P_{\mathrm{c}}(|i\rangle \otimes |j\rangle) = |i\rangle \otimes \zeta^{ij} |j\rangle$, and $N_{\mathrm{c}}(|i\rangle \otimes |j\rangle) = |i\rangle \otimes \zeta^{-ij} |j\rangle$. If we consider the effect of above four controlled gates on the second qudit only, they are equivalent to $U_{i,0}|j\rangle = |j+i\rangle$, $U_{-i,0}|j\rangle = |j-i\rangle$, $U_{0,i}|j\rangle = \zeta^{ij}|j\rangle$, and $U_{0,-i}|j\rangle = \zeta^{-ij}|j\rangle$ respectively. For convenience, in what follows, we will use the latter expression.

3. Quantum encryption scheme for d-level states

In this section we implement the quantum Vernam cipher[14] in d-level systems and perform further analysis of the method.

3.1. The d-level quantum Vernam cipher

We use generalized Bell states as the key in our d-level scheme. The fundamental unit of entanglement for d-level systems is an 'edit'.

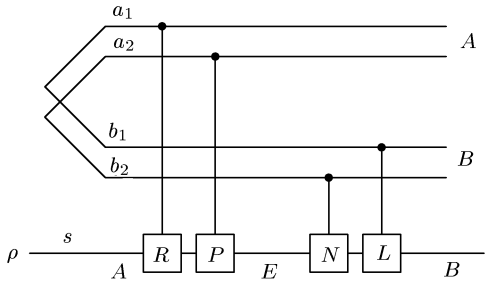


Fig.1. The d-level quantum Vernam cipher to send one qudit. Time runs from left to right. The symbols A, B, and E stand for Alice, Bob, and Eve and denote the owners of the registers.

To send a qudit given by $|\varphi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle$, Alice and Bob previously share two edits (a_1, b_1) and (a_2, b_2), both of which are in the form of

$$|\psi(0,0)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle|j\rangle \,,$$

where Alice possesses a_1 and a_2, Bob possesses b_1 and b_2. In the following, we refer to the register for the

sending message qudit as s. As illustrated in Fig.1, the initial states of Alice and Bob are

$$\begin{aligned}|\Phi_0\rangle =&|\psi(0,0)\rangle_{a_1,b_1}|\psi(0,0)\rangle_{a_2,b_2}|\varphi\rangle_s\\ =&\frac{1}{d}\sum_{i,j,k=0}^{d-1}\alpha_k|i\rangle_{a_1}|i\rangle_{b_1}|j\rangle_{a_2}|j\rangle_{b_2}|k\rangle_s\,.\end{aligned}$$

Alice applies $R_{\rm c}$ to s conditioned on a_1, followed by applying $P_{\rm c}$ to s conditioned on a_2, then $|\Phi_0\rangle$ arrives at

$$|\Phi_1\rangle=\frac{1}{d}\sum_{i,j,k=0}^{d-1}\alpha_k|i\rangle_{a_1}|i\rangle_{b_1}|j\rangle_{a_2}|j\rangle_{b_2}\zeta^{j(k+i)}|k+i\rangle_s\,.$$

When Bob receives s, he applies $N_{\rm c}$ to s conditioned on b_2 followed by applying $L_{\rm c}$ to s conditioned on b_1, then

$$\begin{aligned}|\Phi_1\rangle\rightarrow&\frac{1}{d}\sum_{i,j,k=0}^{d-1}\alpha_k|i\rangle_{a_1}|i\rangle_{b_1}|j\rangle_{a_2}|j\rangle_{b_2}\\ &\otimes\zeta^{j(k+i)}\zeta^{-j(k+i)}|k+i\rangle_s\\ \rightarrow&\frac{1}{d}\sum_{i,j,k=0}^{d-1}\alpha_k|i\rangle_{a_1}|i\rangle_{b_1}|j\rangle_{a_2}|j\rangle_{b_2}|k+i-i\rangle_s\\ =&|\Phi_0\rangle\,,\end{aligned}$$

thus Bob obtains $|\varphi\rangle$. To send an n-qudit state $|\Psi\rangle$, the one-qudit protocol is applied ditwise, as long as Alice and Bob share $2n$ edits named as $(a_1,b_1),...,(a_i,b_i),...,(a_{2n},b_{2n})$.

