scientific reports

Check for updates

OPEN

Multiparty private summation protocol based on two-state quantum-mechanical system

Jason Lin[1], Shao-Lun Huang[1], Chun-Wei Yang[2] & Chia-Wei Tsai[3]✉

With the rapid advancement of information technology, data sharing has become increasingly accessible, leading to a heightened need for robust personal data protection. One important application in privacy-preserving computing is the aggregation of information when collaboratively establishing AI models through public distributed networks. To counter the threat posed by quantum computing to encrypted data, various quantum private summation (QPS) protocols have been proposed thus far. However, some of these existing protocols operate solely under modulo 2, while other approaches for modulo *d* often rely on impractically high-dimensional qudits. Therefore, this study proposes an innovative multiparty QPS method that balances participant data sharing and privacy without requiring high-dimensional photons. The proposed QPS protocol enables participants to contribute aggregated information to third parties without disclosing individual data. A security analysis further demonstrates that the proposed QPS effectively counters common eavesdropping attacks, ensuring reliable protection of personal data.

Keywords Secure multi-party computation, Quantum private summation, Modular arithmetic, Single photons

The rapid development of quantum computing has increased the challenges faced by conventional encryption algorithms. Shor's algorithm[1] demonstrates that the widely used RSA encryption algorithm[2] can potentially be cracked in polynomial time using quantum computers. Consequently, quantum cryptography has emerged as a burgeoning technology to address these challenges. Based on the principles of quantum mechanics and the properties of quantum bits (qubits), quantum cryptography aims to achieve more secure, efficient, and revolutionary methods for information transmission. In classical computing, especially with AI models across networks, data are often exposed to legitimate participants during transmission and processing, which can lead to significant privacy risks. For instance, when aiming to obtain the total sum of all participants' information while protecting their individual secrets from being disclosed, a quantum private summation (QPS) protocol is required to achieve this goal. The QPS protocol typically involves a third party (TP) and at least three agents. TP needs to calculate the sum of all participants' secrets without revealing their actual contents and then publicly disclose the total sum. Throughout the process, the QPS protocol ensures security against eavesdroppers. A more practical example is as follows: Suppose we want to obtain the total score assigned by judges to a group of performers but also want to protect the individual scores given by each judge from being disclosed. In such a scenario, the organizers can implement a QPS protocol, ensuring that the total score is calculated without revealing the individual judges' scores. This approach effectively protects the judges' privacy while ensuring the accuracy of the total score. Moreover, similar quantum protocols have been successfully applied to other privacy-preserving mathematical computations, such as matrix multiplication[3], the greatest common divisor[4], and the least common multiple[5].

In the past two decades, some QPS research[6–19] based on either quantum logic gates or entanglement are proposed to achieve the summation of modulo 2. In 2010, Chen et al.[6] proposed a semi-honest TP to utilize Greenberger-Horne-Zeilinger (GHZ) states for collecting secret bit strings from both communicating parties. The summation of the two secret bit strings is obtained through Bell measurements. Subsequently, in 2014, Zhang et al.[7] started to employ various techniques in quantum secure computation, including Y gate and H gate operations, to achieve the goal of QPS. Over the years, their research has evolved, incorporating different

[1]Department of Computer Science and Engineering, National Chung Hsing University, No. 145, Xingda Rd., South District, Taichung 402202, Taiwan. [2]Master Program for Digital Health Innovation, College of Humanities and Sciences, China Medical University, No. 100, Sec. 1, Jingmao Rd., Beitun Dist., Taichung 406040, Taiwan. [3]Department of Computer Science and Information Engineering, National Taichung University of Science and Technology, No.129, Sec. 3, Sanmin Rd., North Dist., Taichung 404336, Taiwan. ✉email: cwtsai@nutc.edu.tw

methodologies such as BPB states in 2015[8], multi-party protocols in 2017[9], and introducing a three-party semi-QPS protocol using GHZ states in 2021[10]. This showcases a continuous exploration of innovative techniques for secure quantum computation. Liu et al.[11] utilize Pauli gates for encoding and H gates for information extraction. In the security analysis, it is demonstrated that TP can securely obtain the summation of the participants by conducting eavesdropping checks using decoy photons. Shi and Zhang[12] proposed a groundbreaking special two-party QPS protocol, leveraging quantum principles for secure collaborative computation. The applications of their protocol include solving the Hamming distance problem, addressing private set intersection cardinality and private set union cardinality, and facilitating secure trade negotiations. In 2019, Gu et al.[13] proposed an improvement to Zhang et al.'s protocol[9] to address a security vulnerability. They introduced pre-shared keys between participants and a trusted party to enhance security against intercept-and-resend attacks. In 2022, Ye and Xu[14] introduced a three-party QPS protocol that operates without the need for a TP, relying on single-particle states. Hu and Ye[15] proposed a secure three-party semi-QPS protocol, allowing for eavesdropping checks, evaluation of participant honesty, and summation calculations without the need for complex entangled states. Ye et al.[16] proposed a two-party QPS protocol aimed at facilitating summation between communicating parties over a quantum channel affected by noise, with the involvement of a TP. In 2023, Wu and Xie[17] proposed a multi-party QPS protocol using single photons. In this protocol, they apply Y and H gates to the photon sequence using keys generated through quantum key distribution (QKD) protocols and their respective secrets. This process ensures that the photons in the Z and X bases of the photon sequence are randomized and equally distributed, effectively preventing eavesdropping. More recently, in 2024, Tian et al.[18] proposed a set of semi-quantum summation protocols based on single photons, enabling resource-limited participants to securely compute sums without requiring measurement capabilities. Meanwhile, Cheng et al.[19] introduced a multi-party quantum summation protocol utilizing W-class states, enhancing qubit efficiency and security against internal and external attacks.

Since summation modulo 2 is equivalent to a bitwise exclusive-OR operation between secrets, some research suggests that this summation may lack practical significance and has limited applications in scenarios requiring the accumulation of numeric sums. Consequently, several studies have proposed a series of QPS protocols[20–26] that utilize d-level photons, known as quantum digits (qudits), along with the quantum Fourier transform (QFT)[27] to achieve summation modulo d. Other protocols[28–30] extend these capabilities to perform both summation and multiplication modulo d. Nevertheless, while qudits offer enhanced computational capacity compared to qubits, their practical application remains limited due to the complexities involved in preparation and control. Achieving stable, high-dimensional states in qudits demands advanced precision and technical rigor, with additional challenges from environmental interference and noise.

To address these issues, this study proposes replacing high-level qudits with low-level qubits and using straightforward modular arithmetic instead of complex QFT to achieve summation modulo d in QPS. The quantum resources required for computation involve only a two-state quantum mechanical system, which typically consists of two orthogonal states, such as $|0\rangle$ and $|1\rangle$. Through security analysis, the proposed QPS protocol demonstrates resilience against both internal and external eavesdropping attacks, thereby safeguarding the confidentiality of participants' numerical values.

