Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Improvements on quantum designated verifier signature based on Bell states

Cai Zhang
South China Agricultural University
Kechuan Li
South China Agricultural University
Zhiwei Sun
smeker@szpu.edu.cn

Shenzhen Polytechnic University

Research Article

Keywords: Quantum cryptography, Designated verifier signature, Forgery attack, Entanglement-free

Posted Date: July 20th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9990142/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Improvements on quantum designated verifier signature based on Bell states

Cai Zhang[1], Kechuan Li[1], Zhiwei Sun[2*]

[1]College of Mathematics and Informatics, South China Agricultural University, Guangzhou, 510642, Guangdong, China.
[2*]Undergraduate School of Artificial Intelligence, Shenzhen Polytechnic University, Shenzhen, 518055, Guangdong, China.

*Corresponding author(s). E-mail(s): smeker@szpu.edu.cn;
Contributing authors: zhangcai@scau.edu.cn; 2567358216@qq.com;

Abstract

Quantum Designated Verifier Signature (QDVS) is a cryptographic scheme based on quantum mechanics in which a signature can be verified only by a specific designated verifier. Recently, Xin et al. (Quantum Information Processing, 2020, 19(3):79) proposed a QDVS scheme based on Bell states and claimed that it was secure. However, we demonstrate that their scheme is vulnerable to forgery attacks. To overcome this vulnerability, we propose an improved QDVS scheme utilizing single qubits and unitary operations. Compared with Xin et al.'s scheme, our scheme requires neither a trusted center (TC) nor quantum entanglement resources, thereby greatly reducing the implementation complexity. Our security analysis demonstrates that our scheme can resist common attacks, including inter-resending, forgery, and impersonation attacks.

Keywords: Quantum cryptography, Designated verifier signature, Forgery attack, Entanglement-free

1 Introduction

In the contemporary digital landscape, the assurance of data privacy and security has become a critical imperative. Among the various cryptographic primitives, digital signatures [1] hold significant importance because they provide data integrity, authentication, and non-repudiation.

In traditional digital signatures, anyone can verify the signatures by using the signer's public key. However, public verification does not achieve the desired outcome in certain specific scenarios, such as e-voting, calls for tenders, and software licensing. Signers may prefer that their signatures be verifiable only by designated verifiers to protect their privacy. Notably, Jakobsson et al. [2] addressed this issue by proposing designated verifier signatures (DVS) in 1996. A DVS scheme is required to exhibit the following properties [3, 4].

1. Correctness: If a signer generates a DVS by executing the signature algorithm, it can be validated by the designated verifier using the corresponding verification algorithm.
2. Non-transferability: The designated verifier (DV) cannot prove to a third party whether the signature was generated by themselves or the signer, because the DV can simulate the signing algorithm to produce a signature indistinguishable from the signer's.
3. Source hiding: Even if the secret keys of the signer and the designated verifier are known, it remains infeasible for any party to determine the true origin of a given signature.
4. Unforgeability: It is computationally infeasible to generate a valid DVS without possessing the private key of the signer or the designated verifier.

Fundamentally, many classical digital signature schemes [5–12] rely on computationally hard problems, such as the elliptic curve discrete logarithm problem and integer factorization. However, the advent of quantum computing poses a potential threat to the security of traditional DVS, which are built on specific mathematical assumptions [13, 14]. This has naturally led to the exploration of more secure cryptographic techniques, particularly quantum-based solutions, which rely on the physical principles of quantum mechanics. Since the proposal of the first quantum key distribution (QKD) scheme [15], quantum technologies have been widely applied in cryptography. The first quantum digital signature protocol [16] was proposed by Gottesman and Chuang. After that, many general quantum signature schemes were designed, such as arbitrated quantum signature (AQS) [17–19], quantum blind signature [20, 21], quantum group signature [22, 23], and quantum proxy signature [24, 25]. The verification of the effectiveness of these schemes differs from that of the QDVS. In detail, in a general quantum signature scheme, any recipient can verify a signature, and the verifier can even convince a third party of the signer's identity. In contrast, a QDVS scheme must possess properties such as non-transferability and source hiding. Many QDVS schemes have been proposed to date [26–31]. To expand the application scenarios of the QDVS scheme, Zhang et al. first introduced the semi-quantum designated verifier signature (SQDVS) scheme [32], quantum designated multi-verifier signature (QDMVS) scheme [33], and quantum designated verifier multi-signature (QDVMS) scheme [34]. Li et al. [35] proposed a quantum designated verifier signature scheme based on Lagrange interpolation. The scheme utilizes single photons rather than entangled states, and mploys a trusted third party for signature verification.

The QDVS schemes proposed by Shi et al. in [26, 27] have been proven to be vulnerable to forgery attacks by Xin et al. in [29]. In Xin et al.'s scheme, it was

demonstrated that a malicious TC could successfully forge a signature. Compared with Shi et al.'s scheme, Xin et al.'s scheme achieves higher efficiency and security without requiring quantum one-way functions and quantum state comparisons by the partners. However, Xin et al.'s scheme [29] also fails to resist the forgery attack. A malicious Eve can execute a man-in-the-middle attack [36] to forge the signature without the private keys of the signer or the DV. We demonstrate Eve's forgery attack on Xin et al. scheme in section **??**. In addition, the schemes in [26, 29, 37] need a trusted third center (TC). Among them, the TC in the schemes in [26, 37] holds the private key, which becomes a potential security risk. Although the scheme in [29] weakens the capability of the TC, the TC still has to prepare and distribute entangled particles. Overall, the TC may become a bottleneck for the QDVS schemes. To enhance the security and reduce the consumption of quantum resources, we propose a new scheme without entanglement and any TC. The proposed scheme overcomes the security drawbacks in Xin et al.'s scheme. Our scheme also possesses essential security properties such as designated verification, non-transferability, and source hiding.

The rest of the paper is organized as follows. In section 2, Xin et al.'s QDVS scheme [29] is briefly reviewed. In section 3, we present a detailed analysis of the forgery attack on Xin et al.'s QDVS scheme. In section 4, an improved QDVS scheme is proposed. In section 5, the security of our scheme is analyzed. Finally, the conclusion is given in Section 6.

