A lightweight three-user secure quantum summation protocol without a third party based on single-particle states

Tian-Yu Ye[1] · **Tian-Jie Xu[1]**

Abstract

In this paper, a lightweight three-user secure quantum summation protocol is put forward by using single-particle states, which can accomplish the goal that three users cooperate together to calculate the modulo 2 addition of their private messages without the help of a third party. This protocol only requires single-particle states rather than quantum entangled states as the initial quantum resource and only needs single-particle measurements and Bell basis measurements. This protocol needs none of quantum entanglement swapping, the Pauli operations, the controlled-not (CNOT) operation, the Hadamard gate or a pre-shared private key sequence. Security analysis proves that this protocol is secure against both the outside attacks and the participant attacks. Compared with the existing two-dimensional three-user quantum summation protocols, this protocol more or less takes advantage over them on the aspects of the initial quantum resource, users' quantum measurement, the usage of quantum entanglement swapping, the usage of Pauli operations, the usage of CNOT operation or the usage of Hadamard gate.

Keywords Quantum summation · Single-particle state · Outside attack · Participant attack

1 Introduction

It is popularly accepted that secure quantum summation is one of the most fundamental branches of quantum secure computation. For example, it may be used in various scenarios such as quantum anonymous voting [1], quantum private comparison [2],

---

✉ Tian-Yu Ye
happyyty@aliyun.com

[1] College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, P. R. China

and quantum key agreement [3], and so on. The task of secure quantum summation is to ensure the correctness of summation result and avoid the leakage of private inputs. In recent years, secure quantum summation has naturally gained more and more interest because of its importance. In the year of 2002, Heinrich started the research of quantum summation and applied it to integration [4]. Later, he also investigated quantum Boolean summation with repetitions in the case of worst-average setting [5]. So far, numerous quantum summation protocols [1, 6–25] have been constructed from different viewpoints. According to the dimension of quantum system applied, they can be classified into two kinds: two-dimensional quantum summation protocols [6–12] and high-dimensional quantum summation protocols [1, 12–25]. Among the two-dimensional quantum summation protocols [6–12], someones have a third party, but others have none. Among the two-dimensional three-user quantum summation protocols [6, 8, 9, 11, 12], the protocols in Refs. [6, 8, 11, 12] need to employ quantum entangled states as the initial quantum resource, which are more difficult to prepare than single-particle states in practice; the protocol of Ref. [8] needs to perform the $\left\{\gamma_j^1 | j = 1, 2, \ldots, 8\right\}$ basis measurements and the $\left\{\gamma_j^2 | j = 1, 2, \ldots, 8\right\}$ basis measurements, which are much more difficult to realize than the $\{|0\rangle, |1\rangle\}$ basis measurements and the Bell basis measurements; the protocol of Ref. [6] needs quantum entanglement swapping; the protocols of Refs. [6, 11, 12] require the Pauli operations; the protocol of Ref. [9] needs the controlled-not (CNOT) operation; and the protocols of Refs. [9, 11] require the Hadamard gate. Apparently, as for a quantum communication protocol, if the burdens of the initial quantum resource, the quantum measurement and the auxiliary quantum gates are alleviated, its practical implementation feasibility may be greatly improved.

Based on the above analysis, this paper is devoted to designing a lightweight three-user secure quantum summation protocol without a third party by using single-particle states as the initial quantum resource, where three users can cooperate together to calculate the modulo 2 addition of their private messages by themselves. This protocol more or less has better performance than the previous two-dimensional three-user quantum summation protocols of Refs. [6, 8, 9, 11, 12] on the aspects of the initial quantum resource, users' quantum measurement, the usage of quantum entanglement swapping, the usage of Pauli operations, the usage of CNOT operation or the usage of Hadamard gate.

2 Preliminary knowledge

The four Bell states can be depicted as

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

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

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|+\rangle|+\rangle - |-\rangle|-\rangle), \tag{3}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|+\rangle|-\rangle - |-\rangle|+\rangle), \tag{4}$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. It can be easily derived from Eqs. (1–4) that

$$|0\rangle|0\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle), \tag{5}$$

$$|0\rangle|1\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\psi^-\rangle), \tag{6}$$

$$|1\rangle|0\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle - |\psi^-\rangle), \tag{7}$$

$$|1\rangle|1\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\phi^-\rangle), \tag{8}$$

$$|+\rangle|+\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\psi^+\rangle), \tag{9}$$

$$|+\rangle|-\rangle = \frac{1}{\sqrt{2}}(|\phi^-\rangle + |\psi^-\rangle), \tag{10}$$

$$|-\rangle|+\rangle = \frac{1}{\sqrt{2}}(|\phi^-\rangle - |\psi^-\rangle), \tag{11}$$

$$|-\rangle|-\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\psi^+\rangle) \tag{12}$$

3 The proposed three- user secure quantum summation protocol

Assume that Alice, Bob and Charlie's private messages are $X = (x_1, x_2, \ldots, x_n)$, $Y = (y_1, y_2, \ldots, y_n)$ and $Z = (z_1, z_2, \ldots, z_n)$, respectively, where $x_i, y_i, z_i \in \{0, 1\}$, $i = 1, 2, \ldots, n$. They wish to calculate the modulo 2 addition of X, Y and Z, i.e., $X \oplus Y \oplus Z = (x_1 \oplus y_1 \oplus z_1, x_2 \oplus y_2 \oplus z_2, \ldots, x_n \oplus y_n \oplus z_n)$, where $\oplus$ denotes the modulo 2 addition. We construct the following three-user secure quantum summation protocol to finish this task.

