Quantum Information and Computation, Vol. 23, No. 3&4 (2023) 0245–0256

SECURE MULTIPARTY QUANTUM AGGREGATING PROTOCOL

KARTICK SUTRADHAR
Department of Computer Science and Engineering,
Gandhi Institute of Technology and Management, Bengaluru, Karnataka, India
Email: kartick.sutradhar@gmail.com

Secure multiparty quantum computation is an important and essential paradigm of quantum computing. All the existing aggregating protocols are (n, n) threshold approaches, where n represents the total number of players. If one player is dishonest, the aggregation protocols cannot aggregate efficiently. In this paper, we propose a (t, n) threshold-based aggregating protocol, where t represents the threshold number of players. This protocol uses Shamir's secret sharing, quantum state, SUM gate, quantum Fourier transform, blind matrix, and Pauli operator. This protocol can perform the aggregation securely and efficiently. In this protocol, we simulate this aggregating protocol using the IBM quantum processor to verify the correctness and feasibility.

Received November 20, 2022
Revised January 29, 2023

Keywords: Quantum Cryptography, Quantum Computation, Information security, Aggregating Protocol, Quantum Circuit.

1 Introduction

Secure multiparty quantum computation is a technique to perform arithmetic operations (i.e., aggregation, multiplication, comparison, and sorting) securely and distributively. The aggregation is one of the basic arithmetic operation of secure multiparty quantum computation. The secure multiparty quantum aggregation contains a list of secrets and a set of players. These secrets are shared with the total players and the threshold number of players jointly performs aggregation without disclosing their secrets. The existing aggregating protocols are (n, n) threshold approach, where n represents the total number of players. If one player is dishonest, the aggregation protocols cannot aggregate efficiently. In this paper, we propose a (t, n) threshold-based aggregating protocol, where t represents the threshold number of players. This protocol uses Shamir's secret sharing, quantum state, SUM gate, quantum Fourier transform, blind matrix, and Pauli operator to efficiently and securely aggregate the secrets. The proposed protocol can be used to build complex circuits [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12] such as e-voting and e-auction.

1.1 Motivation

The secure multiparty quantum aggregating protocol can securely aggregate the secrets. The existing secure multiparty quantum aggregating protocols are efficient however, these protocols are (n, n) threshold approach, where n denotes the total number of players. If one player of these protocols is dishonest, then these protocols can not be executed efficiently and securely. So, the critical research gap in the secure multiparty quantum aggregating protocol is to design a secure and efficient protocol.

1.2 Contribution

This paper proposes a quantum aggregating protocol using secure multiparty computation. This protocol can securely aggregate the secrets because it uses quantum phenomena such as Shamir's secret sharing, quantum state, SUM gate, quantum Fourier transform, blind matrix, and Pauli operator. The main contributions of this paper can be summarized as follows.

- The proposed secure multiparty quantum aggregating protocol can aggregate the secrets efficiently and securely.
- This protocol is based on (t, n) threshold approach, where t and n denote the threshold number of players, and the total number of players, respectively. This protocol can securely aggregate the secrets if t out of n players execute the protocol honestly.
- Our proposed protocol can prevent the outside (i.e., Intercept, Intercept-Resend, Entangle-Measure, Man-in-the-middle, Collective, Trojan Horse, and Coherent) and participant (i.e., Collusion, Forgery, and Collusion) attacks.
- Our proposed protocol is more secure and efficient as compared to the existing protocols.

The organization of this paper is as follows manner. We first discuss this paper's introduction, motivation, and contributions in Section 1. In Section 2, we provide the relevant related works. The preliminaries are discussed in Section 3. In Section 4, we introduce the proposed protocol. Section 5 introduces the correctness proof, and Section 6 discusses the simulation result. Section 7 introduces the security analysis, and Section 8 discusses the performance analysis, followed by the conclusion in Section 9.

2 Related Work

In quantum computing, there existed some aggregating protocols based on secure multiparty computation. The first secure multiparty quantum aggregating protocol was proposed by Du *et al.* [13] in 2007. This protocol is based on multiparty computation, but it has (n, n) threshold method. Thereafter, Chen *et al.* [14] proposed a secure multiparty quantum aggregating protocol based on multi-particle entangled. This protocol uses multiparty quantum computation, but it is a threshold approach of (n, n), where n out of n honest players requires to execute the protocol efficiently. Zhang *et al.*[15] proposed a polarization-based quantum aggregating protocol. This protocol is based on multiparty computation, but its modulo is too small, and it has a threshold method of (n, n). Zhang *et al.* [16] proposed a secure quantum aggregating protocol in 2015. This protocol is efficient, but it is a three-party protocol. Another secure multiparty quantum aggregating protocol was proposed by Shi *et al.* [17] in 2017. This protocol is based on multiparty computation, but it has a threshold method of (n, n). Thereafter, Shi and Zhang [18] proposed a quantum protocol for aggregating in 2017. This protocol is efficient, but it is two party protocol. Then, Zhang *et al.* [19] proposed a quantum aggregating protocol with modulo 2. This protocol is efficient but not secure because the modulo is too small. In the same year, Liu *et al.* [20] proposed a secure multiparty quantum aggregating protocol. This protocol is efficient, but it is a threshold method of (n, n). Yang and Ye [21] proposed a secure multiparty aggregating protocol based on quantum mechanics in 2018. It is efficient, but it is a threshold method of (n, n). Jiao

