Abstract. E-voting is a kind of election in which voters use digital ballots to present their civil rights, and e-voting gradually becomes an essential need for every organization and nation. There are some requirements in the e-voting process: confidentiality, integrity, authentication, and privacy of ballot. As a result, conducting an e-voting protocol is an important task to ensure the security requirements for e-voting process. In the previous works, researchers have proposed some properties of an esoteric e-voting protocol. The result of analyzing existed protocols shows that these protocols do not fully match properties of the esoteric protocol yet. In this paper, a new protocol which can meet requirements better than the formers is proposed.

Keywords: E-voting · Protocol · Cryptography

1 Introduction

According to The National Democratic, in 2012, recent research has shown that 31 countries around the world have used non-remote electronic voting machines (EVMs) for binding political elections at some point. Some of these countries have experimented with EVMs and then decided not to continue with their use, in some cases after using them for many years. EVMs are being used in 20 countries, with six of these countries still piloting the technology. Globally, very different trends are seen in different regions. Europe and North America can be seen as moving away from the use of EVMs [12], while South America and Asia show increasing interest in using electronic voting technologies [5].

What is e-voting? What vital properties the e-voting protocol need?

E-voting is a kind of election in which voters use digital ballots to present their civil rights, and e-voting gradually becomes an essential need for every organization and nation. There are some requirements in the e-voting process: confidentiality, integrity, authentication, and privacy of ballot [7]. As a result, conducting an e-voting protocol is an important task to ensure the security requirements for e-voting process.

In [13], Schneier proposed properties of the esoteric e-voting protocol with 9 properties: (i) Only authorized voters can vote; (ii) No one can vote more than once; (iii) No one can determine for whom anyone else voted; (iv) No one can duplicate anyone else’s vote; (v) No one can change anyone else’s vote without being discovered; (vi) Every voter can make sure that his vote has been taken into account in the final tabulation; (vii) Everyone knows who voted and who did not; (viii) The voter may change his mind (i.e., cancel his ballot and vote again) for a predetermined period of
time; (ix) If a voter finds that his vote has been counted wrongly, he can file a protest. With the 8th and 9th property are additional properties. There was some proposed protocols such as Simple voting protocol #1, Simple voting protocol #2, Voting with a single central facility using Blind signature [2], Voting with two central facilities Nurmi, Salomaa-Satin [11], Voting with two central facilities Fujioka, Okamoto-Ohta [6]. It can be seen that each protocol has its own advantages and disadvantages; however, all of them have the same disadvantage that is not to fully match the esoteric protocol’s properties. In this paper, a new protocol which can meet requirements better than the formers is proposed. In fact, besides the security requirements, when developing an e-voting system, we also consider other ones such as: system resources, performance, and the importance of election or financial capacity. There are many e-voting protocols in the world, however, each country or organization needs its own e-voting protocol and system depending on their need and capability. Hence, the development e-voting protocol and its system remain a topical and controversial issue in all countries and organizations in over the world. The rest of paper is organized as follows: in the second section, we analyze the advantages and disadvantages of some existed protocols, and then we propose a new protocol for e-voting process. We next describe the results of applying this protocol and assessing the security of the protocol. And the final is the conclusion.

2 Analyze Some Existed Protocols

In this section, we first briefly analyze some existed protocols, then compare these protocols with the esoteric protocol.

Traditional elections: This protocol was shown in, in which, the Central Election Commission (CEC) prepares a list of voters. The voters show their identification cards to register, then they receive ballots which they sign on, choose the desired candidates, and finally, put their ballot into the ballot box. The CEC counts the votes and announces the result. Advantage: invalid voters are restricted to vote; no one can vote more than once; no one can determine for whom anyone else voted; no one can substitute anyone else’s vote, and no one can change anyone else’s vote without being discovered. Disadvantage: the members of the election committee cannot vote in the polling places; cameras can be installed in the polling places; the committee-man can invalidate the ballots; the result can be distorted; it takes much time to count votes; the voters cannot determine whether their votes were counted, and voters do not know who voted and who did not.

