entropy

MDPI

Article

Single-State Multi-Party Quantum Key Agreement with Single-Particle Measurement

Hao Yang [1], Dunbo Cai [2], Ling Qian [2], Runqing Zhang [2], Songfeng Lu [1,3] and Chengfu Sun [4,*]

[1] Hubei Key Laboratory of Distributed System Security, Hubei Engineering Research Center on Big Data Security, School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, China; d202180586@hust.edu.cn (H.Y.); lusongfeng@hust.edu.cn (S.L.)
[2] Center for Technology Research & Innovation, China Mobile (Suzhou) Software Technology Co., Ltd., Suzhou 215163, China; caidunbo@cmss.chinamobile.com (D.C.); qianling@cmss.chinamobile.com (L.Q.); zhangrunqing@cmss.chinamobile.com (R.Z.)
[3] Shenzhen Huazhong University of Science and Technology Research Institute, Shenzhen 518063, China
[4] School of Computer Science and Engineering, Huaiyin Institute of Technology, Huai'an 223003, China
* Correspondence: ajason509@hyit.edu.cn

Abstract: In this study, we propose a single-state multi-party quantum key agreement (MQKA) protocol with single-particle measurement. Firstly, a single-state three-party quantum key agreement protocol with single-particle measurement is introduced, followed by a security analysis that validated its capability to resist potential internal and external attacks. Furthermore, we utilize multi-particle entangled states to present a multi-party version of the single-state multi-party quantum key agreement with single-particle measurement. In comparison to previous MQKA protocols, our approach presents the following advantages: it employs one kind of multi-particle entangled state as the quantum resource; eliminates the need for entanglement swapping techniques, unitary operations, or pre-shared keys between participants; uses only the X measurement basis and Z measurement basis; transmits fewer qubits; consumes fewer qubits; and has higher qubit efficiency.

Keywords: quantum cryptography; quantum entangled states; quantum key agreement

check for updates

Academic Editor: Rosario Lo Franco

Received: 22 January 2025
Revised: 16 March 2025
Accepted: 17 March 2025
Published: 10 April 2025

Citation: Yang, H.; Cai, D.; Qian, L.; Zhang, R.; Lu, S.; Sun, C. Single-State Multi-Party Quantum Key Agreement with Single-Particle Measurement. *Entropy* **2025**, *27*, 405. https://doi.org/10.3390/e27040405

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Quantum cryptography, with its theoretically unconditional security feature, has gradually become an important research area in the field of cryptography. Unlike classical cryptography, the security of quantum cryptography is based on the quantum no-cloning theorem and Heisenberg's uncertainty principle. As a result, it has attracted significant attention from researchers. Quantum cryptography includes several research areas, such as quantum key distribution (QKD) [1–4], quantum secret sharing (QSS) [5–7], quantum secure direct communication (QSDC) [8–10], quantum private query (QPQ) [11–14], and quantum key agreement (QKA). Among these, quantum key agreement (QKA) requires each participant to equally contribute to the generation of the negotiated key, ensuring that any non-trivial subset of participants cannot independently determine the key. In 2004, Zhou et al. [15] innovatively applied quantum teleportation to key agreement, proposing the first quantum key agreement (QKA) protocol. However, Tsai et al. [16] identified a significant flaw in Zhou's protocol where a participant could independently determine the negotiated key. Subsequently, Hsueh et al. [17] implemented a QKA protocol using maximally entangled states. Nevertheless, Hsueh et al.'s protocol was vulnerable to controlled-NOT attacks [18]. In 2011, Chong et al. [19] enhanced the security of Hsueh et al.'s protocol. In 2013, Shi et al. [20] extended the two-party QKA to be multi-party and

proposed the first multi-party QKA protocol, which utilizes the Bell state as the quantum resource state and employs entanglement swapping technology. On this basis, Sun et al. [21] proposed an efficient quantum key agreement protocol based on commutative encryption. Wang et al. [22] proposed a multi-party semiquantum key agreement without entanglement. In addition to these efforts, numerous QKA protocols have been proposed, such as the schemes based on a single particle [23–26], the Bell state [27–32], and a multi-particle entangled state [33–40].

Resently, Xu et al. [41] proposed a single-state multi-party semiquantum key agreement protocol based on multi-particle entangled states which offers several key advantages: it uses only one kind of multi-particle entangled state as the initial quantum resource; it does not require pre-shared keys between different parties; and it eliminates the need for unitary operations or quantum entanglement swapping. Subsequently, Yang et al. [42] proposed an efficient single-state multi-party quantum key agreement which retains most of the advantages of Xu et al.'s scheme while achieving significant improvements in the number of quantum state transmissions, the number of qubits consumed, and qubit efficiency.

In this paper, a single-state three-party quantum key agreement protocol utilizing single-particle measurements is proposed. We conduct a detailed analysis demonstrating that our scheme can resist potential internal and external attacks. Furthermore, we extend the proposed single-state three-party quantum key agreement protocol to be N-party by using N-particle entangled states instead of three-particle entangled states as the quantum resource states. Compared to previous multi-party QKA schemes, our protocol retains most of the advantages presented in references [41,42] while only requiring the use of the X measurement basis and Z measurement basis. Additionally, our protocol further reduces the number of qubits transmitted and consumed, and enhances qubit efficiency.

The rest of the paper is organized as follows: In Section 2, we describe the single-state three-party quantum key agreement protocol in detail. Section 3 provides a security analysis of the protocol. In Section 4, we extend the proposed single-state three-party quantum key agreement protocol to be N-party. Section 5 discusses the performance of our scheme. Section 6 provides a conclusion.

2. The Proposed Single-State Three-Party Quantum Key Agreement with Single-Particle Measurement

Suppose P_1, P_2, and P_3 seek to establish a private key over a quantum channel, ensuring that each participant contributes equally to the generation of the key and that the key cannot be fully determined by any non-trivial subset of them. In the negotiation phase, the utilization of a hash function outputting m bits is necessary.

