Int J Theor Phys (2014) 53:188–193
DOI 10.1007/s10773-013-1796-8

Single Sign-On Under Quantum Cryptography

Guiping Dai · Yong Wang

Received: 22 May 2013 / Accepted: 13 August 2013 / Published online: 7 September 2013

Abstract Single Sign-On (SSO) is an important cryptography mechanism in distributed systems and is implemented in many known systems, such as the famous Kerberos. Quantum cryptography has excellent security properties guaranteed by physical principles and makes great influence on traditional cryptography. In this paper, we combines the SSO mechanism and quantum cryptography together. A SSO solution under quantum cryptography is designed. Through security analysis, we show that this solution has good security properties.

Keywords Single Sign-On · Quantum cryptography · User authentication

1 Introduction

Physical principles, such as Heisenberg uncertainty principle and quantum no-cloning theorem, guarantee the security of quantum cryptography, even under the attacks with quantum computation ability. Since the occurrence of BB84 protocol [1], the first key distribution protocol in quantum cryptography, quantum cryptography has a rapid development, and various directions are developed, such as key distribution [1–3], secure direct communication [4–10], quantum secret sharing [11–30], and also quantum authentication identity [31–38].

There are two kind of channels presented in QKD (quantum key distribution): the quantum channel and the public channel. The quantum channel is protected by quantum mechanisms and can be used to encode bits onto quantum states that any measure can be detected by legitimate users. And the public channel is used to exchange classical information. If

G. Dai (✉)
College of Electronic Information and Automatic Control, Beijing University of Technology, Beijing 100124, China
e-mail: daigping@bjut.edu.cn

Y. Wang
College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China

Mallory controls the classical public channel as well as monitoring the quantum channel, QKD will sure fail. To conquer this problem, QAI (Quantum Authentication Identity) is necessary. The fundamental requirements of authentication are to assure the involved communication partners are all legitimate. That is, QAI is to assure the shared secrets between Alice and Bob are only known to Alice and Bob.

Most QAI protocols use two kind of channels: the quantum channel and the unjammable public channel, and usually they are so-called self-enforcing, that is, there are no parties other than Alice and Bob involved. But, in fact, the realistic channel between Alice and Bob is usually jammable. And also to prevent the "man-in-the-middle" attacks, the introduction of a trusted third party (TTP) is necessary [32, 33].

SSO (Single Sign-On) [39, 40] is an important cryptography solution for distributed systems, and is implemented in many distributed systems, such as the famous Kerberos [41]. With SSO, a user can authenticate himself/herself only once and is automatically logged into ASes (Application Servers) as necessary, without necessarily further manual authentications. Considering SSO solutions under quantum cryptography is interesting. In this paper, we give a quantum SSO solution, though it may be quite simple, it is the first attempt to make SSO under quantum cryptography.

This paper is organized as follows. In Sect. 2, we introduce traditional SSO solution briefly. A Quantum SSO solution is designed in Sect. 3. Then, we analyze the security of the quantum SSO solution in Sect. 4. Finally, we conclude our work in Sect. 5.

2 Traditional SSO Solution

The traditional SSO solution is illustrated in Fig. 1. There are usually four parts in a SSO Solution.

1. TTP (Trusted Third Party): the trusted authority to solve the initial secret among other parts. It has the ability to generate security keys, operate cryptography computations and

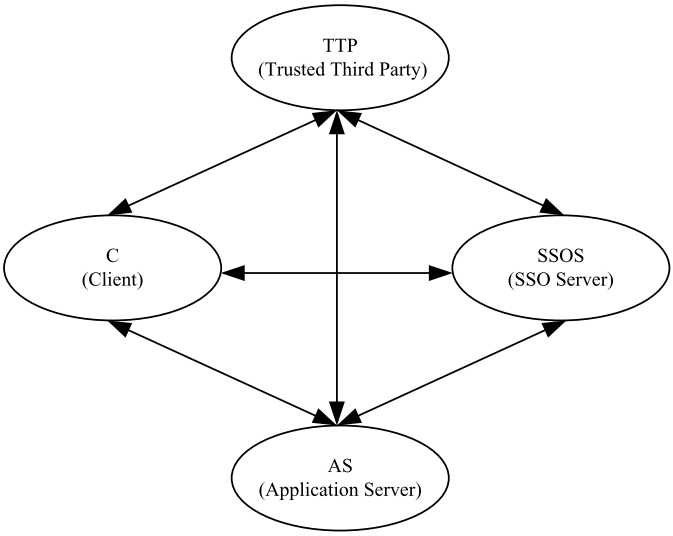

Fig. 1 Traditional SSO solution

exchange information with other parts. The open information of TTP is well known to other parts.
2. SSOS (SSO Server): the server which the client first signs on. It knows all the open information of application servers and has the ability to generate security keys, operate security computations and exchange information with other parts.
3. AS (Application Server): the server which contains various applications. It can also execute cryptography computations and exchange information with other parts.
4. C (Client): the user who wants to access applications located in ASes. He/She can also execute cryptography computations and exchange information with other parts.

