





Multi-function Quantum Cryptography Protocol Based on Bell State

Zheng Tao¹ , Xiang Gao¹, Shibin Zhang¹ , Yan Chang¹,
and Jinyue Xia²

¹ Chengdu University of Information Technology,
Chengdu 610225, Sichuan, China
cuitzsb@cuit.edu.cn

² International Business Machines Corporation (IBM), New York, USA

Abstract. Most of the current quantum cryptographic protocols can only perform a single function, and quantum resources are not fully utilized. In this paper, we propose a multi-function quantum cryptographic protocol based on the Bell state. This protocol can perform quantum private query (QPQ), quantum identity authentication (QIA), and quantum key distribution (QKD) functions. In the QPQ function part, this protocol can effectively improve database security and user privacy. In the QIA function part, this protocol can complete a two-way identity authentication function, which can effectively improve the reliability of identity authentication. In the QKD function part, this protocol can complete the key distribution function efficiently and reliably, and can maximize the utilization efficiency of quantum resources. With a rigorous security analysis, we prove that this protocol can defend against JM attacks, entanglement measurement attacks and external attacks.

Keywords: Bell state · Multi-function · Quantum private query · Quantum identity authentication · Quantum key distribution

1 Introduction

Cryptosystem is the backbone of information security. With the rapid development of quantum technology, especially the advent of quantum computation, the classical cryptosystem was unable to meet the security needs of informationization. Therefore, quantum cryptosystem which is based on quantum mechanics and aims to exchange information absolutely safe in theory has attracted more and more attention in the last thirty decades. In 1984, Bennett and Brassard proposed the first quantum key distribution protocol (QKD), as known as BB84 [1]. After that, a number of quantum private communication schemes has been proposed, including quantum key distribution (QKD) [2–5], quantum secure direct communication (QSDC) [6–11], quantum secret sharing (QSS) [12–16], quantum private comparison (QPC) [17, 18], quantum dialogue (QD) [19, 20], quantum private query (QPQ) [21–28], quantum identity authentication (QIA) [29–32] and many other achievements [33, 34].

Quantum key distribution (QKD) is one of the most successful applications of quantum information technology [2, 3]. It can provide unconditionally secure key

distribution between two remote participants, Alice and Bob. The security of QKD is guaranteed by the fundamental laws of quantum mechanics. In order to make it more robust, Lo et al. proposed the measurement-device-independent QKD (MDI-QKD) protocol, which can remove all detector side-channel attacks that are the major security loopholes in QKD systems. These protocols rigorously prove the security of the key distribution process, but few people consider how to improve the efficiency of particle utilization in the QKD process, that is, how to use all particles for eavesdrop detection and quantum key distribution, minimizing Waste of particle resources in the QKD process.

In another area of application of quantum resources, symmetrically private information retrieval (SPIR) problem also has solutions in the quantum scenarios, like the quantum symmetrically private information retrieval (QSPIR), namely the quantum private queries (QPQ). Giovannetti et al. proposed a novel cheat-sensitive QPQ protocol (GLM-protocol) [26], where the database is represented by an oracle operation which is performed on the coming query states. Although most attempts have aimed at reducing the communication complexity of the protocols, it is shown that the reduction in communication and computational complexity is less valuable than achieving a practical protocol. Because of the use of the oracle operation, the above protocols are difficult to implement for large database and high-dimensional oracle operation. To solve this problem, Jakobi et al. for the first time proposed a novel and practical QPQ protocol (J-protocol) based on SARG04 [3] QKD protocol [27]. Using SARG04 QKD protocol, an asymmetric key can be distributed between Alice and Bob, which is used to encrypt the whole database. Alice only knows few bits of the key, which ensures the database privacy. J-protocol can be easily generalized to large database. In 2012, Gao et al. proposed a flexible QPQ scheme (G-protocol) [28] which shows better performance in flexibility, security and communication complexity. However, these papers do not solve the user privacy problem very well, and the process of the protocol is complicated.

