SCIENTIFIC REPORTS
nature research

OPEN

Hybrid Quantum Protocols for Secure Multiparty Summation and Multiplication

Kartick Sutradhar ✉ & Hari Om

The summation and multiplication are two basic operations for secure multiparty quantum computation. The existing secure multiparty quantum summation and multiplication protocols have (*n*, *n*) threshold approach and their computation type is bit-by-bit, where *n* is total number of players. In this paper, we propose two hybrid (*t*, *n*) threshold quantum protocols for secure multiparty summation and multiplication based on the Shamir's secret sharing, SUM gate, quantum fourier transform, and generalized Pauli operator, where *t* is a threshold number of players that can perform the summation and multiplication. Their computation type is secret-by-secret with modulo *d*, where *d*, $n \leq d \leq 2n$, is a prime. The proposed protocols can resist the intercept-resend, entangle-measure, collusion, collective, and coherent quantum attacks. They have better computation as well as communication costs and no player can get other player's private input.

The secure multiparty quantum computation is an essential component in quantum cryptography. The summation and multiplication are two basic operations for secure multiparty quantum computation. The secure multiparty quantum summation and multiplication include a list of secrets, which is shared among a set of players and the players jointly perform summation or multiplication without revealing their secrets. The classical summation and multiplication protocols cannot provide the unconditional secure communications. However, the quantum summation and multiplication protocols can provide the unconditional security as they are based on the principles of quantum mechanics like quantum correlation[1], entanglement for bipartite system[2], Heisenberg XYZ model[3]. In 2007, Du *et al.*[4] discussed a secure multiparty quantum addition modulo $n+1$ protocol based on the non-orthogonal states, where n is total number of players. In 2010, Chen *et al.*[5] introduced a secure multiparty quantum addition modulo 2 protocol based on multi-particle entangle. In 2014, Zhang *et al.*[6] presented a protocol with addition modulo 2 based on both polarization of a single photon. In 2010, a three-party quantum addition modulo 2 protocol was discussed by Zhang *et al.*[7]. These protocols have some limitations, for example, they cannot perform addition correctly if one player is dishonest as these protocols have (n, n) threshold approach, and the modulo of these protocols is very small. They have high communication and computation costs due to the bit-by-bit computation. In 2015, Shi *et al.*[8] discussed a secure multiparty quantum summation and multiplication protocol. This protocol is efficient, but it has (n, n) threshold approach. In 2017, Shi and Zhang[9] introduced a two-party quantum protocol for summation. This protocol cannot perform summation correctly if one party is dishonest. In the same year, a multiparty quantum summation modulo 2 protocol was discussed by Zhang *et al.*[10]. This protocol is efficient but its modulo is too small. Then, Liu *et al.*[11] discussed a secure multiparty quantum summation protocol based on two particle Bell States. This protocol is efficient but its modulo is 2 and it has (n, n) threshold approach. In 2018, Yang and Ye[12] introduced a secure multiparty quantum protocol for summation based on the quantum Fourier transform. The computation type of this protocol is secret-by-secret, but it has (n, n) threshold approach. Recently, Jiao *et al.*[13] have discussed a secure multiparty quantum summation and multiplication protocol with mutually unbiased bases. This protocol is efficient, but the computation type of this protocol is secret-by-secret and it has (n, n) threshold approach. Most of the existing secure multiparty summation and multiplication protocols have (n, n) threshold approach and bit-by-bit computation type. Further, they are not practically feasible as they require high communication as well as computation costs.

In this paper, we propose two hybrid (t, n) threshold quantum protocols for secure multiparty summation and multiplication. In order to incorporate the advantages of both quantum and classical multiparty summation and multiplication, we apply the quantum methods in a secure multiparty computation. The novelty of the

Indian Institute of Technology (ISM) Dhanbad, Department of Computer Science and Engineering, Dhanbad, 826004, India. ✉e-mail: kartick.sutradhar@gmail.com

proposed work can be summarized as follows. Our protocols have (t, n) threshold approach, where t players can perform the quantum summation and multiplication systematically and efficiently without revealing their privacy. They require less communication and computation costs as their computation type is secret-by-secret. Further, our proposed protocols possess all the benefits(i.e., they use qudit instead of qubit, do not require the secret information to be passed through the transmitted particles, do not require to perform entanglement measurement, and the quantum attacks cannot be performed) of the existing secure multiparty quantum summation and multiplication.

Preliminaries

Here, we introduce the Shamir's secret sharing, quantum state, SUM gate, quantum Fourier transform (*QFT*), and generalized Pauli operator, which will be used in our work.

Shamir's secret sharing. In the Shamir's secret sharing, there is a set of players $\mathscr{P} = \{P_1, P_2, \ldots, P_n\}$ and a dealer[14]. This secret sharing scheme consists of two phases: secret sharing and secret reconstruction. In secret sharing phase, the dealer shares a secret among n players using a $(t-1)$ degree polynomial $f(y)$; each player knows only his share. In secret reconstruction phase, the t players reconstruct the secret using the Lagrange interpolation. The Lagrange Interpolation is defined as follows.

$$f(y) = \sum_{k=1}^{t} f(y_k) \prod_{1 \le j \le t, j \ne k} \frac{y - y_j}{y_k - y_j} \tag{1}$$

For $y = 0$, Eq.(1) can be written as follows.

$$\begin{aligned} f(0) &= \sum_{k=1}^{t} f(y_k) \prod_{1 \le j \le t, j \ne k} \frac{-y_j}{y_k - y_j} \\ &= \sum_{k=1}^{t} f(y_k) \prod_{1 \le j \le t, j \ne k} \frac{y_j}{y_j - y_k} \end{aligned} \tag{2}$$

Quantum State. In quantum computing, the d-level quantum state is defined as follows[15].

$$|\phi\rangle = \sum_{l=0}^{d-1} C_l |l\rangle \tag{3}$$

It must satisfy $\sum_{l=0}^{d-1} |C_l|^2 = 1$, where C_l represents complex number.