Step 1 Bob produces a single-particle sequence $S_B = \{B_1, B_2, \ldots, B_{8(n+\delta)}\}$, where B_j is randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, $j = 1, 2, \ldots, 8(n+\delta)$ and δ is a positive parameter. Afterward, Bob generates γ_b decoy photons for checking the existence of an outside eavesdropper, each of which is also randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and randomly inserts them into S_B to form the new sequence S_B'. Here, γ_b is a positive integer. Finally, Bob sends S_B' to Alice the block transmission technology, which was invented by Ref.[26].

At the same time, Charlie prepares a single-particle sequence $S_C = \{C_1, C_2, \ldots, C_{8(n+\delta)}\}$, where C_j is also randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and $j = 1, 2, \ldots, 8(n+\delta)$. Afterward, in order to check the

existence of an outside eavesdropper, Charlie produces γ_c decoy photons, each of which is also randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and randomly mixes them with S_C to compose the new sequence S_C'. Here, γ_c is a positive integer. Finally, Charlie transmits S_C' to Alice in the manner of block transmission [26].

Step 2 Bob works together with Alice to check the existence of an outside eavesdropper as follows: (1) Bob announces Alice the positions and the preparing bases of decoy photons in S_B'; (2) Alice uses Bob's preparing bases to measure the corresponding decoy photons and informs Bob of her measurement outcomes; (3) Bob checks whether there exists an outside eavesdropper or not by judging the consistency between the initial states of decoy photons and Alice's measurement outcomes. If there exists no outside eavesdropper, the communication will be kept on; otherwise, the communication will be stopped.

In the meanwhile, Charlie also works together with Alice to check the existence of an outside eavesdropper by using the same approach as above.

Step 3 Alice makes the j th particle of S_B and the j th particle of S_C compose the jth particle pair, where $j = 1, 2, \ldots, 8(n + \delta)$. Bob and Charlie ask Alice to perform the Bell basis measurement on each particle pair. Then, Alice measures each particle pair with the Bell basis. When her measurement result is $|\phi^+\rangle$ or $|\psi^-\rangle$, she publishes it directly; and when her measurement result is $|\phi^-\rangle$ or $|\psi^+\rangle$, she publishes 'summation'. Afterward, Bob and Charlie use the measurement results of the particle pairs, each of which has two particles originally prepared in the $\{|+\rangle, |-\rangle\}$ basis, to evaluate Alice's honesty as follows: ① when Alice's measurement result is $|\phi^+\rangle$ or $|\psi^-\rangle$, they check whether Alice's measurement result satisfies Eqs. (9–12) or not. If Alice is distrustful, they will stop the communication; otherwise, they will continue the communication; ② they check the times that Alice published 'summation'. Note that for the particle pairs, each of which has two particles originally prepared in the $\{|+\rangle, |-\rangle\}$ basis, the times that Alice published 'summation' should be approximately $n + \delta$. If it is abnormally high, they will stop the communication; otherwise, they will continue the communication.

Step 4 Among the remaining particle pairs, the number of particle pairs, each of which has two particles originally prepared in the $\{|0\rangle, |1\rangle\}$ basis, is approximately $2(n + \delta)$. For convenience, among these particle pairs, the ones where Alice published 'summation' are named as message particle pairs. Note the number of message particle pairs is approximately $(n + \delta)$. Bob and Charlie check whether the number of message particle pairs is less than n or not. If this is true, they will stop the communication; otherwise, they will continue the communication.

Step 5 Bob and Charlie choose the first n message particle pairs to calculate the summation and inform Alice of their positions. Afterward, Alice, Bob and Charlie derive their one-time pad keys $KA = (ka_1, ka_2, \ldots, ka_n), KB = (kb_1, kb_2, \ldots, kb_n)$ and $KC = (kc_1, kc_2, \ldots, kc_n)$ from these n chosen message particle pairs, respectively. When Alice's measurement result on the i th particle pair is $|\phi^-\rangle$, then $ka_i = 0$; and when it is $|\psi^+\rangle$, then $ka_i = 1$. When the original prepared state of Bob's particle in the i th particle pair is $|0\rangle$, then $kb_i = 0$; and when it is $|1\rangle$, then $kb_i = 1$. Similarly, when the original prepared state of Charlie's particle in the i th particle pair is $|0\rangle$, then $kc_i = 0$; and when it is $|1\rangle$, then $kc_i = 1$. Here, $i = 1, 2, \ldots, n$. Then,

Alice, Bob and Charlie obtain $SA = (sa_1, sa_2, \ldots, sa_n)$, $SB = (sb_1, sb_2, \ldots, sb_n)$ and $SC = (sc_1, sc_2, \ldots, sc_n)$ by computing $sa_i = ka_i \oplus x_i$, $sb_i = kb_i \oplus y_i$ and $sc_i = kc_i \oplus z_i$, respectively, $i = 1, 2, \ldots, n$. Subsequently, Alice, Bob and Charlie publish SA, SB and SC, respectively. Finally, each of Alice, Bob and Charlie calculates $sum_i = sa_i \oplus sb_i \oplus sc_i$ for $i = 1, 2, \ldots, n$ to get the whole summation result $Sum = (sum_1, sum_2, \ldots, sum_n)$.

