entropy

MDPI

Article

Multi-Party Quantum Summation Based on Quantum Teleportation

Cai Zhang [1,2,*], Mohsen Razavi [2,*], Zhiwei Sun [3,4,*], Qiong Huang [1] and Haozhen Situ [1]

1 College of Mathematics and Informatics, South China Agricultural University, Guangzhou 510642, China
2 School of Electronic and Electrical Engineering, University of Leeds, Leeds LS2 9JT, UK
3 School of Artificial Intelligence, Shenzhen Polytechnic, Shenzhen 518055, China
4 Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen 513055, China
* Correspondence: zhangcai.sysu@gmail.com (C.Z.); m.razavi@leeds.ac.uk (M.R.); sunzhiwei1986@gmail.com (Z.S.)

Received: 27 May 2019; Accepted: 9 July 2019; Published: 23 July 2019

Abstract: We present a secure multi-party quantum summation protocol based on quantum teleportation, in which a malicious, but non-collusive, third party (TP) helps compute the summation. In our protocol, TP is in charge of entanglement distribution and Bell states are shared between participants. Users encode the qubits in their hand according to their private bits and perform Bell-state measurements. After obtaining participants' measurement results, TP can figure out the summation. The participants do not need to send their encoded states to others, and the protocol is therefore congenitally free from Trojan horse attacks. In addition, our protocol can be made secure against loss errors, because the entanglement distribution occurs only once at the beginning of our protocol. We show that our protocol is secure against attacks by the participants as well as the outsiders.

Keywords: quantum information; quantum cryptography; quantum summation; quantum teleportation; Bell states; participant attacks

1. Introduction

Secure multi-party computation, as a subfield in cryptography, has been gaining attention in recent years [1–4]. It was first introduced by Yao [5] and later extended by Goldreich et al. [6]. Secure multi-party computation has also been studied in quantum settings [7–11]. Lo [7] pointed out the insecurity of quantum computation without a third party in a two-party scenario. Chau [9] employed quantum resources to speed up classical multi-party computation. Ben-Or et al. [10] investigated distributed quantum computation. They showed how many players must be honest in order to make any multi-party quantum computation secure. Smith [11] proved that any multi-party quantum computation can be secure as long as the number of dishonest players is less than $n/6$, when n, the number of players, is larger than 6.

Secure multi-party quantum summation [12–16], which helps the construction of complex multi-party computation, is a fundamental primitive of secure multi-party quantum computation. In quantum summation protocols, the privacy of participants' inputs is preserved and the correctness of the summation is guaranteed by quantum properties. Quantum summation has also potential applications in quantum voting [17–21] and quantum private equality comparison [22–24]. Designing quantum summation protocols that can be implemented with current or near future quantum technologies is therefore of interest, as we pursue in this paper.

In the past few years, various quantum summation protocols have been proposed by employing a variety of quantum resources. Zhang et al. [25] presented a quantum summation protocol with single photons encoded in both polarization and spatial-mode degrees of freedom in 2014, in which

unitary operations are utilized to encode the private bits on the travelling single photons. Such single photons must somehow be handed over/transmitted to the next user so that the collective sum of all private bits can be calculated. Most other protocols rely on sharing a multipartite entangled state among players. For instance, in 2015, a quantum summation protocol without a trusted third party was constructed [26]. However, the number of participants was limited to three due to the requirement of the so-called genuinely maximally entangled six-qubit states. In 2016, Shi et al. [27] used quantum Fourier transform, controlled NOT (CNOT) gates and oracle operators to propose protocols for summation and multiplication. Later, they proposed a common quantum solution to a class of two-party private summation problems [28]. In 2017, a multi-party quantum summation without a trusted third party was investigated by first generating a multipartite entangled state by one player and then sharing it with other users [29]. In the same year, Liu et al. [30] adopted Bell states to construct multipartite entangled states that were used to carry participants' inputs, where the quantum communication in their protocol is two-way. This means that special care with regard to Trojan horse attacks [31–33] should be provided to participants. Unlike their protocols, participants in our protocol do not need to send the encoded states back to others, thus our protocol is naturally free from Trojan horse attacks and no protection against such attacks are needed. In 2018, Yang et al. [34] provided a quantum solution to secure summation depending on n-partite multi-dimensional entangled states.

One common feature in all hitherto proposed quantum summation protocols is their dependence on a reliable means for quantum state transfer. In the case of protocols that rely on sharing multipartite entangled states [27–30,34], such a state is often generated by one player and then its different components are sent to other players. If any of these components does not reach its respective destination, then the whole procedure must be repeated. In such a case, relying on photons travelling through lossy channels does not seem to be an efficient option. Moreover, it could open us to new security threats that an eavesdropper can exploit by hiding behind the channel loss. Even for the case of the protocol in Ref. [25], the loss of the single photon in any leg of the system requires repeating the whole procedure. In addition, an eavesdropper can send a photon of her choice to a user and measure it after the user has applied his encoding to find out about the user's private bit. Most of these protocols fail to work unless a reliable quantum state transfer (RQST) service is available to them. This is a kind of service that one may expect to have once we have a fully functional quantum network.

There are two well-known approaches to RQST. In one scenario, one distributes entangled states between the two end users of a quantum communication system, and then use teleportation to transfer an unknown quantum state from one place to another. In the second approach, one has to use perhaps complex quantum error correction codes to compensate for the erasure errors caused by photon loss as well as operational errors caused by system components. In both cases, we need quantum memories in our setup to store quantum states and to execute certain quantum processing tasks such as entanglement distillation or quantum error correction. This requirement of the system has thus far been neglected in the design of quantum summation protocols.

In this paper, we take advantage of the idea of quantum teleportation [35] to devise our protocol. In order to get a better insight into the practicality of a quantum summation protocol, in this work, we account for the bipartite entangled states that one would need to distribute if teleportation is used for the RQST part of the protocol. We discover that in fact such Bell states are sufficient to devise a secure quantum summation protocol without requiring the distribution of additional multipartite entangled states. Moreover, by not revealing the information about which Bell state is shared between two players, we, in effect, can protect ourselves against attacks by malicious participants. In our protocol, similar to Ref. [25], participants' private bits are encoded into single-qubit unitary operations. Encoded states are then effectively teleported to the next user by performing local Bell-state measurements (BSMs). This makes our protocol congenitally free from Trojan horse attacks. In our protocol, the required Bell states are shared by a third party (TP), who can be malicious but does not collide with other players. In any case, our protocol does not rely on multipartite entanglement or high-dimensional states, which makes its implementation much more feasible.

Table 1 summarizes the required resources for various protocols as compared to ours. In particular, we have compared these protocols in terms of their efficiency, defined as the number of qubits (quantum memories) they need in order to find the sum of n private bits, when one accounts for a minimum of two quantum memories needed for teleportation. The assumption here is that maximally entangled states are shared among users, but we do not account for additional memories that may be needed for entanglement distillation or for possible repeater nodes. It is clear from this table that our protocol not only is more efficient than other protocols in the table but also only relies on bipartite entanglement rather than multipartitite states.

Table 1. A comparison between different quantum summation (QS) protocols in terms of their required resources and operations, as well as their efficiency.

QS Protocols	Efficiency	Quantum Resource	Quantum Operations
Shi et al.'s [27]	$\frac{1}{3n-2}$	$(n+1)$-partite entangled state	Quantum Fourier operator, CNOT operator, and oracle operator
Zhang et al.'s [29]	$\frac{1}{3n-2}$	n-partite entangled state	CNOT operator and Hadamard operator
Liu et al.'s [30]	$\frac{1}{3n-2}$ or $\frac{1}{3n+1}$	n-partite entangled state or $(n+1)$-partite entangled state	Pauli operators and Hadamard operators
Yang et al.'s [34]	$\frac{1}{3n-2}$	n-partite entangled state	Quantum Fourier operator and Pauli operators
This work	$\frac{1}{2n+3}$	Bell states	Pauli operators and Bell measurement

The rest of this paper is organized as follows. In Section 2, we illustrate our idea to design a secure multi-party quantum summation protocol and provide an example of a two-party scenario. In Section 3, we describe our multi-party quantum summation protocol in detail, followed by its correctness and security analysis in Section 4. Practical considerations of our protocol will be discussed in Section 5, and conclusions are given in Section 6.

