Science in China Series G: Physics, Mechanics & Astronomy

www.scichina.com
phys.scichina.com
www.springerlink.com

Quantum asymmetric cryptography with symmetric keys

GAO Fei[1†], WEN QiaoYan[1], QIN SuJuan[1] & ZHU FuChen[2]

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;
[2] National Laboratory for Modern Communications, Chengdu 610041, China

Based on quantum encryption, we present a new idea for quantum public-key cryptography (QPKC) and construct a whole theoretical framework of a QPKC system. We show that the quantum-mechanical nature renders it feasible and reasonable to use symmetric keys in such a scheme, which is quite different from that in conventional public-key cryptography. The security of our scheme is analyzed and some features are discussed. Furthermore, the state-estimation attack to a prior QPKC scheme is demonstrated.

quantum cryptography, public-key cryptography, entanglement

In the 1970s, the concept of public-key cryptography (PKC), also called asymmetric cryptography, was proposed[1,2]. It represented the radical revision of cryptographic thinking and transformed the world of information security. As described by Rivest, Shamir, and Adleman when they presented the famous RSA scheme[2], a PKC system generally satisfies the following four conditions: (i) a message encrypted with the public key e can be correctly decrypted with the private key d; (ii) both the encryption and the decryption are easy to compute; (iii) it is difficult to compute d from the public e; (iv) a message encrypted with d can also be correctly decrypted with e. Armed with these properties, PKC can be conveniently utilized for key distribution and digital signature[3].

As we know, most of PKC schemes will be broken by future quantum computer[4,5]. It is desirable to find quantum PKC (QPKC)[6] which can stand against quantum computation like other quantum protocols[7−9]. To this end the research is progressing along two directions. One is to look for difficult problems under quantum computation and construct PKC based on them[10−13]. In these schemes the key is still composed of classical bits and consequently the flexibility of PKC is retained. But their security still lies on unproved computational assumptions. For simplicity, we call this kind of cryptosystems QPKC class I. The other direction pursues PKC with perfect security by adding more quantum elements, which is just like that of quantum key distribution (QKD)[14,15]. In these schemes the security is assured by physical laws. However, the keys generally contain qubits, which are more difficult to deal with, and then the flexibility of PKC would be reduced. We call these cryptosystems QPKC class II. In this paper we study the latter.

Recently, Nikolopoulos presented a novel QPKC scheme (GMN scheme) based on single-qubit rotations[14], which is similar to the one proposed by

Received February 22, 2009; accepted August 19, 2009
doi: 10.1007/s11433-009-0299-3
†Corresponding author (email: gaofei_bupt@hotmail.com)
Supported by the National Natural Science Foundation of China (Grant Nos. 60873191, 60821001 and 60903152), the Specialized Research Fund for the Doctoral Program of Higher Education (Grant No. 200800131016), Beijing Nova Program (Grant No. 2008B51), Key Project of Chinese Ministry of Education (Grant No. 109014), Beijing Municipal Natural Science Foundation (Grant No. 4072020) and China Postdoctoral Science Foundation (Grant No. 20090450018)

Citation: Gao F, Wen Q Y, Qin S J, et al. Quantum asymmetric cryptography with symmetric keys. Sci China Ser G, 2009, 52(12): 1925-1931, doi: 10.1007/s11433-009- 0299-3

Gottesman[15]. Here we will point out a potential security problem in GMN scheme, and propose a new theoretical framework for QPKC based on quantum encryption[16,17]. In our scheme two qubits from a Bell state serve as the public key and the private key respectively. Because both qubits are in the maximally mixed state, we actually construct a quantum asymmetric cryptosystem with symmetric keys, which seems unbelievable in conventional cryptography. Actually it is the quantum nature that renders this interesting thing feasible.

