Quantum Information Processing (2022) 21:122
https://doi.org/10.1007/s11128-022-03454-4

Measurement-device-independent quantum secure multiparty summation

Run-Hua Shi[1,2] · Bai Liu[2] · Mingwu Zhang[2]

Received: 21 September 2021 / Accepted: 9 February 2022 / Published online: 30 March 2022

Abstract
In this paper, we define two specific secure multiparty summations and further present the corresponding measurement-device-independent quantum secure multiparty summation protocols, in which each party with a private input only performs simple single-particle operators, not any complex quantum measurements. The proposed protocols not only achieve the information-theoretical security, but also ensure the good feasibility and the high performance.

Keywords Quantum computing · Quantum cryptography · Measurement-device-independent · Secure multiparty summation

1 Introduction

As an important branch of quantum cryptography [1], quantum secure multiparty computation [2] has attracted a lot of scientific attention from the research community. There are many promising applications of quantum secure multiparty computation, e.g., quantum-secured blockchain [3], quantum sealed-bid auction [4], quantum voting [5] and quantum federated learning [6].

Secure multiparty summation (SMS) is a specific secure multiparty computation (SMC) that enables many parties to jointly compute the summation of multiple private inputs (e.g., bits or integers) without disclosing anything about each private input. Accordingly, there appeared many quantum SMS protocols [7–14]. However, most of these protocols only present a theoretical approach or idea to solve the SMS problem, and thus, it is difficult to implement them due to the high complexity of necessary quantum resources, operators and measurements in high-dimensional Hilbert space.

✉ Run-Hua Shi
rhshi@ncepu.edu.cn

[1] School of Control and Computer Engineering, North China Electric Power University, Beijing City 102206, China

[2] School of Computer Science, Hubei University of Technology, Wuhan City 430068, China

Furthermore, even though there are a few feasible quantum SMS protocols, they do not consider imperfections of implementing devices. So, there may still be secure flaws or risks in real-life implementations, e.g., side-channel attacks for detectors [15–17], though the security of these quantum protocols has been rigorously proved based on the laws of quantum mechanics.

On the other hand, in 2012, Lo, et al. [15] presented the novel idea of measurement-device-independent quantum key distribution (MDI-QKD), which not only removes all quantum attacks in the detection part, i.e., the most important security loophole of QKD implementations, but also offers excellent performance with current technology [16].

In this paper, following some ideas from MDI-QKD, we first present measurement-device-independent quantum secure multiparty summation. Especially, we extend the MDI communication model from two parties of QKD to arbitrary multiple parties of SMS, which will possibly solve more practical SMC problems, not only SMS.

In the following section, we first define two specific secure multiparty summations, i.e., secure multiparty modulo-2 summation (SMM2S) and secure multiparty modulo-d summation (SMMdS), and further present the corresponding measurement-device-independent quantum SMM2S and SMMdS protocols. Finally, we prove the security and analyze the performance of the proposed protocols.

2 Quantum secure multiparty modulo-2 summation

Definition 1 (Secure Multiparty Modulo-2 Summation, SMM2S for short). Suppose that there are n parties: P_1, P_2,..., P_n $(n > 2)$, each of which has a private input $x_i \in \{0, 1\}$ $(i = 1, 2, \ldots, n)$. After executing this protocol, it outputs $(x_1 + x_2 + \ldots + x_n)mod2$. (Note. $(x_1 + x_2 + \ldots + x_n)mod2 = x_1 \oplus x_2 \oplus \ldots \oplus x_n$). In addition, it should satisfy the following requirements:

Correctness. If all parties honestly execute this protocol, then the final output is $(x_1 + x_2 + \ldots + x_n)mod2$, i.e., the output is correct.

Fairness. Under no circumstances, one party should have an advantage over another or other parties. In other words, all parties are equivalent entities, and they can get the final output $(x_1 + x_2 + \ldots + x_n)mod2$ with equal opportunities.

Privacy. Any other party except for the party P_i learns no information about x_i except the final output $(x_1 + x_2 + \ldots + x_n)mod2$.

In the following protocol, suppose that n parties are partitioned into two groups by respective locations, where the closer parties P_1, P_2,..., and P_m $(m < n)$ belong to the first group and the remaining parties P_{m+1}, P_{m+2},..., and P_n lie in the second group, as shown in Fig. 1. Furthermore, we assume that there are three agents: Alice, Bob and Charlie, where Alice and Bob will be responsible for generating all quantum resources while Charlie will perform all quantum measurements. In addition, Alice and Bob beforehand shared a key k with the length of t, where $k[j]$ denote the jth bits of k for $j = 1, 2, \ldots t$.

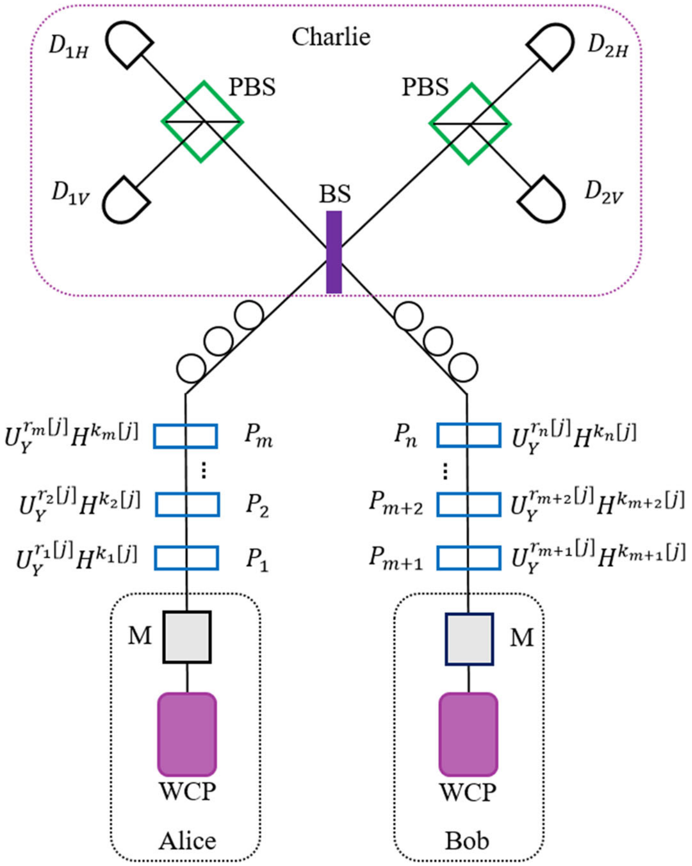


Fig. 1 Sketch for experimental implementation of MDI-SMM2S. WCP: weak coherent pulse; M: polarization and intensity modulators; BS: beam splitter; PBS: polarization beam splitter; D: single-photon detector

