Design and Analysis of Quantum Designated Verifier Signature Scheme

Shanu Poddar[1*] and Vikas Srivastava[2*]

[1*]Department of Computer Science and Engineering, Shiv Nadar Institution of Eminence, Delhi NCR, 201314, India.
[2*]Department of Mathematics, National Institute of Technology Warangal, Hanamkonda, 506004, Telangana, India.

*Corresponding author(s). E-mail(s): sp179@snu.edu.in; vsv@nitw.ac.in;

Abstract

Designated Verifier Signatures (DVS) are an important variant of digital signatures that ensure only a specified verifier can validate a signature, while preserving non-transferability. With the advent of quantum computing, several quantum DVS schemes have been proposed to achieve quantum security. In this paper, we revisit the quantum DVS protocol of Xin et al. [*Quantum Information Processing, 2022*] and provide a structural cryptanalysis of its design. We show that the scheme admits an existential forgery under a chosen-message attack: given a valid quantum signature on one message, an adversary can efficiently transform it into a valid signature on another message without knowledge of the signer's private key. To address this weakness, we propose a minimal countermeasure based on QKD-derived keys and quantum one-time pad encryption. Our findings highlight the importance of protocol-level cryptanalysis for the secure deployment of quantum information technologies.

Keywords: Quantum Signatures, Designated Verifier Signatures, Cryptanalysis, Quantum One-Way Functions, Quantum One-Time Pad

1 Introduction

The widespread use of the Internet has made secure message authentication and integrity protection a major concern. The concept of digital signatures, first introduced by Diffie and Hellman in 1976 [1], addresses this problem by enabling a signer to generate a signature with a private key that can later be verified using the corresponding

public key. Classical digital signature schemes typically rely on hardness assumptions such as the discrete logarithm and integer factorization problems. However, the advent of quantum computing threatens these foundations, since Shor's algorithm can efficiently solve both problems.

To counter this, *quantum signature schemes* have been proposed, which utilize the principles of quantum mechanics rather than computational hardness. Such schemes promise security even in the presence of quantum adversaries. Broadly, quantum signature constructions follow two approaches: symmetric-key and public-key. Symmetric-key variants generally require a trusted third party and often employ techniques such as quantum key distribution or entangled states. Public-key approaches, first proposed by Gottesman and Chuang [2], are instead based on quantum one-way functions (QOWFs). Later extensions included the use of single-qubit rotations and other quantum transformations. Despite their conceptual elegance, several such proposals have been shown to suffer from structural or security limitations. Notable improvements were subsequently made through frameworks such as Kawachi et al. [3], as well as identity-based extensions [4–7] that offer greater flexibility but still depend on a fully trusted third party. Meanwhile, experimental progress has also been impressive [8–11]. These milestones highlight the growing feasibility of practical quantum signatures.

Beyond secure message authentication, quantum signature protocols are expected to become important building blocks for future quantum information and communication infrastructures. They can support authenticated communication over quantum networks, secure distributed quantum computing, quantum cloud services, and other applications where both quantum information processing and authentication are required. As experimental quantum communication technologies continue to mature, ensuring the security of the underlying quantum cryptographic protocols becomes increasingly important. Consequently, rigorous cryptanalysis of quantum signature protocols is essential for identifying subtle protocol-level vulnerabilities before their deployment in practical quantum communication systems.

A key variant of digital signatures, particularly relevant to applications such as e-voting and digital contracts, is the *Designated Verifier Signature* (DVS) scheme. In DVS, only a specified verifier can validate the authenticity of a message-signature pair. Crucially, DVS guarantees *non-transferability*: the designated verifier cannot convince others of the validity of a signature, as he can always simulate a valid-looking signature himself. This distinguishes DVS from classical digital signatures, which inherently provide non-repudiation. The first quantum DVS scheme was proposed by Shi et al. [12, 13], and several subsequent constructions have followed [14–18, 18–20]. Nonetheless, the design of an efficient and secure quantum DVS scheme remains an active research problem.

Motivation. While proposing new constructions is important, *cryptanalysis* of existing protocols is equally critical for the long-term development of secure primitives. Careful analysis helps to identify potential weaknesses at an early stage, thereby preventing insecure schemes from being adopted and informing the design of stronger

ones. With the steady growth of quantum DVS proposals in recent years [14–18, 18–22], it becomes important to rigorously assess their security of quantum DVS. In this work, we revisit the DVS scheme proposed by Xin et al. [22] and show that it contains a structural vulnerability that permits signature forgery. We demonstrate how an adversary can transform a valid signature on one message into a valid signature on another message, thereby undermining the unforgeability of the scheme. We further propose a minimal countermeasure that removes the identified vulnerability while preserving the overall structure of the original protocol. More broadly, this work highlights the importance of protocol-level cryptanalysis in the development of secure quantum information technologies, where even subtle design flaws may compromise the security guarantees of otherwise well-founded quantum primitives.

Our Contribution The main contributions of this paper can be summarized as follows:

- We revisit the DVS scheme of Xin et al. [22] and point out a structural aspect of the design that can be exploited by an adversary.
- We present a concrete forgery attack that allows an adversary who has access to a valid message-signature pair to forge a valid signature on another message without access to the signer's private key. We also present a detailed security analysis of Xin et al. [22] protocol with respect to other attack models such as replay attacks and collusion attacks between dishonest participants. In particular, we have shown that Xin et al.'s DVS [22] is also not secure against replay attacks and collusion attacks.
- We further propose a minimal protocol modification based on quantum key distribution (QKD), keyed hashing, and quantum one-time pad encryption that eliminates the identified forgery attack while preserving the designated-verifier functionality. The resulting construction is analysed with respect to the standard security properties of designated verifier signatures and compared with existing quantum DVS schemes.

Organization of the Paper: Section 1 introduces the problem setting and our motivation for cryptanalysis. Section 2 discusses the preliminaries and standard security notions for a DVS. Section 3 formally describes Xin et al.'s [22] quantum DVS protocol; for concreteness, Subsection 3.1 presents a worked toy example that we later reuse. Section 4 develops our forgery attack in full generality, and Subsection 4.1 demonstrates the attack concretely on the toy instance. Section 4.2 presents a detailed analysis of Xin et al. [22] with respect to other attack models. Finally, Section 5 discusses minimal countermeasures based on QKD-derived hashing quantum one-time pad encryption [23]. In addition, security analysis and performance analysis of the proposed DVS is described in Section 5.1 and 5.2 respectively.

