www.nature.com/scientificreports

SCIENTIFIC REPORTS

OPEN

Secure Multiparty Quantum Computation for Summation and Multiplication

Received: 25 September 2015
Accepted: 08 December 2015
Published: 21 January 2016

Run-hua Shi[1,2], Yi Mu[2], Hong Zhong[1], Jie Cui[1] & Shun Zhang[1]

As a fundamental primitive, Secure Multiparty Summation and Multiplication can be used to build complex secure protocols for other multiparty computations, specially, numerical computations. However, there is still lack of systematical and efficient quantum methods to compute Secure Multiparty Summation and Multiplication. In this paper, we present a novel and efficient quantum approach to securely compute the summation and multiplication of multiparty private inputs, respectively. Compared to classical solutions, our proposed approach can ensure the unconditional security and the perfect privacy protection based on the physical principle of quantum mechanics.

Secure Multiparty Computation (SMC)[1] is an important branch in modern cryptography. Secure Multiparty Summation or Multiplication is a fundamental primitive of SMC that enables multiple parties to jointly compute the summation or multiplication of their respective private inputs without revealing any private input. As we know, Secure Multiparty Summation and Multiplication can be used to build complex secure protocols for other multiparty computations, specially, numerical computations. In addition, there are also lots of other important applications of Secure Multiparty Summation and Multiplication in distributed networks, such as secret sharing, electronic voting, secure sorting, data mining and so on.

On the one hand, there existed some classical protocols for Secure Multiparty Summation[2–4] and Multiplication[5–7], which were based on classical cryptography. However, classical cryptography cannot provide the unconditionally secure communications and cannot resist the attack of the quantum computer especially.

On the other hand, quantum cryptography can provide the unconditional security, which is guaranteed by physical principles of quantum mechanics. Since Bennett and Brassard[8] presented the first quantum key distribution protocol (BB84 protocol), quantum cryptography has been widely studied and rapidly developed. Compared to classical cryptography, the most important advantage is that an eavesdropper can easily be detected by using the characteristics of quantum mechanics. Therefore, a lot of results have been gained, such as quantum key distribution, quantum teleportation, quantum secret sharing, quantum secure direct communication, quantum key agreement, quantum signature and so on. Furthermore, SMC is also studied extensively in quantum cryptography[9–14].

However, there are only a few quantum protocols for Secure Multiparty Summation. In 2007, Du *et al.*[15] presented a secure quantum addition module $n+1$ based on non-orthogonal states, where n denoted the number of all parties. In 2010, Chen *et al.*[16] proposed another secure quantum addition module 2 based on multi-particle entangled states with the trusted third party. However, the module of the two protocols is too small, so that it limits their more extensive applications. Furthermore, the two protocols lack high communication efficiencies due to their bit-by-bit computation and communication. In addition, to the best of our knowledge, there is no any quantum protocol for Secure Multiparty Multiplication.

In this paper, we present a novel quantum approach to systematically and efficiently compute Secure Multiparty Summation and Multiplication, in which the computations of Secure Multiparty Summation and Multiplication are securely translated into the computations of the corresponding phase information by the quantum Fourier transform, and later the phase information is extracted out after performing an inverse quantum Fourier transform.

Here, we first introduce the quantum Fourier transform, which will be used later in proposed protocols. The quantum Fourier transform is a linear transformation on qubits, and is the quantum version of the standard

[1]School of Computer Science and Technology, Anhui University, Hefei City, 230601, China. [2]Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Wollongong NSW 2522, Australia. Correspondence and requests for materials should be addressed to R.H.S. (email: shirh@ahu.edu.cn)

discrete Fourier transform. For $x \in \{0, 1, \ldots, N-1\}$, the quantum Fourier transform and the inverse quantum Fourier transform are defined as follows[17]:

$$QFT: |x\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{2\pi i \frac{x}{N} y}|y\rangle, \tag{1}$$

$$QFT^{-1}: |y\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} e^{-2\pi i \frac{y}{N} x}|x\rangle. \tag{2}$$

Furthermore,

$$\sum_{y=0}^{N-1} e^{2\pi i \frac{x}{N} y} = \begin{cases} 0 & \text{if } x \neq 0 mod N \\ N & \text{if } x = 0 mod N \end{cases}, \tag{3}$$

so,

$$\begin{aligned} QFT^{-1}\left(\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{2\pi i \frac{x}{N} y}|y\rangle\right) &= \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{2\pi i \frac{x}{N} y} QFT^{-1}|y\rangle \\ &= \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{2\pi i \frac{x}{N} y}\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{-2\pi i \frac{y}{N} j}|j\rangle \\ &= \frac{1}{N}\sum_{j=0}^{N-1}\sum_{y=0}^{N-1} e^{2\pi i \frac{x-j}{N} y}|j\rangle \\ &= \frac{1}{N}\sum_{y=0}^{N-1} e^{2\pi i \frac{x-x}{N} y}|x\rangle + \frac{1}{N}\sum_{j=0 \wedge j\neq x}^{N-1}\left(\sum_{y=0}^{N-1} e^{2\pi i \frac{x-j}{N} y}\right)|j\rangle \\ &= \frac{1}{N}\sum_{y=0}^{N-1}|x\rangle + \frac{1}{N}\sum_{j=0 \wedge j\neq x}^{N-1} 0\cdot|j\rangle = |x\rangle \end{aligned}. \tag{4}$$

