entropy

Article

A New Quantum Blind Signature Scheme with BB84-State

Feng-Lin Chen [1,*], Zhi-Hua Wang [1,2] and Yong-Mo Hu [1]

[1] School of Mathematics and Computation Science, Anqing Normal University, Anqing 246133, China; zhihuaw@mail.ustc.edu.cn (Z.-H.W.); huyongmo@aqnu.edu.cn (Y.-M.H.)
[2] School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China
* Correspondence: chenfenglin@aqnu.edu.cn

Received: 21 January 2019; Accepted: 25 March 2019; Published: 28 March 2019

Abstract: The blind signature is widely used in cryptography applications because it can prevent the signer from gaining the original message. Owing to the unconditional security, the quantum blind signature is more advantageous than the classical one. In this paper, we propose a new provable secure quantum blind signature scheme with the nonorthogonal single-photon BB84-state and provide a new method to encode classical messages into quantum signature states. The message owner injects a randomizing factor into the original message and then strips the blind factor from the quantum blind signature signed by the blind signer. The verifier can validate the quantum signature and announce it publicly. At last, the analytical results show that the proposed scheme satisfies all of the security requirements of the blind signature: blindness, unforgeability, non-repudiation, unlinkability, and traceability. Due to there being no use of quantum entanglement states, the total feasibility and practicability of the scheme are obviously better than the previous ones.

Keywords: BB84-state; quantum fingerprint; quantum encryption algorithm; quantum blind signature; unconditional security

1. Introduction

The security of classical signature cryptography depends on solving some difficult mathematical problems, such as factoring large integers and solving the discrete logarithm. It is known that these problems will become rather simple with the emergence of quantum computers. The quantum algorithm proposed by Shor [1] in 1994 can solve the problem of integer factorization in polynomial time. Accordingly, quantum cryptography will make a revolutionary impact on the classical one. One of the known examples of quantum cryptography is the quantum key distribution (QKD) [2–5], which offers a solution of the shared key exchange with information-theoretical security. Quite a few branches of QKD have attracted a great deal of attention, and many effective results have been proposed, including quantum private query (QPQ) [6–8], quantum digital signature (QDS) [9–13] and so on.

The first QDS scheme, which is analogous to the classical Lamport's signature scheme, was proposed by Gottesman et al. [9] in 2001. In 2002, Zeng et al. [10] first proposed the arbitrated QDS scheme with GHZstates based on symmetric cryptography. In 2014, Dunjko et al. [11] proposed the first QDS scheme with no quantum memory, which made the quantum signature feasible and practicable under the current quantum technology. Wallden et al. [12] presented a QDS scheme with quantum-key-distribution components in 2015. In 2016, Amiri et al. [13] proposed a QDS scheme that did not require trusted quantum channels and only relied on secret shared keys generated using QKD. With the proposal of the measurement device-independent (MDI) QKD by Lo et al. [14], Puthoor et al. [15] first presented an MDI-QDS scheme, which is secure against all detector side-channel attacks. In 2017, Yin et al. [16] and Roberts et al. [17] made the attempt to implement experimentally the MDI-QDS.

The blind signature was first proposed by Chaum [18] in 1982. The blind signature can effectively prevent the blind signer from getting the original message because of its blindness, so it has a wide range of applications in the fields of E-commerce and block-chain. So far, some quantum blind signature (QBS) schemes [19–33] have been presented. In 2009, Wen et al. [19] first proposed the weak QBS scheme based on EPRpairs. In 2010, Su et al. [20] proposed a QBS scheme based on EPR with two-state vector formalism, and then, Yang et al. [21] pointed out some attacks on Su's scheme [20] and proposed an enhanced one. However, Zhang et al. [22] declared that the dishonest signer could obtain some secret keys in Yang's improved scheme [21]. In 2014, Khodambashi et al. [23] proposed a sessional QBS based on EPR, where the message signature cannot be forged by the dishonest verifier. In 2015, Shi et al. [24] proposed a new QBS scheme with unlinkability based on EPR and quantum teleportation. In 2017, Luo et al. [25] pointed out a security loophole of forgery in Shi's QBS scheme [24]. With the χ-type entangled states, Yin et al. [26] proposed a QBS scheme in 2012. With the GHZ states, Wang et al. [27] proposed a QBS scheme in 2013. Zuo et al. [28] found that the dishonest verifier could forge the blind signature in [19,26,27]. Accordingly, Zuo et al. [28] and Ribeiro et al. [29] advised that a trusted center should be involved in QBS schemes. Based on offline trusted repositories, Ribeiro et al [29] presented a perfectly secure QBS scheme, which used Bell states, unitary operations, and so on, in 2015. With the two-photon entangled coding matrix to pass the secret shared key, Lai et al. [30] presented a QBS scheme in 2017. Besides the above QBS schemes with multiple photons, Wang et al. [31] proposed a fair QBS scheme with a single photon in 2010. However, He et al. [32] and Zou et al. [33] found that this scheme was vulnerable to non-forgeability attack. All these QBS schemes [19–33] are mainly divided into two broad categories: multi-photon entanglement QBS [19–30] and single-photon QBS [31–33]. Unlike the proposed QBS schemes with the single photon in [31–33], in this paper, we propose a new single-photon QBS scheme encoding with the indistinguishable BB84-state. To guarantee the unconditional security of the proposed scheme, we employ the quantum fingerprint [34] and Zhang et al.'s improved key-controlled-"T" quantum one time pad (QOTP) [35,36] based on Boykin and Roychowdhury's QOTP [37]. In the proposed scheme, we give the hypothesis that a trusted arbitrator is known by all participants prior to the execution of the protocol. We give a proof of the correctness of the scheme. Security analyses show that the scheme satisfies all the properties of the blind signature: blindness, unforgeability, non-repudiation, unlinkability, and traceability.

The rest of this paper is organized as follows. In Section 2, we introduce some necessary preliminaries. In Section 3, we present the new QBS scheme with the BB84-state. Subsequently, the security analyses of this scheme are presented in Section 4. Finally, some conclusions are drawn in Section 5.

2. Preliminary Theory

2.1. Properties of the Blind Signature

In general, a blind signature protocol includes four stages, namely message blinding, blind message signing, message unblinding, and signature verification. The original message owner, Alice, first makes a blind transformation on the original message m and gets blind message $\widetilde{m}$. Alice sends the transformed blind data $\widetilde{m}$ to the blind signer, Bob. Then, Bob signs the $\widetilde{m}$ and obtains the blind signature $Sign(\widetilde{m})$, and the signature is sent back to Alice. Alice strips the blind factor from the $Sign(\widetilde{m})$ and gets the signature $Sign(m)$ of the original message m. The verifier, Charlie, can verify the correctness of $Sign(m)$.

Generally speaking, a perfect blind signature should satisfy the following properties [18].

- Unforgeability: No one can generate an effective blind signature except the signer himself/herself. This is one of the most basic requirements.

- Non-repudiation: Once a signer has signed a message, he/she cannot deny his/her signature of the message.
- Blindness: Although a signer has signed a message, he/she cannot get the concrete content of the message.
- Unlinkability: Once the signature of the message is public, the signer cannot determine whether he/she has signed the message.
- Traceability: Once a dispute happens, the verifier can trace the signature.

