International Journal of Theoretical Physics (2022) 61: 103
https://doi.org/10.1007/s10773-022-05101-1

# Cryptanalysis and Improvement of Three-Party Semi-Quantum Summation Using Single Photons

Hong-Ming Pan [1]

Received: 31 January 2022 / Accepted: 4 April 2022 / Published online: 11 April 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

**Abstract**
Recently, Zhang et al. suggested the first semi-quantum summation protocol by using single photons (Int. J. Theor. Phys. **60**, 3478–3487, 2021). This paper firstly shows that by launching a special participant attack, the third party (TP) can obtain three users' measurement results on the particle groups except for checking the existence of Eve and the honesty of TP without being detected; as a result, the protocol fails to compute the summation, or even worse, TP may obtain three users' private bit strings. Afterward, this paper puts forward an improvement to solve these problems.

**Keywords** Semi-quantum summation · Single photon · Participant attack · Third party

## 1 Introduction

Recent years, more and more attentions have been thrown onto the research of quantum computation, because quantum parallel computation has shown its great potential in accelerating the computing speed. As a famous branch of quantum computation, quantum summation has also aroused more and more interests of scholars. The existing quantum summation schemes [1–9] always ask all participants to be equipped with complete quantum capabilities. However, this requirement may be too strict in some situations. Fortunately, Boyer et al. [10, 11] put forward a brand-new branch for quantum cryptography, i.e., semi-quantum cryptography, which permits a portion of participants not to have complete quantum capabilities. In the year of 2021, Zhang et al. [12] introduced the concept of semi-quantum cryptography and put forward the first semi-quantum summation scheme; and in the year of 2022, Ye et al. [13] proposed a two-party secure semi-quantum summation scheme against the collective-dephasing noise. After putting a deep insight into Zhang et al.'s semi-quantum summation scheme, this paper discovers some severe problems in it. Specifically speaking, by launching a

✉ Hong-Ming Pan
hmpan@zjgsu.edu.cn

[1] Zhejiang Gongshang University Hangzhou College of Commerce, Hangzhou 311508, People's Republic of China

special participant attack, the third party (TP) can obtain three users' measurement results on the particle groups except for checking the existence of Eve and the honesty of TP without being detected; as a result, the protocol fails to compute the summation, or even worse, TP may obtain three users' private bit strings. Hence, this paper suggests an improvement to this scheme to make it work normally.

## 2 Review of Zhang et al.'s Three-Party Semi-Quantum Summation Protocol

In Zhang et al.'s three-party semi-quantum summation protocol [12], there are four parties, including three users $P_1$, $P_2$, $P_3$ and TP. Here, TP is permitted to perform a variety of attacks except colluding with three users; $P_j$ owns a private bit string $M_j = (m_{j1}, m_{j2}, \cdots, m_{jn})$, where $j = 1, 2, 3$. TP helps calculate the addition modulo 2 of $M_1$, $M_2$, $M_3$, i.e., $M_1 \oplus M_2 \oplus M_3$, through the noiseless quantum channels and authenticated classical channels.

Zhang et al.'s three-party semi-quantum summation protocol [12] is reviewed as follows:

Step 1: TP produces $3nq = 3n(32 + r + d + \delta)|+\rangle$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Afterward, TP divides them into three particle sequences: $S_1 = \{p_1^1, p_1^2, \cdots, p_1^{nq}\}$, $S_2 = \{p_2^1, p_2^2, \cdots, p_2^{nq}\}$ and $S_3 = \{p_3^1, p_3^2, \cdots, p_3^{nq}\}$. Finally, TP sends the particles in $S_j$ one by one to $P_j$, where $j = 1, 2, 3$.

Step 2: On receiving a particle from TP, $P_j$chooses randomly the CTRL operation or the SIFT operation. The CTRL operation means to return a particle to TP without disturbance, while the SIFT operation means to measure a particle with the $Z$ basis (i.e., $\{|0\rangle, |1\rangle\}$) and resend it back to TP. After $P_j$ finishes her operations, $S_j$ is changed into $S_j^{'} = \left\{p_j^{'1}, p_j^{'2}, \cdots, p_j^{'nq}\right\}$. Here, $j = 1, 2, 3$.

Step 3: TP makes $S_1^{'}, S_2^{'}, S_3^{'}$ form a new sequence $S = \left\{\left(p_1^{'1}, p_2^{'1}, p_3^{'1}\right), \left(p_1^{'2}, p_2^{'2}, p_3^{'2}\right), \cdots, \left(p_1^{'nq}, p_2^{'nq}, p_3^{'nq}\right)\right\}$, where $\left(p_1^{'i}, p_2^{'i}, p_3^{'i}\right)$ is the $i$th particle group, and $i = 1, 2, \cdots, nq$. For checking the existence of Eve, TP randomly picks out $nr$ groups from these $nq$ particle groups and publishes the positions of these chosen groups to three users. Then, $P_j$ announces his operations for these chosen groups and his corresponding measurement results obtained from the SIFT operations. In case $P_j$ chose the CTRL operations, TP measures the received particles with the $X$ basis (i.e., $\{|+\rangle, |-\rangle\}$); errors will be detected if TP' measurement results are $|-\rangle$, where $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. In case $P_j$ chose the SIFT operations, TP measures the received particles with the Z basis; errors will be detected if TP's measurement results are different from $P_j$'s measurement results. If no error is detected in the end, the communication will be carried on.

