Hindawi
Security and Communication Networks
Volume 2021, Article ID 5551249, 15 pages
https://doi.org/10.1155/2021/5551249

Research Article

Quantum Election Protocol Based on Quantum Public Key Cryptosystem

Wenhua Gao [1,2,3] **and Li Yang** [1,2,3]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing, China*
[2]*School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China*
[3]*Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China*

Correspondence should be addressed to Li Yang; yangli@iie.ac.cn

Received 28 January 2021; Accepted 12 March 2021; Published 14 April 2021

Academic Editor: Prosanta Gope

There is no quantum election protocol that can fulfil the eight requirements of an electronic election protocol, i.e., completeness, robustness, privacy, legality, unreusability, fairness, verifiability, and receipt-freeness. To address this issue, we employ the general construction of quantum digital signature and quantum public key encryption, in conjunction with classic public key encryption, to develop and instantiate a general construction of quantum election protocol. The proposed protocol exhibits the following advantages: (i) no pre-shared key between any two participants is required, and no trusted third party or anonymous channels are required. The protocol is suitable for large-scale elections with numerous candidates and voters and accommodates the situation in which multiple voters vote simultaneously. (ii) It is the first protocol that dismantles the contradiction between verifiability and receipt-freeness in a quantum election protocol. It satisfies all eight requirements stated earlier under the physical assumptions that there exists a one-way untappable channel from the administrator to the voter and that there is no collusion between any of the three parties in the protocol. Compared with current election protocols with verifiability and receipt-freeness, this protocol relies upon fewer physical assumptions. (iii) This construction is flexible and can be instantiated into an election scheme having post-quantum security by applying cryptographic algorithms conveying post-quantum security. Moreover, utilizing quantum digital signature and public key encryption yields a good result: the transmitted ballots are in quantum states, so owing to the no-cloning theorem, ballot privacy is less likely to be compromised, even if private keys of the signature and public key encryption are leaked after the election. However, in existing election protocols employing classic digital signatures and public key encryption, ballot privacy can be easily violated if attackers obtain private keys. Thus, our construction enhances privacy.

1. Introduction

We employ elections for various work- and life-related scenarios. There are several forms and numerous applications of elections, such as the elections of student cadres in universities, chairmen in companies, and presidents in countries. The aforementioned applications require strict and secure election protocols. Fair and reasonable election systems can accommodate the interests of all aspects of a society and reduce or prevent social conflicts and are conducive to the long-term stability of a society. Furthermore, security problems in elections may affect the stability of a group or even an entire society. Therefore, it is of great significance to study election protocols. With the rapid development of the information age, electronic elections are widely replacing traditional paper voting methods, as they are more in line with our everyday lives and work. Designing a secure and effective electronic election protocol is, at present, a prevalent research topic.

Electronic elections generally consist of three parties: the voters, administrator, and counter. The role of the voter is to forward his/her ballot anonymously to the counter, who counts the ballots and publishes the election results on a bulletin board; the administrator is responsible for helping the election run smoothly. Ever since the concept of elections was first proposed, cryptographers have been

committed to constructing a secure and practical election scheme. The first electronic election protocol was proposed by Chaum [1] in 1981, which was followed by numerous other classic electronic election protocols. These classic election protocols can be mainly divided into three categories: electronic election protocols based on hybrid networks [1–4], electronic election protocols based on homomorphic encryption [5–7], and electronic election protocols based on blind signatures [3, 8–10].

Furthermore, for the security of election protocols, Fujioka et al. [9] proposed that a voting scheme should satisfy all of the following seven requirements. completeness: all valid votes are counted correctly by the system when all parties in the protocol are honest; robustness: inappropriate behaviour of dishonest participants or nonparticipants cannot undermine the conduct of the election, and the system is fault-tolerant; privacy: the vote message of the ballot is secret, and only the corresponding voter and the counter can know it. In addition, no one, except the voters themselves, can associate it with the corresponding voter identity; legality: only legitimate voters can vote; unreusability: no voter can vote twice; fairness: during the voting process, the statistics of the votes cast shall not be announced, because the intermediate results of the voting would affect the voting tendency of voters who have not yet voted; verifiability: voters can finally verify whether their votes have been counted correctly. Subsequently, in response to the possibility of vote-buying and coercive vote fraud in the election protocol, Benaloh et al. [11] proposed the requirement of receipt – freeness, that is, the voters cannot prove to a third party the content of their vote. This requirement prevents voters from being bribed or forced to vote. Owing to the contradiction between being receipt-free and verifiable, it is difficult to construct an electronic election with the receipt-freeness property. Presently known receipt-free election schemes are based on the physical assumption that the attackers cannot monitor when voters are voting, because if attackers can monitor, then receipt-free voting cannot be realized. We believe that this assumption is necessary for the receipt-freeness of an election. Most receipt-free classic elections are based on the physical assumption that there is a one-way or two-way untappable channel. In addition, some protocols [4] require large amounts of zero-knowledge proof, which reduces the efficiency of the protocol, while some protocols require an anonymous channel [10] or randomizer [7], which increases the complexity of the protocol.

Most classic electronic election protocols are based on the difficulty assumptions of large integer decomposition or discrete logarithms. The development of quantum computers poses a considerable threat to the security of these protocols. Therefore, constructing quantum election protocols with the property of resisting quantum computer attacks has become a prevalent research topic. Current quantum election protocols are mainly classified into two types: entangled states-based protocols [12–20] and nonentangled states-based protocols [21–23]. Some entangled state-based protocols can only perform a binary vote for "yes" or "no" [13, 14, 16, 17], which is not suitable for scenarios with numerous candidates. Some nonentangled state-based protocols [22, 23] require numerous keys to be pre-shared among the participants. Furthermore, the current quantum election protocols cannot fulfil all eight electoral requirements mentioned above. A quantum election protocol that can resolve the contradiction between receipt-freeness and verifiability has not been developed yet.

To solve the abovementioned problems, considering the advantages of the physical properties of quantum states in the context of an election protocol, we propose the general construction of a quantum election protocol. Our construction is flexible and can thus be instantiated into an election scheme having post-quantum security by applying cryptographic algorithms, which possess post-quantum security properties. The proposed protocol is suitable for scenarios with numerous candidates and can simultaneously achieve all eight election protocol requirements, i.e., completeness, robustness, privacy, legality, unreusability, fairness, receipt-freeness, and verifiability. Our protocol requires fewer assumptions as compared with the classic election protocol.

1.1. Our Contributions. In this study, we utilise the proposed general construction of quantum digital signature [24] and quantum public key encryption [25], in conjunction with classic public key encryption, to develop a general construction of a quantum election protocol.

In our construction, we utilise public key cryptographic algorithms, so no pre-shared key is required for any two participants. The protocol can resist an attack from participants, so there is no need for a trusted third party. Anonymous channels are not required because ballots are delivered with the help of an administrator. The protocol is suitable for large-scale elections with numerous candidates and voters and can accommodate scenarios in which multiple voters vote simultaneously.

The protocol is the first to resolve the conflict between verifiability and receipt-freeness in a quantum election protocol, simultaneously achieving completeness, robustness, privacy, legality, unreusability, fairness, verifiability, and receipt-freeness under only two physical assumptions. The first assumption is that there exists a one-way untappable channel from the administrator to the voter. The second assumption is that there is no collusion between any of the three parties in the protocol. In the actual elections, the administrator and the counter are generally composed of multiple people representing different interested parties; thus, their mutual supervision makes the second assumption easy to implement.

We utilise quantum public key encryption [25] with information theory security, quantum digital signature [24] with post-quantum security, and classic public key encryption with post-quantum security to instantiate the proposed construction into election schemes with post-quantum security. In the existing election protocols with classic digital signature and public key encryption, the transmitted ballots are classic ciphertexts, and the attacker may intercept and copy the ciphertexts. Once the corresponding private keys are known in the future, the attacker

could then decrypt the ciphertexts, thus violating the privacy of the ballots. However, in our construction, the use of quantum digital signature and public key encryption yields a good result: the transmitted votes are delivered in the form of quantum states, which are unknown to the attacker. Therefore, according to the no-cloning theorem, the privacy of the ballots is not compromised even if the corresponding private keys are leaked after the election is completed. As an added benefit, private keys do not need to be kept secret after the election is complete. Furthermore, the keys of the quantum digital signature are classic; thus, classic public key infrastructure (PKI) can be used for key management and distribution.

1.2. Outline of the Paper. The remainder of this paper is organised as follows: Section 2 describes the basic knowledge and definitions of the cryptographic primitives used in the protocol, including public key encryptions and digital signatures, and presents two existing models for quantum public key encryption and quantum digital signatures. Section 3 describes the generic construction of the proposed quantum election. Section 4 analyses the security of the generic construction described in Section 3, including completeness, robustness, privacy, legality, unreusability, fairness, verifiability, and receipt-freeness. Section 5 instantiates the general construction of the election protocol into election schemes with post-quantum security by applying cryptographic algorithms with post-quantum security, analyses the efficiency of the instantiation, and compares the efficiency and security with current protocols. Section 6 summarises our work and presents directions for future work.

2. Preliminaries

For the remainder of this paper, we assume the reader is familiar with the basic notions and notation of quantum computing. These can be found in textbooks such as [26].

Given $|r\rangle$ and $\sum_m \alpha_m |m\rangle$ as input, quantum transformation U_f computing a function $f\colon \{0,1\}^t \times \{0,1\}^n \longrightarrow \{0,1\}^\ell$ is defined as

$$U_f\left(|r\rangle \sum_m \alpha_m |m\rangle|0\rangle\right) = |r\rangle \sum_m \alpha_m |m\rangle|0 \oplus f(r,m)\rangle \xrightarrow{|r\rangle} \sum_m \alpha_m |m\rangle|f(r,m)\rangle, \quad (1)$$

where $\oplus$ denotes bitwise addition. In addition, when given $|r\rangle$ and $\sum_m \alpha_m |m\rangle|f(r,m)\rangle$ as input, we can use unitary transformation again and get

$$U_f\left(|r\rangle \sum_m \alpha_m |m\rangle|f(r,m)\rangle\right) = |r\rangle \sum_m \alpha_m |m\rangle|0\rangle \xrightarrow{|r\rangle} \sum_m \alpha_m |m\rangle|0\rangle. \quad (2)$$

Unitary transformation implemented via quantum circuits of U_f is shown in Figure 1.

