International Journal of Theoretical Physics (2021) 60:3478–3487
https://doi.org/10.1007/s10773-021-04921-x

Secure Three-Party Semi-quantum Summation Using Single Photons

Cai Zhang[1] · Qiong Huang[1] · Yinxiang Long[2] · Zhiwei Sun[3]

Received: 18 December 2020 / Accepted: 29 July 2021 / Published online: 6 August 2021

Abstract
We first propose a three-party semi-quantum summation protocol with an almost-dishonest third party (TP) using single photons. TP who has full quantum power helps three classical users compute the summation of their private bit strings while the privacy of their inputs is preserved. For a particle from TP, three users' operations are limited either to (1) reflect the particle without disturbance back to TP or to (2) measure the particle in the Z basis and resend the measured particle back to TP. We also show that our protocol is secure against both outside and participant attacks.

Keywords Semi-quantum summation · Almost-dishonest third party · Single photons · Participant attacks

1 Introduction

Secure multi-party quantum summation [1–5] is one of the fundamental primitives of secure multi-party quantum computation [6–10]. It can be explained as follows: n users $P_1, P_2, \ldots, P_n$ intend to calculate a summation function $f(x_1, x_2, \ldots, x_n)$, where x_i $(i = 1, 2, \ldots, n)$ presents user P_i's private input. The image of f could be in public revealed or only available to some user. The goals of secure multi-party quantum summation are to ensure the correctness of summation result as well as to preserve the privacy of each user's

✉ Zhiwei Sun
smeker@szpt.edu.cn

[1] College of Mathematics and Informatics, South China Agricultural University, Guangzhou, 510642, China

[2] Department of Automation Engineering, Guangdong Technical College of Water Resources and Electric Engineering, Guangzhou, 510925, China

[3] School of Artificial Intelligence, Shenzhen PolyTechnic, Shenzhen, 518055, China

input. Quantum summation plays a role in the construction of complex multi-party computation and can be potentially applied to scenarios such as quantum private comparison [11–13] and quantum voting [14–18].

Recently, much research on quantum summation protocols has been conducted by using various quantum resources. Zhang et al. [19] employed single photons in both polarization and spatial-mode degrees of freedom to construct a quantum summation protocol, where unitary operations and particle replay are required. In 2015, Zhang et al. [20] presented a three-party quantum summation protocol without a trusted third party in which genuinely maximally entangled six-qubit states were employed. In 2016, Shi et al. [21] made use of quantum Fourier transform, controlled NOT gates and oracle operators to investigate protocols for both summation and multiplication problems. Later, they proposed a common quantum solution to the summation problem in a special two-party scenario [22]. In 2017, Zhang et al. [23] designed a multi-party quantum summation scheme based on multi-partite entangled states that are built on single particles. Liu et al. [24] investigated a quantum summation protocol where a multi-partite entangled state that has a form including Bell states are adopted to encode users' inputs. In 2018, Yang et al. [25] proposed a quantum solution to secure summation problem relying on n-partite d-dimensional entangled states. Ji et al. [26] presented a probabilistic summation protocol depending on the entanglement swapping between Bell states and cat states.

However, users in the previous quantum summation protocols [5, 19–25] are assumed to have full quantum power. That is to say, the users are allowed to operate various quantum devices, such as quantum memory [27], entangled state generator [28] and quantum unitary operators [29]. It is significant to reduce the need of quantum devices for users in quantum cryptographic protocols due to their high cost. Boyer et. al [30] proposed the first semi-quantum cryptographic protocol, semi-quantum key distribution protocol, in which a classical Bob is involved. Since then, a great number of semi-quantum cryptographic protocols for different issues were presented, including semi-quantum key distribution [31–35], semi-quantum secret sharing [36–39], semi-quantum private comparison [40–42] and semi-quantum communication [43] and so on. However, to our best knowledge, there is still no semi-quantum summation protocol. We are therefore taking the first step towards designing a multi-party semi-quantum summation protocol.

In this work, single photons are used to design a three-party semi-quantum protocol, where the measurement in a GHZ-type basis is utilized to detect the honesty of an almost-dishonest third party (TP) as well as to compute the summation of users' private inputs. We assume that TP is almost-dishonest, which means that he has the ability to start all sorts of attacks within quantum boundaries except collusion with other dishonest users. Three users are only allowed to perform one of two operations on a particle received from TP in the following way: (1) reflect the particle without disturbance back to TP, (2) measure the particle in the Z basis ($\{|0\rangle, |1\rangle\}$) and resend it back to TP. We show that the proposed protocol can resist attacks from both outsiders and dishonest participants.

