Tian et al. *EPJ Quantum Technology* (2024) 11:35
https://doi.org/10.1140/epjqt/s40507-024-00247-9

EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH Open Access

Different secure semi-quantum summation models without measurement

Yuan Tian[1*], Nanyijia Zhang[1], Chongqiang Ye[2], Genqing Bian[1] and Jian Li[1,2]

*Correspondence:
tinyuen@xauat.edu.cn
[1]College of Information and Control Engineering, Xi'an University of Architecture and Technology, Xi'an, Shaanxi, China
Full list of author information is available at the end of the article

Abstract

Secure semi-quantum summation entails the collective computation of the sum of private secrets by multi-untrustworthy and resource-limited participants, facilitated by a quantum third-party. This paper introduces three semi-quantum summation protocols based on single photons, where eliminating the need for classical users to possess measurement capabilities. Two-party protocol 1 and protocol 2 are structured upon different models: star and ring, respectively. The security analysis extensively evaluates the protocols' resilience against outside and inside attacks, demonstrating protocols are asymptotically secure. Protocol 3 extends two-party protocol 1 to multi-party scenarios, broadening its applicability. Comparison reveals a reduction in the workload for classical users compared to previous similar protocols, and the protocols' correctness are visually validated through simulation by Qiskit.

Keywords: Quantum communication; Semi-quantum cryptography; Secure semi-quantum summation; Measurement free

1 Introduction

Quantum communication employs qubits as carriers of information exchange, surpassing the limitations of classical information technology in ensuring information security and other aspects. Leveraging the unique physical properties of quantum mechanics, it guarantees non-eavesdropping keys, thus achieving unconditional secure quantum communication in principle and introducing novel concepts for network security [1–4]. The BB84 protocol [5], as the pioneering quantum key distribution (QKD) protocol, showcases the potential of utilizing quantum principles for secure communication, laying the groundwork for the exploration of quantum cryptographic protocols [6–8]. Building upon the foundational work in QKD, researchers have delved into quantum protocols extending beyond secure communication to encompass secure computation [9–12].

Secure multi-party computation (SMC) is a technology enabling multiple parties to collectively compute a predetermined function result without revealing their private data [13, 14]. This technology finds applications in areas such as electronic voting, threshold signatures, and electronic auctions, serving as the cryptographic bedrock for these implementations. However, in 1994, Shor demonstrated the efficacy of quantum algorithms in rapidly factoring large prime numbers [15]. In light of quantum computing, classical SMC

Springer

faces significant threats [16], as it fails to offer robust security reliant on computational power keys. Quantum secure multi-party computation (QSMC) entails integrating fundamental principles of quantum mechanics into the protocol design of secure multi-party computation [17, 18], ensuring resistance against quantum computing attacks and delivering enhanced security performance while fulfilling the function of secure multi-party computation.

Quantum secure multi-party summation (QSMS) is a subfield of QSMC, which can be seen as an extension of classical multi-party privacy summation in the field of quantum mechanics [19–23]. The main purpose of QSMS is to calculate the sum of n participant secret values without revealing their secrets. It can be definition as follows: N participants $P_1, P_2, \ldots, P_N$ try to calculate a summation function $f(y_1, y_2, \ldots, y_N)$, where $y_i \in \{y_1, y_2, \ldots y_N\}$ are present participant P_i's private input.

While research on quantum information technology is still in its nascent stages, technologies such as quantum communication and quantum computing present challenges due to their complexity and difficulty of application in current work and life scenarios. Additionally, quantum devices entail high costs and intricate operations, with stringent requirements for preparing, storing, and transmitting quantum states. The semi-quantum secure communication protocol proposed by Boyer et al. [24] effectively addresses the bottleneck in the current development of quantum secure communication. It offers a relatively easier implementation while ensuring security. This protocol allows one party to possess full quantum capability, while the other party's quantum capability remains limited, thus enabling secure communication between quantum users and classical users.

In the semi-quantum secure communication protocol model, both quantum users and classical users require access to a two-way quantum channel [25–27]. Initially, qubits are transmitted from the quantum user to the classical user and then returned to the quantum user. Upon receiving each qubit, the classical user selects one of the following options: (1) Measurement: conduct a Z-basis measurement on the received particles. (2) Preparation: prepare a quantum state using the Z-basis and send it back to the quantum user. (3) Measurement and resend: perform Z-basis measurements on the received particles and then resend the results to the quantum user as Z-basis particles. This operation combines the above two actions, with the restriction that classical users always send the same state they measure. (4) Reflection: return the particles to the quantum users without any alteration. (5) Rearrangement: rearrange the received qubits without interfering with their states. The classical user does not ascertain the specific qubits, he only reorders them.

The first three-party semi-quantum summation (SQS) protocol was introduced by Zhang et al. [28] in 2021, utilizing single-qubit-based computation to calculate the summation of participants' private inputs. In comparison, the protocol proposed by Hu et al. [29] exhibited improved quantum measurement performance for quantum participants and potentially higher qubit efficiency in 2022. Subsequently, Ye et al. presented a more practical protocol capable of resisting collective-dephasing noise, although it failed to achieve the participants' summation results if a trusted party is absent [30]. In 2024, Lian et al. expanded from dimension 2 to dimension d, aiming to facilitate modulo d addition for more than three semi-quantum users' private integers [31].

However, ongoing research on SQS faces several challenges: (1) Requirement for classical participants: All classical participants must possess the capability to measure and prepare qubits. (2) Communication mode: The communication mode is relatively lim-

ited, achieving star communication but not ring communication. (3) Lack of simulation verification: There is a lack of simulation verification for the proposed protocols.

In this paper, we propose three protocols based on single photons that effectively tackle the aforementioned issues. Protocols 1 and 2 are devised upon different transmission models: one utilizing a star model and the other employing a ring model. Importantly, neither protocol necessitates participants to possess measurement capabilities. In the star model, a semi-honest third-party (TP) simultaneously transmits particles to users 1 and 2. After users 1 and 2 conduct their operations, the particles are returned to TP to finalize communication. Conversely, the ring model involves TP transmitting particles to user 1. Once user 1 completes the operation, the particles are then transmitted to user 2, who subsequently returns them to TP to complete the communication process. Protocol 3 extends protocol 1 (star model) from the two-party SQS to multi-party, thereby enhancing the protocol's applicability across various scenarios.

The contributions of this paper can be summarized as follows: (1) A protocol that does not require participant measurement is proposed, and classical users do not need to have measurement capabilities, further simplifying their operations. (2) Two different models, star and ring, are proposed without the need for measurement, and the star protocol is extended to multiple parties, expanding communication application scenarios. (3) The proposed protocol was simulated and verified, further verifying its correctness and feasibility. These protocols offer promising solutions for overcoming existing challenges in semi-quantum communication, particularly in terms of communication modes and participant capabilities.

The remainder of this paper is structured as follows: In Sect. 2, we introduce two semi-quantum summation protocols. Section 3 provides an analysis of the security aspects of the two proposed protocols. In Sect. 4, we present the simulation results of the two protocols. Following that, Sect. 5 introduces the multi-party protocol. Finally, Sect. 6 contains the discussion and conclusion of this paper.

2 Semi-quantum summation protocol based on single photons

In this section, an SQS protocol using single photons will be proposed. Suppose the quantum channels are ideal (ie, non-lossy and noiseless) and the classical channels are authenticated in the proposed protocol.