That is,

$$QFT^{-1}(QFT|x\rangle) = |x\rangle. \tag{5}$$

In addition, another multi-qubit quantum logic gate, which will be used later in proposed protocols, is the controlled-NOT or *CNOT* gate: $|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |01\rangle, |10\rangle \rightarrow |11\rangle$ and $|11\rangle \rightarrow |10\rangle$, where the first qubit is the control qubit, and the second qubit is the target qubit. That is, if the control qubit is set to 0, then the target qubit is left alone. If the control qubit is set to 1, then the target qubit is flipped.

Results

Proposed protocols.

Secure multiparty quantum summation. Assume that there are n parties: $P_1, P_2, \ldots, P_n$ ($n > 2$), where each party P_k ($1 \leq k \leq n$) has a secret integer $x_k \in \{0, 1, \ldots, N-1\}$ ($N = 2^m$), and further all n parties want to jointly compute the summation $\sum_{k=1}^{n} x_k mod N$ without revealing their respective secret x_ks. In the following Protocol I, we suppose that P_1 is the initiator party.

Protocol I (*Secure multiparty quantum summation*)

Step 1. The initiator P_1 first prepares an m-qubit basis state $|x_1\rangle_h$, where $m = \log N$ and x_1 is his private secret. Then P_1 applies a quantum Fourier transform to the state $|x_1\rangle_h$ and gets the resultant state $|\psi_1\rangle$. That is,

$$|\psi_1\rangle = QFT|x_1\rangle_h = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{x_1}{N} j}|j\rangle_h. \tag{6}$$

Step 2. P_1 prepares another m-qubit ancillary state $|0\rangle_t$ and further performs m *CNOT* gate operators on the product state $|\psi_1\rangle|0\rangle_t$, where each qubit of the first m qubits is the control qubit and the corresponding qubit of the second m qubits is the target qubit. Here we call the resultant state $|\psi_2\rangle$, which is written as

$$\begin{aligned} |\psi_2\rangle &= CNOT^{\otimes m}|\psi_1\rangle 0\rangle_t \\ &= CNOT(1, m+1) \otimes CNOT(2, m+2) \ldots \\ &\quad \otimes CNOT(m, 2m)\left(\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{x_1}{N} j}|j\rangle_h|0\rangle_t\right) \\ &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{x_1}{N} j}|j\rangle_h|j\rangle_t \end{aligned}. \tag{7}$$

Clearly, $|\psi_2\rangle$ is an entangled state, where the subscript h or t denotes that the qubits will stay at home or be transmitted through the quantum channel.

Step 3. P_1 sends the second m qubits (i.e., the ancillary state $|j\rangle_t$) to P_2 through the authenticated quantum channel.

Step 4. After receiving the ancillary state $|j\rangle_t$, P_2 first prepares his secret state $|x_2\rangle$. Then he applies an oracle operator C_j on $|j\rangle_t|x_2\rangle$, where C_j is defined by

$$C_j\colon\ |j\rangle_t|x_2\rangle \rightarrow |j\rangle_t U^j|x_2\rangle, \tag{8}$$

with

$$U|x_2\rangle = e^{2\pi i\frac{x_2}{N}}|x_2\rangle. \tag{9}$$

That is, $|x_2\rangle$ is an eigenvector of U with the eigenvalue $e^{2\pi i\frac{x_2}{N}}$. After applying the oracle operator C_j, the whole composite quantum systems of P_1 and P_2 are in the following state

$$\begin{aligned} |\psi_3\rangle &= C_j\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\frac{x_1}{N}j}|j\rangle_h|j\rangle_t|x_2\rangle \\ &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\frac{x_1}{N}j}|j\rangle_h|j\rangle_t U^j|x_2\rangle \\ &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\frac{x_1}{N}j}|j\rangle_h|j\rangle_t e^{2\pi i\frac{x_2}{N}j}|x_2\rangle \\ &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\frac{x_1+x_2}{N}j}|j\rangle_h|j\rangle_t|x_2\rangle \end{aligned} \tag{10}$$

Step 5. Furthermore, P_2 passes the ancillary state $|j\rangle_t$ to P_3 through the authenticated quantum channel and keeps $|x_2\rangle$ in secret. Afterward, P_3 executes the similar process of P_2, and so on. This process is repeated $n-1$ times, so that, if everyone honestly executes the protocol, the composite quantum systems of all n parties are in the following state

$$|\psi_4\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\left(\frac{\sum_{k=1}^{n}x_k}{N}\right)j}|j\rangle_h|j\rangle_t|x_2\rangle\ldots|x_n\rangle. \tag{11}$$