3 Quantum SMM2S protocol

*Step 1*Alice and Bob prepare t phase randomized weak coherent pulses (WCPs) in the BB84 polarization states [17], respectively, where the basis choice of the j th WCP ($j = 1, 2, \ldots, t$) is determined by the beforehand shared bit $k[j]$ as follows: the basis is $\{|0\rangle, |1\rangle\}$ if $k[j] = 0$, and $\{|+\rangle, |-\rangle\}$ otherwise.

For example, if $k[j] = 0$ then Alice and Bob prepare the j th WCP in the basis of $\{|0\rangle, |1\rangle\}$. But the states of two WCPs prepared by Alice and Bob may be different.

Step 2 Alice sends t WCPs to pass through m parties P_1, P_2,..., and P_m in turn, as shown in Fig. 1. When the party P_i ($i = 1, 2, \ldots, m$) receiving t WCPs, he performs the operators $U_Y^{r_i[j]}H^{k_i[j]}$ on the j th WCP for $j = 1, 2, \ldots, t$, where $r_i[j]$ and $k_i[j]$ are two random bits selected by the party P_i. Here, the operators are defined by [18],

$$U_Y^1 = U_Y = iY = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \tag{1}$$

$$H^1 = H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{2}$$

$$U_Y^0 = H^0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{3}$$

Similarly, Bob sends t WCPs to pass through other $n-m$ parties P_{m+1}, P_{m+2},..., and P_n in turn, as shown in Fig. 1, where the party P_i $(i = m+1, \ldots, n)$ performs $U_Y^{r_i[j]} H^{k_i[j]}$ on the j th WCP for $j = 1, 2, \ldots, t$.

Step 3 After the parties P_m and P_n completing their respective operators, they immediately send the j th WCP pair to Charlie for $j = 1, 2, \ldots, t$.

Step 4 For each pair of WCPs, Charlie performs a Bell state measurement (BSM) that projects incoming signals into a Bell state (Fig. 1). In any case, he announces whether or not his measurements are successful, including the Bell states successfully obtained (i.e., $\left|\psi^+\right\rangle$ or $\left|\psi^+\right\rangle$).

Step 5 Post-processing. ① Each party P_i $(i = 1, 2, \ldots, n)$ opens his random bits $k_i[j]$ s for $j = 1, 2, \ldots, t$. ② All parties select out the useful j s from $j = 1$ to t, where the useful condition of j must satisfy both $\sum_{i=1}^{m} k_i[j] mod 2 = 0$ and $\sum_{i=m+1}^{n} k_i[j] mod 2 = 0$. Please note that the bases of the j th WCP pair will not change when satisfying the useful condition (please see later correctness analysis for details). ③ All parties keep the successful and useful events, i.e., Charlie achieves successful BSMs and the sequence number j satisfies the useful condition, and discard the rest. ④ In order to check the honesty of three agents (i.e., Charlie, Alice and Bob), it requires Charlie to open all successfully measured results and Alice and Bob to open the initial states of the corresponding WCPs, respectively. Furthermore, all parties publicly agree to retain a successful and useful event (including Charlie's measured result and Alice's and Bob's initial states) for later calculation of the final summation. For other successful and useful events, all parties open the corresponding random bits, i.e.,$r_i[j]$ s. All parties can determine whether there is a dishonest agent or the outsider's eavesdropping by Table 1. That is, if there is any case which is not consistent with Table 1, then there must be a dishonest agent or eavesdropping. If there is no finding any dishonest agent or eavesdropper, then all parties will continue to execute the next step.

Table 1 Possible combinations of public information

Initial basis	$\lvert\psi^+\rangle$		$\lvert\psi^-\rangle$	
	$\lvert W_L\rangle_j = \lvert W_R\rangle_j$	$\lvert W_L\rangle_j \neq \lvert W_R\rangle_j$	$\lvert W_L\rangle_j = \lvert W_R\rangle_j$	$\lvert W_L\rangle_j \neq \lvert W_R\rangle_j$
$\{\lvert 0\rangle, \lvert 1\rangle\}$	$r_L[j] \neq r_R[j]$	$r_L[j] = r_R[j]$	$r_L[j] \neq r_R[j]$	$r_L[j] = r_R[j]$
$\{\lvert +\rangle, \lvert -\rangle\}$	$r_L[j] = r_R[j]$	$r_L[j] \neq r_R[j]$	$r_L[j] \neq r_R[j]$	$r_L[j] = r_R[j]$

$\left|\psi^+\right\rangle$ and $\left|\psi^-\right\rangle$ denotes the successfully measured results of Charlie. $|W_L\rangle_j$ and $|W_R\rangle_j$ represent the initial states of the left WCP and the right WCP of the j th WCP pair prepared by Alice and Bob, respectively. $r_L[j] = \sum_{i=1}^{m} r_i[j] mod 2$ and $r_R[j] = \sum_{i=m+1}^{n} r_i[j] mod 2$

Table 2 The corresponding computing results

Initial basis	$\|\psi^+\rangle$		$\|\psi^-\rangle$	
	$\|W_L\rangle_l = \|W_R\rangle_l$	$\|W_L\rangle_l \neq \|W_R\rangle_l$	$\|W_{L\,l} = \|W_{R\,l}$	$\|W_{L\,l} \neq \|W_{R\,l}$
$\{\|0\rangle, \|1\rangle\}$	$r[l] = 1$	$r[l] = 0$	$r[l] = 1$	$r[l] = 0$
$\{\|+\rangle, \|-\rangle\}$	$r[l] = 0$	$r[l] = 1$	$r[l] = 1$	$r[l] = 0$