The rest of this paper is organised as follows. In Section 2, we first introduce the properties of GHZ-type states, and then present the three-party semi-quantum summation protocol, followed by the analyses of the correctness and the security in Section 3. Conclusions are given in Section 4.

2 Three-Party Semi-quantum Summation Protocol

Before our protocol description, let us introduce the properties of GHZ-type states [44] and the notations used in this paper. The GHZ-type states can be written in different bases as follows:

$$\begin{aligned}
|\varphi_{000}\rangle &= \tfrac{1}{\sqrt{2}}(|+++\rangle + |---\rangle) = \tfrac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle), && (1)\\
|\varphi_{001}\rangle &= \tfrac{1}{\sqrt{2}}(|+++\rangle - |---\rangle) = \tfrac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle), && (2)\\
|\varphi_{010}\rangle &= \tfrac{1}{\sqrt{2}}(|--+\rangle + |++-\rangle) = \tfrac{1}{2}(|000\rangle - |011\rangle - |101\rangle + |110\rangle), && (3)\\
|\varphi_{011}\rangle &= \tfrac{1}{\sqrt{2}}(|--+\rangle - |++-\rangle) = \tfrac{1}{2}(|001\rangle - |010\rangle - |100\rangle + |111\rangle), && (4)\\
|\varphi_{100}\rangle &= \tfrac{1}{\sqrt{2}}(|+-+\rangle + |-+-\rangle) = \tfrac{1}{2}(|000\rangle - |011\rangle + |101\rangle - |110\rangle), && (5)\\
|\varphi_{101}\rangle &= \tfrac{1}{\sqrt{2}}(|+-+\rangle - |-+-\rangle) = \tfrac{1}{2}(|001\rangle - |010\rangle + |100\rangle - |111\rangle), && (6)\\
|\varphi_{110}\rangle &= \tfrac{1}{\sqrt{2}}(|-++\rangle + |+--\rangle) = \tfrac{1}{2}(|000\rangle + |011\rangle - |101\rangle - |110\rangle), && (7)\\
|\varphi_{111}\rangle &= \tfrac{1}{\sqrt{2}}(|-++\rangle - |+--\rangle) = \tfrac{1}{2}(|001\rangle + |010\rangle - |100\rangle - |111\rangle), && (8)
\end{aligned}$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ and the set of $\{|\varphi_x\rangle | x \in \{0,1\}^3\}$ forms an orthonormal basis (we call it the GHZ-type basis hereafter) for the space of a tripartite quantum system.

In accordance with (1) and (2), $|+++\rangle$ can be expressed as

$$|+++\rangle = \frac{1}{\sqrt{2}}(|\varphi_{000}\rangle + |\varphi_{001}\rangle), \tag{9}$$

which means that if $|+++\rangle$ is measured in the GHZ-type basis, it will collapse to either $|\varphi_{000}\rangle$ or $|\varphi_{001}\rangle$.

Using (1)–(8), each element in the computational basis for the space of a tripartite quantum system can be expanded in the GHZ-type basis in the forms of:

$$\begin{aligned}
|000\rangle &= \tfrac{1}{2}(|\varphi_{000}\rangle + |\varphi_{010}\rangle + |\varphi_{100}\rangle + |\varphi_{110}\rangle), && (10)\\
|001\rangle &= \tfrac{1}{2}(|\varphi_{001}\rangle + |\varphi_{011}\rangle + |\varphi_{101}\rangle + |\varphi_{111}\rangle), && (11)\\
|010\rangle &= \tfrac{1}{2}(|\varphi_{001}\rangle - |\varphi_{011}\rangle - |\varphi_{101}\rangle + |\varphi_{111}\rangle), && (12)\\
|011\rangle &= \tfrac{1}{2}(|\varphi_{000}\rangle - |\varphi_{010}\rangle - |\varphi_{100}\rangle + |\varphi_{110}\rangle), && (13)\\
|100\rangle &= \tfrac{1}{2}(|\varphi_{001}\rangle - |\varphi_{011}\rangle + |\varphi_{101}\rangle - |\varphi_{111}\rangle), && (14)\\
|101\rangle &= \tfrac{1}{2}(|\varphi_{000}\rangle - |\varphi_{010}\rangle + |\varphi_{100}\rangle - |\varphi_{110}\rangle), && (15)\\
|110\rangle &= \tfrac{1}{2}(|\varphi_{000}\rangle + |\varphi_{010}\rangle - |\varphi_{100}\rangle - |\varphi_{110}\rangle), && (16)\\
|111\rangle &= \tfrac{1}{2}(|\varphi_{001}\rangle + |\varphi_{011}\rangle - |\varphi_{101}\rangle - |\varphi_{111}\rangle). && (17)
\end{aligned}$$

The above properties of GHZ-type states will be used to detect TP's honesty and compute the summation.

