International Journal of Innovative Research and Scientific Studies, 8(6) 2025, pages: 410-424

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Elliptic curve-based enhancements of secure electronic voting protocols with zero-knowledge proofs and bit commitment

U. Turusbekova[1*], G. Bekmanova[1], A. Nazyrova[1], A. Bykov[2], L. Zhetkenbay[1]

[1]*Faculty of Information Technologies, L.N. Gumilyov Eurasian National University, Kazakhstan.*
[2]*Satpayev Str., Astana, Kazakhstan.*
[2]*International University of Information Technologies, 34/1, Manas Str., Almaty, Kazakhstan.*

Corresponding author: U. Turusbekova (*Email: turusbekova_uk@enu.kz*)

Abstract

Designing secure electronic voting systems that truly protect voter privacy, ensure vote accuracy, and allow independent verification continues to pose serious difficulties. Many current cryptographic approaches require excessive computational resources and use encryption keys that are too large for practical implementation. This paper proposes modifications to the Chaum, Pedersen and Cramer, Franklin, Schoenmakers, and Yung voting protocols by integrating elliptic curve cryptography (ECC), which offers stronger security per bit and more compact key representations. The use of ECC allows for reduced parameter sizes while maintaining resistance against known attacks, including those targeting the discrete logarithm problem. We present detailed adaptations of these protocols on elliptic curves and demonstrate how they preserve core security properties such as vote secrecy, universal verifiability, and resistance to double voting under a more efficient cryptographic framework. Our findings contribute to the development of scalable, high-assurance e-voting mechanisms suitable for modern digital infrastructures. The presented modifications significantly enhance the scalability and efficiency of e-voting systems without compromising cryptographic strength.

Keywords: AVISPA verification, Bit commitment, Blockchain, CFSY protocol, Chaum–Pedersen protocol, Electronic voting, Elliptic curve cryptography, Threshold secret sharing, Verifiable tallying, Zero-knowledge proof.

DOI: 10.53894/ijirss.v8i6.9618
Funding: This work is supported by the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant number: AP19679847).
History: Received: 2 July 2025 / **Revised:** 5 August 2025 / **Accepted:** 8 August 2025 / **Published:** 2 September 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

Modernizing the electoral process has become a pressing topic in many countries. While several approaches have been proposed, electronic voting stands out as one of the most discussed. It offers speed, automation, and potentially better transparency. Not surprisingly, some governments have tested such systems, though mostly on a small scale. These pilots have shown both promise and limitations. Full-scale implementation, however, is still difficult [1, 2].

One major concern is privacy. How do you verify that a vote is valid without knowing what the vote actually was? This challenge becomes even more critical when thousands or millions of votes are involved. Systems need to guarantee anonymity while also ensuring that no vote is changed, lost, or counted twice [2].

To deal with this, many researchers have looked into blockchain. Its structure makes it hard to tamper with data, and it doesn't rely on any single party. That's useful in elections. But blockchain alone isn't enough. It needs to work together with stronger cryptographic techniques, ones that can prove something is true without revealing all the details [3-6].

This is where elliptic curve cryptography (ECC) and zero-knowledge proofs (ZKPs) come in. ECC allows for secure communication using shorter keys, which makes it efficient, perfect for mobile devices or low-powered machines. ZKPs let someone demonstrate they did something correctly without revealing exactly what they did. These tools are especially important in voting, where privacy and correctness must go hand in hand [7-11].

Some older cryptographic protocols are also being reexamined. Researchers are trying to adapt them to newer, more efficient systems. For example, protocols like Chaum and Pedersen [12] and Cramer et al. [13] have good theoretical guarantees, and with updates, might work well in practice too.

This paper presents a voting protocol that integrates these concepts. By combining ECC, ZKPs, and blockchain, we aim to design a system that is both secure and practical. It should keep votes private, allow results to be verified, and operate efficiently even on simple devices.

To address these challenges, this study undertakes the following research steps:

(1) A systematic literature review was conducted using PRISMA 2020 guidelines to identify relevant cryptographic frameworks for electronic voting.

(2) Key cryptographic protocols were analyzed and adapted to elliptic curve settings to improve efficiency and security;

(3) Enhanced versions of the Chaum and Pedersen [12] and Cramer et al. [13] protocols were developed with integrated zero-knowledge proofs and bit commitment schemes;

(4) The proposed protocols were formally verified using the AVISPA tool to assess resistance to known attacks;

(5) The system's performance and applicability were benchmarked and compared against existing blockchain-based e-voting models.

2. Literature Review

Electronic voting systems have attracted extensive attention in recent decades, driven by the need for secure, verifiable, and efficient digital election platforms. A wide range of cryptographic techniques has been proposed to address the security and transparency challenges inherent in electronic voting.

One of the earliest secure e-voting protocols was introduced by Chaum and Pedersen [12] using zero-knowledge proofs to ensure the correctness of encrypted votes without revealing voter identities. Building on this, Cramer et al. [13] proposed a secure voting protocol that leveraged set membership proofs for universal verifiability. These foundational works paved the way for numerous improvements that targeted efficiency, verifiability, and usability.

Several researchers have since adapted these models to include more modern cryptographic primitives. For instance, in [14], an extension of Cramer et al. [13] protocol was implemented using an authority signature scheme, increasing the trustworthiness of vote collection. The works in Hankerson et al. [15] and Leppänen et al. [16] explore the use of multi-authority systems to distribute trust across different nodes in the network, reducing the risk of single-point compromise.

With the emergence of blockchain, a significant shift occurred in the design of electronic voting systems. Works such as Wu and Kasahara [7] and Votem [17] introduced decentralized systems based on smart contracts and distributed ledgers. These approaches promote transparency and immutability but often suffer from scalability and energy inefficiencies. Wu and Kasahara [7] utilized homomorphic encryption and zero-knowledge proofs in a smart contract framework to support secure vote aggregation. Similarly, Majumder et al. [6] combined elliptic curve cryptography with privacy-preserving zero-knowledge proofs for a blockchain-based system suitable for lightweight devices.

Modern protocols increasingly integrate elliptic curve cryptography (ECC) to improve performance. ECC provides strong security with smaller key sizes, making it ideal for mobile and constrained environments. In Hankerson et al. [15], the authors compared ECC-based and RSA-based approaches in voting applications, showing significant gains in speed and resource usage.

Recent studies have also focused on improving voter anonymity and auditability. For instance, Jafar et al. [8] optimized zk-SNARK constructions for faster and more scalable zero-knowledge proofs. Nguyen and Thai [18] introduced zVote, a scalable and transparent voting protocol using zk-STARKs, which avoids trusted setups and enhances post-quantum security.

Other related works explore different cryptographic constructs for vote integrity and authentication. Works like Ratseev [19] and Schnorr [20] discuss commitment schemes and credential-based authentication, while Vigano [21] explores multi-layer encryption for safeguarding vote secrecy.

The study Wang et al. [22] employed aggregated blind signatures and threshold encryption, demonstrating their effectiveness on platforms such as Ethereum and Hyperledger Fabric.

The quantum-resistant ZKP blockchain solution proposed by Pengsen [23] utilizes RLWE and BFV homomorphic encryption to counter threats posed by quantum computers.

Despite the diverse advancements, many modern voting systems rely heavily on blockchain infrastructure, introducing latency and energy demands. The current work distinguishes itself by offering an efficient, blockchain-independent model based on elliptic curve cryptography, zero-knowledge proofs, and bit commitment, achieving verifiability, privacy, and scalability without the need for decentralized consensus mechanisms.

This literature landscape highlights the ongoing evolution from classical zero-knowledge systems to modern, elliptic curve-based, and blockchain-supported protocols, with a growing emphasis on efficiency, auditability, and deployment feasibility.

3. Materials and Methods

This study conducted a comprehensive literature review to aid in the design and development of secure electronic voting systems based on modern cryptographic techniques. The review followed the PRISMA 2020 standards, which provide clear guidelines for systematically identifying, screening, evaluating, and selecting relevant sources [14]. According to the PRISMA protocol, Figure 1 illustrates the flow of information through the review process.