Step 1: P_1, P_2, and P_3 randomly generate the CHECK keys

$$\bar{K}_{P_1} = \left\{ \bar{K}_{P_1}^1, \bar{K}_{P_1}^2, \ldots, \bar{K}_{P_1}^l \right\}, \tag{1}$$

$$\bar{K}_{P_2} = \left\{ \bar{K}_{P_2}^1, \bar{K}_{P_2}^2, \ldots, \bar{K}_{P_2}^l \right\}, \tag{2}$$

$$\bar{K}_{P_3} = \left\{ \bar{K}_{P_3}^1, \bar{K}_{P_3}^2, \ldots, \bar{K}_{P_3}^l \right\}, \tag{3}$$

and the INFO keys

$$K_{P_1} = \left\{ K_{P_1}^1, K_{P_1}^2, \ldots, K_{P_1}^n \right\}, \tag{4}$$

$$K_{P_2} = \left\{ K_{P_2}^1, K_{P_2}^2, \ldots, K_{P_2}^n \right\}, \tag{5}$$

$$K_{P_3} = \left\{K_{P_3}^1, K_{P_3}^2, \ldots, K_{P_3}^n\right\}. \tag{6}$$

Here, l represents the number of the CHECK particles, n represents the length of the negotiated key, and $\bar{K}_{P_1}, \bar{K}_{P_2}, \bar{K}_{P_3}, K_{P_1}, K_{P_2}, K_{P_3} \in \{0,1\}$. They calculate the hash values $H(K_{P_1}), H(K_{P_2}), H(K_{P_3})$ corresponding to the keys $K_{P_1}, K_{P_2}, K_{P_3}$ and announce the values.

Step 2: P_1 prepares $l+n$ three-particle GHZ states $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. For each GHZ state, P_1 keeps the first particle, and sends the second particle to P_2 and the third particle to P_3. We denote the first particle sequence as S_{P_1}, the second particle sequence as S_{P_2}, and the third particle sequence as S_{P_3} as follows:

$$S_{P_1} = \left\{S_{P_1}^1, S_{P_1}^2, \ldots, S_{P_1}^{l+n}\right\}, \tag{7}$$

$$S_{P_2} = \left\{S_{P_2}^1, S_{P_2}^2, \ldots, S_{P_2}^{l+n}\right\}, \tag{8}$$

$$S_{P_3} = \left\{S_{P_3}^1, S_{P_3}^2, \ldots, S_{P_3}^{l+n}\right\}. \tag{9}$$

Step 3: After P_2 receives S_{P_2} and P_3 receives S_{P_3}, P_1 randomly selects l particles as the CHECK particles, and informs P_2, P_3 of the positions of the CHECK particles. Here, the CHECK particles held by P_1, P_2, P_3 are denoted as $U_{P_1}, U_{P_2}, U_{P_3}$, respectively, as follows:

$$U_{P_1} = \left\{U_{P_1}^1, U_{P_1}^2, \ldots, U_{P_1}^l\right\}, \tag{10}$$

$$U_{P_2} = \left\{U_{P_2}^1, U_{P_2}^2, \ldots, U_{P_2}^l\right\}, \tag{11}$$

$$U_{P_3} = \left\{U_{P_3}^1, U_{P_3}^2, \ldots, U_{P_3}^l\right\}. \tag{12}$$

Then, P_1, P_2, P_3 announce the CHECK keys $\bar{K}_{P_1}, \bar{K}_{P_2}, \bar{K}_{P_3}$. They calculate

$$\bar{K} = \bar{K}_{P_1} \oplus \bar{K}_{P_2} \oplus \bar{K}_{P_3}. \tag{13}$$

In this equation, $\bar{K} = \left\{\bar{K}^1, \bar{K}^2, \ldots, \bar{K}^l\right\}$. For the q-th CHECK particle, when the value of $\bar{K}^q$ is 0, P_i uses basis Z to measure the particle $U_{P_i}^q$ and publishes the results, where $q \in \{1,2,\ldots,l\}$. When the value of $\bar{K}^q$ is 1, P_i uses basis X to measure the particle $U_{P_i}^q$ and publishes the results, where $q \in \{1,2,\ldots,l\}$. Suppose that the measurement results in basis Z are $U_{zP_i}^q = \{+1,-1\}$, and in basis X are $U_{xP_i}^q = \{+1,-1\}$. According to the entanglement properties of the three-particle GHZ state and Equation (14),

$$\begin{array}{l} |GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \\ = \frac{1}{\sqrt{4}}(|+++\rangle + |+--\rangle + |-+-\rangle + |--+\rangle) \end{array}. \tag{14}$$

P_i can check the correctness of the measurement results. When the chosen basis is Z, the measurement results must satisfy $U_{zP_1}^q = U_{zP_2}^q = U_{zP_3}^q$. When the chosen basis is X, the measurement results must satisfy $\Pi_{i=1}^3 U_{xP_i}^q = 1$. If the error exceeds the threshold, the protocol aborts. The remaining particles serve as INFO particles $V_{P_i} = \left\{V_{P_i}^1, V_{P_i}^2, \ldots, V_{P_i}^n\right\}$. P_i measures the particles with basis Z.

Step 4: The measurement results are represented by V_{zP_i}. If the measurement result is $|0\rangle$, its value is taken as 0; if the measurement result is $|1\rangle$, its value is taken as 1. According to the entanglement properties of the three-particle GHZ state, we can obtain

$V_{zP_1}=V_{zP_2}=V_{zP_3}$. P_1 calculates $E_{P_1} = V_{zP_1} \oplus K_{P_1}$ and sends it to P_2, P_3. P_2 calculates $E_{P_2} = V_{zP_2} \oplus K_{P_2}$ and sends it to P_1, P_3. P_3 calculates $E_{P_3} = V_{zP_3} \oplus K_{P_3}$ and sends it to P_1, P_2.

Step 5: P_1 calculates $H(E_{P_2} \oplus V_{zP_1})$, $H(E_{P_3} \oplus V_{zP_1})$. If $H(E_{P_2} \oplus V_{zP_1}) = H(K_{P_2})$ and $H(E_{P_3} \oplus V_{zP_1}) = H(K_{P_3})$, P_1 will infer the final negotiated key

$$K = K_{P_1} \oplus (E_{P_2} \oplus V_{zP_1}) \oplus (E_{P_3} \oplus V_{zP_1}). \tag{15}$$

P_2 calculates $H(E_{P_1} \oplus V_{zP_2})$, $H(E_{P_3} \oplus V_{zP_2})$. If $H(E_{P_1} \oplus V_{zP_2}) = H(K_{P_1})$ and $H(E_{P_3} \oplus V_{zP_2}) = H(K_{P_3})$, P_2 will infer the final negotiated key

$$K = K_{P_2} \oplus (E_{P_1} \oplus V_{zP_2}) \oplus (E_{P_3} \oplus V_{zP_2}). \tag{16}$$

P_3 calculates $H(E_{P_1} \oplus V_{zP_3})$, $H(E_{P_2} \oplus V_{zP_3})$. If $H(E_{P_1} \oplus V_{zP_3}) = H(K_{P_1})$ and $H(E_{P_2} \oplus V_{zP_3}) = H(K_{P_2})$, P_3 will infer the final negotiated key

$$K = K_{P_3} \oplus (E_{P_1} \oplus V_{zP_3}) \oplus (E_{P_2} \oplus V_{zP_3}). \tag{17}$$

As shown in Figure 1, the flowchart depicts the mechanism of the proposed MQKA protocol.