2 Preliminaries and Security Notions

In this section, we recall the basic syntax and security requirements of a DVS. A DVS scheme consists of the following algorithms:

$$\mathsf{Setup}, \quad \mathsf{KeyGen}, \quad \mathsf{SignDVS}, \quad \mathsf{VerifyDVS}.$$

The signer Anna and the designated verifier Tom generate their respective secret and public information during the key-generation phase. Given a message m, Anna runs $\mathsf{SignDVS}$ and produces a designated-verifier signature σ_m. The verifier Tom runs $\mathsf{VerifyDVS}$ on the pair (m, σ_m), or on an equivalent protocol-dependent representation from which the message is recovered, and outputs either accept or reject. A DVS scheme is correct if, for every honestly generated key pair and every message m, a signature σ_m generated honestly by the signer is accepted by the designated verifier. That is,

$$\mathsf{VerifyDVS}(m, \sigma_m) = 1$$

for every honestly generated signature σ_m.

We now discuss the security notions of unforgeability and non-transferability. A detailed discussion on other security notions of DVS can be found in [24–29].

Unforgeability

The unforgeability requirement for a DVS scheme is defined as a security experiment between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ as follows.

- The challenger $\mathcal{C}$ takes a security parameter k and runs $cp \leftarrow \mathsf{Setup}(k)$, where cp denotes the common public parameters of the scheme.
- The challenger generates the key pairs of the signer and the designated verifier as $(\mathsf{PK}_S, \mathsf{SK}_S) \leftarrow \mathsf{KeyGen}(k, cp)$, $(\mathsf{PK}_D, \mathsf{SK}_D) \leftarrow \mathsf{KeyGen}(k, cp)$. It gives cp, PK_S, and PK_D to the adversary $\mathcal{A}$, while keeping SK_S and SK_D secret.
- The adversary $\mathcal{A}$ may adaptively query a signing oracle on any message m_i of its choice. For each such query, the challenger returns $\sigma_i \leftarrow \mathsf{Sign}(cp, \mathsf{SK}_S, m_i, \mathsf{PK}_D)$. The adversary is allowed to make at most q_s such signing queries.
- Eventually, $\mathcal{A}$ outputs a message–signature pair (m^*, σ^*). The adversary wins the experiment if $\mathsf{Verify}(cp, \mathsf{PK}_S, \mathsf{PK}_D, m^*, \sigma^*) = \mathsf{accept}$, and m^* was not previously submitted to the signing oracle.

The success probability of $\mathcal{A}$ in the above experiment is denoted by

$$\mathsf{Succ}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{DVS},\mathcal{A}}(k).$$

Definition 1 (Unforgeability) A DVS scheme is said to be existentially unforgeable under adaptive chosen-message attack, or (t, ε)-EUF-CMA secure, if for every probabilistic polynomial-time adversary $\mathcal{A}$ running in time at most t and making at most q_s signing queries, we have

$$\mathsf{Succ}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{DVS},\mathcal{A}}(k) \leq \varepsilon,$$

where ε is negligible in the security parameter k.

Non-transferability

The non-transferability property captures the fact that a DVS signature should not convince any third party of the signer's authorship. This is because the designated

verifier can generate a simulated signature that is computationally indistinguishable from a genuine signature produced by the signer. Therefore, any third party will not be able to determine whether a given DVS signature was produced by the signer or simulated by the designated verifier.

Formally, non-transferability is defined through the following game between a distinguisher $\mathcal{D}$ and a challenger $\mathcal{C}$.

- The challenger $\mathcal{C}$ takes a security parameter k and runs $cp \leftarrow \mathsf{Setup}(k)$, where cp denotes the common public parameters.
- The challenger generates the key pairs of the signer and the designated verifier as $(\mathsf{PK}_S, \mathsf{SK}_S) \leftarrow \mathsf{KeyGen}(k, cp)$, $(\mathsf{PK}_D, \mathsf{SK}_D) \leftarrow \mathsf{KeyGen}(k, cp)$. It gives cp, PK_S, and PK_D to the distinguisher $\mathcal{D}$, while keeping SK_S and SK_D secret.
- The distinguisher $\mathcal{D}$ may adaptively make signing queries on messages m_i of its choice. For each query, the challenger returns $\sigma_i \leftarrow \mathsf{Sign}(cp, \mathsf{SK}_S, m_i, \mathsf{PK}_D)$.
- At some point, $\mathcal{D}$ submits a fresh challenge message m^* to $\mathcal{C}$. The challenger chooses a random bit $b \xleftarrow{\$} \{0,1\}$. If $b = 0$, the challenger computes a genuine DVS signature $\sigma^* \leftarrow \mathsf{Sign}(cp, \mathsf{SK}_S, m^*, \mathsf{PK}_D)$. If $b = 1$, the challenger computes a simulated DVS signature $\sigma^* \leftarrow \mathsf{Simulation}(cp, \mathsf{SK}_D, m^*, \mathsf{PK}_S)$. The challenger sends σ^* to $\mathcal{D}$.
- After receiving the challenge signature, $\mathcal{D}$ may continue to make signing queries, but it is not allowed to query the challenge message m^*.
- Finally, $\mathcal{D}$ outputs a bit b'. The distinguisher wins the game if $b' = b$.

The advantage of $\mathcal{D}$ in the above adaptive chosen-message distinguishing game is defined as

$$\mathsf{Adv}^{\mathsf{DCMA}}_{\mathsf{DVS},\mathcal{D}}(k) = \left| \Pr[b' = b] - \frac{1}{2} \right|.$$

Definition 2 (Non-transferability) A DVS scheme is said to satisfy non-transferability against a (t, q_s) adaptive chosen-message distinguisher $\mathcal{D}$ if

$$\mathsf{Adv}^{\mathsf{DCMA}}_{\mathsf{DVS},\mathcal{D}}(k)$$

is negligible for every probabilistic polynomial-time distinguisher $\mathcal{D}$ running in time at most t and making at most q_s signing queries.

3 Quantum DVS Scheme of Xin et al.

Before presenting our cryptanalysis, we first give a detailed description of the DVS scheme proposed by Xin et al. [22]. The protocol proceeds in three phases: (1) Init-KeyGen, (2) signDVS, and (3) verifDVS. For completeness, we outline each phase below.