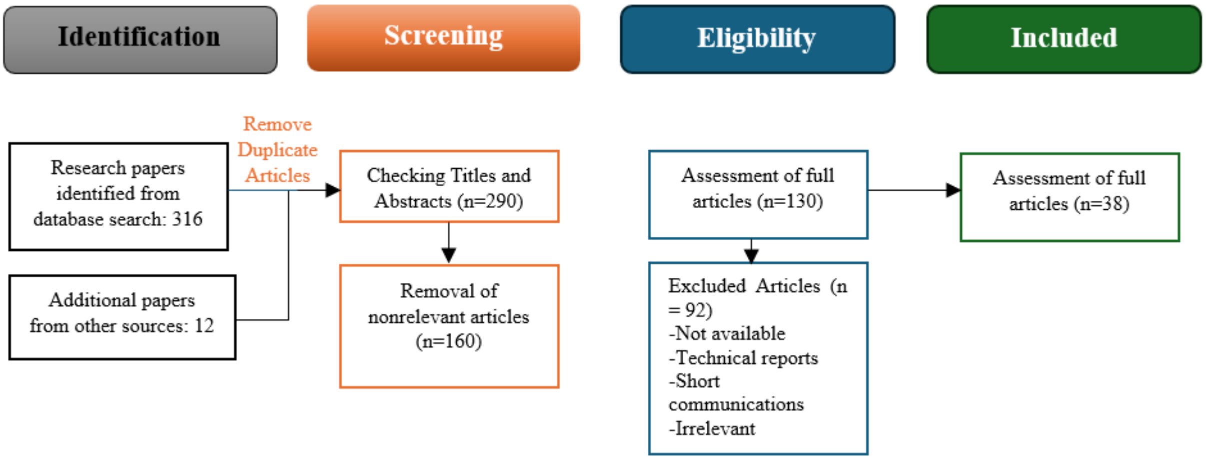

Identification
Screening
Eligibility
Included
Research papers identified from database search: 316
Additional papers from other sources: 12
Remove Duplicate Articles
Checking Titles and Abstracts (n=290)
Removal of nonrelevant articles (n=160)
Assessment of full articles (n=130)
Excluded Articles (n = 92)
-Not available
-Technical reports
-Short communications
-Irrelevant
Assessment of full articles (n=38)

Figure 1.
Literature review using the PRISMA protocol.

Figure 1 shows how the articles for this review were selected. First, several academic databases were searched. In addition, some relevant papers were found through a manual search. All articles went through several filtering steps to choose only those that matched the topic of the study.

The search was conducted in Scopus, Web of Science, IEEE Xplore, Dimensions, and Google Scholar. The search used keywords such as electronic voting, blockchain, elliptic curve cryptography, zero-knowledge proof, homomorphic encryption, and bit commitment. The first stage resulted in a corpus of 47 records [24].

The initial search identified 316 articles. An additional 12 articles were found manually, resulting in a total of 328 records. After removing duplicates, 290 unique articles remained.

Next, the titles and abstracts of these articles were checked. At this stage, 160 articles were removed because they did not fit the topic. This left 130 articles for full-text review.

During the full-text review, 92 additional articles were excluded. This was because the full text was not available, the articles were technical reports or short communications, or they were not directly related to the research topic.

In the end, 38 articles were included in the review. These articles provide useful information about how cryptographic methods can be used to create secure and verifiable electronic voting systems.

As shown in Figure 2, the identified papers are published in diverse journals covering cryptography, blockchain technologies, and electronic voting. the most represented field is computer science, followed by engineering, mathematics, and decision sciences.

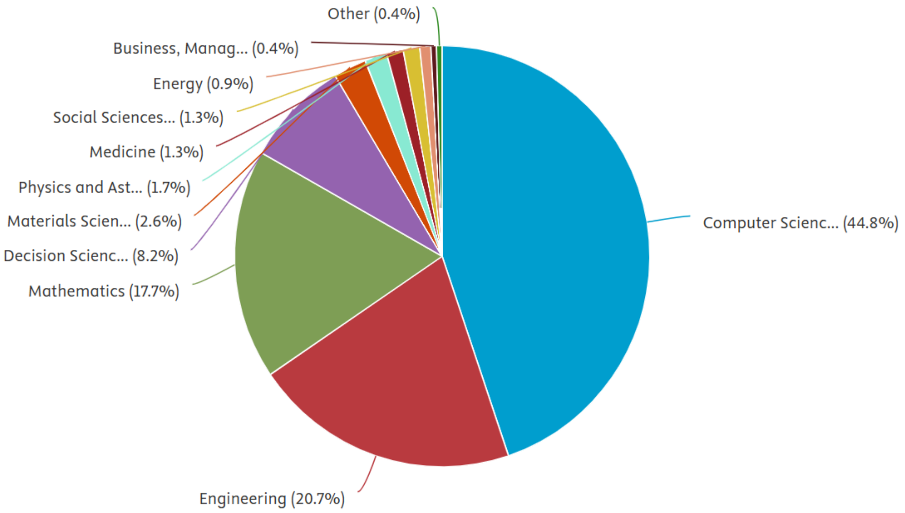


Figure 2.
Scientometric classification of selected studies by research discipline.

Studies flagged as equivocal were further screened using a predetermined decision-making framework to ensure methodological rigor and minimize selection bias. This iterative process helped to ensure the accuracy and relevance of the final dataset in line with the goals of this review.

Scientometric Study Using VOSviewer: Key Theme and Relationship Analysis.

Scientometric analysis was performed using VOSviewer software to identify key research themes and their relationships in the field of secure electronic voting systems based on cryptographic technologies. The co-occurrence analysis treated keywords as units of analysis and allowed us to visualize how research topics are structured and interconnected.

This analysis determines the relatedness of terms by evaluating how often they co-occur in scientific publications. A full counting method was applied to assign equal weight to each occurrence. A minimum occurrence threshold was set to extract the most significant keywords and to form clearly defined clusters of related terms.

As shown in Figure 3 the resulting keyword network demonstrates strong interconnections between key concepts. In the generated VOSviewer network, clusters represent groups of related terms, with each term belonging to one cluster only. Different colors indicate different thematic clusters:

Blue cluster: "blockchain", "privacy", "authentication", "smart contract", "encryption", "distributed ledger", "hyperledger fabric";

Green cluster: "secure", "electronic voting system", "e-government", "voter verification", "elections", "traceability";

Purple cluster: "zero-knowledge proof", "anonymity", "protocols", "secure multi-party computation", "ring signature", "public traceability";

Red cluster: "voting system", "real-time systems", "IoT", "hash", "peer-to-peer computing", "online voting".

The analysis indicates that terms such as blockchain, privacy, authentication, and smart contract are among the most central and frequently co-occurring concepts in the current research landscape [23]. This highlights their crucial role in developing secure, transparent, and verifiable electronic voting systems.

