entropy

IMPACT FACTOR 2.0

Indexed in: PubMed

CITESCORE 5.2

Article

A Quantum Proxy Signature Scheme Without Restrictions on the Identity and Number of Verifiers

Siyu Xiong

MDPI

https://doi.org/10.3390/e27111171

entropy

MDPI

Article

A Quantum Proxy Signature Scheme Without Restrictions on the Identity and Number of Verifiers

Siyu Xiong

Discipline Construction Office, Civil Aviation Flight University of China, Guanghan 618307, China; siyuxiong1996@outlook.com

Abstract

Quantum digital signatures (QDS) establish a framework for information-theoretically secure authentication in quantum networks. As a specialized extension of QDS, quantum proxy signatures facilitate secure delegation of signing privileges in distributed quantum environments. However, existing schemes require the predefinition of verifier identities at the system setup phase, which fundamentally constrains their deployment in real-world scenarios. To address this constraint, we propose a quantum proxy signature scheme supporting verification by arbitrary parties without pre-registration while maintaining information-theoretic security guarantees. This work presents a constructive approach to mitigating verification constraints in quantum proxy signature architectures.

Keywords: quantum digital signature; quantum proxy signature; quantum Fourier transform; quantum cryptography

1. Introduction

Digital signatures, a core modern cryptography technology, underpin data security and the fundamental trust framework for critical digital infrastructures in the digital era. Widely deployed public-key cryptosystems in current classical computing scenarios—typified by RSA [1] and ECDSA [2]—anchor their security on computational complexity-theoretic assumptions, with particular reliance on the intractability of the large integer factorization problem and the discrete logarithm problem in finite fields. The advent of quantum algorithm [3–6] has fundamentally undermined this foundation by solving classically hard computational problems in polynomial time, thereby compromising the security of current cryptographic infrastructures in the era of quantum computation.

The threat posed by quantum computing has catalyzed two distinct cryptographic paradigms: post-quantum cryptography [7–11], which develops classical algorithms resistant to quantum attacks, and quantum cryptography [12–16], which leverages quantum mechanical principles to achieve information-theoretic security. Within quantum cryptography, quantum digital signatures (QDS) represent a class of protocols that harness quantum states to provide non-forgeable and non-repudiable authentication of digital messages, achieving information-theoretic security unattainable in classical cryptography. Following Gottesman and Chuang's seminal theoretical framework [17], subsequent QDS schemes utilizing single photons [18], entangled states [19], and coherent states [20] have advanced rapidly from conception to experimental realization, including metropolitan-scale demonstrations [21] and measurement-device-independent protocols enhancing practical security [22]. Recently, Du et al. demonstrated the feasibility of chip-based quantum-dot

check for updates

Academic Editor: Osamu Hirota

Received: 28 October 2025
Revised: 17 November 2025
Accepted: 18 November 2025
Published: 19 November 2025

Citation: Xiong, S. A Quantum Proxy Signature Scheme Without Restrictions on the Identity and Number of Verifiers. *Entropy* **2025**, *27*, 1171. https://doi.org/10.3390/e27111171

single-photon sources [23], paving the way for large-scale deployment and integration with existing optical fiber infrastructure.

The inherent requirement for authorization delegation in distributed quantum environments has motivated the development of quantum proxy digital signatures (QPDS) as a specialized branch of quantum digital signatures. QPDS addresses this critical need by enabling a fundamental cryptographic operation: the secure transfer of signing privileges from an original signer to a designated proxy while preserving the information-theoretic security of the quantum signature framework. This delegation capability establishes the foundation for practical applications where distributed authority is essential, including collaborative quantum computing [24], quantum blockchain networks [25], and quantum internet of things ecosystems [26].

The research community has proposed various QPDS implementations encompassing diverse technical approaches. In 2008, building upon the foundational principles of classical threshold signature scheme [27], Yang et al. proposed a threshold proxy quantum group signature scheme incorporating threshold-shared verification [28]. The field of quantum proxy signatures has demonstrated remarkable diversification and evolutionary trends, giving rise to numerous variants designed to fulfill specific security and application requirements. For instance, quantum blind proxy signatures [29–31] leverage their distinctive blinding property to ensure signature validity while preserving message content privacy, offering viable solutions for scenarios such as electronic voting. Furthermore, branches including quantum multi-proxy signatures [32–34], threshold quantum proxy signatures [35,36], and quantum proxy group signatures [37–39] have substantially enriched this architecture by respectively addressing critical challenges in distributed collaboration. These diverse schemes exhibit tremendous potential for constructing future complex information security ecosystems.

Nevertheless, current schemes predominantly adhere to a permissioned verification paradigm, wherein the verification mechanism is structurally coupled with specific participant identities or predetermined verifier sets. This design imposes stringent constraints on the verification process: verifiers must belong to a predefined set or complete registration during the system initialization phase. Notably, while schemes based on threshold cryptography offer enhanced security guarantees, their verification mechanisms are inherently bound to a fixed-size group of verifiers, thus incapable of supporting parallel, independent verification by an arbitrary number of verifiers in open environments. In open environments, the identities and quantities of verifiers are highly dynamic and unpredictable, a requirement that the existing permissioned verification paradigm fails to accommodate. This contradiction underscores the central challenge confronting the QPDS field: how to transcend the limitations on verifier identity and quantity while maintaining reasonable cryptographic assumptions, thereby achieving universal verification capability.

