Lin et al. *EPJ Quantum Technology* ( 2026) 13:50
https://doi.org/10.1140/epjqt/s40507-026-00497-9

EPJ.org

EPJ Quantum Technology

RESEARCH Open Access

# An arbitrated quantum signature scheme for classical information using entanglement swapping

Jason Lin[1], Mei-Yen Yen[1], Chia-Wei Tsai[2] and Chun-Wei Yang[3]

*Correspondence:
cwyang@mail.cmu.edu.tw
[3]Master Program for Digital Health Innovation, College of Humanities and Sciences, China Medical University, No. 100, Sec. 1, Jingmao Rd., Beitun Dist., Taichung 406040, Taiwan
Full list of author information is available at the end of the article

**Abstract**

Quantum signature protocols often rely on quantum states to carry signature information directly. However, they need SWAP tests, which require numerous copies to ensure accuracy and security, resulting in high implementation costs. This study proposes an arbitrated quantum signature protocol that incorporates classical information with entanglement swapping. Quantum states are converted into classical information immediately after measurement. The protocol does not rely on SWAP tests, avoids long-term storage of quantum signatures, and employs exclusive-OR operations and hash functions to process signature data. By leveraging a third-party arbitrator, it enables reliable identity verification of the signer and verifier, thereby guaranteeing unforgeability and nonrepudiation.

**Keywords:** Quantum signature; Entanglement swapping; Hash function; Classical information

## 1 Introduction

With the rapid expansion of online services and digital transactions, individuals and organizations increasingly rely on network systems for communication, data exchange, and daily operations. As a result, the demand for robust information security continues to grow, particularly with respect to ensuring data integrity, authenticating identities, and preventing unauthorized tampering. Digital signatures have thus emerged as a fundamental tool in modern cryptographic infrastructures, providing essential guarantees of authenticity, integrity, and non-repudiation.

The concept of digital signatures was first introduced by Diffie and Hellman in 1976 [1]. Classical signature schemes rely on computational hardness assumptions, such as integer factorization in RSA [2] and the discrete logarithm problem in ElGamal [3]. However, the advance of quantum computing poses substantial threats to these schemes. Shor's algorithm [4] can efficiently factor large integers and compute discrete logarithms, threatening the security assumptions of most public-key cryptosystems. Similarly, signature mechanisms based on symmetric-key primitives face vulnerabilities, as Grover's algorithm [5] can quadratically accelerate brute-force key search. Consequently, quantum signature pro-



Springer

tocols have been proposed to achieve unconditional security by exploiting quantum mechanical principles. In this context, a wide range of quantum signature models have been studied, including arbitrated, proxy, blind, and group-based schemes.

In an arbitrated setting, signature schemes are expected to satisfy four fundamental properties: integrity, unforgeability, non-repudiation, and verifiability. Integrity ensures that messages remain unaltered. Unforgeability guarantees that only the signer can generate valid signatures. Non-repudiation prevents both the signer and the verifier from denying their actions. Verifiability enables the receiver or arbitrator to validate a signature and resolve disputes. The earliest developments in this field trace back to the foundational quantum signature scheme of Gottesman and Chuang [6], which utilized quantum one-way functions and the SWAP test [7] to compare unknown quantum states. Building on this foundation, Zeng et al. [8] presented the first AQS protocol using Greenberger–Horne–Zeilinger (GHZ) state and quantum one-time encryption. Li et al. [9] later replaced GHZ states with Bell states to improve practical feasibility, while Zou and Qiu [10] subsequently proposed an entanglement-free AQS construction.

However, Gao et al. [11] highlighted in 2011 that the commutativity of Pauli operators could lead to forgery attacks when photons are independently encrypted with a quantum one-time pad, affecting schemes such as those by Li et al. [9] and Zou and Qiu [10]. To remedy this issue, Li et al. [12] introduced a correlated-qubit CNOT-chain AQS to strengthen security and achieve 100% efficiency, though Luo and Hwang [13] demonstrated that such designs remained forgeable. Zhang et al. [14] later proposed an improved scheme that enhanced forgery resistance by incorporating key-controlled chained CNOT operations. More recent AQS constructions include GHZ-based teleportation signatures [15], GHZ states combined with exclusive-OR (XOR) operations [16], and a chained quantum sequence using key-controlled Pauli and Hadamard operations under a semi-trusted arbitrator [17]. In 2023, Zhang et al. [18] further proposed encoding hash outputs into Bell states and verifying signatures through three-party particle exchange. In addition, the trend toward simplifying physical implementation has become increasingly evident. For example, Zhang et al. [19] proposed a provably secure AQS without entanglement, grounded in key-controlled quantum hash functions and offering formal security against chosen-message attacks. Similarly, Pang and Xiang [20] presented an entanglement-free AQS using the B92 protocol [21], emphasizing the role of trusted classical channels as a design premise. These recent advances highlight both the evolution of AQS security models and the ongoing shift toward protocols requiring fewer quantum resources.

To broaden applicability, several studies have explored extended forms of quantum signatures. For instance, semi-quantum signature protocols [22–25] reduce the requirements of quantum operations on certain participants, enabling more practical implementations. Some other works have examined varying degrees of trust assumptions for the arbitrator [26–28], aiming to reduce reliance on the third party. In addition, specialized quantum signature primitives, such as blind signatures [24, 29, 30], group signatures [31, 32], ring signatures [25, 33–36], and designated-verifier signatures [37–40], have been developed to achieve richer functionality.

Despite these advances, most existing quantum signature schemes can be broadly categorized into two directions. On one hand, many entanglement-based schemes rely on quantum memories for long-term storage of signature states or on SWAP tests to compare unknown quantum states, both of which entail substantial implementation costs and ex-

perimental complexity. On the other hand, several entanglement-free approaches, including those built upon QKD-derived keys, have demonstrated efficient signing mechanisms without requiring entangled states. While these schemes reduce quantum resource consumption, they often depend on chained single-photon operations or multi-round quantum transmissions, which introduce their own practical constraints and potential error propagation issues.

These observations indicate that different design paradigms involve different trade-offs between quantum resource requirements, structural robustness, and implementation feasibility. In particular, reducing dependence on long-term quantum storage and state-comparison operations remains an important objective in entanglement-assisted frameworks. Motivated by this perspective, this study proposes an AQS protocol in which quantum signatures are immediately measured and transformed into classical information for storage and verification. By avoiding SWAP tests, eliminating long-term quantum memory, and processing signature information through classical post-measurement operations, the proposed scheme aims to achieve a balanced design that integrates the structural advantages of entanglement with improved practical feasibility.

The remainder of this paper is organized as follows: Sect. 2 describes the proposed protocol, which is divided into three phases: initialization, signing, and verification. Section 3 presents a comprehensive security analysis. Section 4 compares the proposed protocol with existing schemes in terms of functionality and performance. Section 5 concludes the study by summarizing the main contributions.