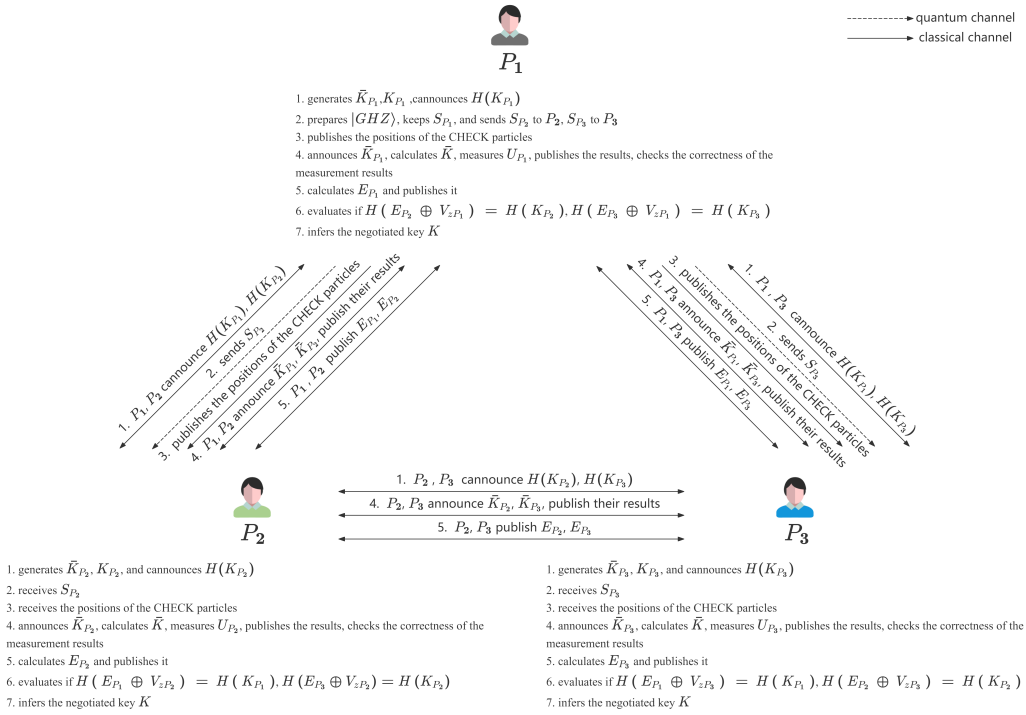


Figure 1. The flowchart depicts the mechanism of the proposed protocol.

3. Security Analysis

This section will discuss the security of the proposed protocol. Without loss of generality, we analyze the security of the proposed three-party QKA protocol. The security analysis encompasses both internal attacks and external attacks.

3.1. External Attack

In the proposed three-party protocol, in order to obtain the negotiated key, an external attacker may launch typical attacks during the transmission of quantum states, including the Trojan horse attack, the intercept–resend attack, the entangle–measure attack, and the measure–resend attack.

3.1.1. The Trojan Horse Attack

In our scheme, since each particle is transmitted only once, our three-party QKA protocol is immune to the delay-photon Trojan horse attack [43] and the invisible eavesdropping Trojan horse attack [44].

3.1.2. The Intercept–Resend Attack

The external attacker may intercept the particles P_1 transmitted and resend the fake states to P_2, P_3. Without loss of generality, suppose that Eve intercepts the particles S_{P_3} and sends the fake particles to P_3. Taking the q-th fake CHECK particle $\tilde{U}^q_{P_3}(|0\rangle)$ as an example, the q-th system state can be described as

$$\begin{aligned}\tilde{\Psi}&=\tfrac{1}{\sqrt{2}}(|00\rangle+|11\rangle)|0\rangle\\&=\tfrac{1}{\sqrt{4}}(|+++\rangle+|++-\rangle+|--+\rangle+|---\rangle)\end{aligned}\ . \tag{18}$$

Firstly, we consider the scenario where the measurement basis is Z. When the measurement results of $U^q_{P_1}, U^q_{P_2}, \tilde{U}^q_{P_3}$ are $|000\rangle$, we can obtain $U^q_{zP_1}=U^q_{zP_2}=\tilde{U}^q_{zP_3}$. Eve is capable of evading eavesdropping detection.

When the measurement results of $U^q_{P_1}, U^q_{P_2}, \tilde{U}^q_{P_3}$ are $|110\rangle$, we can obtain $U^q_{zP_1}=U^q_{zP_2}\neq \tilde{U}^q_{zP_3}$. Eve can be detected by the eavesdropping detection.

Secondly, we consider the scenario where the measurement basis is X. When the measurement results of $U^q_{P_1}, U^q_{P_2}, \tilde{U}^q_{P_3}$ in $|+++\rangle$ or $|--+\rangle$, we can obtain $U^q_{xP_1}\cdot U^q_{xP_2}\cdot \tilde{U}^q_{xP_3}=1$. Eve is capable of evading eavesdropping detection.

When the measurement results of $U^q_{P_1}, U^q_{P_2}, \tilde{U}^q_{P_3}$ in $|++-\rangle$ or $|---\rangle$, we can obtain $U^q_{xP_1}\cdot U^q_{xP_2}\cdot \tilde{U}^q_{xP_3}=-1$. Eve is unable to evade eavesdropping detection.

Therefore, for each CHECK particle, Eve is capable of evading eavesdropping detection with the probability of

$$\tfrac{1}{2}\times\tfrac{1}{2}+\tfrac{1}{2}\times\left(\tfrac{1}{4}+\tfrac{1}{4}\right)=\tfrac{1}{2}\ . \tag{19}$$

For all l CHECK particles, Eve can be detected with the probability of $1-\left(\frac{1}{2}\right)^l$.