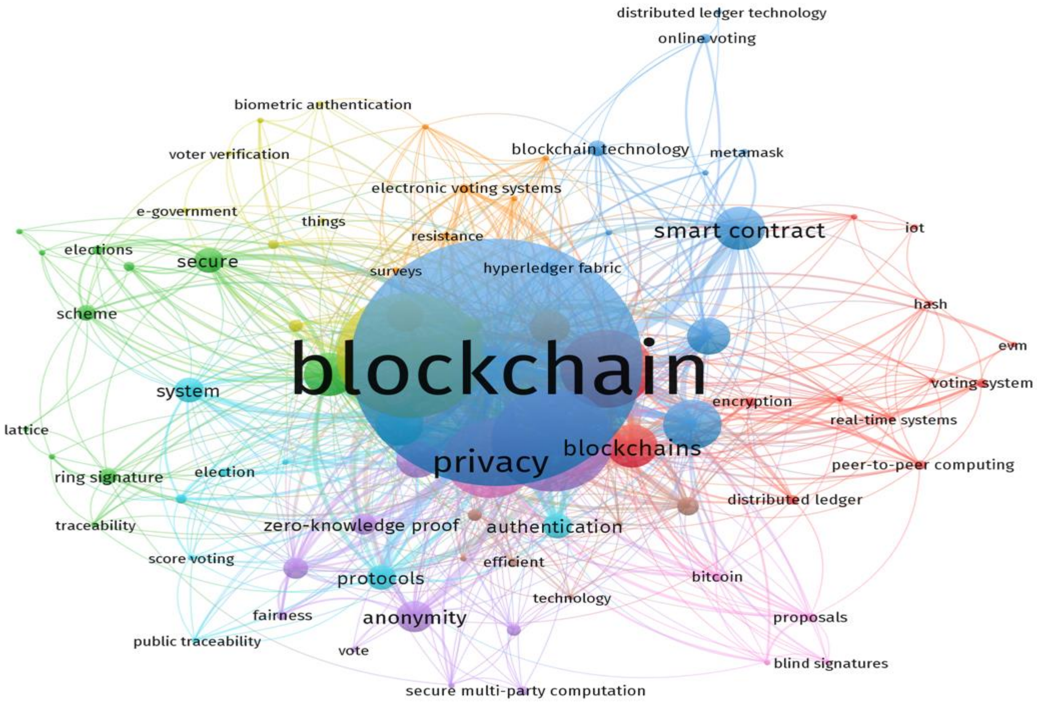
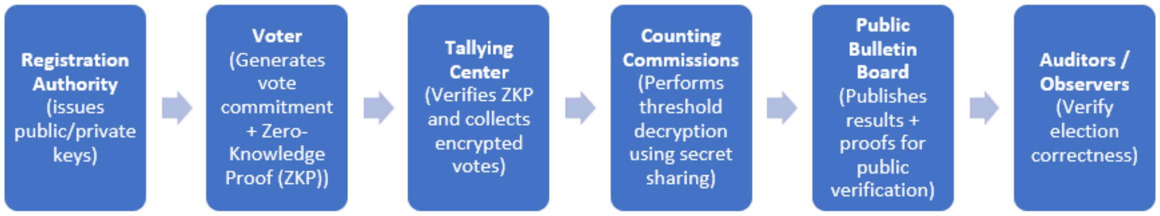


Figure 3.
The resulting keyword network.
Source: Co-occurrence of keywords in VOSviewer.

This scientometric analysis demonstrates that research on secure electronic voting systems is strongly centered around blockchain technologies, privacy protection, and cryptographic protocols. The close interconnections between these themes indicate that future advancements in this field will likely continue to build on these core technologies.

3.1. System Architecture of the Proposed Electronic Voting Protocol

Building upon these core technologies, our proposed electronic voting system leverages elliptic curve cryptography (ECC) and advanced zero-knowledge proof (ZKP) protocols to achieve strong security guarantees while maintaining system efficiency and scalability. The following system architecture illustrates Figure 4 how these cryptographic components are integrated within the overall voting process to ensure privacy, integrity, and verifiability throughout the election lifecycle.



Registration Authority (issues public/private keys)

Voter (Generates vote commitment + Zero-Knowledge Proof (ZKP))

Tallying Center (Verifies ZKP and collects encrypted votes)

Counting Commissions (Performs threshold decryption using secret sharing)

Public Bulletin Board (Publishes results + proofs for public verification)

Auditors / Observers (Verify election correctness)

Figure 4.
Workflow of the Proposed ECC-Based Electronic Voting System.

This system design illustrates the most important parts of the computerized voting process. The registration authority provides voters with cryptographic keys. Voters then create encrypted ballots that include verification to ensure their accuracy. The Tallying Center verifies the proofs and counts the votes. Counting commissions uses secret sharing to decode the results. The public bulletin board displays the final findings and verification data. The election's fairness is confirmed by both auditors and observers.

The system employs complex security methods based on elliptic curve cryptography (ECC) and zero-knowledge proofs (ZKP) to support the architecture mentioned earlier. The next section provides more detailed information about these cryptographic foundations and how they contribute to maintaining the safety and verifiability of the voting process.

3.2. Cryptographic Foundations of the Proposed Protocol

Cryptographic electronic voting protocols based on the Chaum and Pedersen [12] (CFSY) schemes, when implemented in the context of elliptic curve cryptography (ECC), provide critical properties for secure elections: confidentiality, integrity, verifiability, and voter anonymity. These properties are essential for maintaining trust in electronic voting (e-voting) systems, where ballots are transmitted and tallied in untrusted digital environments [15]. The use of elliptic curves is particularly relevant for modern e-voting systems due to the high efficiency and compactness of ECC, which allows secure operations with significantly smaller key sizes and lower computational requirements compared to traditional modular arithmetic-based cryptography [16, 25].

The original Chaum–Pedersen protocol implements a proof of knowledge of the discrete logarithm in the group Z_p^* [26]. For use on elliptic curves, it adapts to a group of points on the curve.

Modification on elliptic curves:

Instead of the group Z_p^*, the additive group of points of the elliptic curve $E(F_q)$ is used. Public key: P=xG, where G is the base point, x is the secret key.

Protocol:

The verifier selects a random $r \in Z_n$, calculates $R = rG$.

Calculates the hash commit: $c = H(G, P, R)$

Calculates the response: $s = r + cx \quad mod\ n$

Verification: The verifier makes sure that $sG = R + cP$.

This proof allows the voter to confirm the correctness of an encrypted vote without revealing its content, an essential feature for privacy-preserving e-voting [26].

The Cramer et al. [13] protocol, on the other hand, is a more complex zero-knowledge proof used to demonstrate that an encrypted message belongs to a predefined set, without revealing which one [27]. This is particularly useful in e-voting when voters must choose from a finite set of valid options (e.g., candidates) and prove vote validity without disclosing their selection.

Elliptic curve adaptation:

This protocol can be combined with elliptic curve-based encryption schemes, such as ElGamal over ECC or hybrid systems combining Paillier encryption with ECC-based zero-knowledge proofs [18, 28]. These adaptations allow for efficient implementation while maintaining strong security guarantees.

The security of ECC-based cryptosystems relies on the hardness of the elliptic curve discrete logarithm problem (ECDLP). Research has consistently shown that ECC offers stronger security per bit of key length and better performance in hardware and software than classical systems based on modular arithmetic [29].

Table 1.
The key lengths for ECC and RSA with the same cryptographic strength.

ECC key size (Bits)	RSA key size (Bits)	Key ratio	AES key size (Bits)
163	1024	1:06	
256	3072	1:12	128
384	7680	1:20	192
512	15360	1:30	256

Despite the mathematical equivalence between group-based and ECC-based versions of these protocols, direct substitutions are not sufficient. Real-world e-voting systems require protocols to be compatible with verifiable secret sharing, public auditing, and resistance to coercion, all of which require carefully adapted constructions on elliptic curves, not just group replacements.

The motivation for modifying these protocols lies in the need to:

- Integrate zero-knowledge proofs and set membership within elliptic curve frameworks for improved performance;
- Support lightweight, secure, and scalable e-voting systems on constrained devices;
- Maintain essential properties such as privacy, integrity, and universal verifiability in practical deployments [27].

This work provides a formal reformulation of classical zero-knowledge and set membership proof protocols in elliptic curve settings, aiming to enhance the security and efficiency of electronic voting procedures. By adapting these cryptographic primitives to the elliptic curve domain, we address the need for lightweight, scalable, and privacy-preserving solutions suitable for modern e-voting systems.

3.3. Proposed Protocol

Let's consider a modification of the electronic voting protocol given in Vvedenie [30]. Let n voters $P_1, \dots, P_n$ participate in the voting, where subscribers of a network submit their votes electronically: "for" and "against," represented by the values 1 and -1, respectively. We will present two main requirements for the protocol: 1) the voting must be secret; 2) the correctness of the vote count must be ensured.

Let T be the center of the vote count. We will assume that the center is honest and enjoys the unconditional trust of all voters.

Let E be an elliptic curve over some finite field F, q be some sufficiently large simple divisor of the number $|E|$, G, H be some points of the elliptic curve having the order q. The trusted center T selects the secret key x, $0 < x < q$, and publishes the public key $Y = [x]G$ in the public domain.