Since Bennett and Brassard published the first QKD protocol [1], many quantum communication protocols, including quantum identity authentication (QIA) protocols, have been suggested in the research [32]. Although the QKDs provide unconditional security, they still require an authentication prior to the communication. In most of QIA protocols, quantum entangled states are used [30, 31]. The maintenance of entangled states is a major obstacle to realization. To compensate for this limit, some protocols use classical cryptography with QKD. For instance, Dušek [29] suggested a quantum identification protocol where the BB84 QKD is used to share an identification sequence as common secret information. After Alice and Bob share these secret sequences, they use a classical channel for identity authentication. In order to improve the security and flexibility of identity authentication, we have proposed a two-way identity authentication protocol in this agreement, which can guarantee the privacy of both parties.

In this paper, a multi-function quantum cryptography protocol has been proposed. Through the quantum cryptographic protocol proposed in this paper, we can complete the quantum private query, quantum identity authentication, and quantum key distribution function at one time, which means that quantum resources can be utilized most efficiently through this protocol.

The organization of this paper is demonstrated as follows. In Sect. 2, we propose our protocol. In Sect. 3, the security of this protocol is discussed. At last, the conclusion is given.

2 The Protocol

Step 1: Alice prepares $2N$ qubits which are randomly in one of the states $\{|00\rangle, |11\rangle, |\phi^+\rangle, |\phi^-\rangle\}$. Here

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

The first and second qubits compose the pair 1 (denotes as P_1), the third and fourth qubits composes pair 2 (denotes as P_2)... the $2n-1$ th and $2n$ th qubits composes pair n (denotes as P_n). All of these qubit pairs composes sequence $S = \{P_1, P_2, \dots, P_{n-1}, P_n\}$. Then Alice sends sequence S to Bob.

Step 2: When Bob receives the sequence S , he first chooses some qubit pairs as checking pairs to detect Alice's malicious behavior. For each checking pair, Bob measures each qubit in the Z basis or Bell basis randomly. Then Bob announces the position of these checking pairs and asks Alice to announce the prepared state. If the prepared basis and measurement basis are different, Bob cannot check Alice's behavior, which the probability is $1/2$; if the prepared basis and the measurement basis are same, Bob's measurement result should be same as Alice's prepared state. If the error rate is higher than the predetermined error rate, they abort the protocol. Otherwise, they discard the decoy pairs, then continue to the next step. This step can prevent Alice sending the fake states or the external eavesdropper using the intercept-resent attack.

Step 3: After confirming that Alice is not cheating, and there is no eavesdropper, Bob measures each qubit in the Z basis or Bell basis randomly, and Bob records the measurement base used for each pair of particles. When Bob uses the Z-based measurement for the particles at the i th position, he records the key value corresponding to the i position as 0. When he uses the Bell base to measure the i th position, he records the key value corresponding to the i th position as 1. Then he generates a binary string $key_b = \{0, 1\}^N$. For each pair, Bob announce "0" or "1", where "0" represents his measurement result is in one of the states $\{|00\rangle, |\phi^+\rangle\}$; "1" represents his measurement result is in one of the state $\{|11\rangle, |\phi^-\rangle\}$. It should be noted that, if Bob's measurement result is in one of the state $\{|\psi^+\rangle, |\psi^-\rangle\}$, he will deduce that Alice is cheating, therefore he aborts the protocol.

Step 4: Similar to the SARG04 QKD protocol, Alice can deduce the oblivious key according to her prepared state and Bob's announcement. For example, if Alice prepares the state $|00\rangle$, and Bob announces "0", Alice cannot deduce the key, which

the probability is 1/2; however if Bob announces “1”, Alice will know that Bob must use the “wrong basis”, and then she can deduce the raw key is “1”. After the above Steps, Alice and Bob can get the raw key which Bob knows the whole key and Alice only knows the 1/4 key. Table 1 shows the relationship between Alice’s prepared state and Bob’s measurement result.

Next we discuss the completion of Quantum private query (QPQ), Quantum identity authentication (QIA), and Quantum key distribution (QKD) with this protocol.

