mathematics

IMPACT FACTOR 2.592

CITESCORE 2.9

Article

Robust Semi-Quantum Summation over a Collective-Dephasing Noise Channel

Chun-Wei Yang, Chia-Wei Tsai, Chi-An Chen and Jason Lin

Special Issue

Quantum Cryptography and Applications

Edited by

Dr. Chun-Wei Yang, Dr. Chia-Wei Tsai and Dr. Jason Lin

MDPI

https://doi.org/10.3390/math11061405

mathematics

MDPI

Article

Robust Semi-Quantum Summation over a Collective-Dephasing Noise Channel

Chun-Wei Yang [1], Chia-Wei Tsai [2], Chi-An Chen [1] and Jason Lin [3,*]

[1] Master Program for Digital Health Innovation, College of Humanities and Sciences, China Medical University, No. 100, Sec. 1, Jingmao Rd., Beitun District, Taichung 406040, Taiwan
[2] Department of Computer Science and Information Engineering, National Taichung University of Science and Technology, No.129, Sec. 3, Sanmin Rd., North District, Taichung 40401, Taiwan
[3] Department of Computer Science and Engineering, National Chung Hsing University, No. 145, Xingda Rd., South District, Taichung 40227, Taiwan
* Correspondence: jasonlin@nchu.edu.tw

Abstract: Quantum summation is one of the various applications in secure multi-party computation. However, most of the existing quantum summation protocols assume that the participants possess all the quantum devices. Considering future applications, the capability of the participants must be adjusted before it can be put into practical use. Although Boyer et al. proposed that the semi-quantum environment could be used to solve this problem; another practical problem is the interference by noise. In 2022, Ye et al. proposed a two-party semi-quantum summation (SQS) protocol resistant to the interference of collective noise, in which two classical participants can accomplish the summation of their private binary sequences with the assistance of a quantum semi-honest third party. They proved that their SQS protocol is resistant to various eavesdropping attacks. This paper unveils two risks of information leakage in Ye et al.'s SQS protocol. If the aforementioned security issues are not resolved, Ye et al.'s SQS protocol may not be able to perform private quantum computations securely. Fortunately, the SQS protocol against the collective-dephasing noise proposed in this study is free from the issue of information leakage as well as resistant to various quantum attacks. In addition, the quantum efficiency of the SQS protocol proposed in this study is four times higher than that of Ye et al.'s SQS protocol, which can effectively improve the quantum utilization rate.

Keywords: quantum cryptography; collective-dephasing noise; measure-resend; semi-quantum summation

MSC: 81P94

Citation: Yang, C.-W.; Tsai, C.-W.; Chen, C.-A.; Lin, J. Robust Semi-Quantum Summation over a Collective-Dephasing Noise Channel. *Mathematics* **2023**, *11*, 1405. https://doi.org/10.3390/math11061405

Academic Editor: Jonathan Blackledge

Received: 14 February 2023
Revised: 10 March 2023
Accepted: 13 March 2023
Published: 14 March 2023

1. Introduction

With the development of quantum information and quantum computation, quantum computers continue to break through technical bottlenecks. Owing to the computing capabilities of quantum computers, studies have confirmed that many mathematical problems, which are difficult to solve using traditional computers, can be solved in polynomial time using quantum computation [1–4]. It can be seen that quantum computation has a huge impact on the future development of cryptography. Among them, secure multiparty quantum summation [5–17] is one of the basic applications of secure multiparty quantum computation [18–22]. which can be explained as: n users $P_1, P_2, \ldots, P_n$ intend to compute a summation function $f(x_1, x_2, \ldots, x_n)$, where x_i $(i = 1, 2, \ldots, n)$ represents the private input of user P_i. Function f can be displayed publicly or only available to certain users. The objective of secure multiparty quantum summation is to ensure the correctness of the summation results and to protect the privacy of users' inputs. Quantum summation plays an important role in the construction of complex multiparty computations and can be

potentially applied to scenarios, such as quantum private comparison [23–27] and quantum voting [28–31].

In recent years, many studies on quantum summation protocols have been flourishing through various quantum states. In 2014, Zhang et al. [8] used a single photon to construct a quantum summation protocol in the photon polarization mode and spatial degree of freedom mode through unitary operation and quantum repetition test. In 2015, Zhang et al. [9] proposed a three-party (TP) quantum summation protocol that does not require an honest third party, in which the quantum entanglement state of six photons is used. In 2016, Shi et al. [10] used quantum Fourier transform, controlled NOT, and oracle operators to study the protocol of quantum summation and quantum multiplication problems. Afterwards, they proposed a common solution to the quantum summation problems in the special case of the two parties [11]. In 2017, Zhang et al. [12] designed a multiparty quantum summation protocol based on a single photon and unitary operation. In the same year, Liu et al. [13] studied a quantum summation protocol using the entanglement states with multiple photons (e.g., Bell state), to encode private computations of users. In 2018, Yang et al. [14] proposed a quantum solution to solve in environments that rely on n-party and d-dimensional entanglement states. In 2019, Ji et al. [15] proposed a probabilistic quantum summation protocol based on the quantum entanglement swapping between the Bell and cat states. In the same year, Gu et al. [16] discovered that the quantum summation protocol proposed by Zhang et al. [8] can be under interception replay attacks, and they proposed an improved strategy.

However, all the above aforementioned quantum summation protocols [5–17] assume that the participants have all the quantum devices. In practice, although quantum computers and the construction of quantum networks have developed rapidly, for ordinary users, quantum devices and instruments are expensive. Therefore, unlike the common study on quantum cryptography protocols, in 2007, Boyer et al. [32] proposed the first semi-quantum key distribution (SQKD) through the generation and measurement of a single photon. According to their definitions, the semi-quantum environment can be simply classified into Alice, a participant with quantum capabilities, and Bob, a participant with classical capabilities. In other words, Alice represents the party with expensive quantum, quantum instruments, and capabilities, while Bob represents the party with fewer capabilities and more constraints. The detailed definitions are as follows: Quantum user Alice can perform the following operations: (1) generate any quantum state, for example, single photon or Bell state; (2) perform any measurement mode, for example, Bell test or measurement of multiple entanglement; (3) possesses quantum memories to store quantum states. However, classical user Bob is limited to performing the following operations: (1) use the Z basis $\{|0>, |1>\}$ to generate quantum states; (2) use the Z basis to measure the received quantum bits (qubit); (3) rearrange qubits by various delayed quantum circuits; (4) directly reflect the received qubits. Because Bob only uses the qubits $|0>$ and $|1>$, and does not consider other quantum superposition of single photons, the operations that can be performed by Bob are similar to the computation in traditional communication.