2.1. Public Key Encryption. Public key encryption algorithms enable participants to transfer information securely without sharing secret key. A classic public key encryption $PKE = (Gen, Enc, Dec)$ consists of three algorithms, a finite message space $\mathcal{M}$, and a ciphertext space $\mathcal{C}$. The key generation algorithm takes a security parameter λ as input and outputs a key pair $(pk_{\text{pke}}, sk_{\text{pke}})$. The encryption algorithm Enc takes public key pk_{pke} and a message $m \in \mathcal{M}$ as input and outputs a ciphertext $c \in \mathcal{C}$. The deterministic decryption algorithm Dec takes sk_{pke} and a ciphertext c as input and outputs either a message $m = Dec(sk_{\text{pke}}, c) \in \mathcal{M}$ or a special symbol $\perp$ to indicate that c is not a valid ciphertext. For correctness, we require that $\Pr[m = Dec(sk_{\text{pke}}, c) | c = Enc(pk_{\text{pke}}, m)] = 1 - \text{negl}(\lambda)$, where $\text{negl}(\lambda)$ denotes a negligible function. We say that PKE is deterministic if Enc is deterministic, while PKE is probabilistic if Enc is probabilistic.

2.1.1. Quantum Public Key Encryption. The difference between quantum and classic public key encryption is that several of the six elements, including public and private keys generated by the key generation algorithm, encryption algorithm, decryption algorithm, plaintext, and ciphertext, may be represented in quantum states.

In 2000, Okamoto [27] proposed the concept of quantum public key encryption. Today, the existing quantum public key encryption schemes can be roughly classified into several categories according to different problems that schemes are based on coding [25, 28–32], quantum algorithms [27, 33], indistinguishable quantum states [34–37], induced trapdoor one-way transformations [24], quantum bit rotation [38–41], and interaction between bell state particles [42–46]. In 2015, Wu et al. [47] classified quantum public key encryption into 64 types, according to whether the six elements of public key encryption belong to quantum space or not.

Liang et al. [36] gave a generic quantum public key encryption construction for encrypting classic messages, where a private key corresponds to an exponent of different public keys. Then, Yang et al. [25] slightly improved the abovementioned scheme by using two Boolean functions instead of using one Boolean function. Every public key in [25] is an unknown quantum state for anyone except its generator, so the ciphertext quantum state obtained by encrypting a plaintext is also unknown to its encrypting party. Moreover, every public key is in different quantum state. These may be useful to achieve the receipt-freeness of election protocol. We briefly recall their generic quantum public key encryption construction $qPKE = (qGen, qEnc, qDec)$. Let p denote the number of messages to be encrypted, and m_i denote the i-th message for $i \in \{1, 2, \ldots, p\}$.

(i) $qGen$. (1) Randomly select two functions F_1, F_2 from a set of polynomial computable functions $\{F\colon \{0,1\}^n \longrightarrow \{0,1\}^n\}$. (2) For $i \in \{1, 2, \ldots, p\}$, randomly select and compute $k_{i,1} = F_1(g_i)$ and $k_{i,2} = F_2(g_i)$. Then, the quantum state $|\psi_{k_{i,1},k_{i,2}}\rangle$ can

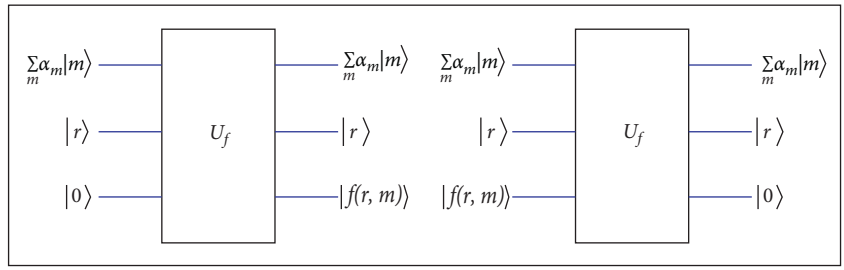

Figure 1: The quantum circuit implementation of U_f.

be efficiently prepared according to $k_{i,1}$ and $k_{i,2}$. (3) Upload all $(g_i, |\psi_{k_{i,1},k_{i,2}}\rangle)$ to the public key register. Function (F_1, F_2) is the private key. (4) In a word, $qGen(1^n) \longrightarrow (pk = \{pk_i\}_{i\in\{1,2,\ldots,p\}}, sk = (F_1, F_2))$, where $pk_i = \{g_i, |\psi_{k_{i,1},k_{i,2}}\rangle\}$.

(ii) *qEnc*. (1) In order to encrypt the i-th message m_i, download the i-th part of the classic and quantum public-key pair $pk_i = (g_i, |\psi_{k_{i,1},k_{i,2}}\rangle)$ from the public key register. (2) Encrypt the classic plaintext m_i by computing $|\psi^{(m_i)}_{k_{i,1},k_{i,2}}\rangle = \mathscr{E}(|\psi_{k_{i,1},k_{i,2}}\rangle, m_i)$, where $\mathscr{E}$ is a quantum encryption transformation, then output the ciphertext $c = (g_i, |\psi^{(m_i)}_{k_{i,1},k_{i,2}}\rangle)$. (3) In a word, $qEnc(pk_i, m_i) \longrightarrow c$.

(iii) *qDec*. (1) Given a ciphertext $c = (g_i, |\psi^{(m_i)}_{k_{i,1},k_{i,2}}\rangle)$, use private key F_1, F_2 to compute $k_{i,1} = F_1(g_i), k_{i,2} = F_2(g_i)$. (2) According to the value of $k_{i,1}, k_{i,2}$, use $\mathscr{D}$ to decrypt $|\psi^{(m_i)}_{k_{i,1},k_{i,2}}\rangle$ and obtain the message $m_i = \mathscr{D}(k_{i,1}, k_{i,2}, |\psi^{(m_i)}_{k_{i,1},k_{i,2}}\rangle)$, where $\mathscr{D}$ is a quantum decryption transformation. (3) In a word, $qDec(sk, c = (g_i, |\psi^{(m_i)}_{k_{i,1},k_{i,2}}\rangle)) \longrightarrow m_i$.

2.2. Digital Signature. A classic digital signature, $Signature = (KeyGen, Sign, Verf)$, consists of three algorithms and a finite message space $\mathscr{M}$. The key generation algorithm takes a security parameter λ as input and outputs a key pair $(vk_{\text{sig}}, sk_{\text{sig}})$. The signature algorithm $Sign$ takes the secret key sk_{sig} and a message $m \in \mathscr{M}$ as input and outputs a signature σ. The verification algorithm $Verf$ inputs vk_{sig} and a pair (m, σ) and outputs a bit message comprising either zero or one (this means that σ is a legal signature of message m). For correctness, we require that, pr $[1 = \text{Verf}(vK_{\text{sig}}, (m, \sigma)) \mid \sigma = \text{Sign}(sK_{\text{sig}}, m)] = 1 - \text{negl}(\lambda)$ where $\text{negl}(\lambda)$ denotes a negligible function.

2.2.1. Quantum Digital Signature. The difference between quantum and classic digital signature is that several of the six elements may be represented in quantum states. These elements include the signature key and the verification key generated by the key generation algorithm, the signature algorithm, the verification algorithm, the plaintext, and the signature results of the quantum digital signature. Because of the special properties of quantum states, it is difficult to achieve a true quantum digital signature, and most existing quantum digital signature schemes require the participation of arbitrators. Quantum digital signatures, such as classic digital signatures, achieve both the identity authentication of signer and the integrity verification of message.

With the development of quantum computer and quantum communication, it is necessary to study quantum digital signature. In 2001, Gottesman and Chuang [48] firstly proposed a quantum digital signature scheme for signing classic message. Subsequently, some arbitrated quantum digital signature protocols requiring the participation of trusted third parties [49–54] were proposed in succession. In 2010, Yang et al. [24] proposed an interactive quantum digital signature protocol for signing quantum message based on induced trapdoor one-way transformations. This protocol exploits the nature of quantum entangled states, realising the identity authentication of signer and protecting the integrity of messages without the participation of arbitrators. Subsequently, several quantum digital signature protocols without quantum memory were proposed [55, 56], thus improving the practicability of quantum signatures.

A general construction of quantum digital signature for signing quantum message is proposed by Yang et al. [24]. The signature scheme $qSignature$ consists of three algorithms $(qKGen, qSign, qVerf)$ which are described as follows:

(i) *qKGen*. Randomly select a trapdoor one-way function $f: \{0,1\}^{t+n} \longrightarrow \{0,1\}^{t'+n'}$ which has a trapdoor f^{-1}. Then, f is the verification key and f^{-1} is the signature secret key. In a word, $qKGen(1^t, 1^n, 1^{t'}, 1^{n'}) \longrightarrow (vk_{\text{sig}} = f, sk_{\text{sig}} = f^{-1})$.

