symmetry

MDPI

Review

A Review of Cryptographic Electronic Voting

Yun-Xing Kho [1,*], Swee-Huay Heng [1,*] and Ji-Jian Chin [2]

[1] Faculty of Information Science and Technology, Multimedia University, Jalan Ayer Keroh Lama, Melaka 75450, Malaysia

[2] Faculty of Computing and Informatics, Multimedia University, Persiaran Multimedia, Cyberjaya 63100, Malaysia; jjchin@mmu.edu.my

* Correspondence: yunxing_535357@hotmail.com (Y.-X.K.); shheng@mmu.edu.my (S.-H.H.)

Abstract: A vast number of e-voting schemes including mix-net-based e-voting, homomorphic e-voting, blind signature-based e-voting, blockchain-based e-voting, post-quantum e-voting, and hybrid e-voting have been proposed in the literature for better security and practical implementation. In this paper, we review various e-voting approaches to date. We first compare the structures, advantages, and disadvantages of the different e-voting approaches. We then summarise the security properties of the e-voting approaches in terms of their functional requirements and security requirements. In addition, we provide a comprehensive review of various types of e-voting approaches in terms of their security properties, underlying tools, distinctive features, and weaknesses. We also discuss some practical considerations in the design of e-voting systems. Subsequently, some potential research directions are suggested based on our observations.

Keywords: blind signature-based e-voting; blockchain-based e-voting; cryptography; homomorphic e-voting; hybrid e-voting; mix-net based e-voting; post-quantum e-voting

check for updates

Citation: Kho, Y.-X.; Heng, S.-H.; Chin, J.-J. A Review of Cryptographic Electronic Voting. *Symmetry* **2022**, *14*, 858. https://doi.org/10.3390/sym14050858

Academic Editor: Yu-Chi Chen

Received: 28 March 2022
Accepted: 8 April 2022
Published: 21 April 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

Electronic voting (e-voting) is an electronic system that allows users to make a collaborative decision or vote for candidates in an election. It handles the registration of voters, input of vote, vote casting, vote encryption, the transmission of the ballot to the server, vote storing, vote counting, and tabulation of the election result. The e-voting system can be used in various applications such as punched cards, smart cards, direct-recording e-voting systems (DRE), optical scan systems, and computers connected to the Internet. The e-voting system offers more accurate election results, faster result tabulation, minimises human errors, more convenience towards disabled or handicapped people, and self-tallying election results [1]. However, according to Peng [2] and Oo and Aung [3], e-voting faces challenges of scalability for large-scale elections, security challenges, unpredictable malfunctions of servers, and others. Some people feel uncomfortable adopting e-voting systems due to voter privacy as voter identity might be disclosed. The most important security properties to preserve as mentioned by Peng [2] and Sebé et al. [4] are the privacy of the voter, fairness, receipt-freeness, coercion-resistance, individual verifiability, universal verifiability, robustness, double-voting prevention, etc. Thus, many researchers have proposed schemes to enhance the security of e-voting systems and put e-voting systems in practice. In this paper, we focus on conventional approaches which cover mix-net-based e-voting, homomorphic e-voting, and blind signature-based e-voting, and latest developments which cover blockchain-based e-voting, post-quantum e-voting, and hybrid e-voting. We aim to draw a bigger picture of past and present e-voting scheme developments to provide readers with an overview of various e-voting approaches, in terms of their structure, advantages, and disadvantages. We then aim to provide a comprehensive review of each e-voting approach in terms of its security properties, underlying tools, distinctive features, and weaknesses. We also discuss some critical practical considerations in the design of e-voting systems. Finally, we conclude our analysis with some potential future research directions.

The mix-net-based e-voting scheme breaks the correlation between the voters and their votes with the shuffling process using the mix-server. Homomorphic e-voting scheme allows the authority to sum all ballots without decrypting them. Blind signature-based e-voting allows the authority to authorise the voter without revealing any information on the ballot by employing a blind signature as the underlying building block. The underlying homomorphic encryption scheme and blind signature scheme are instances of asymmetric cryptographic primitive. Meanwhile, blockchain-based e-voting schemes are immutable, distributed, and do not rely on trusted third parties, therefore minimising potential malicious activities. Post-quantum e-voting schemes are designed to be secure against quantum attacks. A hybrid scheme refers to the scheme that is constructed by integrating two or more approaches.

1.1. Entities in e-Voting System

A generic e-voting scheme involves the following entities:

Voter: Individuals who are eligible to vote for candidates.

Candidate: Nominees seeking to be considered in the election.

Registrar: Registrars are responsible for authenticating the voters.

Authority: Persons in charge of conducting the election.

Auditor: Authorised persons to verify and review election results.

Adversary: Malicious individuals attempt to corrupt elections. There are two main types of adversaries, external and internal [5]. External adversaries, also known as coercers, actively coerce voters to vote in certain ways, whereas internal adversaries attempt to breach the system and corrupt voter privacy and authority.

1.2. Structure of e-Voting System

The structure of e-voting systems consists of three phases [6], namely, pre-voting, prevoting, and post-voting. The processes in the pre-voting phase include the nomination of candidates, computation of the list of candidates, registration of voters, and computation of the list of eligible voters. Eligible voters cast their ballots during the voting phase. The post-voting phase mainly deals with the counting of votes and announcing the election results.

Figure 1 shows the general structure of mix-net-based e-voting, homomorphic e-voting, blind signature-based e-voting, blockchain-based e-voting, and post-quantum e-voting in the pre-voting phase, voting phase, and post-voting phase.

1.3. Advantages and Disadvantages of Various e-Voting Approaches

The summary presented in Table 1 are compiled from the works of [2,4,7–14].

As observed from the comparison analysis in Table 1, it is worth mentioning that hybrid schemes are more practical and efficient than other approaches. A hybrid scheme refers to the scheme that is constructed by integrating two or more approaches. A hybrid scheme inherits the advantages and security properties of combined cryptographic tools and eliminates the weaknesses of cryptographic tools individually. However, the use of these e-voting approaches varies depending on the application to which they are applied [15]. Therefore, different e-voting approaches may be suited for different applications.

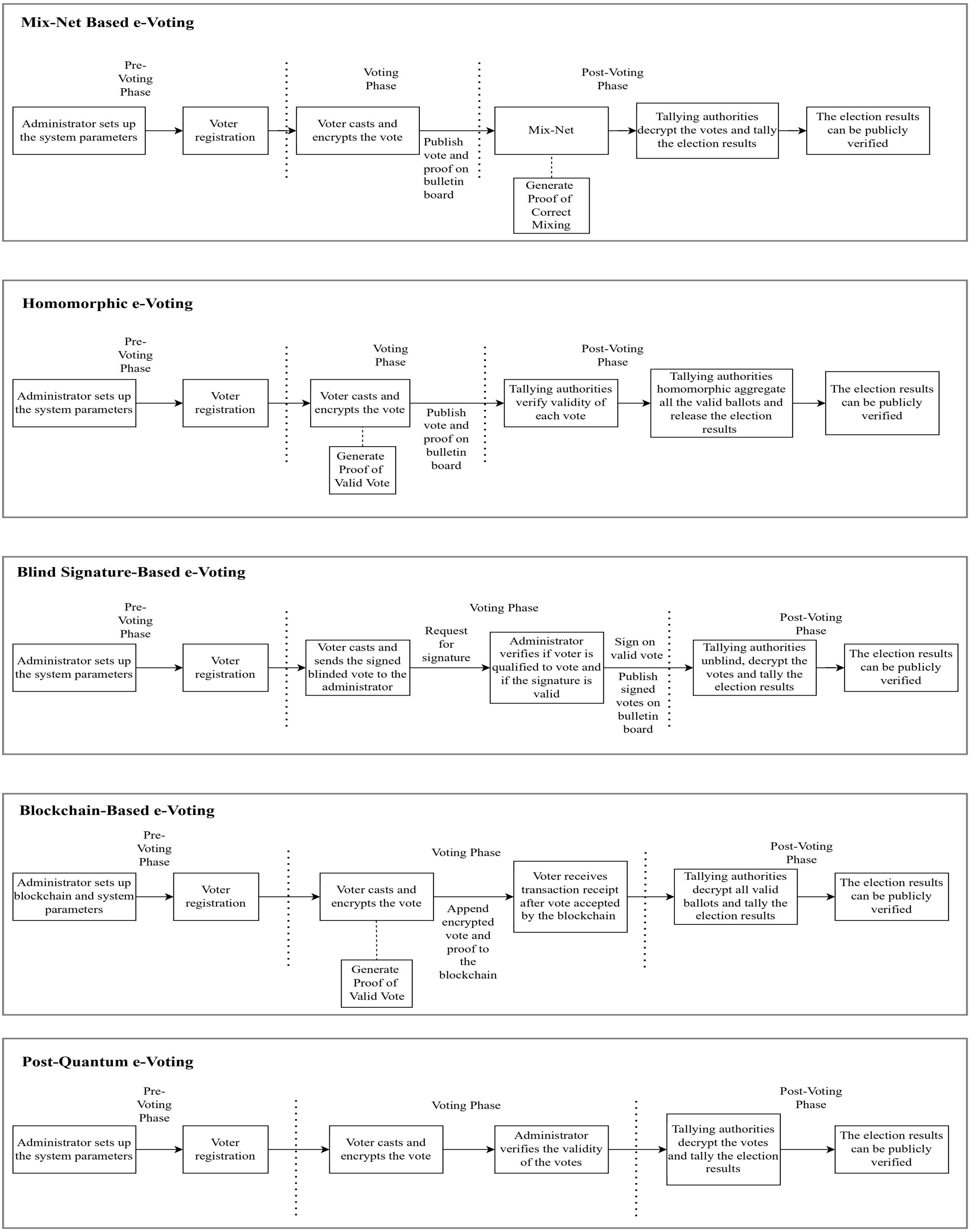
Mix-Net Based e-Voting
Pre-Voting Phase
Voting Phase
Post-Voting Phase
Administrator sets up the system parameters
Voter registration
Voter casts and encrypts the vote
Publish vote and proof on bulletin board
Mix-Net
Generate Proof of Correct Mixing
Tallying authorities decrypt the votes and tally the election results
The election results can be publicly verified
Homomorphic e-Voting
Pre-Voting Phase
Voting Phase
Post-Voting Phase
Administrator sets up the system parameters
Voter registration
Voter casts and encrypts the vote
Generate Proof of Valid Vote
Publish vote and proof on bulletin board
Tallying authorities verify validity of each vote
Tallying authorities homomorphic aggregate all the valid ballots and release the election results
The election results can be publicly verified
Blind Signature-Based e-Voting
Pre-Voting Phase
Voting Phase
Post-Voting Phase
Administrator sets up the system parameters
Voter registration
Voter casts and sends the signed blinded vote to the administrator
Request for signature
Administrator verifies if voter is qualified to vote and if the signature is valid
Sign on valid vote
Publish signed votes on bulletin board
Tallying authorities unblind, decrypt the votes and tally the election results
The election results can be publicly verified
Blockchain-Based e-Voting
Pre-Voting Phase
Voting Phase
Post-Voting Phase
Administrator sets up blockchain and system parameters
Voter registration
Voter casts and encrypts the vote
Generate Proof of Valid Vote
Append encrypted vote and proof to the blockchain
Voter receives transaction receipt after vote accepted by the blockchain
Tallying authorities decrypt all valid ballots and tally the election results
The election results can be publicly verified
Post-Quantum e-Voting
Pre-Voting Phase
Voting Phase
Post-Voting Phase
Administrator sets up the system parameters
Voter registration
Voter casts and encrypts the vote
Administrator verifies the validity of the votes
Tallying authorities decrypt the votes and tally the election results
The election results can be publicly verified

Figure 1. General structure of various e-voting approaches.

Table 1. Advantages and disadvantages of various e-voting approaches.

Approach	Advantages	Disadvantages
Mix-net-Based e-Voting	• Provides unlinkability between voters and their votes • The computation cost is lower than the homomorphic tallying e-voting scheme • Supports write-in ballots	• Difficult to implement on large-scale elections due to its complexity • Large amount of computation power is required for the mix server to prove the correctness of mixing • Vulnerable to DDOS attack
Homomorphic e-Voting	• Suitable for small-scale elections, efficient in the open phase • Do not require decrypting of the encrypted votes to tally the election result. Thus, voter privacy is achieved	• Requires intensive zero knowledge proof to prove the validity of votes (high communication cost) • High computation cost for the vote verification • This is not suitable for multi-candidate elections because the ballot must contain proof of a possible choice in the election; therefore, the encryption cost is high when there is a large range of preference
Blind Signature-Based e-Voting	• Simple, flexible, universally verifiable, and efficient • Intensive zero knowledge proof is not required • Guarantees anonymity • Supports write-in ballots • Most efficient in the tallying phase • Does not require high communication cost for the intensive phase	• Requires an anonymous channel where it suffers from complex computation and might be impractical to implement in the real world • Blind factor can serve as a voting receipt • Receipt-free blind signature e-voting requires physical assumption, e.g., an untappable channel that is impractical to implement over internet • Most of the proposed schemes required certificate authority to distribute key pairs to the voter and it is costly to maintain
Blockchain-Based e-Voting	• The votes stored in the blockchain are immutable • Allows the election results to be generated instantly • Offers transparency while guaranteeing privacy • Able to withstand a DOS attack	• Facing scalability as an issue due to the technology is new • Inadequate testing tools
Post-Quantum e-Voting	• Sustainable against quantum attacks • Does not require intensive zero knowledge proof	• Larger key size than public key algorithms, thus requires more storage space • Large sizes of data for signature and key establishment to be transmitted over communication channels, thus limits the speed of transmission and vulnerable to unforeseen quantum attacks

1.4. Organisation of This Paper

We review the security properties for a secure e-voting system in Section 2. We discuss some common cryptographic preliminaries in Section 3. We review various approaches of e-voting schemes in Section 4. We discuss some practical considerations in the design of e-voting systems in Section 5. We provide potential research directions based on our observations in Section 6. Finally, we conclude our results in Section 7.

2. Security Properties in e-Voting

We summarise the security properties of an e-voting system based on past research. The list of security properties is by no means exhaustive. According to Liaw [16], some of the properties are the same but presented using different terms. Most of the proposed e-voting schemes cannot fulfil all the security properties at once due to the contradiction between some of the security properties. For instance, privacy apparently contradicts verifiability as verifiability is required to link the voters and their votes; coercion-resistance requires sacrificing universal verifiability and the scheme could be complicated, unscalable, and impractical to fulfil the dispute-freeness property. According to Li et al. [5], the use of these security properties varies depending on the voting situation and specific requirements to which they are applied, none of the schemes satisfy all the requirements, because some requirements may overweigh others. However, Lee et al. [7] mentioned that privacy, double-voting prevention, universal verifiability, fairness, robustness and receipt-freeness are the basic security properties to be considered as a secure e-voting scheme. Shirazi et al. [17] also proposed several design principles for secure remote voting schemes. Their principles include voter accessibility and anonymity, vote verification, trustworthy design responsibility, proven security, published source codes, and expert supervision. The majority of their principles correspond to the aforementioned requirements.

We further categorised the established security properties into functional requirements and security requirements as follows [18]:

2.1. Functional Requirements

Functional requirements define the desired end functions and features required by a system. The functional requirements can be directly observed and tested.

Robustness: Any dishonest party cannot disrupt elections.

Fairness: No partial tally is revealed.

Verifiability: The election results cannot be falsified. There are two types of verifiability:

- **Individual verifiability:** The voter can verify whether their vote is included in the final tally.
- **Universal verifiability:** All valid votes are included in the final tally and this is publicly verifiable.

Soundness, completeness and correctness: The final tally included all valid ballots.

Eligibility: Unqualified voters are not allowed to vote.

Dispute-freeness: Any party can publicly verify whether the participant follows the protocol at any phase of the election.

Transparency: Maximise transparency in the vote casting, vote storing and vote counting process while preserving the secrecy of the ballots.

Accuracy: The system is errorless and valid votes must be correctly recorded and counted. This properties can be retained by universal verifiability.

Accountability: If the vote verification process fails, the voter can prove that he has voted and at the same time preserving vote secrecy.

Practicality: The implementation of requirements and assumptions should be able to adapt to large-scale elections.

Scalability: The proposed e-voting scheme should be versatile in terms of computation, communication and storage.

2.2. Security Requirements

A security requirement is the required security functionality that ensures that the scheme satisfies different security properties to solve a specific security problem or to eliminate potential vulnerabilities. Security requirements serve as fundamental security functionality for a system. Therefore, instead of constructing a custom security approach for every system, the standard security requirements allow researchers and developers to reuse the definitions of security controls and best practices.