2 Review of Xin et al.'s scheme

In Xin et al.'s QDVS scheme [29], there are three partners: the trusted center TC, the signer Alice, and the designated verifier Bob. The QDVS scheme includes three phases: initializing phase, signing phase, and verification phase.

2.1 Initializing phase

I-step 1 Alice and Bob share two random secret keys $c = \{c_1, c_2, \ldots, c_n\} \in \{0,1\}^n$ and $k = \{k_1, k_2, \ldots, k_n\} \in \{0,1\}^n$ by performing the quantum key distribution protocol (QKDP) [38, 39].

I-step 2 TC prepares n Bell states $\{|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_n\rangle\}$ where

$$|\phi_i\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_{a_i,b_i} + |11\rangle_{a_i,b_i}\right), \quad i = 1, 2, \ldots, n.$$

The subscripts a_i and b_i denote the first and second particles of $|\phi_i\rangle$, respectively. Then, TC distributes the particle sequences $sa = \{a_1, a_2, \ldots, a_n\}$ and $sb = \{b_1, b_2, \ldots, b_n\}$ to Alice and Bob, respectively, with randomly inserted decoy particles Del. The number of decoy particles must be sufficient for statistical analysis.

I-step 3 Alice and Bob obtain sa and sb after detecting eavesdropping.

2.2 Signing phase

Several operators will be used, including $H = (|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)/\sqrt{2}$, $Y = |0\rangle\langle 1| - |1\rangle\langle 0|$ and $Y^\dagger = |1\rangle\langle 0| - |0\rangle\langle 1|$. And they define $H^0 = Y^0 = (Y^+)^0 = I$

where I is the unit operator. Note that $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Alice signs a message $m = (m_1, m_2, \ldots, m_n) \in \{0,1\}^n$ by carrying out the following steps.

S-step 1 Alice performs the operation H^{c_i} on $|m_i\rangle_{s_i}$ and gets the state $|s\rangle_{s_1,s_2,\ldots,s_n} = \otimes_{i=1}^{n} |\overline{m}_i\rangle_{s_i}$,where

$$|\overline{m}_i\rangle_{s_i} = H^{c_i}|m_i\rangle_{s_i}, i = 1, 2, \ldots, n.$$

S-step 2 Alice performs $(|0\rangle_{a_i}\langle 0| \otimes Y_{s_i}^{k_i} + |1\rangle_{a_i}\langle 1| \otimes Y_{s_i}^{k_i \oplus 1})$ on particles a_i and s_i. After that, the state of the system composed of a_i, b_i and s_i becomes

$$\left|\chi_i^{a_i,b_i,s_i}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_{a_i,b_i} \otimes Y^{k_i}\,|\overline{m}_i\rangle_{s_i} + |11\rangle_{a_i,b_i} \otimes Y^{k_i \oplus 1}\,|\overline{m}_i\rangle_{s_i}\right).$$

Note that the states of s_i $(i = 1, 2, \ldots, n)$ are transformed here and denoted as $|s_i'\rangle$ in Xin et al.'s scheme. Alice sends the quantum signature

$$|s'\rangle = \{|s_1'\rangle, |s_2'\rangle, \ldots, |s_n'\rangle\}$$

and the message m to Bob.

2.3 Verifying phase

In this phase, Bob verifies the signature by performing the controlled-Y operations and the appropriate measurements.

V-step 1 After receiving the signature, Bob performs the operation $(|0\rangle_{b_i}\langle 0| \otimes (Y^{\dagger})_{s_i}^{k_i} + |1\rangle_{b_i}\langle 1| \otimes (Y^{\dagger})_{s_i}^{k_i \oplus 1})$ on particles b_i and s_i according to the secret k. Bob then gets the quantum sequence $|s\rangle_{s_1,s_2,\ldots,s_n} = \otimes_{i=1}^{n} |\overline{m}_i\rangle_{s_i}$.

V-step 2 Bob measures $|s\rangle$ according to the secret key c. For each $|\overline{m}_i\rangle_{s_i}$, if $c_i = 0$, Bob measures $|s_i\rangle$ with the basis $\{|0\rangle, |1\rangle\}$. Otherwise, he measures $|s_i\rangle$ with the basis $\{|+\rangle, |-\rangle\}$. According to the measurement result, he sets

$$m_i' := \begin{cases} 0, & \text{if } |\overline{m}_i\rangle = |0\rangle \text{ or } |+\rangle \\ 1, & \text{if } |\overline{m}_i\rangle = |1\rangle \text{ or } |-\rangle \end{cases}, \quad i = 1, 2, \ldots, n.$$

Therefore, Bob obtains $m' = (m_1', m_2', \ldots, m_n')$ and then compares m' with m. If $m' = m$, Bob accepts the valid signature; otherwise, he rejects it. However, Xin et al.'s scheme fails to resist forgery attacks. Eve can manipulate the signature to forge a valid new one, which remains undetected during transmission from Alice to Bob. A detailed discussion of this attack is presented in the next section.

3 Security analysis of Xin et al.'s scheme

In fact, Xin et al.'s scheme [29] is insecure against forgery attacks. In S-Step 2, during the transmission of the signature from Alice to Bob, the adversary Eve can intercept

and tamper with it. To tamper with the message $m = (m_1, m_2, \ldots, m_n)$ to produce a desired one $m^* = (m_1^*, m_2^*, \ldots, m_n^*)$, Eve intercepts the signature and forges a new valid signature $|s^{*\prime}\rangle$ by performing an XOR operation on m_i and a Y-operation on the corresponding $|s_i'\rangle$ as follow:

$$d_i = m_i^* \oplus m_i, \tag{1}$$

$$|s_i^{*\prime}\rangle = Y^{d_i}|s_i'\rangle. \tag{2}$$

After that, the state of the system turns into

$$\left|\chi_i^{a_i,b_i,s_i}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_{a_i,b_i} \otimes Y^{d_i}Y^{k_i}\,|\overline{m}_i\rangle_{s_i} + |11\rangle_{a_i,b_i} \otimes Y^{d_i}Y^{k_i\oplus 1}\,|\overline{m}_i\rangle_{s_i}\right).$$

