2024

Designing High-Performance Identity-Based Quantum Signature Protocol With Strong Security

Sunil Prajapat
Central University of Himachal Pradesh

Pankaj Kumar
Central University of Himachal Pradesh

Sandeep Kumar
Central University of Himachal Pradesh

Ashok Kumar Das
International Institute of Information Technology

Sachin Shetty
Old Dominion University, sshetty@odu.edu

See next page for additional authors

Original Publication Citation

Prajapat, S., Kumar, P., Kumar, S., Das, A. K., Shetty, S., & Hossain, M. S. (2024). Designing high-performance identity-based quantum signature protocol with strong security. *IEEE Access*, *12*, 14647 - 14658. https://doi.org/10.1109/ACCESS.2024.3355196

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 December 2023, accepted 12 January 2024, date of publication 17 January 2024, date of current version 1 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3355196

RESEARCH ARTICLE

Designing High-Performance Identity-Based Quantum Signature Protocol With Strong Security

SUNIL PRAJAPAT[1], (Associate Member, IEEE), PANKAJ KUMAR[1], SANDEEP KUMAR[2], ASHOK KUMAR DAS[3], (Senior Member, IEEE), SACHIN SHETTY[4], (Senior Member, IEEE), AND M. SHAMIM HOSSAIN[5], (Senior Member, IEEE)

[1]Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, Dharamshala 176215, India
[2]Department of Physics and Astronomical Science, Central University of Himachal Pradesh, Dharamshala 176215, India
[3]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India
[4]Virginia Modeling, Analysis and Simulation Center, Department of Computational Modeling and Simulation Engineering, Old Dominion University, Suffolk, VA 23435, USA
[5]Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 12373, Saudi Arabia

Corresponding author: M. Shamim Hossain (mshossain@ksu.edu.sa)

This work was supported in part by the Department of Defense (DoD) Center of Excellence in AI and Machine Learning (CoE-AIML) through the U.S. Army Research Laboratory under Contract W911NF-20-2-0277; in part by the "Design and Development of a Unified Blockchain Framework for offering National Blockchain Service" Project, through the Ministry of Electronics and Information Technology, New Delhi, Government of India, under Grant 4(4)/2021-ITEA; and in part by the Researchers Supporting Project number (RSP2024R32), King Saud University, Riyadh, Saudi Arabia.

ABSTRACT Due to the rapid advancement of quantum computers, there has been a furious race for quantum technologies in academia and industry. Quantum cryptography is an important tool for achieving security services during quantum communication. Designated verifier signature, a variant of quantum cryptography, is very useful in applications like the Internet of Things (IoT) and auctions. An identity-based quantum-designated verifier signature (QDVS) scheme is suggested in this work. Our protocol features security attributes like eavesdropping, non-repudiation, designated verification, and hiding sources attacks. Additionally, it is protected from attacks on forgery, inter-resending, and impersonation. The proposed scheme benefits from the traditional designated verifier signature schemes. In the proposed scheme, the signer encrypts a message with his or her private key, and the designated verifier validates the accompanying QDVS using the signer's public key, which is the signer's name or email address, which makes the quantum signature system's key management simpler. It uses an entangled state while signing and verifying the signature; however, the verifier is not required to compare quantum states. A detailed comparison analysis with other similar schemes provides more security for the proposed scheme. Furthermore, the proposed scheme's effectiveness and feasibility are validated using quantum simulations.

INDEX TERMS Quantum signature, designated verifier, One-Time-Pad (OTP), unforgeability, security.

I. INTRODUCTION

The application of digital signatures is an essential resource for ensuring the accuracy and integrity of sent messages. In a signature protocol, the signer uses his or her private key to sign the message and create the accompanying signature in order to authenticate the message, and this signature can be easily validated by anyone using the signer's public key. Unforgeability and non-repudiation are security features that should be present in a secure signature technique. Basically, once a polynomial adversary has verified the validity of the signature, the signer cannot contest because it is unforgeable.

The associate editor coordinating the review of this manuscript and approving it for publication was Kashif Saleem.

Consequently, by checking the signed message that was received, anyone can check the message's accuracy and locate the source of the matching message. Therefore, digital signatures are widely used in e-commerce, e-government, and information security.

The public verification feature of digital signatures can occasionally work against preserving the signer's privacy. Sometimes a signer requests that the validity of the signed communication be checked exclusively by the specified verifier. For example, a voter might prefer, due to concern for their safety and personal privacy during an election, that only the designated verifier can authenticate their signature on their vote. The auction is yet another illustration. A bidder may request that only the selected verifier validate their signature on the bid during the auction phase, keeping in mind their financial interests. In order to satisfy the need for a designated verification for signatures, many ''designated verifier signature (DVS)'' protocols have been developed [1], [2], [3], [4], [5], [6], [7], [8], [9], [10]. DVS also offers a tailored solution for the security challenges inherent in IoT environments. In the context of IoT, where resource-constrained devices require efficient cryptographic mechanisms, DVS stands out for selective verification capability [11]. This provides fine-grained access control crucial for IoT ecosystems which offers privacy preservation by allowing devices to selectively disclose information to designated verifiers, addressing concerns related to data confidentiality in large-scale IoT deployments. DVS enhances message integrity and reduces computational overhead by restricting signature verification to designated entities. In essence, the selective verification, computational efficiency, privacy preservation, and fine-grained access control features make DVS a highly suitable cryptographic tool for securing IoT ecosystems. A DVS system should typically include the following security characteristics [5], [6]:

- *Correctness:* During the signing phase, the designated verifier must be able to accept the created signature only if the signer generates the DVS correctly.
- *Non-transferability:* It is a quite difficult job for the designated verifier to demonstrate to a third party that the signature has been generated by the ''signer'' or by ''himself''.
- *Hiding source:* Suppose we are provided with a signature on message μ. Even if both the signer and designated verifier reveal their private keys, it must be difficult to determine which is the original signer.
- *Unforgeability:* When the private key of the signer or the authorized verifier is unknown, it will be impossible to generate a legal DVS.

Nowadays, the majority of DVSs are classical ones. [1], [3], [4], [5], [6], [7], [8], [9], [10]. Classical DVS security is based on some unsubstantiated hardness assumptions of puzzles from mathematics such as the ''discrete logarithm problem (DLP)'' and the ''Diffie-Hellman problem (DHP)''. However, quantum computers are increasingly dependent on these unproven hardness assumptions as quantum computing technology develops [12]. Two QDVS techniques have recently been proposed [13], [14]. Instead of relying on unproven assumptions about the difficulty of mathematical problems, the security of the QDVS methods in [13] and [14] rests on fundamental quantum mechanical phenomena. Therefore, the systems in [13] and [14] ought to be more secure than the traditional digital signature system in [15]. However, in [13], a quantum sequence containing entangled states needs to be generated to encrypt the message in order to sign it. It should be noted that preparing the entangled states is not very convenient given the level of technology. On the other hand, in [13] and [14], the verifier must run the quantum state comparison algorithm to validate a quantum signature [16]. The aforementioned factors are going to significantly impact the efficacy and sustainability of the QDVS protocols.

In this work, utilizing entangled states, a new QDVS protocol is suggested in order to increase the QDVS system's effectiveness. The verifier is not required to do any quantum state comparisons during the signature verification phase. Furthermore, our protocol differs from symmetric quantum signature systems [17], [18], [19], [20], [21], [22], [23], in which the quantum signatures are signed and verified using the same signing keys. The proposed QDVS is a quantum signature system based on identity. In our protocol, each user's private key is generated by a private key generator (PKG) and a dependable third party. The public key of a signer is the same as personal information about them, like their name or email address. The process of encrypting a message is performed by the individual who possesses the private key. Subsequently, the quantum signature associated with the encryption is verified by employing the personal data of the signer. Therefore, the advantages of Shamir's identity-based cryptosystem have been applied to the QDVS scheme proposed in this work [24]. It can make the QDVS protocol's key management simpler. So, the proposed protocol is more effective and workable compared to other similar protocols [15], [25], [26], [27], [28], [29], [30], [31].

A. MOTIVATION AND RESEARCH CONTRIBUTIONS

The security issues in traditional quantum signature protocols [15], [25], [26], [27], [28], [29], [30], [31], motivates us to design an identity-based quantum signature for better efficiency and security. Quantum cryptography offers robust resistance against quantum threats, ensuring the continued integrity and reliability of communications even as quantum computing capabilities advance. Consequently, the transition in accordance with the need to ensure the long-term viability of security measures is important. Hence, we have proposed a quantum signature protocol. The key contributions are specifically listed below.