There are two participants (Alice, Bob) and a semi-honest TP. Alice and Bob are classical participants who have a private n-bit string, eager to summation their private information. TP has full quantum capabilities, who aims to obtain the modulo 2 of Alice and Bob's bit strings. Alice and Bob select an SQKD protocol to pre-shared the length of N keys $K = (K_1, K_2, \ldots, K_N)$. The length of participants' (Alice, Bob) private bit strings (A, B) is n. Alice and Bob private bit strings are denoted as $A = (a_1, a_2, \ldots, a_n)$ and $B = (b_1, b_2, \ldots, b_n)$, where $a_i, b_i \in \{0, 1\}, i = 1, 2, \ldots, n$. On the premise of not disclosing their respective private bit strings, they hope to use TP to help compute the summation:

$$M = A \oplus B = (a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_n \oplus b_n) \tag{1}$$

where, $\oplus$ is the modulo 2 addition.

2.1 Protocol 1: star and concise SQS

Step 1: TP generates $N = 8n$ two-qubit product states, each of which is

$$|+\rangle|+\rangle = \frac{(|0\rangle + |1\rangle)_A}{\sqrt{2}} \otimes \frac{(|0\rangle + |1\rangle)_B}{\sqrt{2}} \tag{2}$$

where A and B denote the system of Alice and Bob. There are two sequences $S_A = \{q_a^1, q_a^2, \ldots, q_a^N\}$ and $S_B = \{q_b^1, q_b^2, \ldots, q_b^N\}$, where q_a^i and q_b^i represent the i-th ($i = 1, 2, \ldots, N$) particle. Then, TP transmits S_A to Alice and S_B to Bob.

Step 2: Upon receiving particles from TP, Alice prepares a sequence $Z_A = \{z_a^1, z_a^2, \ldots, z_a^m\}$, where z_a^i is chosen from $\{|0\rangle, |1\rangle\}$ at random, $i = 1, 2, \ldots, m$. Subsequently, Alice combines Z_A and S_A to compose a new sequence Q_A, and reorders the positions of particles in the Q_A. Alice transmits Q_A to TP, where the length of Q_A is $8n+m$. After receiving the particles sent by TP, Bob implemented the same operation as Alice.

Step 3: When TP is receiving Q_A and Q_B from Alice and Bob, he randomly chooses either σ_Z basis ($\{|0\rangle, |1\rangle\}$) or σ_X basis ($\{|+\rangle, |-\rangle\}$) to measure each particle. Then, TP announces which basis he chose to measure for each particle.

Step 4: Alice and Bob publish the positions of S_A and Z_A in Q_A, S_B and Z_B in Q_B, respectively. According to Alice and Bob's different operations, the following eight cases will occur, and the details are listed in Table 1:

Case 1: TP performs σ_X measurement on the particle which is belongs S_A and S_B. Case 2: TP performs σ_X measurement on the particle which is belongs S_A and Z_B. Case 3: TP performs σ_X measurement on the particle which is belongs Z_A and S_B. Case 4: TP performs σ_X measurement on the particle which is belongs Z_A and Z_B.

The cases 1, 2, 3 and 4 are used for checking eavesdropping. An example is illustrated, in case 1, TP performs σ_X measurement to detect eavesdropping. If there are no eavesdroppers in quantum channel, TP obtains $|+\rangle_A \otimes |+\rangle_B$. Once other quantum states appear, it indicates the presence of eavesdroppers during the communication process. Once the error rate exceeds the pre-threshold value, the protocol will be discarded.

Case 5: TP performs σ_Z measurement on the particle which is belongs S_A and Z_B. Case 6: TP performs σ_Z measurement on the particle which is belongs Z_A and S_B. Case 7: TP performs σ_Z measurement on the particle which is belongs Z_A and Z_B.

The cases 5, 6 and 7, at least one of Alice and Bob has prepared the fresh particle, TP obtains a bit string $r_a^1, r_a^2, \ldots, r_a^{3n}$ and $r_b^1, r_b^2, \ldots, r_b^{3n}$ which measured in σ_Z basis corresponding the positions $r_a^1 r_a^2 \ldots r_a^{3n}$ and $r_b^1 r_b^2 \ldots r_b^{3n}$. The measurement results of Alice and Bob's are denoted as r_a^i and r_b^i which are used for computing the private summation.

Case 8: TP performs σ_Z measurement on the particle which is belongs S_A and S_B.

The case 8 will be discarded by TP.

Step 5: TP chooses a part of bits in $r_a^1 r_a^2 \ldots r_a^{3n}$ and $r_b^1 r_b^2 \ldots r_b^{3n}$ to be TEST bits, and declares the positions and value which he selected. Two participants announce the value of the TEST bits at the corresponding position. They calculate the error rate on TEST bits. Once the error rate is higher than the pre-threshold value, the protocol will be terminated.

Step 6: The participants and TP compute the summation of bit strings. Alice holds $R_A = \{r_a^1 r_a^2 \ldots r_a^n\}$, and Bob holds $R_B = \{r_b^1 r_b^2 \ldots r_b^n\}$. Alice computes $C_A^i = r_a^i \oplus a_i \oplus K_i$, Bob computes $C_B^i = r_b^i \oplus b_i \oplus K_i$, where $\oplus$ is the modulo 2 addition. Then, TP computes $C_A^i \oplus C_B^i \oplus r_a^i \oplus r_b^i = a_i \oplus b_i$, the result is Alice and Bob i-th private summation.

Table 1 Alice, Bob and TP's operations on the particle

Case	Alice's particle	Bob's particle	TP's measurement	Usage
1	S_A	S_B	σ_X basis	Eavesdropping detection
2	S_A	Z_B	σ_X basis	Eavesdropping detection
3	Z_A	S_B	σ_X basis	Eavesdropping detection
4	Z_A	Z_B	σ_X basis	Eavesdropping detection
5	S_A	S_B	σ_Z basis	Discard the particle
6	S_A	Z_B	σ_Z basis	Use Alice's particle to prepare one share of raw keys
7	Z_A	S_B	σ_Z basis	Use Bob's particle to prepare one share of raw keys
8	Z_A	Z_B	σ_Z basis	Obtain the raw key

2.2 Protocol 2: ring and concise SQS

Step 1: TP generates a N single photons S_T sequence which randomly contains $\{|+\rangle, |-\rangle, |0\rangle, |1\rangle\}$, and transmits to Alice.

Step 2: Upon receiving the sequence S_T from TP, Alice prepares a sequence $S_A = \{r_a^1, r_a^2, \ldots, r_a^N\}$, where r_a^i is chosen from $\{|0\rangle, |1\rangle\}$ at random, $i = 1, 2, \ldots, N$. Subsequently, Alice combines S_T and S_A to compose a new sequence S_2, and reorders the positions of particles in the S_2. Alice transmits S_2 to Bob, where the length of S_2 is $2N$.

Step 3: Upon receiving the sequence S_2 from Alice, Bob prepares a sequence $S_B = \{r_b^1, r_b^2, \ldots, r_b^N\}$, where r_b^i is chosen from $\{|0\rangle, |1\rangle\}$ at random, $i = 1, 2, \ldots, N$. Subsequently, Bob combines S_2 and S_B to compose a new sequence S_3, and reorders the positions of particles in the S_3. Bob transmits S_3 to TP, where the length of S_3 is $3N$.

Noticed that, the photons prepared by TP, Alice, Bob are represent CTRL photons, SIFT_A photons, SIFT_B photons, respectively.

Step 4: TP announces to A and B that he received the sequence S_3. Afterwards, two participants respectively declare the orders of the photons in the sequence S_2 and S_3.

Step 5: TP performs σ_X measurement on the CTRL photon, performs σ_Z measurement on the SIFT_A and SIFT_B photon. For detecting eavesdropping, TP calculates the error rate about CTRL photons. If eavesdropping absent, TP's measurement results should be consistent with what he initially prepared. Once the error rate is higher than the pre-threshold value, the protocol will be dropped.

Step 6: TP chooses a part of bits in $S_A = \{r_a^1, r_a^2, \ldots, r_a^N\}$ and $S_B = \{r_b^1, r_b^2, \ldots, r_b^N\}$ to be TEST bits, and declares the positions and value which he selected. Two participants announce the value of the TEST bits at the corresponding position. They calculate the error rate on TEST bits. Once the error rate is higher than the pre-threshold value, the protocol will be terminated.