Simple Voting protocol #1: In the Simple Voting protocol #1 [2], the CEC has a pair of keys (a private key and a public key). After selecting the options, the voter encrypts their ballot by the CEC’s public key and sends them. Receiving the encrypted ballots from the voter, the CEC decrypts these ballots by their private key to get the original ballot, then counts the votes and announces the result. This protocol is rife with problems. The CEC (Central Election Commission) has no idea where the votes are from, so it does not even know if the votes are coming from eligible voters. It has no idea if eligible voters are voting more than once. Furthermore, no one can change
anyone else’s vote, but no one would bother trying to modify someone else’s vote when it is far easier to vote repeatedly for the result of your choice.

Simple Voting Protocol #2: In the Simple Voting Protocol #2 [2], both the CEC and voters have a pair of keys. The CEC gives a public list of eligible voters. The voters register by announcing their public key to Certification Authority to achieve an ID to vote. The voter choose their candidates, and signs on the ballot by their private key, then encrypts all ballot and signature by the CEC’s public key. The CEC decrypts this message by his private key, and verifies the signature on the ballot by the voter’s private key. Last, the CEC counts and publishes result. This protocol satisfies properties one and two of the esoteric protocol (Only authorized voters can vote and no one can vote more than once). Each vote is signed by a voter’s private key, so the CTF knows who voted, who didn’t and how often each voter voted. No one can determine for whom anyone else voted by using CTF’s public key to encrypt and sign on the ballot. However, encrypting the votes with the CTF’s public key prevents anyone from eavesdropping on the protocol and figuring out who voted for whom, but the voters have to trust the CTF completely.

Voting with two central facilities Nurmi, Salomaa-Satin: Voting with 2 central facilities Nurmi, Salomaa-Satin is illustrated in detail in [11]. Here, the registry announces a list of eligible voters. When legal voter registers to vote, they will be sent a unique $M$ label. The voter creates a symmetric key $k_{secr}$ to encrypt both $M$ and ballot, then send anonymously these encrypted files ($M$ and ballot) to the committee. After voting process is completed, the committee will publish encrypted $M$ and ballot. The voter sends anonymously $k_{secr}$ to the committee, the committee will decrypt to receive the ballot. Finally, the committee counts and publishes the results. The protocol has almost all the properties of the esoteric protocol without the third property. Also, this one matches additional properties (8 and 9).

Voting with two central facilities Fujioka, Okamoto-Ohta: The protocol [6] can avoid collusion between the registry and the counter by using blind signature. Both the registry and the voter own each pair of keys which are verified by certification authority. The list of valid voters is published by the registry. The voter creates a symmetric key $k_{secr}$ and chooses his options on his ballot. Then he encrypts the ballot by $k_{secr}$. At this time, the voter uses a blind factor and the registry’s public key to hide the encrypted ballot content, all of which is blindly signed by the voter. The registry receives ID of the voter, blind encrypted ballot, and the blind signature of the voter $DS_{i,bl}$. Subsequently, the registry verifies the valid blind signature, and resign on the blind encrypted ballot $DS_{r,bl}$, and send to the voter. Then the voter unblinds to achieve the registry’s signature on the encrypted ballot and sends them to the committee with label $M$. the next steps is similar to the Voting with 2 central facilities Nurmi, Salomaa-Satin. If the voter does not reveal his identity, the seventh property can be matched. No one can compare simultaneously $DS_{en}$, $DS_{i,bl}$ and $DS_{r,bl}$ also ID and $M$ except the voter, so the choice of the voter is not revealed.