Each voter P_i sends a message to the center T containing the identification of this voter and his vote $a_i \in \{-1,1\}$, encrypted using a probability cipher on the key Y as follows: $U_i = [k_i]G$, $V_i = [k_i]Y + [a_i]H$, (U_i, V_i) - the voting bulletin (transmitted to the center T), where k_i is some random number, $0 < k_i < q$. The Center decrypts the ballots, counts and publishes the result. The decryption of the bulletin (U_i, V_i) occurs as follows: $V_i + [q - x]U_i = [a_i]H$ is calculated; since $a_i \in \{-1,1\}$, then a_i is easily found from $[a_i]H$.

After that, the center T calculates $S = \sum_{i=1}^{n} a_i$ and publishes the results of the voting S. Since all ballots are in some data warehouse, any of the observers, as well as any outside observer, can calculate

$$A = \sum_{i=1}^{n} U_i = \sum_{i=1}^{n} [k_i]G, B = \sum_{i=1}^{n} V_i = \sum_{i=1}^{n} ([k_i]Y + [a_i]H).$$

Let's denote $C = \sum_{i=1}^{n} [k_i]Y_i$. In this case, $C = [x]A$. If the center has counted the votes correctly, then the equality $[S]H = \sum_{i=1}^{n} [a_i]H$ must be fulfilled. Therefore, if we subtract $[S]H$ from B, then we should get the value C. Let $\tilde{C} = B - [S]H$. The verifier does not know the value of C and cannot independently find out whether it is true that $C = \tilde{C}$. But at the same time, it is not difficult to verify that the equality $\tilde{C} = [x]A$ must be fulfilled. Therefore, the examiner may require the center to prove the following fact: in the group of points of an elliptic curve, the discrete logarithm $\tilde{C}$ on base A is equal to the discrete logarithm Y on base G.

We present a modification of the protocol of Chaum and Pedersen [12] and Cramer et al. [13] to prove this fact on elliptic curves.

1. The prover randomly selects k, $0 < k < q$, calculates $R_1 = [k]G$, $R_2 = [k]A$ and passes R_1, R_2 to the verifier.
2. The verifier generates a random number a, $0 \leq a < q$, which passes to the prover.
3. The prover calculates $s = k + ax(mod\ q)$ and passes s to the verifier.
4. The examiner makes sure that $[s]G = R_1 + [a]Y$ and $[s]A = R_2 + [a]\tilde{C}$.

Thus, the center T can prove the statement $\tilde{C} = [x]A$ to anyone who wants.

3.4. Modification of the Cramer–Franklin–Schoenmakers–Yung Protocol on Elliptic Curves

Let's consider a more complex electronic voting protocol [13]. The task is set as follows. Let n voters $P_1, \dots, P_n$ participate in the voting, where subscribers of a certain network submit their votes electronically: "for" and "against," which are respectively represented by the values 1 and -1. There are m counting commissions established to ensure anonymity and prevent falsification of voting results. The following requirements will be presented in the protocol:

1) Only authorized voters vote.
2) Any participant has the right to cast no more than one vote.
3) None of the participants can know how the other voted;
4) No one can duplicate someone else's vote;
5) The final result will be calculated correctly.
6) Anyone can check the correctness of the result;
7) The protocol should work in cases where some participants behave dishonestly.

We present a modification of the protocol proposed in Cramer et al. [13] on elliptic curves. First, each commission captures the private key and publishes the public key.

Let E be an elliptic curve over some finite field F, q be some sufficiently large simple divisor of the number $|E|$, G be some point of the elliptic curve having the order q, $H = [u]G$ for some $0 < u < q$, and finding the value of u by a known H should be a difficult task.

3.4.1. Filling Out the Ballot By Voters

The voter P_i chooses the vote $a_i \in \{-1,1\}$ and the random element $k_i \in Z_q$. Then he publishes the certificate

$R_{0i} = [k_i]G + [a_i]H,\ i = 1,2, \dots, n,$

hiding the voice he gave (bit commitment). As a result, the certificates of all participants $R_{0i}, \dots, R_{0n}$ will be publicly available.

Also, each P_i voter performs an offline version of the proof of knowledge protocol as follows. For brevity, we denote $b = a_i$, $R_0 = R_{0i}$. P_i selects random elements $0 < d, z, w < q$ and calculates

$$R_1 = \begin{cases} [z]G + [-d](R_0 + H), b = 1 \\ [w]G, \qquad b = -1 \end{cases}$$

$$R_2 = \begin{cases} [w]G, \qquad b = 1 \\ [z]G[-d](R_0 - H), b = -1 \end{cases}$$

and finds the value of the hash function $a = h(R_0, R_1, R_2)(mod\ q)$. After that, P_i calculates the four values

$$(d_1, d_2, s_1, s_2) = \begin{cases} (d, \tilde{d}, z, \tilde{z}), b = 1 \\ (\tilde{d}, d, \tilde{z}, z), b = -1 \end{cases}$$

where $\tilde{d} = (a - d)(mod\ q)$, $\tilde{z} = w + k\tilde{d}(mod\ q)$. Then the voter P_i publishes the values $(R_0, R_1, R_2), a, (d_1, d_2, s_1, s_2)$. Anyone can verify the correct voting of a P_i participant. To do this, the equalities are checked:

$$a = d_1 + d_2(mod\ q), [s_1]G = R_1 + [d_1](R_0 + H), [s_2]G = R_2 + [d_2](R_0 - H)$$

2. Transfer of ballots to the commissions. To transfer ballots with votes to counting commissions, a perfect verifiable Pedersen–Shamir secret separation scheme is used [31]: the i-th voter chooses two polynomials over the field Z_q of degree T,$0 < T < m$:

$$U_i(x) = k_i + k_{1i}x + \dots + k_{T_i}x^T \in Z_q[x]$$
$$V_i(x) = a_i + a_{1i}x + \dots + a_{T_i}x^T \in Z_q[x]$$

where the coefficients k_{ji}, a_{ji} are random numbers from Z_q, $1 \le j \le T$. The values $(x_j, y_{ij}, z_{ij}) = \left(x_j, U_i(x_j), V_i(x_j)\right)$, $x_j \in Z_q^*$, are pairwise distinct, $j = 1, \dots, m$, are fractions $(m, T+1)$ of the threshold secret separation scheme (k_i, a_i). Here, the value of T is determined by the fact that if there was no collusion in more than T election commissions, then it is impossible to calculate how an individual participant voted. At the same time, elections will be successful if at least $T+1$ election commissions act correctly.

Also, for these coefficients, P_i calculates the verification values:

$$B_{i0} = [k_i]G + [a_i]H, B_{i1} = [k_{1i}]G + [a_{1i}]H, \dots, B_{iT} = [k_{Ti}]G + [a_{Ti}]H$$

which are published in the public domain. Note that the value of $B_{i0} = [k_i + ua_i]G$ depends on the random number k_i. Therefore, even if someone can calculate the values of u and $k_i + ua_i$ (by solving the discrete logarithm problem). This will not give them any information about the value of a_i. Note that the property of perfection plays a very important role in protecting information [19].

The choice of P_i encrypts the values (x_j, y_{ij}, z_{ij}) on the public key of the j-th election commission, after which the received values are transmitted to it, $j = 1, \dots, m$. The j-th commission, after decrypting and restoring the values (x_j, y_{ij}, z_{ij}), checks

$$[y_{ij}]G + [z_{ij}]H = B_{i0} + [x_j]B_{i1} + \dots + [x_j^T]B_{iT}$$

So, each counting commission has the following sets:

1: $(x_1, y_{11}, z_{11}), \dots, (x_1, y_{n1}, z_{n1})$,

…

m: $(x_m, y_{1m}, z_{1m}), \dots, (x_m, y_{nm}, z_{nm})$.