(ii) *qSign*. The signer signs a n bits quantum message $|\psi\rangle = \sum_m \alpha_m |m\rangle$ to the verifier as follows: (1) the verifier randomly generates a number $r_{\text{ver}} \in \{0,1\}^{t'}$ and sends it to the signer. (2) The signer randomly generates a number $r_{\text{sig}} \in \{0,1\}^{n'}$ and computes $f^{-1}(r_{\text{ver}}, r_{\text{sig}}) = (r, r')$, where $r \in \{0,1\}^t$ and $r' \in \{0,1\}^n$. (3) Then, with r, the signer performs the quantum transformation U_f on the quantum message $|\psi\rangle|0\rangle = \sum_m \alpha_m |m\rangle|0\rangle$ and obtains

$$\sum_m \alpha_m |m\rangle|0\rangle \xrightarrow{(1)} \sum_m \alpha_m |m\rangle|f(r, m)\rangle, \tag{3}$$

and sends quantum state $\sum_m \alpha_m |m\rangle|f(r, m)\rangle$ to the verifier. (4) In a word, $qSign(sk_{\text{sig}}, |\psi\rangle) \longrightarrow \sigma$, where

$$\sigma = \left(r_{\text{ver}}, r, r', \sum_m \alpha_m |m\rangle |f(r,m)\rangle \right). \quad (4)$$

(iii) $qVerf$. (1) The verifier tells the signer that they have received the quantum state. (2) The signer announces r and r'. (3) The verifier computes $f(r,r')$ and checks whether the first t' bits of $f(r,r')$ equal r_{ver}. They then perform the transformation,

$$\sum_m \alpha_m |m\rangle |f(r,m)\rangle \xrightarrow{2} \sum_m \alpha_m |m\rangle |0\rangle, \quad (5)$$

and measure the second quantum register. They accept the signature if and only if the second register is in state $|0\rangle$. In a word, $qVerf(vk_{\text{sig}}, (|\psi\rangle, \sigma)) \longrightarrow 1$ if and only if the second register is in state $|0\rangle$.

3. Generic Construction of Quantum Election

In this section, we present a generic construction of quantum election protocol. Section 3.1 gives an overview of the construction and Section 3.2 gives a more detailed description.

3.1. Overview of Our Construction. The proposed election protocol runs as follows. (1) A voter holds his/her vote message and performs quantum public key encryption on it by using the counter's public key, obtaining the quantum ciphertext which is the ballot of the voter. (2) The ballot is signed by the voter and sent to the administrator. Then, the voter's signature is verified by the administrator. (3) The ballot is signed by the administrator and sent to the counter. Then, the administrator's signature is verified by the counter. (4) The ballot is decrypted by using the counter's private key and verification information is generated by the counter. (5) The information is sent to the voter with the help of the administrator. Finally, the voter can verify whether his/her vote is counted correctly or not.

3.2. Our Concrete Construction. In this section, we give a detailed description of quantum election protocol which consists of four cryptography primitives: classic probabilistic public key encryption $pPKE = (pGen, pEnc, pDec)$, classic deterministic public key encryption $dPKE = (dGen, dEnc, dDec)$, quantum digital signature $qSignature = (qKGen, qSign, qVerf)$, and quantum public key encryption $qPKE = (qGen, qEnc, qDec)$, where quantum public key encryption and quantum digital signature are two generic constructions proposed by Yang et al. [25] and Yang et al. [24], respectively. Please refer to Sections 2.1 and 2.2 for more details.

3.2.1. Initialization. Let p denote the number of voters, and v_i denote the i-th voter for $i \in \{1, 2, \ldots, p\}$. Let q denote the number of legitimate candidates, and $A_j \in \{0,1\}^{n-s}$ represent the identity of the j-th legitimate candidate for each $j \in \{1, 2, \ldots, q\}$. Moreover, let Admin represent the administrator and Counter represent the counter. In the protocol, each voter has a unique identity string denoted by id_i, while Admin has an identity id_{ad}. Identity strings are publicly known. The participants carry on the following steps:

(i) Admin. (1) Admin runs the algorithm $qKGen$ of $qsignature$ and gets a pair of public and private keys $(f_{\text{ad}}, f_{\text{ad}}^{-1})$. (2) Admin runs the algorithm $pGen$ of $pPKE$ and gets a pair of public and private keys $(pk_{\text{ad}}, sk_{\text{ad}})$. (3) Admin runs the algorithm $dGen$ of $dPKE$ and gets a pair of public and private keys $(pk'_{\text{ad}}, sk'_{\text{ad}})$.

(ii) Counter. (1) In order to encrypt p messages, Counter runs the algorithm $qGen$ of $qPKE$ and gets a pair of public and private keys $(\text{pk}_{\text{te}}, \text{sk}_{\text{te}})$, where $\text{pk}_{\text{te}} = \left\{ g_i, |\psi_{k_{i,1},k_{i,2}}\rangle \right\}_{i \in \{1,2,\ldots,p\}}$ and $\text{sk}_{\text{te}} = (F_1, F_2)$.

(iii) v_i. v_i runs the algorithm $qKGen$ of $qsignature$ and gets a pair of public and private keys $(f_{v_i}, f_{v_i}^{-1})$.

3.2.2. Election

(1) Preprocessing:

Each voter randomly selects a public key from the quantum public key register. Taking the public key $(g_i, |\psi_{k_{i,1},k_{i,2}}\rangle)$ chosen by voter v_i as an example and assuming that v_i wants to vote for candidate A_j, v_i carries on the following steps:

(i) v_i downloads one classic and quantum public-key pair $(g_i, |\psi_{k_{i,1},k_{i,2}}\rangle)$ of Counter from the public key register.

(ii) v_i generates a random string $e_i \in \{0,1\}^s$ and selects a candidate $A_j \in \{0,1\}^{n-s}$ to make up a vote message T_{ji}, where $T_{ji} = A_j \| e_i \in \{0,1\}^n$ represents a simple concatenation of A_j and e_i.

(iii) By performing quantum encryption transformation $qEnc$ on the vote message T_{ji}, v_i obtains ciphertext $(g_i, |\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle) = qEnc(|\psi_{k_{i,1},k_{i,2}}\rangle, T_{ji})$. $|\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle$ is the quantum ballot and it is clear that it is an n-bit quantum superposition state which can be denoted as $\sum_m \alpha_m |m\rangle$.

(2) Ballot-casting from voter to administrator:

This process is briefly illustrated in Figure 2. For the purpose of authenticating the identity of v_i and the integrity of ballot, the administrator Admin needs to mutually communicate with v_i so that Admin can verify the correctness of the received signature sent by v_i.

(i) If v_i wants to vote, they will send their id_i to Admin.

(ii) Let $\mathcal{T}$ denote the number of id_i received by Admin at the same time. After receiving id_i, Admin searches the local data set ID; if $\text{id}_i \in \text{ID}$ or $\mathcal{T} > 1$, the request for voting is rejected. Otherwise, Admin randomly generates $r_{\text{ad}_{i,1}} \in \{0,1\}^{t'}$ and sends it to v_i.

(iii) v_i randomly generates a number $r_{v_i} \in \{0,1\}^{n'}$ and computes $f_{v_i}^{-1}(r_{\text{ad}_{i,1}}, r_{v_i}) = (r_{i,1}, r'_{i,1})$, where $r_{i,1} \in \{0,1\}^t$ and $r'_{i,1} \in \{0,1\}^n$.

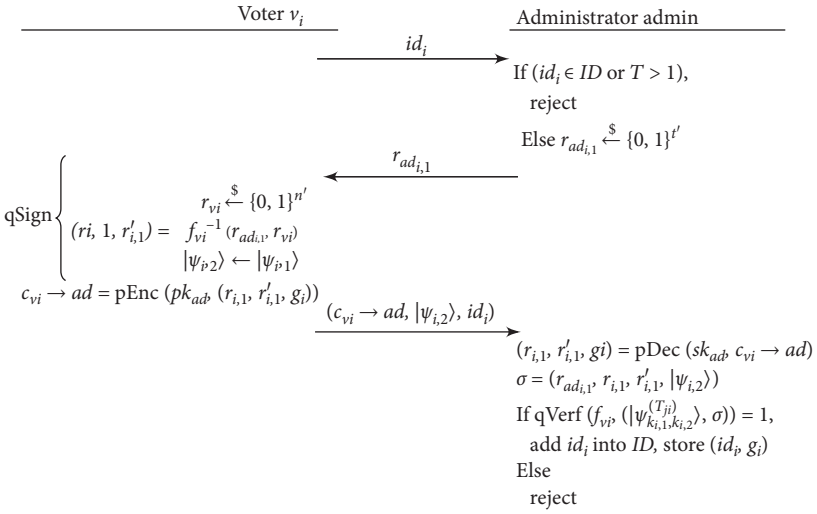

Figure 2: Ballot-casting from voter to administrator.

(iv) With $r_{i,1}$, v_i performs the quantum transformation $U_{f_{v_i}}$ on $|\psi_{i,1}\rangle = |\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle|0\rangle$ and obtains $|\psi_{i,2}\rangle$, where

$$|\psi_{i,1}\rangle = \sum_m \alpha_m |m\rangle|0\rangle \xrightarrow{U_{f_{v_i}}} |\psi_{i,2}\rangle = \sum_m \alpha_m |m\rangle \left|f_{v_i}(r_{i,1}, m)\right\rangle. \tag{6}$$

In a word, $qSign(f_{v_i}^{-1}, |\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle) \longrightarrow \sigma$, and it is easy to see that $\sigma = (r_{ad_{i,1}}, r_{i,1}, r'_{i,1}, |\psi_{i,2}\rangle)$.

(v) By running the encryption algorithm $pEnc$, v_i obtains classic ciphertext $c_{v_i \longrightarrow \text{ad}} = pEnc(\text{pk}_{\text{ad}}, (r_{i,1}, r'_{i,1}, g_i))$. Then, v_i sends $(c_{v_i \longrightarrow \text{ad}}, |\psi_{i,2}\rangle, \text{id}_i)$ to Admin.

(vi) After receiving $(c_{v_i \longrightarrow \text{ad}}, |\psi_{i,2}\rangle, \text{id}_i)$ from v_i, Admin decrypts $c_{v_i \longrightarrow \text{ad}}$ with their private key sk_{ad} and obtains the plaintext $(r_{i,1}, r'_{i,1}, g_i) = pDec(\text{sk}_{\text{ad}}, c_{v_i \longrightarrow \text{ad}})$. As a result, Admin can get the signature $\sigma = (r_{ad_{i,1}}, r_{i,1}, r'_{i,1}, |\psi_{i,2}\rangle)$ of $(|\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle, \sigma)$. If the output of $qVerf(f_{v_i}, (|\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle, \sigma))$ is equal to 1, Admin stores v_i's information (id_i, g_i) into their database. Note that in the computing process of $qVerf$, there exists the following operation to obtain quantum state:

$$|\psi_{i,2}\rangle = \sum_m \alpha_m |m\rangle \left|f_{v_i}(r_{i,1}, m)\right\rangle \xrightarrow{U_{f_{v_i}}} |\psi_{i,1}\rangle = \sum_m \alpha_m |m\rangle|0\rangle. \tag{7}$$

When all voters have completed this stage with Admin, the protocol proceeds to the next stage.