The remainder of this paper is organized as follows. "Proposed multiparty QPS protocol using qubits" section describes the formal process of the proposed QPS protocol. "Security analysis" section presents a security analysis of common attack methods. "Efficiency comparison" section provides an efficiency comparison with several QPS protocols, and "Conclusion" section provides a brief conclusion.

Proposed multiparty QPS protocol using qubits

This section is divided into two subsections: "Process of the proposed QPS protocol" subsection explains how the proposed QPS protocol's process allows TP to obtain the sum of all participants' secret values without revealing any of the participants' individual values. "Example of a four-party QPS protocol" subsection provides an example of a four-party QPS protocol.

Process of the proposed QPS protocol

We assume that the proposed QPS protocol includes one semi-honest TP[31] and N agents: A_1, A_2, …, and A_N. The semi-honest TP is expected to perform any attacks on the protocol except for collusion with participants. All agents A_1, A_2, …, and A_N each possesses a secret numerical value x_1, x_2, …, and x_N, respectively. Suppose that TP is aware of the upper bound of the sum of all agents' secret values, denoted by U, where $\sum_{i=1}^{N} x_i < U$. However, TP does not know the individual secret value of each agent. We represent the modulus U in the quantum channel using k qubits in binary system, where $k = \lceil log_2 U \rceil$. An overview of the proposed QPS protocol is shown in Fig. 1, and the step-by-step process is depicted as follows.

Step 1: TP and each agent individually run a QKD protocol such as BB84[32] or E91[33]. Upon completion, TP and each agent obtain a pre-shared key K_1, K_2, …, and K_N, respectively, where K_i is the pre-shared key between TP and A_i.

Step 2: Agent A_1 selects a random number $S_0 < U$ known only to itself.

Step 3: For i from 1 to N, with A_{N+1} considered as TP: Agent A_i represents the value of $(S_{i-1} + K_i + x_i) \mod U$ in binary using k single photons in Z basis (i.e., $|0\rangle$ or $|1\rangle$), denoted as S_i. The agent then inserts k decoy photons in X basis (i.e., $|+\rangle$ or $|-\rangle$) at arbitrary positions, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Finally, A_i sends this sequence of photons to agent A_{i+1}.

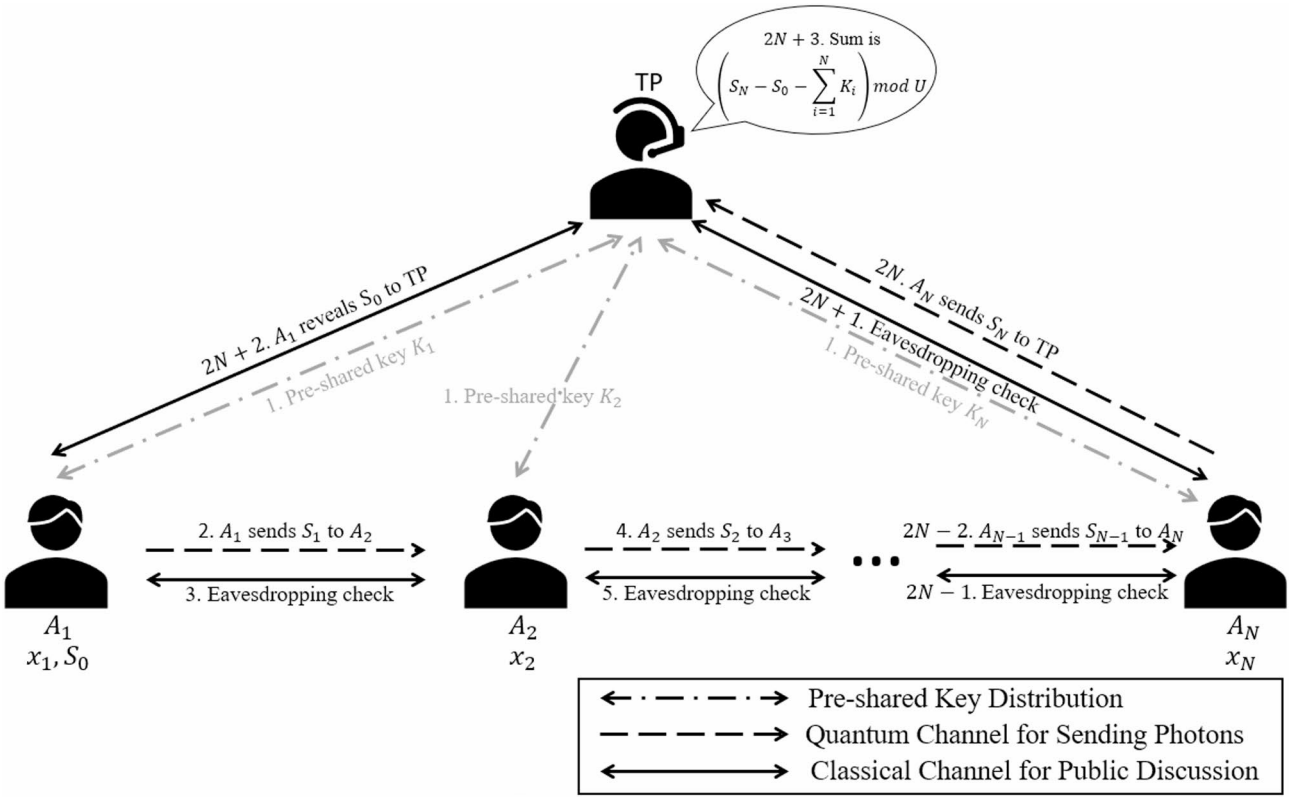

Fig. 1. The process of TP obtains the summation with all agents.

Step 4: After A_{i+1} receives the photons, it engages in a public discussion with A_i to verify if the states of the k decoy photons match those sent by A_i. If the states match, A_{i+1} measures the remaining photons in the Z basis to obtain S_i. If they do not match, the protocol is terminated and restarted from Step 2.

Step 5: A_1 reveals the value of S_0 to TP. TP calculates the result $R = (S_N - S_0 - \sum_{i=1}^{N} K_i) \mathrm{mod} U$, which represents the summation of the secret values x_1 to x_N of agents A_1 to A_N in this protocol.

In the proposed QPS protocol, TP and each agent initially establish a pre-shared key to protect their secrets. The value each agent obtains is the sum of all previous agent' secrets and keys. Since each agent only has their own key and there are numerous possible combinations of additions, they cannot determine the secrets of the other agent. This protocol utilizes the properties of modular arithmetic. Even if an overflow occurs during the process due to addition, the value of TP after subtracting all the keys will revert to the pre-overflow value. Therefore, in a QPS protocol with a known upper bound, there is no need to worry about overflow issues. As for the first agent A_1 who transmits the photon sequence that include the information of $S_1 = S_0 + x_1 + K_1$, the value does not include the accumulated secret sum from previous agents, hence the random number S_0 is used to protect x_1. Without the protection of S_0, TP can deduce A_1's secret value x_1 from S_1 and K_1. Conversely, with the addition of S_0, even if TP intercepts the photon and obtains S_1, it is still unable to determine x_1 without knowing the value of S_0. Finally, with the help of decoy photons, if the photons are intercepted and measured during transmission, the protocol will detect the action and immediately terminate the following process, ensuring its security.