$r[l] = \sum_{i=1}^{n} r_i[l] mod2$. If $r_L[l] = r_R[l]$, then $r[l] = 0$; Otherwise $r[l] = 1$

Step 6 Suppose that the successful and useful event kept to compute the final summation is corresponding to the lth WCP pair. Each party P_i $(i = 1, 2, \ldots, n)$ computes $r_i^*[l]$ as follows:

$$r_i^*[l] = (x_i + r_i[l]) mod2 \tag{4}$$

where x_i is his private input. Furthermore, each party P_i opens $r_i^*[l]$.
Step 7 All parties compute r^* by

$$r^* = \sum_{i=1}^{n} r_i^*[l] mod2 \tag{5}$$

Finally, all parties can deduce $\sum_{i=1}^{n} x_i mod2 = r^*$ or $(r^* + 1)mod2$ by Table 2. That is, if $r[l] = 0$ (i.e., $\sum_{i=1}^{n} r_i[l] = 0$), then $\sum_{i=1}^{n} x_i mod2 = r^*$, and $\sum_{i=1}^{n} x_i mod2 = (r^* + 1)mod2$ otherwise.

For example, if Charlie's measured result is $\left|\psi^+\right\rangle$ and Alice's and Bob's initial states are $|-$ and $|+\rangle$, respectively, then $\sum_{i=1}^{n} x_i mod2 = (r^* + 1)mod2$.

4 Quantum secure multiparty modulo-*d* summation

Secure Multiparty Modulo-d Summation is a natural extension of Secure Multiparty Modulo-2 Summation, which is defined as follows:

Definition 2 (Secure Multiparty Modulo-d Summation, SMMdS for short). Suppose that there are n parties: P_1, P_2,..., P_n $(n > 2)$, each of which has a private input $x_i \in \{0, 1, \ldots, d-1\}$ $(i = 1, 2, \ldots, n)$. After executing this protocol, it finally outputs $(x_1 + x_2 + \ldots + x_n)modd$. Similarly, it should satisfy the secure requirements: Correctness, Fairness and Privacy.

For simplicity, here, we mainly consider a specific quantum SMMdS protocol, in which each party owns a private input $x_i \in \{0, 1\}$, i.e., one bit, and further all parties jointly compute $x_1 + x_2 + \ldots + x_n$, i.e., $d > n$, without revealing any private input. Clearly, we can compute more general SMMdS by bitwise summations from left to right, i.e., the general SMMdS can be fulfilled by executing the specific SMMdS multiple times.

In the following specific quantum SMMdS protocol, we assume that each party initially gets a unique secret $s_i \in \{1, 2, \ldots, n\}$ by the way of on-site draw, such that $s_i \neq s_j$ for any $i \neq j$. Furthermore, to reuse the secret s_i, all parties privately agree on a bijection (i.e., one-to-one) function in advance

$$F : \{0, 1\}^n \to \{P_1, P_2, \ldots, P_{2^n}\} \tag{6}$$

$$F(x) = P_{f(x)}\big(f(x) \in \{1, 2, \ldots, 2^n\}\big) \tag{7}$$

where each P_j is a known one-way permutation function for $j \in \{1, 2, \ldots, 2^n\}$. Therefore, if all parties agree on a public parameter x, then each party will get the same permutation function $P_{f(x)}$, where $f(x)$ is privately but completely determined by the parameter x, e.g., $F(x) = P_{x-1}$ (i.e., $f(x) = x - 1$).

In addition, Alice and Bob shared a t-bit key k by a QKD protocol in advance ($t \approx 16n$).

5 Specific quantum SMMdS protocol

Step 1 All parties negotiate a public parameter s, i.e., they agree on a permutation function $F(s) = P_{f(s)}$. Furthermore, each party privately computes $s_i^* = P_{f(s)}(s_i)$ for $i = 1, 2, \ldots, n$. Clearly, $s_i^* \neq s_j^*$ for any $i \neq j$.
Step 2 Alice and Bob prepare t ($t \approx 16n$) phase randomized weak coherent pulses (WCPs) in the BB84 polarization states, respectively, where the basis choice of the j th WCP ($j = 1, 2, \ldots, t$) is determined by the bit $k[j]$ as follows: the basis is $\{|0\rangle, |1\rangle\}$ if $k[j] = 0$, and $\{|+\rangle, |-\rangle\}$ otherwise.
Step 3 Alice sends t WCPs to pass through m parties P_1, P_2,…, and P_m in turn. When the party P_i ($i = 1, 2, \ldots, m$) receiving t WCPs, he immediately performs the operators $U_Y^{r_i[j]} H^{k_i[j]}$ on the j th WCP for $j = 1, 2, \ldots, t$, where $r_i[j]$ and $k_i[j]$ are two bits randomly selected by the party P_i. Similarly, Bob sends t WCPs to pass through other $n - m$ parties P_{m+1}, P_{m+2},…, and P_n in turn, where the party P_i ($i = m + 1, \ldots, n$) performs $U_Y^{r_i[j]} H^{k_i[j]}$ on the j th WCP for $j = 1, 2, \ldots, t$.
Step 4 After the parties P_m and P_n completing their respective operators, they send all WCPs to Charlie in order.
Step 5 For each pair of WCPs, Charlie performs a BSM that projects incoming signals into a Bell state. In any case, he announces whether or not his measurements are successful, including the Bell states successfully obtained (i.e., $|\psi^+\rangle$ or $|\psi^+\rangle$).
Step 6 Post-processing. ① Each party P_i ($i = 1, 2, \ldots, n$) opens his random bits $k_i[j]$ s for $j = 1, 2, \ldots, t$. ② All parties select out the useful j s from $j = 1$ to t, where the useful condition of j must satisfy both $\sum_{i=1}^{m} k_i[j] \bmod 2 = 0$ and $\sum_{i=m+1}^{n} k_i[j] \bmod 2 = 0$.