1 A security issue in previous QPKC

Let us briefly describe the preparation of the keys in GMN scheme first. The user, say Bob, randomly chooses an integer n, and then chooses N integers $s_1, s_2, \cdots, s_N$ from Z_{2^n} independently, which compose an integer string $\boldsymbol{s} = (s_1, s_2, \cdots, s_N)$. After that Bob generates N single qubits in the states $\{\hat{R}^{(j)}(s_j\theta_n)|0\rangle\}$, where $1 \leqslant j \leqslant N$, $\theta_n = \pi/2^{n-1}$ and $\hat{R}$ is the rotation operation. It can be seen that these qubits are in one-to-one correspondence with all the integers in s. The private key is $d = \{n, \boldsymbol{s}\}$, and the public key is $e = \{N, |\Psi_s^{(PK)}(\theta_n)\rangle\}$, where $|\Psi_s^{(PK)}(\theta_n)\rangle$ represents the state of the sequence of all above N qubits.

As analyzed in ref. [14], the entropy of the private key is relatively high when $n \gg 1$, and becomes higher with the increasing of n. On the contrary, an eavesdropper (Eve) can only obtain limited information about the private key by measuring the public key, which is bounded by Holevo quantity[18] and totally depends on the number of the qubits being measured. Therefore, it seems like that as long as n is large enough Bob can release many copies of his public key without losing the confidentiality of his private key (see eq. (3b) in ref. [14]). However, the publication of multiple copies of public key would give Eve the chance to attack. By measuring the public key, Eve can estimate the private key to certain accuracy and using the result to obtain plaintext from the ciphertext.

To see the particular accuracy to which Eve can estimate the private key, we can use some results in the research of state estimation[19−21]. In GMN scheme, all the single-qubit states lie on the x-z plane of Bloch sphere. In this condition by optimal collective measurements the obtainable fidelity between the estimation result and the object state is[20,21]

$$F = \frac{1}{2} + \frac{1}{2^{M+1}} \sum_{i=0}^{M-1} \sqrt{\binom{M}{i}\binom{M}{i+1}} \approx 1 - \frac{1}{4M}, \qquad (1)$$

where M denotes the number of copies of the object state. That is to say, if Eve has M identical unknown states $|\psi\rangle$ on the x-z plane, she can obtain a known state $|\psi'\rangle$ so that $|\langle\psi|\psi'\rangle|^2 = F$. Suppose Eve can get K public keys in GMN scheme. Without loss of generality, we take one state $|\psi_{s_j}\rangle$ as our example. In this condition Eve can obtain a guessed state $|\psi'_{s_j}\rangle$ by optimal collective measurements so that $|\langle\psi_{s_j}|\psi'_{s_j}\rangle|^2 \approx 1 - 1/(4K)$. As a result, Eve can construct a measurement basis $B_{s_j} = \{|\psi'_{s_j}\rangle, |\psi'^{\perp}_{s_j}\rangle\}$ and measure any single qubit in it ($|\psi'^{\perp}_{s_j}\rangle$ is the state orthogonal with $|\psi'_{s_j}\rangle$).

According to GMN scheme, the ciphertext $|\psi_{s_j}\rangle$ and $|\psi^{\perp}_{s_j}\rangle$ just imply the plaintext $m_j = 0$ and 1 respectively. Therefore, Eve can intercept the ciphertext sent by the sender (Alice) and measure it in the basis B_{s_j} to judge the plaintext. Since $|\psi'_{s_j}\rangle$ and $|\psi_{s_j}\rangle$ might be very close on the Bloch sphere, Eve will obtain the correct plaintext m_j with a high probability, i.e. $P_c = F$. Equivalently, the amount of the information Eve can obtained about m_j equals

$$\begin{aligned} I(A,E) &= H(A) - H(A|E) \\ &= 1 - 2[F\log F + (1-F)\log(1-F)], \end{aligned} \qquad (2)$$

where A and E represent Alice and Eve respectively.