In 2021, Zhang et al. [33] designed a three-party semi-quantum summation protocol using single photons. Among them, the GHZ-based basis measurement technique is used to check the honesty of almost-dishonest TP and to calculate the summation of users' private inputs. In this protocol, it is assumed that TP is almost dishonest, which means that TP is capable of launching all kinds of attacks without violating quantum mechanics, except for the collusion attacks with other dishonest users. The three classical participants who received particles from the TP can only perform the following two modes of operations: (1) reflect particles back to the TP without interference; (2) use Z basis $\{|0>, |1>\}$ to measure the received quantum states, and generate the same quantum states to reflect back to the TP. Zhang et al. [33] claimed that their proposed semi-quantum summation protocol could resist attacks from outside and dishonest parties. In 2022, Hu and Ye [34] constructed a three-party secure semi-quantum summation protocol using a single photon. It can calculate the modulo 2 summation of the private bits from one quantum participant and

two classical participants. In the protocol proposed by Hu and Ye [34], quantum participants need to perform only Z-basis, X-basis, and Bell basis measurements, and do not need to perform quantum entanglement swapping, unitary operations, or shared private keys beforehand. Compared with the semi-quantum summation protocol of Zhang et al. [33], the protocol by Hu and Ye [34] has better performance in quantum measurements by the quantum participants. In addition, the protocol by Hu and Ye [34] has a higher value of quantum efficiency. In 2022, Pan [35] proposed a special participant attack against the semi-quantum summation protocol by Zhang et al. [33] Although the semi-quantum summation protocol by Zhang et al. [33] detects the presence of eavesdroppers and checks the honesty of the TP, the TP can obtain the measurement results of the three participants without being discovered. As a result, the semi-quantum summation protocol by Zhang et al. [33] cannot calculate the summation, and the TP even may access the private information of the three participants.

However, the aforementioned studies on semi-quantum summation protocols [33–35] focused on discussing the design and security of the protocol. Although these studies used the properties of quantum physics to develop security protocols capable of detecting the presence of eavesdroppers, they must have the assumption that there is no noise interference in the communication process, that is, the quantum channel is an ideal channel. Without this assumption, on an actual quantum channel, the error rate produced by the aforementioned semi-quantum summation protocol [33–35] cannot be distinguished as being caused by eavesdropping or noise interference. Therefore, attackers can launch an attack and use the noise to hide the errors caused by the attack, so that the two parties in the communication will mistakenly believe, in their open discussions, that the measurement errors are caused by the noise on the channel.

In 2022, Ye et al. [36] proposed a two-party semi-quantum summation protocol resistant to interference by collective noise, in which the two classical users could accomplish the summation of their private binary sequences with the assistance of a quantum almost-dishonest TP. The term "almost-dishonest" implies that the TP cannot collude with others; however, it can implement all kinds of quantum attack strategies itself. Ye et al.'s semi-quantum summation protocol [36] employs logical qubits as transmission media to overcome the negative influence of collective-dephasing noise and does not make any two parties share a random secret key beforehand. The security analysis of Ye et al. [36] proves that their protocol can effectively prevent outside attacks from eavesdroppers and attacks from TP or inside participants. In addition, the TP has no way of knowing about the summation results.

Although Ye et al. [36] proved in their study that their semi-quantum summation protocol is resistant to all kinds of eavesdropping attacks, this study proves that their semi-quantum summation protocol [36] has two risks of information leakage. If these security issues are not resolved, their semi-quantum summation protocol [36] may not be able to perform private quantum computations securely.

The goal of this study is to propose a semi-quantum summation protocol that is secure and resistant to noise interference. This study also proves that Ye et al.'s semi-quantum summation protocol [36] has two risks of information leakage. Compared with the semi-quantum summation protocol proposed by Ye et al. [36], the semi-quantum summation protocol against the collective-dephasing noise proposed in this study is free from information leakage in addition to being resistant to all kinds of quantum attacks. In addition, the quantum efficiency of the proposed protocol is four times higher than that of Ye et al.'s [36], which can effectively improve the quantum utilization rate.

The rest of this paper is organized as follows. First of all, Section 2 will revisit the step-by-step procedure of Ye et al.'s semi-quantum summation protocol. Then, two security loopholes in their protocol will be pointed out in Section 3 along with a possible solution to remedy these problems. Section 4 will do a thorough security analysis including some common quantum attacks. Section 5 presents the efficiency analysis. Section 6 will give a brief conclusion.

2. Review of Ye et al.'s Semi-Quantum Summation Protocol

To illustrate the results of this study, Section 2.1 introduces the characteristics of collective-dephasing noise. Subsequently, in Section 2.2 the semi-quantum summation protocol by Ye et al. [36] is introduced and reviewed.

2.1. Collective-Dephasing Noise

Noise interference increases the error rate of quantum communication in addition to causing de-coherence, which changes the quantum state or destroys the quantum entanglement, leading to incorrect results in the quantum state measurement. Therefore, the focus of this study is to design a high-efficiency fault-tolerant quantum coding technology that can resist the interference of quantum noise.

Collective-dephasing noise is one of the common collective noises. In the following content, a single photon has been used to introduce the characteristics of collective-dephasing noise and the method of fault-tolerant coding. With the interference of collective-dephasing noise, single photons $|0>$ and $|1>$ will respectively be changed to $|0>$ and $e^{i\theta}|1>$, in which $e^{i\theta}$ will vary with time. To overcome the interference of the collective-dephasing noise, the tensor product of the single photons to each other is calculated, that is, $|00>$, $|01>$, $|10>$ and $|11>$. It can be found that $|01>$ and $|10>$ have the same interference coefficient $e^{i\theta}$. Therefore, [37–41] used $|01>$ and $|10>$ to design fault-tolerant coding, which can resist the interference of collective-dephasing noise. They defined the logical single photon with Z_{dp} basis as $\left|0_{dp}>\right. = \left|01>\right.$ and $\left|1_{dp}>\right. = \left|10>\right.$, then, the other set of X_{dp} basis as $\left|+_{dp}>\right. = \frac{1}{\sqrt{2}}\left(\left|0_{dp}>\right.+\left|1_{dp}>\right.\right) = \frac{1}{\sqrt{2}}(|01>+|10>)$ and $\left|-_{dp}>\right. = \frac{1}{\sqrt{2}}\left(\left|0_{dp}>\right.-\left|1_{dp}>\right.\right) = \frac{1}{\sqrt{2}}(|01>-|10>)$.