- Firstly, we suggest a non-interactive identity-based quantum signature protocol with a designated verifier. Additionally, this protocol utilizes the benefits of quantum and identity-based cryptosystems. We also observed that in a large number of related research

works, people use only verification, not designated verification, to participate in communication, and we have also provided that the sender and receiver can be authenticated, resulting in a diminution of network latency.
- Second, we have also provided a formal security analysis that is employed to display the security of the suggested protocol based on quantum fundamentals. The process of identifying illegal signatures during verification is also explained. The proposed protocol withstands eavesdropping attacks, non-repudiation, design verification properties, and hiding sources.
- We use ''Python'' and ''Scyther'' to integrate performance and simulation of our protocol. The calculation costs for our approach are contrasted, and the experiment's outcome shows how well-suited our protocol is for communication.

B. PAPER STRUCTURE

This work is organized as follows: The ''One-Time-Pad (OTP)'' and the role of quantum communication are briefly explored in Section II. All key ingredients of the proposed scheme are discussed in Section III. Section IV includes formal and informal security examinations and the scyther simulations of the proposed protocol. A detailed comparative study of the proposed protocol with the related existing schemes is provided in Section V. Section VI is devoted to the simulation of the proposed protocol. Finally, the paper is concluded in Section VII.

II. PRELIMINARIES

In this section, we provide the preliminary concepts helpful in quantum computing and the essential theories of quantum mechanics used in our proposed scheme.

A. ONE-TIME-PAD (OTP)

OTP is a ''symmetric encryption technique'' that was first developed by Mille [32], [33], [34], [35]. The secret key is shared by OTP between the sender and the receiver of the communication. Typically, the requirement involves a ''random pad k'' and a ''message μ'' to be sent to have the same size. The sender first computes $\mathcal{C} = \mu \oplus K$ and then sends the ''OTP ciphertext $\mathcal{C}$'' to the receiver in order to encrypt the message μ. The symbol ''$\oplus$'' stands for addition under modular two. The receiver computes $\mathcal{C} = \mu \oplus K$ to decrypt $\mathcal{C}$. Due to OTP's unwavering security, an attacker cannot decrypt μ from the ciphertext $\mathcal{C}$ [36].

B. QUANTUM COMPUTING CHARACTERISTICS

The research area of quantum-based computers is expanding every day because of their effectiveness in quickly tackling various problems, for instance, integer factorization. In contrast, classical computers often need billions of years to do so. The ability of quantum computers to quickly address various issues fascinates major corporations like Google Inc., Microsoft Inc., and Amazon Inc. Therefore, genuine interest from the industry will hasten the release of a quantum computer far sooner than anticipated. Quantum chips, as opposed to the silicon ones found in conventional computers, are the basis of the quantum computer. Starting from the fundamentals of quantum systems and their architecture, we explain the key characteristics of quantum computing in this subsection.

1) QUANTUM SYSTEM FUNDAMENTALS

A binary digit known as a bit is the basis of classical information theory. Classically, it is always read as a 1 (true) or a 0 (false), no matter how physically represented. Contrary to the real numbers, complex numbers are used in quantum mechanics. The generalization of the idea of the classical bit, known as a qubit, is a ''unit of quantum information'' [37]. A state vector in a ''two-level quantum system'', formally identical to a ''two-dimensional Hilbert space'', is applied in quantum computing to describe quantum information (qubits) [38]. The evolution of quantum systems is reversible, and the bit is a way of expressing a system that can exist in either one of two states, i.e., either 1 or 0. The following in Dirac notation can represent these states [39], [40]:

$$\begin{aligned} State(A) &= |1\rangle = [0, 1]^T \\ State(B) &= |0\rangle = [1, 0]^T \end{aligned} \tag{1}$$

In the quantum world, any object can be in state A, state B, or a superposition of both. The quantum mechanical switches in this world can be in an off ($|0\rangle$) or on ($|1\rangle$) state at the same time. Therefore, a two-dimensional quantum system is described by a qubit. A single qubit can be expressed by a linear combination of $|0\rangle$ and $|1\rangle$ [39], [41]:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle, \tag{2}$$

and constrained according to the second axiom of probability theory.

$$|a_0|^2 + |a_1|^2 = 1. \tag{3}$$

In Eq. (3), $|a_0|^2$ and $|a_1|^2$ represent the probabilities of a qubit remaining in states $|0\rangle$ and $|1\rangle$ after measurement, respectively. The implementation of qubits in the universe can be understood by the fact that an electron might be in two different spin states (spin up or spin down) while revolving around the nucleus in an atom. Also, a photon may be in one of two polarized states (horizontal or vertical polarization). As a result, there are enough quantum indeterminacy and superposition effects to represent qubits throughout the universe in all systems.

2) QUANTUM NO-CLONE THEOREM

The No-Cloning property is one key characteristic that sets quantum information apart from classical information [42]. In 1982, Wootters, Zurek, and Dieks proposed the No-Cloning theorem [43]. According to this, an apparatus that can accept a general quantum state as input and output the

original state along with a replica of some information cannot be built [43]. To prove the No-Cloning theorem, consider a unitary operator U_c that can indeed clone an unknown quantum state $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$. Then

$$\begin{aligned}|\psi\rangle|0\rangle \xrightarrow{U_c} |\psi\rangle|\psi\rangle &= (a_0|0\rangle + a_1|1\rangle)(a_0|0\rangle + a_1|1\rangle)\\ &= a_0^2|00\rangle + a_1a_0|10\rangle + a_0a_1|01\rangle\\ &\quad + a_1^2|11\rangle \end{aligned} \tag{4}$$

Now if we apply operator U_c to clone the expansion of $|\psi\rangle$, we get

$$(a_0|0\rangle + a_1|1\rangle)|0\rangle \xrightarrow{U_c} a_0|00\rangle + a_1|11\rangle \tag{5}$$

No cross terms exist in Eq. (5). So, a unitary operator U_c cannot exist because of the contradiction that results from our situation. As a result, it is impossible to create an exact copy from a random, unknowable quantum state. Therefore, the quantum No-Cloning theorem guarantees the confidentiality and secrecy of quantum cryptograms and is the theoretical cornerstone of quantum mechanics and quantum communication [44]. In particular, this theorem prevents the production of an exact copy of an unknown quantum state. Theoretically, an eavesdropper cannot determine the identity of a legitimate user using clone technology.

3) HEISENBERG'S UNCERTAINTY PRINCIPLE

The measurement operator should measure quantum bits before they are transmitted as binary bits. Consider two Hermitian operators O_1 and O_2 corresponding to a normalized quantum state $|\psi\rangle$ such that their expectation values are given by [45]

$$\begin{aligned}\langle O_1\rangle &= \langle\psi|O_1|\psi\rangle\\ \langle O_2\rangle &= \langle\psi|O_1|\psi\rangle\end{aligned} \tag{6}$$

Introducing the operators ΔO_1 and ΔO_2,

$$\begin{aligned}\Delta O_1 &= O_1 - \langle O_1\rangle\\ \Delta O_2 &= O_2 - \langle O_2\rangle,\end{aligned} \tag{7}$$

we have

$$\begin{aligned}\langle\psi|(\Delta O_1)^2|\psi\rangle &= \langle(\Delta O_1)^2\rangle = \langle O_1^2\rangle - \langle O_1\rangle^2\\ \langle\psi|(\Delta O_2)^2|\psi\rangle &= \langle(\Delta O_2)^2\rangle = \langle O_2^2\rangle - \langle O_2\rangle^2\end{aligned} \tag{8}$$

Therefore, the uncertainties ΔO_1 and ΔO_2 can be defined as

$$\begin{aligned}\Delta O_1 &= \sqrt{\langle(\Delta O_1)^2\rangle} = \sqrt{\langle O_1^2\rangle - \langle O_1\rangle^2}\\ \Delta O_2 &= \sqrt{\langle(\Delta O_2)^2\rangle} = \sqrt{\langle O_2^2\rangle - \langle O_2\rangle^2}\end{aligned} \tag{9}$$

Now consider the action of operators ΔO_1 and ΔO_2 on any arbitrary state $|\psi\rangle$ as follows:

$$\begin{aligned}|\chi\rangle &= (O_1 - \langle O_1\rangle)|\psi\rangle\\ |\phi\rangle &= (O_2 - \langle O_2\rangle)|\psi\rangle\end{aligned} \tag{10}$$

Since operators O_1 and O_2 are Hermitian, ΔO_1 and ΔO_2 must be Hermitian. Therefore, the Schwarz inequality for the states $|\chi\rangle$ and $|\phi\rangle$ becomes

$$\langle(\Delta O_1)^2\rangle\langle(\Delta O_2)^2\rangle \geq |\langle\Delta O_1\Delta O_2\rangle|^2 \tag{11}$$

Using the hermicity of operators and commutation relation $[\Delta O_1, \Delta O_2] = [O_1, O_2]$, the above Eq. (11) becomes

$$\langle(\Delta O_1)^2\rangle\langle(\Delta O_2)^2\rangle \geq \frac{1}{4}|\langle[O_1, O_2]\rangle|^2\,, \tag{12}$$

which can be written as:

$$\langle\Delta O_1\rangle\langle\Delta O_2\rangle \geq \frac{1}{2}|\langle[O_1, O_2]\rangle| \tag{13}$$

This uncertainty relation plays an important role in the formalism of quantum mechanics. For example, the Heisenberg uncertainty relations, one of the pillars of quantum mechanics, are produced due to their application to position and momentum operators.