(3) Ballot-casting from administrator to counter:

This process is briefly illustrated in Figure 3. For the purpose of authenticating the identity of Admin and the integrity of ballot, the Counter needs to mutually communicate with Admin so that Counter can verify the correctness of the received signature sent by Admin.

(i) If Admin wants to send v_i's ballot to Counter, they firstly send id_{ad} to Counter.

(ii) After receiving id_{ad}, Counter randomly generates $r_{\text{te}_i} \in \{0,1\}^{t'}$ and sends it to Admin.

(iii) randomly generates $r_{\text{ad}_{i,2}} \in \{0,1\}^{n'}$ and computes $f_{\text{ad}}^{-1}(r_{\text{te}_i}, r_{\text{ad}_{i,2}}) = (r_{i,2}, r'_{i,2})$, where $r_{i,2} \in \{0,1\}^t$ and $r'_{i,2} \in \{0,1\}^n$.

(iv) With $r_{i,2}$, Admin performs the quantum transformation $U_{f_{\text{ad}}}$ on $|\psi_{i,1}\rangle$ and obtains $|\psi_{i,3}\rangle$, where

$$\begin{aligned} |\psi_{i,1}\rangle &= \sum_m \alpha_m |m\rangle|0\rangle \longrightarrow U_{f_{\text{ad}}} |\psi_{i,3}\rangle \\ &= \sum_m \alpha_m |m\rangle \left|f_{\text{ad}}(r_{i,2}, m)\right\rangle. \end{aligned} \tag{8}$$

In a word, $qSign(f_{\text{ad}}^{-1}, |\psi_{i,1}\rangle) \longrightarrow \sigma_{\text{ad}}$, and it is easy to see that $\sigma_{\text{ad}} = (r_{\text{te}_i}, r_{i,2}, r'_{i,2}, |\psi_{i,3}\rangle)$.

(v) Admin sends $(\sigma_{\text{ad}}, g_i)$ to Counter.

(vi) If the output of $qVerf(f_{\text{ad}}, (|\psi_{i,1}\rangle, \sigma_{\text{ad}}))$ equals 1, Counter can make sure the identity of Admin. Note that in the process of the above computing $qVerf$, there exists the following operation to obtain quantum state $|\psi_{i,1}\rangle$,

$$\begin{aligned} |\psi_{i,3}\rangle &= \sum_m \alpha_m |m\rangle \left|f_{\text{ad}}(r_{i,2}, m)\right\rangle \longrightarrow U_{f_{\text{ad}}} |\psi_{i,1}\rangle \\ &= \sum_m \alpha_m |m\rangle|0\rangle. \end{aligned} \tag{9}$$

(vii) With the quantum state $|\psi_{i,1}\rangle = \sum_m \alpha_m |m\rangle|0\rangle$, Counter can obtain voter v_i's ballot $|\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle = \sum_m \alpha_m |m\rangle$ and can get the ciphertext $c = (g_i, |\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle)$.

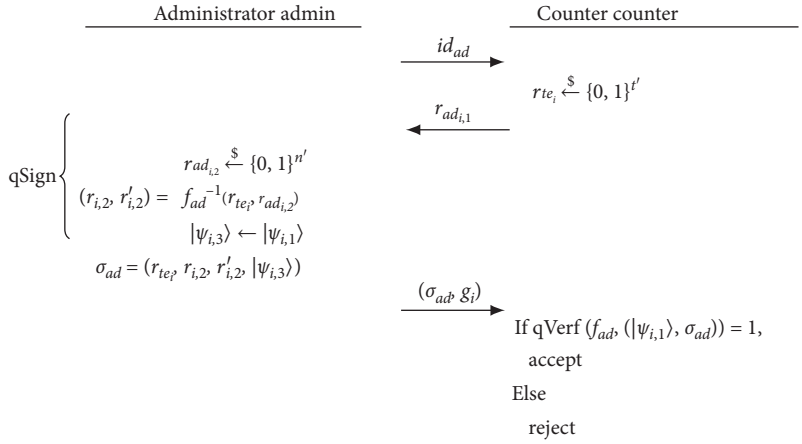

Figure 3: Ballot-casting from administrator to counter.

After Counter receives and verifies all voters' ballots from Admin, the election enters the next stage.

(4) Ballot-counting and result-publishing:

Given the quantum ciphertexts $c = (g_i, |\psi_{k_{i,1},k_{i,2}}^{(T_{ji})}\rangle)$, Counterdecrypts it and publishes the election result.

(i) Counter decrypts the ciphertext c by using $qDec$, i.e., $qDec(\mathrm{sk}, c) = T_{ji} = A_j \| e_i$.

(ii) If the pre-$(n-s)$ bits of the decryption result do not represent a qualified candidate, Counter rejects the ballot. Otherwise, Counter accepts the decryption result T_{ji} and corresponding g_i.

(iii) After accepting all the decryption results from p voters, Counter computes the voting result of every voter v_i in the form of $A_j \| (e_i \oplus dEnc(\mathrm{pk}'_{\mathrm{ad}}, f_i))$, where $f_i \in \{0,1\}^s$ is generated randomly by Counter. Then, Counter collects all the voting results and publishes them on the bulletin board.

(5) Confirming vote and terminating the election:

Counter sends message to v_i with the help of Admin so that v_i can verify whether their vote is counted correctly. Under the physical assumption that there is a one-way noneavesdropping channel from the administrator to the voter, the election satisfies the requirement of receipt − freeness.

(i) By running the encryption algorithm $dEnc$, Counter obtains $c_{\mathrm{te}\longrightarrow\mathrm{ad},i} = dEnc(\mathrm{pk}'_{\mathrm{ad}}, (e_i \oplus f_i))$ and sends $(c_{\mathrm{te}\longrightarrow\mathrm{ad},i}, g_i)$ to Admin.

(ii) Admin utilises g_i as a label to find the corresponding v_i and sends $c_{\mathrm{te}\longrightarrow\mathrm{ad},i}$ to v_i by the one-way untappable channel from Admin to v_i.

(iii) When all voters receive the corresponding ciphertext, Admin announces their private key $\mathrm{sk}'_{\mathrm{ad}}$. Then, v_i obtains $e_i \oplus f_i = dDec(\mathrm{sk}'_{\mathrm{ad}}, c_{\mathrm{te}\longrightarrow\mathrm{ad},i})$. Finally, v_i gets f_i with the knowledge of e_i. With e_i and f_i, v_i can compute and obtain $A_j \| (e_i \oplus dEnc(pk'_{\mathrm{ad}}, f_i))$. Then, v_i can verify whether they have successfully voted. If v_i does not succeed in the verification, they can request a reelection. If all voters can make sure that their votes have been successfully voted, the election is complete and terminated.

4. Security Analysis

We assume that there exists no collusion between any two of the three parties in the protocol. In actual elections, the administrator and the counter are generally composed of multiple people representing different interest groups, so their mutual supervision makes this assumption easy to hold. Both participants and nonparticipants can potentially attack the protocol. We define an attack from participants as an internal attack and an attack from nonparticipants as an external attack. In this section, we prove that our proposed election protocol satisfies the eight requirements, namely, completeness, robustness, privacy, legality, unreusability, fairness, verifiability, and receipt-freeness.

4.1. Completeness

Theorem 1 (completeness). *In the protocol, all valid votes are counted correctly when all participants are honest.*

Proof. (sketch). According to the definition of completeness, all valid votes are counted correctly when all parties in the protocol are honest. A qualified voter v_i for $i \in \{1, 2, \ldots, p\}$ encrypts the vote message $A_j \| e_i$ which is a simple concatenation of binary string A_j, representing a legal candidate and binary string e_i generated randomly by v_i, with a classic and quantum public-key pair $(g_i, |\psi_{k_{i,1},k_{i,2}}\rangle)$ which is selected randomly by v_i from Counter's public key pool. After the ballot $|\psi_{k_{i_1},k_{i_2}}^{(T_{ji})}\rangle$ is signed and verified twice, Counter finally obtains the ciphertext $(g_i, |\psi_{k_{i_1},k_{i_2}}^{(T_{ji})}\rangle)$. Then, Counter can obtain the vote message of v_i's ballot by decrypting the ciphertext with their private key (F_1, F_2).

Hence, it is clear that the proposed protocol satisfies completeness. □

4.2. Robustness

Theorem 2 (robustness). *The inappropriate behaviour of dishonest participants or nonparticipants cannot disrupt the election; i.e., the protocol is fault-tolerant.*

Proof. We analyse the robustness of the protocol by considering the inappropriate behaviour of participants including voters, administrator and counter, and nonparticipants.

(i) When a dishonest voter v_j seeks to disrupt the election, they may have three strategies. In the first case, v_j does not vote, that is, in the ballot-casting from voter to administrator stage, v_j does not send id_j or $(c_{v_j \longrightarrow \mathrm{ad}}, |\psi_{j,2}\rangle, \mathrm{id}_j)$ to Admin. However, it is clear that Admin will be aware of this missing vote. In the second case, v_j sends an invalid message group $(c_{v_j \longrightarrow \mathrm{ad}}, |\psi_{j,2}\rangle, \mathrm{id}_j)_{\mathrm{false}}$ to Admin in the ballot-casting from voter to administrator stage. While the running result of $qVerf$ achieved by Admin will not equal 1, this wrong action will be detected by. In the third case, v_j generates a random binary string A_{false}, which does not represent a qualified candidate and encrypts $A_{\mathrm{false}} \| e_j$ with Counter's public key $(g_j, |\psi_{k_{j,1},k_{j,2}}\rangle)$. However, Counter will find out the illegal A_{false} in the ballot-counting and result-publishing stage and reject the ballot. In a word, the voter v_j cannot succeed in disrupting the election.