SUM gate. In quantum computing, the SUM gate is defined as follows[16].

$$SUM(|u\rangle, |v\rangle) = (|u\rangle, |u + v \bmod d\rangle), \tag{4}$$

where $|u\rangle$ and $|v\rangle$ denote control and target particles, respectively, and $u, v \in \{0, 1, \ldots, d-1\}$.

Quantum Fourier Transform (*QFT*). The discrete Fourier transform is the foundation of *QFT*. The d-level *QFT* is defined as follows[8].

$$QFT|p\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{p.l} |q\rangle \tag{5}$$

where, ω represents $e^{2\pi i}$.

Generalized Pauli operator. In quantum computing, the d-level generalized Pauli operator is defined as follows[17].

$$U_{\gamma,\delta} = \sum_{l=0}^{d-1} \omega^{l.\delta} |l + \gamma\rangle\langle l|, \tag{6}$$

where, $\gamma, \delta \in \{0, 1, \ldots d-1\}$.

Proposed Protocols

In this section, we propose two hybrid (t, n) threshold secure multiparty quantum summation and multiplication protocols. Let X and Y have two secrets a and b, respectively, and want to perform $(a + b)$ or $(a \times b)$ without revealing their secrets. In these proposed protocols, we assume that the set of players $\mathscr{P} = \{P_1, P_2, \ldots, P_n\}$, a qualified subset $\mathbb{S} = \{P_1, P_2, \ldots, P_t\}$, each qualified subset containing t players and player P_1 is an initiator.

Hybrid secure multiparty quantum summation protocol. Here, we discuss our proposed hybrid (t, n) threshold secure multiparty quantum summation, whose procedure is given as follows.

Step 1: The X and Y choose two different polynomials $f(y) = a + c_1 y + c_2 y^2 + \ldots + c_{t-1} y^{t-1} \bmod d$ and $g(y) = b + \bar{c}_1 y + \bar{c}_2 y^2 + \ldots + \bar{c}_{t-1} y^{t-1} \bmod d$, where $c_1, c_2, \ldots, c_{t-1}$ and $\bar{c}_1, \bar{c}_2, \ldots, \bar{c}_{t-1}$ are coefficients and a and b are the secrets of X and Y, respectively. Then, they compute the classical shares $f(y_i)$ and $g(y_i)$, respectively, using the Shamir's Secret Sharing[14] and distribute these shares among the set of players $\mathscr{P} = \{P_1, P_2, \ldots, P_n\}$. Player $P_i, i = 1, 2, \ldots, n$, possesses only his shares $f(y_i)$ and $g(y_i)$.

Step 2: Player $P_i, i = 1, 2, \ldots,$ computes $h(y_i) = f(y_i) + g(y_i) \bmod d$ and keeps $h(y_i)$ secret.

Step 3: Player $P_k, k = 1, 2, \ldots, t$, computes the shadow of his shares, denoting as A_k, as follows.

$$A_k = h(y_k) \prod_{1 \le j \le t, j \ne k} \frac{y_j}{y_j - y_k} \bmod d \tag{7}$$

Step 4: Initiator P_1 prepares t single qudit particles $|0\rangle_1, |0\rangle_2, \ldots, |0\rangle_t$ and applies QFT on the first particle $|0\rangle_1$. The resultant state $|\phi_1\rangle$ is given as follows.

$$|\phi_1\rangle = (QFT|0\rangle_1) = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} |l\rangle_1 \tag{8}$$

Here, $|\phi_1\rangle$ and $|0\rangle_k$'s, $k = 2, 3, \ldots, t$, are control and target qudits, respectively.

Step 5: Player P_1 performs $(t-1)$ SUM operations to produce the entangled state $|\phi_2\rangle$ as follows.

$$|\phi_2\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} |l\rangle_1 |l\rangle_2 \ldots |l\rangle_k. \tag{9}$$

Initiator P_1 sends the particle $|l\rangle_k$ to each player $P_k, k = 2, 3, \ldots, t$.

Step 6: Each player $P_k, k = 2, 3, \ldots, t$, applies the QFT operation on his particle $|l\rangle_k$ and then executes the generalized Pauli operator $U_{A_k,0}, k = 1, 2, \ldots, t$. The quantum state $|\phi_2\rangle$ is evolved as the quantum state $|\phi_3\rangle$, which is obtained as follows:

$$\begin{aligned} |\phi_3\rangle &= U_{A_1,0} QFT \otimes U_{A_2,0} QFT \otimes \ldots \otimes U_{A_k,0} QFT |\phi_2\rangle \\ &= d^{-\frac{t+1}{2}} \sum_{0 \le m_1, m_2, \ldots, m_k < d,\ m_1 + m_2 + \ldots + m_k = 0 \bmod d} |m_1 + A_1\rangle |m_2 + A_2\rangle \ldots |m_k + A_k\rangle \end{aligned} \tag{10}$$

Step 7: In computational basis, each player $P_k, k = 2, 3, \ldots, t$, measures his particle $|m_k + A_k\rangle$ and broadcasts his measurement result $m_k + A_k, k = 1, 2, \ldots, t$.