et al. [22] proposed a quantum-based secure multiparty aggregating protocol. This protocol is efficient, but it is a threshold method of (n, n). Ye and Xu [23] proposed a lightweight quantum protocol for secure summation using single particle states. This protocol can resist the intercept, intercept-resend, and entangle-measure attacks, but it has a threshold method of (n, n) with modulo 2. Thereafter, Hu and Ye [24] proposed a secure quantum summation. This protocol is based on three parties and the threshold method of (n, n). Ye *et al.* [25] proposed another secure quantum summation protocol, but it has only two parties. If one party is dishonest, then summation cannot be performed correctly. Then, Pan [26] improved the three party secure quantum summation protocol. This protocol is secure but has a threshold method of (n, n). Ye and Hu [27] proposed a quantum protocol for secure multiparty summation. This protocol can resist the intercept, intercept-resend, and entangle-measure attacks, but it also has a threshold method of (n, n). Ming-Yi [28] proposed a multiparty quantum summation that is based on a d-level quantum system. This protocol employed the multiparty computation but has a threshold method of (n, n). All the existing quantum protocols [13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28] for multiparty aggregating protocols are threshold method of (n, n), where n out of n players need to be honest. If one player performs the aggregating protocol dishonestly, then the aggregation can not be done efficiently.

3 Preliminaries

In this section, we discuss the preliminaries (i.e., Shamir's secret sharing, quantum Fourier transform (QFT), quantum state, SUM gate, generalized Pauli operator, and blind matrix), which will be used in the proposed protocol.

3.1 Shamir's Secret Sharing [29]

In Shamir's secret sharing, the dealer $\mathbb{D}$ share the secret among the n players $\mathbb{B} = \{\mathbb{B}_1, \mathbb{B}_2, \ldots, \mathbb{B}_n\}$. It is consists of two phases: secret sharing and reconstruction.

3.1.1 Secret Sharing Phase

In secret sharing phase, the dealer selects a polynomial $l(x)$ to share the secret with n players, where the degree of the polynomial is $(t-1)$.

3.1.2 Secret Reconstruction Phase

In secret reconstruction phase, the threshold number of players (t) reconstruction the secret using the Lagrange interpolation formula.

3.2 SUM gate [21]

The d-level quantum SUM gate can be formulated as:

$$SUM(|e\rangle, |k\rangle) = (|e\rangle, |e + k \mod d\rangle),$$

where $|e\rangle$ and $|k\rangle$ represent control and target particles, respectively, and $e, k \in \{0, 1, \ldots, d-1\}$.

3.3 Quantum Fourier Transform (QFT) *[17]*

The QFT is the quantum version of the discrete Fourier transform. The d-level QFT can be formulated as:

$$QFT : |r\rangle \rightarrow \frac{1}{\sqrt{d}} \sum_{s=0}^{d-1} \omega^{r.s} |s\rangle ,$$

where ω denotes $e^{2\pi i}$.

3.4 Generalized Pauli operator [21]

The d-level generalized Pauli operator can be formulated as: $U_{\phi,\varphi} = \sum_{a=0}^{d-1} \omega^{a.\varphi} |a+\phi\rangle \langle a|$, where, $\phi, \varphi \in \{0, 1, \ldots d-1\}$.

3.5 Blind matrix

The Blind matrix [21] is a kind of square matrix. The blind matrix is shown as follows.

$$\begin{pmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ c_{31} & c_{32} & \ldots & c_{3n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{n1} & c_{n2} & \ldots & c_{nn} \end{pmatrix}$$

where c_{pq} denotes the element in the p^{th} row and q^{th} column and $p, q \in (1, \ldots, n)$. It must satisfy $\sum_{q=1}^{n} c_{pq} \pmod d = 0$.

4 Proposed Protocol

Suppose $\mathcal{R} = \{\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_n\}$ be the n secrets and $\mathbb{B} = \{\mathbb{B}_1, \mathbb{B}_2, \ldots, \mathbb{B}_n\}$ be the set of n players. The players $\mathbb{B}_m$ $(1 \leq m \leq n)$ holds the secret $\mathcal{R}_m$ and the qualified subset players can aggregate the secrets. Let $\mathbb{Q} = \{\mathbb{B}_1, \mathbb{B}_2, \ldots, \mathbb{B}_t\}$ be a qualified subset players. Each qualified subset possesses the t number of players $\mathbb{Q} = \{\mathbb{B}_1, \mathbb{B}_2, \ldots, \mathbb{B}_t\}$ and $\mathbb{B}_1$ is an initiator. The process of secure aggregating quantum protocol is shown as follows.

