EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Cryptanalysis and improvement of efficient multiparty quantum secret sharing based on a novel structure and single qubits

Gan Gao[1,2,3*]

[*]Correspondence:
gaogan0556@163.com
[1]Department of Electrical Engineering, Tongling University, Tongling 244061, China
[2]AnHui Engineering Research Center of Intelligent Manufacturing of Copper-Based Materials, Tongling University, Tongling 244061, China
Full list of author information is available at the end of the article

Abstract

In the paper (EPJ Quant. Technol. 10:29, 2023), Kuo *et al.* proposed a multiparty quantum secret sharing protocol based on a novel structure and single qubits. Owing to the absence of an entanglement state, the proposed protocol is more practical than other quantum secret sharing protocols which use entanglement properties. Therefore, we study the security of the proposed protocol and find there exists a security loophole in the n-party ($n \geq 4$) secret sharing case in it, that is, two dishonest agents can collude to obtain (part of) Alice's secret without the help of the other agents. In order to overcome the security loophole, we give an improved protocol and make a security analysis for it. By calculating, the qubit efficiency of the three-party case in it is equal to $\frac{1}{8}$, which is higher than that in Hillery *et al.*'s protocol (Phys. Rev. A 59:1829, 1999).

Keywords: Security loophole; Quantum secret sharing; Single qubits; Rearranging orders

1 Introduction

Cryptography always plays a significant role in human society. Since ancient times, people have relied on cryptography, the art of writing and solving coded messages, to keep their secrets secure. Thus far, many branches of cryptography have been developed. Secret sharing (SS), which was independently proposed by Shamir [3] and Blakley [4] in 1979, is one of the branches. In SS, the secret of a dealer is splitted into several pieces, and each agent holds a piece, and no subset of agents is sufficient to recover the secret, but the entire set is. Twenty years later, by generalizing SS into quantum scenario, Hillery *et al.* [2] proposed the first quantum secret sharing (QSS) protocol using three-particle and four-particle GHZ states of qubits, namely the HBB99 protocol. In fact, the major difference between SS and QSS is what the respective securities rely on. The former's security relies on the high complexity of the underlying mathematical problems, for instance the factorization of large numbers, and so on. And the latter's relies on the fundamental theories in quantum mechanics, for instance the Heisenberg uncertainty principle, the quantum no-cloning theorem, and so on. Another difference between them is the number of actions carried out. SS can only carry out the action of sharing secrets, but not that of checking eavesdropping, while QSS can carry out the two actions simultaneously. Obviously, compared to SS, QSS demonstrates higher security, or say, QSS can ensure the unconditional security of the protocol, but SS can't. According to the definition of SS, we know there are at least two agents in QSS, moreover, there must exist a collaboration between the two agents in recovering the secret of a dealer. In order to prevent the collaboration from dishonestly happening, the attack performed by one agent, that is, the internal attack, needs to be considered during analyzing the security of the protocol.

After the HBB99 protocol was proposed, QSS has received widespread attention and plenty of other protocols [1, 5–65] have been proposed in succession. For instance, in 2003, Bagherinezhad and Karimipour [5] utilized reusable GHZ states as secure carriers to propose a QSS protocol. In 2006, Deng *et al.* [9] proposed a circular QSS protocol, in which the quantum information carrier, single photons or entangled particles, can circularly run. In 2009, Gu *et al.* [14] proposed a high-capacity three-party QSS protocol with quantum superdense coding, in which almost all Einstein-Podolsky-Rosen pairs can be used for carrying useful information. In 2012, Tsai *et al.* [22] proposed a multiparty QSS protocol based on two special entangled states, in which an agent can obtain a shadow of the secret key by simply performing a measurement of single photon without requiring to generate any photon or do any local unitary operation. In 2017, Song *et al.* [28] proposed a (t, n) threshold d-level QSS protocol, in which the d-level secret can be reconstructed only if at least t shares are collected. In 2022, Ju *et al.* [32] proposed a measurement-device-independent QSS protocol, in which the polarization-spatial-mode hyper-encoding technology is used in order to increase single photon's channel capacity, and so on. By the way, two kinds of special QSS have received much attention recently. One is dynamic quantum secret sharing (DQSS) [33–47], in which agents can be added or deleted as well as the secret or sub-secrets (the messages held by agents) can be updated. The other is semi-quantum secret sharing (SQSS) [48–65], in which only the dealer is quantum and all agents are classical.