In addition to the fact that logical single photons can resist collective-dephasing noise, [42] also proposed it using logical Bell states to resist collective-dephasing noise, as shown in Equations (1)–(4), where $\left|\Phi^{\pm}>\right. = \frac{1}{\sqrt{2}}(|00>\pm|11>)$ and $\left|\Psi^{\pm}>\right. = \frac{1}{\sqrt{2}}(|01>\pm|10>)$ are the common Bell states. From Equations (1)–(4), it can be seen that except when directly using the logical Bell basis for measurement, the general Bell basis can also be used for two measurements to distinguish the four logical Bell states.

$$\begin{aligned}\left|\Phi^{+}_{dp}>\right._{1234} &= \frac{1}{\sqrt{2}}\left(\left|+_{dp}>\right.\left|+_{dp}>\right.+\left|-_{dp}>\right.\left|-_{dp}>\right.\right)_{1234} = \frac{1}{\sqrt{2}}\left(\left|0_{dp}>\right.\left|0_{dp}>\right.+\left|1_{dp}>\right.\left|1_{dp}>\right.\right)_{1234}\\ &= \frac{1}{\sqrt{2}}(|01>|01>+|10>|10>)_{1234} = \frac{1}{\sqrt{2}}(|00>|11>+|11>|00>)_{1324}\\ &= \frac{1}{\sqrt{2}}\left(\left|\Phi^{+}>\right.\left|\Phi^{+}>\right.-\left|\Phi^{-}>\right.\left|\Phi^{-}>\right.\right)_{1324}\end{aligned} \tag{1}$$

$$\begin{aligned}\left|\Phi^{-}_{dp}>\right._{1234} &= \frac{1}{\sqrt{2}}\left(\left|+_{dp}>\right.\left|-_{dp}>\right.+\left|-_{dp}>\right.\left|+_{dp}>\right.\right)_{1234} = \frac{1}{\sqrt{2}}\left(\left|0_{dp}>\right.\left|0_{dp}>\right.-\left|1_{dp}>\right.\left|1_{dp}>\right.\right)_{1234}\\ &= \frac{1}{\sqrt{2}}(|01>|01>-|10>|10>)_{1234} = \frac{1}{\sqrt{2}}(|00>|11>-|11>|00>)_{1324}\\ &= \frac{1}{\sqrt{2}}\left(\left|\Phi^{-}>\right.\left|\Phi^{+}>\right.-\left|\Phi^{+}>\right.\left|\Phi^{-}>\right.\right)_{1324}\end{aligned} \tag{2}$$

$$\begin{aligned}\left|\Psi^{+}_{dp}>\right._{1234} &= \frac{1}{\sqrt{2}}\left(\left|+_{dp}>\right.\left|+_{dp}>\right.-\left|-_{dp}>\right.\left|-_{dp}>\right.\right)_{1234} = \frac{1}{\sqrt{2}}\left(\left|0_{dp}>\right.\left|1_{dp}>\right.+\left|1_{dp}>\right.\left|0_{dp}>\right.\right)_{1234}\\ &= \frac{1}{\sqrt{2}}(|01>|10>+|10>|01>)_{1234} = \frac{1}{\sqrt{2}}(|01>|10>+|10>|01>)_{1324}\\ &= \frac{1}{\sqrt{2}}\left(\left|\Psi^{+}>\right.\left|\Psi^{+}>\right.-\left|\Psi^{-}>\right.\left|\Psi^{-}>\right.\right)_{1324}\end{aligned} \tag{3}$$

$$\begin{aligned}\left|\Psi^{-}_{dp}>\right._{1234} &= \frac{1}{\sqrt{2}}\left(\left|-_{dp}>\right.\left|+_{dp}>\right.-\left|+_{dp}>\right.\left|-_{dp}>\right.\right)_{1234} = \frac{1}{\sqrt{2}}\left(\left|0_{dp}>\right.\left|1_{dp}>\right.-\left|1_{dp}>\right.\left|0_{dp}>\right.\right)_{1234}\\ &= \frac{1}{\sqrt{2}}(|01>|10>-|10>|01>)_{1234} = \frac{1}{\sqrt{2}}(|01>|10>-|10>|01>)_{1324}\\ &= \frac{1}{\sqrt{2}}\left(\left|\Psi^{-}>\right.\left|\Psi^{+}>\right.-\left|\Psi^{+}>\right.\left|\Psi^{-}>\right.\right)_{1324}\end{aligned} \tag{4}$$

From Equations (1) and (3), Equation (5) can be deduced as:

$$\left|+_{dp}>\right._{12}\left|+_{dp}>\right._{34} = \frac{1}{\sqrt{2}}\left(\left|\Phi^{+}_{dp}>\right._{1234}+\left|\Psi^{+}_{dp}>\right._{1234}\right) \tag{5}$$

From Equation (5) it can be seen that, if two Bell basis measurements are performed, the measurement result can be deduced as $|\Phi^+>_{13}|\Phi^+>_{24}$, $|\Phi^->_{13}|\Phi^->_{24}$, $|\Psi^+>_{13}|\Psi^+>_{24}$, $|\Psi^->_{13}|\Psi^->_{24}$. Therefore, according to Equations (1)–(4), Equations (6)–(9) can be deduced as:

$$\left|0_{dp}>_{12}\left|0_{dp}>_{34}=\frac{1}{\sqrt{2}}\left(\left|\Phi^+_{dp}>_{1234}+\left|\Phi^-_{dp}>_{1234}\right.\right.\right.\right. \tag{6}$$

$$\left|0_{dp}>_{12}\left|1_{dp}>_{34}=\frac{1}{\sqrt{2}}\left(\left|\Psi^+_{dp}>_{1234}+\left|\Psi^-_{dp}>_{1234}\right.\right.\right.\right. \tag{7}$$

$$\left|1_{dp}>_{12}\left|0_{dp}>_{34}=\frac{1}{\sqrt{2}}\left(\left|\Psi^+_{dp}>_{1234}-\left|\Psi^-_{dp}>_{1234}\right.\right.\right.\right. \tag{8}$$

$$\left|1_{dp}>_{12}\left|1_{dp}>_{34}=\frac{1}{\sqrt{2}}\left(\left|\Phi^+_{dp}>_{1234}-\left|\Phi^-_{dp}>_{1234}\right.\right.\right.\right. \tag{9}$$

2.2. Semi-Quantum Summation Protocol against Collective-Dephasing Noise

Suppose there are two classical participants with limited quantum capabilities, Alice and Bob. Alice's private binary string is denoted as $X = (x_1, x_2, \ldots, x_n)$, while Bob's private binary string is denoted as $Y = (y_1, y_2, \ldots, y_n)$. Here, x_i and y_i are in $\{0, 1\}$, $i = 1, 2, \ldots, n$. Alice and Bob want to calculate the modulo 2 summation of their private binary strings over the collective-dephasing noise quantum channel. In the semi-quantum summation protocol against the collective-dephasing noise, an almost-dishonest TP is used to assist the calculation. The TP has the ability to perform all kinds of attacks but is not allowed to collude attacks with anyone else [43]. A secure semi-quantum summation protocol should meet the following requirements [7]:

1. Correctness: The summation results of the private binary strings of the two participants should be correct.
2. Security: The private binary strings of the two participants cannot be leaked out to an outside eavesdropper.
3. Privacy: The private binary string of each participant should be kept secret from the TP.

Inspired by [44,45], Ye et al. designed a semi-quantum summation protocol to calculate the modulo 2 summation of Alice's and Bob's private binary strings over the collective-dephasing noise quantum channel. The protocol steps are described as follows.