The blind signature satisfying the above properties is considered to be secure. These five properties are the criteria that we should follow in designing blind signatures. The performance of the blind signature is also judged based on these properties.

2.2. Quantum Fingerprint

The quantum fingerprint [34], proposed by Buhrman et al. in 2001, is the most appealing protocol in quantum communication complexity (QCC) protocols [38,39]. In this model, two parties (Alice and Bob) select separately inputs $x, y \in \{0,1\}^n$ and send their quantum fingerprints messages to a third party, called the Referee. The Referee must determine whether x equals y or not with a small error probability ϵ. To construct a large set of nearly orthogonal quantum states explicitly, consider an error-correcting code $E : \{0,1\}^n \longrightarrow \{0,1\}^t$ where the distance between distinct code words $E(x)$ and $E(y)$ is at least $(1-\delta)t$, here $0 < \delta < 1$, $c > 1$, $t = cn$. For each $x \in \{0,1\}^n$, define the $(log_2(t)+1)$-qubit state:

$$|f(x)\rangle \overset{def}{=} \frac{1}{\sqrt{t}} \sum_{i=1}^{t} |i\rangle |E_i(x)\rangle. \tag{1}$$

Note that two distinct code words can be equal in at most δt positions for any $x \neq y$. Consequently, each pair $(|f(x)\rangle, |f(y)\rangle)$ has an inner product $\langle f(x)|f(y)\rangle \leq \delta t/t = \delta$. When the Referee receives the quantum fingerprints $|f(x)\rangle$ and $|f(y)\rangle$, he measures and outputs the first qubit of the states $(H \otimes I)(c\text{-}SWAP)(H \otimes I)|0\rangle|f(x)\rangle|f(y)\rangle$. By measuring the first qubit of this state with computational basis $\{|0\rangle, |1\rangle\}$, the Referee outputs $|1\rangle$ (meaning that $x = y$) with probability $(1 - |\langle f(x)|f(y)\rangle|^2)/2$. The probability is zero if $x = y$ and at least $(1-\delta^2)/2$ if $x \neq y$. Thus, the test determines which case holds with one-sided error probability $(1+\delta^2)/2$. This error probability can be reduced to any $\varepsilon > 0$ by setting the fingerprint $|f(x)\rangle$ to $|f(x)\rangle^{\otimes l}$ for a suitable $l \in O(log_2(1/\varepsilon))$.

So far, several experiments [40–44] have reported successful attempts at implementing the quantum fingerprint.

2.3. Improved QOTP Encryption

In 2003, Boykin and Roychowdhury presented the QOTP encryption [37], which is used to encrypt securely n-qubit quantum states with the secret classical $2n$-bit key. Denote the n-qubit quantum message by $|P\rangle = \bigotimes_{i=1}^{n} |P_i\rangle$ and the n-qubit ciphertext message by $|C\rangle = \bigotimes_{i=1}^{n} |C_i\rangle$, where $|P_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$, $|C_i\rangle = \alpha'_i|0\rangle + \beta'_i|1\rangle$, $|\alpha_i|^2 + |\beta_i|^2 = |\alpha'_i|^2 + |\beta'_i|^2 = 1$, $i \in [1,n]$. With the secret classical $2n$-bit key k, the QOTP encryption E_k on $|P\rangle$ can be described by $E_k|P\rangle = \bigotimes_{i=1}^{n} \sigma_x^{k_{2i}} \sigma_z^{k_{2i-1}} |P_i\rangle$ and the corresponding decryption D_k on $|C\rangle$ by $D_k|C\rangle = \bigotimes_{i=1}^{n} \sigma_z^{k_{2i-1}} \sigma_x^{k_{2i}} |C_i\rangle$. Since the original QOTP [37] is a bitwise protocol, Zhang et al. [35,36] pointed out that it would encounter forgery attack when it is used in the quantum signature. Now, some improved QOTP encryption schemes have been proposed, such as those in [35,36,45]. Since the location permutation of the quantum state is supplemented in the original QOTP, the improved QOTP schemes are no longer the bitwise encryption and provide higher security.

In order to use the improved QOTP to encrypt the classical message, some methods must be used to transform the classical message to the quantum one. Here, we give a simple example to demonstrate this one-to-one correspondence between them. Let us denote the n-bit classical message by $M = M_1 M_2 \cdots M_i \cdots M_n$ and its corresponding n-qubit quantum one by $|M\rangle = \bigotimes_{i=1}^{n} |M_i\rangle_i$, where $i \in [1, n]$. When i is odd, encode M_i with the rectilinear basis, namely $|0\rangle_i = |0\rangle$, $|1\rangle_i = |1\rangle$. When i is even, encode M_i with the diagonal basis, namely $|0\rangle_i = |+\rangle$, $|1\rangle_i = |-\rangle$. According to the parity of the position of each quantum state, a different basis is used to measure the decrypted quantum state, so that the classical message can be recovered when decrypting. Because of the permutation of the quantum position, attacker cannot obtain M from the disordered quantum ciphertext by measurement without the secret key. For the sake of brevity and readability, the improved QOTP encryption on classical M is denoted by $E_k(M)$ with the secret key k. Once the length of the message M exceeds n, we can divide M into several segments of length n and then encrypt them separately.

3. Quantum Blind Signature Scheme

We first give an encoding method of BB84-state so as to establish the one-to-one correspondence between the classical bit and the quantum one. With the BB84-state encoding, we then propose our new QBS scheme.

3.1. BB84-State Encoding

Let $p = (p_1, p_2, \cdots, p_n), q = (q_1, q_2, \cdots, q_n), r = (r_1, r_2, \cdots, r_n) \in \{0, 1\}^n$, where p_i is the ith-bit in p (q_i, r_i in q, r, respectively), $i \in [1, n]$. We give an encoding rule that maps (p_i, q_i) to a quantum BB84-state in set $\{|+\rangle, |-\rangle, |0\rangle, |1\rangle\}$ and define:

$$|\varphi\rangle_{p_i,q_i} \overset{def}{=} \begin{cases} |+\rangle & (p_i = 0, q_i = 0), \\ |-\rangle & (p_i = 1, q_i = 1), \\ |0\rangle & (p_i = 1, q_i = 0), \\ |1\rangle & (p_i = 0, q_i = 1). \end{cases} \tag{2}$$

For n-qubit $|\varphi\rangle_{p,q}$, we define:

$$|\varphi\rangle_{p,q} \overset{def}{=} \otimes_{i=1}^{n} |\varphi\rangle_{p_i,q_i}. \tag{3}$$

According to Equation (2), it is easy to draw the following conclusions, where $\oplus$ is the exclusive-or (XOR) operation and the symbol $\cong$ denotes the equivalence relation between two quantum states, which are different from constant coefficient (for instance, $|+\rangle \cong -|+\rangle$).

Corollary 1. $|\varphi\rangle_{p_i,q_i} = \begin{cases} |0\rangle, |+\rangle & (q_i = 0) \\ |1\rangle, |-\rangle & (q_i = 1) \end{cases}$.

Corollary 2. $|\varphi\rangle_{p_i,q_i} = \begin{cases} |+\rangle, |-\rangle & (p_i \oplus q_i = 0) \\ |0\rangle, |1\rangle & (p_i \oplus q_i = 1) \end{cases}$.