Let Δx and Δp be the uncertainties in position operator X and momentum operator P, respectively. The Heisenberg uncertainty principle gives [45]

$$\langle\Delta x\rangle\langle\Delta p\rangle \geq \frac{1}{2}|\langle[X, P]\rangle| \tag{14}$$

As a result of Eq. (14), we can conclude that a maximum in position (Δx) measurements will result in a minimum in momentum (Δp) measures, and vice versa. In other words, X and P cannot be simultaneously operated for measurements, or a state cannot simultaneously be the eigenstate of both X and P.

4) ENTANGLEMENT AS A QUANTUM PROPERTY

In quantum mechanics, quantum entanglement happens when a system of several particles interacts so that they can only be characterized as a single system as a whole and not as separate, independent systems. In contrast to how composite systems are described in classical phase space, the idea of Hilbert space describes them differently in quantum mechanics. For instance, in the classical description, a multipartite system composed of n-subsystems has a total state space that is just the Cartesian product of n-subsystem spaces. Therefore, the "total state of the system" is always a product of the states of separate n-subsystems.

In quantum formalism, contrary to classical description, the "total Hilbert space (H_T) is a tensor product of n-subsystems Hilbert spaces (H_i)", which can be described as follows:

$$\begin{aligned}H_T &= H_1 \otimes H_2 \otimes H_3 \ldots \otimes H_n\\ &= \otimes_{i=1}^{n} H_n.\end{aligned} \tag{15}$$

Now according to the superposition principle, the total state of the system can be described as

$$|\psi\rangle = \sum_{i_1,i_2,\ldots,i_n} \alpha_{i_1,i_2,\ldots,i_n}|i_1\rangle \otimes |i_2\rangle \otimes \ldots \otimes |i_n\rangle, \tag{16}$$

this total state cannot be described as the tensor product of separate individual n-subsystems, i.e.,

$$|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots |\psi_n\rangle. \tag{17}$$

Therefore, we cannot assign a single state vector to any n-subsystems. In contrast to classical superposition, it formally expresses entanglement phenomena. The entangled state (Eq. (17)) results due to the direct physical interaction; however, entanglement can be indirectly generated by entanglement swapping. The composite quantum bit ($|\psi_{AB}\rangle$) can be described by the four Bell-state-entangled basis

$$\begin{aligned} |\psi^{\pm}_{AB}\rangle &= \frac{1}{\sqrt{2}}[|0_A\rangle \otimes |1_B\rangle \pm |1_A\rangle \otimes |0_B\rangle] \\ |\Phi^{\pm}_{AB}\rangle &= \frac{1}{\sqrt{2}}[|0_A\rangle \otimes |0_A\rangle \pm |1_A\rangle \otimes |1_B\rangle] \end{aligned} \tag{18}$$

These entangled Bell-states (also known as EPR states) have an equal probability of being found in either state $|0\rangle$ or state $|1\rangle$ if one only measures at one of the subsystems. Thus, the states do not reveal any information about the subsystems. Since states are pure as a whole, they provide the maximal knowledge about the total system.

5) QUANTUM SYSTEM ARCHITECTURE

The reversible evolution of quantum systems allows for both the doing and undoing of manipulation. Through undoing, the architecture is transformed into reversible gates. In quantum computing, reversible gates are all unitary matrix-based operations that are not measurements. The fundamental hardware component of the quantum gates is the classical reversible gates, which are used in quantum computing. The Toffoli and Fredkin gates are universal and unitary, in addition to being reversible. These two gates are very well-known classical reversible gates, along with the NOT gate, controlled-NOT gate, and identity gate. Moreover, the no-cloning theorem prohibits all quantum gates from performing the fanout operation. Even though cloning is impossible, it can transmit any arbitrary quantum state from one system to another.

III. QDVS: PROPOSED IDENTITY-BASED QUANTUM-DESIGNATED VERIFIER SIGNATURE PROTOCOL

In the proposed protocol, it is assumed that Alice and Bob perform the roles of the signer and the verifier, respectively. The PKG, being a "trusted private key generator" produces a private key for the signer. The system has four stages: a) initialization, b) key generation, c) signing, and d) verifying. The details of these stages are given in the subsequent subsections.

A. INITIALIZING PHASE

Similar to [46], assume that we have:

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)$$

TABLE 1. Notation table.

Symbol	Description
H	Hadamard operator.
I	Identity operator.
$H_j (j = 1, 2, 3, 4)$	Independent permutation function.
$H_j^{-1} (j = 1, 2, 3, 4)$	Inverse permutation function.
$\oplus$	Xor operator.
F	Cryptographic one way function
K	Private key
q	Decoy particle
$\|\cdot\rangle$	Quantum sequence

as the Hadamard operator. Next, we consider [46]

$$\begin{aligned} Y &= |0\rangle\langle 1| - |1\rangle\langle 0|, \\ Y^{+} &= |1\rangle\langle 0| - |0\rangle\langle 1|, \\ |\pm\rangle &= (|0\rangle \pm |1\rangle)/\sqrt{2}, \end{aligned}$$

assuming that I is the unit operator, we define $H^0 = Y^0 = I$. Now, if we take $a = (a_1, a_2, \ldots, a_m)$ and $b = (b_1, b_2, \ldots, b_m) = \{0, 1\}^m$, then $a \oplus b = (a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_m \oplus b_m)$, where the symbol $\oplus$ signifies the addition operation for modulo 2. Let H_1, H_2, H_3, and H_4 be four publicly accessible, distinctive, and "independent permutation functions" on $\{0, 1\}^m$, respectively, with $j = 1, 2, 3$, and 4. The system chooses one H_j at random. The inverse permutation of H_j is denoted by $H_j^{-1} (j = 1, 2, 3, 4)$. PKG surreptitiously chooses a one-way function $F : \{0, 1\}^* \rightarrow \{0, 1\}^m$ with uniform output distribution as master key F and PKG stores this master key in secret. All the symbols and their descriptions are provided in Table 1.

B. KEY GENERATION PHASE

Assume that Alice's identity is $Id = (Id_1, Id_2, \ldots, Id_m) \in \{0, 1\}^m$. This identity may be her email address. Id serves as Alice's public key. The PKG needs to generate Alice's private key in secret by carrying out the subsequent stages.

1) PKG uses the master key F to evaluate $K = F(Id)$.
2) The quantum key distribution mechanism is used by PKG and Alice to distribute a random string [47]. PKG determines $b = a \oplus K$ and publishes b.
3) Alice generates her private key $K = a \oplus b$ based on the revealed b.

C. SIGNING PHASE

Let the message to be signed be $\mu = (\mu_1, \mu_2, \ldots, \mu_m) \in \{0, 1\}^m$.

- Alice selects three m-bit strings at random as follows: "$x = (x_1, x_2, \ldots, x_m), y = (y_1, y_2, \ldots, y_m)$, and $z = (z_1, z_2, \ldots, z_m)$". She then performs the following calculations [46]:

$$\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m) = x \oplus \mu \oplus Id \tag{19}$$
$$\beta = (\beta_1, \beta_2, \ldots, \beta_m) = y \oplus \mu \oplus Id \tag{20}$$
$$\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_m) = z \oplus \mu \oplus Id \tag{21}$$
$$p = (p_1, p_2, \ldots, p_m) = H_1(K \oplus \mu \oplus Id) \tag{22}$$
$$t = (t_1, t_2, \ldots, t_m) = H_2(x \oplus \mu \oplus Id) \tag{23}$$

$$r = (r_1, r_2, \ldots, r_m) = H_3(y \oplus \mu \oplus Id) \quad (24)$$

$$s = (s_1, s_2, \ldots, s_m) = H_4(z \oplus \mu \oplus Id) \quad (25)$$

- Alice executes the operations $Y^{x_j}H^{p_j \oplus r_j}$, $Y^{y_j}H^{p_j \oplus s_j}$, and $Y^{z_j}H^{p_j \oplus q_j}$ to the variables $|t_j\rangle$, $|r_j\rangle$ and $|s_j\rangle$, respectively. She gets [46]