## 2 Proposed AQS protocol

The protocol involves three participants: a signer Alice, a verifier Bob, and an arbitrator who is defined as an honest third-party TP that performs its operations faithfully according to the protocol without engaging in malicious behavior. The workflow is organized into three phases: Sect. 2.1 introduces the properties of entanglement swapping that enable security, Sect. 2.2 describes the generation of the signature, and Sect. 2.3 explains how the verifier and TP jointly verify both the signer's identity and correctness of the signature.

### 2.1 Properties of entanglement swapping

This study exploits the property of entanglement swapping to conceal partial key information. Entanglement swapping is a process that allows two quantum systems that are not initially entangled to become entangled through suitable measurements.

When one photon from each of two independent Einstein–Podolsky–Rosen (EPR) pairs [41] is jointly measured, the other two photons, which were originally uncorrelated, become entangled and collapse into a new Bell state, as shown in Fig. 1. Let the initial Bell state of the first EPR pair be denoted as $Initial_1$, consisting of photons $IS_1^{(1)}$ and $IS_1^{(2)}$. Similarly, let the initial Bell state of the second EPR pair be denoted as $Initial_2$, consisting of photons $IS_2^{(1)}$ and $IS_2^{(2)}$. After performing a Bell measurement on photons $IS_1^{(1)}$ and $IS_2^{(1)}$, the measurement result is denoted as $MR_1$. The remaining photons $IS_1^{(2)}$ and $IS_2^{(2)}$ become entangled and collapse into another Bell state, denoted as $MR_2$.

Table 1 summarizes the correspondence between the initial Bell states and the resulting states obtained after entanglement swapping. As shown in Table 2, each Bell state can be represented by two classical bits. Let $Initial_1^{(c)}$ and $Initial_2^{(c)}$ denote the classical-bit representations of the two initial Bell states, and let $MR_1^{(c)}$ and $MR_2^{(c)}$ denote the classical-bit

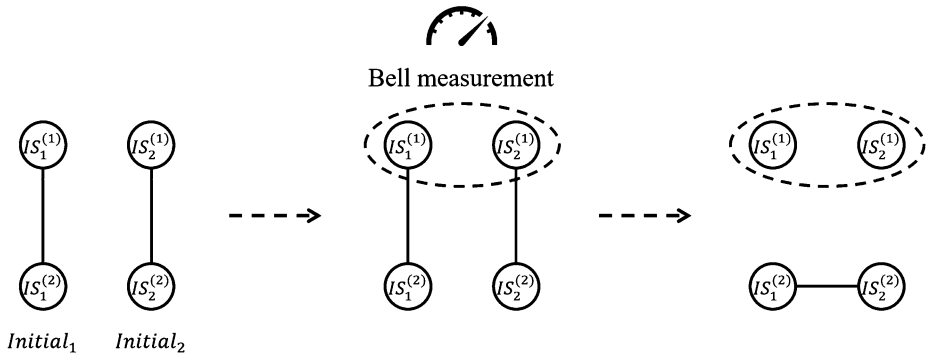


**Figure 1** Entanglement swapping of two EPR pairs

**Table 1** Correspondence between initial Bell states and measurement outcomes in entanglement swapping

| $Initial_1 \bigotimes Initial_2$ | $MR_1 \bigotimes MR_2$ | $Initial_1 \bigotimes Initial_2$ | $MR_1 \bigotimes MR_2$ |
|---|---|---|---|
| $\|\phi^+\rangle \bigotimes \|\phi^+\rangle$ | $\|\phi^+\rangle \bigotimes \|\phi^+\rangle$ | $\|\phi^+\rangle \bigotimes \|\phi^-\rangle$ | $\|\phi^+\rangle \bigotimes \|\phi^-\rangle$ |
| $\|\phi^-\rangle \bigotimes \|\phi^-\rangle$ | $\|\phi^-\rangle \bigotimes \|\phi^-\rangle$ | $\|\phi^-\rangle \bigotimes \|\phi^+\rangle$ | $\|\phi^-\rangle \bigotimes \|\phi^+\rangle$ |
| $\|\psi^+\rangle \bigotimes \|\psi^+\rangle$ | $\|\psi^+\rangle \bigotimes \|\psi^+\rangle$ | $\|\psi^+\rangle \bigotimes \|\psi^-\rangle$ | $\|\psi^+\rangle \bigotimes \|\psi^-\rangle$ |
| $\|\psi^-\rangle \bigotimes \|\psi^-\rangle$ | $\|\psi^-\rangle \bigotimes \|\psi^-\rangle$ | $\|\psi^-\rangle \bigotimes \|\psi^+\rangle$ | $\|\psi^-\rangle \bigotimes \|\psi^+\rangle$ |
| $\|\phi^+\rangle \bigotimes \|\psi^+\rangle$ | $\|\phi^+\rangle \bigotimes \|\psi^+\rangle$ | $\|\phi^+\rangle \bigotimes \|\psi^-\rangle$ | $\|\phi^+\rangle \bigotimes \|\psi^-\rangle$ |
| $\|\psi^+\rangle \bigotimes \|\phi^+\rangle$ | $\|\psi^+\rangle \bigotimes \|\phi^+\rangle$ | $\|\psi^-\rangle \bigotimes \|\phi^+\rangle$ | $\|\psi^-\rangle \bigotimes \|\phi^+\rangle$ |
| $\|\phi^-\rangle \bigotimes \|\psi^-\rangle$ | $\|\phi^-\rangle \bigotimes \|\psi^-\rangle$ | $\|\phi^-\rangle \bigotimes \|\psi^+\rangle$ | $\|\phi^-\rangle \bigotimes \|\psi^+\rangle$ |
| $\|\psi^-\rangle \bigotimes \|\phi^-\rangle$ | $\|\psi^-\rangle \bigotimes \|\phi^-\rangle$ | $\|\psi^+\rangle \bigotimes \|\phi^-\rangle$ | $\|\psi^+\rangle \bigotimes \|\phi^-\rangle$ |

**Table 2** Mapping rules between classical bit pairs and Bell states

| Classical bits | Bell state |
|---|---|
| 00 | $\|\phi^+\rangle = (\|00\rangle + \|11\rangle)/\sqrt{2}$ |
| 01 | $\|\phi^-\rangle = (\|00\rangle - \|11\rangle)/\sqrt{2}$ |
| 10 | $\|\psi^+\rangle = (\|01\rangle + \|10\rangle)/\sqrt{2}$ |
| 11 | $\|\psi^-\rangle = (\|01\rangle - \|10\rangle)/\sqrt{2}$ |

representations of the two measurement results. These classical bits satisfy the following relation:

$$Initial_1^{(c)} \oplus Initial_2^{(c)} = MR_1^{(c)} \oplus MR_2^{(c)}. \tag{1}$$

Equation (1) preserves the two-bit structure of Bell states. Since each Bell state corresponds to one of the four possible two-bit combinations, the entanglement-swapping process maps every two initial Bell states to exactly one of the four Bell states in $MR_2$. This leads to the four-to-four correspondence shown in Table 1. For example, when both initial Bell states are $|\phi^+\rangle$, represented as 00 in Table 2, performing a Bell measurement on photons $IS_1^{(1)}$ and $IS_2^{(1)}$ may yield $MR_1$ equal to $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$, or $|\psi^-\rangle$. The remaining photons $IS_1^{(2)}$ and $IS_2^{(2)}$ then become entangled according to the value of $MR_1$, and the resulting state $MR_2$ is identical to $MR_1$. The detailed derivation of this example is provided

in Eq. (2).