Corollary 3. $X|\varphi\rangle_{p_i,q_i} \cong \begin{cases} |+\rangle & (p_i = 0, q_i = 0) \\ |-\rangle & (p_i = 1, q_i = 1) \\ |1\rangle & (p_i = 1, q_i = 0) \\ |0\rangle & (p_i = 0, q_i = 1) \end{cases}$.

Corollary 4. $Z|\varphi\rangle_{p_i,q_i} \cong \begin{cases} |-\rangle & (p_i = 0, q_i = 0) \\ |+\rangle & (p_i = 1, q_i = 1) \\ |0\rangle & (p_i = 1, q_i = 0) \\ |1\rangle & (p_i = 0, q_i = 1) \end{cases}.$

Corollary 5. $H^{r_i}|\varphi\rangle_{p_i,q_i} = |\varphi\rangle_{p_i \oplus r_i, q_i}$.

Corollary 6. $Y^{r_i}|\varphi\rangle_{p_i,q_i} = \zeta^{r_i(3+2p_i)}|\varphi\rangle_{p_i \oplus r_i, q_i \oplus r_i} \cong |\varphi\rangle_{p_i \oplus r_i, q_i \oplus r_i}$, *where* ζ *is an imaginary unit satisfying* $\zeta^2 = -1$.

3.2. The Proposed Quantum Blind Signature Scheme

Substituting the quantum states for all or part of the classical messages, the so-called QBS inherits the definition and signature framework of the classical one. The QBS could achieve unconditional security through a combination of quantum theory and classical cryptography. The proposed signature scheme consists of the initial phase, the blinding phase, the signing phase, the unblinding phase, and the verifying phase.

3.2.1. Initial Phase

According to the different responsibilities in our proposed QBS scheme, there are five different roles: message owner, blind signer, verifier, arbitrator, and external attacker. Let Alice be the original message owner, Bob the blind signer, Charlie the signature verifier, Trent the arbitrator, and Eve the malicious external attacker. In the scheme, we give the hypothesis that Trent is known by all participants prior to the execution of the protocol and acts as the trusted arbitrator. In the remainder of this paper, we abbreviate Alice to A, Bob to B, Charlie to C, Trent to T, and Eve to E just for brevity. C shares each $2n$-bit secret key k_{AC} and k_{BC} with A and B, respectively. T shares each $2n$-bit secret key k_{AT} and k_{CT} with A and C, respectively. At the same time, A shares a $2n$-bit secret key k_{AB} with B. These keys can be generated in a secure manner, e.g., direct face-to-face contact and QKD protocols with unconditional security such as [2–5].

3.2.2. Blinding Phase

Step B1. The message owner A first prepares the original message m of the n-bit string. Then, A selects randomly the blind factor w of the n-bit string and blinds m to blind message $\widetilde{m}$ based on the formula $\widetilde{m} = m \oplus w$.

Step B2. According to Equations (2) and (3), A generates n-qubit blind states $|\varphi\rangle_{\widetilde{m} \oplus k'_{AB}, \widetilde{m}}$ with the n-bit blind message $\widetilde{m}$ and key k'_{AB}, where the n-bit k'_{AB} is derived from the $2n$-bit shared key k_{AB} satisfying $k'_{AB_i} = k_{AB_{2i}} \oplus k_{AB_{(2i+1)}}$, $i \in [1, n]$. According to Equation (1), A generates quantum fingerprint $|f(\widetilde{m})\rangle$ for blind message $\widetilde{m}$. With the shared key k_{AC} and k_{AB}, A applies the improved QOTP [35,36,45], which is described in Subsection 2.3, to encrypt her classical message m and blind factor w, and then obtains $E_{k_{AB}}(E_{k_{AC}}(m||w))$, where the notation $||$ denotes the concatenation of strings.

Step B3. A denotes $Sign_{AB} \overset{def}{=} \{|\varphi\rangle_{\widetilde{m} \oplus k'_{AB}, \widetilde{m}}, |f(\widetilde{m})\rangle, E_{k_{AB}}(E_{k_{AC}}(m||w))\}$ and transmits $Sign_{AB}{}^{\otimes 2}$ to B through the quantum channel, where $Sign_{AB}{}^{\otimes 2}$ represents two copies of $Sign_{AB}$.

3.2.3. Signing phase

Step S1. Analogous to the method in **Step B1**, B obtains the n-bit key k'_{AB} from the shared $2n$-bit key k_{AB} between A and B. If the k'_{AB_i} is zero, B selects the diagonal basis $\{|+\rangle, |-\rangle\}$, otherwise rectilinear basis $\{|0\rangle, |1\rangle\}$. According to this basis rule, B measures all the qubits of the indistinguishable BB84-state $|\varphi\rangle_{\widetilde{m} \oplus k'_{AB}, \widetilde{m}}$ corresponding in $Sign_{AB}$ and gets the blind message $\widetilde{m}'$ with the key k'_{AB}.

Step S2. According to Equation (1), B generates quantum fingerprint $|f(\widetilde{m}')\rangle$. B then compares the generated $|f(\widetilde{m}')\rangle$ with state $|f(\widetilde{m})\rangle$ from $Sign_{AB}$ and judges whether they are equal based on quantum fingerprint theory in [34]. If they are not equal, then B stops the scheme, otherwise draws the conclusion $\widetilde{m}' = \widetilde{m}$ and goes on.

Step S3. B first selects randomly two n-bit strings u and v. According to Equation (2) and Equation (1), B then generates respectively the QBS BB84-state $|\varphi\rangle_{\widetilde{m}\oplus u,v}$ and quantum fingerprint $|f(u||v||\widetilde{m})\rangle$ with u, v, and $\widetilde{m}$. With the shared key k_{BC}, B encrypts his strings u and v and then gets $E_{k_{BC}}(u,v)$. From the receiving $Sign_{AB}$, B decrypts the $E_{k_{AB}}(E_{k_{AC}}(m||w))$ with his shared key k_{AB} and gets $E_{k_{AC}}(m||w)$, then encrypts it with his shared key k_{BC} and obtains $E_{k_{BC}}(E_{k_{AC}}(m||w))$. B denotes $Sign_{BC} \overset{def}{=} \{|f(u||v||\widetilde{m})\rangle, E_{k_{BC}}(u,v), E_{k_{BC}}(E_{k_{AC}}(m||w))\}$.

Step S4. B transmits ${Sign_{BC}}^{\otimes 2}$ and ${|\varphi\rangle_{\widetilde{m}\oplus u,v}}^{\otimes 2}$ to A through the quantum channel.

3.2.4. Unblinding Phase

Step U1. After receiving the blind signature $|\varphi\rangle_{\widetilde{m}\oplus u,v}$ for blind message $\widetilde{m}$ signed by B, A applies H^w to $|\varphi\rangle_{\widetilde{m}\oplus u,v}$ with her blind factor w and gets $H^w|\varphi\rangle_{\widetilde{m}\oplus u,v}$, which is a quantum signature for the original message m. With the shared key k_{AC}, A generates $E_{k_{AC}}(H^w|\varphi\rangle_{\widetilde{m}\oplus u,v})$ and $E_{k_{AC}}(m||w)$. A denotes $Sign_{AC} \overset{def}{=} \{E_{k_{AC}}(H^w|\varphi\rangle_{\widetilde{m}\oplus u,v}), E_{k_{AC}}(m||w)\}$.

