Quantum Information and Computation, Vol. 11, No. 5&6 (2011) 0434–0443
© Rinton Press

SECURITY OF A KIND OF QUANTUM SECRET SHARING WITH SINGLE PHOTONS

TIAN-YIN WANG*
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications, Beijing, 100876, China
and
School of Mathematical Science, Luoyang Normal University
Luoyang, 471022, China

QIAO-YAN WEN
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications, Beijing, 100876, China

Received May 7, 2010
Revised January 9, 2011

The security of a kind of quantum secret sharing with single photons was analyzed recently, and it was shown that almost all the present schemes in this kind were not secure in the sense that an unauthorized set of participants can gain access to the dealer's secret without introducing any error. In this paper, we give a general model for this kind of quantum secret sharing. Then we analyze the conditions that make it immune to all the present attacks. Finally, we give a feasible way to design secure quantum secret sharing schemes in the model.

Keywords: quantum secret sharing, single photons, model

Communicated by: S Braunstein & R Laflamme

1. Introduction

Secret sharing is a basic cryptographic primitive, whose goal is to divide a secret into n shares such that any k of those shares can be used to reconstruct the secret, but any set of $k-1$ or fewer shares contains no information about the secret. Secret sharing has many different applications, e.g., the management of cryptographic keys, the establishment of access codes with restricted access, and as a component of secure multiparty computation etc. Accordingly, much attention has been payed to secret sharing since it was firstly introduced by Blakely [1] and Shamir [2] independently, respectively. Nevertheless, the security of classical secret sharing schemes [1, 2] is based on an unproven assumption concerning the computational complexity of some algorithms, which may be solved with the development of quantum computation [3, 4].

*wangtianyin@yahoo.cn

The principles of quantum mechanics supplied many interesting applications in the field of cryptography over the years, such as quantum key distribution (QKD) [5-9], quantum secure direct communication (QSDC) [10-14], quantum fingerprinting [15] and quantum bit commitment [16, 17] etc. Especially, the unconditional security of QKD has been proven in theory [18, 19]. The idea of applying quantum mechanics to secret sharing was firstly introduced by Hillery, Buzěk, and Berthiaume [20], which started the vigorous development of quantum secret sharing (QSS). So far, a lot of schemes for QSS have been presented in both theoretical and experimental aspects [21-43].

Based on Deng and Long's QSDC protocol [12], Zhang et al. proposed a novel QSS scheme [44], in which only single photons and local operations are required, and thus it is more feasible with present-day technology in practice. Unfortunately, this scheme is vulnerable to some attacks [45-47]. At the same time, some different improvements [45-48] are proposed to overcome the security flaws in this scheme, but these improvements are vulnerable to a new kind of fake-signal attacks [49-51]. Also, some possible ways to prevent this kind of attacks are discussed [49-51].

In this paper, we give a general model for this kind of QSS [44-49], and then we analyze the conditions that make it immune to all the present attacks. Finally, we give a feasible way to design quantum secret sharing schemes in the model, which can make the designed schemes satisfy all the given conditions.

2. The proposed model

Let s be the security parameter and l be the length of the secret M to be distributed by the dealer Alice. The general procedure for this kind of QSS schemes with single photons [44-49] can be rephrased in the following manner.

(1) The first sharer Bob_1 prepares $l+s$ single photons $\otimes_{i=1}^{l+s}|0\rangle_i$. For each of them, he randomly chooses a unitary operation U_1 from a set $\mathcal{S}$, where $\mathcal{S}$ denotes a set of unitary operations acting on a 2-dimensional Hilbert space. Then he performs the unitary operation U_1 on it. After that, he sends the $l+s$ encrypted photons to the next sharer Bob_2.

(2) After receiving the $l+s$ photons, Bob_2 first ascertains whether each of them is sure a single photon or not by the similar methods in Refs. [14, 45]. If it is not, he aborts the protocol; otherwise, for each of them, he also randomly chooses a unitary operation U_2 from the set $\mathcal{S}$ and performs this operation on it. The similar procedures are repeated until the last sharer Bob_n sends the $l+s$ encrypted photons to the dealer Alice.