Init-KeyGen*:* Let H be one-way hash function $H : \{0,1\}^* \mapsto \{0,1\}^l$. Let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ be the quantum operators. For rotations, define $Y = i(|1\rangle\langle 0| - |0\rangle\langle 1|)$

and $R(\theta) = e^{-i\theta Y/2}$ such that $R(\theta)|0\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)|1\rangle$. Let $\theta_n = \pi/2^{n-1}$ for security parameter $n \gg 1$, and define the quantum one-way function (QOWF):

$$s \mapsto |f(s)\rangle = R(s\theta_n)|0\rangle.$$

- Signer (Anna) picks private vector $a = (a_1, \ldots, a_l)$ with $a_i \in \mathbb{Z}_{2^n}$, computes public key $|f(a)\rangle = \otimes_{i=1}^{l} |f(a_i)\rangle$.
- Verifier (Tom) picks private $b = (b_1, \ldots, b_l)$, computes $|f(b)\rangle = \otimes_{i=1}^{l} |f(b_i)\rangle$.

signDVS*:* Given message $m = (m_1, \ldots, m_l) \in \{0,1\}^l$, signing involves the following steps:

S1*:* Tom prepares $2q$ copies of $|f(b)\rangle$, adds decoy particles, and sends them to Anna.
S2*:* Tom reveals decoy positions; Anna checks the channel and extracts valid copies.
S3*:* Anna repeats the process to send $2q$ copies of $|f(a)\rangle$ to Tom.
S4*:* Anna uses Tom's public key to compute a joint state. For each component $|f(b_i)\rangle$, she applies $R(a_i\theta_n)$ and obtains

$$|f(a+b)\rangle = \otimes_{i=1}^{l} |f(a_i + b_i)\rangle.$$

S5*:* Anna computes the hash $h = H(m\|ID_A\|ID_T) = (h_1, h_2, \ldots, h_l)$. She modifies each $|f(a_i + b_i)\rangle$ depending on h_i. The resulting state is

$$|f_m(a+b)\rangle = \otimes_{i=1}^{l} |f_{m_i}(a_i + b_i)\rangle,$$

where

$$|f_{m_i}(a_i + b_i)\rangle = \begin{cases} |f(a_i + b_i)\rangle, & h_i = 0, \\ X|f(a_i + b_i)\rangle, & h_i = 1. \end{cases}$$

S6*:* Anna encodes the message m into a quantum state

$$|w\rangle = \otimes_{i=1}^{l} |w_i\rangle,$$

using h to determine the encoding rule:

$$|w_i\rangle = \begin{cases} |0\rangle, & h_i = 0, m_i = 0, \\ |1\rangle, & h_i = 0, m_i = 1, \\ |+\rangle, & h_i = 1, m_i = 0, \\ |-\rangle, & h_i = 1, m_i = 1, \end{cases}$$

where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.
S7*:* Anna sends the quantum signature

$$\left\{ \otimes_{i=1}^{2q} |f_m(a+b)\rangle,\ |w\rangle \right\}$$

to Tom via the public quantum channel.

verifDVS*:* The verification proceeds in the following manner.

V1*:* Using the $2q$ copies of Anna's public key $|f(a)\rangle$ received earlier, Tom applies $R(b_i\theta_n)$ to each $|f(a_i)\rangle$ to obtain $|f'(a+b)\rangle = \otimes_{i=1}^{l}|f'(a_i+b_i)\rangle$.
V2A*:* Tom compares the first q copies of $|f'(a_i+b_i)\rangle$ with $|f_{m_i}(a_i+b_i)\rangle$ using quantum state comparison techniques. If they are equal, he sets $h'_i = 0$. Otherwise, he proceeds to the next step.
V2B*:* Tom applies X to the remaining q copies of $|f'(a_i+b_i)\rangle$ to obtain $|f''(a_i+b_i)\rangle$. He then compares these with the unused copies of $|f_{m_i}(a_i+b_i)\rangle$. If equality holds, he sets $h'_i = 1$. If neither comparison succeeds, he sets $h'_i = \perp$, rejects the signature, and aborts. In summary:

$$h'_i = \begin{cases} 0, & |f'(a_i+b_i)\rangle = |f_{m_i}(a_i+b_i)\rangle, \\ 1, & |f''(a_i+b_i)\rangle = |f_{m_i}(a_i+b_i)\rangle, \\ \perp, & \text{otherwise (reject signature).} \end{cases}$$

V3*:* If no rejection occurs, Tom has $h' = (h'_1, h'_2, \ldots, h'_l)$. He now measures each $|w_i\rangle$ depending on h'_i. If $h'_i = 0$, the measurement basis is $\{|0\rangle, |1\rangle\}$; if $h'_i = 1$, the basis is $\{|+\rangle, |-\rangle\}$. Tom decodes the bit as

$$m'_i = \begin{cases} 0, & |w_i\rangle = |0\rangle \text{ or } |+\rangle, \\ 1, & |w_i\rangle = |1\rangle \text{ or } |-\rangle. \end{cases}$$

Finally, Tom reconstructs $m' = (m'_1, m'_2, \ldots, m'_l)$ and verifies whether $H(m' \| ID_A \| ID_T) = h'$. If the condition holds, the signature is accepted; otherwise, it is rejected.

3.1 Toy Example

To better illustrate the working of Xin et al.'s protocol, we now present a small toy instance with concrete parameter values. This example demonstrates how the signer generates a signature, how the verifier obtains the verification string h', and how the message is finally recovered and checked. Later, in Section 4, we will refer back to this toy example to show explicitly how the forgery attack can be carried out.

Init-KeyGen: We fix the parameters as follows:

$$n = 4 \;\Rightarrow\; \theta_n = \frac{\pi}{2^{n-1}} = \frac{\pi}{8}, \qquad l = 4, \qquad q = 2.$$

Anna's private rotation vector is $a = (a_1, a_2, a_3, a_4) = (1, 3, 2, 0)$, and Tom's private rotation vector is $b = (b_1, b_2, b_3, b_4) = (2, 1, 3, 1)$. Anna's quantum public key

is $|f(a)\rangle = |f(1)\rangle \otimes |f(3)\rangle \otimes |f(2)\rangle \otimes |f(0)\rangle$, while Tom's quantum public key is $|f(b)\rangle = |f(2)\rangle \otimes |f(1)\rangle \otimes |f(3)\rangle \otimes |f(1)\rangle$. The joint state is $|f(a+b)\rangle = |f(3)\rangle \otimes |f(4)\rangle \otimes |f(5)\rangle \otimes |f(1)\rangle$.

signDVS: Suppose Anna wants to sign the message $m = (1, 0, 1, 0)$. The hash is computed as

$$h = H(m \| ID_A \| ID_T) = (0, 1, 1, 0) \quad (say).$$

For each component of $|f(a+b)\rangle$, Anna modifies according to h:

$$|f_m(a+b)\rangle = |f_{m_1}(a_1 + b_1)\rangle \otimes |f_{m_2}(a_2 + b_2)\rangle \otimes |f_{m_3}(a_3 + b_3)\rangle \otimes |f_{m_4}(a_4 + b_4)\rangle$$

$$= |f(3)\rangle \otimes X|f(4)\rangle \otimes X|f(5)\rangle \otimes |f(1)\rangle.$$