Step 1: TP generates an initial state $|+_{dp}>_{12}=\frac{1}{\sqrt{2}}\left(\left|0_{dp}>+\right|1_{dp}>\right)=\frac{1}{\sqrt{2}}(|01>+|10>)_{12}$, and then all the first and second photons with $\left|+_{dp}>_{12}\right.$ are assembled into photon groups $S_1=\left\{s_1^1, s_1^2, \ldots, s_1^n\right\}$ and $S_2=\left\{s_2^1, s_2^2, \ldots, s_2^n\right\}$ respectively, where s_1^i and s_2^i, respectively, denote the ith photon in S_1 and S_2. Finally, the TP sends the photons of S_1 and S_2 to Alice and Bob one by one, respectively.

Step 2: For each received photon, Alice and Bob will immediately perform the following two operations, respectively:

(1.) CTRL mode: directly reflecting it back to TP.

(2.) SIFT mode: measuring the photon with Z_{dp} basis and resending the same photon as the received one to TP.

The photon sequences after Alice's and Bob's operations are denoted as S'_1 and S'_2, respectively. The TP stores the received photon sequences S'_1 and S'_2 in a quantum memory.

Step 3: To check the presence of eavesdroppers, TP chooses a group of photons randomly in S'_1 and S'_2 to perform eavesdropping detection. The TP tells Alice and Bob the positions of the chosen photons, and they reply to the TP that the choice is the CTRL mode or the SIFT mode and their respective measurement results.

(1.) For CTRL mode: TP measures the photons with the X_{dp} basis and determines whether the measurement results are identical to the initial state $\left|+_{dp}\right>_{12}$.

(2.) For SIFT mode: TP measures photons with a Z_{dp} basis and determines whether the measurement results are identical to those announced by Alice and Bob.

Step 4: After passing the eavesdropping detection, Alice and Bob ask TP to perform Bell basis measurements twice on the remaining photon sequences and announce the measurement results. After TP announces all the measurement results, Alice and Bob randomly choose a part of the measurement results to check the honesty of TP. If Alice and Bob both choose the CTRL mode, the measurement results announced by TP should be $\left|\Phi^+\right>_{13}\left|\Phi^+\right>_{24}$, $\left|\Phi^-\right>_{13}\left|\Phi^-\right>_{24}$, $\left|\Psi^+\right>_{13}\left|\Psi^+\right>_{24}$, $\left|\Psi^-\right>_{13}\left|\Psi^-\right>_{24}$ (Equation (5)). If both Alice and Bob choose the SIFT mode, the measurement results announced by TP should correspond to Equations (6)–(9). For example, if the measurement results of Alice and Bob are $\left|0_{dp}\right>_{12}$ and $\left|0_{dp}\right>_{34}$, the measurement results announced by TP should be $\left|\Phi^+\right>_{13}\left|\Phi^+\right>_{24}$, $\left|\Phi^-\right>_{13}\left|\Phi^-\right>_{24}$, $\left|\Phi^+\right>_{13}\left|\Phi^-\right>_{24}$, $\left|\Phi^-\right>_{13}\left|\Phi^+\right>_{24}$.

Step 5: After passing the honesty check of TP, Alice and Bob announce the selection mode of the remaining photon sequences. Only when Alice and Bob both choose the SIFT mode can they be used to make secret keys. If Alice's or Bob's measurement result is $\left|0_{dp}\right>$, the respective bit of private key k_j^a and k_j^b is recorded as "0", where $j = 1, 2, \ldots, n$. Conversely, if Alice's or Bob's measurement result is $\left|1_{dp}\right>$, the respective bit of private key k_j^a and k_j^b is recorded as "1". Therefore, Alice and Bob can get their own private keys $K_A = \left\{k_1^a, k_2^a, \ldots, k_n^a\right\}$ and $K_B = \left\{k_1^b, k_2^b, \ldots, k_n^b\right\}$. Alice and Bob can derive the calculated value $C_T = \left\{k_1^t, k_2^t, \ldots, k_n^t\right\}$ of TP from the measurement results. If the measurement result announced by the TP is $\left|\Phi^+\right>_{13}\left|\Phi^+\right>_{24}$, $\left|\Phi^-\right>_{13}\left|\Phi^-\right>_{24}$, $\left|\Phi^+\right>_{13}\left|\Phi^-\right>_{24}$, $\left|\Phi^-\right>_{13}\left|\Phi^+\right>_{24}$, k_j^t will be "0", where $j = 1, 2, \ldots, n$. Conversely, if the measurement result announced by TP is $\left|\Psi^+\right>_{13}\left|\Psi^+\right>_{24}$, $\left|\Psi^-\right>_{13}\left|\Psi^-\right>_{24}$, $\left|\Psi^+\right>_{13}\left|\Psi^-\right>_{24}$, $\left|\Psi^-\right>_{13}\left|\Psi^+\right>_{24}$, then k_j^t will be "1". Alice and Bob calculate their modulo 2 summations $c_j^a = k_j^a \oplus x_j$ and $c_j^b = k_j^b \oplus y_j$, respectively, where $j = 1, 2, \ldots, n$. Subsequently, Alice and Bob tell each other their calculation results $C_A = \left\{c_1^a, c_2^a, \ldots, c_n^a\right\}$ and $C_B = \left\{c_1^b, c_2^b, \ldots, c_n^b\right\}$ respectively. Finally, Alice and Bob calculate $r_j = c_j^a \oplus c_j^b \oplus k_j^t$ to obtain the summation result $R = \{r_1, r_2, \ldots, r_n\}$.

3. Security Issues and Research Methodology

Section 3.1 of this study shows that the semi-quantum summation protocol against the collective-dephasing noise [36] has the problem of the order, in which the participants announce the results. In Section 3.2, the issue of information leakage in the semi-quantum summation protocol against the collective-dephasing noise has been illustrated. Finally, Section 3.3 presents the semi-quantum summation protocol against collective-dephasing noise proposed in this study.

3.1. Issues for the Order of Results Announced by Participants in Ye et al.'s Protocol

Without loss of generality, it is assumed that Bob is a malicious participant in the protocol. If he wants to obtain the result of the quantum summation by himself, he can calculate $r_j = c_j^a \oplus c_j^b \oplus k_j^t$, using his own calculation results $C_B = \left\{c_1^b, c_2^b, \ldots, c_n^b\right\}$ along with $C_T = \left\{k_1^t, k_2^t, \ldots, k_n^t\right\}$ announced by TP and $C_A = \left\{c_1^a, c_2^a, \ldots, c_n^a\right\}$ announced by Alice, so as to obtain the summation $R = \{r_1, r_2, \ldots, r_n\}$. Subsequently, if he maliciously does not announce $C_B = \left\{c_1^b, c_2^b, \ldots, c_n^b\right\}$ to Alice, Alice cannot get the result of the summation.

Therefore, in Ye et al.'s semi-quantum summation protocol against the collective-dephasing noise, for the participants Alice or Bob, the one who announces the summation results first will be the one with a disadvantage. Therefore, there can be a dispute on the unfairness in the design of this protocol.

3.2. Security Issues Owing to Information Leakage in Ye et al.'s Protocol

Unlike the general active attacks, the security issues owing to information leakage are that the eavesdropper Eve can directly analyze the communication data and obtain part or all of the secret information in the communication process without performing any destructive direct attacks. Therefore, this security issue cannot be detected using any detection method. Hence, care must be taken in the design of the protocol, especially in the design of the coding method.