$$|e_j\rangle = Y^{z_j}H^{p_j \oplus t_j}|t_j\rangle \quad (26)$$

$$|f_j\rangle = Y^{x_j}H^{p_j \oplus r_j}|r_j\rangle \quad (27)$$

$$|g_j\rangle = Y^{y_j}H^{p_j \oplus s_j}|s_j\rangle \quad (28)$$

  Assume that, $|e\rangle = \otimes_{j=1}^{m}|e_j\rangle$, $|f\rangle = \otimes_{j=1}^{m}|f_j\rangle$ and $|g\rangle = \otimes_{j=1}^{m}|g_j\rangle$.
- For detecting eavesdropping, Alice randomly creates $3q(q \ll m)$ decoy particles from the set $(|0\rangle, |1\rangle, |+\rangle, |-\rangle)$. She then adds q decoy particles at random to the quantum sequence $|e\rangle$ and obtains the matching quantum sequence $|e'\rangle$. Similar to this, she generates the appropriate quantum sequence $|f'\rangle$ by randomly inserting q decoy particles from the remaining $2q$ decoy particles in the quantum sequence $|f\rangle$. She then generates the relevant quantum sequence by randomly inserting the remaining q decoy particles in the quantum sequence [46]. Alice send the sequence $\{\mu, Id, |e'\rangle, |f'\rangle, |g'\rangle\}$ to Bob.
- After verifying Bob has received $\{\mu, Id, |e'\rangle, |f'\rangle, |g'\rangle\}$, Alice transmits the "coordinates and initial states of all the decoy particles in the quantum sequences $|e'\rangle$, $|f'\rangle$, and $|g'\rangle$". Bob finally compares the measurement results with each decoy particle's original condition after measuring each decoy particle with the appropriate foundation. Bob completes the subsequent step if there are no mistakes. Otherwise, he needs to restart the protocol. When, no errors occur, both Alice and Bob need to share two secrets which are random m-bit pads, denoted by u and λ, in accordance with the same measurement results of the decoy particles implanted into $|e'\rangle$, $|f'\rangle$ and $|g'\rangle$ [46]. Alice then performs the calculations for $v = u \oplus y$ and $\theta = z \oplus \lambda$. Finally, Alice releases v and θ.
- In the above step, Bob checks for eavesdropping attempts before recovering $|e\rangle$, $|f\rangle$, and $|g\rangle$ from $|e'\rangle$, $|f'\rangle$, and $|g'\rangle$, respectively. Bob stores the quantum signature on μ as $\{\mu, Id, v, \theta, |e\rangle, |f\rangle, |g\rangle\}$.

D. VERIFICATION PHASE

This phase involves the following steps:

- Bob first calculates "$y = (y_1, y_2, \ldots, y_m) = u \oplus v$ and $z = (z_1, z_2, \ldots, z_m) = \theta \oplus \lambda$" using the secret pads u and λ information he and Alice shared. Bob determines r using Eq. (24), and y. Bob does out the operation $H^{r_j}(Y^+)^{Z_j}$ on each $|e_j\rangle$, and he obtains

$$|\eta_j\rangle = H^{r_j}(Y^+)^{Z_j}|e_j\rangle \quad (29)$$

  let $|\eta\rangle = \otimes_{j=1}^{m}|\eta_j\rangle$.
- Bob generates $3q(q \ll m)$ decoy particles at random from the set of $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ for the purpose of detecting eavesdropping attacks. He next generates the appropriate quantum sequence $|\eta'\rangle$ by randomly inserting q decoy particles into the quantum sequence $|\eta\rangle$. Additionally, he gets the appropriate quantum sequence $|f''\rangle$ by randomly inserting q decoy particles from the remaining $2q$ decoy particles into the quantum sequence $|f\rangle$. Finally, he generates the appropriate quantum sequence $|g''\rangle$ by randomly inserting the remaining q decoy particles into the quantum sequence $|g\rangle$ and transmits sequences $\{\mu, Id, |\eta'\rangle, |f''\rangle, |g''\rangle\}$ to PKG.
- Bob reveals the "coordinates and initial states of all the decoy particles in the quantum sequences $|\eta'\rangle$, $|f''\rangle$ and $|g''\rangle$ after confirming that PKG has received $\{\mu, Id, |\eta'\rangle, |f''\rangle, |g''\rangle\}$". PKG then compares the measurement result with each decoy particle's initial condition after measuring each decoy particle with the appropriate foundation. PKG executes the subsequent step if there are no errors; otherwise, he restarts the protocol.
- PKG retrieves $|\eta\rangle, |f\rangle$ and $|g\rangle$ from the quantum sequences $|\eta'\rangle, |f''\rangle$ and $|g''\rangle$, respectively, after evaluating eavesdropping attacks. The private key $K = F(Id)$ and p are then calculated by PKG using Id, μ, and the master key F using Eq. (22). After that, PKG runs the operation H^{p_j} on $|\eta_j\rangle$ for each instance of $|\eta_j\rangle$, returning

$$|\alpha_j\rangle = H^{p_j}|\eta_j\rangle, \quad j = 1, 2, \ldots, m \quad (30)$$

  Following this, PKG measures each $|\alpha_j\rangle$ using the $|0\rangle, |1\rangle$ foundation. If the result of the measurement is 0, PKG either sets $\alpha_j = 0$ or $\alpha_j = 1$. Suppose $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m)$, then PKG computes

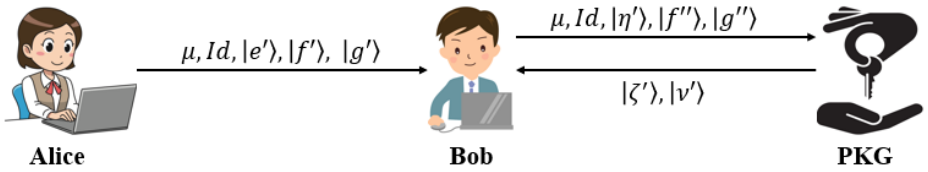
$$x = (x_1, x_2, \ldots, x_m) = \alpha \oplus \mu \oplus Id. \quad (31)$$

- PKG determines t using Eq. (23) with the private keys K, μ, and Id. The operation $H^{t_j}(Y^+)^{x_j}$ is then carried out by PKG on each $|f_j\rangle$ and $|g_j\rangle$. Then he receives

$$|\zeta_j\rangle = H^{t_j}(Y^+)^{x_j}|f_j\rangle \quad (32)$$

$$|\nu_j\rangle = H^{t_j}(Y^+)^{x_j}|g_j\rangle \quad (33)$$

  Assume that $|\zeta\rangle = \otimes_{j=1}^{m}|\zeta_j\rangle$ and $|\nu\rangle = \otimes_{j=1}^{m}|\nu_j\rangle$.
- In order to identify eavesdropping attacks, PKG generates $2q(q \ll m)$ decoy particles at random from a set of $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$. The quantum sequence $|\zeta\rangle$ is then randomly inserted with q decoy particles to produce the matching sequence $|\zeta'\rangle$. Similar to it, he generates the quantum sequence $|\nu'\rangle$ by randomly inserting the remaining q decoy particles into the quantum sequence $|\nu\rangle$. Finally, PKG gives Bob the sequences $|\zeta'\rangle$ and $|\nu'\rangle$.
- PKG communicates "all of the positions and initial states of forge particles in the quantum sequences $|\zeta'\rangle$ and $|\nu'\rangle$ after confirming that Bob has received $|\zeta'\rangle$ and $|\nu'\rangle$". Bob then compares the measurement results with each decoy particle's original condition after measuring each decoy particle with the appropriate foundation. Bob



- Alice determine $\alpha, \beta, \gamma, p, t, r$ and s.
- Alice compute $|e\rangle, |f\rangle$, and $|g\rangle$.
- Send $\mu, Id, |e'\rangle, |f'\rangle$, and $|g'\rangle$ to Bob .
- Bob checks eavesdropping, calculates and publishes v and θ.
- Bob retrieve $|e\rangle, |f\rangle, |g\rangle$ and $\{\mu, Id, v, \theta, |e\rangle, |f\rangle, |g\rangle\}$ as the quantum signature.
- Bob compute y, z and $|\eta\rangle$.
- Send $\mu, Id, |\eta'\rangle, |f''\rangle, |g''\rangle$ to PKG .
- PKG retrieve $|\eta\rangle, |f\rangle, |g\rangle$.
- Alice compute $|e\rangle, |f\rangle, |g\rangle$, compute and measures $|\alpha\rangle$. Then he gets x.
- PKG compute $t, |\zeta\rangle$ and $|\nu\rangle$.
- Send $|\zeta'\rangle$ and $|\nu'\rangle$ to Bob.
- Bob checks eavesdropping.
- Bob retrieve $|\zeta\rangle, |\nu\rangle$, and computes σ', ρ'. He proceeds by comparing σ & ρ with σ' and ρ' respectively.

FIGURE 1. The schematic of proposed QDVS.

completes the subsequent step if there are no mistakes; otherwise, he restarts the protocol.

