Scientific Research Publishing

Journal of Quantum Information Science, 2026, 16(3), 398-424
https://www.scirp.org/journal/jqis
ISSN Online: 2162-576X
ISSN Print: 2162-5751

# An Identity-Based Quantum Partially Blind Signature Scheme Based on Quantum Teleportation

**Juxiu Zhong*, Rongbo Lu*, Wei Li**

School of Computer and Artificial Intelligence, Huaihua University, Huaihua, China
Email: *zhongjx914@163.com, *lurongbo8563@163.com, liwei@hhtc.edu.cn

**How to cite this paper:** Zhong, J.X., Lu, R.B. and Li, W. (2026) An Identity-Based Quantum Partially Blind Signature Scheme Based on Quantum Teleportation. *Journal of Quantum Information Science*, **16**, 398-424.
https://doi.org/10.4236/jqis.2026.163014

**Received:** August 7, 2026
**Accepted:** September 15, 2026
**Published:** September 18, 2026

Copyright © 2026 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

## Abstract

Traditional digital signatures are based on mathematical hard problems that are vulnerable to quantum attacks. For privacy-sensitive applications such as electronic cash and electronic voting, partially blind signatures are preferable because they protect private messages while allowing signers to verify necessary public information. This paper proposes an identity-based quantum partially blind signature scheme based on quantum teleportation. Each signing session is assigned a unique identifier. The user blinds the private binary message by applying Pauli-X operations with a one-time random string, while public information remains visible to the signer. A trusted PKG performs identity authentication, signature authorization, session-key distribution, and time-period-based key lifecycle management. Quantum tags and quantum authentication codes provide verification and arbitration evidence, while quantum teleportation is used to transmit quantum information. In case of disputes, an arbitrator can verify independently stored quantum evidence, and channel monitoring enables the detection of eavesdropping and tampering. Security analysis shows that the proposed scheme satisfies partial blindness, unforgeability, and non-repudiation, and resists malicious third-party attacks. It is suitable for privacy-preserving and restricted-authorization applications such as electronic cash and electronic voting.

## Keywords

Quantum Teleportation, Partially Blind Quantum Signature, Quantum Tag, Quantum Arbitration

## 1. Introduction

Digital signatures are a core cryptographic mechanism in modern information security systems for achieving identity authentication, data integrity, non-forgea-

bility, and non-repudiation. Following the introduction of public-key cryptography by Diffie and Hellman in 1976, the development of digital signatures was driven by the introduction of schemes such as the RSA signature scheme, the ElGamal signature, the Schnorr signature, and short signatures based on bilinear pairs [1]-[6]. However, the security of RSA, DSA, and Schnorr-type schemes primarily relies on integer factorization or the discrete logarithm problem, and Shor's algorithm demonstrates that large-scale quantum computers with sufficient fault tolerance can solve these problems in polynomial time [7]. Consequently, in recent years, the focus of research has shifted significantly from optimizing the efficiency of classical signatures to the design, standardization, and migration implementation of post-quantum signatures, encompassing post-quantum signature approaches such as lattice, hash, coding, and multivariate schemes [8]. The advancement of quantum computing poses a fundamental threat to cryptosystems based on traditional number-theoretic problems [7] [9]. Against this backdrop, quantum signature schemes based on the principles of quantum mechanics have emerged; their security relies on physical properties such as the quantum no-cloning theorem and quantum entanglement, rather than the computational complexity of mathematical problems [10].

Blind signatures allow signers to complete a signature without knowing the content of the original message. The concept was first proposed by Chaum in 1983; its core feature is that the signer cannot see the specific content of the message being signed, and it is widely used in scenarios such as anonymous electronic cash, privacy-preserving authentication, and electronic voting [11]. Quantum blind signatures utilize mechanisms such as non-clonability, quantum one-time pad, and quantum key distribution to achieve the security properties of the signature scheme [12]. Early research on quantum blind signatures primarily focused on entanglement resources, trusted arbitration, verification efficiency, and anonymity [13]-[15]. Subsequently, entanglement-free quantum group-blind signatures and schemes based on BB84 single-photon states were proposed to enhance the anonymity of electronic voting and reduce the difficulty of quantum state preparation [16] [17]. In recent years, research in this field has continued to focus on protocol innovation while placing greater emphasis on applications, resource overhead, and formal security: In 2022, Luo *et al*. applied controlled quantum teleportation to proxy blind signatures [18]. In 2024, Gupta *et al*. constructed an electronic cash transaction scheme based on quantum blind signatures [19]. In 2025, Wang *et al*. proposed a bit-by-bit quantum blind signature protocol based on single-qubit rotations, utilizing qubit rotations to perform message obfuscation and signing, thereby reducing the complexity of the signing process, minimizing reliance on large amounts of quantum resources, and lowering implementation costs [20]. In 2026, Zhang *et al*. analyzed quantum blind signatures in supply chain finance, revealing risks such as insider attacks and entanglement measurement attacks. They constructed a security model and formally characterized the security properties of the improved scheme through four security games [21].

Although fully blind signatures can conceal the message and its session context, they make it difficult to restrict the use of the signature, which may be exploited by malicious requesters for unauthorized purposes. Partially blind signatures enhance controllability while maintaining blindness by binding public information—such as expiration dates or business categories—to private messages. In 1996, Abe and Fujisaki proposed the concept of partial blinding, which incorporates public attributes into blind signatures [22]; in 2000, Abe and Okamoto further provided a formal definition of partial blind signatures, defined completeness, partial blindness, and unforgeability, and constructed a classically provably secure scheme [23]. In the realm of quantum partially blind signatures, Cai and Niu were among the first to propose a partially blind signature scheme based on quantum cryptography, which attempts to balance the protection of private messages with control over the use of signatures by utilizing pre-negotiated shared information [24]. After analyzing existing quantum partially blind signature schemes, Zhong *et al*. proposed a quantum partially blind signature scheme that does not require entangled states, with the scheme's security guaranteed by a secure quantum key distribution protocol and quantum one-time pad [25]. In contrast to the relatively limited literature on quantum partial blind signatures, the past five years have seen more systematic, provably secure research on classical post-quantum partial blind signatures. For example, in 2024, Katsumata *et al*. constructed the homomorphic cryptographic blind signature and partial blind signature scheme CSI-Otter based on the CSIDH group action [26], In 2026, Kuchta *et al*. constructed the post-quantum blind signature scheme MEBS based on the equivalence group action of the MEDS matrix code and extended it to a partial blind signature [27].

Identity-based signatures use an identity string as public verification information, which can reduce the certificate management overhead of traditional public-key infrastructure [28]. Since Shamir proposed identity-based cryptosystems and the concept of identity signatures in 1984, this technology has been widely applied in cloud computing, the Internet of Things, and lightweight authentication systems [29]. Identity-based quantum signatures integrate identity mapping with quantum cryptography, simplifying certificate management while leveraging the properties of quantum mechanics to enhance security [30]. In 2020, Xin *et al*. proposed an identity-based quantum signature based on Bell states, enabling verifiers to complete verification using the signer's identity [31]. In the same year, they further developed an identity-based public-key quantum signature scheme that does not require long-term quantum storage and exhibits high efficiency in quantum key exchange [32]. In 2023, Huang *et al*. improved upon related schemes by generating a private key based on the signer's identity and combining it with the verifier's secret parameter to generate the signature; this eliminated the need for key exchange prior to signing, thereby improving protocol execution efficiency [33]. In 2024, Prajapat *et al*. constructed an identity-based quantum designated-verifier signature and analyzed its feasibility through quantum simulation [34]; Liu *et al*. further proposed an identity-based quantum sig-

nature scheme using Bell states, which reduced the implementation complexity by employing a classical bit string key and supporting key reuse [35]. In 2025, Mohanty *et al*. proposed an identity-based quantum signature scheme and verified its correctness and preliminary feasibility through instance runs on the IBM Qiskit simulator and the IBM Q Lima real quantum backend [36].

Quantum teleportation utilizes pre-shared entanglement, Bell-basis joint measurements, and classical auxiliary information to reconstruct the corresponding quantum state at a remote location without directly transmitting the original particle carrying the unknown input state. Bennett *et al*. first proposed the quantum teleportation protocol in 1993 [37]. Zeng and Keitel proposed an early quantum arbitration signature scheme by combining GHZ states, quantum one-time pad, and a trusted arbitration mechanism [38]. Wen *et al*. further constructed a quantum multi-signature protocol [39]; however, subsequent analysis revealed vulnerabilities to insider attacks and external attacks, indicating that the correctness of quantum teleportation cannot substitute for a security proof of the signature [40]. In 2019, Feng *et al*. introduced quantum walk teleportation, enabling the generation of entangled states during the signing phase [41]. In recent years, Lu *et al*. proposed a verifiable arbitration quantum signature scheme based on controlled quantum teleportation, incorporating identity authentication and eavesdropping detection mechanisms [42]; Singh *et al*. investigated the combined application of quantum digital signatures and quantum teleportation in protecting blockchain transactions [43]; Zhao *et al*. proposed a continuous-variable quantum digital signature protocol based on quantum teleportation, providing a continuous-variable implementation path for teleportation-based quantum signatures [44].

Existing quantum signature schemes still face limitations in privacy-sensitive applications. Conventional schemes may expose the complete message to the signer, whereas fully blind signatures conceal even the public information required for authorization or constraint verification. In addition, identity and session binding, one-time authorization, key revocation, dispute traceability, and the separation of signing and verification capabilities remain insufficiently addressed in many existing quantum blind and partially blind signature schemes. This paper proposes an identity-based quantum partially blind signature scheme based on quantum teleportation. In this scheme, users quantize classical binary information using a one-time random string and then apply Pauli-X blinding, while the pre-shared public information remains visible to the signer. The trusted private key generation center (PKG) is responsible for participant identity authentication, session establishment, blinding key freezing, signature authorization, and session key distribution. It also implements the lifecycle management of signature keys through session *IDs*, validity periods, and key states. The signer encodes the participants' identities, public information, session identifiers, and other data into quantum tags, which are incorporated into the quantum authentication payload along with the blinded message to generate direct verification evidence for a designated verifier and independent arbitration evidence for an arbitrator, respectively. This scheme employs security-verified EPR entanglement resources and quantum tel-

eportation to transmit the quantum payload. This paper presents the specific operations and quantum state evolutions for each phase and analyzes the scheme's security in terms of correctness, partial blindness, forgery resistance, non-repudiation, resistance to third-party attacks, and dispute arbitration.

## 2. Relevant Basic Knowledge

**Pauli gate:** $I, X, Y, Z$, where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

**The BB84 detection rule:** The communicating parties randomly select $I$ qubits and $I$ qubits for measurement. Following communication, half of the measured qubits and their corresponding results are randomly disclosed. The average bit error rate $e$ of the channel is calculated, and a threshold $e_{\text{th}}$ is set. If $e > e_{\text{th}}$, it is determined that the channel is under an eavesdropping attack.