Ye et al.'s semi-quantum summation protocol against the collective-dephasing noise has been analyzed in detail in the following section. In Ye et al.'s semi-quantum summation protocol, TP must announce all the measurement results, C_T, to prevent the almost-dishonest TP from cheating. Subsequently, in Step 5, Alice and Bob announce their calculation results C_A and C_B, respectively. Therefore, the eavesdropper Eve can obtain C_T, C_A and C_B, calculate and obtain $X \bigoplus Y (= C_T \bigoplus C_A \bigoplus C_B)$. In this way, there are four combinations $\{00,\ 01,\ 10,\ 11\}$ of the calculated summations of Alice and Bob for eavesdropper Eve to guess in the first place; however, owing to the obtained $X \bigoplus Y$, Eve can rule out the other two possibilities, leaving only two possible combinations, which causes the issue of information leakage (see also Table 1). For example, Eve calculates $X \bigoplus Y = 0$. It can be deduced that the summation of Alice and Bob will be one of the following two possibilities: $\{00,\ 11\}$. Therefore, Eve can determine that the summation of Alice and Bob must be either one in $\{00,\ 11\}$. Thus, Eve can obtain the $-\sum_i p_i \log_2 p_i = -2 \times \frac{1}{2} \log_2 \frac{1}{2} = 1$ bit of the calculated value. Consequently, if there are two secret bits of calculation results, then one of them gets leaked to Eve.

Table 1. Corresponding table of information leakage.

C_T	C_A	C_B	$C_T \oplus C_A \oplus C_B = X \oplus Y$
0	0	0	0
	0	1	1
	1	0	1
	1	1	0
1	0	0	1
	0	1	0
	1	0	0
	1	1	1

3.3. Proposed Semi-Quantum Summation Protocol against Collective-Dephasing Noise

This section presents the semi-quantum summation protocol against the collective-dephasing noise proposed in this study. Suppose there are two classical participants with limited quantum capabilities, Alice and Bob. Alice's private binary string is denoted as $X = (x_1, x_2, \ldots, x_n)$, while Bob's private binary string is denoted as $Y = (y_1, y_2, \ldots, y_n)$. Here x_i and y_i belong to $\{0, 1\}$, $i = 1, 2, \ldots, n$. Alice and Bob want to calculate the modulo 2 summation of their private binary string over the collective-dephasing noise quantum channel. The almost-dishonest TP has the ability to perform all kinds of attacks but is not allowed to collude attacks with anyone else.

To solve the security issues owing to information leakage, the semi-quantum summation protocol against the collective-dephasing noise proposed in this study allows Alice and Bob to share one secret key K_{AB} in advance. Therefore, an outside attacker cannot obtain

the XOR results of the C_A and C_B values during the communication process. Accordingly, the semi-quantum summation protocol against the collective-dephasing noise proposed in this study does not have security issues owing to information leakage. The steps to the semi-quantum summation protocol against the collective-dephasing noise proposed in this study are described as follows.

Step 1: Alice and Bob share one secret key $K_{AB} = \left\{k_1^{ab}, k_2^{ab}, \ldots, k_n^{ab}\right\}$ through the mediated SQKD protocol [46–54].

Step 2: TP generates an initial state $\left|+_{dp}\right\rangle_{12} = \frac{1}{\sqrt{2}}\left(\left|0_{dp}\right\rangle + \left|1_{dp}\right\rangle\right) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{12}$. Subsequently, all the first and second photons of $\left|+_{dp}\right\rangle_{12}$ are assembled into photon sequences $S_1 = \left\{s_1^1, s_1^2, \ldots, s_1^n\right\}$ and $S_2 = \left\{s_2^1, s_2^2, \ldots, s_2^n\right\}$ respectively, where s_1^i and s_2^i, respectively, denote the ith photon in S_1 and S_2. Finally, the TP sends the photons of S_1 and S_2 to Alice and Bob one by one, respectively.

Step 3: For each received photon, Alice and Bob immediately perform the following two operations, respectively:

(1) CTRL mode: directly reflecting it back to the TP.
(2) SIFT mode: measuring the photon with Z_{dp} basis and resending the same photon as the received one to the TP.

The photon sequences after Alice's and Bob's operations are denoted as S'_1 and S'_2, respectively. The TP stores the received photon sequences S'_1 and S'_2 in a quantum memory.

Step 4: To check the presence of eavesdroppers, Alice and Bob announce their respective chosen modes. They perform the following steps depending on the chosen mode.

(1) Both Alice and Bob choose the SIFT mode: if both Alice and Bob choose the SIFT mode, they can be used for summation calculation and move to Step 5.
(2) Alice chooses the SIFT mode, while Bob chooses the CTRL mode: TP uses the Z_{dp} basis to measure photons and asks Alice to announce the measurement result. Subsequently, it is determined whether the measurement results of both parties are identical. TP uses the X_{dp} basis to measure the photons reflected by Bob, and it is determined whether the measurement result is identical to the initial state $\left|+_{dp}\right\rangle_{12}$.
(3) Alice chooses the CTRL mode, while Bob chooses the SIFT mode: TP uses the X_{dp} basis to measure the photons reflected by Alice and determines whether the measurement result is identical to the initial state $\left|+_{dp}\right\rangle_{12}$. TP uses the Z_{dp} basis to measure photons and asks Bob to announce the measurement result to determine whether the measurement results of the two parties are identical.
(4) Both Alice and Bob choose the CTRL mode: TP uses the X_{dp} basis to measure the photons reflected by Alice and Bob, and determine whether the measurement result is identical to the initial state $\left|+_{dp}\right\rangle_{12}$.

In the checking modes of Steps (2)~(4), if the error rate exceeds the preset threshold, the protocol is terminated and restarted. If it passes the eavesdropping detection, move to Step 5.

Step 5: After passing the eavesdropping detection, only the result that Alice and Bob both choose the SIFT mode is retained. If Alice's or Bob's measurement result is $\left|0_{dp}\right\rangle$, the respective bit of private key k_j^a and k_j^b is recorded as "0", where j = 1, 2, . . . , n. Conversely, if Alice's or Bob's measurement result is $\left|1_{dp}\right\rangle$, the respective bit of private key k_j^a and k_j^b is recorded as "1". Therefore, Alice and Bob can get their own private keys $K_A = \left\{k_1^a, k_2^a, \ldots, k_n^a\right\}$ and $K_B = \left\{k_1^b, k_2^b, \ldots, k_n^b\right\}$. Subsequently, Alice and Bob, respectively, calculate their modulo 2 summations

$c_j^a = k_j^{ab} \oplus k_j^a \oplus x_j$ and $c_j^b = k_j^{ab} \oplus k_j^b \oplus y_j$, where $j = 1, 2, \ldots, n$. Finally, Alice and Bob send their calculation results $C_A = \{c_1^a, c_2^a, \ldots, c_n^a\}$ and $C_B = \{c_1^b, c_2^b, \ldots, c_n^b\}$ to the TP, respectively.