Step 8: Finally, they jointly compute the summation by adding their measurement results. The summation of the secrets is computed as: $(a + b) = \sum_{k=1}^{t} m_k + A_k \bmod d$.

Hybrid secure multiparty quantum multiplication protocol. Here, we discuss our proposed quantum protocol for secure multiparty multiplication, whose procedure is given as follows.

Step 1: Initially, X and Y select two different polynomials $f(y) = a + c_1 y + c_2 y^2 + \ldots + c_{t-1} y^{t-1} \bmod d$ and $g(y) = b + \bar{c}_1 y + \bar{c}_2 y^2 + \ldots + \bar{c}_{t-1} y^{t-1} \bmod d$, where a and b are the secrets of X and Y, $c_1, c_2, \ldots, c_{t-1}$ and $\bar{c}_1, \bar{c}_2, \ldots, \bar{c}_{t-1}$ are coefficients of polynomials $f(y)$ and $g(y)$, respectively. Then, they compute the classical shares $f(y_i)$ and $g(y_i)$, respectively, and distribute them among n players. Player $P_i, i = 1, 2, \ldots, n$, knows his shares $f(y_i)$ and $g(y_i)$ only.

Step 2: Player $P_i, i = 1, 2, \ldots, n$, computes $h'(y_i) = f(y_i) \times g(y_i) \bmod d$ and shares $h'(y_i)$ among n players using new random polynomial $z_i(x) = h'(y_i) + \beta_1 x + \beta_2 x^2 + \ldots + \beta_{t-1} x^{t-1} \bmod d$. The total polynomial, denoted as T_i, is computed by each player $P_i, i = 1, 2, \ldots, n$, using the Vandermonde matrix[18]. Player P_i, $i = 1, 2, \ldots, n$, knows T_i only.

Step 3: Each player $P_k, k = 1, 2, \ldots, t$, computes the shadow B_k of his share as follows.

$$B_k = T_k \prod_{1 \le j \le t, j \ne k} \frac{x_j}{x_j - x_k} \bmod d \tag{11}$$

Step 4: Initiator P_1 prepares t single qudit particles $|0\rangle_1, |0\rangle_2, \ldots, |0\rangle_t$ and applies QFT on the first particle 0_1. The resultant state $|\Phi_1\rangle$ is given as follows.

$$|\Phi_1\rangle = (QFT|0\rangle_1) = \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} |r\rangle_1. \tag{12}$$

Here, $|\Phi_1\rangle$ denotes control qudit and $|0\rangle_k$'s, $k = 2, 3, \ldots, t$), denote target qudits.

Step 5: Initiator executes $(t-1)$ SUM operations to get the entangled state $|\Phi_2\rangle$, as follows.

$$|\Phi_2\rangle = \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} |r\rangle_1 |r\rangle_2 \ldots |r\rangle_k. \tag{13}$$

Initiator P_1 sends the particle $|r\rangle_k$ to each player $P_k, k = 2, 3, \ldots, t$.

Step 6: Each player $P_k, k = 2, 3, \ldots, t$, applies QFT on his particle $|r\rangle_k$, followed by the generalized Pauli operator $U_{B_k,0}$. The quantum state $|\Phi_2\rangle$ is evolved as the resultant state $|\Phi_3\rangle$,which is given below:

$$\begin{aligned} |\Phi_3\rangle &= U_{B_1,0}QFT \otimes U_{B_2,0}QFT \otimes \ldots \otimes U_{B_k,0}QFT|\Phi_2\rangle \\ &= d^{-\frac{t+1}{2}} \sum_{0\le w_1,w_2,\ldots,w_k<d,\ w_1+w_2+,\ldots,+w_k=0 \bmod d} |w_1+B_1\rangle|w_2+B_2\rangle\ldots|w_k+B_k\rangle \end{aligned} \tag{14}$$

Step 7: Each player $P_k, k = 2, 3, \ldots, t$, measures his particle $|w_k + B_k\rangle$ in computational basis and broadcasts his measurement result $w_k + B_k$.

Step 8: Finally, they compute the multiplication by adding their measurement results. The multiplication of the secrets is computed as: $(a \times b) = \sum_{k=1}^{t} w_k + B_k \bmod d$.

Correctness

In this section, we prove the correctness of our proposed protocols. We discuss the correctness proof of the secure multiparty quantum summation protocol only. The correctness proof of the secure multiparty quantum multiplication protocol is very much similar to that of the secure multiparty quantum summation protocol.