4 Correctness analysis

In this protocol, Alice, Bob and Charlie utilize the first n message particle pairs to calculate the summation of X, Y and Z. Obviously, it can be derived that

$$ka_i \oplus kb_i \oplus kc_i = 0, \tag{13}$$

where $i = 1, 2, \ldots, n$. After Alice, Bob and Charlie publish SA, SB and SC, respectively, each of them calculates

$$sum_i = sa_i \oplus sb_i \oplus sc_i$$

$$= (ka_i \oplus x_i) \oplus (kb_i \oplus y_i) \oplus (kc_i \oplus z_i)$$

$$= (ka_i \oplus kb_i \oplus kc_i) \oplus (x_i \oplus y_i \oplus z_i) \tag{14}$$

According to Eq. (13), it can be obtained from Eq. (14) that

$$sum_i = x_i \oplus y_i \oplus z_i \tag{15}$$

It can be concluded that the correctness of summation result of this protocol can be guaranteed.

5 Security analysis

5.1 The outside attack

Apparently, the transmission of S'_B from Bob to Alice is dependent from that of S'_C from Charlie to Alice. Without loss of generality, here only analyze the security of the transmission of S'_B against an outside eavesdropper Eve.

(1) The Trojan horse attacks

The Trojan horse attacks mainly refer to the invisible photon eavesdropping attack [27] and the delay-photon Trojan horse attack [28, 29]. As the particles of S'_B only undergo the one-way transmission, this protocol can naturally prevent the Trojan horse attacks from Eve.

(2) The measure-resend attack

As Eve is unknown about the positions of decoy photons, in order to try to get Bob's one-time pad key, after intercepting S'_B sent out from Bob, Eve has to measure all of its particles with the $\{|0\rangle, |1\rangle\}$ basis and send the fresh ones in the same states as found to Alice. As for one decoy photon, if it is in the $\{|0\rangle, |1\rangle\}$ basis, Eve's attack will incur no error; and if it is in the $\{|+\rangle, |-\rangle\}$ basis, Eve's attack will be detected with the probability of $\frac{1}{2}$; in conclusion, the probability that Eve's attack can be detected is $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$. For γ_b decoy photons, Eve's attack will be detected with the probability of $1 - \left(\frac{3}{4}\right)^{\gamma_b}$, which will converge to 1 if γ_b is big enough.

(3) The intercept-resend attack

As Eve has no access to the positions of decoy photons, in order to try to get Bob's one-time pad key, after intercepting S'_B sent out from Bob, Eve has to substitute all of its particles with the fake ones she generated beforehand randomly in the $\{|0\rangle, |1\rangle\}$ basis and send them to Alice. As for one decoy photon, if it is in the $\{|0\rangle, |1\rangle\}$ basis, Eve's attack will be detected with the probability of $\frac{1}{2}$; and if it is in the $\{|+\rangle, |-\rangle\}$ basis, Eve's attack will be also detected with the probability of $\frac{1}{2}$; in conclusion, the probability that Eve's attack can be detected is $\frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{1}{2}$. For γ_b decoy photons, Eve's attack will be detected with the probability of $1 - \left(\frac{1}{2}\right)^{\gamma_b}$, which will converge to 1 if γ_b is big enough.

(4) The entangle-measure attack

Eve may try to extract some useful information by entangling her auxiliary particle $|\varepsilon\rangle$ with the one in S'_B through a unitary operation $\hat{E}$. As a result, it can be obtained that

$$\hat{E}|0\rangle|\varepsilon\rangle = \alpha_1|0\rangle|\varepsilon_{00}\rangle + \beta_1|1\rangle|\varepsilon_{01}\rangle, \tag{16}$$

$$\hat{E}|1\rangle|\varepsilon\rangle = \beta_2|0\rangle|\varepsilon_{10}\rangle + \alpha_2|1\rangle|\varepsilon_{11}\rangle, \tag{17}$$

where $\varepsilon_{00}, \varepsilon_{01}, \varepsilon_{10}$ and ε_{11} are Eve's probe states, and $|\alpha_i|^2 + |\beta_i|^2 = 1$ for $i = 1, 2$. Consequently, it can be derived that