**Quantum Teleportation (Standard):** The entangled pair shared by both parties is $\left|\Phi^+\right\rangle_{us}$, where the signer holds $s$ and the user holds $u$. The user has an unknown state $\left|\varphi\right\rangle$, then, $\left|\varphi\right\rangle_q \left|\Phi^+\right\rangle_{us} = \frac{1}{2}\sum_{x,z\in\{0,1\}} \left|\Phi^+_{x,z}\right\rangle_{qu} X^x Z^z \left|\varphi\right\rangle_s$, where $\left|\Phi^+_{x,z}\right\rangle$ represents the Bell basis, and $(x,z)$ corresponds to the measurement result on $\left(\left|\varphi\right\rangle, u\right)$.

Performing a Bell measurement yields a two-bit result $\gamma \in \{00,01,10,11\}$, the uncorrected state at the signer's end is $\left|\varphi_\gamma\right\rangle_s = X^x Z^z \left|\varphi\right\rangle_s$.

The user sends $\gamma$ to the signer, and the signer performs the corresponding Pauli operation $U_\gamma$ on $s$, causing $s$ to collapse into $\left|\varphi\right\rangle_s$:

$Z^z X^x \left|\varphi_\gamma\right\rangle_s = Z^z X^x X^x Z^z \left|\varphi\right\rangle_s = \mathrm{e}^{i\theta} \left|\varphi\right\rangle_s$.

**Quantum One-Time Pad (QOTP):** Suppose the message to be encrypted is a quantum state $\rho_M$ consisting of $n$ qubits. The encryption algorithm is defined as $Enc_{a,b}(\rho_M) = P_{a,b}\rho_M P_{a,b}^\dagger$, where $P_{a,b} = \otimes_{i=1}^n X_i^{a_i} Z_i^{b_i}$, and $a,b \in \{0,1\}^n$ are uniformly random classical keys. Here, $a_i = 1$ applies the Pauli-$X$ operator and $b_i = 1$ applies the Pauli-$Z$ operator on the $i$-th qubit.

The decryption algorithm is $Dec_{a,b}(\sigma) = P_{a,b}^\dagger \sigma P_{a,b}$. Therefore,

$Dec_{a,b}\left(Enc_{a,b}(\rho_M)\right) = P_{a,b}^\dagger P_{a,b} \rho_M P_{a,b}^\dagger P_{a,b} = \rho_M$.

Furthermore, QOTP provides perfect secrecy: $\frac{1}{4^n}\sum_{a,b} P_{a,b}\rho_M P_{a,b}^\dagger = \frac{I_M}{2^n}$, which holds for any input state $\rho_M$.

## 3. Detailed Design of a Quantum Partially Blind Signature Scheme

The proposed scheme is characterized by the following features. First, the protocol adopts a partially blind message structure in which the private message is hidden from the signer while the agreed public information *info* remains visible and is

explicitly bound to the corresponding session. Second, a globally unique session identifier $sid$ and a one-time authorization value $\omega_{sid}$ are introduced to bind identities, public information, temporal information, and verification labels to a unique protocol execution. Third, two independent evidence branches are generated during signing: direct-verification evidence $\Sigma_D$ and arbitration evidence $\Sigma_A$, protected by independent session keys $k_D^{sid}$ and $k_A^{sid}$, respectively. Finally, a temporal key-evolution and revocation mechanism is introduced to bind signing authority to a specific time period and support dynamic revocation.

**Participants and Roles:** The proposed quantum partial-blind signature scheme involves five types of participants: the PKG, User, Signer, Verifier, and Arbitrator.

**PKG:** The Private Key Generator (PKG) is responsible for key generation and management, EPR entangled state generation and distribution, as well as system parameter generation.

**User:** The user is the owner of the message to be signed and holds a conventional message awaiting signature. The identity information of the User is denoted as $ID_U$.

**Signer:** The signer generates a signature for the User's message. The identity information of the Signer is denoted as $ID_S$, and the public information $info$ is shared with the User.

**Verifier:** The verifier is the unique entity responsible for validating the signature and verifying its legitimacy and correctness.

**Arbitrator:** The arbitrator participates only when disputes regarding signature information occur. Under normal circumstances, the arbitration procedure is not invoked.

**Session ID and Label:** Each protocol execution uses a globally unique session ID ($sid \in \{0,1\}^{\lambda_{sid}}$), where $\lambda_{sid}$ is the length of the session ID. PKG ensures that the same $sid$ is not reused. The complete information is:
$Ctx[sid] = (ID_X, info, n, T)$, where $T$ represents the validity period for this authorization and verification, $Ctx$ is a database record, and $sid$ is the unique index for that record. $ID_X$ is the identity information of the participants.

PKG generates a one-time authorization number when approving a signature: $\omega_{sid}^{s} \leftarrow (0,1)^{\lambda_\omega}$. The protocol uses three short-purpose constants: AUTH, DIRECT, and ARBITRATION.

The authorization tag, direct verification tag, and arbitration tag are defined as follows:

$$\begin{aligned} L_{\text{auth}} &= \text{Canon}(sid, \omega_{sid}, \text{AUTH}), \\ L_D &= \text{Canon}(sid, \omega_{sid}, \text{DIRECT}), \\ L_A &= \text{Canon}(sid, \omega_{sid}, \text{ARBITRATION}). \end{aligned} \tag{1}$$

Canon denotes a normalized encoding function that is unambiguous.

The quantum authentication code is defined as $Q_{\text{Auth}}.\text{Enc}_k(\rho)$, $Q_{\text{Auth}}.\text{Dec}_k(\Sigma) = (f, \rho')$.

Where $k$ denotes the one-time quantum authentication key, $\rho$ is the quan-

tum payload to be authenticated, and Σ is the authenticated quantum state after encoding. The variable $f \in \{\text{acc}, \text{rej}\}$ denotes the authentication result. When $f = \text{acc}$, $\rho'$ represents the recovered payload.

The security of the authentication scheme is characterized by the parameter $\varepsilon_{\text{auth}}$, satisfying $\Pr[f = \text{acc} \wedge \rho' = \rho] \le \varepsilon_{\text{auth}}$.

### 3.1. System Initialization Phase

**(1) Parameter generation:** PKG specifies the security parameters: $\lambda = (\lambda_{sid}, \lambda_{\omega}, S_{\text{auth}}, \varepsilon_{\text{auth}}, n_{\max})$, where $\lambda_{sid}$ denotes the length of the session ID, $\lambda_{\omega}$ denotes the length of the one-time authorization code, $S_{\text{auth}}$ denotes the size of quantum authentication redundancy or trap qubits, $\varepsilon_{\text{auth}}$ denotes the upper bound of the quantum authentication error acceptance probability, and $n_{\max}$ denotes the maximum binary message length allowed by the system.

PKG selects a publicly available quantum authentication scheme: $Q_{\text{Auth}} = (Q_{\text{Auth}}.\text{Enc}, Q_{\text{Auth}}.\text{Dec})$, and a normalized encoding rule: $\text{Canon}(x_1, \cdots, x_t)$.

The valid identity information of each participant is denoted as $ID_X$, $X \in \{U, S, V, A\}$.

Finally, PKG establishes a session database $D_{sid}$ for storing session keys.

**(2) Participant identity registration:** Each participant $X \in \{U, S, V, A\}$ submits identity verification information to the PKG. After successful verification, the PKG establishes an identity–key mapping: $ID_X \to k_X$, where $ID_X$ denotes the identity information of participant $X$, and $k_X$ denotes the corresponding one-time control key pool. The mapping information is stored securely in the PKG's protected database.

**(3) Establishing a session key based on identity:**

**1) Session establishment:** The user, signer, and verifier submit their identities and public information to the PKG: $ID_U, ID_S, ID_V, ID_A, info, n, T$. The PKG verifies $1 \le n \le n_{\max}$, $T > t$, and checks whether the permissions for each identity are valid. Upon successful verification, a unique session ID is generated: $sid \in \{0,1\}^{\lambda_{sid}}$, ensuring that it does not duplicate any ID in the session database. The PKG records this information: $Ctx[sid] = (ID_U, ID_S, ID_V, ID_A, info, n, T)$.

**2) One-time control key:** Based on the identities and the session, the PKG generates one-time quantum authentication keys: $k_{PU}^{R}, k_{PS}^{Req}, k_{PS}^{Auth}$, for subsequent processes.

Specifically, $k_{PU}^{R}$ is used by the user to register with the PKG and freeze the blinding key; $k_{PS}^{Req}$ is used by the signer to submit an authorization request to the PKG; $k_{PS}^{Auth}$ is used by the PKG to send a one-time quantum authorization token to the signer.

These keys are all bound to $sid$, the sender's and recipient's identities, and the intended use, and are destroyed after this session

**3) Entanglement resource initialization:** Based on the security parameter $\lambda$, the PKG generates $n$ independent sets of EPR entanglement pairs, where each

pair is in a maximally entangled state: $\otimes_{i=1}^{n}\left|\phi^{+}\right\rangle_{U_iS_i}=\otimes_{i=1}^{n}\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right)_{U_iS_i}$.

The PKG distributes the particle set $S=\{S_1,S_2,\cdots,S_n\}$ to the signer and the particle set $U=\{U_1,U_2,\cdots,U_n\}$ to the user, thereby establishing a shared quantum channel between them.

**(4) Identity-Based Quantum Private Key Extraction:** The signer sends its identity to the PKG. The temporal revocable-key model divides the system's operational lifetime into a sequence of discrete time periods and assigns each signer mutually independent or unidirectionally evolving signing keys for different periods.

Let $N$ denote the maximum number of signatures supported by the system. The corresponding set of time or state indices is defined as: $\mathcal{T}=\{1,2,\cdots,N\}$. For signer $S$, its identity is denoted as $ID_S$. In the $i$-th time period, the signer holds a signing key $sk_{S,i}$, $i\in\mathcal{T}$, which is bound to its identity and time state. The corresponding key state is represented as: $st_{S,i}=\left(ID_S,i,sk_{S,i},status_{S,i}\right)$, where $status_{S,i}$ denotes the valid state of the signer in the $i$-th time period. It can take the following values:

$status_{S,i}\in\{\text{CREATED},\text{FROZEN},\text{AUTHORIZED},\text{SIGNED},\text{DELIVERED},$
$\text{VERIFIED},\text{DISPUTED},\text{CLOSED},\text{ABORTED}\}$.

The time-period-related revocation list $RL_i$ records identities that no longer possess signing authority during the $i$-th time period and subsequent periods. If $ID_S\in RL_i$, the signer is revoked from the $i$-th time period, and the system no longer generates, extracts, or updates valid signing keys for this signer. For any $j\geq i$, it holds that $ID_S\in RL_j$, which provides backward revocation and terminates the signing authority for future periods. For a non-revoked signer, the signing key is updated according to the time period: $sk_{S,i+1}\leftarrow keyupd\left(sk_{S,i},ID_S,i\right)$. After updating, the previous key is immediately deleted: $Erase\left(sk_{S,i}\right)$. The key update mechanism only supports forward evolution and prevents recovery of previous keys. Therefore, given the current key $sk_{S,i}$, it is infeasible to derive any previous key $sk_{S,j}$, $j<i$. During the $i$-th time period, the signer uses only the valid key $sk_{S,i}$ to generate a signature: $\sigma_i\leftarrow Sign\left(params,sk_{S,i},ID_S,i,m\right)$. When verifying a signature, the verifier must simultaneously check the correctness of the signature, the validity of the time state, and the signer's revocation status. The verification algorithm is denoted as:

$b\leftarrow Verify\left(params,ID_S,i,m,\sigma_i,RL_i\right)$, where $b\in\{0,1\}$.