- Following an evaluation of eavesdropping attacks, Bob is able to extract $|\zeta\rangle$ and $|\nu\rangle$ from $|\zeta'\rangle$ and $|\nu'\rangle$, accordingly. Bob determines r, s (using Eqs. (24) and (25)), μ, Id, and the secret parameters y and z. Then Bob executes on $|\zeta\rangle$ and $|\nu\rangle$ the operations H^{r_j} and H^{s_j}, respectively. Therefore, Bob gets

$$|s'_j\rangle = H^{r_j}|\zeta_j\rangle, \quad j = 1, 2, \ldots, m, \tag{34}$$
$$|r'_j\rangle = H^{s_j}|\nu_j\rangle, \quad j = 1, 2, \ldots, m. \tag{35}$$

Bob measures each $|s'_j\rangle$ with the basis of $|0\rangle$ and $|1\rangle$. If the measurement result is 0, Bob either sets $s_{j'} = 0$ or $s'_j = 1$. Let's say that $s' = (s'_1, s'_2, \ldots, s'_m)$. Similar to this, Bob measures each $|r'_j\rangle$ with a basis of $|0\rangle$ and $|1\rangle$. Bob either sets $r'_j = 0$ or $r'_j = 1$ if the measurement result is 0. Let $r' = (r'_1, r'_2, \ldots, r'_m)$. Next, Bob inverts s' or r' using the permutations H_3^{-1} and H_4^{-1} to obtain

$$\rho' = H_4^{-1}(s'), \tag{36}$$
$$\sigma' = H_3^{-1}(r'). \tag{37}$$

On the other hand, Bob determines σ by using Eqs. (19) and (20), μ, Id, and the secret parameters y and z. Before the conclusion, Bob compares (σ, ρ) with (σ', ρ'). Bob accepts the quantum signature if $\sigma = \sigma'$ and $\rho = \rho'$; otherwise, he rejects it.

IV. SECURITY ANALYSIS

A. CORRECTNESS

In this section, we provide the correctness of the verification and signature algorithm. Firstly, it is simple to prove that using Eqs. (19), (22), (26), and (29).

$$|\eta_j\rangle = H^{r_j}(Y^+)^{Z_j} \cdot Y^{z_j} H^{p_j \oplus t_j}|t_j\rangle \tag{38}$$

Second, based on Eqs. (32), (34) and (36), we get

$$\rho' = H_4^{-1}(sH^{r_j} \cdot H^{t_j}(Y^+)^{x_j}|f_j\rangle) \tag{39}$$

As a result, both the verification and the signature algorithm are correct.

In the following sections, we demonstrate that the selected verifier is also able to establish a quantum signature using the signer's private key, K. Fig. 1 briefly describes the schematic of the proposed protocol [46]. A security analysis [46] of the proposed protocol is done in the following subsections.

B. FORMAL SECURITY ANALYSIS

According to Menezes et al. [48] and Yang *et al.* [49], a "secure public-key cryptosystem" must be resistant to the "indistinguishably under chosen plaintext attack ($\mathcal{IND}-\mathcal{CPA}$)". Accordingly, under quantum $\mathcal{IND}-\mathcal{CPA}$ a "safe quantum public-key cryptosystem should be information-theoretically indistinguishable" [46], [50].

Definition 1: If the probability $Pr(\cdot)$ is satisfied for each quantum circuit family $\mathcal{C}_m$, each positive polynomial $P(\cdot)$, each fairly large m, and every bit-string a, b in plaintext space, then a quantum public-key encryption method is ciphertext-indistinguishable under a quantum chosen-plaintext attack.

Here,

$$|Pr[\mathcal{C}_m(\mathcal{E}_{\mathcal{L}(1^m)}(a)) = 1] - Pr[\mathcal{C}_m(\mathcal{E}_{\mathcal{L}(1^m)}(b)) = 1]| < \frac{1}{P(m)} \tag{40}$$

where $\mathcal{L}$ stands as the programme's internal coin tosser, $\mathcal{E}(a)$ and $\mathcal{E}(b)$ are ciphertexts, and $\mathcal{E}$ is a quantum encryption method. According to quantum $\mathcal{IND}-\mathcal{CPA}$, "a quantum public-key encryption protocol is information-theoretically equivalent to the trace distance between any two quantum ciphertext states is less than $1/P(m)$" [46], [50].

Theorem 1: Suppose $\mathcal{P}_a$ and $\mathcal{P}_b$ denote the density operators of the cipher states $\mathcal{E}(a)$ and $\mathcal{E}(b)$, respectively, for all plaintexts a and b. If a quantum public-key encryption system exhibits information-theoretic indistinguishably for all positive polynomials $P(\cdot)$ and sufficiently high values of m, then

$$D(\mathcal{P}_a, \mathcal{P}_b)| < \frac{1}{P(m)}. \tag{41}$$

Proof: Let μ and μ^* be the respective plaintext of the ciphertext $|e\rangle$ and $|e^*\rangle$, respectively. The density operators of $|e\rangle$ and $|e^*\rangle$ can accept any probable value of the private key K and the secret parameters x, y, and z for an adversary $\mathcal{A}$. Because α, p, and r satisfy Eqs. (19), (22) and (24), which state that x, K, y, H_1, and H_3 have uniform distributions. Therefore, α, p, and r also have uniform distributions. We may determine the density operator for $|e\rangle$.

$$\begin{aligned}\mathcal{P}_{e,\mu} &= \frac{1}{2^{4m}} \sum_{K,x,y,z} |e\rangle\langle e| \\ &= \frac{1}{2^{4m}} \sum_{p,r,\alpha,z} \otimes_{j=1}^{m} (Y^{z_j} H^{p_j \oplus t_j} |\alpha_j\rangle \langle \alpha_j| H^{p_j \oplus t_j} (Y^{+})^{z_j}) \\ &= \frac{1}{2}. \end{aligned} \tag{42}$$

On the same footing, we get the density operator for $|e^*\rangle$ as

$$\mathcal{P}_{e^*,\mu^*} = \frac{1}{2^{4m}} \sum_{K,x,y,z} |e^*\rangle\langle e^*| = \frac{1}{2^m}. \tag{43}$$

Hence,

$$\mathcal{D}(\mathcal{P}_{e,\mu}, \mathcal{P}_{e^*,\mu^*}) = 0. \tag{44}$$

Again, let μ and μ^* be the respective different plaintexts of the ciphertexts $|f\rangle$ and $|f^*\rangle$, respectively. The density operators of $|f\rangle$ and $|f^*\rangle$ can accept any probable value of the private key K and the secret parameters x, y, and z for an adversary $\mathcal{A}$. Since t, r and s satisfy Eqs. (23) – (25), which assume that K, y, z, H_2, H_3, and H_4 have uniform distributions, it follows that t, r and s also have uniform distributions. So, as follows, we may construct the density operator for $|f\rangle$.

Now,

$$\begin{aligned}\mathcal{P}_{f,\mu} &= \frac{1}{2^{4m}} \sum_{K,x,y,z} |f\rangle\langle f| \\ &= \frac{1}{2^{4m}} \sum_{p,r,\alpha,z} \otimes_{j=1}^{m} (Y^{x_j} H^{p_j \oplus r_j} |s_j\rangle \langle s_j| H^{p_j \oplus r_j} (Y^{+})^{x_j}) \\ &= \frac{1}{2}. \end{aligned} \tag{45}$$

The density operator for $|f^*\rangle$ is given by

$$\mathcal{P}_{f^*,\mu^*} = \frac{1}{2^{4m}} \sum_{K,x,y,z} |f^*\rangle\langle f^*| = \frac{1}{2^m}. \tag{46}$$

Hence,

$$\mathcal{D}(\mathcal{P}_{f,\mu}, \mathcal{P}_{f^*,\mu^*}) = 0. \tag{47}$$

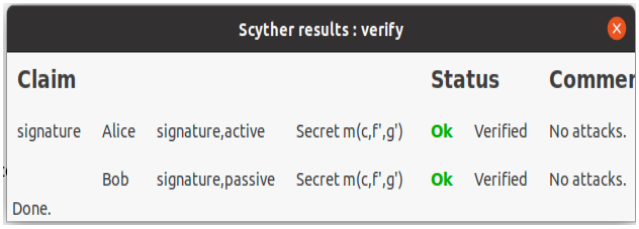


FIGURE 2. Security validation of the proposed protocol.