Privacy and vote secrecy: The cast votes are anonymous to any party.

Double-voting prevention, unicity and unreusability: Eligible voters cannot vote more than once.

Receipt-freeness: The voter cannot attain any information that can be used to prove how he voted for any party.

Coercion-resistance: Coercers cannot insist that voters vote in a certain way and the voter cannot prove his vote to the information buyer.

Anonymity: The identity of the voter remains anonymous.

Authentication: Only eligible voters were allowed to vote.

Integrity: The system can detect the dishonest party that modifies the election results.
Unlinkability: The voter and his vote cannot be linked.

3. Cryptographic Preliminaries

In this section, we discuss some common cryptographic tools and assumptions that are used to construct a secure e-voting scheme.

3.1. Cryptographic Assumptions

Secure channels. For secure communication between two parties over an insecure medium, typically between the authorities and the voters. The following channels are categorised as secure channels:

- **Untappable channel**, proposed by Sako and Kilian [19]. It is a theoretically unobservable and secret communication channel. However, this channel is not practical for real-world implementation. Some of the proposed schemes make it even stronger with an unrealistic assumption, which is called an anonymous untappable channel.
- **Private channel**, proposed by Cramer et al. [20]. An observable but secure communication channel is implemented by a public or private key cryptosystem.

Anonymous channel. A communication channel that allows the adversary to spy on and intercept the information. This channel provides privacy to the voter's (sender) identity, where the identity of the voter is anonymous to the authorities (receiver) and observer. The mix-net proposed by Chaum [21] is analogous to an anonymous channel.

Voting booth. This assumption offers a receipt-freeness property. The voting booth was governed by authorities. Usually, the booth can only be entered by a voter at a time to cast a vote and there exists a communication channel between the authorities and the voting booth. If there is generation of receipt after the voter casts the vote, the voter is required to destroy the receipt before leaving the voting booth. However, this physical assumption is claimed to be impractical to implement in a remote voting scheme [5].

Bulletin board. As defined by Cramer et al. [22], a bulletin board is a public broadcast communication channel with memory. The voters are able to append and read their ballots to the bulletin board and the ballots are stored in the memory.

Decision Diffie–Hellman assumption (DDH). The DDH assumption is based on G. Given $D = (y_1, g_1, y_2, g_2)$, where $g_1, g_2 \in G, y_1 = g_1^x$, and $y_2 = g_2^x$ for $x \in \mathbb{Z}_q$. Given $D' = (y_1, g_1, y_2, g_2)$, where $y_1, g_1, y_2, g_2 \in G$ at random distribution. This assumption states that there is no polynomial time algorithm with a non-negligible probability that can distinguish between D and D'.

Computational Diffie–Hellman assumption (CDH). Assuming a large prime number, q, a $q-$ order cyclic group, G, generator of group G, P and binary tuple $(xP, yP) \in G^2$ for unknown integers $x, y \in \mathbb{Z}_q^*$. The problem of CDH in G is the computation of $(xyP) \in G$.

3.2. Cryptographic Tools

Plaintext equivalence test (PET). The PET operates on the ciphertext in the threshold cryptosystem. A pair of ciphertexts serves as an input and PET outputs a single bit to indicate whether the pair of ciphertexts is the same. PET revealed no additional data regarding the plaintext. Given two ciphertexts $\{v_1\}_k^{r_1}$ and $\{v_2\}_k^{r_2}$, which are encrypted with the same key. The decryption authority can identify that both ciphertexts are the same without disclosing any data regarding v_1, v_2 and the decryption key.

ElGamal cryptosystem. The computational hardness is based on discrete logarithms problems. It has three algorithms, namely, Key generation, Encryption and Decryption.

- **Key generation:** A generator g generates a large cyclic group G of prime order q and publish g, q and G. Alice randomly selects $x \in \mathbb{Z}_q^*$ and generates $y = g^x$. Alice keeps her private key, x and publishes her public key, y.

- **Encryption:** Bob encrypts message m with the public key of Alice. Bob first converts m into the element of G and selects a random $r \in \mathbb{Z}_q^*$. Second, he computes $d = m \cdot y^r$ and $c = g^r$. The cryptogram is a tuple (c, d).
- **Decryption:** Alice uses her private key to decrypt (c, d) by computing $m = \frac{d}{c^x}$ in G.

ElGamal cryptosystem supports (t, k) threshold secret sharing scheme.

Paillier cryptosystem. The computational hardness is based on the factoring problem. It has three algorithms, namely, Key generation, Encryption and Decryption.

- **Key generation:** Let $N = pq$ where N is RSA modulus and p, q are the prime integers. Let g be the integer order of multiple of N modulo N^2. The private key, $x = \lambda(N)$, where $\lambda(N) = lcm((p-1)(q-1))$ and the public key, $y = (N, g)$.
- **Encryption:** Let $m \in \mathbb{Z}_n$ as the plaintext message, select $x \in \mathbb{Z}_n^*$ randomly and generate the ciphertext, $c = g^M x^N \ mod\ N^2$.
- **Decryption:** Compute $m = \frac{L(c^{\lambda(N)}\ mod\ N^2}{L(g^{\lambda(N)}\ mod\ N^2} mod\ N$ to decrypt c, where L - function takes set $S_N = \{u < N^2 |\ u = 1\ mod\ N\}$ as the input and output $(u) = \frac{u-1}{N}$.

Cryptography over an elliptic curve. A public key cryptosystem can be constructed over a prime order subgroup of a group of points on elliptic curve and the computational hardness is based on the discrete logarithms problem. An elliptic curve E over a finite field $\mathbb{Z}_p$ can be defined by $y^2 = x^3 + Ax + B\ mod\ p$, where $A, B \in \mathbb{Z}_p$ constants with $4A^3 + 27B^2 \neq 0\ mod\ p$. Let $E(\mathbb{Z}_p)$ denote set of pairs of the curve $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$.

Secret sharing scheme. An election scheme with a single authority may corrupt the election results. This problem can be solved by introducing multi-authorities to share the secret such as the decryption key. There are variants of secret sharing schemes.

- $\boldsymbol{(t, k)}$ **threshold secret sharing scheme** proposed by Shamir [23], a secret is shared among k authorities where $t \leq k$. This scheme required a trusted party T to compute the shared-key generation protocol to generate the private key $X = K^{-1}$, publish the public key and compute k shares for the private key. T sends a share x_i to the authority via private communication channels. t or more honest authorities are required to submit their shares to be combined and construct the private key. The private key can resist collusion up to $t-1$ corrupt and $k-1$ dishonest authorities.
- **Verifiable secret sharing scheme** proposed by Chor et al. [24], trusted party T distributedly implementing by k authorities themselves with increase in the communication and computation. The verification of the protocol can only be done by k authorities; thus, any dispute requires a trusted third party to resolve.
- **Publicly verifiable secret sharing scheme (PVSS)** proposed by Schoenmakers [25], the verification of the correctness of each protocol can be conducted by any external party. This scheme provides the dispute-freeness property.

Homomorphic encryption. Given $E_K(m_1)$ and $E_K(m_2)$, $E_K(m_1 \oplus m_2)$ or $E_K(m_1 \otimes m_2)$ can be obtained without decrypting m_1 and m_2.

Homomorphic signcryption. Zhang et al. [26] first proposed a homomorphic signcryption scheme. This scheme combines homomorphism and signcryption, thereby allowing voters to encrypt and sign a ballot in a single step. The scheme consists of six algorithms, namely, Setup, Key Generation for Receiver (KeyGenR), Key Generation for Sender (KeyGenS), Signcrypt, Unsigncrypt, and Verification.

- **Setup:** This algorithm takes security parameter, λ as input and generates *params* as the output.
- **KeyGenR:** This algorithm takes *params* as the input and generates the private key and public key of the receiver.
- **KeyGenS:** This algorithm takes *params* as the input and generates the private key and public key, of the sender.
- **Signcrypt:** This algorithm takes *params*, the receiver's public key, sender's private key, and plaintext message, m from the message space, M as the input and generates homomorphic signcryption $HSC(m)$.

- **Unsigncrypt:** This algorithm takes *params*, the sender's public key, receiver's private key, and $HSC(m)$ as the input and generates plaintext message m.
- **Verification:** This algorithm takes *params*, the sender's public key, receiver's private key, $HSC(m)$, and a message, m'as the input, and generate 1 if $m = m'$, otherwise generate 0.

Digital signature. The digital signature scheme guarantees the integrity of the message and is able to identify the message sent from a particular sender.

- **RSA digital signature:** There are three algorithms in the RSA digital signature scheme, namely Key Generation, Signing, and Verification.
  - **Key Generation:** Input security parameter to compute (N, e, d). Private key, $y = (N, d)$ and public key, $x = (N, e)$.
  - **Signing** Compute the signature, $S = m^d \ mod \ N$ with private key and message, $m \in \mathbb{Z}_N^*$.
  - **Verification:** Input $x, m \in \mathbb{Z}_q^*$, and $S \in \mathbb{Z}_q^*$, output 1 if $m = S^e \ mod \ N$.
- **Escrowed linkable ring signature:** The origin ring signature scheme proposed by Rivest et al. [27] allows the signer to sign on the message in such a way that anyone can verify that the signature is signed by a signer from the signer group but cannot identify the real signer. This signature scheme enjoys the property of anonymity; no one can identify the identity of the real signer except for the signer himself. A linkable ring signature was first proposed by Liu et al. [28]. In addition to the ring signature scheme, this scheme enables anyone to identify whether the two signatures are signed by the same signer. Linking can be performed by linking authority in the escrowed linkable ring signature scheme. The linkability tag is encrypted with probabilistic encryption and cannot prove the non-authorship of others' signatures. In e-voting, a linkable ring signature can prevent double-voting and the escrowed linkable ring signature can detect the dishonest voting authority.
- **Blind signature:** It enables one to sign the message without revealing any information about the message, thus guaranteeing anonymity. There are five algorithms in this signature scheme, namely, Key Generation, Blinding, Signing, Unblinding, and Verification.
  - **Key Generation:** Compute the private key and public key of the signer.
  - **Blinding:** Sender computes their private key and public key, uses the private key to the blind message and sends the message to the signer.
  - **Signing:** Signer uses their private key to sign the blinded message and sends the signed blinded message to the sender.
  - **Unblinding:** The sender unblinds the message and sends the signature and message to the receiver.
  - **Verification:** The receiver verifies the message and uses the public key of the signer to verify the signature.

Lattices. Lattice L is a set of points in $n-$ dimensional space, typically $\mathbb{R}^n$ with periodic structure, the two conditions are as follows [29].

- It is an additive subgroup: $0 \in L$ and $\forall x, y \in L \quad -x, x + y \in L$.
- It is discrete: $\forall x \in L$, there exists a neighbourhood of x in $\mathbb{R}^n$ such that x is the only point of the lattice.

The common lattice computational problems are as follows [30].

- Shortest vector problem (SVP): Given a lattice basis $\mathbf{B}$, find the shortest nonzero vector in $\mathcal{L}(\mathbf{B})$.
- Closest vector problem (CVP): Given a lattice basis $\mathbf{B}$ and a target vector $\mathbf{t}$, find the lattice point $v \in \mathcal{L}(\mathbf{B})$ closest to $\mathbf{t}$ where the $\mathbf{t}$ is not compulsory in the lattice.
- Shortest independent vectors problem (SIVP): Given a lattice basis $\mathbf{B} \in \mathbb{Z}^{n*n}$, find n linearly independent lattice vectors $S = [s_1, ..., s_n]$ where $s_i \in \mathcal{L}(\mathbf{B})$ for all i minimise the quantity, $||S|| = max_i ||s_i||$.

4. Review of Various e-Voting Approaches

In this section, we perform a comprehensive review on various e-voting approaches and discuss the development of each approach. We also provide a comparison analysis of the different schemes under each approach in terms of their structure, security properties, underlying tools, distinctive features, and weaknesses. Please note that the weaknesses summarised in Tables 2–7 are presented to the best of our knowledge based on the available information from the existing literature. Further study is required to be conducted in order to find out if there exists any possible weakness in some other mentioned schemes.

4.1. Mix-Net-Based e-Voting

4.1.1. Scheme Development

Mix-net-based e-voting was first proposed by Chaum [21], the function of mix-net is to create an anonymous channel for anonymous communication. It is a trusted third party that breaks the link (shuffles) between the sender, recipient and the message, thus eavesdropping does not work in this case. In the e-voting scheme, it breaks the link between voters and their ballots. As highlighted by Jakobsson et al. [31], mix-net should be robust, guarantee privacy and operate correctly.

Mix-net schemes have two categories, decryption mix-net and re-encryption mix-net. The first proposed mix-net was decryption mix-net by Chaum [21]; it is a simple RSA decryption mix-net. Every mix server contains a key pair; the sender encrypts the message iteratively with the public keys of mix servers reversely (onion encryption). The first mix server decrypts the outer layer of the ciphertexts, shuffles it, and passes the result to the next server. The second mix server repeats the same process as the first mix server. The process is completed if all the mix servers perform the process simultaneously. The encryptions were all removed and the messages were posted in random order.

The second type of mix-net is the re-encryption mix-net proposed by Park et al. [32] based on randomisation. It has two phases: mixing and decryption phases. In the mixing phase, the encrypted messages are shuffled and re-encrypted. In the decryption phase, the output is decrypted from the mixing phase. The server in the mixing and decryption phases can be either a different server or the same server. The proposed scheme of Park et al. [32] works as follows: the ElGamal cryptosystem is used in the proposed re-encryption mix-net. Several trustees share the key pair and the sender encrypts the message with the public key of the trustees. The first mix server re-encrypts the encrypted message of the sender, shuffles it, and sends it to the next mix servers. All the mix servers repeat the same process once. The results were posted in random order. The presence of decryption process depends on different applications. The recently proposed schemes mostly employed the re-encryption mix-net in the e-voting system as it is more efficient, robust and flexible. Re-encryption mix-net is more lightweight than the decryption mix-net as the input message is encrypted only once with a public key, whereas in the decryption mix-net, the input message is encrypted iteratively (onion encryption). In addition, the re-encryption mix-net has an advantage over the decryption mix-net in terms of its robustness. In a re-encryption mix-net, a single faulty mix does not affect the election process, unlike in a decryption mix-net. This is because of the re-encryption step in the mixing phase of the re-encryption mix-net. During the mixing phase of the re-encryption mix-net, the inputs are mixed and re-encrypted. However, in the decryption mix-net, a fixed set of mixes is required to be selected and to provide their keys in advance of voting, which leads to the decryption mix-net prompting failure to complete the election process if a single faulty mix exists.

According to Lee et al. [7], the decryption mix-net and re-encryption mix-net can be further categorised into optimistic mix-net and verifiable mix-net based on their correctness proof. In an optimistic mix-net, each mix server will not generate its proof of correct shuffling and the proof is generated as a whole after the plaintext shuffling results are produced by the mix-net. The limitations of the optimistic mix-net are that the malicious mix server cannot be detected instantly and plaintext shuffling results are generated even if the shuffling is inaccurate. While in verifiable mix-net, each mix server will generate its proof of correct shuffling after the shuffling operation. Peng [2] pointed out that verifiable mix-nets have low efficiency and optimistic mix-nets have weak robustness and are vulnerable to attack against privacy via malicious mix-nets.

4.1.2. Comparison Analysis

Table 2 shows the detailed comparison of mix-net based e-voting schemes since 1994.

Table 2. Comparison of mix-net-based e-voting schemes.