$$
\begin{aligned}
&\left|\phi^{+}\right\rangle_{12} \otimes \left|\phi^{+}\right\rangle_{34} \\
&= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{12} \otimes \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{34} \\
&= \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\right)_{1234} \\
&= \frac{1}{2}\left(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle\right)_{1324} \\
&= \frac{1}{2}\left[\left(\left|\phi^{+}\right\rangle + \left|\phi^{-}\right\rangle\right)^{2} + \left(\left|\psi^{+}\right\rangle + \left|\psi^{-}\right\rangle\right)^{2} + \left(\left|\psi^{+}\right\rangle - \left|\psi^{-}\right\rangle\right)^{2} + \left(\left|\phi^{+}\right\rangle - \left|\phi^{-}\right\rangle\right)^{2}\right]_{1324} \\
&= \frac{1}{2}\left(\left|\phi^{+}\right\rangle \otimes \left|\phi^{+}\right\rangle + \left|\phi^{-}\right\rangle \otimes \left|\phi^{-}\right\rangle + \left|\psi^{+}\right\rangle \otimes \left|\psi^{+}\right\rangle + \left|\psi^{-}\right\rangle \otimes \left|\psi^{-}\right\rangle\right)_{1324}
\end{aligned} \tag{2}
$$

This study enables the signer and verifier to authenticate both the origin and content of a message with the assistance of TP by leveraging this property, even when they possess only partial information.

### 2.2 Initialization phase

This phase presents the prerequisites that must be satisfied before the signer initiates the signing process, as well as the information required by the arbitrator and verifier during the verification phase. The signer, Alice, and the verifier, Bob, must first complete a registration process with a trusted authority, hereafter referred to as TP, to obtain their respective public identification numbers, denoted as $id_A$ and $id_B$. Upon completion of the registration, TP establishes a shared secret key with both Alice and Bob to support subsequent identity authentication. Shared keys can be generated using a proven secure quantum key distribution protocol such as BB84 [42]. The shared key between Alice and TP is denoted as $K_{AT}$, whereas the key between Bob and TP is denoted as $K_{BT}$. The length of each key was set to $n$, where $n$ is an even integer. Let $H : \{0,\ 1\}^* \rightarrow \{0,\ 1\}^n$ be a one-way hash function that accepts an arbitrary-length classical bit string as input and outputs a fixed-length hash value of $n$ bits, where $n$ matches the key length. Additionally, this study defines another hash function $H^+ : \{0,\ 1\}^* \rightarrow \{0,\ 1\}^n$, which serves a different purpose from $H$. The hash function $H^+$ is used during the final verification phase, in which TP applies it to the data submitted by Bob to produce an auxiliary authentication token.

### 2.3 Signing phase

In the signing phase, Alice informs both TP and Bob of the message she intends to sign. Based on the message and her shared key $K_{AT}$ with TP, she generates a sequence of corresponding Bell states. After verifying that the message raises no security concerns, Bob uses his shared key $K_{BT}$ with TP to generate his own sequence of Bell states. The two parties then exchange the selected photons and perform the Bell measurements. Afterward, Alice produces a signature based on the measurement results. An overview of the signing process is shown in Fig. 2. The following provides the step-by-step procedure for the signing phase.

Step 1: Alice first concatenates the document $doc$, $id_A$, and $id_B$ to form the message string $M = doc \parallel id_A \parallel id_B$, where $M \in \{0,1\}^*$. Alice then inputs $M$ into the hash function $H$ to compute the corresponding hash value $h_M = H(M)$ and performs an

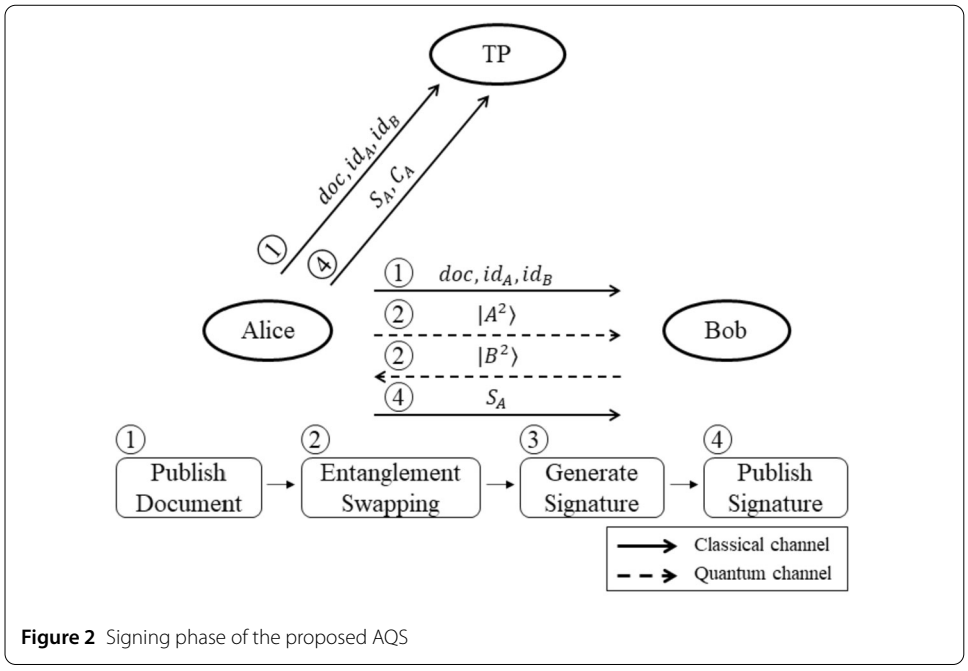


**Figure 2** Signing phase of the proposed AQS

XOR operation between $h_M$ and the shared key $K_{AT}$ with TP to obtain the encrypted hash value $C_M = h_M \oplus K_{AT}$.

Step 2: Subsequently, Alice transmits the values of $doc$, $id_A$, and $id_B$ to Bob and TP through an authenticated classical channel.

Step 3: Alice divides $C_M$ into groups of two bits and converts each pair into a Bell state according to the encoding rules defined in Table 2. As a result, she generates a sequence of EPR pairs $A = \left\{\left(A_i^1, A_i^2\right) \mid i \in \{1, 2, \ldots, \lceil n/2 \rceil\}\right\}$, where $A_i^1$ and $A_i^2$ represent the two particles of the $i$-th EPR pair. Similarly, Bob uses his shared key $K_{BT}$ with TP to generate his own sequence of EPR pairs $B = \left\{\left(B_i^1, B_i^2\right) \mid i \in \{1, 2, \ldots, \lceil n/2 \rceil\}\right\}$, where $B_i^1$ and $B_i^2$ are the two particles of each EPR pair. Alice retains each $A_i^1$ and sends $A_i^2$ to Bob, whereas Bob retains $B_i^1$ and sends $B_i^2$ to Alice. Alice performs Bell measurements on each pair $\left(A_i^1, B_i^2\right)$, and according to the correspondence in Table 2, converts the measurement results into an $n$-bit string $MR_A$. Similarly, Bob performs Bell measurements on pairs $\left(B_i^1, A_i^2\right)$ and obtains another $n$-bit string $MR_B$.