③ All parties keep the successful and useful events, i.e., Charlie achieves successful BSMs and the sequence number j satisfies the useful condition, and discard the rest. Please note that about a half of the total t events will be successful (i.e., about $8n$ events are successful). Furthermore, about a quarter of all successful events will be useful (i.e., about $2n$ events are both successful and useful).

Step 7 For all successful and useful events, Charlie opens all measured results and Alice and Bob open the initial states of the corresponding WCP pairs. Furthermore, among about $2n$ successful and useful events, all parties randomly select out n successful and useful events as encoding events to compute the final summation, and the remaining (about$n$) events as the checking events to check the honesty of the agents or the outsider's eavesdropping.

Step 8 For the checking events, all parties open the corresponding random bits, i.e., $r_i[j]$ s. Similarly, all parties determine whether there is a dishonest agent or eavesdropping by Table 1. If no finding any dishonest agent or eavesdropping, it continues to execute the next step. Otherwise, it terminates this protocol.

Step 9 Without loss of generality, n encoding events are represented as the l_1th, l_2th,..., and l_nth WCP pairs among all t WCP pairs, where each WCP pair is prepared by Alice and Bob, respectively. Each party P_i $(i = 1, 2, \ldots, n)$ computes $r_i^*\left[l_j\right]$ for $j = 1, 2, \ldots, n$ as follows:

$$r_i^*\left[l_j\right] = \begin{cases} \left(x_i + r_i\left[l_j\right]\right) mod\ 2, & if j = s_i^* \\ r_i\left[l_j\right], & \text{otherwise} \end{cases} \tag{8}$$

where x_i is his private input. That is, he only embeds his secret x_i into the s_i^*th encoding event in all n encoding events. Furthermore, each party P_i opens all $r_i^*\left[l_j\right]$ s for $j = 1, 2, \ldots, n$.

Step 10 All parties compute $r^*\left[l_j\right]$ for $j = 1, 2, \ldots, n$ by

$$r^*\left[l_j\right] = \sum_{i=1}^{n} r_i^*\left[l_j\right] \text{mod} 2 \tag{9}$$

Similarly, for the j th encoding event (i.e., the l_jth WCP pair corresponding to the public $r^*\left[l_j\right]$), all parties can deduce the j th summation $sum(j) = r^*\left[l_j\right]$ or $\left(r^*\left[l_j\right] + 1\right) mod 2$ with Charlie's measured result and Alice and Bob's public information according to Table 2.

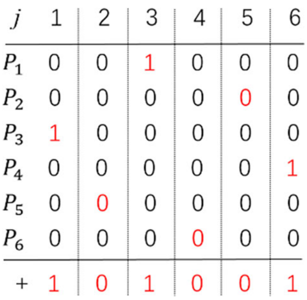
On the other hand, $sum(j) = (0 + \ldots + 0 + x_i + 0 \ldots + 0)$mod2, i.e., the summation of the j th column in Fig. 2, where only one party P_i inputs x_i and all other parties input 0, that is, it satisfies the implicit condition that $j = s_i^*$ but i is private. Clearly, $sum(j) = x_i$.

Step 11

Finally, all parties compute

$$\sum_{i=1}^{n} x_i = \sum_{j=1}^{n} sum(j) \tag{10}$$

Fig. 2 Schematic diagram of Multiparty Secure Summation



j	1	2	3	4	5	6
P_1	0	0	1	0	0	0
P_2	0	0	0	0	0	0
P_3	1	0	0	0	0	0
P_4	0	0	0	0	0	1
P_5	0	0	0	0	0	0
P_6	0	0	0	0	0	0
+	1	0	1	0	0	1

Here, we give a simple example. In this example, suppose that there are six parties: P_1, P_2, P_3, P_4, P_5 and P_6, where their private inputs are listed as: $x_1 = 1$, $x_2 = 0$, $x_3 = 1$, $x_4 = 1$, $x_5 = 0$ and $x_6 = 0$, respectively. Furthermore, we assume that the unique secrets of six parties are distributed as follows: $s_1^* = 3$, $s_2^* = 5$, $s_3^* = 1$, $s_4^* = 6$, $s_5^* = 2$ and $s_6^* = 4$, respectively. The idea of specific SMMdS is to first compute the summation of each column by using quantum SMM2S protocol, where each column only hides one private input (see red digit in Fig. 2), and further compute the final summation of all public column summations, as shown in Fig. 2. Here, the function or effect of the unique secrets $\{s_1^*,s_2^*,s_3^*,s_4^*,s_5^*,s_6^*\}$ is equivalent to permute the private inputs $\{x_1,x_2,x_3,x_4,x_5,x_6\}$ to get the public outputs $\{1,0,1,0,0,1\}$, so that all parties can get the final summation, i.e., 3, but not know whose private input each public output is. Please note that the detailed processes of quantum SMM2S protocols are omitted in Fig. 2, which may refer to Fig. 1.

6 Analysis

6.1 Correctness

According to the above example in Fig. 2, the proposed specific quantum SMMdS protocol is to calculate the summation of n private bits (i.e., n private inputs) by equivalently executing quantum SMM2S protocols n times, where each quantum SMM2S protocol (corresponding to each column in Fig. 2) gets a private bit (corresponding to a real input), but anyone except the actual owner cannot knows whose bit/input it is. Clearly, the correctness of the proposed specific quantum SMMdS protocol can be guaranteed by that of the quantum SMM2S protocol. So, we main analyze the correctness of the quantum SMM2S protocol as follows:

Theorem 1 *The proposed quantum SMM2S protocol is correct, when all parties honestly execute the protocol.*

Proof On the one hand, we first study the effect of quantum operators on each WCP's state before sending it to Charlie to perform a BSM.

