entropy

IMPACT FACTOR 2.738

Indexed in: PubMed

Article

Cryptanalysis of a Semi-Quantum Bi-Signature Scheme Based on W States

Chun-Wei Yang, Jason Lin, Chia-Wei Tsai and Ching-Lin Cheng

Special Issue
Quantum Control and Quantum Computing

Edited by
Dr. Xi Chen

MDPI

https://doi.org/10.3390/e24101408

entropy

MDPI

Article

Cryptanalysis of a Semi-Quantum Bi-Signature Scheme Based on W States

Chun-Wei Yang [1], Jason Lin [2], Chia-Wei Tsai [3,*] and Ching-Lin Cheng [1]

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

Abstract: Recently, Zhao et al. proposed a semi-quantum bi-signature (SQBS) scheme based on W states with two quantum signers and just one classical verifier. In this study, we highlight three security issues with Zhao et al.'s SQBS scheme. In Zhao et al.'s SQBS protocol, an insider attacker can perform an impersonation attack in the verification phase and an impersonation attack in the signature phase to capture the private key. In addition, an eavesdropper can perform a man-in-the-middle attack to obtain all of the signer's secret information. All of the above three attacks can pass the eavesdropping check. Without considering these security issues, the SQBS protocol could fail to ensure the signer's secret information.

Keywords: quantum cryptography; semi-quantum; quantum signature; bi-signature; W-like state

Citation: Yang, C.-W.; Lin, J.; Tsai, C.-W.; Cheng, C.-L. Cryptanalysis of a Semi-Quantum Bi-Signature Scheme Based on W States. *Entropy* **2022**, *24*, 1408. https://doi.org/10.3390/e24101408

Academic Editor: Xi Chen

Received: 9 September 2022
Accepted: 29 September 2022
Published: 1 October 2022

1. Introduction

With advances in quantum information science, various quantum techniques have been applied in quantum cryptography, such as entanglement swapping [1], quantum teleportation [2–4], and quantum remote control [5–10]. Quantum cryptography techniques can be used in various network communication environments, among which quantum signature is an important topic. In 2001, Gottesman and Chuang [11] proposed the first quantum signature concept. In 2002, Zeng and Keitel [12] proposed the first arbitrated quantum signature protocol based on the Green–Horne–Zeilinger (GHZ) state. Since then, various quantum signature protocols have been proposed, for example, arbitrated quantum signature [13–20], quantum blind signature [21–26], quantum proxy signature [27,28], and quantum group signature [29]. Inspired by the above quantum signature schemes [11–29], Zhao et al. [30] proposed a signature scheme based on the concept of "bi-signature." In Zhao et al.'s quantum bi-signature protocol, two participants sign their signatures on the same message.

The aforementioned quantum signature schemes [11–30] all require the assumption that all participants in the protocol are quantum-capable, i.e., they must have devices such as photonic generators, quantum memory, and photonic measurement devices. In the absence of these devices, quantum signature protocols [11–30] cannot be executed. However, quantum devices are not widely available, and not all participants have access to such devices. In 2007, Boyer et al. [31] introduced the concept of a semi-quantum environment. In 2009, the same authors [32] proposed two types of semi-quantum key distribution protocols. Since then, various semi-quantum cryptographic protocols and applications have flourished. For example, various applications of the semi-quantum key distribution (SQKD) protocol have been reported. Some studies [33–36] have implemented SQKD protocols using single photons. Zhu et al. [37] design a SQKD protocol involving

GHZ states. Considering the multiparticipant scenario, researchers have [38–40] proposed mediated SQKD protocols. Some studies [41] also discuss the implementation of SQKD protocols by excluding the measurement capabilities of classical participants. On the other hand, several studies [42–45] have investigated the implementation of authenticated SQKD protocols. Unlike SQKD protocols, another application environment is one in which the boss has quantum capabilities, and the agent has only classical capabilities. The boss divides the secret key into several parts and gives them to the agents for custody. The agents must work together to obtain the boss's secret key. Current semi-quantum secret-sharing protocols are available in single photons [46–49], entangled states [50–53], GHZ states [54–57], W states [58], and cluster states [59]. In 2014, Zou and Qiu [60] proposed a three-step semi-quantum secure direct communication (SQSDC) protocol allowing a classical participant who does not have a quantum register to securely send a secret message to a quantum participant. Since then, many SQSDC protocols with an entanglement state [61–68] and without entanglement [69] have been proposed. Private comparison is primitive for many cryptographic tasks, and recently, several schemes for semi-quantum private comparison with single photons [70–73], Bell states [74–77], GHZ-like states [78–80], and W states [81] have been proposed.

In 2019, Zhao et al. [82] proposed a semi-quantum bi-signature (SQBS) scheme based on W-like states [83–85] and a quantum teleportation technique [86]. In the SQBS protocol, two participants are quantum-capable signers, and one is conventionally capable verifier. The main technique is to transmit the secret message of the signature to another signer through W-state teleportation technology. Then, the two signers transmit the signature messages to the verifier via their pre-shared keys. Finally, the verifier confirms that the two received signatures are identical, and the signature is completed.

Although Zhao et al. [82] proposed an SQBS protocol and proved the security of their protocol, in this study we highlight three security problems with the proposed SQBS protocol [82].