(ii) If the internal attacker Admin wants to disrupt the election, they may have two strategies. In the first case, Admin tampers with the quantum state $|\psi_{i,1}\rangle$ from a legitimate voter v_i in the ballot-casting from administrator to counter stage. However, because Admin does not know the candidate that v_i is going to vote for, their random tampering will result in a random decrypting of the result obtained by Counter in the ballot-counting and result-publishing stage. Then, Counter will reject the ballot with a high probability. Because the probability that Admin successfully guesses the candidate that is voted for by v_i is $1/q$, the probability that they correctly tamper with the quantum state is also $1/q$. Then, the probability that the decrypted result obtained by Counter represents a legitimate candidate is also $1/q$, so the probability that the ballot is rejected in the ballot-counting and result-publishing stage by Counter is $(q-1)/q$. In addition, even if the tampered ballot is accepted by Counter, v_i can be aware that their vote is not counted correctly in the confirming vote and terminating the election stage. Then, v_i can request a reelection. In the second case, Admin may substitute the quantum state $|\psi_{i,1}\rangle$. In this manner, Counter will accept the decrypted result, but v_i will find that their vote has not been counted correctly during the confirming vote and terminating the election stage, and they can request a reelection.

(iii) If Counter wants to destroy the election, they may modify the vote message of the accepted ballot and then publish the modified result in the ballot-counting and result-publishing stage. Suppose that Counter tampers with the vote message $A_j \| e_i$ of eligible voter v_i to $A_{j'} \| e_i$. To be unnoticed by v_i, Counter must send a f_{false} so that v_i can verify their vote successfully. To achieve that, Counter can find another vote message, such as $A_j \| e_o$, which is chosen by another legal voter v_o and make f_{false} satisfy $e_i \oplus dEnc(\mathrm{pk}'_{\mathrm{ad}}, f_{\mathrm{false}}) = e_o \oplus dEnc(\mathrm{pk}'_{\mathrm{ad}}, f_o)$. However, because *Counter* does not have Admin's private key $\mathrm{sk}'_{\mathrm{ad}}$, it is difficult for Counter to provide a f_{false} that can make v_i verify their vote message on the bulletin board successfully. Therefore, the misbehaviour of Counter cannot be successful if the classic deterministic public key encryption $dPKE$ is secure.

(iv) If external attackers want to tamper with the ballot from a legitimate voter v_i, they can only attack during the transmission of $(c_{v_i \longrightarrow \mathrm{ad}}, |\psi_{i,2}\rangle, \mathrm{id}_i)$ in the ballot-casting from voter to administrator stage or during the transmission of $(\sigma_{\mathrm{ad}}, g_i)$ in the ballot-casting from administrator to counter stage. However, the security of the quantum signature algorithm *qSignature* enables this attack to be detected by Admin or Counter.

Hence, the protocol is robust. □

4.3. Privacy

Theorem 3 (privacy). *In the protocol, the vote message of the ballot is secret, and only the corresponding voter and the counter can know it. In addition, no one except the voters themselves can associate it with the corresponding voter identity.*

Proof. Nonparticipants of the protocol, the administrator, and the counter are all likely to attack the privacy of ballots, so we analyse the three cases in turn. Meanwhile, to prove our election can achieve privacy, we use the no-cloning theorem [57], which states that an exact copy of an unknown quantum state is impossible to achieve in quantum mechanics.

(i) Resistance to attacks from nonparticipants: if a nonparticipant of the protocol wants to attack the privacy of v_i's ballot, the only possible opportunity occurs during the transmission of information in the ballot-casting from voter to administrator stage and ballot-casting from administrator to counter stage. Assuming that the attacker intercepts $(c_{v_i \longrightarrow \mathrm{ad}}, |\psi_{i,2}\rangle, \mathrm{id}_i)$ in the ballot-casting from voter to administrator stage, the security of $pPKE$ ensures that the attackers cannot decrypt $c_{v_i \longrightarrow \mathrm{ad}}$ to obtain $(r_{i,1}, r'_{i,1}, g_i)$ and cannot obtain the signature $\sigma =$

$(r_{\mathrm{ad}_{i,1}}, r_{i,1}, r'_{i,1}, |\psi_{i,2}\rangle)$ of $|\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle$. Then, the attacker cannot untangle quantum state $|\psi_{i,2}\rangle$ to obtain $|\psi_{i,1}\rangle$ and the ciphertext $c = (g_i, |\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle)$, let alone obtain the vote message of the ballot, because they do not know Counter's private key (F_1, F_2). Moreover, if the transmitted ballot is classic, the attacker may copy it during its transmission. Once the corresponding private keys are known in the future, the attacker could then violate the privacy of the ballot. However, in our construction, the ballot is transmitted in the form of a quantum state, and $|\psi_{i,2}\rangle$ is unknown to the attacker. Owing to the no-cloning theorem, after the election is completed, even if the private keys (F_1, F_2) and sk_{ad} are leaked, the privacy of the ballots is not compromised. If the attacker intercepts $(\sigma_{\mathrm{ad}}, g_i)$ in the ballot-casting from administrator to counter stage, they can untangle $|\psi_{i,3}\rangle$ with $r_{i,2}$ to obtain $|\psi_{i,1}\rangle$ and the ciphertext $c = (g_i, |\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle)$. However, they cannot decrypt the ciphertext to obtain v_i's vote message, because the attacker does not know Counter's private key (F_1, F_2). In this case, $|\psi_{i,1}\rangle$ is unknown to the attacker. Thus, the attacker cannot copy this state and obtain the vote message of the ballot even if the private key (F_1, F_2) is leaked after the election.

(ii) Resistance to an attack from Admin: Admin can obtain the ciphertext $c = (g_i, |\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle)$ in the stage of ballot-casting from voter to administrator, but the security of $qPKE$ ensures that they cannot obtain the vote message of the ballot, because Counter's private key (F_1, F_2) is unknown. Similar to the earlier analysis, $c = (g_i, |\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle)$ is unknown to Admin, so they cannot copy the ciphertext c. Going further, they cannot obtain the vote message of the ballot even if the private key (F_1, F_2) is leaked after the election.

(iii) Resistance to an attack from Counter: if Counter wants to attack the privacy of v_i's ballot, they may attack in the stages of ballot-casting from voter to administrator and ballot-casting from administrator to counter. In the stage of ballot-casting from voter to administrator, Counter may intercept $(c_{v_i \longrightarrow \mathrm{ad}}, |\psi_{i,2}\rangle, \mathrm{id}_i)$ during the transformation and attempt to obtain v_i's vote message via the intercepted information. However, similar to this type of attack from nonparticipants, the security of $pPKE$ ensures that Counter cannot obtain $(r_{i,1}, r'_{i,1}, g_i)$ and obtain the signature $\sigma = (r_{ad_{i,1}}, r_{i,1}, r'_{i,1}, |\psi_{i,2}\rangle)$ of $|\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle$. Thus, Counter cannot untangle quantum state $|\psi_{i,2}\rangle$ to obtain $|\psi_{i,1}\rangle$ and the ciphertext $c = (g_i, |\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle)$. Therefore, it is impossible for Counter to use the private key (F_1, F_2) to decrypt the ciphertext to obtain v_i's vote message. In this stage, $|\psi_{i,2}\rangle$ is unknown to Counter; thus, they cannot copy it and associate $v'_i s$ ballot content with v_i's identity even if Admin's private key $\mathrm{sk}_{\mathrm{ad}}$ is leaked after the election. Moreover, it is worth noting that Counter cannot utilise g_i, which is obtained in the stage of ballot-casting from administrator to counter, as a label of $v'_i s$ identity to associate $v'_i s$ vote message with v_i's identity because g_i is encrypted by $pPKE$ in the stage of ballot-casting from voter to administrator. In the stage of ballot-casting from administrator to counter, even though Counter can finally obtain v_i's vote message, they do not know which voter the decrypted ballot comes from because Admin replaces the voter identity id_i with g_i at this stage.

As a result, the protocol can satisfy the privacy requirement during an election, and the privacy will not be threatened even if corresponding private keys are leaked after the election. □

4.4. Legality

Theorem 4 (legality). *In the protocol, only legitimate voters can vote.*

Proof. (sketch). The security of $qSignature$ ensures that only the vote cast by a legitimate voter v_i for $i \in \{1, 2, \ldots, p\}$ can be accepted. In the stage of ballot-casting from voter to administrator, v_i performs the quantum algorithm to sign their ballot $|\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle$ with their private key $f^{-1}_{v_i}$, i.e., $qSign(f^{-1}_{v_i}, |\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle) \longrightarrow \sigma$. Then,Admin verifies the signature with v_i's public key f_{v_i}, i.e., $qVerf(f_{v_i}, (|\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle, \sigma))$. The Admin accepts the information from v_i only if the output of $qVerf$ equals 1, which ensures that Admin only accepts the ballot from legitimate voter v_i. Similarly, Counter only accepts the ballot from Admin. Therefore, only legitimate voters can vote successfully. □

4.5. Unreusability

Theorem 5 (unreusability). *In the protocol, no voter can vote twice.*

Proof. (sketch). In the stage of ballot-casting from voter to administrator, if the legal voter v_i wants to vote, they send id_i Admin to first. The condition that $\mathrm{id}_i \notin \mathrm{ID}$ and $\mathscr{T} \leq 1$ ensures that Admin accepts id_i only once, so v_i can vote only once. Furthermore, in the case where voter v_i pretends to be another legitimate voter $v_{i'}$ and sends $\mathrm{id}_{i'}$ to Admin, the illegal ballot from v_i will not be accepted by Admin because v_i has no private key $f^{-1}_{v_{i'}}$ and the security of $qSignature$ ensures that the output of quantum verification algorithm $qVerf$ is not 1. Thus, one legal voter can vote only once. □

4.6. Fairness

Theorem 6 (fairness). *In the protocol, the intermediate results of the voting do not affect the preference of those who have not yet voted.*

Proof. (sketch). After accepting all the vote messages from q voters, Counter collects the voting result of every voter and then publishes all results on the bulletin board in the stage of ballot-counting and result-publishing. Therefore, no one can obtain the intermediate results of the election, and the protocol is fair. □

4.7. Verifiability

Theorem 7 (verifiability). *In the protocol, voters can finally verify whether their votes have been counted correctly.*