Addressing this challenge, this paper proposes a novel quantum proxy signature scheme which constructs the one-way function based on the quantum Fourier transform. The scheme integrates quantum key distribution for secure key establishment and utilizes unitary transformations for quantum state manipulation in the signature process. Our scheme achieves universal verification, allowing an arbitrary number of verifiers of any identity to verify signatures without requiring pre-registration. This approach effectively overcomes the verification constraints in existing architectures while providing a practical solution for distributed quantum applications.

The organization of the rest of this paper is as follows. We begin with an introduction to the core of our scheme—the construction of the quantum Fourier transform-based one-way function—in Section 2. Section 3 then gives the complete description of our quantum proxy signature scheme. Following that, a security analysis is conducted in Section 4. Finally, we summarize our work in Section 5.

2. The Construction of Quantum One-Way Function

The security of our quantum proxy signature scheme is built upon the quantum one-way function constructed using the quantum Fourier transform (QFT). This approach leverages the inherent computational asymmetry of QFT to create an irreversible transformation that is secure against both classical and quantum attacks, forming the foundational component of our scheme. Here, we provide the detailed description of this construction.

Based on the QFT, the one-way function f_{QFT} can map the classical bit string M of length m to the quantum state consisting of n quantum bits. Suppose the classical bit string M of length m can be expressed as

$$M = (M_0, M_1, \ldots, M_{m-1}), \tag{1}$$

where $M_i \in \{0, 1\}$. And a quantum state consisting of n qubits is the vector in the complex vector space of dimension 2^n, which can be expressed as

$$|\psi\rangle = \sum_{x=0}^{2^n-1} \alpha_x |x\rangle, \tag{2}$$

where α_x represents the complex amplitude, and $|x\rangle$ refers to the ground state. QFT is a linear transformation that maps the computational basis state $|x\rangle$ to the Fourier basis state $|y\rangle$. For n qubits, the definition of QFT is

$$|x\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i x y/2^n} |y\rangle, \tag{3}$$

where $\frac{1}{\sqrt{2^n}}$ is the normalization factor, and y is the index of the Fourier basis state, ranging from 0 to $2^n - 1$. Meanwhile, QFT is a unitary transformation, which satisfies

$$QFT^{\dagger} QFT = I. \tag{4}$$

When constructing a quantum one-way function based on the QFT, first, the classical bit string M is encoded into an integer x, that is

$$x = \sum_{i=0}^{m-1} M_i 2^i. \tag{5}$$

Subsequently, the QFT is applied to the computational basis state $|x\rangle$, resulting in the output quantum state

$$|\psi_{QFT}\rangle = |f_{QFT}(M)\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \left(\sum_{i=0}^{m-1} M_i 2^i\right) y/2^n} |y\rangle \tag{6}$$

Here, n should be large enough to accommodate all possible values of x, that is

$$n \geq \lceil \log_2(2^m) \rceil = m. \tag{7}$$

When calculating $|f_{QFT}(M)\rangle$, the QFT needs to be executed, and its complexity for simulation on a classical computer is $O(n^2)$. However, the inverse transformation, that is, reversing from $|f_{QFT}(M)\rangle$ to x on a classical computer is not feasible because the output of QFT is a highly complex quantum state, which cannot be directly measured to obtain x.

Quantum one-way function based on the QFT anchors its security in the physical nature of quantum state phase information, thereby providing information-theoretic security

without relying on computational assumptions. It inherently resists quantum computing attacks and seamlessly integrates with quantum protocols, making it readily adaptable to broader quantum-safe security frameworks.

3. The Proposed Scheme

A quantum proxy signature scheme primarily enables a designated proxy signer to securely sign a message on behalf of the original signer, while ensuring the authenticity, integrity, and non-repudiation of the signed message under information-theoretic security. The proposed quantum proxy signature scheme involves three types of participants, as follows.

- Original signer: This participant has the original signing authority. They share the key with the proxy signatory through quantum key distribution and delegate the signing authority to the proxy signatory.
- Proxy signer: After this participant shares a key with the original signer through quantum key distribution, they sign on behalf of the original signer.
- Trusted center: An advanced trusted node, possessing control over the entire scheme.

Here, taking the case of the minimum number of participants for each identity, that is, one participant for each identity, we provide the detailed introduction to the quantum proxy signature scheme that is publicly verifiable. The entire signature scheme consists of four stages: the initialization stage, the authorization stage, the signature stage, and the verification stage. The protocol is executed through four sequential stages involving three participants: **original signer (OS)**, **proxy signer (PS)**, and **trusted center (TC)**. The complete workflow is formalized in the algorithms. The following provides detailed explanations for each stage.

3.1. The Initialization Stage

During this stage, the trusted center (TC) collaborates with the original signer Alice and the proxy signer Bob by executing a quantum key distribution protocol, generating three sets of keys of length $2n$, namely K_{AB}, K_{TA}, K_{TB}. Let $S = \{AB, TA, TB\}$ represent the set of key types, and $I = \{1, 2, \cdots, n\}$ represent the index set. The three sets of keys can be expressed as

$$K : S \times I \times \{1,2\} \to \mathbb{Z}_2, \;\; K(s,i,j) = \begin{cases} a_i, & s = AB, j = 1 \\ b_i, & s = AB, j = 2 \\ c_i, & s = TA, j = 1 \\ d_i, & s = TA, j = 2 \\ e_i, & s = TB, j = 1 \\ f_i, & s = TB, j = 2 \end{cases}, \tag{8}$$

where $s \in S$, $i \in I$, and $j \in \{1,2\}$. TC performs the quantum entanglement establishment process described between the original signer and the proxy signer. Each of the three parties simultaneously generates $2n$ entangled pairs. The entangled pairs between Alice and Bob can be expressed as