(3) After receiving the $l+s$ photons, Alice also first ascertains whether each of them is sure a single photon or not. If it is not, she aborts the protocol; otherwise, she randomly chooses s samples from them to check eavesdropping. Specifically, she publicly announces the s photons' positions, then for each of them, she randomly selects a sharer one by one and lets him tell her his unitary operation on it till she obtains all the sharers' operations. After that, Alice can performs an inverse unitary operation on each of them, then the s sample photons' states reverse to the initial state $|0\rangle$ if they are not disturbed, and therefore she can determine the error rate and judge whether the quantum channel is disturbed or not by measuring the s sample photons with Z-basis. If it is not, she aborts the protocol; otherwise, she continues to perform the following process.

(4) Alice performs the unitary operation I or U on the remaining l photons according to

the secret M, where

$$I = |0\rangle\langle 0| + |1\rangle\langle 1|, U = |0\rangle\langle 1| - |1\rangle\langle 0|, \tag{1}$$

i.e., if the secret bit is "0", she performs the unitary operation I; otherwise, she does the unitary operation U. Then she sends the l encoded photons to one of the sharers (e.g., Bob_k, $k \in \{1, 2, \ldots, n\}$) in a secure way.

(5) Alice publicly announces a small part of her secret for all the sharers to check whether the l encoded photons traveling from Alice site to Bob_k's have been attacked. If it is not, she aborts the protocol; otherwise, the secret M has been successfully distributed.

(6) When all the sharers approve to recover Alice's secret, they can deduce Alice's encoding operations and recover the secret M by using correct measuring basis to measure every encoded photon.

3. The proposed conditions

As mentioned in Refs. [20, 21, 45, 46, 47], the security of QSS is more complex than QKD and QSDC because not all of the legitimate sharers in QSS schemes are credible, that is, some of them may deceive. In contrast to other adversaries outside, the dishonest sharers have a lot of advantages. Firstly, they know partial information legally. Secondly, they can tell a lie in the process of eavesdropping detection to try to avoid introducing errors. Therefore, the main goal for the security of a QSS scheme is to prevent the dishonest sharers from stealing the secret. In other words, if a QSS scheme is secure to the dishonest sharers, then it is secure to any adversary.

For QSS in the proposed model, the security includes two aspects: the sharers' encryption operations (sub-secrets) and the dealer's secret M. The QSS scheme in the proposed model is secure if and only if nobody can recover the secret M except that all the sharers collaborate, and nobody can learn a sharer's sub-secret except himself. Now we analyze the conditions that can satisfy the security requirements.

Firstly, we analyze the conditions that nobody can learn a sharer's sub-secret except himself. To steal a sharer Bob_i's sub-secret U_i, an adversary must have the ability to discriminate the unitary operation U_i from the set $\mathcal{S}$, where U_i is Bob_i's encryption operation. Some possible attack strategies to discriminate the unitary operation U_i from the set $\mathcal{S}$ have been presented [45-47], and these strategies can be classified into kinds: one sends multi-photon signal to Bob_i [45, 46], i.e., Trojan horse attack, and the other only sends a single photon (one qubit of a maximally entangled state) to Bob_i [46, 47]. To prevent the first kind of attacks, the sharer Bob_i must have the ability to judge whether each quantum signal only contains a single photon. Gisin et al. [52] pointed out that this kind of attacks can be prevented by technical measures. A feasible way to solve this problem was proposed [14], which can filter out invisible photons. Specifically, Bob_i adds a filter in his laboratory first. All photon pulses should pass through his filter first. Only wavelengths close to the operating wavelength can be let in. Thus, the adversary's invisible photons can be filtered out by using the filter. If the adversary's spy photons cannot be filtered out, Deng et al. [45] gave a feasible way to detect them. Specifically, Bob_i chooses some sample signals and splits them with a photon number splitter, and then measures the two signals with Z-basis or X-basis randomly. If both the measurements have an outcome, Bob_i judges the quantum signal is a multi-photon signal.

To prevent the second kind of attacks [46, 47], the sufficient and necessary condition is that when the unitary operations in the set $\mathcal{S}$ are performed on a single qubit or one qubit of any entangled state, respectively, the quantum states are nonorthogonal. Therefore, we can get that the sufficient and necessary conditions that nobody can learn a sharer's sub-secret except himself are that he can judge whether each quantum signal only contains a single photon, and the unitary operations in the set $\mathcal{S}$ cannot be discriminated when they are performed only on a single qubit or one qubit of any entangled state, respectively.