2. Key Idea of Our Protocol

In this section, we work out our proposed quantum summation protocol for the particular case of two participants and a malicious but non-collusive third party (TP). TP has to calculate the modulo 2 sum of the participants' secret bits by satisfying the following requirements:

1. Correctness: the result of summation in modulo two of all participants' private input bits is correct.
2. Security: an eavesdropping outsider cannot learn any information about participants' private input bits without being detected.
3. Privacy: TP cannot learn about participants' private inputs.

Note that although TP cannot obtain two participants' private bits in the two-party scenario, each participant can find out the private bit of the other participant once the sum is known. Nevertheless, this is a simple example by which we can explain our protocol. In Section 3, we generalize this idea to the multiple participants scenario, where the privacy requirement will be extended to include most participants as well as TP.

Our protocol relies on sharing a chain of Bell states among participants and teleporting an unknown state by TP to itself via this chain; see Figure 1. Along the way participants can affect the linked states by applying local operations on their share of entangled states. TP can calculate the sum by comparing the teleported state with the original state she has generated.

Before describing the protocol, let us first review the teleportation protocol and introduce the notation used in the paper. In general, Bell states are of the following form

$$|B_{xy}\rangle = \frac{1}{\sqrt{2}}(|0,x\rangle + (-1)^y|1,x\oplus 1\rangle), \tag{1}$$

where $x, y \in \{0,1\}$ and $\oplus$ represents addition modulo 2. The relationship between Bell states and classical bits can be defined as

$$|B_{xy}\rangle \leftrightarrow xy, x, y \in \{0,1\}. \tag{2}$$

For any qubit $|\varphi\rangle$ and any single-qubit unitary operation U, a general teleportation equation, based on an initial Bell state $|B_{ab}\rangle, a, b \in \{0,1\}$, shared between the two users, can be written as

$$|\varphi\rangle_1 \otimes (I \otimes U)|B_{ab}\rangle_{2,3} = \frac{1}{2}\sum_{x\in\{0,1\}}\sum_{y\in\{0,1\}}(-1)^{b\cdot x}|B_{xy}\rangle_{1,2} \otimes UZ^{y\oplus b}X^{x\oplus a}|\varphi\rangle_3, \tag{3}$$

where $X = (|0\rangle\langle 1| + |1\rangle\langle 0|)$, $Z = (|0\rangle\langle 0| - |1\rangle\langle 1|)$ and the subscripts denote different systems.

In this work, we are particularly interested in the unitary operation $U = ZX$, for which we have:

$$\begin{aligned} UZ^bX^a &= ZXZ^bX^a = (-1)^bZ^bZXX^a = (-1)^bZ^bZX^aX \\ &= (-1)^b\cdot(-1)^aZ^bX^aZX = (-1)^{a\oplus b}Z^bX^aZX \\ &= (-1)^{a\oplus b}Z^bX^aU, \end{aligned} \tag{4}$$

where $a, b \in \{0,1\}$. Additionally, the following equations

$$U|0\rangle = ZX|0\rangle = -|1\rangle, \tag{5}$$
$$U|1\rangle = ZX|1\rangle = |0\rangle, \tag{6}$$
$$U|+\rangle = ZX|+\rangle = |-\rangle, \tag{7}$$
$$U|-\rangle = ZX|-\rangle = -|+\rangle, \tag{8}$$

hold, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Note that both computational basis $\{|0\rangle, |1\rangle\}$ and diagonal basis $\{|+\rangle, |-\rangle\}$ are closed under U. Ignoring the phase, U swaps $|0\rangle$ and $|1\rangle$ ($|+\rangle$ and $|-\rangle$). We use $U = ZX$ from now on and it will be applied on one of the two components of a Bell state if the participants' private bit is 1.

Now, let us describe a simple version of our protocol that, for now, does not fulfill the security requirement; see Figure 1. Suppose each participant has two quantum memories. Then, we implement the following steps:

(Step 1) Entanglement distribution. TP distributes Bell states, each of which is randomly selected from the Bell basis, among participants and generates a state $|\varphi\rangle_T$ chosen randomly from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. The state $|\varphi\rangle_T$ is stored in quantum memory T.

(Step 2) Private inputs encoding. P_1 (P_2) applies $U = ZX$ on quantum memory 1 (quantum memory 3) if her private bit is 1. Otherwise, she does nothing.

(Step 3) Bell-state measurement. TP measures quantum memories T and 0 in the Bell basis. Similarly, P_1 (P_2) measures quantum memories 1 and 2 (3 and 4) in the Bell basis. P_1 and P_2 will announce their measurement results to TP.

(Step 4) Correction and computation. After necessary corrections on quantum memory 5 depending on all the measurement results and the original Bell states, TP measures quantum memory 5 in the same basis as that of the original state of quantum memory T. If the state of quantum memory 5 is the same as the original state of quantum memory T, TP concludes that the sum is 0, otherwise, the sum is 1.

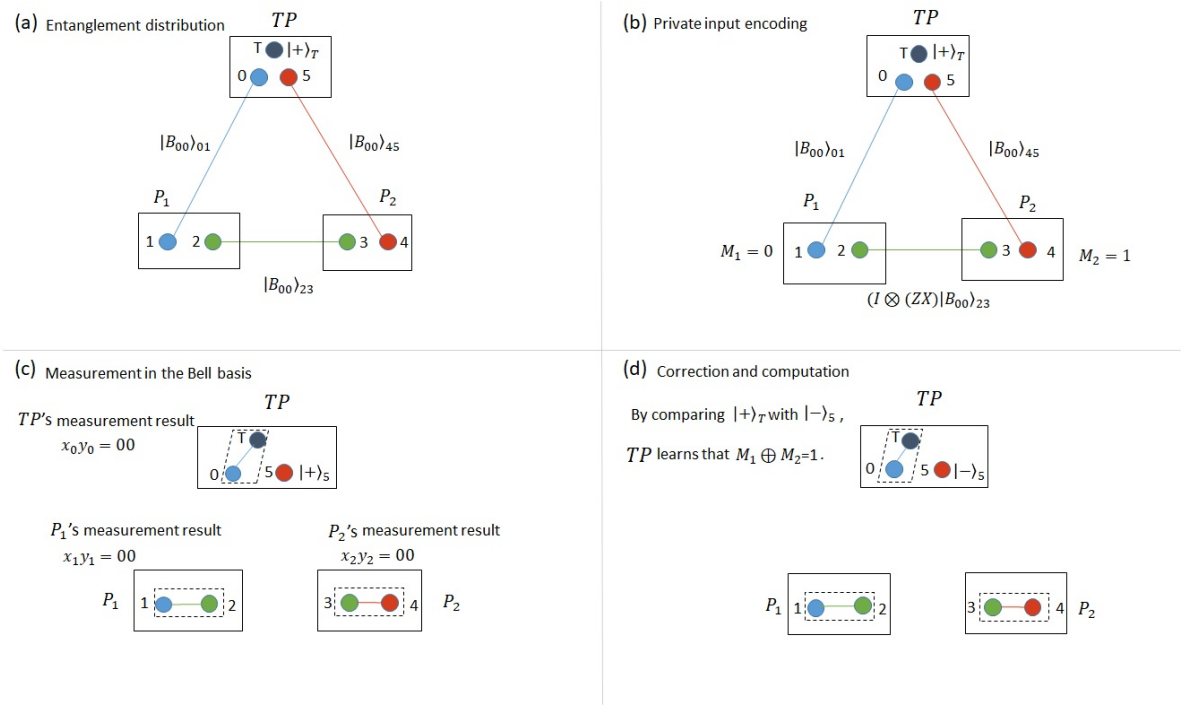

Figure 1. A simple example of our protocol in the two-party scenario. (**a**) Step 1: third party (TP) shares entangled states among users to create a chain of entangled links back to herself. In this example, we assume state $|B_{00}\rangle$ is shared over all links. In general, different Bell states can be shared over different links, and only TP knows which state has been shared. (**b**) Step 2: users with private bit 1 apply operator U to thier first qubit. Here, only P_2 must do this. (**c**) Step 3: all players perform a Bell-state measurements (BSM) on their two qubits and let TP know of the results. In our example, we have assumed $|B_{00}\rangle$ has been obtained in all cases. (**d**) Step 4: TP measures qubit 5 in the same basis as her originally chosen basis for qubit T. By comparing the result with the original state of T, TP can calcualte $M_1 \oplus M_2$.