Without loss of generality, we only consider the j th WCP prepared by Alice, as shown in Fig. 1. By Eqs. (1) and (2), we can infer the following equations:

$$H^2 = U_Y^2 = I \tag{11}$$

$$HU_Y H = -U_Y \tag{12}$$

$$HU_Y = -U_Y H \tag{13}$$

Suppose that the initial state of the j th WCP is $|W\rangle_j \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. By Fig. 1, when the party P_m completing his operators, the state of the j th WCP will be changed as

$$\left|W^*\right\rangle_j = U_Y^{r_m[j]} H^{k_m[j]} \ldots U_Y^{r_2[j]} H^{k_2[j]} U_Y^{r_1[j]} H^{k_1[j]} |W\rangle_j \tag{14}$$

By Eqs. (11)-(13), we can further get

$$\left|W^*\right\rangle_j = (-1)^l U_Y^{\sum\limits_i r_i[j]} H^{\sum\limits_i k_i[j]} |W\rangle_j. \tag{15}$$

By the useful condition of the sequence number j, $\sum\limits_i k_i[j] = 0 mod 2$, so

$$\left|W^*\right\rangle_j = (-1)^l U_Y^{\sum\limits_i r_i[j]} |W\rangle_j. \tag{16}$$

In addition, we know

$$\begin{aligned} &U_Y|0\rangle \rightarrow |1\rangle \\ &U_Y|1\rangle \rightarrow -|0\rangle \\ &U_Y|+\rangle \rightarrow |-\rangle \\ &U_Y|-\rangle \rightarrow -|+\rangle \end{aligned} \tag{17}$$

By Eqs. (16) and (17), we further know that the current state, i.e., $|W^*\rangle_j$, will remain the same as the initial state, i.e., $|W^*\rangle_j$, except for a global phase, if the number of performing U_Y is even (i.e., $\sum\limits_i r_i[j] mod 2 = 0$), otherwise it will change, but it keeps the same basis.

In short, the facts that the common bit $k[j]$ shared by Alice and Bob in advance and the useful condition publicly selected out by all parties (i.e., both $\sum\limits_{i=1}^{m} k_i[j] mod 2 = 0$ and $\sum\limits_{i=m+1}^{n} k_i[j] mod 2 = 0$) ensure that the bases of each incoming WCP pair are exactly the same. Furthermore, if $\sum\limits_{i=1}^{m} r_i[j] mod 2 = 0$ $\left(\sum\limits_{i=m+1}^{n} r_i[j] mod 2 = 0\right)$, the state of the j th WCP prepared by Alice (Bob) will not change; if $\sum_{i=1}^{m} r_i[j] mod 2 = 1$ $\left(\sum_{i=m+1}^{n} r_i[j] mod 2 = 1\right)$, the state of the j th WCP prepared by Alice (Bob) will change as follows: $|0\rangle \leftrightarrow |1\rangle$ or $|+\rangle \leftrightarrow |-\rangle$.

On the other hand, a successful BSM of Charlie corresponds to the observation of precisely two detectors being triggered [15]: A click in D_{1H} and D_{2V}, or in D_{1V} and D_{2H}, indicates a projection into the Bell state $|\psi^-\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$, while a click in D_{1H} and D_{1V}, or in D_{2H} and D_{2V}, reveals a projection into the Bell state $|\psi^+\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$. However, if it inputs other two Bell states $|\phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$ and $|\phi^-\rangle = 1/\sqrt{2}(|00\rangle - |11\rangle)$, Charlie cannot successfully identify them with 100% probability, i.e., the fail event.

In turn, two polarization states with the same basis can be represented by four Bell states as follows:

$$|00\rangle = 1/\sqrt{2}\left(|\phi^+\rangle + |\phi^-\rangle\right) \tag{18}$$

$$|01\rangle = 1/\sqrt{2}\left(|\psi^+\rangle + |\psi^+\rangle\right) \tag{19}$$

$$|10\rangle = 1/\sqrt{2}\left(|\psi^+\rangle - |\psi^+\rangle\right) \tag{20}$$

$$|11\rangle = 1/\sqrt{2}\left(|\phi^+\rangle - |\phi^-\rangle\right) \tag{21}$$

$$|{+}{+}\rangle = 1/\sqrt{2}\left(|\phi^+\rangle + |\psi^+\rangle\right) \tag{22}$$

$$|{+}{-}\rangle = 1/\sqrt{2}\left(|\phi^-\rangle - |\psi^-\rangle\right) \tag{23}$$

$$|{-}{+}\rangle = 1/\sqrt{2}\left(|\phi^-\rangle + |\psi^-\rangle\right) \tag{24}$$

$$|{-}{-}\rangle = 1/\sqrt{2}\left(|\phi^+\rangle - |\psi^+\rangle\right) \tag{25}$$

Therefore, we can deduce the measurement results of honest Charlie for various combinations, as listed in Table 3, where Fail means that the measurement result is not $|\psi^+\rangle$ or $|\psi^+\rangle$ precisely. For example, the initial states of the WCP pair prepared by Alice and Bob are $|0\rangle$ and $|1\rangle$, respectively. Furthermore, $\sum_{i=1}^{m} r_i[j] = 1$ and $\sum_{i=m+1}^{n} r_i[j] = 0$. So, two incoming states of Charlie will be $|1\rangle$ and $|1\rangle$. By Eq. (21), Charlie will get the fail event, i.e., he cannot identify if the projection result is $|\phi^+\rangle$ or $|\phi^-\rangle$ precisely.

Furthermore, by Table 3, it is easy to summarize various cases of Table 1.