Step 6. Finally, P_n sends the ancillary state $|j\rangle_t$ back to P_1. After receiving the ancillary state $|j\rangle_t$, P_1 again applies $CNOT^{\otimes m}$ on his $2m$ qubits, where each qubit of the first m qubits is the control qubit and the corresponding qubit of the second m qubits is the target qubit. Call the resultant state $|\psi_5\rangle$. That is,

$$\begin{aligned} |\psi_5\rangle &= CNOT^{\otimes m}|\psi_4\rangle \\ &= CNOT^{\otimes m}\left[\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\left(\frac{\sum_{k=1}^{n}x_k}{N}\right)j}|j\rangle_h|j\rangle_t|x_2\rangle\ldots|x_n\rangle\right]. \\ &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\left(\frac{\sum_{k=1}^{n}x_k}{N}\right)j}|j\rangle_h|0\rangle_t|x_2\rangle\ldots|x_n\rangle \end{aligned} \tag{12}$$

Step 7. Furthermore, P_1 measures the second m qubits (i.e., $|0\rangle_t$) in the computational basis. If the measured result is $|0\rangle$, then he continues to execute the next step; otherwise he believes that there is at least one dishonest party and ends this protocol.

Step 8. Finally, P_1 applies QFT^{-1} to the first m qubits and further measures it to obtain $|\omega\rangle$, where $\omega = \sum_{k=1}^{n}x_k modN$.

The correctness proof.

$$\begin{aligned} QFT^{-1}\left(\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\left(\frac{\sum_{k=1}^{n}x_k}{N}\right)j}|j\rangle_h\right) &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\left(\frac{\sum_{k=1}^{n}x_k}{N}\right)j}QFT^{-1}|j\rangle_h \\ &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\left(\frac{\sum_{k=1}^{n}x_k}{N}\right)j}\left(\frac{1}{\sqrt{N}}\sum_{l=0}^{N-1}e^{-2\pi i\frac{j}{N}l}|l\rangle_h\right) \\ &= \frac{1}{N}\sum_{j=0}^{N-1}\sum_{l=0}^{N-1}e^{2\pi i\frac{(\sum_{k=1}^{n}x_k)-l}{N}j}|l\rangle_h \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{N}\sum_{j=0}^{N-1}\left|\sum_{k=1}^{n}x_k modN\right\rangle_h \\
&\quad +\frac{1}{N}\sum_{\substack{l=0\\ l\neq\sum_{k=1}^{n}x_k modN}}^{N-1}\left(\sum_{j=0}^{N-1}e^{2\pi i\frac{(\sum_{k=1}^{n}x_k)-l}{N}j}\right)|l\rangle_h \\
&= \left|\sum_{k=1}^{n}x_k modN\right\rangle_h + \frac{1}{N}\sum_{\substack{l=0\\ l\neq\sum_{k=1}^{n}x_k modN}}^{N-1} 0\cdot|l\rangle_h \quad (\text{by Eq. (3)}) \\
&= \left|\sum_{k=1}^{n}x_k modN\right\rangle_h = |\omega\rangle_h.
\end{aligned}
\tag{13}
$$

Therefore, if all parties honestly execute this protocol, P_1 will rightly get $\sum_{k=1}^{n} x_k modN$.

Secure multiparty quantum multiplication. Assume that there are n parties $P_1, P_2, \ldots, P_n (n > 2)$, each party with a private secret $x_k \in \{0, 1, 2\ldots, N-1\} (N = 2^m)$, and all n parties want to jointly compute the multiplication of their respective private secret, i.e., $\prod_{k=1}^{n} x_k modN$. Since each secret x_k can be split and expressed as $x_k = 2^{m_k}\cdot s_k$, where s_k is an odd integer, then we can get

$$
\prod_{k=1}^{n} x_k modN = \left(2^{\sum_{k=1}^{n} m_k}\prod_{k=1}^{n} s_k\right) modN. \tag{14}
$$

By Eq. (14), if we get the results of $\sum_{k=1}^{n} m_k modN$ and $\prod_{k=1}^{n} s_k modN$, then we can easily compute $\prod_{k=1}^{n} x_k modN$. Accordingly, the computation of $\prod_{k=1}^{n} x_k modN$ can be translated into the computations of $\sum_{k=1}^{n} m_k modN$ and $\prod_{k=1}^{n} s_k modN$, respectively. We have proposed Protocol I to compute $\sum_{k=1}^{n} m_k modN$. Furthermore, we present Protocol II to compute $\prod_{k=1}^{n} s_k modN$, where all s_ks are odd integers. Similarly, in the following Protocol II, we suppose that P_1 is the initiator.

Protocol II (*Secure multiparty quantum multiplication*)

Step 1. The initiator P_1 randomly chooses an odd integer $r \in \{1, 3\ldots, N-1\}$ and further prepares two m qubits in the original state $\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i\frac{r}{N}j}|j\rangle_{t_1}|j\rangle_{t_2}$, where the preparation process is the same as that of Step 1 and 2 in Protocol I. Then P_1 sends $|j\rangle_{t_1}$ to P_2 through the authenticated quantum channel and keeps $|j\rangle_{t_2}$ in hand.