Let us work out a simple example to show how the protocol works. In Figure 1,

(Step 1) Entanglement distribution. Suppose the initial state among TP, P_1 and P_2 is given by

$$|\zeta_j^0\rangle = |+\rangle_T \otimes |B_{00}\rangle_{01} \otimes |B_{00}\rangle_{23} \otimes |B_{00}\rangle_{45}. \tag{9}$$

(Step 2) Private input encoding. Suppose P_1's (P_2's) private bit is 0 (1), P_1 then does nothing on quantum memory 1, but P_2 applies $U = ZX$ on quantum memory 3. According to Equations (3)–(8), the state becomes

$$\begin{aligned}|\zeta_j^1\rangle =& |+\rangle_T \otimes (I \otimes I)|B_{00}\rangle_{01} \otimes (I \otimes (ZX))|B_{00}\rangle_{23} \otimes |B_{00}\rangle_{45} \\ =& \frac{1}{8} \sum_{x_0 \in \{0,1\}} \sum_{y_0 \in \{0,1\}} \sum_{x_1 \in \{0,1\}} \sum_{y_1 \in \{0,1\}} \sum_{x_2 \in \{0,1\}} \sum_{y_2 \in \{0,1\}} \\ & |B_{x_0y_0}\rangle_{T0}|B_{x_1y_1}\rangle_{12}|B_{x_2y_2}\rangle_{34} Z^{y_1 \oplus y_2 \oplus y_3} X^{x_1 \oplus x_2 \oplus x_3}|-\rangle_5,\end{aligned} \tag{10}$$

where a global phase in the state of quantum memory 5 is ignored.

(Step 3) Bell-state measurement. Suppose all the measurement results are $x_0y_0 = x_1y_1 = x_2y_2 = 00$, and they are announced to TP. Then, effectively, the state of T is teleported to qubit 1, and then teleported to qubit to 3, at which point it is flipped by the U operation, and teleported back to TP.

(Step 4) Correction and computation. In this particular case, there is no correction needed by TP. TP measures quantum memory 5 in the basis $\{|+\rangle, |-\rangle\}$, and finds that the state of quantum memory 5 is different from the original state of quantum memory T. TP concludes that the sum is 1.

In (Step 3) of the above example, if not all the measurement results are 00, TP can correct the state of quantum memory 5 by performing quantum operations on it using Equations (3) and (4) before she measures quantum memory 5.

In a full protocol, we need to include steps that alert us to possible attacks. We consider two kinds of attacks in our protocol: those by outsides and those by malicious participants. We employ extra Bell states to detect these attacks and meet the security requirements. By measuring each component of a Bell state in the same basis (all in the computational basis or all in the diagonal basis) and comparing the measurement results, these attacks can be detected. The details of the detection process can be found in Section 3.

3. Multi-Party Quantum Summation

We assume that the classical channels are authenticated and quantum channels are noiseless. The third party, TP, who conducts the summation is assumed to be malicious but non-collusive. That is to say, TP can do whatever she would like within boundaries of quantum mechanics except collision with dishonest participants. The summation can be revealed in public. For simplicity, we denote TP as P_0 in the rest of the paper.

Suppose that the q-th participant ($q = 1, 2, \ldots, n$; $n > 2$) has a private bit string M_q. P_0 computes the summation $\oplus \sum_{q=1}^{n} M_q$, where $\oplus \sum$ denotes pointwise addition in modulo 2, and

$$\begin{array}{rcl} M_1 & = & (m_{11}, m_{12}, \ldots, m_{1L}), \\ M_2 & = & (m_{21}, m_{22}, \ldots, m_{2L}), \\ & \cdots & , \\ M_n & = & (m_{n1}, m_{n2}, \ldots, m_{nL}), \\ \oplus \sum_{q=1}^{n} M_q & = & (\sum_{i=1}^{n} m_{i1}, \sum_{i=1}^{n} m_{i2}, \ldots, \sum_{i=1}^{n} m_{iL}), \end{array} \tag{11}$$

where L is the length of each private bit string.

Our n-party ($n > 2$) summation protocol shall meet the following requirements:

1. Correctness: the result of pointwise summation in modulo two of all participants' private input bits is correct.
2. Security: an outside eavesdropper cannot learn any information about participants' private input bits without being detected.
3. Privacy: no participant can learn about other participants' private input bits without being detected, except in the obvious case of $n - 1$ players collaborating to learn the remaining user's private bits.

Our full protocol is described in the following.

(Step 1) *Entanglement distribution.* P_0 uses a certain entanglement distribution protocol [36–40] to distribute $(n + 1)(L + R)$ ordered Bell states, $K_i = (|\psi_1^i\rangle_{(2i)(2i+1)} |\psi_2^i\rangle_{(2i)(2i+1)} \cdots |\psi_{L+R}^i\rangle_{(2i)(2i+1)})$ ($i = 0, 1, \ldots, n$), where $|\psi_1^i\rangle_{(2i)(2i+1)}$ is chosen from the set $\{|B_{xy}\rangle | x, y \in \{0, 1\}\}$, to n participants such that these states form a chain. Specifically, for K_i, all first (second) components of Bell states are stored in quantum memory G_{2i}^i (G_{2i+1}^i). As shown in Figure 2, banks of quantum memories G_{2i-1}^{i-1} and G_{2i}^i belong to P_i ($i = 1, 2, \ldots, n$) and quantum memories G_0^0 and G_{2n}^{2n+1} are held by P_0. P_0 also generates L ordered states, $A_T = (|\varphi_1\rangle_T, |\varphi_2\rangle_T, \ldots, |\varphi_L\rangle_T)$, where $|\varphi_i\rangle_T$ ($i = 1, 2, \ldots, L$) is randomly chosen from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. These states remain in P_0's quantum memory G_T^0. Note that all the initial states are only known to P_0.

(Step 2) Security detection. Participants detect if genuine Bell states are shared among them in an honest way.

(Step 2.1) To examine the genuinity of the Bell states shared between P_0 and P_1, P_1 first randomly chooses R Bell states shared between quantum memory G_0^0 and quantum memory G_1^0 and asks P_0 to announce the corresponding initial states. P_1 then measures each corresponding component in G_1^0 randomly in the computational basis $\{|0\rangle, |1\rangle\}$ or in the diagonal basis $\{|+\rangle, |-\rangle\}$, and keeps the measurement results to herself. Subsequently, P_1 asks P_0 to measure the corresponding components in the same basis as P_1 does and publicize the measurement results. According to the property of Bell states, P_1 checks if these measurement results are correlated with each other. If the error rate exceeds a certain threshold, the protocol will be aborted and repeated from (Step 1). Otherwise, the protocol will continue.

(Step 2.2) To check the genuinity of the Bell states shared between P_0 and P_n, P_n also uses R Bell states to complete this detection utilizing the similar method as that used by P_1. If the error rate exceeds the threshold, the protocol will be aborted and repeated from (Step 1). Otherwise, the protocol will continue.

(Step 2.3) To check the genuinity of the Bell states shared between P_i and P_{i+1} $(i = 1, 2, \ldots, n-1)$, P_i randomly selects $R/2$ Bell states shared between G_{2i}^i and G_{2i+1}^i and asks P_0 to announce the corresponding initial states. Later, P_i measures each corresponding component in G_{2i}^i randomly in the computational basis or in the diagonal basis, announcing the measurement results. Next, P_{i+1} measures each component in G_{2i+1}^i entangled with the one in P_i's hands in the same basis, publicizing the measurement results. P_i and P_{i+1} can finally check if these measurement results are correlated according to the initial states and the property of Bell states. The same procedure will be used by P_{i+1} with $R/2$ Bell states of his choice and randomly selected measurement bases. If the error rate in either case exceeds the threshold, the protocol will be aborted and repeated from (Step 1). Otherwise, they ensure that the states shared between them are genuine Bell states and distributed in an honest way, and the protocol will continue.