The verification algorithm outputs 1 if and only if all the following conditions are satisfied: $ID_S\notin RL_i$, $1\leq i\leq N$, and $\sigma_i$ is a valid signature generated by the valid key of the $i$-th time period. Otherwise, the verification algorithm outputs 0.

**(5) Signing authorization request:** The signer requests signing authorization from the PKG by sending its identity information $ID_S$ and the session identifier $sid$ to the PKG. The PKG verifies whether the required conditions are satisfied,

namely, whether the signer's identity has been authenticated, whether the user has frozen the blinding key, and whether the current request has not expired. Once all conditions are satisfied, the PKG grants authorization and independently and randomly generates two session keys: $k_D^{sid}=(e_D,p_D)$, $k_A^{sid}=(e_A,p_A)$. The independence requirement is defined as follows: $\mathcal{H}_{k_A}$ and $\mathcal{H}_{k_D}$ are mutually independent Hilbert spaces, and $\rho_{k_Ak_D}=\rho_{k_A}\otimes\rho_{k_D}$. There exists no quantum operation that can recover $k_A^{sid}$ from $k_D^{sid}$. Therefore, even if one key is compromised, the other key cannot be derived. The PKG distributes $k_D^{sid}$ to the signer $S$ and the verifier $V$, and distributes $k_A^{sid}$ to the signer $S$ and the arbitrator $A$. The PKG then generates a unique authorization serial number $\omega_{sid}$. The corresponding authorization content is defined as: $Auth_{sid}=\mathrm{Canon}(ID_X,sid,info,n,\omega_{sid})$. Finally, the PKG updates the signer's state as: $status_{S,i}=\mathrm{AUTHORIZED}$.

### 3.2. Blinding Phase

Assume that the message to be signed by the user is a private binary message $msg=\{msg_1,msg_2,\cdots,msg_i,\cdots,msg_n\}$, $msg_i\in\{0,1\}$, with the agreed-upon public message $info$ and the entangled-particle sequence $U=\{U_1,U_2,\cdots,U_n\}$, which is pre-shared through the PKG.

**(1) The message is quantum-encoded and partially blinded.** Specifically, only the private message $msg$ is blinded, while the public information $info$ remains unblinded. The user first uniformly and randomly generates a basis-selection string $b=(b_1,b_2,\cdots,b_n)\xleftarrow{\$}\{0,1\}^n$, $b_i\in\{0,1\}$, and an $n$-bit classical blinding-key string $r=(r_1,r_2,\cdots,r_n)\xleftarrow{\$}\{0,1\}^n$, $r_i\in\{0,1\}$. For each private message bit $msg_i$, the user first performs a logical blinding operation using the Pauli-$X$ operator: $X_i^{r_i}|msg_i\rangle=|msg_i\oplus r_i\rangle$. The resulting logical bit is then encoded according to the basis-selection bit $b_i$. Thus, the $i$ th blinded message qubit is prepared as $|\phi_i^B\rangle=H_i^{b_i}X_i^{r_i}|msg_i\rangle=H_i^{b_i}|msg_i\oplus r_i\rangle$, namely,

$$|\phi_i^B\rangle=\begin{cases}|0\rangle, & msg_i\oplus r_i=0,\ b_i=0,\\ |1\rangle, & msg_i\oplus r_i=1,\ b_i=0,\\ |+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle), & msg_i\oplus r_i=0,\ b_i=1,\\ |-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle), & msg_i\oplus r_i=1,\ b_i=1.\end{cases}\tag{2}$$

When $b_i=0$, the blinded logical bit is encoded in the computational, or $Z$, basis $Z=\{|0\rangle,|1\rangle\}$; when $b_i=1$, it is encoded in the Hadamard, or $X$, basis $X=\{|+\rangle,|-\rangle\}$. Here, the symbol $X_i$ in the blinding operation denotes the Pauli-$X$ operator, whereas $X=\{|+\rangle,|-\rangle\}$ denotes the Hadamard measurement basis.

Let $|msg\rangle=\otimes_{i=1}^n|msg_i\rangle$, $H^b=\otimes_{i=1}^nH_i^{b_i}$, $X^r=\otimes_{i=1}^nX_i^{r_i}$, therefore, the complete partially blinded quantum message is

$$\begin{aligned}\left|m_{\text{blind}}\right\rangle &= \bigotimes_{i=1}^{n} H_i^{b_i} X_i^{r_i} \left|msg_i\right\rangle \\ &= \bigotimes_{i=1}^{n} H_i^{b_i} \left|msg_i \oplus r_i\right\rangle \\ &= H^b X^r \left|msg\right\rangle.\end{aligned} \tag{3}$$

It should be noted that, in $H^b X^r \left|msg\right\rangle$, the Pauli-$X$ blinding operation $X^r$ acts first on the logical message bits, followed by the basis-encoding operation $H^b$. Hence, for both $b_i = 0$ and $b_i = 1$, the random bit $r_i$ effectively maps the logical message bit $msg_i$ to $msg_i \oplus r_i$.

To prevent the user from selecting a new blinding key or a new basis-selection string after obtaining the signature, the user must register the blinding information with the PKG before signing. The registration information is defined as $R_{sid} = \text{Canon}(sid, \text{block}, b, r)$. The user prepares the corresponding quantum state $\left|R_{sid}\right\rangle$ and encodes it as $\Gamma_R = Q_{\text{Auth}}.\text{Enc}_{k_{PU}^R}\left(\left|R_{sid}\right\rangle\left\langle R_{sid}\right|\right)$, which is then sent to the PKG.

Upon receiving $\Gamma_R$, the PKG performs authentication decoding: $\left(f_R, \rho'_{R_{sid}}\right) = Q_{\text{Auth}}.\text{Dec}_{k_{PU}^R}\left(\Gamma_R\right)$. Only when $f_R = \text{acc}$ and the decoded registration information matches the current session does the PKG store $\text{Rec}[sid].(b,r) = (b,r)$. From that point onward, the registered basis-selection string $b$ and blinding-key string $r$ are frozen and cannot be modified for the current session.

**(2) Quantum Teleportation (Teleporting a Blinded State to the Signer):** The user performs a joint Bell measurement on the transmitted state particle and the EPR particle. Taking a single particle as an example: let $\left|\phi\right\rangle_{m_{b_i}} = \alpha\left|0\right\rangle_{m_{b_i}} + \beta\left|1\right\rangle_{m_{b_i}}$, and let the EPR state be $\left|\Phi^+\right\rangle_{U_iS_i} = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)_{U_iS_i}$. At this point, the entire system can be described as:

$$\begin{aligned}\left|\varphi_0\right\rangle_{m_{b_i}U_iS_i} &= \left|\phi\right\rangle_{m_{b_i}} \otimes \left|\Phi^+\right\rangle_{U_iS_i} \\ &= \left(\alpha\left|0\right\rangle_{m_{b_i}} + \beta\left|1\right\rangle_{m_{b_i}}\right) \otimes \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_{U_i}\left|0\right\rangle_{S_i} + \left|1\right\rangle_{U_i}\left|1\right\rangle_{S_i}\right) \\ &= \frac{1}{\sqrt{2}}\left(\alpha\left|000\right\rangle + \alpha\left|011\right\rangle + \beta\left|100\right\rangle + \beta\left|111\right\rangle\right)_{m_{b_i}U_iS_i}.\end{aligned} \tag{4}$$

Then, the user performs a CNOT operation and obtains $\left|\varphi_1\right\rangle$:

$$\begin{aligned}\left|\varphi_1\right\rangle_{m_{b_i}U_iS_i} &= \left(\text{CNOT} \otimes I\right)\left|\varphi_0\right\rangle_{m_{b_i}U_iS_i} \\ &= \left(\text{CNOT} \otimes I\right)\frac{1}{\sqrt{2}}\left(\alpha\left|000\right\rangle + \alpha\left|011\right\rangle + \beta\left|100\right\rangle + \beta\left|111\right\rangle\right)_{m_{b_i}U_iS_i} \\ &= \frac{1}{\sqrt{2}}\left(\alpha\left|000\right\rangle + \alpha\left|011\right\rangle + \beta\left|110\right\rangle + \beta\left|101\right\rangle\right)_{m_{b_i}U_iS_i}.\end{aligned} \tag{5}$$

The function of the H-Gate: $H\left|0\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right)$, $H\left|1\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right)$; User applies an H-gate to the first qubit, resulting in $\left|\varphi_2\right\rangle$:

$$
\begin{aligned}
\left|\varphi_2\right\rangle_{m_{b_i}U_iS_i} &= \left(H\otimes I\otimes I\right)\left|\varphi_1\right\rangle_{m_{b_i}U_iS_i} \\
&= \left(H\otimes I\otimes I\right)\frac{1}{\sqrt{2}}\left(\alpha\left|000\right\rangle+\alpha\left|011\right\rangle+\beta\left|110\right\rangle+\beta\left|101\right\rangle\right)_{m_{b_i}U_iS_i} \\
&= \frac{1}{\sqrt{2}}\left[\alpha\frac{1}{\sqrt{2}}\left(\left|0\right\rangle+\left|1\right\rangle\right)\otimes\left(\left|00\right\rangle+\left|11\right\rangle\right)\right. \\
&\quad \left.+\beta\frac{1}{\sqrt{2}}\left(\left|0\right\rangle-\left|1\right\rangle\right)\otimes\left(\left|10\right\rangle+\left|01\right\rangle\right)\right] \\
&= \frac{1}{2}\left(\alpha\left|000\right\rangle+\alpha\left|100\right\rangle+\alpha\left|011\right\rangle+\alpha\left|111\right\rangle\right. \\
&\quad \left.+\beta\left|010\right\rangle-\beta\left|110\right\rangle+\beta\left|001\right\rangle-\beta\left|101\right\rangle\right)_{m_{b_i}U_iS_i}.
\end{aligned}
\tag{6}
$$

To make the measurement results easier to read, we rearrange $\left|\varphi_2\right\rangle$ to get:

$$
\begin{aligned}
\left|\varphi_2\right\rangle_{m_{b_i}U_iS_i} &= \frac{1}{2}\left(\left|00\right\rangle_{m_{b_i}U_i}\otimes\left(\alpha\left|0\right\rangle+\beta\left|1\right\rangle\right)_{S_i}+\left|10\right\rangle_{m_{b_i}U_i}\otimes\left(\alpha\left|0\right\rangle-\beta\left|1\right\rangle\right)_{S_i}\right. \\
&\quad \left.+\left|01\right\rangle_{m_{b_i}U_i}\otimes\left(\alpha\left|1\right\rangle+\beta\left|0\right\rangle\right)_{S_i}+\left|11\right\rangle_{m_{b_i}U_i}\otimes\left(\alpha\left|1\right\rangle-\beta\left|0\right\rangle\right)_{S_i}\right).
\end{aligned}
\tag{7}
$$

Next, the user measures the two qubits in the computational basis $\left\{\left|0\right\rangle,\left|1\right\rangle\right\}$. The four possible measurement outcomes and the corresponding recovery operations are summarized in Table 1.