Step 4: Alice computes the signature sequence $S_A = MR_A \oplus K_{AT}$. She then computes the encrypted hash value $C_A = H(MR_A \parallel K_{AT}) \oplus MR_A$. Afterwards, Alice publishes $S_A$ and $C_A$ through an authenticated classical channel.

After the signing phase, Alice and Bob obtain their measurement results $MR_A$ and $MR_B$, respectively. Since neither of them can access each other's outcome, these results remain private information and can serve as evidence of whether the operations were properly conducted or whether malicious modifications occurred. The signature $S_A$ is generated from $MR_A$ together with the shared key $K_{AT}$, which is held exclusively by Alice and TP. Consequently, in the subsequent verification phase, only TP is capable of reconstructing $MR_A$ from $K_{AT}$, thereby confirming the authenticity and correctness of the signature.

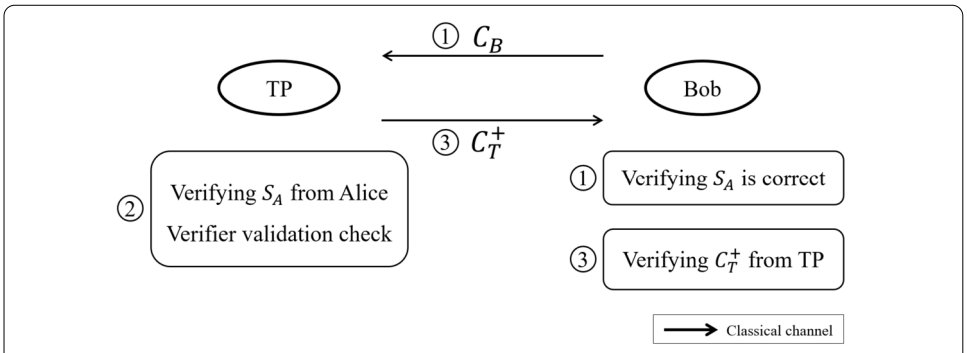


**Figure 3** Verification phase of the proposed protocol

## 2.4 Verification phase

In the verification phase, Bob and TP verify the authenticity of the signature to ensure that the message is indeed generated by the signer Alice, and that both the signer and verifier have completed the required operations, as shown in Fig. 3. The following presents the step-by-step procedure for the verification phase.

Step 1: Bob reconstructs the message $M'$ by concatenating Alice's publicly announced information, including the document $doc$, $id_A$, and $id_B$ (i.e., $M' = doc \parallel id_A \parallel id_B$). He then computes the hash value $h'_M = H\left(M'\right)$, followed by the computation of $R_A = h'_M \oplus S_A$. If the result $R_A$ is equal to $R_B = K_{BT} \oplus MR_B$, Bob proceeds to compute $C_B = H(MR_B \parallel K_{BT}) \oplus MR_B$ and transmits $C_B$ to TP. If the results do not match, Bob rejects the signature.

Step 2: TP performs the following verification steps based on the information disclosed by Alice and Bob. First, TP verifies whether the signature $S_A$ was indeed generated by Alice. It computes $MR'_A = S_A \oplus K_{AT}$. TP then inputs $MR'_A$ into the hash function to obtain $H(MR'_A \parallel K_{AT})$ and further computes the result $C'_A = H(MR'_A \parallel K_{AT}) \oplus MR'_A$. The value of $C'_A$ is compared with the publicly announced $C_A = H(MR_A \parallel K_{AT}) \oplus MR_A$. If they match, TP confirms that Alice generated the signature and proceeds to the next step. Otherwise, the signature is rejected. Next, TP verifies whether Bob has correctly performed the verification process. TP reconstructs the message $M''$ by concatenating the public elements: $M'' = doc \parallel id_A \parallel id_B$. TP then computes Bob's expected measurement result as $MR'_B = H\left(M''\right) \oplus S_A \oplus K_{BT}$. After that, TP calculates $C'_B = H(MR'_B \parallel K_{BT}) \oplus MR'_B$. TP compares $C'_B$ with the value $C_B$ received from Bob. If they do not match, the signature is rejected. If they match, TP records the tuple ($doc$, $id_A$, $id_B$, $S_A$, $MR_A$, $MR_B$). Finally, TP computes an additional authentication tag: $C_T^+ = H^+(\left(H\left(M''\right) \oplus S_A \oplus K_{BT}\right) \parallel K_{BT}) \oplus MR'_B$. This value is returned to Bob for final verification.

Step 3: Bob computes $C_B^+ = H^+(MR_B \parallel K_{BT}) \oplus MR_B$ and compares $C_T^+$ with $C_B^+$. If the values do not match, then Bob rejects the signature. If they match, Bob accepts the signature and stores both $S_A$ and $MR_B$ for potential dispute resolution.

During the signing phase, Alice and Bob obtain their respective measurement results. $MR_A$ and $MR_B$. Alice computes the signature $S_A = MR_A \oplus K_{AT}$, using her measurement result and secret key $K_{AT}$, and then publishes $S_A$. According to the property of entanglement swapping, the following relation holds between the parties: $K_{AT} \oplus H(M) \oplus K_{BT} =$

$MR_A \oplus MR_B$, where $H(M)$ is public information, while $K_{AT}$, $K_{BT}$, $MR_A$, and $MR_B$ remain private. Since Bob holds both $K_{BT}$ and $MR_B$, he can compute $K_{BT} \oplus MR_B \oplus H(M)$, which yields $S_A = MR_A \oplus K_{AT}$. By comparing this signature with Alice's published signature, Bob can verify the validity of $S_A$. Subsequently, Alice and Bob applied a one-way hash function to their measurement results and transmitted the outputs to TP for further verification. TP first recovers Alice's measurement result via $MR'_A = S_A \oplus K_{AT}$, and then computes $C'_A = H\left(MR'_A \parallel K_{AT}\right) \oplus MR'_A$ which is compared with Alice's announced value $C_A = H(MR_A \parallel K_{AT}) \oplus MR_A$ to confirm that the signature was indeed generated by Alice. Next, TP derives Bob's measurement result from the public information and the signature as $MR'_B = S_A \oplus H(M) \oplus K_{BT}$, and verifies whether its corresponding hash value matches Bob's transmitted $C_B = H(MR_B \parallel K_{BT}) \oplus MR_B$. Since $MR_B$ can only be obtained by Bob through actual protocol execution, successful verification confirms that both Alice and Bob have honestly participated and performed the required operations, thereby ensuring the authenticity and integrity of the signature. Once the above verification is complete and TP validates the signature, TP further computes an additional hash value $C_T^+ = H^+((H\left(M''\right) \oplus S_A \oplus K_{BT}\right) \parallel K_{BT}) \oplus MR'_B$, and sends it to Bob. Upon receiving $C_T^+$, Bob compares it to the locally computed result $C_B^+$ from $MR_B$. If the values of $C_T^+$ and $C_B^+$ coincide, the signature is considered valid. At this point, Bob retains both $S_A$ and $MR_B$ as evidence in the case of future disputes, which can be resolved through arbitration by TP. Since only TP possesses both $K_{AT}$ and $K_{BT}$, and only Alice and Bob hold $MR_A$ and $MR_B$ respectively, TP is the sole party capable of computing $MR'_A$ and $MR'_B$. Therefore, TP issues $C_T^+$ to Bob only after confirming Alice's measurement result $MR_A$, ensuring the correctness of the final confirmation step.