$$ES : (C, |\Phi_{\text{init}}\rangle) \to |\Phi_{\text{final}}\rangle = \bigotimes_{i=1}^{2n} |\phi_i\rangle = \bigotimes_{i=1}^{2n} \frac{1}{\sqrt{2}} \left(|0_{a_i} 0_{b_i}\rangle + |1_{a_i} 1_{b_i}\rangle \right), \tag{9}$$

where C is the control information of TC as the advanced node during the entanglement establishment process, that is, the relevant measurement results. Through this entanglement establishment process, Alice and Bob generate $2n$ pairs of entangled particles. The particle sequences owned by Alice and Bob are respectively denoted as $|\phi\rangle_a$ and $|\phi\rangle_b$, which can be written as

$$|\phi_a\rangle = \{|\phi_{a_1}\rangle, |\phi_{a_2}\rangle, \cdots, |\phi_{a_{2n}}\rangle\},\ |\phi_b\rangle = \left\{|\phi_{b_1}\rangle, |\phi_{b_2}\rangle, \cdots, |\phi_{b_{2n}}\rangle\right\}. \tag{10}$$

Furthermore, TC also needs to prepare n quantum states based on the keys K_{TA} and K_{TB}, and the composite system becomes

$$|\Psi_T\rangle = \bigotimes_{i=1}^{n} \left|\psi_{c_i,f_i}\right\rangle = \bigotimes_{i=1}^{n} \frac{1}{\sqrt{2}}[(1-f_i)|c_i\rangle + f_i(|0\rangle + (-1)^{c_i}|1\rangle)]. \tag{11}$$

TC uses pairs of entangled particles as the quantum channel, and the prepared $|\Psi_T\rangle$ is sent to the original signer Alice through teleportation. The message that the original signer Alice needs to sign is assumed to be

$$M = (m_i)_{i=1}^{n},\ m_i \in \{0,1\}. \tag{12}$$

TC calculates the exclusive OR (XOR) result

$$g = (g_i)_{i=1}^{n} = \left(m_i \bigoplus c_i \bigoplus e_i\right)_{i=1}^{n} \tag{13}$$

based on the keys K_{TA} and K_{TB}.

Using this XOR result, TC calculates and publishes its outcome based on the quantum one-way function, which can be expressed as

$$\left|\psi_{\mathrm{QFT}}(g)\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i\left(\sum_{i=1}^{n} g_i \cdot 2^{i-1}\right) y/2^n} |y\rangle. \tag{14}$$

The initialization stage establishes the foundational quantum resources and cryptographic keys required for the protocol. Algorithm 1 details the steps performed by the trusted center to set up the system.

Algorithm 1: Initialization Stage

Input: Security parameter n

Output: Shared keys K_{AB}, K_{TA}, K_{TB}, entangled states $|\phi_a\rangle, |\phi_b\rangle$, transformed state $|\Psi_T\rangle$, public QFT output $|\psi_{\mathrm{QFT}}(g)\rangle$

Key Distribution via QKD;
  $K_{AB} \leftarrow \mathrm{QKD}(OS, PS)$;
  $K_{TA} \leftarrow \mathrm{QKD}(TC, OS)$;
  $K_{TB} \leftarrow \mathrm{QKD}(TC, PS)$;

Entanglement Establishment;
  $(|\phi_a\rangle, |\phi_b\rangle) \leftarrow \mathrm{EstablishEntanglement}(OS, PS, 2n)$;

State Preparation and Teleportation;
  $|\Psi_T\rangle \leftarrow \bigotimes_{i=1}^{n} \frac{1}{\sqrt{2}}[(1-f_i)|c_i\rangle + f_i(|0\rangle + (-1)^{c_i}|1\rangle)]$;
  $\mathrm{Teleport}(|\Psi_T\rangle, OS)$;

Public Parameter Publication;
  $g \leftarrow (g_i)_{i=1}^{n} = (m_i \oplus c_i \oplus e_i)_{i=1}^{n}$;
  $|\psi_{\mathrm{QFT}}(g)\rangle \leftarrow \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i(\sum_{i=1}^{n} g_i \cdot 2^{i-1}) y/2^n} |y\rangle$;
  $\mathrm{Publish}(|\psi_{\mathrm{QFT}}(g)\rangle)$;

return $K_{AB}, K_{TA}, K_{TB}, |\phi_a\rangle, |\phi_b\rangle, |\Psi_T\rangle, |\psi_{\mathrm{QFT}}(g)\rangle$

3.2. The Authorization Stage

The original signer Alice constructs a proxy certificate information sequence characterized by a quantum state sequence, which indicates the identity information of the proxy signer, the valid period of the authorization, and other specific constraints that may exist regarding the signature authority granted to Bob, and the sequence is denoted as

$$|\mathrm{Y}_{auth}\rangle = \left\{\left|\gamma^1_{auth}\right\rangle, \left|\gamma^2_{auth}\right\rangle, ..., \left|\gamma^{2n}_{auth}\right\rangle\right\}, \ \left|\gamma^i_{auth}\right\rangle \in \{|0\rangle, |1\rangle\}. \tag{15}$$

According to this sequence, Alice measures the sequence $|\phi_a\rangle$ obtained through entanglement establishment, and the set of measurement operators is

$$\begin{array}{l} \Pi_Z = \{\Pi_{Z0} = |0\rangle\langle 0|, \ \Pi_{Z1} = |1\rangle\langle 1|\}, \\ \Pi_X = \left\{\Pi_{X+} = \frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|), \ \Pi_{X-} = \frac{1}{2}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)\right\} \end{array}, \tag{16}$$