Step 1: Initially, the player $\mathbb{B}_1$ (initiator) creates single qudit t particles $|r\rangle_1, |r\rangle_2, \ldots, |r\rangle_t$.

Step 2: Then, the initiator player $\mathbb{B}_1$ performs the QFT on the first particle $|r\rangle_1$. The resultant quantum state $|\psi_1\rangle$ is shown as follows.

$$|\psi_1\rangle = (QFT\,|r\rangle_1) = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a\rangle_1 \tag{1}$$

Here, the control and target qudits are $|\psi_1\rangle$ and $|r\rangle_m$'s, $m = 2, 3, \ldots, t$, respectively.

Step 3: Thereafter, the initiator player $\mathbb{B}_1$ applies the SUM gate to create an entangled quantum state $|\psi_2\rangle = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a\rangle_1 |a\rangle_2 \ldots |a\rangle_t$. The initiator player $\mathbb{B}_1$ sends the quantum particle $|a\rangle_m$ to other player $\mathbb{B}_m$, $m = 2, 3, \ldots, t$.

Step 4: Furthermore, m number of polynomials (such as $\bar{a}(h), \bar{b}(h), \ldots, \bar{n}(h)$) selected by the each player $\mathbb{B}_m$ to calculate the shares of secrets $\bar{a}(h_m), \bar{b}(h_m), \ldots, \bar{n}(h_m)$, where degree

of the polynomial is $(t-1)$. Then, the player $\mathbb{B}_m$ transfers the shares with the n players.

Step 5: Each player $\mathbb{B}_m$ computes $l(h_m) = \bar{a}(h_m) + \bar{b}(h_m) + \cdots + \bar{n}(h_m)$, $m = 1, 2, \ldots, n$.

Step 6: Then, each player $\mathbb{B}_m$ computes the shadow (k_m) of the share $l(h_m)$, $m = 1, 2, \ldots, t$. The shadow can be computed as follows:

$$k_m = l(h_i) \prod_{1 \leq j \leq t, j \neq f} \frac{h_j}{h_j - h_m} \mod d. \tag{2}$$

Step 7: Thereafter, each player $\mathbb{B}_m$ compute the c_m, $m = 1, 2, \ldots, t$, using the blind matrix [21].

Step 8: Furthermore, each player $\mathbb{B}_m$, $m = 2, 3, \ldots, t$, performs the QFT on his/her particle $|a\rangle_m$ and also applies the generalized Pauli operator $U_{k_m,0}$, $m = 1, 2, \ldots, t$. The quantum state $|\psi_3\rangle$ can be computed as follows:

$$\begin{aligned} |\psi_3\rangle &= U_{k_1,0}QFT \otimes U_{k_2,0}QFT \otimes \cdots \otimes U_{k_m,0}QFT\,|\psi_2\rangle \\ &= d^{-\frac{t+1}{2}} \sum_{\substack{0 \leq c_1, \ldots, c_m < d, \\ c_1 + , \ldots, + c_m = 0 \mod d}} |c_1 + k_1\rangle \ldots |c_m + k_m\rangle \end{aligned} \tag{3}$$

Step 9: Each player $\mathbb{B}_m$, $m = 2, 3, \ldots, t$, perform the measurement operation on his/her particle $|c_m + k_m\rangle$ and broadcasts the result of the measurement $c_m + k_m$, $m = 1, 2, \ldots, t$.

Step 10: Finally, they jointly added their measurement results to aggregate the secrets. The aggregation of the secrets can be computed as: $\mathcal{R} = \sum_{m=1}^{t} c_m + k_m \mod d$.

5 Correctness Proof

This section proves the correctness of secure multiparty quantum aggregating protocol.

Lemma 1: Suppose the players $\mathbb{B}_m$ holds the secrets $\mathcal{R}_1, \ldots, \mathcal{R}_m$, $m = 1, 2, \ldots, t$. If the players $\mathbb{B}_m$ execute the QFT and Pauli operator efficiently, then they can aggregate the secrets $\mathcal{R} = \sum_{m=1}^{t}(c_m + k_m) \mod d$.