Now we consider the disturbance brought by Eve though it is not involved in ref. [14]. To avoid being discovered in above attack, Eve can resend her measurement result $|\psi'_{s_j}\rangle$ or $|\psi'^{\perp}_{s_j}\rangle$ to Bob after the measurement. In this condition an error occurs with the probability

$$P_e = 2F(1-F). \qquad (3)$$

From eqs. (2) and (3) it can be seen that Eve can obtain nearly all the plaintext and, at the same time, introduce few errors when K is large (see Table 1 and Figure 1 for details).

Table 1 The values of $I(A,E)$ and P_e with different K

	K=10	K=20	K=50	K=100	K=1000
$I(A,E)$	0.6627	0.8061	0.9092	0.9496	0.9933
P_e	0.0488	0.0247	0.0100	0.0050	0.0005

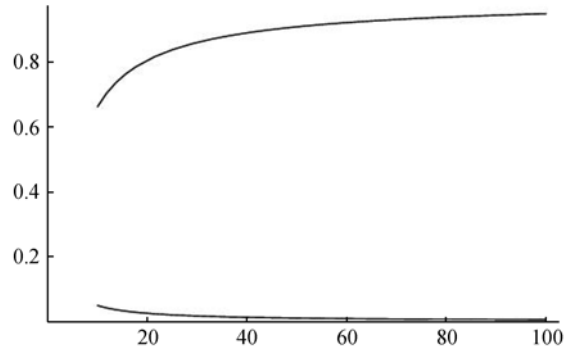

Figure 1 $I(A,E)$ and P_e as functions of K. The horizontal axis represents the values of K. The upper line and the lower line indicate $I(A,E)$ and P_e, respectively.

Finally, in ref. [14] and its very recent Erratum[22], it was pointed out that each bit in the plaintext should be encrypted into several or more qubits so that this scheme can stand against the SWAP-test attack. In this condition our attack strategy may not be so effective either. However, as a special attack on QPKC, the state-estimation attack seems more straightforward and practical, and should be paid attention in future research.

2 QPKC based on quantum encryption

From above discussion we can see that the model of key generation in previous QPKC schemes may be vulnerable to the state-estimation attack. More concretely, though Eve cannot obtain the exact private key by measuring multiple copies of the public key, she can still get an approximate private key and then use it to elicit information about the plaintext. Therefore, it would be desirable to find a new way to generate keys in QPKC. Here we will give a scheme using the qubits from Bell state as keys, in which, as in almost all existing protocols of quantum cryptography, the process of eavesdropping detection is introduced and the security is guaranteed by it.

Before the description of our QPKC scheme, it is necessary to introduce several basic assumptions about this system. That is, (A1) there is a believable center (Trent) in the QPKC system; (A2) Trent can authenticate every user's identity in the communications between them, which can be realized by quantum authentication protocols[23,24]; (A3) the information transmitted in the classical channels can be eavesdropped, but cannot be modified. These assumptions are reasonable and generally accepted in PKC (e.g. A1 and A2) and quantum cryptography (e.g. A3).

This scheme consists of the following four stages.

Stage 1: Key generation. Trent generates a pair of keys, i.e. the public key e and the private key d, for each user. Without loss of generality, consider Bob as our example. The particular process is as follows.

(i) Trent prepares a sequence of qubit pairs $S_1 = \{(p_1,q_1),(p_2,q_2),\cdots,(p_n,q_n)\}$. Each pair is in the Bell state

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right). \tag{4}$$

Two qubit sequences $S_p = \{p_1, p_2, \cdots, p_n\}$ and $S_q = \{q_1, q_2, \cdots, q_n\}$ will be used as Bob's public key and private key, respectively.