Step 2. After receiving $|j\rangle_{t_1}$, P_2 applies an oracle operator U_2 on $|j\rangle_{t_1}$ by his private secret s_2, where U_2 is defined by,

$$
U_2|j\rangle_{t_1} = |js_2^{-1} modN\rangle_{t_1}. \tag{15}
$$

Please note that s_2 is an odd integer and $N = 2^m$, thus there exists its modulo-N multiplicative inverse s_2^{-1}, which implies that U_2 is inverse. Furthermore, P_2 sends $|js_2^{-1}modN\rangle_{t_1}$ to P_3 through the authenticated quantum channel. Afterward, P_3 executes the similar process of P_2 (i.e., $U_3|js_2^{-1}modN\rangle_{t_1} = |js_2^{-1}s_3^{-1}modN\rangle_{t_1}$), and so on. This process is repeated $n-1$ times, so that, if everyone honestly executes the protocol, the final quantum states of the qubits of the subscripts t_1 and t_2 are in,

$$
\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i\frac{r}{N}j}|js_2^{-1}\ldots s_n^{-1}modN\rangle_{t_1}|j\rangle_{t_2}. \tag{16}
$$

Finally, P_n sends $|js_2^{-1}\ldots s_n^{-1}modN\rangle_{t_1}$ back to P_1.

Step 3. After receiving the returned state $|js_2^{-1}\ldots s_n^{-1}modN\rangle_{t_1}$, P_1 continues to send $|j\rangle_{t_2}$ to P_2 through the authenticated quantum channel.

Step 4. After receiving the state $|j\rangle_{t_2}$, P_2 again applies the oracle operator U_2 on $|j\rangle_{t_2}$ by his private input s_2, i.e., $U_2|j\rangle_{t_2} = |js_2^{-1}modN\rangle_{t_2}$. Furthermore he sends it to P_3 through the authenticated quantum channel, and so on. This process is repeated $n-1$ times, so that, if everyone honestly executes the protocol, the final quantum states of the $2m$ qubits are in,

$$
\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i\frac{r}{N}j}|js_2^{-1}\ldots s_n^{-1}modN\rangle_{t_1}|js_2^{-1}\ldots s_n^{-1}modN\rangle_{t_2}. \tag{17}
$$

Finally, P_n again sends $|js_2^{-1}\ldots s_n^{-1}modN\rangle_{t_2}$ back to P_1.

Step 5. After receiving the state $|js_2^{-1}\ldots s_n^{-1}modN\rangle_{t_2}$, P_1 performs m *CNOT* gate operators on the two returned states, such that the quantum systems of the subscripts t_1 and t_2 will be disentangled. That is,

$$CNOT^{\otimes m}\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\frac{r}{N}j}|js_2^{-1}\ldots s_n^{-1}modN\rangle_{t_1}|js_2^{-1}\ldots s_n^{-1}modN\rangle_{t_2}$$
$$=\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\frac{r}{N}j}|js_2^{-1}\ldots s_n^{-1}modN\rangle_{t_1}|0\rangle_{t_2}. \tag{18}$$

Furthermore, P_1 measures the qubits of the subscript t_2 in the computation basis. If the measured result is $|0\rangle_{t_2}$, then he continues to execute the next step. Otherwise, he believes that there is at least one dishonest party and ends this protocol.

Step 6. Finally P_1 applies an inverse quantum Fourier transform QFT^{-1} on the remaining qubits and further measures it to obtain $|\varpi\rangle_{t_1}$ in the computation basis, where $\varpi = rs_2\ldots s_n modN$. Then P_1 outputs $s_1r^{-1}\varpi modN$. That is, $\prod_{k=1}^{n} s_k modN = s_1r^{-1}\varpi modN$.

The correctness proof.

$$QFT^{-}\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\frac{r}{N}j}|js_2^{-1}\ldots s_n^{-1}modN\rangle_{t_1}$$
$$=\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\frac{r}{N}j}QFT^{-1}|js_2^{-1}\ldots s_n^{-1}modN\rangle_{t_1}$$
$$=\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\frac{r}{N}j}\frac{1}{\sqrt{N}}\sum_{l=0}^{N-1}e^{-2\pi i\frac{js_2^{-1}\ldots s_n^{-1}modN}{N}l}|l\rangle_{t_1}$$
$$=\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi i\frac{r}{N}j}\frac{1}{\sqrt{N}}\sum_{l=0}^{N-1}e^{-2\pi i\frac{ls_2^{-1}\ldots s_n^{-1}modN}{N}j}|l\rangle_{t_1}$$
$$=\frac{1}{N}\sum_{l=0}^{N-1}\sum_{j=0}^{N-1}e^{2\pi i\frac{r-ls_2^{-1}\ldots s_n^{-1}}{N}j}|l\rangle_{t_1}$$
$$=\frac{1}{N}\sum_{j=0}^{N-1}|rs_2\ldots s_n modN\rangle_{t_1}+\frac{1}{N}\sum_{\substack{l=0\\ l\neq rs_2\ldots s_n modN}}^{N-1}\sum_{j=0}^{N-1}e^{2\pi i\frac{r-ls_2^{-1}\ldots s_n^{-1}}{N}j}|l\rangle_{t_1}$$
$$=\frac{1}{N}\sum_{j=0}^{N-1}|rs_2\ldots s_n modN\rangle_{t_1}+\frac{1}{N}\sum_{\substack{l=0\\ l\neq rs_2\ldots s_n modN}}^{N-1}0|l\rangle_{t_1}\text{ (by Eq. (3))}$$
$$=|rs_2\ldots s_n modN\rangle_{t_1}=|\varpi\rangle_{t_1}, \tag{19}$$