$$\begin{aligned}
\hat{E}|+\rangle|\varepsilon\rangle &= \frac{1}{\sqrt{2}}(\alpha_1|0\rangle|\varepsilon_{00}\rangle + \beta_1|1\rangle|\varepsilon_{01}\rangle + \beta_2|0\rangle|\varepsilon_{10}\rangle + \alpha_2|1\rangle|\varepsilon_{11}\rangle) \\
&= \frac{1}{\sqrt{2}}[|0\rangle(\alpha_1|\varepsilon_{00}\rangle + \beta_2|\varepsilon_{10}\rangle) + |1\rangle(\beta_1|\varepsilon_{01}\rangle + \alpha_2|\varepsilon_{11}\rangle)] \\
&= \frac{1}{2}[(|+\rangle + |-\rangle)(\alpha_1|\varepsilon_{00}\rangle + \beta_2|\varepsilon_{10}\rangle) + (|+\rangle - |-\rangle)(\beta_1|\varepsilon_{01}\rangle + \alpha_2|\varepsilon_{11}\rangle)] \\
&= \frac{1}{2}[|+\rangle(\alpha_1|\varepsilon_{00}\rangle + \beta_2|\varepsilon_{10}\rangle + \beta_1|\varepsilon_{01}\rangle + \alpha_2|\varepsilon_{11}\rangle) + |-\rangle(\alpha_1|\varepsilon_{00}\rangle \\
&\quad + \beta_2|\varepsilon_{10}\rangle - \beta_1|\varepsilon_{01}\rangle - \alpha_2|\varepsilon_{11}\rangle)], \tag{18}
\end{aligned}$$

$$\hat{E}|-\rangle|\varepsilon\rangle = \frac{1}{\sqrt{2}}(\alpha_1|0\rangle|\varepsilon_{00}\rangle + \beta_1|1\rangle|\varepsilon_{01}\rangle - \beta_2|0\rangle|\varepsilon_{10}\rangle - \alpha_2|1\rangle|\varepsilon_{11}\rangle)$$

$$= \frac{1}{\sqrt{2}}[|0\rangle(\alpha_1|\varepsilon_{00}\rangle - \beta_2|\varepsilon_{10}\rangle) + |1\rangle(\beta_1|\varepsilon_{01}\rangle - \alpha_2|\varepsilon_{11}\rangle)]$$

$$= \frac{1}{2}[(|+\rangle + |-\rangle)(\alpha_1|\varepsilon_{00}\rangle - \beta_2|\varepsilon_{10}\rangle) + (|+\rangle - |-\rangle)(\beta_1|\varepsilon_{01}\rangle - \alpha_2|\varepsilon_{11}\rangle)]$$

$$= \frac{1}{2}[|+\rangle(\alpha_1|\varepsilon_{00}\rangle - \beta_2|\varepsilon_{10}\rangle + \beta_1|\varepsilon_{01}\rangle - \alpha_2|\varepsilon_{11}\rangle) + |-\rangle(\alpha_1|\varepsilon_{00}\rangle$$

$$-\beta_2|\varepsilon_{10}\rangle - \beta_1|\varepsilon_{01}\rangle + \alpha_2|\varepsilon_{11}\rangle)] \tag{19}$$

In order for not being detected by Alice and Bob, according to Eqs. (16–19), it should satisfy that

$$\beta_1 = \beta_2 = 0, \tag{20}$$

$$\alpha_1|\varepsilon_{00}\rangle + \beta_2|\varepsilon_{10}\rangle - \beta_1|\varepsilon_{01}\rangle - \alpha_2|\varepsilon_{11}\rangle = 0, \tag{21}$$

$$\alpha_1|\varepsilon_{00}\rangle - \beta_2|\varepsilon_{10}\rangle + \beta_1|\varepsilon_{01}\rangle - \alpha_2|\varepsilon_{11}\rangle = 0. \tag{22}$$

It can be deduced from Eqs. (20–22) that

$$\alpha_1|\varepsilon_{00}\rangle = \alpha_2|\varepsilon_{11}\rangle. \tag{23}$$

Consequently, in order for not being detected by Alice and Bob, the final state of Eve's auxiliary particle should be independent of the particle of S'_B, which makes Eve acquire nothing by launching this kind of attack.

5.2 The participant attack

The participant attack, which is generally more powerful than the outside attack [30], is further analyzed here. Naturally, in a quantum summation protocol with p users, when any $p - 1$ users conspire together, they can easily derive the left one's privacy from the final summation result. Here, p is a positive integer equal or greater than 3. Hence, it is only necessary to analyze the participant attack from one dishonest user.

(1) The participant attack by Alice

Alice can hear SB and SC from Bob and Charlie, respectively. Apparently, in order to decode out Y and Z, Alice should know KB and KC in advance, respectively. Hence, Alice may adopt the following attack strategy: in Step 3, she employs the $\{|0\rangle, |1\rangle\}$ basis rather than the Bell basis to measure two particles in each of the remaining $8(n + \delta)$ particle pairs and publishes Bob and Charlie the fake Bell basis measurement result in hope of escaping the honesty check against her. For one particle pair for checking Alice's honesty, when her measurement result is $|0\rangle|0\rangle$ or $|1\rangle|1\rangle$, she randomly publishes the fake measurement result $|\phi^+\rangle$ or 'summation'; and when her measurement result is $|0\rangle|1\rangle$ or $|1\rangle|0\rangle$, she randomly publishes the fake measurement result $|\psi^-\rangle$ or 'summation'. Without loss of generality, suppose that the particle pair is $|+\rangle|+\rangle$. When Alice's measurement result is $|0\rangle|0\rangle$ or $|1\rangle|1\rangle$, according to Eqs.