Let $|g\rangle$ and $|g^*\rangle$ represent, respectively, the ciphertexts of two distinct plaintexts μ and μ^*. Therefore, $\mathcal{P}_{g,\mu}, \mathcal{P}_{g^*,\mu^*}$ are, respectively, the density operators of $|g\rangle$ and $|g^*\rangle$. Using the same methodology as above, we can determine

$$\mathcal{D}(\mathcal{P}_{g,\mu}, \mathcal{P}_{g^*,\mu^*}) = 0. \tag{48}$$

Hence, by Definition 1, these bounds make the proposed quantum signature "information-theoretically $\mathcal{INDCPA}$ secure". □

C. INFORMAL SECURITY ANALYSIS

1) EAVESDROPPING ATTACKS

In our proposed protocol, the signer creates $3q$ decoy particles for monitoring eavesdropping attacks during the signature phase. These particles are chosen at random from the set $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$. A portion of the decoy particles is bound to be disturbed by an outside attacker's eavesdropping activity on the quantum channels, according to the security analysis of the quantum key distribution protocol provided in [47]. Therefore, Bob must also discover the eavesdropping activity on the quantum channels during the signature verification step.

2) NON-REPUDIATION

Non-repudiation should be a feature of a safe quantum signature scheme. That is, neither the signer nor the person who verifies signatures can contest the authenticity of a signature. PKG, a dependable third party for our signature, never shares the signer's private key. We can conclude that the proposed protocol is secure against forgery from Section IV-B. Therefore, neither the signer nor the verifier may challenge the validity of the quantum signature once the signature has passed verification.

3) DESIGNATED VERIFICATION PROPERTY

The secret pad $\mathcal{C}$ and the chosen verifier's private key K must be employed during the signature verification stage. Keep in mind that only Bob has access to the private key K and the secret pad $\mathcal{C}$. PKG has the ability to calculate the private key K but is ignorant of the pad $\mathcal{C}$. Without knowledge of the pad $\mathcal{C}$, PKG is unable to calculate ρ_j' in verification. Therefore, not even PKG can validate the QDVS. So, the designated verification attribute is present in our scheme.

4) HIDING SOURCE

Our QDVS protocol has the source-hiding security feature. In our system, the identical QDVS can be produced by both

the signer and the designated verifier. For a given signature, no one can distinguish between Alice and Bob as the original signer. Even if the private key K is made public, PKG and other parties cannot determine the signer's identity because

$$\rho' = H_4^{-1}(sH^{r_j} \cdot H^{t_j}(Y^+)^{x_j}|f_j\rangle) \tag{49}$$

which is perfectly symmetric for Alice and Bob. Therefore, our protocol has the ability to conceal the source.

5) NON-TRANSFERABILITY

According to the information provided in sections III-C and IV-A, it is evident that both Alice and Bob have the capability to produce identical QDVS for the message μ. The signature produced by Bob is indistinguishable from the one provided by Alice. Therefore, the chosen verifier is unable to provide evidence to any external entity that the signature was generated by either the signer or themselves. Consequently, QDVS cannot be transferred.

6) UNFORGEABILITY

Under the supposition that the density operator against the polynomial-time algorithm is complex, the QDVS scheme is shown to be existentially unforgeable against strong adversaries in the random oracle model. Thus, the subsection IV-B contains Theorem 1 for adversary.

D. FORMAL SECURITY VERIFICATION USING SCYTHER TOOL

A widely used software toolkit, called Scyther [51], has been used for simulation. It contains a ''graphical user interface (GUI)'' which uses the ''command-line'' and ''Python scripting interfaces''. These help the utilization of Scyther in a ''large-scale protocol verification'' test.

We have checked the security validation against the issues of ''confidentiality'', ''authorization'', ''accessibility'', ''reachability'', ''credibility'' and ''integrity''. Most importantly, we have checked the ''issue of secrecy of all the credentials (secret keys, identity, random numbers, parameters, and time)''. However, the results produced by the entire protocol simulation code indicate that these issues are secure from any threats and undesirable events. The outcome of security validation of the proposed protocol against active and passive attacks is shown in Fig. 2.

V. COMPARATIVE STUDY WITH OTHER SCHEMES

The proposed protocol is evaluated with some existing protocols on the premises of various security features in Table 2. Considered parameters of the comparison are the following: a) number of signatures, b) security, c) privacy, d) algorithm complexity, e) security against PKG's forgery attacks, f) ''reusability of the public key'', and g) ''requirement for quantum swap test''. Lucidly, it can be depicted from the comparison Table 2 that the proposed scheme provides a number of advantages over the preexisting protocols.

```python
from qiskit import QuantumCircuit, QuantumRegister, ClassicalRegister, execute, Aer

def hadamard_qubit(qc, qr):
    qc.h(qr)

def generate_keys_circuit(n):
    private_key_qr = QuantumRegister(n, name='K')
    public_key_qr = QuantumRegister(n, name='G')
    qc = QuantumCircuit(private_key_qr, public_key_qr)

    for i in range(n):
        hadamard_qubit(qc, private_key_qr[i])
        hadamard_qubit(qc, public_key_qr[i])

    return qc

def sign_circuit(qc, message, private_key_qr):
    for i, bit in enumerate(message):
        if bit == 1:
            qc.z(private_key_qr[i])

def verify_circuit(qc, message, signature, public_key_qr):
    for i, bit in enumerate(message):
        if bit == 1:
            qc.z(public_key_qr[i])

    for i, bit in enumerate(signature):
        if bit == 1:
            qc.z(public_key_qr[i])


def generate_keys_circuit(n):
          n =  16
    message = [0, 1, 1, 0, 1, 0, 0, 1]
    private_key_qr = QuantumRegister(n, name='K')
    public_key_qr = QuantumRegister(n, name='G')
    message_qr = QuantumRegister(n, name='message')
    signature_qr = QuantumRegister(n, name='signature')
    verify_qr = QuantumRegister(n, name='verify')
    c = ClassicalRegister(n, name='c')
    qc = QuantumCircuit(private_key_qr, public_key_qr, message_qr, signature_qr, verify_qr, c)
```

FIGURE 3. Simulation code of the proposed scheme.

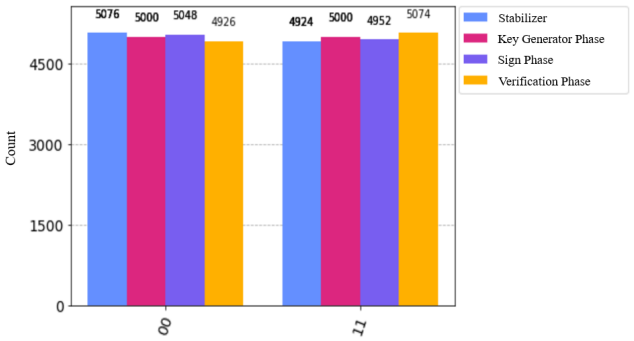


FIGURE 4. Measurement of states used in various phases of the proposed scheme.

VI. SIMULATION RESULTS AND DISCUSSIONS

A. SIMULATION USING PYTHON

The proposed protocol is then further tested for effectiveness using a Python simulation of the signature scheme. For simulation, we use quantum bit rather than classical bit. The no-cloning theorem and the uncertainty principle provide the quantum security to the proposed protocol. we use the ''Qiskit'' and ''pylatexenc'' libraries for quantum simulations.

B. SIMULATION ENVIRONMENT

The considered simulation environment consists of the following:

TABLE 2. Comparison of security features with existing schemes.

Scheme	[15]	[25]	[26]	[27]	[28]	[29]	[30]	[31]	Proposed
Number of signatures	Single	Single	Single	Single	Single	Single	More than two	More than two	Single
Security	×	×	✓	✓	✓	✓	✓	×	✓
Privacy	–	–	×	✓	×	×	✓	✓	✓
Algorithm complexity	Security depends on algorithm complexity	Security depends on algorithm complexity	Security depends on algorithm complexity	Security depends on algorithm complexity	Security depends on algorithm complexity	Security depends on algorithm complexity	Security depends on algorithm complexity	Security independents on algorithm complexity	Security independents on algorithm complexity
Security against PKG's forgery attacks	–	×	✓	✓	✓	✓	✓	✓	✓
Public key reusability	×	✓	×	✓	✓	✓	✓	✓	✓
Quantum swap Requirement test	✓	✓	✓	✓	✓	✓	✓	✓	×

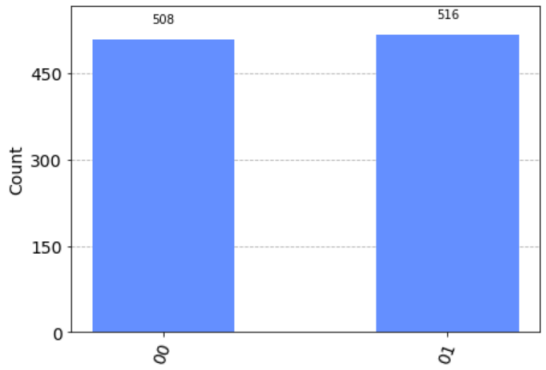


FIGURE 5. Measurement of states used in signing phase.