Voting with Blind Signature: The protocol is based on using blind signature [2] but it is applied for e-voting such as Voting with two central facilities Fujioka, Okamoto-Ohta and Sensus [9], this protocol is applied for label $M$ to ensure the anonymity of voter (property 3). The process of voting with blind signature is similar to Voting with two central facilities Fujioka, Okamoto-Ohta; however, there is only a
committee participating in the protocol and the voter sends the committee a encrypted file including label $M$, digital signature and ballot, which are against the alteration of the ballot. The protocol matches most of the esoteric protocol’s properties except for property 7. Table 1 gives the comparison between the existed protocols and the esoteric protocol, so it can be seen that these protocols do not have enough features to effectively implement an actual election. Therefore, it is necessary to develop a new protocol to meet all properties of the esoteric protocol. It is a goal of the paper to describe a new protocol which can satisfy the esoteric protocol. The security of this protocol is the very security of blind signature algorithm on Elliptic curve [13].

<table>
<thead>
<tr>
<th>Esoteric properties</th>
<th>Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Traditional</td>
</tr>
<tr>
<td>1. Only authorized voters can vote</td>
<td>+</td>
</tr>
<tr>
<td>2. No one can vote more than once</td>
<td>+</td>
</tr>
<tr>
<td>3. No one can determine for whom anyone else voted</td>
<td>+</td>
</tr>
<tr>
<td>4. No one can manipulate anyone else’s vote</td>
<td>−</td>
</tr>
<tr>
<td>5. No one can change anyone else’s vote without being discovered</td>
<td>−</td>
</tr>
<tr>
<td>6. Every voter can make sure that his vote has been taken into account in the final tabulation</td>
<td>−</td>
</tr>
<tr>
<td>7. Everyone knows who voted and who did not</td>
<td>+</td>
</tr>
<tr>
<td>8. The voter may change his mind (i.e., cancel his ballot and vote again) for a predetermined period of time</td>
<td>−</td>
</tr>
<tr>
<td>9. If a voter finds that his vote has been counted wrongly, he can file a protest</td>
<td>−</td>
</tr>
</tbody>
</table>

3 A New Proposed Protocol

The urgent need to develop a new e-voting protocol leads to the creation of a special data protection mechanism. Therefore, we need to build a set of solutions to protect data in all period: transmission, processing, and storage. Hence, developing the new protocol involves 3 sub-tasks, such as: (i) Encrypt transmitted data; (ii) Integrity of
information; (iii) Security of election process. Because the transmitted data is blocked, as well as due to the good points of block cipher feedback mode and based on comparison in [3, 4] we should select the cipher feedback mode system to protect the transmitted date and AES algorithm [1]. To protect the communication between Server and Client, the paper proposes the output feedback mode (OFB) which is safer than basic mode [8]. Then the data encryption mode is created by these basics. To solve the integrity of information, we implement Digital signature technique to authenticate users, system’s objects; to verify the data origin and to verify the reliability of the channel communication and not to repudiate the data origin. Based on the analyzing the data integrity verification algorithms, the paper choose the digital signature based on Elliptic Curve followed by GOST standard in [14]. There are following details:

+ Elliptic curve modulus, is prime number, satisfying the inequality $p > 2^{255}$;
+ Elliptic curve $E$ defined by coefficients $a$ and $b$, belonging to $GF(p)$;
+ Integer $m$ is an elliptic curve $E$ point group order;
+ Primer number $q$ is an order of a cyclic subgroup of the elliptic curve $E$ points group, which satisfies the following conditions:

$$m = nq, n \in \mathbb{Z}, n \geq 1$$

$$2^{254} < q < 2^{256}$$

+ Point $P \neq O$ of an elliptic curve $E$, with coordinates $(x_p, y_p)$, satisfying the equality $qP = O$.
+ Hash function maps the messages represented as binary vectors of arbitrary finite length onto binary vectors of a 256-bit length.

Every user of the digital signature scheme must have his personal keys:

+ Signature key, which is an integer $d$, satisfying the inequality $0 < d < q$;
+ Verification key, which is an elliptic curve point $Q$ with coordinate $(x_q, y_q)$, satisfying the equality $dP = Q$.