Step U2. A generates $E_{k_{AT}}({Sign_{AC}}^{\otimes 2}, {Sign_{BC}}^{\otimes 2})$ and transmits it to T through the quantum channel.

Step U3. T decrypts the received $E_{k_{AT}}({Sign_{AC}}^{\otimes 2}, {Sign_{BC}}^{\otimes 2})$ and gets ${Sign_{AC}}^{\otimes 2}$ and ${Sign_{BC}}^{\otimes 2}$. Then, T performs the C-SWAPtest [34] to compare the two copies of $Sign_{AC}$ in ${Sign_{AC}}^{\otimes 2}$. The same test is also done on ${Sign_{BC}}^{\otimes 2}$. Once an unequal result of the comparison occurs, T draws the conclusion that the signature is invalid and aborts the process. After T finishes the comparison tests successfully, he preserves one copy of $Sign_{AC}$ and $Sign_{BC}$ to be prepared to solve disputes when they arise in the future. Finally, T generates $E_{k_{CT}}(Sign_{AC}, Sign_{BC})$ with another copy of $Sign_{AC}$ and $Sign_{BC}$ and transmits it to C through the quantum channel.

3.2.5. Verifying Phase

Step V1. C first gets $Sign_{AC}$ and $Sign_{BC}$ from the received $E_{k_{CT}}(Sign_{AC}, Sign_{BC})$ with his shared key k_{CT}. Then, C decrypts the $E_{k_{BC}}(E_{k_{AC}}(m||w))$ in $Sign_{BC}$ with his shared key k_{BC}, gets $E'_{k_{AC}}(m||w)$, and performs the C-SWAP test [34] to compare it with $E_{k_{AC}}(m||w)$ in $Sign_{AC}$. If the result of the comparison is not equal, C draws the conclusion that the signature is invalid and aborts the process. Otherwise, C then applies the key-controlled-"T" QOTP to decrypt $E_{k_{AC}}(m||w)$ with his shared key k_{AC} and finally gets (m, w).

Step V2. After getting $E_{k_{BC}}(u,v)$ from the $Sign_{BC}$, C decrypts $E_{k_{BC}}(u,v)$ with his shared key k_{BC} and then gets (u, v).

Step V3. From the received $Sign_{AC}$, C decrypts $E_{k_{AC}}(H^w|\varphi\rangle_{\widetilde{m}\oplus u,v})$ with his shared key k_{AC} and gets $H^w|\varphi\rangle_{\widetilde{m}\oplus u,v}$. With the m obtained in ***Step V1***, C applies H^m to $H^w|\varphi\rangle_{\widetilde{m}\oplus u,v}$ and gets $H^m H^w|\varphi\rangle_{\widetilde{m}\oplus u,v}$.

Step V4. With the u, v obtained in ***Step V2***, C performs single-particle measurements on the n-qubit $H^m H^w|\varphi\rangle_{\widetilde{m}\oplus u,v}$ obtained in ***Step V3*** and gets u', v'. The rules of measurement are as follows. According to Corollary 2, C uses diagonal basis $\{|+\rangle, |-\rangle\}$ to measure the BB84-state if $u_i \oplus v_i = 0$, otherwise rectilinear basis $\{|0\rangle, |1\rangle\}$. Based on the measurement result and Equation (2), C can deduce the corresponding u'_i, v'_i. C aborts the process if $u_i \neq u'_i$ or $v_i \neq v'_i$ for some $i \in [1, n]$, otherwise goes on.

Step V5. C generates quantum fingerprint $|f(u||v||(m \oplus w))\rangle$ with the deduced (u, v) and (m, w) and then compares it with $|f(u||v||\widetilde{m})\rangle$ in $Sign_{BC}$ from B. If the result of comparison is equal, C draws the conclusion that the signature is valid, otherwise declares that the signature is not valid.

Step V6. According to Equation (2), C regenerates the quantum BB84-state signature $|\varphi\rangle_{m\oplus u,v}$ with the known m, u, and v. C announces publicly the QBS correctness and declares the signature

$\{m, |\varphi\rangle_{m\oplus u,v}\}$ to the public.

The whole flow-process diagram of the proposed QBS scheme is given in Figure 1.

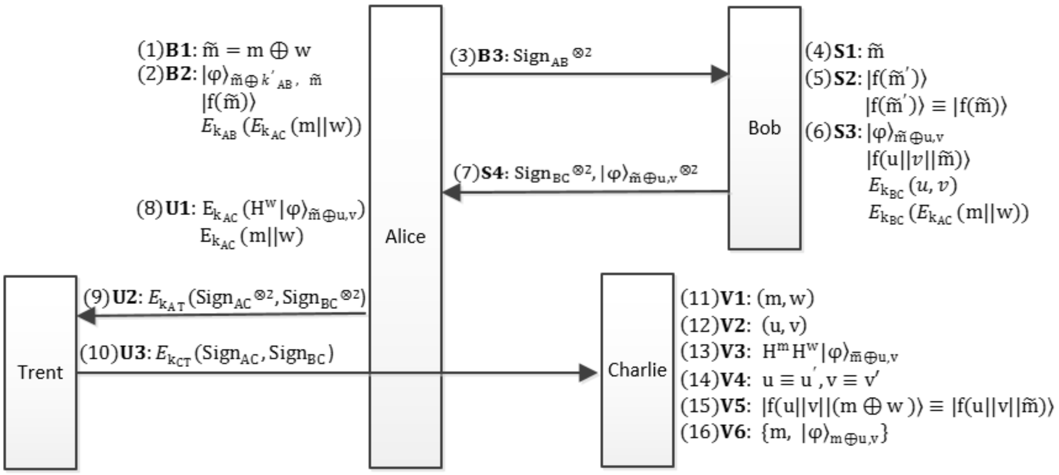
(1)**B1**: $\tilde{m} = m \oplus w$
(2)**B2**: $|\varphi\rangle_{\tilde{m}\oplus k'_{AB},\ \tilde{m}}$
$|f(\tilde{m})\rangle$
$E_{k_{AB}}(E_{k_{AC}}(m||w))$
(3)**B3**: $\mathrm{Sign}_{AB}{}^{\otimes 2}$
(4)**S1**: $\tilde{m}$
(5)**S2**: $|f(\tilde{m}')\rangle$
$|f(\tilde{m}')\rangle \equiv |f(\tilde{m})\rangle$
(6)**S3**: $|\varphi\rangle_{\tilde{m}\oplus u,v}$
$|f(u||v||\tilde{m})\rangle$
$E_{k_{BC}}(u, v)$
$E_{k_{BC}}(E_{k_{AC}}(m||w))$
Bob
(7)**S4**: $\mathrm{Sign}_{BC}{}^{\otimes 2}, |\varphi\rangle_{\tilde{m}\oplus u,v}{}^{\otimes 2}$
(8)**U1**: $E_{k_{AC}}(H^{w}|\varphi\rangle_{\tilde{m}\oplus u,v})$
$E_{k_{AC}}(m||w)$
Alice
(9)**U2**: $E_{k_{AT}}(\mathrm{Sign}_{AC}{}^{\otimes 2}, \mathrm{Sign}_{BC}{}^{\otimes 2})$
(10)**U3**: $E_{k_{CT}}(\mathrm{Sign}_{AC}, \mathrm{Sign}_{BC})$
Trent
Charlie
(11)**V1**: (m, w)
(12)**V2**: (u, v)
(13)**V3**: $H^{m}H^{w}|\varphi\rangle_{\tilde{m}\oplus u,v}$
(14)**V4**: $u \equiv u', v \equiv v'$
(15)**V5**: $|f(u||v||(m \oplus w))\rangle \equiv |f(u||v||\tilde{m})\rangle$
(16)**V6**: $\{m, |\varphi\rangle_{m\oplus u,v}\}$