Table 1. The relationship between Alice’s prepared state and Bob’s measurement result

Alice’s prepared state	Bob’s measurement basis (raw key)	Bob’s measurement result (announcement)	Alice’s deduction
00⟩	Z basis (0)	00⟩ (0)	Cannot deduce
	Bell basis (1)	ϕ^+ ⟩, (0) ϕ^- ⟩ (1)	Cannot deduce 1
11⟩	Z basis (0)	11⟩ (1)	Cannot deduce
	Bell basis (1)	ϕ^+ ⟩, (0) ϕ^- ⟩ (1)	1 Cannot deduce
ϕ^+ ⟩	Z basis (0)	00⟩ (0) 11⟩ (1)	Cannot deduce 0
	Bell basis (1)	ϕ^+ ⟩ (0)	Cannot deduce
ϕ^- ⟩	Z basis (0)	00⟩ (0) 11⟩ (1)	0 Cannot deduce
	Bell basis (1)	ϕ^- ⟩ (1)	Cannot deduce

2.1 Quantum Private Query

Step 5: After step 4 is completed, Alice and Bob can get the raw key which Bob knows the whole key and Alice only knows the 1/4 key. Just as Jakobi et al. provided the practical QPQ protocol (J-protocol), and to reduce the bits Alice known in the raw key the shared in the above steps, Alice and Bob execute classical post-processing to the final key. We suppose the length of raw key is kN , where k is a natural number, Alice and Bob break raw key up into k parts, thus length of each parts is N . By adding the k parts bitwise, the raw key becomes a final key with length N . Bob knows the whole key, while Alice only knows several bits. The process is similar to that in J-protocol, G-protocol and Y-protocol. If Alice knows nothing of the final key after this post-processing, the protocol should be restarted.

Step 6: At last, Bob can encrypt the database using One-Time-Pad(OTP). Suppose Alice knows the j th bit in the final key, and she wants to know the j th item in the database, she will announce a shift value $s = j - i$. So Bob can shift his final key by s . Finally Bob encrypted the whole database and sent it to Alice. According to i and j , Alice can correctly get the item which she paid for it. At this point, this protocol has completed the quantum private query (QPQ) function.

2.2 Two-Way Quantum Identity Authentication

Step 7: After step 4 is completed, Alice and Bob can get the raw key which Bob knows the whole key (denoted as key_{Bob}) and Alice only knows the 1/4 key (denoted as key_{Alice1}). Alice announces the particle position and key value corresponding to the known key in key_{Alice1} . Bob queries the key value key_{Bob1} of the corresponding particle position in the key_{Bob} according to the content published by Alice. If $key_{Alice1} = key_{Bob1}$, Bob passes Alice's identity authentication, the agreement goes to the next step, otherwise, the agreement is cancelled.

Step 8: Bob sends the measured particle sequence (denoted as S_1) to Alice. Alice randomly selects some particles for sequence S_1 to detect eavesdropping. She randomly selects the Z basis or the Bell basis to measure the selected particles. Alice informs Bob of the particle position information she selected and asks Bob to publish the status information of these particles in S_1 (Similar to step 3, Alice can detect if Bob is cheating, therefore he aborts the protocol). After completing the bit error rate detection, Alice discards the eavesdropping particles and notifies Bob to announce all the particle position information in the Z-base state in sequence S_1 . Alice performs Z-based measurements on these particles. According to the coding rules published by Bob in step 3, Alice encodes the measured particles to obtain key_{Alice2} . At this time, Bob announces the key value key_{Bob2} of the corresponding position. If $key_{Alice2} = key_{Bob2}$, Alice passes the authentication of Bob. At this point, this protocol has completed the two-way identity authentication (two-way QIA) function.