Proof: The Lemma 1 proves that the proposed protocol can aggregate the secrets efficiently. If the players execute the following procedure correctly, then the players jointly can aggregate the secrets. In initial stage, each players $\mathbb{B}_m$, $m = 1, 2, \ldots, t$, executes the QFT operation on his/her particle $|a\rangle_m$ and then performs the Pauli operator $U_{k_m,0}$ on it. The quantum state $|\psi_2\rangle$ is converted to the quantum state $|\psi_3\rangle$ as follows:

$$\begin{aligned} |\psi_3\rangle &= U_{k_1,0}QFT \otimes U_{k_2,0}QFT \otimes \cdots \otimes U_{k_m,0}QFT\,|\psi_2\rangle \\ &= d^{-\frac{t+1}{2}} \sum_{\substack{0 \leq c_1, \ldots, c_m < d, \\ c_1 + , \ldots, + c_m = 0 \mod d}} |c_1 + k_1\rangle \ldots |c_m + k_m\rangle \end{aligned} \tag{4}$$

In computational basis, each player $\mathbb{B}_m$ perform the measurement operation his/her particle $|c_m + k_m\rangle$, and broadcasts the measurement results $(c_m + k_m)$, where $m = 1, 2, 3, \ldots, t$. Furthermore, they jointly sum up the measurement results to aggregate the secrets. The aggregated the secrets is shown as: $\mathcal{R} = \sum_{m=1}^{t} c_m + k_m \mod d$.

6 Simulation Results of Proposed Protocol

In this section, we discuss the simulation results of the proposed secure multiparty quantum aggregating protocol. We have developed a generalized circuit diagram for n players and n qubits. We also simulated it using IBM quantum computer. In this circuit diagram, the Hadamard gate is use as the quantum Fourier transform. In the initial stage, the t particle quantum state created by the initiator player $\mathbb{B}_1$. Thereafter, initiator player $\mathbb{B}_1$ performs the QFT on the first particle $|r\rangle_1$. Furthermore, the initiator player $\mathbb{B}_1$ applies the SUM gate to create the entangled quantum state and sends the quantum particle $|a\rangle_m$, to the player $\mathbb{B}_m$, $m = 2, 3, \ldots, t$. Then, each player $\mathbb{B}_m$, $m = 1, 2, \ldots, t$, compute c_m using the blind matrix. Furthermore, each player $\mathbb{B}_m$, $m = 2, 3, \ldots, t$, performs the QFT on his/her particle $|a\rangle_m$ and also applies the generalized Pauli operator $U_{k_m,0}$, $m = 1, 2, \ldots, t$. Each player $\mathbb{B}_m$, $m = 2, 3, \ldots, t$, perform the measurement operation on his/her particle $|c_m + k_m\rangle$ and broadcasts the result of the measurement $c_m + k_m$, $m = 1, 2, \ldots, t$. Finally, they jointly added their measurement results to secrets. The aggregation of the secrets can be computed as: $\mathcal{R} = \sum_{m=1}^{t} c_m + k_m \mod d$. The Figure 1 shows the generalized circuit diagram for n players and n qubits. We have simulated this circuit diagram with three players and three qubits, three players and four qubits, and three players and five qubits. In experiment 1, we

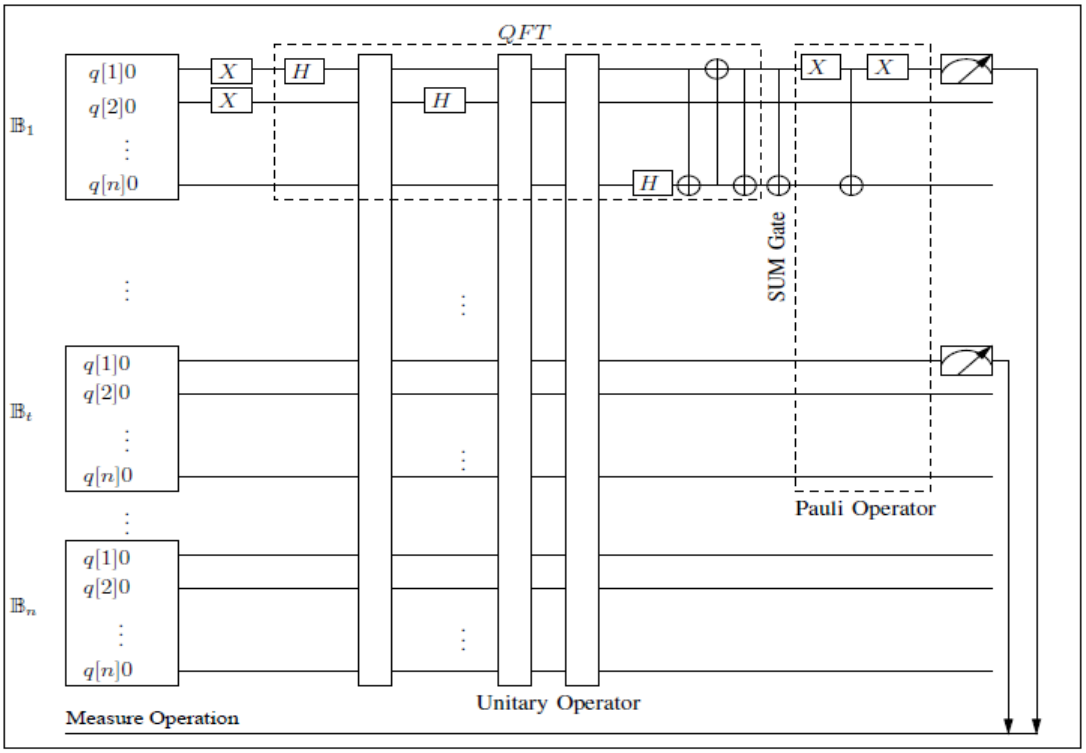

Fig. 1: Generalized circuit diagram for n players and n qubits.