Secondly, we analyze the conditions that nobody can recover the secret M except that all the sharers collaborate. To steal the dealer Alice's secret M, the adversary must have the ability to discriminate the encoding operations I and U. A direct way to deduce the encoding operations is to intercept the l encoded qubits and measure them, which needs to discriminate the sets $S_1 = \{|\chi\rangle||\chi\rangle = I\overline{U}|0\rangle, \overline{U} \in \mathcal{S}\}$ and $S_2 = \{|\chi^{'}\rangle||\chi^{'}\rangle = U\overline{U}|0\rangle, \overline{U} \in \mathcal{S}\}$, but it is impossible in general such as that in Refs. [44-49]. Another way is to send fake qubits to Alice, but the adversary must escape the eavesdropping detection in step (3). By this way, some possible attack strategies are presented [46, 49, 50, 51], and these strategies also can be classified into two kinds: one steals the secret M by inserting some spy photons (e.g., invisible photon) in each original photon when it is sent to Alice [46], and the other steals the secret M by sending $l + s$ fake photons (each of them is one qubit of a Bell state) instead of the original ones to Alice [49-51]. The first kind of attack strategies can be prevented with the same way as Bob_i does. Nevertheless, we show the second kind of attack strategies cannot be prevented with present methods. The basic principle of this kind of attack strategies can be described as the following.

In step (2), the dishonest sharer (e.g., Bob_n) sends $l+s$ fake photons (each of them is one qubit of a Bell state) instead of the original ones to Alice. At the same time, he stores the $l+s$ original photons and the remaining $l + s$ qubits of the Bell states in his quantum database. In step (3), when a photon is chosen as the sample for checking eavesdropping by Alice, Bob_n performs a teleportation measurement on the corresponding original photon and the remaining qubit of the corresponding Bell state. By this way, the state of the corresponding original photon can be teleported to the fake one (i.e., the one qubit of the corresponding Bell state sent to Alice) by the principle of teleportation except the lack of a unitary operation, and thus the dishonest sharer can hide his replacing deception by announcing the corresponding unitary operation. In step (4), after Alice's encoding on the l fake qubits, the dishonest sharer Bob_n intercepts them, and performs a joint measurement on them and the remaining l qubits of the corresponding Bell states, then he can successfully obtain the secret M by the comparison of the measurement outcomes and the initial states.

One simple way to prevent this kind of attacks is to ensure that the transmission of the l encoded photons between the dealer and the receiver Bob_k is secure in step (4), but it will be not valid if the receiver Bob_k is also dishonest and collaborates with Bob_n. To prevent this kind of attacks, Deng et al. [50] proposed a possible way with decoy photons, which can improve a lot of QSS protocols' security by eliminating the cooperation of the dishonest sharers in the process of eavesdropping detection. Nevertheless, this way is invalid to QSS in the proposed model since the eavesdropping check in step (3) must require the cooperation of all the sharers. Another way to prevent this kind of attacks is also discussed [40], in which the dealer Alice keeps the sample photons' initial states secret to all the sharers, and she measures

them before announcing their positions, by this way, the dishonest sharers cannot teleport the state of the original photon to the fake one since it is considered that the correlation between the entangled state prepared by the dishonest sharers and the original sample photon does not exist in Ref. [40]. Nevertheless, the correlation is invariant whether Alice measures the sample photons before announcing their positions or not, so this way is also invalid to prevent this kind of attacks.

Accordingly, as far as we know, under the proposed model in Section 2, there is no way to prevent this kind of attack strategies [49-51]. Now we analyze how to prevent this kind of attack strategies under the proposed model. Since there is no way to discriminate the fake photons and the original ones to the dealer Alice only by physical equipments when she receives them in step (3), the only possible way to detect the dishonest sharers' deception is to restrict their announcements, i.e., the dishonest sharers cannot announce the proper unitary operations to hide their deception in the process of eavesdropping detection. Let $\mathcal{U}$ denote a unitary operation set, which consists of the four unitary operations corresponding to the teleportation measurement outcomes, we can get that a necessary condition to prevent this kind of attack strategies is $\mathcal{U} \not\subseteq \mathcal{S}$, but it is not sufficient, e.g., if a element of $\mathcal{U}$ is not in $\mathcal{S}$, but it is the product of the others that are in $\mathcal{S}$, thus three dishonest sharers can collaborate to hide their deception by announcing the other three unitary operations in $\mathcal{S}$ respectively if the unitary operation is required. Let $(\mathcal{S})$ denote a unitary operation set, which consists of all the elements in $\mathcal{S}$ and all the possible products of them, then we can get that the sufficient and necessary condition to prevent this kind of attack strategies is $\mathcal{U} \not\subseteq (\mathcal{S})$.