(9–12), Alice will be detected with the probability of 0 if she publishes the fake measurement result $\left|\phi^{+}\right\rangle$, and will be also detected with the probability of 0 if she publishes 'summation', as there is no check for this case; when Alice's measurement result is $|0\rangle|1\rangle$ or $|1\rangle|0\rangle$, according to Eqs. (9–12), Alice will be detected with the probability of 1 if she publishes the fake measurement result $\left|\psi^{-}\right\rangle$, and will be detected with the probability of 0 if she publishes 'summation', as there is no check for this case. To sum up, when the particle pair is $|+\rangle|+\rangle$, the probability that Alice can be detected is $\frac{1}{4} \times \frac{1}{2} \times 1 + \frac{1}{4} \times \frac{1}{2} \times 1 = \frac{1}{4}$. For $2(n + \delta)$ particle pairs for checking Alice's honesty, the probability that Alice can be detected is $1 - \left(\frac{3}{4}\right)^{2(n+\delta)}$, which will converge to 1 if $2(n + \delta)$ is large enough.

Moreover, Alice may also adopt the following attack strategy: in Step 3, she employs the $\{|0\rangle, |1\rangle\}$ basis rather than the Bell basis to measure two particles in each of the remaining $8(n + \delta)$ particle pairs, and always publishes 'summation' in hope of escaping the honesty check against her. As a result, the times that Alice published 'summation' for the particle pairs, each of which has two particles originally prepared in the $\{|+\rangle, |-\rangle\}$ basis, is approximately $2(n + \delta)$. When Bob and Charlie check the times that Alice published 'summation' for the particle pairs, each of which has two particles originally prepared in the $\{|+\rangle, |-\rangle\}$ basis, they will easily discover Alice's this kind of cheating behavior.

(2) The participant attack from Bob or Charlie

In this protocol, the role of Bob is identical to that of Charlie. Without loss of generality, Bob is supposed to be dishonest. Bob can hear SA and SC from Alice and Charlie, respectively. Apparently, in order to decode out X and Z, Bob should know KA and KC in advance, respectively. KA and KC are produced from the message particle pairs. As a result, in order to obtain KC, Bob may launch his attack as follows: he intercepts $S_{C}^{'}$ sent out from Charlie, uses the $\{|0\rangle, |1\rangle\}$ basis to measure the particles in $S_{C}^{'}$ whose counterparts in $S_{B}^{'}$ were prepared by him in the $\{|0\rangle, |1\rangle\}$ basis, and sends the fresh ones in the same states as found together with other ones in $S_{C}^{'}$ to Alice. However, Bob inevitably leaves his trace on the decoy photons in $S_{C}^{'}$. Concretely speaking, as for one decoy photon, the probability that Eve's attack can be detected is $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$; hence, Eve's attack will be detected with the probability of $1 - \left(\frac{3}{4}\right)^{\tau}$, where τ is the number of decoy photons measured by Bob.

In addition, Bob has no opportunity to deduce KA from KB and KC, since he cannot get KC beforehand without being detected. Furthermore, Bob has no chance to know KA just by Alice's publishment of 'summation'.

6 Discussion

We further compare this protocol with the two-dimensional three-user quantum summation protocols in Refs. [6, 8, 9, 11, 12] where three users participate in the calculation of modulo 2 addition of their private messages. The comparison results are listed in Table 1 for clarity. Note that we ignore the quantum resource and the classical resource

Table 1 Comparision results of different two-dimensitional three-user quantum summation protocols

	The protocol of Ref. [6]	The protocol of Ref. [8]	The protocol of Ref. [9]	The protocol of Ref. [11]	The protocol of Ref. [12]	This protocol
The existence of a third party	No	No	No	No	No	No
Initial quantum resource	Single-particle states and GHZ states	Six-particle entangled states	Single-particle states	Three-particle entangled states	Bell states	Single-particle states
Users' quantum measurement	$\{\lvert+\rangle, \lvert-\rangle\}$ basis measurements and Bell basis measurements	$\{\lvert0\rangle, \lvert1\rangle\}$ basis measurements, $\{\lvert+\rangle, \lvert-\rangle\}$ basis measurements, Bell basis measurements, $\left\{\gamma_j^1 \mid j = 1, 2, \ldots, 8\right\}$ basis measurements and $\left\{\gamma_j^2 \mid j = 1, 2, \ldots, 8\right\}$ basis measurements	$\{\lvert0\rangle, \lvert1\rangle\}$ basis measurements and $\{\lvert+\rangle, \lvert-\rangle\}$ basis measurements	$\{\lvert0\rangle, \lvert1\rangle\}$ basis measurements	$\{\lvert0\rangle, \lvert1\rangle\}$ basis measurements	$\{\lvert0\rangle, \lvert1\rangle\}$ basis measurements and Bell basis measurements
Usage of quantum entanglement swapping	Yes	No	No	No	No	No
Usage of Pauli operations	Yes	No	No	Yes	Yes	No
Usage of CNOT operation	No	No	Yes	No	No	No