Let us now advance to the description of our three-party semi-quantum summation protocol that satisfies the following requirements:

1. Correctness: The result of summation of three users' private bit strings is correct.
2. Security: An outside eavesdropper cannot learn any information about users' private inputs.

3. Privacy: TP and a dishonest participant cannot obtain other users' private inputs.

We assume that the quantum channels are ideal (i.e., non-lossy and noiseless) and that the classical channels are authenticated. In our protocol, there are three users (P_1, P_2 and P_3) and an almost-dishonest third party (TP). Each user has a private n-bit string. TP, who aims at evaluating the summation modulo 2 of three users' bit strings, is allowed to launch a variety of attacks without violation of quantum mechanics except collusion with other users. Dishonest users cannot collude with each other, either.

Suppose that P_j $(j = 1, 2, 3)$ has a private n-bit string M_j,

$$M_1 = (m_{11}, m_{12}, \dots, m_{1n}), \tag{18}$$

$$M_2 = (m_{21}, m_{22}, \dots, m_{2n}), \tag{19}$$

$$M_3 = (m_{31}, m_{32}, \dots, m_{3n}). \tag{20}$$

TP helps compute the summation $M_1 \oplus M_2 \oplus M_3$:

$$M_1 \oplus M_2 \oplus M_3 = (m_{11} \oplus m_{21} \oplus m_{31}, m_{12} \oplus m_{22} \oplus m_{32}, \dots, m_{1n} \oplus m_{2n} \oplus m_{3n}), \tag{21}$$

where $\oplus$ denotes the addition modulo 2. Our protocol works as follows:

(Step 1) TP prepares $N = 3n*(32+r+d+\delta) = 3nq$ particles, each of which is in the state $|+\rangle$, where $3nr$ and $3nd$ particles will be used to detect outside eavesdropping and TP's honesty, respectively, and δ is a parameter such that each participant can get an n-bit private key to encrypt their private n-bit strings in the last step. TP then divides these particles into three sequences: $S_1 = \{q_1^1, q_1^2, \dots, q_1^{nq}\}$, $S_2 = \{q_2^1, q_2^2, \dots, q_2^{nq}\}$ and $S_3 = \{q_3^1, q_3^2, \dots, q_3^{nq}\}$. q_j^i $(j \in \{1, 2, 3\}$; $i = 1, 2, \dots, nq$) represents the i-th particle for P_j. Later, TP sends particles one by one in S_j $(j = 1, 2, 3)$ to P_j. Note that TP should honestly prepare every particle in the state $|+\rangle$. If TP prepares every particle in the computational basis $\{|0\rangle, |1\rangle\}$, he/she can easily obtain the users' private keys as the measurement of the particles in the computational basis introduces no disturbance to them .TP can eventually get the users' private inputs based on their private keys. This bad behaviour should be detected. Thus, it is important to check TP's honesty.

(Step 2) Upon receiving a particle from TP, P_j $(j = 1, 2, 3)$ chooses randomly either to reflect the particle without disturbance back to TP or to measure it in the Z basis $\{|0\rangle, |1\rangle\}$ and resend it back to TP (measurement-resending). After that, S_1, S_2 and S_3 turn into S_1', S_2' and S_3', respectively.

(Step 3) TP combines S_1', S_2' and S_3' to form a sequence $S = \{(q_1'^1, q_2'^1, q_3'^1), (q_1'^2, q_2'^2, q_3'^2), \dots, (q_1'^{nq}, q_2'^{nq}, q_3'^{nq})\}$. TP then randomly chooses nr positions from these nq trios of particles and announces the information of positions to P_j $(j = 1, 2, 3)$. Next, TP and P_j start the first public discussion to check whether their transmission is secure. P_j first announces his choices and his measurement results from the measurement-resending operations in (Step 2) for these positions to TP. TP then adopts different actions based on P_j's choices to detect outside eavesdropping:

In case P_j reflected the particle in (Step 2). TP measures this particle in the X basis $\{|+\rangle, |-\rangle\}$. If the measurement result is $|-\rangle$, it indicates the particle was disturbed, and the protocol will abort and restart from the beginning;

In case P_j measured the particle and sent it back to TP in (Step 2). TP measures this particle in the Z basis $(|0\rangle, |1\rangle)$. If the measurement result from TP and that from P_j in (Step 2) are different, the protocol will abort and restart from the beginning.

