Revisiting the "improving the security of multi-party quantum key agreement with five- qubit Brown states"

Yu-Yuan Chou[1], Hsien-Hung Liu, [2], Jue-Sam Chou [3*]

[1] Department of Physics, National Central University, Taiwan
warrior1819150@gmail.com
[2]Graduate Institute of Religious Studies College of Nanhua University, Taiwan
10769553@nhu.edu.tw
[3]Department of Information Management, Nanhua University, Taiwan *: corresponding author: jschou@nhu.edu.tw Tel: 886+ (05)+272-1001 ext.56536

Abstract

In 2018 Cai et al. proposed a multi-party quantum key agreement with five-qubit Brown states. They confirmed the security of their proposed scheme. However, Elhadad, Ahmed, et al. found the scheme cannot resist the collusion attack launched by legal participants. They suggested a modification and declared that their improved version is capable of resisting this type of attack. Nevertheless, after analysis, we found that the collusion attack still exists. Subsequently, we proposed a straightforward modification to prevent the attack. After analysis, we conclude that our modification meets the required security and collusion attack prevention, which are very important in the quantum key agreement scheme.

Keywords: quantum key agreement,five-qubit Brown state, collusion attack, one-way hash function, quantum channel

1. Introduction

Due to the physics phenomenon of quantum mechanics, quantum cryptography security has been proven to be secure by [19]. It can provide absolute security. For coping with the information security issue in the upcoming quantum world, quantum key agreement is therefore doomed to be a fundamental tool in the information security applied to the near future quantum communication network. Quantum key agreement allows two or more parties negotiate a session key with equal influence on the key instead of some subset of them can determine it themselves. Several quantum key agreement related articles have been proposed. There are two categories of algorithms, namely the quantum key agreement protocols [5-16], and the measurement-device-independent quantum key agreement protocols for two-party and three-party, respectively in [17, 18]. Type (2) is based on the observation that type (1) suffers from practical implementation issues. It is prone to quantum attacks in the detection part. However, the authors of the two type (2) protocols could not extend it to the multi-party case. The multi-party case is more suitable for real-life applications [4]. Therefore, there are many researchers working in this area. They proposed the multi-party quantum key agreement protocols [4, 19-26].

In 2005, Brown et al. presented a procedure to search for highly entangled states and found a new type of entangled state named as brown state which has stronger

entanglement than the four-qubit and five-qubit GHZ states [1]. In 2020, Elhadad, Ahmed, et al. [3] proposed a "Improving the security of multi-party quantum key agreement with five-qubit Brown states" to resolve the collusion attack found in Cai et al.s' "a multi-party quantum key agreement with five-qubit brown states". They claimed that their scheme can solve the conspiracy problem of [1]. However, upon closer examination, we discovered that it does not meet the security requirement for preventing this type of attack. We will display it in the article. In order to enhance its security, we will modify their scheme to incorporate this feature. Additionally, we conduct cryptoanalysis to ensure the security of our enhancement.

The arrangement of the article is as follows. In Section 2, we briefly introduce Ahmed, et al. S' modification. In Section 3, we analyze its weaknesses. The modifications and the security issues are demonstrated and discussed in Section 4 and 5, respectively. Finally, a conclusion is given in Section 6.

2. **Review of Ahmed, et al.s' modification**

In 2018 Cai et al. Proposed a multi-party quantum key agreement with five-qubit brown states. They validated the security of their proposed scheme. However, Elhadad, Ahmed, et al. found that the scheme cannot resist the collusion attack launched by legal participants. They therefore proposed a modification and declared that their improved version can resist this type of attack. Cai et al.s' scheme can be referred to [1]. Here, we just review Ahmed, et al.s' modification [2]. Other than the participants in Cai et al.s'scheme, Ahmed, et al.s' modification also consists of a semi-trusted third party (TP) distributing random keys K_1, K_2,…, K_M to participants P_1, P_2, …,P_M, respectivly. K_1, K_2,…, K_M , each having bit length n, are the corresponding private keys of P_1, P_2, …, P_M. Additionally, TP creates keys $\overline{K1}, \overline{K2}, \ldots, \overline{KM}$, every one of which has bit length n, and computes $\overline{K} = \overline{K1} \oplus \overline{K2} \oplus \ldots \oplus \overline{KM}$. He sends $\overline{Ki}$, i=1 to M, to participant Pi , and $\overline{K}$ to all participants. Then, P_i calculates $Tki=\overline{Ki} \oplus K_i$**.** Finally, P_i can obtain the final common key K by computing $K=(\overline{K} \oplus \mathbf{K_{pi}} \oplus Tk_i) = K_i \oplus K_{pi} = K_1 \oplus K_2 \oplus \ldots \oplus K_M$. We roughly delineate their modifications as follows. The detailed information can be referered to [3], the original article.