since

$$r-ls_2^{-1}\ldots s_n^{-1}=0modN\Rightarrow l=rs_2\ldots s_n modN. \tag{20}$$

Obviously, $s_1r^{-1}\varpi modN = s_1r^{-1}rs_2\ldots s_n modN = s_1s_2\ldots s_n modN$, where r is an odd integer. Therefore, Protocol II can rightly output $\prod_{k=1}^{n} s_k modN$. Furthermore, in order to perfectly compute $\prod_{k=1}^{n} x_k modN$, the initiator first calls Protocol I to securely compute $M=\sum_{k=1}^{n} m_k modN$ and then calls Protocol II to securely compute $S=\prod_{k=1}^{n} s_k modN$. Finally, the initiator computes $X=(2^M S) modN$. Obviously, $X=\prod_{k=1}^{n} x_k modN$.

Security Analysis. We have analyzed the correctness of Protocol I and II, and further analyze their securities. In order to save space, please note that we mainly analyze the security of Protocol I, because the security of Protocol II is the same as that of Protocol I.

We first analyze that P_2 does not get any secret information about the initiator P_1's input x_1. In Protocol I, P_1 only sends the ancillary state $|j\rangle_t$ to P_2 without any classical information. So, for a dishonest P_2, if he wants to eavesdrop P_1's secret, all possible attacks he can perform with the present technology are as follows:

(1) P_2 directly measures the ancillary state $|j\rangle_t$ in the computational basis. Obviously, he will get $|j\rangle$ ($j\in\{0, 1, \ldots, N-1\}$) with the equal probability of $\frac{1}{N}$, but the measured result j is independent of P_1's secret x_1. That is, this attack is infeasible.
(2) After applying a unitary operator on the ancillary state $|j\rangle_t$, P_2 again measures it. Especially, P_2 has a knowledge that P_1's secret state $|x_1\rangle$ has evolved into the same state (i.e., $|j\rangle_h$) as the ancillary state $|j\rangle_t$ based on the quantum Fourier transform, so he may perform an inverse quantum Fourier transform QFT^{-1} on the ancillary state $|j\rangle_t$ to expect to extract out x_1. That is, this attack can be described as follows:

$$\begin{aligned} QFT^{-1}\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{x_1}{N} j}|j\rangle_h |j\rangle_t &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{x_1}{N} j}|j\rangle_h QFT^{-1}|j\rangle_t \\ &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{x_1}{N} j}|j\rangle_h \left(\frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} e^{-2\pi i \frac{j}{N} l}|l\rangle_t\right) \\ &= \frac{1}{N}\sum_{l=0}^{N-1}\sum_{j=0}^{N-1} e^{2\pi i \frac{x_1 - l}{N} j}|j\rangle_h |l\rangle_t. \end{aligned} \tag{21}$$

By the above equation, if P_2 measures the ancillary state, he will get $|l\rangle_t$ $(l \in \{0, 1, \ldots, N-1\})$ with the equal probability of $\frac{1}{N}$. It implies that P_2 cannot get any secret information about P_1's private input, because he cannot extract out the global phase information from the partial qubits of the entangled quantum systems with the subscripts h and t. In fact, any local unitary operator on the partial qubits cannot fully disentangle the entanglement of the composite system unless directly measured. Therefore, even if P_2 performs this attack, he still cannot get any private information about P_1's secret x_1.

(3) P_2 performs a more complicated entangle-measure attack that he is able to prepare another ancillary system $|0\rangle_{P_2}$ and entangle the two ancillary systems by his local unitary operations, where one is transmitted from P_1, and afterward he can measure the ancillary system prepared by himself to get the partial information about P_1's private inputs. P_2's dishonest action when he receives P_1's ancillary $|j\rangle_t$ can be described by a unitary operator $\widetilde{U}_{tP_2}$, which acts on $|j\rangle_t$ and $|0\rangle_{P_2}$. We can describe it as follows:

$$\widetilde{U}_{tP_2}|j\rangle_t|0\rangle_{P_2} = \sqrt{\eta_j}|j\rangle_t|\phi(j)\rangle_{P_2} + \sqrt{1-\eta_j}|V(j)\rangle_{tP_2}, \tag{22}$$

where $|V(j)\rangle_{tP_2}$ is a vector orthogonal to $|j\rangle_t|\phi(j)\rangle_{P_2}$, i.e.,

$${}_t\langle j|_{P_2}\langle\phi(j)|V(j)\rangle_{tP_2} = 0. \tag{23}$$

In order to completely pass the honest test (see Step 7), it can easily deduce that $\eta_j = 1$. That is, the whole quantum systems of P_1 and P_2 should be in the following state after performing $\widetilde{U}_{tP_2}$:

$$\widetilde{U}_{tP_2}\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{x_1}{N} j}|j\rangle_h|j\rangle_t|0\rangle_{P_2} = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{x_1}{N} j}|j\rangle_h|j\rangle_t|\phi(j)\rangle_{P_2}. \tag{24}$$