Proof. (sketch). Counter announces the voting result of every voter v_i in the form of $A_j||(e_i \oplus dEnc(\mathrm{pk}'_{\mathrm{ad}}, f_i))$. Subsequently, running the encryption algorithm $dEnc$, Counter obtains $c_{\mathrm{te}\longrightarrow\mathrm{ad},i} = dEnc(\mathrm{pk}'_{\mathrm{ad}}, (e_i \oplus f_i))$; they then send $c_{\mathrm{te}\longrightarrow\mathrm{ad},i}$ to v_i with the help of Admin. After v_i receives it, Admin publishes their private key $\mathrm{sk}'_{\mathrm{ad}}$. Running the decryption algorithm $dDec$, v_i obtains $e_i \oplus f_i = dDec(\mathrm{sk}'_{\mathrm{ad}}, c_{\mathrm{te}\longrightarrow\mathrm{ad},i})$. v_i obtains f_i with the knowledge of e_i. With e_i, f_i, and $\mathrm{pk}'_{\mathrm{ad}}$, v_i can compute $e_i \oplus dEnc(\mathrm{pk}'_{\mathrm{ad}}, f_i)$. By searching for $e_i \oplus dEnc(\mathrm{pk}'_{\mathrm{ad}}, f_i)$ on the bulletin board and verifying whether the candidate information corresponding to $e_i \oplus dEnc(\mathrm{pk}'_{\mathrm{ad}}, f_i)$ is A_j, v_i can verify whether their vote has been counted correctly. □

4.8. Receipt-Freeness

Theorem 8 (receipt-freeness). *In the protocol, the voter cannot prove to a third party the content of their vote.*

Proof. The protocol can achieve receipt-freeness under the physical assumption that there is a one-way untappable channel from the authority (i.e., the administrator) to the voter [4, 58]. By a standard exclusive-OR trick, this assumption can be implemented by having a number of one-way channels, assuming that the adversary cannot simultaneously tap every one of them [4].

Suppose that voter v_i wants to vote for candidate A_j, while there is a briber who requires v_i to vote for candidate A_a. In this protocol, under the premise that the number of ballots for candidate A_a displayed on the bulletin board does not affect the judgment of the briber (for example, the number of votes for candidate A_a is zero, and this case can be ignored in a large-scale election), and v_i can vote for candidate according to their preferences, but lie to the briber successfully by providing the briber with false evidence to prove that they voted for candidate A_a.

In the pre-voting stage, the briber may have asked voter to provide e_i as evidence for future verification. In this stage, v_i performs quantum encryption transformation $qEnc$ on T_{ji}, obtaining the ciphertext $(g_i, |\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle) = qEnc(|\psi_{k_{i,1},k_{i,2}}\rangle, T_{ji})$. In v_i's view, the density operator of the quantum public key $|\psi_{k_{i,1},k_{i,2}}\rangle$ is

$$\begin{aligned}\rho_{\mathrm{pk},i} &= \Pr[F_1, F_2] \cdot \sum_{F_1}\sum_{F_2} \left|\psi_{F_1(g_i),F_2(g_i)}\right\rangle \left\langle t\psi_{F_1(g_i),F_2(g_i)}\right| \\ &= \frac{1}{2^{2n}} \sum_{k_{i,1}}\sum_{k_{i,2}} \left|\psi_{k_{i,1},k_{i,2}}\right\rangle \left\langle t\psi_{k_{i,1},k_{i,2}}\right| \\ &= \frac{I}{2^n}.\end{aligned} \tag{10}$$

That is, in v_i's view, the quantum public key $|\psi_{k_{i,1},k_{i,2}}\rangle$ is in the maximum mixed state. Then, the quantum ciphertext $|\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle$ is also in the maximum mixed state for v_i. So, even if v_i sells all known information to the briber, the briber cannot obtain any information about the vote message of v_i by eavesdropping $(c_{v_i\longrightarrow\mathrm{ad}}, |\psi_{i,2}\rangle, \mathrm{id}_i)$ on the channel from v_i to Admin in the ballot-casting from voter to administrator stage. Therefore, the step of computing the ciphertext, i.e., $(g_i, |\psi^{(T_{ji})}_{k_{i,1},k_{i,2}}\rangle) = qEnc(|\psi_{k_{i,1},k_{i,2}}\rangle, T_{ji})$, avoids the requirement that the channel from the v_i to Admin is untappable.

In the stage of confirming vote and terminating the election, v_i receives $c_{\mathrm{te}\longrightarrow\mathrm{ad},i}$ by the one-way untappable channel from Admin and obtains $e_i \oplus f_i = dDec(\mathrm{sk}'_{\mathrm{ad}}, c_{\mathrm{te}\longrightarrow\mathrm{ad},i})$ by performing $dDec$. Finally, v_i obtains $\mathrm{f_i}$ with the knowledge of e_i. Now, we show that v_i cannot prove their vote to the briber according to f_i. v_i first searches for a vote for candidate A_a on the bulletin board. Assuming the voter v_a has voted for the candidate A_a, then their corresponding message, which is published by Counter on the bulletin board, is $A_a \| (e_a \oplus dEnc(\mathrm{pk}'_{\mathrm{ad}}, f_a)$, where e_a and f_a are binary strings of lengths randomly generated by v_a and Counter, respectively. As $\mathrm{sk}'_{\mathrm{ad}}$ is known, v_i can obtain f_{false} which satisfies $e_a \oplus dEnc(\mathrm{pk}'_{\mathrm{ad}}, f_a) = e_i \oplus dEnc(\mathrm{pk}'_{\mathrm{ad}}, f_{\mathrm{false}})$. Then, v_i can obtain f_{false} by running the $dDec$ algorithm, i.e., $f_{\mathrm{false}} = dDec(\mathrm{sk}'_{\mathrm{ad}}, e_i \oplus e_a \oplus dEnc(\mathrm{pk}'_{\mathrm{ad}}, f_a))$. Then, v_i tells f_{false} to the briber, such that the briber can find $A_a \| (e_i \oplus dEnc(\mathrm{pk}'_{\mathrm{ad}}, f_{\mathrm{false}}))$ on the bulletin board. Therefore, with f_i, v_i cannot prove to the briber how they voted. In conclusion, the protocol is receipt-free. □

5. Instantiation of Our Generic Construction

In this section, we instantiate the general construction of the election protocol.

5.1. Instantiation

5.1.1. Quantum Public Key Encryption $qPKE = (qGen, qEnc, qDec)$. To achieve post-quantum security for the protocol, we instantiate the construction of quantum public key cryptography $qPKE$ with quantum

public key encryption scheme [25] based on conjugate encoding which is information-theoretic secure.

Let I and Y be two of the Pauli matrices and H be the Hadamard transformation, where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{11}$$

For $k = (k_1, k_2, \ldots, k_n) \in \{0,1\}^n$, we define $H_k = H^{k_1} \otimes H^{k_2} \otimes \cdots \otimes H^{k_n}$, where H is the Hadamard transformation mentioned as above, $H^0 = I, H^1 = H$, and $\otimes$ is the tensor product. Similarly, we also define $Y_k = Y^{k_1} \otimes Y^{k_2} \otimes \cdots \otimes Y^{k_n}$, where Y is one of the Pauli matrices defined as above. Let p denote the number of messages to be encrypted, and $m_i \in \{0,1\}^n$ denote the i-th message for $i \in \{1, 2, \ldots, p\}$.

(i) *qGen*. (1) Randomly select two functions F_1, F_2 as private key from a set of polynomial computable functions $\{F\colon \{0,1\}^n \longrightarrow \{0,1\}^n\}$. (2) Randomly select $g_i \in \{0,1\}^n$ and compute $k_{i,1} = F_1(g_i)$ and $k_{i,2} = F_2(g_i)$. (3) Apply $H_{k_{i,1}}$ to $|k_{i,2}\rangle$ and obtain $H_{k_{i,1}}|k_{i,2}\rangle$. Take $(g_i, H_{k_{i,1}}|k_{i,2}\rangle)$ as one public key. (4) In a word, $qGen(1^n) \longrightarrow (\mathrm{pk} = \{\mathrm{pk}_i\}_{i\in\{1,2,\ldots,p\}}$, $\mathrm{sk} = (F_1, F_2))$, where $\mathrm{pk}_i = \{g_i, H_{k_{i,1}}|k_{i,2}\rangle\}$.

(ii) *qEnc*. (1) In order to encrypt the classic message m_i, download the classic and quantum public-key pair $\mathrm{pk}_i = (g_i, H_{k_{i,1}}|k_{i,2}\rangle)$ from the public key register. (2) Encrypt $m_i \in \{0,1\}^n$ by applying Y_{m_i} to $H_{k_{i,1}}|k_{i,2}\rangle$, then get the ciphertext $c = (g_i, Y_{m_i}H_{k_{i,1}}|k_{i,2}\rangle)$. It is clear that $\mathscr{E}(m_i, H_{k_{i,1}}|k_{i,2}\rangle) = Y_{m_i}H_{k_{i,1}}|k_{i,2}\rangle$. (3) In a word, $qEnc(\mathrm{pk}_i, m_i) \longrightarrow c$.

(iii) *qDec*. (1) Given the ciphertext $c = (g_i, Y_{m_i}H_{k_{i,1}}|k_{i,2}\rangle)$, use private key F_1, F_2 to compute $k_{i,1} = F_1(g_i), k_{i,2} = F_2(g_i)$. (2) According to $k_{i,1}$, apply $H_{k_{i,1}}$ to $Y_{mi}H_{k_{i,1}}|k_{i,2}\rangle$ and measure on the basis $\{|0\rangle, |1\rangle\}^n$ to obtain $m_i \oplus k_{i,2}$. Then, with $k_{i,2}$, perform an exclusive OR on $m_i \oplus k_{i,2}$ to get m_i. (3) It is clear that the algorithm $\mathscr{D}$ is the whole process of step (2) described as above. (4) In a word, $qDec(\mathrm{sk}, c = (g_i, Y_{m_i}H_{k_{i,1}}|k_{i,2}\rangle)) \longrightarrow m_i$.