Their modified steps are described as follows:

(1)Preparation.

P_i generates L Brown states $|B_0\rangle_{12345}$, where $L =$ $(n/5)$, and $i = 1, 2, \ldots, M$. P_i then denotes the L Brown states with the following notation: $\{(b_1^1, b_1^2, \ldots, b_1^l), (b_2^1, b_2^2, \ldots, b_2^l), \ldots, (b_l^1, b_l^2, \ldots, b_l^l)\}$. The subscripts denote the order of the Brown states and the superscripts represent five qubits for each Brown state. Subsequently, P_i forms five subsequences by selecting the 1st, 2nd, 3rd, 4th and 5th photons from each Brown state, ($s_{i,i\oplus1}^1=\{b_1^1, b_2^1, \ldots, b_l^1\}$,$s_i^2=\{b_1^2, b_2^2, \ldots, b_l^2\}$,$s_{i,i\oplus1}^3=\{b_1^3, b_2^3, \ldots, b_l^3\}$,$s_i^4=\{b_1^4, b_2^4, \ldots, b_l^4\}$, ,$s_{i,i\oplus1}^5=\{b_1^5, b_2^5, \ldots, b_l^5\}$). Then, P_i prepares enough decoy qubits, which are randomly chosen from four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and randomly inserts them into three sequences $s_{i,i\oplus1}^1$, $s_{i,i\oplus1}^3$, $s_{i,i\oplus1}^5$ to obtain three new sequences $s_{i,i\oplus1}^{1*}$, $s_{i,i\oplus1}^{3*}$, $s_{i,i\oplus1}^{5*}$. P_i sends $s_{i,i\oplus1}^{1*}$, $s_{i,i\oplus1}^{3*}$, $s_{i,i\oplus1}^{5*}$ to his next participant $P_{i\oplus1}$ over the quantum channel.

(2)Encoding.

Upon confirming that the communication channel is secure, $P_{i\oplus1}$ discards the decoy particles from $s^{1*}_{i,i\oplus1}$, $s^{3*}_{i,i\oplus1}$, $s^{5*}_{i,i\oplus1}$ to obtain the original sequences $s^{1}_{i,i\oplus1}$, $s^{3}_{i,i\oplus1}$, $s^{5}_{i,i\oplus1}$, respectively. According to $P_{i\oplus1}$'s secret, he performs the encoding operation by performing unitary operations u^1_j, u^3_j , u^5_j (j $\in$ {1, 2, ... , n/5}) onto qubits b^1_j, b^3_j , b^5_j in the sequences $s^{1}_{i,i\oplus1}$, $s^{3}_{i,i\oplus1}$, $s^{5}_{i,i\oplus1}$, respectively.

Then, he uses the decoy method described in step (2) to generate new sequences $s^{1*}_{i,i\oplus2}$, $s^{3*}_{i,i\oplus2}$, $s^{5*}_{i,i\oplus2}$ and sends the evolved sequences to his next party $P_{i\oplus2}$.

(3)Security confirmation and encoding of secret by $P_{i\oplus2}$, $P_{i\oplus3}$, ⋯ , $P_{i\oplus(i-1)}$, sequentially.

As described in step (2), participants $P_{i\oplus2}$, $P_{i\oplus3}$, ⋯ , $P_{i\oplus(i-1)}$ confirm the security of the quantum channel and encode messages sequentially. If all the sequences are secure, they encode their secret on the corresponding qubits of each sequence and insert decoy qubits randomly, sending them to the next participant. Otherwise, they reject.

(4)Generation.