(ii) To securely transmit S_q to Bob, Trent also generates a certain quantity of decoy states $S_d = \{d_1, d_2, \cdots, d_k\}$, where every qubit is randomly in one of the states

$$\left\{\left|0\right\rangle,\left|1\right\rangle,\left|+\right\rangle = 1/\sqrt{2}\left(\left|0\right\rangle+\left|1\right\rangle\right),\ \left|-\right\rangle = 1/\sqrt{2}\left(\left|0\right\rangle-\left|1\right\rangle\right)\right\}.$$

(iii) Trent inserts each qubit in S_d into a random position of the sequence S_q, obtaining a new qubit sequence S_{qd}. Then Trent sends S_{qd} to Bob via a quantum channel.

(iv) After Bob received all these qubits, Trent tells Bob the position and the basis (i.e. $B_z = \{\left|0\right\rangle,\left|1\right\rangle\}$ or $B_x = \{\left|+\right\rangle,\left|-\right\rangle\}$) of each decoy state.

(v) Bob measures all decoy states in their corresponding bases, and then announces the measurement results to Trent. By comparing these results with the initial states of these qubits, Trent can judge whether the transmitted sequence is disturbed.

(vi) If no eavesdropping occurs, Bob obtains his private key d, i.e. the sequence S_q. At the same time, Trent stores Bob's public key e, i.e. S_p, for future usage. Otherwise the communication may be insecure and will abort.

In the following stages we can see that the keys might be not enough for encrypting a long message, or be

consumed gradually. But whenever it is not enough to be used, Trent can generate new Bell-state pairs to refuel the keys.

Stage 2: Encryption. Suppose a user, say Alice, wants to send an *r*-bit message $m=\{m_1,m_2,\cdots,m_r\}$ to Bob, where $m_i=0$ or 1, and $r\leqslant n$. Then Alice can encrypt it according to the following steps.

(i) Alice requests Trent to send her *r* qubits of Bob's public key.

(ii) Trent sends the first *r* qubits of the sequence S_p to Alice. Here we use S_p^r to denote this part of sequence, i.e. $S_p^r=\{p_1,p_2,\cdots,p_r\}$. Similar to that in Stage 1, Trent also utilizes decoy states so that these qubits are securely transmitted to Alice.

(iii) Alice generates an *r*-qubit sequence $L=\{l_1,l_2,\cdots,l_r\}$ with states $\{|m_1\rangle,|m_2\rangle,\cdots,|m_r\rangle\}$ respectively, which corresponds to her message to be encrypted.

(iv) Alice encrypts her message *L* with the public key S_p^r. More concretely, Alice uses one qubit in S_p^r to encrypt her corresponding message qubit via a CNOT operation. For example, to encrypt l_i, Alice performs a CNOT gate $C_{p_il_i}$ (the first subscript p_i denotes the controller and the second l_i represents the target) on qubits p_i and l_i, that is

$$C_{p_il_i}|\Phi^+\rangle_{p_iq_i}|m_i\rangle_{l_i}=\frac{1}{\sqrt{2}}\left(|00m_i\rangle+|11\overline{m}_i\rangle\right)_{p_iq_il_i}, \quad (5)$$

where $\overline{m}_i=1-m_i$.

(v) After the encryption of all her message qubits, Alice sends the sequence *L* (the ciphertext) to Bob through a quantum channel.

Stage 3: Decryption. After Bob received all these qubits, he can execute the following steps to recover the message *m*.

(i) For each qubit in the ciphertext *L*, Bob performs a CNOT operation $C_{q_il_i}$ to decrypt it. Then the state changes into

$$C_{q_il_i}\frac{1}{\sqrt{2}}\left(|00m_i\rangle+|11\overline{m}_i\rangle\right)_{p_iq_il_i}=|\Phi^+\rangle_{p_iq_i}|m_i\rangle_{l_i}. \quad (6)$$

(ii) Bob measures each qubit in *L* in basis B_z. From eq. (6) we can see that the measurement results exactly compose the message *m*. Thus the message sent by Alice is recovered and the decryption is finished.

Stage 4: Key recycling. There is a good property in the above communication, that is, the states of Bob's keys are still unchanged after the processes of encryption and decryption. Therefore, the keys can be recycled according to the following steps.