Suppose the characteristic function is

$$\chi\left(\left|\gamma^i_{auth}\right\rangle\right) = \begin{cases} 1, & \text{if } \left|\gamma^i_{auth}\right\rangle = |0\rangle \\ 0, & \text{else} \end{cases}, \tag{17}$$

then the resulting measurement can be expressed as

$$MR_A = \bigotimes_{i=1}^{2n}\left(\chi\left(\left|\gamma^i_{auth}\right\rangle\right)\frac{\Pi_{Zm_i}|\phi_{a_i}\rangle}{\sqrt{\langle\phi_{a_i}|\Pi_{Zm_i}|\phi_{a_i}\rangle}} + \left(1-\chi\left(\left|\gamma^i_{auth}\right\rangle\right)\right)\frac{\Pi_{Xm_i}|\phi_{a_i}\rangle}{\sqrt{\langle\phi_{a_i}|\Pi_{Xm_i}|\phi_{a_i}\rangle}}\right), \tag{18}$$

Here, m_i represents the measurement result of the i-th particle. Subsequently, Alice transforms the particle sequence $|\Psi_T\rangle$ received through teleportation from TC using the key K_{AB}, and after the transformation, it becomes

$$|\Psi_{TA}\rangle = \left(\bigotimes_{i=1}^{n} U(a_i)V(b_i)\right)|\Psi_T\rangle, \tag{19}$$

where $U(a_i)$ satisfies $U(0) = |0\rangle\langle 0| + |1\rangle\langle 1|, U(1) = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ and $V(b_i)$ satisfies $V(0) = |0\rangle\langle 0| - |1\rangle\langle 1|, V(1) = H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|$. Alice encrypts the content generated by the above process using the key K_{AB} to generate the message

$$|S_A\rangle = E_{K_{AB}}(|\mathrm{Y}_{auth}\rangle, MR_A, |\Psi_{TA}\rangle), \tag{20}$$

where the encryption of the classical bit sequence MR_A uses the XOR operation of the key, while the encryption methods for quantum states $|\mathrm{Y}_{auth}\rangle$ and $|\Psi_{TA}\rangle$ are as follows: Firstly, each binary bit in the key K_{AB} is mapped to a quantum bit; for example, 0 is mapped to $|0\rangle$, 1 is mapped to $|1\rangle$, and then a controlled operation is performed on the quantum state, which is controlled by the key bit. The commonly used controlled operation is the controlled NOT gate. That is, if the key bit is 0, no operation is performed on the quantum state; if the key bit is 1, a quantum NOT gate operation is performed on the quantum state. After the encryption is completed, Alice sends the message $|S_A\rangle$ to the proxy signer Bob. Algorithm 2 formalizes this authorization process.

Algorithm 2: Authorization Stage

Input: $|Y_{auth}\rangle, |\phi_a\rangle, |\Psi_T\rangle, K_{AB}$

Output: Encrypted authorization message $|S_A\rangle$

Proxy Certificate Creation;
  $|Y_{auth}\rangle \leftarrow \{|\gamma^1_{auth}\rangle, |\gamma^2_{auth}\rangle, ..., |\gamma^{2n}_{auth}\rangle\}, |\gamma^i_{auth}\rangle \in \{|0\rangle, |1\rangle\}$;
Entanglement Measurement;
  for $i = 1$ **to** $2n$ **do**
    if $|\gamma^i_{auth}\rangle = |0\rangle$ **then**
      $m_i \leftarrow \text{Measure}(|\phi_{a_i}\rangle, \Pi_Z)$;
    end
    else
      $m_i \leftarrow \text{Measure}(|\phi_{a_i}\rangle, \Pi_X)$;
    end
  end
  $MR_A \leftarrow (m_1, m_2, \ldots, m_{2n})$;
State Transformation;
  $|\Psi_{TA}\rangle \leftarrow (\bigotimes_{i=1}^{n} U(a_i)V(b_i))|\Psi_T\rangle$;
  where: $U(0) = I, U(1) = i\sigma_y, V(0) = Z, V(1) = H$;
Encryption and Transmission;
  $|S_A\rangle \leftarrow E_{K_{AB}}(|Y_{auth}\rangle, MR_A, |\Psi_{TA}\rangle)$;
  SendTo$(PS, |S_A\rangle)$;
return $|S_A\rangle$

3.3. The Signature Stage

After receiving $|S_A\rangle$, the proxy signer Bob decrypts it using the key. The specific decryption method is the same as the encryption principle. Upon receiving $|Y_{auth}\rangle$, MR_A, and $|\Psi_{TA}\rangle$, Bob first verifies the authenticity and validity of the $2n$-length quantum state sequence $|Y_{auth}\rangle$ before performing any further operations. Specifically, Bob conducts a verification procedure by measuring the received quantum state sequence $|Y_{auth}\rangle$ and comparing it with the locally held entangled state sequence $|\phi_b\rangle$ of identical length $2n$, which was established during the prior entanglement distribution phase. If $|\gamma^i_{auth}\rangle = |0\rangle$, then the Z basis (i.e., $\{|0\rangle, |1\rangle\}$) is chosen to measure $|\varphi_{b_i}\rangle$; if $|\gamma^i_{auth}\rangle = |1\rangle$, then the X basis (i.e., $\{|+\rangle, |-\rangle\}$, where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$) is chosen to measure $|\varphi_{b_i}\rangle$. The measurement result is denoted as MR_B. If the condition

$$MR_A = MR_B \tag{21}$$

is satisfied, the signature authorization is accepted; otherwise, the signature is rejected. If the signature authorization is accepted, then Bob will commence the subsequent proxy signature operation. First, Bob generates a sequence of $2n$ quantum random numbers

$$R_B = (h_1, j_1, h_2, j_2, ..., h_n, j_n),\ h_i, j_i \in \{0, 1\} \tag{22}$$

as his private key. Bob performs the XOR operation with the generated key on the random number sequence between himself and TC, as well as between himself and Alice, and obtains the result

$$K_{PB} = R_B \bigoplus K_{TB} \bigoplus K_{AB} = (p_1, q_1, p_2, q_2, ..., p_n, q_n). \tag{23}$$