She prepares $2q = 4$ copies of this state. Anna also encodes the message into the quantum state $|w\rangle$ based on h:

$$|w\rangle = |1\rangle \otimes |+\rangle \otimes |-\rangle \otimes |0\rangle,$$

where $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Finally, she sends the quantum signature

$$\left\{ \otimes_{i=1}^{4} |f_m(a+b)\rangle,\ |w\rangle \right\}$$

to Tom.

verifDVS: Tom reconstructs the expected joint state using Anna's public key and his private key:

$$|f'(a+b)\rangle = |f(3)\rangle \otimes |f(4)\rangle \otimes |f(5)\rangle \otimes |f(1)\rangle.$$

To recover the verification string h', Tom compares each component $|f'(a_i+b_i)\rangle$ against the corresponding part of the received state $|f_m(a_i + b_i)\rangle$:

$$h'_i = \begin{cases} 0, & \text{if } |f'(a_i + b_i)\rangle = |f_{m_i}(a_i + b_i)\rangle, \\ 1, & \text{if } X|f'(a_i + b_i)\rangle = |f_{m_i}(a_i + b_i)\rangle, \\ \perp, & \text{if neither condition holds (reject).} \end{cases}$$

In this toy example, the component-wise comparisons succeed as follows:

$$\begin{aligned} |f'(a_1 + b_1)\rangle = |f(3)\rangle = |f_{m_1}(3)\rangle \quad &\Rightarrow \quad h'_1 = 0, \\ X|f'(a_2 + b_2)\rangle = X|f(4)\rangle = |f_{m_2}(4)\rangle \quad &\Rightarrow \quad h'_2 = 1, \\ X|f'(a_3 + b_3)\rangle = X|f(5)\rangle = |f_{m_3}(5)\rangle \quad &\Rightarrow \quad h'_3 = 1, \\ |f'(a_4 + b_4)\rangle = |f(1)\rangle = |f_{m_4}(1)\rangle \quad &\Rightarrow \quad h'_4 = 0. \end{aligned}$$

Therefore, Tom reconstructs the string

$$h' = (0, 1, 1, 0).$$

With h' determined, Tom measures each component of $|w\rangle$ in the correct basis:

$$\begin{aligned}
h'_1 = 0 &\Rightarrow \text{measure in } \{|0\rangle, |1\rangle\}, \quad |w_1\rangle = |1\rangle \Rightarrow m'_1 = 1,\\
h'_2 = 1 &\Rightarrow \text{measure in } \{|+\rangle, |-\rangle\}, \quad |w_2\rangle = |+\rangle \Rightarrow m'_2 = 0,\\
h'_3 = 1 &\Rightarrow \text{measure in } \{|+\rangle, |-\rangle\}, \quad |w_3\rangle = |-\rangle \Rightarrow m'_3 = 1,\\
h'_4 = 0 &\Rightarrow \text{measure in } \{|0\rangle, |1\rangle\}, \quad |w_4\rangle = |0\rangle \Rightarrow m'_4 = 0.
\end{aligned}$$

Tom reconstructs

$$m' = (1, 0, 1, 0).$$

Finally, he checks consistency:

$$H(m' \| ID_A \| ID_T) \stackrel{?}{=} h'.$$

Since equality holds, the signature is accepted.

4 Forgery Attack on Xin et al. DVS

The security of a quantum cryptographic protocol depends not only on the security of its underlying quantum primitives but also on the correctness of the protocol composition. Even when quantum one-way functions and quantum state transmission remain secure, improper integration of these components may introduce exploitable structural vulnerabilities. We therefore examine the protocol of Xin et al. [22] from a protocol-design perspective rather than from the viewpoint of breaking the underlying quantum assumptions.

We now revisit the unforgeability argument of Xin et al. [22]. In Section 3.6 of their paper, Xin et al. argue that an adversary who wants to forge a signature on a new message m^* must be able to compute the joint state

$$|f(a+b)\rangle,$$

which is treated as a secret quantum Diffie–Hellman-type key derived from the quantum public keys $|f(a)\rangle$ and $|f(b)\rangle$. Since this state cannot be computed without knowing either Anna's private key a or Tom's private key b, they conclude that no quantum adversary can generate a valid forgery.

However, this argument only rules out a *from-scratch forgery*, where the adversary attempts to generate a fresh valid signature without having access to any previously valid message-signature pair. This is not sufficient for the standard unforgeability requirement of a DVS. As recalled in Section 2, unforgeability must also consider the case where the adversary is given a valid message-signature pair (m, σ_m).
We demonstrate that the quantum DVS scheme of [22] is *forgeable*. Given a valid quantum signature on a message m, an adversary can transform it into a valid quantum signature on another message $\bar{m}$ without access to Anna's private key. Hence the scheme is malleable and does not satisfy the standard unforgeability definition of a DVS.

Step 1: The adversary obtains Anna's quantum signature

$$\left\{\otimes_{i=1}^{2q}|f_m(a+b)\rangle,\ |w\rangle\right\}$$

corresponding to the message m.
Step 2: The adversary chooses a new target message $\bar{m} = (\bar{m}_1, \ldots, \bar{m}_l)$ on which he wishes to forge Anna's signature.
Step 3: He computes the new hash

$$\bar{h} = H(\bar{m}\|ID_A\|ID_T) = (\bar{h}_1, \ldots, \bar{h}_l).$$

Step 4: For each i, compare $\bar{h}_i$ with the original h_i (derived from m). If $\bar{h}_i \oplus h_i = 1$, the adversary applies the Pauli X gate to the i-th component of the quantum state $|f_m(a+b)\rangle$; otherwise, he does nothing. This transforms

$$|f_m(a+b)\rangle \quad \mapsto \quad |f_{\bar{m}}(a+b)\rangle.$$

Step 5: The adversary similarly encodes the message $\bar{m}$ into a quantum state

$$|\bar{w}\rangle = \otimes_{i=1}^{l}|\bar{w}_i\rangle,$$

using $\bar{h}$ to choose the encoding basis (computational if $\bar{h}_i = 0$, Hadamard if $\bar{h}_i = 1$).

Thus, the adversary outputs the forged quantum signature

$$\left\{\otimes_{i=1}^{2q}|f_{\bar{m}}(a+b)\rangle,\ |\bar{w}\rangle\right\},$$

which will pass verification for the new message $\bar{m}$. This shows that the scheme admits existential forgery under a chosen-message attack.