Step 7: The participants and TP compute the summation of bit strings. Alice holds $R_A = \{r_a^1 r_a^2 \ldots r_a^n\}$, and Bob holds $R_B = \{r_b^1 r_b^2 \ldots r_b^n\}$. Alice computes $C_A^i = r_a^i \oplus a_i \oplus K_i$, Bob computes $C_B^i = r_b^i \oplus b_i \oplus K_i$, where $\oplus$ is the modulo 2 addition. Then, TP computes $C_A^i \oplus C_B^i \oplus r_a^i \oplus r_b^i = a_i \oplus b_i$, the result is Alice and Bob i-th private summation.

3 Security analysis

In this section, we analyze the proposed SQS protocols' security. Generally speaking, when analyzing SQS security, the following two attack scenarios need to be considered [7, 16, 28]. Outside attack: Malicious attacker attempts to obtain the privacy strings of participants. Inside attack: TP and participants attempt to steal the privacy strings of other

participants. Suppose Eve has fully quantum capability. The following will prove that Eve's access to any private information will introduce errors.

3.1 Security analysis of SCSQS

Outside attacker Eve attempts to grab the participants' private bit strings, and he needs to obtain the keys that the participant uses to encrypt their private inputs. Here is an analysis of Eve's desire to obtain Alice's private bit string, similar to the analysis of Bob's private bit string.

Intercept-resend attack Eve intercepts the sequence S_A which is sending to Alice from TP, and re-prepares self a sequence S_E. Eve sends Alice S_E instead of S_A. When Alice received S_E, she combines S_E with Z_A to obtain Q'_A, and transmits Q'_A to TP. Then, Eve intercepts Q'_A, attempts to infer which particles Alice prepared. He prepares a fake sequence Q''_A, and sends to TP. Unfortunately, Eve will be detected with high probability causing he does not realize the order of Q'_A.

When conducting eavesdropping detection in Step 4, TP performs σ_X measurement on the particle with 1/2, situation 1 with 1/2: particle in Z_A, there are no error introduce; situation 2 with 1/2: particle in S_A, Eve has a probability of 1/2 being detected. Hence, the total detection rate is $1/2 * (1/2 * 0 + 1/2 * 1/2) = 1/8$ in Step 4. Specifically, in case 1&2, the detection particle in S_A which generated by TP. When Eve sents particle one of $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ to TP with 1/4. Eve prepares $|+\rangle$ particle, he can pass the detection with 1/4. If Eve prepares $|0\rangle(|1\rangle)$, he can pass the detection with 1/2. Eve prepares $|-\rangle$ particle, he will be noticed by TP. In case 3&4, the detection particle in Z_A which generated by Alice. Because TP will take σ_X on the particle Z_A, the measurement results are $|+\rangle$ or $|-\rangle$, he cannot distinguish the fake particle.

For eavesdropping detection in Step 5, TP performs σ_Z measurement on the particle with 1/2, situation 3 with 1/2: the Z_A particle, Eve has a probability of 1/2 being detected. Situation 4 with 1/2: particle in S_A, discard. Hence, the total detection rate is $1/2 * 1/2 * 1/2) = 1/8$ in Step 5.

Measure-resend attack Eve intercepts and measures the sequence S_A which is sending to Alice from TP. He re-generates a sequence S_E with same measurement results and transmits to Alice. When Alice received S_E, she prepares a sequence Q'_A of S_E and Z_A together, and sends to TP. Subsequently, Eve intercepts and measures Q'_A to obtain Alice keys. And he generates a false sequence Q''_A, sends to TP. Apparently, because of Q'_A ordered by Alice, Eve can be detected with high probability.

For eavesdropping detection in Step 4, TP measures the particle using σ_X basis with 1/2, situation 1 with 1/2: the Z_A particle, there are no error introduce; situation 2 with 1/2: the S_A particle, Eve has a probability of 1/4 being detected. Hence, the total detection rate is $1/2 * (1/2 * 0 + 1/2 * 1/4) = 1/16$ in Step 4. Specifically, in case 1&2, the detection particle in S_A which prepared by TP. Eve cannot know which basis TP choice to generate particles. Eve chose σ_Z with 1/2, he can pass the detection with 1/2. Eve chose σ_X with 1/2, TP cannot notice he. In case 3&4, the detection particle in Z_A which prepared by Alice. Because TP will take σ_X on the particle Z_A, the measurement results are $|+\rangle$ or $|-\rangle$, he cannot distinguish the fake particle.

When conducting eavesdropping detection in Step 5, TP measures the particle using σ_Z basis with 1/2, situation 3 with 1/2: particle in Z_A, there are no error introduce. Situation 4 with 1/2: particle in S_A, discard. Eve does not introduce any errors in step 5.

Entangle-measure attack Eve performs attacks via two unitary operations on qubits: U_E operation to entangle the ancillary particle $|0\rangle_E$ for particles transferred from TP to Alice, and U_F operation to measure the ancillary particle $|0\rangle_E$ for particles transferred from Alice to TP. In the proposed protocol, Eve may perform attack on each qubit in Q_A and Q_B to entangle the qubit with its auxiliary qubits. After Alice and Bob pronounced the order of Q_A and Q_B, Eve then measures the auxiliary particles entangled with the particle to obtain information about Alice and Bob's key bits. The global state of the composite system composed by particles A, B and E is $A + B + E$.

A. Particles same sorted position which are in Z_A and Z_B. The state of $A + B + E$ becomes $|z_1z_2\rangle_{AB}|e_{Z_1Z_2}\rangle$, where $z_1, z_2 \in \{0, 1\}$. For Eve passing the detection in Step 5, U_F should satisfies:

$$U_F\big(|z_1z_2\rangle_{AB}|e_{Z_1Z_2}\rangle\big) = |z_1z_2\rangle_{AB}|f_{Z_1Z_2}\rangle \tag{3}$$

which means there is no change on the state of $A + B$.

B. Alice's particle in Z_A and Bob's particle in S_B. When z_a is $|0\rangle$, the state of $A + B + E$ becomes $|00\rangle_{AB}|e_{00}\rangle + |01\rangle_{AB}|e_{01}\rangle$, or the state of $A + B + E$ becomes $|10\rangle_{AB}|e_{10}\rangle + |11\rangle_{AB}|e_{11}\rangle$ when z_a is $|1\rangle$.

Let z_a is $|0\rangle$. After Eve performs U_F, state evolves into:

$$\begin{aligned} &U_F\big(|00\rangle_{AB}|e_{00}\rangle + |01\rangle_{AB}|e_{01}\rangle\big) \\ &\quad = |00\rangle_{AB}|f_{00}\rangle + |01\rangle_{AB}|f_{01}\rangle \\ &\quad = |0\rangle_A\big(|0\rangle_B|f_{00}\rangle + |1\rangle_B|f_{01}\rangle\big). \end{aligned} \tag{4}$$

Bring $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$ and $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$ into $B + E$ in equation (6):

$$\begin{aligned} &|0\rangle_B|f_{00}\rangle + |1\rangle_B|f_{01}\rangle \\ &\quad = |+\rangle_B\frac{|f_{00}\rangle + |f_{01}\rangle}{\sqrt{2}} + |-\rangle_B\frac{|f_{00}\rangle - |f_{01}\rangle}{\sqrt{2}}. \end{aligned} \tag{5}$$