1. In the final step of the verification phase, the verifier (Charlie) performs an XOR operation with the pre-shared keys of two signers (Alice and Bob). If the verification passes, it means that the signature message is the same. Therefore, Bob can infer Alice's pre-shared key and forge Alice's signature later.
2. In the final step of the signature phase, the signer (Alice) transmits the signature message and the W-state measurement results to the verifier (Charlie) through the public classical channel. The public classical channel can be eavesdropped on and tampered with. Therefore, Bob can use the received secret message, Alice's signature message, and measurement results to infer Alice's pre-shared key, which can then be used to forge Alice's signature.
3. The signer (Alice) transmits the secret message to another signer (Bob) through W-state teleportation technology; however, Alice and Bob do not perform any eavesdropping checks during the teleportation stage. Therefore, the eavesdropper (Eve) will be able to capture the secret message through a man-in-the-middle attack.

The rest of this paper is organized as follows. In Section 2, we review Zhao et al.'s SQBS protocol. In Section 3, we discuss three security issues associated with the protocol. Finally, in Section 4 we present our conclusions and discussion.

2. Review of Zhao et al.'s SQBS Protocol

In Zhao et al.'s SQBS protocol [82], there are three participants: Alice and Bob (signers with quantum capabilities) and Charlie (a verifier with only classical capabilities); the classical capabilities of Charlie limit him to the use of the Z basis $\{|0\rangle, |1\rangle\}$ to measure and generate single photons and to directly return the received quantum state. The eavesdropper, Eve, can perform any attack without violating the definition of quantum mechanics. Zhao et al.'s SQBS protocol is divided into three phases: the initial phase, the signature phase, and the verification phase. An overview of Zhao et al.'s SQBS protocol is shown in Figure 1. The detailed steps of Zhao et al.'s SQBS protocol are described as follows.

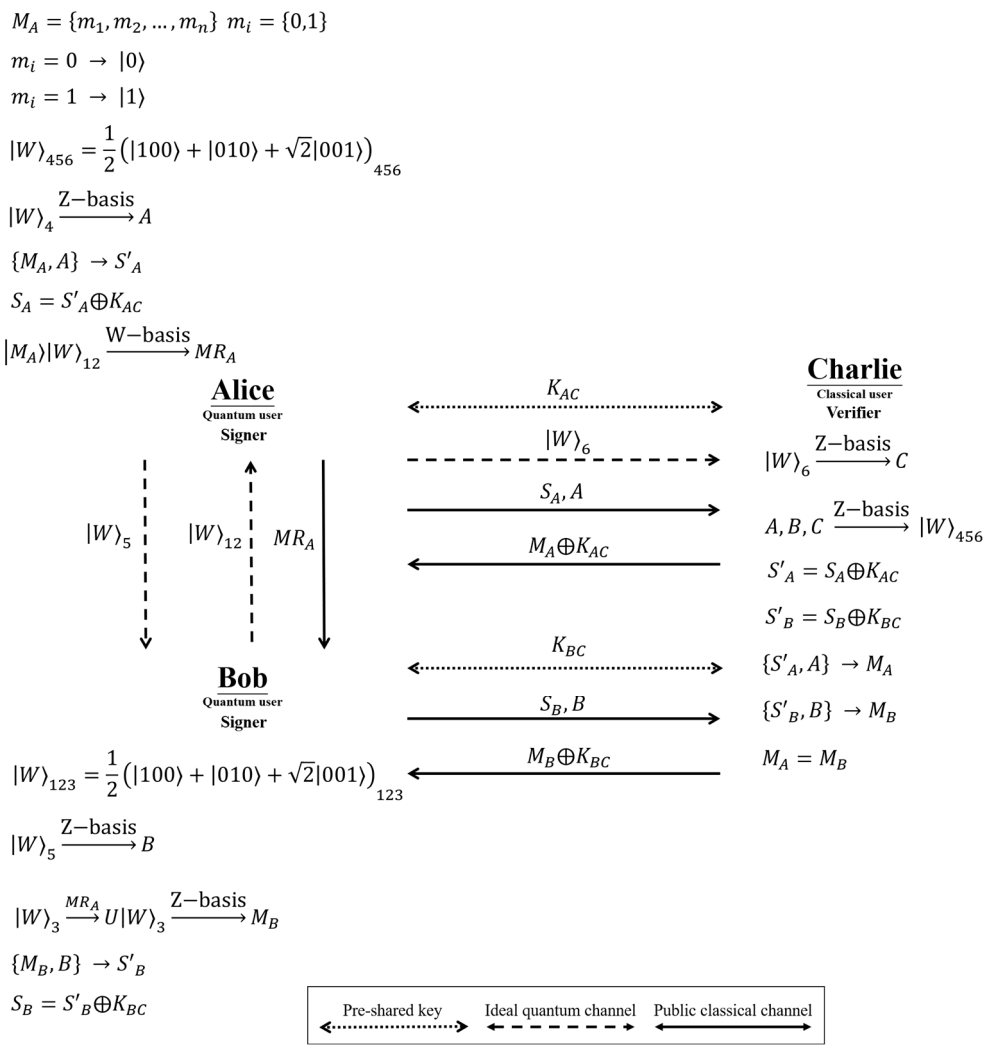

Figure 1. Zhao et al.'s SQBS protocol.

2.1. Initial Phase

In the initial phase, the pre-shared keys, K_{AC} and K_{BC}, are allocated, and the W-like state is prepared to provide the execution requirements in the subsequent signature phase and verification phase.