4.1 Toy Example of Forgery

Recall from the toy example (refer section 3.1) that for $m = (1, 0, 1, 0)$ we have

$$h = (0, 1, 1, 0), \qquad |f_m(a+b)\rangle = |f(3)\rangle \otimes X|f(4)\rangle \otimes X|f(5)\rangle \otimes |f(1)\rangle,$$

and the transmitted package is $\left\{\otimes_{i=1}^{4}|f_m(a+b)\rangle,\ |w\rangle\right\}$ with

$$|w\rangle = |1\rangle \otimes |+\rangle \otimes |-\rangle \otimes |0\rangle.$$

Let the target message be

$$\bar{m} = (1, 1, 0, 0), \qquad \text{and say we obtain } \bar{h} = H(\bar{m}\|ID_A\|ID_T) = (0, 1, 1, 1).$$

The adversary computes the bitwise difference

$$\bar{h} \oplus h = (0,1,1,1) \oplus (0,1,1,0) = (0,0,0,1).$$

He applies a X to the *fourth* tensor component of each of the $2q = 4$ copies of the received state (and does nothing to the other components):

$$|f_m(a+b)\rangle \;\longmapsto\; |f_{\bar{m}}(a+b)\rangle = |f(3)\rangle \otimes X|f(4)\rangle \otimes X|f(5)\rangle \otimes X|f(1)\rangle,$$

which exactly matches the flip pattern prescribed by $\bar{h} = (0,1,1,1)$. He also re-encodes the message into

$$|\bar{w}\rangle = \bigotimes_{i=1}^{4} |\bar{w}_i\rangle, \quad |\bar{w}_1\rangle = |1\rangle \ (\bar{h}_1 = 0, \bar{m}_1 = 1),\ |\bar{w}_2\rangle = |-\rangle \ (\bar{h}_2 = 1, \bar{m}_2 = 1),$$

$$|\bar{w}_3\rangle = |+\rangle \ (\bar{h}_3 = 1, \bar{m}_3 = 0),\ |\bar{w}_4\rangle = |+\rangle \ (\bar{h}_4 = 1, \bar{m}_4 = 0),$$

so that

$$|\bar{w}\rangle = |1\rangle \otimes |-\rangle \otimes |+\rangle \otimes |+\rangle.$$

The forged signature that he outputs is

$$\Big\{ \otimes_{i=1}^{4} |f_{\bar{m}}(a+b)\rangle,\ |\bar{w}\rangle \Big\}.$$

Verification

Tom reconstructs the reference state as before:

$$|f'(a+b)\rangle = |f(3)\rangle \otimes |f(4)\rangle \otimes |f(5)\rangle \otimes |f(1)\rangle.$$

He derives $\bar{h}'$ componentwise by comparison:

$$\bar{h}'_i = \begin{cases} 0, & \text{if } |f'(a_i+b_i)\rangle = |f_{\bar{m}_i}(a_i+b_i)\rangle, \\ 1, & \text{if } X|f'(a_i+b_i)\rangle = |f_{\bar{m}_i}(a_i+b_i)\rangle, \\ \perp, & \text{otherwise (reject).} \end{cases}$$

In this case,

$$\begin{aligned} |f'(a_1+b_1)\rangle = |f(3)\rangle = |f_{\bar{m}_1}(3)\rangle &\Rightarrow \bar{h}'_1 = 0, \\ X|f'(a_1+b_1)\rangle = X|f(4)\rangle = |f_{\bar{m}_2}(4)\rangle &\Rightarrow \bar{h}'_2 = 1, \\ X|f'(a_1+b_1)\rangle = X|f(5)\rangle = |f_{\bar{m}_3}(5)\rangle &\Rightarrow \bar{h}'_3 = 1, \\ X|f'(a_1+b_1)\rangle = X|f(1)\rangle = |f_{\bar{m}_4}(1)\rangle &\Rightarrow \bar{h}'_4 = 1, \end{aligned}$$

hence

$$\bar{h}' = (0,1,1,1) = \bar{h}.$$

With $\bar{h}'$ known, Tom measures $|\bar{w}\rangle$ in the bases dictated by $\bar{h}'$:

$$\begin{aligned}
&\bar{h}'_1 = 0 : \{|0\rangle, |1\rangle\}, \quad |1\rangle \Rightarrow \bar{m}'_1 = 1, \\
&\bar{h}'_2 = 1 : \{|+\rangle, |-\rangle\}, \quad |-\rangle \Rightarrow \bar{m}'_2 = 1, \\
&\bar{h}'_3 = 1 : \{|+\rangle, |-\rangle\}, \quad |+\rangle \Rightarrow \bar{m}'_3 = 0, \\
&\bar{h}'_4 = 1 : \{|+\rangle, |-\rangle\}, \quad |+\rangle \Rightarrow \bar{m}'_4 = 0,
\end{aligned}$$

so that

$$\bar{m}' = (1, 1, 0, 0) = \bar{m}.$$

Finally, Tom verifies

$$H(\bar{m}' \| ID_A \| ID_T) \stackrel{?}{=} \bar{h}'.$$

Since equality holds, the forged signature is accepted.

4.2 Discussion of Other Attack Models

4.2.1 Collusion-Based Attack

We now discuss a collusion-based attack scenario. This discussion is motivated by the notion of *non-delegatability* in DVS. Lipmaa, Wang and Bao [27] introduced non-delegatability as an important security requirement for DVS. Informally, non-delegatability requires that neither the signer nor the designated verifier should be able to give a third party a restricted signing capability without revealing the corresponding secret key. Later works also studied designated verifier signature schemes satisfying non-delegatability [28, 29].
Consider the following collusion scenario. Suppose the signer Anna gives Linda a valid message-signature pair (m, σ_m), where

$$\sigma_m = \left\{ \bigotimes_{j=1}^{2q} |f_h(a+b)\rangle, \ |w_m\rangle \right\}, \qquad h = H(m \| ID_A \| ID_T).$$

Here Linda does not know Anna's private key a, Tom's private key b, or the unmodified joint state $|f(a+b)\rangle$. However, since Anna gives Linda the message m together with the corresponding quantum signature package, Linda can compute

$$h = H(m \| ID_A \| ID_T).$$

Now Linda chooses a fresh target message $\bar{m} \neq m$ and computes

$$\bar{h} = H(\bar{m} \| ID_A \| ID_T).$$

For each component i, she applies the public Pauli operation

$$X^{h_i \oplus \bar{h}_i}$$

to the i-th component of every copy of the received state $|f_h(a+b)\rangle$. Since $X^2 = I$, we obtain

$$X^{h_i \oplus \bar{h}_i} X^{h_i} |f(a_i + b_i)\rangle = X^{\bar{h}_i} |f(a_i + b_i)\rangle.$$

Hence Linda transforms the hash-dependent part of the original signature into the hash-dependent part required for the new message:

$$|f_h(a+b)\rangle \longmapsto |f_{\bar{h}}(a+b)\rangle.$$

She then prepares a fresh message register

$$|w_{\bar{m}}\rangle$$

according to the encoding rule of the protocol using $\bar{m}$ and $\bar{h}$. Therefore she obtains

$$\sigma_{\bar{m}} = \left\{ \bigotimes_{j=1}^{2q} |f_{\bar{h}}(a+b)\rangle,\ |w_{\bar{m}}\rangle \right\}.$$

During verification, Tom reconstructs the reference state $|f'(a+b)\rangle$, recovers $\bar{h}$ through the comparison procedure, measures $|w_{\bar{m}}\rangle$ in the bases determined by $\bar{h}$, obtains $\bar{m}$, and finally checks

$$H(\bar{m} \| ID_A \| ID_T) = \bar{h}.$$

Thus Tom accepts $\sigma_{\bar{m}}$ as a valid signature on $\bar{m}$. Linda can generate a valid signature on a fresh message without learning Anna's private key or Tom's private key. Thus, Xin et al. [22] is not secure against collusion based attack based on non-delegatibility security requirements.