3.2. Informational security of the scheme

When Alice sends one qudit given by the density matrix $\rho=\sum_{m,n=0}^{d-1}\alpha_m\alpha_n^*|m\rangle\langle n|$ to Bob, they use two edits both given by $|\psi(0,0)\rangle$. Since s is the only register that carries the transmitted qudit, here we consider the effect of the controlled gates on s only, and use $U_{i,0}$ and $U_{0,j}$ to express the controlled-shift gate ($R_{\rm c}$) and controlled-phase gate ($P_{\rm c}$), respectively. From Eve's point of view, Alice is sending

$$\begin{aligned}\rho'=&\frac{1}{d^2}\sum_{i,j=0}^{d-1}U_{0,j}U_{i,0}\rho U_{i,0}^\dagger U_{0,j}^\dagger\\ =&\frac{1}{d^2}\sum_{i,j,m,n=0}^{d-1}\alpha_m\alpha_n^*\zeta^{j(m-n)}|m+i\rangle\langle n+i|\\ =&\frac{1}{d}\sum_{i,m=0}^{d-1}\alpha_m\alpha_m^*|m+i\rangle\langle m+i|\\ =&\frac{1}{d}[|\alpha_0|^2+\cdots+|\alpha_{d-1}|^2][|0\rangle\langle 0|\\ &+|1\rangle\langle 1|+\cdots+|d-1\rangle\langle d-1|]=\frac{I}{d}\,,\end{aligned}$$

which is independent of the input state ρ, and the third equation is obtained by summing over j and using the identity $\frac{1}{d}\sum_{j=0}^{d-1}\zeta^{jn}=\delta(n,0)$. To send an n-qudit state ρ with the kth qudit ρ^k, the one qudit scheme is applied ditwise. Let K be a $2n$-edit key with every two edits forming a block, and let the kth block denote the two-edit key acting on the kth qudit. The state from Alice to Bob is $\rho'=U_K\rho U_K^\dagger$, where $U_K=\otimes_k U_{0,j}^k U_{i,0}^k$, and for any $k\in\{1,2,...,n\}$, i and j are some certain values from $\{0,1,...,d-1\}$. $U_{i,0}^k$ and $U_{0,j}^k$ express $R_{\rm c}$ and $P_{\rm c}$ on the kth qudit respectively. From Eve's point of view, the n-qudit state ρ' is

$$\begin{aligned}\rho'=&\frac{1}{d^{2n}}\sum_K U_K\rho U_K^\dagger\\ =&\frac{1}{d^{2n}}\otimes_{k=1}^n\sum_{i,j=0}^{d-1}U_{0,j}^kU_{i,0}^k\rho^k(U_{i,0}^k)^\dagger(U_{0,j}^k)^\dagger=\frac{1}{d^n}I^{\otimes n}\,.\end{aligned}$$

Then according to Ref.[9], because the output state ρ' is the totally mixed state $\frac{1}{d^n}I^{\otimes n}$ for every input state ρ, the scheme is informationally secure.

4. Error correction

In the absence of eavesdropping, the circuit in Fig.1 acts trivially, so the message qudit is recovered, and the edit key is regenerated. In the following, we assume that during the transmission, Eve can take control of the sending qudit and thus introduce errors to it. Without loss of generality, we can represent the general errors with Pauli errors such as $U_{m,n}$ defined above. We will show that the d-level quantum encryption scheme can detect and correct any Pauli error appearing on the transmitted qudit. Firstly, in a similar way to that in Ref.[14], we have the following four basic error patterns (see Fig.2).