Step 1. Alice prepares the secret message, $M_A = \{m_1, m_2, \ldots, m_n\}$, where $m_i = \{0, 1\}$. The agreed encoding rule is as follows: if the classical bit is "0", then $|0\rangle$ is generated; if the classical bit is "1", then $|1\rangle$ is generated.

Step 2. Bob and Alice prepare n sets of W-like states, $|W\rangle_{123} = \frac{1}{2}\left(|100\rangle + |010\rangle + \sqrt{2}|001\rangle\right)_{123}$ and $|W\rangle_{456} = \frac{1}{2}\left(|100\rangle + |010\rangle + \sqrt{2}|001\rangle\right)_{456}$.

Step 3. Through Krawec's semi-quantum key distribution protocol [36], Alice and Charlie can share a private key, K_{AC}; Bob and Charlie can share a private key, K_{BC}.

2.2. Signature Phase

This phase focuses on Alice and Bob generating their respective signatures and sending them to Charlie. In addition, Alice sends the secret message, $M_A = \{m_1, m_2, \ldots, m_n\}$, to Bob through the quantum teleportation of the W-like state.

Step 1. Alice sends $|W\rangle_5$ and $|W\rangle_6$ of $|W\rangle_{456} = \frac{1}{2}\left(|100\rangle + |010\rangle + \sqrt{2}|001\rangle\right)_{456}$ to Bob and Charlie, respectively, keeping $|W\rangle_4$ for herself. Then, Bob sends $|W\rangle_{12}$ of $|W\rangle_{123} = \frac{1}{2}\left(|100\rangle + |010\rangle + \sqrt{2}|001\rangle\right)_{123}$ to Alice and keeps $|W\rangle_3$ for himself.

Step 2. Alice, Bob, and Charlie perform Z-basis measurements on their respective $|W\rangle_4$, $|W\rangle_5$, and $|W\rangle_6$ and obtain the measurement results for A, B, and C.

Step 3. Based on Alice's secret message (M_A) and the measurement result (A) of $|W\rangle_4$, Alice's signature message (S'_A) can be obtained through the coding rule listed in Table 1. Then, the signature message (S'_A) and the pre-shared key (K_{AC}) perform the exclusive or (XOR) operation to obtain Alice's signature, $S_A = S'_A \bigoplus K_{AC}$. Finally, Alice sends the signature (S_A) and the measurement result (A) to Charlie through the public classical channel.

Step 4. Alice generates the secret message (M_A) as a single photon $|M_A\rangle$ according to the coding rules (i.e., if the classical bit is "0", then generate $|0\rangle$; if the classical bit is "1", then $|1\rangle$ is generated). Next, Alice measures $|M_A\rangle$ with $|W\rangle_{12}$ in the W-basis $\left\{|\kappa^{\pm}\rangle = \frac{1}{2}\left(|010\rangle + |001\rangle \pm \sqrt{2}|100\rangle\right), |\gamma^{\pm}\rangle = \frac{1}{2}\left(|110\rangle + |101\rangle \pm \sqrt{2}|000\rangle\right)\right\}$ and announces the measurement result to Bob. Based on the measurement result, Bob can perform the corresponding operation $\left\{\sigma_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \sigma_4 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\right\}$ in $|W\rangle_3$ to obtain $|M_B\rangle$. Finally, Bob measures $|M_B\rangle$ in Z basis to obtain Alice's secret message (M_B).

Step 5. Based on the received secret message (M_B) and the measurement result (B) of $|W\rangle_5$, Bob can obtain the signature message (S'_B) via the coding rule listed in Table 1. Then, the signature message (S'_B) and the pre-shared key (K_{BC}) can be used to perform the XOR operation to obtain Bob's signature, $S_B = S'_B \bigoplus K_{BC}$. Finally, Bob sends the signature (S_B) and the measurement result (B) to Charlie through the public classical channel.

Table 1. The coding rule of signature message.

	$M_A = 0$	$M_A = 1$
$A = 0$	$S'_A = 1$	$S'_A = 0$
$A = 1$	$S'_A = 0$	$S'_A = 1$

2.3. Verification Phase

This stage involves Charlie verifying whether Alice's and Bob's signatures are correct; the verification steps are as follows.

Step 1. Charlie first checks that Alice's, Bob's, and his own measurement results (A, B, and C) are consistent with the W-like state, $|W\rangle_{456} = \frac{1}{2}\left(|100\rangle + |010\rangle + \sqrt{2}|001\rangle\right)_{456}$. If the measurement result does not match, the SQBS protocol is canceled; otherwise, Charlie continues with the next step.

Step 2. Charlie can deduce Alice's and Bob's signature messages through K_{AC} and K_{BC} as $S'_A = S_A \bigoplus K_{AC}$ and $S'_B = S_B \bigoplus K_{BC}$, respectively.

Step 3. Charlie can deduce Alice's secret message (M_A) by S'_A and A through the coding rules listed in Table 1. Similarly, Charlie can deduce Bob's secret message (M_B) by S'_B and B.

Step 4. Charlie compares M_A and M_B; if $M_A = M_B$, then Charlie accepts Alice's and Bob's signature; otherwise, Charlie rejects this signature. Finally, Charlie sends $M_A \bigoplus K_{AC}$ and $M_B \bigoplus K_{BC}$ to Alice and Bob, respectively.

3. Security Issues of Zhao et al.'s SQBS Protocol

In this study, we identified three security problems in Zhao et al.'s SQBS protocol: an impersonation attack in the verification phase, an impersonation attack in the signature

phase, and a man-in-the-middle attack. The mechanisms of these three attack patterns are explained below.