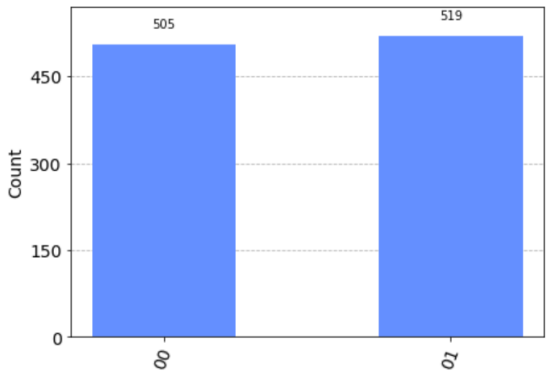


FIGURE 6. Measurement of states used in verification phase.

- *Hardware environment:* We conducted experiments on a machine using 11^{th} Gen Intel(R) Core(TM) i7-1165G7 laptop @ 2.80GHz processor.
- *Software environment:* We use Python 3.8.11 coding using GMP and compiling with the optimization option using appropriate parameters. The AerSimulator backend operates by design by mimicking a real device's operation. If a quantum circuit with measurements is performed, then a "count dictionary holding the final values of any classical registers in the circuit will be returned". A customized simulator instruction set covered in a different notebook may be in the circuit, including gates, measurements, resets, conditionals, and other elements.

C. ANALYSIS OF SIMULATED DATA

The implementation code used is provided in Fig. 3. The file has been splitted across several data of q-bits. The proposed scheme has improved signature efficiency as shown in Fig. 4. Therefore, we put the efficiency simulation of signature verification into action.

The effectiveness of verification with fixed q-bits is the subject of simulations. When the size of the user's data in q-bits is fixed. Additionally, Fig. 5 and Fig. 6 are obtained from the simulations and represent the measurement of states used in the sign and verification phases, respectively. Lucidly, we can observe from Fig. 4 that the measurement of states used in various phases of our protocol.

VII. CONCLUSION

We proposed a QDVS protocol based on identity. The proposed scheme features security attributes such as eavesdropping attacks, non-repudiation, and designated verification property by hiding source. Also, it is protected from attacks on forgery, interception, and impersonation. The signer's public key, which serves as identifying information, is generated by PKG. The signer uses a private key to encrypt a message, and the quantum signature corresponding to that encryption is validated using the identities of the signer and the selected verifier without the use of any quantum key certificates which makes the quantum signature system's key management faster. Moreover, the scheme does not require the verifier to compare quantum states during the signature verification step. Therefore, the proposed protocol is more practicable, secure, and efficient.

REFERENCES

[1] X. Xin, Z. Wang, Q. Yang, and F. Li, "Identity-based quantum designated verifier signature," *Int. J. Theor. Phys.*, vol. 59, no. 3, pp. 918–929, Mar. 2020.

[2] J. C. Choon and J. Hee Cheon, "An identity-based signature from gap Diffie–Hellman groups," in *Public Key Cryptography—PKC 2003*. Cham, Switzerland: Springer, 2002, pp. 18–30.

[3] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 1996, pp. 143–154.

[4] S. Saeednia, S. Kremer, and O. Markowitch, "An efficient strong designated verifier signature scheme," in *Proc. ICISC*. Cham, Switzerland: Springer, 2004, pp. 40–54.

[5] B. Kang, C. Boyd, and E. Dawson, "A novel identity-based strong designated verifier signature scheme," *J. Syst. Softw.*, vol. 82, no. 2, pp. 270–273, Feb. 2009.

[6] V. Kuchta, R. A. Sahu, V. Saraswat, G. Sharma, N. Sharma, and O. Markowitch, "Anonymous yet traceable strong designated verifier signature," in *Proc. ISC*. Cham, Switzerland: Springer, 2018, pp. 403–421.

[7] P. Rastegari, M. Berenjkoub, M. Dakhilalian, and W. Susilo, "Universal designated verifier signature scheme with non-delegatability in the standard model," *Inf. Sci.*, vol. 479, pp. 321–334, Apr. 2019.

[8] G. K. Verma, B. B. Singh, and H. Singh, "Bandwidth efficient designated verifier proxy signature scheme for healthcare wireless sensor networks," *Ad Hoc Netw.*, vol. 81, pp. 100–108, Dec. 2018.

[9] P. Rastegari, W. Susilo, and M. Dakhilalian, "Certificateless designated verifier signature revisited: Achieving a concrete scheme in the standard model," *Int. J. Inf. Secur.*, vol. 18, no. 5, pp. 619–635, Oct. 2019.

[10] A. U. Khan, B. K. Ratha, and S. Mohanty, "A timestamp-based strong designated verifier signature scheme for next-generation network security services," in *Proc. ICCCCS*, vol. 1. Cham, Switzerland: Springer, 2017, pp. 311–320.

[11] F. Ye, Z. Zhou, and Y. Li, "Quantum-assisted blockchain for IoT based on quantum signature," *Quantum Inf. Process.*, vol. 21, no. 9, p. 327, Sep. 2022.

[12] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, Jan. 1999.

[13] W.-M. Shi, Y.-H. Zhou, and Y.-G. Yang, "A real quantum designated verifier signature scheme," *Int. J. Theor. Phys.*, vol. 54, no. 9, pp. 3115–3123, Sep. 2015.

[14] W.-M. Shi, Y.-M. Wang, Y.-H. Zhou, Y.-G. Yang, and J.-B. Zhang, "A scheme on converting quantum signature with public verifiability into quantum designated verifier signature," *Optik*, vol. 164, pp. 753–759, Jul. 2018.

[15] D. Gottesman and I. Chuang, "Quantum digital signatures," 2001, *arXiv:quant-ph/0105032*.

[16] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, "Quantum fingerprinting," *Phys. Rev. Lett.*, vol. 87, no. 16, Sep. 2001, Art. no. 167902.

[17] G. Zeng and C. H. Keitel, "Arbitrated quantum-signature scheme," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 4, Apr. 2002, Art. no. 042312.

[18] Y.-G. Yang, H. Lei, Z.-C. Liu, Y.-H. Zhou, and W.-M. Shi, "Arbitrated quantum signature scheme based on cluster states," *Quantum Inf. Process.*, vol. 15, no. 6, pp. 2487–2497, Jun. 2016.

[19] Y.-G. Yang, Z. Zhou, Y.-W. Teng, and Q.-Y. Wen, "Arbitrated quantum signature with an untrusted arbitrator," *Eur. Phys. J. D*, vol. 61, no. 3, pp. 773–778, Feb. 2011.

[20] T.-Y. Wang and Z.-L. Wei, "One-time proxy signature based on quantum cryptography," *Quantum Inf. Process.*, vol. 11, no. 2, pp. 455–463, Apr. 2012.

[21] T.-Y. Wang and Z.-L. Wei, "Analysis of forgery attack on one-time proxy signature and the improvement," *Int. J. Theor. Phys.*, vol. 55, no. 2, pp. 743–745, Feb. 2016.

[22] X. Xin, Q. He, Z. Wang, Q. Yang, and F. Li, "Security analysis and improvement of an arbitrated quantum signature scheme," *Optik*, vol. 189, pp. 23–31, Jul. 2019.

[23] M. N. S. Perera, T. Nakamura, M. Hashimoto, H. Yokoyama, and K. Sakurai, "Almost fully anonymous attribute-based group signatures with verifier-local revocation and member registration from lattice assumptions," *Theor. Comput. Sci.*, vol. 891, pp. 131–148, Nov. 2021.

[24] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*. Cham, Switzerland: Springer, 1985, pp. 47–53.

[25] F.-L. Chen, W.-F. Liu, S.-G. Chen, and Z.-H. Wang, "Public-key quantum digital signature scheme with one-time pad private-key," *Quantum Inf. Process.*, vol. 17, no. 1, pp. 1–14, Jan. 2018.

[26] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, pp. 20632–20640, 2018.

[27] X. Xin, Z. Wang, Q. Yang, and F. Li, "Efficient identity-based public-key quantum signature scheme," *Int. J. Mod. Phys. B*, vol. 34, no. 10, Apr. 2020, Art. no. 2050087.

[28] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.

[29] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep. 2018.

[30] X.-F. Niu, J.-Z. Zhang, S.-C. Xie, and B.-Q. Chen, "A practical e-payment protocol based on quantum multi-proxy blind signature," *Commun. Theor. Phys.*, vol. 70, no. 5, p. 529, Nov. 2018.

[31] L. Yan, Y. Chang, S. Zhang, G. Han, and Z. Sheng, "A quantum multi-proxy weak blind signature scheme based on entanglement swapping," *Int. J. Theor. Phys.*, vol. 56, no. 2, pp. 634–642, Feb. 2017.

[32] F. Miller, *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams*. C.M. Cornwell, 1882. [Online]. Available: https://books.google.co.in/books?id=tT9WAAAAYAAJ

[33] S. M. Bellovin, "Frank Miller: Inventor of the one-time pad," *Cryptologia*, vol. 35, no. 3, pp. 203–222, Jul. 2011.