Scheme	Security Properties	Cryptographic Tools	Distinctive Features	Weaknesses
Chaum [21]	Anonymity, Privacy	RSA-based Public Key Encryption	Do not require universally trusted authority	Less efficient as it required a large length of ciphertext [32]
Park et al. [32]	Fairness	ElGamal Encryption	Computationally secure and efficient anonymous channel without a ciphertext length expansion problem	The anonymous channel is not secure [33]
Sako and Kilian [19]	Receipt-Freeness, Individual Verifiability	Chameleon Bit Commitment Scheme	First receipt-free mix-net-based e-voting, reduce the requirement of physical assumption to achieve receipt-freeness	Robustness and privacy problem [34]
Michels and Horster [34]	Not provided	Chameleon Bit Commitment Scheme	Perform cryptanalysis on [19]'s proposed scheme	
Abe [35]	Robustness, Universal Verifiability	Threshold ElGamal Decryption, ElGamal Encryption	Introduce universally verifiable mix-net	Inefficient in computation and communication, not suitable for large-scale elections [31]
Neff [36]	Soundness, Completeness	ElGamal Encryption	The voting credentials are mixed before the election day	Size and complexity [36] and when there are large inputs, proving the correctness is inefficient [37]
Jakobsson et al. [31]	Privacy, Robustness, Universal Verifiability	Not provided	RPC-based mix-net (Randomised Partial Checking)	Weak privacy guarantee [37]
Boneh and Golle [37]	Soundness, Robustness, Privacy, Correctness, Universal Verifiability	ElGamal Re-Encryption Mix-Net	Ensure correct mixing for a large e-voting system, low computational mixing	Weak privacy guarantee [37]
Chaum [38]	Vote Secrecy, Robustness	Public Key Encryption, Digital Signature, Visual Cryptography	Voter-verifiable e-voting scheme	Complexity [39]
Ryan [39]	Not provided	Onion Encryption	Voter-verifiable e-voting scheme, easy implementation	
Lee et al. [7]	Privacy, Double-Voting Prevention, Universal Verifiability, Fairness, Robustness, Receipt-Freeness	Threshold Decryption Protocol, ElGamal Encryption	Introduce tamper-resistant randomiser (TRR) in receipt-free mix-net-based e-voting	Less efficient due to the employment of verifiable mix-net that required higher bandwidth and computation [40]
Aditya et al. [40]	Privacy, Eligibility, Double-Voting Prevention, Fairness, Receipt-Freeness, Robustness, Verifiability	Threshold Version of ElGamal Encryption	Enhance the efficiency of receipt-free mix-net-based e-voting	Rely on the trust assumption on administrator and vulnerable to invalidation attack by a misbehaviour mix server [40]

Table 2. *Cont.*

Scheme	Security Properties	Cryptographic Tools	Distinctive Features	Weaknesses
Chaum et al. [41]	Vote Secrecy, Transparency, Verifiability	Onion Encryption	Improve the origin mix-net-based e-voting scheme to be a voter-verifiable e-voting system	Employ anonymous channel that is impractical in real-world [42]
Juels et al. [43]	Correctness, Coercion-Resistance, Verifiability	Threshold version ElGamal Encryption, Plaintext Equivalence Test (PET)	Allow adversaries to coerce the voter to disclose their private key and to vote in a certain way (JCJ protocol)	Poor efficiency in removing duplicated and illegal votes [44]
Her et al. [45]	Not provided	ElGamal Encryption	Introduce universal re-encryption mix-net and RFID system in the e-voting system	
Carroll and Grosu [46]	Privacy, Fairness, Accuracy, Robustness, Coercion-Resistance, Universal Verifiability	Threshold Version ElGamal Encryption	Combine the user-centric mix networks and voter-verifiable receipts	
Zwierko and Kotulski [47]	Privacy, Completeness, Soundness, Unreuseability, Eligibility, Receipt-Freeness, Robustness, Verifiability	Merkle's Puzzles, Secure Secret Sharing Scheme	Multi-interface with mobile voting architecture	
Clarkson et al. [48]	Coercion-Resistance, Universal Verifiability	RSA ElGamal Encryption	Suitable for remote e-voting (Civitas)	Robustness and the coercion-resistance problem [17]
Sebé et al. [4]	Authentication, Unicity, Privacy, Integrity, Coercion-Resistance, Fairness	ElGamal Encryption, Elliptic Curves	Hash-based with ElGamal homomorphic properties	
Furukawa et al. [49]	Universal Verifiability	ElGamal Encryption, Elliptic Curve	Suitable to be used in a private organisation with over 20,000 voters	Do not achieve receipt-freeness and do not guarantee the privacy of abstaining voters
Lee et al. [50]	Privacy, Unreusability, Eligibility, Fairness, Completeness, Soundness	ElGamal Encryption	Provide voters with a receipt with the divide-and-choose method	Difficult to compare verification codes on the screen and printed receipt, voters need to choose numerous random selections [50]
Bulens et al. [51]	IND-CCA2 Security assuming the DDH problem is hard	Submission Secure Augmented (SSA) Cryptosystem	Introduce mix-net in Helios 3.1	
Peng [2]	Privacy, Soundness	Threshold Version ElGamal Encryption	More efficient and robust with ElGamal encryption	
Spycher et al. [44]	Privacy, Accuracy, Coercion-Resistance	Plaintext Equivalence Test (PET), ElGamal Encryption	Coercion-resistant e-voting scheme in linear time	The scheme does not fulfil coercion-resistance [52]
Bibiloni et al. [10]	Privacy	Signed ElGamal Encryption	The validity of votes is checked during the election period instead of the tallying process	
Tamura et al. [53]	Privacy, Fairness, Robustness, Verifiability	Not provided	Employ modified simplified verifiable re-encryption mix-nets (SVRM)	Less efficient as the scheme assumed there is a state erasable voting booth [54]

Table 2. *Cont.*

Scheme	Security Properties	Cryptographic Tools	Distinctive Features	Weaknesses
Chang et al. [55]	Privacy, Fairness, Robustness, Completeness, Unreusability, Eligibility, Receipt-Freeness, Verifiability	ElGamal Encryption	End-to-end verifiability mix-net based on Helios 1.0	
AboSamra et al. [11]	Integrity, Accuracy, Scalability, Practicality, Privacy, Eligibility, Fairness, Coercion-Resistance, Receipt-Freeness, Transparency, Verifiability	Threshold Secret Sharing Scheme, Digital Signature, Public Key Encryption	Use voting machine and paper ballots	
Alam et al. [54]	Privacy, Accuracy, Integrity, Coercion-Resistance, Fairness, Robustness	ElGamal Encryption	Employ modified SVRM and confirmation numbers (CN)	
McMurtry et al. [56]	Privacy, Verifiability, Weak Receipt-Freeness	ElGamal Encryption, Pedersen Commitment	Voting integrity is ensured even though all electronic devices are corrupted	The protocol ensures the weak receipt-freeness property [56]
Rønne et al. [57]	Universal Verifiability, Individual Verifiability, Privacy, Receipt-Freeness, Coercion-Resistance	Homomorphic Encryption, Plaintext Equivalence Test (PET)	End-to-end verifiable e-voting scheme (Selene)	
Tejedor-Romero et al. [58]	Verifiability, Privacy, Integrity, Eligibility	Shamir Secret Sharing	Remote end-to-end verifiable e-voting scheme (DiverSEC)	Voters are able to prove their votes to coercers; no real-time troubleshooting protocols that can withstand integrity attacks [58]

Park et al. [32] improved the efficiency of the mix-net based e-voting scheme proposed by Chaum [21]. However the Park et al. [32]'s scheme was broken by Pfitzmann [33]. Ogata et al. [59] then improved the Park et al. [32] scheme.

Sako and Kilian [19] proposed the first receipt-free mix-net-based e-voting, Michels and Horster [34] performed cryptanalysis on the proposed scheme of Sako and Kilian [19] and proved that the Sako and Kilian [19] scheme has robustness and privacy problems.

Aditya et al. [40] modified both Lee et al. [7]'s scheme from verifiable mix-net to optimistic mix-net and Golle et al. [60]'s optimistic mix-net scheme to offer receipt-freeness. The modified schemes are then combined to form an efficient receipt-free mix-net-based e-voting scheme.

Chaum [38] proposed a voter-verifiable e-voting scheme that provides maximum transparency while preserving vote secrecy using visual cryptography. The Prêt à Voter scheme was proposed by Ryan [39], which employed onion encryption to guarantee privacy of the voter. It is an end-to-end verifiable paper-based scheme that issues the voter a receipt after receiving the voter's vote; thus, the voter can verify that the vote is not altered. This proposed scheme replaced visual cryptography in the Chaum [38] scheme with an encoded vote in two aligned columns of paper strips.

Juels et al. [43] introduced the first coercion-resistance mix-net-based e-voting scheme. Civitas [48] was the first e-voting scheme that satisfied both verifiability and coercion-resistance. The construction of Civitas was based on the construction of Juels et al. [43]. Spycher et al. [44] claimed that Juels et al. [43]'s scheme is impractical to implement due to the poor efficiency in removing duplicated and illegal votes. Spycher et al. [44] solved the efficiency problem in Juels et al. [43]'s scheme while maintaining the same security properties and trust assumptions. Spycher et al. [44] employed a linear time scheme to remove duplicated votes and implement an electoral roll to identify illegal votes.

Adida [61] proposed a web-based open audit e-voting scheme, namely, Helios 1.0, which is based on Benaloh [62]'s scheme. However, the mix-net integrity proof cannot be directly verifiable and the verification cost is high due to the implementation of zero-knowledge interactive proof in the setting. Thus, Helios 1.0 is not efficient in large-scale elections. Chang et al. [55] improved Helios 1.0 by employing a more easy mix-net integrity proof and faster computations in the mixing phase. The proposed scheme is called Apollo. Bulens et al. [51] proposed a variant of Helios that uses a mix-net-based tallying method.

Rønne et al. [57] proposed an end-to-end verifiable e-voting scheme, namely Selene. The scheme was designed for use in the voting booth at the polling station using paper ballots. The system employed a smartcard-based public-key scheme to achieve verifiability. The authors left the security model with analysis and proofs for future work. Potential future work will also include user experience, usability testing, and exploring the postal version of the voting scheme.

4.2. Homomorphic e-Voting

4.2.1. Scheme Development

Homomorphism allows the tallier to operate on ciphertext without decrypting it. For example, suppose there are $E_K(m_1)$ and $E_K(m_2)$, then $E_K(m_1 \odot m_2)$ can be obtained, $\odot$ can be either modular addition $\oplus$ or modular multiplication $\otimes$. There are two types of homomorphic schemes: partially homomorphic and fully homomorphic. A partially homomorphic encryption scheme performs only addition operations on ciphertext. The Paillier cryptosystem [63], RSA cryptosystem [64] and ElGamal cryptosystem [65] are common choices for partially homomorphic schemes. However, ElGamal encryption distributed key generation is more efficient than the Paillier encryption scheme when the same security is required [66]. ElGamal is most often used in homomorphic encryption e-voting schemes due to its exponential form for achieving an additive homomorphism, whereas a fully homomorphic scheme was first proposed by Gentry [67]. A fully homomorphic encryption scheme can perform both addition and multiplication operations on the ciphertexts.

Homomorphic e-voting consists of two variants, additive $\oplus$ homomorphism first proposed by Cohen and Fischer [68] and multiplicative $\otimes$ homomorphism first proposed by Peng et al. [69]. Homomorphic e-voting is suitable for small-scale elections (YES/NO elections). The difference between additive homomorphic e-voting and multiplicative homomorphic e-voting schemes is in the tallying phase. In the additive homomorphic e-voting tallying phase, it recovers the sum of votes for the candidates: $E(m_1)E(m_2) = E(m_1 + m_2)$. No vote is decrypted. In the multiplicative homomorphic e-voting tallying phase, the ballot is decrypted to recover the product of votes, and the product is then factorised to obtain votes: $E(m_1 m_2) = E(m_1)E(m_2)$.

4.2.2. Comparison Analysis

Table 3 shows the detailed comparison of homomorphic e-voting schemes since 1986.

Table 3. Comparison of homomorphic e-voting schemes.

Scheme	Security Properties	Cryptographic Tools	Distinctive Features	Weaknesses
Cohen and Fischer [68]	Privacy, Correctness	Public Key Encryption	Hide the actual votes value instead of hiding the voters	Do not satisfy vote secrecy [22]
Benaloh and Yung [70]	Privacy, Correctness	Probabilistic Encryption	Enhance privacy of voters	Efficiency problem [32]
Benaloh [71]	Robustness, Verifiability	Probabilistic Encryption, Threshold Decryption	Multi-authority election	Rely on r-th residuosity assumptions, once the assumption is broken, the ballots can be decrypted [22]

Table 3. *Cont.*

Scheme	Security Properties	Cryptographic Tools	Distinctive Features	Weaknesses
Sako and Kilian [72]	Universal Verifiability	Families of Partially Compatible Homomorphic Encryption Functions	A partially compatible homomorphic encryption function	Less efficient as the scheme relied on discrete logarithm assumption, robustness is not fully addressed [20]
Benaloh and Tuinstra [73]	Privacy, Correctness, Receipt-Freeness, Verifiability	Probabilistic Encryption	Implement voting booth and the scheme can be either one tallying authority or multiple tallying authorities	Rely on *r*-th residuosity assumptions, once the assumption is broken, the ballots can be decrypted [22]
Cramer et al. [20]	Privacy, Robustness, Universal Verifiability	Homomorphic Encryption	A non-interactive verifiable secret sharing based on discrete logarithms	Computational and communication complexity [22]
Cramer et al. [22]	Privacy, Robustness, Double-Voting Prevention, Universal Verifiability	Threshold version ElGamal Encryption	Multi-authority election	Only support Yes/No elections [74] and not suitable for large-scale elections [52]
Hirt and Sako [75]	Privacy, Receipt-Freeness, Correctness	ElGamal Encryption	Vote-and-go e-voting scheme	Employ a one-way untappable channel that is a weak physical assumption for receipt-freeness [76]
Lee and Kim [77]	Privacy, Completeness, Soundness, Unreusability, Eligibility, Fairness, Robustness, Receipt-Freeness, Universal Verifiability	Threshold version ElGamal Encryption	Implement honest verifier in the receipt-free scheme	The malicious honest verifier can falsify the result of the vote; the voter can cast an invalid vote with the assistance of the malicious honest verifier [78]
Hirt [78]	Receipt-Freeness	Homomorphic Encryption Scheme	Implement shuffling technique with a randomiser	Employ a two-way untappable channel that is difficult to implement in the real-world [76]
Magkos et al. [79]	Privacy, Robustness, Double-Voting Prevention, Universal Verifiability, Receipt-Freeness	Threshold version ElGamal Encryption	Employ a tamper-resistance smartcard and fulfil receipt-freeness without the implementation of untappable channels between voting authorities and the voter	Do not satisfy receipt-freeness [76]
Damgård and Jurik [80]	Not provided	Paillier Probabilistic Public-Key Encryption	Multi-authority election	Privacy is guaranteed if the verifier is honest [81]
Baudron et al. [74]	Privacy, Receipt-Freeness, Robustness, Verifiability	Paillier Encryption, Threshold Decryption	Support countrywide elections	If all tallying authorities collectively corrupt, the ballot secrecy will not be protected [15]
Katz et al. [82]	Privacy, Robustness, Universal Verifiability	Encryption Scheme Employing Quadratic Residuosity	Introduce a cryptographic counter	Do not support receipt-freeness and prevention of double-voting; less practical due to the number of rounds needed for voting to be carried out [82]
Kiayias and Yung [1]	Privacy, Dispute-Freeness, Fairness, Perfect Vote Secrecy, Universal Verifiability	Homomorphic Encryption	In the tallying phase, any third party can be the tallier, often referred to as self-tallying election	Privacy is guaranteed if the verifiers are honest [81]
Lee and Kim [76]	Privacy, Completeness, Soundness, Unreusability, Eligibility, Fairness, Robustness, Receipt-Freeness, Coercion-Resistance, Universal Verifiability	ElGamal Encryption, Threshold ElGamal Decryption	Introduce a tamper-resistance randomiser in receipt-free scheme	Less efficient in vote validity checking [83]

Table 3. *Cont.*

Scheme	Security Properties	Cryptographic Tools	Distinctive Features	Weaknesses
Peng et al. [69]	Unlinkability, Verifiability	ElGamal Encryption	Multiplicative homomorphism	Weak privacy [66]
Adida [61]	Privacy, Coercion-Resistance, Verifiability	ElGamal Encryption	First web-based and open audit homomorphic e-voting (Helios 1.0)	High computational cost and complex proof of integrity of mix-net [55]
Chow et al. [15]	Receipt-Freeness, Correctness, Vote Secrecy, Universal Verifiability	ElGamal Encryption, Escrowed Linkable Ring Signatures	Vote-and-go election scheme without tamper-resistant hardware and anonymous channel	
Peng and Bao [84]	Privacy, Robustness, Correctness	Distributed Paillier Encryption	Improve the efficiency of the proof of vote validity in homomorphic e-voting	Privacy is guaranteed if the verifier is honest [81]
Peng and Bao [83]	Not provided	Paillier Encryption and Distributed Decryption, Digital Signature	A special membership proof is introduced to improve the efficiency in the proof of the validity of votes	The scheme is efficient if only one verifier checks the vote validity, thus it is not universally verifiable [81]
Huszti [85]	Privacy, Receipt-Freeness, Eligibility, Coercion-Resistance, Unreusability, Verifiability	Distributed ElGamal Encryption, RSA Blind Signature, Meta-ElGamal Signature	Combine the signature scheme with the homomorphic e-voting system	
Peng [81]	Privacy	Distributed Paillier Encryption	Improve the efficiency of the proof of vote validity	
Bernhard et al. [86]	Vote Secrecy	ElGamal Encryption	Multi-authority election	
Yi and Okamoto [87]	Coercion-Resistance, Verifiability	Threshold version ElGamal Encryption, Modified ElGamal Signature	Large-scale remote end-to-end homomorphic e-voting	Employ an untappable channel in the proposed scheme
Shinde et al. [88]	Privacy, Completeness, Double-Voting Prevention, Eligibility, Fairness, Correctness, Receipt-Freeness, Universal Verifiability	Modified ElGamal Encryption, ElGamal Digital Signature	Combine the signature scheme with the homomorphic e-voting system	
Àngels Cerveró et al. [89]	Privacy, Fairness, Authentication, Integrity, Unicity, Coercion-Resistance, Verifiability	Elliptic Curve ElGamal Encryption, Digital Signature	Remote and large-scale elections	
Kiayias et al. [90]	Privacy, Verifiability	ElGamal Encryption	An end-to-end verifiable e-voting without any setup assumptions or any existence of random oracle	
Yang et al. [91]	Privacy, Integrity, Correctness, Verifiability	Exponential ElGamal Encryption	Multi-authority election and end-to-end voter-verifiable scheme	Security assumption relies on the existence of at least one authority that is honest [91] and high computational cost [92]
Fan et al. [93]	Privacy, Correctness, Eligibility, Unicity, Transparency	Homomorphic Signcryption, Distributed Homomorphic Encryption	Election result can be tallied by anyone	
Fan et al. [92]	Privacy, Eligibility, Transparency, Unicity, Correctness, Verifiability	Homomorphic Signcryption	Lighten the tallying process by employing homomorphic signcryption scheme	Support only Yes/No elections [92]

The homomorphic e-voting scheme proposed by Cohen and Fischer [68] was the first end-to-end verifiable scheme, but the scheme did not satisfy vote secrecy as the government could read any of the votes. Benaloh and Tuinstra [73], Cramer et al. [22] and Hirt and Sako [75] further improved the scheme of Cohen and Fischer [68].