## 3 Security analysis

This section analyzes the security of the proposed protocol. The analysis included three parts: the security of photon transmission, non-repudiation of signing and verification, and unforgeability of the signature. Section 3.1 discusses the security of the photon transmission. Section 3.1.1 examines whether an attacker can obtain the initial quantum state by intercepting photons, and Sect. 3.1.2 analyzes whether Trojan-horse attacks can reveal operational information. Section 3.2 discusses non-repudiation, where Sect. 3.2.1 considers the possibility of Alice denying the signature and Sect. 3.2.2 considers the possibility of Bob denying the verification. Section 3.3 discusses unforgeability, where Sect. 3.3.1 addresses Bob forging a signature as an internal attacker and Sect. 3.3.2 addresses an external attacker forging Alice's signature.

### 3.1 Security of photon transmission

In this study, the quantum state exchange process involved numerous photon transmissions. The quantum states of these photons contain information related to the keys provided by Alice and Bob. To ensure the security of the transmission process, we first examine whether an attacker can obtain the original quantum states by intercepting the transmitted photons. Then, it analyzes whether an attacker can infer the receiver's operations through external interference or device behavior, which corresponds to a Trojan horse attack.

### *3.1.1 Intercepting photons to obtain the initial quantum state*

Unlike many quantum signature protocols that require explicit eavesdropping detection through decoy photons, the proposed AQS protocol does not rely on such mechanisms. This omission does not assume a trusted quantum channel. Instead, it follows from the fact that each transmitted photon is only one particle of an EPR pair, and any eavesdropper can access at most a single subsystem. Since Alice prepares one of the four Bell states $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$, and $|\psi^-\rangle$ with equal probability based on $H(M) \oplus K_{AT}$, the global two-photon system has the density matrix as follows.

$$\rho_{A_1A_2} = \frac{1}{4}(|\phi^+\rangle\langle\phi^+| + |\phi^-\rangle\langle\phi^-| + |\psi^+\rangle\langle\psi^+| + |\psi^-\rangle\langle\psi^-|) = \frac{I}{4} \tag{3}$$

When Eve intercepts the transmitted particle $A_2$, the reduced-density operator is obtained by tracing out $A_1$ from the global system, as shown in Eq. (4).

$$\rho_{A_2} = Tr_{A_1}\left(\rho_{A_1A_2}\right) = Tr_{A_1}\left(\frac{I}{4}\right) = \frac{I}{2} \tag{4}$$

This result indicates that the quantum information in subsystem $A_2$ is uniformly distributed. Therefore, an eavesdropper cannot extract useful information. Similarly, when Bob sends a particle of the Bell state to Alice, Eve cannot obtain meaningful information by observing that particle alone. Based on this property, Bob cannot extract Alice's private information by measuring the photon she sends and Alice cannot recover key-related information from Bob's photon $B_2$. If TP detects abnormal behavior, inconsistent data, or prolonged use of the same key, it assumes the presence of eavesdropping and notifies both parties to replace the key in order to maintain communication security.

### *3.1.2 Trojan-horse attacks*

There are two common types of Trojan-horse attacks. One is an invisible photon attack [43] and the other is a delay photon attack [44]. In an invisible-photon attack, an attacker injects photons with wavelengths that cannot be detected by the receiver into a quantum channel. These photons are intended to extract information regarding the operations performed by the receiver. A typical approach for defending against such attacks is to install wavelength filters at the receiver end. These filters block photons with unexpected wavelengths and prevent unauthorized access outside the protocol design. In a delayed photon attack, the attacker attaches a delayed photon close to a legitimately transmitted photon. After the operation is completed, the delayed photon is reflected and collected to infer the quantum logic applied by the receiver. A common countermeasure against this type of attack is the use of a photon-number splitter (PNS), which detects whether a single pulse contains more than one photon. This helps to identify and eliminate any additional photons that may have been inserted by the attacker.

A one-way photon transmission structure was used in the proposed protocol. Upon arrival, each photon was measured immediately using Bell measurement. There was no photon return or need for storage. Consequently, even if an attacker successfully injects a photon into a channel, the information carried by the photon cannot be retrieved. In addition, all quantum operations in the protocol are fixed and predetermined. Therefore, an attacker cannot gain any meaningful information through observation or inference.

In summary, although these two types of attacks may pose theoretical threats to certain protocols, they have no practical effect on their structures. Therefore, additional components such as wavelength filters or PNS devices are not required under the current protocol structure. The protocol can still achieve equivalent defense capability. This reduces the implementation cost and improves practical feasibility.

In addition to security against active attacks, it is worth noting that practical quantum channels are subject to photon loss and operational imperfections. In the proposed protocol, each transmitted particle corresponds to one half of a Bell pair. Photon loss therefore results in a failed Bell measurement rather than an incorrect signature acceptance. Such events can be treated as protocol aborts or retransmission cases and do not compromise the logical correctness or security properties of the scheme. Similarly, moderate operational noise may introduce mismatched measurement outcomes, which lead to verification failure instead of undetected forgery. Consequently, channel imperfections primarily influence implementation efficiency rather than structural security.

## 3.2 Non-repudiation

Nonrepudiation is an important property of arbitrary quantum signature schemes. This ensures that the signer cannot deny having signed the message and the verifier cannot deny having verified it. This section is divided into two parts that examine whether the signer can deny the act of signing and whether the verifier can deny the verification result. Once a message has been processed by the signing procedure, neither the signer nor the verifier can deny participation in the protocol.

### *3.2.1 Signer's repudiation*

After the signer publishes $S_A$, TP can recover the signer's measurement result $MR_A$ by computing $S_A \oplus K_{AT}$. In addition, the signer also publishes the value $H(MR_A \parallel K_{AT}) \oplus MR_A$. As long as $K_{AT}$ is not leaked, no one else can reconstruct $MR_A$. Therefore, only the signer can compute $H(MR_A \parallel K_{AT}) \oplus MR_A$, which proves that the signer is the only one who could have produced the signature. Consequently, the signer cannot deny signing a message.

