International Journal of Theoretical Physics (2019) 58:2986–2993
https://doi.org/10.1007/s10773-019-04178-5

Two Semi-Quantum Direct Communication Protocols with Mutual Authentication Based on Bell States

Zheng Tao[1] · **Yan Chang**[1] · **Shibin Zhang**[1] · **Jinqiao Dai**[1] · **Xueyang Li**[1]

Received: 10 March 2019 / Accepted: 29 May 2019 / Published online: 11 June 2019

Abstract

In this paper, we proposed two semi-quantum direct communication protocols based on Bell states. By pre-sharing two secret keys between two communicants, Alice with the advanced quantum ability can transmit secret messages to the classical Bob who can only perform the limited classical operations. At the same time, both sides of the communication can comfirm the legitimacy of each other's identity. Security and qubit efficency analysis have been given. The analysis results show that the two protocols can resistant to several well-known attacks and their qubit efficency is higher than some current protocols.

Keywords Authentication · Semi-quantum direct communication · Bell states

PACS 03.67.-a03.65.-w03.65.Ud

1 Introduction

With the rapid development of quantum technology, especially the realization of quantum computing, the current classical cryptography schemes are potentially in danger. Quatum cryptography utilizes the principle of quantum mechanics to provide unconditionally secure information exchange. Since the first quantum key distribution (QKD) was proposed in 1984 [1], a lot of quantum information schemes have been proposed, such as quantum secret sharing (QSS) [2–7], and quantum teleportation [8–12].

In the past decade, quantum secure direct communication (QSDC) has attracted great attention of researchers. In the QSDC protocol, the secret message is transmitted directly without first

---

✉ Shibin Zhang
cuitzsb@cuit.edu.cn

Zheng Tao
296017090@qq.com

[1] School of Cybersecurity, Chengdu University of Information Technology, Chengdu 610225, China

establishing a key to encrypt it. The first QSDC protocol was proposed by Long and Liu in 2000 [13]. In their pionner two-step protocol, they selected an Einstein-Podolsky-Rosen (EPR) pair as the carrier qubit. The concept of quantum data block was proposed to detect eavesdropping efficiently. After that, many QSDC protocols was proposed [14–20]. However, most existing QSDC protocols require users to have full quantum capabilities. Obviously, it's unrealistic for every participant to have such expensive quantum resource and the ability to prepare or measure arbitrary quantum state. To resolve these issues, in 2007, Boyer et al. [21] proposed the first semi-quantum cryptography protocol base on BB84 protocol. In this paper, participants meeting the following criteria are defined as "classical": (1) Reflect the qubits to the sender without disturbance (referred to as REFLECT). (2) Measure the qubits in the basis and then resend the same states of these qubits to the sender (referred to as MEASURE). In 2009, Boyer et al. [22] proposed the semi-quantum key distribution (SQKD) protocol based on randomization by using single photons to further improve the concept of semi-quantum. Since then, the idea of semi-quantum was applied into different quantum information processing task. There are researches focus on semi-quantum secret sharing (SQSS) [23–25], semi-quantum secure direct communication (SQSDC) [26–29] and so on. In 2014, Yu et al. [28] proposed the first authenticated SQKD (ASDKD) protocol. In this paper, by pre-sharing a secret key, a quantum sender can transmit a working key to a classical receiver, and they also modify the operations of semi-quantum. In the operation of MEASURE, the classical receiver don't need to send the measurement results back to the quantum sender. In 2016, Luo and Hwang [29] proposed the two authenticated semi-quantum direct communication protocols without any classical channel. By pre-sharing a master secret key between two communicants, a sender with advanced quantum devices can transmit a secret message to a receiver who can only perform classical operations without any information leakage. In 2017, Meslouhi et al. [30] proposed a cryptanalysis on Yu's ASQKD protocol. In this paper, they pointed out a malicious person can recover a partial master key and launch Man-In-The-Middle attack. Besides, they proved that Bob's operation (MEASURE or REFLECT) must be random.

Inspired by Yu et al. and Luo et al., we propose two authenticated SQSDC protocols based on Bell states by which quantum Alice can transmit a secret message directly to classical Bob. By using uncertainty principle and the quantum entanglement of Bell state, the two proposed protocols rely on the Bell states to share the secret information between Alice and Bob. Both sides of the communication can comfirm the legitimacy of each other's identity, and the difference between these two protocols is that we introduce the quantum error correction code in the second protocol so that it can resist noise.

The rest of this paper is organized as follows. Our two SQSDC protocols is presented in Section 2 and the security analysis is discussed in Section 3. Finally, a discussion and conclusion is drawn in Section 4.