3.1. Impersonation Attack in the Verification Phase

Consider Bob as the insider attacker. If Bob wants to impersonate Alice's identity, he must obtain Alice's private key with Charlie, K_{AC}. The following illustrates how Bob attacks.

In Step 4 of the verification phase, if Charlie accepts Alice's and Bob's signatures, then Charlie sends $M_A \bigoplus K_{AC}$ and $M_B \bigoplus K_{BC}$ to Alice and Bob, respectively. In this step, Bob intercepts the result of copying $M_A \bigoplus K_{AC}$. Furthermore, if the signature is passed, it means that Bob's message (M_B) is the same as M_A. Therefore, Bob can deduce that $M_A \bigoplus K_{AC} = M_B \bigoplus K_{AC}$ and learn the value of K_{AC}. In this way, Bob can impersonate Alice's identity and communicate with Charlie through K_{AC}.

3.2. Impersonation Attack in the Signature Phase

Similarly, considering Bob as the insider attacker, if Bob wants to impersonate Alice's identity, he must obtain Alice's private key, K_{AC}. The following describes Bob's attack strategy.

In Step 3 of the signature phase, Alice sends her signature (S_A) and the measurement result (A) to Charlie through the public classical channel. Hence, Bob can intercept and learn Alice's signature (S_A) and the measurement result (A). In Step 4 of the signature phase, Bob can obtain Alice's message (M_B) through the quantum teleportation of the W-like state. In this way, Bob has both M_B and A and can deduce Alice's ${S'}_A$ in Table 1. Then, through ${S'}_A$ and S_A, Bob can deduce Alice's private key, $K_{AC} = {S'}_A \bigoplus S_A$. Finally, Bob can impersonate Alice's identity through K_{AC} to communicate with Charlie.

3.3. Man-in-the-Middle Attack

In the quantum signature protocol, the signer's message cannot be known by anyone other than the signer. Therefore, Alice's secret message (M_A) cannot be eavesdropped on. Once the signer's secret message is leaked, the protocol is declared a failure. In Zhao's SQBS protocol, the signers (Alice and Bob) protect Alice's secret messages (M_A) through the quantum teleportation of the W-like state. However, in this study, we revealed that the eavesdropper, Eve, can perform a man-in-the-middle attack to obtain Alice's secret message (M_A) without being detected. Because Alice and Bob do not have any protection or checking mechanism when executing quantum teleportation, Eve can capture the secret message (M_A). An overview of the man-in-the-middle attack on Zhao's SQBS protocol is shown in Figure 2. The attack strategy is described as follows.

Step A1. In Step 1 of the signature phase, Bob sends the state $|W\rangle_{12}$ of $|W\rangle_{123} = \frac{1}{2}\left(|100\rangle + |010\rangle + \sqrt{2}|001\rangle\right)_{123}$ to Alice. At this point, Eve intercepts $|W\rangle_{12}$ and generates another set of W-like states, $|W\rangle_{123}^{E} = \frac{1}{2}\left(|100\rangle + |010\rangle + \sqrt{2}|001\rangle\right)_{123}^{E}$, and sends $|W\rangle_{12}^{E}$ to Alice.

Step A2. In Step 4 of the signature phase, Alice measures $|M_A\rangle$ and $|W\rangle_{12}^{E}$ in the W-basis $\left\{|\kappa^{\pm}\rangle = \frac{1}{2}\left(|010\rangle + |001\rangle \pm \sqrt{2}|100\rangle\right), |\gamma^{\pm}\rangle = \frac{1}{2}\left(|110\rangle + |101\rangle \pm \sqrt{2}|000\rangle\right)\right\}$ and informs Bob of the measurement result. In this step, Eve intercepts Alice's measurement result (MR_A); then, based on the measurement result (MR_A), Eve can perform the corresponding operation $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ in $|W\rangle_{3}^{E}$ to obtain $|M_A\rangle$. Thus, Eve can measure $|M_A\rangle$ in the Z basis to obtain Alice's secret message (M_A).

Step A3. After Eve obtains M_A, Eve generates $|M_A\rangle$ and measures it with the intercepted $|W\rangle_{12}$ in the W-basis $\left\{|\kappa^{\pm}\rangle, |\gamma^{\pm}\rangle\right\}$. Then, Eve informs Bob of the measurement result (MR_A^E). Based on the measurement result (MR_A^E), Bob can perform the

corresponding operation $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ in $|W\rangle_3$ to obtain $|M_A\rangle$. Finally, $|M_A\rangle$ is measured through the Z-basis to obtain Alice's secret message (M_A).