2.3 Quantum Key Distribution

Step 9: After completing step 8, Alice performs a Bell-based measurement on the remaining particles (theoretically all of the Bell state particles), and also obtains the key string key_{Alice3} according to the encoding rule published by Bob in step 3. Alice combines the key string $key_{Alice} = key_{Alice1} + key_{Alice2} + key_{Alice3}$ according to the order of receiving sequence S_1 . At this time, $key_{Alice} = key_{Bob}$ holds, and Alice shares a string of identical binary key strings with Bob. At this point, this protocol has completed the quantum key distribution (QKD) function.

3 Examples of the Protocol

We give an example of the protocol in this section, explaining in detail how this protocol accomplishes QIA and QKD functions. Note that: in our example, Alice and Bob's encoding rules follow the rules that Bob published in step 3. To be more clearly, for each pair, Bob announce "0" or "1", where "0" represents his measurement result is in one of the states $\{|00\rangle, |\phi^+\rangle\}$; "1" represents his measurement result is in one of the state $\{|11\rangle, |\phi^-\rangle\}$.

3.1 Examples of Two-Way QIA

Examples of Step 7

We assume that the particle sequence obtained after bob measurement is $S_1 = \{|00\rangle, |\phi^-\rangle, |\phi^+\rangle, |11\rangle, |\phi^+\rangle, |11\rangle, |00\rangle, |\phi^-\rangle, |\phi^+\rangle, |11\rangle, |\phi^+\rangle, |11\rangle\}$, thus $Key_{Bob} = \{0101010101\}$.

Alice can correctly release the 2nd, 4th, and 6th bits of the key, and Alice's key is $Key_{Alice1} = \{?1?1?1????\}$. Alice announces Key_{Alice1} , and Bob checks the value of the corresponding position in Key_{Bob} . Since $Key_{Bob1} = Key_{Bob(2,4,6)} = \{111\} = Key_{Alice1}$ is established, Bob authenticates the identity of Alice.

Examples of Step 8

Bob sends the sequence S_1 to Alice, Alice selects the first, third, and eighth bits, randomly selects the measurement base for eavesdropping detection, and informs Bob to announce the particle state information of the corresponding position in S_1 . After the eavesdropping test passes, Alice informs Bob to announce all the particle positions and key values in the Z-base state in sequence S_1 (removing the particles used for eavesdrop detection). That is, bob publishes $Key_{Bob2} = Key_{Bob(4,6,7,10,12)} = \{11011\}$, and Alice performs Z-based measurement on the particles in her hands according to the position announced by Bob, and obtains $Key_{Alice2} = \{11011\}$. Because $Key_{Alice2} = Key_{Bob2}$ is established, Alice passes the identity authentication of bob.

3.2 Examples of QKD

Examples of Step 9

Alice performs a Bell-based measurement on the remaining particles (the 2nd, 5th, 9th, and 11th bits remain) to obtain the key sequence $Key_{Alice3} = \{1000\}$. Alice combines the key sequences Key_{Alice1} , Key_{Alice2} and Key_{Alice3} in the subscript order when receiving the sequence s_1 to obtain a Key_{Alice} . At this point, $Key_{Alice} = Key_{Bob} = \{110100101\}$ is established, they finish the quantum key distribution (QKD).

4 Security Analysis

According to the protocol description, the security analysis of this protocol mainly focuses on QPQ and two-way QIA. Note that: the JM attack analysis and the Entangled-Measurement attack analysis for QIA is similar to QPQ (The main safety hazard appears in step 8), so we will not repeat the security analysis.

4.1 The Outsider Attack

4.1.1 The Outsider Attack of QPQ

Compared with QPQ based on B92 protocol, our protocol can stand against an external eavesdropper. Suppose Eve is a malicious eavesdropper who wants to know Alice's secret item in the database. Because one-time-pad (OTP) is proved to be unconditionally