Table 1. Correspondence between the user's measurement outcomes and the signer's quantum-state recovery operations.

| Measurement outcome | Post-measurement state of $S_i$ | Recovery operation $U_\gamma$ | Probability |
|---|---|---|---|
| 00 | $\alpha\left\|0\right\rangle+\beta\left\|1\right\rangle$ | $I$ | 1/4 |
| 01 | $\alpha\left\|1\right\rangle+\beta\left\|0\right\rangle$ | $X$ | 1/4 |
| 10 | $\alpha\left\|0\right\rangle-\beta\left\|1\right\rangle$ | $Z$ | 1/4 |
| 11 | $\alpha\left\|1\right\rangle-\beta\left\|0\right\rangle$ | $ZX$ | 1/4 |

The quantum circuit design is as shown in Figure 1:

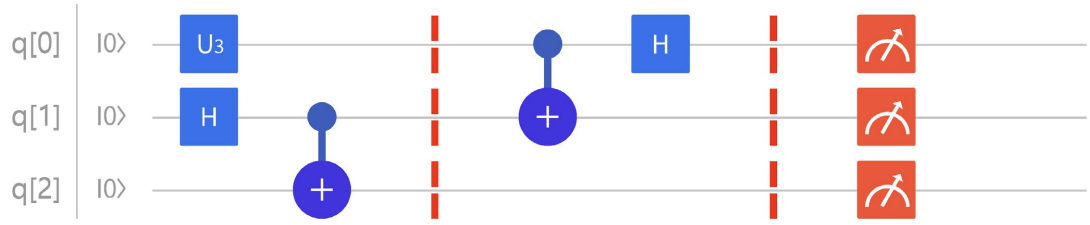


Figure 1. Three-qubit simulation circuit for quantum teleportation.

$U_3\left(\theta,\phi,\lambda\right)=\begin{bmatrix}\cos\frac{\theta}{2} & -e^{i\lambda}\sin\frac{\theta}{2}\\ e^{i\phi}\sin\frac{\theta}{2} & e^{i(\lambda+\phi)}\cos\frac{\theta}{2}\end{bmatrix}$, assume that $\theta=\pi/2$, $\phi=0$, and $\lambda=0$; the three-Qubit measurement results are output as Figure 2:

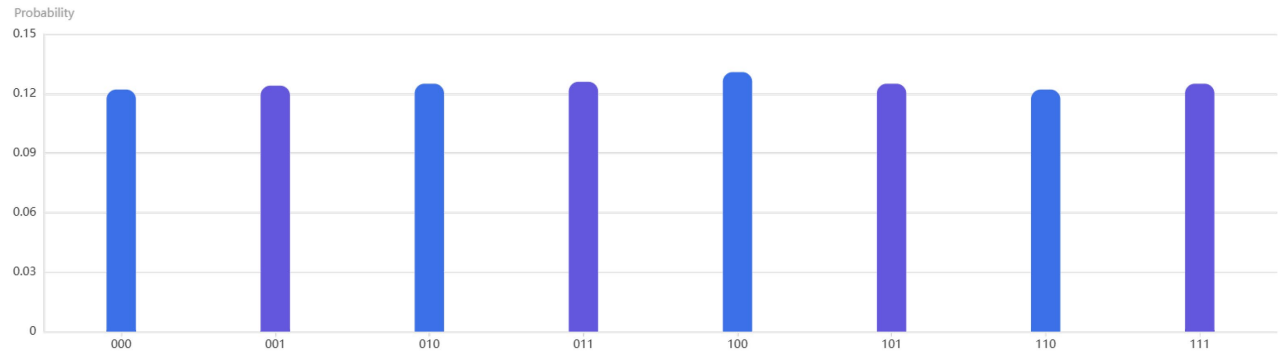


**Figure 2.** Probability distribution of three-qubit measurement outcomes in the quantum teleportation circuit.

The simulator measures all three qubits and therefore reports eight three-bit outcomes, each occurring with an ideal probability of approximately 1/8. However, only the last two measured bits constitute the Bell-measurement outcome $\gamma_i = (x_i, z_i)$. By marginalizing over the receiver-qubit measurement result, the corresponding Bell-outcome probabilities are

$$\begin{aligned} P_{\text{Bell}}(00) &= P(000) + P(100), \\ P_{\text{Bell}}(01) &= P(001) + P(101), \\ P_{\text{Bell}}(10) &= P(010) + P(110), \\ P_{\text{Bell}}(11) &= P(011) + P(111), \end{aligned} \tag{8}$$

which are all approximately 1/4 under ideal teleportation.

**Table 2.** Measurement probabilities corresponding to different Bell measurement outcomes.

| Bell measurement outcome $(x,z)$ | Quantum state $(q_2,q_1,q_0)$ | State probability | Measurement-outcome probability |
|---|---|---|---|
| 00 | $\|000\rangle$ | 0.1220703 | 0.2529296 |
| | $\|100\rangle$ | 0.1308593 | |
| 01 | $\|001\rangle$ | 0.1240234 | 0.2490234 |
| | $\|101\rangle$ | 0.1250000 | |
| 10 | $\|010\rangle$ | 0.1250000 | 0.2470703 |
| | $\|110\rangle$ | 0.1220703 | |
| 11 | $\|011\rangle$ | 0.1259765 | 0.2509765 |
| | $\|111\rangle$ | 0.1250000 | |

The above results were obtained through online testing on the Origin Quantum platform, with the number of shots set to 1024. Table 2 presents the simulation results for the four possible Bell measurement outcomes. For each measurement outcome , the corresponding probability is obtained by summing the probabilities of the two associated computational-basis states. The resulting probabilities for the four outcomes are all close to the theoretical value of (1/4), indicating an ap-

proximately uniform distribution of the Bell measurement results.

The user performs a Bell-basis measurement on $\left(\left|m_{\text{blind}}\right\rangle, U\right)$ and obtains a 2-bit classical result $\gamma_i = (x_i, z_i) \in \{0,1\}^2$, $\gamma_i \in \{00,01,10,11\}$, $\gamma = \{(x_1, z_1), \cdots, (x_i, z_i), \cdots, (x_n, z_n)\} \in \{0,1\}^{2n}$.

Then the user sends $(sid, \gamma, info)$ to the signer via a classical channel; the signer can only retrieve the message $info$, but cannot access the original message $msg$ or quantum state $|msg\rangle$ to be signed.

In order to check whether the channel is secure, the user generates $d$ decoy states randomly, selecting them from four sets of non-orthogonal states: $|0\rangle$, $|1\rangle$, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. From each group, $X$-basis and $Z$-basis states are randomly selected to prepare the quantum states. The detection bit is then sent to the signer through the quantum channel.

### 3.3. Signing Phase

After receiving the decoy states sent by the user, both the user and the signer randomly select the $X$ basis or $Z$ basis for measurement. All measurement bases and measurement outcomes are stored. Half of the measurement bases and their corresponding measurement results are randomly disclosed, and the average channel error rate $e$ is calculated. Let $e_{\text{th}}$ denote the threshold. If $e > e_{\text{th}}$, it is determined that an eavesdropping attack exists on the channel, and set $status_{S,i} = \text{ABORTED}$; otherwise, proceed with the subsequent signature operations.

Quantum collapse state: After the user performs the Bell-basis measurement, the particle $S$ in the hands of the remote signer collapses, and its state is denoted as: $\left|\varphi_\gamma\right\rangle_{S_i} = U_\gamma^\dagger \left|m_{\text{blind}}\right\rangle$. If the signer performs the corresponding Pauli operation $U_\gamma$ on $S_i$, where $U_\gamma = Z^{z_i} X^{x_i}$, then

$$\begin{aligned} U_\gamma \left|\varphi_\gamma\right\rangle_{S_i} &= Z^{z_i} X^{x_i} \left|\varphi_\gamma\right\rangle_{S_i} \\ &= Z^{z_i} X^{x_i} X^{x_i} Z^{z_i} \left|m_{\text{blind}}\right\rangle \\ &= \mathrm{e}^{\mathrm{i}\theta} \left|m_{\text{blind}}\right\rangle. \end{aligned} \tag{9}$$

Since a global phase has no physical effect, this operation restores the blinded state: $\left|m_{\text{blind}}\right\rangle = U_\gamma \left|\varphi_\gamma\right\rangle_{S_i}$.

Therefore, after receiving $(sid, \gamma, info)$, the signer performs the Bell correction to obtain $\left|m_{\text{blind}}\right\rangle$. The signer only signs when the following conditions are met: $status_{S,i} = \text{AUTHORIZED}$, $ID_S \notin RL_i$, and $1 \le i \le N$. The generated state signature is as follows:

$$\sigma_i = Enc_{sk_{S,i}}\left(\left|m_{\text{blind}}\right\rangle, ID_S, i, sid\right). \tag{10}$$

The direct verification tag is $L_D = \text{Canon}(sid, \omega_{sid}, i, \text{DIRECT})$, the arbitration tag is $L_A = \text{Canon}(sid, \omega_{sid}, i, \text{ARBITRATION})$, and the signer prepares these as

the computational basis quantum states: $|L_D\rangle, |L_A\rangle$.

The direct verification payload is $|W_D\rangle = |m_{\text{blind}}\rangle_D \otimes |L_D\rangle$, with density operator $\rho_{W_D} = |W_D\rangle\langle W_D|$; and the signer computes

$$\Sigma_D = Q_{Auth}.Enc_{k_D^{sid}}\left(\rho_{W_D}, \sigma_i\right). \tag{11}$$

$\Sigma_D$ is the quantum signature evidence provided to the user and ultimately verified by the designated verifier. Execute $status_{S,i} = \text{SIGNED}$, and share the temporal key $sk_{S,i}$ with the verifier after the signature is completed. This temporal key will immediately lose its signature capability after the signature is completed within the period, and can only be used for subsequent verification of the completed signature.

The arbitration payload is $|W_A\rangle = |m_{\text{blind}}\rangle_A \otimes |L_A\rangle$, and its density operator is $\rho_{W_A} = |W_A\rangle\langle W_A|$. The signer computes $\Sigma_A = Q_{\text{Auth}}.Enc_{k_A^{sid}}\left(\rho_{W_A}, \sigma_i\right)$; $\Sigma_A$ must be delivered directly by the signer to the arbitrator and cannot be relayed through the user or verifier.