The steps of the SSO solution are as follows.

1. TTP generates security keys for SSOS (K_{SSOS}), ASes (K_{AS}) and C (K_C).
2. C requests to TTP for a session key with SSOS, denotes as $K_{C,SSOS}$.
3. TTP sends the session key $K_{C,SSOS}$ to involved C and SSOS.
4. C requests to SSOS with an authentication message encrypted by $K_{C,SSOS}$.
5. SSOS returns the session key $K_{C,AS}$ to involved C and AS.
6. C requests to the AS with an authentication message encrypted by $K_{C,AS}$, may be along with the application data.
7. AS responds to C and a session is established.

3 A Quantum SSO Solution

In Fig. 2, a quantum solution for SSO is given. There are three kind of channels in this solution: the quantum channel used to distribute security keys, the unjammable public channel used to distribute the session key, and the jammable public channel used to process actual sessions.

3.1 Preparing Phase

1. TTP sends to SSOS a long bit string encoded using the BB84 protocol [1] or other QKD protocols along with error correction and privacy amplification to generate a security key K_{SSOS} through the quantum channel between TTP and SSOS.
2. Similarly, TTP sends to AS a long bit string encoded using the BB84 protocol [1] or other QKD protocols along with error correction and privacy amplification to generate a security key K_{AS} through the quantum channel between TTP and AS.
3. Similarly, TTP sends to C a long bit string encoded using the BB84 protocol [1] or other QKD protocols along with error correction and privacy amplification to generate a security key K_C through the quantum channel between TTP and C.

3.2 Authenticating Between C and SSOS Phase

1. C requests to TTP for a session key $K_{C,SSOS}$ with SSOS through the unjammable public channel between C and TTP.
2. TTP generates the session key $K_{C,SSOS}$, encrypts the identity of C with K_{SSOS} to $\{I_C\}_{K_{SSOS}}$, then encrypted these message with K_C to $\{K_{C,SSOS}, \{I_C\}_{K_{SSOS}}\}_{K_C}$, and sends it to C through the unjammable public channel between C and TTP.
3. TTP also sends the generated session key $K_{C,SSOS}$ encrypted by K_{SSOS} to SSOS through the unjammable public channel between TTP and SSOS.