If no eavesdropping is detected, the protocol will proceed to the next step.

(Step 4) In this step, three users will check if TP is honest. Three users ask TP to measure the rest trios of particles in the GHZ-type basis. Note that if a trio of particles is prepared in the state $|+\rangle|+\rangle|+\rangle$ by TP and these particles are reflected to TP, the measurement result obtained by TP will be $|\varphi_{000}\rangle$ or $|\varphi_{001}\rangle$. We will use this fact to check if TP is honest. If the measurement result is $|\varphi_{000}\rangle$ or $|\varphi_{001}\rangle$, TP then announces it to users. If the measurement result is $|\varphi_{110}\rangle$ or $|\varphi_{111}\rangle$, TP then writes it down and announces the corresponding message "summation" to users. This kind of measurement results will be used for the computation in the last step. The detection of TP's honesty is as following: after removing the trios that were employed in (Step 3), the users randomly select nd trios from the rest $(32+d+\delta)n$ trios to discuss in public to decide whether TP is honest or not. If three users reflected the particles in the same position in (Step 2) and TP's corresponding message is "summation", it shows that TP dishonestly prepared fake quantum states, according to (9). The protocol will abort and restart from the beginning.

Note that three users do not concern about the measurement results that are not in the above case. If TP's honesty is guaranteed, the protocol will continue.

(Step 5) TP will calculate the summation of three users' bit strings. Three users announce the locations where they have performed the measurement-resending operations in (Step 3). With the messages "summation" announced by TP, they can locate the positions where the messages "summation" were announced and all the corresponding choices by three users were the measurement-resending operations. There are about $(32+\delta)n \times \frac{1}{8} \times \frac{1}{4} = n + \frac{n\delta}{32}$ such positions. The trios in the first n positions will be employed to generate the users' private keys. In particular, P_j $(j = 1, 2, 3)$ selects the first n positions and changes the corresponding n-bit measurement results obtained in (Step 2) into his key (K_i) according the coding rule: $|0\rangle \rightarrow 0, |1\rangle \rightarrow 1$. The users then tell TP the information of these n positions. P_j computes $C_j = K_j \oplus M_j$, where $\oplus$ denotes the point-wise addition modulo 2 operation, and sends C_j to TP through the authenticated classical channel. Meanwhile, TP produces a private bit string T from his corresponding measurement results in the following way. If the measurement result is $|\varphi_{110}\rangle$ $(|\varphi_{111}\rangle)$, the corresponding private bit is 0 (1). TP eventually computes $C_1 \oplus C_2 \oplus C_3 \oplus T$ and announces the result to the users.

3 Analysis of the Proposed Protocol

In this section, we will give a detailed analyses of the correctness and the security of our protocol.

3.1 Correctness Analysis

We assume that the classical channels are authenticated and quantum channels are ideal (i.e., non-lossy and noiseless). A third party TP, who helps compute a summation, is assumed to be almost-dishonest. That is to say, TP is able to initiate all possible attacks by using various quantum resources, but he cannot collude with dishonest users.

As can be seen in (Step 5) of the proposed protocol, TP transforms measurement results $|\varphi_{110}\rangle$ and $|\varphi_{111}\rangle$ to bits 0 and 1, respectively. For the q-th ($q = 1, 2, \ldots, n$) position of the first n positions in (Step 5), if TP's measurement result is $|\varphi_{110}\rangle$, three users' measurement results should be one element of the set $\{|0\rangle|0\rangle0\rangle, |0\rangle|1\rangle1\rangle\}, |1\rangle|0\rangle1\rangle, |1\rangle1\rangle|0\rangle\}$, according to (10)–(17). Thus, if $T_q = 0$, then $K_{1q}K_{2q}K_{3q} \in \{000, 011, 101, 110\}$, where T_q, K_{1q}, K_{2q}, and K_{3q} denote the q-th bit of T, K_1, K_2, K_3, respectively. Likewise, if $T_q = 1$, then $K_{1q}K_{2q}K_{3q} \in \{001, 010, 100, 111\}$. Both cases give us