Example of a four-party QPS protocol

We now provide a four-party example of the proposed QPS protocol, which includes one semi-honest TP and three agents: A_1, A_2, and A_3. Suppose the three agents A_1, A_2, and A_3 possess with secret values $x_1 = 1$, $x_2 = 4$, and $x_3 = 9$ respectively. TP knows that the upper bound of the sum of the three agents is 16, which means that the modulus of this protocol is 16, which can be represented in binary using 4 qubits in the quantum channel. The following steps are illustrated in Fig. 2. Note that the step numbers here do not correspond to those in "Process of the proposed QPS protocol" section or Fig. 2. However, the process is consistent with the flow in "Process of the proposed QPS protocol" section and Fig. 2.

Step 1: TP and each of the three agents individually run any QKD protocol to generate a pre-shared key. We assume that the three keys are $K_1 = 2$, $K_2 = 7$, and $K_3 = 6$.

Step 2: Let us assume that agent A_1 randomly selects a number $S_0 = 3$ and keep this number to itself.

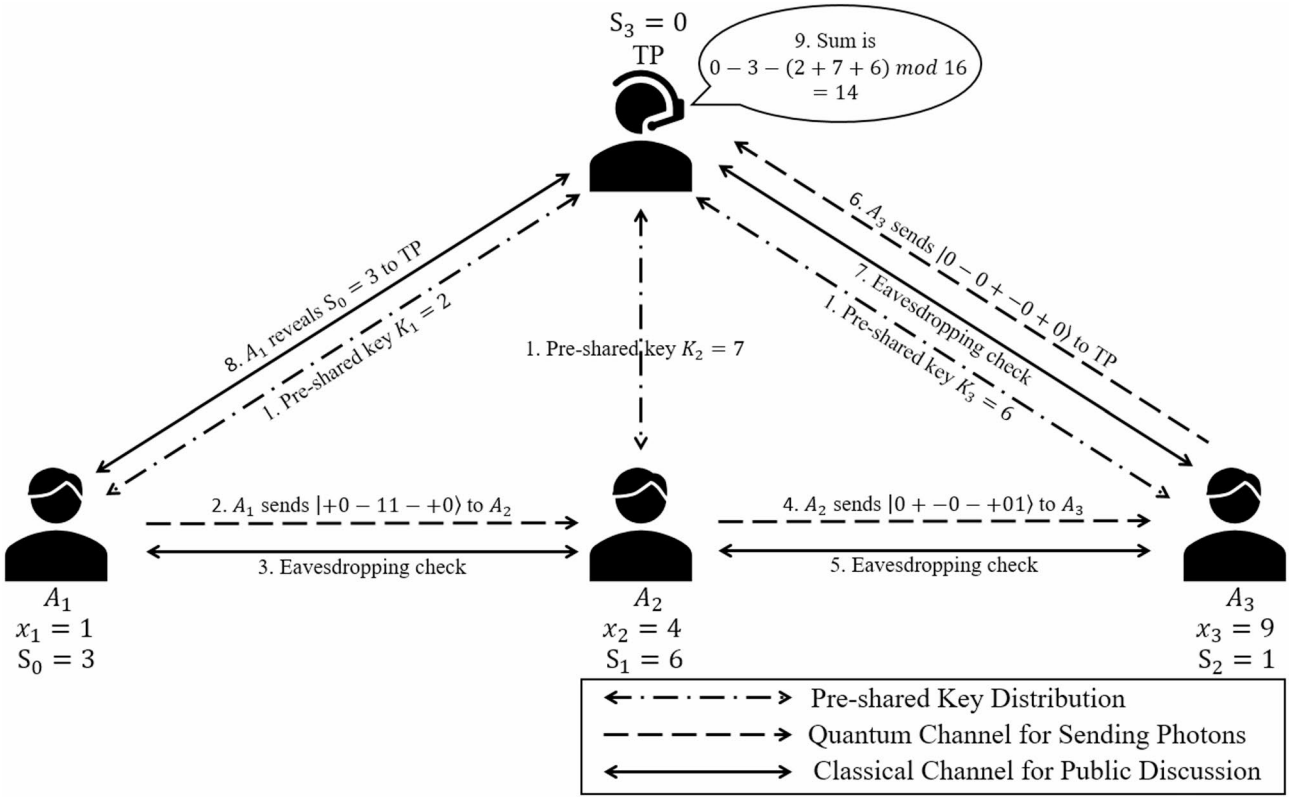

Fig. 2. The example of TP obtains the summation with all agents.

Step 3.1: A_1 calculates the result of $S_0 + K_1 + x_1$ to obtain $S_1 = (3 + 2 + 1) \bmod 16 = 6$ and converts it into binary form 0110_2, which is then encoded on qubits as $|0110\rangle$. A_1 inserts four decoy photons in X basis into this sequence of qubits. The resulting sequence of photons is then transmitted to agent A_2.

Step 3.2: After A_2 receives the photons, it engages in a public discussion with A_1 to verify whether the states of the four decoy photons match those sent by A_1. If the states match, A_2 measures the remaining photons on a Z basis to obtain S_1. Otherwise, the protocol is terminated and restarted from Step 2.

Step 4.1: A_2 calculates the result of $S_1 + K_2 + x_2$ to obtain $S_2 = (6 + 7 + 4) \bmod 16 = 1$ and converts it into binary form 0001_2, which is represented in qubits as $|0001\rangle$. Subsequently, four decoy photons are generated in X basis and inserted into the sequence before being transmitted to agent A_3.

Step 4.2: Upon receiving the photons, A_3 initiates a public discussion with A_2 to confirm the conformity of the states of the four decoy photons to those transmitted by A_2. If the states align, A_3 proceeds to measure the remaining photons on the Z basis to derive S_2. In case of a discrepancy, the protocol is terminated and restarted from Step 2.

Step 5.1: A_3 calculates the result of $S_2 + K_3 + x_3$ to yield $S_3 = (1 + 6 + 9) \mod 16 = 0$ and convert it into binary form 0000_2, which is represented as $|0000\rangle$. A_3 inserts four decoy photons in X basis into the sequence and transmitted back to TP.

Step 5.2: Upon receiving the photons, TP initiates a public discussion with A_3 to validate the states of the four decoy photons against those originally dispatched by A_3. If the states match, TP proceeds to measure the remaining photons on a Z basis to ascertain S_3. Otherwise, the protocol terminated and restarted from Step 2.

Step 6: A_1 discloses to TP that the random number $S_0 = 3$. TP then calculates and discloses the summation of agents' secret values as $[S_3 - S_0 - (K_1 + K_2 + K_3)] = [0 - 3 - (2 + 7 + 6)] \bmod 16 = 14$(i.e., $x_1 = 1$, $x_2 = 4$, and $x_3 = 9$) for the three agents in this protocol.