3.1.3. The Entangle–Measure Attack

The external attacker may perform the entangle–measure attack. Without loss of generality, suppose that Eve intercepts the particles P_1 transmitted to P_2 (P_3), and performs unitary operation U_E on the intercepted particles. If this attack does not introduce any errors, the system state of Eve's probe should be independent of the measurement results of $S_{P_1}, S_{P_2}, S_{P_3}$. The effect of U_E on $|0\rangle$ and $|1\rangle$ can be described as

$$U_E(|0\rangle|E\rangle)=\varepsilon_{00}|0\rangle|e_{00}\rangle+\varepsilon_{01}|1\rangle|e_{01}\rangle\ , \tag{20}$$

$$U_E(|1\rangle|E\rangle)=\varepsilon_{10}|0\rangle|e_{10}\rangle+\varepsilon_{11}|1\rangle|e_{11}\rangle\ . \tag{21}$$

In this equation, $|e_{00}\rangle$, $|e_{01}\rangle$, $|e_{10}\rangle$, and $|e_{11}\rangle$ are the probe state of Eve on U_E, and $|\varepsilon_{00}|^2+|\varepsilon_{01}|^2=1$, $|\varepsilon_{10}|^2+|\varepsilon_{11}|^2=1$. The global state of the system can be described as

$$
\begin{aligned}
&U_E\left(|GHZ\rangle_{P_1P_2P_3}|E\rangle\right)\\
&=U_E\left(\tfrac{1}{\sqrt{2}}\left(|0\rangle_{P_1}|0\rangle_{P_2}|0\rangle_{P_3}+|1\rangle_{P_1}|1\rangle_{P_2}|1\rangle_{P_3}\right)|E\rangle\right)\\
&=\tfrac{1}{\sqrt{2}}\left\{\begin{array}{l}|0\rangle_{P_1}\left(\varepsilon_{00}|0\rangle_{P_2}|e_{00}\rangle+\varepsilon_{01}|1\rangle_{P_2}|e_{01}\rangle\right)\left(\varepsilon_{00}|0\rangle_{P_3}|e_{00}\rangle+\varepsilon_{01}|1\rangle_{P_3}|e_{01}\rangle\right)+\\ |1\rangle_{P_1}\left(\varepsilon_{10}|0\rangle_{P_2}|e_{10}\rangle+\varepsilon_{11}|1\rangle_{P_2}|e_{11}\rangle\right)\left(\varepsilon_{10}|0\rangle_{P_2}|e_{10}\rangle+\varepsilon_{11}|1\rangle_{P_2}|e_{11}\rangle\right)+\end{array}\right\},\\
&=\tfrac{1}{\sqrt{2}}\left\{\begin{array}{l}\varepsilon_{00}\varepsilon_{00}|0\rangle_{P_1}|0\rangle_{P_2}|0\rangle_{P_3}|e_{00}\rangle|e_{00}\rangle+\varepsilon_{00}\varepsilon_{01}|0\rangle_{P_1}|0\rangle_{P_2}|1\rangle_{P_3}|e_{00}\rangle|e_{01}\rangle+\\ \varepsilon_{01}\varepsilon_{00}|0\rangle_{P_1}|1\rangle_{P_2}|0\rangle_{P_3}|e_{01}\rangle|e_{00}\rangle+\varepsilon_{01}\varepsilon_{01}|0\rangle_{P_1}|1\rangle_{P_2}|1\rangle_{P_3}|e_{01}\rangle|e_{01}\rangle+\\ \varepsilon_{10}\varepsilon_{10}|1\rangle_{P_1}|0\rangle_{P_2}|0\rangle_{P_3}|e_{10}\rangle|e_{10}\rangle+\varepsilon_{10}\varepsilon_{11}|1\rangle_{P_1}|0\rangle_{P_2}|1\rangle_{P_3}|e_{10}\rangle|e_{11}\rangle+\\ \varepsilon_{11}\varepsilon_{10}|1\rangle_{P_1}|1\rangle_{P_2}|0\rangle_{P_3}|e_{11}\rangle|e_{10}\rangle+\varepsilon_{11}\varepsilon_{11}|1\rangle_{P_1}|1\rangle_{P_2}|1\rangle_{P_3}|e_{11}\rangle|e_{11}\rangle\end{array}\right\}
\end{aligned}
\tag{22}
$$

In this equation, the subscripts P_1, P_2, and P_3 denote the particles from S_{P_1}, S_{P_2}, and S_{P_3}, respectively. If Eve does not introduce any errors during the eavesdropping check by participants, the measurement results of P_1, P_2, and P_3 should be the same. Thereby, Eve's attack U_E should be satisfied with the conditions

$$
\begin{aligned}
&U_E\left(|GHZ\rangle_{P_1P_2P_3}|E\rangle\right)\\
&=\tfrac{1}{\sqrt{2}}\left(\varepsilon_{00}\varepsilon_{00}|0\rangle_{P_1}|0\rangle_{P_2}|0\rangle_{P_3}|e_{00}\rangle|e_{00}\rangle+\varepsilon_{11}\varepsilon_{11}|1\rangle_{P_1}|1\rangle_{P_2}|1\rangle_{P_3}|e_{11}\rangle|e_{11}\rangle\right)
\end{aligned}
\tag{23}
$$

Based on Equation (22), we can infer

$$
\begin{array}{l}\varepsilon_{00}\varepsilon_{01}|e_{00}\rangle|e_{01}\rangle+\varepsilon_{01}\varepsilon_{00}|e_{01}\rangle|e_{00}\rangle+\varepsilon_{01}\varepsilon_{01}|e_{01}\rangle|e_{01}\rangle+\\ \varepsilon_{10}\varepsilon_{10}|e_{10}\rangle|e_{10}\rangle+\varepsilon_{10}\varepsilon_{11}|e_{10}\rangle|e_{11}\rangle+\varepsilon_{11}\varepsilon_{10}|e_{11}\rangle|e_{10}\rangle=0\end{array}\ . \tag{24}
$$

Here, 0 represents a column zero vector. Then, we can obtain

$$
\varepsilon_{00}\varepsilon_{01}+\varepsilon_{01}\varepsilon_{00}+\varepsilon_{01}\varepsilon_{01}+\varepsilon_{10}\varepsilon_{10}+\varepsilon_{10}\varepsilon_{11}+\varepsilon_{11}\varepsilon_{10}=0\ . \tag{25}
$$

Furthermore, we can obtain

$$
\varepsilon_{00}\varepsilon_{00}=\varepsilon_{11}\varepsilon_{11}\ . \tag{26}
$$

$$
|e_{00}\rangle|e_{00}\rangle=|e_{00}\rangle|e_{11}\rangle\ . \tag{27}
$$

Therefore, we can obtain

$$
U_E\left(|GHZ\rangle_{P_1P_2P_3}|E\rangle\right)=|GHZ\rangle_{P_1P_2P_3}|e_{00}\rangle|e_{00}\rangle\ . \tag{28}
$$

Based on the aforementioned proof, in the absence of errors induced by Eve's attack, the ultimate system state of Eve's probe should be independent of the measurement results of the particles from S_{P_1}, S_{P_2}, and S_{P_3}. Therefore, Eve is unable to obtain any useful information about the measured particles. Once Eve acquires any useful information, Eve's attack will be detected with a nonzero probability.