[34] M. Ghafourian, J. Fierrez, R. Vera-Rodriguez, A. Morales, and I. Serna, "OTB-Morph: One-time biometrics via morphing," *Mach. Intell. Res.*, vol. 20, no. 6, pp. 855–871, Dec. 2023.

[35] M. de Ree, G. Mantas, and J. Rodriguez, "A cryptographic perspective to achieve practical physical layer security," in *Proc. IEEE Global Commun. Conf.*, Dec. 2022, pp. 4038–4043.

[36] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[37] M. Hirvensalo, *Quantum Computing*. Cham, Switzerland: Springer, 2003.

[38] V. Vedral, "Quantum entanglement," *Nature Phys.*, vol. 10, no. 4, pp. 256–258, 2014.

[39] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Rev. Mod. Phys.*, vol. 81, p. 865, Jun. 2009.

[40] S. Pratap, "Transport properties of zigzag graphene nanoribbons in the confined region of potential well," *Superlattices Microstruct.*, vol. 100, pp. 673–682, Jan. 2016.

[41] J. L. Hevia, G. Peterssen, C. Ebert, and M. Piattini, "Quantum computing," *IEEE Softw.*, vol. 38, no. 5, pp. 7–15, Sep. 2021.

[42] V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 3, pp. 1844–1852, Sep. 1996.

[43] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

[44] H. Y. Wong, "No-cloning theorem and quantum teleportation I," in *Introduction to Quantum Computing*. Cham, Switzerland: Springer, 2022, pp. 173–182.

[45] N. Zettili, *Quantum Mechanics: Concepts and Applications*. American Association of Physics Teachers, 2003.

[46] X. Xin, Z. Wang, and Q. Yang, "Identity-based quantum signature scheme with strong security," *Opt. Quantum Electron.*, vol. 51, no. 12, pp. 1–13, Dec. 2019.

[47] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," 2020, *arXiv:2003.06557*.

[48] A. Menezes, P. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

[49] L. Yang, B. Yang, and J. Pan, "Quantum public-key encryption protocols with information-theoretic security," *Proc. SPIE*, vol. 8440, pp. 71–77, Jan. 2012.

[50] Y. Li, X. Chong, and L. Bao, "Quantum probabilistic encryption scheme based on conjugate coding," *China Commun.*, vol. 10, no. 2, pp. 19–26, Feb. 2013.

[51] C. J. F. Cremers, "The Scyther tool: Verification, falsification, and analysis of security protocols: Tool paper," in *Computer Aided Verification*. Berlin, Heidelberg: Springer, 2008, pp. 414–418.

SUNIL PRAJAPAT (Associate Member, IEEE) received the M.Sc. degree in mathematics from the Central University of Himachal Pradesh, Dharamshala, Himachal Pradesh, India, where he is currently pursuing the Ph.D. degree with the Srinivasa Ramanujan Department of Mathematics. His research interests include quantum cryptography and post-quantum cryptography, coding theory, blockchain, and various applications of cryptographic primitives in the real world.

PANKAJ KUMAR received the M.Sc. degree from Chaudhary Charan Singh University, Meerut, India, in 2005, and the Ph.D. degree from Galgotias University, in 2020. He has been an Assistant Professor with the Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, Dharamshala, Himachal Pradesh. He has published more than 40 academic research papers on information security and privacy preservation. His current research interests include cryptography, blockchain, wireless network security, information theory, and network coding.

SANDEEP KUMAR received the M.Sc. degree in physics from Kurukshetra University, Kurukshetra, Haryana, India. He is currently pursuing the Ph.D. degree with the Department of Physics and Astronomical Sciences, Central University of Himachal Pradesh, Dharamshala, Himachal Pradesh, India. His research interests include quantum transportation in low-dimensional material and quantum cryptography.

ASHOK KUMAR DAS (Senior Member, IEEE) received the M.Sc. degree in mathematics, the M.Tech. degree in computer science and data processing, and the Ph.D. degree in computer science and engineering from IIT Kharagpur, India. He is currently a Full Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India, and a Visiting Faculty with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA, USA. His Google Scholar H-index is 83 and i10-index is 251 with over 19,700 citations. His research interests include cryptography, system and network security, blockchain, security in the Internet of Things (IoT), the Internet of Vehicles (IoV), the Internet of Drones (IoD), smart grids, smart city, cloud/fog computing, intrusion detection, AI/ML security, and post-quantum cryptography. He has authored over 385 papers in international journals and conferences in the above areas, including more than 325 reputed journal articles. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He served as one of the Technical Program Committee Chairs for the first International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, in June 2019, the International Conference on Applied Soft Computing and Communication Networks (ACN'20), Chennai, India, in October 2020, and the second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, in October 2020. He is/was on the editorial board of IEEE Systems Journal, *Journal of Network and Computer Applications* (Elsevier), *Computer Communications* (Elsevier), *Journal of Cloud Computing* (Springer), *Cyber Security and Applications* (Elsevier), *IET Communications*, *KSII Transactions on Internet and Information Systems*, and *International Journal of Internet Technology and Secured Transactions* (Inderscience). He has been listed in the Web of Science (Clarivate^{TM}) Highly Cited Researcher in recognition of his exceptional research performance, in 2022 and 2023.

SACHIN SHETTY (Senior Member, IEEE) received the Ph.D. degree in modeling and simulation from Old Dominion University, in 2007. He was an Associate Professor with the Department of Electrical and Computer Engineering, Tennessee State University, USA. He is currently a Professor with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University. He holds a joint appointment with the Department of Modeling, Simulation and Visualization Engineering and the Center for Cybersecurity Education and Research. He has authored or coauthored over 200 research articles in journals and conference proceedings and two books. His research interests include the intersection of computer networking, network security, and machine learning. He was a recipient of the DHS Scientific Leadership Award. He has served as the Technical Program Committee Member for ACM CCS, IEEE INFOCOM, IEEE ICDCN, and IEEE ICCCN.

M. SHAMIM HOSSAIN (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, ON, Canada, in 2009. He is currently a Professor with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He is also an Adjunct Professor with the School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON, Canada. He has authored and coauthored more than 355 publications, including refereed journals (280+SCI/ISI-Indexed papers, 150+IEEE/ACM Transactions/Journal articles, 23+ESI Highly Cited Papers, two Hot Papers), conference papers, books, and book chapters. His research interests include cloud networking, smart environment (smart city, smart health), AI, deep learning, edge computing, the Internet of Things (IoT), multimedia for health care, and multimedia big data. He has served as the co-chair, general chair, workshop chair, publication chair, and TPC in several IEEE and ACM conferences. He is the Chair of the IEEE Special Interest Group on Artificial Intelligence (AI) for Health with the IEEE ComSoc eHealth Technical Committee and the Saudi Arabia Section of the Instrumentation and Measurement Society Chapter, the Organizing Co-Chair of the Special Sessions with IEEE I2MTC 2022, the Symposium Chair of Selected Areas in Communications (E-Health) with IEEE GLOBECOM 2024, and the Technical Program Co-Chair of ACM Multimedia 2023. He serves as the Co-Chair for the 1st, 2nd, and 3rd IEEE GLOBECOM Workshop on Edge-AI and IoT for Connected Health. He was a recipient of a number of awards, including the Best Conference Paper Award, the 2016 *ACM Transactions on Multimedia Computing, Communications and Applications* (TOMM) Nicolas D. Georganas Best Paper Award, the 2019 King Saud University Scientific Excellence Award (Research Quality), and the Research in Excellence Award from the College of Computer and Information Sciences (CCIS), King Saud University (3 times in a row). He is on the editorial board of the IEEE Transactions on Instrumentation and Measurement (TIM), IEEE Transactions on Multimedia (TMM), *ACM Transactions on Multimedia Computing, Communications, and Applications* (TOMM), IEEE Multimedia, *IEEE Network*, IEEE Wireless Communications, *Journal of Network and Computer Applications* (Elsevier), and *Games for Health Journal*. He has served as a Lead Guest Editor for more than two dozen of Special Issues (SIs), including *ACM Transactions on Multimedia Computing, Communications, and Applications*, *ACM Transactions on Internet Technology*, IEEE Transactions on Consumer Electronics, *IEEE Communications Magazine*, *IEEE Network*, IEEE Transactions on Information Technology in Biomedicine (currently JBHI), IEEE Transactions on Cloud Computing, *International Journal of Multimedia Tools and Applications* (Springer), *Cluster Computing* (Springer), and *Future Generation Computer Systems* (Elsevier). He is a Distinguished Member of the ACM and an IEEE Distinguished Lecturer (DL). He is the Highly Cited Researcher in the field of Computer Science (Web of Science^{TM}).