The signer sends $\Sigma_D \to U$ to the user, and the signer sends $\Sigma_A \to A$ to the arbitrator. The arbitrator only stores $\Sigma_A$ and the receipt time, without decoding it immediately.

After confirming that the arbitrator has received $\Sigma_A$, PKG marks this session as signed.

Sign output: The user holds $\Sigma_D$; the arbitrator holds $\Sigma_A$; PKG stores $\omega_{sid}$, $k_D^{sid}$, $k_A^{sid}$, and the frozen $(b, r)$.

### 3.4. Verification Phase

The user sends the direct verification evidence $\Sigma_D$ to the designated verifier via quantum teleportation. To ensure that the verification input clearly corresponds to the message $m$, the user can additionally prepare a reference message state $|M_{\text{ref}}\rangle \equiv |msg\rangle$ and deliver it to the verifier via quantum teleportation. Since $m$ is a classical binary string, preparing a reference state on a computational-basis state does not violate the no-cloning theorem.

The user sends an unblinding request $Open_{sid} = \text{Canon}(sid, \text{OPEN})$ to the PKG. After the PKG verifies the user's identity, session status, and arbitration-evidence receipt record, it securely releases the data $\left(r, b, k_D^{sid}, \omega_{sid}, Ctx[sid]\right)$ to the designated verifier. At this stage, only the value of $(b, r)$ frozen in the database prior to signing may be retrieved; the user cannot submit a new value $(b', r')$.

The unblinding output $\left(\Sigma_D, |M_{\text{ref}}\rangle, r, k_D^{sid}, \omega_{sid}, Ctx[sid]\right)$ is held by the verifier, who decodes it using a one-time direct verification key: $\left(f_D, \rho'_{W_D}, \sigma'_i\right) = Q_{\text{Auth}}.Dec_{k_D^{sid}}(\Sigma_D)$. If $f_D = \text{rej}$, the request is immediately rejected. If authentication succeeds, the verifier records the recovered payload as $\rho'_{W_D} = |m'_{\text{blind}}\rangle\langle m'_{\text{blind}}| \otimes |L'_D\rangle\langle L'_D|$, where $|m'_{\text{blind}}\rangle$ is the recovered blinded-mes-

sage register; $|L_D'\rangle$ is the recovered direct-verification-tag register. $\sigma_i'$ is the temporal signature obtained after decoding. The verifier performs decryption on $\sigma_i'$ using the temporal key $sk_{S,i}$ shared with the signer:

$$Dec_{sk_{S,i}}(\sigma_i') = Dec_{sk_{S,i}}\left(Enc_{sk_{S,i}}\left(|m_{\text{blind}}\rangle, ID_S, i, sid\right)\right) \tag{12}$$

and obtains $\left(|m''_{\text{blind}}\rangle, ID_S', i', sid'\right)$. It then compares $sid \stackrel{?}{=} sid'$; if they are the same, verification continues; otherwise, the signature is declared invalid.

The verifier measures the tag register to obtain $L_D'$ and computes $L_D^{\text{exp}} = \text{Canon}\left(sid, \omega_{sid}, i, \text{DIRECT}\right)$ based on the values of $sid$ and $\omega_{sid}$ provided by the PKG. The verification condition is $L_D' = L_D^{\text{exp}}$. At the same time, the verifier checks the PKG's immutable record: $Ctx[sid] = (ID_U, ID_S, ID_V, ID_A, info, n, T)$, and confirms $Ctx[sid].ID_V = ID_V$, $Ctx[sid].ID_S = ID_S'$, $Ctx[sid].info = info$, and $Ctx[sid].T > t$. This step enables the short tag to indirectly bind the complete public information through $sid$ and $\omega_{sid}$.

Perform quantum unblinding: The verifier applies the inverse basis-encoding operation followed by the Pauli-$X$ unblinding operation to the blinded-message register: $|M'\rangle = X^r H^b |m_{\text{blind}}\rangle$. Under honest conditions, $|m_{\text{blind}}\rangle = H^b X^r |msg\rangle$. Therefore,

$$\begin{aligned} |M'\rangle &= X^r H^b |m_{\text{blind}}\rangle \\ &= X^r H^b H^b X^r |msg\rangle \\ &= X^r X^r |msg\rangle \\ &= |msg\rangle. \end{aligned} \tag{13}$$

Then, the verifier performs the same unblinding operation on the blinded-message state $|m''_{\text{blind}}\rangle$ recovered from the temporal protected payload: $|M''\rangle = X^r H^b |m''_{\text{blind}}\rangle$. If the temporal protection is correct, then $|m''_{\text{blind}}\rangle = |m_{\text{blind}}\rangle = H^b X^r |msg\rangle$. Hence,

$$\begin{aligned} |M''\rangle &= X^r H^b |m''_{\text{blind}}\rangle \\ &= X^r H^b H^b X^r |msg\rangle \\ &= X^r X^r |msg\rangle \\ &= |msg\rangle. \end{aligned} \tag{14}$$

The verifier can perform a quantum equality check without immediately measuring the complete message. It prepares two independent auxiliary registers, $|0\rangle_{C_1}^{\otimes n}$ and $|0\rangle_{C_2}^{\otimes n}$, and executes the following sequence:

$$\prod_{i=1}^{n} \text{CNOT}_{M_i' \to C_{1,i}} \text{CNOT}_{M_{\text{ref},i} \to C_{1,i}}, \quad \prod_{i=1}^{n} \text{CNOT}_{M_{\text{ref},i} \to C_{2,i}} \text{CNOT}_{M_i'' \to C_{2,i}}. \tag{15}$$

If $|M'\rangle = |M_{\text{ref}}\rangle$, then the auxiliary register $C_1$ retains the value $|0\rangle_{C_1}^{\otimes n}$. If $|M_{\text{ref}}\rangle = |M''\rangle$, then the auxiliary register $C_2$ retains the value $|0\rangle_{C_2}^{\otimes n}$. The auxiliary-register measurement result is defined as:

$$f_M = \begin{cases} 1, & C_1 = 0^n \text{ and } C_2 = 0^n, \\ 0, & \text{otherwise.} \end{cases} \tag{16}$$

The final acceptance criterion is defined as follows:
$\text{Accept} \Leftrightarrow \left[f_D = \text{acc}\right] \wedge \left[L'_D = L_D^{\exp}\right] \wedge \left[f_M = 1\right] \wedge \left[Ctx\left[sid\right] \text{valid}\right]$. The verifier then declares the signature valid and sets $status_{S,i} = \text{VERIFIED}$.

### 3.5. Arbitration Phase

When a user, signer, or verifier disputes the verification result, the arbitrator uses $\Sigma_A$—which was submitted directly by the signer and stored during the signing phase—to render a decision.

The PKG securely releases $\left(r, k_A^{sid}, \omega_{sid}, Ctx\left[sid\right]\right)$ to the arbitrator. The arbitrator decodes the arbitration evidence as

$$\left(f_A, \rho'_{W_A}, \sigma''_i\right) = Q_{\text{Auth}}.Dec_{k_A^{sid}}\left(\Sigma_A\right). \tag{17}$$

If $f_A = \text{rej}$, the arbitration evidence is declared invalid. If authentication succeeds, the arbitrator recovers

$$\rho'_{W_A} = \left|m'_{\text{blind}}\right\rangle\left\langle m'_{\text{blind}}\right| \otimes \left|L'_A\right\rangle\left\langle L'_A\right|, \tag{18}$$

where $\sigma''_i$ is the temporal signature obtained after decoding.

The arbitrator decrypts $\sigma''_i$ using the temporal key $sk_{S,i}$ shared with the signer:

$$\begin{aligned} Dec_{sk_{S,i}}\left(\sigma''_i\right) &= Dec_{sk_{S,i}}\left(Enc_{sk_{S,i}}\left(\left|m_{\text{blind}}\right\rangle, ID_S, i, sid\right)\right) \\ &= \left(\left|m''_{\text{blind}}\right\rangle\right\rangle ID'_S, i', sid'\right). \end{aligned} \tag{19}$$

The arbitrator then compares $sid \stackrel{?}{=} sid'$. If the two session identifiers are equal, the arbitration procedure continues; otherwise, the signature is declared invalid.

Then, the arbitrator calculates the expected label $L_A^{\exp} = \text{Canon}\left(sid, \omega_{sid}, i, \text{ARBITRATION}\right)$, and checks $L'_A = L_A^{\exp}$, then performs unblinding: $\left|M_A\right\rangle = X^r H^b \left|m'_A\right\rangle$, $\left|M''\right\rangle = X^r H^b \left|m''_{\text{blind}}\right\rangle$. The arbitrator performs an equality check between $\left|M_A\right\rangle$, $\left|M''\right\rangle$, and the reference state $\left|M_{\text{dis}}\right\rangle$ of the disputed message. The condition for arbitration acceptance is
$\text{Accept} \Leftrightarrow \left[f_A = \text{acc}\right] \wedge \left[L'_A = L_A^{\exp}\right] \wedge \left[\left|M_A\right\rangle = \left|M''\right\rangle = \left|M_{\text{dis}}\right\rangle\right] \wedge \left[Ctx\left[sid\right] \text{valid}\right]$.
Since $\Sigma_A$ is evidence sent directly by the signer to the arbitrator and protected by an independent key $k_A^{sid}$, neither the user nor the verifier can fabricate valid arbitration evidence by modifying or re-encoding $\Sigma_D$. If the results of routine verification do not match the arbitration results, the protocol treats $\Sigma_A$ stored by the arbitrator as the official evidence of the dispute.

## 4. Security Analysis

In our security model, both the PKG and the arbitrator are assumed to be trusted and non-colluding entities; scenarios in which either the PKG or the arbitrator is

fully compromised are outside the scope of this work.

### 4.1. Correctness Analysis

The correctness of the proposed scheme requires that, when all participants honestly follow the protocol and the quantum channels are ideal, a legitimately generated signature is accepted by the designated verifier.

The user's original message is represented by the computational-basis state $|msg\rangle$. Before signing, the user randomly selects a basis-selection string $b \in \{0,1\}^n$ and a blinding key $r \in \{0,1\}^n$, and performs the bitwise Pauli-$X$ operation followed by the basis encoding, $|m_{\text{blind}}\rangle = H^b X^r |msg\rangle$. During quantum teleportation, the user performs Bell-basis measurements and obtains the classical outcome $\gamma = ((x_1, z_1), \cdots, (x_n, z_n))$.

After receiving $\gamma$, the signer applies $U_\gamma$ and obtains $|m_{\text{blind}}\rangle$. The signer then generates the temporal signature $\sigma_i$ and constructs the direct-verification evidence $\Sigma_D$. Under honest execution, quantum authentication decoding succeeds: $(f_D, \rho'_{W_D}, \sigma'_i) = Q_{\text{Auth}}.\text{Dec}_{k_D^{sid}}(\Sigma_D)$. Using the corresponding temporal key $sk_{S,i}$, the verifier recovers $(|m''_{\text{blind}}\rangle, ID_{S'}, i', sid') = (|m_{\text{blind}}\rangle, ID_S, i, sid)$.