have developed a circuit diagram for three players and three qubits similar to the generalized

circuit diagram for n players and n qubits. This circuit diagram is simulated using an IBM quantum computer. It is for three players and three qubits. We have simulated this circuit diagram using 1024, 4096, and 8192 average shots. In this experiment, we got the efficient result after performing the 8192 average shots. In experiment 2, we have constructed the circuit diagram for three players and four qubits and also simulated using an IBM quantum computer. In this experiment, we simulated this circuit using 1024, 4096, and 8192 average shots; and got the efficient result with 8192 average shots. In experiment 3, we have developed the circuit diagram for three players and five qubits, and this diagram is simulated by the IBM quantum computer. This circuit diagram also simulated using 1024, 4096, and 8192 average shots, and we got the efficient result with 8192 average shots.

7 Security Analysis

This section presents the security analysis of the proposed protocol. This protocol can resist the quantum attacks such as intercept (IT), intercept-resend (IR), entangle-measure (EM), collusion (CA), collective (COA), coherent (COH), man-in-the-middle (MIM), trojan horse (TH).

7.1 Intercept attack

The attacker grabs the quantum particle to perform this attack. Suppose the attacker grab the quantum particle $|a\rangle_m$, $m = 1, 2, \ldots, t$, and perform the measurement operation to reveal the shadow k_m. The attacker manages to get a with the probability $\frac{1}{d}$ from this measurement operation. Form this attack, the attacker is unable to reveal the information of shadow k_m because the quantum particle does not carry any valuable information of shadow k_m.

7.2 Intercept-resend attack

The attacker grabs the quantum particle, prepares an ancillary particle, and sends it to other players to perform this attack. Suppose the attacker grab the quantum particle $|a\rangle_m$, $m = 1, 2, \ldots, t$, prepare an ancillary particle $|\bar{a}\rangle_m$, and sends it to other players. Then, the attacker performs the measurement operation on the intercepted quantum particle $|a\rangle_m$ to reveal the shadow k_m. From this measurement result, the unable to get the information of shadow k_m because the intercepted quantum particle $|a\rangle_m$ possesses only a; nothing else.

7.3 Entangle-measure attack

The attacker grab all the quantum particles during sends one player to other players. Suppose the attacker grab the quantum particles $|a\rangle_m$, $m = 1, 2, \ldots, t$, during sends the initiator $\mathbb{B}_1$ to player $\mathbb{B}_m$, $m = 2, 3, \ldots, t$. Thereafter, the attacker selects an intercepted quantum particle $|a\rangle_v$, $v = 1, 2, \ldots, t$, and prepares an ancillary particle $|\bar{a}\rangle_v$. Then, the attacker applies the SUM gate on the quantum particle $|a\rangle_v$, $v = 1, 2, \ldots, t$, to entangle the ancillary quantum particle $|\bar{a}\rangle_v$. Furthermore, another ancillary quantum particle $|\bar{a}\rangle_u$, $u = 1, 2, \ldots, t$, creates by the attacker and applies the SUM gate on the quantum particle $|a\rangle_v$. Finally, the attacker perform the measurement operation and able to gets the value a with the probability $\frac{1}{d}$. The attacker concludes that the quantum particles $|a\rangle_m$ and $|a\rangle_v$ are the same particles. So, the attacker only able to gets a from this attack but a does not carry any information about shadow k_m.

7.4 Collusion attack

The player $\mathbb{B}_m$, $m = 1, 2, \ldots, t$, perform the measurement operation on his/her quantum particle $|c_m + k_m\rangle$ and sends this measurement result $c_m + k_m$ to other players. From this measurement result, the players cannot get any information about shadow k_m. To reveal the shadow k_m, the players $\mathbb{B}_{g-1}$ and $\mathbb{B}_{g+1}$ collude together however they cannot get the shadow k_m because the player $\mathbb{B}_m$, $m = 1, 2, \ldots, t$, send only the quantum particles $|a\rangle_m$ and this particles does not contain information about shadow k_m. So, this attack is infeasible.

7.5 Collective attack

The attacker creates an ancillary quantum particle $|\bar{a}\rangle_m$ to reveal the shadow k_m by interacting with each qubit of all players. Suppose the attacker creates an ancillary quantum particle $|\bar{a}\rangle_m$ and interacts with the intercepted quantum particles $|a\rangle_m$ to reveal the shadow k_m and perform the measurement operation on these intercepted quantum particles. From the measurement operation, the attacker manages to get a with the probability $\frac{1}{d}$. So, the attacker cannot get any information about shadow k_m because the intercepted quantum particles $|a\rangle_m$ do not contain the information about shadow k_m.