Benaloh and Tuinstra [73] first introduced receipt-freeness in homomorphic e-voting based on the assumption of a voting booth. Hirt and Sako [75] claimed that in one tallying authority scheme of Benaloh and Tuinstra [73] satisfied receipt-freeness but did not satisfy vote secrecy, while in a multiple tallying authority scheme, it maintained vote secrecy but did not satisfy receipt-freeness. Hirt and Sako [75] improved the scheme by introducing the physical assumption of a one-way secret communication channel between voters and authorities.

Lee and Kim [77] proposed receipt-free e-voting by employing honest verifier to verify the validity of the first ballot of the voter and provide a randomisation service. The proposed scheme was constructed based on the Cramer et al. [22] scheme. However, the malicious honest verifier can falsify the result of the vote, the voter can cast an invalid vote with the assistance of the malicious honest verifier and the voter can obtain the voting receipt as the voter chooses the hash value for the first ballot. The value can serve as the receipt, which faces the same attack as the Benaloh and Tuinstra [73] scheme. Hirt [78] fixed the issues in the Lee and Kim [77] scheme by introducing a third party randomiser to replace the honest verifier.

Magkos et al. [79] proposed a receipt-free e-voting scheme using a tamper-resistance smartcard and the proposed scheme was based on the scheme proposed by Cramer et al. [22]. However, the scheme faced the same issues as Benaloh and Tuinstra [73] and Lee and Kim [77]. Lee and Kim [76] fixed the issue in Magkos et al. [79]'s scheme by introducing a tamper-resistant randomiser (TRR). The voter encrypts the vote via an interactive protocol using the TRR. Thus, the voter loses its randomness.

Peng et al. [69] noticed a limitation in all additive homomorphic e-voting schemes. The decryption key must be shared among talliers. The implementation of key generation in a distributed manner is inefficient for practical additive homomorphic encryption and requires a strong trust. It is impractical to implement in e-voting scheme. Thus, Peng et al. [69] proposed a multiplicative homomorphic e-voting scheme to overcome this limitation.

Bernhard et al. [86] claimed that the Helios 1.0 e-voting scheme did not fulfil vote privacy. Bernhard et al. [86] improved vote privacy in Helios 3.0, while maintaining the system architecture and trust assumptions.

Zhang et al. [26] first introduced homomorphic signcryption in an e-voting system. The security of the scheme was not tested properly because it does not verify the signature; it only verifies the encryption part and only a single authority to tally the election result. According to the concept proposed by Zhang et al. [26], Fan et al. [93] implemented a distributed homomorphic signcryption e-voting scheme called DHS-voting. This scheme can verify the signatures in less time and the election results can be tallied by anyone.

Microsoft developed an e-voting system used in voting booths, namely ElectionGuard. The system supports end-to-end verifiable elections and is an open-source software development kit freely available on GitHub [94]. The system uses ElGamal, homomorphic tallying, and sigma protocols to allow universal verifiability without adversely affecting privacy [95].

4.3. Blind Signature-Based e-Voting

4.3.1. Scheme Development

A blind signature is a specially featured digital signature. The message was blinded before the message was signed. It was first proposed by Chaum [96] for an untraceable payment system. Fujioka et al. [97] first implemented a blind signature in an e-voting system. Blind signature-based e-voting allows the voter to blind his vote; thus, the voting authority can validate the vote without knowing the value. There are various types of blind signatures, such as threshold blind signatures and identity-based blind signatures. The threshold blind signature scheme avoids single point failure and thus enhances robustness. The process is repeated N times among the entities. It assumes at least t replicated works where the threshold t must be more than 1 and less than N . The signing process on blind message is carried out by each of the N entities and only if the message is signed by *t* entities is it considered a valid signature. An identity-based blind signature was first proposed by Zhang and Kim [98]. Kumar et al. [99] subsequently implemented an identity-based blind signature in an e-voting system. In this setting, the proposed system issues the receipt to the voter and the voting information can serve as proof. However, this may cause vote selling.

However, e-voting schemes that employ blind signatures as the underlying tools suffer from the abstaining voter problem [100], and it is challenging to design a blind signature system that does not allow a corrupted election authority to add votes of its choice. This problem could be resolved by employing multi-authority e-voting scheme so that the single corrupt authority does not have the power to control the entire election process [101,102].

4.3.2. Comparison Analysis

Table 4 shows the detailed comparison of blind signature-based e-voting schemes since 1996.

Table 4. Comparison of Blind Signature-Based e-Voting Schemes.

Scheme	Security Properties	Cryptographic Tools	Distinctive Features	Weaknesses
Fujioka et al. [97]	Completeness, Soundness, Privacy, Unreusability, Eligibility, Fairness, Verifiability	Bit-Commitment, Digital Signature, Blind Signature	Support large-scale elections at the same time ensure fairness and privacy	Voters are required to join the election from registering phase to the counting phase [103]
Okamoto [104]	Privacy, Fairness, Anonymity, Receipt-Freeness	RSA Blind Signature, Public-Key Encryption, Trap-Door Bit-Commitments	Implemented using a one-way anonymous communication channel between voter and authority	Coercers can force voters to use special parameters, thus the ballot can open in one way and the scheme is not receipt-freeness [8]
Okamoto [105]	Receipt-Freeness	RSA Blind Signature, Public-Key Encryption	Introduce a voting commission and untappable channel, suitable for large-scale elections	The voter is required to be active in all election phases, relying on a anonymous one-way secret communication assumption where this is difficult to implement in practice [75]
Ohkubo et al. [103]	Privacy, Completeness, Eligibility, Fairness, Unreusability, Verifiability	Threshold Encryption, Blind Signature, Digital Signature	Introduce the vote-and-go concept	The scheme does not satisfy receipt-freeness [106]
Jan et al. [107]	Privacy, Accuracy	Blind Signature	A practical e-voting scheme with the integration of e-mail and a web browser	
Magkos and Chrissikopoulos [108]	Privacy, Accuracy, Verifiability	RSA Public Key Encryption, Blind Signature	Equitably fair blind signature-based e-voting scheme	
Ibrahim et al. [109]	Universal Verifiability	Digital Signature, Blind Signature, Diffie–Hellman Key Exchange, Password-Based Encryption	Implement Java socket technology and a BouncyCastle cryptography provider	
Liaw [16]	Completeness, Coercion-Resistance, Unicity Robustness, Fairness, Anonymity, and Verifiability	RSA Blind Signature	Enhance the blind signature-based e-voting to satisfy maximum properties	
Xia and Schneider [8]	Receipt-Freeness, Individual Verifiability	RSA Blind Signature, mix-net	First voter-verifiable receipt-free e-voting scheme	

Table 4. *Cont.*

Scheme	Security Properties	Cryptographic Tools	Distinctive Features	Weaknesses
Cetinkaya and Doganaksoy [42]	Privacy, Eligibility, Coercion-Resistance, Unicity, Fairness, Robustness, Accuracy, Individual Verifiability, Universal Verifiability	RSA Blind Signature, Threshold encryption	Combine blind signature-based e-voting with s Pseudo Voter Identity (PVID) scheme (DynaVote)	Privacy issues and less efficient in the recast process in counting phase [110]
Cetinkaya and Koc [110]	Privacy, Coercion-Resistance, Accuracy, Unicity, Robustness, Fairness, Eligibility, Individual Verifiability	RSA Blind Signature	Employ a PVID scheme	
Koenig et al. [111]	Privacy, Anonymity	Threshold Blind Signature	Multi-authority election scheme	May be prone to denial of service attacks and anonymity problems [112]
Zhang et al. [113]	Correctness	Identity-Based Blind Signature	Combine identity-based cryptography with a blind signature	High computational cost to manage certificates [114]
Kucharczyk [115]	Vote Secrecy, Anonymity	RSA Blind Signature	Enhance the anonymity of voter and system authorisation	Easy to create proof of vote and vote selling [115]
Mohanty and Majhi [116]	Privacy, Anonymity, Unlinkability, Unicity, Coercion-Resistance, Verifiability	Blind signature	Multi-authority election scheme	
Buccafurri et al. [117]	Robustness, Unicity, Scalability, Secrecy, Verifiability	Digital Signature, Blind and Partially Blind Signature	Lightweight e-voting scheme that relies on the existing social networks	
Song and Cui [118]	Completeness, Accuracy, Unreusability, Robustness, Verifiability	ElGamal Blind Signature	Combine ElGamal blind signature and XML	
Nguyen and Dang [52]	Privacy, Unicity, Eligibility, Receipt-Freeness, Coercion-Resistance, Fairness, Accuracy, Individual Verifiability, Universal Verifiability	RSA Blind Signature, ElGamal Encryption, PET	Allow more powerful adversaries to collude in the proposed scheme	
López-García et al. [119]	Privacy, Eligibility, Unicity, Coercion-Resistance, Receipt-Freeness, Accuracy, Verifiability	Elliptic Curves, Bilinear Pairings, Short Signature, Blind Signature	Introduce pairing-based blind signature	Security assumption relies on the existence of an honest third party [91]
Chen et al. [120]	Vote Secrecy, Fairness, Anonymity, Coercion-Resistance, Verifiability	Secret Sharing Scheme, ElGamal Blind Signature	Combine a secret sharing scheme and ElGamal blind signature	
Zhang et al. [9]	Privacy, Anonymity, Unicity, Accuracy, Fairness, Verifiability	Blind Signature	Integrate blind signature-based e-voting with a Kerberos authentication mechanism	Collusion of multiple servers and vulnerable to denial of service attacks are suffered by this scheme [9] and high computational cost to manage certificates [114]
Garciía [121]	Privacy, Eligibility, Dispute-Freeness, Fairness, Coercion-Resistance, Scalability, Robustness, Verifiability	RSA Blind Signature	Coercion-resistant e-voting that can also be used as debate tools	

Table 4. *Cont.*

Scheme	Security Properties	Cryptographic Tools	Distinctive Features	Weaknesses
Darwish and Gendy [106]	Privacy, Robustness, Receipt-Freeness, Correctness, Fairness, Coercion-Resistance, Verifiability	Public Key Infrastructure (PKI), RSA Public Key Encryption, RSA Blind Signature	Combine blind signature-based e-voting with a bit commitment scheme	
Kumar et al. [114]	Completeness, Secure Against Replay Attack	Elliptic Curve, Bilinear Pairing, Blind Signature, Identity-Based Signature, Short Signature	Combine a blind signature scheme with identity-based cryptosystem and short signature scheme	Not suitable for large-scale elections due to the key escrow problem in the identity-based blind signature scheme [99]
Kumar et al. [122]	Completeness	Elliptic Curve, Bilinear Pairing, Blind Signature, Identity-Based Signature, Short Signature	Combine [123] the blind signature scheme, [124] identity-based signature, and [125] short signature	
Aziz [126]	Privacy, Vote Secrecy, Receipt-Freeness, Coercion-Resistance, Accountability, Individual Verifiability, Universal Verifiability	RSA Blind Signature, Mix-Net	The voter is not required to sign on anything and not required to generate any key	The scheme is assumed to be secure if the registrar is not corrupted and the scheme does not satisfy individual verifiability [126]
Kumar et al. [99]	Anonymity, Integrity, Coercion-Resistance, Unicity, Individual Verifiability, Universal Verifiability	Identity-Based Blind Signature, Short Signature	Employ identity-based blind signature and a short signature scheme	
Waheed et al. [127]	Integrity, Authentication, Unlinkability	Blind Signcryption, Elliptic Curve Cryptosystem (ECC)	Small key size, low computational and communication costs	

Okamoto [105] improved the proposed scheme of Okamoto [104] as [104] did not provide a formal definition and formal proof for receipt-freeness. Although Benaloh and Tuinstra [73]'s scheme defined the formal definition of receipt-freeness, it did not fit in the Okamoto [104] proposed scheme.

Ohkubo et al. [103] improved the blind signature-based e-voting scheme of Fujioka et al. [97]. In the Fujioka et al. [97] scheme, the voter is required to join the election from the registration phase to the counting phase. Ohkubo et al. [103] enhanced the convenience of voters so that voters could leave the election once they cast their votes.

Xia and Schneider [8] claimed that the non-transferable proof employed in the schemes proposed by Hirt and Sako [75], Magkos et al. [79], Lee and Kim [76] and Lee et al. [7] only verified the ballot recording process, but not the ballot counting process. Xia and Schneider [8] introduced the security properties of individual verifiability and the secret ballot technique introduced by Chaum et al. [41] to the proposed scheme of Okamoto [104] to allow the voter to verify both the ballot recording process and ballot counting process with the receipt-freeness property by employing a two-way untappable channel assumption between administrator and voters and the one-way untappable channel between the voter and counter.

Cetinkaya and Levent Koc [110] overcame the privacy issue in DynaVote proposed by Cetinkaya and Doganaksoy [42]. Cetinkaya and Levent Koc [110] introduced the collector authority to minimise the power of the counter. Secondly, Cetinkaya and Levent Koc [110] replaced DateTime in the originally proposed scheme to sequence numbers to ease and enhance the efficiency of the recast process in the counting phase.

Nguyen and Dang [52] claimed that the schemes proposed by Juels et al. [43], Cetinkaya and Doganaksoy [42] and Spycher et al. [44] did not fulfil coercion-resistance. The adversaries can collude with the voter and voting authorities to learn how the voter votes and if the voter follows their instructions in the Cetinkaya and Doganaksoy [42] scheme, while the adversaries can communicate with the registrars in the schemes of Juels et al. [43] and

Spycher et al. [44]. Furthermore, the [105] scheme implemented an untappable channel as the physical assumptions are impractical to implement over the Internet. Nguyen and Dang [52] proposed a system that overcame the drawbacks mentioned above and could defect powerful adversaries that colluded with voting authorities and the protocol claimed to be faster and more efficient.

Kumar et al. [99] extended Kumar et al. [114]'s scheme to ensure anonymity of the voter and enhanced the functional variant of the digital signature. In Kumar et al. [114]'s scheme, the identity-based blind signature scheme inherits the key escrow problem and is not suitable for large scale networks. Kumar et al. [99] adopted the short signature scheme proposed by Boneh et al. [125] to fulfil the integrity of votes with a smaller size for the ballot.