(i) Alice sends Bob's public key, i.e. the qubit sequence S_p^r to Trent.

(ii) To ensure the security of these recycled key qubits, Trent randomly selects a certain number of them from S_p^r as the test qubits, and measures each of them in B_z or B_x at random.

(iii) Trent tells Bob the position and the measurement basis of each test qubit.

(iv) Bob measures his corresponding qubits in the same bases and announces his results. Because every two corresponding qubits in two keys should be in Bell state $|\Phi^+\rangle$, the measurement results would exhibit deterministic correlations.

(v) By comparing their measurement results Trent can judge whether these qubits are attacked. If they are not, Trent and Bob store the remaining qubits to refuel the public key and the private key. Otherwise the recycled key qubits would be discarded.

Now we have described the QPKC scheme based on quantum encryption. It can be seen that both the qubits in public key and the ones in private key come from Bell state $|\Phi^+\rangle$, and are in the same state (i.e. the maximally mixed state $\rho=1/2\left(|0\rangle\langle 0|+|1\rangle\langle 1|\right)$). Therefore, an interesting event happens. That is, this QPKC scheme essentially uses a pair of symmetric keys. In fact the basic idea of this scheme is similar to that of quantum Vernam cipher[25]. In conventional cryptography, as we know, the Vernam cipher (i.e. one-time pad)[26] can never be used in PKC because its decryption key and encryption key are equal, and they can be copied at will. But in the quantum context things become totally different. That is, one cannot obtain the decryption key (i.e. private key) by replicating a copy of the encryption key (i.e. public key) even though they are in the same state, which is guaranteed by quantum no-cloning theorem[27].

Finally, about this QPKC scheme, there are some issues to be clarified. (1) In fact the public key obtained by Alice is a sub-sequence of S_p. After Alice received these qubits, it is necessary for Trent to tell Bob which

sub-sequence of S_p was sent to Alice so that Bob can use his corresponding qubits to decrypt Alice's ciphertext. (2) To enable Alice and Bob to discover denial-of-service (DoS) attack[28,29], the method of message authentication can be introduced to this scheme. (3) When channel noise is concerned, the technologies of entanglement purification[30,31] and quantum privacy amplification[32] can be introduced in this scheme to improve the quality of Bell states after the transmissions.

3 Security analysis

For a QPKC system, it must be ensured that Eve cannot obtain Bob's private key or Alice's plaintext. In our scheme some familiar and reliable manners are utilized to guarantee its security. For example, BB84-type qubits are used as the decoy states to protect the transmitted sequence, and conjugate-bases measurements to identify the state of recycled key qubits. In the following we will briefly discuss the security with respect to different stages of this scheme.

Key generation. In this stage Trent prepares EPR pairs in $\left|\Phi^+\right\rangle$ and sends one qubit in each pair (i.e. the sequence S_q) to Bob as his private key. Because Trent is believable we only need to consider the attack from an outside eavesdropper (Eve). In this process Eve has the chance to obtain Bob's private key, with which she can decrypt any ciphertext sent to Bob. However, Eve's goal will not be achieved because of the usage of decoy states. The reasons are as follows.

Firstly, quantum no-cloning theorem[27] ensures that Eve cannot replicate the qubits in the private key. This point is very different from that in conventional PKC systems, in which the private key can never be transmitted in the public channel because it is in the form of bits and can be easily copied.

Secondly, since both the decoy qubits and the private-key ones are in the same state, i.e. the maximally mixed state $\rho = 1/2(\left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|)$, these two kinds of qubits cannot be distinguished. That is to say, any attack operation which is expected to be performed on the private-key qubits will be also inevitably executed on the decoy ones. As a result, the attack would leave a trace on the decoy states and then be discovered by legal users. Here we will not demonstrate the security brought by such decoy states in detail, which is just like that in BB84 protocol[33] and has been generally accepted.