3.1.4. The Measure–Resend Attack

The external attacker may intercept the particles P_1 transmitted, measure the particles, and resend the fake states to P_2, P_3. Without loss of generality, suppose that Eve intercepts the particles S_{P_3}, measures the intercepted particles with Z basis, and sends the fake particles to P_3. Clearly, the system state has a probability of $\frac{1}{2}$ for being $|000\rangle$ and a probability of $\frac{1}{2}$ for being $|111\rangle$.

Firstly, we consider the scenario where the system state is $|000\rangle$. When the measurement basis is Z, the measurement results of $U^q_{P_1}$, $U^q_{P_2}$, $\tilde{U}^q_{P_3}$ are $|000\rangle$, and we can obtain $U^q_{zP_1}=U^q_{zP_2}=\tilde{U}^q_{zP_3}$. Eve is capable of evading eavesdropping detection.

When the measurement basis is X and the measurement results of $U_{P_1}^q$, $U_{P_2}^q$, $\tilde{U}_{P_3}^q$ in $|+++\rangle$, $|+--\rangle$, $|-+-\rangle$ or $|--+\rangle$, we can obtain $U_{xP_1}^q \cdot U_{xP_2}^q \cdot \tilde{U}_{xP_3}^q = 1$. Eve is capable of evading eavesdropping detection.

When the measurement results of $U_{P_1}^q$, $U_{P_2}^q$, $\tilde{U}_{P_3}^q$ in $|++-\rangle$, $|+-+\rangle$, $|-++\rangle$ or $|---\rangle$, we can obtain $U_{xP_1}^q \cdot U_{xP_2}^q \cdot \tilde{U}_{xP_3}^q = -1$. Eve is unable to evade eavesdropping detection.

Secondly, we consider the scenario where the system state is $|111\rangle$. When the measurement basis is Z, the measurement results of $U_{P_1}^q$, $U_{P_2}^q$, $\tilde{U}_{P_3}^q$ are $|111\rangle$, and we can obtain $U_{zP_1}^q = U_{zP_2}^q = \tilde{U}_{zP_3}^q$. Eve is capable of evading eavesdropping detection.

When the measurement basis is X and the measurement results of $U_{P_1}^q$, $U_{P_2}^q$, $\tilde{U}_{P_3}^q$ in $|+++\rangle$, $|+--\rangle$, $|-+-\rangle$ or $|--+\rangle$, we can obtain $U_{xP_1}^q \cdot U_{xP_2}^q \cdot \tilde{U}_{xP_3}^q = 1$. Eve is capable of evading eavesdropping detection.

When the measurement results of $U_{P_1}^q$, $U_{P_2}^q$, $\tilde{U}_{P_3}^q$ in $|++-\rangle$, $|+-+\rangle$, $|-++\rangle$ or $|---\rangle$, we can obtain $U_{xP_1}^q \cdot U_{xP_2}^q \cdot \tilde{U}_{xP_3}^q = -1$. Eve is unable to evade eavesdropping detection.

Therefore, for each CHECK particle, Eve is capable of evading eavesdropping detection with the probability of

$$\frac{1}{2} \times \left(\frac{1}{2} \times 1 + \frac{1}{2} \times \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} \right) \right) + \frac{1}{2} \times \left(\frac{1}{2} \times 1 + \frac{1}{2} \times \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} \right) \right) = \frac{3}{4} \ . \quad (29)$$

For all l CHECK particles, Eve can be detected with the probability of $1 - \left(\frac{3}{4}\right)^l$.

3.2. Internal Attack

A secure quantum key agreement protocol is required to possess the fairness property, ensuring that all participants contribute equally to the negotiated key. In the proposed protocol, under the condition that all participants honestly execute the protocol prior to Step 4, they will be able to successfully obtain $V_{zP_1} = V_{zP_2} = V_{zP_3}$. In Step 4, P_i calculates the value of $E_{P_i} = V_{zP_i} \oplus K_{P_i}$ and publishes it to other participants, where $i \in \{1, 2, 3\}$. However, P_i may announce the false value of $\tilde{E}_{P_i}$. Without loss of generality, suppose that P_1 intends to determine the negotiated key $\tilde{K} = \left\{\tilde{K}^1, \tilde{K}^2, \ldots, \tilde{K}^N\right\}$ alone. In Step 4, P_2 publishes the value of $E_{P_2} = V_{zP_2} \oplus K_{P_2}$, and P_3 publishes the value of $E_{P_3} = V_{zP_3} \oplus K_{P_3}$. Based on the value of E_{P_2} and E_{P_3}, P_1 can calculate the value of

$$\tilde{E}_{P_1} = V_{zP_1} \oplus \left(\tilde{K} \oplus \left(E_{P_2} \oplus V_{zP_1} \right) \oplus \left(E_{P_3} \oplus V_{zP_1} \right) \right) \ . \quad (30)$$

and announce the false value of $\tilde{E}_{P_1}$ to P_2, P_3, where $\tilde{E}_{P_1} = \left\{ \tilde{E}_{P_1}^1, \tilde{E}_{P_1}^2, \ldots, \tilde{E}_{P_1}^n \right\}$.

Based on the value of $\tilde{E}_{P_1}$, P_2 can infer the false value of

$$\tilde{K} = K_{P_2} \oplus \left(\tilde{E}_{P_1} \oplus V_{zP_2} \right) \oplus \left(E_{P_3} \oplus V_{zP_2} \right) \ . \quad (31)$$

P_3 can infer the false value of

$$\tilde{K} = K_{P_3} \oplus \left(\tilde{E}_{P_1} \oplus V_{zP_3} \right) \oplus \left(E_{P_2} \oplus V_{zP_3} \right) \ . \quad (32)$$

Nevertheless, as the hash value,

$$H\left(\tilde{E}_{P_1} \oplus V_{zP_2} \right) \neq H\left(K_{P_1} \right) \ . \quad (33)$$

$$H\left(\tilde{E}_{P_1} \oplus V_{zP_3} \right) \neq H\left(K_{P_1} \right) \ . \quad (34)$$

The dishonest behavior of P_1 will be detected by P_2, P_3.