If Eve wants to induce no error, TP should obtain the $|-\rangle$ with the probability of 0. Therefore,

$$|f_{00}\rangle = |f_{01}\rangle \tag{6}$$

Let z_a is $|1\rangle$. After Eve performs U_F, state evolves into:

$$\begin{aligned} &U_F\big(|10\rangle_{AB}|e_{10}\rangle + |11\rangle_{AB}|e_{11}\rangle\big) \\ &\quad = |10\rangle_{AB}|f_{10}\rangle + |11\rangle_{AB}|f_{11}\rangle \\ &\quad = |1\rangle_A\big(|0\rangle_B|f_{10}\rangle + |1\rangle_B|f_{11}\rangle\big). \end{aligned} \tag{7}$$

Bring $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$ and $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$ into $B + E$ in equation (6):

$$\begin{aligned} &|0\rangle_B|f_{10}\rangle + |1\rangle_B|f_{11}\rangle \\ &\quad = |+\rangle_B \frac{|f_{10}\rangle + |f_{11}\rangle}{\sqrt{2}} + |-\rangle_B \frac{|f_{10}\rangle - |f_{11}\rangle}{\sqrt{2}}. \end{aligned} \tag{8}$$

If Eve wants to induce no error, TP should obtain the $|-\rangle$ with the probability of 0. Therefore,

$$|f_{10}\rangle = |f_{11}\rangle \tag{9}$$

C. Alice's particle in S_A and Bob's particle in Z_B. When z_b is $|0\rangle$, the state of $A + B + E$ becomes $|00\rangle_{AB}|e_{00}\rangle + |10\rangle_{AB}|e_{10}\rangle$, or the state of $A+B+E$ becomes $|01\rangle_{AB}|e_{01}\rangle + |11\rangle_{AB}|e_{11}\rangle$ when z_b is $|1\rangle$.

Assume z_b is $|0\rangle$. After Eve performs U_F, state evolves into:

$$\begin{aligned} &U_F\big(|00\rangle_{AB}|e_{00}\rangle + |10\rangle_{AB}|e_{10}\rangle\big) \\ &\quad = |00\rangle_{AB}|f_{00}\rangle + |10\rangle_{AB}|f_{10}\rangle \\ &\quad = |0\rangle_B\big(|0\rangle_A|f_{00}\rangle + |1\rangle_A|f_{10}\rangle\big). \end{aligned} \tag{10}$$

Bring $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$ and $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$ into $A + E$ in equation (6):

$$\begin{aligned} &|0\rangle_A|f_{00}\rangle + |1\rangle_A|f_{10}\rangle \\ &\quad = |+\rangle_A \frac{|f_{00}\rangle + |f_{10}\rangle}{\sqrt{2}} + |-\rangle_A \frac{|f_{00}\rangle - |f_{10}\rangle}{\sqrt{2}}. \end{aligned} \tag{11}$$

If Eve wants to induce no error, TP should obtain the $|-\rangle$ with the probability of 0. Therefore,

$$|f_{00}\rangle = |f_{10}\rangle \tag{12}$$

Assume z_b is $|1\rangle$. After Eve performs U_F, state evolves into:

$$\begin{aligned} &U_F\big(|01\rangle_{AB}|e_{01}\rangle + |11\rangle_{AB}|e_{11}\rangle\big) \\ &\quad = |01\rangle_{AB}|f_{01}\rangle + |11\rangle_{AB}|f_{11}\rangle \\ &\quad = |1\rangle_B\big(|0\rangle_A|f_{01}\rangle + |1\rangle_A|f_{11}\rangle\big). \end{aligned} \tag{13}$$

Bring $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$ and $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$ into $A + E$ in equation (15):

$$\begin{aligned} &|0\rangle_A|f_{01}\rangle + |1\rangle_A|f_{11}\rangle \\ &\quad = |+\rangle_A \frac{|f_{01}\rangle + |f_{11}\rangle}{\sqrt{2}} + |-\rangle_A \frac{|f_{01}\rangle - |f_{11}\rangle}{\sqrt{2}}. \end{aligned} \tag{14}$$

If Eve wants to induce no error, TP should obtain the $|-\rangle$ with the probability of 0. Therefore,

$$|f_{01}\rangle = |f_{11}\rangle \tag{15}$$

According equation (8), (11), (14) and (17), it can be inferred that:

$$|f_{00}\rangle = |f_{01}\rangle = |f_{10}\rangle = |f_{11}\rangle = |f\rangle \tag{16}$$

D. Particles same sorted position which are in S_A and S_B. The state of $A + B + E$ becomes $|00\rangle_{AB}|e_{00}\rangle + |01\rangle_{AB}|e_{01}\rangle + |10\rangle_{AB}|e_{10}\rangle + |11\rangle_{AB}|e_{11}\rangle$. After Eve performs U_F, state evolves into:

$$\begin{aligned} &U_F\big(|00\rangle_{AB}|e_{00}\rangle + |01\rangle_{AB}|e_{01}\rangle + |10\rangle_{AB}|e_{10}\rangle + |11\rangle_{AB}|e_{11}\rangle\big) \\ &\quad = |00\rangle_{AB}|f_{00}\rangle + |01\rangle_{AB}|f_{01}\rangle + |10\rangle_{AB}|f_{10}\rangle + |11\rangle_{AB}|f_{11}\rangle. \end{aligned} \tag{17}$$

For no errors are introduced under Eve's attack, the measurement result of the state of $A + B$ should be $|++\rangle$. According equation (18), (19) can be rewritten as follows:

$$\begin{aligned} &U_F\big(|00\rangle_{AB}|e_{00}\rangle + |01\rangle_{AB}|e_{01}\rangle + |10\rangle_{AB}|e_{10}\rangle + |11\rangle_{AB}|e_{11}\rangle\big) \\ &\quad = |{+}{+}\rangle_{BC}|f\rangle. \end{aligned} \tag{18}$$

And according equation (18), (5), (6), (9), (12) and (15) can be rewritten as follows:

$$\begin{aligned} U_F\big(|z_1z_2\rangle_{AB}|e_{Z_1Z_2}\rangle\big) &= |z_1z_2\rangle_{AB}|f_{Z_1Z_2}\rangle \\ &= |z_1z_2\rangle_{AB}|f\rangle, \end{aligned} \tag{19}$$

$$\begin{aligned} U_F\big(|00\rangle_{AB}|e_{00}\rangle + |01\rangle_{AB}|e_{01}\rangle\big) &= |00\rangle_{AB}|f_{00}\rangle + |01\rangle_{AB}|f_{01}\rangle \\ &= |0{+}\rangle_{AB}|f\rangle, \end{aligned} \tag{20}$$

$$\begin{aligned} U_F\big(|10\rangle_{AB}|e_{10}\rangle + |11\rangle_{AB}|e_{11}\rangle\big) &= |10\rangle_{AB}|f_{10}\rangle + |11\rangle_{AB}|f_{11}\rangle \\ &= |1{+}\rangle_{AB}|f\rangle, \end{aligned} \tag{21}$$

$$\begin{aligned} U_F\big(|00\rangle_{AB}|e_{00}\rangle + |10\rangle_{AB}|e_{10}\rangle\big) &= |00\rangle_{AB}|f_{00}\rangle + |10\rangle_{AB}|f_{10}\rangle \\ &= |{+}0\rangle_{AB}|f\rangle, \end{aligned} \tag{22}$$

$$\begin{aligned} U_F\big(|01\rangle_{AB}|e_{01}\rangle + |11\rangle_{AB}|e_{11}\rangle\big) &= |01\rangle_{AB}|f_{01}\rangle + |11\rangle_{AB}|f_{11}\rangle \\ &= |{+}1\rangle_{AB}|f\rangle. \end{aligned} \tag{23}$$

Obviously, Eve induces no error, his probes are independent of two participants measurement results.

TP attack A semi-honest TP is defined as someone who needs to follow the protocol steps but is not allowed to collude with others, and can only attempt to deduce the participant's secret by collecting public information. Although TP can acquire the order of Q_A (Q_B), he does not know the pre-shared keys K between Alice and Bob. As a consequence, he cannot obtain the private bit strings.