Then Bob announces this sequence K_{PB} as his public key. Bob uses the private key R_B to transform the quantum state sequence $|\Psi_{TA}\rangle$ and generates the proxy signature as follows

$$|S\rangle = \left(\bigotimes_{i=1}^{n}(U(h_i)V(j_i))\right)|\Psi_{TA}\rangle, \tag{24}$$

where $U(0) = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U(1) = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$, $V(0) = |0\rangle\langle 0| - |1\rangle\langle 1|$, $V(1) = H = 1/\sqrt{2}(|0\rangle + |1\rangle)\langle 0| + 1/\sqrt{2}(|0\rangle - |1\rangle)\langle 1|$. Algorithm 3 specifies the signature generation process.

Algorithm 3: Signature Stage

Input: $|S_A\rangle, |\phi_b\rangle, K_{AB}, K_{TB}$
Output: Signature $|S\rangle$, public key K_{PB}

Decryption and Verification;
  $(|Y_{auth}\rangle, MR_A, |\Psi_{TA}\rangle) \leftarrow D_{K_{AB}}(|S_A\rangle)$;
  for $i = 1$ **to** $2n$ **do**
    if $|\gamma^i_{auth}\rangle = |0\rangle$ **then**
      $m_i \leftarrow \text{Measure}(|\phi_{b_i}\rangle, \Pi_Z)$;
    end
    else
      $m_i \leftarrow \text{Measure}(|\phi_{b_i}\rangle, \Pi_X)$;
    end
  end
  $MR_B \leftarrow (m_1, m_2, \ldots, m_{2n})$;
  if $MR_B \neq MR_A$ **then**
    abort "Authorization failed";
  end
Key Generation;
  $R_B \leftarrow (h_1, j_1, h_2, j_2, ..., h_n, j_n), h_i, j_i \in \{0, 1\}$;
  $K_{PB} \leftarrow (p_1, q_1, p_2, q_2, ..., p_n, q_n) = R_B \oplus K_{TB} \oplus K_{AB}$;
  Publish(K_{PB});
Signature Generation;
  $|S\rangle \leftarrow (\otimes_{i=1}^{n} U(h_i)V(j_i))|\Psi_{TA}\rangle$;
  where: $U(0) = I, U(1) = i\sigma_y, V(0) = Z, V(1) = H$;
return $|S\rangle, K_{PB}$

3.4. The Verification Stage

The generated proxy signature can be used for public verification, meaning that any user can verify the validity of the signature. Suppose user Charlie needs to verify the signature, then the following steps need to be executed. Charlie, using Bob's public key K_{PB}, performs a transformation on the signature $|S\rangle$ to obtain the verification state

$$|S_C\rangle = \left(\bigotimes_{i=1}^{n}(U(p_i)V(q_i))\right)|S\rangle, \tag{25}$$

where $U(0) = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U(1) = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$, $V(0) = |0\rangle\langle 0| - |1\rangle\langle 1|$, $V(1) = H = 1/\sqrt{2}(|0\rangle + |1\rangle)\langle 0| + 1/\sqrt{2}(|0\rangle - |1\rangle)\langle 1|$. Charlie measured the verification state using the Z basis measurement operator

$$\Pi_Z = \{\Pi_{Z0} = |0\rangle\langle 0|, \Pi_{Z1} = |1\rangle\langle 1|\}, \tag{26}$$

and the result was recorded as

$$MR_C = (mr_1, mr_2, ..., mr_n). \tag{27}$$

Charlie combines the measurement result with the message bit using an XOR operation, obtaining

$$g_C = \left(g_C^1, g_C^2, ..., g_C^n\right) = \left(mr_1 \bigoplus m_1, mr_2 \bigoplus m_2, ..., mr_n \bigoplus m_n\right). \tag{28}$$

After that Charlie calculated the result

$$\left|\psi_{\mathrm{QFT}}(g_C)\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \left(\sum_{i=1}^{n} g_C^i \cdot 2^{i-1}\right) y/2^n} |y\rangle \tag{29}$$

based on the quantum Fourier transform. If

$$\left|\psi_{\mathrm{QFT}}(g_C)\right\rangle = \left|\psi_{\mathrm{QFT}}(g)\right\rangle, \tag{30}$$

the signature is valid; otherwise, the signature is rejected. Algorithm 4 defines the universal verification procedure.