Similarly, in the event that two dishonest participants collude to execute the cheating behavior, their cheating behavior will be exposed through the utilization of the hash function's properties.

4. The Extension of the Proposed Scheme

Suppose $P_1, P_2, \ldots, P_N$ seek to establish a private key over a quantum channel, ensuring that each participant contributes equally to the generation of the key and that the key cannot be fully determined by any non-trivial subset of them. In the negotiation phase, the utilization of a hash function outputting m bits is necessary.

Step 1: P_i randomly generates the CHECK keys

$$\bar{K}_{P_i} = \left\{ \bar{K}_{P_i}^1, \bar{K}_{P_i}^2, \ldots, \bar{K}_{P_i}^l \right\} , \tag{35}$$

and the INFO keys

$$K_{P_i} = \left\{ K_{P_i}^1, K_{P_i}^2, \ldots, K_{P_i}^n \right\} . \tag{36}$$

Here, l represents the number of the CHECK particles, n represents the length of the negotiated key, and $\bar{K}_{P_i}, K_{P_i} \in \{0,1\}, i \in \{1,2,\ldots,N\}$. P_i calculates the hash values $H\left(K_{P_i}\right)$ and announces the values.

Step 2: P_1 prepares $l+n$ N-particle GHZ states $|GHZ\rangle_N = \frac{1}{\sqrt{2}}(|00,\ldots,0\rangle + |11,\ldots,1\rangle)$. For each GHZ state, P_1 keeps the first particle, and sends the t-th particle to P_t, where $t \in \{2,\ldots,N\}$. We denote the i-th particle sequence as S_{P_i} as follows:

$$S_{P_i} = \left\{ S_{P_i}^1, S_{P_i}^2, \ldots, S_{P_i}^{l+n} \right\} . \tag{37}$$

Here, $i \in \{1,2,\ldots,N\}$.

Step 3: After P_i receives S_{P_i}, P_1 randomly selects l particles as the CHECK particles and informs other participants of the positions of the CHECK particles. Here, the CHECK particles respectively held by P_i are denoted as U_{P_i} as follows:

$$U_{P_i} = \left\{ U_{P_i}^1, U_{P_i}^2, \ldots, U_{P_i}^l \right\}. \tag{38}$$

Then, P_i announces the CHECK keys $\bar{K}_{P_i}$ and calculates

$$\bar{K} = \bar{K}_{P_1} \oplus \bar{K}_{P_2} \oplus \ldots \oplus \bar{K}_{P_N} . \tag{39}$$

Here, $\bar{K} = \left\{ \bar{K}^1, \bar{K}^2, \ldots, \bar{K}^l \right\}$. For the q-th CHECK particle, when the value of $\bar{K}^q$ is 0, P_i uses the Z basis to measure the particle $U_{P_i}^q$ and publishes the measurement results, where $q \in \{1,2,\ldots,l\}$. When the value of $\bar{K}^q$ is 1, P_i uses the X basis to measure the particle $U_{P_i}^q$ and publishes the measurement results, where $q \in \{1,2,\ldots,l\}$. Suppose that the measurement results in basis Z are $U_{zP_i}^q = \{+1,-1\}$ and in basis X are $U_{xP_i}^q = \{+1,-1\}$. According to the entanglement properties of the N-particle GHZ state and Equation (40),

$$\begin{aligned} |GHZ\rangle_N &= \frac{1}{\sqrt{2}} \left(\underbrace{|00,\ldots,0\rangle}_{N} + \underbrace{|11,\ldots,1\rangle}_{N} \right) \\ &= \frac{1}{2^{\frac{N+1}{2}}} \sum_{\sigma_1 \sigma_2, \ldots, \sigma_N} (|\sigma_1 \sigma_2, \ldots, \sigma_N\rangle) \end{aligned} . \tag{40}$$

In this equation, $\sigma_i \in \{+,-\}$, $i \in \{1,2,\ldots,N\}$, $\sigma_1 \oplus \sigma_2 \oplus \cdots \oplus \sigma_N$=0. P_i can check the correctness of the measurement results. When the chosen basis is Z, the measurement results must satisfy $U^q_{zP_1}$=$U^q_{zP_2}$=...=$U^q_{zP_N}$. When the chosen basis is X, the measurement results must satisfy $\Pi_{i=1}^{N} U^q_{xP_i} = 1$. If the error exceeds the threshold, the protocol aborts. The remaining particles serve as INFO particles $V_{P_i} = \left\{V^1_{P_i}, V^2_{P_i}, \ldots, V^n_{P_i}\right\}$. P_i measures the particles with the Z basis.

Step 4: The measurement results are represented by V_{zP_i}. If the measurement result is $|0\rangle$, its value is taken as 0; if the measurement result is $|1\rangle$, its value is taken as 1. According to the entanglement properties of the N-particle GHZ state, we can obtain V_{zP_1}=V_{zP_2}=...=V_{zP_N}. P_i calculates $E_{P_i} = V_{zP_i} \oplus K_{P_i}$ and sends it to other participants.

Step 5: P_i calculates $H\left(E_{P_j} \oplus V_{zP_i}\right)$. If $H\left(E_{P_j} \oplus V_{zP_i}\right) = H\left(K_{P_j}\right)$, P_i will infer the final negotiated key

$$K = \sum_{j=1}^{N} \left(E_{P_j} \oplus V_{zP_i}\right)(mod\ 2)\ , \tag{41}$$

In this equation, $i \in \{1,2,\ldots,N\}$, $j \in \{1,2,\ldots,N\}$. If any participant refuses K as the negotiated key, the protocol will be terminated and restarted.

5. Discussions

Reference [45] provides a definition of qubit efficiency,

$$\eta = \frac{f}{q+c}\ , \tag{42}$$

In this equation, q is the number of transmitted qubits, c is the number of consumed classical bits, and f is the number of bits of the negotiated key. In the proposed protocol, P_1 prepares $l+n$ N-particle entangled states, and it has $q = (l+n)N$. For the consumed classical bits, in order to announce the hash $H\left(K_{P_i}\right)$, the CHECK keys $\bar{K}_{P_i}$, the measurement results of U_{P_i}, and the ciphertext E_{P_i}, P_i needs to spend m, l, l, and n classical bits, respectively, where m is the length of the hash function $H(x)$. For N participants, the number of needed classical bits is $c = (2l+n+m)N$. The length of the negotiated key is n; therefore, $f = n$. Therefore, the qubit efficiency is $\eta = \frac{n}{(3l+2n+m)N}$. When l is the same as n, the qubit efficiency $\eta = \frac{n}{(5n+m)N}$.