4.4. Blockchain-Based e-Voting

4.4.1. Scheme Development

In e-voting, blockchain stores cast ballots [13] where the votes stored in the blockchain cannot be deleted or altered. Blockchain is immutable as each block consists of a previous block hash, thus all blocks are linked. However, blockchain-based e-voting is immature as it has not been fully implemented in a large-scale election [128]. There are also inadequate testing tools to test whether blockchain-based e-voting is superior to current e-voting systems in terms of security, computation, communication, storage, etc.

Liu and Wang [129] stated that some of the proposed schemes involve a trusted third party because it is simple to control and implement in the system, but a powerful trusted third party in the e-voting system might corrupt the system. The integration of e-voting with blockchain technology can be implemented without a trusted third party and guarantees verifiability and anonymity. Furthermore, the blockchain is transparent, thus the entire election process is transparent to the public, and this offers validity and fairness.

However, blockchain-based e-voting introduces additional problems to e-voting systems [130,131]. Despite the fundamental security issues of elections that can be solved by introducing blockchain technology into voting systems, this also imposes new difficulties on the system. The decentralised nature of blockchain significantly increases the complexity of the system [130]. This leads to difficulties in managing the system, and more time is required to resolve or deploy the security fixes in a decentralised system. Ballots stored in a blockchain are difficult to verify and require software for the verification process. Verifiability can be deceived if the software is compromised. Thus, software independence is difficult to achieve if ballots are stored in the blockchain [131].

Furthermore, the immutability of blockchains is a significant challenge to the integrity of voting systems. In a scenario such as the alteration of a voter's vote before reaching the blockchain, the voter is unaware of this alteration, which causes an incorrect tally result in the voting system [131].

In addition, a permissioned blockchain does not satisfy the verifiability requirements of e-voting. Voters cannot read or verify whether their votes are included in the final tally. Moreover, there are key management issues in a permissioned blockchain [130].

For example, Voatz is a blockchain-based mobile voting application deployed in West Virginia to allow the overseas military to vote in US midterm elections in 2018 [132,133]. The system has serious vulnerabilities that allow the adversary to monitor the vote casting process and modify or stop ballots on a large scale without the awareness of election authorities and voters.

Therefore, the suitability of employing blockchain in current e-voting systems requires extensive study to propose a secure and efficient blockchain-based e-voting scheme.

4.4.2. Comparison Analysis

Table 5 shows the detailed comparison of blockchain-based e-voting schemes since 2017.

Table 5. Comparison of blockchain-based e-voting schemes.

Scheme	Security Properties	Cryptographic Tools	Type of Blockchain	Platform	Distinctive Features	Weaknesses
McCorry et al. [134]	Privacy, Dispute-Freeness	Smart Contract	Ethereum test network	Ethereum Blockchain	Decentralised, self-tallying, do not rely on any trusted authority	
Liu and Wang [129]	Universal Verifiability, Individual Verifiability, Anonymity, Transparency	Blind Signature	Can deploy in both public and permissioned blockchains	Not provided	The proposed scheme can be integrated with either a public blockchain or permissioned blockchain	The scheme is assumed to be secure if the inspector and organiser are honest and privacy of voters may disclose via IP address [129]
Cruz and Kaji [112]	Completeness, Robustness, Anonymity, Soundness, Privacy, Unreusability, Fairness, Eligibility, Individual Verifiability, Universal Verifiability	Blind Signature	Public blockchain	Bitcoin Blockchain	Prepaid bitcoin card for voter registration	The scheme is impractical if there is large a number of voters due to the distribution of Prepaid Bitcoin cards (PBCs) [112]
Gong et al. [135]	Eligibility, Anonymity, Verifiability, Fairness	Threshold Blind Signature, Threshold ElGamal Decryption	Public blockchain	Not provided	Employ distributed authority	
Gao et al. [136]	Anonymity, Unicity, Fairness, Verifiability, secure against quantum attack	Public Key Encryption Based on Coding Theory, Ring Signature	Permissioned blockchain	Not provided	The scheme can resist quantum attacks	Less efficient if there is a large number of voters [136]
Chaieb and Yousfi [137]	Eligibility, Completeness, Soundness, Robustness, Fairness, Integrity, Privacy, Universal Verifiability, Receipt-Freeness, Coercion-Resistance	ElGamal Encryption, Short Group Signature Scheme, Mix-Net	Public blockchain	Not provided	End-to-end verifiable large-scale elections with linear complexity in the vote tallying process (LOKI Vote)	
Zhou et al. [138]	Eligibility, Privacy, Fairness, Unicity, Receipt-Freeness, Individual Verifiability, Universal Verifiability, Coercion-Resistance	Blind Signature, Bit Commitment, Smart Contract	Permissioned blockchain	Hyperledger Fabric	Implement smart contract instead of trusted third party	
Priya and Rupa [139]	Privacy	Smart Contract	Public blockchain	Ethereum Blockchain	Implement a smart contract instead of a trusted third party	
Zaghloul et al. [140]	Double-Voting Prevention, Anonymity, Unlinkability, Coercion-Resistance	Digital Signature, Smart Contract	Public blockchain	Not provided	This scheme can be implemented in IoT devices and can support large-scale elections	
Kim et al. [141]	Verifiability, Integrity, Transparency	Ring Signature, Homomorphic Encryption	Permissioned blockchain	Hyperledger Fabric	Support large-scale elections	
Lu et al. [142]	Verifiability, Robustness, Anonymity, Fairness, Receipt-Freeness	Mix-Net, Public Key Encryption, Joint Shamir Random Secret Sharing	Public blockchain	Bitcoin Blockchain	Integrate mix-net in blockchain e-voting to ensure strong anonymity (BEvote)	

Table 5. *Cont.*

Scheme	Security Properties	Cryptographic Tools	Type of Blockchain	Platform	Distinctive Features	Weaknesses
Ye et al. [143]	Coercion-Resistance, Correctness, Privacy, Verifiability, Fairness, Eligibility	Smart Contract, Modified ElGamal Encryption	Not provided	Not provided	Coercion-resistant e-voting secure under DDH assumption	Better efficiency in small-scale elections [143]
Rathore and Ranga [144]	Authentication, Anonymity, Unicity	Smart Contract, Elliptic Curve Cryptography	Permissioned blockchain	Ethereum Blockchain	Remote e-voting scheme that can be integrated with any existing system	
Hassan et al. [145]	Anonymity	Smart Contract	Permissioned blockchain	Hyperledger Fabric	Lowers the cost of conducting nationwide elections	
ElSheikh and Youssef [146]	Completeness, Soundness, Dispute-Freeness	Smart Contract	Not provided	Ethereum Blockchain	Higher scalability by preforming all the heavy computations off-chain	

Self-tallying and decentralised blockchain-based e-voting was first proposed by McCorry et al. [134] using smart contracts in Ethereum. The proposed scheme did not involve a trusted third party in the tally phase to maximise the privacy of voters.

Srivastava et al. [147,148] proposed a model that can be integrated into any e-voting approach using PHANTOM, which is a blockchain protocol proven to be secure under any throughput that the network can support and secure against dishonest blocks. PHANTOM uses a directed acyclic graph of blocks that is suitable for large and fast blocks. Thus, the number of voters can be in millions. However, the proposed model is encouraged to be implemented in voting booths rather than in IoT devices to avoid malware and virus attacks.

The Chaieb and Yousfi [137] scheme was constructed based on the Araujo and Traore [149] scheme inspired by the Juels et al. [43]'s scheme. Both the schemes of Juels et al. [43] and Araujo and Traore [149] are mix-net based. Chaieb and Yousfi [137] combined the Araujo and Traore [149] scheme with blockchain technology.

Zhou et al. [138] improved the Fujioka et al. [97] blind signature-based e-voting scheme using blockchain technology and replaced the trusted third party with a smart contract. The proposed scheme is more practical and versatile and minimises the trust assumptions.

4.5. Post-Quantum e-Voting

4.5.1. Scheme Development

The implementation of post-quantum cryptography in e-voting schemes is a new research direction and few have implemented it in e-voting. Fully homomorphic encryption and lattice-based cryptography are common tools used to construct a post-quantum e-voting system. Post-quantum cryptography is based on different hardness assumptions, e.g., multivariate linear equations and lattices [12].

The security of schemes based on computational complexity/classical assumptions is not secure in terms of quantum attacks owing to the advancement of quantum computers on the horizon [150]. Example of computational hardness is the discrete logarithm problem, factoring problem, Diffie–Hellman problem, elliptic curve discrete logarithm problem, etc.

4.5.2. Comparison Analysis

Table 6 shows the detailed comparison of post-quantum e-voting schemes since 2016.

Table 6. Comparison of post-quantum e-voting schemes.

Scheme	Security Properties	Cryptographic Tools	Distinctive Features	Weaknesses
Chillotti et al. [151]	Privacy, Verifiability, Correctness	Existentially Unforgeable Signatures, Non-Malleable Encryption, LWE-based Homomorphic Encryption, Trapdoors for Lattices	Employ fully homomorphic encryption scheme in Helios	The security of the scheme relied on the honest bulletin board [151]
Aziz et al. [152]	Privacy, Eligibility, Accuracy, Fairness, Receipt-Freeness, Coercion-Resistance, Dispute-Freeness, Robustness, Scalability, Verifiability	Fully Homomorphic Encryption	Fully homomorphic encryption based on cloud services	The public key size and vote size can be decreased [152]
Pinilla [29]	Not provided	Lattice-based	First shuffling proof for lattice-based mix-net based on the intractability of the following lattice-problem: Inhomogeneous Short Integer Solution (ISIS) and Ring Learning With Errors (RLWE)	
Dong and Yang [12]	Completeness, Privacy, Robustness, Unreusability, Verifiability, Eligibility, Fairness	Encrypted No-Key (ENK) Protocol, Message Authentication Code (MAC)	e-Voting scheme based on post-quantum security and physical laws	
Ronne et al. [153]	Not provided	Fully Homomorphic Encryption	Enhances Juels et al.'s (2005) e-voting scheme to be quantum safe	No formal security proof to prove if the scheme is secure against classical adversary [153]
Boyen et al. [154]	Privacy, Accountability, Verifiability	IND-CCA2-Secure Threshold Public Key Encryption	First practical, verifiable lattice-based decryption mix-net based e-voting	
Liao [155]	Anonymity, Unicity, Completeness, Universal Verifiability	Elliptic Curve Digital Signature, Identity Based Fully Homomorphic Encryption	Multi-candidate e-voting	High time complexity of asymmetric encryption [155]
Feng et al. [156]	Anonymity, Completeness, Universal Verifiability	Traceable Ring Signature, Lattice-based	Employ efficient traceable ring signature from lattices that secure in quantum random oracle model	
Farzaliyev et al. [157]	Completeness, Soundness, Privacy	Mix-Net, Ring-LWE Encryption	Design quantum-resistant mix-net for large-scale e-voting that can support 100,000 votes	
Kaim et al. [158]	Correctness, Verifiability, Anonymity	Lattice-based, Threshold Version of Blind Signature	Support multi-candidates and complex ballots structure	

Gentry [67] proposed the first fully homomorphic encryption method based on lattice-based cryptography. Chillotti et al. [151] first combined the LWE fully homomorphic encryption scheme with Helios. Helios is a homomorphic e-voting system. The proposed scheme does not require intensive zero knowledge proof to prove that the voter's vote is valid and the decryption of result is correct.

Dong and Yang [12] proposed an e-voting scheme based on post-quantum security and physical laws that fulfil the following security properties: completeness, privacy, robustness, unreusability, verifiability, eligibility and fairness. The proposed scheme employs a encrypted no-key (ENK) protocol and message authentication code (MAC). The function of the ENK protocol is to transmit the message in the channel that cannot be attacked by ion-trap quantum computing and the MAC ensures that the message cannot be tampered with by any part.

Rønne et al. [153] introduced a fully homomorphic encryption scheme in the tallying phase of Juels et al. [43]'s e-voting scheme in linear time to enhance the scheme to be quantum resistant.

Kaim et al. [158] improved Fujioka et al. [97]'s scheme by introducing threshold version of the blind signature scheme that can resist quantum attacks and the voter "Vote and Go" concept. The proposed scheme does not implement the intensive zero-knowledge proof.

4.6. Hybrid e-Voting

4.6.1. Scheme Development

The hybrid e-voting system combines the advantages of both underlying schemes and building blocks to form an efficient e-voting system. A hybrid e-voting scheme that combines mix-net based e-voting and homomorphic e-voting enjoys the advantages of a homomorphic e-voting scheme that has a simple tallying process along with the advantage of mix-net based e-voting that does not require vote validity checking and supports complex elections.

A hybrid e-voting scheme that combines homomorphic e-voting and blind signature-based e-voting enjoys the advantage of additive homomorphic property, and the election result is able to tally without performing decryption on the ballots. While the RSA blind signature blinds the identity of the voter and their votes, anonymity is achieved.

According to Lee et al. [7], there is no combination of mix-net based e-voting and blind signature-based e-voting because a blind signature-based e-voting scheme employs an anonymous channel that is implemented using mix-net and a secure mix-net does not need a blind signature.

4.6.2. Comparison Analysis

Table 7 shows the detailed comparison of hybrid e-voting schemes since 2004.

Table 7. Comparison of hybrid e-voting schemes.

Scheme	Security Properties	Cryptographic Tools	Hybrid Combination	Distinctive Features	Weaknesses
Kiayias and Yung [159]	Robustness, Fairness, Universal Verifiability	Threshold Homomorphic Encryption and Capacity Assumption	Mix-net + homomorphic	Accept write-in ballots	Required more work and time as the voters have to prove the consistency of vector ballots [159]
Aditya [160]	Privacy, Anonymity, Unlinkability	Threshold ElGamal Encryption	Multiplicative homomorphism + mix-net	Flexible ballot structure	
Peng [161]	Privacy, Soundness	ElGamal Encryption	Shuffling technique + multiplicative homomorphic tallying	Support complex election, efficient key generation distribution	Receipt-freeness does not focus in this paper [161]
Peng and Bao [66]	Privacy	ElGamal Encryption with Distributed Decryption, Fujisaki–Okamoto commitment algorithm	Shuffling technique + multiplicative homomorphic scheme	Simple vote format, efficient vote validity check	Receipt-freeness and coercion-resistance were not the focus of this paper [66]
Hussien and Aboelnaga [162]	Eligibility, Secrecy, Unicity, Privacy, Accuracy	Paillier Encryption, RSA Blind Signature	Homomorphic + blind signature	The proposed scheme is deployed in the voting machine in the poll station	
Mateu et al. [163]	Privacy, Fairness, Unicity, Authentication, Verifiability	Elliptic ElGamal Encryption	Mix-net + homomorphic e-voting	Combine zero knowledge proof for mixing and homomorphic tallying	

Aditya [160] combined the vector ballot approach proposed by Kiayias and Yung [159] with multiplicative homomorphic encryption and mix-net to form a hybrid scheme. The proposed scheme accepts write-in ballots.

Peng and Bao [66] claimed that the multiplicative homomorphic e-voting scheme proposed by Peng et al. [69] has weak privacy and is inefficient due to the vote validity checking and overflow of product of votes in the multiplicative modulus, which leads to the failure of factorising process. Invalid votes must be detected and removed before the tallying process to ensure the correctness of the election results. However, vote validity checking is performed using a zero knowledge proof, which is costly. Peng and Bao [66] improved Peng et al. [69]'s scheme by designing a mechanism for vote validity checking represented in prime integers. The second improvement employed a mechanism for vote grouping to solve the overflow of product of votes and to enhance the privacy of the groups by shuffling the groups. Receipt-freeness and coercion-resistance were not the focus of the proposed scheme.

5. Practical Considerations in e-Voting

According to the technical report presented by National Academies of Sciences, Engineering, and Medicine in 2018 [131], e-voting is a cybersecurity issue that has many factors to be considered before it can be implemented in real-world applications. Cybersecurity is a continuous challenge because adversaries constantly implement new techniques to breach system defences. e-Voting systems connected to the Internet are the most vulnerable to attack via wireless or physical access and during data transmission. All e-voting schemes, including voting at polling stations and remote e-voting, are vulnerable to the following attacks.

- Denial-of-service (DoS) attacks. The main goal of DoS attacks is to slow down computer systems and to the extent that it affects the casting of votes, tallying of votes, and the auditing process.
- Malware attacks. Malicious software that can disrupt the casting of votes and the auditing process, and alter or destroy stored ballots.
- Malicious individuals or servers break into the system to retrieve administrator-level sensitive data such as voters' credentials.