Step 6: After the TP receives $C_A = \{c_1^a, c_2^a, \ldots, c_n^a\}$ and $C_B = \{c_1^b, c_2^b, \ldots, c_n^b\}$ from Alice and Bob, it performs two Bell measurements on the quantum states of the corresponding positions reflected by Alice and Bob, obtaining the measurement result $C_T = \{k_1^t, k_2^t, \ldots, k_n^t\}$. If the measurement result of TP is $|\Phi^+>_{13}|\Phi^+>_{24}$, $|\Phi^->_{13}|\Phi^->_{24}$, $|\Phi^+>_{13}|\Phi^->_{24}$, $|\Phi^->_{13}|\Phi^+>_{24}$, k_j^t will be "0", where $j = 1, 2, \ldots, n$. Conversely, if the measurement result of TP is $|\Psi^+>_{13}|\Psi^+>_{24}$, $|\Psi^->_{13}|\Psi^->_{24}$, $|\Psi^+>_{13}|\Psi^->_{24}$, $|\Psi^->_{13}|\Psi^+>_{24}$, k_j^t will be "1". Finally, by calculating $r_j = c_j^a \oplus c_j^b \oplus k_j^t$, the TP obtains the summation result $R = \{r_1, r_2, \ldots, r_n\}$, then announces R to Alice and Bob.

4. Security Analysis

In this section, the correctness, security, and privacy of the proposed semi-quantum summation protocol against the collective-dephasing noise will be analyzed.

4.1. Correctness

In this study, the TP can obtain the summation result $R = \{r_1, r_2, \ldots, r_n\}$ by calculating $r_j = c_j^a \oplus c_j^b \oplus k_j^t$, and announce R to Alice and Bob. According to Equations (6)–(9), $k_j^a \oplus k_j^b \oplus k_j^t = 0$ can be deduced. Therefore, $r_j = x_j \oplus y_j$ can be obtained by calculating Equation (10), which means that the proposed protocol can deduce the summation result of both parties correctly, that is, can achieve correctness.

$$\begin{aligned} r_j &= c_j^a \oplus c_j^b \oplus k_j^t = \left(k_j^{ab} \oplus k_j^a \oplus x_j\right) \oplus \left(k_j^{ab} \oplus k_j^b \oplus y_j\right) \oplus k_j^t \\ &= (x_j \oplus y_j) \oplus \left(k_j^a \oplus k_j^b \oplus k_j^t\right) \oplus \left(k_j^{ab} \oplus k_j^{ab}\right) = x_j \oplus y_j \end{aligned} \tag{10}$$

4.2. Security

The main requirement for security is that Alice's and Bob's private binary strings cannot be leaked to an outside eavesdropper, Eve. To steal Alice's or Bob's private binary strings x_j or y_j, Eve must intercept the photons sent by the TP to Alice and Bob in Step 2. Subsequently, Eve performs the measurement and generates the corresponding photons according to the measurement results, and reflects them back to the TP. If Eve can pass the eavesdropping detection in Step 4, Eve can obtain k_j^a and k_j^b. However, for each transmission, Alice, Bob, and the TP have a probability of 0.75 for eavesdropping detections (i.e., Alice chooses SIFT mode while Bob chooses CTRL mode, Alice chooses CTRL mode while Bob chooses SIFT mode, and Alice chooses CTRL mode and Bob chooses CTRL mode). Therefore, if Eve does not know whether Alice and Bob chose the SIFT or the CTRL mode, the probability that Eve can pass the eavesdropping detection is 0.25. Hence, the probability of Eve being discovered is $1 - (0.25)^n$. When the value of n is large enough, the probability of Eve being discovered will converge to 1.

4.3. Privacy

Privacy implies that both Alice's and Bob's private binary strings should be kept secret from the TP. That is, the TP can only calculate $r_j = x_j \oplus y_j$, and there is no way to further obtain the private value of x_j or y_j. Compared with Eve, the TP has a distinct advantage, because the TP can participate in the protocol process and then obtain some useful information. In Step 4, to check the presence of the eavesdroppers, Alice and Bob announce their respective chosen modes, so that the TP can know the choices of Alice and Bob. For detection, the TP performs the eavesdropping detection honestly, therefore Alice and Bob cannot discover whether the TP is lying. In Step 5, after passing the eavesdropping detection, only the result when both Alice and Bob choose the SIFT mode is retained. The

TP uses the Z-basis to measure the photons reflected by Alice and Bob under the SIFT mode so that it can obtain k_j^a and k_j^b. However, the TP still has no way to know the private values x_j or y_j, because Alice and Bob calculate their modulo 2 summations $c_j^a = k_j^{ab} \bigoplus k_j^a \bigoplus x_j$ and $c_j^b = k_j^{ab} \bigoplus k_j^b \bigoplus y_j$ separately. Therefore, without k_j^{ab}, the TP cannot deduce the private value of x_j or y_j.

5. Efficiency Analysis

Table 2 compares the important functions in Ye et al.'s [36] semi-quantum summation protocol with the semi-quantum summation protocol proposed in this study. Consider the quantum efficiency calculation equation of the quantum cryptography protocol [55–57] is $\eta = \frac{c}{q}$, where c is the number of bits of the last shared secret information, and q is the number of qubits generated in the communication protocol. In general, it is assumed that during the eavesdropping detection step of the communication protocol, half of the transmitted qubits are used to detect the presence of eavesdroppers.

Table 2. Performance comparison of Ye et al.'s semi-quantum summation protocol and the proposed protocol.

	Ye et al.'s [36] Semi-Quantum Summation Protocol	**Proposed Protocol**
Quantum efficiency	0.015625	0.0625
Security issues owing to information leakage	Exists	Not Exists

In Ye et al.'s semi-quantum summation protocol against the collective-dephasing noise, the TP must generate $2n$ logical single photons (i.e., $4n$ qubits), and each group of logical single photons can be used to calculate one classical private bit. To prevent eavesdropping, the TP randomly chooses half of the photons in the photon sequences $S\prime_1$ and $S\prime_2$, to perform eavesdropping detection. After eavesdropping detection, Alice and Bob ask the TP to perform two Bell basis measurements on the remaining half of the photon sequences and announce the measurement results. After the TP announces all the measurement results, Alice and Bob randomly choose half of the measurement results to perform the TP honesty check. After passing the honesty check of TP, Alice and Bob announce the chosen mode of the remaining photon sequences. Only when Alice and Bob both choose the SIFT mode can they be used to make secret keys, and its probability is 0.25. Therefore, the quantum efficiency of Ye et al.'s semi-quantum summation protocol against the collective-dephasing noise is $\frac{n}{4n} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{4} = 0.015625$.