Figure 1. The flow-process diagram of the proposed QBS scheme. Alice blinds the message m with blind factor w and passes $\widetilde{m}$ to Bob. With the proposed encoding method of the BB84-state, Bob signs $\widetilde{m}$ with u and v and then sends the blind signature $|\varphi\rangle_{\widetilde{m}\oplus u,v}$ back to Alice. Two copies of the unblinding signature are sent to Trent. After Trent's identical verification for the two signatures, one of the signatures is transmitted to Charlie. Once Charlie verifies the validity of the signature, he publishes the signature $\{m, |\varphi\rangle_{m\oplus u,v}\}$.

4. Security Analyses

In this section, we show that the proposed scheme is correct and satisfies the properties of blind signatures described in the preliminary section.

4.1. Correctness

Theorem 1. *The QBS scheme is correct.*

Proof. We prove the correctness of the scheme in two cases.

(1) B can correctly recover the blind message $\widetilde{m}$ from A.

In the blinding phase, B received the $|\varphi\rangle_{\widetilde{m}\oplus k_{AB},\widetilde{m}}$ from A. According to Corollary 2, the correct chosen basis (diagonal or rectilinear) to measure $|\varphi\rangle_{\widetilde{m}_i\oplus k_{AB_i},\widetilde{m}_i}$ is determined by $(\widetilde{m}_i \oplus k_{AB_i}) \oplus \widetilde{m}_i = k_{AB_i}$. In the cases in which A is an honest blind message sender and no eavesdropper E exists in the quantum channel, as long as B measures $|\varphi\rangle_{\widetilde{m}\oplus k_{AB},\widetilde{m}}$ in the correct basis determined by the shared key k_{AB}, B will always get the correct blind message $\widetilde{m}$ with the probability one by comparison of his measurement results with Equation (2). However, if A is not an honest blind message sender or eavesdropper E exists in the quantum channel, B will find, with high probability, a contradiction with the measurement results and aborts.

(2) C can correctly validate the quantum signature $H^{w}|\varphi\rangle_{\widetilde{m}\oplus u,v}$ for A's original message m.

After recovering the blind message $\widetilde{m}$ from $|\varphi\rangle_{\widetilde{m}\oplus k_{AB},\widetilde{m}}$, B signs $\widetilde{m}$ with his u and v and gets QBS $|\varphi\rangle_{\widetilde{m}\oplus u,v}$ based on Equation (2). Once A gets the QBS $|\varphi\rangle_{\widetilde{m}\oplus u,v}$ from B, she strips the blind factor w by applying H^{w} to $|\varphi\rangle_{\widetilde{m}\oplus u,v}$ and gets quantum signature $H^{w}|\varphi\rangle_{\widetilde{m}\oplus u,v}$. In fact, according to Corollary 5, A obtains the result:

$$H^{w}|\varphi\rangle_{\widetilde{m}\oplus u,v} = |\varphi\rangle_{(\widetilde{m}\oplus u)\oplus w,v} = |\varphi\rangle_{(m\oplus w)\oplus u\oplus w,v} = |\varphi\rangle_{m\oplus u,v}.$$

In ***Step V3***, after receiving $E_{k_{AC}}(H^w|\varphi\rangle_{\widetilde{m}\oplus u,v})$ from A, C decrypts it and gets $H^w|\varphi\rangle_{\widetilde{m}\oplus u,v}$ with his shared key k_{AC}, then applies H^m to $H^w|\varphi\rangle_{\widetilde{m}\oplus u,v}$ to generate $H^m H^w|\varphi\rangle_{\widetilde{m}\oplus u,v}$, i.e.,

$$H^m H^w|\varphi\rangle_{\widetilde{m}\oplus u,v} = H^m|\varphi\rangle_{m\oplus u,v} = |\varphi\rangle_{(m\oplus u)\oplus m,v} = |\varphi\rangle_{u,v}.$$

With the decrypted u and v from B, C selects a suitable basis and measures $H^m H^w|\varphi\rangle_{\widetilde{m}\oplus u,v}$(namely, $|\varphi\rangle_{u,v}$). It is obvious that the measurement results must match u and v. Thus, we can draw the conclusion that C can correctly validate the quantum signature $H^w|\varphi\rangle_{\widetilde{m}\oplus u,v}$ for A's original message m. □

4.2. Against External Attack

It is impossible for external attacker E to attack a legitimate signature. Being external, the attacker has less available resources than A or B. The only way for him/her to obtain information is to intercept the quantum states or eavesdrop on the quantum channel. In the proposed scheme, there are three forms of quantum states on the quantum channel: quantum fingerprint states, BB84-states, and encrypted quantum states.

For the quantum fingerprint in the quantum channel, it is impossible for E to deduce conversely the original input on the basis of [34]. At the same time, if any quantum states are measured or replaced, this attack is detected by participants' comparison of quantum fingerprint states. Therefore, it is impossible for E to forge the scheme by attacking the quantum fingerprint states.

Both BB84-states and encrypted quantum states, which are n-qubit tensor products, consist of elements in set $\{|+\rangle, |-\rangle, |0\rangle, |1\rangle\}$. Assuming that the secret keys and signature parameters are uniformly distributed, each qubit is randomly located in one of two conjugate bases. Thus, the quantum states are essentially the same as the BB84 QKD one. According to the quantum indistinguishability, non-cloning, and immeasurability, E cannot distinguish the nonorthogonal states. E cannot perform the correct unitary operation for each photon. In terms of mathematical probability, he/she only speculates each photon state with the correct probability $\frac{1}{4}$. Therefore, the probability of misjudgment for n photons is:

$$P = 1 - (\frac{1}{4})^n. \tag{4}$$

Obviously, this probability infinitely tends to one with the increase of n. E cannot obtain any message from the transmitted particles yet. Consider the density matrix of n particles,

$$\rho = (\frac{1}{4})^n(|+\rangle\langle+| + |-\rangle\langle-| + |0\rangle\langle 0| + |1\rangle\langle 1|)^{\otimes n} = \frac{1}{2^n}\mathbf{I}. \tag{5}$$

This illustrates that the quantum states distribute in a uniform way so that no information might be leaked to the eavesdropper E. Consequently, external attack would not take effect.

4.3. Blindness

In the blinding phase, A sends the BB84-state $|\varphi\rangle_{\widetilde{m}\oplus k_{AB},\widetilde{m}}$, which contains blind message $\widetilde{m}$, to B. To measure $|\varphi\rangle_{\widetilde{m}\oplus k_{AB},\widetilde{m}}$ using the corresponding basis matching the shared key k_{AB}, B can recover the blind message $\widetilde{m}$ from A. For $\widetilde{m} = m \oplus w$; thus, B cannot recover m directly from known $\widetilde{m}$ without w.