Let us summarize the above example. Even though A_2 and A_3 know that $S_1 = 6$ and $S_2 = 1$, respectively, neither of them can accurately determine the other participants' secret values because they do not know the values of the pre-shared keys between those participants and TP. On the other hand, despite TP having those keys, it still cannot determine the value of x_1 from S_1 because the value of S_0 is unknown. Finally, TP measures the qubits of S_3 and obtain its decimal value as $S_3 = 0$. It then subtracts S_0, which was announced by A_1, and the three keys to get a result $R = -18$. Taking the value of R modulo 16 gives 14, which is the sum of the three participants.

Security analysis

In "Measure-and-resend attack" to "Third-party attacks" subsections, we discuss how this protocol defends against the measure-and-resend attack, the entangle-and-measure attack, Trojan horse attacks, the collusion attack, and TP's attack, respectively.

Measure-and-resend attack

In the realm of quantum communication, measure-and-resend[34,35] attacks pose a significant threat. In these attacks, the eavesdropper aims to capture and measure all photons sent by the original sender to extract crucial information, as shown in Fig. 3. The quantum non-cloneable theorem[36] prevents the creation of identical copies, compelling the eavesdropper to use destructive measurements on the original photons to gain insights into the sender's data. The uncertainty principle[37] in quantum mechanics adds complexity, making it challenging for the eavesdropper to precisely determine the sender's encoding basis. Randomly selecting bases introduces a $\frac{3}{4}$ chance of obtaining correct information and a $\frac{1}{4}$ chance of measuring erroneous data. Transitioning to the 'resend' phase, the eavesdropper transmits photons to the receiver based on their measurements. Quantum communication protocol transparency facilitates public discussions, enabling thorough eavesdropping checks. Discrepancies in measurement results using the same basis indicate the presence of an eavesdropper, as their chosen basis differs from that of the original sender.

In summary, using decoy photons[38,39] for eavesdropping checks is an effective security mechanism. Each decoy photon has a $\frac{1}{4}$ probability of successfully detecting the eavesdropper, leading to a detection probability of $1-(\frac{3}{4})^k$ as the number of decoy photons k increases. That is, with a sufficient number of decoy photons, the probability of successful detection gradually approaches 1. This ensures a high detection success rate, making it difficult for an eavesdropper to evade detection, as shown in Fig. 4. In quantum security protocols, to maximize detection effectiveness, a common strategy is to allocate half of the photon string to decoy photons. This aims to increase the chances of detecting the eavesdropper while simultaneously reducing the likelihood of their successful eavesdropping attempts. Such distribution strategies not only enhance security but also make eavesdropping activities highly risky, ensuring the confidentiality of communication. Overall, the introduction of decoy photons plays a crucial role in quantum communication protocols, improving the reliability of eavesdropping checks and ensuring communication security. The use of this method is an effective and flexible means to ensure the credibility and security of quantum communication when transmitting sensitive information.

Entangle-and-measure attacks

In entangle-and-measure attack[40–42], eavesdroppers employ CX gates for their intrusion, as shown in Fig. 5. Assuming that the photons in the quantum channel are in the Z basis, the eavesdropper designates the transmitted photons in the channel as the control qubit, while preparing a Z basis photon as the target qubit. If the photons in the channel are $|0\rangle$, the eavesdropper's photon remains unchanged; conversely, if the photons in the channel are $|1\rangle$, the eavesdropper's photon undergoes a flip. Since the control qubit remains unaffected, neither communicating party can detect the presence of the eavesdropper.

However, in the proposed QPS protocol, all decoy photons used in each transmission are in X basis. If the eavesdropper applies the $CNOT$ gate to launch the attack, the two photons become entangled, resulting in an entangled state of either $\frac{1}{\sqrt{2}}(|0\ 0\rangle \pm |1\ 1\rangle)$ or $\frac{1}{\sqrt{2}}(|+\ +\rangle \pm |-\ -\rangle)$. This introduces a $\frac{1}{2}$ probability that the measurement of decoy photons by the receiving party differs from the state transmitted by the sender. With half of the channel consisting of decoy photons and each decoy photon having a $\frac{1}{2}$ chance of inducing a state change,

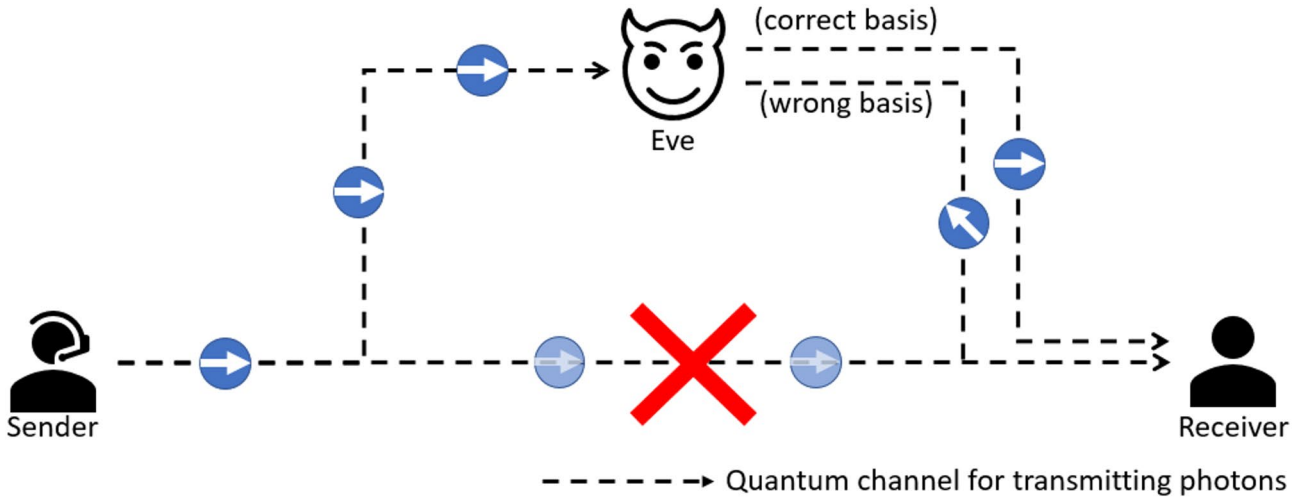

Fig. 3. Measure-and-resend attack scenario.