Digital signature generation for message $M$ is performed the following algorithm [14]:

1. Calculate the message hash code $M : \tilde{h} = h(M)$;
2. Calculate an integer $\epsilon$, binary representation of which is the vector $\tilde{h}$, and determine $e \equiv \epsilon (mod q)$. If $e = 0$, then assign $e = 1$.
3. Generate a random (pseudorandom) integer $k$, satisfying the inequality: $0 < k < q$;
4. Calculate the elliptic curve point $C = kP$ and determine if $r \equiv x_c (mod q)$, where $x_c$ is $x$-coordinate of the point $C$. If $r = 0$, return to step 3.
5. Calculate the value: $s \equiv (rd + ke)(mod q)$. If $s = 0$, return to step 3.
6. Calculate the binary vectors, corresponding to $r$ and $s$, and determine the digital signature $\zeta = (\tilde{r} \parallel \tilde{s})$ as a concatenation of these two binary vectors.

To verify digital signatures for the received message $M$, it is necessary to perform the following steps, by using verification key $Q$ [14]:

1. Calculate the integers $r$ and $s$ using the received signature $\zeta$. If the inequalities $0 < r < q$, $0 < s < q$ hold, go to the next step. Otherwise, the signature is invalid.
2. Calculate the hash code of the received message $M$: $\bar{h} = h(M)$.
3. Calculate the integer $z$, the binary representation or which is the vector $\bar{h}$, and determine if: $e \equiv z \pmod{q}$. If $e = 0$, then assign $e = 1$. 
4. Calculate the value $v \equiv e^{-1} \pmod{q}$.
5. Calculate the values: $z_1 \equiv sv \pmod{q}$, $z_2 \equiv -rv \pmod{q}$;
6. Calculate the elliptic curve point $C = z_1P + z_2Q$ and determine if: $R \equiv x_c \pmod{q}$, where $x_c$ is $x$-coordinate of the point $C$.
7. If the equality $R = r$ holds, then the signature is accepted. Otherwise, the signature is invalid.

The correctness of scheme is proved:

$$C = se^{-1} \pmod{q}P - re^{-1} \pmod{q}Q, \quad R = x_c \pmod{q}, \quad R \equiv r \quad (1.1)$$

Digital signature scheme ensures the integrity of data and allows tracing errors in intentional and unintentional situations. Besides, to solve the confidentiality of the vote’s ballot, the paper proposes blind signature protocol in the election process [2]. Based on the analysis of available algorithms, we choose the digital signature on the Elliptic Curve. And we modify these algorithms to meet the requirements of blind signature. To ensure three above analyzed requirements and to fully match the properties of the esoteric protocol, the proposed applying blind signature e-voting protocol is described below. We illustrate the process of the e-voting protocol based on the blind signature on Elliptic Curve and explain it using the following steps. The definitions of used notations are given in the Table 2.

**Table 2.** The notations and its definitions in the e-voting protocol based on the blind signature on elliptic curve.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k_{i, pub}$</td>
<td>The voter’s public key</td>
</tr>
<tr>
<td>$k_{i, priv}$</td>
<td>The voter’s private key</td>
</tr>
<tr>
<td>$k_{secr}$</td>
<td>The voter’s secret key</td>
</tr>
<tr>
<td>$B$</td>
<td>A ballot</td>
</tr>
<tr>
<td>$D_{S_i}$</td>
<td>Digital signature of the voter</td>
</tr>
<tr>
<td>$sign(x)$</td>
<td>The function of signature generation</td>
</tr>
<tr>
<td>$unsign(x)$</td>
<td>The function of signature verification</td>
</tr>
<tr>
<td>$encrypt(x)$</td>
<td>Encryption function</td>
</tr>
<tr>
<td>$decrypt(x)$</td>
<td>Decryption function</td>
</tr>
<tr>
<td>$m$</td>
<td>The encrypted ballot</td>
</tr>
<tr>
<td>$m'$</td>
<td>The blind ballot</td>
</tr>
<tr>
<td>$s'$</td>
<td>The blind signature of the registry on $m'$</td>
</tr>
<tr>
<td>$s$</td>
<td>The unblind signature of registry on $m$</td>
</tr>
<tr>
<td>$f(x)$</td>
<td>The reverse function</td>
</tr>
</tbody>
</table>
There are following details of the proposed e-voting protocol based on the blind signature on Elliptic Curve:

1. First, the voter prepares his own ballot, then encrypts the ballot by his private key to get the cipher text $m$. Next, he sends $m$ and his own signature to the registry.
2. The registry verifies received signature whether it belongs to registered voter. If this voter has not voted yet, registry will create number $k$ (where $0 < k < q$). Then he calculates the point $R' = kP$, and sends the voter the coordinate of the point $R' = (x_{R'}, y_{R'})$.
3. The voter chooses the random number $a < q$, then calculates the point $R = aR' = akP$ and the first component of the signature $r = x_{R'} \mod q$; the mask $\beta = \frac{f(x_{R})}{f(y_{R'})} \mod q$ and the value $m' = a\beta^{-1}f(m) \mod q$. Then he sends the registry $m'$.
4. The registry signs the received values to get his signature $s' = (df(x_{R'}) + km')$ and sends $s'$ for the voter.
5. The voter unblinds $s'$ to gain $s = s' \beta \mod q$, and decrypted ballot, and the signed values by the registrar $(m, (r, s))$.
6. Next, the voter sends $(m, (r, s))$ for the counter to count the ballot and to publish the election result.
7. The counter verifies the registry’s signature on the encrypted ballot, if valid, they sends the voter a receipt which becomes a evidence of listing ballot and being available for decrypting. The following steps of the signature verification: calculates the point $R = f(m)^{-1}(sP - f(r)Q)$ and if the equality $x_{R} = r$ holds, the signature is valid. Indeed, if replacing 2 parameters $s$ and $Q$ in the verifiable equality, we achieve:

$$
R = f(m)^{-1}(sP - f(r)Q) \\
= f(m)^{-1}P(df(x_{R}) + kzf(m)) - f(r)dPf(m)^{-1} \\
= f(m)^{-1}Pdf(r) + kzf(m)f(m)^{-1}f(r)Pd \\
= kxfP
$$

So, if the message was not changed and was signed by the owner of the key $d$, the equality $x_{R} \mod q = r$ is true.
8. After receiving the receipt, the voter provides the decrypt key to the counter. The counter decrypts the encrypted ballot by the key which the voter provided, and adds the result to the total election. At the end of process, the counter publishes the decrypt key with the ballot for the voter to check independently the result of e-voting.

The security of this protocol bases on the security of the logarithm on Elliptic Curve.
4 The Experimental Results of the Proposed Protocol

The contextual model of the experimental program involves the following steps: (1) The voter sends their identification to the registry; (2) The voter also sends their blinded ballot to the registry; (3) The registry verifies the valid of the voter’s identification and responds to the voter; (4) Then the registry signs the blinded ballot and sends this ballot back to the voter; (5) Next, the voter unblinds and obtains the registry’s signature on the ballot. Then, they send the ballot and the registry’s signature to the election committee; (6) The committee verifies the registry’s signature and sends the message to voter; (7) The committee counts the votes and publishes the result (Fig. 1).

5 Assessing the Security of the Proposed Protocol

To assess the security of the proposed protocol, the paper analyzes 2 main proposes of the e-voting process:

- Analyzing the cryptographic method applied to developing the e-voting protocol;
- Comparing the developed protocol with the esoteric protocol and analyzing the ability to overcome the risks of the e-voting system.

