Article

Designing a Robust Quantum Signature Protocol Based on Quantum Key Distribution for E-Voting Applications

Sunil Prajapat, Urmika Gautam, Deepika Gautam, Pankaj Kumar and Athanasios V. Vasilakos

Article

Designing a Robust Quantum Signature Protocol Based on Quantum Key Distribution for E-Voting Applications

Sunil Prajapat [1], Urmika Gautam [1], Deepika Gautam [1], Pankaj Kumar [1,*] and Athanasios V. Vasilakos [2,3,*]

1 Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh,
Dharamshala 176215, India; cuhp21rdmath13@hpcu.ac.in (S.P.); urmika52@gmail.com (U.G.);
cuhp21rdmath05@hpcu.ac.in (D.G.)
2 Department of Networks and Communications, College of Computer Science and Information Technology,
Imam Abdulrahman Bin Faisal University (IAU), P.O. Box 1982, Dammam 31441, Saudi Arabia
3 Center for AI Research (CAIR), University of Agder (UiA), 4879 Grimstad, Norway
* Correspondence: pkumar240183@hpcu.ac.in (P.K.); thanos.vasilakos@uia.no (A.V.V.)

Abstract: The rapid advancement of internet technology has raised attention to the importance of electronic voting in maintaining democracy and fairness in elections. E-voting refers to the use of electronic technology to facilitate the casting and counting of votes in elections. The need for designated verification arises from concerns about voter privacy, auditability, and the prevention of manipulation. Traditional e-voting systems use cryptographic techniques for security but lack verifiable proof of integrity. Integrating e-voting with a quantum designated verifier could address these challenges by leveraging the principles of quantum mechanics to enhance security and trustworthiness. In light of this, we propose a quantum e-voting scheme that uses a designated verifier signature. To ensure the confidentiality and authenticity of the voting process, the scheme uses quantum features like the no-cloning theorem and quantum key distribution. The proposed scheme has security properties like source hiding, non-transferability, and message anonymity. The proposed scheme is resistant to many quantum attacks, such as eavesdropping and impersonation. Due to designated verification, the scheme minimizes the risk of tempering. This paper provides a detailed description of the proposed scheme and analyzes its security properties. Therefore, the proposed scheme is efficient, practical, and secure.

Keywords: quantum electronic voting; designated verifier; quantum key distribution; signature; unconditional security

MSC: 81P94

1. Introduction

Voting has always been crucial in democratic processes, and in the context of internet development, the voting system is evolving to meet the demands of modern society. In the traditional voting system, voters cast their paper ballots in person at the polling station. However, driven by the need for efficiency, accessibility, accuracy, and the dynamic requirements of elections, this paper-based voting method has been replaced with an electronic voting system. E-voting is an electronic system for collaborative decision-making or voting, with the potential to make casting votes easier and more inclusive [1]. It handles voter registration, vote input and casting, encryption, transmission, storage, counting, and result tabulation. E-voting systems not only minimize the time spent voting and counting but also reduce human errors in the voting process. The entities involved in electronic voting include election authorities, voters, and the tally clerk [2]. Election authorities are responsible for initiating voting activities, including determining the list of candidates, legitimate voters, and other relevant parameters. The role of voters is to cast a legal vote on voting content initiated by election authorities and to generate a valid signature on their ballots. Meanwhile, the tally clerks verify and count each vote and then announce the result [3].

While e-voting has advantages in terms of security, convenience, and accuracy compared with manual voting, there are still areas that require improvement in electronic voting systems. The primary concerns of these systems are regarding the confidentiality and verifiability of ballots, scalability, and vulnerabilities against cyber-attacks, including hacking, manipulation, and unauthorized access, potentially compromising the accuracy of election results [4]. Additionally, substantial privacy concerns regarding potential identity theft, vote purchasing, and coercion can damage voter anonymity. These inherent challenges underscore the urgent need for more secure, private, scalable, and transparent alternatives to electronic voting.

Cryptographic protocols such as encryption, signature, and authentication are the underlying components that provide security against several security threats in the e-voting system [5]. Numerous signature and authentication protocols are in the literature. Furthermore, currently deployed systems such as the Estonian one, Helios, and the Swiss voting system employ cryptographic protocols whose security depends on computationally hard problems such as factoring large numbers or resolving discrete logarithm problems. However, with the development of quantum computers, the security of these cryptographic approaches is challenging because of their ability to efficiently solve these problems [6]. Hence, the significant processing power of quantum computers poses a potential threat to conventional cryptography, making widely used algorithms susceptible to Shor's algorithm [7]. Therefore, it makes the classical e-voting system vulnerable to quantum attacks. It is imperative to find solutions that not only resolve the inherent challenges of classical e-voting but also resolve quantum challenges.

A novel approach called "quantum e-voting" uses quantum mechanics and offers potential solutions that enhance the robustness and security of electronic voting systems. Quantum voting approaches depend on the principles of quantum mechanics, such as the no-cloning theorem, quantum entanglement, and the Heisenberg Uncertainty Principle [8]. Quantum electronic voting uses quantum phenomena in encryption and secure transmission protocols to encode and protect voting data, ensuring voter privacy and making it extremely difficult for third parties to access or manipulate voter information [9]. Furthermore, because of quantum computing's inherent parallelism and computational power, it can handle a significantly larger number of voters. Quantum e-voting, which uses quantum cryptographic techniques, can provide security and verifiability. Quantum cryptography has become a significant area in secure communication, drawing on the fundamental principles of quantum mechanics. Quantum cryptography-based authentication and signature protocols have emerged, attracting the attention of researchers and academia. A quantum-designated verifier signature (QDVS) is a digital signature that is applicable in various applications, including electronic voting systems [10]. In the context of e-voting, a designated verifier is an entity that can verify the integrity of a quantum signature without being able to transfer the conviction to any third party [11]. Voters can ensure verifiability and confidentiality by employing this to prove the authenticity of their votes without revealing their exact content. QDVS employs the principles of quantum mechanics, such as quantum entanglement and superposition, which also provide security against quantum attacks [12]. Therefore, this integration of quantum cryptography and quantum e-voting is able to resolve the intrinsic challenges and quantum threats of the classical voting system.