### *3.2.2 Verifier's repudiation*

TP can compute the verifier's measurement result $MR'_B$ by checking whether $MR'_B$ is equal to $H\,(doc \parallel id_A \parallel id_B) \oplus S_A \oplus K_{BT}$, both the document $doc$ and the signature $S_A$ are public information, but only Bob, who actually performed the measurement, can compute $H(MR_B \parallel K_{BT}) \oplus MR_B$. Since TP holds $K_{BT}$, it can derive $MR'_B$ and compute the corresponding value $H(MR_B \parallel K_{BT}) \oplus MR'_B$. Therefore, the only party capable of producing the value $H(MR_B \parallel K_{BT}) \oplus MR_B$ is Bob. This confirms that Bob participated in the verification process and cannot repudiate his involvement.

## 3.3 Unforgeability

To prevent identity forgery, this study ensures that no entity without the correct key can generate a valid signature that passes the verification. This section is divided into two parts: Sect. 3.3.1 discusses whether the verifier can impersonate the signer and deceive TP by accepting a forged signature. Section 3.3.2 analyzes whether an external attacker, who is not involved in the protocol, can forge a signature under the signer's identity.

#### *3.3.1 Forgery by the verifier*

If the verifier attempts to impersonate the signer, it must possess key $K_{BT}$ and pass TP's verification process. In this case, the verifier may attempt to generate a forged signature $S_B$ and send it to TP for verification. TP will then compute $S_B \oplus K_{AT}$ to reconstruct the corresponding measurement result $MR'_A$ and verify it. However, from the perspective of the verifier, $K_{AT}$ is a completely unknown random variable. Each bit of the key is independent and has an equal probability of being either zero or one. Therefore, the uncertainty of $K_{AT}$ can be described using Shannon entropy [45] as follows:

$$\mathcal{H}(K_{AT}) = -\sum_i p\,(x_i) \log_2 p(x_i), \tag{5}$$

where $x_i \in \{0,1\}^n$. Since $K_{AT}$ is an $n$-bit string, and each possible combination is equally likely, we have $p\,(x_i) = \frac{1}{2^n}$, and the calculation of entropy becomes $\mathcal{H}(K_{AT}) = -\sum_i \frac{1}{2^n} \log_2 \frac{1}{2^n} = n$. This shows that the key has the maximum uncertainty. As a result, it is nearly impossible for the verifier to forge a valid signature that can pass TP's verification.

#### *3.3.2 Forgery by the external attacker*

As explained in Sect. 3.3.1, even the verifier who holds its own key $K_{BT}$ and measurement result $MR_B$ cannot forge the signer's identity because it cannot derive $K_{AT}$ or the signer's measurement result $MR_A$. An external attacker has access to even less information than a verifier, making it even more difficult to perform a successful forgery. Therefore, the protocol is secure against impersonation attacks from both internal and external attackers.

## 4 Performance comparison

In this section, we provide a quantitative comparison of representative AQS protocols by evaluating the quantum resources and operations required by each scheme, and by examining whether additional costs arise from defenses against Trojan-horse attacks or from the use of the SWAP test. The quantum resource in Table 3 refers to the states prepared at the beginning of the signing phase, whereas the subsequent transformations, including quantum gates and measurements, are counted as quantum operations. The analysis focuses on logical resource consumption and qubit utilization at the protocol level. Practical performance under specific experimental channel conditions depends on the underlying implementation and hardware configurations, and is therefore not explicitly modeled in this comparative study.

Many AQS protocols [9, 15, 16] employ the SWAP test to determine whether two unknown quantum states are identical. However, since the SWAP test is probabilistic, achieving high verification accuracy requires a significant amount of photon copies, which increases resource consumption. The proposed protocol avoids this issue by converting quantum signatures into classical bit strings for verification, thereby eliminating the need to generate multiple identical quantum states.

The qubit efficiency $\eta$ used in this work follows the definition in Zhang et al. [18], where $\eta = m/q$ with $m$ denoting the number of valid bits in the final signature and $q$ representing the number of consumed qubits (excluding decoy photons). To ensure fairness, all efficiencies in Table 3 are recalculated using this metric. In our protocol, producing a two-bit signature (i.e., $m = 2$) requires Alice and Bob each prepares one EPR pair, performs particle exchange, and completes the measurement process, resulting in a total consumption

**Table 3** Efficiency comparison of AQS protocols

| | PNS, wavelength filters | SWAP test | Quantum resource | Quantum operation | Qubit efficiency |
|---|---|---|---|---|---|
| Li et al. [9] | Yes | Yes | Bell state, single photon | Bell measurement, $I$ gate, $X$ gate, $Z$ gate | 25% |
| Zheng et al. [15] | Yes | Yes | GHZ state, single photon | Bell measurement, $I$ gate, $X$ gate, $Z$ gate | 8.3% |
| Zheng and Kuang [16] | No | Yes | GHZ state, single photon | CNOT gate | 16.7% |
| Xin et al. [17] | No | No | Bell state | Single photon measurement, $H$ gate, $CH$ gate, $CY$ gate, $CY^+$ gate | 50% |
| Zhang et al. [18] | No | No | Bell state | Bell measurement | 33.3% |
| Zhang et al. [19] | Yes | No | Single photon | Single photon measurement, $CH$ gate, $Y$ gate | 50% |
| Pang and Xiang [20] | Yes | No | Single photon | Single photon measurement | 50% |
| Proposed method | No | No | Bell state | Bell measurement | 50% |

of four qubits (i.e., $q = 4$). Therefore, for $2n$ bits of signature, the qubit efficiency of the proposed AQS is $\eta = \frac{2n}{4n} = \frac{1}{2}$.

In Xin et al.'s scheme [17], although they claimed that each EPR pair encodes two bits of signed message, only one of these two bits is actually verified during the protocol. The first bit is publicly announced by the signer and only specifies the measurement basis, while the second bit is determined by the joint measurement of the verifier and the arbitrator. Therefore, the protocol achieves an efficiency of 50% under our definition, as summarized in Table 3. Furthermore, Xin et al. rely on a chained single-photon structure in which each photon is processed with $Y^+$ or Hadamard gates based on hashed classical information and the state of the preceding photon. Although this design is compact, it introduces practical challenges. After a Hadamard operation, the resulting $|+\rangle$ or $|-\rangle$ states are probabilistic superpositions in the Z-basis rather than deterministic $|0\rangle$ or $|1\rangle$ states. This makes it difficult to use the preceding photon's state as a reliable reference for subsequent operations, reducing the stability of chained logic. Errors or decoherence in any intermediate photon may also propagate through the entire chain, imposing stringent requirements on quantum memory and operational precision. By contrast, the proposed AQS protocol avoids chained dependencies by treating each Bell state independently, thereby reducing error accumulation and improving the feasibility of practical implementation.