After receiving the final qubit sequences $s^{1*}_{i,i\oplus2}$, $s^{3*}_{i,i\oplus2}$, $s^{5*}_{i,i\oplus2}$, Pi performs security check with Pi−1. If it is safe, Pi performs unitary operations and performs single qubit measurements on five distinct qubits $\{(b^1_1, b^2_1, ..., b^l_1)$, $(b^1_2, b^2_2, ..., b^l_2)$, ..., $(b^1_l, b^2_l, ..., b^l_l)\}$. In reality, they are located in the corresponding positions of $s^1_{i,i}$, s^2_i, $s^3_{i,i}$, s^4_i $s^5_{i,i}$. Therefore, according to the relationship described in Table 2 of [3], Pi obtains the final measurement results (SPi) for the brown states that have been received. Combining with the encoding rule in Table 1 of [3] and the final result SPi, he will obtain the corresponding joint key KPi from other participants Pi⊕1,Pi⊕2, ... , Pi⊕(i−1). Finally, all the Pis know the final agreement common key by computing K= KPi ⊕ Ki .

(5)Collusion attack detection.

To avoid someone from destroying this protocol, all participants select a percentage of keys from his key sequence randomly in the same position as the test keys and publish the test keys at the same time. If the test keys are not the same, it indicates that there are some dishonest participants. We terminate this quantum key agreement. Otherwise, it succeeds in generating a session key by all participants with the left key sequence.

3. **Weakness of the scheme**

From the equation K=($\overline{K} \oplus \mathbf{K_{pi}} \oplus Tk_i$) = $K_i \oplus K_{pi}$= $K_1 \oplus K_2 \oplus \ldots \oplus K_M$ in Section 2, we can see that if any M-1 participants collude, they can know the remainder participant's

private key. Without loss of generality, we assume that the first M-1 partner collaborated. Then, they can deduce the private key of P_M by computing $K_M = K \oplus K_1 \oplus K_2 \oplus \ldots \oplus K_{M-1}$. As a result,, althoug Ahmed, et al.s' modification has strengthen Cai et al.s' scheme, they also suffers from the collusive attack.

4. Modification

Due to the conspiracy attack that Ahmed et al.'s modification suffered, we propose a simple improvement that adopts a one-way hash function as follows.

Since TP and all partners had pre-shared a key $\overline{K}$, we can use the cryptographic one-way hash function $H(.)$ to make their scheme better. For example, TP calculates $\overline{K}=\overline{K1} \oplus \overline{K2} \oplus \ldots \oplus \overline{KM} \oplus H(K_1 \oplus K_2 \oplus \ldots \oplus K_M)$ and sends it to all the participants, rather than the original content $\overline{K}=\overline{K1} \oplus \overline{K2} \oplus \ldots \oplus \overline{KM}$. That is, each partner calculates $K=(\overline{K} \oplus \mathbf{K_{pi}} \oplus Tk_i) = K_i \oplus H(K_1 \oplus K_2 \oplus \ldots \oplus K_M) \oplus K_{pi} = K_1 \oplus K_2 \oplus \ldots \oplus K_M \oplus H(K_1 \oplus K_2 \oplus \ldots \oplus K_M)$. If one is concerned about its computational security in the upcoming quantum era, one can adopt an unconditional hash function [2].

5. Security analysis

After the above modification, we can see that if any M-1 participants collude, they cannot know the remainder participant's private key due to the one-way hash function property. For clarity, without loss of generality, we assume that the first M-1 partner colludes. Although, the colluders know the value of $K_1 \oplus K_2 \oplus \ldots \oplus K_{M-1}$. Without the knowledge of K_M, they cannot compute $H(K_1 \oplus K_2 \oplus \ldots \oplus K_M)$ to deduce the private key of P_M by computing $K_M = K \oplus K_1 \oplus K_2 \oplus \ldots \oplus K_{M-1} \oplus H(K_1 \oplus K_2 \oplus \ldots \oplus K_M)$. Even if concerned about the computational security of the hash function in the upcoming quantum era, we can use the unconditional secure hash, as mentioned in the context of [2]. Therefore, we have successfully strengthened Ahmed, et al.s' excellent modification. The collusion attack on the modification has been thrown away.

6. Conclusion

In this paper, we demonstrated that Ahmed et al.'s modification of Cai et al.'s "multi-party quantum key agreement with five-qubit Brown states" has vulnerabilities. It is also susceptible to collusion attacks. To address this issue, we modified the original approach to eliminate this weakness. As shown in the analyses in Section 5, we have enhanced its security.

References

[1] Cai, Tao, Min Jiang, and Gang Cao. "Multi-party quantum key agreement with five-qubit brown states." Quantum Information Processing 17 (2018): 1-18.