7.6 Coherent attack

All qubits of each player interacted by the attacker to perform the coherent attack. Let the ancillary particle $|\bar{a}\rangle_m$ created by the attacker to interact with all qubits of each player and perform the measurement operation on the intercepted quantum particle $|a\rangle_m$. From this measurement operation, the attacker manages to get a with the probability $\frac{1}{d}$. So, the attacker gets only a; nothing about shadow k_m because the measurement does not contain any information about shadow k_m.

7.7 Man-in-the-middle attack

The attacker misled the players during the communication to reveal the shadow k_m of the honest players. The attacker creates an ancillary quantum particle $|\bar{a}\rangle_m$ to intercept the original quantum particles, and the attacker intercepts the quantum particle $|a\rangle_m$. After intercepting the quantum particle $|a\rangle_m$, the attacker performs the measurement operation in computational basis. From this measurement operation, the attacker manages to get a with probability $\frac{1}{d}$ however the attacker is unable to reveal the shadow k_m because the intercepted the quantum particle $|a\rangle_m$ does not hold any information about the shadow k_m. So, this attack is not possible.

7.8 Trojan Horse attack

The attacker can execute the invisible and delay photon attacks because the information is transmitted through photons. The players jointly can resist the invisible photon attack using the wavelengths filter, which can operate the wavelength. The delay photon attack can be resisted by selecting the sample signals from the subset of the received photon signals.

8 Performance Analysis

Based on the three parameters such as cost, attack, and model, we analyze the performance and compare of proposed protocol with existing aggregating protocols. The Du *et al.'s* aggregating protocol [13] uses the modulo $n + 1$ and computation type is bit-by-bit however it is

the threshold method of (n, n). This protocol can resist the intercept and entangle-measure attacks, but it cannot resist the collusion, collective, and coherent attacks. The protocols [14, 15, 16] has a bit-by-bit computation type however, these are threshold method of (n, n) and the modulo is 2. This protocol can resist the intercept-resend attack however, these cannot resist the collective and coherent attacks. The Shi *et al.'s* aggregating protocol [17] uses the multiparty computation, and the type of computation is secret-by-secret however it is the threshold method of (n, n). This protocol can resist intercept and collusion attacks however it cannot resist the man-in-the-middle and trojan horse attacks. This protocol needs one QFT, $(n-1)$ unitary operations, 2 measure operations, and n number of decoy particles need to transfer. Shi's aggregating protocol [18] uses the multiparty computation and bit-by-bit computation type however it is the threshold method of (n, n). This protocol can resist intercept and entangle-measure attacks, but it cannot resist the collusion, man-in-the-middle, and trojan horse attacks. The Zhang *et al.'s* aggregating protocol[19] uses the multiparty computation and bit-by-bit computation type however it is the threshold method of (n, n) and modulo is 2. This protocol can resist the intercept, intercept-resend, entangle-measure, and coherent attacks, but it cannot resist the collusion, man-in-the-middle, and trojan horse attacks. This protocol requires n number of measure operations. The Liu *et al.'s* aggregating protocol [20] uses the multiparty computation and bit-by-bit computation type however it is the threshold method of (n, n) and modulo is 2. This protocol can resist intercept, intercept-resend, entangle-measure, and collusion attacks however it cannot resist the man-in-the-middle and trojan horse attacks. This protocol needs n number of measure operations, and n number of decoy particles need to transfer. Yang's aggregating protocol [21] uses the multiparty computation however it is the threshold method of (n, n). This protocol can resist intercept-resend, entangle-measure, and collective attacks however it cannot resist collusion, man-in-the-middle, and trojan horse attacks. This protocol needs one QFT, n number of measure operations, and $(n-1)$ number of decoy particles need to transfer. The Jiao *et al.'s* aggregating protocol [22] uses multiparty computation and bit-by-bit computation type however it is the threshold method of (n, n). This protocol can resist the intercept, intercept-resend, entangle-measure, coherent, man-in-the-middle, and trojan horse attacks however it cannot resist collusion attack. This protocol needs n number of unitary operation, n number of measure operation, and n number of decoy particles need to transfer. Ye and Xu's [23] protocol uses single particle states and bit-by-bit computation type. This protocol can resist the intercept, intercept-resend, and entangle-measure attacks, but it has a threshold method of (n, n) with modulo 2. This protocol needs n number of measure operations and n number of decoy particles that need to transfer. Hu and Ye's [24] protocol is based on three parties and the threshold method of (n, n). This protocol can resist the intercept, intercept-resend, entangle-measure, man-in-the-middle, and trojan horse attacks. This protocol needs n number of measure operations and n number of decoy particles that need to transfer. Ye *et al.'s* [25] is based on only two parties. If one party is dishonest, then summation cannot be performed correctly. This protocol can resist intercept, intercept-resend, man-in-the-middle, and trojan horse attacks. Pan's [26] protocol is only for three parties. It is secure but has a threshold method of (n, n). This protocol needs n number of measure operations and n number of decoy particles that need to transfer. Ye and Hu's [27] protocol can resist the intercept, intercept-resend, and entangle-measure attacks, but it also has a threshold method