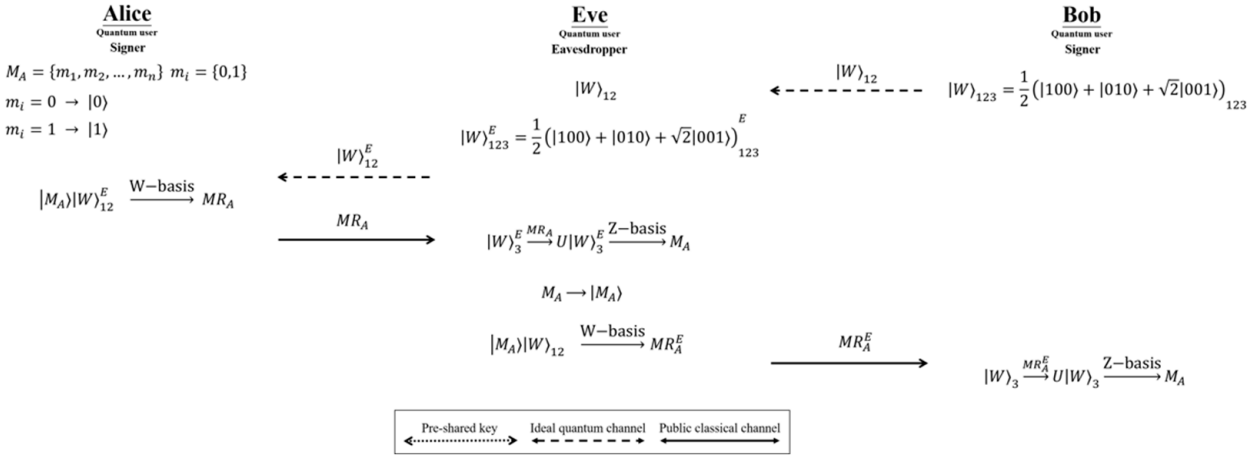

Figure 2. The process of the man-in-the-middle attack on Zhao's SQBS protocol.

Because Eve's attack does not destroy the secret message (M_A), Charlie's inspection of Alice's and Bob's signatures will pass smoothly in the final verification stage. Therefore, Eve successfully executes the man-in-the-middle attack to capture Alice's secret message (M_A) and is not discovered.

4. Conclusions

In this study, we highlight three security issues with Zhao et al.'s SQBS protocol: an impersonation attack in the verification phase, an impersonation attack in the signature phase, and a man-in-the-middle attack. In the impersonation attack, the insider attacker can capture the private key and impersonates the signer's identity to communicate with the verifier. In the man-in-the-middle attack, the eavesdropper can obtain all the signer's secret messages. All of the above three attacks can pass the eavesdropping check. Without considering these security issues, the SQBS protocol could fail to ensure the security of the signature. A possible solution is to add an eavesdropping check, for example, using decoy photons as an eavesdropping check. However, this requires an authenticated channel between the verifier and each signer and is therefore not very elegant. Improved solutions for this new issue in the SQBS protocol need to be designed in future research.

Author Contributions: Conceptualization, C.-W.Y. and C.-W.T.; methodology, C.-W.Y., J.L. and C.-W.T.; investigation, J.L. and C.-L.C.; formal analysis, C.-W.Y.; writing—original draft, C.-W.Y. and C.-W.T.; writing—review and editing, C.-W.Y. and C.-W.T.; 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 110-2221-E-143-003, NSTC 110-2221-E-259-001, NSTC 110-2221-E-143-004, NSTC 110-2222-E-005-006, NSTC 110-2634-F-005-006, NSTC 111-2218-E-005-007-MBK, NSTC 111-2221-E-005-048, and NSTC 111-2221-E-025-010) and China Medical University, Taiwan (Grant Nos. CMU110-S-21 and CMU111-MF-112).