1.1. Motivation and Research Contribution

The rise of quantum computers has resulted in security concerns in classical DVS systems. This prompted us to develop a quantum-designated verifier scheme based on identity that offers improved security and efficiency. Our aim is to overcome significant challenges by exploring the domain of quantum security. Moreover, this motivation emphasizes the significance of participating in the development of novel cryptographic methods that use quantum principles. As a result, we have proposed a scheme for electronic voting that uses quantum-designated verifier signatures. The main contributions of our work are as follows:

- Firstly, an identity-based quantum designated verifier signature scheme for e-voting is proposed. This framework incorporates important security properties and is a unique approach.
- Secondly, a comprehensive security analysis is conducted to ensure the robustness of the proposed quantum signature framework. The framework demonstrates resilience against various cryptographic attacks.
- Thirdly, our scheme is implemented using the programming language Python and the tool Scyther, which effectively combines execution and simulation. We carefully evaluate the costs and advantages of our protocol and find that it is well suited for secure communication.

In summary, our study introduces a secure e-voting scheme and a resilient quantum signature framework and demonstrates the effectiveness of our protocol in real-world scenarios.

1.2. Related Work

Several studies have proposed different approaches for designing robust quantum signature protocols for e-voting applications. In 2006, Hillery et al. [13] introduced the concept of the traveling ballot and distributed ballot schemes for quantum voting. Ensuring privacy in communication, especially in contexts such as fair voting, is crucial. This study examines the use of quantum resources to enhance privacy levels and presents novel quantum protocols. The discussion also considers the potential for secure voting schemes, emphasizing the progress in quantum communication for protecting sensitive interactions.

In 2007, Vaccaro et al. proposed a quantum protocol for voting and surveying [14]. In their scheme, quantum protocols offer anonymity and efficient tallying through entangled states, providing significant reduction computational complexity compared with classical schemes. Horoshko et al. [15] proposed a quantum anonymous voting with an anonymity check. Their proposed work offers robust protection against both curious tallymen and dishonest voters. It allows voters to verify anonymity through entangled states, and any attempted cheating by the tallyman is detectable, ensuring the integrity of the voting process.

In 2017, Zhang et al. [1] proposed a quantum signature protocol based on entanglement swapping. The scheme applies the physical attributes of quantum mechanics to enable voting, counting, and immediate supervision. The quantum voting scheme leverages the quantum proxy blind signature and Charlie's oversight to ensure fairness and prevent manipulation by Bob. In their protocol, the designated verifier can verify the signature without knowing the signed message by exploiting the entanglement between the signer and the verifier.

In 2021, Li et al. [16] proposed a quantum voting protocol using unitary operations and encrypted ballots based on single-particle states that offers a secure and tamper-resistant approach for selecting multiple winners. The implemented grouping strategies effectively mitigate the impact of candidate and voter numbers on quantum state preparation, reinforcing the protocol's resilience against various malicious attacks.

In 2021, Zheng et al. [17] proposed a practical quantum designated verifier signature scheme for e-voting applications. They also claimed that existing quantum designated verifier signature (QDVS) schemes pose challenges in implementation. This study introduced a practical QDVS scheme tailored for E-voting applications. The proposed scheme uses quantum key distribution (QKD) without entanglement, offering straightforward deployment over existing networks while satisfying the main security requirements. It also demonstrates the demonstrating resilience against common cyber-attacks. The majority of voting protocols rely on quantum entanglement, which is challenging because of decoherence effects. Eliminating the requirement of entanglement is a significant advancement toward practical quantum voting protocols. A Quantum Electronic voting scheme is proposed in this paper, which is based on a quantum-designated verifier. The proposed scheme is an ID-based scheme that uses quantum key distribution for the distribution of keys. One time pad (OTP) [18] is also used in our proposed scheme, which ensures security by using each key only once, preventing information leakage and enhancing the privacy and authenticity

of the quantum signature. The key used for signature generation is never reused, making it resistant to cryptographic attacks.

1.3. Paper Structure

This paper is structured as follows: Section 2 discusses the system model of the proposed scheme. Section 3 discusses the proposed e-voting scheme. Section 4 examines the security analysis of the proposed scheme. Section 5 evaluates the performance of the proposed scheme. Finally, the paper is concluded in Section 6.