Then P_2 sends $|j\rangle_t$ back to P_1. After P_1 performing $CNOT^{\otimes m}$ and further measuring the ancillary system t, the state of the remaining quantum system becomes

$$\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{x_1}{N} j}|j\rangle_h|\phi(j)\rangle_{P_2}. \tag{25}$$

Now if P_2 measures his ancillary state $|\phi(j)\rangle_{P_2}$, as the above analysis in the case of (2), he still cannot get any secret information about x_1 because of the entanglement of $|j\rangle_h$ and $|\phi(j)\rangle_{P_2}$. If P_1 further applies QFT^{-1} to the first m qubits, the state of the remaining quantum system will be updated into

$$\begin{aligned} & QFT^{-1}\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{x_1}{N} j}|j\rangle_h|\phi(j)\rangle_{P_2} \\ &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{x_1}{N} j} QFT^{-1}|j\rangle_h|\phi(j)\rangle_{P_2} \\ &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{x_1}{N} j}\left(\frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} e^{-2\pi i \frac{j}{N} l}|l\rangle_h\right)|\phi(j)\rangle_{P_2} \\ &= \frac{1}{N}\sum_{j=0}^{N-1} e^{2\pi i \frac{x_1}{N} j}\left[e^{-2\pi i \frac{x_1}{N} j}|x_1\rangle_h + \sum_{l=0 \wedge l \neq x_1}^{N-1} e^{-2\pi i \frac{l}{N} j}|l\rangle_h\right]|\phi(j)\rangle_{P_2} \\ &= \frac{1}{N}\sum_{j=0}^{N-1}|x_1\rangle_h|\phi(j)\rangle_{P_2} + \frac{1}{N}\sum_{j=0, l=0 \wedge l \neq x_1}^{N-1} e^{2\pi i \frac{x_1 - l}{N} j}|l\rangle_h|\phi(j)\rangle_{P_2}. \end{aligned} \tag{26}$$

This equation shows that if P_1 measures his remaining m qubits, he will get $|l\rangle_h$ $(l \in \{0, 1, \ldots, N-1\})$ with the equal probability of $\frac{1}{N}$, which implies that the probability of getting $|x_1\rangle_h$ is also $\frac{1}{N}$, unless $\phi(j)$ is independent of j. Similarly, P_2 cannot get the secret x_1 with the probability of more than $\frac{1}{N}$ due to their entanglement yet. It implies that P_2 cannot get any secret information about P_1's private input x_1. Therefore, the entangle-measure attack is infeasible.

From what we have analyzed above, we can see clearly that P_2 cannot get any secret information about x_1. Furthermore, we can easily and naturally generalize that any party $P_k\,(k \neq 1)$ cannot obtain any secret information about P_1's private input. Therefore, the initiator's private input is unconditionally secure against other dishonest parties. In turn, if all party honesty execute this protocol, P_1 only gets the final summation $\sum_{k=1}^{n} x_i modN$ $(n > 2)$, instead of single party's private secret x_k. However, if the parties P_{k-1} and P_{k+1} are dishonest, they can collude to get P_k's private input x_k. In order to overcome this weakness, we can use the communication model in a random order instead of the fixed order, that is, how to choose the next party is randomly determined by the party himself, not pre-determined by a designated party.

In addition, in order to full resist the collusion attack of any less $n - 1$ parties, we can design the following Protocol III, in which all parties are full parity.

Protocol III (to compute $\sum_{k=1}^{n} x_i modN$)

Round 1

Step 1. Each party $P_k\,(1 \leq k \leq n)$ randomly generates $n - 1$ integers $x_{k1}, x_{k2}, \ldots, x_{k(n-1)}$ in $\{0,\ 1,\ \ldots,\ N - 1\}$, and then computes $x_{kn} = \left(x_k - \sum_{j=1}^{n-1} x_{kj}\right) modN$. That is,

$$x_k = \sum_{j=1}^{n} x_{kj} modN. \tag{27}$$

Step 2. Each party $P_k\,(1 \leq k \leq n)$ as the initiator calls Protocol I to compute

$$y_k = \sum_{j=k}^{(k+n-1)\,modn} x_{jk} modN, \tag{28}$$

where x_{kk} is P_k's the initial input.

Round 2

Finally, all parties designate an agent who could be one of them to again call Protocol I to compute and announce

$$y = \sum_{k=1}^{n} y_k modN. \tag{29}$$

Obviously,

$$\begin{aligned} y &= \sum_{k=1}^{n} y_k modN \\ &= \sum_{k=1}^{n} \sum_{j=k}^{(k+n-1)\,modn} x_{jk} modN \\ &= \sum_{j=1}^{n} \sum_{k=1}^{n} x_{jk} modN \\ &= \sum_{j=1}^{n} x_j modN. \end{aligned} \tag{30}$$

Because Protocol I can ensure the unconditional security of the private input of the initiator, every sub-secret x_{kk} of $P_k\,(1 \leq k \leq n)$ in Round 1 of Protocol III is unconditionally secure against any less $n - 1$ parties. Therefore, Protocol III is unconditional secure against any collusion attack, unless there are $n - 1$ cheating parties.