So far, we have analyzed the conditions to prevent all the present attacks in the proposed model, i.e., (i) the dealer and every sharer have the ability to judge whether each quantum signal only contains a single photon; (ii) the unitary operations in the set $\mathcal{S}$ cannot be discriminated when they are performed only on a single qubit or one qubit of any entangled state, respectively; (iii) the sets S_1 and S_2 cannot be discriminated; (iv) $\mathcal{U} \not\subseteq (\mathcal{S})$.

Using the given conditions, we can judge whether a QSS scheme in the proposed model is secure or not, i.e., if a QSS scheme in the proposed model does not satisfy all the conditions (i)-(iv), this scheme must be not secure, e.g., the schemes in Refs. [44-49]; otherwise, this scheme is immune to all the present attacks in the sense that these attacks will be detected by the dealer Alice in the process of eavesdropping detection with probability p. The probability p can be computed by the following equation

$$p = 1 - (1 - \frac{k}{s+l} p_e)^s, \tag{2}$$

where p_e denotes the least probability that an adversary introduces an error when a single photon attacked by him is chosen as a sample to check eavesdropping, and k denotes the number of the photons attacked by the adversary. Suppose a scheme in the proposed model satisfies all the conditions (i)-(iv), the least probability p_e only depends on the set $\mathcal{S}$ since the multi-photon signal attack and the invisible photon attack must be detected by the condition (i), and the least probability p_e is no less than 12.5% since at least one of the four unitary operations corresponding to teleportation measurement cannot be properly announced by the condition (iv).

From Eq. (2), we can see that p is exponentially close to 1 with the increase of the security parameter s, which means that the adversary's attack will be detected by Alice with

probability exponentially close to 1.

It is evident that if the adversary's attack is detected by the dealer Alice, he will get no information on the message M. Nevertheless, Alice cannot distinguish which one is the cheater when she finds there is cheating among the sharers in the process of eavesdropping detection, which will induce that a participant may like to take the risk to cheat, because if the cheating is not detected then he will be benefited, while even if it is detected, Alice does not know which sharer to blame. Furthermore, when k is very small, the dishonest sharer may have a chance to escape Alice's detection, and the proportion on the message M that he can get in this case is

$$\begin{aligned} p_{\varepsilon} &= 1 - H(\frac{l+s+k}{2(l+s)}) \\ &= 1 + \frac{l+s+k}{2(l+s)} \log \frac{l+s+k}{2(l+s)} + (1 - \frac{l+s+k}{2(l+s)}) \log(1 - \frac{l+s+k}{2(l+s)}), \end{aligned} \tag{3}$$

where $H(\cdot)$ denotes the entropy function. If the message M is a random key, we can use privacy amplification [52] to distill a secure key, but if the message M is a secret, in our opinion, this loophole cannot be fixed with present methods.

Using the given conditions, we also can judge whether a QSS scheme is not secure if it is similar to the proposed model, e.g., the schemes in Refs. [37-40] are not secure since these schemes do not satisfy the condition (iv). Nevertheless, we cannot give a full classification on the security of previous schemes by the conditions (i)-(iv) since most of them are far different from the proposed model.

4. The proposed way

In the proposed model, the key to design a QSS scheme that can prevent all the present attacks is to find such a set $\mathcal{S}$ that satisfies the conditions (ii)-(iv). To find such a set $\mathcal{S}$ that satisfies the conditions (ii) and (iii) is not difficult. Nevertheless, to prove the set $\mathcal{S}$ also satisfies the conditions (iv) is very difficult if $|(\mathcal{S})|$ is large, where $|(\mathcal{S})|$ denotes the element number in the set $(\mathcal{S})$, this is because that there are a lot of choices for joint measurement, and we must consider every set $\mathcal{U}$ that depends on the corresponding joint measurement. In the following, we give a way to construct such a set $\mathcal{S}$ that can be proven to satisfy the conditions (ii)-(iv).

To reduce the complexity of the proof, one possible way is to reduce the element number $|(\mathcal{S})|$ under the conditions that the set $\mathcal{S}$ satisfies the conditions (ii) and (iii). We can prove that the element number $|(\mathcal{S})|$ is no less than three if the set $\mathcal{S}$ satisfies the conditions (ii) and (iii) by Theorem 1.

Theorem 1: Let a unitary operation set $\mathcal{S}$ satisfy the conditions (ii) and (iii). Then the element number $|(\mathcal{S})|$ is no less than three.