Subsequently, Eve sends the new signature $|s^{*\prime}\rangle = \{|s_1^{*\prime}\rangle, |s_2^{*\prime}\rangle, \ldots, |s_n^{*\prime}\rangle\}$ to Bob with the tampered message m^*. Upon receiving the signature, according to V-Step 1, Bob performs the operation $(|0\rangle_{b_i}\langle 0| \otimes (Y^\dagger)^{k_i}_{s_i} + |1\rangle_{b_i}\langle 1| \otimes (Y^\dagger)^{k_i\oplus 1}_{s_i})$ on particles b_i and s_i according to the secret k. It is straightforward to verify that $Y^\dagger = -Y$. Thus, $(Y^\dagger)^{k_i}Y^{d_i} = (-1)^{k_i}Y^{k_i}Y^{d_i}$ and $Y^{d_i}(Y^\dagger)^{k_i} = (-1)^{k_i}Y^{d_i}Y^{k_i}$. Since $Y^{k_i}Y^{d_i} = Y^{d_i}Y^{k_i}$, we obtain $(Y^\dagger)^{k_i}Y^{d_i} = Y^{d_i}(Y^\dagger)^{k_i}$. Based on this, the state of the system becomes

$$\begin{aligned}
|\chi_i^*\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_i,b_i} \otimes (Y^\dagger)^{k_i}Y^{d_i}Y^{k_i}\,|\overline{m}_i\rangle_{s_i} + |11\rangle_{a_i,b_i} \otimes (Y^\dagger)^{k_i\oplus 1}Y^{d_i}Y^{k_i\oplus 1}\,|\overline{m}_i\rangle_{s_i}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_i,b_i} \otimes Y^{d_i}(Y^\dagger)^{k_i}Y^{k_i}\,|\overline{m}_i\rangle_{s_i} + |11\rangle_{a_i,b_i} \otimes Y^{d_i}(Y^\dagger)^{k_i\oplus 1}Y^{k_i\oplus 1}\,|\overline{m}_i\rangle_{s_i}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_i,b_i} \otimes Y^{d_i}\,|\overline{m}_i\rangle_{s_i} + |11\rangle_{a_i,b_i} \otimes Y^{d_i}\,|\overline{m}_i\rangle_{s_i}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_i,b_i} \otimes Y^{d_i}H^{c_i}\,|m_i\rangle_{s_i} + |11\rangle_{a_i,b_i} \otimes Y^{d_i}H^{c_i}\,|m_i\rangle_{s_i}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_i,b_i}\, Y^{d_i}H^{c_i}\,|m_i\rangle_{s_i} + |11\rangle_{a_i,b_i}\, Y^{d_i}H^{c_i}\,|m_i\rangle_{s_i}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_i,b_i} + |11\rangle_{a_i,b_i}\right) \otimes Y^{d_i}H^{c_i}\,|m_i\rangle_{s_i}.
\end{aligned} \tag{3}$$

Finally, Bob obtains the quantum sequence $|\overline{m}^*\rangle_{s_1,s_2,\ldots,s_n} = \otimes_{i=1}^n |\overline{m}_i^*\rangle_{s_i} = \otimes_{i=1}^n Y^{d_i}H^{c_i}|m_i\rangle_{s_i}$.

It is easy to obtain $Y|0\rangle = -|1\rangle, Y|1\rangle = |0\rangle$, $Y|+\rangle = |-\rangle, Y|-\rangle = -|+\rangle$. That is, if the measurement result on $H^{c_i}|m_i\rangle_{s_i}$ is m_i', then the measurement result on $YH^{c_i}|m_i\rangle_{s_i}$ is $m_i' \oplus 1$, as specified in **V-step2**.

In the case where $m_i^* = m_i$ $(i = 1, 2, \ldots, n)$, this implies that $d_i = 0$ and Bob obtains $|\overline{m}_i^*\rangle_{s_i} = Y^0H^{c_i}|m_i\rangle_{s_i} = |\overline{m}_i\rangle_{s_i}$ in **V-step 1**; when Bob measures particle s_i in the appropriate basis based on c_i in **V-step 2**, he gets the same result m_i' that equals m_i^*. Similarly, in the case where $m_i^* = m_i \oplus 1$, Bob obtains the opposite result $m_i' \oplus 1$ that also equals m_i^* in **V-step 2**. Therefore, Eve can tamper with the message

m and the corresponding signature $|s'\rangle$ to generate a new signature that matches the fake message m^*. In the following, we illustrate this attack with an example.

Suppose that Alice has message $m = (m_1, m_2, m_3, m_4) = (0, 1, 1, 0)$, and secret keys $c = (c_1, c_2, c_3, c_4) = (1, 0, 0, 1)$ and $k = (k_1, k_2, k_3, k_4) = (0, 1, 0, 1)$. Since the keys c and k are shared by Alice and Bob, Bob also holds them. Eve aims to replace m with a new message $m^* = (m_1^*, m_2^*, m_3^*, m_4^*) = (1, 0, 1, 1)$ and forge a corresponding signature. From Equation (1), we obtain $d = (d_1, d_2, d_3, d_4) = (1, 1, 0, 1)$. After the initializing phase and the signing phase, the states of the four systems become

$$
\begin{aligned}
|\chi_1\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_1,b_1} \otimes Y^{k_1} |\overline{m}_1\rangle_{s_1} + |11\rangle_{a_1,b_1} \otimes Y^{k_1 \oplus 1} |\overline{m}_1\rangle_{s_1}\right) \\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_1,b_1} \otimes Y^{k_1} H^{c_1} |m_1\rangle_{s_1} + |11\rangle_{a_1,b_1} \otimes Y^{k_1 \oplus 1} H^{c_1} |m_1\rangle_{s_1}\right) \\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_1,b_1} \otimes Y^{0} H^{1} |0\rangle_{s_1} + |11\rangle_{a_1,b_1} \otimes Y^{0 \oplus 1} H^{1} |0\rangle_{s_1}\right). \\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_1,b_1} \otimes |+\rangle_{s_1} + |11\rangle_{a_1,b_1} \otimes |-\rangle_{s_1}\right),
\end{aligned}
$$