Table 1 (continued)

	The protocol of Ref. [6]	The protocol of Ref. [8]	The protocol of Ref. [9]	The protocol of Ref. [11]	The protocol of Ref. [12]	This protocol
Usage of Hadamard gate	No	No	Yes	Yes	No	No
Usage of a pre-shared private key sequence	No	No	No	No	No	No
Summation type	Modulo 2 addition	Modulo 2 addition	Modulo 2 addition	Modulo 2 addition	Modulo 2 addition	Modulo 2 addition
Computation way	Bit-by-bit	Bit-by-bit	Bit-by-bit	Bit-by-bit	Bit-by-bit	Bit-by-bit
Qubit efficiency	$\frac{1}{8}$	$\frac{L}{6\left(\left\lceil\frac{L}{2}\right\rceil+\delta\right)+3L}$	$\frac{1}{3(1+d)+3}$	$\frac{1}{4}$	$\frac{1}{9}$	$\frac{n}{16(n+\delta)+3n}$

consumed for the security check against Eve in Table 1, as it often can be regarded to be relatively independent of the main part of a quantum communication protocol.

In Table 1, the qubit efficiency is expressed as [31]

$$\lambda = \frac{v}{q+r}, \tag{24}$$

where v represents the number of classical bits to be calculated for summation, q denotes the number of qubits consumed, and r represents the number of classical bits consumed.

In this protocol, each of X, Y and Z has n bits, hence $v = n$; both S_B and S_C have $8(n + \delta)$ single particles randomly in the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, so $q = 8(n + \delta) \times 2 = 16(n + \delta)$; and Alice, Bob and Charlie need to publish SA, SB and SC, respectively, hence $r = 3n$. Consequently, the qubit efficiency of this protocol is $\lambda = \frac{n}{16(n+\delta)+3n}$.

In the protocol of Ref.[6], the secret bit string from the user A_i has L bits, where $i = 1, 2, 3$, hence $v = L$; A_1 needs to produce L three-particle entangled states, while both A_2 and A_3 need to generate L single photons, so $q = 5L$; both A_2 and A_3 need to cooperate to publish the classical bits coded from their Bell basis measurement results, while A_1 needs to publish the final summation result, in order to let A_2 and A_3 know it, hence $r = 3L$. Consequently, the qubit efficiency of the protocol of Ref. [6] is $\lambda = \frac{L}{5L+3L} = \frac{1}{8}$.

In the protocol of Ref. [8], the secret bit string from the user P_i has L bits, where $i = 1, 2, 3$, hence $v = L$; P_1 needs to prepare $\lceil \frac{L}{2} \rceil + \delta$ genuinely maximally six-particle entangled states, so $q = 6(\lceil \frac{L}{2} \rceil + \delta)$; and P_i needs to publish C_i, hence $r = 3L$. Consequently, the qubit efficiency of the protocol of Ref. [8] is $\lambda = \frac{L}{6(\lceil \frac{L}{2} \rceil + \delta) + 3L}$.

In the protocol of Ref. [9], the user P_i has one secret bit, where $i = 1, 2, 3$, hence $v = 1$; P_i needs to produce three single particle sequences, each of whose length is $1 + d$, so $q = 3(1 + d)$; and P_i needs to publish the ciphertext c_i, hence $r = 3$. Consequently, the qubit efficiency of the protocol of Ref. [9] is $\lambda = \frac{1}{3(1+d)+3}$.

In the protocol of Ref. [11], the secret bit string from the user P_i has L bits, where $i = 1, 2, 3$, hence $v = L$; P_1 needs to prepare L three-particle entangled states, so $q = 3L$; and in order to make the other two users know the final summation result, P_1 needs to publish it, hence $r = L$. Consequently, the qubit efficiency of the protocol of Ref. [11] is $\lambda = \frac{L}{3L+L} = \frac{1}{4}$.

In the protocol of Ref.[12], the secret bit string from the user A_i has m bits, where $i = 1, 2, 3$, hence $v = m$; each user needs to generate m Bell states, so $q = 6m$; and A_i needs to publish the result P_i, hence $r = 3m$. Consequently, the qubit efficiency of the protocol of Ref. [12] is $\lambda = \frac{m}{6m+3m} = \frac{1}{9}$.

According to Table 1, we can draw the following conclusions: ① As for the initial quantum resource, this protocol exceeds the protocols of Refs. [6, 8, 11, 12], as the preparations of Bell states and multiple-particle entangled states are much more difficult than that of single-particle states; ② as for users' quantum measurement, this protocol takes advantage over the protocol of Ref. [8], as the $\left\{ \gamma_j^1 | j = 1, 2, \ldots, 8 \right\}$

basis measurements and the $\left\{\gamma_j^2 | j = 1, 2, \ldots, 8\right\}$ basis measurements are much more complicated to realize than the $\{|0\rangle, |1\rangle\}$ basis measurements and the Bell basis measurements; ③ as for the usage of quantum entanglement swapping, this protocol defeats the protocol of Ref.[6], as it doesn't need to employ quantum entanglement swapping; ④ as for the usage of Pauli operations, this protocol has better performance than the protocols of Refs.[6, 11, 12], as it doesn't need to adopt the Pauli operations; ⑤ as for the usage of CNOT operation, this protocol exceeds the protocol of Ref.[9], as it doesn't require the CNOT operation; ⑥ as for the usage of Hadamard gate, this protocol exceeds the protocols of Refs.[9, 11], as it doesn't need the Hadamard gate.