Table 3 Detailed combinations of public information

$\|\|W_L\rangle_j$	$\|\|W_R\rangle_j$	$r_L[j]$	$r_R[j]$	Charlie's measured results
$\|0\rangle$	$\|0\rangle$	0	0	Fail
$\|0\rangle$	$\|0\rangle$	0	1	$\|\psi^+\rangle/\|\psi^-\rangle$
$\|0\rangle$	$\|0\rangle$	1	0	$\|\psi^+\rangle/\|\psi^-\rangle$
$\|0\rangle$	$\|0\rangle$	1	1	Fail
$\|0\rangle$	$\|1\rangle$	0	0	$\|\psi^+\rangle/\|\psi^-\rangle$
$\|0\rangle$	$\|1\rangle$	0	1	Fail
$\|0\rangle$	$\|1\rangle$	1	0	Fail
$\|0\rangle$	$\|1\rangle$	1	1	$\|\psi^+\rangle/\|\psi^-\rangle$
$\|1\rangle$	$\|0\rangle$	0	0	$\|\psi^+\rangle/\|\psi^-\rangle$
$\|1\rangle$	$\|0\rangle$	0	1	Fail
$\|1\rangle$	$\|0\rangle$	1	0	Fail
$\|1\rangle$	$\|0\rangle$	1	1	$\|\psi^+\rangle/\|\psi^-\rangle$
$\|1\rangle$	$\|1\rangle$	0	0	Fail
$\|1\rangle$	$\|1\rangle$	0	1	$\|\psi^+\rangle/\|\psi^-\rangle$
$\|1\rangle$	$\|1\rangle$	1	0	$\|\psi^+\rangle/\|\psi^-\rangle$
$\|1\rangle$	$\|1\rangle$	1	1	Fail
$\|+\rangle$	$\|+\rangle$	0	0	Fail/$\|\psi^+\rangle$
$\|+\rangle$	$\|+\rangle$	0	1	Fail/$\|\psi^-\rangle$
$\|+\rangle$	$\|+\rangle$	1	0	Fail/$\|\psi^-\rangle$
$\|+\rangle$	$\|+\rangle$	1	1	Fail/$\|\psi^+\rangle$
$\|+\rangle$	$\|-\rangle$	0	0	Fail/$\|\psi^-\rangle$
$\|+\rangle$	$\|-\rangle$	0	1	Fail/$\|\psi^-\rangle$
$\|+\rangle$	$\|-\rangle$	1	0	Fail/$\|\psi^+\rangle$
$\|+\rangle$	$\|-\rangle$	1	1	Fail/$\|\psi^+\rangle$
$\|-\rangle$	$\|+\rangle$	0	0	Fail/$\|\psi^-\rangle$
$\|-\rangle$	$\|+\rangle$	0	1	Fail/$\|\psi^+\rangle$
$\|-\rangle$	$\|+\rangle$	1	0	Fail/$\|\psi^+\rangle$
$\|-\rangle$	$\|+\rangle$	1	1	Fail/$\|\psi^-\rangle$
$\|-\rangle$	$\|-\rangle$	0	0	Fail/$\|\psi^+\rangle$
$\|-\rangle$	$\|-\rangle$	0	1	Fail/$\|\psi^-\rangle$
$\|-\rangle$	$\|-\rangle$	1	0	Fail/$\|\psi^-\rangle$
$\|-\rangle$	$\|-\rangle$	1	1	Fail/$\|\psi^+\rangle$

$r_L[j] = \sum_{i=1}^{m} r_i[j]mod2$ and $r_R[j] = \sum_{i=m+1}^{n} r_i[j]mod2$

In turn, by Alice and Bob's initial states and Charlie's measured result, it can accurately deduce $r[l] = \sum_{i=1}^{n} r_i[l]mod2 = 1$ or 0, as listed in Table 2. That is, if $r_L[l] = r_R[l]$, then $r[l] = r_L[l] + r_R[l] = 0$; Otherwise $r[l] = 1$.

In addition,

$$\begin{aligned} r^* &= \sum_{i=1}^{n} (x_i + r_i[l])mod2 \\ &= \sum_{i=1}^{n} x_i mod2 + \sum_{i=1}^{n} r_i[l]mod2 \end{aligned} \tag{26}$$

So, it can get $\sum_{i=1}^{n} x_i mod2 = r^*$ or $(r^* + 1)mod2$ accordingly. For example, Alice, Bob and Charlie's public messages are $|1\rangle$, $|1\rangle$ and $|\psi^+\rangle/|\psi^+\rangle$, respectively. By Eq. (21), Charlie should get the fail event theoretically, instead of the successful event (i.e., $|\psi^+\rangle/|\psi^+\rangle$). That can only mean $\sum_{i=1}^{n} r_i[l]mod2 = 1$. Accordingly, $\sum_{i=1}^{n} x_i mod2 = (r^* + 1)mod2$. Table 4 lists all successful combinations.

Therefore, our proposed quantum SMM2S protocol is correct.

Please note that in the proof above, we assume that the proposed protocols run in ideal conditions (i.e., there are no technical errors and the transmission channels are lossless and noiseless).

Table 4 The final computing results

$\|\|W_L\rangle_l$	$\|\|W_R\rangle_l$	Charlie's measured results	$r[l]$	$\sum_{i=1}^{n} x_i$
$\|0\rangle$	$\|0\rangle$	$\|\psi^+\rangle/\|\psi^-\rangle$	1	$r^* + 1$
$\|0\rangle$	$\|1\rangle$	$\|\psi^+\rangle/\|\psi^-\rangle$	0	r^*
$\|1\rangle$	$\|0\rangle$	$\|\psi^+\rangle/\|\psi^-\rangle$	0	r^*
$\|1\rangle$	$\|1\rangle$	$\|\psi^+\rangle/\|\psi^-\rangle$	1	$r^* + 1$
$\|+\rangle$	$\|+\rangle$	$\|\psi^+\rangle$	0	r^*
$\|+\rangle$	$\|+\rangle$	$\|\psi^-\rangle$	1	$r^* + 1$
$\|+\rangle$	$\|-\rangle$	$\|\psi^-\rangle$	0	r^*
$\|+\rangle$	$\|-\rangle$	$\|\psi^+\rangle$	1	$r^* + 1$
$\|-\rangle$	$\|+\rangle$	$\|\psi^-\rangle$	0	r^*
$\|-\rangle$	$\|+\rangle$	$\|\psi^+\rangle$	1	$r^* + 1$
$\|-\rangle$	$\|-\rangle$	$\|\psi^+\rangle$	0	r^*
$\|-\rangle$	$\|-\rangle$	$\|\psi^-\rangle$	1	$r^* + 1$

6.2 Security

According to the specific quantum SMMdS protocol, it is equivalent to running the quantum SMM2S protocol n times (see Fig. 2). So, the security of the specific quantum SMMdS protocol is guaranteed by that of the proposed quantum SMM2S protocol. In the following theorem, we will prove that our proposed quantum SMM2S protocol is information-theoretically secure.