In comparison to the previous MQKA protocols, as illustrated in Table 1, our protocol demonstrates great advantages. Our scheme retains most of the advantages of the schemes in [41,42] using one kind of multi-particle entangled state as the initial quantum resource, and eliminates the need for entanglement swapping techniques, unitary operations, or pre-shared keys between participants. In addition, our scheme uses only the X and Z bases for measurement, making it simpler and more practical than scheme [41], which uses GHZ and Z bases, and scheme [42], which uses X, Y, and Z bases. In terms of qubit transmission, our scheme and reference [42] require only one transmission from participant P1 to P2 (P3), while scheme [41] involves additional steps of reflecting or resending particles. Regarding qubit consumption, our scheme and reference [42] consume $2nN$ qubits, whereas reference [41] consumes $2^{N-1}n(3N-1)$ qubits. Moreover, our scheme achieves a qubit efficiency of $\frac{n}{5nN+mN}$, compared to $\frac{n}{2^{N-1}n(3N-1)+mN+nN}$ for reference [41] and $\frac{n}{6nN+mN}$ for reference [42]. These advantages make our scheme more efficient and practical for implementation.

Table 1. Comparison between our protocol and the previous MQKA protocols.

The MQKA Protocols	Quantum Resource States	Entanglement Swapping Technology	Unitary Operations	Pre-Shared Keys	Extra Qubits Transmission	Measurement Bases	Consumed Qubits	Quantum Efficiency
Protocol [41]	GHZ states	No	No	No	Yes	GHZ basis, Z basis	$2^{N-1}n$ $(3N-1)$	$\frac{n}{2^{N-1}n(3N-1)+mN+nN}$
Protocol [42]	GHZ states	No	No	No	No	X basis, Y basis, Z basis	$2nN$	$\frac{n}{6nN+mN}$
Our scheme	GHZ states	No	No	No	No	X basis, Z basis	$2nN$	$\frac{n}{5nN+mN}$

6. Conclusions

In this paper, a single-state multi-party quantum key agreement (MQKA) protocol utilizing single-particle measurement is proposed. We introduce a single-state three-party quantum key agreement protocol with single-particle measurement followed by a comprehensive security analysis. Building on this foundation, we further extend this approach by employing multi-particle entangled states to develop a multi-party version of the single-state multi-party quantum key agreement with single-particle measurement. Specifically, it employs one kind of multi-particle entangled state as the quantum resource, eliminating the need for entanglement swapping techniques, unitary operations, or pre-shared keys between participants. Moreover, the protocol uses only the X measurement basis and Z measurement basis, which results in fewer qubits being transmitted and consumed, and higher qubit efficiency. While our method can be extended to a multi-party version, the preparation of multi-particle entangled states remains a significant challenge that warrants further investigation.

Author Contributions: Writing—original draft, H.Y., D.C., L.Q. and R.Z.; Writing—review and editing, H.Y., D.C., L.Q., R.Z., S.L. and C.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Major Research Plan of Hubei Province under Grant/Award NO. 2023BAA027; the Key Research & Development Plan of Hubei Province of China under Grant No. 2024BAB049 and the project of Science, Technology and Innovation Commission of Shenzhen Municipality of China under Grant No. GJHZ20240218114659027.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: Authors Dunbo Cai, Ling Qian, and Runqing Zhang were employed by the company of China Mobile (Suzhou) Software Technology Co., Ltd. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as potential conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

QKD	Quantum Key Distribution
QSS	Quantum Secret Sharing
QSDC	Quantum Secure Direct Communication
QPQ	Quantum Private Query
QKA	Quantum Key Agreement