(Step 3) *Private input encoding*. P_0 removes R states used for detection from quantum memory G_0^0 (G_{2n+1}^n), leaving L ordered states, denoted by V_0^0 (V_{2n+1}^n), in it. P_i $(i = 1, 2, \ldots, n)$ also removes R states used for checking from quantum memory G_{2i-1}^{i-1} (G_{2i}^i), resulting in L ordered states, denoted by V_{2i-1}^{i-1} (V_{2i}^i), in it. Note that quantum memories G_{2i}^i and G_{2i+1}^i $(i = 0, 1, \ldots, n)$ now share L ordered Bell states, which form L chains of Bell states among all participants (inlucding P_0). Namely, the j-th $(j = 1, 2, \ldots, L)$ state of V_{2i}^i in G_{2i}^i and the j-th one of V_{2i+1}^i in G_{2i+1}^i form a Bell state. Afterwards, P_i $(i = 1, 2, \ldots, n)$ performs $U_i^{m_{i1}} \otimes U_i^{m_{i2}} \otimes \ldots \otimes U_i^{m_{iL}}$ on the ordered sequence V_{2i-1}^{i-1}, where $U_i = U = ZX$ and $(m_{i1}, m_{i2}, \ldots, m_{iL})$ is P_i's private bit string.

(Step 4) *Bell-state measurement*. P_0 measures the j-th $(j = 1, 2, \ldots, L)$ state of V_0^0 and the j-th one in quantum memory G_T^0 in the Bell basis, obtaining measurement results $(x_{01}y_{01}, x_{02}y_{02}, \ldots, x_{0L}y_{0L})$ in accordance with Equation (2). Similarly, P_i $(i = 1, 2, \ldots, n)$ measures the j-th state of V_{2i-1}^{i-1} and the j-th one of V_{2i}^i in the Bell basis, attaining measurement results $(x_{i1}y_{i1}, x_{i2}y_{i2}, \ldots, x_{iL}y_{iL})$. Finally, They announce the measurement results to P_0.

(Step 5) Correction and computation. Based on all the measurement results and the knowledge of original Bell states (only known to P_0), P_0 performs correcting operations on the j-th $(j = 1, 2, \ldots, L)$ state of V_{2n+1}^n. Next, P_0 measures these resulting states in the same basis as the original states in quantum memory G_T^0, gaining the measurement results $(t_1, t_2, \ldots, t_L)$. With these measurement results, P_0 compares the j-th state of V_{2n+1}^n with the j-th original state in quantum memory G_T^0. If these two states are the same (different), P_0 knows that the j-th bit of the sum is 0 (1). At last, P_0 can achieve the sum modulo 2 of participants' private bit strings, and the privacy of these private strings is preserved.

Note that, if the summation is only intended for a certain participant, say P_i, she can be selected as the one who distributes Bell states like TP. The process is analogous to that with TP if P_i is also assumed to be malicious, but non-collusive.

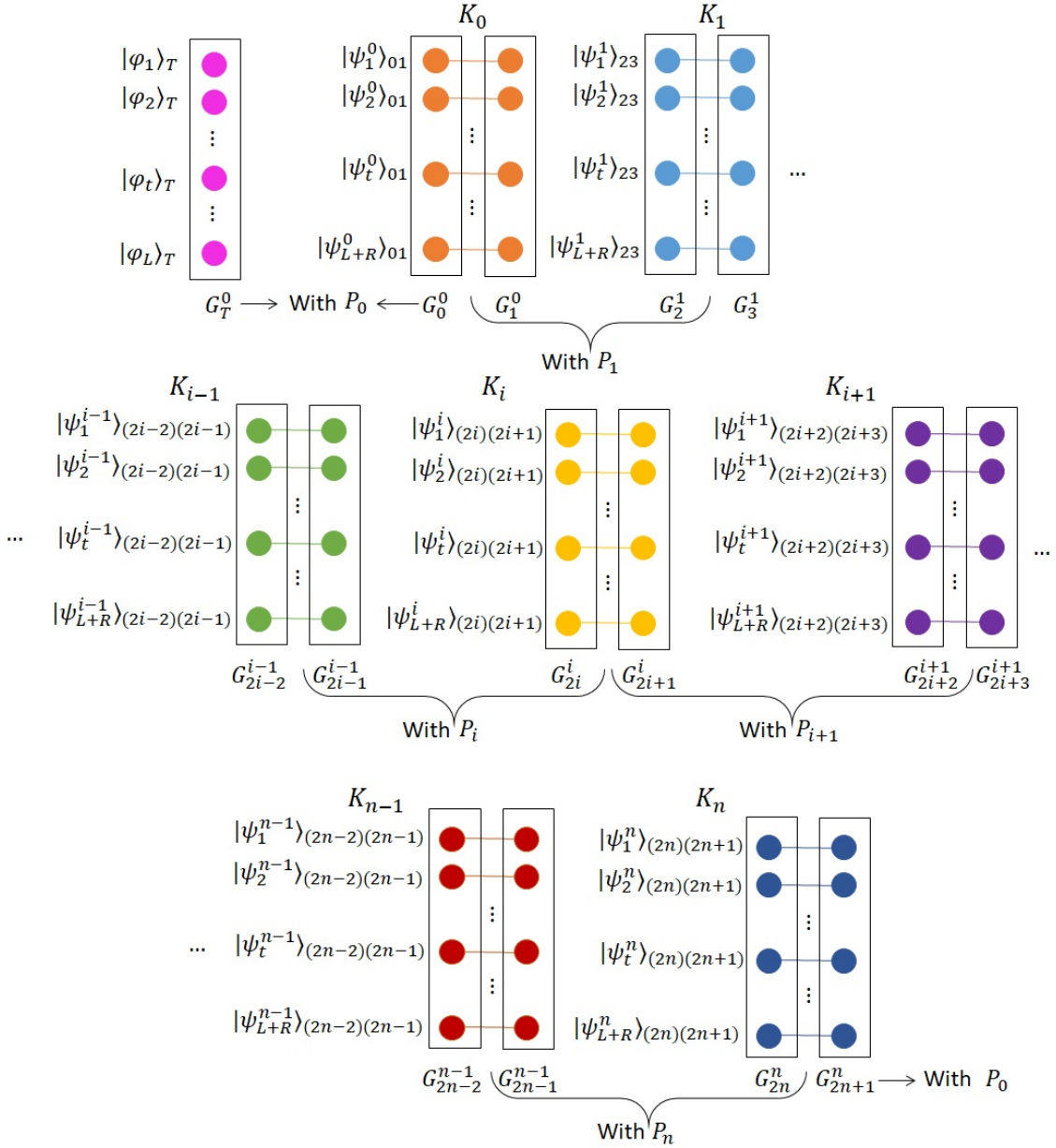

Figure 2. Entanglement distribution by P_0. Each player has a qubit which is entangled with another qubit held by the next user in the chain. At the start of the protocol, TP shares $L + R$ Bell states over each link, where R of which (randomly chosen) is used for detecting malicious activities.

4. Analysis of the Multi-Party Quantum Summation

In this section, we study the security of our protocol. It can be verified that the protocol would provide us with the correct sum if all parties follow the protocol. A detailed derivation of the correctness is given in Appendix A. In terms of security, we have to show that our protocol is secure against both outsider and participant attacks, and it fulfills the security and privacy requirements mentioned in Section 3. In our case, an outsider can potentially influence our protocol via the initial entanglement distribution. We show here how by using extra Bell states we can verify if the distributed states are genuinely Bell states. There also exist Trojan horse attacks [31–33], such as the delay-photon Trojan

horse attack and the invisible photon eavesdropping Trojan horse attack if quantum states are encoded and relayed in quantum communications protocols. Since our protocol uses Bell states to compute the summation and no encoded states are needed to be relayed, our protocol is secure against these attacks. We therefore focus here on the case of an attack by the TP, or possibly an outsider, and leave the details of the security against other malicious participants to Appendix A.