Theorem 2 *The proposed quantum SMM2S protocol is information-theoretically secure.*

Proof On the one hand, before publishing the classical information of $k_i[j]$, each party P_i privately performs two quantum operators $U_Y^{r_i[j]}H^{k_i[j]}$ on the j th WCP, that is, he encrypts the j th WCP by using two random but private bits. Similarly, it is a perfect quantum encryption [19], which is information-theoretically secure.

Now, the protocol is informationally secure if for every input state ρ, the output state ρ_c is the totally mixed state: The relation of the input state ρ_{in} and the output state ρ_{out} is as follows:

$$\rho_{out} = \sum_k p_k U_k \rho_{in} U_k^\dagger = \frac{1}{2^t} I \tag{27}$$

Here, ρ_{in} is the density matrix of all possible t-qubit input states and U_k is the corresponding unitary operator applied to the input state.

For simplicity, we only analyze the j th WCP in our protocol. Accordingly, we can get

$$\rho_{in}(WCP_j) = \left(\frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|\right) \tag{28}$$

Furthermore,

$$r_i[j],\ k_i[j] \in_R \{0,\ 1\} \tag{29}$$

So, after the party P_i performing the corresponding operators, the output state should be in

$$\begin{aligned}\rho_{out}(WCP_j) =& \frac{1}{4}\left[U_Y^0 H^0\left(\frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|\right)\right] \\ &+ \frac{1}{4}\left[U_Y^0 H^1\left(\frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|\right)\right] \\ &+ \frac{1}{4}\left[U_Y^1 H^0\left(\frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|\right)\right] \\ &+ \frac{1}{4}\left[U_Y^1 H^1\left(\frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|\right)\right]\end{aligned}$$

$$
\begin{aligned}
&+\frac{1}{4}\left[\left(\frac{1}{4}|+\rangle\langle+| + \frac{1}{4}|-\rangle\langle-|\right) + \frac{1}{4}|0\rangle\langle0| + \frac{1}{4}|1\rangle\langle1|\right]\\
&+\frac{1}{4}\left[\left(\frac{1}{4}|1\rangle\langle1| + \frac{1}{4}\Big|0\rangle\langle0\Big| + \frac{1}{4}\Big|-\rangle\langle-\Big| + \frac{1}{4}\Big|+\rangle\langle+\Big|\right)\right]\\
&+\frac{1}{4}\left[\left(\frac{1}{4}|-\rangle\langle-| + \frac{1}{4}|+\rangle\langle+| + \frac{1}{4}|1\rangle\langle1| + \frac{1}{4}|0\rangle\langle0|\right)\right]\\
&=\frac{1}{4}[|0\rangle\langle0|+|1\rangle\langle1|+|+\rangle\langle+|+|-\rangle\langle-|]\\
&=\frac{1}{4}\left[\begin{pmatrix}1&0\\0&0\end{pmatrix}+\begin{pmatrix}0&0\\0&1\end{pmatrix}+\frac{1}{2}\begin{pmatrix}1&1\\1&1\end{pmatrix}+\frac{1}{2}\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\right]\\
&=\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}=\frac{1}{2}I
\end{aligned}
\tag{30}
$$

From Eq. (30), we can see that the output of the j th WCP after the party P_i performing private operators is just a totally mixed state. So, anyone including the next party P_{i+1} cannot get any information about the party P_i's secret bits $r_i[j]$ and $k_i[j]$. That is, it is a perfect quantum encryption.

After publishing the classical information of $k_i[j]$, each party P_i computes and opens $r_i^*[l] = (x_i + r_i[l]) mod 2$, where $r_i[l]$ is random and private. Clearly, it is a classical one-time pad.

In short, perfect quantum encryption and classical one-time pad can ensure the information-theoretical security of the proposed quantum protocols.

In addition, the checking events, which are similar to the decoy WCPs in MDI-QKD protocols [20], can ensure the honesty of all agents and resist the outsider's eavesdropping.

Of course, only if all parties execute the protocol honestly, it can output the right results. Due to perfect quantum encryption (by Theorem 2), the party P_{i-1} or P_{i+1} cannot get more information about any party P_i than other parties, though all quantum resources are transmitted in order from P_1 (P_{m+1}) to P_m (P_n). So, the proposed quantum SMM2S protocol can achieve the fairness.

In addition, like most existing multiparty quantum computations, our proposed quantum SMM2S protocol needs authenticated quantum channels, which can ensure the authenticity of quantum resources and participant identities. In principle, we may combine quantum authentication technologies [21] with classical authentication technologies [22] to implement various authentications in quantum channels.

6.3 Performance

The proposed quantum SMM2S protocol takes weak coherent pulses (WCPs) as quantum resources and accordingly needs single-particle operators (i.e., U_Y and$H$) and Bell state measurements (i.e., identifications). Obviously, it is acceptable and feasible with current technology. Furthermore, in the specific quantum SMMdS protocol, there are

t WCP pairs ($t \approx 16n$) prepared by Alice and Bob, respectively. Accordingly, the proposed specific quantum SMMdS protocol's communicational complexity is $O\left(n^2\right)$, which just achieves the optimal bound of the information-theoretically secure SMS.

In above proposed quantum SMM2S/ SMMdS protocols, we divide all parties into two groups, so the probability satisfying the useful condition of the sequence number j (i.e., both $\sum_{i=1}^{m} k_i[j] mod 2 = 0$ and $\sum_{i=m+1}^{n} k_i[j] mod 2 = 0$) is $1/4$. If we only consider all parties located in a group, then the probability will be increased to $1/2$. In addition, if we introduce a quantum cloud who is responsible for generating all quantum resources, then we can discard the assumption that Alice and Bob shared a key k in advance.

Furthermore, we give detailed performance comparisons of our proposed SMM2S/SMMdS protocols with other related protocols in terms of the main quantum resources, the required operators and measurements, the transmitted qubits, and other features, respectively, which are listed in Table 5.