of (n, n). This protocol needs n number of measure operations. Ming-Yi [28] protocol is based on a d-level quantum system. This protocol can resist intercept, intercept-resend, man-in-the-middle, and trojan horse attacks. This protocol employed the multiparty computation, but it has a threshold method of (n, n). Our protocol perform based on multiparty computation, threshold method of (t, n), and secret-by-secret computation type with modulo d. The proposed protocol needs one QFT, $(t-1)$ number of unitary operations, and t number of measure operations. The proposed protocol is more secure, flexible, and practical as compared to the existing aggregating protocols. The performance analysis can be shown in Table 1. In this table, QFT, MO, UO, DP, IT, IR, EM, CA, COA, COH, MIM, and TH denote quantum Fourier transform, measure operation, unitary operation, decoy particle, intercept, intercept-resend, entangle-measure, collusion, collective, coherent, man-in-the-middle, trojan horse attacks, respectively.

Table 1: Performance analysis

Protocols	Performance Parameters												
	Costs				Attacks								Model
	QFT	MO	UO	DP	IT	IR	EM	CA	COA	COH	MIM	TH	
Ref. [13]	-	-	-	-	Y	-	Y	N	N	N	-	N	(n, n)
Ref. [14]	-	-	-	-	Y	Y	Y	N	-	N	N	N	(n, n)
Ref. [15]	-	-	1	-	-	Y	-	N	N	N	N	N	(n, n)
Ref. [16]	-	-	1	-	Y	Y	Y	N	-	N	N	N	(n, n)
Ref. [17]	1	2	n-1	n	-	Y	-	-	Y	-	N	N	(n, n)
Ref. [18]	-	-	-	-	Y	-	Y	N	-	-	N	N	(n, n)
Ref. [19]	-	n	-	-	Y	Y	Y	N	-	Y	N	N	(n, n)
Ref. [20]	-	n	-	n	-	Y	Y	Y	Y	-	N	N	(n, n)
Ref. [21]	n	n	-	n-1	-	Y	Y	N	Y	Y	N	N	(n, n)
Ref. [22]	-	n	n	n	Y	Y	Y	N	Y	-	Y	Y	(n, n)
Ref. [23]	-	n	n	n	Y	Y	Y	N	N	N	N	N	(n, n)
Ref. [24]	-	n	-	n	Y	Y	-	Y	N	N	Y	Y	(n, n)
Ref. [25]	-	n	n	-	-	Y	Y	N	N	N	Y	Y	(n, n)
Ref. [26]	-	n	n	n	Y	Y	-	N	N	N	N	N	(n, n)
Ref. [27]	-	n	-	-	Y	Y	Y	N	N	N	N	N	(n, n)
Ref. [28]	-	n	n	n	Y	Y	-	N	N	N	Y	Y	(n, n)
Proposed	1	t	t-1	-	Y	Y	Y	Y	Y	Y	Y	Y	(t, n)

9 Conclusion

In this paper, we presented a quantum protocol for aggregating the secrets. The proposed protocol can efficiently and securely aggregate the secrets. The proposed protocol can resist the quantum attacks i.e., intercept, intercept-resend, entangle-measure, collusion, collective, coherent, man-in-the-middle, and trojan horse attacks. We simulated this protocol using an IBM quantum processor and got the efficient results of the proposed protocol after taking 8192 average shots. The proposed protocol can be used to build the e-voting and e-auction protocols.