However, the blind signer B has two strategies to find some original message if A's quantum signature is transmitted in the form $H^w|\varphi\rangle_{\widetilde{m}\oplus u,v}$ (namely,$|\varphi\rangle_{m\oplus u,v}$) in $Sign_{AC}$. B's first strategy is to measure A's $|\varphi\rangle_{m_i\oplus u_i,v_i}$ with computational basis $\{|0\rangle, |1\rangle\}$ or diagonal basis $\{|+\rangle, |-\rangle\}$. Suppose $u_i = v_i = 0$; once B measures the $|\varphi\rangle_{m_i\oplus u_i,v_i}$ (namely, $|\varphi\rangle_{m_i,0}$) with the computational basis and gets the measurement result $|1\rangle$, he can come to the conclusion that $|\varphi\rangle_{m_i,0}$ cannot be $|0\rangle$ and must be $|+\rangle$. This shows that Alice's original message must be $m_i = 0$. On average, Bob's strategy thus reveals $\frac{1}{4}n$ bits of A's original message. The result is the same for the use of the diagonal basis. B's second strategy is to perform the C-SWAP test [34] between his $|\varphi\rangle_{\widetilde{m}_i\oplus u_i,v_i}$ and A's $|\varphi\rangle_{m_i\oplus u_i,v_i}$ if B can certainly confirm that A's stripped signature $|\varphi\rangle_{m_i \oplus u_i, v_i}$ corresponds to his blind signature $|\varphi\rangle_{\widetilde{m_i} \oplus u_i, v_i}$. According to the comparison result, B can come to the conclusion that $m_i = \widetilde{m}_i$ ($m_i = \widetilde{m}_i \oplus 1$) if $|\varphi\rangle_{\widetilde{m}_i \oplus u_i, v_i}$=$|\varphi\rangle_{m_i \oplus u_i, v_i}$ ($|\varphi\rangle_{\widetilde{m}_i \oplus u_i, v_i} \neq |\varphi\rangle_{m_i \oplus u_i, v_i}$), and then, B can get A's original message m_i.

To avoid the two extreme strategies of B existing in his blind signature and A's stripped one, the quantum signature $H^w|\varphi\rangle_{\widetilde{m} \oplus u, v}$ is encrypted with the key k_{AC} in the proposed scheme, and then, $E_{k_{AC}}(H^w|\varphi\rangle_{\widetilde{m} \oplus u, v})$ is transmitted to C in **Step U2**. In such circumstances, the two strategies of B become invalid. Thus, our proposed scheme meets the standard of blindness.

4.4. Unforgeability

There are two kinds of forgeries. One forgery is done by the internal participants and the other by the external attacker E. The attacks of the internal participants involve message owner A, blind signer B, and the signature verifier C. With the following analyses, it can be shown that the two kinds of forgery cannot forge legitimate signatures so as to achieve the purpose of passing C's verification.

The message owner A cannot forge the quantum signature. For the blind message $\widetilde{m} = m_1 \oplus w_1$ corresponding to original message m_1 and blind factor w_1, A would reach her purpose of forgery if she succeeds in forging message pair (m_2, w_2) to replace the true message (m_1, w_1) and making C validate it. Obviously, $m_1 \oplus w_1$ must be equal to $m_2 \oplus w_2$, otherwise C will find the inconformity in **Step V5**. There are two ways for A to forge. One way is that A prepares the original message pair (m_1, w_1) in **Step B1** and $E_{k_{AB}}(E_{k_{AC}}(m_1, w_1))$ in **Step B2** and at the same time generates $E_{k_{AC}}(H^{w_2}|\varphi\rangle_{\widetilde{m} \oplus u, v})$ and $E_{k_{AC}}(m_2, w_2)\}$ in **Step U1**. In this way, C will find that (m_1, w_1) is not equal (m_2, w_2) and abort this signature. Thus, this strategy is unsuccessful. Another way for A's forgery is to generate $E_{k_{AC}}(H^{w_2}|\varphi\rangle_{\widetilde{m} \oplus u, v})$ and $E_{k_{AC}}(m_1, w_1)\}$ in **Step U1**. This way can pass C's examination in **Step V1**, but C would still find this strategy in **Step V3** and **Step V4**. In **Step V3**, C applies H^{m_1} to $H^{w_2}|\varphi\rangle_{\widetilde{m} \oplus u, v}$ and gets:

$$H^{m_1} H^{w_2}|\varphi\rangle_{\widetilde{m} \oplus u, v} = |\varphi\rangle_{m_1 \oplus w_2 \oplus \widetilde{m} \oplus u, v} = |\varphi\rangle_{m_1 \oplus w_2 \oplus (m_1 \oplus w_1) \oplus u, v} = |\varphi\rangle_{w_1 \oplus w_2 \oplus u, v}.$$

Obviously, if the w_1 is not equal w_2 and thus $w_1 \oplus w_2 \oplus u$ is not equal to u, C would find this strategy with the examination in **Step V4** for this way. Thus, the two forgery ways for A are not effective, and the unforgeability of the proposed scheme holds.

It is impossible for the blind signer B to forge a legitimate signature. The forgery way of B is to masquerade as the message owner A to sign the message alone and attempt to let the verifier C verify this forged signature. At first, B generates the forged message m' and the blind parameter w'. Then, B takes the place of A to get the unblinding quantum signature $H^{w'}|\varphi\rangle_{\widetilde{m'} \oplus u, v} = |\varphi\rangle_{m' \oplus u, v}$ in **Step U1**. According to our scheme, m' and w' must be encrypted with the shared key $k_{A'C}$, and then, $E_{k_{A'C}}(m', w')$ will be transmitted to C. In **Step V1**, C decrypts $E_{k_{A'C}}(m', w')$ with the shared key k_{AC}, but C cannot get the correct m' and w' because of B's random guess key $k_{A'C}$. In **Step V4**, C will find the forgery trick because the equations are not satisfied.

The signature verifier C cannot forge the quantum signature. After the arbitrator T receives the two copies of signatures $E_{k_{AT}}(Sign_{AC}{}^{\otimes 2}, Sign_{BC}{}^{\otimes 2})$ encrypted with the shared key k_{AT} from A, he retains one copy and then encrypts another to C with shared key k_{CT}. If C forges a blind signature and tries to cheat the message owner A, it will cause a dispute. In this dispute, T can judge that C is the forger. This is because T retains a legitimate signature. According to the signature data provided by C, T can regenerate C's signature. With the C-SWAP test [34], T can compare the preserved signatures with C's forged signature and will find the inconformity, so C's forgery strategy fails. Therefore, with the help of the trusted arbitrator T, C's forgery strategy is not feasible.

4.5. Non-Repudiation

There are three possible ways for participants to repudiate the quantum signature afterwards. The first way is that A, the original message owner, repudiates that she has ever blinded message m

to $\widetilde{m}$ with random w in the blinding phase and stripped blind factor w from blind signature in the unblinding phase. The second way is that B, the blind signer, repudiates that he has signed the blind message $\widetilde{m}$ with the random parameters u and v. The third way is that the signature verifier C denies that he has verified the legitimate signature from message owner A.