$$
\begin{aligned}
|\chi_2\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_2,b_2} \otimes Y^{k_2} |\overline{m}_2\rangle_{s_2} + |11\rangle_{a_2,b_2} \otimes Y^{k_2 \oplus 1} |\overline{m}_2\rangle_{s_2}\right) \\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_2,b_2} \otimes Y^{k_2} H^{c_2} |m_2\rangle_{s_2} + |11\rangle_{a_2,b_2} \otimes Y^{k_2 \oplus 1} H^{c_2} |m_2\rangle_{s_2}\right) \\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_2,b_2} \otimes Y^{1} H^{0} |1\rangle_{s_2} + |11\rangle_{a_2,b_2} \otimes Y^{1 \oplus 1} H^{0} |1\rangle_{s_2}\right). \\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_2,b_2} \otimes |0\rangle_{s_2} + |11\rangle_{a_2,b_2} \otimes |1\rangle_{s_2}\right),
\end{aligned}
$$

$$
\begin{aligned}
|\chi_3\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_3,b_3} \otimes Y^{k_3} |\overline{m}_3\rangle_{s_3} + |11\rangle_{a_3,b_3} \otimes Y^{k_3 \oplus 1} |\overline{m}_3\rangle_{s_3}\right) \\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_3,b_3} \otimes Y^{k_3} H^{c_3} |m_3\rangle_{s_3} + |11\rangle_{a_3,b_3} \otimes Y^{k_3 \oplus 1} H^{c_3} |m_3\rangle_{s_3}\right) \\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_3,b_3} \otimes Y^{0} H^{0} |1\rangle_{s_3} + |11\rangle_{a_3,b_3} \otimes Y^{0 \oplus 1} H^{0} |1\rangle_{s_3}\right). \\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_3,b_3} \otimes |1\rangle_{s_3} + |11\rangle_{a_3,b_3} \otimes |0\rangle_{s_3}\right),
\end{aligned}
$$

$$
\begin{aligned}
|\chi_4\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_4,b_4}\otimes Y^{k_4}\,|\overline{m}_4\rangle_{s_4}+|11\rangle_{a_4,b_4}\otimes Y^{k_4\oplus 1}\,|\overline{m}_4\rangle_{s_4}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_4,b_4}\otimes Y^{k_4}H^{c_4}\,|m_4\rangle_{s_4}+|11\rangle_{a_4,b_4}\otimes Y^{k_4\oplus 1}H^{c_4}\,|m_4\rangle_{s_4}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_4,b_4}\otimes Y^{1}H^{1}\,|0\rangle_{s_4}+|11\rangle_{a_4,b_4}\otimes Y^{1\oplus 1}H^{1}\,|0\rangle_{s_4}\right).\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_4,b_4}\otimes |-\rangle_{s_4}+|11\rangle_{a_4,b_4}\otimes |+\rangle_{s_4}\right).
\end{aligned}
$$

When Alice sends the signature $|s'\rangle_{s_1,s_2,s_3,s_4}=\{|s'_1\rangle,|s'_2\rangle,|s'_3\rangle,|s'_4\rangle\}$ and the message m to Bob. Eve intercepts them and replaces m with m^*. Simultaneously, Eve performs Y^{d_i} $(i=1,2,3,4)$ on particle s_i. After that, the states of the four systems are converted into

$$
\begin{aligned}
|\chi_1^*\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_1,b_1}\otimes Y^{d_1}\,|+\rangle_{s_1}+|11\rangle_{a_1,b_1}\otimes Y^{d_1}\,|-\rangle_{s_1}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_1,b_1}\otimes Y\,|+\rangle_{s_1}+|11\rangle_{a_1,b_1}\otimes Y\,|-\rangle_{s_1}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_1,b_1}\otimes |-\rangle_{s_1}+|11\rangle_{a_1,b_1}\otimes (-|+\rangle_{s_1})\right),\\
|\chi_2^*\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_2,b_2}\otimes Y^{d_2}\,|0\rangle_{s_2}+|11\rangle_{a_2,b_2}\otimes Y^{d_2}\,|1\rangle_{s_2}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_2,b_2}\otimes Y\,|0\rangle_{s_2}+|11\rangle_{a_2,b_2}\otimes Y\,|1\rangle_{s_2}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_2,b_2}\otimes (-\,|1\rangle_{s_2})+|11\rangle_{a_2,b_2}\otimes |0\rangle_{s_2}\right),\\
|\chi_3^*\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_3,b_3}\otimes Y^{d_3}\,|1\rangle_{s_3}+|11\rangle_{a_3,b_3}\otimes Y^{d_3}\,|0\rangle_{s_3}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_3,b_3}\otimes Y^{0}\,|1\rangle_{s_3}+|11\rangle_{a_3,b_3}\otimes Y^{0}\,|0\rangle_{s_3}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_3,b_3}\otimes |1\rangle_{s_3}+|11\rangle_{a_3,b_3}\otimes |0\rangle_{s_3}\right),\\
|\chi_4^*\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_4,b_4}\otimes Y^{d_4}\,|-\rangle_{s_4}+|11\rangle_{a_4,b_4}\otimes Y^{d_4}\,|+\rangle_{s_4}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_4,b_4}\otimes Y^{1}\,|-\rangle_{s_4}+|11\rangle_{a_4,b_4}\otimes Y^{1}\,|+\rangle_{s_4}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_4,b_4}\otimes (-\,|+\rangle_{s_4})+|11\rangle_{a_4,b_4}\otimes |-\rangle_{s_4}\right).
\end{aligned}
$$