In the semi-quantum summation protocol against the collective-dephasing noise proposed in this study, each logical Bell state (i.e., $4n$ qubits) can be used to calculate one classical bit of secret information. Only when Alice and Bob both choose the SHIF mode can they be used to calculate the summation, and the probability of its occurrence is 0.25. Therefore, the quantum efficiency of the semi-quantum summation protocol against the collective-dephasing noise proposed in this study is $\frac{n}{4n} \times \frac{1}{4} = 0.0625$. It is evident that the quantum efficiency of the semi-quantum summation protocol against the collective-dephasing noise proposed in this study is four times higher than that of Ye et al.'s semi-quantum summation protocol. The proposed protocol can effectively improve the quantum utilization rate with no information leakage.

6. Conclusions

This study proved that Ye et al.'s semi-quantum summation protocol against the collective-dephasing noise has security issues owing to information leakage. This study also proposed an efficient and safe semi-quantum summation protocol against the collective-dephasing noise. In Ye et al.'s semi-quantum summation protocol against the collective-

dephasing noise, the dishonest participant is allowed to not announce the calculation results first, thereby obtaining the calculation results of the other party, and calculating the summation of the two parties. Furthermore, eavesdroppers can obtain some secret information during the communication process without performing any active attack. To solve these security issues, this study proposes a new semi-quantum summation protocol against the collective-dephasing noise. The semi-quantum summation protocol against the collective-dephasing noise proposed in this study is free from information leakage, also in addition to being resistant to other well-known attack modes. In addition, the quantum efficiency of the semi-quantum summation protocol against the collective-dephasing noise proposed in this study is four times higher than that of Ye et al.'s semi-quantum summation protocol. Therefore, the proposed method performs safely and improves the quantum efficiency. Although the proposed semi-quantum summation protocol can only resist the interference of the collective-dephasing noise, further research will be conducted to build a semi-quantum summation protocol that can resist the collective-rotation noise. However, in order to counteract the collective rotation noise, at least two-particle entangled states must be generated. In the assumption of a semi-quantum environment, a classical participant can only generate photons in the Z-basis. Therefore, in the measure-resend environment, the classical participants cannot generate entangled states, and thus cannot resist the interference of the collective-rotation noise. This is worth further investigation.

Author Contributions: Conceptualization, C.-W.Y. and C.-W.T.; methodology, C.-W.Y., J.L. and C.-W.T.; investigation, C.-W.T. and C.-A.C.; formal analysis, C.-W.Y. and C.-A.C.; writing—original draft, C.-W.Y. and J.L.; writing—review and editing, C.-W.Y. and J.L.; project administration, C.-W.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially supported by the National Science and Technology Council, Taiwan, R.O.C. (Grant Nos. NSTC 111-2221-E-039-014, NSTC 111-2221-E-005-048, NSTC 111-2634-F-005-001, NSTC 111-2218-E-005-007-MBK, NSTC 111-2221-E-143-006-MY2, and NSTC 111-2221-E-025-010) and China Medical University, Taiwan (Grant No. CMU111-S-28).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, Los Alamitos, CA, USA, 20–22 November 1994; pp. 124–134.
2. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332. [CrossRef]
3. Jozsa, R. Quantum factoring, discrete logarithms, and the hidden subgroup problem. *Comput. Sci. Eng.* **2001**, *3*, 34–43. [CrossRef]
4. Proos, J.; Zalka, C. Shor's discrete logarithm quantum algorithm for elliptic curves. *Quantum Inf. Comput.* **2003**, *3*, 317–344. [CrossRef]
5. Heinrich, S. Quantum Summation with an Application to Integration. *J. Complex.* **2002**, *18*, 1–50. [CrossRef]
6. Heinrich, S.; Novak, E. On a problem in quantum summation. *J. Complex.* **2003**, *19*, 1–18. [CrossRef]
7. 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.* **2010**, *49*, 2793–2804. [CrossRef]
8. 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.* **2014**, *53*, 933–941. [CrossRef]
9. Zhang, C.; Sun, Z.-W.; Huang, X.; Long, D.-Y. Three-party quantum summation without a trusted third party. *Int. J. Quant. Inf.* **2015**, *13*, 1550011. [CrossRef]
10. Shi, R.-H.; Mu, Y.; Zhong, H.; Cui, J.; Zhang, S. Secure Multiparty Quantum Computation for Summation and Multiplication. *Sci. Rep.* **2016**, *6*, 19655. [CrossRef]
11. Shi, R.-H.; Zhang, S. Quantum solution to a class of two-party private summation problems. *Quantum Inf. Process.* **2017**, *16*, 225. [CrossRef]
12. Zhang, C.; Situ, H.; Huang, Q.; Yang, P. Multi-party quantum summation without a trusted third party based on single particles. *Int. J. Quant. Inf.* **2017**, *15*, 1750010. [CrossRef]