In 2023, Kuo *et al.* [1] proposed a multiparty QSS protocol based on a novel structure and single qubits. For simplicity, we will call this protocol the KTYC protocol later. It is interesting that the KTYC protocol can ensure the independence of each agent and grant them equal privileges. However, it is somewhat a pity that there exists a security loophole in the n-party ($n \geq 4$) secret sharing case in the KTYC protocol, that is, two dishonest agents can collude to obtain (part of) Alice's secret messages without the help of the other agents.

2 Review of the KTYC protocol

A brief description of the n-party ($n \geq 4$) case in the KTYC protocol [1] is given as follows:

(1) Each agent prepares a sequence composed of $\frac{S}{N}$ qubits. Here, S and N ($N = n - 1$) represent the length of the secret and the number of agents, respectively, and each qubit is randomly in one of the four states: $|0\rangle, |1\rangle, |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. For convenience, $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ are refereed to as the Z and X basis, respectively. Noted that, the prepared sequences must contain decoy qubits for channel checking.

(2) Alice selects out some qubits from the sequence of each agent as decoy qubits to check the security of channels.

(3) After the check, Alice joins these sequences together, that is, she holds one long sequence now. Next, Alice rearranges the order of qubits in the long sequence. Then, she

encodes her secret into the sequence by using $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $Y = |0\rangle\langle 1| - |1\rangle\langle 0|$ gates according to her message "0" and "1", respectively, and divides the long sequence back into N short sequences. Alice inserts decoy qubits into the short sequences and sends them back to all agents.

(4) After receiving the short sequence, each agent checks the security of the channel by the inserted decoy qubits. After confirming all channels are safe, Alice publishes the order of the qubits.

(5) All agents have to cooperate to recover the secret by exchanging the information on original quantum states.

In order that the security loophole can be clearly shown later, the simplest four-party case in the KTYC protocol is described as follows:

(1′) Bob, Charlie and Dave are agents and prepare the short sequences S_B (composed of B_1 and B_d), S_C (composed of C_1 and C_d) and S_D (composed of D_1 and D_d), respectively. Here, B_1, C_1 and D_1 stand for three qubits to carry information and B_d, C_d and D_d stand for decoy qubits. Then they send their sequences to Alice.

(2′) Suppose that Alice chooses B_d, C_d and D_d to check the security of channels. After the check, she drops those qubits.

(3′) Alice combines the three short sequences to be a long sequence S_L, which is denoted with $[B_1, C_1, D_1]$. Assume that S_L becomes $[D_1, B_1, C_1]$ after Alice rearranges the order. According to the secret messages, Alice performs I, Y, and Y gates on qubits B_1, C_1 and D_1, respectively. Then she divides $[D_1, B_1, C_1]$ back into three short sequences and inserts decoy qubits into them. Last, Alice sends sequences S'_B (composed of D_1 and B'_d), S'_C (composed of B_1 and C'_d) and S'_D (composed of C_1 and D'_d) to Bob, Charlie and Dave, respectively.

(4′) Bob, Charlie and Dave check the channels with Alice through the decoy qubits B'_d, C'_d and D'_d. After the check, the decoy qubits are discarded. At this moment, Bob, Charlie and Dave hold only D_1, B_1 and C_1, respectively. Then Alice publishes the order of the encoding qubits.

(5′) Each agent must cooperate to extract the secret by exchanging their bases and secret from Alice.

3 The security loophole

In this section, we will propose a attack on the simplest four-party case. It is seen that, in step (4′), Bob holds qubit D_1 which part of Alice's secret has been encoded on. But, he can't extract the part alone since he can't select the correct basis to measure qubit D_1. Also it is seen that qubit D_1 is prepared by Dave in step (1′). Thus, he knows the basis which qubit D_1 can be correctly measured in. Notice that, Bob doesn't know that the qubit in his hand is qubit D_1 until Alice publishes the order of the encoding qubits. As soon as the order is published, Bob only collaborates with Dave and they can easily extract the secret message encoded on qubit D_1. In other words, Bob and Dave can collude to extract the secret message without the help of Charlie. Similarly, Charlie (Dave) and Bob (Charlie) can collude to extract the secret message encoded on qubit B_1 (C_1) without the help of Dave (Bob). By the way, if the amount of secret message shared by Alice is 1 bit, one single qubit will be only needed. Let's assume that the needed qubit is qubit B_1, which will mean that, without the help of Dave, Bob and Charlie can collaborate to extract the one-bit secret message, that is, all secret messages of Alice. In the case, it isn't known how Dave participates in sharing the one-bit secret message, either.