Algorithm 4: Verification Stage

Input: Signature $|S\rangle$, public key K_{PB}, message M, public QFT state $|\psi_{\mathrm{QFT}}(g)\rangle$
Output: Verification result {Accept, Reject}

Reverse Transformation;
  $|S_C\rangle \leftarrow (\bigotimes_{i=1}^{n} U(p_i)V(q_i))|S\rangle$;
  where: $U(0) = I, U(1) = i\sigma_y, V(0) = Z, V(1) = H$;
Measurement and Computation;
  $MR_C \leftarrow (mr_1, mr_2, ..., mr_n) \leftarrow \mathrm{Measure}(|S_C\rangle, \Pi_Z)$;
  $g_C \leftarrow (g_C^1, g_C^2, ..., g_C^n) = (mr_1 \oplus m_1, mr_2 \oplus m_2, ..., mr_n \oplus m_n)$;
  $|\psi_{\mathrm{QFT}}(g_C)\rangle \leftarrow \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \left(\sum_{i=1}^{n} g_C^i \cdot 2^{i-1}\right) y/2^n} |y\rangle$;
Validation;
  if $\left|\psi_{QFT}(g_C)\right\rangle = \left|\psi_{QFT}(g)\right\rangle$ **then**
    return "Accept";
  end
  else
    return "Reject";
  end

The schematic diagrams of each stage of the scheme are shown in Figure 1. The final proxy signature generated can be used for public verification and can be carried out at any time after the signature stage is completed. There is no limit on the number of verifiers who complete the verification. Due to the openness of information, the verification information of the completed verifiers does not affect the verification of subsequent verifiers. Multiple verifiers can conduct the verification simultaneously, which has a high signature verification efficiency.

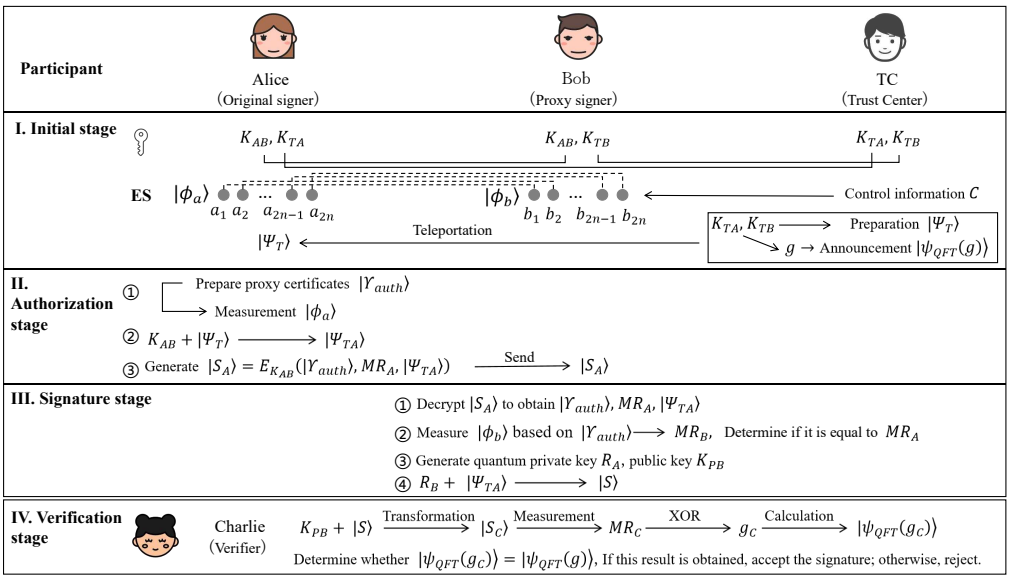

Figure 1. The schematic diagram of the proposed quantum proxy signature scheme.

4. Security Analysis

The security of the proposed proxy signature scheme for individual original signatories is analyzed below. The security analysis follows the established framework common in digital signature schemes [40,41], which ensures a comprehensive evaluation by examining the following three critical aspects: anti-honesty termination, anti-repudiation attack, and anti-forgery attack.

4.1. Anti-Honesty Termination

The anti-trust termination property of the proposed scheme mainly indicates whether the verifier can successfully verify the signature when all participants are honest and there is no external attack. In the initial stage, the trusted center (TC) prepares the quantum state sequence $|\Psi_T\rangle$ based on the keys K_{TC} and K_{TB}, and this sequence subsequently evolves into

$$|\Psi_T\rangle \xrightarrow{K_{AB}} |\Psi_{TA}\rangle \xrightarrow{R_B} |S\rangle \xrightarrow{K_{PB}=R_B \oplus K_{TB} \oplus K_{AB}} |S_C\rangle. \tag{31}$$

Due to the unitary transformations performed during the evolution process, based on the Equations (11), (19), (22) and (23), the relationship can be obtained as follows

$$MR_i = c_i \bigoplus e_i, \tag{32}$$

Therefore, it can always ensure

$$g_C = g,\ |\psi_{\mathrm{QFT}}(g_C)\rangle = |\psi_{\mathrm{QFT}}(g)\rangle, \tag{33}$$

That is, in a situation where there is no interference from either internal or external dishonesty, the signature can always be verified as successful.

4.2. Anti-Repudiation Attack

Firstly, for the original signer Alice, since the quantum states $|\Psi_T\rangle$, $|\psi_{\mathrm{QFT}}(g)\rangle$, $|\Psi_{TC}\rangle$ and the public key K_{PB} involve the key K_{AB} between Alice and Bob, as well as the key K_{TC} between Alice and TC, if the final verification is successful, Alice's use of the key makes it impossible for her to deny that she performed the proxy authorization. For the proxy signer Bob, since the proxy authorization certificate $|\Phi_w\rangle$ is a known quantum state containing Bob's identity information, and the signature $|S\rangle$ and the public key K_{PB} are

derived from the shared key K_{TB} and K_{AB} held by Bob, thus Bob cannot deny that he performed the proxy signature on the message M.

4.3. Anti-Forgery Attack

The anti-forgery property of the proposed scheme can be analyzed from two aspects: anti-external attack and anti-internal attack.