Similar to the notation in Xin et al. [29], we denote the state of particle s_i $(i=1,2,3,4)$ at this point by $|s''_i\rangle$. Eve sends $\{|s''_1\rangle,|s''_2\rangle,|s''_3\rangle,|s''_4\rangle\}$ as the new signature and the tampered message m^* to Bob. Subsequently, Bob performs the operation $(|0\rangle_{b_i}\langle 0|\otimes (Y^{\dagger})^{k_i}_{s_i}+|1\rangle_{b_i}\langle 1|\otimes (Y^{\dagger})^{k_i\oplus 1}_{s_i})$ on particles b_i and s_i $(i=1,2,3,4)$ with the

secret key k. The states of the four systems are now transformed into

$$\begin{aligned}
|\overline{\chi}_1^*\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_1,b_1}\otimes(Y^\dagger)^{k_1}|-\rangle_{s_1}+|11\rangle_{a_1,b_1}\otimes(Y^\dagger)^{k_1\oplus 1}(-|+\rangle_{s_1})\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_1,b_1}\otimes(Y^\dagger)^{0}|-\rangle_{s_1}+|11\rangle_{a_1,b_1}\otimes(Y^\dagger)^{1}(-|+\rangle_{s_1})\right))\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_1,b_1}\otimes|-\rangle_{s_1}+|11\rangle_{a_1,b_1}\otimes|-\rangle_{s_1}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_1,b_1}\otimes+|11\rangle_{a_1,b_1}\right)\otimes|-\rangle_{s_1},
\end{aligned}$$

$$\begin{aligned}
|\overline{\chi}_2^*\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_2,b_2}\otimes(Y^\dagger)^{k_2}(-|1\rangle_{s_2})+|11\rangle_{a_2,b_2}\otimes(Y^\dagger)^{k_2\oplus 1}|0\rangle_{s_2}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_2,b_2}\otimes(Y^\dagger)(-|1\rangle_{s_2})+|11\rangle_{a_2,b_2}\otimes(Y^\dagger)^{0}|0\rangle_{s_2}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_2,b_2}\otimes|0\rangle_{s_2}+|11\rangle_{a_2,b_2}\otimes|0\rangle_{s_2}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_2,b_2}+|11\rangle_{a_2,b_2}\right)\otimes|0\rangle_{s_2},\\
|\overline{\chi}_3^*\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_3,b_3}\otimes(Y^\dagger)^{k_3}|1\rangle_{s_3}+|11\rangle_{a_3,b_3}\otimes(Y^\dagger)^{k_3\oplus 1}|0\rangle_{s_3}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_3,b_3}\otimes(Y^\dagger)^{0}|1\rangle_{s_3}+|11\rangle_{a_3,b_3}\otimes(Y^\dagger)^{1}|0\rangle_{s_3}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_3,b_3}\otimes|1\rangle_{s_3}+|11\rangle_{a_3,b_3}\otimes|1\rangle_{s_3}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_3,b_3}+|11\rangle_{a_3,b_3}\right)\otimes|1\rangle_{s_3},\\
|\overline{\chi}_4^*\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_4,b_4}\otimes(Y^\dagger)^{k_4}(-|+\rangle_{s_4})+|11\rangle_{a_4,b_4}\otimes(Y^\dagger)^{k_4\oplus 1}|-\rangle_{s_4}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_4,b_4}\otimes(Y^\dagger)^{1}(-|+\rangle_{s_4})+|11\rangle_{a_4,b_4}\otimes(Y^\dagger)^{0}|-\rangle_{s_4}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_4,b_4}\otimes|-\rangle_{s_4}+|11\rangle_{a_4,b_4}\otimes|-\rangle_{s_4}\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{a_4,b_4}+|11\rangle_{a_4,b_4}\right)\otimes|-\rangle_{s_4}.
\end{aligned}$$

Bob then measures particles s_1, s_2, s_3, and s_4 in the respective bases $\{|+\rangle,|-\rangle\}$, $\{|0\rangle,|1\rangle\}$, $\{|0\rangle,|1\rangle\}$, and $\{|+\rangle,|-\rangle\}$ according to $c=(c_1,c_2,c_3,c_4)=(1,0,0,1)$, obtaining the measurement results $|-\rangle$, $|0\rangle$, $|1\rangle$, and $|-\rangle$. Therefore, Bob attains $m'=(m'_1,m'_2,m'_3,m'_4)=(1,0,1,1)$. Finally, Bob accepts the forged signature as $m^*=m'$. Eve's forgery attack is successful.

4 Improved scheme

To address the security drawbacks and reduce the consumption of quantum resources, we propose a novel alternative. The proposed scheme involves only two partners: a signer(Alice) and a designated verifier(Bob). It comprises three phases: initializing, signing, and verification phases.

4.1 Initializing phase

Similar to Xin et al.'s scheme [29], the operators $H = (|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)/\sqrt{2}$, $Y = |0\rangle\langle 1| - |1\rangle\langle 0|$ and $Y^\dagger = |1\rangle\langle 0| - |0\rangle\langle 1|$ will be used in our scheme. We also define $H^0 = Y^0 = (Y^\dagger)^0 = I$, where I is the unit operator. Let $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.

Alice and Bob share two random secret keys $d = \{d_1, d_2, \ldots, d_n\} \in \{0,1\}^n$ and $t = \{t_1, t_2, \ldots, t_n\} \in \{0,1\}^n$ by performing the QKDP [38, 39].

4.2 Signing phase

Suppose that Alice has the original message $m = (m_1, m_2, \ldots, m_n) \in \{0,1\}^n$ that needs to be signed. Then Alice signs m by performing the following steps.

S-step 1 Alice converts the message m into a sequence of qubits as follows:

$$(m_1, m_2, \ldots, m_n) \longrightarrow (|m_1\rangle, |m_2\rangle, \ldots, |m_n\rangle). \tag{4}$$

S-step 2 Alice applies the operations H^{d_i} and Y^{t_i} to $|m_i\rangle$ using the secret keys d and t, respectively. Alice then obtains $|s\rangle = \otimes_{i=1}^n |s_i\rangle$, where

$$|s_i\rangle = Y^{d_i} H^{t_i} |m_i\rangle, i = 1, 2, \ldots, n. \tag{5}$$

$|s\rangle$ is the signature on the message m. To ensure the security of the quantum channel, Alice randomly inserts a number of decoy particles into the signature, as described in [40, 41], where the states of the decoy particles are randomly selected from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. The number of the decoy particles should be enough for the statistical analysis. Alice sends the signature with the randomly inserted decoy particles and the message m to Bob.