$$K_{1q} \oplus K_{2q} \oplus K_{3q} \oplus T_q = 0, \tag{22}$$

or equivalently,

$$K_1 \oplus K_2 \oplus K_3 \oplus T = (0, 0, \ldots, 0). \tag{23}$$

Consequently, when TP receives C_j ($j = 1, 2, 3$) from P_j, he can compute

$$\begin{aligned} C_1 \oplus C_2 \oplus C_3 \oplus T &= K_1 \oplus M_1 \oplus K_2 \oplus M_2 \oplus K_3 \oplus M_3 \oplus T \\ &= M_1 \oplus M_2 \oplus M_3 \oplus K_1 \oplus K_2 \oplus K_3 \oplus T \\ &= M_1 \oplus M_2 \oplus M_3, \end{aligned} \tag{24}$$

which is the summation of three users' private bit strings.

3.2 Security Analysis

In this subsection, the security of our protocol will be analysed. In general, the security analysis of quantum summation is more complicated than that of quantum key distribution, quantum secret sharing, and quantum secure direct communication. On the one hand, outside eavesdroppers wish to learn about users' private bit strings. On the other hand, dishonest users (including TP) may intend to obtain other users' private inputs. The proposed protocol should therefore be secure against outside as well as participant attacks.

Outside Attacks To begin with, we show that outside attacks are invalid to our protocol. To steal users' private bit strings, the outside attacker Eve has to know their keys that encrypt their private inputs. We consider here the case where Eve wants to attain user P_1's private bit string. Other cases where Eve attempts to take P_2's or P_3's private inputs can be analysed in a similar way.

One strategy Eve may adopt is the intercept-and-resend attack. Eve first intercepts all particles S_1 sent from TP to P_1 in (Step 1) and measures them in the Z basis. She then generates new particles in the Z basis whose polarizations are the same as the measurement results and sends them to P_1 to obtain P_1's private key K_1. However, this attack will be detected in (Step 3) due to Eve's lack of knowledge of nr positions randomly chosen by TP. For a particular particle chosen for detection, P_1 reflects this particle back to TP with probability 1/2. Hence, Eve has a probability of $(1/2) * (1/2) = (1/4)$ of being detected. That is to say, she can pass the detection with probability 3/4. For nr particles that are used for detection, the probability of Eve being caught turns into $1 - (3/4)^{3nr}$, which will approach 1 if $3nr$ is large enough.

Eve may also start the controlled NOT (CNOT) attack [30] on our protocol. The CNOT gate is defined as

$$CNOT_{12} = |00\rangle_{12}\langle 00| + |01\rangle_{12}\langle 01| + |11\rangle_{12}\langle 10| + |10\rangle_{12}\langle 11|, \tag{25}$$

where the first and second qubits are two input qubits, known as the control qubit and the target qubit, respectively.

Eve can perform CNOT operation on the particles in S_1 as the control qubits and her ancillary particles as the target qubits in (Step 1). When the particles are reflected back to TP, Eve can perform CNOT operation again on the particles in S_1' as the control qubits and her ancillary particles as the target bits in (Step 2), trying to escape the detection. Otherwise, Eve does not apply the second CNOT operation; instead, she measures her ancillary particles to derive P_1's key. However, Eve fails to decide whether to do the second CNOT operation or not because she learns nothing about P_1's choices. To escape the detection, Eve has to perform CNOT operation on particles both when they are sent to P_1 and sent back to TP. In this case, Eve will obtain nothing about P_1's key. Consider a particle in S_1 and an ancillary particle $|0\rangle$ generated by Eve, Eve performs the first CONT operation on these two particles when the particle is sent to P_1. After that, the state of these two particles becomes

$$CNOT_{1\mathrm{E}}|+\rangle_1|0\rangle_{\mathrm{E}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{1\mathrm{E}}, \tag{26}$$

where the scripts 1 and E denote the particle in S_1 and Eve's ancillary particle, respectively.

If P_1 reflects the particle and Eve performs the second CNOT operation on these two particles, the state turns into

$$CNOT_{1\mathrm{E}}\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{1\mathrm{E}} = |+\rangle_1|0\rangle_{\mathrm{E}}. \tag{27}$$

If P_1 measures the particle and obtains the measurement result $|0\rangle_1$ ($|1\rangle_1$), then the state of the ancillary particle collapses into $|0\rangle_E$ ($|1\rangle_E$). After Eve performs the second CNOT operation on these two particles, the state changes to

$$CNOT_{1\mathrm{E}} \quad = |0\rangle_1|0\rangle_{\mathrm{E}} = |0\rangle_1|0\rangle_{\mathrm{E}} \tag{28}$$

$$(CNOT_{1\mathrm{E}} \quad = |1\rangle_1|1\rangle_{\mathrm{E}} = |1\rangle_1|0\rangle_{\mathrm{E}}). \tag{29}$$

We can see from (27)–(29) that the state of Eve's ancillary particle $|0\rangle_E$ tells nothing about P_1's key.