These four circuits are very simple, and here we only explain the last one as an example. Without loss of generality, let the message be $|\varphi\rangle=\sum_{i=0}^{d-1}\alpha_i|i\rangle$. Ordering the registers as (a,b,s), the system has an initial state $|\psi(0,0)\rangle|\varphi\rangle=\frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}\alpha_i|j\rangle|j\rangle|i\rangle$. Then the state changes as follows:

$$\rightarrow\frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}\alpha_i|j\rangle|j\rangle\zeta^{ji}|i\rangle \qquad (1)$$

$$\rightarrow\frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}\alpha_i|j\rangle|j\rangle\zeta^{ji}|i+m\rangle \qquad (2)$$

$$\rightarrow \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\zeta^{-jm}|j\rangle|j\rangle\sum_{i=0}^{d-1}\alpha_i|i+m\rangle\,, \qquad (3)$$

which describes the encoding Eq.(1), an error $U_{m,0}$ that has appeared on the message register s Eq.(2), and the edit key and message state after decoding Eq.(3). As can be seen after Bob's decoding, the message qudit and the edit key are disentangled. Summing up the above four situations, we find the effect of errors in the d-level Vernam cipher when sending one qudit (see Fig.3).

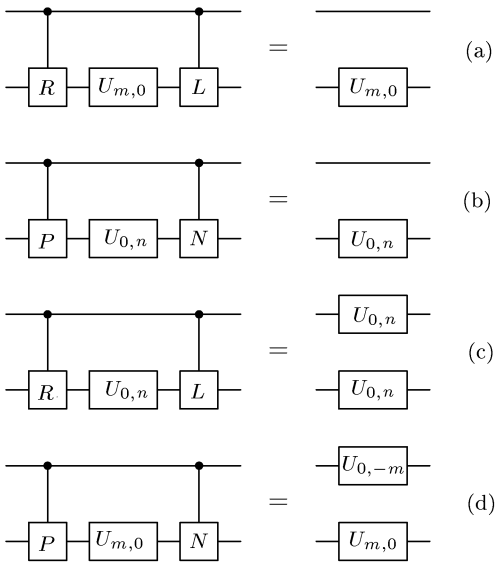


Fig.2. The entire four possible error patterns when Alice and Bob use an edit $|\psi(0,0)\rangle$ to send a message qudit: (a) A $U_{m,0}$ error in the transmitted cipher-text propagates to the decoded message; (b) A $U_{0,n}$ error in the transmitted cipher-text propagates to the decoded message; (c) A $U_{0,n}$ error in the transmitted cipher-text propagates to the decoded message together with a $U_{0,n}$ error on the edit key; (d) A $U_{m,0}$ error in the transmitted cipher-text propagates to the decoded message together with a $U_{0,-m}$ error on the edit key.

A $U_{m,0}$ error on the transmitted cipher-text propagates to the decoded message together with a $U_{0,-m}$ error on b_2, changing (a_2,b_2) from $|\psi(0,0)\rangle$ to

$$|\psi(0,-m)\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\zeta^{-jm}|j\rangle|j\rangle\,.$$

Likewise, a $U_{0,n}$ error on the transmitted cipher-text changes (a_1,b_1) from $|\psi(0,0)\rangle$ to

$$|\psi(0,n)\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\zeta^{jn}|j\rangle|j\rangle\,,$$

and a $U_{m,n}$ error turns (a_1,b_1) to $|\psi(0,n)\rangle$ and (a_2,b_2) to $|\psi(0,-m)\rangle$ (i.e. $|\psi(0,d-m)\rangle$) at the same time. Alice and Bob can distinguish $|\psi(0,n)\rangle$ for any $n\in\{0,1,...,d-1\}$ by independently measuring their own particles of the Bell state along $\{|\bar{l}\rangle\}$ basis, and comparing their results on a broadcast channel. Since

$$\begin{aligned}\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\zeta^{jn}|j\rangle|j\rangle=&\frac{1}{d\sqrt{d}}\sum_{j=0}^{d-1}\zeta^{jn}\sum_{i=0}^{d-1}\zeta^{-ji}|\bar{i}\rangle\sum_{l=0}^{d-1}\zeta^{-jl}|\bar{l}\rangle\\ =&\frac{1}{d\sqrt{d}}\sum_{j,i,l=0}^{d-1}\zeta^{j(n-i-l)}|\bar{i}\rangle|\bar{l}\rangle\\ =&\frac{1}{\sqrt{d}}\sum_{i,l=0}^{d-1}|\bar{i}\rangle|\bar{l}\rangle\,,\end{aligned}$$

where the last equation is obtained by summing over j and it holds iff $n=(i+l)$ mod d. Therefore, when Alice and Bob announce their measurements, they know the value of n. According to the form the two-edit key has changed into, they know the associated error appearing on the message, and then they can correct it using local unitary operations. The same argument applies to transmitting n qudits.