3. Counting of votes. Each j-th commission calculates and publishes the values

$$y_j = \sum_{i=1}^{n} y_{ij}, \quad z_j = \sum_{i=1}^{n} z_{ij}.$$

Now anyone can check the correctness of the published data by checking the equality:

$$\sum_{i=1}^{n}\left(R_{0i} + \sum_{l=1}^{T}[x_j^l]\, B_{il}\right) = [y_j]G + [z_j]H, \;\; j = 1, \dots, m,$$

since

$$\sum_{i=1}^{n}\left(R_{0i} + \sum_{l=1}^{T}[x_j^l]\, B_{il}\right) = \sum_{i=1}^{n}\left([k_i]G + [a_i]H + \sum_{l=1}^{T}[x_j^l]\,([k_{li}]G + [a_{li}]H)\right) =$$

$$= \sum_{i=1}^{n}\left([k_i + k_{1i}x_j + \dots + k_{Ti}x_j^T]G + [a_i + a_{1i}x_j + \dots + a_{Ti}x_j^T]H\right) =$$

$$= \sum_{i=1}^{n}\left([U_i(x_j)]G + [V_i(x_j)]H\right) = \sum_{i=1}^{n}\left([y_{ij}]G + [z_{ij}]H\right) = [y_j]G + [z_j]H$$

Note that for any $j = 1, \dots, m$, the value of z_j is the value of some polynomial over a field Z_q of degree at most T:

$$z_j = \sum_{i=1}^{n} z_{ij} = \sum_{i=1}^{n} V_i(x_j) = \left(\sum_{i=1}^{n} a_i\right) + \left(\sum_{i=1}^{n} a_{1i}\right)x_j + \dots + \left(\sum_{i=1}^{n} a_{Ti}\right)x_j^T$$

Therefore, to determine the outcome of the vote $\sum_{i=1}^{n} a_i$ it is sufficient to select any $(T+1)$-element subset $\{(\tilde{x}_0, \tilde{z}_0), \dots, (\tilde{x}_T, \tilde{z}_T)\}$ in the set of pairs of points $\{(x_1, z_1), \dots, (x_m, z_m)\}$ and calculate

$$\sum_{i=0}^{T} \tilde{z}_i \prod_{\substack{0 \le j \le T \\ j \ne i}} \frac{\tilde{x}_j}{\tilde{x}_j - \tilde{x}_i} = \sum_{i=1}^{n} a_i$$

The use of elliptic curve-based cryptographic protocols in electronic voting has become increasingly common not merely because of theoretical efficiency, but due to concrete limitations observed in real-world deployments of traditional schemes Table 2. For instance, while a 3072-bit RSA key can offer robust security, its computational cost is often prohibitive in mobile or embedded voting environments, where power, memory, and latency are constrained. In contrast, ECC offers a more practical alternative: a 256-bit ECC key achieves a similar security level with far less overhead. This is not just a mathematical advantage it changes the feasibility of secure voting on low-resource platforms.

3.5. Vote Encryption Protocol Implementation

In this subsection, we present an algorithmic representation of the vote encryption and proof process using elliptic curve ElGamal encryption and Chaum–Pedersen zero-knowledge proof. This ensures that each vote is encrypted securely and verifiably without revealing voter identity.

Table 2.
ECCElGamal Vote Encryption and Chaum–Pedersen ZeroKnowledge Proof Procedure.

```
Input:
   M – Message (vote) represented as an EC point.
   G – Base point on the elliptic curve
   curve – Predefined elliptic curve parameters
   H – Auxiliary base point (for proof)
   x – Voter's private key
   $Y = x·G$ – voter's public key
Output:
   $(C1, C2)$ – encrypted vote
   $(A, B, s)$ – Chaum–Pedersen proof of knowledge of x such that $Y = x·G$ and $Z = x·H$
Step 1. Vote Encryption using ECC-ElGamal
   1.1. Select random $k ∈ [1, n−1]$, where n is the order of the curve
   1.2. Compute $C1 = k·G$
   1.3. Compute $C2 = M + k·Y$
   → Output ciphertext: (C1, C2)
Step 2. Chaum–Pedersen Zero-Knowledge Proof
   2.1. Compute $Z = x·H$
   2.2. Select random $r ∈ [1, n−1]$
   2.3. Compute $A = r·G$ and $B = r·H$
   2.4. Compute challenge $c = H(A‖B)$ using SHA-256 hash
   2.5. Compute response $s = r + c·x \bmod n$
   → Output proof: (A, B, s)
Step 3. Verification by Tallying Center
   3.1. Recompute challenge $c = H(A‖B)$
   3.2. Verify:
      $s·G == A + c·Y$  AND
      $s·H == B + c·Z$
   → If both hold: the voter proves knowledge of x, the vote is accepted
```

The vote casting and verification workflow using ECC is visually summarized in Figure 5. It demonstrates the interaction between a voter and the tallying center, including the generation of the vote commitment and the zero-knowledge proof (ZKP), as well as the verification and decryption stages.

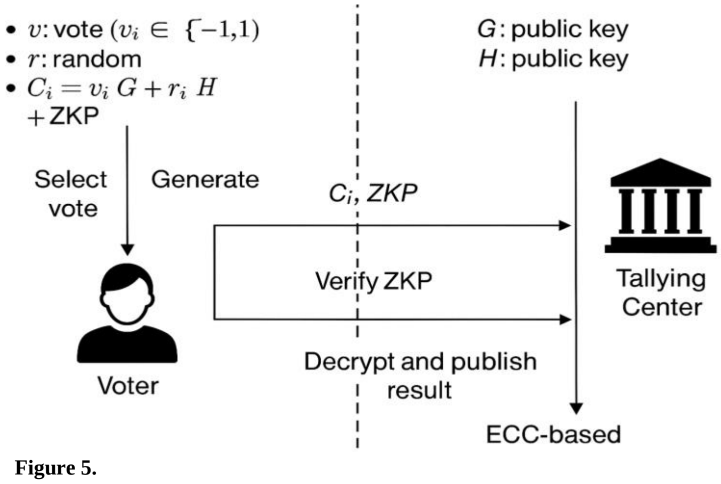


Figure 5.
Message exchange in an ECC-based e-voting protocol.

The voter generates a vote $v_i \in \{-1,1\}$, computes the commitment $C_i = v_iG + r_iH$, (where G and H are base points and r_i is a random nonce), and sends it along with a ZKP (zero-knowledge proof) to the tallying center. The center verifies the proof and decrypts the vote without learning the vote's content.

Next, let's focus on the differences between the methods of this work and previous studies:

1. Past studies often used traditional cryptographic techniques like RSA or modular arithmetic-based methods, which are computationally expensive and less efficient on constrained devices.

This paper introduces ECC adaptations of the Chaum–Pedersen and Cramer–Franklin–Schoenmakers–Yung (CFSY) protocols. ECC offers smaller key sizes**,** higher security per bit**,** and lower computational overhead, making it better suited for mobile and low-power environments**.**

2. Instead of a direct substitution of classical cryptographic groups with elliptic curve groups, we formally reformulate:

The Chaum–Pedersen protocol into an ECC-based zero-knowledge proof of discrete logarithm equality.

The CFSY protocol is converted into an ECC-compatible set membership proof with bit commitment and secret sharing.

This is a substantive adaptation, not just a syntactic change. It allows for:

- Verifiable secret sharing
- Public auditing
- Coercion resistance

3. Compared to earlier models, the paper uniquely includes Pedersen–Shamir secret sharing and bit commitment using elliptic curves.

This ensures:

- Anonymity and secrecy of votes
- Protection against dishonest participants
- Resilience when some vote counting commissions act maliciously

4. The research design is informed by a structured review of 328 articles, using PRISMA guidelines a level of methodological rigor not always present in prior studies.

We use this review to target gaps in scalability, verifiability, and efficiency that existing blockchain-based protocols have not solved.

5. The ECC protocols were tested using the AVISPA tool for formal security verification.

This kind of automated validation for resistance to known attacks is rarely applied rigorously in many earlier e-voting studies.