2. Quantum E-Voting System

There are three participants involved in our scheme: voters—individuals casting their votes electronically; election authority—responsible for managing keys and overseeing the election; and tally clerk—who verifies the authenticity of the votes. Each participant is connected to the election authority. Several specific properties of the quantum e-voting system are described below Figure 1.
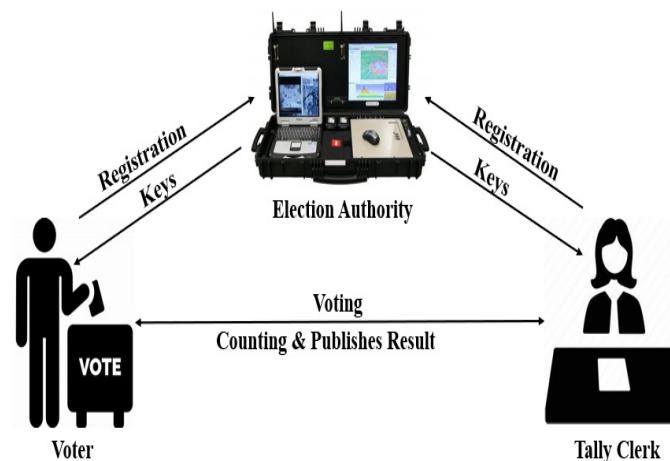

Figure 1. System model.

1. The election authority has many quantum resources and computational capabilities, whereas participants in the same domain have limited resources.
2. Through the election authority, participants exchange distributed and correlated key strings by executing the quantum portion of quantum key distribution (QKD).
3. A designated participant acts as the voter and tally clerk to start electronic voting. The election authority sends the voting content as a judgment question to the other participants.
4. Other participants create pre-signatures for a one-bit answer. Bit 1 (Yes) indicates approval, while bit 0 (No) indicates disapproval, serving as their ballots.
5. Participants send their pre-signatures to the election authority and ask for actual signatures to be sent to the ballot collector.
6. The ballot collector gathers all signatures and counts the number of ballots issued, concluding the voting process.

3. Preliminaries

In this particular section, we describe the fundamental concepts that are of assistance in the domain of quantum computing. In addition, we discuss the fundamental principles of quantum mechanics that are employed in our proposed framework.

3.1. No-Cloning Theorem

The no-cloning theorem was first formulated in 1982 by Wootters, Zurek, and Dieks [19]. It states that it is impossible to create an identical copy (or clone) of an arbitrary unknown quantum state. This theorem is important for quantum information and computing. In

classical information theory, the act of duplicating information is typically possible, but this is not the case in the quantum realm. The no-cloning theorem posits that the replication of an arbitrary unknown quantum state with complete precision is not feasible. This limitation is related to quantum superposition and entanglement. It implies that measuring or copying a quantum state disturbs it and perfect copies of quantum information cannot be made. This limitation affects cryptographic protocols, quantum information processing, and quantum communication systems' unique features and security.

3.2. Heisenberg Uncertainty Principle

The Heisenberg Uncertainty Principle was introduced in 1927 by German physicist Werner Heisenberg [20]. It explains that some physical properties cannot be measured with complete accuracy. More precise knowledge of one property leads to less precise knowledge of another.

Mathematically, the Heisenberg Uncertainty Principle is commonly expressed as:

$$\Delta x . \Delta p \geq h/2 \tag{1}$$

where:

Δx is the uncertainty in position.
Δp is the uncertainty in momentum.
h is the reduced Planck constant, approximately equal to 1.054571×10^{-34} Js.

The Heisenberg Uncertainty Principle sets constraints on how well certain pairs of properties can be known at the same time. This is a fundamental aspect of quantum systems, not due to experimental constraints. The more precisely one measures position, the less precisely momentum can be determined. The principle has profound implications for understanding particle behavior at the quantum level and has far-reaching consequences in quantum fields. It challenges the classical intuition and assumes a central position in the establishment of quantum mechanics.

3.3. Quantum Key Distribution (QKD)

Quantum key distribution (QKD) is a cryptographic method that allows two parties, often called Alice and Bob, to create a shared secret key over an unsecured channel (Figure 2). This key is utilized for encrypting and decrypting messages, guaranteeing secure communication between the two parties. QKD protocols are built to withstand different eavesdropping attempts by leveraging principles from quantum mechanics like the uncertainty principle and the no-cloning theorem [21].
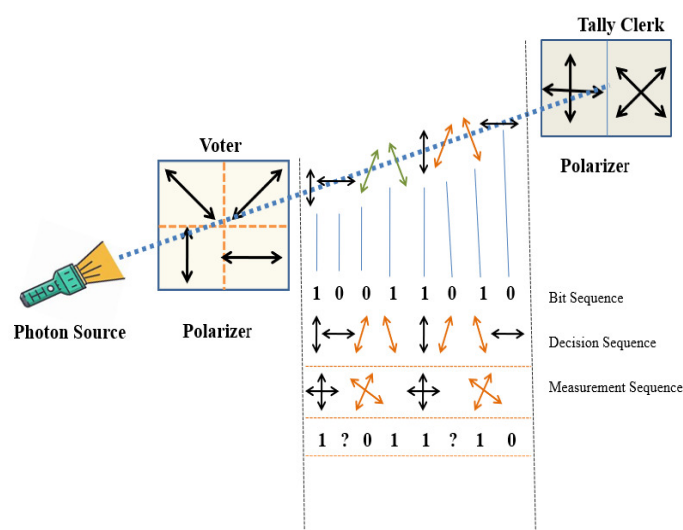

Figure 2. Illustration of photon polarization.