As for Protocol II, obviously P_1's secret s_1 is unconditionally secure because the transmitted quantum messages don't include any private information about s_1. Conversely, if all parties honestly execute Protocol II, P_1 only gets the final multiplication $\prod_{k=1}^{n} s_i modN\ (n > 2)$, instead of certain party's secret s_k. In addition, the n-th party P_n can easily perform an intercept-resend attack. That is, he intercepts all qubits passing through his hands, and then sends fake qubits back to P_1. Accordingly, P_n may finally obtain $|\varpi\rangle_{t_1}$ after applying m $CNOT$ gate operators and an inverse quantum Fourier transform QFT^{-1} to his intercepted qubits, where $\varpi = rs_2 \ldots s_n modN$. However, P_n does not know r, so he still cannot get any secret information about other parties' private inputs. Therefore, this attack is infeasible. Furthermore, in order to resist the collusion attack, we can also use the communication model in a random order instead of the fixed order. Similarly, we can also design the unconditionally secure quantum protocol for Secure Multiparty Multiplication.

Protocol IV (to compute $\prod_{k=1}^{n} x_k mod\mathrm{N}$)

Round 1

Step 1. Each party P_k $(1 \leq k \leq n)$ splits his secret x_k into n random integers $x_{k1},\ x_{k2},\ \ldots,\ x_{kn}$ in $\{0,\ 1,\ \ldots,\ N - 1\}$, such that

$$x_k = \prod_{j=1}^{n} x_{kj} modN, \tag{31}$$

where $x_{kj} = 2^{m_{kj}} \cdot s_{kj}$. That is, $\prod_{k=1}^{n} x_k modN = 2^{\sum_{k=1}^{n} \sum_{j=1}^{n} m_{kj}} \prod_{k=1}^{n} \prod_{j=1}^{n} s_{kj} modN$.

Step 2. Each party $P_k (1 \leq k \leq n)$ as the initiator calls Protocol III to compute

$$M = \sum_{k=1}^{n}\sum_{j=1}^{n} m_{jk} modN, \tag{32}$$

where m_{kk} is P_k's the initial input.

Step 3. At the same time, each party $P_k (1 \leq k \leq n)$ as the initiator calls Protocol II to compute

$$s_k = \prod_{j=1}^{n} s_{jk} modN. \tag{33}$$

where s_{kk} is P_k's the initial input.

Round 2

Finally, all parties designate an agent who could be one of them to again call Protocol II to compute $S = \prod_{k=1}^{n} s_k modN$ and to further announce

$$X = 2^M SmodN. \tag{34}$$

As for the security of the quantum channel, we can use the decoy technology to check eavesdropping in all proposed protocols. That is, the initiator randomly inserts enough decoy particles into the qubit sequence to be transmitted, where every decoy particle is prepared randomly with either Z-basis (i.e. $\{|0\rangle, |1\rangle\}$ or X-basis (i.e. $\left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}\right)$. After confirming that the receiver has received the transmitted sequence, the initiator announces the positions of partial decoy particles and the corresponding measurement basis. The receiver measures these decoy particles according to the initiator's announcements and tells the initiator his measurement results. Then the initiator compares the measurement results of the receiver with the initial states of these corresponding decoy particles in the transmitted sequence and analyzes the security of the transmissions. If the error rate is higher than the threshold determined by the channel noise, they cancel this protocol and restarts; or else they continue to the next step.

In addition, the authenticated quantum channel can further ensure the security of quantum communications. Like most existing secure multiparty quantum computations, our protocols need there is an authenticated quantum channel. This is the only assumption we need to have for proposed protocols to work. In principle, we may use a quantum authentication scheme (QAS)[18] based on Clifford operators introduced in[19] to implement it. We may also use quantum encryptions combined with classical authenticated keys[20,21]. In addition, we may still ensure the authentication by sharing the entangled quantum resources in advance[22] or using the detecting (or decoy) particle technologies[23].

Discussion

In this paper, we presented a novel and efficient quantum approach to systematically compute secure multiparty summation and multiplication. In our approach, there is an initiator who prepares an entangled state and further transmits the partial qubits of the entangled state to every party in turn through the quantum channel. According to the different computations, there are two specific processing ways: the receiver in computing the summation adds his secret into the global phase of the entangled state by an oracle operator, while the receiver in computing the multiplication embeds his secret into the received basis state by another oracle operator. Finally, the initiator takes the transmitted qubits back and subtly extracts out the corresponding summation and multiplication from the phase information by an inverse quantum Fourier transform. More specifically, we proposed several quantum protocols for secure multiparty summation and multiplication, where Protocol I and II have higher efficiency due to the linear communication complexity, and Protocol III and IV provide the unconditional security and the perfect privacy protection with $O(n^2)$ communication complexity.

In conclusion, our approach securely implements the fundamental arithmetic operations (i.e., summation and multiplication) in secret-by-secret way instead of bit-by-bit way, which may give some good references for solving other SMC problems. In theory, it can be generalized to compute lots of secure multiparty numerical computations.