secure, as long as Eve does not know the oblivious key, he cannot get the confidential information. In order to get the oblivious key, he needs to know Bob's operation (whether measure the qubit pair in the Z basis or in the Bell basis). In step 3, Bob will announce some information, only if Eve knows Alice's initial state, he can deduce the secret key. Therefore Eve may take an Intercept-resend attack, however without Alice prepared basis, his malicious behavior will be caught easily. For example, in step 1, suppose Alice prepares state $|00\rangle$ and send them to Bob. Eve may intercept the sequence S, and measures them in Z basis or Bell basis randomly. If he uses right basis (in this case is Z basis), his malicious behavior will not be caught; however if he uses the wrong basis (in this case is Bell basis), he will get the measurement result $|\phi^+\rangle$ or $|\phi^-\rangle$ with equal probability. In step 2, when Bob uses the Z basis to measure the checking sequence, Eve's malicious behavior will be caught with the probability of 1/4. As the checking photons are large enough, he will be caught easily.

4.1.2 The User Privacy of QPQ

Most of the current protocol are cheat-sensitive QPQ protocol. "Cheat-sensitive" means that dishonest database holder Bob will run the risk of being detected if he tries to obtain Alice's query address. In our protocol, Bob only announce in the public channel in step 4, that gives him no chance to send a fake quantum state. Because Alice does not announce anything, so Bob cannot deduce Alice's prepared states. For example, if Bob's measurement result is $|00\rangle$, he cannot judge whether Alice is sending $|00\rangle$, $|\phi^+\rangle$ or $|\phi^-\rangle$. Therefore our protocol has a perfect user privacy.

4.1.3 The Outsider Attack of QIA

As the analysis of QPQ, Eve may intercept the sequence S_1 , and measures them in Z basis or Bell basis randomly. If he uses right basis (in this case is Z basis), his malicious behavior will not be caught; however if he uses the wrong basis (in this case is Bell basis), he will get the measurement result $|\phi^+\rangle$ or $|\phi^-\rangle$ with equal probability. In step 8, when Alice uses the Z basis to measure the checking sequence, Eve's malicious behavior will be caught with the probability of 1/4. As the checking photons are large enough, he will be caught easily too. More importantly, this protocol is a two-way QIA protocol. Anyone who has a dishonest behavior on either Alice or Bob will be detected. Therefore, this quantum protocol is safe and reliable for QIA purposes.

4.2 The JM Attack

In QPQ protocol, we assume Alice is dishonest, i.e. she will try every means to get more oblivious key illegally (more than 1/4 of the raw key) in our protocol. In this section, we will analyze two kind of attack from Alice, i.e. the joint-measurement (JM) attack and entangled-measurement attack.

In 2016, Wei et al. pointed out that the JM attack poses a noticeable threat to the database security in the QPQ protocol. By taking such attack strategy, the malicious user Alice can deduce more item from the database without being caught. To conduct a JM attack, the malicious Alice must hold the states and knows which states contribute the final key simultaneously. However our protocol can resist such kind of attack.

Because in step 1, Alice holds the carrier state, however she doesn't know which states contributes the final key in step 4, she cannot take the joint-measurement attack, because the carrier states are not in her hand anymore after she sending the sequence S to Bob in step 1. Therefore, because the two essential elements for JM attack is isolate, Alice cannot perform the JM attack. More generally, Alice can prepare an entangled states, instead of $\{|00\rangle, |11\rangle, |\phi^+\rangle, |\phi^-\rangle\}$. If Alice can pass the eavesdropping check, Alice will know which qubits will generate a final key and performs joint-measurement to those qubits in her hand. However this malicious behavior will be caught easily. For example, Alice will prepares this quantum state in step 1

$$\begin{aligned} |\Psi\rangle &= \frac{1}{\sqrt{2}} [|000\rangle + |111\rangle]_{123} \\ &= \frac{1}{\sqrt{2}} [(0+1)(00+11) + (0-1)(00-11)]_{123} \end{aligned}$$

Alice keep the first qubit in her hand, and sends particle 2 and 3 to Bob. After Bob receive the particle 2 and 3, he will measure them in Z basis or Bell basis, here we suppose Bob measure them in the Bell basis. Bob will get the measurement result $|\phi^+\rangle$ or $|\phi^-\rangle$ with equal probability. We suppose Bob's measurement result is $|\phi^-\rangle$. Then in step 2, Bob will ask Alice publish her prepared basis and result. Because Alice doesn't know which basis Bob chooses, Alice can only publish the answer randomly. For example, if she announces "Bell basis and $|\phi^+\rangle$ ", Bob will know Alice must sending the fake states, Therefore Alice cannot send the entangled states in order to perform the JM attack.