5.1 Analyzing the Cryptographic Method Applied to Developing the E-Voting Protocol

With a large key length (≥128 bit), AES can overcome basic attacks, such as brute force attack [8], the differential and linear attack. Therefore, it is necessary to choose AES. Digital signature on the Elliptic Curve is much more secure than RSA or Elgamal signature [10]. The security of digital signature on the ECC bases on the difficulty of
the analyzing integer into primes as well as the discrete logarithm in the algebraic systems. Now, there is no algorithm whose computing speed is smaller than the discrete logarithm on Elliptic Curve, the key length which goes down many times leads to faster speed. And the complexity of the algorithm is:

\[
O\left(\exp\left((c + o(1))(\ln p)^{1/3}(\ln \ln p^{2/3})\right)\right)
\]

So, the best choice for the data integrity is the digital signature on the Elliptic Curve. In the third task, the blind signature on the ECC is used to ensure the confidential of the ballot in the protocol. The blind signature scheme allows a person to sign a message without revealing any information of message and the signer only verify the blind signature without get any relation between the message and the signature. With the blind signature, the identification of the signature requester does not disclose.

5.2 Comparing the Developed Protocol with the Esoteric Protocol and Analyzing the Ability to Overcome the Risks of the E-Voting System

The paper analyses the proposed protocol base on each property of the esoteric protocol:

- Satisfying the property 1 and 7 of the esoteric protocol: In proposed protocol, register function is not built and the system creates an available voter database at the registry where information of the voter is filled up and an ID with the election status (“No” has not voted yet, “Yes” has voted) is given to the voter. Therefore, only the voter, who has the ID in database, has the right to vote. The registry can know who voted and who did not (matching property 1 and 7). With this property, the system can defend both the outside and inside users, who have no right to vote but connect the voters to sell the ballot.

- Matching the esoteric protocol’s property 2: When the voter has voted, the election status transforms from “No” into “Yes”. The system does not update the option of voter if happening two following cases: (1) The voter attempt to enter his ID; (2) The registry resets the voter’s status from “Yes” to “No” to vote again.

- Being content with the esoteric property 3: After the voter registers to vote, a blind ballot is sent to the Registrary, then they sign blindly on this ballot to prove the validity of this ballot. With the advantages of blind signature, the content of ballot is blinded, and the registry does not know whom the voter selects. And the committee receives only the encrypted ballot with the valid signature of the registry, so they only know the content of ballot.

- Filling the property 4 and 5: After the voter’s vote, the committee receives the encrypted ballot by the voters and the signature of the registry on this ballot. This ballot has a connection between the content of the ballot and the voter’s signature and the registry’s signature, so if there is any modification of ballot, the voter’s signature alters, leading to change the registry’s one. This violates the integrity of the ballot.
– **Comparing with the property 6:** The voter selects candidates on the ballot and conducts the election, the result is updated to the committee, then the committee saves the result and posts on the website, and sends the voter identification card to prove that the ballot is counted. The voters can see their result on the website after the election ends. This matches the property 6.

– **Discussing with the property 8:** At the committee, there are some functions such as “add” and “delete” the ballot so the voters completely change their decision on the system, and update the status of election again from “Yes” to “No” at the registry side to conduct re-vote. Therefore, it is appropriate with the esoteric protocol’s property 8.

– **Being suitable for the property 9 of the esoteric protocol:** If there is any complaint about the election’s result, the committee completely cancels the result with the “cancel” function. To sum up, we can see that the proposed protocol which is the two central facilities based on the blind signature on the Elliptic Curve can fully meet the properties of the esoteric protocol in [13].

### 6 Conclusion

The paper analyzed some available e-voting protocols, and then proposed new e-voting protocol can fully meet properties of the esoteric one. The paper also presented some experimental results of applying the proposed protocol to develop e-voting system, as well as analyzed the security of this protocol. As a result, this protocol completely can be researched more detail to apply to the actual e-voting system.

### References