Correctness Proof. **lemma 1** If all players in a qualified subset $\mathbb{S} = \{P_1, P_2, \ldots, P_t\}$ act honestly, then they can perform summation $(a + b) = \sum_{k=1}^{t} A_k \bmod d$.

proof 1 On Applying QFT and Pauli operators by each player $P_k, k = 1, 2, \ldots, t$, on his particle gives the quantum state as follows.

$$\begin{aligned} |\phi_3\rangle &= U_{A_1,0}QFT \otimes U_{A_2,0}QFT \otimes \ldots \otimes U_{A_t,0}QFT\left(\frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}|l\rangle_1|l\rangle_2\ldots|l\rangle_t\right) \\ &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1} U_{A_1,0}QFT|l\rangle_1 \otimes U_{A_2,0}QFT|l\rangle_2 \otimes \ldots \otimes U_{A_t,0}QFT|l\rangle_t \\ &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\left(U_{A_1,0}\frac{1}{\sqrt{d}}\sum_{m_1=0}^{d-1}\omega^{m_1 l}|m_1\rangle\right)\otimes\left(U_{A_2,0}\frac{1}{\sqrt{d}}\sum_{m_1=0}^{d-1}\omega^{m_2 l}|m_2\rangle\right) \\ &\quad \otimes\ldots\otimes\left(U_{A_t,0}\frac{1}{\sqrt{d}}\sum_{m_1=0}^{d-1}\omega^{m_t l}|m_t\rangle\right) \\ &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1} d^{\frac{-t}{2}} \sum_{0\le m_1,m_2,\ldots,m_t<d}\omega^{(m_1+\ldots+m_t)l}|m_1+A_1\rangle\otimes|m_2+A_2\rangle\otimes\ldots \\ &\quad \otimes|m_t+A_t\rangle \\ &= d^{-\frac{t+1}{2}} \sum_{0\le m_1,m_2,\ldots,m_t<d}\sum_{l=0}^{d-1}\omega^{(m_1+\ldots+m_t)l}|m_1+A_1\rangle\otimes|m_2+A_2\rangle\otimes\ldots \\ &\quad \otimes|m_t+A_t\rangle \\ &= d^{-\frac{t+1}{2}} s_0 d \sum_{0\le m_1,m_2,\ldots,m_t<d,\ m_1+m_2+,\ldots,+m_t=0 \bmod d}|m_1+A_1\rangle\otimes|m_2+A_2\rangle\otimes\ldots \\ &\quad \otimes|m_t+A_t\rangle \end{aligned}$$

Each player $P_k, k = 1, 2, \ldots, t$, measures his particle in computational basis. The compute the sum after receiving others players' measurement results.

$$\sum_{k=1}^{t} m_k + A_k \overset{d}{\equiv} \sum_{k=1}^{t} m_k + \sum_{k=1}^{t} A_k \overset{d}{\equiv} \sum_{k=1}^{t} A_k \bmod d \tag{15}$$

From Eq. (15), we get sum of the secrets $(a + b) = \sum_{k=1}^{t} A_k \bmod d$.

Example

Here, we illustrate our proposed secure multiparty quantum summation and multiplication protocols using an example. Suppose X and Y have two secrets 4 and 2, respectively, and want to compute their sum and multiplication without revealing their secrets. The X and Y share these secrets among 7 players $\mathscr{P} = \{P_1, P_2, \ldots, P_7\}$ and the qualified subset $\mathbb{S} = \{P_1, P_2, P_3\}$ computes the summation and multiplication. The X and Y select prime as 11. Thus, prime $d = 11$, threshold $t = 3$, and total number of players $n = 7$.

Players		P_1	P_2	P_3	P_4	P_5	P_6	P_7
Shares	$f(y_i)$	9	9	4	5	1	3	0
	$g(y_i)$	6	1	9	8	9	1	6
	$h(y_i)=f(y_i)+g(y_i)$	4	10	2	2	10	4	6
	$h'(y_i)=f(y_i)\times g(y_i)$	10	9	3	7	9	3	0
Polynomials: $z_i(x)$		$10+x+2x^2$	$9+3x+x^2$	$3+2x+2x^2$	$7+2x+3x^2$	$9+5x+x^2$	$3+2x+x^2$	$0+x+5x^2$
Shares	$z_1(x_i)$	2	9	9	2	10	0	5
	$z_2(x_i)$	2	8	5	4	5	8	2
	$z_3(x_i)$	7	4	5	10	8	10	5
	$z_4(x_i)$	1	1	7	8	4	6	3
	$z_5(x_i)$	4	1	0	1	4	9	5
	$z_6(x_i)$	8	8	3	4	0	2	10
	$z_7(x_i)$	6	0	4	7	9	10	10
	T_i	7	9	3	0	0	3	9

Table 1. Share Computation for Summation and Multiplication.

Summation example. **Example**. Consider that X and Y choose their respective polynomials $f(y) = 4 + 2y + 3y^2 \bmod 11$ and $g(y) = 2 + 3y + y^2 \bmod 11$. They compute their classical shares $f(y_i)$ and $g(y_i)$ and distribute these shares among 7 players $\mathscr{P} = \{P_1, P_2, \ldots, P_7\}$. Each player P_i, $i = 1, 2, \ldots, 7$, computes $h(y_i) = f(y_i) + g(y_i) \bmod 11$. The computation of share and $h(y_i)$ are shown in Table 1. Each player P_k, $k=1, 2, 3$, (of qualified subset $\mathbb{S} = \{P_1, P_2, P_3\}$) computes the shadow of his share A_k as follows:

$$A_k = h(y_k) \prod_{1\le j\le t, j\neq k} \frac{y_j}{y_j - y_k} \bmod d$$

$$A_1 = 4 \times \left(\frac{2}{2-1} \times \frac{3}{3-1}\right) \bmod 11 = 1$$

$$A_2 = 10 \times \left(\frac{1}{1-2} \times \frac{3}{3-2}\right) \bmod 11 = 3$$

$$A_3 = 2 \times \left(\frac{1}{1-3} \times \frac{2}{2-3}\right) \bmod 11 = 2$$

Initiator P_1 computes $|\phi_2\rangle = \frac{1}{\sqrt{11}} \sum_{l=0}^{10} |l\rangle_1 |l\rangle_2 |l\rangle_3$ and sends the particle $|l\rangle_k$ to each player P_k, $k=2, 3$. Each player P_k (of qualified subset $\mathbb{S} = \{P_1, P_2, P_3\}$) applies QFT and generalized Pauli operators $U_{1,0}$, $U_{3,0}$, $U_{2,0}$ on his particle. Hence,

$$\begin{aligned}
|\phi_3\rangle &= U_{1,0}QFT \otimes U_{3,0}QFT \otimes U_{2,0}QFT \left(\frac{1}{\sqrt{11}} \sum_{l=0}^{10} |l\rangle_1 |l\rangle_2 |l\rangle_3\right) \\
&= \frac{1}{\sqrt{11}} \sum_{l=0}^{10} U_{1,0}QFT|l\rangle_1 \otimes U_{3,0}QFT|l\rangle_2 \otimes U_{2,0}QFT|l\rangle_3 \\
&= \frac{1}{\sqrt{11}} \sum_{l=0}^{10} U_{1,0}\left(\frac{1}{\sqrt{11}} \sum_{m_1=0}^{10} \omega^{m_1 l}|m_1\rangle\right) \otimes U_{3,0}\left(\frac{1}{\sqrt{11}} \sum_{m_2=0}^{10} \omega^{m_2 l}|m_2\rangle\right) \\
&\quad \otimes U_{2,0}\left(\frac{1}{\sqrt{11}} \sum_{m_3=0}^{10} \omega^{m_3 l}|m_3\rangle\right) \\
&= \frac{1}{11} \sum_{l=0}^{10} \sum_{0\le m_1,m_2,m_3\le 10} \omega^{(m_1+m_2+m_3)l} |m_1+1\rangle|m_2+3\rangle|m_3+2\rangle \\
&= \frac{1}{11} \sum_{0\le m_1,m_2,m_3\le 10} \sum_{l=0}^{10} \omega^{(m_1+m_2+m_3)l} |m_1+1\rangle|m_2+3\rangle|m_3+2\rangle \\
&= 11 s_1 \sum_{0\le m_1,m_2,m_3\le 10,\ m_1+m_2+m_3=0 \bmod 11} |m_1+1\rangle|m_2+3\rangle|m_3+2\rangle
\end{aligned}$$

Finally, the players measure (computational basis) their particles and broadcast their respective measurement results m_1+1, m_2+3, m_3+2. They get the sum by adding their measurement results as follows:

$$m_1 + 1 + m_2 + 3 + m_3 + 2 \overset{11}{\equiv} m_1 + m_2 + m_3 + 6 \overset{11}{\equiv} 6 \bmod 11 = 6$$

Example of multiplication. **Example**. Similar to summation, X and Y select their respective polynomials $f(y) = 4 + 2y + 3y^2 \bmod 11$ and $g(y) = 2 + 3y + y^2 \bmod 11$ and compute their respective classical shares $f(y_i)$ and $g(y_i)$. They distribute these shares among 7 players $\mathscr{P} = \{P_1, P_2, \ldots, P_7\}$. Each player $P_i, i = 1, 2, \ldots, 7$, computes $h'(y_i) = f(y_i) \times g(y_i) \bmod d$ and these $h'(y_i)$ shares are shared among n players using new random polynomial $z_i(x) = h'(y_i) + \beta_1 x + \beta_2 x^2 + \ldots + \beta_{t-1} x^{t-1} \bmod d$. The shares of total polynomial, denoted as T_i, are computed by each player $P_i, i = 1, 2, \ldots, 7$, using the Vandermonde matrix[18]. The computation of T_i is shown in Table 1. Each player P_k, $k=1, 2, 3$, (of qualified subset $\mathbb{S} = \{P_1, P_2, P_3\}$) computes the shadow of his shares B_k as follows.

$$B_k = T_k \prod_{1 \le j \le t, j \ne k} \frac{y_j}{y_j - y_k} \bmod d$$

$$B_1 = 7 \times \left(\frac{2}{2-1} \times \frac{3}{3-1}\right) \bmod 11 = 10$$

$$B_2 = 9 \times \left(\frac{1}{1-2} \times \frac{3}{3-2}\right) \bmod 11 = 6$$

$$B_3 = 3 \times \left(\frac{1}{1-3} \times \frac{2}{2-3}\right) \bmod 11 = 3$$

Initiator P_1 computes $|\Phi_2\rangle = \frac{1}{\sqrt{11}} \sum_{r=0}^{10} |r\rangle_1 |r\rangle_2 |r\rangle_3$, sends the particle $|r\rangle_k$ to player P_k, $k=2, 3$. Each player P_k (of qualified subset $\mathbb{S} = \{P_1, P_2, P_3\}$) applies QFT operation and generalized Pauli operators $U_{10,0}$, $U_{6,0}$, $U_{3,0}$ on his particles as follows.