4. The Proposed Quantum E-Voting Scheme

4.1. Initialization Phase

There are three partners involved in our scheme: the voter, election authority (EA), and tally clerk. Let ID_{Ai} be the IDs of the voters having a string of length d, where $d = \lceil \log_2 N \rceil$ which defines the number of potential participants N. Define $T_i : \{0,1\}^n \longrightarrow \{0,1\}^n$; $i = 1, 2, 3, \ldots$, and T_i^{-1} is the inverse permutation of T_i. Let ID_q be the broadcast question of length u. Let $ID_A = (x_1, x_2, \ldots, x_n)$ be the identity of the voter and $ID_B = (y_1, y_2, \ldots, y_n)$ be the identity of the tally clerk having a string of length n. We also use the Hadamard operator (Table 1)

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

and on the other hand, we define $H^0 = I$, where I is the unit operator.

Table 1. Notation table.

Symbol	Description
H	Hadamard Operator
I	Identity operator
$\oplus$	XOR operator
T_i	Permutation function
T_i^{-1}	Inverse permutation function
l	Decoy Particle
d	Logarithmic function
K	Cryptographic one-way function
β	Private Key
N	No. of Voters
ID_{Ai}	Voter's Identities
ID_q	Broadcasting Question

4.2. Key Generation Phase

1. The EA established a bulletin board and revealed specific identification numbers N, ID_{A_i} and ID_q for participants.

2. A voter A_i submits a registration application to EA, who confirms the voter's identity and eligibility to vote.

3. EA privately selects a hash function $K : \{0,1\}^* \longrightarrow \{0,1\}^n$ with equal distribution before generating the key. K is the master key of the EA, and it generates private keys for voters and tally clerks using its own master key:

$$\beta_A = K(ID_A), \tag{2}$$
$$\beta_B = K(ID_B). \tag{3}$$

where $ID_A = (x_1, x_2, ..., x_n)$ and $ID_B = (y_1, y_2, ..., y_n)$ are the identities of the voter and clerk.

4. According to the quantum key distribution protocol, EA distributes the pads e and d with voter:

$$e' = e \oplus \beta_A \tag{4}$$
$$d' = d \oplus \beta_B \tag{5}$$

where $\beta_A = \beta_1^A, \beta_n^A, ..., \beta_n^A$ and $\beta_B = \beta_1^B, \beta_1^B, ..., \beta_n^B$ are the private keys of the voter and tally clerk.

5. EA makes public e' and d'. Then, using secret pads, the voter and tally clerk calculate their private keys:

$$\beta_A = e' \oplus e \tag{6}$$

$$\beta_B = d' \oplus d \tag{7}$$

4.3. Voting Phase

1. In this step, the voter and tally clerk make use of quantum key distribution (QKD) to establish a shared secret string $s = (s_1, s_2, s_3, ..., s_n)$ of n bits. Let $m = (m_1, m_2, ..., m_n) \in \{0, 1\}^m$ be the vote to be signed. This string will serve as an OTP in the future. EA picks n-bit strings at random $p = (p_1, p_2, p_3, ..., p_n)$, $q = (q_1, q_2, q_3, ..., q_n)$ and $r = (r_1, r_2, r_3, ..., r_n)$ and defines:

$$q_i = p_i \oplus \beta_i{}^B \tag{8}$$

$$r_i = p_i \oplus \beta_i{}^A \tag{9}$$

for each $|q_i\rangle$ and $|r_i\rangle$.

2. Next, EA performs $H^{\beta_i{}^A}$ and $H^{\beta_i{}^B}$ on $|q_i\rangle$ and $|r_i\rangle$ to obtain the sequences:

$$|\alpha_i\rangle = H^{\beta_i{}^A}|q_i\rangle \tag{10}$$

$$|\gamma_i\rangle = H^{\beta_i{}^B}|r_i\rangle \tag{11}$$

3. Let $|\alpha\rangle = \otimes_{i=1}^{N}|\alpha_i\rangle$ and $|\gamma\rangle = \otimes_{i=1}^{N}|\gamma_i\rangle$. After that, EA generates l decoy particles ($l \gg n$) chosen from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ for checking eavesdropping. EA obtains $\left|\alpha_i{}'\right\rangle$ by inserting l into $|\alpha_i\rangle$ and obtains $\left|\gamma_i{}'\right\rangle$ by inserting l into $|\gamma_i\rangle$. Then, we send $\left|\alpha_i{}'\right\rangle$ to the voter and $\left|\gamma_i{}'\right\rangle$ to the tally clerk, respectively.

4. In the quantum sequences $\left|\alpha_i{}'\right\rangle$ and $\left|\gamma_i{}'\right\rangle$, the positions and states of decoy particles are revealed. The EA confirms the receipt of particles. Decoy particles are measured and compared to their initial state. The protocol continues if there are no errors; otherwise, it is resumed or restarted.

5. The voter and tally clerk are able to recover the quantum sequences $|\alpha_i\rangle$ from $\left|\alpha_i{}'\right\rangle$ and $|\gamma_i\rangle$ from $\left|\gamma_i{}'\right\rangle$ after testing eavesdropping. For every $|q_i\rangle$, the voter performs the operation $H^{\beta_i{}^A}$ on $|\alpha_i\rangle$ and obtains $|q_i\rangle$:

$$|q_i\rangle = H^{\beta_i{}^A}|\alpha_i\rangle \tag{12}$$

The voter measures each $|q_i\rangle$ with the basis $\{|0\rangle, |1\rangle\}$. If the measurement outcome is $|0\rangle$, then the voter sets $q_i = 0$; otherwise, the voter sets $q_i = 1$ and obtains $q = (q_1, q_2, ..., q_n)$.