Encryption. As introduced in Sec. 3, we use symmetric keys in our QPKC scheme. That is, the public key and the private one are in the same state. Therefore, anyone who has the public key can also decrypt the ciphertext encrypted by this key. In this stage Eve has the chance to touch the public key when it is transmitted from Trent to Alice. However, similar to that in Stage 1, Eve can never replicate those qubits and the decoy states ensure the security of the public key. Consequently, any effective attack on the public key will be discovered by legal users.

Now let us observe what Eve can obtain from the ciphertext when it is transmitted from Alice to Bob. From above analysis, it can be seen that Eve cannot elicit any helpful information from the transmitted key qubits, including both the public key and the private key, if she does not want to bring disturbance to the decoy states. In this condition Eve can obtain nothing about the plaintext from the ciphertext because all ciphertext qubits are in the same state $\rho = 1/2(\left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|)$ in spite of the value (0 or 1) of corresponding message bit.

Decryption. In this stage Eve has no chance to attack because no qubits are transmitted in the channel. After Bob obtained the plaintext, he can judge whether DoS attack occurred with the help of message authentication codes.

Key recycling. In this stage Alice sends the public key back to Trent. This situation, as far as Eve is concerned, is similar to that in the beginning of Stage 2. But here we should also consider the attack from Alice. Because the recycled public-key qubits will be reused in later applications where another one (say Charlie) sends his message to Bob, Alice can do something for future illegal decryption. For example, Alice can entangle her ancilla into each Bell states and use it to decrypt the ciphertext sent by Charlie later (similar to Eve's strategy in refs. [34,35]).

Taking above threat into account, we have to ensure that the states of the public-key qubits Alice sent back are unchanged (that is, each qubit is still in Bell state $\left|\Phi^+\right\rangle$ with its corresponding particle in Bob's hand). In our scheme we use the manner of conjugate-bases measurements to detect eavesdropping, which can resist attacks from both Eve and Alice. This manner has been widely used in quantum cryptography and its reliability

has been proved[36−39]. Here we will not repeat the analysis any more.

Finally, it is well known that, in a practical QKD system, Eve may attack only a little part of the transmitted particles so that the introduced disturbance will be covered up by channel noises. In this case the users can perform privacy amplification[40] on the raw key and then obtain a final key with unconditional security. In our QPKC scheme, similar problem also exists. Eve may attack only a little part of the key qubits and then obtain some information about the plaintext. In this condition we introduce entanglement purification[30,31] and quantum privacy amplification[32] in our scheme, which makes it possible to achieve unconditional security in theory.

4 Discussion and conclusions

Compared with the previous QPKC system (GMN scheme)[14], our scheme has the following features.

(i) The roles of public key and private key are equal, which satisfies the basic requirement (C4) of PKC as described in Sec. 1. In this condition the users can also use private key to encrypt a message and use public key to decrypt it correctly. This feature makes it possible to construct a quantum signature protocol[41] based on our scheme.

(ii) The manner to verify the identity of public key is presented, which is a crucial point for the security of whole QPKC system. On the one hand, the decoy-states detection is utilized to protect the public-key qubits from being attacked by Eve. On the other hand, because the key qubits are from the same Bell state $\left|\Phi^+\right\rangle$, entanglement purification and quantum privacy amplification can be easily performed on them in the sense that they are existing technologies for Bell states[30−32]. Through these manners high-fidelity Bell state can be finally obtained even under a noisy channel, or equivalently, the state of public key can be authenticated.

(iii) The state-estimation attack, as described in Sec. 2, is invalid for our scheme. Here any two qubits from different public key belong to different EPR pairs and there are no correlations between them. Eve cannot get more useful information from multiple public key than that from one.

(iv) The keys can be reused and refuelled whenever it is needed.