Step 4: Three users require TP to use the GHZ-type basis to measure the rest $n(32 + d + \delta)$ particle groups. If TP's measurement result is $|\varphi_{000}\rangle$ or $|\varphi_{001}\rangle$, she will announce it to three users directly; if TP's measurement result is $|\varphi_{110}\rangle$ or $|\varphi_{111}\rangle$, she will announce 'summation' to three users. Then, three users randomly pick out $nd$ groups from the

rest $n(32 + d + \delta)$ particle groups to check the honesty of TP as follows: as for the positions where all of them performed the CTRL operations, if TP announces 'summation', then TP's cheating behavior will be detected. If TP is found to be honesty in the end, the communication will be carried on. Here, $|\varphi_{000}\rangle = \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$, $|\varphi_{001}\rangle = \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)$, $|\varphi_{110}\rangle = \frac{1}{2}(|000\rangle + |011\rangle - |101\rangle - |110\rangle)$ and $|\varphi_{111}\rangle = \frac{1}{2}(|001\rangle + |010\rangle - |100\rangle - |111\rangle)$.

Step 5: For the rest $n(32 + \delta)$ particle groups, each user announces the positions where he selected the SIFT operations; there are $n + \frac{n\delta}{32}$ positions where three users all selected the SIFT operations and TP announced 'summation'. The first $n$ positions are selected to generate private keys for three users as follows: if the measurement result of $P_j$ ($j = 1, 2, 3$) is $|0\rangle$, the corresponding key bit of $K_j$ is 0; otherwise, the corresponding key bit of $K_j$ is 1. Three users tell TP the information of these $n$ positions. Then, $P_j$ computes $C_j = M_j \oplus K_j$ and sends it to TP. In the same time, TP generates a private bit string $T$ from her corresponding measurement results: if her corresponding measurement result is $|\varphi_{110}\rangle$, the corresponding private bit of $T$ will be 0; if her corresponding measurement result is $|\varphi_{111}\rangle$, he corresponding private bit of $T$ will be 1. Finally, TP computes $C_1 \oplus C_2 \oplus C_3 \oplus T$ and publishes the summation result to three users.

## 3 TP's Participant Attack on Zhang et al.'s Three-Party Semi-Quantum Summation Protocol

In this section, it will be demonstrated that by launching a special attack, TP can obtain the measurement results of three users on the rest $n(32 + \delta)$ particle groups without being discovered. In this way, she makes the protocol fail to compute the summation. Even worse, she may obtain three users' private bit strings.

TP's special attack is depicted as follows:

TP honestly implements Steps 1–3, but she does nothing when three users ask her to use the GHZ-type basis to measure the rest $n(32 + d + \delta)$ particle groups in Step 4. Instead, she always randomly announces $|\varphi_{000}\rangle$ or $|\varphi_{001}\rangle$ to three users. Apparently, after three users randomly pick out $nd$ groups from the rest $n(32 + d + \delta)$ particle groups and check the honesty of TP, TP can easily pass this check, because three users only check the positions of $nd$ groups where all of them chose the CTRL operations. Then, in Step 5, after each user announces the positions of the rest $n(32 + \delta)$ particle groups where he selected the SIFT operations, TP measures the corresponding received particles in her hand with the $Z$ basis. In this way, TP can obtain the measurement results of three users on these positions without being detected. Moreover, since three users receive no information about 'summation' from TP, they don't know how to implement the remaining procedure. In this way, if three users abandon the communication, the protocol will fail. Even worse, if $P_j (j = 1, 2, 3)$ still continues to tell TP the information of the $n$ positions for computing summation, compute $C_j = M_j \oplus K_j$ and send $C_j$ to TP, TP will easily decode out $M_j$ from $C_j$, as she has obtained $K_j$ from her $Z$ basis measurements and $P_j$'s information of the $n$ positions for computing summation.

## 4 An Improvement to Zhang et al.'s Three-Party Semi-Quantum Summation Protocol

An improvement to Zhang et al.'s three-party semi-quantum summation protocol is that changing its Step 4 into the following one:

> Step 4#: Three users require TP to use the GHZ-type basis to measure the rest $n(32 + d + \delta)$ particle groups. If TP's measurement result is $|\varphi_{000}\rangle$ or $|\varphi_{001}\rangle$, she will announce it to three users directly; if TP's measurement result is $|\varphi_{110}\rangle$ or $|\varphi_{111}\rangle$, she will announce 'summation' to three users. Then, three users randomly pick out $nd$ groups from the rest $n(32 + d + \delta)$ particle groups to check the honesty of TP as follows: as for the positions where all of them performed the CTRL operations, if TP announces 'summation', then TP's cheating behavior will be detected; as for the positions where all of them performed the SIFT operations, three users check whether the announcement of TP is correct or not. If TP is found to be honesty in the end, the communication will be carried on.