In our protocol, Eve can perform the Trojan horse attack [45, 46]; she can insert the Trojan horse photons into S_1 in (Step 1) to reveal P_1's choices in (Step 2), based on which to attain P_1's key. However, the photon number splitter and the optical wavelength filter devices [47, 48] can be utilized to detect such an attack.

TP's Attacks Let us now consider TP's attacks. In our protocol, there is no doubt that TP is more powerful than users. We assume that TP is almost-dishonest, which means that he can perform all sorts of attacks by using various quantum resources except collusion with any dishonest user.

If TP attempts to obtain all of the users' keys to derive their private inputs, he may try to predetermine users' keys and announce fake measurement results in (Step 4) to pass users' detection.

If TP intends to get all users' private key in advance, he can prepare all the quantum states in the Z basis ($|0\rangle$, $|1\rangle$) and sends these states to all users in (Step 1) in which way he will obtain all users' private keys in (Step 5). However, this dishonest behavior will be detected in (Step 4) during the detection of TP's honesty. Note that TP may also prepare entangled states, but this offers no more help than preparing all states in the Z basis to obtain users' private keys.

For a valid trio of particle chosen for the detection of TP's honesty, he can pass the detection with the probability of $1/4$, according to (10)–(17). For nd trios of particles utilized to detect TP's honesty, the number of the valid trios (each of the trio of particle is reflected back to TP) will be $(1/2)^3 nd = (1/8)nd$. The probability of passing the detection will therefore be $(1/4)^{(1/8)nd}$, approaching 0 when $(1/8)nd$ is large enough.

TP may only desire one of three users' private inputs (say P_1's private input). In this case, TP only prepares quantum states for P_1 in the Z basis, and other quantum states in the state $|+\rangle$. The probability of passing the detection will be $|\langle\varphi_{000}|w++\rangle|^2 + |\langle\varphi_{001}|w++\rangle|^2 = 1/2, w \in \{0,1\}$. Similarly, for nd trios of particles utilized to detect TP's honesty, the probability of passing the detection is $(1/2)^{(1/8)nd}$ that will be approaching 0 when $(1/8)nd$ is large enough.

Therefore, TP cannot obtain any user's private input without being caught.

Attacks from one of the Three Users Finally, we come to the analysis of attacks from dishonest users. Note that any two users can easily collaborate to get the third one's private bit string relying on the summation result in our three-party scenario. Hence, we account for attacks from one dishonest user who cannot be able to collude with other users.

We assume that P_1 is the dishonest user who has a strong desire to learn about the other two users' private bit strings. Suppose that P_1 endeavours to take P_2's private input. Analogously, the case of stealing P_3's private bit string can be analysed in a similar way.

To obtain P_2's private bit string M_2, P_1 has to figure out P_2's private key K_2 that encrypts M_2. Note that K_2 is generated from the measurement results, for which three users choose the measurement-resending operations in the same positions and TP's responding message is "summation". Unlike Eve, P_1 may measure a particle in S_2 only when he measures his in the same position of that particle. So P_1 performs the measurement-resending operations on half of the particles in both S_1 and S_2 in the same positions by intercepting S_2 from TP in (Step 1). S_2 is changed to S_2^1 after P_1's operations. P_1 then sends S_2^1 to P_2. Similarly, P_1 applies the same operations on S_2' in (Step 2) to get K_2 . However, this attack will be detected, because P_1 dose not know P_2's choices in (Step 3). For a trio of particles chosen for detection, P_1 chooses the measurement-resending operations on his particle with probability $1/2$; P_2 reflects his particle in the same position with probability $1/2$, the probability of P_1 being detected will be $(1/2) * (1/2) * (1/2) = 1/8$. For nr trios of particles for detection, the probability that P_1 will be caught becomes $1 - \left(\frac{7}{8}\right)^{nr}$. When nr is large enough, this probability will be close to 1. P_1 cannot thus obtain any user's private input without being caught.

4 Discussion and Conclusions

We have employed single photons to construct a secure three-party semi-quantum summation protocol with an almost-dishonest third party (TP), who is in charge of generating photons and computing the summation of three users' private bit strings. We have also analysed in detail the correctness and the security of our protocol.