$$\begin{aligned}
|\Phi_3\rangle &= U_{10,0}QFT \otimes U_{6,0}QFT \otimes U_{3,0}QFT \left(\frac{1}{\sqrt{11}} \sum_{r=0}^{10} |r\rangle_1 |r\rangle_2 |r\rangle_3\right) \\
&= \frac{1}{\sqrt{11}} \sum_{r=0}^{10} U_{10,0}QFT|r\rangle_1 \otimes U_{6,0}QFT|r\rangle_2 \otimes U_{3,0}QFT|r\rangle_3 \\
&= \frac{1}{\sqrt{11}} \sum_{r=0}^{10} U_{10,0} \left(\frac{1}{\sqrt{11}} \sum_{w_1=0}^{10} \omega^{w_1 r} |w_1\rangle\right) \otimes U_{6,0} \left(\frac{1}{\sqrt{11}} \sum_{w_2=0}^{10} \omega^{w_2 r} |w_2\rangle\right) \\
&\quad \otimes U_{3,0} \left(\frac{1}{\sqrt{11}} \sum_{w_3=0}^{10} \omega^{w_3 r} |w_3\rangle\right) \\
&= \frac{1}{11} \sum_{r=0}^{10} \sum_{0 \le w_1, w_2, w_3 \le 10} \omega^{(w_1+w_2+w_3)r} |w_1 + 10\rangle |w_2 + 6\rangle |w_3 + 3\rangle \\
&= \frac{1}{11} \sum_{0 \le w_1, w_2, w_3 \le 10} \sum_{r=0}^{10} \omega^{(w_1+w_2+w_3)r} |w_1 + 10\rangle |w_2 + 6\rangle |w_3 + 3\rangle \\
&= 11 s_1 \sum_{0 \le w_1, w_2, w_3 \le 10,\ w_1+w_2+w_3 = 0 \bmod 11} |w_1 + 10\rangle |w_2 + 6\rangle |w_3 + 3\rangle
\end{aligned}$$

Finally, players measure (computational basis) their particle and broadcasts their measurement results w_1+10, w_2+6, w_3+3. They get the multiplication by adding measurement results as follows:

$$w_1 + 10 + w_2 + 6 + w_3 + 3 \overset{11}{\equiv} w_1 + w_2 + w_3 + 19 \overset{11}{\equiv} 19 \bmod 11 = 8$$

Security Analysis

In this section, we analyze the security of our proposed secure multiparty quantum summation and multiplication protocols. We mainly focus on the security analysis of summation protocol because the security analysis of multiplication protocol is very much similar to that of summation protocol.

Intercept-resend attack. Suppose an eavesdropper E intercepts the particle $|l\rangle_k$ and measures it in the computational basis $\{|1\rangle, |2\rangle, \ldots, |d-1\rangle\}$ to extract the information about the shadow of the share. The eavesdropper E prepares a fake particle $\tilde{l}_k$ and resends it to player $P_k, k = 2, 3, \ldots, t$. If E performs this attack, then he can compute l correctly with probability $\frac{1}{d}$. But E cannot get any valuable information about the share of the shadow from l, because $|l\rangle_k$ does not contain any valuable information about the shadow of the share.

Collusion attack. In our proposed protocols, each player P_k measures his particle $|m_k + A_k\rangle$ and broadcasts his measurement result $m_k + A_k, k = 1, 2, \ldots, t$. Thus, other players cannot obtain the shadow of the share (A_k). Suppose the dishonest players P_{r-1} and P_{r+1} collude together to obtain other players' shadow of the share A_k. They cannot get any information about the shadow of the share because player P_1 only sends the particles $|l\rangle_k$ to other players; nothing else, and the particles $|l\rangle_k$ don't carry any valuable information about the shadow of the share. So, this attack is not possible in our proposed protocols.

Entangle-measure attack. In this attack, the eavesdropper E intercepts all the particles $|l\rangle_k$, when the initiator P_1 sends the particles $|l\rangle_k$ to player $P_k, k = 2, 3, \ldots, t$. Further, E selects a intercepted particle $|l\rangle_m$ and prepares an ancillary particle $|c\rangle$. The d-level SUM operation is performed by E on $|l\rangle_m$ to entangle the ancillary particle $|c\rangle$. The quantum state $|\phi_2\rangle$ is evolved as $|\phi_2\rangle'$, which is given below.

$$\begin{aligned} |\phi_2\rangle' &= (SUM(|l\rangle_m, |c\rangle))|\phi_2\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1} |l\rangle_1, |l\rangle_2, \ldots, |l\rangle_t |l \oplus c\rangle \end{aligned}$$

E prepares another secret particle $|l\rangle_o$ and performs d-level SUM operation on $|c\rangle$. The quantum state $|\phi_2\rangle'$ is evolved as $|\phi_2\rangle''$, which is given below.

$$\begin{aligned} |\phi_2\rangle'' &= (SUM(|l\rangle_o, |l \oplus c\rangle))|\phi_2\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1} |l\rangle_1, |l\rangle_2, \ldots, |l\rangle_t |l \oplus l \oplus c\rangle \\ &= |\phi_2\rangle|c\rangle \end{aligned}$$

The ancillary particle $|c\rangle$ is measured by E and gets the initial value $|c\rangle$. So, E concludes that the particles $|l\rangle_m$ and $|r\rangle_r$ are the same. Based on this conclusion, E assumes that all the particles $|l\rangle_k$'s are same. Thus, E cannot get any information about the shadow of the share from this attack.