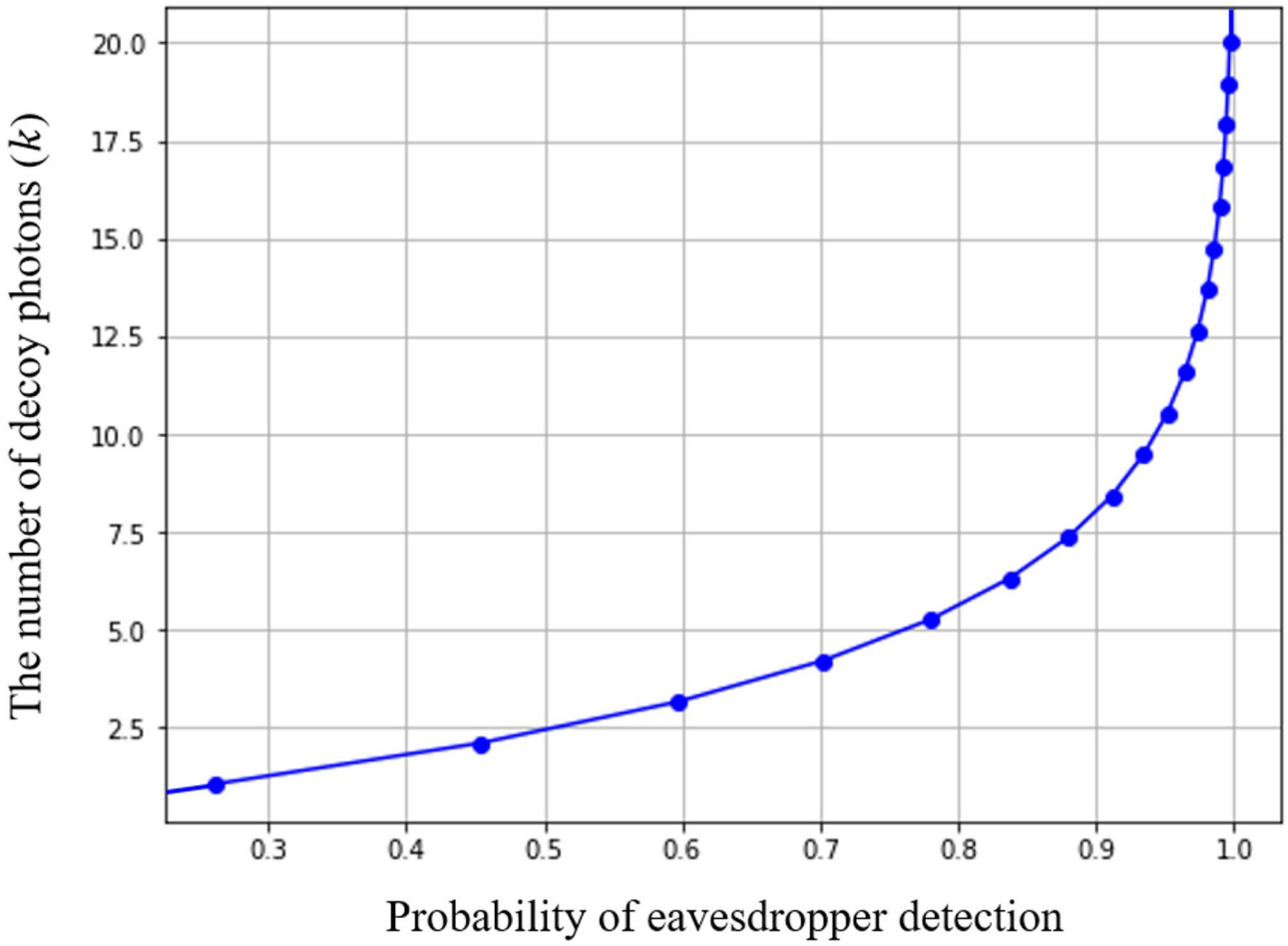

Fig. 4. Trend of the detection rate of an eavesdropper as the number of decoy photons increases.

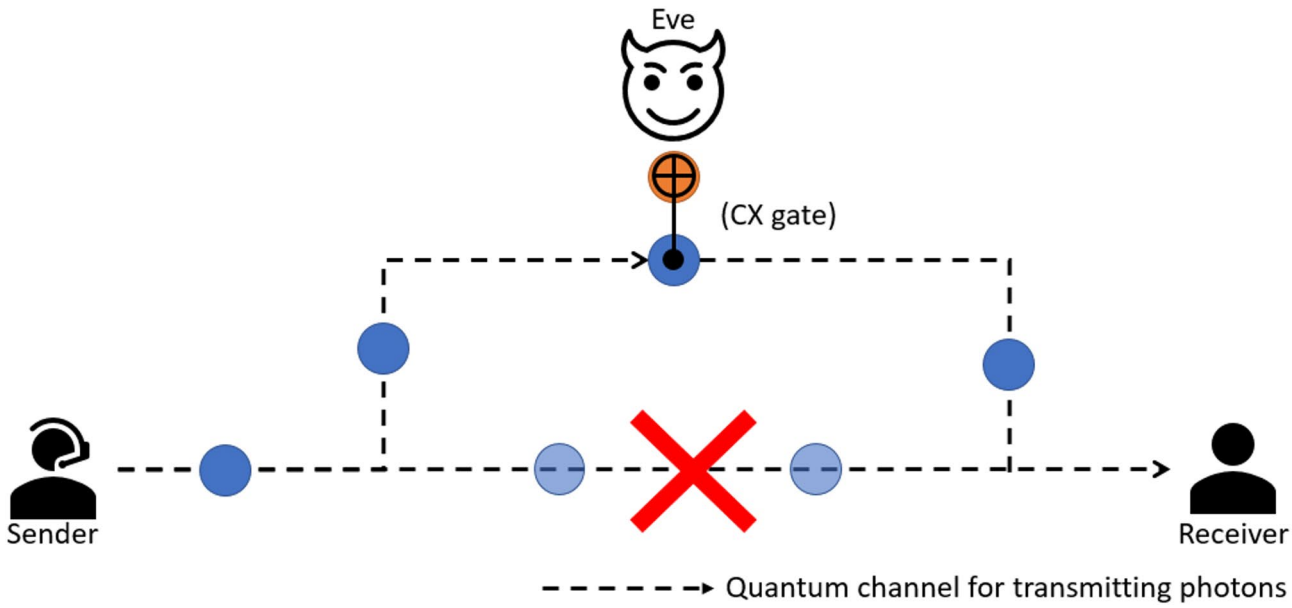

Fig. 5. Entangle-and-measure attack scenario.

the probability of detecting the eavesdropper when there are k decoy photons are $1-(\frac{3}{4})^k$. As k increases, the probability approaches to one. Therefore, entangle-and-measure attack is ineffective in this protocol.

Trojan Horse attacks

Trojan horse attacks come in two forms[43–45]. The first form is the delayed photon Trojan horse attack. In this scenario, eavesdroppers attach several delayed photons to each photon in the original sequence. Since the communicating parties measure photons only within specific time windows, these delayed photons remain undetected. When the receiver encodes the photon sequence, the delayed photons are also affected. After the receiver sends out the encoded sequence, the eavesdropper retrieves the delayed photons to get the encoding operations performed by the receiver. Common countermeasures include using optical delays to separate adjacent photons for observation and employing a photon number splitter to detect multiple photons within the same time window, indicating the presence of delayed photons launched by an attacker. The second type of attack is known as the invisible photon Trojan horse attack. In this scenario, the attacker injects an undetectable photon into each qubit transmitted to the participant. Since this photon is invisible to the participant's detector, the participant unwittingly performs a unitary operation on the compromised qubit. This method allows the attacker to gain insights into the participant's operations, akin to the delayed photon attack. To counteract this, common defenses include implementing filters that block photons with wavelengths outside the detection range of the single-photon detector.