The following are some of the factors that affect an adversary's ability to breach the system.

- If the system is designed properly.
- If the system is configured and updated accordingly.
- If the system is operated and managed accordingly.
- Resources and skills of potential attackers.

We do not have the technology to offer a secure method to support e-voting at present. The Internet is unsuitable for transmitting ballots, and currently, there is no realistic mechanism to fully secure the casting of votes and tabulation of election results from cyberattacks. In addition, there are no technical mechanisms to guarantee that a computer system can generate accurate results, and each layer of the computer system is not modified. Furthermore, e-voting schemes that deploy emails are more vulnerable than other forms of e-voting because the emails do not utilise a secure channel. Moreover, not all vendors follow the best practices in developing, maintaining, and operating e-voting systems. Therefore, to achieve strong defenses against cyber threats, it is necessary to deploy state-of-the-art technologies and practices and expand new cybersecurity knowledge.

6. Potential Research Directions

Many current studies rely on strong assumptions, such as perfect random oracles, honest registrars, and honest bulletin boards. Most of the schemes suffer from high computational costs, thus it is desirable to consider developing more lightweight systems that can still satisfy the necessary security properties.

Post-quantum e-voting is still in its initial stages and has not been fully developed. Further research is expected to improve the current results and implement it in a fully practical scenario. Post-quantum e-voting has drawn great attention in recent years to design a system that can resist quantum adversaries. Chillotti et al. [151] first proposed an LWE-based e-voting scheme. The bulletin board in the proposed scheme has an additional function that is required to check whether the ballot is generated correctly before the ballot is cast with an additional secret key. Their proposed scheme relies on the honest bulletin board, which leads to an open problem if the proposed scheme is secure against dishonest bulletin boards and can be improved to be more practical. The scheme proposed by Dong and Yang [12] can be further extended to explore whether the proposed e-voting scheme is secure in quantum computing environments, such as cavity quantum electrodynamics. Rønne et al. [153] employed a fully homomorphic encryption scheme in linear time in the Juels et al. [43]'s coercion-resistance e-voting scheme. The proposed scheme was not supported by a formal security proof to prove that the modified Juels et al. [43] scheme can be secure against classical adversaries.

Meanwhile, further research is expected to analyse, study, and improve the scalability of blockchain-based e-voting systems, such as the implementation of blockchain-based e-voting in large-scale elections, as the current blockchain-based e-voting systems are only implemented in boardroom and small organisation elections [128]. Further research is also expected to improve the computational cost, reduce delays, and high bandwidth. According to Liu and Wang [129], the coercion-resistance property is difficult to fulfill owing to the transparency property of the blockchain. Thus, future research could be carried out to balance the properties of transparency and coercion-resistance.

Additionally, it would be interesting to study blockchain-based e-voting using post-quantum algorithms that can resist quantum attacks [136,164]. According to Fernández-Caramés and Fraga-Lamas [165], the challenges of post-quantum blockchain include the key size required for post-quantum cryptosystems which is larger than that required for public-key cryptosystems, typically between 128 and 4096 bits. Moreover, some post-quantum schemes restrict the number of messages that can be signed by using a single key for security reasons. Consequently, continuous generation of new keys is required, which leads to high computational resource consumption and slacking of certain blockchain processes.Therefore, further research is required to balance the efficiency of blockchain and key generation and key size issues. Esgin et al. [164] suggested that their proposed post-quantum blockchain scheme can be implemented in privacy preserving applications such as e-voting systems. Gao et al. [136] constructed their scheme with code-based cryptography proposed by McEliece [166], which has not been broken so far, to be secure against quantum attacks.

From the latest works on various e-voting schemes, we observed that the current research trend for e-voting schemes has been diverted towards blockchain technology and post-quantum cryptography. In mix-net-based e-voting, Pinilla [29], Boyen et al. [154], Rønne et al. [153] migrated mix-net-based e-voting to post-quantum cryptography. On the other hand, Gong et al. [135] and Chaieb and Yousfi [137] integrated mix-net with blockchain technology. In homomorphic e-voting, recent studies on post-quantum homomorphic e-voting schemes have been conducted by Aziz et al. [152] and Liao [155]. Some studies have proposed homomorphic e-voting with lattice-based cryptography and fully homomorphic encryption because fully homomorphic encryption and lattice-based cryptography are new research directions. In blind signature-based e-voting, recent studies by Liu and Wang [129], Cruz and Kaji [112], and Zhou et al. [138] integrated blind signature-based e-voting with blockchain technology. Kaim et al. [158] proposed a blind signature-based e-voting scheme that can resist quantum attacks.

It is also interesting to find out the possibility of performing generic transformation from e-voting to e-cash and e-voting to e-cheque, as conjectured by Kho and Heng [167]. They showed that e-cash and e-cheque have high similarities with e-voting in terms of their structure and security properties.

7. Conclusions

We performed a comprehensive comparison analysis between the various e-voting approaches, namely, mix-net based e-voting, homomorphic e-voting, blind signature-based e-voting, blockchain-based e-voting, post-quantum e-voting, and hybrid e-voting. The development of the respective approaches was reviewed, and a detailed comparison was conducted on the specific schemes in each approach. We also discussed some practical considerations in the design of e-voting systems. Finally, we outlined some potential research directions based on our observations.

Author Contributions: Conceptualization, Y.-X.K., S.-H.H. and J.-J.C.; methodology, Y.-X.K., S.-H.H. and J.-J.C.; validation, Y.-X.K., S.-H.H. and J.-J.C.; resources, Y.-X.K., S.-H.H. and J.-J.C.; writing—original draft preparation, Y.-X.K.; writing—review and editing, Y.-X.K., S.-H.H. and J.-J.C.; visualization, Y.-X.K., S.-H.H. and J.-J.C.; supervision, S.-H.H. and J.-J.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Ministry of Higher Education of Malaysia's Fundamental Research Grant Scheme (FRGS/1/2018/ICT04/MMU/01/01).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kiayias, A.; Yung, M. Self-Tallying Elections And Perfect Ballot Secrecy. In *Public Key Cryptography*; Lecture Notes in Computer Science; Naccache, D., Paillier, P., Eds.; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2274, pp. 141–158. [CrossRef]
2. Peng, K. An Efficient Shuffling Based eVoting Scheme. *J. Syst. Softw.* **2011**, *84*, 906–922. [CrossRef]
3. Oo, H.N.; Aung, A. A Survey Of Different Electronic Voting Systems. *Int. J. Sci. Eng. Res.* **2014**, *3*, 3460–3464.
4. Sebé, F.; Miret, J.M.; Pujolàs, J.; Puiggalí, J. Simple And Efficient Hash-Based Verifiable Mixing For Remote Electronic Voting. *Comput. Commun.* **2010**, *33*, 667–675. [CrossRef]
5. Li, H.; Kankanala, A.R.; Zou, X. A Taxonomy And Comparison Of Remote Voting Schemes. In Proceedings of the 2014 23rd International Conference on Computer Communication and Networks (ICCCN), Shanghai, China, 4–7 August 2014; pp. 1–8. [CrossRef]
6. OASIS (Organization for the Advancement of Structured Information Standards);Office of the e-Envoy. Election Markup Language (EML) Process and Data Requirements 4.0a. 2013. Available online: https://www.oasis-open.org/standards (accessed on 12 December 2020)
7. Lee, B.; Boyd, C.; Dawson, E.; Kim, K.; Yang, J.; Yoo, S. Providing Receipt-Freeness In Mixnet-Based Voting Protocols. In *Information Security and Cryptology. ICISC 2003*; Lecture Notes in Computer Science; Lim, J.I., Lee, D.H., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 2971, pp. 245–258. [CrossRef]
8. Xia, Z.; Schneider, S. A New Receipt-Free E-Voting Scheme Based On Blind Signature (Abstract). *WOTE* **2006**, *6*, 127–135.
9. Zhang, H.; You, Q.; Zhang, J. A Lightweight Electronic Voting Scheme Based On Blind Signature And Kerberos Mechanism. In Proceedings of the 2015 IEEE 5th International Conference on Electronics Information and Emergency Communication, Beijing, China, 14–16 May 2015; pp. 210–214. [CrossRef]
10. Bibiloni, P.; Escala, A.; Morillo, P. Vote Validatability in Mix-Net-Based eVoting. In *E-Voting and Identity. Vote-ID 2015*; Lecture Notes in Computer Science; Haenni, R., Koenig, R.E., Wikström, D., Eds.; Springer International Publishing: Cham, Switzerland, 2015; Volume 9269, pp. 92–109. [CrossRef]
11. AboSamra, K.M.; AbdelHafez, A.A.; Assassa, G.M.; Mursi, M.F. A Practical, Secure, and Auditable e-Voting System. *J. Inf. Secur. Appl.* **2017**, *36*, 69–89. [CrossRef]
12. Dong, H.; Yang, L. A Voting Scheme with Post-Quantum Security Based on Physical Laws. *arXiv* **2018**, arXiv:1805.12480.
13. Hardwick, F.S.; Gioulis, A.; Akram, R.N.; Markantonakis, K. E-Voting With Blockchain: An E-Voting Protocol with Decentralisation And Voter Privacy. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Communications in Computer and Information Science. Halifax, NS, Canada, 30 July–3 August 2018; pp. 1561–1567. [CrossRef]
14. Çabuk, U.; Adiguzel, E.; Karaarslan, E. A Survey On Feasibility And Suitability of Blockchain Techniques for the E-Voting Systems. *Int. J. Adv. Res. Comput. Commun. Eng. (IJARCCE)* **2018**, *7*, 124–134. [CrossRef]
15. Chow, S.; Liu, J.; Wong, D. Robust Receipt-Free Election System With Ballot Secrecy And Verifiability. In Proceedings of the Network and Distributed System Security Symposium, NDSS 2008, San Diego, CA, USA, 10–13 February 2008; The Internet Society: San Diego, CA, USA, 2008; Volume 8, pp. 81–94.
16. Liaw, H.T. A Secure Electronic Voting Protocol For General Elections. *Comput. Secur.* **2004**, *23*, 107–119. [CrossRef]
17. Shirazi, F.; Neumann, S.; Ciolacu, I.; Volkamer, M. Robust Electronic Voting: Introducing Robustness In Civitas. In Proceedings of the 2011 International Workshop on Requirements Engineering for Electronic Voting Systems, Trento, Italy, 29 August 2011; pp. 47–55. [CrossRef]

18. Ikonomopoulos, S.; Lambrinoudakis, C.; Gritzalis, D.; Kokolakis, S.; Vassiliou, K. Functional requirements for a secure electronic voting system. In *Security in the Information Society*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 507–519.
19. Sako, K.; Kilian, J. Receipt-Free Mix-Type Voting Scheme. In *Advances in Cryptology—EUROCRYPT '95*; Lecture Notes in Computer Science; Guillou, L.C., Quisquater, J.J., Eds.; Springer: Berlin/Heidelberg, Germany, 1995; Volume 921, pp. 393–403. [CrossRef]
20. Cramer, R.; Franklin, M.; Schoenmakers, B.; Yung, M. Multi-Authority Secret-Ballot Elections With Linear Work. In *Advances in Cryptology. EUROCRYPT '96*; Lecture Notes in Computer Science; Maurer, U., Ed.; Springer: Berlin/Heidelberg, Germany, 1996; Volume 1070, pp. 72–83. [CrossRef]
21. Chaum, D.L. Untraceable Electronic Mail, Return Addresses, And Digital Pseudonyms. *Commun. ACM* **1981**, *24*, 84–90. [CrossRef]
22. Cramer, R.; Gennaro, R.; Schoenmakers, B. A Secure And Optimally Efficient Multi-Authority Election Scheme. In *Advances in Cryptology. EUROCRYPT '97*; Lecture Notes in Computer Science; Fumy, W., Ed.; Springer: Berlin/Heidelberg, Germany, 1997; Volume 1233, pp. 103–118. [CrossRef]
23. Shamir, A. How To Share A Secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
24. Chor, B.; Goldwasser, S.; Micali, S.; Awerbuch, B. Verifiable Secret Sharing And Achieving Simultaneous Broadcast. In Proceedings of the 26th Symposium on Foundations of Computer Science, Portland, OR, USA, 21–23 October 1985; pp. 335–344.
25. Schoenmakers, B. A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting. In *Advances in Cryptology—CRYPTO' 99*; Wiener, M., Ed.; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1666, pp. 148–164. [CrossRef]
26. Zhang, P.; Yu, J.; Liu, H. A Homomorphic Signcryption Scheme and Its Application In Electronic Voting. *J. Shenzhen Univ. Sci. Eng.* **2011**, *28*, 489–494.
27. Rivest, R.L.; Shamir, A.; Tauman, Y. How To Leak A Secret. In *Advances in Cryptology—ASIACRYPT 2001*; Boyd, C., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2248, pp. 552–565. [CrossRef]
28. Liu, J.K.; Wei, V.K.; Wong, D.S. Linkable Spontaneous Anonymous Group Signature For Ad Hoc Groups. In *Information Security and Privacy*; Wang, H., Pieprzyk, J., Varadharajan, V., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3108, pp. 325–335. [CrossRef]
29. Pinilla, R.M. Fully Post-Quantum Protocols for e-Voting, Coercion Resistant Cast as Intended and Mixing Networks. Ph.D. Thesis, Universitat Politècnica de Catalunya, Barcelona, Spain, 2018.
30. Bernstein, D.J. Introduction to post-quantum cryptography. In *Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 1–14.
31. Jakobsson, M.; Juels, A.; Rivest, R.L. Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking. In Proceedings of the 11th USENIX Security Symposium, Washington, DC, USA, 2 March 2002; USENIX Association: Washington, DC, USA, 2002; pp. 339–353. [CrossRef]
32. Park, C.; Itoh, K.; Kurosawa, K. Efficient Anonymous Channel And All/Nothing Election Scheme. In *Advances in Cryptology. EUROCRYPT '93*; Lecture Notes in Computer Science; Helleseth, T., Ed.; Springer: Berlin/Heidelberg, Germany, 1994; Volume 765, pp. 248–259. [CrossRef]
33. Pfitzmann, B. Breaking An Efficient Anonymous Channel. In *Advances in Cryptology—EUROCRYPT'94*; Lecture Notes in Computer Science; Santis, A.D., Ed.; Springer: Berlin/Heidelberg, Germany, 1995; Volume 950, pp. 332–340. [CrossRef]
34. Michels, M.; Horster, P. Some Remarks On A Receipt-Rree And Universally Verifiable Mix-Type Voting Scheme. In *Advances in Cryptology. ASIACRYPT '96*; Lecture Notes in Computer Science; Kim, K., Matsumoto, T., Eds.; Springer: Berlin/Heidelberg, Germany, 1996; Volume 1163, pp. 125–132. [CrossRef]
35. Abe, M. Universally Verifiable Mix-Net with Verification Work Independent of the Number of Mix-Servers. In *Advances in Cryptology—EUROCRYPT'98*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1998; Volume 1403, pp. 437–447. [CrossRef]
36. Neff, C.A. A Verifiable Secret Shuffle and Its Application to E-Voting. In Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS '01), Philadelphia, PA, USA, 6–8 November 2001; Association for Computing Machinery: New York, NY, USA, 2001; pp. 116–125. [CrossRef]
37. Boneh, D.; Golle, P. Almost Entirely Correct Mixing with Applications to Voting. In Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS '02, Washington, DC, USA, 18–22 November 2002; Kim, K., Ed.; Association for Computing Machinery: New York, NY, USA, 2002; pp. 68–77. [CrossRef]
38. Chaum, D. Secret-Ballot Receipts: True Voter-Verifiable Elections. *IEEE Secur. Priv.* **2004**, *2*, 38–47. [CrossRef]
39. Ryan, P.Y.A. *A Variant of the Chaum Voter-Verifiable Scheme*; Technical Report CS-TR: 864; University of Newcastle upon Tyne: Newcastle upon Tyne, UK, 2004.
40. Aditya, R.; Lee, B.; Boyd, C.; Dawson, E. An Efficient Mixnet-Based Voting Scheme Providing Receipt-Freeness. In *Trust and Privacy in Digital Business. TrustBus 2004*; Lecture Notes in Computer Science; Katsikas, S., Lopez, J., Pernul, G., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3184, pp. 152–161. [CrossRef]
41. Chaum, D.; Ryan, P.Y.A.; Schneider, S. A Practical Voter-Verifiable Election Scheme. In *Computer Security. ESORICS 2005*; Lecture Notes in Computer Science; de Capitani di Vimercati, S., Syverson, P., Gollmann, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3679, pp. 118–139. [CrossRef]