References

1. Yao, A. C. Protocols for secure computations. In Proc. *23rd IEEE Symposium on Foundations of Computer Science (FOCS' 82)*, 160 (1982).
2. Clifton, C., Kantarcioglu, M., Vaidya, J., Lin, X. & Zhu, M. Y. Tools for Privacy-Preserving Distributed Data Mining. *ACM SIGKDD Explorations Newsletter* **4,** 28–34 (2002).
3. Sanil, A. P., Karr, A. F., Lin, X. & Reiter, J. P. Privacy preserving regression modeling via distributed computation. In Proc. *the 2004 ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 677-682 (2004).
4. Atallah, M., Bykova, M., Li, J., Frikken, K. & Tophara, M. Private collaborative forecasting and benchmarking. In Proc. *the 2004 ACM Workshop on Privacy in the Electronic Society*, 103-114 (2004).
5. Masayuki, A. Non-interactive and optimally resilient distributed multiplication (Special Section on Discrete Mathematics and Its Applications). *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **E83A,** 598–605 (2000).
6. Ronald, C., Ivan, D. & Robbert, D. H. Atomic Secure Multi-party Multiplication with Low Communication. In Proc. *Advances in Cryptology-EUROCRYPT 2007. LNCS* 4515, 329-346 (2007).
7. Peter, L. Secure Distributed Multiplication of Two Polynomially Shared Values: Enhancing the Efficiency of the Protocol. In Proc. *3rd International Conference on Emerging Security Information, Systems and Technologies*, 286-291 (2009).
8. Bennett, C. H. & Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proc. *IEEE International Conference on Computers, Systems, and Signal Processing*, 175-179 (1984).
9. Lo, H. K. Insecurity of quantum secure computations. *Phys. Rev. A* **56,** 1154–1162 (1997).

10. Colbeck, R. The impossibility of secure two-party classical computation. *Phys. Rev. A* **76,** 062308 (2007).
11. Buhrman, H., Christandl, M. & Schaffner, C. Complete Insecurity of Quantum Protocols for Classical Two-Party Computation. *Phys. Rev. Lett.* **109,** 160501 (2012).
12. Crépeau, C., Gottesman, D. & Smith, A. Secure multi-party quantum computation. In Proc. *STOC'02 Proceedings of the thirty-fourth annual ACM symposium on Theory of Computing*, 643-652 (2002).
13. Ben-or, M., Crépeau, C., Gottesman, D., Hassidim, A. & Smith, A. Secure Multiparty Quantum Computation with (Only) a Strict Honest Majority. In Proc. *FOCS'06, 47th Annual IEEE Symposium on Foundations of Computer Science*, 249-260 (2006).
14. Unruh, D. Universally Composable Quantum Multi-party Computation. In Proc. *Advances in Cryptology - EUROCRYPT 2010, LNCS* 6110, 486-505 (2010).
15. Du, J. Z., Chen, X. B., Wen, Q. X. & Zhu, F. C. Secure multiparty quantum summation. *Acta Phys Sin-Ch Ed* **56,** 6214–6219 (2007).
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 Phys.* **49,** 2793–2804 (2010).
17. Diao, Z. J., Huang, C. F. & Wang, K. Quantum Counting: Algorithm and Error Distribution. *Acta Appl Math.* **118,** 147–159 (2012).
18. Barnum, H., Crépeau, C., Gottesman, D., Smith, A. & Tapp, A. Authentication of quantum messages. In Proc. *43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 449–458 (2002).
19. Aharonov, D., Ben-Or, M. & Eban, E. Interactive proofs for quantum computations. In Proc. *Innovations in Computer Science*, arxiv.org/abs/0810.5375 (2008).
20. Yu, K. F., Yang, C. W., Liao, C. H. & Hwang, T. Authenticated semi-quantum key distribution protocol using Bell states. *Quantum Inf. Process*. **13,** 1457–1465 (2014).
21. Guan, D. J., Wang, Y. J. & Zhuang, E. S. A practical protocol for three-party authenticated quantum key distribution. *Quantum Inf. Process*. **13,** 2355–2374 (2014).
22. Farouk, A., Zakaria, M., Megahed, A. & Omara, F.A. A generalized architecture of quantum secure direct communication for N disjointed users with authentication. *Sci. Rep* **5,** 16080 (2015).
23. Shi, R. H., Mu, Y., Zhong, H., Cui, J. & Zhang, S. Two Quantum Protocols for Oblivious Set-member Decision Problem. *Sci. Rep* **5,** 15914 (2015).

Acknowledgements
This work was supported by National Natural Science Foundation of China (Nos 61173187, 61173188 and 11301002), the Ministry of Education institution of higher learning doctor discipline and scientific research fund aids a project financially (No. 20133401110004), Natural Science Foundation of Anhui Province (No. 1408085QF107), and the 211 Project of Anhui University (Nos 33190187 and 17110099).

Author Contributions
Study conception, design, and writing of the manuscript: R.-H.S. and Y.M. Analysis and discussion: H.Z., J.C. and S.Z. All authors reviewed the manuscript.

Additional Information
Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Shi, R.- *et al.* Secure Multiparty Quantum Computation for Summation and Multiplication. *Sci. Rep.* **6**, 19655; doi: 10.1038/srep19655 (2016).