Participant attack Suppose Alice is a dishonest participant who wants obtain the keys between TP and Bob, and infers to Bob's private bit string. When Alice attacks, she will use any possible attack methods, including the intercept-resend, measure-resend and

entangle-measure attacks used by outside attacker Eve. In addition, she will also adopt more serious attack methods.

3.2 Security analysis of RCSQS

Security analysis of RCSQS protocol is similar to SCSQS protocol. Here, we focus on analyzing dishonest participants'(dishonest Alice and dishonest Bob) attacks.

Intercept-resend attack Suppose Alice is a dishonest participant who wants to obtain SIFT_B, and intercepts the S_3. Then, she prepares $3N$ fake photons (S_3') and sends S_3' to TP. When Bob posted his rearranged order, Alice could measure the corresponding photons using σ_Z basis to obtains the Bob's bit string. However, Alice will be detected. To begin with, Alice's attack on CTRL photons can be easily detected because she does not know which state TP is prepared for. Besides, Alice's attack on SIFT_B photons can be easily detected because she does not distinguish the state and position of Bob's prepared particles.

For eavesdropping detection in Step 5, TP measures the particle using σ_X or σ_Z. Alice randomly prepared particle is $|1\rangle$ or $|0\rangle$, after measured by TP, the state will be $|+\rangle$, $|-\rangle$, $|0\rangle$ or $|1\rangle$. Hence, the detection rate is 1/4 in Step 5. When conducting eavesdropping detection in Step 6, TP will verify the state of the TEST bit with Bob, and there is a half chance that $|1\rangle$ or $|0\rangle$ randomly prepared by Alice will be the same as the state prepared by Bob. Hence, the detection rate is 1/2 in Step 6.

The security analysis of dishonest participant Bob using intercept-resend attack is similar to the analysis of Alice.

Measure-resend attack Suppose Bob is a dishonest participant who desires to acquire SIFT_A. When Bob received S_2, he measures all particles in S_2 using σ_Z basis and prepares new particles with same measurement results. Then, he prepares $3N$ fake photons S_3' and transmits to TP. When Alice posted her rearranged order, Bob could measure the corresponding photons using σ_Z basis to obtains the Alice's bit string. Nevertheless, Bob will be detected. Bob's attack on CTRL photons can be easily detected because she does not know which state TP is prepared for.

When conducting eavesdropping detection in Step 5, TP measures the particle using σ_X or σ_Z. Bob randomly prepared particle is $|1\rangle$ or $|0\rangle$, after measured by TP, the state will be $|+\rangle$, $|-\rangle$, $|0\rangle$ or $|1\rangle$. Hence, the detection rate is 1/4 in Step 5.

The security analysis of dishonest participant Alice using measure-resend attack is similar to the analysis of Bob.

Entangle-measure attack Considering that the sequence sent S_T by TP to Alice does not contain any valid information, Eve will perform two unitary operations on the qubits: U_S operation to entangle the ancillary particle for particles transferred from Alice to Bob, and U_T operation to measure the ancillary particle for particles transferred from Bob to TP.

A. Suppose Eve performs attack (U_S, U_T). Defined $|0\rangle_T$, $|1\rangle_T$, $|+\rangle_T$ and $|-\rangle_T$ represent the CTRL qubit, and SIFT_A qubits are represented as $|0\rangle_A$ and $|1\rangle_A$, and SIFT_B qubits are represented as $|0\rangle_B$ and $|1\rangle_B$. When Eve performed U_S, the composite system particles T and A become:

$$U_S\big(|0\rangle_T|g\rangle\big) = |0\rangle_T|g_{00}\rangle + |1\rangle_T|g_{01}\rangle, \tag{24}$$

$$U_S\big(|1\rangle_T|g\rangle\big) = |0\rangle_T|g_{10}\rangle + |1\rangle_T|g_{11}\rangle, \tag{25}$$

$$U_S\big(|+\rangle_T|g\rangle\big) = |0\rangle_T|g_{+0}\rangle + |1\rangle_T|g_{+1}\rangle, \tag{26}$$

$$U_S\big(|-\rangle_T|g\rangle\big) = |0\rangle_T|g_{-0}\rangle + |1\rangle_T|g_{-1}\rangle, \tag{27}$$

$$U_S\big(|0\rangle_A|g\rangle\big) = |0\rangle_A|g_{00}\rangle + |1\rangle_A|g_{01}\rangle, \tag{28}$$

$$U_S\big(|1\rangle_A|g\rangle\big) = |0\rangle_A|g_{10}\rangle + |1\rangle_A|g_{11}\rangle. \tag{29}$$

B. After Eve performed U_T, the composite system particles T, A and B become:

$$U_T U_S\big(|0\rangle_T|g\rangle\big) = U_T\big(|0\rangle_T|t_{00}\rangle + |1\rangle_T|t_{01}\rangle\big), \tag{30}$$

$$U_T U_S\big(|1\rangle_T|g\rangle\big) = U_T\big(|0\rangle_T|t_{10}\rangle + |1\rangle_T|t_{11}\rangle\big), \tag{31}$$

$$U_T U_S\big(|+\rangle_T|g\rangle\big) = U_T\big(|0\rangle_T|t_{+0}\rangle + |1\rangle_T|t_{+1}\rangle\big), \tag{32}$$

$$U_T U_S\big(|-\rangle_T|g\rangle\big) = U_T\big(|0\rangle_T|t_{-0}\rangle + |1\rangle_T|t_{-1}\rangle\big), \tag{33}$$

$$U_T U_S\big(|0\rangle_A|g\rangle\big) = U_T\big(|0\rangle_A|t_{00}\rangle + |1\rangle_A|t_{01}\rangle\big), \tag{34}$$

$$U_T U_S\big(|1\rangle_A|g\rangle\big) = U_T\big(|0\rangle_A|t_{10}\rangle + |1\rangle_A|t_{11}\rangle\big), \tag{35}$$

$$U_T\big(|0\rangle_B|t\rangle\big) = |0\rangle_B|t_{00}\rangle + |1\rangle_B|t_{01}\rangle, \tag{36}$$

$$U_T\big(|1\rangle_B|t\rangle\big) = |0\rangle_B|t_{10}\rangle + |1\rangle_B|t_{11}\rangle. \tag{37}$$

C. Eve can not be detected through eavesdropping, the following conditions will be met:

$$\begin{aligned} U_T U_S\big(|0\rangle_T|g\rangle\big) &= U_T\big(|0\rangle_T|t_{00}\rangle + |1\rangle_T|t_{01}\rangle\big) \\ &= |0\rangle_T|T_0\rangle, \end{aligned} \tag{38}$$

$$\begin{aligned} U_T U_S\big(|1\rangle_T|g\rangle\big) &= U_T\big(|0\rangle_T|t_{10}\rangle + |1\rangle_T|t_{11}\rangle\big) \\ &= |1\rangle_T|T_1\rangle, \end{aligned} \tag{39}$$

$$\begin{aligned} U_T U_S\big(|+\rangle_T|g\rangle\big) &= U_T\big(|0\rangle_T|t_{+0}\rangle + |1\rangle_T|t_{+1}\rangle\big) \\ &= \frac{1}{\sqrt{2}}U_T\big(|0\rangle_T|t_{00}\rangle + |1\rangle_T|t_{01}\rangle\big) + \frac{1}{\sqrt{2}}U_T\big(|0\rangle_T|t_{10}\rangle + |1\rangle_T|t_{11}\rangle\big) \\ &= \frac{1}{2}\big[|+\rangle_T\big(|T_0\rangle + |T_1\rangle\big) + |-\rangle_T\big(|T_0\rangle - |T_1\rangle\big)\big] \\ &= \frac{1}{2}|+\rangle_T\big(|T_0\rangle + |T_1\rangle\big), \end{aligned} \tag{40}$$