References

1. Quanrun Li, Min Luo, Chingfang Hsu, Lianhai Wang, and Debiao He. A quantum secure and noninteractive identity-based aggregate signature protocol from lattices. *IEEE Systems Journal*, 2021.
2. Ahmed Louri. Three-dimensional optical architecture and data-parallel algorithms for massively parallel computing. *IEEE Micro*, 11(2):24–27, 1991.
3. Quintin Fettes, Mark Clark, Razvan Bunescu, Avinash Karanth, and Ahmed Louri. Dynamic voltage and frequency scaling in nocs with supervised and reinforcement learning techniques. *IEEE Transactions on Computers*, 68(3):375–389, 2018.
4. Dominic DiTomaso, Avinash Karanth Kodi, Ahmed Louri, and Razvan Bunescu. Resilient and power-efficient multi-function channel buffers in network-on-chip architectures. *IEEE Transactions on Computers*, 64(12):3555–3568, 2015.
5. Randy W Morris, Avinash Karanth Kodi, Ahmed Louri, and Ralph D Whaley. Three-dimensional stacked nanophotonic network-on-chip architecture with minimal reconfiguration. *IEEE Transactions on Computers*, 63(1):243–255, 2012.
6. Avinash Karanth Kodi, Ashwini Sarathy, and Ahmed Louri. Adaptive channel buffers in on-chip interconnection networksa power and performance analysis. *IEEE Transactions on Computers*, 57(9):1169–1181, 2008.
7. Yuechen Chen and Ahmed Louri. An approximate communication framework for network-on-chips. *IEEE Transactions on Parallel and Distributed Systems*, 31(6):1434–1446, 2020.
8. Wo-Tak Wu and Ahmed Louri. A methodology for cognitive noc design. *IEEE Computer Architecture Letters*, 15(1):1–4, 2015.
9. Pavan Poluri and Ahmed Louri. Shield: A reliable network-on-chip router architecture for chip multiprocessors. *IEEE Transactions on Parallel and Distributed Systems*, 27(10):3058–3070, 2016.
10. Avinash Karanth Kodi and Ahmed Louri. Design of a high-speed optical interconnect for scalable shared-memory multiprocessors. *IEEE micro*, 25(1):41–49, 2005.
11. Pavan Poluri and Ahmed Louri. A soft error tolerant network-on-chip router pipeline for multi-core systems. *IEEE computer architecture letters*, 14(2):107–110, 2014.
12. Avinash Karanth Kodi and Ahmed Louri. Optisim: A system simulation methodology for optically interconnected hpc systems. *IEEE micro*, 28(5):22–36, 2008.
13. Chen Jian-Zhong, Du ann Xiu-Bo and Wen Qiao-Yan. Secure multiparty quantum summation. *Acta Physica Sinica*, 56(11):6214–6219, 2007.
14. Xiu-Bo Chen, Gang Xu, Yi-Xian Yang, and Qiao-Yan Wen. An efficient protocol for the secure multi-party quantum summation. *International Journal of Theoretical Physics*, 49(11):2793–2804, 2010.
15. Cai Zhang, Zhiwei Sun, Yi Huang, and Dongyang Long. High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. *International Journal of Theoretical Physics*, 53(3):933–941, 2014.
16. Cai Zhang, Zhi-Wei Sun, Xiang Huang, and Dong-Yang Long. Three-party quantum summation without a trusted third party. *International Journal of Quantum Information*, 13(02):1550011, 2015.
17. Run-hua Shi, Yi Mu, Hong Zhong, Jie Cui, and Shun Zhang. Secure multiparty quantum computation for summation and multiplication. *Scientific reports*, 6:19655, 2016.
18. Run-Hua Shi and Shun Zhang. Quantum solution to a class of two-party private summation problems. *Quantum Information Processing*, 16(9):225, 2017.
19. Cai Zhang, Haozhen Situ, Qiong Huang, and Pingle Yang. Multi-party quantum summation without a trusted third party based on single particles. *International Journal of Quantum Information*, 15(02):1750010, 2017.
20. Wen Liu, Yong-Bin Wang, and Wen-Qin Fan. An novel protocol for the quantum secure multi-party summation based on two-particle bell states. *International Journal of Theoretical Physics*, 56(9):2783–2791, 2017.
21. Hui-Yi Yang and Tian-Yu Ye. Secure multi-party quantum summation based on quantum fourier

transform. *Quantum Information Processing*, 17(6):129, 2018.
22. Shu-Xin Lv, Xian-Fang Jiao, and Ping Zhou. Multiparty quantum computation for summation and multiplication with mutually unbiased bases. *International Journal of Theoretical Physics*, pages 1–11, 2019.
23. Tian-Yu Ye and Tian-Jie Xu. A lightweight three-user secure quantum summation protocol without a third party based on single-particle states. *Quantum Information Processing*, 21(9):1–15, 2022.
24. Jia-Li Hu and Tian-Yu Ye. Three-party secure semiquantum summation without entanglement among quantum user and classical users. *International Journal of Theoretical Physics*, 61(6):1–11, 2022.
25. Tian-Yu Ye, Tian-Jie Xu, Mao-Jie Geng, and Ying Chen. Two-party secure semiquantum summation against the collective-dephasing noise. *Quantum Information Processing*, 21(3):1–14, 2022.
26. Hong-Ming Pan. Cryptanalysis and improvement of three-party semi-quantum summation using single photons. *International Journal of Theoretical Physics*, 61(4):1–5, 2022.
27. Tian-Yu Ye and Jia-Li Hu. Quantum secure multiparty summation based on the phase shifting operation of d-level quantum system and its application. *International Journal of Theoretical Physics*, 60(3):819–827, 2021.
28. Duan Ming-Yi. Multi-party quantum summation within a d-level quantum system. *International Journal of Theoretical Physics*, 59(5):1638–1643, 2020.
29. Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.