4.3 Verification phase

After Bob receives the signature with the randomly inserted decoy particles, Alice publishes the locations and states of these decoy particles via a classical authenticated channel. Bob then checks whether any decoy particle has been disturbed by an eavesdropper. If the check passes, Bob removes all the decoy particles to recover the signature; otherwise, he discards it.

V-step 1 After receiving the signature successfully, Bob performs the operations $(H^\dagger)^{d_i}$ and $(Y^\dagger)^{t_i}$ on $|s_i\rangle$ according to the respective secret keys d and t. Bob then

obtains $|w\rangle = \otimes_{i=1}^{n}|w_i\rangle$, where

$$|w_i\rangle = (H^{\dagger})^{d_i}(Y^{\dagger})^{t_i}|s_i\rangle, i = 1, 2, \ldots, n. \tag{6}$$

V-step 2 Bob measures $|w_i\rangle$ $(i = 1, 2, \ldots, n)$ in the basis $\{|0\rangle, |1\rangle\}$, obtaining $m' = (m'_1, m'_2, \ldots, m'_n)$, where

$$m'_i = \begin{cases} 0, & \text{if } |w_i\rangle = |0\rangle \\ 1, & \text{if } |w_i\rangle = |1\rangle \end{cases}, \quad i = 1, 2, \ldots, n. \tag{7}$$

Finally, Bob checks whether $m = m'$. If $m = m'$, Bob accepts and announces that the signature is valid; otherwise, he rejects it.

5 Security analysis

The correctness of our scheme is evident. Therefore, this section focuses on its security analysis. We first prove that the signature of the proposed scheme satisfies ciphertext indistinguishability, which serves as the core security foundation of our design. On this basis, we focus on the forgery attack launched by the adversary, and demonstrate that our scheme can resist various typical attacks, such as the impersonation attack. It is worth noting that our proposed scheme inherently resists Trojan horse attacks as it does not need to relay the encoded states. Finally, we verify that the proposed scheme meets all required core properties of QDVS, including designated verification, non-transferability, and source hiding.

5.1 Information-theoretic security

This section is devoted to a proof of the information-theoretic security of the proposed scheme. Our QDVS scheme can be viewed as a quantum encryption scheme, where the QDVS serves as the quantum ciphertext of the plaintext m. A quantum encryption scheme is considered information-theoretically secure if it is ciphertext-indistinguishable under a quantum chosen-plaintext attack [42–44].

Definition 1 [43, 44] For every quantum circuit family $\{C_n\}$, every positive polynomial $p(\cdot)$, all sufficiently large n, and every pair of bit-strings m and m^* in the plaintext space, a quantum encryption scheme is ciphertext-indistinguishable under a quantum chosen-plaintext attack if the probability $Pr(\cdot)$ satisfies:

$$\left|\Pr\left[C_n\left(E_{L(1^n)}(m)\right) = 1\right] - \Pr\left[C_n\left(E_{L(1^n)}\left(m^*\right)\right) = 1\right]\right| < 1/p(n), \tag{8}$$

where the encryption algorithm E is a quantum algorithm, L is its internal coin tosser for the algorithm, and the resulting ciphertexts $E(m)$ and $E(m^*)$ are quantum states. As shown by Yang et al. in [44], the indistinguishability of the quantum ciphertext under a selective plaintext attack is characterized by the trace distance between the density operators of cipher states $E(m)$and $E(m^*)$.

Theorem 1 [44] *A quantum encryption scheme is information-theoretically indistinguishable if, for all plaintexts m and m' with corresponding ciphertext density operators ρ_m and $\rho_{m'}$, and for every positive polynomial $p(\cdot)$ and all sufficiently large n, the trace distance satisfies*

$$D(\rho_m, \rho_{m'}) < 1/p(n). \tag{9}$$

Theorem 2 *The proposed QDVS scheme is information-theoretically indistinguishable.*

Proof In the proposed QDVS scheme, the quantum signature is generated by encrypting the message m during the signing phase. Consequently, the quantum signatures $|s\rangle$ and $|s'\rangle$ can be viewed as quantum ciphertexts of distinct messages m and m', respectively. From the adversary's perspective, the density operator of $|s\rangle$ must account for all possible values of the secret keys d and t. Based on Equation (5), this density operator becomes

$$\rho_s = \left(\frac{1}{2}\right)^{2n} \bigotimes_{i=1}^{n} \sum_{d_i, t_i \in \{0,1\}} Y^{d_i} H^{t_i} |m_i\rangle\langle m_i| (H^\dagger)^{t_i} (Y^\dagger)^{d_i}. \tag{10}$$

For the i-th single qubit ($i = 1, 2, \ldots, n$), d_i and t_i have four possible combinations: $(00, 01, 10, 11)$. The corresponding density operator is

$$\rho_i = \begin{cases} \frac{1}{4}(|0\rangle\langle 0| + |+\rangle\langle +| + |1\rangle\langle 1| + |-\rangle\langle -|) = \frac{I}{2}, & \text{if } |m_i\rangle = |0\rangle \\ \frac{1}{4}(|1\rangle\langle 1| + |-\rangle\langle -| + |0\rangle\langle 0| + |+\rangle\langle +|) = \frac{I}{2}, & \text{if } |m_i\rangle = |1\rangle \end{cases}, \quad 1 \le i \le n. \tag{11}$$

It follows that the density operator of the n qubits becomes

$$\begin{aligned} \rho_s &= \rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n \\ &= \left(\frac{I}{2}\right) \otimes \left(\frac{I}{2}\right) \otimes \cdots \otimes \left(\frac{I}{2}\right) \\ &= \frac{I^{\otimes n}}{2^n}. \end{aligned} \tag{12}$$

Similarly, the density operator of $|s'\rangle$ is $\rho_{s'} = \frac{I^{\otimes n}}{2^n}$. Clearly, the trace distance between $|s\rangle$ and $|s'\rangle$ is $D(\rho_m, \rho_{m'}) = 0$. Hence, according to Theorem 1, our QDVS scheme is information-theoretically secure.