$$\begin{aligned} U_T U_S\big(|-\rangle_T|g\rangle\big) &= U_T\big(|0\rangle_T|t_{-0}\rangle + |1\rangle_T|t_{-1}\rangle\big) \\ &= \frac{1}{\sqrt{2}}U_T\big(|0\rangle_T|t_{00}\rangle + |1\rangle_T|t_{01}\rangle\big) - \frac{1}{\sqrt{2}}U_T\big(|0\rangle_T|t_{10}\rangle + |1\rangle_T|t_{11}\rangle\big) \\ &= \frac{1}{2}\big[|+\rangle_T\big(|T_0\rangle - |T_1\rangle\big) + |-\rangle_T\big(|T_0\rangle + |T_1\rangle\big)\big] \\ &= \frac{1}{2}|-\rangle_T\big(|T_0\rangle + |T_1\rangle\big), \end{aligned} \tag{41}$$

which can be obtained that $|T_0\rangle = |T_1\rangle = |T\rangle$. So,

$$U_T U_S\big(|0\rangle_T|g\rangle\big) = |0\rangle_T|T\rangle, \tag{42}$$

$$U_T U_S\big(|1\rangle_T|g\rangle\big) = |1\rangle_T|T\rangle, \tag{43}$$

$$U_T U_S\big(|+\rangle_T|g\rangle\big) = |+\rangle_T|T\rangle, \tag{44}$$

$$U_T U_S\big(|-\rangle_T|g\rangle\big) = |-\rangle_T|T\rangle, \tag{45}$$

$$\begin{aligned} U_T U_S\big(|0\rangle_A|g\rangle\big) &= U_T\big(|0\rangle_B|t_{00}\rangle + |1\rangle_B|t_{01}\rangle\big) \\ &= |0\rangle_B|T\rangle, \end{aligned} \tag{46}$$

$$\begin{aligned} U_T U_S\big(|1\rangle_A|g\rangle\big) &= U_T\big(|0\rangle_B|t_{10}\rangle + |1\rangle_B|t_{11}\rangle\big) \\ &= |1\rangle_B|T\rangle, \end{aligned} \tag{47}$$

$$\begin{aligned} U_T\big(|0\rangle_B|t\rangle\big) &= |0\rangle_B|t_{00}\rangle + |1\rangle_B|t_{01}\rangle \\ &= |0\rangle_B|T\rangle, \end{aligned} \tag{48}$$

$$\begin{aligned} U_T\big(|1\rangle_B|t\rangle\big) &= |0\rangle_B|t_{10}\rangle + |1\rangle_B|t_{11}\rangle \\ &= |1\rangle_B|T\rangle. \end{aligned} \tag{49}$$

The above equations show that Eve's ancillary particle is independent of CTRL, SIFT_A and SIFT_B photons, so if Eve does not want to be detected for his eavesdropping behavior, he will also be unable to obtain information.

4 Simulation of the presented protocols

To demonstrate the correctness of the outputs of the three protocols, we conducted simulation experiments using IBM's Qiskit without considering the eavesdropping inspection process [32].

4.1 Simulation of the SCSQS protocol

Assuming that the particles sent by TP to Alice are $|+\rangle$, $|+\rangle$, $|+\rangle$ and $|+\rangle$, represented by quantum registers q_0, q_1, q_2 and q_3, respectively. The particle states prepared by Alice themselves are $|0\rangle$, $|1\rangle$, $|0\rangle$ and $|1\rangle$, represented by registers q_4, q_5, q_6 and q_7, respectively.

According to the protocol steps, TP randomly performs σ_X and σ_Z measurements on the received particles. In the simulation phase, it is assumed that TP performs σ_X measurements on registers q_0, q_1, q_4 and q_5, and σ_Z measurements on q_2, q_3, q_6 and q_7. The relevant circuit diagram is shown in Fig. 1, and the corresponding measurement results are shown in Fig. 2.

4.2 Simulation of the RCSQS protocol

Assuming that the particles sent by TP to Alice are $|+\rangle$, $|-\rangle$, $|0\rangle$ and $|1\rangle$, represented by quantum registers q_0, q_1, q_2 and q_3, respectively. The particle states prepared by Alice themselves are $|1\rangle$, $|0\rangle$, $|1\rangle$ and $|0\rangle$, represented by registers q_4, q_5, q_6 and q_7, respectively. The particle states prepared by Bob themselves are $|0\rangle$, $|1\rangle$, $|0\rangle$ and $|0\rangle$, represented by registers q_8, q_9, q_{10} and q_{11}, respectively.

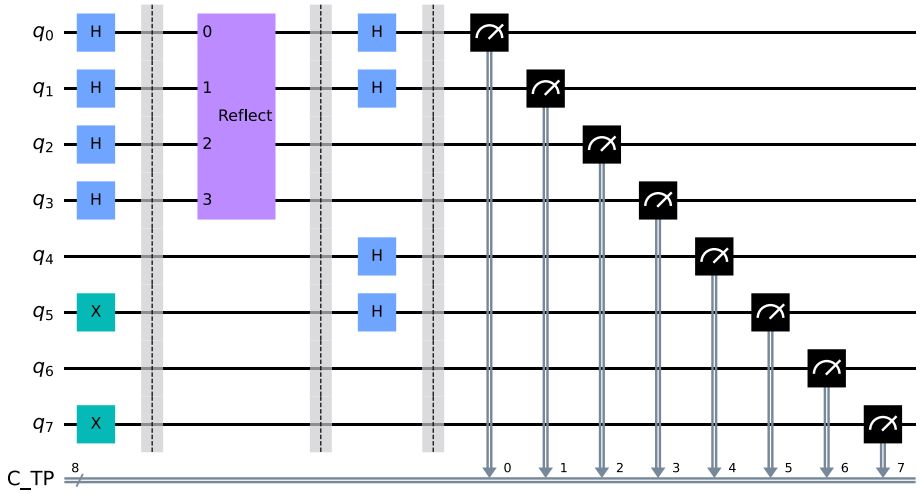
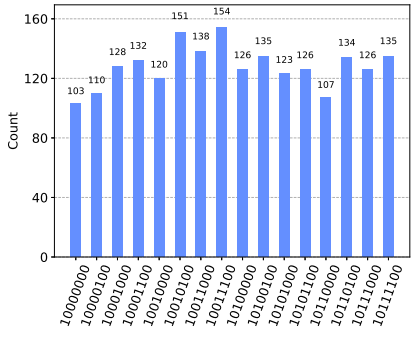


Figure 1 Circuit diagram for SCSQS

Figure 2 Measurement results of SCSQS



According to the protocol steps, TP performs σ_X and σ_Z measurements on the CTRL particles. In the simulation phase, it is show that TP performs σ_X measurements on registers q_0, q_1, and σ_Z measurements on q_2, q_3. The relevant circuit diagram is shown in Fig. 3, and the corresponding measurement results are shown in Fig. 4.

5 Protocol 3: multi-party SCSQS

In this section, based on SCSQS protocol, the MPSQS protocol will be proposed.