6. According to $\{m, ID_A, ID_B, q, s\}$, and the voter's private key β_A, the voter computes $\phi = (\phi_1, \phi_2, ..., \phi_n)$ and $\psi = (\psi_1, \psi_2, ..., \psi_n)$, where

$$\phi_i = \beta_i{}^A \oplus q_i \oplus s_i \tag{13}$$

$$\psi_i = m_i \oplus x_i \oplus y_i \tag{14}$$

7. For each $|\psi_i\rangle$, the voter performs the operation for each $|\psi_i\rangle$, on H_i^{β} on $|\psi_i\rangle$ and obtains

$$|v_i\rangle = H_i^{\beta}|\psi_i\rangle \text{ for } i = 1, 2, 3, ... \tag{15}$$

8. Let $|v\rangle = \otimes_{i=1}^{N}|v_i\rangle$ after that. To check the eavesdropping attack, the voter generates decoy particles l ($l \gg n$) at random from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. The voter inserts

these particles into $|v\rangle$ and obtains $|v'\rangle$. The voter sends $\{m, ID_A, ID_B, |v'\rangle\}$ to the tally clerk. The tally clerk measures each decoy particle and compares the results. If there is an error, the protocol is restarted; otherwise, the next step is executed.

9. After ensuring there is no eavesdropping, the tally clerk recovers the quantum sequence $|v\rangle$ from $|v'\rangle$ and keeps $\{m, ID_A, ID_B, |v\rangle\}$ as the quantum vote.

4.4. Counting Phase

The tally clerk confirms the given vote $\{m, ID_A, ID_B, |v\rangle\}$ from the voter. The tally clerk confirms it by performing the following steps:

1. According to the tally clerk's private key, for that received from EA in step 5, β_B, the tally clerk performs operation $H^{\beta_i^B}$ on $|\gamma_i\rangle$ and obtains:

$$|r_i\rangle = H^{\beta_i^B}|\gamma_i\rangle \tag{16}$$

Next, the tally clerk measures $|r_i\rangle$ using the basis $|0\rangle, |1\rangle\}$, and if $|0\rangle$ is the measurement result, they set $r_i = 0$. In the other case, they set $r_i = 1$. The tally clerk then obtains $r = (r_1, r_2, \ldots, r_n)$.

2. According to r, β_B, and the secret pad s, the tally clerk calculates:

$$\phi'_i = r_i \oplus \beta_i^B \oplus s_i \quad \text{for } (i = 1, 2, \ldots, n) \tag{17}$$

3. Let $\phi' = (\phi'_1, \phi'_2, \cdots, \phi'_n)$. Then, for each $|v_i\rangle$, the tally clerk executes the operation $H^{\phi'_i}$ on $|v_i\rangle$ and finds:

$$\psi'_i = H^{\phi'_i}|v_i\rangle \tag{18}$$

The tally clerk conducts measurements on each $|\psi'_i\rangle$ using the basis $\{|0\rangle, |1\rangle\}$ and assigns $\psi'_i = 0$ if the measurement yields $|0\rangle$. Alternatively, if the measurement outcome is $|1\rangle$, they assign $\psi'_i = 1$. Consequently, they obtain $\psi' = (\psi'_1, \psi'_2, \ldots, \psi'_n)$.

4. According to m, ID_A, ID_B, w, and Equation (14), the tally clerk calculates $\psi = (\psi_1, \psi_2, \ldots, \psi_n)$.

5. Finally, the tally clerk verifies $\psi = \psi'$. If $\psi = \psi'$, the tally clerk accepts $\{m, ID_A, ID_B, |v\rangle\}$ as the valid vote of the voter; otherwise, the tally clerk rejects the vote.

6. After N participants A_i for $i = 1, 2, \ldots, N$ have finished voting, the tally clerk publishes the final voting results and the corresponding ID_{Ai} on the bulletin board for further checking the availability. Finally, Bob counts all the voting results and announces the winning judgment option on the bulletin board.

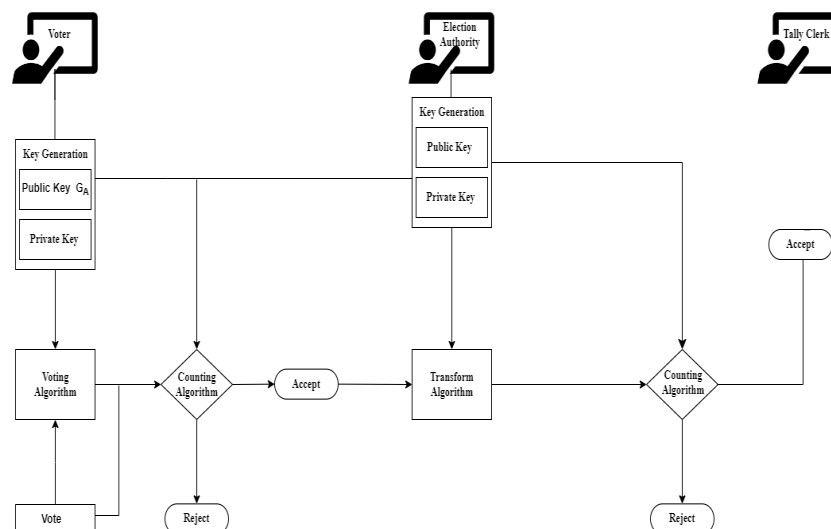Figure 3 shows the flow diagram of the proposed algorithm.

Figure 3. Flow diagram of the proposed algorithm.

5. Security Analysis

In security and analysis phase, we examine the proposed scheme's security features such as non-repudiation, designated verification, non-transferability and so on.