One may argue that our scheme does not look like a practical PKC system (e.g. any familiar conventional PKC such as the famous RSA scheme) for the following two reasons: (1) Some QKD-like strategies for eavesdropping detection are used to guarantee the security; (2) It uses symmetric keys. We emphasize that all these facts have their roots in the quantum nature of QPKC. Now let us give further interpretations about above two questions.

(i) As we know, the quantum-mechanical nature of qubits renders eavesdropping detectable, which is the root of the unconditional security of quantum cryptography. To obtain this advantage in a quantum protocol, an eavesdropping-detection process is absolutely necessary. It is also the fact in QPKC because the public key, generally composed by qubits, must be authenticated after the transmission. Note that there are no such strategies in GMN scheme because the content of public-key authentication is not contained in ref. [14].

(ii) By choosing Bell-state qubits as the keys we initially intended to avoid the state-estimation attack as in GMN scheme. In fact Bell states have a special feature which is suitable for QPKC. That is, these states can be authenticated by existing technologies (especially entanglement purification and quantum privacy amplification), which is an important issue in QPKC but still not resolved in the previous scheme. We know that people can never use equal keys in a conventional PKC system because in this condition anyone can get the private key just by replicating a copy of the public key, and then decrypt all corresponding ciphertexts. Thus we really need to design two different keys so that Eve cannot obtain the private key from the public one. However, in the quantum circumstance, things go very differently. On the one hand, quantum no-cloning theorem does not allow the replication of qubits any more. On the other hand, the authentication of public key is necessary in QPKC and, at the same time, whenever the authentication is successful it generally ensures that Eve cannot read any information from public key. In this condition, therefore, we have no need to design two different keys any more. That is, equal keys are competent for QPKC. In fact we have shown that it is feasible to use symmetric keys in QPKC system, which touches on the very nature of the quantum state.

In conclusion, we gave a new elementary idea for QPKC and constructed a whole theoretical framework of

a QPKC system. It was shown that symmetric keys could be used in QPKC, which is quite different from that in conventional PKC. The security and features of this scheme were discussed. In addition, a possible attack to GMN scheme[14] was demonstrated. Combining the unconditional security of QKD and the significant flexibility of PKC, QPKC has been an expected goal of the scholars in the field of quantum cryptography for a long time. But to design a practical QPKC scheme, or alternatively, to demonstrate its feasibility, is still a difficult work. This study can be seen as a step towards this direction.