2 The Two Protocols

We suppose that quantum Alice wants to transmit n bits secret message m to semi-quantum Bob. Let's first introduce some prior theoretical basis in these two protocols:

(1) We assume that Alice and Bob pre-shared two secret keys k_1 and k_2, where $k_1, k_2 \in \{0, 1\}^n$. This step can be implemented by using the semi-quantum key distribution protocol, which is proved to be unconditional secure.

(2) When Alice sends particles to Bob, $k_1$is used to encrypt these particles, and k_2 is used to rearrange the order of the encrypted sequence. When Bob sends back particles to Alice, on the contrary, $k_2$is used to encrypt these particles, and k_1 is used to rearrange the order of the encrypted sequence.

(3) We introduce the quantum error correction code (**QECC**) to protect quantum information from errors due to decoherence and other quantum noise. **QECC** is essential if one is to achieve fault-tolerant quantum communication and it contains ***the bit flip code, the sign flip code, the shor code, the Bosonic codes and the general codes***. As described in Luo et al. [29], in this paper, we also conceive that the error correction code, which uses $\frac{n}{4}$-bit codeword to encode s-bit information using generator matrix $G(x^s)$ and can correct t codeword error bits with the error-correcting function $D\left(y^{\frac{n}{4}}\right)$ [31–33].

(4) After performing the Z-based measurement, the encoding rules for the particles are: If the measuremet result is $|0\rangle$, we encode it as 0. If the measuremet result is $|1\rangle$, we encode it as 1.

2.1 The ASQDC Protocol

We assume that the quantum channels here are assumed to be noiseless and lossless. The procedure of this protocol is described in the following steps:

Step 1: Quantum Alice prepares $N = 4n(1+\delta)+k$bits Bell states from$\{|\phi^+\rangle, |\psi^+\rangle\}$, where n is the length of the secret message and $\delta$is a fixed parameter, and k is the length of eavesdropping checking qubits. If the *ith* bit of message is zero, Alice produces the state$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{12}$. Otherwise, she produces the state $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{12}$. Note that the state $|\phi^+\rangle$ is used to encode the bit 0: If the first and second qubits of the state ($q_1$andq_2) are measured separately in Z-basis, according to the encoding rules, we always have$q_1 \oplus q_2 = 0$. Similarly, we uses the state $|\psi^+\rangle$ to encode the bit 1. After that, Alice generates a sequence of Bell states $S = (S_1, ..., S_n)$based on the secret message m, and a sequence of Bell states$C = (C_1, ..., C_k)$based on the checking photons. Alice divides each Bell states of the sequence S into the first qubit as home sequence (H) and the second qubit as travel sequence (T). Alice divides the sequence$C$ into two ordered sequences with the same length, $C_A = \{C^1{}_1, ..., C^1{}_k\}$ and$C_B = \{C^2{}_1, ..., C^2{}_k\}$. To resist the two kinds of Trojan horse attacks [34–36], Bob must place a wavelength filter and a photon number spliter (PNS) before he receives the qubits.

Step 2: Alice encrypts the travel sequence (T) with key k_1 and gets the sequence $Q = E_{k_1}(T)$, then she rearranges the two sequences Q and C_B with key $k_2$and gets the sequence$S_N = R_{k_2}(Q, C_B)$. Alice keeps home sequence (H) and C_A and sends S_N to Bob. It should be noted that the encryption and decryption algorithm used by these two protocol must be classical algorithm.

Step 3: After receiving the sequenceS_N, Bob uses key $k_1$to decrypt it and restores the correct order of sequence $T$and C_B with keyk_2. For sequence$T$, he uses the Z-basis $(|0\rangle, |1\rangle)$ to measure the qubits and keeps the result to composeMR_B. Bob encrypts the sequence C_B with key k_2 and get the new sequence$C_{BE} = E_{k_2}(C_B)$, and he reoders C_{BE} with key k_1 to get$C_{BER} = R_{k_1}(C_{BE})$. Then Bob sends C_{BER} back to Alice.

Step 4: When Alice receives the sequenceC_{BER}, she can restore the correct order of C_{BER} to get C_{BE} with keyk_1, and she decrypts C_{BE} with key k_2 to get the sequence which name isC_{BD}. Alice performs Bell measurement on C_{BD} and C_A to obtainC_N, and she cheak whether each corresponding set of two qubits in C_N is consistent with the initial eavesdropping checking qubits sequence$C$. More specifically, if$C_N = C$, it means that the transmission between Alice and Bob is secure. Otherwise, they will terminate the protocol and restart it.