Proof: If $|(\mathcal{S})| = 1$, the set $\mathcal{S}$ must only contain one element. It is evident that the set $\mathcal{S}$ cannot satisfy the conditions (ii) and (iii). If $|(\mathcal{S})| = 2$, the set $\mathcal{S}$ must contain no more than two elements. We have proven that the set $\mathcal{S}$ cannot satisfy the conditions (ii) and (iii) if it contains one element. Therefore, we only consider the case that the set $\mathcal{S}$ contains two

elements. In this case, we can get $\mathcal{S} = (\mathcal{S})$, by the group theorem, the set $\mathcal{S}$ must form a group on the algebraic operation between the unitary operations; furthermore, the group $\mathcal{S}$ must be $\{I, U^{'}\}$, where $U^{'}$ is a unitary operation that satisfies the conditions $U^{'} \neq I$ and $U^{'2} = I$. By simple computation, we can get the eigenvalues of the unitary operation $U^{'}$ is 1 and -1, thus $\Theta(I^{\dagger}U^{'}) = \pi$, where $\Theta(I^{\dagger}U^{'})$ denotes the length of the smallest arc containing all the eigenvalues of $I^{\dagger}U^{'}$ on the unit circle, which means that the unitary operations I and $U^{'}$ can be discriminated by performing them on a suitable single-particle state or one qubit of a entangled state, respectively [53], and therefore the set $\mathcal{S}$ cannot satisfy the condition (ii) in this case $\square$.

A natural question is that whether we can find a set $\mathcal{S}$ that can satisfy all the conditions (ii)-(iv) when $|(\mathcal{S})| = 3$. In the following, we show that it is possible by Theorem 2.

Theorem 2: Let $\mathcal{S} = \{U(0), U(\frac{2}{3}\pi), U(\frac{4}{3}\pi)\}$, where

$$U(\theta) = \cos\theta|0\rangle\langle 0| - \sin\theta|0\rangle\langle 1| + \sin\theta|1\rangle\langle 0| + \cos\theta|1\rangle\langle 1|, \theta = 0, \frac{2}{3}\pi, \frac{4}{3}\pi. \tag{4}$$

Then the set $\mathcal{S}$ satisfies all the conditions (ii)-(iv).

Proof: By simple computation, we can get $U(0)^2 = U(0), U(\frac{2}{3}\pi)^2 = U(\frac{4}{3}\pi), U(\frac{4}{3}\pi)^2 = U(\frac{2}{3}\pi)$, $U(\frac{2}{3}\pi)U(\frac{4}{3}\pi) = U(0)$, which means that the set $\mathcal{S}$ forms a group on the algebraic operation and $\mathcal{S} = (\mathcal{S})$. Now we prove that the set $\mathcal{S}$ satisfies all the conditions (ii)-(iv).

Firstly, we prove that the set $\mathcal{S}$ satisfies the condition (ii). Since $\Theta(U(0)^{\dagger}U(\frac{2}{3}\pi)) = \Theta(U(0)^{\dagger}U(\frac{4}{3}\pi)) = \Theta(U(\frac{2}{3}\pi)^{\dagger}U(\frac{4}{3}\pi)) = \frac{2}{3}\pi < \pi$, by the theorem in Ref. [53], there is no way to discriminate $U(0)$, $U(\frac{2}{3}\pi)$, $U(\frac{4}{3}\pi)$ when they are performed only on a single qubit or one qubit of any entangled state, respectively.

Secondly, we prove that the set $\mathcal{S}$ satisfies the condition (iii). Since

$$S_1 = \{|0\rangle, \cos\frac{2}{3}\pi|0\rangle + \sin\frac{2}{3}\pi|1\rangle, \cos\frac{4}{3}\pi|0\rangle + \sin\frac{4}{3}\pi|1\rangle\}, \tag{5}$$

$$S_2 = \{-|1\rangle, -\cos\frac{2}{3}\pi|1\rangle + \sin\frac{2}{3}\pi|0\rangle, -\cos\frac{4}{3}\pi|1\rangle + \sin\frac{4}{3}\pi|0\rangle\}, \tag{6}$$

by simple computation, we can see that the two sets are not linearly independent, by the theorem in Ref. [54], unambiguous discrimination between them is impossible.

Finally, we prove that the set $\mathcal{S}$ satisfies the condition (iv). Since the number of the corresponding unitary operations on the joint measurement is four, i.e., $|\mathcal{U}| = 4$, and $|(\mathcal{S})| = 3$, it is impossible to find a set $\mathcal{U}$ such that $\mathcal{U} \subseteq (\mathcal{S})$ $\square$.