Fortunately, our QPS protocol is immune to these attacks. Each participant in the process only measures photons without performing any operations, and there is no scenario where the same sequence of photons enters and exits the quantum channel more than once. Therefore, both forms of Trojan horse attacks are not applicable to the proposed QPS in this study.

Collusion attacks

In general, when considering private summation, we do not evaluate collusion attacks involving $n-1$ agents. This is because, in addition to the nature of summation itself, if the values of $n-1$ terms are known, the remaining value can naturally be deduced. For example, given the summation equation $x_1+x_2+\cdots+x_n=s$, if the result s is known and the values of $n-1$ terms are given, the value of the last term x_i can be inevitably determined.

However, certain collusion attacks[46–48] exist in both ring-type and relay-type multiparty scenarios, where A_{i-1} sends photons to A_i, and A_{i+1} receives photons from A_i. In such cases, A_{i-1} and A_{i+1} may collaborate to obtain A_i's secret value, as shown in Fig. 6. When A_{i+1} measures the values of the photons sent by A_i, A_{i-1} reveals to A_{i+1} the numbers that A_{i-1} sent to A_i. By subtracting the two numbers, they can deduce the added numbers by A_i. Fortunately, in the proposed QPS protocol, the added numbers include K_i and x_i. Since the two agents A_{i-1} and A_{i+1} do not know the exact value of K_i, they cannot determine the value of x_i. Therefore, the utilization of such pre-shared keys between TP and each agent can safeguard the secret of their data. As a result, the proposed QPS is immune to the collusion attacks.

Third-party attacks

In our proposed QPS protocol, the third-party TP is assumed to be semi-honest, meaning it cannot collude with any agent to learn an agent's secret value. Although TP can perform attacks other than collusion, the random number S_0 in Step 2 of "Proposed multiparty QPS protocol using qubits" section ensures the secrecy of the first agent A_1's number x_1 from TP. Since the only information transmitted by A_1 is $S_1=S_0+x_1+K_1$, TP cannot infer x_1 without knowing the value of S_0. Furthermore, other agents compute the summation iteratively using the recurrence relation $S_i=S_{i-1}+x_i+K_i$, making it difficult for TP to deduce any individual value x_i from the accumulated sum S_i for $i\geq 2$. As a result, the proposed QPS protocol remains secure against TP's attacks.

Efficiency comparison

In this section, we compare our proposed QPS protocol with some representative existing research[6,7,9,17,20,21,23]. The comparison metrics include the quantum resources used in the protocols, the quantum operations performed on primary photons, the requirement for quantum devices to resist Trojan horse attacks, the transmission mode's load on each participant, the arithmetic calculations that the protocols can achieve, and the number of required photons, which are summarized in Table 1.

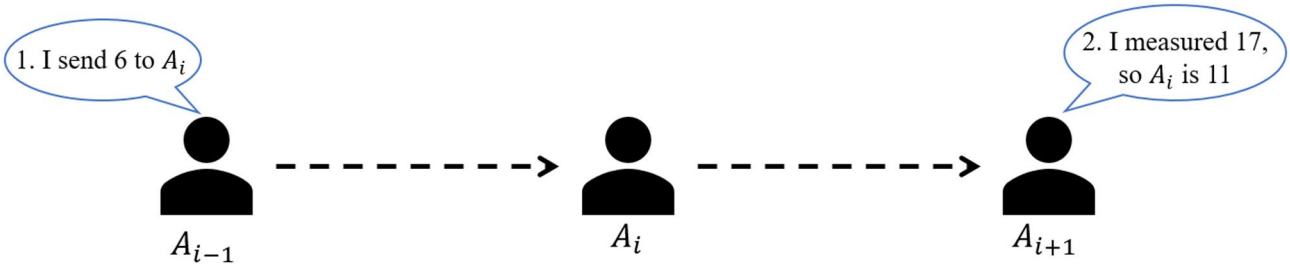

Fig. 6. Collusion attack scenario.

Protocol	Chen et al.[6]	Zhang et al.[7]	Zhang et al.[9]	Wu and Xie (2023) [17]	Yang and Ye (2018) [20]	Ji et al.[21]	Wu and Ma[23]	Proposed QPS
Quantum resource	GHZ state	Single qubits	GHZ state	Single qubits	d-level entangled state	d-level entangled state	d-level entangled state	Single qubits
Operation on primary photons	H, I, Z	I, Y	H	Y, H	QFT,U_k	d-level Bell measurement	QFT,U_x	None
Devices for Trojan horse attacks	No	Yes	No	Yes	No	No	Yes	No
Transmission type	Tree	Ring	Tree	Ring	Tree	Tree	Ring	Relay
Arithmetic calculations	Modulo-2 summation	Modulo-2 summation	Modulo-2 summation	Modulo-2 summation	Modulo-d summation	Modulo-d summation	Modulo-d summation	Modulo-d summation
Number of photons	k ($3N+1$)	k ($1+N/2$)	k ($3N-1$)	k ($N+2$)	k ($2N$-1)	$4Nk+5N+k+1$	k ($N+3$)	$2kN$

Table 1. Efficiency comparison of several QPS protocols.

We assume that the summation has an upper bound of k bits, and N denotes the total number of agents participating in the protocol, excluding TP. During the transmission of each photon sequence, an equal number of decoy photons are required to ensure that there are no eavesdroppers in the communication. That is, each transmitted photon has a 50% probability of being used for security checks. Since existing QPS studies utilizing modulo-2 summation do not account for carry-over bits[6,7,9,17], the summation of two bit-strings is simply performed using the exclusive-OR operation (e.g., $1010 \oplus 1011 = 0001$). Compared to QPS studies using modulo-d summation[20,21,23], it is not possible to directly assess the range of sum values obtained between the two approaches. Therefore, in terms of efficiency comparison, this study focuses on evaluating the quantum resource costs (i.e., the number of photons) required to implement each QPS protocol. In the following discussion, we divide the comparisons into two parts: the first part discusses QPS research related to summation modulo 2 (i.e., bitwise exclusive-OR), and the second part focuses on QPS research related to summation modulo d.