5.1.2. Quantum Digital Signature qSignature = (qKGen, qSign, qVerf) The function of quantum signature in the election protocol is to make the verifier get the information that the signer wants to send authenticatively. To achieve post-quantum security for the protocol, we instantiate the construction of quantum digital signature *qSignature* with quantum digital signature [24] which is constructed based on the McEliece cryptosystem with post-quantum security [59]. The McEliece secret key consists of a nonsingular $n \times n$ matrix S; a generator matrix G size of $n \times t$ for a Goppa code; and a $t \times t$ permutation matrix P. The McEliece public key is the $n \times t$ matrix SGP. In the following, $t' = (t/2)$ and $n' = (t/2)$.

(i) *qKGen*. (1) Generate the McEliece public and secret key (SGP, (S, G, P)). (2) Let the secret key $\mathrm{sk}_{\mathrm{sig}}$ be (S, G, P) and the verification key $\mathrm{vk}_{\mathrm{sig}}$ be $G' = \mathrm{SGP}$.

(ii) *qSign*. The signer signs a n bits quantum message $|\psi\rangle = \sum_m \alpha_m |m\rangle$ to the verifier as follows: (1) the verifier randomly generates a number $r_{\mathrm{ver}} \in \{0,1\}^{t'}$ and sends it to the signer. (2) The signer randomly generates a number $r_{\mathrm{sig}} \in \{0,1\}^{n'}$. (3) With the knowledge of $\mathrm{sk}_{\mathrm{sig}} = (S, G, P)$, the signer can get (r, r') which satisfy that $r'G' \oplus r = (r_{ver}, r_{sig})$, where $r \in \{0,1\}^t, r' \in \{0,1\}^n$. (4) Note that f^{-1} is the whole process of step (3) described as above and $f(r, r') = r'G' \oplus r$. (5) Then, with r, the signer performs the quantum transformation U_f on the quantum message $|\psi\rangle|0\rangle = \sum_m \alpha_m |m\rangle|0\rangle$ and obtains

$$\sum_m \alpha_m |m\rangle|0\rangle \xrightarrow{(1)} \sum_m \alpha_m |m\rangle|f(r,m)\rangle, \tag{12}$$

and sends quantum state $\sum_m \alpha_m |m\rangle|f(r,m)\rangle$ to the verifier. (4) In a word, $qSign(\mathrm{sk}_{\mathrm{sig}}, |\psi\rangle) \longrightarrow \sigma$, where

$$\sigma = \left(r_{\mathrm{ver}}, r, r', \sum_m \alpha_m |m\rangle|f(r,m)\rangle\right). \tag{13}$$

(iii) *qVerf*. (1) The verifier tells the signer that they have received the quantum state. (2) The signer announces r and r'. (3) The verifier computes $f(r, r') = r'G' \oplus r$ and checks whether the first t' bits of $f(r, r')$ equal r_{ver}. They then perform the transformation

$$\sum_m \alpha_m |m\rangle|f(r,m)\rangle \xrightarrow{(2)} \sum_m \alpha_m |m\rangle|0\rangle, \tag{14}$$

and measure the second quantum register. They accept the signature if and only if the second register is in state $|0\rangle$. In a word, $qVerf(\mathrm{vk}_{\mathrm{sig}}, (|\psi\rangle, \sigma)) \longrightarrow 1$ if and only if the second register is in state $|0\rangle$.

5.1.3. Classic Public Key Encryption pPKE and dPKE. The classic probabilistic public key encryption *pPKE* in the instantiation can be any classic public key encryption schemes with post-quantum security such as public key

Algorithm dGen :
(*pk*, *sk*)←pGen
return (*pk*, (*pk*, *sk*))
	Algorithm dDec (*sk*, *c*) :
	m←pDec (*sk*, *c*)
	R←H (*pk*, *m*)
	If pEnc (*pk*, *m*, *R*) = *c*, then
	return *m*
	Else
	return ⊥

Algorithm dEnc (*pk*, *m*) : *R*←H (*pk*, *m*) c←pEnc (*pk*, *m*, *R*) return *c*	

Figure 4: Deterministic *PKE* construction.

Table 1: Performance comparison.

Schemes	Quantum resource	Efficiency	Interactive times
LZWL20 [15]	Cluster states	1/9	4
ZXZ17 [19]	Entangled states	1/6	9
CDY16 [12]	Bell states	1/4	9
ZZX18 [20]	Cluster states	1/4	4
WXJ20 [18]	GHZ states	1/3	3
Ours	Entangled states	> 1/4	8

Table 2: Security comparison.

Schemes	Completeness	Robustness	Privacy	Legality	Unreusability	Fairness	Verifiability	Receipt-freeness
LZWL20 [15]	✓	×	✓	✓	✓	✓	✓	×
ZXZ17 [19]	✓	×	✓	✓	✓	✓	✓	×
CDY16 [12]	✓	×	✓	✓	✓	✓	✓	×
ZZX18 [20]	✓	×	✓	✓	✓	×	✓	×
WXJ20 [18]	✓	×	✓	✓	✓	×	✓	×
Ours	✓	✓	✓	✓	✓	✓	✓	✓

encryption based on coding [59], lattices [60], and multivariates [61].

Bellare et al. [62] proposed a generic deterministic public key encryption construction from probabilistic public key encryption, i.e., if there exists a probabilistic public key encryption $pPKE = (pGen, pEnc, pDec)$, then there is a classic deterministic public key encryption scheme $dPKE = (dGen, dEnc, dDec)$ which is illustrated in Figure 4. In the deterministic *PKE* construction, H denotes a hash function, such as SHA2 and SHA3.

5.2. Efficiency Analysis. According to Ref. [18], quantum bit efficiency of quantum election protocol is defined as

$$n = C/Q, \tag{15}$$

where the total number of transmitted classic bits (message bits) is C and the total number of quantum bits generated is Q.

We can split this protocol into two parts. In the first part, the voter passes the vote message to Counter with the help of Admin. In the second part, Counter passes the verification information to the corresponding voter with the help of Admin. In the first part, the valid classic information transmitted is T_{ji}, and its number of bits is n. To transmit T_{ji}, the n bits quantum public key $H_{k_{i,1}}|k_{i,2}\rangle$, n bits quantum ciphertext $Y_{m_i}H_{k_{i,1}}|k_{i,2}\rangle$, and $|\psi_{i,2}\rangle$, $|\psi_{i,3}\rangle$ are generated, where $|\psi_{i,2}\rangle$, $|\psi_{i,3}\rangle$ are both $n + t$ bits quantum states generated during the signature process. Hence, in this part, total of $4n + 2t$ quantum bits are generated. In the second part, the valid classic information transmitted is $f_i \oplus e_i$, whose length is s, where there is no quantum bit generated. Thus, the number C of valid classic bits transmitted in the protocol is $n + s$, and the number Q of quantum bits generated in the protocol is $4n + 2t$. Subsequently, the efficiency of the protocol is

$$\eta = \frac{n + s}{4n + 2t}. \tag{16}$$

When s is equal to t, the efficiency is greater than 1/4.

5.2.1. Performance Comparison. There exist many quantum election protocols based on entangled states [12–14, 16–20]. However, some [13, 14, 16, 17] of these protocols can only perform a binary vote for "yes" or "no." As a result, we make a performance comparison between our protocol and the quantum election protocols [12, 15, 18–20] which are applicable for scenarios with numerous candidates. Please read Table 1 for more details.

5.3. Security Comparison. This protocol is an instantiation of our general construction. We have proved that our general construction satisfies the eight requirements of election, so the instantiation also satisfies the eight

requirements. For the same reason which is described in Section 5.2, we make a security comparison between our protocol and the quantum election protocols [12, 15, 18–20] which are applicable for scenarios with numerous candidates. Please read Table 2 for more details. It is clear that our election protocol is much more secure than other schemes.

6. Conclusion

In this paper, we utilise the general construction of quantum digital signature [24] and quantum public key encryption [25], in conjunction with classic public key encryption, to develop a general construction of a quantum election protocol. The protocol is suitable for large-scale elections with numerous candidates and voters and accommodates scenarios in which multiple voters vote simultaneously. The protocol does not require any two participants to pre-share a secret key, nor does it require anonymous channels or a trusted third party. This construction is the first to achieve the properties of completeness, robustness, privacy, legality, unreusability, fairness, verifiability, and receipt-freeness under attacks from both external and internal agents in the current quantum election protocols. We instantiate the general construction into an election scheme with post-quantum security by applying cryptographic algorithms having post-quantum security. Furthermore, our election protocol has higher security than that of existing protocols. All the keys of the quantum digital signature are classic so that the classic PKI can be used for key management and distribution.

This construction is a theoretical achievement, and any practical application remains a distant goal. The quantum public key cryptosystem has significant room for development in comparison with the relatively well-established conventional public key cryptosystem. Numerous problems remain to be solved, such as developing the quantum PKI.

Data Availability

The data used are available within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 61672517), National Natural Science Foundation of China (Key Program, Grant No. 61732021), National Cryptography Development Fund (Grant No. MMJJ20170108), and Beijing Municipal Science & Technology Commission (Grant no. Z191100007119006).

References

[1] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.

[2] M. Abe, "Universally verifiable mix-net with verification work indendent of the number of mix-servers," *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, vol. 1403, pp. 1431–1440, 1998.

[3] J. D. Cohen and M. J. Fischer, "A robust and verifiable cryptographically secure election scheme (extended abstract)," in *Proceedings of the 26th Annual Symposium on Foundations of Computer Science*, pp. 372–382, Portland, OR, USA, October 1985.

[4] K. Sako and J. Kilian, "Receipt-free mix-type voting scheme," in *Proceedings of the EUROCRYPT*, Saint-Malo, France, May 1995.

[5] J. Benaloh, "Verifiable secret-ballot elections," Ph.D. thesis, Yale University Department of Computer Science Department, New Haven, CT, USA, 1987.

[6] S. B. Cramer R and R. Gennaro, "A secure and optimally efficient multi-authority election scheme," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 103–118, Konstanz, Germany, May 1997.

[7] M. Hirt, "Multi-party computation: efficient protocols, general adversaries, and voting," Ph.D.thesis, ETH, Zurich, Switzerland, 2001.