Now, we demonstrate the security of the above improvement against TP's attack illustrated in Section 3. After three users ask her to use the GHZ-type basis to measure the rest $n(32 + d + \delta)$ particle groups in Step 4, she does nothing but always randomly announces $|\varphi_{000}\rangle$ or $|\varphi_{001}\rangle$ to three users. Then, three users randomly pick out $nd$ groups from the rest $n(32 + d + \delta)$ particle groups to check the honesty of TP. As for the position where three users all performed the CTRL operations, TP introduces no error; as for the position where they all performed the SIFT operations, TP introduces an error with the probability of $\frac{1}{2}$, according to Eqs.(10–17) of Ref. [12]. For $nd$ groups used to check the honesty of TP, the probability that TP's attack can be detected is $1-\left(\frac{1}{2}\right)^{\frac{nd}{8}}$. If $nd$ is large enough, TP's attack will be detected absolutely. Consequently, in order not to be detected, TP has to honestly implement Step 4#. In Step 5, after each user announces the positions of the rest $n(32 + \delta)$ particle groups where he selected the SIFT operations, even though TP measures the corresponding particles in her hand with the $Z$ basis, she obtains nothing about the measurement results of three users on these positions, according to Eqs.(1–8) of Ref. [12]. After $P_j (j = 1, 2, 3)$ tells TP the information of the $n$ positions for computing summation, computes $C_j = M_j \oplus K_j$ and sends $C_j$ to TP, TP cannot decode out $M_j$ from $C_j$, as she has no knowledge about $K_j$.

It is necessary to emphasize that the above improvement doesn't alter the security against Eve, because it makes no change to Step 3.

## 5 Conclusion

To sum up, this paper firstly points out the severe problems existing in Zhang et al.'s three-party semi-quantum summation protocol [12]. Specifically speaking, by launching a special participant attack, TP can obtain the measurement results of three users on the particle groups except for checking the existence of Eve and the honesty of TP without being detected. In this way, the protocol fails to compute the summation, or even worse, TP may obtain three users' private bit strings. Afterward, this paper puts forward an improvement to remedy these drawbacks and validates the effectiveness of the improving method.

## Declarations

**Conflict of Interest** No conflict of interest exists.

## References


1. Chen, X.B., Xu, G., Yang, Y.X., Wen, Q.Y.: An efficient protocol for the secure multi-party quantum summation. Int. J. Theor. Phys. **49**(11), 2793–2804 (2010)
2. Zhang, C., Sun, Z.W., Huang, X.: Three-party quantum summation without a trusted third party. Int. J. Quantum Inf. **13**(2), 1550011 (2015)
3. Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep. **6**, 19655 (2016)
4. Yang, H.Y., Ye,T.Y.: Secure multi-party quantum summation based on quantum Fourier transform. Quantum Inf. Process. **17**(6), 129 (2018)
5. Ji, Z.X., Zhang, H.G., Wang, H.Z., Wu, F.S., Jia, J.W., Wu, W.Q.: Quantum protocols for secure multi-party summation. Quantum Inf. Process. **18**, 168 (2019)
6. Duan, M.Y.: Multi-party quantum summation within a d-level quantum system. Int. J. Theor. Phys. **59**(5), 1638–1643 (2020)
7. Ye, T.Y., Hu, J.L.: Quantum secure multiparty summation based on the phase shifting operation of d-level quantum system and its applicatiwon. Int. J. Theor. Phys. **60**(3), 819–827 (2021)
8. Yi, X., Cao, C., Fan, L., Zhang, R.: Quantum secure multi-party summation protocol based on blind matrix and quantum Fourier transform. Quantum Inf. Process. **20**, 249 (2021)
9. Wang, Y.L., Hu, P.C., Xu, Q.L.: Quantum secure multi-party summation based on entanglement swapping. Quantum Inf. Process. **20**, 319 (2021)
10. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical bob. Phys. Rev. Lett. **99**(14), 140501 (2007)
11. Boyer, M., Gelles, R., Kenigsberg, D., Mor, T.: Semiquantum key distribution. Phys. Rev. A **79**(3), 032341 (2009)
12. Zhang, C., Huang, Q., Long, Y.X., Sun, Z.W.: Secure three-party semi-quantum summation using single photons. Int. J. Theor. Phys. **60**, 3478–3487 (2021)
13. Ye, T.Y., Xu, T.J., Geng, M.J., Chen, Y.: Two-party secure semiquantum summation against the collective-dephasing noise. Quantum Inf. Process. **21**, 118 (2022)


**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.