Attacks from P_0. We here consider the attacks from P_0 who cannot collude with any other participants. For simplicity, we suppose that P_0 wants to obtain one bit of P_i's ($i \neq 1, n$) private bit string and consider the chain related to this bit. In order to learn about this bit of P_i, P_0 has to find out if P_i performs quantum operation $U = ZX$ on her memory. P_0 can therefore launch entanglement swapping attack on this chain, as shown in Figure 3.

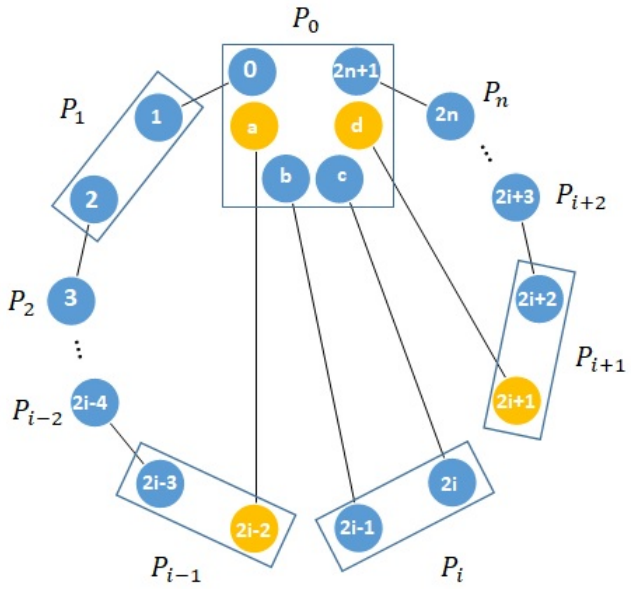

Figure 3. Entanglement swapping attack by P_0 through sharing entangled states in a dishonest way.

Suppose, in Figure 3, the states of quantum memories b and $(2i-1)$ and quantum memories c and $(2i)$ distributed by P_0 are $|B_{00}\rangle_{b(2i-1)}$ and $|B_{00}\rangle_{c(2i)}$, respectively. P_i will apply $U = ZX$ on quantum memory $(2i-1)$ if her secret bit is 1, otherwise she will do nothing. P_i then measures quantum memories $(2i-1)$ and $(2i)$ in the Bell basis and announces her measurement result $x_i y_i$ to P_0 as described in (Step 4) in the proposed protocol. After that, P_0 can measure quantum memories b and c as well and obtain the measurement result $x_c y_c$. Because the original states of quantum memories b and $(2i-1)$ and quantum memories c and $(2i)$ are the same, if $x_i y_i$ and $x_c y_c$ are the same, P_0 knows that P_i has not performed U on quantum memory $(2i-1)$ and learns about P_i's private bit being 0, according to the entanglement swapping property. Otherwise, P_0 concludes that P_i's private bit is 1. However, this attack will be detected in (Step 2) where the genuinity of Bell states shared between P_i and P_{i+1} (between P_{i-1} and P_i) is checked.

To show this note that Bell states can be rewritten in linear and diagonal bases as follows

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle), \tag{12}$$

$$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle), \tag{13}$$

$$|B_{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|++\rangle - |--\rangle), \tag{14}$$

$$|B_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|-+\rangle - |+-\rangle). \tag{15}$$

If P_i and P_{i+1} shared a known Bell state, and each one measures one component of the Bell state in the same basis (in the computational basis or in the diagonal basis), they will obtain a certain relationship between their measurement results. For a fake Bell state (the state of quantum memories $(2i-1)$ and $(2i-2)$ is not a Bell state, we call it a fake Bell state) used for detection, P_0 is able to pass the detection with probability of $\frac{1}{2}$. P_0 may distribute only one fake Bell state between P_i and P_{i+1} and another fake Bell state between P_{i-1} and P_i such that these two states are in the same chain to obtain P_i's private bit. At the same time, P_0 can get the maximum probability of passing the detection. In this case, these two states should not be chosen for detection. The probability of escaping the detection is $L^2/(L+R)^2$. For $i=1$ or $i=n$, this probability becomes $L/(L+R)$. These two probabilities of P_0 passing the detection and obtaining one bit of one participant will approach 0 if R is large enough. As a result, P_0 fails to steal participants' private input bits.

5. Practical Considerations

In this section, we discuss some practical aspects of our protocol in the light of new developments in the field. In general, secure multi-party quantum computation requires an infrastructure for reliable quantum communications as provided by quantum repeaters and quantum networks. Our protocol is not an exception, but given that some of the required resources for our protocol, as listed in Table 1, are easier to achieve, we can envisage a small-scale demonstration of this protocol in the near future. Multicore optical fibres [41,42] can be used to fish this task.

One of the key requirements in our scheme is to distribute Bell states between two parties. A full implementation of this aspect over any arbitrary distance is only possible with fully functional quantum repeaters. This may not be possible in the near future. But, a small-scale quantum network with nodes within tens of kilometers from each other is within reach. In fact, there are activities in Netherlands, for instance, to implement a four node quantum network within the country. Such a network can then be used for an initial demonstration of protocols like ours.

Another requirement of our system is that of quantum memories for storing and processing entangled states. In principle, we can run our protocol once all required entangled states are shared among users. This may increase the waiting time as well as the required storage/coherence time for memories. For a small-scale demonstration, with a few number of players at short distances from each other, this, can, however, be manageable. Quantum memories such as nitrogen vacancy centers in diamond [43] , or trapped ions [44,45], offer long storage times that could be suitable for our protocol. Plus, both these memories offer settings in which high-quality deterministic CNOT gates can be performed. The latter is necessary in order to keep our protocol loss resilient.

In terms of performance, there are two parameters that typically matter: at what rate, we can distribute entangled states among parties, and what would be the quality of the generated entangled state. The rate of entanglement generation is mainly affected by channel loss, but, for moderately short links, this may not be the major obstacle. For instance, if the maximum distance between two players is 50 km, for standard optical fiber channels with 0.2 dB/km loss, we have a channel transmissivity of 0.1. By accounting for a similar efficiency, for other parts of the system, we have a 1% chance in generating entangled states in every attempt. For a repetition rate of 1 M/s, we can then generate 10,000 entangled links per second, which should be sufficient for a small-scale demonstration. In terms of quality, in our analysis, we have assumed perfect Bell states can be exchanged among users. This is in principle possible if one can use entanglement distillation or error correction techniques. For a simple demonstration, however, it is more likely that we have to accept a bit of error in our system. This error rate would scale with the distance between the shared entangled state versus maximally entangled states, as well as with the number of players. One should also add to that the errors that might arise during the Bell-state measurements. In the end, if the error caused by imperfections in the system is too high, the protocol will abort during its verification stage.

One final note is about the number of Bell states that are needed for attack detection in our protocol. Here, in principle, we are using similar ideas as those used in quantum key distribution (QKD) for detecting eavesdroppers. But, unlike QKD, the ratio L/R, in our case, should be very low to keep the protocol secure. The main reason behind this is that in any quantum summation protocol, the protocol fails even if only one of the private bits gets revealed. That is, we have no chance to remove the information that has leaked to an eavesdropper once it has happened, whereas, in QKD, one can use privacy amplification to reduced the amount of leaked information about the final key. This seems to be a common issue in all quantum summation protocols and is not specific to our case.

6. Conclusions

We proposed a secure multi-party quantum summation protocol based on quantum teleportation, in which a TP, who could be malicious but non-collusive, was involved. The correctness and the security of the protocol were analyzed in detail. Our protocol did not require multi-partite entangled states. Only bipartite states (Bell states), Pauli operators and Bell measurement were needed in our protocol. The latter were all required in any teleportation protocol, which would be implicitly used in all other quantum summation protocols as well. By reducing the required resources to those needed for teleportation, we, in effect, proposed the most feasible quantum summation protocol, which could, in principle, be demonstrated, at small scales, using current quantum technologies. A more detailed error analysis is needed to account for the effect of imperfect entanglement distribution and/or operation errors. We will consider these imperfections in our future work.

Author Contributions: Investigation, C.Z. and Z.S.; methodology, C.Z.; writing—original draft preparation, C.Z. and Z.S.; writing—review and editing, M.R., Q.H. and H.S.