4 The improved protocol

In the following, we will discuss how to improve the KTYC protocol so that it can stand against the above proposed attack. Of curse, we try our best to retain the features of original protocol. The detailed improvement is as follows.

($1''$) Each of Bob, Charlie and Dave prepares a sequence composed of single qubits, where each qubit is randomly in one of the four states: $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$. Then they send their sequences to Alice.

($2''$) After receiving the sequences, Alice randomly selects out some qubits from every sequence, which act as decoy qubits, and publishes the positions of the selected qubits, and then requires Bob, Charlie and Dave to publish the states of the selected qubits. So she can use the appropriate basis to measure every selected qubit. By comparing the measurement outcomes and the published states, Alice can analyze the error rate of every sequence transmission. If the error rate goes beyond a certain threshold, the process is aborted. Otherwise, the process goes on.

($3''$) Alice discards the selected qubits. At this moment, for convenience, Bob's, Charlie's and Dave's sequences are denoted with $[B_1, B_2, \ldots, B_m]$, $[C_1, C_2, \ldots, C_m]$ and $[D_1, D_2, \ldots, D_m]$, respectively. Next, Alice encodes her secret by performing I or Y gate on each of B_i, C_i and D_i. All participants agree that I and Y are encoded into "0" and "1", respectively. If the secret is "0" ("1"), the gates she can perform are three I gates or one I and two Y gates (three Y gates or one Y and two I gates). Then Alice inserts decoy qubits, which each is randomly in one of the four states: $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$, into the three sequences and sends them back to Bob, Charlie and Dave.

($4''$) After confirming that the sequences have been received, Alice publishes the positions and states of the decoy qubits. So Bob, Charlie and Dave can use the appropriate basis to measure every decoy qubit. By comparing the measurement outcomes and the published states, they can analyze the error rate of the sequence transmission. If the error rate goes beyond a certain threshold, the process is aborted. Otherwise, the process goes on.

($5''$) Discarding decoy qubits, Bob, Charlie and Dave use the appropriate basis to measure the qubits in the same positions in their respective sequence, and can infer the gates performed by Alice. If they want to extract Alice's secret, they must collaborate honestly.

5 Performance analysis

In this section, we will analyze the security and efficiency of the improved protocol.

5.1 Security analysis

In general, in the QSS protocol, internal attackers, that is, dishonest agents, are more powerful than external attackers because they know more information about the secret. Thus, we will focus on the security of the improved protocol for dishonest agents below. In essence, the security of the improved protocol is based on the public discussion on some single qubits (decoy qubits). Next, we will analyze the intercept-resend attack and entanglement-measure attack against the improved protocol.

(i) The improved protocol stands against the intercept-resend attack

Assume that both Bob and Charlie in the improved protocol are dishonest agents. In order to obtain Alice's secret messages without the help of Dave, they can try to launch the intercept-resend attack as follows: in step ($1''$), when Dave's sequence is traveling from

Dave to Alice, they intercept it and immediately measure each qubit in it in the Z basis or X basis. According to the measurement outcomes, they prepare a false sequence which is as long as Dave's sequence and send it to Alice. Since they don't know which state each qubit is in, the probability of guessing right is $\frac{3}{4}$ (the same as in the BB84 protocol [66]). Assume that, the number of the qubits that Alice selects to check eavesdropping is l. As a result, the probability that the false sequence isn't discovered is $(\frac{3}{4})^l$. While l is large enough, $(\frac{3}{4})^l$ is very small. Therefore, the improved protocol can stand against the intercept-resend attack launched by Bob and Charlie.

(ii) The improved protocol stands against entangle-measure attack

As the improved protocol only uses decoy qubits to check eavesdropping, we only consider the effect on decoy qubits for entangle-measure attacks. Similarly, assume that Bob and Charlie are internal attackers. They can try to launch the entangle-measure attack as follows: in advance, they prepare some auxiliary qubits which each is in $|\xi\rangle$. When Dave's sequence is traveling from Dave to Alice, they entangle the qubits in it with the auxiliary qubits by performing a unitary operation U_E. After U_E is performed, the following relations should be established:

$$U_E|0\rangle|\xi\rangle = a|0\rangle|\xi_{00}\rangle + b|1\rangle|\xi_{01}\rangle, \tag{1}$$