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
2. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
3. Bennett, C.H.; Brassard, G.; Mermin, N.D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **1992**, *68*, 557. [CrossRef]
4. Liao, S.K.; Cai, W.Q.; Liu, W.Y.; Zhang, L. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43–47. [CrossRef] [PubMed]
5. Hillery, M.; Buzek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829–1834. [CrossRef]
6. Zhang, Z.J; Li, Y.; Man, Z.X. Multiparty quantum secret sharing. *Phys. Rev. A* **2005**, *71*, 044301. [CrossRef]
7. Zhou, Y.; Yu, J.; Yan, Z. Quantum secret sharing among four players using multipartite bound entanglement of an optical field. *Phys. Rev. Lett.* **2018**, *121*, 150502. [CrossRef]
8. Deng, F.G.; Long, G.L. Secure direct communication with a quantum one-time pad. *Phys. Rev. A* **2004**, *69*, 052319. [CrossRef]
9. Zhang, W.; Ding, D.S.; Sheng, Y.B.; Zhou, L.; Shi, B.S.; Guo, G.C. Quantum secure direct communication with quantum memory. *Phys. Rev. Lett.* **2017**, *118*, 220501. [CrossRef]
10. Zhou, L.; Sheng, Y.B.; Long, G.L. Device-independent quantum secure direct communication against collective attacks. *Sci. Bull.* **2020**, *65*, 12–20. [CrossRef]
11. Giovannetti, V.; Lloyd, S.; Maccone, L. Quantum private queries. *Phys. Rev. Lett.* **2017**, *100*, 230502. [CrossRef]
12. Gao, F.; Qin, S.; Huang, W. Quantum private query: A new kind of practical quantum cryptographic protocol. *Sci. China Phys. Mech. Astron.* **2019**, *62*, 1–12. [CrossRef]
13. Ye, T.Y.; Li, H.K.; Hu, J.L. Multi-user quantum private query protocol. *Int. J. Theor. Phys.* **2020**, *59*, 2867–2874. [CrossRef]
14. Yang, H.; Xiao, M. Multi-user quantum private query. *Quantum Inf. Process.* **2020**, *19*, 253. [CrossRef]
15. Zhou, N.; Zeng, G.; Xiong, J. Quantum key agreement protocol. *Electron. Lett.* **2004**, *40*, 1149. [CrossRef]
16. Tsai, C.; Hwang, T. *On Quantum Key Agreement Protocol*; Technical Report, C-S-I-E; NCKU: Taiwan, China, 2009.
17. Hsueh, C.C.; Chen, C.Y. Quantum key agreement protocol with maximally entangled states. In Proceedings of the 14th Information Security Conference (ISC 2004), National Taiwan University of Science and Technology, Taipei, Taiwan, 10–11 June 2004; pp. 10–11.
18. Tsai, C.W.; Chong, S.K.; Hwang, T. Comment on quantum key agreement protocol with maximally entangled states. In Proceedings of the 20th Cryptology and Information Security Conference (CISC 2010), National Chiao Tung University, Hsinchu, Taiwan, 27–28 May 2010; pp. 210–213.
19. Chong, S.K.; Tsai, C.W.; Hwang, T. Improvement on "quantum key agreement protocol with maximally entangled states". *Int. J. Theor. Phys.* **2011**, *50*, 1793–1802. [CrossRef]
20. Shi, R.H.; Zhong, H. Multi-party quantum key agreement with bell states and bell measurements. *Quantum Inf. Process.* **2013**, *12*, 921–932. [CrossRef]
21. Sun, Z.; Huang, J.; Wang, P. Efficient multiparty quantum key agreement protocol based on commutative encryption. *Quantum Inf. Process.* **2016**, *15*, 2101–2111. [CrossRef]
22. Wang, M.M.; Han, R.F.; Gong, L.M. Multiparty semiquantum key agreement without entanglement. *Commun. Theor. Phys.* **2020**, *72*, 065107. [CrossRef]
23. Li, H.H.; Gong, L.H.; Zhou, N.R. New semi-quantum key agreement protocol based on high-dimensional single-particle states. *Chin. Phys. B.* **2020**, *29*, 11. [CrossRef]
24. Tang, R.H.; Zhang, C.; Long, D.Y. An efficient circle-type multiparty quantum key agreement protocol with single particles. *Int. J. Mod. Phys. B.* **2020**, *34*, 20. [CrossRef]
25. Sun, Z.W.; Wu, C.H.; Zheng, S.G. Efficient multiparty quantum key agreement with a single d-level quantum system secure against collusive attack. *IEEE Access* **2019**, *7*, 102377–102385. [CrossRef]
26. Xu, T.J.; Gan, Z.G.; Ye, T.Y. Multiparty semiquantum key agreement with d-level single-particle states. *Phys. A-Stat. Mech. Its Appl.* **2023**, *625*, 128991. [CrossRef]
27. Shukla, C.; Alam, N.; Pathak, A. Protocols of quantum key agreement solely using Bell states and Bell measurement. *Quantum Inf. Process.* **2014**, *13*, 2391–2405. [CrossRef]
28. Huang, W.; Wen, Q.Y.; Liu, B. Quantum key agreement with EPR pairs and single-particle measurements. *Quantum Inf. Process.* **2014**, *13*, 649–663. [CrossRef]
29. Zhu, Z.C.; Hu, A.Q.; Fu, A.M. Improving the security of protocols of quantum key agreement solely using Bell states and Bell measurement. *Quantum Inf. Process.* **2015**, *14*, 4245–4254. [CrossRef]
30. Liu, W.J.; Xu, Y.; Yang, C.N. An Efficient and Secure Arbitrary N-Party Quantum Key Agreement Protocol Using Bell States. *Int. J. Theor. Phys.* **2018**, *57*, 195–207. [CrossRef]

31. Yang, Y.G.; Li, B.R.; Li, D. New quantum key agreement protocols based on Bell states. *Quantum Inf. Process.* **2019**, *18*, 322. [CrossRef]
32. Yan, L.; Zhang, S.; Chang, Y. Semi-Quantum Key Agreement and Private Comparison Protocols Using Bell States. *Int. J. Theor. Phys.* **2019**, *58*, 3852–3862. [CrossRef]
33. Zhou, N.R.; Min, S.Q.; Chen, H.Y. Three-Party Quantum Key Agreement Protocol with Seven-Qubit Entangled States. *Int. J. Theor. Phys.* **2018**, *57*, 3505–3513. [CrossRef]
34. Cai, T.; Jiang, M.; Cao, G. Multi-party quantum key agreement with five-qubit brown states. *Quantum Inf. Process.* **2018**, *17*, 103. [CrossRef]
35. Tang, J.; Shi, L.; Wei, J. Controlled quantum key agreement based on maximally three-qubit entangled states. *Modern Phys. Lett. B* **2020**, *34*, 2050201. [CrossRef]
36. Liu, L.J.; Li, Z.H. A verifiable quantum key agreement protocol based on six-qubit cluster states. *Eur. Phys. J. D* **2021**, *75*, 193. [CrossRef]
37. Xu, Y.; Wang, C.; Cheng, K. A Novel Three-Party Mutual Authentication Quantum Key Agreement Protocol with GHZ States. *Int. J. Theor. Phys.* **2022**, *61*, 245. [CrossRef]
38. Zhou, N.R.; Liao, Q.; Zou, X.F. Multi-Party Semi-Quantum Key Agreement Protocol Based on the Four-Qubit Cluster States. *Int. J. Theor. Phys.* **2022**, *61*, 114. [CrossRef]
39. Liu, C.; Cheng, S.; Li, H.H. New Semi-Quantum Key Agreement Protocol Based on the χ-Type Entanglement States. *Int. J. Theor. Phys.* **2022**, *61*, 60. [CrossRef]
40. Liu, B.X.; Huang, R.C.; Yang, Y.G.; Xu, G.B. Measurement-device-independent multi-party quantum key agreement. *Front. Quantum Sci. Technol.* **2023**, *2*, 1182637. [CrossRef]
41. Xu, T.J.; Chen, Y.; Geng, M.J. Single-state multi-party semiquantum key agreement protocol based on multi-particle GHZ entangled states. *Quantum Inf. Process.* **2022**, *21*, 266. [CrossRef]
42. Yang, H.; Lu, S.F.; Zhou, Q.; Wang, M.; Feng, B.Y.; Zhou, X.J. Efficient single-state multi-party quantum key agreement. *Quantum Inf. Process.* **2024**, *23*, 150. [CrossRef]
43. Li, X.H.; Deng, F.G.; Zhou, H.Y. Improving the security of secure direct communication based on the secret transmitting order of particles. *Phys. Rev. A* **2019**, *74*, 054302. [CrossRef]
44. Cai, Q.Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys. Lett. A* **2006**, *351*, 23–25. [CrossRef]
45. Cabello, A. Quantum key distribution in the Holevo limit. *Phys. Rev. Lett.* **2000**, *85*, 5635. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.