In Table 5, the first two protocols only need ideal single photons, while the middle two protocols require multi-qubit entangled states. At present, it is still difficult to prepare multi-qubit entangled states and accordingly implement the complicated oracle operators and measurements in high-dimensional Hilbert space. Furthermore, the former three protocols only compute the bitwise XOR (i.e., modulo-2 summation), not any modulo-d summation. In Table 5, only our proposed protocols are based on measurement-device-independent quantum cryptography. It is well known that it is immune to all side-channel attacks against the detectors of measurement-device-independent quantum cryptography. That is, it removes all quantum attacks in the detection part, so our measurement devices can be controlled by an untrusted third party.

At present, we do not consider noise of quantum channels and loss of WCPs in our proposed quantum protocols. Obviously, we can increase the number of transmitting WCPs (i.e., increasing t) in practical applications and adopt classical error-correction technology to avoid these problems. In addition, when the parties are far apart, we may deploy a quantum repeater at a certain party, which is used to forward private and unknown states of qubits based on teleportation.

In a word, it is feasible to implement our proposed quantum protocols with the present quantum technologies.

7 Conclusion

In this paper, we defined two kinds of secure multiparty summations. Furthermore, under considering the practical security and technical feasibility, we presented the corresponding measurement-device-independent quantum secure multiparty summation protocols, which take weak coherent pulses as quantum resources and only need to perform simple single-particle operators and Bell-state identifications. Therefore, the proposed MDI quantum protocols are feasible with the current technology.

Table 5 The performance comparisons

Protocols	Quantum resources	Quantum operators	Quantum measurements	Transmitted qubits	The Third Party	MDI-based
Zhang et al. [9]	Single Photons	SOs	SMs	$O(n\log N)$	Semi-honest	–
Zhang et al. [12]	Single Photons	$CNOT$ s and H s	SMs	$O(n\log N)$	No	–
Chen et al. [8]	n-qubit GHZ states	SOs	BMs, SMs	$O(n\log N)$	Semi-honest	–
Shi et al. [11]	$O(\log N)$-qubit entangled states	$CNOT$ s, QFT s,QFT^{-1} s, and Oracle operators	$O(\log N)$-qubit projective measurements	$O(n\log N)$	No	–
SMM2S	WCPs	SOs	Bell-state identifications	$O(n\log N)$	Untrusted	Yes
SMMdS	WCPs	SOs	Bell-state identifications	$O\left(n^2\log N\right)$	Untrusted	Yes

SO: Single-photon operators, BM: Bell measurements, SM: Single-photon projective measurements, and QFT: quantum Fourier transform. In addition, n and $\log N$ denote the number of the participants and the bit length of each private input, respectively

There are good application prospects of our proposed protocols in future quantum internet, e.g., quantum-secured blockchain and quantum federated learning. In addition, the proposed quantum protocols show a feasible MDI communication model, which is also suitable for more secure multiparty computations, e.g., quantum secret sharing.

Acknowledgements This work was supported by National Natural Science Foundation of China (No. 61772001).

Data availability Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors declare they have no financial interests.

References

1. Yang, Y.G., Wang, Y.C., Yang, Y.L., et al.: Participant attack on the deterministic measurement-device-independent quantum secret sharing protocol. Sci. China-Phys. Mech. Astron. **64**(6), 260321 (2021)
2. Shi, R.H., Mu, Y., Zhong, H., Zhang, S., Cui, J.: Quantum private set intersection cardinality and its application to anonymous authentication. Inform. Sci. **370–371**, 147–158 (2016)
3. Kiktenko, E.O., Pozhar, N.O., Anufriev, M.N., et al.: Quantum-secured blockchain. Quantum Sci Technol **3**, 035004 (2018)
4. Shi, R.H., Zhang, M.: Privacy-preserving quantum sealed-bid auction based on grover's search algorithm. Sci. Rep. **9**, 7626 (2019)
5. Vaccaro, J.A., Spring, J., Chefles, A.: Quantum protocols for anonymous voting and surveying. Phys. Rev. A **75**(1), 012333 (2007)
6. Chen S.Y., Yoo S.: Federated Quantum Machine Learning, arXiv:math/2103.12010, (2021)
7. Du, J.Z., Chen, X.B., Wen, Q.X., Zhu, F.C.: Secure multiparty quantum summation. Acta Physica Sinica **56**(11), 6214–6219 (2007)
8. 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)
9. 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)
10. Zhang, C., Sun, Z.W., Huang, X.: Three-party quantum summation without a trusted third party. Int. J. Quantum Inf. **13**(2), 1550011 (2015)
11. Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep. **6**, 19655 (2016)
12. 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)
13. Shi, R.H., Zhang, S.: Quantum solution to a class of two-party private summation problems. Quantum Inf Process **16**, 225 (2017)
14. Yang, H.Y., Ye, T.Y.: Secure multi-party quantum summation based on quantum Fourier transform. Quantum Inf Process **17**, 129 (2018)
15. Lo, H.-K., Curty, M., Qi, B.: Measurement device independent quantum key distribution". Phys. Rev. Lett. **108**, 130503 (2012)
16. Xu, F., Qi, B., Liao, Z., Lo, H.-K.: Long distance measurement-device-independent quantum key distribution with entangled photon sources. Appl. Phys. Lett. **103**, 061101 (2013)
17. Xu, F., Curty, M., Qi, B., Lo, H.-K.: Measurement-device-independent quantum cryptography. IEEE J. Sel. Top. Quantum Electron. **21**(3), 6601111 (2014)
18. Nielsen M.A., & Chuang I.L.: Quantum Computation and Quantum Information: 10th Anniversary Edition, Cambridge University Press. (2011)

19. Boykin, P.O., Roychowdhury, V.: Optimal encryption of quantum bits. Phys. Rev. A **67**(4), 042317 (2003)
20. Hwang, W.-Y.: Quantum key distribution with high loss: toward global secure communication. Phys. Rev. Lett. **91**, 057901 (2003)
21. Shi, R.H.: Anonymous quantum sealed-bid auction. IEEE Trans. Circuits Syst. II: Exp. Briefs (Early Access) (2021). https://doi.org/10.1109/TCSII.2021.3098755
22. Shi, R.H.: Useful equations about bell states and their applications to quantum secret sharing. IEEE Commun. Lett. **24**(2), 386–390 (2019)

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