$$U_E|1\rangle|\xi\rangle = c|0\rangle|\xi_{10}\rangle + d|1\rangle|\xi_{11}\rangle \tag{2}$$

here, $\|a\|^2 + \|b\|^2 = 1$ and $\|c\|^2 + \|d\|^2 = 1$, and $|\xi_{00}\rangle$, $|\xi_{01}\rangle$, $|\xi_{10}\rangle$ and $|\xi_{11}\rangle$ represent four states probed by Bob and Charlie. If they want to introduce no error in the eavesdropping check by Alice, U_E must satisfy the following conditions:

$$U_E|0\rangle|\xi\rangle = a|0\rangle|\xi_{00}\rangle + b|1\rangle|\xi_{01}\rangle = a|0\rangle|\xi_{00}\rangle, \tag{3}$$

$$U_E|1\rangle|\xi\rangle = c|0\rangle|\xi_{10}\rangle + d|1\rangle|\xi_{11}\rangle = d|1\rangle|\xi_{11}\rangle, \tag{4}$$

$$\begin{aligned} U_E|+\rangle|\xi\rangle &= \big(a|0\rangle|\xi_{00}\rangle + b|1\rangle|\xi_{01}\rangle + c|0\rangle|\xi_{10}\rangle + d|1\rangle|\xi_{11}\rangle\big)/\sqrt{2} \\ &= |+\rangle\big(a|\xi_{00}\rangle + b|\xi_{01}\rangle + c|\xi_{10}\rangle + d|\xi_{11}\rangle\big)/2 \\ &\quad + |-\rangle\big(a|\xi_{00}\rangle - b|\xi_{01}\rangle + c|\xi_{10}\rangle - d|\xi_{11}\rangle\big)/2 \\ &= |+\rangle(a|\xi_{00}\rangle + b|\xi_{01}\rangle + c|\xi_{10}\rangle + d|\xi_{11}\rangle)/2, \end{aligned} \tag{5}$$

$$\begin{aligned} U_E|-\rangle|\xi\rangle &= \big(a|0\rangle|\xi_{00}\rangle + b|1\rangle|\xi_{01}\rangle - c|0\rangle|\xi_{10}\rangle - d|1\rangle|\xi_{11}\rangle\big)/\sqrt{2} \\ &= |+\rangle\big(a|\xi_{00}\rangle + b|\xi_{01}\rangle - c|\xi_{10}\rangle - d|\xi_{11}\rangle\big)/2 \\ &\quad + |-\rangle\big(a|\xi_{00}\rangle - b|\xi_{01}\rangle - c|\xi_{10}\rangle + d|\xi_{11}\rangle\big)/2 \\ &= |-\rangle\big(a|\xi_{00}\rangle - b|\xi_{01}\rangle - c|\xi_{10}\rangle + d|\xi_{11}\rangle\big)/2. \end{aligned} \tag{6}$$

From equations (3)–(6), we can obtain as follows:

$$b = c = 0, \tag{7}$$

$$a|\xi_{00}\rangle - b|\xi_{01}\rangle + c|\xi_{10}\rangle - d|\xi_{11}\rangle = \mathbf{0,} \tag{8}$$

$$a|\xi_{00}\rangle + b|\xi_{01}\rangle - c|\xi_{10}\rangle - d|\xi_{11}\rangle = \mathbf{0} \tag{9}$$

here, **0** denotes a null vector. Therefore, we can conclude that, only when the auxiliary qubit and decoy qubit are in the product state, Bob and Charlie will introduce no error in the eavesdropping check. This means which the improved protocol can stand against the entangle-measure attack.

5.2 Efficiency analysis

There exist two rounds of eavesdropping check in the improved protocol, and decoy qubits are used in each round. In the first round, some qubits are selected from the sequences of agents as decoy qubits. In the second round, decoy qubits are prepared by Alice, in fact, they can be also selected from the sequences of agents. Assume that, in each round, half of the transmitted states are used for the check. Next, let us calculate the qubit efficiency of the improved protocol according to $\eta_q = \eta_u/\eta_t$, where η_q stands for the efficiency, η_u is the number of bits shared and η_t is the total number of qubits. By analyzing, $(n-1)$ qubits carry one-bit classical information in the improved protocol. Furthermore, half qubits in the sequences of agents are discarded in the first round, and half the remaining qubits are discarded again in the second round. Therefore, the qubit efficiency of the improved protocol $\eta_q = \frac{1}{4(n-1)}$. If the improved protocol is three-party QSS protocol, its η_q will be equal to $\frac{1}{8}$. By calculating, we can also obtain that η_q of the three-party HBB99 protocol is equal to $\frac{1}{12}$. Obviously, in the three-party case, the qubit efficiency of the improved protocol is higher than that of the HBB99 protocol.