There are $n(n \geq 2)$ participants $(P_1, P_2, \ldots, P_n)$ and a semi-honest TP. The participants $P_j(2 \leq j \leq n)$ are classical participants who have a private N-bit string, eager to summation their private information. TP has full quantum capabilities, who aims to obtain the modulo 2 of the participants' bit strings. The participants select an SQKD protocol to pre-shared the length of N keys $K = (K^1, K^2, \ldots, K^N)$. The length of participants' private bit strings $(M_1, M_2, \ldots, M_n)$ is N, which are denoted as $M_1 = (m_1^1, m_1^2, \ldots, m_1^N)$, $M_2 = (m_2^1, m_2^2, \ldots, m_2^N), \ldots, M_n = (m_n^1, m_n^2, \ldots, m_n^N)$, where $m_j^i \in \{0, 1\}$, $i = 1, 2, \ldots, N$. On the premise of not disclosing their respective private bit strings, they hope to use TP to help

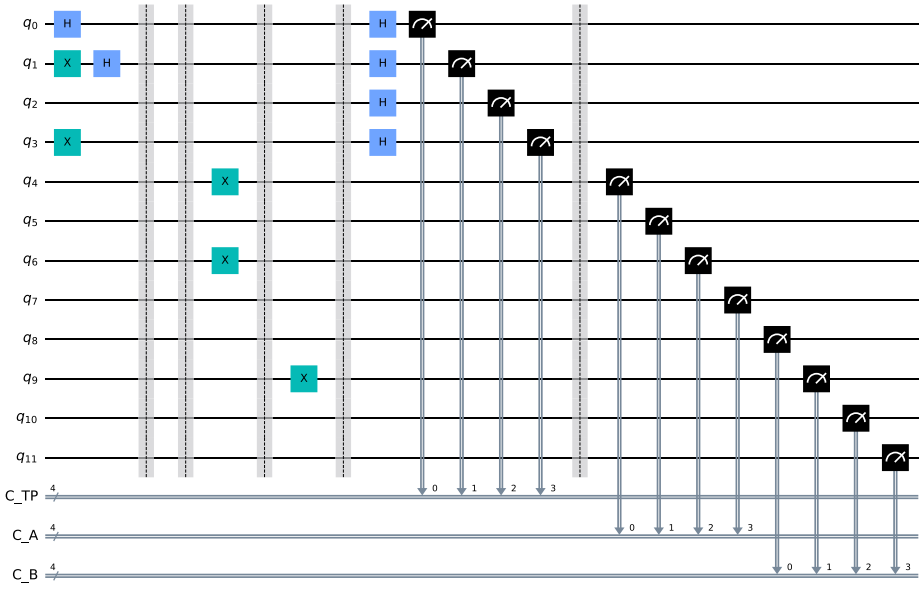
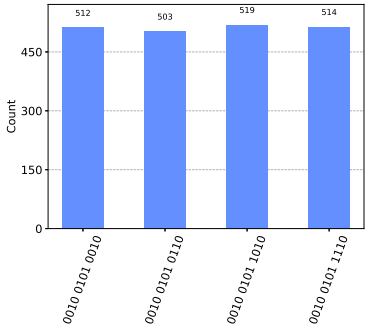


Figure 3 Circuit diagram for RCSQS

Figure 4 Measurement results of RCSQS



compute the summation:

$$\begin{aligned} M &= M_1 \oplus M_2 \oplus \cdots \oplus M_n \\ &= \left(m_1^1 \oplus m_2^1 \oplus \cdots \oplus m_n^1, m_1^2 \oplus m_2^2 \oplus \cdots \oplus m_n^2, m_1^N \oplus m_2^N \oplus \cdots \oplus m_n^N\right) \end{aligned} \tag{50}$$

where, $\oplus$ is the modulo 2 addition.

Step 1: TP generates $N = 8n$ n-qubit product states, each of which is

$$|+\rangle|+\rangle ... |+\rangle = \frac{(|0\rangle + |1\rangle)_1}{\sqrt{2}} \otimes \frac{(|0\rangle + |1\rangle)_2}{\sqrt{2}} \otimes \cdots \otimes \frac{(|0\rangle + |1\rangle)_n}{\sqrt{2}} \tag{51}$$

where $1, 2, \ldots, n$ denote the system of n participants. There are n sequences $Q_1 = \{q_1^1, q_1^2, \ldots, q_1^N\}$, $Q_2 = \{q_2^1, q_2^2, \ldots, q_2^N\}$, $\ldots$, $Q_n = \{q_n^1, q_n^2, \ldots, q_n^N\}$, where q_j^i represents the i-th ($i = 1, 2, \ldots, N$) particle for j-th participant. Then, TP transmits Q_j to each participant.

Step 2: Upon receiving particles from TP, P_j prepares a sequence $Z_j = \{z_a^1, z_a^2, \ldots, z_a^m\}$, where z_j^i is chosen from $\{|0\rangle, |1\rangle\}$ at random, $i = 1, 2, \ldots, m$. Subsequently, P_j combines Z_j

and Q_j to compose a new sequence S_j, and reorders the positions of particles in the S_j. P_j transmits S_j to TP, where the length of N_j is $8n + m$.

Step 3: When TP is receiving S_j from P_j, he randomly chooses either σ_Z basis ($\{|0\rangle, |1\rangle\}$) or σ_X basis ($\{|+\rangle, |-\rangle\}$) to measure each particle. Then, TP announces which basis he chose to measure for each particle.

Step 4: P_j publishs the positions of Q_j and Z_j in S_j. According to P_j's different operations, the following various cases will occur:

The cases which TP performed σ_X measurement on the particle are used for checking eavesdropping. An example is illustrated, if there are no eavesdroppers in quantum channel, TP obtains $|+\rangle_1 \otimes |+\rangle_2 \otimes \cdots \otimes |+\rangle_n$. Once other quantum states appear, it indicates the presence of eavesdroppers during the communication process.

The case which TP performs σ_Z measurement on the particle which is belongs Q_1, Q_2, …, Q_n will be discarded.

The cases which TP performed σ_Z measurement at least one of Alice and Bob has prepared the fresh particles are used for computing the private summation. TP obtains a bit string $r_1^1, r_1^2, \ldots, r_1^{3n}, r_2^1, r_2^2, \ldots, r_2^{3n}, \ldots, r_n^1, r_n^2, \ldots, r_n^{3n}$ which measured in σ_Z basis corresponding the positions $r_1^1 r_1^2 \ldots r_1^{3n}$, $r_2^1 r_2^2 \ldots r_2^{3n}$ and $r_n^1 r_n^2 \ldots r_n^{3n}$. The measurement result of P_1, P_2 and P_n's are denoted as r_1^i, r_2^i and r_n^i.

Step 5: TP chooses a part of bits in $r_1^1 r_1^2 \ldots r_1^{3n}$, $r_2^1 r_2^2 \ldots r_2^{3n}$ and $r_n^1 r_n^2 \ldots r_n^{3n}$ to be TEST bits, and declares the positions and value which he selected. Two participants announce the value of the TEST bits at the corresponding position. They calculate the error rate on TEST bits. Once the error rate is higher than the predefined threshold value, the protocol will be terminated.

Step 6: The participants and TP compute the summation of bit strings. P_1 holds $R_1 = \{r_1^1, r_1^2, \ldots, r_1^n\}$, P_2 holds $R_2 = \{r_2^1, r_2^2, \ldots, r_n^n\}$, …, P_n holds $R_n = \{r_n^1, r_n^2, \ldots, r_n^n\}$. P_1 computes $C_1^i = r_1^i \oplus m_1^i \oplus K^i$, P_2 computes $C_2^i = r_2^i \oplus m_2^i \oplus K^i$, …, P_n computes $C_n^i = r_n^i \oplus m_n^i \oplus K^i$ where $\oplus$ is the modulo 2 addition. Then, TP computes $C_1^i \oplus C_2^i \oplus \cdots \oplus C_n^i \oplus r_1^i \oplus r_2^i \oplus \cdots \oplus r_n^i = m_1^i \oplus m_2^i \oplus \cdots \oplus m_n^i$, the result is Alice and Bob i-th private summation.

6 Discussion and conclusion

We compare the proposed protocols with similar protocols in detail are shown in Table 2. Zhang et al. [28], Hu et al. [29] and our protocols based on single qubits which are easier to generate the qubits. Zhang et al. [28] and Ye et al. [30] implement communication between three participants, but Hu et al. [29] and our protocols communication with only two participants. Importantly, previous SQS protocols necessitated classical user measurements, while the proposed protocols eliminate this requirement, with TP only requiring single-particle measurements.