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. Xie, C.; Liu, Y.-M.; Chen, J.; Yin, X.; Zhang, Z.-J. Quantum entanglement swapping of two arbitrary biqubit pure states. *Sci. China Phys.* **2016**, *59*, 1–9. [CrossRef]
2. Yuan, H.; Zhang, Z. Optimizing the scheme of bidirectional controlled quantum teleportation with a genuine five-qubit entangled state. *Mod. Phys. Lett. A* **2020**, *35*, 2050301. [CrossRef]
3. Zhang, W.; Li, B.; Zhang, Z. Cyclic deterministic bidirectional quantum controlled teleportation with maximally seven-qubit entangled state. *Laser Phys. Lett.* **2020**, *17*, 125202. [CrossRef]
4. Zhang, Z.; Xie, C.; Ye, B. Teleportation with Mixing State from Two Bell States Due to Qubit Confusion. *Int. J. Theor. Phys.* **2020**, *59*, 3249–3255. [CrossRef]
5. Zhang, Z.; Xing, H.; Ye, B.; Xie, C. Four-party quantum operation sharing with composite quantum channel in Bell and Yeo–Chua product state. *Mod. Phys. Lett. B* **2020**, *35*, 2150024. [CrossRef]
6. Zhang, Z.; Zhang, W.; Ye, B. Tripartite Quantum Operation Sharing with Six-Qubit Entangled State. *Int. J. Theor. Phys.* **2020**, *59*, 1605–1611. [CrossRef]
7. Zhang, Z. Tripartite quantum operation sharing with six-qubit highly entangled state. *Mod. Phys. Lett. A* **2021**, *36*, 2150034. [CrossRef]
8. Zhang, Z.; Yuan, H. Deterministic tripartite sharing of an arbitrary single-qubit operation with the five-qubit cluster state in a given entanglement structure. *Quantum Inf. Process.* **2021**, *20*, 3. [CrossRef]
9. Zhang, Z.; Zhang, L.; Zhuge, B.; Ye, B. Four-party deterministic quantum operation sharing with a generalized seven-qubit Brown state. *Laser Phys. Lett.* **2021**, *18*, 55202. [CrossRef]
10. Zhang, Z.; Zhang, L.; Zhuge, B.; Yuan, H.; Ye, B. Tripartite Quantum Operation Sharing with a Six-Qubit Absolutely Maximally Entangled State. *Int. J. Theor. Phys.* **2021**, *60*, 2520–2530. [CrossRef]
11. Gottesman, D.; Chuang, I. Quantum digital signatures. *arXiv* **2001**, arXiv:quant-ph/0105032.
12. Zeng, G.; Keitel, C.H. Arbitrated quantum-signature scheme. *Phys. Rev. A* **2002**, *65*, 42312. [CrossRef]
13. Lee, H.; Hong, C.; Kim, H.; Lim, J.; Yang, H.J. Arbitrated quantum signature scheme with message recovery. *Phys. Lett. A* **2004**, *321*, 295–300. [CrossRef]
14. Li, Q.; Chan, W.H.; Long, D.Y. Arbitrated quantum signature scheme using Bell states. *Phys. Rev. A* **2009**, *79*, 54307. [CrossRef]
15. Dunjko, V.; Wallden, P.; Andersson, E. Quantum digital signatures without quantum memory. *Phys. Rev. Lett.* **2014**, *112*, 40502. [CrossRef] [PubMed]
16. Luo, Y.P.; Hwang, T. Arbitrated quantum signature of classical messages without using authenticated classical channels. *Quantum Inf. Process.* **2014**, *13*, 113–120. [CrossRef]
17. Yang, Y.G.; Lei, H.; Liu, Z.C.; Zhou, Y.H.; Shi, W.M. Arbitrated quantum signature scheme based on cluster states. *Quantum Inf. Process.* **2016**, *15*, 2487–2497. [CrossRef]
18. Chen, F.L.; Liu, W.F.; Chen, S.G.; Wang, Z.H. Public-key quantum digital signature scheme with one-time pad private-key. *Quantum Inf. Process.* **2017**, *17*, 10. [CrossRef]
19. Zhang, L.; Sun, H.W.; Zhang, K.J.; Jia, H.Y. An improved arbitrated quantum signature protocol based on the key-controlled chained CNOT encryption. *Quantum Inf. Process.* **2017**, *16*, 70. [CrossRef]
20. Xin, X.; Wang, Z.; He, Q.; Yang, Q.; Li, F. New public-key quantum signature scheme with quantum one-way function. *Int. J. Theor. Phys.* **2019**, *58*, 3282–3294. [CrossRef]
21. Wen, X.; Niu, X.; Ji, L.; Tian, Y. A weak blind signature scheme based on quantum cryptography. *Opt. Commun.* **2009**, *282*, 666–669. [CrossRef]
22. Su, Q.; Zheng, H.; Qiaoyan, W.; Wenmin, L. Quantum blind signature based on two-state vector formalism. *Opt. Commun.* **2010**, *283*, 4408–4410.
23. 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]
24. Li, W.; Shi, J.; Shi, R.; Guo, Y. Blind quantum signature with controlled four-particle cluster States. *Int. J. Theor. Phys.* **2017**, *56*, 2579–2587. [CrossRef]
25. Luo, Y.P.; Tsai, S.L.; Hwang, T.; Kao, S.H. On "A new quantum blind signature with unlinkability". *Quantum Inf. Process.* **2017**, *16*, 87. [CrossRef]
26. Guo, X.; Zhang, J.Z.; Xie, S.C. A trusted third-party e-payment protocol based on quantum blind signature without entanglement. *Int. J. Theor. Phys.* **2018**, *57*, 2657–2664. [CrossRef]
27. Wang, T.Y.; Wei, Z.L. One-time proxy signature based on quantum cryptography. *Quantum Inf. Process.* **2012**, *11*, 455–463. [CrossRef]
28. Yang, C.W.; Luo, Y.P.; Hwang, T. Forgery attack on one-time proxy signature and the improvement. *Quantum Inf. Process.* **2014**, *13*, 2007–2016. [CrossRef]
29. Guo, R.; Cheng, X. Cryptanalysis and improvement of a (t, n) threshold group signature scheme. *Quantum Inf. Process.* **2022**, *21*, 37. [CrossRef]
30. Zhao, X.Q.; Wang, Y.Q.; Gong, L.H.; Zeng, Q.W. New bi-signature scheme based on GHZ states and W states. *Int. J. Theor. Phys.* **2019**, *58*, 1555–1567. [CrossRef]