Funding: This work is supported by the National Natural Science Foundation of China (Grant Nos.11647140, 61602316, 61872152, 61502179), the Natural Science Foundation of Guangdong Province of China (Grant Nos. 2018A030310147, 2016A030310027, 2014A030310265), Guangdong Program for Special Support of Top-notch Young Professionals (No. 2015TQ01X796), Pearl River Nova Program of Guangzhou (No. 201610010037), the Science and Technology Innovation Projects of Shenzhen (No. JCYJ20170818140234295), and the CICAEET fund and the PAPD fund (No. KJR1615). Mohsen Razavi acknowledges the support of UK EPSRC Grant EP/M013472/1. Cai Zhang is sponsored by the State Scholarship Fund of the China Scholarship Council. All data generated in this paper can be reproduced by the provided methodology.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Analysis of the Multi-Party Quantum Summation

Appendix A.1. Correctness Analysis

We assume that all participants provide correct private bit strings. For the convenience of analyzing the correctness of our protocol, we define the relationship between quantum states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and classical bits as follows:

$$E(|\varphi\rangle) = \begin{cases} 0, \ if \ |\varphi\rangle \in \{|0\rangle, |+\rangle\}, \\ 1, \ if \ |\varphi\rangle \in \{|1\rangle, |-\rangle\}. \end{cases} \tag{A1}$$

Furthermore, if

$$|\varphi'\rangle = U^m|\varphi\rangle, \tag{A2}$$

where $m \in \{0,1\}$, $|\varphi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, $U = ZX$ and a global phase is ignored, then

$$E(|\varphi'\rangle) = E(|\varphi\rangle) \oplus m. \tag{A3}$$

In (Step 3) of the protocol, V_{2i}^i and V_{2i+1}^i $(i = 0, 1, \ldots, n)$ form L ordered Bell states. V_0^0 and V_{2n+1}^n are held by P_0 and V_{2i-1}^{i-1} and V_{2i}^i $(i = 1, 2, \ldots, n)$ are in P_i's hands. For the j-th $(j = 1, 2, \ldots, L)$ Bell state between V_{2i}^i and $V_{2i+1}^i (i = 0, 1, \ldots, n)$, combining with the j-th state in quantum memory G_T^0, the initial state is

$$|\zeta_j^0\rangle = |\varphi_j\rangle_T \otimes |\psi'^0_j\rangle_{01} \otimes |\psi'^1_j\rangle_{23} \otimes \ldots \otimes |\psi'^n_j\rangle_{(2n)(2n+1)}. \tag{A4}$$

Suppose that

$$|\psi'^0_j\rangle_{01} = |B_{a_0b_0}\rangle^j_{01}, \tag{A5}$$
$$|\psi'^1_j\rangle_{23} = |B_{a_1b_1}\rangle^j_{23}, \tag{A6}$$
$$\ldots, \tag{A7}$$
$$|\psi'^n_j\rangle_{(2n)(2n+1)} = |B_{a_nb_n}\rangle^j_{(2n)(2n+1)}, \tag{A8}$$

and P_i $(i = 1, 2, \ldots, n)$ performs $U_i^{m_{ij}}$ $(U_i = U = ZX)$ on the j-th state of V^{i-1}_{2i-1}, the state becomes

$$\begin{aligned} |\zeta_j^1\rangle = \; & \tfrac{1}{2^{n+1}} \textstyle\sum_{x_{0j}\in\{0,1\}} \sum_{y_{0j}\in\{0,1\}} \sum_{x_{1j}\in\{0,1\}} \sum_{y_{1j}\in\{0,1\}} \cdots \sum_{x_{nj}\in\{0,1\}} \sum_{y_{nj}\in\{0,1\}} \\ & (-1)^{\Sigma_{i=0}^n x_{ij}\cdot b_i} \quad |B_{x_{0j}y_{0j}}\rangle^j_{T0} \otimes |B_{x_{1j}y_{1j}}\rangle^j_{12} \otimes \ldots \otimes |B_{x_{nj}y_{nj}}\rangle^j_{(2n-1)(2n)} \\ & \otimes Z^{\oplus\Sigma_{i=0}^n b_i \oplus y_{ij}} \quad X^{\oplus\Sigma_{i=0}^n a_i \oplus x_{ij}} U^{\oplus\Sigma_{i=1}^n m_{ij}} |\varphi_j\rangle_{2n+1}, \end{aligned} \tag{A9}$$

according to Equations (3)–(8), and a global phase of the state of quantum memory $(2n + 1)$ is ignored.

After P_i $(i = 0, 1, \ldots, n)$ measures the corresponding states in the Bell basis, obtaining the measurement outcome $x_{ij}y_{ij}$ $(j = 1, 2, \ldots, L)$, the state of quantum memory $(2n + 1)$ collapses to

$$Z^{\oplus\Sigma_{i=0}^n b_i \oplus y_{ij}} X^{\oplus\Sigma_{i=0}^n a_i \oplus x_{ij}} U^{\oplus\Sigma_{i=1}^n m_{ij}} |\varphi_j\rangle_{2n+1}. \tag{A10}$$

With the announcement of $x_{ij}y_{ij}$ $(i = 1, 2, \ldots, n)$ provided by P_i, P_0 knowing the initial Bell states can calculate

$$\oplus \textstyle\sum_{i=0}^n \quad a_i \oplus x_{ij}, \tag{A11}$$
$$\oplus \textstyle\sum_{i=0}^n \quad b_i \oplus y_{ij}. \tag{A12}$$

Later, $X^{\oplus\Sigma_{i=0}^n a_i \oplus x_{ij}} Z^{\oplus\Sigma_{i=0}^n b_i \oplus y_{ij}}$ is performed on quantum memory $(2n + 1)$. Consequently, the state of quantum memory $(2n + 1)$ turns into

$$|\varphi'_j\rangle_{2n+1} = U^{\oplus\Sigma_{i=1}^n m_{ij}} |\varphi_j\rangle_{2n+1}. \tag{A13}$$

After the measurement of quantum memory $(2n + 1)$ in the same basis as that of quantum memory T, P_0 gains

$$E(|\varphi_j\rangle_T) \oplus (\oplus\Sigma_{i=1}^n m_{ij}) = E(|\varphi'_j\rangle_{2n+1}), \tag{A14}$$

and therefore obtains the result

$$\oplus\, \Sigma_{i=1}^n m_{ij} = E(|\varphi_j\rangle_T) \oplus E(|\varphi'_j\rangle_{2n+1}), \tag{A15}$$

for the j-th bit of the sum modulo 2 of participants' private bit strings, by using Equations (A1)–(A3). In the end, P_0 is able to learn about the sum modulo 2 of participants' private bit strings.

Appendix A.2. Security Analysis

There exist two types of participant attacks, one from TP(P_0) and the other from some dishonest participants. We showed earlier how our protocol is secure against attacks by TP. Here we demonstrate how our protocol can be kept secure in the presence of malicious participants. Note that $n - 1$ dishonest participants can easily steal the honest participant's private bit string if the summation is revealed in

public. But if the summation is kept secret in TP's hands, $n-1$ dishonest participant cannot obtain anything about the honest participant's private input. Here, we show that our protocol is secure against the collusive attack of $n-2$ dishonest participants, which is the maximum possible in this case.

Attacks from $(n-2)$ dishonest participants (not including P_0). If $(n-2)$ dishonest participants wish to steal the other two honest participants' private bit strings M_p and M_q $(p<q)$, they may employ the states in their hands to get useful information. We consider the j-th bit $(j=1,2,\ldots,L)$ in M_p and M_q and the corresponding states.