4.2.2 Replay Attacks

In the signing phase, the hash value is computed as

$$h = H(m \| ID_A \| ID_T),$$

and no nonce, timestamp, session identifier, or verifier challenge is included. Therefore, if an adversary obtains a valid quantum signature package

$$\sigma_m = \left\{ \bigotimes_{j=1}^{2q} |f_h(a+b)\rangle,\ |w_m\rangle \right\},$$

the same package remains valid for the same message and the same identities as long as the quantum registers can be preserved and delivered to Tom.

This is not a cloning-based replay attack. The adversary cannot copy an unknown quantum signature state and use it many times. Rather, it is a delayed-delivery or

one-time replay attack: the adversary stores or delays the valid quantum package and presents it to Tom at a later time. Since the verification condition only checks

$$H(m'\|ID_A\|ID_T) = h',$$

Tom has no cryptographic way to determine whether the signature belongs to the current session or to an earlier execution of the protocol.

A standard countermeasure is to bind the signature to a fresh session value. For example, Tom may choose a fresh random nonce r_T, and Anna may compute

$$h = H(m\|ID_A\|ID_T\|r_T\|sid),$$

where sid is a session identifier. Tom should accept only if the nonce and session identifier are fresh and unused. This prevents an old quantum signature package from being accepted in a later protocol execution.

5 Probable Countermeasures to the Forgery Attack

Having identified the structural weakness responsible for the forgery attack, we now present a minimal modification that preserves the overall architecture of Xin et al.'s protocol [22] while eliminating the identified vulnerability. Rather than redesigning the complete quantum signature mechanism, the proposed modification introduces only lightweight cryptographic enhancements based on quantum key distribution, keyed hashing, and quantum one-time pad encryption. Consequently, the protocol remains compatible with the original design philosophy while achieving stronger security guarantees.

Anna and Tom run quantum key distribution (QKD) to obtain a shared key K. They fix a KDF/PRF KDF. Given m, Anna computes a *keyed* hash

$$\tilde{h} = H(m\|ID_A\|ID_T\|sid\|\rho_T\|K) \in \{0,1\}^l,$$

where sid and ρ_T denotes the session identifier and a verifier-generated nonce respectively.
She forms the flip pattern using $\tilde{h}$ (i.e., apply X to the ith component iff $\tilde{h}_i = 1$) and produces

$$|f_{\tilde{h}}(a{+}b)\rangle \;=\; \bigotimes_{i=1}^{l} \big(X^{\tilde{h}_i} |f(a_i{+}b_i)\rangle \big).$$

Next, she derives quantum one–time pad (QOTP) keys from K and $\tilde{h}$:

$$(r, s) = \mathsf{KDF}(K, \tilde{h}\|sid\|\rho_T) \in \{0,1\}^l \times \{0,1\}^l.$$

She encodes m into $|w\rangle$ using the *public* basis rule determined by $\tilde{h}$ as before, and then applies the QOTP:

$$|w_{\mathsf{enc}}\rangle \;=\; \Big(\bigotimes_{i=1}^{l} Z^{s_i} X^{r_i}\Big)\,|w\rangle.$$

The signature sent is $\{\otimes_{j=1}^{2q}|f_{\tilde{h}}(a{+}b)\rangle,\ |w_{\mathsf{enc}}\rangle\}$.

Tom reconstructs $|f'(a{+}b)\rangle$ and determines $\tilde{h}'$ *componentwise* by comparison, exactly as in the original protocol (match $\Rightarrow 0$, X-match $\Rightarrow 1$, else reject). With $\tilde{h}'$ in hand, he recomputes $(r', s') = \mathsf{KDF}(K, \tilde{h}')$ and decrypts

$$|w\rangle \;=\; \Big(\bigotimes_{i=1}^{l} X^{r'_i} Z^{s'_i}\Big)\,|w_{\mathsf{enc}}\rangle,$$

then measures $|w\rangle$ in bases selected by $\tilde{h}'$ to obtain m', and checks

$$H(m' \| ID_A \| ID_T \| K \| sid \| \rho_T) \stackrel{?}{=} \tilde{h}'.$$

5.1 Security Analysis

We now discuss the security of the proposed DVS. The purpose of the modification is not to redesign all components of Xin et al.'s protocol, but to remove the malleability that enables the message-signature-pair forgery described in Section 4. The remaining security arguments follow the same structure as in Xin et al.'s scheme [22].

5.1.1 Unforgeability

The proposed modification prevents the forgery attack because the message-dependent flip pattern is no longer publicly computable. In the original scheme, if an adversary obtained a valid message-signature pair (m, σ_m), then she could compute

$$h = H(m \| ID_A \| ID_T)$$

and, for any fresh target message m^*, compute

$$h^* = H(m^* \| ID_A \| ID_T).$$

She could then modify the quantum signature component by applying Pauli operators according to $h \oplus h^*$.
In the revised scheme, the flip pattern is computed as

$$\tilde{h} = H(m \| ID_A \| ID_T \| sid \| \rho_T \| K),$$

where K is a secret key shared only between Anna and Tom through QKD, sid is the session identifier, and ρ_T is Tom's fresh nonce. Hence, even if the adversary obtains a valid signature on m, she cannot compute the correct flip pattern for a fresh message m^*, namely

$$\tilde{h}^* = H(m^* \| ID_A \| ID_T \| sid^* \| \rho_T^* \| K),$$

because she does not know K. Therefore, she cannot determine how to transform

$$|f_{\tilde{h}}(a+b)\rangle$$

into the valid component

$$|f_{\tilde{h}^*}(a+b)\rangle$$

required for the new message.
Moreover, the message register is encrypted by a quantum one-time pad. The QOTP keys are derived as

$$(r, s) = \mathsf{KDF}(K, \tilde{h} \| sid \| \rho_T),$$

and are therefore unknown to the adversary. Thus, even if the adversary tries to alter the message register, she cannot prepare a valid encrypted encoding of a chosen fresh message m^* without knowing the corresponding QOTP keys.
During verification, Tom first recovers the candidate value $\tilde{h}'$ from the quantum signature component, derives the QOTP keys from

$$(r', s') = \mathsf{KDF}(K, \tilde{h}' \| sid \| \rho_T),$$

decrypts the message register, obtains m', and checks

$$H(m' \| ID_A \| ID_T \| sid \| \rho_T \| K) = \tilde{h}'.$$

Thus, both parts of the signature must be consistent with the same secret keyed value $\tilde{h}'$. A previously obtained signature cannot be modified into a valid signature on a new message unless the adversary can predict the keyed hash/KDF output or break the underlying quantum one-way construction. Therefore, the proposed countermeasure prevents the message-signature-pair forgery attack.