42. Cetinkaya, O.; Doganaksoy, A. A Practical Verifiable e-Voting Protocol for Large Scale Elections over A Network. In Proceedings of the Second International Conference on Availability, Reliability and Security (ARES'07), Vienna, Austria, 10–13 April 2007; pp. 432–442. [CrossRef]
43. Juels, A.; Catalano, D.; Jakobsson, M. Coercion-Resistant Electronic Elections. In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, WPES '05, Alexandria, VA, USA, 7 November 2005; Association for Computing Machinery: New York, NY, USA, 2005; pp. 61–70. [CrossRef]
44. Spycher, O.; Koenig, R.; Haenni, R.; Schläpfer, M. A New Approach towards Coercion-Resistant Remote E-Voting in Linear Time. In *Financial Cryptography and Data Security*; Lecture Notes in Computer Science; Danezis, G., Ed.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7035, pp. 182–189. [CrossRef]
45. Her, Y.S.; Saito, J.; Imamoto, K.; Sakurai, K. Security And Privacy in E-voting and RFID System Based on Universal. In Proceedings of the 2005 Symposium on Cryptography and Information Security, Istanbul, Turkey, 26–28 October 2005; pp. 907–912.
46. Carroll, T.E.; Grosu, D. A Secure And Efficient Voter-Controlled Anonymous Election Scheme. In Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05)—Volume II, Las Vegas, NV, USA, 4–6 April 2005; Volume 1, pp. 721–726. [CrossRef]
47. Zwierko, A.; Kotulski, Z. A Light-Weight e-Voting System With Distributed Trust. *Electron. Notes Theor. Comput. Sci.* **2007**, *168*, 109–126. [CrossRef]
48. Clarkson, M.R.; Chong, S.; Myers, A.C. Civitas: Toward A Secure Voting System. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA, USA, 18–22 May 2008; pp. 354–368. [CrossRef]
49. Furukawa, J.; Mori, K.; Sako, K. An Implementation of a Mix-Net Based Network Voting Scheme and Its Use in A Private Organization. In *Towards Trustworthy Elections: New Directions in Electronic Voting*; Lecture Notes in Computer Science; Chaum, D., Jakobsson, M., Rivest, R.L., Ryan, P.Y.A., Benaloh, J., Kutylowski, M., Adida, B., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6000, pp. 141–154. [CrossRef]
50. Lee, Y.; Park, S.; Mambo, M.; Kim, S.; Won, D. Towards Trustworthy e-Voting Using Paper Receipts. *Comput. Stand. Interfaces* **2010**, *32*, 305–311. [CrossRef]
51. Bulens, P.; Giry, D.; Pereira, O. Running Mixnet-Based Elections With Helios. In *2011 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 11)*; USENIX Association: San Francisco, CA, USA, 2011; Volume 11, p. 6.
52. Nguyen, T.A.T.; Dang, T.K. Enhanced Security In Internet Voting Protocol Using Blind Signature And Dynamic Ballots. *Electron. Commer. Res.* **2013**, *13*, 257–272. [CrossRef]
53. Tamura, S.; Haddad, H.; Islam, N.; Alam, K. An Incoercible E-Voting Scheme Based On Revised Simplified Verifiable Re-encryption Mix-nets. *Inf. Secur. Comput. Fraud* **2015**, *3*, 32–38. [CrossRef]
54. Alam, K.M.R.; Tamura, S.; Rahman, S.M.S.; Morimoto, Y. An Electronic Voting Scheme Based On Revised-SVRM And Confirmation Numbers. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 400–410. [CrossRef]
55. Chang, D.; Chauhan, A.K.; Kang, J. Apollo: End-to-End Verifiable Voting Protocol Using Mixnet and Hidden Tweaks. In *Information Security and Cryptology—ICISC 2015*; Lecture Notes in Computer Science; Kwon, S., Yun, A., Eds.; Springer International Publishing: Cham, Switzerland, 2016; Volume 9558, pp. 194–209. [CrossRef]
56. McMurtry, E.; Boyen, X.; Culnane, C.; Gjøsteen, K.; Haines, T.; Teague, V. Towards Verifiable Remote Voting with Paper Assurance. *arXiv* **2021**, arXiv:2111.04210.
57. Rønne, P.B.; Ryan, P.Y.; Zollinger, M.L. Electryo, in-person voting with transparent voter verifiability and eligibility verifiability. *arXiv* **2021**, arXiv:2105.14783.
58. Tejedor-Romero, M.; Orden, D.; Marsa-Maestre, I.; Junquera-Sanchez, J.; Gimenez-Guzman, J.M. Distributed Remote E-Voting System Based on Shamir's Secret Sharing Scheme. *Electronics* **2021**, *10*, 3075. [CrossRef]
59. Ogata, W.; Kurosawa, K.; Sako, K.; Takatani, K. Fault Tolerant Anonymous Channel. In *Information and Communications Security*; Lecture Notes in Computer Science; Han, Y., Okamoto, T., Qing, S., Eds.; Springer: Berlin/Heidelberg, Germany, 1997; Volume 1334, pp. 440–444. [CrossRef]
60. Golle, P.; Zhong, S.; Boneh, D.; Jakobsson, M.; Juels, A. Optimistic Mixing For Exit-Polls. In *Advances in Cryptology. ASIACRYPT 2002*; Lecture Notes in Computer Science; Zheng, Y., Ed.; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2501, pp. 451–465. [CrossRef]
61. Adida, B. Helios: Web-Based Open-Audit Voting. In Proceedings of the 17th Conference on Security Symposium (SS'08), San Jose, CA, USA, 28 July–1 August 2008; USENIX Association: Washington, DC, USA, 2008; Volume 17, pp. 335–348.
62. Benaloh, J. Simple Verifiable Elections. In Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing, EVT'06, Vancouver, BC, Canada, 1 August 2006; USENIX Association: Washington, DC, USA, 2006; p. 5. [CrossRef]
63. Paillier, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *Advances in Cryptology. EUROCRYPT '99*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1592, pp. 223–238. [CrossRef]
64. Rivest, R.L.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
65. ElGamal, T. A Public Key Cryptosystem And A Signature Scheme Based On Discrete Logarithms. *IEEE Trans. Inf. Theory* **1985**, *31*, 469–472. [CrossRef]

66. Peng, K.; Bao, F. Efficient Multiplicative Homomorphic E-Voting. In *Information Security*; Lecture Notes in Computer Science; Burmester, M., Tsudik, G., Magliveras, S., Ilić, I., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6531, pp. 381–393. [CrossRef]
67. Gentry, C. Fully Homomorphic Encryption Using Ideal Lattices. In Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, STOC '09, Bethesda, MD, USA, 31 May–2 June 2009; Association for Computing Machinery: New York, NY, USA, 2009; pp. 169–178. [CrossRef]
68. Cohen, J.D.; Fischer, M.J. A Robust and Verifiable Cryptographically Secure Election Scheme. In Proceedings of the 26th Annual Symposium on Foundations of Computer Science, SFCS '85, Washington, DC, USA, 21–23 October 1985; pp. 372–382. [CrossRef]
69. Peng, K.; Aditya, R.; Boyd, C.; Dawson, E.; Lee, B. Multiplicative Homomorphic E-Voting. In *Progress in Cryptology–INDOCRYPT 2004*; Lecture Notes in Computer Science; Canteaut, A., Viswanathan, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3348, pp. 61–72. [CrossRef]
70. Benaloh, J.C.; Yung, M. Distributing the Power of a Government to Enhance the Privacy of Voters. In Proceedings of the Fifth Annual ACM Symposium on Principles of Distributed Computing, PODC '86, Calgary, AB, Canada, 11–13 November 1986; Association for Computing Machinery: New York, NY, USA, 1986; pp. 52–62. [CrossRef]
71. Benaloh, J. Verifiable Secret-Ballot Elections. Ph.D. Thesis, Yale University, New Haven, CT, USA, 1987.
72. Sako, K.; Kilian, J. Secure Voting Using Partially Compatible Homomorphisms. In *Advances in Cryptology—CRYPTO '94*; Lecture Notes in Computer Science; Desmedt, Y.G., Ed.; Springer: Berlin/Heidelberg, Germany, 1994; Volume 839, pp. 411–424. [CrossRef]
73. Benaloh, J.; Tuinstra, D. Receipt-Free Secret-Ballot Elections (Extended Abstract). In Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing, STOC '94, Montreal, QC, Canada, 23–25 May 1994; Association for Computing Machinery: New York, NY, USA, 1994; pp. 544–553. [CrossRef]
74. Baudron, O.; Fouque, P.A.; Pointcheval, D.; Stern, J.; Poupard, G. Practical Multi-Candidate Election System. In Proceedings of the Twentieth Annual ACM Symposium on Principles of Distributed Computin, PODC '01, Newport, RI, USA, 26–29 August 2001; Association for Computing Machinery: New York, NY, USA, 2001; pp. 274–283. [CrossRef]
75. Hirt, M.; Sako, K. Efficient Receipt-Free Voting Based on Homomorphic Encryption. In *Advances in Cryptology. EUROCRYPT 2000*; Lecture Notes in Computer Science; Preneel, B., Ed.; Springer: Berlin/Heidelberg, Germany, 2000; Volume 1807, pp. 539–556. [CrossRef]
76. Lee, B.; Kim, K. Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer. In *Information Security and Cryptology. ICISC 2002*; Lecture Notes in Computer Science; Lee, P.J., Lim, C.H., Eds.; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2587, pp. 389–406. [CrossRef]
77. Lee, B.; Kim, K. Receipt-free Electronic Voting through Collaboration of Voter and Honest Verifier. In Proceedings of the JW-ISC2000, Okinawa, Japan 25–26 January 2000; pp. 101–108.
78. Hirt, M. Multi-Party Computation: Efficient Protocols, General Adversaries, and Voting. Ph.D. Thesis, ETH Zurich, Zürich, Switzerland, 2001.
79. Magkos, E.; Burmester, M.; Chrissikopoulos, V. Receipt-freeness in Large-Scale Elections without Untappable Channels. In *Towards the E-Society: E-Commerce, E-Business, and E-Government*; IFIP International Federation for Information Processing; Schmid, B., Stanoevska-Slabeva, K., Tschammer, V., Eds.; Springer: Boston, MA, USA, 2001; Volume 74, pp. 683–693. [CrossRef]
80. Damgård, I.; Jurik, M. A Generalisation, A Simplification and Some Applications of Paillier's Probabilistic Public-Key System. In *Public Key Cryptography. PKC 2001*; Lecture Notes in Computer Science; Kim, K., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 1992, pp. 119–136. [CrossRef]
81. Peng, K. Efficient Proof of Vote Validity without Honest-Verifier Assumption in Homomorphic E-Voting. *J. Inf. Process. Syst.* **2011**, *7*, 549–560. [CrossRef]
82. Katz, J.; Myers, S.; Ostrovsky, R. Cryptographic Counters and Applications to Electronic Voting. In *Advances in Cryptology. EUROCRYPT 2001*; Lecture Notes in Computer Science; Pfitzmann, B., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2045, pp. 78–92. [CrossRef]
83. Peng, K.; Bao, F. Efficient Proof of Validity of Votes in Homomorphic E-Voting. In Proceedings of the 2010 Fourth International Conference on Network and System Security, Melbourne, VIC, Australia, 1–3 September 2010; pp. 17–23. [CrossRef]
84. Peng, K.; Bao, F. Efficient Vote Validity Check in Homomorphic Electronic Voting. In *Information Security and Cryptology—ICISC 2008*; Lecture Notes in Computer Science; Lee, P.J., Cheon, J.H., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5461, pp. 202–217. [CrossRef]
85. Huszti, A. A Homomorphic Encryption-Based Secure Electronic Voting Scheme. *Publ. Math.* **2011**, *79*, 479–496. [CrossRef]
86. Bernhard, D.; Cortier, V.; Pereira, O.; Smyth, B.; Warinschi, B. Adapting Helios For Provable Ballot Privacy. In *Computer Security—ESORICS 2011*; Lecture Notes in Computer Science; Atluri, V., Diaz, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6879, pp. 335–354. [CrossRef]
87. Yi, X.; Okamoto, E. Practical Remote End-to-End Voting Scheme. In *Electronic Government and the Information Systems Perspective*; Lecture Notes in Computer Science; Andersen, K.N., Francesconi, E., Åke, G., van Engers, T.M., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6866, pp. 386–400. [CrossRef]
88. Shinde, S.S.; Shukla, S.; Chitre, D. Secure E-voting Using Homomorphic Technology. *Int. J. Emerg. Technol. Adv. Eng.* **2013**, *3*, 203–206.

89. Àngels Cerveró, M.; Mateu, V.; Miret, J.M.; Sebé, F.; Valera, J. An Efficient Homomorphic E-Voting System over Elliptic Curves. In *Electronic Government and the Information Systems Perspective. EGOVIS 2014*; Lecture Notes in Computer Science; Kő, A., Francesconi, E., Eds.; Springer International Publishing: Cham, Switzerland, 2014; Volume 8650, pp. 41–53. [CrossRef]
90. Kiayias, A.; Zacharias, T.; Zhang, B. An Efficient E2E Verifiable E-voting System without Setup Assumptions. *IEEE Secur. Priv.* **2017**, *15*, 14–23. [CrossRef]
91. Yang, X.; Yi, X.; Nepal, S.; Kelarev, A.; Han, F. A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption. *IEEE Access* **2018**, *6*, 20506–20519. [CrossRef]
92. Fan, X.; Wu, T.; Zheng, Q.; Chen, Y.; Alam, M.; Xiao, X. HSE-Voting: A Secure High-Efficiency Electronic Voting Scheme Based On Homomorphic Signcryption. *Future Gener. Comput. Syst.* **2020**, *111*, 754–762. [CrossRef]
93. Fan, X.; Wu, T.; Zheng, Q.; Chen, Y.; Xiao, X. DHS-Voting: A Distributed Homomorphic Signcryption E-Voting. In *Dependability in Sensor, Cloud, and Big Data Systems and Applications. DependSys 2019*; Communications in Computer and Information Science; Wang, G., Bhuiyan, M.Z.A., di Vimercati, S.D.C., Ren, Y., Eds.; Springer: Singapore, 2019; Volume 1123, pp. 40–53. [CrossRef]
94. Benaloh, J. Electionguard Preliminary Specification v0.85. Available online: https://github.com/microsoft/electionguard (accessed on 24 February 2022).
95. Haines, T.; Goré, R.; Stodart, J. Machine-checking the universal verifiability of ElectionGuard. In Proceedings of the Nordic Conference on Secure IT Systems, Virtual Event, 3 March 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 57–73.
96. Chaum, D. Blind Signatures for Untraceable Payments. In *Advances in Cryptology*; Chaum, D., Rivest, R.L., Sherman, A.T., Eds.; Springer: Boston, MA, USA, 1983; pp. 199–203. [CrossRef]
97. Fujioka, A.; Okamoto, T.; Ohta, K. A Practical Secret Voting Scheme For Large Scale Elections. In *Advances in Cryptology. AUSCRYPT '92*; Lecture Notes in Computer Science; Seberry, J., Zheng, Y., Eds.; Springer: Berlin/Heidelberg, Germany, 1993; Volume 718, pp. 244–251. [CrossRef]
98. Zhang, F.; Kim, K. ID-Based Blind Signature and Ring Signature from Pairings. In *Advances in Cryptology—ASIACRYPT 2002*; Lecture Notes in Computer Science; Zheng, Y., Ed.; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2501, pp. 533–547. [CrossRef]
99. Kumar, M.; Chand, S.; Katti, C.P. A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature. *IEEE Syst. J.* **2020**, *14*, 2032–2041. [CrossRef]
100. Cetinkaya, O.; Doganaksoy, A. A practical privacy preserving e-voting protocol using dynamic ballots. In Proceedings of the 2nd National Cryptology Symposium, Virtual, 11–14 January 2006; Citeseer: Forest Grove, OR, USA, 2006.
101. Adewole, A.P.; Sodiya, A.; Arowolo, O. A receipt-free multi-authority e-voting system. *Int. J. Comput. Appl.* 2011, *30*, 15–23.
102. Schmid, M.; Grünert, A. *Blind Signatures and Blind Signature E-Voting Protocols*; University of Applied Science Biel: Bern, Switzerland 2008.
103. Ohkubo, M.; Miura, F.; Abe, M.; Fujioka, A.; Okamoto, T. An Improvement on a Practical Secret Voting Scheme. In *International Workshop on Information Security*; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1729, pp. 225–234. [CrossRef]
104. Okamoto, T. An Electronic Voting Scheme. In *Advanced IT Tools*; Terashima, N., Altman, E., Eds.; IFIP—The International Federation for Information Processing; Springer: Boston, MA, USA, 1996; pp. 21–30. [CrossRef]
105. Okamoto, T. Receipt-Free Electronic Voting Schemes For Large Scale Elections. In *Security Protocols*; Lecture Notes in Computer Science; Christianson, B., Crispo, B., Lomas, M., Roe, M., Eds.; Springer: Berlin/Heidelberg, Germany, 1998; Volume 1361, pp. 25–35. [CrossRef]
106. Darwish, A.; Gendy, M. A New Cryptographic Voting Verifiable Scheme for E-Voting System Based on Bit Commitment and Blind Signature. *Int. J. Swarm Intell. Evol. Comput.* **2017**, *6*, 2. [CrossRef]
107. Jan, J.K.; Chen, Y.Y.; Lin, Y. The Design of Protocol for e-Voting on the Internet. In Proceedings of the IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No.01CH37186), London, UK, 16–19 October 2001; pp. 180–189. [CrossRef]
108. Magkos, E.; Chrissikopoulos, V. Equitably Fair Internet Voting. *J. Internet Technol.* **2002**, *3*, 187–192.
109. Ibrahim, S.; Kamat, M.; Salleh, M.; Aziz, S. Secure E-voting With Blind Signature. In Proceedings of the 4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings, Shah Alam, Malaysia, 14–15 January 2003; pp. 193–197. [CrossRef]
110. Cetinkaya, O.; Koc, M.L. Practical Aspects of DynaVote e-Voting Protocol. *Electron. J. E-Gov.* **2009**, *7*, 327–338.
111. Koenig, R.; Dubuis, E.; Haenni, R. Why Public Registration Boards Are Required in E-Voting Systems Based on Threshold Blind Signature Protocols. In Proceedings of the Electronic Voting 2010, EVOTE 2010—4th International Conference, Castle Hofen, Bregenz, Austria, 21–24 July 2010; Krimmer, R., Grimm, R., Eds.; pp. 255–266.
112. Cruz, J.P.; Kaji, Y. E-voting System Based on the Bitcoin Protocol and Blind Signatures. *IPSJ Trans. Math. Model. Its Appl.* **2017**, *10*, 14–22.
113. Zhang, L.; Hu, Y.; Tian, X.; Yang, Y. Novel Identity-Based Blind Signature for Electronic Voting System. In Proceedings of the 2010 Second International Workshop on Education Technology and Computer Science, Wuhan, China, 6–7 March 2010; Volume 2, pp. 122–125. [CrossRef]
114. Kumar, M.; Katti, C.P.; Saxena, P.C. A Secure Anonymous E-Voting System Using Identity-Based Blind Signature Scheme. In *Information Systems Security. ICISS 2017*; Lecture Notes in Computer Science; Shyamasundar, R.K., Singh, V.,Vaidya, J., Eds.; Springer International Publishingg: Cham, Switzerland, 2017; Volume 10717, pp. 29–49. [CrossRef]