13. 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.* **2017**, *56*, 2783–2791. [CrossRef]
14. Yang, H.-Y.; Ye, T.-Y. Secure multi-party quantum summation based on quantum Fourier transform. *Quantum Inf. Process.* **2018**, *17*, 129. [CrossRef]
15. Ji, Z.; Zhang, H.; Wang, H.; Wu, F.; Jia, J.; Wu, W. Quantum protocols for secure multi-party summation. *Quantum Inf. Process.* **2019**, *18*, 168. [CrossRef]
16. 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.* **2019**, *58*, 2213–2217. [CrossRef]
17. 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.* **2021**, *20*, 249. [CrossRef]
18. Lo, H.-K. Insecurity of quantum secure computations. *Phys. Rev. A* **1997**, *56*, 1154–1162. [CrossRef]
19. Chau, H.F. Quantum-classical complexity-security tradeoff in secure multiparty computations. *Phys. Rev. A* **2000**, *61*, 032308. [CrossRef]
20. Crépeau, C.; Gottesman, D.; Smith, A. Secure multi-party quantum computation. In Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing, Montreal, QC, Canada, 19–21 May 2002; pp. 643–652.
21. Ben-Or, M.; Crepeau, C.; Gottesman, D.; Hassidim, A.; Smith, A. Secure Multiparty Quantum Computation with (Only) a Strict Honest Majority. In Proceedings of the 2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06), Berkeley, CA, USA, 21–24 October 2006; pp. 249–260.
22. Lipinska, V.; Ribeiro, J.; Wehner, S. Secure multiparty quantum computation with few qubits. *Phys. Rev. A* **2020**, *102*, 022405. [CrossRef]
23. Ji, Z.; Zhang, H.; Fan, P. Two-party quantum private comparison protocol with maximally entangled seven-qubit state. *Mod. Phys. Lett. A* **2019**, *34*, 1950229. [CrossRef]
24. Xu, L.; Zhao, Z.-W. High-capacity quantum private comparison protocol with two-photon hyperentangled Bell states in multiple-degree of freedom. *Eur. Phys. J. D* **2019**, *73*, 58. [CrossRef]
25. Lang, Y.-F. Quantum Private Comparison Using Single Bell State. *Int. J. Theor. Phys.* **2021**, *60*, 4030–4036. [CrossRef]
26. Lang, Y.-F. Fast Quantum Private Comparison Without Keys and Entanglement. *Int. J. Theor. Phys.* **2022**, *61*, 45. [CrossRef]
27. Tsai, C.-W.; Lin, J.; Chao, H.-C.; Yang, C.-W. Cryptanalysis and improvement on two party quantum private comparison based on seven-qubit and eight-qubit states. *Mod. Phys. Lett. A* **2022**, *37*, 2250120. [CrossRef]
28. Li, Y.; Zeng, G. Quantum anonymous voting systems based on entangled state. *Opt. Rev.* **2008**, *15*, 219–223. [CrossRef]
29. Wang, Q.; Yu, C.; Gao, F.; Qi, H.; Wen, Q. Self-tallying quantum anonymous voting. *Phys. Rev. A* **2016**, *94*, 022333. [CrossRef]
30. Bao, N.; Yunger Halpern, N. Quantum voting and violation of Arrow's impossibility theorem. *Phys. Rev. A* **2017**, *95*, 062306. [CrossRef]
31. Xue, P.; Zhang, X. A simple quantum voting scheme with multi-qubit entanglement. *Sci. Rep.* **2017**, *7*, 7586. [CrossRef] [PubMed]
32. Boyer, M.; Kenigsberg, D.; Mor, T. Quantum Key Distribution with Classical Bob. *Phys. Rev. Lett.* **2007**, *99*, 140501. [CrossRef]
33. Zhang, C.; Huang, Q.; Long, Y.; Sun, Z. Secure Three-Party Semi-quantum Summation Using Single Photons. *Int. J. Theor. Phys.* **2021**, *60*, 3478–3487. [CrossRef]
34. Hu, J.-L.; Ye, T.-Y. Three-Party Secure Semiquantum Summation without Entanglement Among Quantum User and Classical Users. *Int. J. Theor. Phys.* **2022**, *61*, 170. [CrossRef]
35. Pan, H.-M. Cryptanalysis and Improvement of Three-Party Semi-Quantum Summation Using Single Photons. *Int. J. Theor. Phys.* **2022**, *61*, 103. [CrossRef]
36. Ye, T.-Y.; Xu, T.-J.; Geng, M.-J.; Chen, Y. Two-party secure semiquantum summation against the collective-dephasing noise. *Quantum Inf. Process.* **2022**, *21*, 118. [CrossRef]
37. Zhang, M.-H.; Cao, Z.-W.; Peng, J.-Y. Fault-tolerant asymmetric quantum dialogue protocols against collective noise. *Quantum Inf. Process.* **2018**, *17*, 204. [CrossRef]
38. Lang, Y.-F. Fault Tolerant Authenticated Quantum Dialogue Based on Logical Qubits and Controlled-Not Operations. *Int. J. Theor. Phys.* **2019**, *58*, 531–542. [CrossRef]
39. Wang, S.-S.; Jiang, D.-H.; Xu, G.-B.; Zhang, Y.-H.; Liang, X.-Q. Quantum key agreement with Bell states and Cluster states under collective noise channels. *Quantum Inf. Process.* **2019**, *18*, 190. [CrossRef]
40. Yang, Y.-G.; Gao, S.; Li, D.; Zhou, Y.-H.; Shi, W.-M. Three-party quantum secret sharing against collective noise. *Quantum Inf. Process.* **2019**, *18*, 215. [CrossRef]
41. Zhang, M.-H.; Cao, Z.-W.; Peng, J.-Y.; Chai, G. Fault tolerant quantum dialogue protocol over a collective noise channel. *Eur. Phys. J. D* **2019**, *73*, 57. [CrossRef]
42. Yang, C.-W.; Tsai, C.-W.; Hwang, T. Fault tolerant two-step quantum secure direct communication protocol against collective noises. *Sci. China Phys.* **2011**, *54*, 496–501. [CrossRef]
43. Yang, Y.-G.; Xia, J.; Jia, X.; Zhang, H. Comment on quantum private comparison protocols with a semi-honest third party. *Quantum Inf. Process.* **2013**, *12*, 877–885. [CrossRef]
44. Zhang, M.-H.; Li, H.-F.; Peng, J.-Y.; Feng, X.-Y. Fault-tolerant Semiquantum key Distribution Over a Collective-dephasing Noise Channel. *Int. J. Theor. Phys.* **2017**, *56*, 2659–2670. [CrossRef]

45. Lin, P.-H.; Hwang, T.; Tsai, C.-W. Efficient semi-quantum private comparison using single photons. *Quantum Inf. Process.* **2019**, *18*, 207. [CrossRef]
46. Krawec, W.O. Mediated semiquantum key distribution. *Phys. Rev. A* **2015**, *91*, 032323. [CrossRef]
47. Liu, Z.-R.; Hwang, T. Mediated Semi-Quantum Key Distribution without Invoking Quantum Measurement. *Ann. Phys.* **2018**, *530*, 1700206. [CrossRef]
48. Lin, P.-H.; Tsai, C.-W.; Hwang, T. Mediated Semi-Quantum Key Distribution Using Single Photons. *Ann. Phys.* **2019**, *531*, 1800347. [CrossRef]
49. Massa, F.; Yadav, P.; Moqanaki, A.; Krawec, W.O.; Mateus, P.; Paunković, N.; Souto, A.; Walther, P. Experimental Quantum Cryptography with Classical Users. *arXiv* **2019**, arXiv:1908.01780.
50. Tsai, C.-W.; Yang, C.-W.; Lee, N.-Y. Lightweight mediated semi-quantum key distribution protocol. *Mod. Phys. Lett. A* **2019**, *34*, 1950281. [CrossRef]
51. Lu, Y.-C.; Tsai, C.-W.; Hwang, T. Collective Attack and Improvement on "Mediated Semi-Quantum Key Distribution Using Single Photons". *Ann. Phys.* **2020**, *532*, 1900493. [CrossRef]
52. Chen, L.; Li, Q.; Liu, C.; Peng, Y.; Yu, F. Efficient mediated semi-quantum key distribution. *Phys. A* **2021**, *582*, 126265. [CrossRef]
53. Tsai, C.-W.; Yang, C.-W. Lightweight mediated semi-quantum key distribution protocol with a dishonest third party based on Bell states. *Sci. Rep.* **2021**, *11*, 23222. [CrossRef] [PubMed]
54. Mutreja, S.; Krawec, W.O. Improved semi-quantum key distribution with two almost-classical users. *Quantum Inf. Process.* **2022**, *21*, 319. [CrossRef]
55. Yang, C.-W.; Hwang, T. Improved QSDC Protocol over a Collective-Dephasing Noise Channel. *Int. J. Theor. Phys.* **2012**, *51*, 3941–3950. [CrossRef]
56. Yang, C.-W.; Hwang, T. Quantum dialogue protocols immune to collective noise. *Quantum Inf. Process.* **2013**, *12*, 2131–2142. [CrossRef]
57. Yang, C.-W.; Hwang, T.; Luo, Y.-P. Enhancement on "Quantum Blind Signature Based on Two-State Vector Formalism". *Quantum Inf. Process.* **2013**, *12*, 109–117. [CrossRef]