In our protocol, the summation result is revealed by TP in the end. If the summation result is secret and should be known only to three users, a trap method [11, 49] can be employed to solve this problem by using a pre-shared key among three users. Note that, an n-party ($n > 3$) semi-quantum summation protocol can be extended with the similar method in our paper. However, it needs a multitude of quantum resources and the measurements for multi-partite entangled states remain difficult. In addition, quantum channels are usually noisy and lossy. Thus, designing an efficient and practical n-party ($n > 3$) semi-quantum summation protocol over noisy and lossy quantum channels will be our future work.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant Nos. 61902132, 11647140, and 61872152), the Guangdong Basic and Applied Basic Research Foundation (Grant No. 2021A1515011985), the Natural Science Foundation of Guangdong Province of China (Grant No. 2018A030310147), the Shenzhen Polytechnic Youth Innovation Project (Grant Nos. 6019310010K0 and 6019310007K0), and the Shenzhen Technical Project (No. JCYJ20190809152003992).

References

1. Heinrich, S.: Quantum summation with an application to integration. J. Complex. **18**(1), 1–50 (2002)
2. Heinrich, S., Novak, E.: On a problem in quantum summation. J. Complex. **19**(1), 1–18 (2003)
3. Heinrich, S., Kwas, M., Wozniakowski, H.: Quantum boolean summation with repetitions in the worst-average setting. arXiv:quant-ph/0311036 (2003)
4. Du, J.Z., Chen, X.B., Wen, Q.Y., Zhu, F.C.: Secure multiparty quantum summation. Acta Phys. Sin. **56**(11), 6214 (2007)
5. Chen, X.B., Xu, G., Yang, Y.X., Wen, Q.Y.: An efficient protocol for the secure multi-party quantum summation. Int. J. Theo. Phy. **49**(11), 2793–2804 (2010)
6. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**, 1154–1162 (1997)
7. Crépeau, C., Gottesman, D., Smith, A.: Secure multi-party quantum computation. In: Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing, pp. 643–652. ACM (2002)
8. Chau, H.F.: Quantum-classical complexity-security tradeoff in secure multiparty computations. Phys. Rev. A **61**, 032308 (2000)
9. Ben-Or, M., Crepeau, C., Gottesman, D., Hassidim, A., Smith, A.: Secure multiparty quantum computation with (only) a strict honest majority. In: 47th Annual IEEE Symposium on Foundations of Computer Science, 2006. FOCS'06, pp. 249–260 (2006)
10. Smith, A.: Multi-party quantum computation. arXiv:quant-ph/0111030 (2010)
11. Sun, Z., Yu, J., Wang, P., Xu, L., Wu, C.: Quantum private comparison with a malicious third party. Quantum Inf. Process **14**(6), 2125–2133 (2015)
12. Hung, S.M., Hwang, S.L., Hwang, T., Kao, S.H.: Multiparty quantum private comparison with almost dishonest third parties for strangers. Quantum Inf. Process **16**(2), 36 (2017)
13. He, G.P.: Quantum private comparison protocol without a third party. Int. J. Quantum Inf. **15**(02), 1750014 (2017)
14. Hillery, M., Ziman, M., Bužek, V., Bieliková, M.: Towards quantum-based privacy and voting. Phys. Lett. A **349**(1-4), 75–81 (2006)
15. Li, Y., Zeng, G.: Quantum anonymous voting systems based on entangled state. Optical Review **15**(5), 219–223 (2008)
16. Wang, Q., Yu, C., Gao, F., Qi, H., Wen, Q.: Self-tallying quantum anonymous voting. Phys. Rev. A **94**(2), 022333 (2016)
17. Xue, P., Zhang, X.: A simple quantum voting scheme with multi-qubit entanglement. Scientific Reports **7**(1), 7586 (2017)
18. Bao, N., Halpern, N.Y.: Quantum voting and violation of arrow's impossibility theorem. Phys. Rev. A **95**(6), 062306 (2017)
19. Zhang, C., Sun, Z., Huang, Y., Long, D.: High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. Int. J. Theor. Phys. **53**(3), 933–941 (2014)
20. Zhang, C., Sun, Z.W., Huang, X., Long, D.Y.: Three-party quantum summation without a trusted third party. Int. J. Quantum Inf. **13**(02), 1550011 (2015)
21. Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep. **6**, 19655 (2016)
22. Shi, R.H., Zhang, S.: Quantum solution to a class of two-party private summation problems. Quantum Inf. Process **16**(9), 225 (2017)