5.1.2 Designated Verification

We now explain why only the designated verifier Tom can complete the verification of the proposed quantum designated-verifier signature. In the revised construction, the received signature package has the form

$$\left\{ \bigotimes_{j=1}^{2q} |f_{\tilde{h}}(a+b)\rangle,\ |w_{\mathsf{enc}}\rangle \right\}.$$

To verify it, Tom must first reconstruct the reference state

$$|f'(a+b)\rangle$$

using Anna's public quantum state and his private key b. He then compares it with the received state in order to recover the candidate value $\tilde{h}'$. This step cannot be performed by an outside party, because constructing $|f'(a+b)\rangle$ requires knowledge of at least one private contribution, namely Anna's private key a or Tom's private key b.

Furthermore, even if a third party attempts to process the message register, the register is not $|w\rangle$ but the encrypted state

$$|w_{\mathsf{enc}}\rangle = \left(\bigotimes_{i=1}^{l} Z^{s_i} X^{r_i} \right) |w\rangle.$$

The keys (r, s) are derived from

$$(r, s) = \mathsf{KDF}(K, \tilde{h} \| sid \| \rho_T),$$

where K is known only to Anna and Tom. Hence, a third party cannot decrypt $|w_{\mathsf{enc}}\rangle$ or measure it in the correct bases to recover the message. Therefore, the verification procedure can be completed only by the designated verifier Tom.

5.1.3 Non-transferability

The non-transferability property requires that Tom should not be able to convince an external party that a valid signature was generated specifically by Anna. In a designated-verifier signature scheme, this is achieved by ensuring that the designated verifier can simulate a valid signature that is indistinguishable from a genuine signature generated by the signer. The revised construction preserves this property. Tom knows his private key b, has access to Anna's quantum public state, and shares the QKD key K with Anna. Therefore, Tom can reconstruct

$$|f'(a+b)\rangle = |f(a+b)\rangle.$$

For any message m, Tom can compute

$$\tilde{h} = H(m \| ID_A \| ID_T \| sid \| \rho_T \| K),$$

prepare the hash-dependent state

$$|f_{\tilde{h}}(a+b)\rangle = \bigotimes_{i=1}^{l} X^{\tilde{h}_i} |f(a_i + b_i)\rangle,$$

derive

$$(r, s) = \mathsf{KDF}(K, \tilde{h} \| sid \| \rho_T),$$

encode m into $|w\rangle$, and encrypt it as

$$|w_{\mathsf{enc}}\rangle = \left(\bigotimes_{i=1}^{l} Z^{s_i} X^{r_i} \right) |w\rangle.$$

Thus, Tom can generate a valid signature package

$$\left\{ \bigotimes_{j=1}^{2q} |f_{\tilde{h}}(a+b)\rangle,\ |w_{\mathsf{enc}}\rangle \right\}$$

that is indistinguishable from a package generated by Anna. Consequently, if Tom presents a valid signature package to a third party, the third party cannot determine whether the package was produced by Anna or simulated by Tom. Hence, Tom cannot transfer the signature as convincing evidence of Anna's authorship to any third party. This establishes non-transferability.

5.2 Comparative Analysis

In addition to improving the formal security properties of the protocol, it is also important to assess whether the proposed modifications preserve its practical applicability within quantum communication environments. Since the proposed countermeasure retains the original protocol structure and introduces only lightweight cryptographic operations, it can be incorporated into existing implementations with minimal additional complexity.

We now provide a comparative analysis of the proposed scheme with existing state-of-the-art DVS [14, 15, 17, 30–32] in quantum domain. From the viewpoint of key management, the proposed scheme has a clear advantage over many existing arbitrated quantum DVS schemes such as [14, 15, 17, 30–32]. In those schemes, the signer and the designated verifier often have to share their private keys, private quantum states, or entangled particles with a trusted third party. In our construction, however, the private keys of Anna and Tom are generated by the users themselves and remain secret with them throughout the protocol. Hence, no external party is required to store, know, or distribute the private information of the participants. This feature also eliminates the key escrow problem. In arbitrated schemes, the security of the users' private keys depends on the honesty of the trusted third party, since the TP may possess or help manage secret information. Such a trust assumption is undesirable in an open network environment, where no party can be assumed to be fully trustworthy. In contrast, the proposed quantum public-key DVS scheme does not rely on any TP for protecting the users' private keys.

Unlike many existing quantum DVS schemes, the proposed scheme avoids TP-related communication overhead and prevents the TP from becoming a bottleneck in the quantum network. Moreover, the proposed scheme does not require the participants to prepare or share entangled particles. This makes the scheme simpler and more practical than several entanglement-based quantum DVS schemes.
Table 1 summarizes the security comparison of the proposed scheme with several existing quantum DVS schemes [14, 15, 17, 30–32]. It can be observed that most of the earlier schemes satisfy the basic DVS requirements such as designated verification, non-transferability, source non-traceability, resistance to inter-resending attacks, resistance to impersonation attacks, and resistance to man-in-the-middle attacks. However, many of these schemes do not provide complete secrecy of the users' private keys, since they

Table 1 Security Comparison of the Proposed Scheme with Existing DVS Schemes

Security Property ↓	[32]	[30]	[17]	[15]	[31]	[14]	Xin [22]	**Ours**
Secrecy of Private Key	No	No	No	No	No	No	Yes	Yes
Designated Verification	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Non-Transferability	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Source Non-Traceability	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Inter-resending Attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security against Impersonation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security against Man-in-the-Middle Attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Unforgeability	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Replay Attacks	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Collusion Attacks	No	No	No	No	No	No	No	Yes

rely on a trusted third party or require some private information to be shared during initialization, key distribution, or verification.
The quantum DVS scheme of Xin et al. [22] improves this aspect by avoiding the key escrow problem and preserving the secrecy of the signer and verifier private keys. Nevertheless, our cryptanalysis shows that the scheme is not unforgeable. In particular, once a valid pair (m, σ_m) is available, an attacker can generate a forged signature on a new message $m*$ without using the private keys of Anna or Tom. Thus, although Xin et al.[22] satisfies several standard DVS properties, it fails to resist the forgery attack identified in this work. Moreover, [22] does not prevent the collusion-based attacks and replay attacks. In contrast, the proposed scheme preserves the positive features of Xin et al. [22] construction while removing these weaknesses.