Compared with Zhang et al.'s AQS [19], the proposed AQS protocol does not rely on a reversible quantum hash structure or key-controlled single-qubit operations. Although their method also achieves 50% qubit efficiency, it requires two sequential transmissions of $n$ photons and incorporates reversible transformations that must be applied consistently across the signature sequence. In addition, the verifier must return a sequence of quantum states to the arbitrator during the verification phase, which exposes the protocol to potential Trojan-horse attacks because injected or delayed photons may leak information about the verifier's applied operations. Our protocol avoids this vulnerability by performing a single round of Bell-state preparation, transmission, and immediate measure-

ment, without any quantum-state return path. In contrast, our protocol performs only one round of Bell-state preparation, transmission, and immediate measurement, without any quantum-state return path. This simplifies the operational structure, reduces susceptibility to channel-injection attacks, and improves the overall feasibility and stability of implementation.

Pang and Xiang's B92-based protocol [20] also yields a qubit efficiency of 50% under our definition, in which two copies of $n$ single photons for $n$-bit signature are transmitted during the signing phase. However, practical performance is adversely affected by the inconclusive-measurement behavior inherent to nonorthogonal states $|0\rangle$ and $|+\rangle$ and by the need to prepare a large number of decoy photons for eavesdropping check. In addition, their design also does not incorporate defenses against Trojan-horse attacks, as the verifier still returns quantum states to the arbitrator. In contrast, the proposed protocol uses Bell states and immediate measurement to obtain deterministic outcomes and reduces the attack surface associated with channel injection. In contrast, the proposed protocol uses Bell states and immediate measurement to obtain deterministic outcomes and reduces the attack surface associated with channel injection.

Trojan-horse attacks [43, 44] are common threats in quantum cryptographic settings. As detailed in the security analysis, the proposed protocol inherently prevents such attacks because each received photon is immediately measured and the protocol does not rely on secret-dependent quantum operations. As a result, injected photons cannot extract meaningful information. Furthermore, no additional countermeasures, such as wavelength filters or photon-number splitters, are required. This design reduces implementation cost and enhances practical feasibility.

## 5 Conclusion

This paper presents a high-efficiency arbitrated quantum signature protocol characterized by several distinctive design features. Upon signature generation, the quantum states are immediately measured and converted into storable classical data, eliminating the need for SWAP tests and long-term quantum storage. The protocol leverages entanglement swapping to embed both public and concealed information within the initial quantum states, while XOR operations and hash functions streamline the signing and verification processes. Its one-way transmission architecture reduces reliance on additional channel protection mechanisms and lowers the quantum-operation overhead. From a security perspective, the protocol ensures unforgeability and non-repudiation, and demonstrates structural resistance to Trojan-horse attacks and photon-interception threats under the protocol assumptions described in this work. In terms of performance, the protocol achieves a qubit efficiency of 50%, matching the best existing approaches under the adopted efficiency metric and indicating competitive practical feasibility.

Future research may focus on reducing the degree of trust required of the arbitrator to broaden applicability in low-trust environments. Currently, the protocol relies on the synchronized arrival of photons in the entanglement-swapping process to complete Bell measurements, which introduces certain experimental constraints. A promising direction is to investigate the use of single-photon operations and measurements to simplify system design, relax synchronization requirements, and further lower barriers to practical implementation.

**Author contributions**
J.L. and C.-W.Y. conceptualized the study, and M.-Y.Y. conducted the literature investigation. J.L. developed the methodology, while C.-W.T. and M.-Y.Y. performed the formal analysis. C.-W.T. also validated the correctness of the proposed scheme. M.-Y.Y. prepared the original draft of the manuscript, and both J.L. and C.-W.Y. reviewed and revised the manuscript. C.-W.Y. supervised the project administration. All authors have read and agree to the manuscript.

**Funding information**
This work was partially supported by the National Science and Technology Council, Taiwan, R.O.C. (Grant Nos. NSTC 114-2221-E-005-087, NSTC 114-2221-E-039-013-MY3, NSTC 114-2221-E-025-006-MY2, and NSTC 114-2634-F-005-001-MBK) and China Medical University, Taiwan (Grant No. CMU114-S-48).

**Data availability**
No datasets were generated or analysed during the current study.

## Declarations

**Competing interests**
The authors declare no competing interests.

**Author details**
[1]Department of Computer Science and Engineering, National Chung Hsing University, No. 145, Xingda Rd., South District, Taichung 402202, Taiwan. [2]Department of Computer Science and Information Engineering, National Taichung University of Science and Technology, No. 129, Sec. 3, Sanmin Rd., North Dist., Taichung 404336, Taiwan. [3]Master Program for Digital Health Innovation, College of Humanities and Sciences, China Medical University, No. 100, Sec. 1, Jingmao Rd., Beitun Dist., Taichung 406040, Taiwan.

Received: 22 September 2025 Accepted: 6 March 2026 Published online: 19 March 2026

**References**

1. Diffie W, Hellman ME. New directions in cryptography. 1st ed. In: Democratizing cryptography: the work of Whitfield Diffie and Martin Hellman. New York: ACM; 2022. p. 365–90. https://doi.org/10.1145/3549993.3550007.
2. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21(2):120–6. https://doi.org/10.1145/359340.359342.
3. Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory. 1985;31(4):469–72. https://doi.org/10.1109/TIT.1985.1057074.
4. Shor P. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th annual symposium on foundations of computer science. Santa Fe, NM, USA. Nov. 20–22, 1994. p. 124–134. https://doi.org/10.1109/SFCS.1994.365700.
5. Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th annual ACM symposium on theory of computing. Philadelphia, PA, USA. 1996. p. 212–9. https://doi.org/10.1145/237814.23786.
6. Gottesman D, Chuang I. Quantum digital signatures. 2001. arXiv:quant-ph/0105032.
7. Buhrman H, Cleve R, Watrous J, de Wolf R. Quantum fingerprinting. Phys Rev Lett. 2001;87(16):167902. https://doi.org/10.1103/PhysRevLett.87.167902.
8. Zeng G, Keitel CH. Arbitrated quantum-signature scheme. Phys Rev A. 2002;65(4):042312. https://doi.org/10.1103/PhysRevA.65.042312.
9. Li Q, Chan WH, Long D-Y. Arbitrated quantum signature scheme using Bell states. Phys Rev A. 2009;79(5):054307. https://doi.org/10.1103/PhysRevA.79.054307.
10. Zou X, Qiu D. Security analysis and improvements of arbitrated quantum signature schemes. Phys Rev A. 2010;82(4):042325. https://doi.org/10.1103/PhysRevA.82.042325.
11. Gao F, Qin S-J, Guo F-Z, Wen Q-Y. Cryptanalysis of the arbitrated quantum signature protocols. Phys Rev A. 2011;84(2):022344. https://doi.org/10.1103/PhysRevA.84.022344.
12. Li F-G, Shi J-H. An arbitrated quantum signature protocol based on the chained CNOT operations encryption. Quantum Inf Process. 2015;14(6):2171–81. https://doi.org/10.1007/s11128-015-0981-5.
13. Luo Y-P, Hwang T. Comment on an arbitrated quantum signature protocol based on the chained CNOT operations encryption. 2015. arXiv:1512.00711.
14. Zhang L, Sun H-W, Zhang K-J, Jia H-Y. An improved arbitrated quantum signature protocol based on the key-controlled chained CNOT encryption. Quantum Inf Process. 2017;16(3):70. https://doi.org/10.1007/s11128-017-1531-0.
15. Zheng T, Chang Y, Zhang S-B. Arbitrated quantum signature scheme with quantum teleportation by using two three-qubit GHZ states. Quantum Inf Process. 2020;19(5):163. https://doi.org/10.1007/s11128-020-02665-x.
16. Zheng X-Y, Kuang C. Arbitration quantum signature protocol based on XOR encryption. Int J Quantum Inf. 2020;18(05):2050025. https://doi.org/10.1142/S0219749920500252.
17. Xin X, Ding L, Yang Q, Li C, Zhang T, Sang Y. Efficient chain-encryption-based quantum signature scheme with semi-trusted arbitrator. Quantum Inf Process. 2022;21(7):246. https://doi.org/10.1007/s11128-022-03593-8.
18. Zhang T, Li C, Xin X. Secure arbitrated quantum signature scheme with Bell state. In: International conference on frontiers in cyber security. Chengdu, China. August 21–23, 2023. p. 283–294. https://doi.org/10.1007/978-981-99-9331-4_19.
19. Zhang T, Xin X, Sun L, Li C, Li F. Secure quantum signature scheme without entangled state. Quantum Inf Process. 2024;23(2):49. https://doi.org/10.1007/s11128-024-04257-5.
20. Pang Z, Xiang H. A simplified arbitrated quantum signature protocol without entanglement: design premise and security analysis. Opt Commun. 2025;595:132315. https://doi.org/10.1016/j.optcom.2025.132315.