Step 5: Alice performs Z-basis measurement on sequence $H$and gets the measurement resultMR_A. Alice can get a binary key string $k_a$based on the encoding rules: When MR_A is in state $|0\rangle$, she assigns the value of k_a to 0. Otherwise, the value of k_a is 1. Bob gets a binary key string k_b according to the same encoding rules.

Step 6: Alice publishes her keychainsk_a. Then Bob uses k_a and k_b to recover the secret message by$m = k_a \oplus k_b$. More specifically, Bob performs the XOR operation for each bit pair in k_a andk_b.

2.2 The Noise-Resistant ASQDC Protocol

Noise exists in the real communication environment and it will change the quantum qubit state. In order to resist noise in the quantum channel, we use the linear error correction code with our protocol 2.

Step 1★: Alice follows the same steps of Sect. 2.1 to generate the sequence $H$and$T$. Then Alice generates the checking value of the eavesdropping sequence C randomly in the bit of 0 and 1. After that, Alice divides the sequence C into C_A and C_B and calculates the codeword of C_B under ***QECC***, denoted asC_{BECC}.

Step 2★: Same as Protocol 1.

Step 3★: Bob gets the sequence C_{BECC} and $T$with key $k_1$andk_2. For sequence$T$, he performs the same procedures as Protocol 1 to obtainMR_B. Bob uses the key $k_1$andk_2 to encrypt and reorder theC_{BECC}, and sends back the new sequence C_{BECCN} to Alice.

Step 4★: After Alice receivesC_{BECCN}, she reoders and decrypts it to recovery C_{BECC} based on the key $k_1$andk_2. Through the same process as Protocol 1, Alice performs Bell measurement on C_{BECCN} and C_A to obtainC_{NECC}. Similarly, if$C_{NECC} = C$, it means the message transfer process is secure. Otherwise, the protocol must be shut down and restart.

Step 5★: Alice and Bob obtain the binary key string k_a and k_b after the same operation as Step 5 in Protocol 1.

Step 6★: Alice publishes her keychaink_a, and Bob performs XOR operation to recover the secret message by$m = k_a \oplus k_b$.

3 Security Analysis

In this section, we will analysis the Impersonation attack, the Intercept-and-resend attack, and the Trojan horse attack. We also analysis the reuse of the two pre-shared key and the qubits efficiency. It should be noted that, the security analysis of the noise-resistant ASQDC protocol is the same.

3.1 The Impersonation Attack

Eve may try to impersonate Alice to send a forged message to Bob. Suppose Eve generates a sequence of qubitsS_{NE}, and sends them to Bob in Step 2. However, Eve cannot perform the correct reorder and encrypt operation on S_{NE} without knowing the pre-shared the key k_1 andk_2, and the comparison will be failed. So Eve will be caught by Bob with a probability close to 1. On the other hand, Eve may try to impersonate Bob to cheat Alice by intercept the sequence S_N from Alice to Bob in Step 2. Since Eve doesn't know the secret key k_1 andk_2, Eve doesn't know how to reoder the qubit sequence. Suppose Eve successfully restored the correct order of the particles, however, Eve cannot encrypt and reoder the checking qubit sequence$C_B$without known the key k_1 andk_2. In this case, the illegal operation of Eve will definitely be discovered.

3.2 The Intercept-and-Resend Attack

The Eve can take the intercept-and-resend attack to get the secret message m without being detected. Eve intercepts the sequence S_N and measures it with the Z-basis. Then Eve generates the same states based on the measurement result and sends them to Bob. However, the original sequence S_N is reordered with the checking sequenceC_B and the sequence Q based onk_2, where the sequence $Q$is obtained by the sequence T being encrypted byk_1. Eve knows nothing about the key $k_1$andk_2, so Eve cannot correctly distinguish between the sequence$C_B$and the sequence$T$, if Eve performs the wrong operation, Alice will detect the eavesdropping behavior of Eve. More importantly, the sequence is always in the hands of Alice and will not be published. Even if Eve obtains the measurement result of the sequence$T$, it cannot obtain the information directly related to the message m.

3.3 The Trojan Horse Attack

Our protocol is a two-way communication process, so there may be the Trojan horse attack. The Eve or malicious Bob may implement a Trojan attack to get the secret key. To resist the two kinds of Trojan horse attacks [34–36], Alice and Bob must place a wavelength filter and a photon number spliter (PNS) before she and he receives the qubits. If it is found that the wavelength of the received particle is not within the previously agreed range, the protocol will terminate and redistribute the secret key.