6 Conclusion

In conclusion, we have pointed out there exists a security loophole in the KTYC protocol, that is, two dishonest agents can collude to obtain (part of) Alice's secret without the help of the other agents. In addition, it is worth emphasizing that our attack on the KTYC protocol doesn't require the dishonest agents to perform any intercepting, entangling, measuring or resending operation, but requires that two special agents can only collude to steal special secret. Here, the "special" means that Bob and Dave can't steal Alice's secret messages encoded on qubits B_1 and C_1, and can only steal that on qubit D_1. So to speak, the security loophole can be pointed out by us since there exists a design flaw in the KTYC protocol itself, that is, part agents can't actively participate in sharing the secret in their protocol. In the end, we give a feasible improvement of the KTYC protocol, which can stand against the attack proposed by us. By the way, in the improved protocol, the agents needn't perform any quantum gate operation, which is similar to the HBB99 protocol.

Acknowledgements
I thank my parents for their encouragements.

Funding
This work is supported by the Program for Academic Leader Reserve Candidates in Tongling University under Grant No. 2020tlxyxs43, the Talent Scientific Research Fundation of Tongling University under grant No. 2015tlxyrc01 and the 2014-year Program for Excellent Youth Talents in University of Anhui Province.

Abbreviations
QKD, Quantum Key Distribution; QSDC, Quantum Secure Direct Communication; QSS, Quantum Secret Sharing; KTYC, S-Y Kuo K-C Tseng C-C Yang and Y-H Chou.

Data availability
No datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare no competing interests.

Author contributions

Gan Gao is the sole author of this manuscript.

Author details
[1]Department of Electrical Engineering, Tongling University, Tongling 244061, China. [2]AnHui Engineering Research Center of Intelligent Manufacturing of Copper-Based Materials, Tongling University, Tongling 244061, China. [3]Anhui Joint Key Laboratory of Critical Technologies for High-End Copper-Based New Materials, Tongling University, Tongling 244061, China.

Received: 10 December 2023 Accepted: 14 March 2024 Published online: 25 March 2024