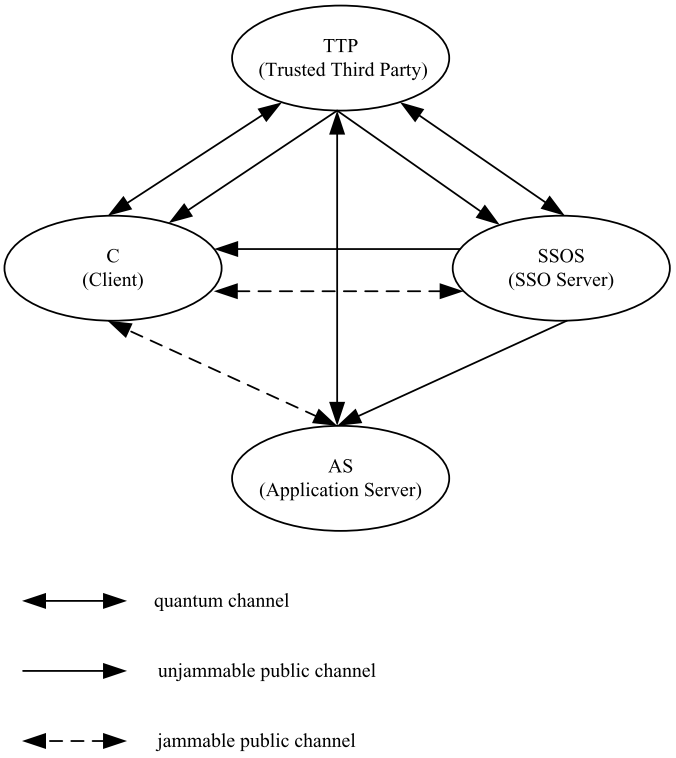

Fig. 2 A quantum SSO solution

3.3 Authenticating Between C and AS Phase

1. C requests to SSOS with a message $I_{AS}, \{I_C\}_{K_{SSOS}}, \{A_C\}_{K_{C,SSOS}}$ through the jammable public channel between C and SSOS for a session key $K_{C,AS}$, where I_{AS} is the identity of AS, I_C is the identity of C, A_C is the authentication message from C.
2. SSOS gets I_{AS} and encrypts it with the security key of AS K_{AS}, generates the session key $K_{C,AS}$, and then encrypts with $K_{C,SSOS}$ to get $\{\{I_{AS}\}_{K_{AS}}, K_{C,AS}\}_{K_{C,SSOS}}$, and responds it to C through the jammable public channel between C and SSOS.
3. SSOS also sends the generated session key $K_{C,AS}$ encrypted by K_{AS} to AS through the unjammable public channel between SSOS and AS.
4. C requests to AS with a message $\{I_{AS}\}_{K_{AS}}, \{A_C\}_{K_{C,AS}}$ through the jammable public channel between C and AS. Then AS responds to C and a session is established.

4 Security Analysis

In the quantum solution for SSO, the preparing phase uses QKD to distribute security keys through the quantum channel. The security of the preparing phase is guaranteed by the quantum mechanisms and is so-called non-conditional secure which is assured by quantum physical principles.

The security of authenticating phase is dependent on traditional cryptography, that is, some computational assumptions. Especially for interactions through the jammable public

channel, the algorithms, length of the session key is very important. To prevent some known attacks, such as replay attacks, in the authentication messages, a timestamp and a random number can be placed.

But, in the quantum solution for SSO, the TTP knows the session key $K_{C,SSOS}$ and the SSOS knows the session key $K_{C,AS}$. This makes the interaction between C and SSOS is open for TTP and the interaction between C and AS is open for SSOS. This solution will be refined in future.

5 Conclusions

SSO is important for distributed systems. In this paper, we design a solution for SSO under quantum cryptography. Though this solution is quite simple, as we known, it is the first attempt to give SSO a quantum solution. This solution uses QKD to distribute the security keys which is so-called non-conditional secure. In future, we will do more works to make it more secure by use of techniques of quantum cryptography.

Acknowledgements This research was partly supported by Beijing Municipal Education Commission Projects grants JC007011201004, Beijing Municipal Education Colleges and Universities to Deepen Talents Scheme, and CSC Projects in China.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179. IEEE Press, New York (1984)
2. Ekert, A.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661–664 (1991)
3. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)
4. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
5. 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)
6. Lin, S., Wen, Q.Y., Gao, F., Zhu, F.C.: Quantum secure direct communication with chi-type entangled states. Phys. Rev. A **78**, 064304 (2008)
7. Wang, T.-Y., Wen, Q.-Y., Zhu, F.-C.: Multiparty controlled quantum secure direct communication with phase encryption. Int. J. Quantum Inf. **9**(2), 801–807 (2011)
8. Yang, Y.-G., Wen, Q.-Y.: Threshold quantum secure direct communication without entanglement. Sci. China Ser. G, Phys. Astron. **51**(2), 176–183 (2008)
9. Cao, W.-F., Yang, Y.-G., Wen, Q.-Y.: Quantum secure direct communication with cluster states. Sci. China Ser. G, Phys. Astron. **53**(7), 1271–1275 (2010)
10. Gao, F., Qin, S.J., Wen, Q.Y., et al.: Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. Opt. Commun. **283**, 192 (2010)
11. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
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. Guo, G.P., Guo, G.C.: Quantum secret sharing without entanglement. Phys. Lett. A **310**, 247–251 (2003)
15. Zhang, Z.J., Man, Z.X.: Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys. Rev. A **72**, 022303 (2005)
16. Yang, Y.-G., Wang, Y., Chai, H.-P., Teng, Y.-W., Zhang, H.: Member expansion in quantum (t,n) threshold secret sharing schemes. Opt. Commun. **284**(13), 3479–3482 (2011)
17. Lin, S., Wen, Q.Y., Qin, S.J., et al.: Multiparty quantum secret sharing with collective eavesdropping check. Opt. Commun. **282**, 4455–4459 (2009)