3.4 The Analysis of the Two Pre-Share Keys

Due to the unconditional security of semi-quantum key distribution, only Alice and Bob know the secret key $k_1$andk_2. During the communication process, they must never publish the two secret pre-shared keys. After the above analysis, the malicious users cannot the two pre-shared keys by the Impersonation attack, the Intercept-and-resend attack, and the Trojan horse attack. As long as they key is well preserved, the communicants do not have to renew the secret keys, only when a failure occurs in the eavesdropping check or when the secret keys are used for a long period of time does, the new secret keys have to be shared again between Alice and Bob.

Table 1 The comparison of qubit efficiency

Protocol	b_s	q_c	d	q_t	b_t	efficiency
SPQSDC1	n	$4n$	$17n$	$21n$	$2n$	$\eta = 4.35\%$
SPQSDC2	n	$3n$	$11n$	$14n$	$2n$	$\eta = 6.25\%$
SQSDC	n	$2n$	$4n$	$6n$	0	$\eta = 16.7\%$

3.5 The Efficiency Analysis

The information theoretical efficiency [37] is defined as$\eta = \frac{b_s}{q_t + b_t} \times 100\%$, where$b_s$, q_t and $b_t$are the secret information bits transmitted, the total qubits used and the classical bits exchanged between Alice and Bob. And$q_t = q_c + d$, where q_c means the number of qubits used for both sending the message and $d$means the number of qubits used for checking an eavesdropping attempt. In 2017, Shukla et al. [38] have analyzed the efficiency values of these four protocols in detail and given the reasons for explanation. We use their ideas to calculate the efficiency of our two protocols. Note that: The information transfer process of our two protocols is the same.

Firstly, Bob does not need to exchange any classical information with Alice in our two protocols. So the$b_t = 0$. We suppose the length of the secret message m is n, which means the$b_s = n$. In order to transmit n bits of message, Alice needs to use *2n* bits quantum qubits to carry them (n bits Bell states), so the$q_c = 2n$. Alice sends the sequence C_B(2n) to Bob for eavesdropping detection. Then Bob sends the encrypted sequence C_B (2n) back to Alice. So we obtain the$d = 2n + 2n = 4n$, the qubit efficiency will be$\eta = \frac{n}{6n+0} \times 100\% = 16.7\%$. From Table 1, we can see it is obvious that the efficiency of our protocol is higher than these two protocols in Shukla et al. [38] Here we will abbreviate these two protocols as **SPQSDC1, SPQSDC2**, and our protocol is denoted as **SQSDC**.

4 Discussion and Conclusion

In this paper, we proposed two authenticated SQSDC protocols, which can be used between a quantum sender and a classical receiver. The first protocol is in the ideal environment. The second protocol, with the introduction of a linear error correction code, can resist the random noise in the quantum channel. With the pre-shared key $k_1$andk_2, both proposed protocols can complete the mutual authentication. Efficiency analysis proves that our two protocols have good qubit efficiency and security analyses show that the proposed peotocol are resistant to the Impersonation attack, the Intercept-and-resend attack, and the Trojan horse attack. The pre-shared two secret keys can be reused mutiple times.

Acknowledgments We are very grateful to the reviewers and the editors for their invaluable comments and detailed suggestions that helped to improve the quality of the present paper.

This work is supported by the National Natural Science Foundation of China (Grant Nos.61572086, 61402058), the Application Foundation Project of Sichuan Province of China (Grant No. 2017JY0168), the National Key Research and Development Program (No. 2017YFB0802302) , Sichuan innovation team of quantum security communication (No.17TD0009), Sichuan academic and technical leaders training funding support projects(No. 2016120080102643)the Fund for Middle and Young Academic Leaders of CUIT (Grant No. J201511).