It is noted that we only give a simple example in Theorem 2, and we may find a lot of similar sets $\mathcal{S}$ that only contain three elements. Furthermore, these do not mean that a set $\mathcal{S}$ that contains no less than four elements cannot satisfy all the conditions (ii)-(iv).

By Theorem 2, we can design a QSS scheme in the proposed model that can prevent all the present attacks. Specifically, in the model, we take $\mathcal{S} = \{U(0), U(\frac{2}{3}\pi), U(\frac{4}{3}\pi)\}$ as the unitary operation set, and require that the dealer Alice and every sharer judge whether each quantum signal only contains a single photon when receiving it with the similar methods in Refs. [14, 45, 46].

Accordingly, we can design a lot of QSS schemes in the proposed model by giving different sets $\mathcal{S}$ so long as these sets satisfy all the conditions (ii)-(iv).

5. Conclusions

In summary, we give a general model for a kind of quantum secret sharing with single photons. Under the proposed model, we analyze the conditions that make it immune to all the present attacks. Finally, we give a feasible way to design QSS schemes in the model that can satisfy all the given conditions.

Acknowledgements

We are grateful to the anonymous referees for helpful comments and detailed suggestions on revisions. This work is supported by the National Natural Science Foundation of China, Grant Nos. 60873191, 60903152, 61003286, 60821001, the Specialized Research Fund for the Doctoral Program of Higher Education, Grant Nos. 200800131016, 20090005110010, Beijing Nova Program, Grant No. 2008B51, Key Project of Chinese Ministry of Education, Grant No. 109014, the Natural Science Foundation of Henan Province, Grant No. 112300410192, and the Natural Science Foundation of Education Bureau of Henan Province, Grant No. 2010B120008, 2011A120006.

References

1. G. Blakely (1979), *Safeguarding cryptographic keys*, in *Proc. the National Computer Conference*, AFIPS, New York, pp. 313-317.
2. A. Shamir (1979), *How to share a secret*, Commun. ACM, 22, pp. 612-613.
3. P. W. Shor (1997), *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Computing, 26, pp. 1484-1509; P. W. Shor (1999), *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Review, 41, 303-332.
4. E. Knill, R. Laflamme, and W. H. Zurek (1998). *Resilient quantum computation*, Science, 279, pp. 342-345; E. Knill, R. Laflamme, G. J. Milburn (2001), *A scheme for efficient quantum computation with linear optics*, Nature, 409, pp. 46-52.
5. C. H. Bennett and G. Brassard (1984), *Quantum cryptography: Public key distribution and coin tossing*, in *Proc. IEEE International Conference on Computers, Systems, and Signal Processing*, IEEE Press, New York, pp. 175-179.
6. A. K. Ekert (1991), *Quantum cryptography based on bell theorem*, Phys. Rev. Lett., 67, pp. 661-663.
7. C. H. Bennett (1992), *Quantum cryptography using any 2 nonorthogonal states*, Phys. Rev. Lett., 68, pp. 3121-3124.
8. H.-K. Lo, X. F. Ma, and K. Chen (2005), *Decoy state quantum key distribution*, Phys. Rev. Lett., 94, pp. 230504.
9. F. G. Deng and G. L. Long (2003), *Controlled order rearrangement encryption for quantum key distribution*, Phys. Rev. A, 68, pp. 042315; F. G. Deng and G. L. Long (2004), *Bidirectional quantum key distribution protocol with practical faint laser pulses*, Phys. Rev. A, 70, pp. 012311.
10. K. Boström and T. Felbinger (2002), *Deterministic secure Direct communication using entanglement*, Phys. Rev. Lett., 89, pp. 187902.
11. F. G. Deng, G. L. Long, and X. S. Liu (2003), *Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block*, Phys. Rev. A, 68, pp. 042317.
12. F. G. Deng and G. L. Long (2004), *Secure direct communication with a quantum one-time-pad*, Phys. Rev. A, 69, pp. 052319.
13. M. Lucamarini and S. Mancini (2005), *Secure deterministic communication without entanglement*, Phys. Rev. Lett., 94, pp. 140501.