The existing QPS protocols on summation modulo 2 are discussed as follows. Chen et al.[6] proposed a QPS scheme that apply the GHZ state as the quantum resource, which is more challenging to prepare compared to the single photons used in our QPS protocol. Their protocol involves operations on primary photons using H, I, and Z gates, whereas our protocol only requires single-photon measurement without any logic gate operations. Their transmission mode is tree-based, with the burden concentrated on TP, which can be viewed as a cloud service. In contrast, our protocol uses a relay transmission model, distributing the load evenly among all participants. Zhang et al.[7] also utilizes single photons, which is similar to our scheme. Their protocol involves operations on primary photons using I and Y gates. Their protocol relies on optical devices such as the wavelength filter and photon number splitting (PNS) to resist Trojan horse attacks, while the proposed QPS does not. In terms of transmission, the ring type requires TP to send photons, whereas the relay type does not. Zhang et al.[9] uses GHZ states as the quantum resource, which is more complex to prepare compared to the single photons used in our protocol. Their protocol involves operating on primary photons using H gates, whereas the proposed QPS only requires single-photon measurement without any logic gate operations. Both protocols do not require optical devices to resist Trojan horse attacks. In terms of transmission, their protocol employs a tree-based mode that places the burden on TP, while our scheme distributes the load evenly among all participants. Wu and Xie[17] have been the most inspirational in shaping our research. In their protocol, TP shares a secure key with each agent individually, using this key to encrypt information. Since TP holds the keys for all agents, it can decrypt the information when the photons are returned to TP. Note that our QPS protocol use single photons as the quantum resource. Wu and Xie's protocol requires operations on primary photons using Y and H gates, whereas our protocol only requires single-photon measurement without any logic gate operations. Since Wu and Xie's protocol involves the same sequence of photons repeatedly entering and exiting the quantum channel, it requires optical devices that are resistant to Trojan horse attacks, whereas our protocol does not.

Among these existing QPS protocols utilizing modulo-2 summation, the required number of photons in each scheme is evaluated as follows. In Chen et al.'s QPS protocol[6], TP prepares k sets of $N+1$ GHZ states, sending one photon from each set to every agent, resulting in $k(N+1)$ photons. Each agent also prepares k single photons (i.e., kN), and the transmission process requires kN decoy photons, leading to a total of $k(3N+1)$ photons. Zhang et al.[7] introduce a QPS protocol in which each round-trip transmission involves half of the photons being decoy photons, reducing the overall photon consumption to $k(1+N/2)$. They later proposed another QPS protocol[9] in which each agent generates k photons (i.e., kN), consumes k photons to verify the first agent's honesty, and uses k decoy photons per round-trip transmission, resulting in a total of $k(3N-1)$ photons. Wu and Xie's QPS protocol[17] requires k single photons for message transmission and $k(N+1)$ decoy photons, amounting to $k(N+2)$ photons.

Similarly, we evaluate the required number of photons in each QPS scheme utilizing modulo-d summation, including the proposed QPS in this study. In Yang et al.'s QPS protocol[20], k d-level N-particle entangled states are prepared and divided into N sequences, with $N-1$ sets of decoy photons inserted into the second to the N-th sequence, leading to $k(2N-1)$ photons. Ji et al. propose two different QPS protocols[21], and in the more efficient one, TP prepares $(k+1)$ $(N+1)$-particle cat states, each participant prepares $2(k+1)N$ d-level Bell states, and N sets of decoy photons (i.e., kN) to ensure communication security. Additionally, each participant generates an extra $2N$ d-level Bell states, resulting in a total photon cost of $4Nk+5N+k+1$.

Wu and Ma's QPS protocol[23] uses $2k$ Bell-state photons for message transmission and $k(N+1)$ decoy photons for verification, resulting in a total of $k(N+3)$ photons. In the proposed QPS protocol, k photons are used to compute the upper bound of 2^k, and each agent transmits $2k$ photons (with k carrying messages and k serving as decoy photons) to the next participant. With N agents, the total photon count required for the proposed scheme is $2kN$.

Although our proposed QPS protocol appears to require slightly more photons to complete the process, the QPS protocols proposed by Yang and Ye[20], Ji et al.[21], and Wu and Ma[23] all utilize high-level qudits, which necessitate complex QFT to convert from the computational basis to the Fourier basis. In contrast, our QPS protocol eliminates the need for such complex QFT, making it significantly simpler to implement. Operationally, their protocols store secrets on qudits using phase shifting, whereas our scheme relies solely on single-photon measurements without any logic gate operations. In summary, the proposed QPS protocol provides a simpler and more cost-effective approach for computing summation modulo d while achieving a higher success rate.

Conclusion

This paper presents a multiparty QPS protocols that calculates the summation of agents' secrets in modulo d without revealing their contents. The proposed QPS protocol simplifies the use of qubits instead of qudits, eliminating the need for complex quantum Fourier transform. It also employs pre-shared keys to protect each participant's secrets, allowing participants to only measure photons rather than perform logic gate operations, significantly enhancing success rates. Additionally, decoy photons enable any participant to immediately check for eavesdropping upon receiving photons, ensuring protocol security. If an eavesdropping attempt is detected, the protocol is promptly aborted. Extensive analysis of common attacks confirms the protocol's reliability. In future work, the proposed QPS protocol could be explored for its potential to support multiplication. However, due to the limited combinations of multiplication operations and the significance of prime numbers, participants could potentially deduce others' secrets more effectively, which warrants further observations.

Data availability

The datasets analyzed during the current study are available from the corresponding author on reasonable request.