References

1. Bennett C.H., Brassard, G.: Public key distribution and coin tossing. In: Proceedings of the IEEE international conference on computers, systems and signal processing, Bangalore, pp. 175–179. IEEE, New York (1984)
2. Hillery, M., Buoek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A. **59**, 1829 (1999)
3. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A. **69**, 052307 (2004)
4. Han, L.F., Liu, Y.M., Shi, S.H., Zhang, Z.J.: Improving the security of a quantum secret sharing protocol between multiparty and multiparty without entanglement. Phys. Lett. A. **361**, 24 (2007)
5. Deng, F.G., et al.: Efficient high-capacity quantum secret sharing with two-photon entanglement. Phys. Lett. A. **372**, 1957 (2008)
6. Han, L.F., et al.: Multiparty quantum secret sharing of secure direct communication using single photons. Opt. Commun. **281**, 2690 (2008)
7. Li, X.H., et al.: Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state. J. Phys. B. **39**, 1975 (2006)
8. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **70**, 1895 (1993)
9. Man, Z.X., Xia, Y.J., An, N.B.: Genuine multiqubit entanglement and controlled teleportation. Phys. Rev. A. **75**, 052306 (2007)
10. Han, L.F., et al.: Communications in Theoretical Physics Revisiting Probabilistic Teleportation Scheme for atomic state via cavity QED. Commun. Theor. Phys. **46**, 217 (2006)
11. Deng, F.G., et al.: Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement. Phys. Rev. A. **72**, 022338 (2005)
12. Huelga, S.F., Plenio, M.B., Vaccaro, J.A.: Remote control of restricted sets of operations: teleportation of angles. Phys. Rev. A. **65**, 042316 (2002)
13. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A. **65**, 032302 (2002)
14. Bostrom, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
15. Long, G.L., et al.: Quantum secure direct communication and deterministic secure quantum communication. Front Phys. China. **2**, 251 (2002)
16. Liu, D., Chen, J.L., Jiang, W.: High-capacity quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom. Int. J. Theor. Phys. **51**, 2923 (2012)
17. Chang, Y., et al.: Quantum broadcast communication and authentication protocol with a quantum one-time pad. Chin. Phys. B. **23**, 010305 (2014)
18. Li, X.H., et al.: Quantum secure direct communication with quantum encryption based on pure entangled states. Chin. Phys. **16**, 2149 (2007)
19. Gu, B., et al.: Robust quantum secure direct communication with a quantum one-time pad over a collective-noise channel. Sci. China Phys. Mech. Astron. **54**, 942 (2011)
20. Wang, C., et al.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A. **71**, 044305 (2005)
21. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical bob. Phys. Rev. Lett. **99**(14), 140501 (2007)
22. Boyer, M., Gelles, R., Kenigsberg, D., et al.: Semiquantum key distribution. Phys. Rev. A. **79**, 032341 (2009)
23. Li, Q., Chan, W.H., Long, D.Y.: Semiquantum secret sharing using entangled states. Phys. Rev. A. **82**(2), 022303 (2010)
24. Li, L.Z., Qiu, D.W., Mateus, P.: Quantum secret sharing with classical bobs. J. Phys. A Math. Theor. **46**, 045304 (2013)
25. Lin, J., Yang, C.W., Tsai, C.W., Hwang, T.: Intercept-resend attacks on semi-quantum secret sharing and the improvements. Int. J. Theor. Phys. **52**, 156–162 (2013)
26. Zou, X.F., Qiu, D.W.: Three-Step semiquantum secure direct communication protocol. Science China Physics, Mechanics Astronomy (2014)
27. Yang, C.W., Hwang, T., Lin, T.H.: Modification attack on QSDC with authentication and the improvement. Int. J. Theor. Phys. **52**(7), 2230–2234 (2013)

28. Yu, K.F., Yang, C.W., Liao, C.H., Hwang, T.: Authenticated semi-quantum key distribution protocol using bell states. Quantum Inf. Process. **13**(6), 1457–1465 (2014)
29. Luo, Y.P., Hwang, T.: Authenticated semi-quantum direct communication protocols using bell states. Quantum Inf. Process. **15**, 947–958 (2016)
30. Meslouhi, A., Hassouni, Y.: Cryptanalysis on authenticated semi-quantum key distribution protocol using bell states. Quantum Inf. Process. **16**(18), (2017)
31. Li, Y.-B., Qin, S.-J., Yuan, Z., Huang, W., Sun, Y.: Quantum private comparison against decoherence noise. Quantum Inf. Process. **12**(6), 2191–2205 (2013)
32. Li, Y.-B., Wang, T.-Y., Chen, H.-Y., Li, M.-D., Yang, Y.-T.: Fault-tolerate quantum private comparison based on GHZ states and ECC. Int. J. Theor. Phys. **52**(8), 2818–2825 (2013)
33. Li, Y.-B., Wen, Q.-Y., Qin, S.-J., Guo, F.-Z., Sun, Y.: Practical quantum all-or-nothing oblivious transfer protocol. Quantum Inf. Process. **13**(1), 131–139 (2014)
34. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A. **351**, 23 (2006)
35. Deng, F.G., Li, X.H., Zhou, H.Y., et al.: Erratum: improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A. **73**, 049901 (2006)
36. Yang, Y.G., Sun, S.J., Zhao, Q.Q.: Trojan-horse attacks on quantum key distribution with classical bob. Quantum Inf. Process. **14**, 681 (2015)
37. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**, 5635 (2000)
38. Shukla, C., Thapliyal, K., Pathak, A., et al.: Asymmetric quantum dialogue in noisy environment. Quantum Inf. Process. **16**, 295 (2017)