6 Conclusion

In this paper, we analyzed the quantum DVS scheme proposed by Xin et al. [22] and demonstrated that it is vulnerable to an existential forgery under a chosen-message attack. To address this issue, we proposed a minimal modification in which the signer and verifier establish a shared secret through QKD, use it to compute a keyed hash, and protect the message register using a quantum one-time pad. The proposed modification removes the identified structural vulnerability while preserving the designated-verifier functionality of the original protocol.

More broadly, our results emphasize that the security of quantum cryptographic protocols depends not only on the security of individual quantum primitives but also on their correct integration within the protocol design. As quantum information technologies continue to evolve towards practical deployment, rigorous cryptanalysis of proposed protocols remains indispensable for ensuring their reliability and long-term security.

Declarations

Ethics Approval

This study did not involve human participants, animals, or identifiable personal data. Therefore, approval from an Institutional Review Board (IRB) or Ethics Committee was not required.

Consent to Participate

Not applicable.

Consent for Publication

Not applicable.

Funding

Vikas Srivastava acknowledges the financial support received from the ANRF-PMECRG project (Ref. No. ANRF/ECRG/2025/002808/PMS).

Availability of Data and Materials

No datasets were generated or analysed during the current study.

Competing Interests

The authors declare that they have no competing interests.

Author Contributions

Shanu Poddar and Vikas Srivastava contributed equally to the conception, analysis, and manuscript drafting. Both the authors reviewed and approved the final manuscript.

Acknowledgement

Vikas Srivastava acknowledges the support received from the ANRF-PMECRG project with Ref. No. ANRF/ECRG/2025/002808/PMS

References

[1] Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions on Information Theory **22**(6), 644–654 (1976)

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

[3] Kawachi, A., Koshiba, T., Nishimura, H., Yamakami, T.: Computational indistinguishability between quantum states and its cryptographic application. Journal of Cryptology **25**(4), 528–555 (2012)

[4] Huang, Y., Xu, G., Song, X.: An improved efficient identity-based quantum signature scheme: Y. huang et al. Quantum Information Processing **22**(1), 36 (2022)

[5] Prajapat, S., Kumar, P., Kumar, S., Das, A.K., Shetty, S., Hossain, M.S.: Designing high-performance identity-based quantum signature protocol with strong security. IEEE Access **12**, 14647–14658 (2024)

[6] Xin, X., Wang, Z., Yang, Q.: Identity-based quantum signature scheme with strong security. Optical and Quantum Electronics **51**(12), 393 (2019)

[7] Mohanty, T., Srivastava, V., Debnath, S.K., Roy, D., Sakurai, K., Mukhopadhyay, S.: An experimentally validated feasible quantum protocol for identity-based signature. Sādhanā **50**(1), 1–11 (2025)

[8] Yin, H.-L., Yao, F., Zeng, B.-C.: Practical quantum digital signature. Physical Review A **93**(3), 032316 (2016)

[9] An, X.-B., Zhang, H., Zhang, C.-M., *et al.*: Practical quantum digital signature with a gigahertz bb84 quantum key distribution system. Optics Letters **44**(1), 139–142 (2019)

[10] Ding, H.-J., Chen, J.-J., Ji, L., *et al.*: 280-km experimental demonstration of a quantum digital signature with one decoy state. Optics Letters **45**(7), 1711–1714 (2020)

[11] Zhang, C.-H., Zhou, X.-Y., Zhang, C.-M., *et al.*: Twin-field quantum digital signatures. Optics Letters **46**(15), 3757–3760 (2021)

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

[13] Shi, W.M., Wang, Y.M., Zhou, Y.H., *et al.*: A scheme on converting quantum signature with public verifiability into quantum designated verifier signature. Optik **164**, 753–759 (2018)

[14] Zheng, M., Xue, K., Li, S., Yu, N.: A practical quantum designated verifier signature scheme for e-voting applications. Quantum Information Processing **20**(7), 230 (2021)

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

[16] Prajapat, S., Dhiman, A., Kumar, S., Kumar, P.: A practical convertible quantum signature scheme with public verifiability into universal quantum designated verifier signature using self-certified public keys: S. prajapat et al. Quantum Information Processing **23**(10), 331 (2024)

[17] Xin, X., Wang, Z., Yang, Q., Li, F.: Quantum designated verifier signature based on bell states: X. xin et al. Quantum Information Processing **19**(3), 79 (2020)

[18] Zhang, Y., Xin, X., Li, F.: Secure and efficient quantum designated verifier signature scheme. Modern Physics Letters A **35**(18), 2050148 (2020)

[19] Xin, X., Wang, Z., Yang, Q., *et al.*: Quantum designated verifier signature based on bell states. Quantum Information Processing **19**, 79 (2020)

[20] Zhang, L., Gui, Q., Xin, X.-J., Li, C.-Y.: A quantum designated multi-verifiers signature scheme based on liop states. Modern Physics Letters A **39**(23n24), 2450111 (2024)

[21] 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)

[22] 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)

[23] Boykin, P.O., Roychowdhury, V.: Optimal encryption of quantum bits. Physical Review A **67**(4), 042317 (2003) https://doi.org/10.1103/PhysRevA.67.042317 quant-ph/0003059

[24] Li, Y., Susilo, W., Mu, Y., Pei, D.: Designated verifier signature: definition, framework and new constructions. In: International Conference on Ubiquitous Intelligence and Computing, pp. 1191–1200 (2007). Springer

[25] 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

[26] Steinfeld, R., Bull, L., Wang, H., Pieprzyk, J.: Universal designated-verifier signatures. In: International Conference on the Theory and Application of Cryptology and Information Security, pp. 523–542 (2003). Springer

[27] Lipmaa, H., Wang, G., Bao, F.: Designated verifier signature schemes: Attacks, new security notions and a new construction. In: International Colloquium on Automata, Languages, and Programming, pp. 459–471 (2005). Springer

[28] Huang, X., Susilo, W., Mu, Y., Wu, W.: Universal designated verifier signature without delegatability. In: Information and Communications Security. Lecture

Notes in Computer Science, vol. 4307, pp. 479–498. Springer, (2006)

[29] Huang, Q., Susilo, W., Wong, D.S.: Non-delegatable Identity-based Designated Verifier Signature. Cryptology ePrint Archive, Report 2009/367 (2009)

[30] 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)

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

[32] 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)