[2] Zeng, Guihua. Quantum private communication. Springer Publishing Company, Incorporated, 2010.

[3] Elhadad, Ahmed, et al. "Improving the security of multi-party quantum key agreement with five-qubit Brown states." Computer Communications 159 (2020): 155-160.

[4] Abulkasim, Hussein, Eatedal Alabdulkreem, and Safwat Hamad. "Improved multi-party quantum key agreement with four-qubit cluster states." CMC-Computers Materials & Continua 73 (2022): 225-232.

[5] Chong, Song-Kong, and Tzonelih Hwang. "Quantum key agreement protocol based on BB84." Optics Communications 283.6 (2010): 1192-1195.

[6] Liu, Bin, et al. "Multiparty quantum key agreement with single particles." Quantum information processing 12 (2013): 1797-1805.

[7] Huang, Wei, et al. "Quantum key agreement with EPR pairs and single-particle measurements." Quantum information processing 13 (2014): 649-663.

[8] Xu, Guang-Bao, et al. "Novel multiparty quantum key agreement protocol with GHZ states." Quantum information processing 13 (2014): 2587-2594.

[9] He, Ye-Feng, and Wen-Ping Ma. "Quantum key agreement protocols with four-qubit cluster states." Quantum Information Processing 14 (2015): 3483-3498.

[10] Sun, Zhiwei, Jiwu Huang, and Ping Wang. "Efficient multiparty quantum key agreement protocol based on commutative encryption." Quantum Information Processing 15 (2016): 2101-2111.

[11] Mohajer, Razieh, and Ziba Eslami. "Cryptanalysis of a multiparty quantum key agreement protocol based on commutative encryption." Quantum Information Processing 16 (2017): 1-9.

[12] Yang, Yu-Guang, et al. "New quantum key agreement protocols based on cluster states." Quantum Information Processing 18 (2019): 1-17.

[13] Zhou, Nan-Run, Kong-Ni Zhu, and Yun-Qian Wang. "Three-party semi-quantum key agreement protocol." International Journal of Theoretical Physics 59 (2020): 663-676.

[14] Li, Lei, and Zhi Li. "A verifiable multiparty quantum key agreement based on bivariate polynomial." Information Sciences 521 (2020): 343-349.

[15] Lin, Song, et al. "Multiparty quantum key agreement." Physical Review A 104.4 (2021): 042421.

[16] Zhou, Nanrun, Guihua Zeng, and Jin Xiong. "Quantum key agreement protocol." Electronics Letters 40.18 (2004): 1.

[17] Yang, Yu-Guang, et al. "Detector-device-independent quantum key agreement based on single-photon bell state measurement." International Journal of Theoretical Physics 61.2 (2022): 50.

[18] Cai, Xiao-Qiu, et al. "Long distance measurement-device-independent three-party quantum key agreement." Physica A: Statistical Mechanics and its Applications 607 (2022): 128226.

[19] Zhu, Hongfeng, et al. "Multi-party quantum key agreement protocol for smart home environment." *International Journal of Theoretical Physics* 60 (2021): 3948-3960.

[20] Tang, Jie, et al. "Novel multi-party quantum key agreement protocols under collective noise." *Modern Physics Letters B* 35.08 (2021): 2150137.

[21] Li, Lei, and Zhi Li. "A verifiable multi-party quantum key distribution protocol based on repetitive codes." *Information Sciences* 585 (2022): 232-245.

[22] Ma, Xiyuan, et al. "Multi-party quantum key distribution protocol with new bell states encoding mode." *International Journal of Theoretical Physics* 60 (2021): 1328-1338.

[23] Zhao, Wei, et al. "Conference key agreement based on continuous-variable quantum key distribution." *Laser Physics Letters* 18.7 (2021): 075205.

[24] Liu, Li-Juan, and Zhi-Hui Li. "A verifiable quantum key agreement protocol based on six-

qubit cluster states." *The European Physical Journal D* 75.7 (2021): 193.
[25] Kim, Jeong San. "Entanglement of formation and monogamy of multi-party quantum entanglement." *Scientific Reports* 11.1 (2021): 2364.
[26] Cai, Zhengying, et al. "A quantum blind multi-signature method for the industrial blockchain." *Entropy* 23.11 (2021): 1520.