For $q \neq p+1$, we first show how dishonest participants try to learn about m_{pj}, as shown in Figure A1. In this case, P_{p+1} does not apply unitary operation on quantum memory $(2p+1)$ and Bell-state measurement on quantum memories $(2p+1)$ and $(2p+2)$. After the private input encoding stage (Step 3), the state of quantum memory T and quantum memories $0 \sim (2p+1)$ will be

$$\begin{aligned} |\zeta_j^1\rangle = \quad & \tfrac{1}{2^p}\textstyle\sum_{x_0\in\{0,1\}} \quad \sum_{y_0\in\{0,1\}}\sum_{x_1\in\{0,1\}}\sum_{y_1\in\{0,1\}}\cdots\sum_{x_p\in\{0,1\}}\sum_{y_p\in\{0,1\}} \\ & (-1)^{\Sigma_{k=0}^{p} x_k\cdot b_k} \quad |B_{x_0y_0}\rangle_{T0}^{j}\otimes|B_{x_1y_1}\rangle_{12}^{j}\otimes\ldots\otimes|B_{x_py_p}\rangle_{(2p-1)(2p)}^{j} \\ & \otimes Z^{\oplus\Sigma_{k=0}^{p} b_k\oplus y_k} \quad X^{\oplus\Sigma_{k=0}^{p} a_k\oplus x_k}U^{\oplus\Sigma_{k=1}^{p} m_{kj}}|\varphi_j\rangle_{2p+1}, \end{aligned} \tag{A16}$$

where the j-th state in quantum memory T is $|\varphi_j\rangle_T$ and the j-th Bell state shared between P_s and P_{s+1} $(s=0,1,\ldots,p)$ is $|B_{a_sb_s}\rangle_{(2s)(2s+1)}^{j}$. The dishonest participants try to get m_{pj} from quantum memory $(2p+1)$. However, they will fail.

From Equation (A16), we can see that if P_{p+1} knows m_{sj} $(s=1,2,\ldots,p-1)$, the basis of $|\varphi_j\rangle_T$ and (a_r,b_r) $(r=0,1,\ldots,p)$ (the information about the initial Bell states), she can first apply the right correction on quantum memory $(2p+1)$ and measure it in the right basis. According to m_{sj} $(s=1,2,\ldots,p-1)$, she can then obtain m_{pj}. But she cannot do that. Even though P_{p+1} knows m_{sj} $(s=0,1,\ldots,p-1)$ with the assistance of P_s and the measurement results $(x_0y_0,x_1y_1,\ldots,x_py_p)$, she knows nothing about the basis of $|\varphi_j\rangle_T$ and (a_r,b_r) that are kept secret by P_0. Thus, she cannot perform the right correction on quantum memory $(2p+1)$ and measure it in the right basis. Finally, she fails to obtain m_{pj}, let alone M_p. Similarly, they cannot learn about M_q.

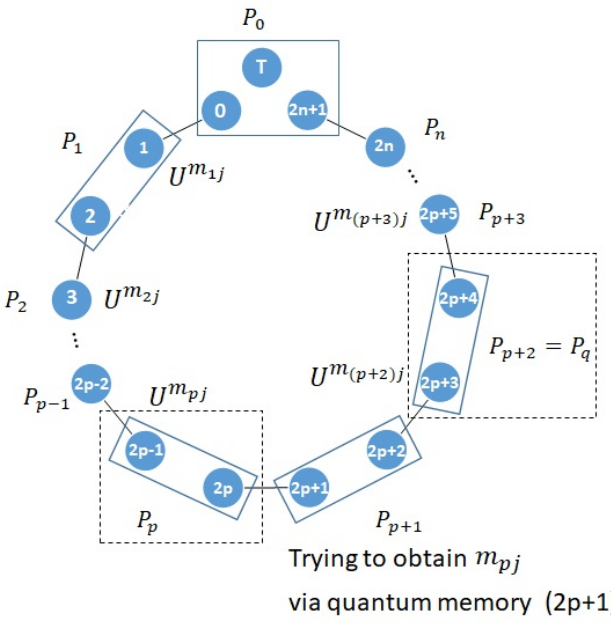

Figure A1. Attack by $(n-2)$ participants, where P_p and P_q are honest participants.

For $q = p + 1$, they may use a similar method as in the above case to take M_p and M_q. Namely, P_{p+2} does nothing on quantum memory $(2p + 3)$ and skips Bell-state measurement on the corresponding state. In this case. the dishonest participants cannot even get the $m_{pj} \oplus m_{(p+1)j}$. Therefore, the privacy of M_p and M_q is preserved.

For any two Bell states $|B_{xy}\rangle_{12}$ and $|B_{ab}\rangle_{34}$, if quantum memories 2 and 3 are measured in the Bell basis and the measurement outcome $|B_{km}\rangle_{23}$ is obtained, the state of quantum memories 1 and 4 then collapses to $|B_{xy\oplus ab\oplus km}\rangle_{14}$ due to the Bell entanglement swapping property.

The dishonest participants may also start an attack based on the entanglement swapping property. For the case of $q \neq p + 1$, as shown in the dash box in Figure A2, the j-th Bell state shared between P_{p-1} and P_p and that shared between P_p and P_{p+1} are $|B_{a_{p-1}b_{p-1}}\rangle^j_{(2p-2)(2p-1)}$ and $|B_{a_pb_p}\rangle^j_{(2p)(2p+1)}$, respectively. After P_p performs $U_p^{m_{pj}}(U_p = ZX)$ on quantum memory $(2p - 1)$ and then measures quantum memories $(2p - 1)$ and $(2p)$ in the Bell basis, obtaining the measurement outcome $|B_{x_py_p}\rangle^j_{(2p-1)(2p)}$, the state of quantum memories $(2p - 2)$ and $(2p + 1)$ becomes

$$(I \otimes U_p^{m_{pj}})|B_{(a_{p-1}b_{p-1})\oplus(a_pb_p)\oplus(x_py_p)}\rangle^j_{(2p-2)(2p+1)}, \tag{A17}$$

due to the property of entanglement swapping. P_{p+1} skips the private input encoding stage, instead she can collaborate with P_{p-1} to measure quantum memories $(2p - 2)$ and $(2p + 1)$ in the Bell basis. Can the dishonest participants find out $U_p^{m_{pj}}$ performed by P_p to steal m_{pj}? The answer is no. Although P_{p-1} and P_{p+1} can measure quantum memories $(2p - 2)$ and $(2p + 1)$ in the Bell basis and get x_py_p after P_p's announcement, they have to know $a_{p-1}b_{p-1}$ and a_pb_p to derive $U_p^{m_{pj}}$, but this information is unknown to them. For the case of $q = p + 1$, the analysis is similar. Therefore, this attack is also invalid to our protocol.

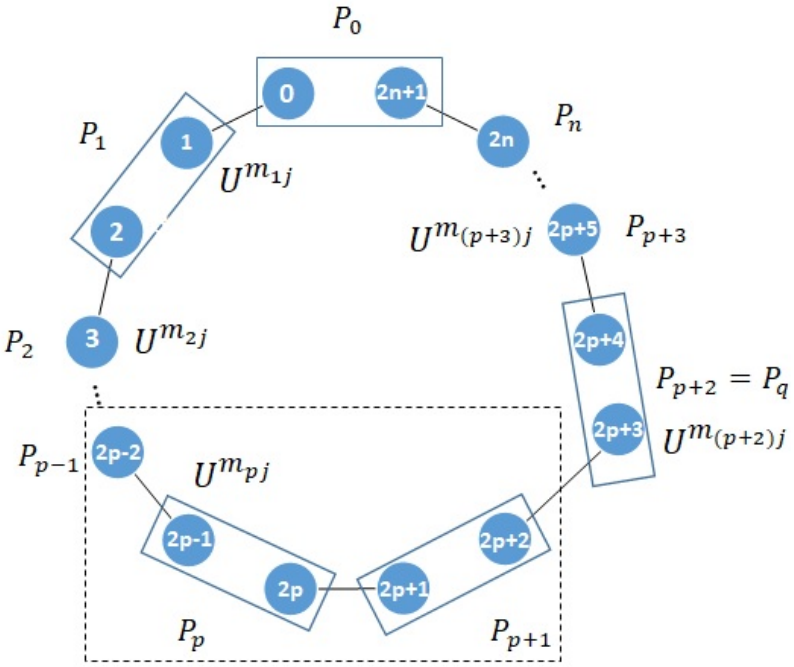

Figure A2. Entanglement swapping attack by $(n - 2)$ participants, where P_p and P_q are honest participants.