Collective attack. In this attack, E interacts with each qudit by preparing an independent ancillary particle and jointly performs the measurement operation on all the ancillary qudit to get the shadow of the share. E prepares an independent ancillary particle $|c\rangle$ to interact with each qudit of player P_k, $k = 1, 2, \ldots, t$. After interacting, E gets the particle $|l\rangle_k$ and jointly performs the measurement operation in the computational basis $\{|1\rangle, |2\rangle, \ldots, |d-1\rangle\}$ to learn the shadow of the share. From this joint measurement, E cannot get any information about the shadow of the share because $|l\rangle_k$ does not contain any information of the shadow of the share.

Coherent attack. In coherent attack, E jointly interacts with all qudit of player P_k, $k = 1, 2, \ldots, t$, by preparing an independent ancillary particle $|c\rangle$ and he gets each player's particle $|l\rangle_k$. E jointly performs the measurement operation in computational basis $\{|1\rangle, |2\rangle, \ldots, |d-1\rangle\}$ on each player's particle $|l\rangle_k$. From this measurement of particle $|l\rangle_k$, E only gets l with probability $\frac{1}{d}$. But, l does not contain any valuable information about the shadow of the share. Here, E only knows the interacting particle $|l\rangle_k$, nothing else. So, from this attack, E cannot learn the shadow of the share.

Performance Analysis

Here, we analyze the performance of our proposed secure multiparty quantum summation and multiplication protocols and compare it with that of ten existing secure multiparty quantum summation and multiplication protocols: Du *et al.'s* protocol[4], Chen *et al.'s* protocol[5], Zhang *et al.'s* protocol[6], Zhang *et al.'s* protocol[7], Shi *et al.'s* protocol[8], Shi's protocol[9], Zhang *et al.'s* protocol[10], Liu *et al.'s* protocol[11], Yang's protocol[12] and Jiao *et al.'s* protocol[13] based on three parameters: cost, universality, and attack. The Du *et al.'s* protocol[4] is based on multiparty computation but it has (n, n) threshold approach and its modulo is $n+1$ and computation type is bit-by-bit. The Chen *et al.'s*[5], Zhang *et al.s*[6], Zhang *et al.'s*[7] protocols are based on multiparty computation but they have (n, n) threshold approach; their modulo are 2 and computation type is bit-by-bit. The protocols of Chen *et al.*[5] and Zhang *et al.*[6] perform 1 Unitary operation. Both the protocols of Shi *et al.*[8] are based on multiparty computation and computation type is secret-by-secret, but they have (n, n) threshold approach. In the Shi *et al.'s* protocols[8], the QFT is applied on the first particle by initiator Bob_1,who sends second particle to next player. Then, the unitary operation is performed by each player Bob_i, $i=2, 3, \ldots, n$. Initiator Bob_1 applies QFT^{-1} on his particle. So, the total computation and communication costs of these protocols are $1QFT + 1QFT^{-1} + (n-1)$ unitary operations $+ 2$ measure operation and n, respectively. The Shi's protocol[9] is based on multiparty computation but it has (n, n) threshold approach and its computation type is bit-by-bit. The Zhang *et al.'s* protocol[10] is based on multiparty computation but it has (n, n) threshold approach with bit-by-bit computation type and modulo of 2. The total computation cost of this protocol is n measure operations. The Liu *et al.'s* protocol[11] is based on multiparty computation but it has (n, n) threshold approach with bit-by-bit computation type and modulo of 2. The total computation and

Protocols				Du[4]	Chen[5]	Zhang[6]	Zhang[7]	Shi[8]		Shi[9]	Zhang[10]	Liu[11]	Yang[12]	Jiao[13]		Proposed	
Operation				Summ.	Summ.	Summ.	Summ.	Summ.	Multi.	Summ.	Summ.	Summ.	Summ.	Summ.	Multi.	Summ.	Multi.
Performance Parameters	Costs	Comt.	QFT	—	—	—	—	1	1	—	—	—	n	—	—	1	1
			QFT^{-1}	—	—	—	—	1	1	—	—	—	—	—	—	—	—
			Unitary Operation	—	1	1	—	$n-1$	$n-1$	—	—	—	—	n	n	$t-1$	$n-1$
			Measure Operation	—	—	—	—	2	2	—	n	n	n	n	n	t	t
		Com.	Message Particle	—	—	—	—	—	—	—	—	—	—	—	—	$t-1$	$t-1$
			Decoy Particle	—	—	—	—	n	n	—	—	n	$n-1$	n	n	—	—
	Univ.	Model		(n, n)	(n, n)	(n, n)	(n, n)	(n, n)	(n, n)	(n, n)	(n, n)	(n, n)	(n, n)	(n, n)	(n, n)	(t, n)	(t, n)
		Modulo		$n+1$	2	2	2	N	N	—	2	2	d	N	N	d	d
		Qubits		—	—	—	—	$\lceil log_2^d \rceil n$	$\lceil log_2^d \rceil n$	$2\lceil log_2^d \rceil n$	—	2	—	—	—	—	—
		Type of Computation		b-by-b	b-by-b	b-by-b	b-by-b	s-by-s	s-by-s	b-by-b	b-by-b	b-by-b	s-by-s	b-by-b	b-by-b	s-by-s	s-by-s
	Attacks	IR		—	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	—	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
		Collusion		—	*Yes*	*No*	*No*	—	—	—	*Yes*	—	*Yes*	—	—	*Yes*	*Yes*
		EM		—	—	*Yes*	—	*Yes*	*Yes*	—	—	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
		Collective		—	—	—	—	—	—	—	—	—	—	—	—	*Yes*	*Yes*
		Coherent		—	—	—	—	—	—	—	—	—	—	—	—	*Yes*	*Yes*