1 Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inform Theor, 1976, 22: 644－654
2 Rivest R L, Shamir A, Adleman L A. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM, 1978, 21: 120－126
3 Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. 2nd ed. New York: John Wiley and Sons, 1996. 24－29
4 Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on the Foundations of Computer Science. Los Alamitos: IEEE, 1994. 124－134
5 Grover L K. A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing. New York: ACM, 1996. 212－219
6 Zeng G H. Quantum Cryptography (in Chinese). Beijing: Science Press, 2006. 147-153
7 Chen W, Han Z F, Mo X F, et al. Active phase compensation of quantum key distribution system. Chin Sci Bull, 2008, 53: 1310－1314
8 Gao F, Guo F Z, Wen Q Y, et al. Comparing the efficiencies of different detect strategies in the ping-pong protocol. Sci China Ser G-Phys Mech Astron, 2008, 51: 1853－1860
9 Gao F, Guo F Z, Wen Q Y, et al. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. Sci China Ser G-Phys Mech Astrom, 2008, 51: 559－566
10 Okamoto T, Tanaka K, Uchiyama S. Quantum public-key cryptosystems. In: Advances in Cryptology: Crypto 2000 Proceedings. Berlin: Springer, 2000. LNCS, 1880: 147－165
11 Kawachi A, Koshiba T, Nishimura H, et al. Computational indistinguishability between quantum states and its cryptographic application. In: Advances in Cryptology: Eurocrypt 2005 Proceedings. Berlin: Springer, 2005. LNCS, 3494: 268－284
12 Yang L. Quantum public-key cryptosystem based on classical NP-complete problem. arXiv: quant-ph/0310076
13 Koshiba T. Security notions for quantum public-key cryptography. arXiv: quant-ph/0702183
14 Nikolopoulos G M. Applications of single-qubit rotations in quantum public-key cryptography. Phys Rev A, 2008, 77: 032348
15 Gottesman D, Chuang I L. Quantum digital signatures. arXiv: quant-ph/0105032
16 Zhang Y S, Li C F, Guo G C. Quantum key distribution via quantum encryption. Phys Rev A, 2001, 64: 024302
17 Zeng G H. Encrypting binary bits via quantum cryptography. Chin J Electr, 2004, 13: 651－653
18 Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000. 531－533
19 Massar S, Popescu S. Optimal extraction of information from finite quantum ensembles. Phys Rev Lett, 1995, 74: 1259－1263
20 Derka R, Buzek V, Ekert A K. Universal algorithm for optimal estimation of quantum states from finite ensembles via realizable generalized measurement. Phys Rev Lett, 1998, 80: 1571－1575
21 Bagan E, Baig M, Munoz-Tapia R. Optimal scheme for estimating a pure qubit state via local measurements. Phys Rev Lett, 2002, 89: 277904
22 Nikolopoulos G M. Erratum: Applications of single-qubit rotations in quantum public-key cryptography. Phys Rev A, 2008, 78: 019903
23 Dusek M, Haderka O, Hendrych M, et al. Quantum identification system. Phys Rev A, 1999, 60: 149－156
24 Zeng G H, Zhang W P. Identity verification in quantum key distribution. Phys Rev A, 2000, 61: 022303
25 Leung D W. Quantum Vernam cipher. Quantum Inf Comput, 2002, 2: 14－34
26 Vernam G S. Cipher printing telegraph systems for secret wire and radio telegraphic communications. J Am Inst Elect Eng, 1926, 55: 109－115
27 Wootters W K, Zurek W H. A single quantum cannot be cloned. Nature (London), 1982, 299: 802－803
28 Cai Q Y. The "Ping-Pong" protocol can be attacked without eavesdropping. Phys Rev Lett, 2003, 91: 109801
29 Gao F, Guo F Z, Wen Q Y, et al. Consistency of shared reference frames should be reexamined. Phys Rev A, 2008, 77: 014302
30 Bennett C H, Brassard G, Popescu S, et al. Purification of noisy entanglement and faithful teleportation via noisy channels. Phys Rev Lett, 1996, 76: 722－725
31 Pan J W, Gasparoni S, Ursin R, et al. Experimental entanglement purification of arbitrary unknown states. Nature (London), 2003, 423: 417－422
32 Deutsch D, Ekert A, Jozsa R, et al. Quantum privacy amplification and the security of quantum cryptography over noisy channels. Phys Rev Lett, 1996, 77: 2818－2821
33 Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 1999, 283: 2050－2056
34 Gao F, Guo F Z, Wen Q Y, et al. Comment on "Quantum secret sharing based on reusable Greenberger-Horne-Zeilinger states as secure carriers". Phys Rev A, 2005, 72: 036302
35 Gao F, Guo F Z, Wen Q Y, et al. Comment on "Quantum key distribution for d-level systems with generalized Bell states". Phys Rev A, 2005, 72: 066301
36 Bennett C H, Brassard G, Mermin N D. Quantum cryptography without Bell theorem. Phys Rev Lett, 1992, 68: 557－559
37 Waks E, Zeevi A, Yamamoto Y. Security of quantum key distribution with entangled photons against individual attacks. Phys Rev A, 2002, 65: 052310
38 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319
39 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68: 042317
40 Bennett C H, Brassard G, Robert J. Privacy amplification by public discussion. SIAM J Comput, 1988, 17: 210－229
41 Zeng G H, Keitel C H. Arbitrated quantum-signature scheme. Phys Rev A, 2002, 65: 042312