After the PKG releases the basis-selection string $b$ and the blinding key $r$ that were frozen before signing, the verifier performs unblinding:

$$\begin{aligned} |M'\rangle &= X^r H^b |m'_{\text{blind}}\rangle \\ &= X^r H^b H^b X^r |msg\rangle \\ &= X^r X^r |msg\rangle \\ &= |msg\rangle, \end{aligned} \tag{20}$$

and similarly, $|M''\rangle = X^r H^b |m''_{\text{blind}}\rangle = |msg\rangle$.

Since the reference state satisfies $|M_{\text{ref}}\rangle = |msg\rangle$, the message-consistency test yields $|M'\rangle = |M''\rangle = |M_{\text{ref}}\rangle$. Therefore, every legitimately generated signature is accepted by the designated verifier, which establishes the correctness of the proposed scheme.

### 4.2. Non-Forgeability Analysis

If an attacker does not know $k_D^{sid}$ or $k_A^{sid}$, the probability that an unauthorized modification to $\Sigma_D$ or $\Sigma_A$ is erroneously accepted is at most $\varepsilon_{\text{auth}}$. Moreover, since the authorization tag is bound to the one-time values $sid$ and $\omega_{sid}$, the attacker cannot transplant authentication evidence from another session into the current session.

If the verifier accepts a different payload $\tilde{m}_1 \neq msg$, or a different tag $\tilde{L}_D \neq L_D$, then the attacker has compromised the integrity of the quantum authentication code. Therefore,

$$\Pr\left[ f_D = \text{acc} \wedge (\tilde{m}_1, \tilde{L}_D) \neq (m, L_D) \right] \leq \varepsilon_{\text{auth}}. \tag{21}$$

To forge a valid signature, an external attacker must generate direct verification

evidence that can pass the verifier's authentication procedure:

$$\Sigma_D = Q_{\text{Auth}}.\text{Enc}_{k_D^{sid}}\left(\rho_{W_D}, \sigma_i\right). \tag{22}$$

Assume that the session key $k_D^{sid}$ is a uniformly random classical key of length $2n$. If the attacker has no information about this key, the probability of correctly guessing the entire key is

$$\left(\frac{1}{2}\right)^{2n} = \frac{1}{2^{2n}}, \tag{23}$$

which decreases exponentially with $n$.

The temporal signature $\sigma_i$ is generated using the temporal signing key $sk_{S,i}$:

$$\sigma_i = \text{Enc}_{sk_{S,i}}\left(\left|m_{\text{blind}}\right\rangle, ID_S, i, sid\right). \tag{24}$$

Assume that $sk_{S,i}$ is a uniformly random $n$-bit key. Without knowledge of the key, an attacker attempting to forge a temporal signature can guess each key bit correctly with probability 1/2. Consequently, the probability of correctly guessing the entire key is $\frac{1}{2^n}$, which also decreases exponentially with $n$.

### 4.3. Non-Repudiation Analysis

**(1) Non-repudiation of the signer**

The signer's non-repudiation is mainly guaranteed by the independent arbitration evidence $\Sigma_A$. The evidence $\Sigma_A$ is generated by the signer during the signing phase and is delivered directly to the arbitrator for storage. Unlike the direct-verification evidence $\Sigma_D$ used for routine verification, $\Sigma_A$ is protected by the independent arbitration key $k_A^{sid}$ and is not transmitted through either the user or the designated verifier. Therefore, other participants cannot replace or regenerate valid arbitration evidence.

The temporal signature contained in the arbitration evidence is record as $\sigma_i$ and the arbitration tag is defined as $Ł_A$. The arbitration evidence is bound to the signer identity $ID_S$, the session identifier $sid$, the time period $i$, the one-time authorization value $\omega_{sid}$, and the corresponding blinded message. Valid arbitration evidence generated in one authorized session cannot be transferred to another signer, time period, or session without causing the corresponding identity, session, or tag-consistency verification to fail.

Moreover, the blinding key $r$ and the basis-selection string $b$ is frozen by the PKG before the signing operation, and the corresponding session information is stored in the immutable record: $Ctx[sid]$. Therefore, after the signature has been generated, the signer cannot deny the completed signing operation by modifying the message, identity information, authorization information, or session parameters, since such a claim would be inconsistent with the arbitration evidence and the session record maintained by the PKG.

In addition, the arbitration key $k_A^{sid}$ and the direct-verification key $k_D^{sid}$ are independently generated, and $k_A^{sid}$ is not disclosed to the user or the designated

verifier. Therefore, neither the user nor the verifier can construct valid arbitration evidence $\Sigma_A$ from the direct-verification evidence $\Sigma_D$. If an adversary modifies or forges $\Sigma_A$ without authorization and the forged evidence is nevertheless accepted, then the integrity of the underlying quantum authentication scheme has been compromised. Thus, $\Pr\left[f_A = \mathrm{acc} \wedge \left(\tilde{\rho}_{W_A}, \tilde{\sigma}_i\right) \neq \left(\rho_{W_A}, \sigma_i\right)\right] \leq \varepsilon_{\mathrm{auth}}$.

Therefore, under the assumptions that the PKG is trustworthy, the session record is immutable, and the arbitration key $k_A^{sid}$ remains secret, once $\Sigma_A$ passes authentication and its identity, time-period, session, and message information are consistent with the system records, the signer cannot deny having completed the signature in the corresponding authorized session.

**(2) Non-repudiation of the user**

The user's non-repudiation mainly ensures that the user cannot deny participation in the corresponding signing session or the blinding information submitted and frozen before signing. Before the signing operation begins, the user generates the blinding key $r$ and the basis-selection string $b$, and registers $R_{sid}$ with the PKG. The PKG stores $\mathrm{Rec}[sid].(b,r) = (b,r)$ only if authentication succeeds and the $sid$ contained in the authenticated data matches the current session. Once this record has been established, the blinding key $r$ and the basis-selection string $b$ are frozen for the current session and cannot be replaced by different value $b', r'$ after signing.

Since $sid$ is a globally unique session identifier and $Ctx[sid]$ records the user identity $ID_U$ together with the parameters of the corresponding session, the user identity, signing session, and frozen basis-selection string and blinding key are bound to the same session record. If the user later denies participation in the session or claims that a different basis-selection string $b' \neq b$ or blinding key $r' \neq r$ was used, such a claim will be inconsistent with the authenticated registration record stored by the PKG.

Furthermore, the corresponding blinded message is contained in the arbitration evidence. Under honest protocol execution, $|m_{\mathrm{blind}}\rangle = H^b X^r |msg\rangle$. Using the basis-selection string $b$ and the blinding key $r$ frozen by the PKG before signing, the original message can be recovered as $X^r H^b |m_{\mathrm{blind}}\rangle = |msg\rangle$. If the user attempts to replace the original blinding key with a different value $r' \neq r$ after signing, then $X^{r'} H^b |m_{\mathrm{blind}}\rangle = X^{r'} H^b H^b X^r |msg\rangle = |msg \oplus r \oplus r'\rangle$, which, in general, differs from the original message $|msg\rangle$. Therefore, the result cannot simultaneously satisfy the consistency requirements of the arbitration evidence and the frozen blinding information maintained by the PKG.

Moreover, if an adversary attempts to forge or modify the user's blinding-key registration information, it must construct authenticated data without knowledge of $k_{PU}^R$. According to the security of the quantum authentication scheme, the probability that a forged or modified registration is nevertheless accepted satisfies $\Pr\left[f_R = \mathrm{acc} \wedge \tilde{R}_{sid} \neq R_{sid}\right] \leq \varepsilon_{\mathrm{auth}}$.

Therefore, under the assumptions that the PKG is trustworthy, the session record is immutable, $k_{PU}^R$ remains secret, and the blinding key $r$ is correctly fro-

zen before signing, the user cannot deny participation in the corresponding signing session or alter the signing result by replacing the blinding parameter after the signature has been generated.

### 4.4. Partial Blindness Analysis

Given public information $info$ and two distinct private messages $msg_0 \neq msg_1$, corresponding to the quantum states $|msg_0\rangle$ and $|msg_1\rangle$, the protocol satisfies partial blindness if the signer's complete views for the two messages are indistinguishable, *i.e.*, $\rho_{(msg_0|info)} = \rho_{(msg_1|info)}$.

**User blindness and the Bell-measurement process:** Let the private message quantum state be $|msg\rangle = \otimes_{i=1}^{n} |msg_i\rangle$, $msg_i \in \{0,1\}$. Before signing, the user uniformly and randomly selects a basis-selection string $b$ and a blinding-key string $r$. The user first performs the Pauli-$X$ blinding operation on the logical message bits and then performs the basis encoding. Thus, $|m_{\text{blind}}\rangle = H^b X^r |msg\rangle$.

For the $i$th message bit, $|\phi_i^B\rangle = H_i^{b_i} X_i^{r_i} |msg_i\rangle = H_i^{b_i} |msg_i \oplus r_i\rangle$. When $b_i = 0$, $|\phi_i^B\rangle = |msg_i \oplus r_i\rangle$, whereas when $b_i = 1$, $|\phi_i^B\rangle = H_i |msg_i \oplus r_i\rangle$. Hence, the random bit $r_i$ blinds the logical value before either encoding basis is applied.

Let $U_i$ and $S_i$ denote the user's and signer's entangled particles, respectively. The shared EPR state is $|\Phi^+\rangle_{U_iS_i} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{U_iS_i}$. The joint system is expressed as

$$|\Psi\rangle = |\phi_i^B\rangle_{m_{U_i}} \otimes |\Phi^+\rangle_{U_iS_i}. \tag{25}$$

The user performs the Bell-basis operations $\text{CNOT}_{m_{U_i} \to U_i}$ and $H_{m_{U_i}}$, where

$$\text{CNOT}|a\rangle|b\rangle = |a\rangle|a \oplus b\rangle, \tag{26}$$

and

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{27}$$

For the $i$th qubit, the Bell-basis measurement produces the two-bit classical result $\gamma_i = (x_i, z_i) \in \{00,01,10,11\}$. For the complete $n$-qubit message, the Bell-measurement result is $\gamma = ((x_1, z_1), \cdots, (x_n, z_n)) \in \{0,1\}^{2n}$. Under ideal teleportation, the Bell-measurement outcomes are uniformly distributed and independent of the input state, and hence $\Pr[\gamma] = \frac{1}{4^n}$.

**Quantum state received by the signer:** According to the quantum teleportation protocol, the Bell-measurement result $\gamma$ determines the Pauli correction

$$U_\gamma = \overset{n}{\underset{i=1}{\otimes}} Z_i^{z_i} X_i^{x_i} \in \{I, X, Z, XZ\}^{\otimes n}. \tag{28}$$

After receiving $\gamma$, the signer performs the corresponding correction and obtains $U_\gamma |\varphi_\gamma\rangle \doteq |m_{\text{blind}}\rangle = H^b X^r |msg\rangle$, where $\doteq$ denotes equality up to an irrelevant global phase.