Table 2. Comparison in terms of Cost, Universality, and Attack.

computation costs of this protocol is n and n, respectively. The Yang's protocol[12] is based on multiparty computation but it has (n, n) threshold approach. The total computation and communication costs of this protocol are $nQFT + n$ measure operation and $(n-1)$, respectively. The Jiao *et al.'s* protocol[13] is based on multiparty computation but it has (n, n) threshold approach with bit-by-bit computation type. The total computation and communication costs of this protocol is n unitary operation $+ n$ measure operations and n, respectively. However, our proposed summation and multiplication protocols are based on multiparty computation with modulo d, have (n, n) threshold approach, and their computation type is secret-by-secret. The total computation and communication costs of these protocols are $1QFT + (t-1)$ unitary operation $+ t$ measure operation and $(t-1)$, respectively. So, our protocols are more secure, flexible, and practical as compared to the existing summation and multiplication protocols. The comparison of cost, universality, and attack are shown in Table 2. In this table, *IR*, *EM*, *Comt*, *Com*, s-by-s, b-by-b, Summ. and Multi. denote intercept-resend attack, entangle-measure attack, computation cost, communication cost, secret-by-secret, bit-by-bit, summation and multiplication, respectively.

Conclusion

In this paper, we have presented the hybrid (t, n) threshold quantum protocols for multiparty summation and multiplication. They have better communication and computation costs as the type of computation is secret-by-secret. They can resist the quantum attacks, i.e., intercept-resend, entangle-measure, collusion, collective, and coherent. No player cannot get other players' private information. Our protocols are more secure, flexible, and practical as compared to the existing summation and multiplication protocols. Further, they possess all the benefits (i.e., use qudit instead of qubit, do not pass any secret information through the transmitted particles, do not perform entanglement measurement, and quantum attacks are not possible) of the existing secure multiparty quantum summation and multiplication.

Received: 26 July 2019; Accepted: 6 May 2020;
Published online: 04 June 2020

References

1. Hu, X., Fan, H., Zhou, D. & Liu, W.-M. Necessary and sufficient conditions for local creation of quantum correlation. *Physical Review A* **85**, 032102 (2012).
2. Li, Z.-G., Fei, S.-M., Wang, Z. & Liu, W. Evolution equation of entanglement for bipartite systems. *Physical Review A* **79**, 024303 (2009).
3. Abliz, A., Gao, H., Xie, X., Wu, Y. & Liu, W. Entanglement control in an anisotropic two-qubit heisenberg x y z model with external magnetic fields. *Physical Review A* **74**, 052105 (2006).
4. Jian-Zhong, C. Du ann Xiu-Bo & Qiao-Yan, W. Secure multiparty quantum summation. *Acta Physica Sinica* **56**, 6214–6219 (2007).
5. Chen, X.-B., Xu, G., Yang, Y.-X. & Wen, Q.-Y. An efficient protocol for the secure multi-party quantum summation. *International Journal of Theoretical Physics* **49**, 2793–2804 (2010).
6. Zhang, C., Sun, Z., Huang, Y. & Long, D. High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. *International Journal of Theoretical Physics* **53**, 933–941 (2014).
7. Zhang, C., Sun, Z.-W., Huang, X. & Long, D.-Y. Three-party quantum summation without a trusted third party. *International Journal of Quantum Information* **13**, 1550011 (2015).
8. Shi, R.-h, Mu, Y., Zhong, H., Cui, J. & Zhang, S. Secure multiparty quantum computation for summation and multiplication. *Scientific reports* **6**, 19655 (2016).

9. Shi, R.-H. & Zhang, S. Quantum solution to a class of two-party private summation problems. *Quantum Information Processing* **16**, 225 (2017).
10. Zhang, C., Situ, H., Huang, Q. & Yang, P. Multi-party quantum summation without a trusted third party based on single particles. *International Journal of Quantum Information* **15**, 1750010 (2017).
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. *International Journal of Theoretical Physics* **56**, 2783–2791 (2017).
12. Yang, H.-Y. & Ye, T.-Y. Secure multi-party quantum summation based on quantum fourier transform. *Quantum Information Processing* **17**, 129 (2018).
13. Lv, S.-X., Jiao, X.-F. & Zhou, P. Multiparty quantum computation for summation and multiplication with mutually unbiased bases. *International Journal of Theoretical Physics* 1–11 (2019).
14. Shamir, A. How to share a secret. *Communications of the ACM* **22**, 612–613 (1979).
15. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, New York, NY, USA, 2011), 10th edn.
16. Nielsen, M. A. & Chuang, I. *Quantum computation and quantum information* (2002).
17. Thas, K. The geometry of generalized pauli operators of n-qudit hilbert space, and an application to mubs. *EPL (Europhysics Letters)* **86**, 60005 (2009).
18. Turner, L. R. *Inverse of the vandermonde matrix with applications* (1966).

Acknowledgements

This work is partially supported by Indian Institute of technology (ISM) Dhanbad.

Author contributions

Study conception, design, and writing of the manuscript: K.S. Analysis: H.O. All authors reviewed the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to K.S.

Reprints and permissions information is available at www.nature.com/reprints.

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