In conclusion, this paper introduces three secure semi-quantum summation protocols, all of which operate without classical measurement and are capable of computing the modulo 2 addition of participants' private bits. When designing these protocols, the following key aspects were considered: (1) Minimizing the classical participants' capabilities to only preparing qubits using Z-basis, while employing methods that don't require measurement capabilities. (2) Designing protocols based on different transmission modes, namely star and ring protocols. (3) Extending protocols applicable to two or three parties to support N-party scenarios. With these design principles in mind, SCSQS is a star protocol that

Table 2 Comparison of the protocols

Protocol	Quantum resource	Number of communicants	Classical participant measurement	TP's measurement	The dimension
[28]	Single qubit	2	Required	Single qubit and three-qubit entangled	2
[29]	Single qubit	2	Required	Single qubit and two-qubit entangled	2
[30]	Two-qubit entangled	2	Required	Single qubit and two-qubit entangled	2
[31]	D-dimensional single qubit	D	Required	D-dimensional single qubit	D
SCSQS	Single qubit	2	Not required	Single qubit	2
RCSQS	Single qubit	2	Not required	Single qubit	2
MPSQS	Single qubit	N	Not required	Single qubit	2

eliminates the need for measurement, RCSQS is a ring protocol also devoid of measurement requirements, and MPSQS extends from SCSQS to N-party scenarios. These proposed protocols have been demonstrated to effectively prevent typical attack behaviors such as intercept-resend attacks, measure-resend attacks, entangle-measure attacks, TP attacks, and participant attacks. Moreover, it's worth noting that the designed protocols come with certain limitations, such as the requirement for participants to pre-share keys. These limitations provide areas for future research and improvement in semi-quantum communication protocols.

Abbreviations
QKD, Quantum Key Distribution; SMC, Secure Multi-party Computation; QSMC, Quantum Secure Multi-party Computation; QSMS, Quantum secure Multi-party Summation; SQS, Semi-Quantum Summation; TP, Third-Party; SCSQS, Star and Concise Semi-Quantum Summation; RCSQS, Ring and Concise Semi-Quantum Summation; MPSQS, Multi-Party Semi-Quantum Summation.

Author contributions
A. wrote the main manuscript text B. Comparative analysis of relevant protocols C. Draw a protocol simulation diagram D. Verified the correctness of the protocol E. Secondary editing of the manuscript

Funding
Project supported by the Natural Science Basic Research Program of Shaanxi (Program No. 2024JC-YBQN-0688) and the China Scholarship Council.

Data Availability
No datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare no competing interests.

Author details
[1] College of Information and Control Engineering, Xi'an University of Architecture and Technology, Xi'an, Shaanxi, China.
[2] School of Cyberspace Security, Beijing University of Post and Telecommunications, Beijing, China.

Received: 3 April 2024 Accepted: 8 May 2024 Published online: 22 May 2024

References
1. Cabello A. Quantum key distribution in the Holevo limit. Phys Rev Lett. 2000;85(26):5635.
2. Grasselli F. Quantum cryptography. Quantum science and technology. Cham: Springer; 2021.

3. Aumasson JP. The impact of quantum computing on cryptography. Comput. Fraud Secur.. 2017;6:8–11.
4. Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inf Theory. 1976;22(6):644–54.
5. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE international conference on computers, systems and signal processing. Bangalore. 1984. p. 175–9.
6. Yin J, Li YH, Liao SK, Yang M, Cao Y, Zhang L, Ren JG, Cai WQ, Liu WY, Li SL, Shu R, Huang YM, Deng L, Li L, Zhang Q, Liu NL, Chen YA, Lu CY, Wang XB, Xu FH, Wang JY, Peng CZ, Ekert A, Pan JW. Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature. 2020;582(7813):501–5.
7. Renner R, Wolf R. Quantum advantage in cryptography. AIAA J. 2023;61(5):1895–910.
8. Sonko S, Ibekwe KI, Ilojianya VI, Etukudoh EA, Fabuyide A. Quantum cryptography and US digital security: a comprehensive review: investigating the potential of quantum technologies in creating unbreakable encryption and their future in national security. Comput. Sci. IT Res. J.. 2024;5(2):390–414.
9. Sutradhar K. Secure multiparty quantum aggregating protocol. Quantum Inf Comput. 2023;23(3&4):245–56.
10. Sun Z, Song L, Huang Q, Yin L, Long G, Lu J, Hanzo L. Toward practical quantum secure direct communication: a quantum-memory-free protocol and code design. IEEE Trans Commun. 2020;68(9):5778–92.
11. Grassl M. Entanglement-assisted quantum communication beating the quantum Singleton bound. Phys Rev A. 2021;103(2):L020601.
12. Yang Z, Zolanvari M, Jain R. A survey of important issues in quantum computing and communications. IEEE Commun Surv Tutor 2023.
13. Goldreich O. Secure multi-party computation. Manuscript Preliminary version. 1998;78(110):1–108.
14. Knott B, Venkataraman S, Hannun A, Sengupta S, Ibrahim M, vander Maaten L. Crypten secure multi-party computation meets machine learning. Adv Neural Inf Process Syst. 2021;34:4961–73.
15. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th annual symposium on foundations of computer science. Piscataway: IEEE; 1994. p. 124–34.
16. Grasselli F. Quantum cryptography. Quantum science and technology. Cham: Springer; 2021.
17. Lo HK. Insecurity of quantum secure computations. Phys Rev A. 1997;56(2):1154.
18. Bartusek J. Secure quantum computation with classical communication. In: Proceedings of the theory of cryptography conference. Cham: Springer; 2021. p. 1–30.
19. Shi RH, Zhang S. Quantum solution to a class of two-party private summation problems. Quantum Inf Process. 2017;16:1–9.
20. Yang HY, Ye TY. Secure multi-party quantum summation based on quantum Fourier transform. Quantum Inf Process. 2018;17(6):129.
21. Ji Z, Zhang H, Wang H, Wu F, Jia J, Wu W. Quantum protocols for secure multi-party summation. Quantum Inf Process. 2019;18:1–19.
22. Sutradhar K, Om H. A generalized quantum protocol for secure multiparty summation. IEEE Trans Circuits Syst II, Express Briefs. 2020;67(12):2978–82.
23. Lu Y, Ding G. Quantum secure multi-party summation with graph state. Entropy. 2024;26(1):80.
24. Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob. Phys Rev Lett. 2007;99(14):140501.
25. Zou X, Qiu D, Li L, Wu L, Li L. Semi-quantum key distribution using less than four quantum states. Phys Rev A. 2009;79(5):1744.
26. Iqbal H, Krawec WO. Semi-quantum cryptography. Quantum Inf Process. 2020;19(3):1–52.
27. Tian Y, Li J, Chen XB, Ye CQ, Li HJ. An efficient semi-quantum secret sharing protocol of specific bits. Quantum Inf Process. 2021;20(6):1–11.
28. Zhang C, Huang Q, Long Y, Sun Z. Secure three-party semi-quantum summation using single photons. Int J Theor Phys. 2021;60(9):3478–87.
29. Hu JL, Ye TY. Three-party secure semiquantum summation without entanglement among quantum user and classical users. Int J Theor Phys. 2022;61(6):170.
30. Ye TY, Xu TJ, Geng MJ, Chen Y. Two-party secure semiquantum summation against the collective-dephasing noise. Quantum Inf Process. 2022;21(3):118.
31. Lian JY, Ye TY. Hybrid protocols for multi-party semiquantum private comparison, multiplication and summation without a pre-shared key based on d-dimensional single-particle states. EPJ Quantum Technol. 2024;11(1):17.
32. Ye CQ, Li J, Chen XB, Hou Y. A feasible semi-quantum private comparison based on entanglement swapping of Bell states. Phys A, Stat Mech Appl. 2023;625:129023.

Publisher's Note