14. X. H. Li, F. G. Deng, and H. Y. Zhou (2006), *Improving the security of secure direct communication based on the secret transmitting order of particles*, Phys. Rev. A, 74, 054302; Q. Y. Cai (2006), *Eavesdropping on the two-way quantum communication protocols with invisible photons*, Phys. Lett. A, 351, pp. 23-25.
15. H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf (2001), *Quantum fingerprinting*, Phys. Rev. Lett., pp. 167902.
16. H.-K. Lo and H. F. Chau (1997), *Is quantum bit commitment really possible*, Phys. Rev. Lett., pp. 3410-3413; D. Mayes (1997), *Unconditionally secure quantum bit commitment is impossible*, Phys. Rev. Lett., 78, pp. 3414-3417.
17. H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S.Wehner (2006), *Security of quantum bit string commitment depends on the information measure*, Phys. Rev. Lett., 97, pp. 250501; H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner (2008), *Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment*, Phys. Rev. A, 78, pp. 022316.
18. H.-K. Lo and H. F. Chau (1999), *Unconditional security of quantum key distribution over arbitrarily long distances*, Science, 283, pp. 2050-2056; P. W. Shor and J. Preskill (2000), *Simple proof of security of the BB84 quantum key distribution protocol*, Phys. Rev. Lett., 85, pp. 441-444; C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo and X. Ma (2009), *Security proof of quantum key distribution with detection efficiency mismatch*, Quant. Inf. Comput., 9, pp. 131-165.
19. D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill (2004), *Security of quantum key distribution with imperfect devices*, Quant. Inf. Comput., 4, pp. 325-360; H.-K. Lo and J. Preskill (2007), *Security of quantum key distribution using weak coherent states with nonrandom phases*, Quant. Inf. Comput., 7, pp. 431-458; L. Lydersena, J. Skaar (2010), *Security of quantum key distribution with bit and basis dependent detector flaws*, Quant. Inf. Comput., 10, pp. 0060-0076.
20. M. Hillery, V. Buzěk, and A. Berthiaume (1999), *Quantum secret sharing*, Phys. Rev. A, 59, pp. 1829-1834.
21. A. Karlsson, M. Koashi, and N. Imoto (1999), *Quantum entanglement for secret sharing and secret splitting*, Phys. Rev. A, 59, pp. 162-168.
22. D. Gottesman (2000), *Theory of quantum secret sharing*, Phys. Rev. A, 61, pp. 042311.
23. R. Cleve, D. Gottesman, and H.-K. Lo (1999), *How to share a quantum secret*, Phys. Rev. Lett., 83, pp. 648-651.
24. S. Bandyopadhyay (2000), *Teleportation and secret sharing with pure entangled states*, Phys. Rev. A, 62, pp. 012308.
25. A. C. A. Nascimento, J. Mueller-Quade, and H. Imai (2001), *Improving quantum secret-sharing schemes*, Phys. Rev. A, 64, pp. 042311.
26. W. Tittel, H. Zbinden, and N. Gisin (2001), *Experimental demonstration of quantum secret sharing*, Phys. Rev. A, 63, pp. 042301.
27. V. Karimipour, A. Bahraminasab, and S. Bagherinezhad (2002), *Entanglement swapping of generalized cat states and secret sharing*, Phys. Rev. A, 65, pp. 042320.
28. S. Bagherinezhad and V. Karimipour (2003), *Quantum secret sharing based on reusable Greenberger-Horne-Zeilinger states as secure carriers*, Phys. Rev. A, 67, pp. 044302.
29. L. Y. Hsu (2003), *Quantum secret-sharing protocol based on Grover's algorithm*, Phys. Rev. A, 68, pp. 022306.
30. L. Xiao, G. L. Long, F. G. Deng, and J. W. Pan (2004), *Efficient multiparty quantum secret sharing schemes*, Phys. Rev. A , 69, pp. 052307; F. G. Deng, X. H. Li, C. Y. Li, P. Zhou, and H. Y. Zhou (2005), *Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs*, Phys. Rev. A, pp. 72, 044301.
31. A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam (2004), *Tripartite quantum state sharing*, Phys. Rev. Lett., 92, pp. 177903; A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, T. Tyc, T. C. Ralph, and P. K. Lam (2005), *Continuous-variable quantum-state sharing via quantum disentanglement*, Phys. Rev. A, 71, 033814.
32. S. J. Qin, F. Gao, Q. Y. Wen, and F. C. Zhu (2007), *Cryptanalysis of the Hillery-Buzěk-*