31. Boyer, M.; Kenigsberg, D.; Mor, T. Quantum key distribution with classical bob. *Phys. Rev. Lett.* **2007**, *99*, 140501. [CrossRef] [PubMed]
32. Boyer, M.; Gelles, R.; Kenigsberg, D.; Mor, T. Semiquantum key distribution. *Phys. Rev. A* **2009**, *79*, 32341. [CrossRef]
33. Zou, X.; Qiu, D.; Li, L.; Wu, L.; Li, L. Semiquantum-key distribution using less than four quantum states. *Phys. Rev. A* **2009**, *79*, 52312. [CrossRef]
34. Krawec, W.O. Restricted attacks on semi-quantum key distribution protocols. *Quantum Inf. Process.* **2014**, *13*, 2417–2436. [CrossRef]
35. Krawec, W.O. Security of a semi-quantum protocol where reflections contribute to the secret key. *Quantum Inf. Process.* **2016**, *15*, 2067–2090. [CrossRef]
36. Wang, M.M.; Gong, L.M.; Shao, L.H. Efficient semiquantum key distribution without entanglement. *Quantum Inf. Process.* **2019**, *18*, 260. [CrossRef]
37. Zhu, K.N.; Zhou, N.R.; Wang, Y.Q.; Wen, X.J. Semi-quantum key distribution protocols with GHZ states. *Int. J. Theor. Phys.* **2018**, *57*, 3621–3631. [CrossRef]
38. Krawec, W.O. Mediated semiquantum key distribution. *Phys. Rev. A* **2015**, *91*, 32323. [CrossRef]
39. Tsai, C.W.; Yang, C.W.; Lee, N.Y. Lightweight mediated semi-quantum key distribution protocol. *Mod. Phys. Lett. A* **2019**, *34*, 1950281. [CrossRef]
40. 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]
41. Zou, X.; Qiu, D.; Zhang, S.; Mateus, P. Semiquantum key distribution without invoking the classical party's measurement capability. *Quantum Inf. Process.* **2015**, *14*, 2981–2996. [CrossRef]
42. Yu, K.F.; Yang, C.W.; Liao, C.H.; Hwang, T. Authenticated semi-quantum key distribution protocol using Bell states. *Quantum Inf. Process.* **2014**, *13*, 1457–1465. [CrossRef]
43. Tsai, C.W.; Yang, C.W. Lightweight authenticated semi-quantum key distribution protocol without trojan horse attack. *Laser Phys. Lett.* **2020**, *17*, 75202. [CrossRef]
44. Wang, H.W.; Tsai, C.W.; Lin, J.; Huang, Y.Y.; Yang, C.W. Efficient and secure measure-resend authenticated semi-quantum key distribution protocol against reflecting attack. *Mathematics* **2022**, *10*, 1241. [CrossRef]
45. Wang, H.W.; Tsai, C.W.; Lin, J.; Yang, C.W. Authenticated semi-quantum key distribution protocol based on W states. *Sensors* **2022**, *22*, 4998. [CrossRef]
46. Gheorghiu, V. Generalized semiquantum secret-sharing schemes. *Phys. Rev. A* **2012**, *85*, 052309. [CrossRef]
47. Yang, C.W.; Hwang, T. Efficient key construction on semi-quantum secret sharing protocols. *Int. J. Quantum Inf.* **2013**, *11*, 1350052. [CrossRef]
48. Li, Z.; Li, Q.; Liu, C.; Peng, Y.; Chan, W.H.; Li, L. Limited resource semiquantum secret sharing. *Quantum Inf. Process.* **2018**, *17*, 285. [CrossRef]
49. Tsai, C.W.; Chang, Y.C.; Lai, Y.H.; Yang, C.W. Cryptanalysis of limited resource semi-quantum secret sharing. *Quantum Inf. Process.* **2020**, *19*, 224. [CrossRef]
50. Li, Q.; Chan, W.H.; Long, D.Y. Semiquantum secret sharing using entangled states. *Phys. Rev. A* **2010**, *82*, 22303. [CrossRef]
51. Lin, J.; Yang, C.W.; Tsai, C.W.; Hwang, T. Intercept-resend attacks on semiquantum secret sharing and the improvements. *Int. J. Theor. Phys.* **2013**, *52*, 156–162. [CrossRef]
52. Yin, A.H.; Tong, Y. A novel semi-quantum secret sharing scheme using entangled states. *Mod. Phys. Lett. B* **2018**, *32*, 1850256. [CrossRef]
53. Tian, Y.; Li, J.; Chen, X.B.; Ye, C.Q.; Li, H.J. An efficient semi-quantum secret sharing protocol of specific bits. *Quantum Inf. Process.* **2021**, *20*, 217. [CrossRef]
54. Xie, C.; Li, L.; Qiu, D. A novel semi-quantum secret sharing scheme of specific bits. *Int. J. Theor. Phys.* **2015**, *54*, 3819–3824. [CrossRef]
55. Yin, A.; Fu, F. Eavesdropping on semi-quantum secret sharing scheme of specific bits. *Int. J. Theor. Phys.* **2016**, *55*, 4027–4035. [CrossRef]
56. Gao, X.; Zhang, S.; Chang, Y. Cryptanalysis and improvement of the semi-quantum secret sharing protocol. *Int. J. Theor. Phys.* **2017**, *56*, 2512–2520. [CrossRef]
57. Tsai, C.W.; Yang, C.W.; Lin, J. Multiparty mediated quantum secret sharing protocol. *Quantum Inf. Process.* **2022**, *21*, 63. [CrossRef]
58. Tsai, C.W.; Yang, C.W.; Lee, N.Y. Semi-quantum secret sharing protocol using W-state. *Mod. Phys. Lett. A* **2019**, *34*, 1950213. [CrossRef]
59. Li, C.; Ye, C.; Tian, Y.; Chen, X.B.; Li, J. Cluster-state-based quantum secret sharing for users with different abilities. *Quantum Inf. Process.* **2021**, *20*, 385. [CrossRef]
60. Zou, X.; Qiu, D. Three-step semiquantum secure direct communication protocol. *Sci. China Phys. Mech.* **2014**, *57*, 1696–1702. [CrossRef]
61. Zhang, M.H.; Li, H.F.; Xia, Z.Q.; Feng, X.Y.; Peng, J.Y. Semiquantum secure direct communication using EPR pairs. *Quantum Inf. Process.* **2017**, *16*, 117. [CrossRef]
62. Xie, C.; Li, L.; Situ, H.; He, J. Semi-quantum secure direct communication scheme based on Bell States. *Int. J. Theor. Phys.* **2018**, *57*, 1881–1887. [CrossRef]