23. Zhang, C., Situ, H., Huang, Q., Yang, P.: Multi-party quantum summation without a trusted third party based on single particles. Int. J. Quantum Inf.: 1750010 (2017)
24. Liu, W., Wang, Y.B., Fan, W.Q.: An novel protocol for the quantum secure multi-party summation based on two-particle bell states. Int. J. Theor. Phys. **56**(9), 2783–2791 (2017)
25. Yang, H.Y., Ye, T.Y.: Secure multi-party quantum summation based on quantum fourier transform. Quantum Inf. Process **17**(6), 129 (2018)
26. Ji, Z., Zhang, H., Wang, H., Wu, F., Jia, J., Wu, W.: Quantum protocols for secure multi-party summation. Quantum Inf. Process **18**(6), 168 (2019)
27. Julsgaard, B., Sherson, J., Cirac, J.I., Fiurášek, J., Polzik, E.S.: Experimental demonstration of quantum memory for light. Nature **432**(7016), 482 (2004)
28. Yao, X.C., Wang, T.X., Xu, P., Lu, H., Pan, G.S., Bao, X.H., Peng, C.Z., Lu, C.Y., Chen, Y.A., Pan, J.W.: Observation of eight-photon entanglement. Nature Photonics **6**(4), 225 (2012)
29. Nielson, M.A., Chuang, I.L.: Quantum computation and quantum information (2000)
30. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical bob. In: 2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07), pp. 10–10. IEEE (2007)
31. Zou, X., Qiu, D., Li, L., Wu, L., Li, L.: Semiquantum-key distribution using less than four quantum states. Phy. Rev. A **79**(5), 052312 (2009)
32. Jian, W., Sheng, Z., Quan, Z., Chao-Jing, T.: Semiquantum key distribution using entangled states. Chinese Phys. Lett. **28**(10), 100301 (2011)
33. Krawec, W.O.: Mediated semiquantum key distribution. Phys. Rev. A **91**(3), 032323 (2015)
34. Li, Q., Chan, W.H., Zhang, S.: Semiquantum key distribution with secure delegated quantum computation. Scientific Reports **6**, 19898 (2016)
35. Liu, Z.R., Hwang, T.: Mediated semi-quantum key distribution without invoking quantum measurement. Annalen der Physik **530**(4), 1700206 (2018)
36. Li, Q., Chan, W.H., Long, D.Y.: Semiquantum secret sharing using entangled states. Phys. Rev. A **82**, 022303 (2010)
37. Wang, J., Zhang, S., Zhang, Q., Tang, C.J.: Semiquantum secret sharing using two-particle entangled state. Int. J. Quantum Inf. **10**(05), 1250050 (2012)
38. Li, L., Qiu, D., Mateus, P.: Quantum secret sharing with classical bobs. J. Phys. A: Mathematical and Theoretical **46**(4), 045304 (2013)
39. Yang, C.W., Hwang, T.: Efficient key construction on semi-quantum secret sharing protocols. Int. J. Quantum Inf. **11**(05), 1350052 (2013)
40. Chou, W.H., Hwang, T., Gu, J.: Semi-quantum private comparison protocol under an almost-dishonest third party. arXiv:1607.07961 (2016)
41. Yan-Feng, L.: Semi-quantum private comparison using single photons. Int. J. Theor. Phys. **57**(10), 3048–3055 (2018)
42. Lin, P.H., Hwang, T., Tsai, C.W.: Efficient semi-quantum private comparison using single photons. Quantum Inf. Process **18**(7), 207 (2019)
43. Shukla, C., Thapliyal, K., Pathak, A.: Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. Quantum Inf. Process **16**(12), 295 (2017)
44. Dür, W., Vidal, G., Cirac, J.I.: Three qubits can be entangled in two inequivalent ways. Phys. Rev. A **62**(6), 062314 (2000)
45. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**(1-2), 23–25 (2006)
46. Kraus, B., Tittel, W., Gisin, N., Nilsson, M., Kröll, S., Cirac, J.: Quantum memory for nonstationary light fields based on controlled reversible inhomogeneous broadening. Phys. Rev. A **73**(2), 020302 (2006)
47. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against trojan horse attack. Phys. Rev. A **72**(4), 044302 (2005)
48. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A **74**(5), 054302 (2006)
49. Gu, J., Ho, C.Y., Hwang, T.: Statistics attack on 'quantum private comparison with a malicious third party'and its improvement. Quantum Inf. Process **17**(2), 23 (2018)