Berthiaume quantum secret-sharing protocol, Phys. Rev. A, 76, pp. 062324.
33. S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter (2007), *Experimental demonstration of four-Party quantum secret sharing*, Phys. Rev. Lett., 98, pp. 020503.
34. T. Y. Wang, Q. Y. Wen, F. Gao, S. Lin, and F. C. Zhu (2008), *Cryptanalysis and improvement of multiparty quantum secret sharing schemes*, Phys. Lett. A, 373, pp. 65-68.
35. D. Markham and B. C. Sanders (2008), *Graph states for quantum secret sharing*, Phys. Rev. A, 78, pp. 042309.
36. G. P. Guo and G. C. Guo (2003), *Quantum secret sharing without entanglement*, Phys. Lett. A, 310, pp. 247-251.
37. F. L. Yan and T. Gao (2005), *Quantum secret sharing between multiparty and multiparty without entanglement*, Phys. Rev. A , 72, pp. 012304.
38. C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter (2005), *Experimental single qubit quantum secret sharing*, Phys. Rev. Lett., 95, pp. 230505.
39. J. Bogdanski, N. Rafiei, and M. Bourennane (2008), *Experimental quantum secret sharing using telecommunication fiber*, Phys. Rev. A, 78, pp. 062307.
40. T. Y. Wang, Q. Y. Wen, X. B. Chen, F. Z. Guo, and F. C. Zhu (2008), *An efficient and secure multiparty quantum secret sharing scheme based on single photons*, Opt. Commun., 281, pp. 6130-6134.
41. P. K. Sarvepalli and A. Klappenecker (2009), *Sharing classical secrets with Calderbank-Shor-Steane codes*, Phys. Rev. A, 80, pp. 022321.
42. S. J. Qin, F. Gao, Q. Y. Wen, and F. C. Zhu (2009), *Security of quantum secret sharing with two-particle entanglement against individual attacks*, Quant. Inf. Comput., 9, pp. 0765-0772.
43. G. P. He and Z. D. Wang (2010), *Single qubit quantum secret sharing with improved security*, Quant. Inf. Comput., 10, pp. 28-40.
44. Z. J. Zhang, Y. Li, and Z. X. Man (2005), *Multiparty quantum secret sharing*, Phys. Rev. A, 71, pp. 044301.
45. F. G. Deng, X. H. Li, H. Y. Zhou, and Z. J. Zhang (2005), *Improving the security of multiparty quantum secret sharing against Trojan horse attack*, Phys. Rev. A, 72, pp. 044302.
46. F. G. Deng, X. H. Li, H. Y. Zhou, and Z. J. Zhang (2006), *Erratum: Improving the security of multiparty quantum secret sharing against Trojan horse attack*, Phys. Rev. A., 73, pp. 049901(E).
47. S. J. Qin, F. Gao, Q. Y. Wen, and F. C. Zhu (2006), *Improving the security of multiparty quantum secret sharing against an attack with a fake signal*, Phys. Lett. A, 357, pp. 101-103.
48. L. F. Han, Y. M. Liu, J. Liu, and Z. J. Zhang (2008), *Multiparty quantum secret sharing of secure direct communication using single photons*, Opt. Commun., 281, pp. 2690-2694.
49. S. J. Qin, F. Gao, Q. Y. Wen, and F. C. Zhu (2008), *A special attack on the multiparty quantum secret sharing of secure direct communication using single photons*, Opt. Commun., 281, pp. 5472-5474.
50. F. G. Deng, X. H. Li, P. Chen, and H. Y. Zhou (2006), *Fake-signal-and-cheating attack on quantum secret sharing*, quant-ph/0604060.
51. G. Gao (2009), *Reexamining the security of the improved quantum secret sharing scheme*, Opt. Commun., 282, pp. 4464-4466.
52. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden (2002), *Quantum cryptography*, Rev. Mod. Phys., 74, pp. 145-195.
53. A. Acín (2001), *Statistical distinguishability between unitary operations*, Phys. Rev. Lett., 87, pp. 177901; G. M. DA'riano, P. LoPresti, and M. G. A. Paris (2001), *Using entanglement improves the precision of quantum measurements*, Phys. Rev. Lett., 87, 270404; R. Y. Duan, Y. Feng, and M. S. Ying (2007), *Entanglement is not necessary for perfect discrimination between unitary operations*, Phys. Rev. Lett., 98, pp. 100503.
54. S. Y. Zhang and M. S. Ying (2002), *Set discrimination of quantum states*, Phys. Rev. A, 65, pp. 062322.