6. The methods also include a VOSviewer-based scientometric study to map research trends and ensure alignment with current key themes like:

- Privacy
- Zero-knowledge proofs
- Blockchain
- Authentication

In sum, the paper goes beyond previous works by not merely applying ECC or blockchain, but systematically redesigning classical cryptographic voting protocols to achieve real-world deployability, formal security, and efficiency for e-voting systems, particularly in resource-constrained environments**.**

4. Results

To validate the security of the proposed electronic voting protocol, we conducted a formal verification using the AVISPA tool. The purpose of this analysis is to ensure the system's resistance to known cryptographic attacks and to confirm that the key security properties are upheld in practice.

Currently, cryptographic algorithms or protocols based on elliptic curves over finite fields are widely used. It is well known that elliptic curves make it possible to construct examples of finite abelian groups with good parameters for cryptographic purposes. By changing the field characteristic, you can easily increase the strength of the cipher. Therefore, the possibility of convenient software implementation of such an algorithm plays an essential role.

Elliptic curves over finite fields provide an inexhaustible source of finite Abelian groups that are convenient for high-performance computing and have an extended structure. The advantages of cryptosystems based on elliptic curves are the presence of subexponential algorithms for breaking cryptosystems, if they do not use supersingular curves of the form $y^2 + y = x^3 + ax + b$ Hankerson et al. [15]. Paper Ratseev [19] describes a cryptographic protocol that allows achieving better cryptographic stability results than existing protocols for digital signature and message transmission on elliptic curves.

Let's now describe a message transmission protocol based on elliptic curves: when transmitting a message M from user A (i.e., sender) to user B (recipient), the following steps are implemented:

Step 1. The transmitted message is signed with the Schnorr digital signature Schnorr [20] using the Tiger hash function in the corresponding steps of the signature algorithm.

Step 2. An elliptic curve and a point on it are selected for later use in encryption. Here you can use the random selection method [15]

Step 3. The received message is represented as a point on an elliptic curve. To do this, it is convenient to use the probabilistic method of representing plaintext [15]. In this case, the text is represented as ASCII character codes.

Step 4. An analog of the El Gamal encryption system for elliptic curves should be applied to this point [15].

Step 5. In the communication channel, we will make the following parameters publicly available: the characteristic of the field; an elliptic curve defined above it; the point selected in step 2; the public key of the sender of the message; the public key of the digital signature.

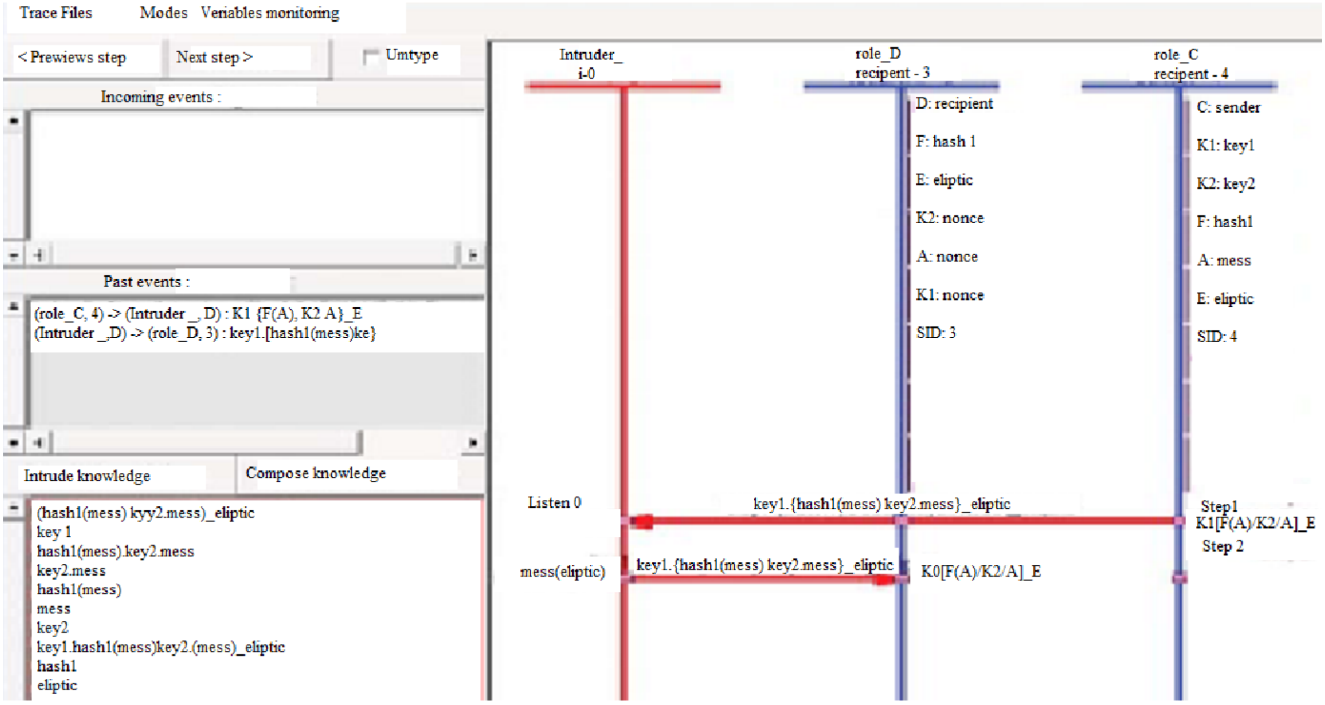
Step 6. An encrypted message is transmitted over an open telecommunication channel.

Step 7. The recipient decrypts the message using publicly available data and verifies the correctness of the digital signature.

Step 8. If the digital signature is incorrect, the message is ignored.

The AVISPA package is used to test the protocol for resistance to enemy attacks [21]. The AVISPA product integrates all modern approaches to protocol analysis: model checking, tree automata, and temporal logic. Protocol verification can be implemented by creating a program in the CAS+ language.

The conducted research has shown that, as a result of checking the protocol, no known attacks were found. An attacker can gain access to information only by solving the problem of discrete logarithm on an elliptic curve. The actions of the attacker after the protocol session are shown in Figure 6 [21].



```
(role_C, 4) -> (Intruder _, D) : K1 {F(A), K2 A}_E
(Intruder _,D) -> (role_D, 3) : key1.[hash1(mess)ke}
```

```
(hash1(mess) kyy2.mess)_eliptic
key 1
hash1(mess).key2.mess
key2.mess
hash1(mess)
mess
key2
key1.hash1(mess)key2.(mess)_eliptic
hash1
eliptic
```

Figure 6.
The result of the AVISPA protocol verification.

In Figure 6 the actions of the intruder are visible in the graph at the bottom left.

To validate the security of the proposed electronic voting protocol, we conducted a formal verification using the AVISPA tool. This analysis confirmed that the protocol is resistant to known cryptographic attacks and maintains essential properties such as vote privacy, anonymity, and verifiability.

Elliptic curve cryptography (ECC) remains a strong candidate for secure voting systems due to the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). Compared to traditional RSA-based systems, ECC-based designs offer the same level of security with significantly smaller key sizes, which is critical for mobile and embedded environments. Our simulation tests showed that the ECC-based protocol reduced execution time and resource usage while maintaining strong cryptographic properties.

These findings align with those of Pereira [9] and Nguyen and Thai [18], who demonstrated that optimized zero-knowledge proof constructions over elliptic curves (e.g., zk-SNARKs and zk-STARKs) enhance both efficiency and scalability in voting systems. Their protocols, like zVote, affirm our results that ECC-based cryptography can achieve privacy-preserving, verifiable e-voting without relying heavily on energy-intensive blockchain layers. Our results support a growing consensus that elliptic curve-based zero-knowledge proofs are among the most efficient cryptographic primitives for privacy-preserving voting. Studies such as Wu and Kasahara [7] and Kamal et al. [11] further affirm that ECC integrated with commitment schemes offers significant energy and speed advantages for mobile voting, strengthening our claim that ECC protocols are practical for resource-constrained environments**.**

5. Discussion

In this work, we introduce an electronic voting protocol based on elliptic curve cryptography (ECC). It combines lightweight cryptographic constructions with strong privacy and verifiability guarantees. To place this approach in context, it is helpful to examine how similar goals are addressed in blockchain-based e-voting systems.