Therefore, the blindness analysis must consider the signer's state after the Bell-measurement result $\gamma$ has been received and the corresponding correction has been completed. For any fixed basis-selection string $b$ and Bell-measurement result $\gamma$, since the blinding-key string $r$ is uniformly random and remains unknown to the signer, the density operator observed by the signer is

$$\begin{aligned}\rho(msg\,|\,b,\gamma) &= \frac{1}{2^n}\sum_{r\in\{0,1\}^n} H^b X^r \left|msg\right\rangle\left\langle msg\right| X^r H^b \\ &= H^b\left[\frac{1}{2^n}\sum_{r\in\{0,1\}^n}\left|msg\oplus r\right\rangle\left\langle msg\oplus r\right|\right]H^b \\ &= H^b\frac{I_{2^n}}{2^n}H^b \\ &= \frac{I_{2^n}}{2^n}.\end{aligned} \tag{29}$$

For any two distinct private messages $msg_0 \neq msg_1$, we therefore have

$$\rho(msg_0\,|\,b,\gamma)=\frac{I_{2^n}}{2^n},\rho(msg_1\,|\,b,\gamma)=\frac{I_{2^n}}{2^n}. \tag{30}$$

Consequently, $\rho_S(msg_0\,|\,b,\gamma)=\rho_S(msg_1\,|\,b,\gamma)$.

The above result holds for every basis-selection string $b$ and every Bell-measurement result $\gamma$. In particular, when $b_i=0$, the Pauli-$X$ operation gives $X_i^{r_i}\left|msg_i\right\rangle=\left|msg_i\oplus r_i\right\rangle$. When $b_i=1$, the logical value is first blinded by $X_i^{r_i}$ and then encoded in the Hadamard basis: $H_i X_i^{r_i}\left|msg_i\right\rangle=H_i\left|msg_i\oplus r_i\right\rangle$. Thus, the logical message value is randomized by $r_i$ under either message-encoding basis.

Finally, the signer obtains not only the restored blinded quantum state, but also the Bell-measurement result $\gamma$ and the public information $info$. Hence, the signer's complete classical–quantum view can be written as

$$\rho(msg\,|\,b,info)=\frac{1}{4^n}\sum_{\gamma\in\{0,1\}^{2n}}\left|\gamma\right\rangle\left\langle\gamma\right|\otimes\frac{I_{2^n}}{2^n}\otimes\left|info\right\rangle\left\langle info\right|. \tag{31}$$

Therefore, for any two distinct private messages $msg_0$ and $msg_1$ associated with the same public information $info$, $\rho(msg_0\,|\,b,info)=\rho(msg_1\,|\,b,info)$. Hence, even after receiving the complete Bell-measurement result $\gamma$ and restoring the blinded quantum state, the signer cannot distinguish the user's private message, while the agreed public information $info$ remains visible. Therefore, the proposed protocol satisfies partial blindness.

### 4.5. Resistance against Third-Party Attacks

**Entangling-Probe Attack:** The attacker Eve prepares a blank ancillary particle in the state $\left|e\right\rangle$ and applies an interaction $V$ satisfying

$$V\left|0\right\rangle\left|e\right\rangle=\left|0\right\rangle\left|e_{00}\right\rangle+\left|1\right\rangle\left|e_{01}\right\rangle,\ V\left|1\right\rangle\left|e\right\rangle=\left|1\right\rangle\left|e_{10}\right\rangle+\left|1\right\rangle\left|e_{11}\right\rangle, \tag{32}$$

where the ancillary vectors satisfy the unitarity condition $V^{\dagger}V=I$. For uni-

formly distributed inputs in the $Z$ basis, the induced error rate is

$$e_Z = \frac{1}{2}\left(\langle e_{01}|e_{01}\rangle + \langle e_{10}|e_{10}\rangle\right). \tag{33}$$

If the attacker introduces strictly zero errors in both the $Z$ and $X$ bases, then the attacker cannot obtain any information about the original bit. Zero error in the $Z$ basis requires

$$V|0\rangle|e\rangle = |0\rangle|e_0\rangle,\ V|1\rangle|e\rangle = |1\rangle|e_1\rangle. \tag{34}$$

For $|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$, linearity gives: $V|+\rangle|e\rangle = \frac{|0\rangle|e_0\rangle + |1\rangle|e_1\rangle}{\sqrt{2}}$. For

$$|0\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle + |-\rangle\right),\ |1\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle - |-\rangle\right), \tag{35}$$

we obtain

$$V|+\rangle|e\rangle = \frac{1}{2}\left[|+\rangle\left(|e_0\rangle + |e_1\rangle\right) + |-\rangle\left(|e_0\rangle - |e_1\rangle\right)\right]. \tag{36}$$

If the interaction also introduces no error in the $X$ basis, the coefficient of $|-\rangle$ must vanish. Hence, $|e_0\rangle = |e_1\rangle \equiv |e'\rangle$. Consequently,

$$V|0\rangle|e\rangle = |0\rangle|e'\rangle,\ V|1\rangle|e\rangle = |1\rangle|e'\rangle. \tag{37}$$

For an arbitrary input state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, it follows that

$$V|\psi\rangle|e\rangle = |\psi\rangle|e'\rangle. \tag{38}$$

Therefore, the state of the attacker's ancillary system is independent of the input state, and Eve cannot obtain any information without introducing detectable errors.

**Intercept-Measure-Resend Attack:** Assume that an external attacker, Eve, intercepts particles transmitted to the user or the signer. Eve measures each intercepted particle and, according to the measurement outcome, prepares a new particle and sends it to the legitimate participant. Eve randomly selects either the $Z$ basis or the $X$ basis for measurement.

The channel-security test requires the insertion of decoy states. For a single decoy particle, the probability of detecting Eve is $p_{\text{det}} = \frac{1}{4}$, whereas the probability that Eve escapes detection is $p_{\text{und}} = \frac{3}{4}$. When $d$ decoy particles are used, the probability that Eve is detected is

$$P_{\text{det}}(d) = 1 - \left(\frac{3}{4}\right)^d. \tag{39}$$

If Eve attacks each transmitted particle independently with probability $\eta$, then the probability that none of the $d$ decoy particles reveals the attack is

$$P_{\text{und}}(d,\eta) = \left(1 - \frac{\eta}{4}\right)^d. \tag{40}$$

Accordingly, the overall detection probability is

$$P_{\text{det}}(d,\eta)=1-\left(1-\frac{\eta}{4}\right)^{d}. \tag{41}$$

Therefore, the detection probability increases with both the attack ratio $\eta$ and the number of decoy particles $d$.

### 4.6. Communication Resource Analysis

In terms of communication resource overhead, let $n$ denote the length of the private message, and let $q_D$ and $q_A$ denote the lengths of the direct verification evidence and arbitration evidence, respectively. During one complete execution of the protocol, the blinded message $U \to S$, the direct verification evidence $S \to U$ and $U \to V$, the arbitration evidence $S \to A$, and the reference message $U \to V$ are transmitted through quantum teleportation. Therefore, the total number of logical qubits to be teleported is $Q = 2n + 2q_D + q_A$.

Since teleporting a $q$-qubit register requires $q$ fresh EPR pairs and $2q$ authenticated classical bits for Bell-measurement correction, the total number of consumed EPR pairs is $N_{\text{EPR}} = Q$, and the corresponding classical correction cost is $q_c^{\text{tele}} = 2(2n + 2q_D + q_A)$.

Let $d$ denote the number of decoy particles used for the quantum transmission, the total quantum and classical communication costs can be expressed as $q_t = 3(2n + 2q_D + q_A) + d + q_{\text{key}}$, and $q_c = 2(2n + 2q_D + q_A) + L$, respectively, where $q_{\text{key}}$ denotes the additional quantum resources required for key establishment, and $L$ includes the session identifier, authorization information, participant identities, and other authenticated classical control data. The comparison analysis with existing schemes is illustrated in Table 3.

Table 3. Comparison of functionality and resource overhead with related schemes.

| Scheme | Partial blindness | Teleportation | Arbitration | Designated verification | Temporal protection | Signature size $q_s$ | Quantum cost $q_t$ | Classical cost $q_c$ |
|---|---|---|---|---|---|---|---|---|
| Cai and Niu [24] | Yes | NR | No | No | No | NR | NR | NR |
| Zhong *et al.* [25] | Yes | No | No | No | No | NR | NR | NR |
| Xia *et al.* [45] | No | No | NR | No | No | $n$ | $27n$ | $2n$ |
| Tan and Ye [46] | No | Yes | No | No | No | $2n$ | $30n$ | $l+4n$ |
| **Proposed scheme** | **Yes** | **Yes** | **Yes** | **Yes** | **Yes** | $q_D + q_A$ | $3(2n + 2q_D + q_A) + d + q_{\text{key}}$ | $2(2n + 2q_D + q_A) + L$ |

*Note*: NR denotes that the corresponding quantity is not reported or is not directly comparable under a unified resource-counting convention.

## 5. Conclusions

This paper proposes an identity-based quantum partially blind signature scheme based on quantum teleportation. With the aid of a random bit string of length $n$, the user encodes binary information into a quantum state, blinds it according to the blinding key $r$, and keeps the public information $info$ openly visible, thereby achieving the partially blind signature property.

The PKG is responsible for participant identity authentication, session establishment, blind-key freezing, signature authorization, and one-time session-key distribution, and implements key lifecycle management through a unique session identifier, validity period, and state records. Signers generate direct verification evidence for a designated verifier and independent arbitration evidence for an arbitrator, respectively; the relevant quantum information is transmitted via security-verified EPR entanglement resources and quantum teleportation.

Verifiers perform routine verification through quantum authentication decoding, tag verification, and message de-blinding; in the event of a dispute, the arbitrator renders a decision based on the quantum evidence independently preserved during the signing phase. Security analysis shows that, under conditions such as a trusted PKG and arbitrator, secure classical communication channels, an ideal random source, one-time session keys, and secure quantum authentication codes, this scheme can achieve security properties including correctness, partial blindness, forgery resistance, and non-repudiation, while also providing resistance to third-party attacks.

However, its security is based on information-theoretic security under explicit attack models and trust assumptions; at the same time, quantum labels, authentication-assisting qubits, and two-branch evidence also entail certain quantum resource and storage overheads.

## Acknowledgements

We express our gratitude to all contributors who engaged in the discussion of this work. This work was supported by the Hunan Provincial Natural Science Foundation of China (GrantNos.2025JJ70445), the Joint Open Fund Project of "Hunan Provincial Science and Technology Innovation Team, Hunan Provincial Key Laboratory and Provincial Characteristic Discipline of Control Science and Engineering" (Grant NO.ZNKZN2024-4).

## Author Contributions

Conceptualization, Juxiu Zhong and Rongbo Lu; methodology, Juxiu Zhong; validation, Juxiu Zhong, Rongbo Lu and Wei Li; writing-original draft preparation, Juxiu Zhong; writing-review and editing, Rongbo Lu and Wei Li. All authors have read and agreed to the published version of the manuscript.

## Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

## References


[1] Diffie, W. and Hellman, M.E. (1976) New Directions in Cryptography. *IEEE Transactions on Information Theory*, **22**, 644-654. https://doi.org/10.1109/tit.1976.1055638

[2] Rivest, R.L., Shamir, A. and Adleman, L. (1978) A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, **21**, 120-126. https://doi.org/10.1145/359340.359342

[3] Elgamal, T. (1985) A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, **31**, 469-472. https://doi.org/10.1109/tit.1985.1057074

[4] Goldwasser, S., Micali, S. and Rivest, R.L. (1988) A Digital Signature Scheme Secure against Adaptive Chosen-Message Attacks. *SIAM Journal on Computing*, **17**, 281-308. https://doi.org/10.1137/0217017

[5] Schnorr, C.P. (1991) Efficient Signature Generation by Smart Cards. *Journal of Cryptology*, **4**, 161-174. https://doi.org/10.1007/bf00196725

[6] Boneh, D., Lynn, B. and Shacham, H. (2004) Short Signatures from the Weil Pairing. *Journal of Cryptology*, **17**, 297-319. https://doi.org/10.1007/s00145-004-0314-9

[7] Shor, P.W. (1997) Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, **26**, 1484-1509. https://doi.org/10.1137/s0097539795293172

[8] Thomas, M., Mathews, M.M., Panchami, V., *et al*. (2026) Securing the Future: A Comprehensive Review of Post-Quantum Digital Signatures. *Computer Science Review*, **61**, Article 100935. https://doi.org/10.1016/j.cosrev.2026.100935

[9] Shor, P.W. (1994) Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Proceedings of the* 35*th Annual Symposium on Foundations of Computer Science*, Santa Fe, 20-22 November 1994, 124-134. https://doi.org/10.1109/sfcs.1994.365700

[10] Gottesman, D. and Chuang, I.L. (2001) Quantum Digital Signatures. arXiv:quant-ph/0105032. https://arxiv.org/abs/quant-ph/0105032

[11] Chaum, D. (1983) Blind Signatures for Untraceable Payments. In: *Advances in Cryptology*, Springer US, 199-203. https://doi.org/10.1007/978-1-4757-0602-4_18

[12] Li, Q., Chan, W.H. and Long, D.Y. (2021) Quantum Blind Signature: Principles, Advances and Challenges. *Physics Reports*, **924**, 1-47.

[13] Wen, X., Niu, X., Ji, L. and Tian, Y. (2009) A Weak Blind Signature Scheme Based on Quantum Cryptography. *Optics Communications*, **282**, 666-669. https://doi.org/10.1016/j.optcom.2008.10.025

[14] Wang, T.Y. and Wen, Q.Y. (2010) Fair Quantum Blind Signatures. *Chinese Physics B*, **19**, Article 060307. https://doi.org/10.1088/1674-1056/19/6/060307

[15] Su, Q., Huang, Z., Wen, Q.Y. and Li, W.M. (2010) Quantum Blind Signature Based on Two-State Vector Formalism. *Optics Communications*, **283**, 4408-4410. https://doi.org/10.1016/j.optcom.2010.06.061

[16] Xu, R., Huang, L., Yang, W. and He, L. (2011) Quantum Group Blind Signature Scheme without Entanglement. *Optics Communications*, **284**, 3654-3658. https://doi.org/10.1016/j.optcom.2011.03.083

[17] Chen, F.L., Wang, Z.H. and Hu, Y.M. (2019) A New Quantum Blind Signature Scheme with BB84-State. *Entropy*, **21**, Article 336. https://doi.org/10.3390/e21040336

[18] Luo, Q., Zhang, T., Huang, X. and Jing, N. (2022) Two Quantum Proxy Blind Signa-

ture Schemes Based on Controlled Quantum Teleportation. *Entropy*, **24**, Article 1421. https://doi.org/10.3390/e24101421

[19] Gupta, A., Chandra, G.V., Das, N. and Paul, G. (2024) An Efficient and Secure Quantum Blind Signature-Based Electronic Cash Transaction Scheme. *IET Quantum Communication*, **5**, 619-631. https://doi.org/10.1049/qtc2.12109

[20] Wang, F., Yu, Y., Wei, Z., Zhao, T. and Wang, J. (2025) Quantum Blind Signature Protocol Based on Single Qubit Rotation. *Optics Communications*, **583**, Article 131629. https://doi.org/10.1016/j.optcom.2025.131629

[21] Zhang, J.H., Wang, H., Xiao, W.E. and Huang, X. (2026) Cryptanalysis of the Quantum Blind Signature Scheme for Supply Chain Finance and Its Improvement. *Advanced Quantum Technologies*, **9**, e00785. https://doi.org/10.1002/qute.202500785

[22] Abe, M. and Fujisaki, E. (1996) How to Date Blind Signatures. In: *Lecture Notes in Computer Science*, Springer, 244-251. https://doi.org/10.1007/bfb0034851

[23] Abe, M. and Okamoto, T. (2000) Provably Secure Partially Blind Signatures. In: *Lecture Notes in Computer Science*, Springer, 271-286. https://doi.org/10.1007/3-540-44598-6_17

[24] Cai, X.Q. and Niu, H.F. (2012) Partially Blind Signatures Based on Quantum Cryptography. *International Journal of Modern Physics B*, **26**, Article 1250163. https://doi.org/10.1142/s0217979212501639

[25] Zhong, J., Liao, B., Shi, Y. and Lu, R. (2022) A Quantum Partially Blind Signature Scheme without Entanglement. *International Journal of Modern Physics B*, **36**, Article 2250128. https://doi.org/10.1142/s0217979222501284

[26] Katsumata, S., Lai, Y., LeGrow, J.T. and Qin, L. (2024) CSI-Otter: Isogeny-Based (Partially) Blind Signatures from the Class Group Action with a Twist. *Designs, Codes and Cryptography*, **92**, 3587-3643. https://doi.org/10.1007/s10623-024-01441-7

[27] Kuchta, V., LeGrow, J.T. and Persichetti, E. (2026) Post-Quantum (Partially) Blind Signatures from Matrix Code Equivalence. *Cryptography and Communications*. https://doi.org/10.1007/s12095-026-00879-x

[28] Jia, X., He, D., Zeadally, S. and Li, L. (2017) Efficient Revocable Id-Based Signature with Cloud Revocation Server. *IEEE Access*, **5**, 2945-2954. https://doi.org/10.1109/access.2017.2676021

[29] Shamir, A. (1985) Identity-Based Cryptosystems and Signature Schemes. In: *Lecture Notes in Computer Science*, Springer, 47-53. https://doi.org/10.1007/3-540-39568-7_5

[30] Chen, F.L., Liu, W.F., Chen, S.G. and Wang, Z.H. (2018) Public-Key Quantum Digital Signature Scheme with One-Time Pad Private-Key. *Quantum Information Processing*, **17**, Article No. 10. https://doi.org/10.1007/s11128-017-1778-5

[31] Xin, X., Wang, Z. and Yang, Q. (2020) Identity-Based Quantum Signature Based on Bell States. *Optik*, **200**, Article 163388. https://doi.org/10.1016/j.ijleo.2019.163388

[32] Xin, X., Wang, Z., Yang, Q. and Li, F. (2020) Efficient Identity-Based Public-Key Quantum Signature Scheme. *International Journal of Modern Physics B*, **34**, Article 2050087. https://doi.org/10.1142/s0217979220500873

[33] Huang, Y., Xu, G. and Song, X. (2023) An Improved Efficient Identity-Based Quantum Signature Scheme. *Quantum Information Processing*, **22**, Article No. 36. https://doi.org/10.1007/s11128-022-03786-1

[34] Prajapat, S., Kumar, P., Kumar, S., Das, A.K., Shetty, S. and Hossain, M.S. (2024)

Designing High-Performance Identity-Based Quantum Signature Protocol with Strong Security. *IEEE Access*, **12**, 14647-14658. https://doi.org/10.1109/access.2024.3355196

[35] Liu, B., Zhu, P. and Guo, K. (2024) A Secure and Efficient Identity-Based Quantum Signature Scheme. *AIP Advances*, **14**, Article 065020. https://doi.org/10.1063/5.0212258

[36] Mohanty, T., Srivastava, V., Debnath, S.K., Roy, D., Sakurai, K. and Mukhopadhyay, S. (2025) An Experimentally Validated Feasible Quantum Protocol for Identity-Based Signature. *Sādhanā*, **50**, 23. https://doi.org/10.1007/s12046-025-02676-3

[37] Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A. and Wootters, W.K. (1993) Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. *Physical Review Letters*, **70**, 1895-1899. https://doi.org/10.1103/physrevlett.70.1895

[38] Zeng, G.H. and Keitel, C.H. (2002) Arbitrated Quantum-Signature Scheme. *Physical Review A*, **65**, Article 042312. https://doi.org/10.1103/physreva.65.042312

[39] Wen, X.J., Liu, Y. and Sun, Y. (2007) Quantum Multi-Signature Protocol Based on Teleportation. *Zeitschrift für Naturforschung A*, **62**, 147-151. https://doi.org/10.1515/zna-2007-3-405

[40] Zuo, H.J., Zhang, K.J. and Song, T.T. (2013) Security Analysis of Quantum Multi-Signature Protocol Based on Teleportation. *Quantum Information Processing*, **12**, 2343-2353. https://doi.org/10.1007/s11128-013-0524-x

[41] Feng, Y., Shi, R., Shi, J., Zhou, J. and Guo, Y. (2019) Arbitrated Quantum Signature Scheme with Quantum Walk-Based Teleportation. *Quantum Information Processing*, **18**, Article No. 154. https://doi.org/10.1007/s11128-019-2270-1

[42] Lu, D., Li, Z., Yu, J. and Han, Z. (2022) A Verifiable Arbitrated Quantum Signature Scheme Based on Controlled Quantum Teleportation. *Entropy*, **24**, Article 111. https://doi.org/10.3390/e24010111

[43] Singh, S., Rajput, N.K., Rathi, V.K., Pandey, H.M., Jaiswal, A.K. and Tiwari, P. (2023) Securing Blockchain Transactions Using Quantum Teleportation and Quantum Digital Signature. *Neural Processing Letters*, **55**, 3827-3842. https://doi.org/10.1007/s11063-020-10272-1

[44] Zhao, W., Wang, F.Q., Mao, Y.Y., Zhong, H., *et al*. (2023) Teleportation-Based Continuous-Variable Quantum Digital Signature. *Results in Physics*, **53**, Article 107018. https://doi.org/10.1016/j.rinp.2023.107018

[45] Xia, C., Li, H. and Hu, J. (2021) A Semi-Quantum Blind Signature Protocol Based on Five-Particle GHZ State. *The European Physical Journal Plus*, **136**, Article No. 633. https://doi.org/10.1140/epjp/s13360-021-01605-7

[46] Tan, X. and Ye, T.Y. (2024) Semiquantum Proxy Blind Signature Based on Quantum Teleportation. *Scientia Sinica Physica, Mechanica & Astronomica*, **54**, Article 230313. https://doi.org/10.1360/sspma-2023-0426