References

1. Kuo SY, Tseng KC, Yang CC, Chou YH. Efficient multiparty quantum secret sharing based on a novel structure and single qubits. EPJ Quantum Technol. 2023;10:29.
2. Hillery M, Buzk V, Berthiaume A. Quantum secret sharing. Phys Rev A. 1999;59:1829.
3. Shamir A. Commun ACM. 1979;22:612.
4. Blakley GR. International workshop on managing requirements knowledge, 04-07 June 1979, New York, NY, USA. 1979. p. 313.
5. Bagherinezhad S, Karimipour V. Quantum secret sharing based on reusable Greenberger-Horne-Zeilinger states as secure carriers. Phys Rev A. 2003;67:044302.
6. Zhang ZJ et al. Multiparty quantum secret sharing. Phys Rev A. 2005;71:044301.
7. Li CM et al. Comment on "Quantum secret sharing between multiparty and multiparty without entanglement". Phys Rev A. 2006;73:016301.
8. Wang HF et al. Improving the security of multiparty quantum secret splitting and quantum state sharing. Phys Lett A. 2006;358:11.
9. Deng FG et al. Circular quantum secret sharing. J Phys A, Math Gen. 2006;39:14089.
10. Xue ZY, Yi YM, Cao ZL. Scheme for sharing classical information via tripartite entangled states. Chin Phys B. 2006;15:01421.
11. Guo Y, Zeng GH, Chen ZG. Multiparty quantum secret sharing of quantum states using entanglement states. Chin Phys Lett. 2007;24:863.
12. Markham D, Sanders BC. Graph states for quantum secret sharing. Phys Rev A. 2008;78:042309.
13. Wang C, Zhang Y. Quantum secret sharing protocol using modulated doubly entangled photons. Chin Phys B. 2009;18:3238.
14. Gu B, Li CQ, Xu F, Chen YL. High-capacity three-party quantum secret sharing with superdense coding. Chin Phys B. 2009;18:4690.
15. Gao G. Reexamining the security of the improved quantum secret sharing scheme. Opt Commun. 2009;282:4464.
16. Gao G. Multiparty quantum secret sharing using two-photon three-dimensional Bell states. Commun Theor Phys. 2009;52:421.
17. Zhu ZC, Zhang YQ. Cryptanalysis and improvement of a quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations. Chin Phys Lett. 2010;27:060303.
18. Gao G. Cryptanalysis of multiparty quantum secret sharing with collective eavesdropping-check. Opt Commun. 2010;283:2997.
19. Hwang T, Hwang CC, Li CM. Multiparty quantum secret sharing based on GHZ states. Phys Scr. 2011;83:045004.
20. Gao G, Fang M, Cheng MT. Cryptanalysis and improvement of a quantum network system of QSS-QDC using χ-type entangled states. Chin Phys Lett. 2012;29:110305.
21. Tseng CW et al. Quantum secret sharing based on quantum search algorithm. Int J Theor Phys. 2012;51:3101–8.
22. Tsai CW et al. Multi-party quantum secret sharing based on two special entangled states. Sci China, Phys Mech Astron. 2012;55:460–4.
23. Zhu ZC, Hu AQ, Fu AM. Cryptanalysis of a new circular quantum secret sharing protocol for remote agents. Quantum Inf Process. 2013;12:1173–83.
24. Lin J et al. New circular quantum secret sharing for remote agents. Quantum Inf Process. 2013;12:685–97.
25. Gao G. Secure multiparty quantum secret sharing with the collective eavesdropping-check character. Quantum Inf Process. 2013;12:55.
26. Chen XB, Niu XX, Zhou XJ, Yang YX. Multi-party quantum secret sharing with the single-particle quantum state to encode the information. Quantum Inf Process. 2013;12:365.
27. Gao G. Improvement of efficient multiparty quantum secret sharing based on Bell states and continuous variable operations. Int J Theor Phys. 2014;53:2231.
28. Song XL et al. (t,n) threshold d-level quantum secret sharing. Sci Rep. 2017;7:6366.
29. Gao G, Wang Y, Wang D. Multiparty semiquantum secret sharing based on rearranging orders of qubits. Mod Phys Lett B. 2016;30:1650130.
30. Gao G, Wang Y. Comment on "Proactive quantum secret sharing". Quantum Inf Process. 2017;16:74.