5.2 Inter-resending attack

Within the QDVS framework, a valid signature must be generated and verified strictly following the signing phase and the verification phase, respectively. An adversary attempting to forge a signature using the attack methods described in Section **??** is impossible. For example, if Eve intercepted and tampered with a signature during the

transmission from Alice to Bob. This would also alter the states of the decoy particles inserted in $|s\rangle$. After Bob receives this signature with the randomly inserted decoy particles, he checks whether the attack exists using the locations and states of the decoy particles published by Alice in the verification phase. Clearly, Bob can detect the presence of interference in the quantum channel, and he discards the signature.

5.3 Unforgeability

The secret keys d and t are established between Alice and Bob using an unconditionally secure QKDP [38, 39], which inherently secures the keys against any adversary during distribution. Thus, the access to the secret keys d and t in the initializing phase cannot be achieved. This security guarantee is further strengthened by the information-theoretic indistinguishability established in Section 5.1: the quantum signature $|w\rangle$ reveals no information about the keys; no adversary can acquire the keys d and t. Besides, the decoy particles were employed to ensure the secure transmission of the signature; any attempt to tamper with the signature or the message will be detected. Therefore, the forgery attack on our scheme fails.

5.4 Impersonation attack

It is infeasible for an adversary to impersonate the partners in any phase. To begin with, it is impossible for Eve to impersonate Alice during the signature phase, because our QDVS scheme is unforgeable, which has been demonstrated in section 5.3. It is also infeasible for Eve to impersonate Bob during the verification phase, because only the designated verifier Bob possesses the secret keys t and d. As a result, Bob is the only party capable of verifying the quantum signature.

5.5 Designated verification property

In our QDVS scheme, the verification requires the secret keys t and d. Crucially, only the designated verifier Bob possesses these keys; hence, no one but Bob can verify the quantum signature. Therefore, our scheme satisfies the designated verification property.

5.6 Non-transferability

For the non-transferability property of our QDVS scheme, the designated verifier Bob must be capable of simulating the signer's quantum signature. In the following, we show the procedure by which Bob generates the same quantum signature as Alice.

Based on the secret key d and t, Bob applies the operations Y^{d_i} and H^{t_i} on $|m_i\rangle$ $(i = 1, 2, \ldots, n)$, yielding the final state $|s\rangle = \otimes_{i=1}^{n}|s_i\rangle$, where $|s_i\rangle = Y^{d_i}H^{t_i}|m_i\rangle$.

Given the signing algorithm in section 4.2 and Bob's simulation process above, the quantum signatures generated by Alice and Bob are provably identical and therefore indistinguishable. It follows directly from this that Bob cannot convince a third party of the signature's origin, thus ensuring the non-transferability of our QDVS scheme.

5.7 Hiding source

In our scheme, both the signer and the designated verifier can generate identical signatures. Since the signatures are provably identical, no outside party can distinguish the signer's signature from the verifier's simulated one, even if the secret keys are disclosed. Consequently, our QDVS has the hiding source property.

6 Conclusion

In this paper, we demonstrated that Xin et al.'s scheme [29] is vulnerable to forgery attacks. To remedy this, we proposed an improved scheme based on single particles. Our scheme eliminates the need for a trusted third center and is easier to implement compared with Xin et al.'s scheme [29]. The security analysis confirms that the proposed scheme is secure against common attacks such as intercept-resending, forgery, and impersonation attacks.

Acknowledgments

This work is supported by the Shenzhen Polytechnic University Research Fund (Grant No. 6024310040K), Research Projects of Department of Education of Guangdong Province (Grant No. 2023ZDZX1081), and the National Natural Science Foundation of China (Grant No. 62471187).

References

[1] Diffie, W.: New direction in cryptography. IEEE Trans. Inform. Theory **22**, 472–492 (1976)

[2] Jakobsson, M., Sako, K., Impagliazzo, R.: Designated verifier proofs and their applications. In: International Conference on the Theory and Applications of Cryptographic Techniques, pp. 143–154 (1996). Springer

[3] Lee, J.-S., Chang, J.H., Lee, D.H.: Forgery attacks on kang et al.'s identity-based strong designated verifier signature scheme and its improvement with security proof. Computers & Electrical Engineering **36**(5), 948–954 (2010)

[4] Kang, B., Boyd, C., Dawson, E.: A novel identity-based strong designated verifier signature scheme. Journal of Systems and Software **82**(2), 270–273 (2009)

[5] Chow, S.S.: Identity-based strong multi-designated verifiers signatures. In: European Public Key Infrastructure Workshop, pp. 257–259 (2006). Springer

[6] Laguillaumie, F., Vergnaud, D.: Multi-designated verifiers signatures: anonymity without encryption. Information Processing Letters **102**(2-3), 127–132 (2007)

[7] Duan, C., Su, L.: Designated verifier multisignature schemes based on elgamal scheme. Comput Eng Appl **43**, 153–156 (2007)

[8] Li, N., Wang, S.-P., Zhang, Y.-L., Wang, X.: Multi-signers strong designated verifier signature scheme. Jisuanji Gongcheng yu Yingyong(Computer Engineering and Applications) **46**(36), 105–108 (2010)

[9] DU, H.-z., WEN, Q.-y.: Certificateless strong designated verifier multi-signature. Journal on Communications **37**(6), 20–28 (2016)

[10] Zuo, W., Liu, Y., Wang, S.: An id-based designated-verifier proxy multi-signature scheme. In: 2012 Fourth International Conference on Multimedia Information Networking and Security, pp. 576–579 (2012). IEEE