Moreover, the comparison results of the proposed protocol and the semiquantum summation protocols of Refs. [32, 33] are further summarized in Table 2.

7 Conclusions

In conclusion, a lightweight three-user secure quantum summation protocol without the existence of a third party based on single-particle states is proposed in this paper, which can calculate the modulo 2 addition of three users' private messages. Single-particle states rather than quantum entangled states are employed as the initial quantum resource. Three users are only required to implement single-particle measurements and Bell basis measurements. None of quantum entanglement swapping, the Pauli operations, the CNOT operation or the Hadamard gate are required. Moreover, three users are not required to share a private key sequence among them beforehand. This protocol is secure against both the outside attacks and the participant attacks. Compared with the previous two-dimensional three-user quantum summation protocols of Refs. [6, 8, 9, 11, 12], this protocol more or less takes advantage over them on the aspects of the initial quantum resource, users' quantum measurement, the usage of quantum entanglement swapping, the usage of Pauli operations, the usage of CNOT operation or the usage of Hadamard gate.

Besides, the proposed protocol needs to perform the complete Bell basis measurement. At present, it is hard to realize in linear optics but can be achieved via cross-Kerr nonlinearities or cavity-assisted light-matter interactions [34–36].

Moreover, the proposed protocol can be extended into the collective-dephasing noise resistant version and the collective-rotation noise resistant version, as long as the single-particle sequences generated in Step 1 are composed by the logical qubits $\left\{|0_{dp}\rangle, |1_{dp}\rangle, |+_{dp}\rangle, |-_{dp}\rangle\right\}$ and $\{|0_r\rangle, |1_r\rangle, |+_r\rangle, |-_r\rangle\}$, respectively. Here, $|0_{dp}\rangle = |01\rangle, |1_{dp}\rangle = |10\rangle, |+_{dp}\rangle = \frac{1}{\sqrt{2}}(|0_{dp}\rangle + |1_{dp}\rangle), |-_{dp}\rangle = \frac{1}{\sqrt{2}}(|0_{dp}\rangle - |1_{dp}\rangle), |0_r\rangle = |\phi^+\rangle, |1_r\rangle = |\psi^-\rangle, |+_r\rangle = \frac{1}{\sqrt{2}}(|0_r\rangle + |1_r\rangle)$ and $|-_r\rangle = \frac{1}{\sqrt{2}}(|0_r\rangle - |1_r\rangle)$[37–40].

In addition, semiquantum summation [32, 33, 41], which is the semiquantum counterpart of quantum summation, has been put forward recently. In the future, it is also worth studying how to design secure semiquantum summation protocols.

Table 2 Comparision results of the proposed protocol and the protocols of Ref. [32, 33]

	The protocol of Ref [32]	The protocol of Ref [33]	This protocol
Quantum channel	Ideal quantum channel	Ideal quantum channel	Ideal quantum channel
Function	Calculating the summation of the private bits from three classical participants	Calculating the summation of the private bits from one quantum participant and two classical participants	Calculating the summation of the private bits from three quantum participants
Number of involved participants	Four	Three	Three
Initial quantum resource	$|+\rangle$	$|+\rangle$	$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$
Quantum measurement of quantum participant	$\{|0\rangle, |1\rangle\}$ basis measurements, $\{|+\rangle, |-\rangle\}$ basis measurements and GHZ-type basis measurements	$\{|0\rangle, |1\rangle\}$ basis measurements, $\{|+\rangle, |-\rangle\}$ basis measurements and Bell basis measurements	$\{|0\rangle, |1\rangle\}$ basis measurements, $\{|+\rangle, |-\rangle\}$ basis measurements and Bell basis measurements
Quantum measurement of classical participants	$\{|0\rangle, |1\rangle\}$ basis measurements	$\{|0\rangle, |1\rangle\}$ basis measurements	/
Usage of quantum entanglement swapping	No	No	No
Usage of unitary operations	No	No	No
Usage of a pre-shared private key	No	No	No
Summation type	Modulo 2 addition	Modulo 2 addition	Modulo 2 addition
Computation way	Bit-by-bit	Bit-by-bit	Bit-by-bit

Data availability The datasets used during the current study are available from the corresponding author on reasonable request.