References

1. Halevi, S.; Ishai, Y.; Jain, A.; Kushilevitz, E.; Rabin, T. Secure multiparty computation with general interaction patterns. In Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science, Cambridge, MA, USA, 14–17 January 2016; pp. 157–168.
2. Baum, C.; Damgård, I.; Toft, T.; Zakarias, R. Better preprocessing for secure multiparty computation. In Proceedings of the International Conference on Applied Cryptography and Network Security, London, UK, 19–22 June 2016; pp. 327–345.
3. Ben-Efraim, A.; Lindell, Y.; Omri, E. Optimizing semi-honest secure multiparty computation for the internet. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 578–590.
4. Keller, M.; Yanai, A. Efficient maliciously secure multiparty computation for RAM. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, 29 April–3 May 2018; pp. 91–124.
5. Yao, A.C. Protocols for secure computations. In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), Chicago, IL, USA, 3–5 November 1982; pp. 160–164.
6. Goldreich, O.; Micali, S.; Wigderson, A. How to play any mental game. In Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing, New York, NY, USA, 25–27 May 1987; pp. 218–229.
7. Lo, H.K. Insecurity of quantum secure computations. *Phys. Rev. A* **1997**, *56*, 1154–1162. [CrossRef]
8. Crépeau, C.; Gottesman, D.; Smith, A. Secure multi-party quantum computation. In Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing, Montreal, QC, Canada, 19–21 May 2002; pp. 643–652.
9. Chau, H.F. Quantum-classical complexity-security tradeoff in secure multiparty computations. *Phys. Rev. A* **2000**, *61*, 032308. [CrossRef]
10. Ben-Or, M.; Crepeau, C.; Gottesman, D.; Hassidim, A.; Smith, A. Secure multiparty quantum computation with (only) a strict honest majority. In Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06), Berkeley, CA, USA, 21–24 October 2006; pp. 249–260.
11. Smith, A. Multi-party Quantum Computation. *arXiv* **2010**, arXiv:quant-ph/0111030.
12. Heinrich, S. Quantum summation with an application to integration. *J. Complex.* **2002**, *18*, 1–50. [CrossRef]
13. Heinrich, S.; Novak, E. On a problem in quantum summation. *J. Complex.* **2003**, *19*, 1–18. [CrossRef]
14. Heinrich, S.; Kwas, M.; Wozniakowski, H. Quantum Boolean Summation with Repetitions in the Worst-Average Setting. *arXiv* **2003**, arXiv:quant-ph/0311036.
15. Du, J.Z.; Chen, X.B.; Wen, Q.Y.; Zhu, F.C. Secure multiparty quantum summation. *Acta Phys. Sin.* **2007**, *56*, 6214.
16. Chen, X.B.; Xu, G.; Yang, Y.X.; Wen, Q.Y. An efficient protocol for the secure multi-party quantum summation. *Int. J. Theor. Phy.* **2010**, *49*, 2793–2804. [CrossRef]
17. Hillery, M.; Ziman, M.; Bužek, V.; Bieliková, M. Towards quantum-based privacy and voting. *Phys. Lett. A* **2006**, *349*, 75–81. [CrossRef]
18. Li, Y.; Zeng, G. Quantum anonymous voting systems based on entangled state. *Opt. Rev.* **2008**, *15*, 219–223. [CrossRef]
19. Wang, Q.; Yu, C.; Gao, F.; Qi, H.; Wen, Q. Self-tallying quantum anonymous voting. *Phys. Rev. A* **2016**, *94*, 022333. [CrossRef]
20. Xue, P.; Zhang, X. A simple quantum voting scheme with multi-qubit entanglement. *Sci. Rep.* **2017**, *7*, 7586. [CrossRef] [PubMed]
21. Bao, N.; Halpern, N.Y. Quantum voting and violation of Arrow's impossibility theorem. *Phys. Rev. A* **2017**, *95*, 062306. [CrossRef]
22. Sun, Z.; Yu, J.; Wang, P.; Xu, L.; Wu, C. Quantum private comparison with a malicious third party. *Quantum Inf. Process.* **2015**, *14*, 2125–2133. [CrossRef]
23. 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.* **2017**, *16*, 36. [CrossRef]
24. He, G.P. Quantum private comparison protocol without a third party. *Int. J. Quantum Inf.* **2017**, *15*, 1750014. [CrossRef]

25. 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.* **2014**, *53*, 933–941. [CrossRef]
26. Zhang, C.; Sun, Z.W.; Huang, X.; Long, D.Y. Three-party quantum summation without a trusted third party. *Int. J. Quantum Inf.* **2015**, *13*, 1550011. [CrossRef]
27. Shi, R.H.; Mu, Y.; Zhong, H.; Cui, J.; Zhang, S. Secure multiparty quantum computation for summation and multiplication. *Sci. Rep.* **2016**, *6*, 19655. [CrossRef]
28. Shi, R.H.; Zhang, S. Quantum solution to a class of two-party private summation problems. *Quantum Inf. Process.* **2017**, *16*, 225. [CrossRef]
29. 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.* **2017**, 1750010. [CrossRef]
30. 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.* **2017**, *56*, 2783–2791. [CrossRef]
31. 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* **2005**, *72*, 044302. [CrossRef]
32. Gisin, N.; Fasel, S.; Kraus, B.; Zbinden, H.; Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **2006**, *73*, 022320. [CrossRef]
33. 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* **2006**, *74*, 054302. [CrossRef]
34. Yang, H.Y.; Ye, T.Y. Secure multi-party quantum summation based on quantum Fourier transform. *Quantum Inf. Process.* **2018**, *17*, 129. [CrossRef]
35. Bennett, C.H.; Brassard, G.; Crépeau, C.; Jozsa, R.; Peres, A.; Wootters, W.K. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **1993**, *70*, 1895. [CrossRef]
36. Sangouard, N.; Simon, C.; de Riedmatten, H.; Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **2011**, *83*, 33–80. [CrossRef]
37. Razavi, M.; Shapiro, J.H. Nonadiabatic approach to entanglement distribution over long distances. *Phys. Rev. A* **2007**, *75*, 032318. [CrossRef]
38. Amirloo, J.; Razavi, M.; Majedi, A.H. Quantum key distribution over probabilistic quantum repeaters. *Phys. Rev. A* **2010**, *82*, 032304. [CrossRef]
39. Lo Piparo, N.; Razavi, M. Long-distance quantum key distribution with imperfect devices. *Phys. Rev. A* **2013**, *88*, 012332. [CrossRef]
40. Bruschi, D.E.; Barlow, T.M.; Razavi, M.; Beige, A. Repeat-until-success quantum repeaters. *Phys. Rev. A* **2014**, *90*, 032306. [CrossRef]
41. Bacco, D.; Ding, Y.; Dalgaard, K.; Rottwitt, K.; Oxenløwe, L.K. Space division multiplexing chip-to-chip quantum key distribution. *Sci. Rep.* **2017**, *7*, 12459. [CrossRef] [PubMed]
42. Eriksson, T.A.; Hirano, T.; Puttnam, B.J.; Rademacher, G.; Luís, R.S.; Fujiwara, M.; Namiki, R.; Awaji, Y.; Takeoka, M.; Wada, N.; et al. Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels. *Commun. Phys.* **2019**, *2*, 9. [CrossRef]
43. Kalb, N.; Reiserer, A.A.; Humphreys, P.C.; Bakermans, J.J.W.; Kamerling, S.J.; Nickerson, N.H.; Benjam S.C.; Twitchen, D.J.; Markham, M.; Hanson, R. Entanglement Distillation between Solid-State Quantum Network Nodes. *Science* **2017**, *356*, 928. [CrossRef]
44. Moehring, D.L.; Maunz, P.; Olmschenk, S.; Younge, K.C.; Matsukevich, D.N.; Duan, L.M.; Monroe, C. Entanglement of single-atom quantum bits at a distance. *Nature* **2007**, *449*, 68–71. [CrossRef] [PubMed]
45. Schäfer, V.M.; Ballance, C.J.; Thirumalai, K.; Thirumalai, L.J.; Ballance, T.G.; Steane, A.M.; Lucas D.M. Fast quantum logic gates with trapped-ion qubits. *Nature* **2018**, *555*, 75–78.