63. Yan, L.; Sun, Y.; Chang, Y.; Zhang, S.; Wan, G.; Sheng, Z. Semi-quantum protocol for deterministic secure quantum communication using Bell states. *Quantum Inf. Process.* **2018**, *17*, 315. [CrossRef]
64. Sun, Y.; Yan, L.; Chang, Y.; Zhang, S.; Shao, T.; Zhang, Y. Two semi-quantum secure direct communication protocols based on Bell states. *Mod. Phys. Lett. A* **2019**, *34*, 1950004. [CrossRef]
65. Yang, C.W.; Tsai, C.W. Intercept-and-resend attack and improvement of semiquantum secure direct communication using EPR pairs. *Quantum Inf. Process.* **2019**, *18*, 306. [CrossRef]
66. Rong, Z.; Qiu, D.; Zou, X. Semi-quantum secure direct communication using entanglement. *Int. J. Theor. Phys.* **2020**, *59*, 1807–1819. [CrossRef]
67. Yang, C.W. Efficient and secure semi-quantum secure direct communication protocol against double CNOT attack. *Quantum Inf. Process.* **2020**, *19*, 50. [CrossRef]
68. Yang, C.W.; Tsai, C.W. Advanced semi-quantum secure direct communication protocol based on bell states against flip attack. *Quantum Inf. Process.* **2020**, *19*, 126. [CrossRef]
69. Zhang, X.; Zhou, R.G. An efficient and novel semi-quantum deterministic secure quantum communication protocol. *Int. J. Theor. Phys.* **2022**, *61*, 94. [CrossRef]
70. Yan-Feng, L. Semi-quantum private comparison using single photons. *Int. J. Theor. Phys.* **2018**, *57*, 3048–3055. [CrossRef]
71. Ye, T.Y.; Ye, C.Q. Measure-resend semi-quantum private comparison without entanglement. *Int. J. Theor. Phys.* **2018**, *57*, 3819–3834. [CrossRef]
72. Lin, P.H.; Hwang, T.; Tsai, C.W. Efficient semi-quantum private comparison using single photons. *Quantum Inf. Process.* **2019**, *18*, 207. [CrossRef]
73. Li, Y.C.; Chen, Z.Y.; Xu, Q.D.; Gong, L.H. Two semi-quantum private comparison protocols of size relation based on single particles. *Int. J. Theor. Phys.* **2022**, *61*, 157. [CrossRef]
74. Jiang, L.Z. Semi-quantum private comparison based on Bell states. *Quantum Inf. Process.* **2020**, *19*, 180. [CrossRef]
75. Tsai, C.W.; Lin, J.; Yang, C.W. Cryptanalysis and improvement in semi-quantum private comparison based on Bell states. *Quantum Inf. Process.* **2021**, *20*, 120. [CrossRef]
76. Xie, L.; Li, Q.; Yu, F.; Lou, X.; Zhang, C. Cryptanalysis and improvement of a semi-quantum private comparison protocol based on Bell states. *Quantum Inf. Process.* **2021**, *20*, 244. [CrossRef]
77. Li, Z.; Liu, T.; Zhu, H. Private comparison protocol for multiple semi-quantum users based on Bell States. *Int. J. Theor. Phys.* **2022**, *61*, 177. [CrossRef]
78. Tian, Y.; Li, J.; Chen, X.B.; Ye, C.Q.; Li, C.Y.; Hou, Y.Y. An efficient semi-quantum private comparison without pre-shared keys. *Quantum Inf. Process.* **2021**, *20*, 360. [CrossRef]
79. Yan, L.; Zhang, S.; Chang, Y.; Wan, G.; Yang, F. Semi-quantum private comparison protocol with three-particle G-like states. *Quantum Inf. Process.* **2021**, *20*, 17. [CrossRef]
80. Li, Q.; Li, P.; Xie, L.; Chen, L.; Quan, J. Security analysis and improvement of a semi-quantum private comparison protocol with three-particle G-like states. *Quantum Inf. Process.* **2022**, *21*, 127. [CrossRef]
81. Tian, Y.; Li, J.; Ye, C.; Chen, X.B.; Li, C. W-state-based semi-quantum private comparison. *Int. J. Theor. Phys.* **2022**, *61*, 18. [CrossRef]
82. Zhao, X.Q.; Chen, H.Y.; Wang, Y.Q.; Zhou, N.R. Semi-quantum bi-signature scheme based on W states. *Int. J. Theor. Phys.* **2019**, *58*, 3239–3251. [CrossRef]
83. Ozaydin, F.; Bugu, S.; Yesilyurt, C.; Altintas, A.A.; Tame, M.; Özdemir, Ş.K. Fusing multiple W states simultaneously with a Fredkin gate. *Phys. Rev. A* **2014**, *89*, 42311. [CrossRef]
84. Bugu, S.; Ozaydin, F.; Ferrus, T.; Kodera, T. Preparing Multipartite Entangled Spin Qubits via Pauli Spin Blockade. *Sci. Rep.* **2020**, *10*, 3481. [CrossRef]
85. Ozaydin, F.; Yesilyurt, C.; Bugu, S.; Koashi, M. Deterministic preparation of W states via spin-photon interactions. *Phys. Rev. A* **2021**, *103*, 52421. [CrossRef]
86. Li, K.; Kong, F.-Z.; Yang, M.; Ozaydin, F.; Yang, Q.; Cao, Z.-L. Generating multi-photon W-like states for perfect quantum teleportation and superdense coding. *Quantum Inf. Process.* **2016**, *15*, 3137–3150. [CrossRef]