- *Designated verification property*
  The proposed QDVS scheme for electronic voting ensures the fulfillment of the designated verification attribute. The tally clerk's secret key β_B and secret pad s play a crucial role during the counting stage, with only the tally clerk being privy to the knowledge of the secret pad s and private key β_B. Although EA can calculate β_B, they know nothing about the secret pad s so EA cannot compute ϕ' in the counting phase step 2. So even the EA cannot verify the QDVS. Therefore, our scheme possesses the property of designated verification.

- *Hiding source*
  The proposed QDVS scheme satisfies the feature of the hiding source. In our scheme, both the signer and the designated verifier can generate the same QDVS. Given a signature, no one can judge who the original signer is in between the voter and tally clerk. Even if both confidential keys β_A and β_B are revealed, an attacker will still not be able to determine the true identity of the original voter, whether it is the voter or the designated verifier tally clerk. This characteristic guarantees that both the voter and designated verifier can generate identical QDVS. No external entity, including EA, can decide who the signer is since

$$|v_i\rangle = H^{\beta_i^A \oplus \beta_i^B \oplus p_i \oplus s_i}|m \oplus x_i \oplus y_i\rangle \tag{19}$$

- *Unconditional security*
  Our proposed scheme ensures security through the incorporation of two approaches: the integration of the BB84 protocol to securely establish cryptographic keys between the eligible voters and the election authority by using quantum key distribution, in conjunction with the use of the one-time pad (OTP) for encryption. The security of OTPs lies in the fact that each key is used only once and is never reused. In QDVS, this means that for each voting session, new quantum-generated keys are used to encrypt the votes, which ensures that if an attacker intercept the ciphertext, they cannot derive any meaningful information without the one time pad. The unconditional security of both of these features has been established through empirical demonstrations. Therefore, our proposed QDVS scheme is unconditionally secure.

- *Message privacy*
  The execution of a one-way hashing function $K : \{0,1\}^* \longrightarrow \{0,1\}^n$ for the purpose of generating secret keys enhances the level of security. The utilization of XOR operations in both the fourth and fifth steps of Section 4.2 serves to safeguard the quantum keys β_A and β_B during the process of distribution. The involvement of public permutation functions T_i adds complexity to the scheme.

- *Non-transferability property*
  According to Section 4.3, we know that the voter and tally clerk can create an identical QDVS for the vote. The signature created by the voter is indistinguishable from the signature generated by the tally clerk. Hence, the designated verifier cannot prove to any third party that the signature is generated by the voter or by himself. Therefore, the QDVS is non-transferable.

- *Security of secret keys and sensitive parameters*
  Firstly, an attacker cannot compute the private keys β_A and β_B of the voter and tally clerk from the public identities ID_A and ID_B. These secret keys are shared securely by using the quantum key distribution protocol.
  Note that

$$\beta_A = K(ID_A)$$
$$\beta_B = K(ID_B)$$

where K is the master key of EA. If one-way function K is chosen as a random one-way permutation oracle, the number of set element is $2n!$. The attacker has a low chance of guessing the master key K with probability $1/2n!$. The attacker cannot derive β_A and β_B without knowledge of the master key K.

Secondly, an outside attacker cannot decrypt the private keys from the OTP cipher text $e' = e \oplus \beta_A$ and $d' = d \oplus \beta_B$. The OTPs e and d are only known to the voter and tally clerk.

- *Non- repeatability:*
  Each voter can only vote once and cannot vote again because it holds the property of the no-cloning theorem [19]. The election authority distributes random voter's IDs to prevent forgery and easily detect repeated voting.

- *Untraceability:*
  The trace EA should be used to accurately determine the true identify of the target voter who was engaging in malicious communication. Exclusive access to the genuine identities of voters should be limited to the electoral authority alone. The employment of OTP pad with voter IDs and random quantum strings by EA ensures that the original identity cannot be traced by unauthorized individuals, effectively preventing many identity assaults.

5.1. Security Features

The proposed scheme is compared to existing protocols to evaluate its security features. The parameters of comparison include the third participant, the need for quantum one-way function, the need for quantum state swapping test, the need for quantum key distribution protocol, and the probabilistic verification result. The comparison in Table 2 shows that the proposed protocol has several advantages over pre-existing protocols.

5.2. SCYTHER Tool

The paper presents the formal security verification and simulation of the framework using the Scyther simulation tool [22], which is an effective tool for assessing and identifying potential threats and weaknesses in network security protocols. By utilizing the Scyther tool, we demonstrate the resilience of the method against various forms of cryptographic attacks.

Scyther utilizes a security protocol definition as an input to specify security properties, referred to as claim events and outputs, in the overview report and graph for each specific sort of cryptographic attack. The framework is defined in the "security protocol description language (SPDL)". Furthermore, the protocol definition establishes the particular order in which the voter, election authority, and tally clerk are involved. Figure 4 presents the outcome of the security verification of the proposed protocol using the Scyther tool. The findings suggest that none of the assertions made in the proposed protocol were subjected to any cryptographic attacks.

Table 2. Comparisons of security features.

Scheme	The Third Participant	Entanglement	Swapping Test	QKD Algorithm	Verification Result
[11]	Trusted	✓	✓	✓	probabilistic
[23]	Trusted	✓	×	×	Accurate
[24]	Trusted	×	×	×	Accurate
[25]	Trusted	×	×	✓	probabilistic
[26]	-	✓	✓	×	probabilistic
[27]	Trusted	×	✓	×	Accurate
Proposed	Semi-Trusted	×	×	✓	Accurate

✓: a characteristic is satisfied in a scheme; ×: a characteristic is not satisfied in a scheme.