For external attacks, assume the attacker is Eve, and her possible attack methods include auxiliary particle attack and interception retransmission attack. When Eve conducts an auxiliary particle attack, she uses the entangled pairs generated between Alice and Bob to entangle with them. Since the entangled pairs between Alice and Bob are generated by the given entanglement establishment process and not generated and distributed separately by TC, the scheme can effectively resist the auxiliary particle attack. If Eve chooses to carry out an interception retransmission attack, she needs to intercept the transmitted quantum state and replace it with a tampered quantum state. Since the transmission of quantum states in the given scheme uses encryption with the key generated by quantum key distribution, its security is guaranteed by the one-time key generated by quantum key distribution. When considering unconditional security for one-time pad encryption, the proposed scheme can completely resist this attack.

For the internal forgery attack, consider that both the original signer Alice and the proxy signer Bob could be the implementers of the forgery attack. If Alice is the attacker, she might forge the proxy signature $|S\rangle$ that should have been generated by Bob based on $|\Psi_{TA}\rangle$. The generation of signature $|S\rangle$ requires the participation of keys K_{TB} and K_{AB}, as can be seen from Equation (24), $|S\rangle$ is obtained from $|\Psi_{TA}\rangle$ through a specific unitary transformation. If Alice forges $|S\rangle$ merely by guessing the key, the probability of success is

$$P_{\text{Forged by Alice}} = \frac{1}{2^{4n}}. \tag{34}$$

If Bob is the perpetrator of the forgery attack, he might carry out the forgery by generating an effective signature that is different from $|S\rangle$. According to the equation (14), the trusted center TC calculates and makes public the quantum state $|\psi_{QFT}(g)\rangle$ after the action of the one-way function based on quantum Fourier transform. This means that the message to be signed M cannot be forged or altered. According to the properties of the quantum one-way function, Bob cannot generate two different signatures using the same message. Moreover, the successful verification of the signature depends on the key K_{TC} between Alice and TC, and Bob, without this key information, cannot forge other signatures that can be successfully verified.

5. Summary

This paper presents a quantum proxy signature scheme that allows any number of verifiers to validate the validity of the signature. This scheme can be used when any number of network nodes participate in the signature verification process, and there is no need for the verification nodes to have prior information exchange with the nodes involved in the signature. It has high efficiency and flexibility in network applications. The use of one-way functions based on quantum Fourier transformation in the signature relies on the principles of quantum state non-clonability and the difficulty of precisely controlling quantum entanglement, which are quantum characteristics. The cryptographic foundation of this scheme guarantees its security against future quantum attacks, meaning that even with highly developed quantum computers, it is infeasible for attackers to reverse the input of the function.

Funding: This work is supported by the Civil Aviation Development Fund Education Talents Project (Grants: mhjy2025029; mhjy2025033), the General Fund of Civil Aviation Flight University of China (Grants: xyjy2025001; xyjy2025002), Special Project for Guiding the Construction of World-Class Universities (Disciplines) and Characteristic Development in Central Universities (Grants: CZLY2025009).

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author

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

References

1. Rivest, R.L.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Koblitz, N. Elliptic Curve Cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
3. 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.
4. Grover, L.K. A Fast Quantum Mechanical Algorithm for Database Search. In Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; pp. 212–219.
5. Pedernales, J.S.; Di Candia, R.; Egusquiza, I.L.; Casanova, J.; Solano, E. Efficient Quantum Algorithm for Computing n-time Correlation Functions. *Phys. Rev. Lett.* **2014**, *113*, 020505. [CrossRef] [PubMed]
6. Sato, Y.; Tezuka, H.; Kondo, R.; Yamamoto, N. Quantum Algorithm for Partial Differential Equations of Nonconservative Systems with Spatially Varying Parameters. *Phys. Rev. Appl.* **2025**, *23*, 014063. [CrossRef]
7. Bernstein, D.J.; Lange, T. Post-Quantum Cryptography. *Nature* **2017**, *549*, 188–194. [CrossRef]
8. Singh, M.; Sood, S.K.; Bhatia, M. Post-Quantum Cryptography: A Review on Cryptographic Solutions for the Era of Quantum Computing. *Arch. Comput. Methods Eng.* **2025**. [CrossRef]
9. Cherkaoui, D.K.; Tasic, I.; Cano, M.D. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. *Technologies* **2024**, *12*, 241. [CrossRef]
10. Liu, Y.K.; Dustin, M. Post-quantum cryptography and the quantum future of cybersecurity. *Phys. Rev. Appl.* **2024**, *21*, 040501. [CrossRef]
11. Kim, M.S.; Rehman, S.; Khan, M.F.; Kim, S. Mem-Transistor-Based Gaussian Error–Generating Hardware for Post-Quantum Cryptography Applications. *Adv. Quantum Technol.* **2025**, *8*, 2400394. [CrossRef]
12. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
13. Huang, X.; Zhang, W.; Wang, X.; Zhang, S.; Khan, M.K. QF2PM: Quantum-Secure Fine-Grained Privacy-Preserving Profile Matching for Mobile Social Networks. *IEEE Trans. Netw. Sci. Eng.* 2025, *early access*. [CrossRef]
14. Huang, X.; Zhang, W.; Zhang, S. Quantum multi-party private set intersection using single photons. *Phys. A Stat. Mech. Its Appl.* **2024**, *649*, 129974. [CrossRef]
15. Guo, H. *Quantum Cryptography*, 1st ed.; Science Press: Beijing, China, 2023; pp. 45–89.
16. Huang, X.; Zhang, W.; Zhang, S. Practical quantum protocols for blind millionaires' problem based on rotation encryption and swap test. *Phys. A Stat. Mech. Its Appl.* **2024**, *637*, 129614. [CrossRef]
17. Gottesman, D.; Chuang, I. Quantum digital signatures. *arXiv* **2001**, arXiv:quant-ph/0105032. [CrossRef]
18. Zhan, L.; Zhang, C.-H.; Lu, N.; Qian, X.-R.; Ding, H.-J.; Liu, J.-Y.; Zhou, X.-Y.; Wang, Q. Experimental quantum digital signature based on heralded single-photon sources. *Quantum Inf. Process.* **2024**, *23*, 25. [CrossRef]
19. Chapman, J.C.; Alshowkan, M.; Qi, B.; Peters, N.A. Entanglement-based quantum digital signatures over a deployed campus network. *Opt. Express* **2024**, *32*, 7521. [CrossRef]
20. Clarke, P.J.; Collins, R.J.; Dunjko, V.; Andersson, E.; Jeffers, J.; Buller, G.S. Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. *Nat. Commun.* **2012**, *3*, 1174. [CrossRef]
21. 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. *Phys. Rev. A* **2017**, *95*, 042338. [CrossRef]
22. Puthoor, I.V.; Amiri, R.; Wallden, P.; Curty, M.; Andersson, E. Measurement-device-independent quantum digital signatures. *Phys. Rev. A* **2016**, *94*, 022328. [CrossRef]
23. Du, Y.; Li, B.-H.; Hua, X.; Cao, X.-Y.; Zhao, Z.; Xie, F.; Zhang, Z.; Yin, H.-L.; Xiao, X.; Wei, K. Chip-integrated quantum signature network over 200 km. *Light Sci. Appl.* **2025**, *14*, 108. [CrossRef]
24. Tian, Y.-L.; Feng, T.-F.; Zhou, X.-Q. Collaborative quantum computation with redundant graph state. *Acta Phys. Sinaca* **2019**, *68*, 110302. [CrossRef]