For A, she cannot repudiate her blinding behavior because she transmits the blind message $\widetilde{m}$ encoding the quantum BB84-state with the shared key k_{AB} and the quantum fingerprint $|f(\widetilde{m})\rangle$ to B in the blinding phase. She cannot also repudiate her unblinding behavior because she encrypts the blind factor w with shared key k_{AC} and transmits $E_{k_{AC}}(m||w)$ to C in the unblinding phase.

For B, he encrypts his blind signature parameters u and v with the shared key $E_{k_{BC}}$ and passes $E_{k_{BC}}(u,v)$ to C, so he cannot repudiate the behavior of his choosing of the parameters. Meanwhile, in the verifying phase, C generates $|f(u||v||(m \oplus w))\rangle$ and compares it to the receiving $|f(u||v||\widetilde{m})$ from B and thus further validates the signature parameters $\{w,u,v\}$ and denies A's repudiation and B's one as a whole.

For C, his undeniable attribute is determined by his declaration behavior in the verifying phase. That is to say, in several consecutive judgments, once C announces the correct judgment of the signature, he cannot deny all previous declarations including this one. The received $E_{k_{CT}}(Sign_{AC}, Sign_{BC})$, which is encrypted with his shared key k_{CT}, comes from the trusted arbitrator T. In **Step V1** of the verifying phase, it indicates that the $E_{k_{AC}}(m||w)$ is equal in $Sign_{AC}$ and $Sign_{BC}$. C confirms the fact of C not aborting the signature verification procedure. If so, C can not deny this verification step. In **Step V4** of the verifying phase, C performs single-particle measurements on the quantum signature and deduces B's signature parameters u' and v'. C would aborts the process if he finds disagreement between the derivative results (u',v') and received results (u,v). Thus, C cannot deny his actions in this step. In **Step V5** of the verifying phase, C validates the quantum fingerprint and judge A's blind parameter w. Similarly, his announcement for A's blindness cannot be disavowed. In the whole process, it shows that C has accepted the process of signature verification and cannot deny his validation fact if C does not abandon the verification in the verifying phase.

4.6. Unlinkability

Once the original message m and its quantum signature $|\varphi\rangle_{m \oplus u,v}$ are public, the proposed scheme guarantees that the blind signer B cannot determine whether the open message m is associated with the blind message $\widetilde{m}$ or not. Suppose C opens publicly two different signatures $\{m_1, |\varphi\rangle_{m_1 \oplus u,v}\}$ and $\{m_2, |\varphi\rangle_{m_2 \oplus u,v}\}$; the blind signer B can certainly validate the correctness of each signature with the open m_1 (m_2) and his secret u and v. Meanwhile, B can recover his blind signature $\{\widetilde{m}, |\varphi\rangle_{\widetilde{m} \oplus u,v}\}$ with A's blind message $\widetilde{m}$ and B's (u,v). Because B does not know A's blind factors w_1 and w_2, facing the open messages m_1 and m_2, B cannot be sure whether his blind message $\widetilde{m}$ is associated with the open message m_1 or m_2 besides only verifying the correctness of these signatures. Thus, this proposed scheme is shown to admit the property of unlinkability.

4.7. Traceability

The scheme is verified to satisfy the security demand of full traceability. Under the supervision of trusted arbitrator T, the verifier C is provided with traceability when the dispute occurs. Because the message owner A's blind parameter w and original message m are all encrypted and transmitted to C, C can trace the whole original message sender A's process. At the same time, C is traceable to B's blind signature process because B's blind signature parameters u and v are also encrypted and transmitted to C. Thus, this signature scheme satisfies the condition of traceability.

5. Conclusions

In this paper, we presented a new provable QBS scheme with the nonorthogonal single-photon BB84-state. We supposed that the arbitrator was trusted by everyone. Following the classical blind signature, our scheme consisted of the initial, blinding, signing, unblinding, and verifying phases.

The original message owner was responsible for the blinding and unblinding messages. The duty of blind signer was to sign the blinding message without knowing the original message. When a dispute occurred, the trusted arbitrator could open the quantum signature to identify the original message owner, blind signer, or signature message verifier. Based on quantum indistinguishability, the quantum encryption algorithm, the quantum fingerprint, and so on, the scheme provided unconditional security. Differing from the previous QBS schemes with some security vulnerability in basis security requirements, the security analyses showed that the proposed scheme satisfied the five properties of the blind signature protocol. Therefore, our scheme could be safely applied in some special environments.

Based on the current development level of quantum experiment technology, it is not ideal enough to achieve multi-photon quantum entanglement in practice. Our scheme uses only the single-photon BB84-state instead of quantum multi-photon entanglement states. Therefore, under the current technology and experiment condition, our scheme is realizable. The technical threshold is low, so our scheme is practical and feasible.

Until now, all the current quantum signature schemes, including our proposed QBS scheme, have used quantum symmetric encryption technology, which would lead to some problems, such as the management, storage, and transmission of shared keys. It will be more convenient to realize the quantum signature if it does not rely on the quantum encryption technology, but quantum public-key cryptography as the classical signature. However, the current quantum public-key cryptography is still in the initial stage of research and not yet mature for use in the quantum digital signature. It is believed that the quantum signature will become more concise and easier to realize with the continuing development of quantum public-key cryptography in the future.

Author Contributions: F.-L.C. designed the scheme and wrote the manuscript; Z.-H.W. and Y.-M.H. analyzed the scheme's security properties and approved the final manuscript.

Funding: This work was supported in part by the Natural Science Foundation of the Education Department of Anhui Province (Grant Nos. KJ2018A0363, KJ2017A356), the National Natural Science Foundation of China (Grant No. 61702012), and the University Outstanding Young Talent Support Project of Anhui Province of China (Grant No. gxyq2017026).

Conflicts of Interest: The authors declare that there is no conflict of interest regarding the publication of this paper.

References

1. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.
2. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
3. Bennett, C.H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **1992**, *68*, 3121–3124. [CrossRef]
4. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
5. Sasaki, T.; Yamamoto, Y.; Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **2014**, *509*,475–478. [CrossRef] [PubMed]
6. Giovannetti, V.; Lloyd, S.; Maccone, L. Quantum private queries. *Phys. Rev. Lett.* **2008**, *100*, 230502. [CrossRef] [PubMed]
7. Liu, B.; Gao, F.; Huang, W.; Wen, Q.Y. QKD-Based quantum private query without a failure probability. *Sci. China-Phys. Mech. Astron.* **2015**, *58*, 100301. [CrossRef]
8. Wei, C.Y.; Cai, X.Q.; Liu, B.; Wang, T.-Y.; Gao, F. A Generic Construction of Quantum-Oblivious-Key-Transfer-Based Private Query with Ideal Database Security and Zero Failure. *IEEE Trans. Comput.* **2018**, *67*, 2–8. [CrossRef]
9. Gottesman, D.; Chuang, I. Quantum digital signatures. *arXiv* **2001**, arXiv:quant-ph/0105032.
10. Zeng, G.H.; Keitel, C.H. Arbitrated quantum-signature scheme. *Phys. Rev. A* **2002**, *65*, 042312. [CrossRef]