5 The Entangled-Measurement Attack

The malicious user Alice may take an entangled-measurement attack. Without loss of generality, the malicious Alice may prepare some auxiliary particles $|e\rangle$, and perform unitary operation U to entangle them with the particles in sequence S. After the operation U, state $|0\rangle, |1\rangle$ will change to:

$$\begin{aligned} U \otimes |0e\rangle &= a|0e_{00}\rangle + b|1e_{01}\rangle, \\ U \otimes |1e\rangle &= b'|0e_{10}\rangle + a'|1e_{11}\rangle, \end{aligned}$$

The entangled state $|\phi^+\rangle$ will change to:

$$\begin{aligned} |\phi\rangle_{Eve} &= U \otimes |\phi^+\rangle \\ &= \frac{1}{\sqrt{2}} [(a|0e_{00}\rangle + b|1e_{01}\rangle) \otimes |0\rangle + (b'|0e_{10}\rangle + a'|1e_{11}\rangle) \otimes |1\rangle] \\ &= \frac{1}{\sqrt{2}} (a|0e_{00}0\rangle + b|1e_{01}0\rangle + b'|0e_{10}1\rangle + a'|1e_{11}1\rangle) \end{aligned}$$

When Bob perform the Bell measurement on the checking pairs, only if $|a'| = |a|$, he can escape from the detecting which the probability is $P_{Eve} = \frac{|a|^2 + |a'|^2}{2} = |a|^2$. As the checking photons are large enough, she will be caught easily.

6 Conclusion and Discussion

In this paper, we proposed a novel Quantum cryptography protocol based on Bell state. Our protocol is a multi-function quantum protocol, which can be used to perform QPQ, QIA, and QKD functions. This protocol can improve the utilization efficiency of entangled particles, and can complete a variety of practical functions by preparing only one primary particle. Therefore, our protocol doesn't need the wave-length filter and PNS technique, and our protocol only need 4 kinds of quantum states and realize almost perfect user privacy. By using Bell entangled state, our protocol show better performance in the collective-noise channels.

Acknowledgments. The authors would like to thank the reviewers and editors who have helped to improve the paper.

This work is supported by the National Key Research and Development Project of China (No. 2017YFB0802302), the National Natural Science Foundation of China (No. 61572086, No. 61402058), the Innovation Team of Quantum Security Communication of Sichuan Province (No. 17TD0009), the Academic and Technical Leaders Training Funding Support Projects of Sichuan Province (No. 2016120080102643), the Application Foundation Project of Sichuan Province (No. 2017JY0168), the Key Research and Development Project of Sichuan Province (No. 2018TJPT0012), the Science and Technology Support Project of Sichuan Province (No. 2016FZ0112, No. 2018GZ0204).

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp 175–179. IEEE, Bangalore (1984)
2. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell theorem. *Phys. Rev. Lett.* **68**, 557–559 (1992)
3. Scarani, V., Acin, A., Ribordy, G., Gisin, N.: Quantum cryptography protocols robust against Photon number splitting attacks for. *Phys. Rev. Lett.* **92**, 057901 (2004)
4. Deng, F.G., Long, G.L.: Controlled order rearrangement encryption for quantum key distribution. *Phys. Rev. A* **68**, 042315 (2003)
5. Li, X.H., Deng, F.G., Zhou, H.Y.: Efficient quantum key distribution over a collective noise channel. *Phys. Rev. A* **78**, 022321 (2008)
6. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **65**, 032302 (2002)
7. 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* **68**, 042317 (2003)
8. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. *Phys. Rev. A* **69**, 052319 (2004)