Figure 4. Result of the Scyther tool.

6. Performance Analysis

The efficacy of the proposed protocol is subsequently assessed by employing a Python simulation of the signature scheme. In simulations, we utilize quantum bits instead of classical bits. The proposed scheme takes advantage of the quantum security provided by the no-cloning theorem and the uncertainty principle. We utilize the "Qiskit" and "pylatexenc" libraries for conducting quantum simulations.

6.1. Experimental Environment

The simulation environment under consideration has the following factors:

- Hardware environment: We conduct experiments on a machine using 11th Gen Intel® Core™ i7-1165G7 laptop @ 2.80 GHz processor.
- Software environment: We utilize Python 3.8.11 for coding, employing GMP, and compiling with optimization options. We also employ the "Qiskit" and "pylatexenc" packages to carry out quantum simulations with suitable parameters. The "AerSimulator" backend functions by emulating the operation of an actual device. Performing a quantum circuit with measurements will result in the return of a "count dictionary" that contains the final values of any classical registers in the circuit. The circuit may contain a specialized instruction set, documented in a separate notebook, which includes gates, measurements, resets, conditionals, and other components.

6.2. Experiment Analysis

Due to the limitations of quantum devices, we select single-photon measurements as compared to joint measurements. The circuit diagram for the experiment, implemented on the IBM-Perth quantum computer, is depicted in Figure 5.
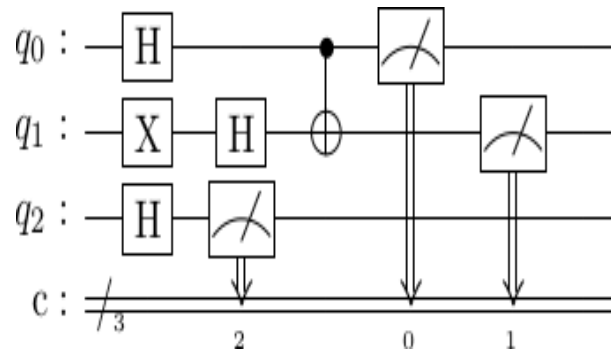
Figure 5. Quantum circuit diagram.

Using the $|\phi\rangle_{ij}$ (where $i, j \in \{0, 1\}$) state as the beginning state, Alice selects the $|\phi\rangle_{00}$, Bob selects the $|\phi\rangle_{11}$, and the theoretical outcomes are shown in Figure 6.
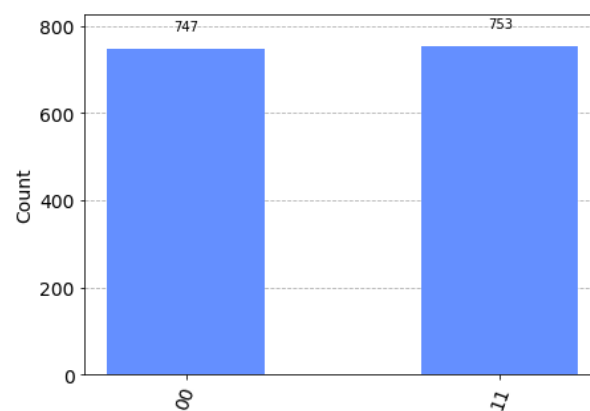

Figure 6. Theoretical results.

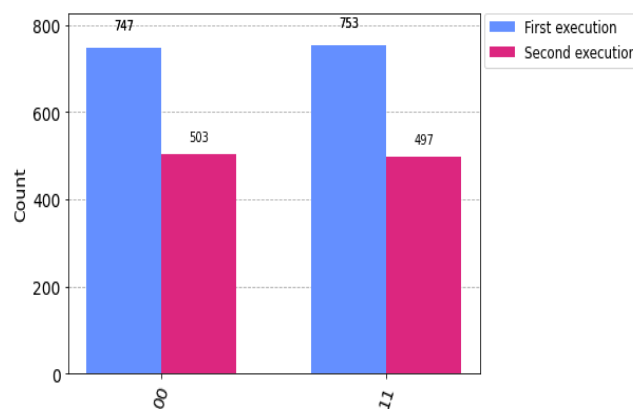The experimental results obtained from running the IBM-Perth quantum computer 1000 times are shown in Figure 7.

Figure 7. Experimental results.

The experiment demonstrates a 93.33% accuracy rate, attributing any discrepancies to errors in the quantum device. Furthermore, the experimental outcomes align with the theoretical predictions, affirming that our protocol enables a just exchange of quantum information.

7. Conclusions

The proposed quantum e-voting scheme with designated verification is a secure and efficient method for electronic voting, which uses principles of quantum mechanics like

quantum key distribution (QKD), the no-cloning theorem, and OTPs. In the initialization phase, three entities are used: voter Alice, election authority, and tally clerk Bob. The voting phase uses QKD to establish a shared secret string and this ensures secure key exchange. Eavesdropping is addressed through decoy particles and verification processes. The counting phase involves the tally clerk confirming the quantum vote's signature and ensuring its integrity. The proposed scheme has security features, including designated verification, non-transferability, unconditional security, message privacy, impossibility of forgery, and non-repeatability. The proposed scheme demonstrates robustness against security threats, making it a promising solution for electronic voting systems.