11. Dunjko, V.; Wallden, P.; Andersson, E. Quantum digital signatures without quantum memory. *Phys. Rev. Lett.* **2014**, *112*, 040502. [CrossRef]
12. Wallden, P.; Dunjko, V.; Kent, A.; Andersson, E. Quantum digital signatures with quantum key distribution components. *Phys. Rev. A* **2015**, *91*, 042304. [CrossRef]
13. Amiri, R.; Wallden, P.; Kent, A.; Andersson, E. Secure quantum signatures using insecure quantum channels. *Phys. Rev. A* **2016**, *93*, 032325. [CrossRef]
14. Lo, H.-K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phy. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
15. Puthoor, I.V.; Amiri, R.; Wallden, P.; Curty, M.; Andersson, E. Measurement-device-independent quantum digital signatures. *Phy. Rev. A* **2016**, *94*, 022328. [CrossRef]
16. Yin, H.L.; Wang, W.L.; Tang, Y.L.; Zhao, Q.; Liu, H.; Sun, X.-X.; Zhang, W.-J.; Li, H.; Puthoor, I.V.; You, L.-X.; et al. Experimental measurement-device-independent quantum digital signatures over a metropolitan network. *Phy. Rev. A* **2017**, *95*, 042338. [CrossRef]
17. Roberts, G.L.; Lucamarini, M.; Yuan, Z.L.; Dynes, J.F. Experimental measurement-device-independent quantum digital signatures. *Nat. Comun.* **2017**, *8*, 1098. [CrossRef] [PubMed]
18. Chaum, D. Blind signature for untraceable payments. In *Advances in Cryptology*; Springer: Boston, MA, USA, pp. 199–203.
19. Wen, X.; Niu, X.; Ji, L.; Tian, Y. A weak blind signature scheme based on quantum cryptography. *Opt. Commun.* **2009**, *282*, 666–669. [CrossRef]
20. Qi, S.; Zheng, H.; Wen, Q.; Li, W. Quantum blind signature based on two-state vector formalism. *Opt. Commun.* **2010**, *283*, 4408–4410. [CrossRef]
21. Yang, C.W.; Hwang, T.; Luo, Y.P. Enhancement on "quantum blind signature based on two-state vector formalism". *Quantum Inf. Process.* **2012**, *12*, 109–117. [CrossRef]
22. Zhang, M.; Xu, G.A.; Chen, X.B.; Yang, S.; Yang, Y.-X. Attack on the improved quantum blind signature protocol. *Int. J. Theor. Phys.* **2013**, *52*, 331–335. [CrossRef]
23. Khodambashi, S.; Zakerolhosseini, A. A sessional blind signature based on quantum cryptography. *Quantum Inf. Process.* **2014**, *13*, 121–130. [CrossRef]
24. Shi, W.M.; Zhang, J.B.; Zhou, Y.H.; Yang, Y.G. A new quantum blind signature with unlinkability. *Quantum Inf. Process.* **2015**, *14*, 3019–3030. [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. Yin, X.; Ma, W.; Liu, W. A blind quantum signature scheme with χ-type entangled states. *Int. J. Theor. Phys.* **2012**, *51*, 455–461. [CrossRef]
27. Wang, M.M.; Chen, X.B.; Yang, Y.X. A blind quantum signature protocol using the GHZ states. *Sci. China Phys. Mech. Astron.* **2013**, *56*, 1636–1641. [CrossRef]
28. Zuo, H.J. Cryptanalysis of quantum blind signature scheme. *Int. J. Theor. Phys.* **2013**, *52*, 322–329. [CrossRef]
29. Ribeiro, J.; Souto, A.; Mateus, P. Quantum blind signature with an offline repository. *Int. J. Quantum Inf.* **2015**, *13*, 1550016. [CrossRef]
30. Lai, H.; Luo, M.X.; Pieprzyk, J.; Qu, Z.G.; Li, S.; Orgun, M.A. An efficient quantum blind digital signature scheme. *Sci. China Inf. Sci.* **2017**, *60*, 082501. [CrossRef]
31. Wang, T.Y.; Wen, Q.Y. Fair quantum blind signatures. *Chin. Phys. B* **2010**, *19*, 0307.
32. He, L.B.; Huang, L.S.; Yang, W.; Xu, R. Cryptanalysis of fair quantum blind signatures. *Chin. Phys. B* **2012**, *21*, 030306. [CrossRef]
33. Zou, X.F.; Qiu, D.W. Attack and improvements of fair quantum blind signature schemes. *Quantum Inf. Process.* **2013**, *12*, 2071–2085. [CrossRef]
34. Buhrman, H.; Cleve, R.; Watrous, J.; De, W.R. Quantum Fingerprinting. *Phys. Rev. Lett.* **2001**, *87*, 167902. [CrossRef] [PubMed]
35. Zhang, K.J.; Zhang, W.W.; Li, D. Improving the security of arbitrated quantum signature against the forgery attack. *Quantum Inf. Process.* **2013**, *12*, 2655–2669. [CrossRef]
36. Zhang, K.J.; Qin, S.J.; Sun, Y.; Song, T.T.; Su, Q. Reexamination of arbitrated quantum signature: the impossible and the possible. *Quantum Inf. Process.* **2013**, *12*, 3127–3141. [CrossRef]
37. Boykin, P.; Roychowdhury, V. Optimal encryption of quantum bits. *Phys. Rev. A* **2003**, *67*, 042317. [CrossRef]
38. Brassard, G. Quantum communication complexity (a survey). *arXiv* **2001**, arXiv:quant-ph/0101005.

39. Buhrman, H.; Cleve, R.; Massar, S.; Wolf, R.D. Non-Locality and communication complexity. *Rev. Mod. Phys.* **2009**, *82*, 665–698. [CrossRef]
40. Horn, R.T.; Babichev, S.A.; Marzlin, K.P.; Lvovsky, A.I.; Sanders, B.C. Single-Qubit optical quantum fingerprinting. *Phys. Rev. Lett.* **2005**, *95*, 150502. [CrossRef]
41. Du, J.; Zou, P.; Peng, X.; Oi, D.K.L.; Kwek, L.C.; Oh, C.H.; Ekert, A. Experimental quantum multimeter and one-qubit fingerprinting. *Phys. Rev. A* **2006**, *74*, 042319. [CrossRef]
42. Xu, F.; Miguel, A.J.; Wei, K.; Wang, W.; Palacios-Avila, P.; Feng, C.; Sajeed, S.; Lütkenhaus, L.; Lo, H.-K. Experimental quantum fingerprinting with weak coherent pulses. *Nat. Commun.* **2015**, *6*, 8735. [CrossRef] [PubMed]
43. Arrazola, J.M.; Lutkenhaus, N. Quantum fingerprinting with coherent states and a constant mean number of photons. *Phys. Rev. A* **2014**, *89*, 062305. [CrossRef]
44. Guan, J.Y.; Xu, F.; Yin, H.L.; Li, Y.; Zhang, Y.-J.; Chen, S.-J.; Yang, X.-Y.; Li, L.; You, L.-X.; Chen, T.-Y.; et al. Observation of Quantum Fingerprinting Beating the Classical Limit. *Phys. Rev. Lett.* **2016**, *116*, 240502. [CrossRef]
45. Li, F.G.; Shi, J.H. An arbitrated quantum signature protocol based on the chained CNOT operations encryption. *Quantum Inf. Process* **2015**, *14*, 2171–2181. [CrossRef]