25. Krishnaswamy, D. Quantum blockchain networks. In Proceedings of the Twenty-First International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, Virtual, 11–14 October 2020; Association for Computing Machinery: New York, NY, USA, 2020; Volume 6, pp. 327–332.
26. Chawla, D.; Kumari, S.; Rathore, R.S.; Mehra, P.S.; Das, A.K.; Kumar, N. Quantum Blockchain for Internet of Things: A systematic review, proposed solutions and challenges. *Comput. Electr. Eng.* **2025**, *126*, 110524. [CrossRef]
27. Hillery, M.; Bužek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829–1834. [CrossRef]
28. Yang, Y.; Wen, Q. Threshold proxy quantum signature scheme with threshold shared verification. *Sci. China Ser. G Phys. Mech. Astron.* **2008**, *51*, 1079–1088. [CrossRef]
29. Wang, Z.; Li, J.; Chen, X.B.; Ye, C. Quantum multi-proxy strong blind signature based on block blind coding. *Quantum Inf. Process.* **2022**, *21*, 386. [CrossRef]
30. Lou, X.; Zan, H.; Xu, X. Quantum circuit-based proxy blind signatures: A novel approach and experimental evaluation on the IBM quantum cloud platform. *Chin. Phys. B* **2024**, *33*, 050307. [CrossRef]
31. Prajapat, S.; Obaidat, M.S.; Bharmaik, V.; Thakur, G.; Kumar, P. Quantum Safe Proxy Blind Signature Protocol Based on 3D Entangled GHZ-Type States. *Trans. Emerg. Telecommun. Technol.* **2025**, *36*, e70140. [CrossRef]
32. Niu, X.F.; Zhang, J.Z.; Xie, S.C. A Quantum multi-proxy blind signature scheme based on entangled four-qubit cluster state. *Commun. Theor. Phys.* **2018**, *70*, 043. [CrossRef]
33. Wang, T.Y.; Wang, X.X.; Cai, X.Q.; Zhang, R.L. Analysis of efficient quantum multi-proxy signature. *Quantum Inf. Process.* **2020**, *19*, 8. [CrossRef]
34. Chen, J.J.; You, F.C.; Li, Z.Z. Quantum multi-proxy blind signature based on cluster state. *Quantum Inf. Process.* **2022**, *21*, 104. [CrossRef]
35. Yu, J.; Zhang, J. Quantum proxy threshold multiple signature scheme. *Int. J. Theor. Phys.* **2021**, *60*, 2709–2721. [CrossRef]
36. Lu, Z.; Xue, Q.; Zhang, T.; Cai, J.; Han, J.; He, Y.; Li, Y. Locally verifiable approximate multi-member quantum threshold aggregation digital signature scheme. *Comput. Commun.* **2024**, *228*, 107934. [CrossRef]
37. Jin-jing, S.; Rong-hua, S.; Ying, T. A multiparty quantum proxy group signature scheme for the entangled-state message with quantum Fourier transform. *Quantum Inf. Process.* **2011**, *10*, 653–670. [CrossRef]
38. Şahin, M.S.; Akleylek, S. A survey of quantum secure group signature schemes: Lattice-based approach. *J. Inf. Secur. Appl.* **2023**, *73*, 103432. [CrossRef]
39. Lan, L.; Lu, R.; Zhong, J.; Shi, Y. A Secure Quantum Proxy Group Signature Scheme Based on Three-qubit Entangled States. *Int. J. Theor. Phys.* **2024**, *63*, 59. [CrossRef]
40. Xiong, S.; Tang, B.; Han, H.; Huang, J.; Bai, M.; Li, F.; Yu, W.; Mo, Z.; Liu, B. Efficient arbitrated quantum digital signature with multi-Receiver verification. *Adv. Quantum Technol.* **2024**, *7*, 2400110. [CrossRef]
41. Zeng, G.; Keitel, C.H. Arbitrated quantum-signature scheme. *Phys. Rev. A* **2002**, *65*, 042312. [CrossRef]