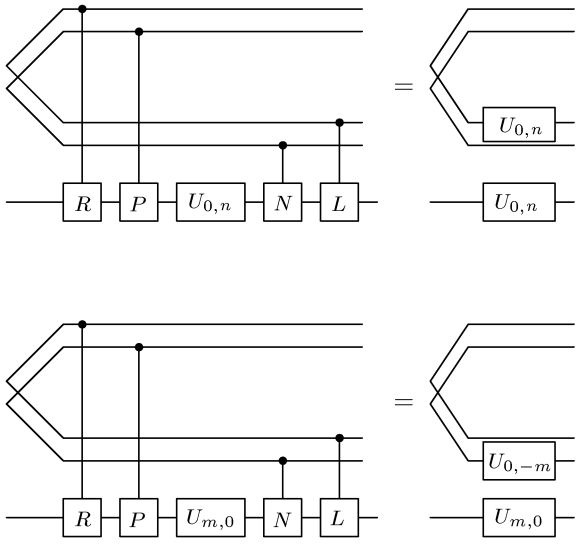


Fig.3. The overall possible error patterns in the d-level Vernam cipher.

Up to now, we have shown that the d-level Vernam cipher can correct any Pauli error. According to Ref.[14], the scheme can correct arbitrary errors; when many qudits are sent, it is possible to use less entanglement (edit) for correcting errors with high probability. The remaining Bell states can be recycled with semantic security.

5. Conclusions

In this paper, we have presented a quantum encryption scheme for d-level states, which is in fact an implementation of the quantum Vernam cipher in d-level systems. By showing that the transmitted state is a totally mixed state, we have proved that the scheme is informationally secure. Furthermore, by showing that the scheme can correct any Pauli error such as $U_{m,n}$, we have shown that the scheme can correct arbitrary errors on the transmitted message, and the entanglement key used to encrypt can be recycled with semantic security.

References

[1] Vernam G S 1926 *J. Am. Inst. Elec. Eng.* **55** 109

[2] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computer, Systems, and Signal Processing* (NewYork:IEEE Press) p 175

[3] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[4] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[5] Zhang Q, Tang C J and Zhang S Q 2002 *Acta Phys. Sin.* **51** 1439 (in Chinese)

[6] Okamoto T, Tanaka K and Uchiyama S 2000 *Proceedings of CRYPTO 2000*, *LNCS* **1880** (Berlin: Springer) p147

[7] Brown M S 2004 quant-ph/0404061

[8] Zhang Y S, Li C F and Guo G C 2001 *Phys. Rev.* A **64** 024302

[9] Boykin P O and Roychowdhury V 2003 *Phys. Rev.* A **67** 042317

[10] Karimipour V and Bahraminasab A 2002 *Phys. Rev.* A **65** 052331

[11] Deng F G and Long G L 2003 *Phys. Rev.* A **68** 042315

[12] Ambainis A, Mosca M, Tapp A and de Wolf R 2000 (Los Alamitos, CA: IEEE Computer Society Press) in *Proc 41st Annual Symposium on Foundations of Computer Science* p 547

[13] Zhou N R, Zeng G H 2005 *Chin. Phys.* **14** 2164

[14] Leung D W 2002 *Quantum Inform. Comput.* **2** (1) 14

[15] Steane A 1998 *Rep. Prog. Phys.* **64** 117

[16] Cerf N J, Bourennane M, Karlsson A and Gisin N 2002 *Phys. Rev. Lett.* **88** 127902

[17] Gottesman D 1998 quant-ph/9802007

[18] Alber G, Delgado A, Gisin N and Jex I 2000 quant-ph/0008022