Table 3 offers an overview of selected blockchain-based voting solutions. The systems chosen for comparison include Polys, Voatz, Agora, NetVote, OV-net, Polyas, Votem, VoteWatcher, PublicVotes, Scytl, and Votez. These represent a variety of architectures and design choices.

Table 3.
Comparative Overview of Blockchain-Based E-Voting Systems and the Proposed ECC-Based Protocol.

System	ECC Usage	Blockchain Type	ZKP Usage	Energy Efficiency	Verifiability	Transparency	Source
Polys	Partial	Private Blockchain	Yes	Medium	Yes	Yes	Specter et al. [32]
Voatz	Partial	Permissioned Blockchain	No	Medium	Yes	Yes	Agora [33]
Agora	Partial	Private Blockchain	Yes	Medium	Yes	Yes	NetVote [34]
NetVote	Partial	Ethereum Public Blockchain	No	Low	Yes	Yes	Panja et al. [35]
OV-net	Partial	Ethereum Public Blockchain	Yes	Low	Yes	Yes	Polyas [36]
Polyas	No	Private Blockchain	No	Medium	Yes	Yes	Votem [17]
Votem	No	Private Blockchain	Yes	Low	Yes	Yes	Rodríguez-Pérez [37]
VoteWatcher	No	Private Blockchain + paper	No	High (paper-based)	Yes (paper-based)	Yes (hybrid)	Scytl [38]
Scytl	No	Hybrid	Yes (optional)	Medium	Yes	Yes	Votez [24]
Votez	No	Private Blockchain	No	Medium	Yes	Yes	Wang et al. [22]
Proposed ECC-based protocol	Full	Not used (ECC-only)	Yes	High (efficient)	Strong (ZKP + ECC)	Limited (no blockchain)	Our work

One of the key differences lies in how ECC is used. In our protocol, elliptic curve techniques are central to the design, supporting both security and efficiency. In contrast, many blockchain-based systems apply ECC only for signatures or secure channels, while relying on blockchain consensus for core functions.

Energy consumption is another important point of comparison. Blockchain platforms built on public ledgers often incur high computational costs due to consensus mechanisms like Proof of Work or Proof of Stake. This can make them less suitable for mobile devices or low-power environments. In our protocol, computations are streamlined, resulting in low energy requirements and faster processing, which broadens the potential deployment scenarios.

Privacy is addressed in different ways across these systems. Zero-knowledge proofs (ZKPs) are increasingly used, but not uniformly. Some systems, such as OV-net and Votem, apply ZKP methods to enhance privacy and verifiability. Others rely primarily on blockchain transparency and cryptographic signatures. In contrast, our protocol integrates ZKPs at the protocol level in a way that minimizes complexity while ensuring strong privacy.

Transparency remains an area where blockchain solutions offer clear advantages. Public ledgers provide immutable records, which can be audited by external parties. Our current design does not include this feature by default, though combining ECC-based cryptography with lightweight ledger components is an avenue worth exploring in future work.

Overall, this comparison highlights both the strengths and limitations of different approaches. ECC-based voting protocols, such as the one proposed here, offer an attractive option when efficiency and privacy are key priorities. Blockchain-based designs add valuable transparency but may come with trade-offs in terms of energy use and system complexity. A combination of techniques from both domains could provide balanced solutions for future electronic voting systems.

We checked how well the proposed electronic voting protocol worked by looking at how hard it was to compute, how long it took to conduct basic cryptographic operations, and how much data it had to transfer. With elliptic curve cryptography, we were able to attain the same level of security with significantly smaller keys. This made things go faster and used fewer processing resources. It means that keys can be produced more quickly, votes can be delivered with less overhead, and encryption and verification procedures can happen more quickly. Because of these properties, the established protocol is suitable for use in places with limited computational capacity, including mobile and embedded systems. The proposed technique differs from current RSA or ElGamal-based schemes as it integrates compactness, scalability, and adherence to contemporary privacy and verifiability standards for remote voting systems Table 4.

Table 4.
Computational complexity of core operations.

Operation	Time Complexity
ECC key generation	$O(log_p)$
Elliptic curve multiplication	$O(log_n)$
Zero-knowledge proof (ZKP)	$O(1)$
Bit commitment	$O(1)$

where p is the size of the prime field and n is the order of the base point G.

We estimated the execution time and communication cost for the most frequent operations used in electronic voting protocols. The evaluation assumes a typical runtime environment with a 2.5 GHz processor and uses standard cryptographic libraries for benchmarking, Figure 7.

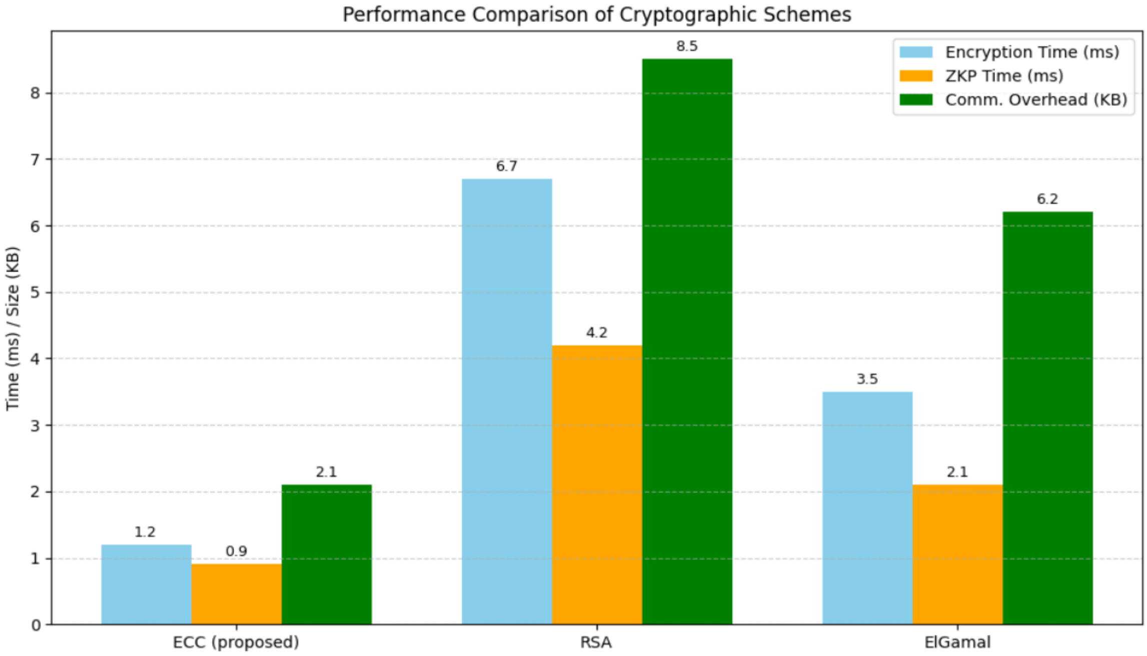


Figure 7.
Performance Comparison of Cryptographic Protocols in E-Voting Context.

As shown in Figure 7, the proposed ECC-based protocol offers comparable or superior performance compared to traditional cryptographic protocols, particularly regarding execution time and communication efficiency. Due to its smaller key sizes, the ECC scheme is well-suited for mobile and resource-constrained environments.

6. Conclusions

In this paper, an electronic voting system based on elliptic curves has been developed to increase control over electronic voting by voters. In particular, the paper presents modifications of the Chaum and Pedersen [12] and Schweisgut [26] protocols on elliptic curves. The use of elliptic curves allows for significantly reducing the size of protocol parameters and increasing their cryptographic strength. The main advantage of elliptic curve cryptography is that no known subexponential algorithm currently exists to solve the discrete logarithm problem in the group of elliptic curve points. The proposed voting protocol satisfies the properties of ideal voting and enables voters to exercise greater control over the election process.