31. Liao Q, Liu H, Zhu L, Guo Y. Phys Rev A. 2021;103:032410.
32. Ju XX, Zhong W, Sheng YB, Zhou L. Measurement-device-independent quantum secret sharing with hyper-encoding. Chin Phys B. 2022;31:100302.
33. Jia H-Y, Wen Q-Y, Gao F, Qin S-J, Guo F-Z. Dynamic quantum secret sharing. Phys Lett A. 2012;376(10–11):1035–41.
34. Hsu JL, Chong SK, Hwang T, Tsai CW. Dynamic quantum secret sharing. Quantum Inf Process. 2013;12(1):331–44.
35. Liao C-H, Yang C-W, Hwang T. Comment on "Dynamic quantum secret sharing". Quantum Inf Process. 2013;12(10):3143–7.
36. Wang T-Y, Li Y-P. Cryptanalysis of dynamic quantum secret sharing. Quantum Inf Process. 2013;12(5):1991–7.
37. Liao C-H, Yang C-W, Hwang T. Dynamic quantum secret sharing protocol based on GHZ state. Quantum Inf Process. 2014;13(8):1907–16.
38. Mishra S, Shukla C, Pathak A, Srikanth R, Venugopalan A. An integrated hierarchical dynamic quantum secret sharing protocol. Int J Theor Phys. 2015;54(9):3143–54.
39. Liu H, Ma H, Wei K, Yang X, Qu W, Dou T, Chen Y, Li R, Zhu W. Multi-group dynamic quantum secret sharing with single photons. Phys Lett A. 2016;380(31):2349–53.
40. Qin H, Dai Y. Dynamic quantum secret sharing by using d-dimensional GHZ state. Quantum Inf Process. 2017;16(3):64.
41. Du Y-T, Bao W-S. Dynamic quantum secret sharing protocol based on two-particle transform of Bell states. Chin Phys B. 2018;27(8):080304.
42. Song Y, Li Z, Li Y. A dynamic multiparty quantum direct secret sharing based on generalized GHZ states. Quantum Inf Process. 2018;17(9):244.
43. Gao G, Wei C-C, Wang D. Cryptanalysis and improvement of dynamic quantum secret sharing protocol based on two-particle transform of Bell states. Quantum Inf Process. 2019;18(6):186.
44. Yang C-W, Tsai C-W. Improved dynamic multiparty quantum direct secret sharing protocol based on generalized GHZ states to prevent collusion attack. Mod Phys Lett A. 2020;35(8):2050040.
45. Yang C-W, Tsai C-W. Participant attack and improving dynamic quantum secret sharing using d-dimensional GHZ state. Mod Phys Lett A. 2020;35(6):2050024.
46. Yang C-W, Tsai C-W. Efficient and secure dynamic quantum secret sharing protocol based on bell states. Quantum Inf Process. 2020;19(5):162.
47. Hu W, Zhou R-G, Li X, Fan P, Tan C. A novel dynamic quantum secret sharing in high-dimensional quantum system. Quantum Inf Process. 2021;20(5):159.
48. Wang J, Zhang S, Zhang Q, Tang C-J. Semiquantum secret sharing using two-particle entangled state. Int J Quantum Inf. 2012;10(5):1250050.
49. Li LZ, Qiu DW, Mateus P. Quantum secret sharing with classical Bobs. J Phys A, Math Theor. 2013;46(4):045304.
50. Lin J, Yang C-W, Tsai C-W, Hwang T. Intercept-resend attacks on semiquantum secret sharing and the improvements. Int J Theor Phys. 2013;52(1):156–62.
51. Yang C-W, Hwang T. Efficient key construction on semi-quantum secret sharing protocols. Int J Quantum Inf. 2013;11(05):1350052.
52. Xie C, Li L, Qiu D. A novel semi-quantum secret sharing scheme of specific bits. Int J Theor Phys. 2015;54(10):3819–24.
53. Yin A, Fu F. Eavesdropping on semi-quantum secret sharing scheme of specific bits. Int J Theor Phys. 2016;55(9):4027–35.
54. Gao X, Zhang S, Chang Y. Cryptanalysis and improvement of the semi-quantum secret sharing protocol. Int J Theor Phys. 2017;56(8):2512–20.
55. Yu K-F, Gu J, Hwang T, Gope P. Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing. Quantum Inf Process. 2017;16(8):194.
56. Chen B, Yang W, Huang L. Cryptanalysis and improvement of the novel semi-quantum secret sharing scheme based on Bell states. Mod Phys Lett B. 2018;32(25):1850294.
57. Gao G, Wang Y, Wang D. Cryptanalysis of a semi-quantum secret sharing scheme based on Bell states. Mod Phys Lett B. 2018;32(09):1850117.
58. Li Z, Li Q, Liu C, Peng Y, Chan WH, Li L. Limited resource semiquantum secret sharing. Quantum Inf Process. 2018;17(10):285.
59. Yin AH, Tong Y. A novel semi-quantum secret sharing scheme using entangled states. Mod Phys Lett B. 2018;32(22):1850256.
60. He Q, Yang W, Chen B, Huang L. Cryptanalysis and improvement of the novel semi-quantum secret sharing scheme using entangled states. Mod Phys Lett B. 2019;32(25):1950045.
61. Tsai C-W, Yang C-W, Lee N-Y. Semi-quantum secret sharing protocol using W-state. Mod Phys Lett A. 2019;34(27):1950213.
62. Xiang Y, Liu J, Bai M-Q, Yang X, Mo Z-W. Limited resource semi-quantum secret sharing based on multi-level systems. Int J Theor Phys. 2019;58:2883–92.
63. Tsai C-W, Chang Y-C, Lai Y-H, Yang C-W. Cryptanalysis of limited resource semi-quantum secret sharing. Quantum Inf Process. 2020;19(8):224.
64. Li C, Ye C, Tian Y, Chen X-B, Li J. Cluster-state-based quantum secret sharing for users with different abilities. Quantum Inf Process. 2021;20(12):385.
65. Tian Y, Li J, Chen X-B, Ye C-Q, Li H-J. An efficient semi-quantum secret sharing protocol of specific bits. Quantum Inf Process. 2021;20(6):217.
66. Bennett CH, Brassard G. Proceedings of the IEEE international conference on computers, systems and signal processings. Bangalore, India. New York: IEEE; 1984. p. 175–9.

Publisher's Note