115. Kucharczyk, M. Blind Signatures in Electronic Voting Systems. In *Computer Networks*; Communications in Computer and Information Science; Kwiecień, A., Gaj, P., Stera, P., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; Volume 79, pp. 349–358. [CrossRef]
116. Mohanty, S.; Majhi, B. A Secure Multi Authority Electronic Voting Protocol Based on Blind Signature. In Proceedings of the 2010 International Conference on Advances in Computer Engineering, Bangalore, India, 20–21 June 2010; pp. 271–273. [CrossRef]
117. Buccafurri, F.; Fotia, L.; Lax, G. Allowing Continuous Evaluation of Citizen Opinions through Social Networks. In *Advancing Democracy, Government and Governance. EGOVIS/EDEM 2012*; Lecture Notes in Computer Science; Kő, A., Leitner, C., Leitold, H., Prosser, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7452, pp. 242–253. [CrossRef]
118. Song, F.; Cui, Z. Electronic Voting Scheme about Elgamal Blind-Signatures Based on XML. *Procedia Eng.* **2012**, *29*, 2721–2725. [CrossRef]
119. López-García, L.; Perez, L.J.D.; Rodríguez-Henríquez, F. A Pairing-Based Blind Signature E-Voting Scheme. *Comput. J.* **2014**, *57*, 1460–1471. [CrossRef]
120. Chen, C.L.; Chen, Y.Y.; Jan, J.K.; Chen, C.C. A Secure Anonymous e-Voting System Based on Discrete Logarithm Problem. *Appl. Math. Inf. Sci.* **2014**, *8*, 2571–2578. [CrossRef]
121. García, D.L. A Flexible e-Voting Scheme For Debate Tools. *Comput. Secur.* **2016**, *56*, 50–62. [CrossRef]
122. Kumar, M.; Katti, C.; Saxena, P. An Identity-Based Blind Signature Approach For E-voting System. *Int. J. Mod. Educ. Comput. Sci.* **2017**, *9*, 47–54. [CrossRef]
123. Boldyreva, A. Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme. In *Public Key Cryptography. PKC 2003*; Lecture Notes in Computer Science; Desmedt, Y.G., Ed.; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2567, pp. 31–46. [CrossRef]
124. Choon, J.C.; Cheon, J.H. An Identity-Based Signature from Gap Diffie-Hellman Groups. In *Public Key Cryptography. PKC 2003*; Lecture Notes in Computer Science; Desmedt, Y.G., Ed.; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2567, pp. 18–30. [CrossRef]
125. Boneh, D.; Lynn, B.; Shacham, H. Short Signatures From The Weil Pairing. In *Advances in Cryptology. ASIACRYPT 2001*; Lecture Notes in Computer Science; Boyd, C., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2248, pp. 514–532. [CrossRef]
126. Aziz, A. Coercion-Resistant E-Voting Scheme with Blind Signatures. In Proceedings of the 2019 Cybersecurity and Cyberforensics Conference (CCC), Melbourne, Australia, 8–9 May 2019; pp. 143–151. [CrossRef]
127. Waheed, A.; Din, D.N.; Umar, A.; Ullah, R.; Amin, U. Novel Blind Signcryption Scheme for E-Voting System Based on Elliptic Curves. *Mehran Univ. Res. J. Eng. Technol.* **2021**, *40*, 314–322. [CrossRef]
128. Jafar, U.; Aziz, M.J.A. A State of the Art Survey and Research Directions on Blockchain Based Electronic Voting System. In *Advances in Cyber Security*; Communications in Computer and Information Science; Anbar, M., Abdullah, N., Manickam, S., Eds.; Springer: Singapore, 2021; Volume 1347, pp. 248–266. [CrossRef]
129. Liu, Y.; Wang, Q. An E-voting Protocol Based On Blockchain. *IACR Cryptol. EPrint Arch.* **2017**, *2017*, 1043.
130. Park, S.; Specter, M.; Narula, N.; Rivest, R.L. Going from bad to worse: From internet voting to blockchain voting. *J. Cybersecur.* **2021**, *7*, 25. [CrossRef]
131. National Academies of Sciences, Engineering, and Medicine. In *Securing the Vote: Protecting American Democracy*; The National Academies Press: Washington, DC, USA, 2018. [CrossRef]
132. West Virginia Secretary of State's Office. 24 Counties to Offer Mobile Voting Option for Military Personnel Overseas. 2018. Available online: https://sos.wv.gov/news/Pages/09-20-2018-A.aspx (accessed on 2 December 2021).
133. West Virginia Secretary of State's Office. Warner Pleased with Participation in Test Pilot for Mobile Voting. 2018. Available online: https://sos.wv.gov/news/Pages/11-16-2018-A.aspx (accessed on 2 December 2021).
134. McCorry, P.; Shahandashti, S.F.; Hao, F. A Smart Contract For Boardroom Voting With Maximum Voter Privacy. In *Financial Cryptography and Data Security*; Kiayias, A., Ed.; Springer International Publishing: Cham, Switzerland, 2017; Volume 10322, pp. 357–375. [CrossRef]
135. Gong, B.; Lu, X.; Fat, L.W.; Au, M.H. Blockchain-Based Threshold Electronic Voting System. In *Security and Privacy in Social Networks and Big Data*; Communications in Computer and Information Science; Meng, W., Furnell, S., Eds.; Springer: Singapore, 2019; Volume 1095, pp. 238–250. [CrossRef]
136. Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C. An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function. *IEEE Access* **2019**, *7*, 115304–115316. [CrossRef]
137. Chaieb, M.; Yousfi, S. LOKI Vote: A Blockchain-Based Coercion Resistant E-Voting Protocol. In *Information Systems. EMCIS 2020*; Lecture Notes in Business Information Processing; Themistocleous, M., Papadaki, M., Kamal, M.M., Eds.; Springer International Publishing: Cham, Switzerland, 2020; Volume 402, pp. 151–168. [CrossRef]
138. Zhou, Y.; Liu, Y.; Jiang, C.; Wang, S. An Improved FOO Voting Scheme Using Blockchain. *Int. J. Inf. Secur.* **2020**, *19*, 303–310. [CrossRef]
139. Priya, K.L.S.; Rupa, C. Block chain technology based electoral franchise. In Proceedings of the 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 5–7 March 2020; pp. 1–5. [CrossRef]
140. Zaghloul, E.; Li, T.; Ren, J. d-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting. *IEEE Internet Things J.* **2021**, *8*, 16585–16597. [CrossRef]

141. Kim, H.; Kim, K.E.; Park, S.; Sohn, J. E-voting System Using Homomorphic Encryption and Blockchain Technology to Encrypt Voter Data. *arXiv* **2021**, arXiv:2111.05096.
142. Lu, N.; Xu, X.; Choi, C.; Fei, T.; Shi, W. BEvote: Bitcoin-Enabled E-Voting Scheme with Anonymity and Robustness. *Secur. Commun. Netw.* **2021**, *2021*. [CrossRef]
143. Ye, K.; Zheng, D.; Guo, R.; He, J.; Chen, Y.; Tao, X. A Coercion-Resistant E-Voting System Based on Blockchain Technology. *Int. J. Netw. Secur.* **2021**, *23*, 791–806.
144. Rathore, D.; Ranga, V. Secure Remote E-Voting using Blockchain. In Proceedings of the 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 6–8 May 2021; pp. 282–287. [CrossRef]
145. ul Hassan, C.A.; Hammad, M.; Iqbal, J.; Hussain, S.; Ullah, S.S.; AlSalman, H.; Mosleh, M.A.; Arif, M. A Liquid Democracy Enabled Blockchain-Based Electronic Voting System. *Sci. Program.* **2022**, *2022*. [CrossRef]
146. ElSheikh, M.; Youssef, A.M. Dispute-free Scalable Open Vote Network using zk-SNARKs. *arXiv* **2022**, arXiv:2203.03363.
147. Srivastava, G.; Dwivedi, A.D.; Singh, R. PHANTOM Protocol as the New Crypto-Democracy. In *Computer Information Systems and Industrial Management*; Saeed, K., Homenda, W., Eds.; Springer International Publishing: Cham, Switzerland, 2018; Volume 11127, pp. 499–509. [CrossRef]
148. Srivastava, G.; Dwivedi, A.D.; Singh, R. Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology. In Proceedings of the ICETE, Hyderabad, India, 22–23 March 2018; pp. 674–679.
149. Araújo, R.; Traoré, J. A Practical Coercion Resistant Voting Scheme Revisited. In *E-Voting and Identify. Vote-ID 2013*; Lecture Notes in Computer Science; Heather, J., Schneider, S., Teague, V., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; Volume 7985, pp. 193–209. [CrossRef]
150. Xu, R.; Huang, L.; Yang, W.; He, L. Quantum Group Blind Signature Scheme Without Entanglement. *Opt. Commun.* **2011**, *284*, 3654–3658. [CrossRef]
151. Chillotti, I.; Gama, N.; Georgieva, M.; Izabachène, M. A Homomorphic LWE Based E-voting Scheme. In *Post-Quantum Cryptography*; Lecture Notes in Computer Science; Takagi, T., Ed.; Springer International Publishing: Cham, Switzerland, 2016; Volume 9606, pp. 245–265. [CrossRef]
152. Aziz, A.; Qunoo, H.; Abusamra, A. Using Homomorphic Cryptographic Solutions on E-voting Systems. *Int. J. Comput. Netw. Inf. Secur.* **2018**, *10*, 44–59. [CrossRef]
153. Rønne, P.B.; Atashpendar, A.; Gjøsteen, K.; Ryan, P.Y.A. Short Paper: Coercion-Resistant Voting in Linear Time Via Fully Homomorphic Encryption. In *Financial Cryptography and Data Security*; Lecture Notes in Computer Science; Bracciali, A., Clark, J., Pintore, F., Rønne, P.B., Sala, M., Eds.; Springer International Publishing: Cham, Switzerland, 2020; Volume 11599, pp. 289–298. [CrossRef]
154. Boyen, X.; Haines, T.; Müller, J. A Verifiable and Practical Lattice-Based Decryption Mix Net with External Auditing. In *Computer Security. ESORICS 2020*; Lecture Notes in Computer Science; Chen, L., Li, N., Liang, K., Schneider, S., Eds.; Springer International Publishing: Cham, Switzerland, 2020; Volume 12309, pp. 336–356. [CrossRef]
155. Liao, G. Multi-Candidate Electronic Voting Scheme Based on Fully Homomorphic Encryption. *J. Phys. Conf. Ser.* **2020**, *1678*, 012064. [CrossRef]
156. Feng, H.; Liu, J.; Wu, Q.; Li, Y.N. Traceable Ring Signatures with Post-quantum Security. In *Topics in Cryptology—CT-RSA 2020*; Jarecki, S., Ed.; Springer International Publishing: Cham, Switzerland, 2020; pp. 442–468.
157. Farzaliyev, V.; Willemson, J.; Kaasik, J.K. Improved Lattice-Based Mix-Nets for Electronic Voting. Cryptol. ePrint Archive, Report 2021/1499. 2021. Available online: https://ia.cr/2021/1499 (accessed on 27 March 2022).
158. Kaim, G.; Canard, S.; Roux-Langlois, A.; Traoré, J. Post-quantum Online Voting Scheme. In *Financial Cryptography and Data Security. FC 2021 International Workshops*; Springer: Berlin/Heidelberg, Germany, 2021; Volume 12676, pp. 290–305. [CrossRef]
159. Kiayias, A.; Yung, M. The Vector-Ballot e-Voting Approach. In *Financial Cryptography*; Lecture Notes in Computer Science; Juels, A., Ed.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3110, pp. 72–89. [CrossRef]
160. Aditya, R. Secure Electronic Voting with Flexible Ballot Structure. Ph.D. Thesis, Information Security Institute, Queensland University of Technology, Brisbane, Australia, 2005.
161. Peng, K. A Hybrid E-Voting Scheme. In *Information Security Practice and Experience*; Lecture Notes in Computer Science; Bao, F., Li, H., Wang, G., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5451, pp. 195–206. [CrossRef]
162. Hussien, H.; Aboelnaga, H. Design of a Secured e-Voting System. In Proceedings of the 2013 International Conference on Computer Applications Technology (ICCAT), Sousse, Tunisia, 20–22 January 2013; pp. 1–5. [CrossRef]
163. Mateu, V.; Miret, J.M.; Sebe, F. A Hybrid Approach To Vector-Based Homomorphic Tallying Remote Voting. *Int. J. Inf. Secur.* **2016**, *15*, 211–221. [CrossRef]
164. Esgin, M.F.; Zhao, R.K.; Steinfel, R.; Liu, J.K.; Liu, D. MatRiCT: Efficient, Scalable And Post-Quantum Blockchain Confidential Transactions Protocol. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS '19, London, UK, 11–15 November 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 567–584. [CrossRef]
165. Fernandez-Carames, T.M.; Fraga-Lamas, P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access* **2020**, *8*, 21091–21116. [CrossRef]
166. McEliece, R.J. A Public-Key Cryptosystem Based On Algebraic. *Coding Thv* **1978**, *4244*, 114–116.
167. Kho, Y.X.; Heng, S.H. Comparison Analysis of Cryptographic Electronic Systems. In Proceedings of the 7th International Cryptology and Information Security Conference 2020, CRYPTOLOGY 2020, Putrajaya, Malaysia, 9–10 June 2020; pp. 151–164.