18. Yang, Y.-G., Wen, Q.-Y.: Comment on: "Efficient high-capacity quantum secret sharing with two-photon entanglement" [Phys. Lett. A **372**, 1957 (2008)]. Phys. Lett. A **373**(3), 396–398 (2009)
19. Wang, T.Y., Wen, Q.Y., Gao, F., Lin, S., Zhu, F.C.: Cryptanalysis and improvement of multiparty quantum secret sharing schemes. Phys. Lett. A **373**, 65–68 (2008)
20. Yang, Y.-G., Teng, Y.-W., Chai, H.-P., Wen, Q.-Y.: Verifiable quantum (k,n)-threshold secret key sharing. Int. J. Theor. Phys. **50**(3), 792–798 (2011)
21. Yang, Y.-G., Wen, Q.-Y.: Threshold multiparty quantum-information splitting via quantum channel encryption. Int. J. Quantum Inf. **7**(6), 1249–1254 (2009)
22. Wang, T.Y., Wen, Q.Y.: Security of a kind of quantum secret sharing with single photons. Quantum Inf. Comput. **11**(5–6), 434–443 (2011)
23. Lin, S., Wen, Q.Y., Gao, F., Qin, S.J., et al.: Improving the security of multiparty quantum secret sharing based on the improved Bostrom-Felbinger protocol. Opt. Commun. **281**, 4553–4554 (2008)
24. Yang, Y.-G., Teng, Y.-W., Chai, H.-P., Wen, Q.-Y.: Fault tolerant quantum secret sharing against collective noise. Phys. Scr. **83**(2), 025003 (2011)
25. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: A special attack on the multiparty quantum secret sharing of secure direct communication using single photons. Opt. Commun. **281**, 5472–5474 (2008)
26. Wang, T.Y., Wen, Q.Y., Zhu, F.-C.: Cryptanalysis of multiparty quantum secret sharing with Bell states and Bell measurements. Opt. Commun. **284**(6), 1711–1713 (2011)
27. Yang, Y.-G., Wang, Y., Teng, Y.-W., Wen, Q.-Y.: Universal three-party quantum secret sharing against collective noise. Commun. Theor. Phys. **55**(4), 589–593 (2011)
28. Yang, Y.-G., Chai, H.-P., Wang, Y., Teng, Y.-W., Wen, Q.-Y.: Fault tolerant quantum secret sharing against collective-amplitude-damping noise. Sci. China Ser. G, Phys. Astron. **54**(9), 1619–1624 (2011)
29. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs. Phys. Rev. A **72**, 044301 (2005)
30. Qin, S.-J., Gao, F., Wen, Q.-Y., Zhu, F.-C.: Cryptanalysis of the Hillery-Bužek-Berthiaume quantum secret-sharing protocol. Phys. Rev. A **76**, 062324 (2007)
31. Dušek, M., Haderka, O., Hendrych, M., et al.: Quantum identification system. Phys. Rev. A **60**, 149–156 (1999)
32. Curty, M., Santos, D.J.: Quantum authentication of classical messages. Phys. Rev. A **64**, 062309 (2001)
33. Ljunggren, D., Bourennane, M., Karlsson, A.: Authority-based user authentication in quantum key distribution. Phys. Rev. A **62**, 022305 (2000)
34. Zhang, Z.S., Zeng, G.H., Zhou, N.R., Xiong, J.: Quantum identity authentication based on ping-pong technique for photons. Phys. Lett. A **356**, 199–205 (2006)
35. Huang, P., Zhu, J., Lu, Y., Zeng, G.H.: Quantum identity authentication using Gaussian-modulated squeezed states. Int. J. Quantum Inf. **9**(2), 701–721 (2011)
36. Wang, J., Zhang, Q., Tang, C.J.: Multiparty simultaneous quantum identity authentication based on entanglement swapping. Chin. Phys. Lett. **23**(9), 2360–2363 (2006)
37. Yang, Y.-G., Wen, Q.-Y.: Economical multiparty simultaneous quantum identity authentication based on Greenberger-Horne-Zeilinger states. Chin. Phys. B **18**(8), 3233–3236 (2009)
38. Yang, Y.-G., Wen, Q.-Y.: Multiparty simultaneous quantum identity authentication with secret sharing. Sci. China Ser. G, Phys. Astron. **51**(3), 321–327 (2008)
39. Botzum, K.: Single Sign On—a contrarian view (2013). http://www.opengroup.org/security/topics.htm
40. Pashalidis, A., Mitchell, C.: A taxonomy of Single Sign-On systems (2013). http://www.isg.rhul.ac.uk
41. Steiner, J., Neuman, C., Schiller, J.: Kerberos: an authentication service for open network systems (1988). http://www.cse.nd.edu/courses/cse598z/www/papers/kerberos.pdf