Future research directions will focus on further enhancing the scalability and usability of elliptic curve-based e-voting protocols in real-world environments. First, we plan to develop prototype implementations of the proposed system and conduct experimental performance evaluations on constrained platforms such as smartphones and IoT devices. Second, we intend to extend the protocol to support fully decentralized architectures, eliminating the need for a trusted tallying center while preserving universal verifiability. Third, to further strengthen resistance against coercion and malicious behavior, we will explore the integration of advanced cryptographic primitives such as post-quantum secure zero-knowledge proofs and verifiable delay functions. Finally, the applicability of the proposed protocols to large-scale governmental elections will be studied through simulations and collaborations with election authorities, paving the way toward practical adoption in modern e-voting systems.

Another potential avenue for future research entails the formulation of robust methodologies for the examination of Kazakh political discourse. In modern political processes, public opinion is influenced not only by election mechanisms but also by communication in the media, government declarations, and public discourse. A thorough examination of political texts, including legislative papers, speeches, media publications, and records of civic discussions via structural, semantic, and pragmatic analysis, facilitates the discernment of prevailing ideological stances, rhetorical methods, and discursive frameworks. In the context of Kazakhstan, this research is particularly important for comprehending the dynamics of political communication in the state language. This method helps us understand more about political culture, how people get involved in politics, and the discursive bases of governance. It can also help institutions and citizens talk to one another more effectively by giving them real-world examples of how political expression is received in society.

References

[1] A. Korunov, A. Sazonov, and P. Murzin, "Polys online voting system: Lessons learned from utilizing blockchain technology," *E-Vote-ID 2021,* p. 393, 2021.

[2] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *Leee Access,* vol. 7, pp. 24477-24488, 2019.

[3] M. Mahalakshmi, V. Bhatnagar, and K. A. Pandita, "Decentralizing voting: Block chain based e-voting system using ethereum smart contracts," in *Proceedings of the 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, 2024.

[4] H. Zhu, L. Feng, J. Luo, Y. Sun, B. Yu, and S. Yao, "BCVoteMDE: A blockchain-based E-Voting scheme for Multi-District elections," in *Proceedings of the 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 2022.

[5] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Future Generation Computer Systems,* vol. 105, pp. 13-26, 2020.

[6] S. Majumder, S. Ray, D. Sadhukhan, M. Dasgupta, A. K. Das, and Y. Park, "ECC-EXONUM-eVOTING: A novel signature-based e-voting scheme using blockchain and zero knowledge property," *IEEE Open Journal of the Communications Society,* vol. 5, pp. 583-598, 2023.

[7] Y. Wu and S. Kasahara, "Smart contract-based E-voting system using homomorphic encryption and zero-knowledge proof," in *Proceedings of the International Conference on Applied Cryptography and Network Security*, 2023.

[8] U. Jafar, M. J. Ab Aziz, Z. Shukur, and H. A. Hussain, "Empowering secure and cost-efficient blockchain electronic voting by optimized ZK-SNARK algorithm," in *Proceedings of the 2023 International Conference on Electrical Engineering and Informatics (ICEEI)*, 2023.

[9] H. V. L. Pereira, "Efficient AGCD-based homomorphic encryption for matrix and vector arithmetic," in *Proceedings of the Applied Cryptography and Network Security, Cham*, M. Conti, J. Zhou, E. Casalicchio, and A. Spognardi, Eds., 2020.

[10] M. Woda and Z. Huzaini, *Use of ECC to secure blockchain-based e-voting system in dependability and complex systems*. Cham: Springer, 2021.

[11] K. K. Kamal, S. Gupta, P. Joshi, and M. Kapoor, "A secure and efficient mobile ID framework for authentication with enhanced ECC," *International Journal of System of Systems Engineering,* vol. 14, no. 5, pp. 461-479, 2024.

[12] D. Chaum and T. P. Pedersen, *Wallet databases with observers in advances in cryptology—CRYPTO'92*. Berlin, Heidelberg: Springer, 1992.

[13] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung, *Multi-authority secret-ballot elections with linear work," in advances in cryptology – EUROCRYPT'96*. Berlin, Germany: Springer, 1996.

[14] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *Annals of Internal Medicine,* vol. 151, no. 4, pp. 264-269, 2009. https://doi.org/10.7326/0003-4819-151-4-200908180-00135

[15] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*. New York, NY, USA: Springer-Verlag, 2004.

[16] T. Leppänen, C. Savaglio, and G. Fortino, "Service modeling for opportunistic edge computing systems with feature engineering," *Computer Communications,* vol. 157, pp. 308-319, 2020. https://doi.org/10.1016/j.comcom.2020.04.011

[17] Votem, "Blockchain voting platform [Whitepaper]," 2019. https://votem.com

[18] T. Nguyen and M. T. Thai, "zVote: A blockchain-based privacy-preserving platform for remote e-voting," in *ICC 2022-IEEE International Conference on Communications*, 2022: IEEE, pp. 4745-4750.

[19] S. M. Ratseev, "Some generalizations of Shannon's theory of perfect ciphers," *Vestnik Yuzhno-Ural'skogo Universiteta. Seriya Matematicheskoe Modelirovanie i Programmirovanie,* vol. 8, no. 1, pp. 111-127, 2015.

[20] C.-P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology,* vol. 4, no. 3, pp. 161-174, 1991.

[21] L. Vigano, "Automated security protocol analysis with the AVISPA tool," *Electronic Notes in Theoretical Computer Science,* vol. 155, pp. 61-86, 2006.

[22] B. Wang, F. Guo, Y. Liu, B. Li, and Y. Yuan, "An efficient and versatile e-voting scheme on blockchain," *Cybersecurity,* vol. 7, no. 1, p. 62, 2024. https://doi.org/10.1186/s42400-024-00226-8

[23] Y. Pengsen, "Quantum-resistant zero-knowledge proof blockchain electronic voting system," *Computer Fraud and Security,* vol. 2, pp. 958-981, 2025. https://doi.org/10.52710/cfs.606

[24] Votez, "Blockchain-based voting for enterprises," 2025. https://votez.com

[25] P. Choudhary and R. Vyas, "A critical study on disaster management and role of ICT in minimizing its impact," in Performance Management of Integrated Systems and its Applications in Software Engineering, M. Pant, T. K. Sharma, S. Basterrech, and C. Banerjee Eds. Singapore: Springer Singapore, 2020, pp. 183-187. https://doi.org/10.1007/978-981-13-8253-6_18

[26] J. Schweisgut, "Coercion-resistant electronic elections with observer," in *Proceedings of the Electronic Voting 2006–2nd International Workshop, Co-organized by Council of Europe, ESF TED, IFIP WG 8.6, and E-Voting. CC*, 2006.

[27] A. Kiayias and M. Yung, *The vector-ballot e-voting approach," in financial cryptography*. Berlin, Heidelberg: Springer, 2004.

[28] N. Nguyen and K. Nguyen-An, "A transparent scalable e-voting protocol based on open vote network protocol and zk-starks," in *International Conference on Intelligence of Things*, 2023: Springer, pp. 414-427.

[29] Y. Abuidris, R. Kumar, T. Yang, and J. Onginjo, "Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding," *Etri Journal,* vol. 43, no. 2, pp. 357-370, 2021.

[30] k. Vvedenie, *Under a general edition of V. V. Yashchenko*. Moscow: MTsNMO Publ, 2012.

[31] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proceedings of the Annual International Cryptology Conference*, 1991.

[32] M. A. Specter, J. Koppel, and D. Weitzner, "The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in {US}. federal elections," in *Proceedings of the 29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 1535-1553.

[33] Agora, "Blockchain voting for elections," Technical Whitepaper, 2018. https://agora.vote

[34] NetVote, "Open source voting platform using Ethereum blockchain," GitHub Repository, 2025. https://github.com/netvote

[35] S. Panja, S. Bag, F. Hao, and B. Roy, "A smart contract system for decentralized borda count voting," *IEEE Transactions on Engineering Management,* vol. 67, no. 4, pp. 1323-1339, 2020.

[36] Polyas, "Certified online voting system," 2025. https://www.polyas.com

[37] A. Rodríguez-Pérez, "My vote, my (personal) data: Remote electronic voting and the general data protection regulation," in *Proceedings of the International Joint Conference on Electronic Voting*, 2020.

[38] Scytl, "Secure electronic voting solutions: Technical overview," 2025.