[8] D. Chaum, "Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA," *Lecture Notes in Computer Science*, pp. 177–182, 1988.

[9] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections," in *Proceedings of the ASIACRYPT'92: Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology*, pp. 244–251, Gold Coast, Australia, December 1992.

[10] T. Okamoto, "Receipt-free electronic voting schemes for large scale elections," in *Proceedings of the 5th International Workshop Security Protocols*, Paris France, April 1997.

[11] J. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections," in *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing*, pp. 544–553, Montreal, Canada, May 1994.

[12] H.-J. Cao, L.-Y. Ding, Y.-F. Yu, and P.-F. Li, "A electronic voting scheme achieved by using quantum proxy signature," *International Journal of Theoretical Physics*, vol. 55, no. 9, pp. 4081–4088, 2016.

[13] M. Hillery and Ziman, "Towards quantum-based privacy and voting," *Physics Letters A*, vol. 349, pp. 75–81, 2006.

[14] D. Horoshko and S. Kilin, "Quantum anonymous voting with anonymity check," *Physics Letters A*, vol. 375, no. 8, pp. 1172–1175, 2011.

[15] Y. Li, F. Zhou, T. Wang, and L. Lu, "Novel quantum voting protocol with eight-qubit cluster entangled state," *International Journal of Theoretical Physics*, vol. 1, pp. 1–10, 2020.

[16] J.-H. Tian, J.-Z. Zhang, and Y.-P. Li, "A voting protocol based on the controlled quantum operation teleportation," *International Journal of Theoretical Physics*, vol. 55, no. 5, pp. 2303–2310, 2016.

[17] J. A. Vaccaro, J. Spring, and A. Chefles, "Quantum protocols for anonymous voting and surveying," *Physical Review A*, vol. 75, Article ID 012333, 2007.

[18] J. Wang, G. Xu, and D. Jiang, "Quantum voting scheme with greenberger-horne-zeilinger states," *International Journal of Theoretical Physics*, vol. 59, no. 12, 2020.

[19] J. Zhang, S. Xie, and J. Zhang, "An elaborate secure quantum voting scheme," *International Journal of Theoretical Physics*, vol. 56, pp. 3019–3028, 2017.

[20] J. Zhang, J. Zhang, and S. Xie, "A choreographed distributed electronic voting scheme," *International Journal of Theoretical Physics*, vol. 57, no. 2, pp. 1–11, 2018.

[21] K. S. T. Okamoto and Y. Tokunaga, "Quantum voting scheme based on conjugate coding," *NTT Technical Review*, vol. 6, no. 1, pp. 1–8, 2008.

[22] R. Zhou and L. Yang, "Quantum election scheme based on anonymous quantum key distribution," *Chinese Physics B*, vol. 21, no. 8, Article ID 080301, 2012.

[23] R. Zhou and L. Yang, "Distributed quantum election scheme," 2013, https://arxiv.org/abs/1304.0555.

[24] L. Yang, M. Liang, B. Li, L. Hu, and D. Feng, "Quantum public-key cryptosystems based on induced trapdoor one-way transformations," 2010, https://arxiv.org/abs/1012.5249.

[25] L. Yang, B. Yang, and C. Xiang, "Quantum public-key encryption schemes based on conjugate coding," *Quantum Information Processing*, vol. 19, no. 11, pp. 1–16, 2020.

[26] M. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, UK, 2010.

[27] T. Okamoto, K. Tanaka, and S. Uchiyama, "Quantum public-key cryptosystems," in *Proceedings of the Advances in Cryptology—CRYPTO*, pp. 147–165, Santa Barbara, CA, USA, August 2000.

[28] W. G. Voigt and C. R Johnson, "Aestivation and thermoregulation in the Texas tortoise, *Gopherus berlandieri*," *Comparative Biochemistry and Physiology Part A: Comparative Physiology*, vol. 53, no. 1, pp. 41–44, 1976.

[29] X. Li and L. Li, "Quantum public-key cryptosystem using non-orthogonal states," *Journal of Software*, vol. 8, no. 8, pp. 1906–1913, 2013.

[30] C. Wu and L. Yang, "Bit-oriented quantum public-key encryption based on quantum perfect encryption," *Quantum Information Processing*, vol. 15, no. 8, pp. 3285–3300, 2016.

[31] L. Yang, "Quantum public-key cryptosystem based on classical Np-complete problem," 2003, https://arxiv.org/abs/quant-ph/0310076.

[32] L. Yang, "A public-key cryptosystem for quantum message transmission," *Proceedings of Spie the International Society for Optical Engineering*, vol. 5631, pp. 233–236, 2005.

[33] W. Luo and G. Liu, "Asymmetrical quantum encryption protocol based on quantum search algorithm," *China Communications*, vol. 11, no. 9, pp. 104–111, 2014.

[34] A. Kawachi, T. Koshiba, H. Nishimura, and T. Yamakami, "Computational indistinguishability between quantum states and its cryptographic application," in *Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 268–284, Aarhus, Denmark, May 2005.

[35] A. Kawachi, T. Koshiba, H. Nishimura, and T. Yamakami, "Computational indistinguishability between quantum states and its cryptographic application," *Journal of Cryptology*, vol. 25, no. 3, pp. 528–555, 2012.

[36] M. Liang and L. Yang, "Public-key encryption and authentication of quantum information," *Science China Physics, Mechanics and Astronomy*, vol. 55, pp. 1618–1629, 2012.

[37] J. P. L. Yang, "Quantum public-key encryption with information theoretic security," 2010, https://arxiv.org/abs/1006.0354.

[38] G. M. Nikolopoulos, "Applications of single-qubit rotations in quantum public-key cryptography," *Physical Review A*, vol. 78, no. 1, Article ID 032348, 2008.

[39] U. Seyfarth, G. Nikolopoulos, and G. Alber, "Symmetries and security of a quantum-public-key encryption based on single-qubit rotations," *Physical Review A*, vol. 85, Article ID 022342, 2012.

[40] S. Zheng, L. Gu, and D. Xiao, "Bit-oriented quantum public key probabilistic encryption schemes," *International Journal of Theoretical Physics*, vol. 53, no. 1, pp. 116–124, 2014.

[41] S. Zheng, K. Wen, and L. Gu, "An efficient multi-bit quantum public key encryption scheme," *Journal of China Universities of Posts and Telecommunications*, vol. 2014, no. 1, pp. 104–111, 2019.

[42] F. Gao, Q. Wen, S. Qin, and F. Zhu, "Quantum asymmetric cryptography with symmetric keys," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, pp. 1925–1931, 2009.

[43] X. Li and Y. Ma, "Unconditionally secure public-key cryptosystem using entangled quantum states," *Information Technology Journal*, vol. 12, no. 16, pp. 3820–3824, 2013.

[44] X. Li and D. Zhang, "Quantum public-key cryptosystem based on super dense coding technology," *Journal of Computers*, vol. 8, no. 12, pp. 3168–3175, 2013.

[45] C. Wu and L. Yang, "Qubit-wise teleportation and its application in public-key secret communication," *Science China (Information Sciences)*, vol. 60, pp. 183–194, 2017.

[46] W. Wu, Q. Cai, H. Zhang, and X. Liang, "Bit-oriented quantum public-key cryptosystem based on bell states," *International Journal of Theoretical Physics*, vol. 57, no. 6, pp. 1705–1715, 2018.

[47] C. Wu and L. Yang, *A Complete Classification of Quantum Public-Key Encryption Protocols*, International Society for Optics and Photonics, Bellingham, WA, USA, 2015.

[48] D. Gottesman and I. Chuang, "Quantum digital signatures," 2001, https://arxiv.org/abs/quant-ph/0105032.

[49] F. Gao, S. Qin, F. Guo, and Q. Wen, "Cryptanalysis of the arbitrated quantum signature protocols," *Physical Review A*, vol. 84, Article ID 022344, 2011.

[50] H. Lee, C. Hong, H. Kim, J. Lim, and H. J. Yang, "Arbitrated quantum signature scheme with message recovery," *Physics Letters A*, vol. 321, no. 5-6, pp. 295–300, 2004.

[51] Y.-P. Luo and T. Hwang, "Arbitrated quantum signature of classical messages without using authenticated classical channels," *Quantum Information Processing*, vol. 13, no. 1, pp. 113–120, 2014.

[52] X. Lv and D. Feng, "An arbitrated quantum message signature scheme," in *Proceedings of the International Conference on Computational and Information Science*, pp. 1054–1060, Shanghai, China, December 2004.

[53] Y. Yang and Q. Wen, "Arbitrated quantum signature of classical messages against collective amplitude damping noise," *Optics Communications*, vol. 283, no. 19, pp. 3198–3201, 2010.

[54] G. Zeng and C. H. Keitel, "Arbitrated quantum-signature scheme," *Physical Review A*, vol. 65, Article ID 042312, 2002.

[55] R. J. Collins, R. J. Donaldson, V. Dunjko et al., "Realization of quantum digital signatures without the requirement of quantum memory," *Physical Review Letters*, vol. 113, no. 4, Article ID 040502, 2014.

[56] V. Dunjko, P. Wallden, and E. Andersson, "Quantum digital signatures without quantum memory," *Physical Review Letters*, vol. 112, Article ID 040502, 2014.

[57] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802-803, 1982.
[58] M. Hirt and K. Sako, "Efficient receipt-free voting based on homomorphic encryption," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, Bruges, Belgium, May 2000.
[59] R. J. Mceliece, "A public-key cryptosystem based on algebraic coding theory," *DSN Progress Report*, vol. 42, no. 44, pp. 114–116, 1978.
[60] S. G. Oded Goldreich and S. Halevi, "Public-key cryptosystems from lattice reduction problems," in *Proceedings of the Advances in Cryptology-CRYPTO*, pp. 112–131, Santa Barbara, CA, USA, August 1997.
[61] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, Innsbruck, Austria, May 2001.
[62] M. Bellare, A. Boldyreva, and A. ONeill, *Deterministic and Efficiently Searchable Encryption*, Springer, Berlin, Germay, 2012.