References

1. Zhang, J.L.; Xie, S.C.; Zhang, J.Z. An elaborate secure quantum voting scheme. *Int. J. Theor. Phys.* **2017**, *56*, 3019–3028. [CrossRef]
2. Gao, W.; Yang, L. Quantum election protocol based on quantum public key cryptosystem. *Secur. Commun. Netw.* **2021**, *2021*, 5551249. [CrossRef]
3. Li, Q.; He, D.; Chen, Y.; Wen, J.; Yang, Z. An efficient quantum-resistant undeniable signature protocol for the E-voting system. *J. Inf. Secur. Appl.* **2024**, *81*, 103714. [CrossRef]
4. Bernhard, M.; Benaloh, J.; Alex Halderman, J.; Rivest, R.L.; Ryan, P.Y.; Stark, P.B.; Teague, V.; Vora, P.L.; Wallach, D.S. Public evidence from secret ballots. In Proceedings of the Electronic Voting: Second International Joint Conference, E-Vote-ID 2017, Bregenz, Austria, 24–27 October 2017; Proceedings 2; Springer: Berlin/Heidelberg, Germany, 2017; pp. 84–109.
5. Del Pino, R.; Lyubashevsky, V.; Neven, G.; Seiler, G. Practical quantum-safe voting from lattices. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 1565–1581.
6. Prajapat, S.; Rana, A.; Kumar, P.; Das, A.K. Quantum safe lightweight encryption scheme for secure data sharing in Internet of Nano Things. *Comput. Electr. Eng.* **2024**, *117*, 109253. [CrossRef]
7. Hayward, M. *Quantum Computing and Shor's Algorithm*; Macquarie University Mathematics Department: Sydney, NSW, Australia, 2008; Volume 1.
8. Wang, Q.; Yu, C.; Gao, F.; Qi, H.; Wen, Q. Self-tallying quantum anonymous voting. *Phys. Rev.* **2016**, *94*, 022333. [CrossRef]
9. Arapinis, M.; Lamprou, N.; Kashefi, E.; Pappa, A. Definitions and security of quantum electronic voting. *ACM Trans. Quantum Comput.* **2021**, *2*, 4. [CrossRef]
10. Kang, B.; Boyd, C.; Dawson, E. A novel identity-based strong designated verifier signature scheme. *J. Syst. Softw.* **2009**, *82*, 270–273. [CrossRef]
11. 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* **2018**, *164*, 753–759. [CrossRef]
12. Shi, W.M.; Wang, Y.M.; Zhou, Y.H.; Yang, Y.G. A scheme on converting quantum deniable authentication into universal quantum designated verifier signature. *Optik* **2019**, *190*, 10–20. [CrossRef]
13. Hillery, M.; Ziman, M.; Bužek, V.; Bieliková, M. Towards quantum-based privacy and voting. *Phys. Lett.* **2006**, *349*, 75–81. [CrossRef]
14. Vaccaro, J.A.; Spring, J.; Chefles, A. Quantum protocols for anonymous voting and surveying. *Phys. Rev.* **2007**, *75*, 012333. [CrossRef]
15. Horoshko, D.; Kilin, S. Quantum anonymous voting with anonymity check. *Phys. Lett.* **2011**, *375*, 1172–1175. [CrossRef]
16. Li, Y.R.; Jiang, D.H.; Zhang, Y.H.; Liang, X.Q. A quantum voting protocol using single-particle states. *Quantum Inf. Process.* **2021**, *20*, 110. [CrossRef]
17. Zheng, M.; Xue, K.; Li, S.; Yu, N. A practical quantum designated verifier signature scheme for E-voting applications. *Quantum Inf. Process.* **2021**, *20*, 230. [CrossRef]
18. Bellovin, S.M. Frank Miller: Inventor of the one-time pad. *Cryptologia* **2011**, *35*, 203–222. [CrossRef]
19. Wootters, W.K.; Zurek, W.H. The no-cloning theorem. *Phys. Today* **2009**, *62*, 76–77. [CrossRef]
20. Heisenberg, W. Heisenberg Uncertainty Principle. 1927. Available online: https://uomustansiriyah.edu.iq/media/lectures/6/6_2023_11_13!04_59_02_PM.pdf (13 November 2023).
21. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]

22. Prajapat, S.; Kumar, P.; Kumar, S. A privacy preserving quantum authentication scheme for secure data sharing in wireless body area networks. *Clust. Comput.* **2024**, 1–17. [CrossRef]

23. Xin, X.; Wang, Z.; Yang, Q.; Li, F. Identity-based quantum designated verifier signature. *Int. J. Theor. Phys.* **2020**, *59*, 918–929. [CrossRef]

24. Xin, X.; Wang, Z.; Yang, Q.; Li, F. Quantum designated verifier signature based on Bell states. *Quantum Inf. Process.* **2020**, *19*, 79. [CrossRef]

25. Xin, X.; Ding, L.; Li, C.; Sang, Y.; Yang, Q.; Li, F. Quantum public-key designated verifier signature. *Quantum Inf. Process.* **2022**, *21*, 33. [CrossRef]

26. Zhang, Y.; Xin, X.; Li, F. Secure and efficient quantum designated verifier signature scheme. *Mod. Phys. Lett.* **2020**, *35*, 2050148. [CrossRef]

27. Zhang, L.; Zhang, J.H.; Xin, X.J.; Li, C.Y.; Huang, M. Quantum designated verifier signature scheme with semi-trusted third-party. *Int. J. Theor. Phys.* **2023**, *62*, 166. [CrossRef]