References

1. Hillery, M., Ziman, M., Buzek, V., Bielikova, M.: Towards quantum-based privacy and voting. Phys. Lett. A **349**(1–4), 75–81 (2006)
2. Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J. Phys. A: Math. Theor. **42**, 055305 (2009)
3. Zhou, N.R., Zeng, G.H., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**, 1149–1150 (2004)
4. Heinrich, S.: Quantum summation with an application to integration. J. Complex. **18**(1), 1–50 (2002)
5. Heinrich, S., Kwas, M., Wozniakowski, H.: Quantum Boolean summation with repetitions in the worst-average setting. (2003). https://arxiv.org/abs/quant-ph/0311036
6. 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)
7. Zhang, C., Sun, Z.W., Huang, Y., Long, D.Y.: 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)
8. Zhang, C., Sun, Z.W., Huang, X., Long, D.Y.: Three-party quantum summation without a trusted third party. Int. J. Quantum Inf. **13**(2), 1550011 (2015)
9. Zhang, C., Situ, H.Z., Huang, Q., Yang, P.: Multi-party quantum summation without a trusted third party based on single particles. Int. J. Quantum Inf. **15**(2), 1750010 (2017)
10. Gu, J., Hwang, T., Tsai, C.W.: Improving the security of 'High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom.' Int. J. Theor. Phys. **58**, 2213–2217 (2019)
11. 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**, 2783–2791 (2020)
12. Wu, W.Q., Ma, X.X.: Multi-party quantum summation without a third party based on d-dimensionalal bell states. Quantum Inf. Process. **20**, 200 (2021)
13. Du, J.Z., Chen, X.B., Wen, Q.Y., Zhu, F.C.: Secure multiparty quantum summation. Acta Phys. Sin. **56**(11), 6214–6219 (2007)
14. Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep. **6**, 19655 (2016)
15. Yang, H.Y., Ye, T.Y.: Secure multi-party quantum summation based on quantum Fourier transform. Quantum Inf. Process. **17**(6), 129 (2018)
16. 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)
17. Lv, S.X., Jiao, X.F., Zhou, P.: Multiparty quantum computation for summation and multiplication with mutually unbiased bases. Int. J. Theor. Phys. **58**, 2872–2882 (2019)
18. Duan, M.Y.: Multi-party quantum summation within a d-level quantum system. Int. J. Theor. Phys. **59**(5), 1638–1643 (2020)
19. Gan, Z.G.: Improvement of quantum protocols for secure multi-party summation. Int. J. Theor. Phys. **59**(10), 3086–3092 (2020)
20. Sutradhar, K., Om, H.: A generalized quantum protocol for secure multiparty summation. IEEE Trans. Circuits Syst. II: Exp. Briefs **67**(12), 2978–2982 (2020)
21. Sutradhar, K., Om, H.: Hybrid quantum protocols for secure multiparty summation and multiplication. Sci Rep **10**, 9097 (2020)
22. Ye, T.Y., Hu, J.L.: Quantum secure multiparty summation based on the phase shifting operation of d-level quantum system and its application. Int J Theor Phys **60**(3), 819–827 (2021)

23. 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)
24. Wang, Y.L., Hu, P.C., Xu, Q.L.: Quantum secure multi-party summation based on entanglement swapping. Quantum Inf. Process. **20**, 319 (2021)
25. Zhang, C., Long, Y.X., Li, Q.: Quantum summation using d-level entanglement swapping. Quantum Inf. Process. **20**, 137 (2021)
26. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
27. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**(1–2), 23–25 (2006)
28. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**(1), 145–195 (2002)
29. Deng, F.G., Zhou, P., Li, X.H., et al.: Robustness of two-way quantum communication protocols against Trojan horse attack. https://arxiv.org/abs/quant-ph/0508168 (2005)
30. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the Bradler-Dusek protocol. Quantum Inf. Comput. **7**, 329 (2007)
31. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**, 5635 (2000)
32. 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)
33. Hu, J.L., Ye, T.Y.: Three-party secure semiquantum summation without entanglement among quantum user and classical users. Int. J. Theor. Phys. **61**(6), 170 (2022)
34. Nemoto, K., Munro, W.J.: Nearly deterministic linear optical controlled-NOT gate. Phys. Rev. Lett. **93**, 250502 (2004)
35. Bonato, C., Haupt, F., Oemrawsingh, S.S.R., Gudat, J., et al.: CNOT and Bell-state analysis in the weak-coupling cavity QED regime. Phys. Rev. Lett. **104**, 160503 (2010)
36. Sheng, Y.B., Deng, F.G., Long, G.L.: Complete hyperentangled-Bell-state analysis for quantum communication. Phys. Rev. A **82**, 032318 (2010)
37. Walton, Z.D., Abouraddy, A.F., Sergienko, A.V., et al.: Decoherence-free subspaces in quantum key distribution. Phys. Rev. Lett. **91**, 087901 (2003)
38. Zhang, Z.J.: Robust multiparty quantum secret key sharing over two collective-noise channels. Phys. A **361**, 233–238 (2006)
39. Yang, C.W., Tsai, C.W., Hwang, T.: Fault tolerant two-step quantum secure direct communication protocol against collective noises. Sci. China Ser. G- Phys. Mech. Astron. **54**(3), 496–501 (2011)
40. Gu, B., Zhang, C.Y., Cheng, G.S., Huang, Y.G.: Robust quantum secure direct communication with a quantum one-time pad over a collective-noise channel. Sci. China Ser. G-Phys. Mech. Astron. **54**(5), 942–947 (2011)
41. 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**(3), 118 (2022)