9. Wang, C.: Quantum secure direct communication with high-dimension quantum superdense coding. *Phys. Rev. A* **71**, 044305 (2005)
10. Ye, T.Y., Jiang, L.Z.: Improvement of controlled bidirectional quantum direct communication using a GHZ state. *Chin. Phys. Lett.* **30**(4), 040305 (2013)
11. Chen, Y., Man, Z.X., Xia, Y.J.: Quantum bidirectional secure direct communication via entanglement swapping. *Chin. Phys. Lett.* **24**(1), 19 (2007)
12. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. *Phys. Rev. A* **59**, 1829–1834 (1999)
13. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A* **59**, 162–168 (1999)
14. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes. *Phys. Rev. A* **69**, 052307 (2004)
15. Deng, F.G., Zhou, H.Y., Long, G.L.: Circular quantum secret sharing. *J. Phys. A* **39**, 14089–14099 (2006)
16. Cleve, R., Gottesman, D., Lo, H.K.: How to share a quantum secret. *Phys. Rev. Lett.* **83**, 648 (1999)
17. Yang, Y.G., Wen, Q.Y.: *J. Phys. A - Math. Theor.* **42**, 055305 (2009)
18. Tseng, H.Y., Lin, J., Hwang, T.: *Quantum Inf. Process.* **11**, 373 (2012)
19. Zhang, Z.J., Man, Z.X.: Secure direct bidirectional communication protocol using the Einstein-Podolsky-Rosen pair block. [arXiv:0403215](https://arxiv.org/abs/0403215) pdf (2004)
20. Zheng, C., Long, G.F.: Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs. *Sci. China-Phys. Mech. Astron.* **57**(7), 1238–1243 (2014)
21. Chor, B., Goldreich, O., Kushilevitz, E., Sudan, M.: Private information retrieval. In: *Proceedings 36th IEEE Symposium on Foundations of Computer Science*. IEEE Press (1995)
22. Gertner, Y., Ishai, Y., Kushilevitz, E., Malkin, T.: Protecting data privacy in private information retrieval schemes. *J. Comput. Syst. Sci.* **60**(3), 592–629 (2000)
23. Shor, P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**(5), 1484–1509 (1997)
24. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: QKD-Based quantum private query without a failure probability. *Sci. China-Phys. Mech. Astron.* **58**(10), 100301 (2015)
25. Yang, Y.G., Sun, S.J., Xue, P., Tian, J.: Flexible protocol for quantum private query based on b92 protocol. *Quant. Inf. Process* **13**(3), 805–813 (2014)
26. Giovannetti, V., Lloyd, S., Maccone, L.: Quantum private queries. *Phys. Rev. Lett.* **100**(23), 230502 (2008)
27. Jakobi, M., et al.: Practical private database queries based on a quantum-key-distribution protocol. *Phys. Rev. A* **83**(2), 022301 (2011)
28. Gao, F., Liu, B., Wen, Q.Y.: Flexible quantum private queries based on quantum key distribution. *Opt. Exp.* **20**(16), 17411–17420 (2012)
29. Dušek, M., Haderka, O., Hendrych, M., Mayska, R.: Quantum identification system. *Phys. Rev. A* **60**, 149 (1999)
30. Stinson, D.R.: *Cryptography: Theory and Practice*, 3rd edn. CRC Press, Boca Raton (2005)
31. Kang, M.S., Hong, C.H., Heo, J., Lim, J.I., Yang, H.J.: Controlled mutual quantum entity authentication using entanglement swapping. *Chin. Phys. B* **24**, 090306 (2015)
32. Mihara, T.: Quantum identification schemes with entanglements. *Phys. Rev. A* **65**, 052326 (2002)
33. Tang, X., Juan, X., Duan, B.: A memory-efficient simulation method of Grover's search algorithm. *CMC: Comput. Mater. Continua* **56**(2), 307–319 (2018)
34. Tan, X., Li, X., Yang, P.: perfect quantum teleportation via Bell states. *CMC: Comput. Mater. Continua* **57**(3), 495–503 (2018)