21. Bennett CH. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett. 1992;68(21):3121–4. https://doi.org/10.1103/PhysRevLett.68.3121.
22. Zhao X-Q, Chen H-Y, Wang Y-Q, Zhou N-R. Semi-quantum bi-signature scheme based on W states. Int J Theor Phys. 2019;58(10):3239–51. https://doi.org/10.1007/s10773-019-04199-0.
23. Chen L-Y, Liao Q, Tan R-C, Gong L-H, Chen H-Y. Offline arbitrated semi-quantum signature scheme with four-particle cluster state. Int J Theor Phys. 2020;59(12):3685–95. https://doi.org/10.1007/s10773-020-04605-y.
24. Xia C, Li H, Hu J. A semi-quantum blind signature protocol based on five-particle GHZ state. Eur Phys J Plus. 2021;136(6):633. https://doi.org/10.1140/epjp/s13360-021-01605-7.
25. He R-Z, Li Z-Z, Wang Q-H, Li Y-J, Li Z-C. Semi-quantum ring signature protocol based on multi-particle GHZ state. Quantum Inf Process. 2023;22(9):337. https://doi.org/10.1007/s11128-023-04087-x.
26. Yang Y-G, Zhou Z, Teng Y-W, Wen Q-Y. Arbitrated quantum signature with an untrusted arbitrator. Eur Phys J D. 2011;61(3):773–8. https://doi.org/10.1140/epjd/e2010-10157-4.
27. Luo M-X, Chen X-B, Yun D, Yang Y-X. Quantum signature scheme with weak arbitrator. Int J Theor Phys. 2012;51(7):2135–42. https://doi.org/10.1007/s10773-012-1093-y.
28. Su Q, Li W-M. Improved quantum signature scheme with weak arbitrator. Int J Theor Phys. 2013;52(9):3343–52. https://doi.org/10.1007/s10773-013-1631-2.
29. Wen X, Niu X, Ji L, Tian Y. A weak blind signature scheme based on quantum cryptography. Opt Commun. 2009;282(4):666–9. https://doi.org/10.1016/j.optcom.2008.10.025.
30. Xu R, Huang L, Yang W, He L. Quantum group blind signature scheme without entanglement. Opt Commun. 2011;284(14):3654–8. https://doi.org/10.1016/j.optcom.2011.03.083.
31. Xu G-B, Zhang K-J. A novel quantum group signature scheme without using entangled states. Quantum Inf Process. 2015;14(7):2577–87. https://doi.org/10.1007/s11128-015-0995-z.
32. Wen X, Tian Y, Ji L, Niu X. A group signature scheme based on quantum teleportation. Phys Scr. 2010;81(5):055001. https://doi.org/10.1088/0031-8949/81/05/055001.
33. Qu W, Zhang Y, Liu H, Dou T, Wang J, Li Z, Yang S, Ma H. Multi-party ring quantum digital signatures. J Opt Soc Am B. 2019;36(5):1335–41. https://doi.org/10.1364/JOSAB.36.001335.
34. Qiu C, Zhang S, Chang Y, Huang X, Chen H. Electronic voting scheme based on a quantum ring signature. Int J Theor Phys. 2021;60(4):1550–5. https://doi.org/10.1007/s10773-021-04777-1.
35. Xiong Z, Yin A. A novel quantum ring signature scheme without using entangled states. Quantum Inf Process. 2022;21(4):140. https://doi.org/10.1007/s11128-022-03481-1.
36. Shujing Q, Xiangjun X, Jiahao Z, Chaoyang L, Fagen L, Qian Z. Comment and improvement on the "semi-quantum ring signature protocol based on multi-particle GHZ state". Quantum Inf Process. 2024;23(8):287. https://doi.org/10.1007/s11128-024-04500-z.
37. Xin X, Ding L, Li C, Sang Y, Yang Q, Li F. Quantum public-key designated verifier signature. Quantum Inf Process. 2022;21(1):33. https://doi.org/10.1007/s11128-021-03387-4.
38. Zhang L, Zhang J-H, Xin X-J, Li C-Y. Quantum designated verifier signature without third party. Quantum Inf Process. 2023;22(12):452. https://doi.org/10.1007/s11128-023-04183-y.
39. Zhang L, Zhang J-H, Xin X-J, Li C-Y, Huang M. Quantum designated verifier signature scheme with semi-trusted third-party. Int J Theor Phys. 2023;62(8):166. https://doi.org/10.1007/s10773-023-05428-3.
40. Zhang Y, Xin X, Li F. Secure and efficient quantum designated verifier signature scheme. Mod Phys Lett A. 2020;35(18):2050148. https://doi.org/10.1142/s0217732320501485.
41. Nielsen MA, Chuang IL. Quantum computation and quantum information. 10th ed. Cambridge: Cambridge University Press; 2010.
42. Bennett CH, Brassard G. Quantum cryptography: public key distribution, and coin-tossing. In: Proceedings of IEEE international conference on computers, systems, and signal processing. Bangalore, India. 1984. p. 175–9.
43. Cai Q-Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys Lett A. 2006;351(1–2):23–5. https://doi.org/10.1016/j.physleta.2005.10.050.
44. Gisin N, Fasel S, Kraus B, Zbinden H, Ribordy G. Trojan-horse attacks on quantum-key-distribution systems. Phys Rev A. 2006;73(2):022320. https://doi.org/10.1103/PhysRevA.73.022320.
45. Shannon CE. A mathematical theory of communication. Bell Syst Tech J. 1948;27(3):379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.


## Publisher's note