[11] Tan, C., Chen, Y., Wu, Y., He, X., Li, T.: A designated verifier multi-signature scheme in multi-clouds. Journal of Cloud Computing **11**(1), 61 (2022)

[12] Weiping, Z., Caifen, W., Xiaoya, Y.: A designated-verifier proxy multi-signature scheme with message recovery. Journal of Wuhan University: Natural Science Edition **54**(05), 561–564 (2008) https://doi.org/10.14188/j.1671-8836.2008.05.020

[13] Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review **41**(2), 303–332 (1999)

[14] Huang, Y., Su, Z., Zhang, F., Ding, Y., Cheng, R.: Quantum algorithm for solving hyperelliptic curve discrete logarithm problem. Quantum Information Processing **19**(2) (2020)

[15] Bennett, C.H., Brassard, G., et al.: Proceedings of the ieee international conference on computers, systems and signal processing. IEEE New York (1984)

[16] Gottesman, D., Chuang, I.: Quantum digital signatures. arXiv preprint quant-ph/0105032 (2001)

[17] Zeng, G., Keitel, C.H.: Arbitrated quantum-signature scheme. Physical review A **65**(4), 042312 (2002)

[18] Zhang, Y., Zeng, J.: An improved arbitrated quantum scheme with bell states. International Journal of Theoretical Physics **57**(4), 994–1003 (2018)

[19] Jiang, D.-H., Xu, Y.-L., Xu, G.-B.: Arbitrary quantum signature based on local indistinguishability of orthogonal product states. International Journal of Theoretical Physics **58**(3), 1036–1045 (2019)

[20] Lou, X., Tang, W., Long, H., Cheng, Y.: A quantum blind signature scheme based on block encryption and quantum fourier transfer. International Journal of Theoretical Physics **58**(10), 3192–3202 (2019)

[21] Xing, K., Yin, A.-H., Xue, Y.-Q.: A quantum blind signature scheme based on dense coding for non-entangled states. Chinese Physics B **33**(6), 060309 (2024)

[22] Xiaojun, W.: An e-payment system based on quantum group signature. Physica Scripta **82**(6), 065403 (2010)

[23] Feng, Y., Zhou, J., Li, J., Zhao, W., Shi, J., Shi, R., Li, W.: Skc-ccco: an encryption algorithm for quantum group signature. Quantum Information Processing **21**(9) (2022)

[24] Zhang, J.-L., Zhang, J.-Z., Xie, S.-C.: Improvement of a quantum proxy blind signature scheme. International Journal of Theoretical Physics **57**(6), 1612–1621 (2018)

[25] Chen, J.-J., You, F.-C., Li, Z.-Z.: Quantum multi-proxy blind signature based on cluster state. Quantum Information Processing **21**(3), 104 (2022)

[26] Shi, W.-M., Zhou, Y.-H., Yang, Y.-G.: A real quantum designated verifier signature scheme. International Journal of Theoretical Physics **54**(9), 3115–3123 (2015)

[27] Shi, W.-M., Wang, Y.-M., Zhou, Y.-H., Yang, Y.-G., Zhang, J.-B.: A scheme on converting quantum signature with public verifiability into quantum designated verifier signature. Optik **164**, 753–759 (2018)

[28] Rong, M., Xin, X., Li, F.: Quantum signature for designated verifier with strong security. Acta Physica Sinica **69**, 190302 (2020)

[29] Xin, X., Wang, Z., Yang, Q., Li, F.: Quantum designated verifier signature based on bell states. Quantum Information Processing **19**(3) (2020)

[30] Xin, X., Ding, L., Li, C., Sang, Y., Yang, Q., Li, F.: Quantum public-key designated verifier signature. Quantum Information Processing **21**(1), 33 (2022)

[31] Zhang, L., Zhang, J.-H., Xin, X.-J., Li, C.-Y.: Quantum designated verifier signature without third party. Quantum Information Processing **22**(12), 452 (2023)

[32] Zhang, L., Zhang, J.-H., Xin, X.-J., Huang, M., Li, C.-Y.: Semi-quantum designated verifier signature scheme. International Journal of Theoretical Physics **62**(12), 254 (2023)

[33] Zhang, L., Zhang, J.-H., Xin, X.-J., Huang, M., Li, C.-Y.: Quantum designated multi-verifier signature. International Journal of Theoretical Physics **63**(1), 11 (2024)

[34] Zhang, L., Gui, Q., Xin, X.J., Li, C.Y., Gong, L.: Quantum designated verifier multi-signature scheme without arbitrator. Physica Scripta **100**(7), 075107 (2025)

[35] Li, X.-F., Jiang, D.-H., Yang, Y.-G., Xu, G.-B.: Quantum designated verifier signature scheme based on lagrange interpolation. Chinese Physics B **35**(4), 040304 (2026)

[36] Gao, F., Qin, S.-J., Guo, F.-Z., Wen, Q.-Y.: Cryptanalysis of quantum secure direct communication and authentication scheme via bell states. Chinese Physics Letters **28**(2), 020303 (2011)

[37] Xin, X., Wang, Z., Yang, Q., Li, F.: Identity-based quantum designated verifier signature. International Journal Of Theoretical Physics **59**(3), 918–929 (2020)

[38] Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. Theoretical computer science **560**, 7–11 (2014)

[39] Long, G.-L., Liu, X.-S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Physical Review A **65**(3), 032302 (2002)

[40] Deng, F.-G., Long, G.L., Liu, X.-S.: Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block. Physical Review A **68**(4), 042317 (2003)

[41] Ekert, A.K.: Quantum cryptography based on bell's theorem. Physical review letters **67**(6), 661 (1991)

[42] Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC press, Boca Raton (1996)

[43] Yang, L., Yang, B., Pan, J.: Quantum public-key encryption protocols with information-theoretic security. In: Quantum Optics II, vol. 8440, pp. 71–77 (2012). SPIE

[44] Li, Y., Chong, X., Bao, L.: Quantum probabilistic encryption scheme based on conjugate coding. China Communications **10**(2), 19–26 (2013)