Received: 5 December 2024; Accepted: 5 June 2025
Published online: 02 July 2025

References

1. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **41**(2), 303–332 (1999).
2. Rivest, R. L., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**(2), 120–126 (1978).
3. Liu, W.-J. & Li, Z.-X. Secure and efficient two-party quantum scalar product protocol with application to privacy-preserving matrix multiplication. *IEEE Trans. Circuits Syst. I Regul. Pap.* **70**(11), 4456–4469 (2023).
4. Li, Z.-X., Liu, W.-J. & Su, B.-M. Efficient quantum secure multi-party greatest common divisor protocol and its applications in private set operations. *EPJ Quantum Technol.* **11**(1), 57 (2024).
5. Li, Z.-X. & Liu, W.-J. Quantum secure multi-party computation protocols for solving least common multiple problem. *Chin. J. Comput.* **47**(6), 1393–1412 (2024).
6. Chen, X. B., Xu, G., Yang, Y. X. & Wen, Q. Y. An efficient protocol for the secure multi-party quantum summation. *Int. J. Theor. Phys.* **49**, 2793–2804 (2010).
7. Zhang, C., Sun, Z., Huang, Y. & Long, D. High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. *Int. J. Theor. Phys.* **53**, 933–941 (2014).
8. Zhang, C., Sun, Z. W., Huang, X. & Long, D. Y. Three-party quantum summation without a trusted third party. *Int. J. Quantum Inf.* **13**(02), 1550011 (2015).
9. Zhang, C., Situ, H., Huang, Q. & Yang, P. Multi-party quantum summation without a trusted third party based on single particles. *Int. J. Quantum Inf.* **15**(02), 1750010 (2017).
10. Zhang, C., Huang, Q., Long, Y. & Sun, Z. Secure three-party semi-quantum summation using single photons. *Int. J. Theor. Phys.* **60**(9), 3478–3487 (2021).
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. *Int. J. Theor. Phys.* **56**, 2783–2791 (2017).
12. Shi, R. H. & Zhang, S. Quantum solution to a class of two-party private summation problems. *Quantum Inf. Process.* **16**, 1–9 (2017).
13. Gu, J., Hwang, T. & Tsai, C. W. Improving the security of 'high-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom'. *Int. J. Theor. Phys.* **58**, 2213–2217 (2019).
14. Ye, T. Y. & Xu, T. J. A lightweight three-user secure quantum summation protocol without a third party based on single-particle states. *Quantum Inf. Process.* **21**(9), 309 (2022).
15. Hu, J. L. & Ye, T. Y. Three-party secure semiquantum summation without entanglement among quantum user and classical users. *Int. J. Theor. Phys.* **61**(6), 170–180 (2022).
16. Ye, T. Y., Xu, T. J., Geng, M. J. & Chen, Y. Two-party secure semiquantum summation against the collective-dephasing noise. *Quantum Inf. Process.* **21**(3), 118 (2022).
17. Wu, W. Q. & Xie, M. Z. Quantum secure multi-party summation using single photons. *Entropy* **25**(4), 590 (2023).
18. Tian, Y., Zhang, N., Ye, C., Bian, G. & Li, J. Different secure semi-quantum summation models without measurement. *EPJ Quantum Technol.* **11**(1), 35 (2024).
19. Cheng, Q., Situ, H., Huang, Q. & Zhang, C. Secure three-party quantum summation based on W-class states. *Int. J. Theor. Phys.* **63**(4), 98 (2024).
20. Yang, H. Y. & Ye, T. Y. Secure multi-party quantum summation based on quantum Fourier transform. *Quantum Inf. Process.* **17**(6), 129 (2018).
21. Ji, Z. et al. Quantum protocols for secure multi-party summation. *Quantum Inf. Process.* **18**, 1–19 (2019).
22. Sutradhar, K. & Om, H. A generalized quantum protocol for secure multiparty summation. *IEEE Trans. Circuits Syst. II Express Briefs* **67**(12), 2978–2982 (2020).

23. Wu, W. & Ma, X. Multi-party quantum summation without a third party based on d-dimensional Bell states. *Quantum Inf. Process.* **20**(6), 200 (2021).
24. Ye, T. Y. & Hu, J. L. Quantum secure multiparty summation based on the phase shifting operation of d-level quantum system and its application. *Int. J. Theor. Phys.* **60**, 819–827 (2021).
25. Yi, X., Cao, C., Fan, L. & Zhang, R. Quantum secure multi-party summation protocol based on blind matrix and quantum Fourier transform. *Quantum Inf. Process.* **20**(7), 249 (2021).
26. Cai, X. Q., Wang, T. Y., Wei, C. Y. & Gao, F. Cryptanalysis of secure multiparty quantum summation. *Quantum Inf. Process.* **21**(8), 285 (2022).
27. Coppersmith, D. An approximate Fourier transform useful in quantum factoring. Preprint at quant-ph/0201067. (2002).
28. Shi, R. H., Mu, Y., Zhong, H., Cui, J. & Zhang, S. Secure multiparty quantum computation for summation and multiplication. *Sci. Rep.* **6**(1), 19655 (2016).
29. Lv, S. X., Jiao, X. F. & Zhou, P. Multiparty quantum computation for summation and multiplication with mutually unbiased bases. *Int. J. Theor. Phys.* **58**, 2872–2882 (2019).
30. Sutradhar, K. & Om, H. Hybrid quantum protocols for secure multiparty summation and multiplication. *Sci. Rep.* **10**(1), 9097 (2020).
31. Zhang, W. W. & Zhang, K. J. Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party. *Quantum Inf. Process.* **12**, 1981–1990 (2013).
32. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December. 9–12 (1984).
33. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**(6), 661–663 (1991).
34. Zhang, Z. J. Multiparty quantum secret sharing of secure direct communication. *Phys. Lett. A* **342**(1–2), 60–66 (2005).
35. Han, L. F., Liu, Y. M., Liu, J. & Zhang, Z. J. Multiparty quantum secret sharing of secure direct communication using single photons. *Opt. Commun.* **281**(9), 2690–2694 (2008).
36. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299**(5886), 802–803 (1982).
37. Busch, P., Heinonen, T. & Lahti, P. Heisenberg's uncertainty principle. *Phys. Rep.* **452**(6), 155–176 (2007).
38. Li, C.-Y., Zhou, H.-Y., Wang, Y. & Deng, F.-G. Secure quantum key distribution network with Bell states and local unitary operations. *Chin. Phys. Lett.* **22**(5), 1049–1052 (2005).
39. Li, C.-Y. et al. Efficient quantum cryptography network without entanglement and quantum memory. *Chin. Phys. Lett.* **23**(11), 2896–2899 (2006).
40. Deng, F. G., Long, G. L. & Liu, X. S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys. Rev. A* **68**(4), 042317 (2003).
41. Gao, F., Guo, F., Wen, Q. & Zhu, F. Comparing the efficiencies of different detect strategies in the ping-pong protocol. *Sci. China Ser. G* **51**(12), 1853–1860 (2008).
42. Wang, T.-Y., Wen, Q.-Y. & Zhu, F.-C. Secure authentication of classical messages with single photons. *Chin. Phys. B* **18**(8), 3189–3192 (2009).
43. Deng, F. G., Li, X. H., Zhou, H. Y. & Zhang, Z. J. Improving the security of multiparty quantum secret sharing against Trojan horse attack. *Phys. Rev. A* **72**(4), 044302 (2005).
44. Cai, Q. Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys. Lett. A* **351**(1–2), 23–25 (2006).
45. Gisin, N., Fasel, S., Kraus, B., Zbinden, H. & Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **73**(2), 022320 (2006).
46. Wang, T. Y., Wen, Q. Y., Gao, F., Lin, S. & Zhu, F. C. Cryptanalysis and improvement of multiparty quantum secret sharing schemes. *Phys. Lett. A* **373**(1), 65–68 (2008).
47. Gao, G. Simple collaboration eavesdropping on the improved multiparty quantum secret sharing protocol. *Int. J. Theor. Phys.* **49**, 2210–2214 (2010).
48. Wang, S. H., Chong, S. K. & Hwang, T. On multiparty quantum secret sharing with Bell states and Bell measurements. *Opt. Commun.* **283**(21), 4405–4407 (2010).

Author contributions

Jason Lin: Conceptualization, Methodology, Investigation, Formal Analysis, Writing – Review & Editing. Shao-Lun Huang: Methodology, Formal Analysis, Writing – Original Draft. Chun-Wei Yang: Formal Analysis, and Review manuscript. Chia-Wei Tsai: Review the manuscript and project administration.

Funding

This work was partially supported by the National Science and Technology Council, Taiwan, R.O.C. (Grant Nos. NSTC 113–2221-E-025–014, NSTC 113–2221-E-039–020, NSTC 113–2221-E-005–086, and NSTC 113–2634-F-005–001-MBK) and China Medical University, Taiwan (Grant No. CMU112-S-42).

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to C.-W.T.

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.