# Internet Voting Protocols: An Analysis of the Cryptographic Operations per Phase

Cristina Satizábal [1], Rafael Páez[2]

[1]LACSER (Laboratory for Advanced Computational Science and Engineering Research), Universidad Antonio Nariño, Colombia
[2] SiDRe, Pontificia Universidad Javeriana, Colombia

***Abstract*:** Internet voting is a good option for Colombia thanks to the expansion of mobile technology throughout the country and the interest of the government to implement the e-voting. For this reason, we study the e-voting protocols to establish if any of them is suitable for Colombian elections. However, some of them imply a great number of cryptographic operations and therefore a great computational cost for the devices, which sometimes exceed their capacity. In this paper, we determine the number of cryptographic operations per phase of four e-voting protocols: one based on blind signatures (Li, Hwang and Lai protocol), one based on mix nets (Meng protocol), one based on homomorphic encryption (EVIV protocol) and one used in real electoral processes (I-Voting for Estonian Elections). Then, we analyze the changes in the number of operations when the number of voters, number of votes, number of authorities and number of candidates increase for small, medium and large elections. Finally, we establish the protocol that imply a less number of cryptographic operations and is suitable for big electoral processes, such as congress elections in Colombia.

***Keywords*:** Cryptographic operations, e-voting systems, Internet voting protocols, protocol phases, security.

## 1. Introduction

Nowadays, the interest for Internet voting systems has grown due to their benefits such as to vote from any place through different types of devices. In Colombia, this type of voting system is a good option, thanks to the great expansion of mobile technology throughout the country and the interest of the government to implement the electronic voting [1]. However, people mistrust the security of these systems. For this reason, many authors have designed e-voting protocols that include different security features. Since, all e-voting protocols include cryptographic operations to add security features to the system, the entities involve in an electoral process must have some computational capacity to carry out these operations on time. In Colombia, this is important, because the voting and counting processes must be carried out the same day of the election, so it is necessary to determine if the designed protocols, in addition to include the security features, can be implemented easily or they require an extremely great computational capacity. Thus, in this paper, the number of cryptographic operations per phase of four Internet voting protocols is analyzed to establish which of them implies a less number of cryptographic operations with a suitable level of security and determine if any is suitable for the different types of electoral processes in Colombia, especially for congress elections that imply around 36 millions of voters and more than 100 candidates, in order to create, in the future, an auditable and secure electronic voting system through Internet.

This paper includes the following sections: in section 2, we present the related work; in section 3, we explain the procedure carried out for the analysis and the notation used; section 4 contains the description of the four Internet voting protocols chosen for the analysis; section 5 includes the results obtained and their analysis; section 6 includes the appendices with the explanation of the phases of the four protocols using sequence diagrams; section 7 contains the conclusions; section 8 presents the acknowledgments; and the final section contains the references.

## 2. Related Work

There are basically three types of e-voting protocols. Some of them use blind signatures (this term is defined in [2]) to protect anonymity of votes, such as: [3] [4] [5]; other use mix-nets (this term is defined in [6]) to implement an anonymous channel or to cut the voter-vote link, such as:[7] [8]; and another use homomorphic encryption (this term is defined in [9]) to protect vote's privacy and increase the speed of vote tallying, such as: [10] [11] [12].

Many authors test specific security features of the e-voting protocols. For example, Cortier et al [13] review all the definitions of verifiability in the literature, compare them and obtain a general definition; Dreier, Lafourcade and Lakhnech [14] define a family of privacy notions and assess the level of privacy of several existing voting protocols to show that this model allows to compare them; Miramirkhani, Jalili and Yarmohamadi [15] prove by inductive analysis that the protocol FOO'92 guarantees eligibility.

Other authors create frameworks to evaluate the e-voting protocols, such as: Sampigethaya and Poovendran [16], that provide a framework and a set of metrics to compare the properties of voting schemes; Langer et al [17], that define different levels of election secrecy and verifiability so an appropriate level of the requirements can be selected for different types of elections; Smyth [18], that aids the secure design of cryptographic protocols and facilitates the evaluation of the properties of existing schemes because defines election verifiability, user-controlled anonymity and a procedure to automatically evaluate observational equivalence. However, none of the authors compare the number of cryptographic operations carried out by the different entities, that is the focus of this paper.

## 3. Notation and Method

To carry out the analysis of the Internet voting protocols, first the protocols were chosen. In the election of the protocols, we looked for protocols whose description comprises enough information on cryptographic operations carried out. Unfortunately, we found that many authors do

not specify step by step all the cryptographic operations of the protocols (such as: [7] [19] [20] [21]) or use a complicated notation that is difficult to understand (such as: [10] [12] [22]). In addition, we wanted to include the three types of e-voting protocols found literature, that is to say: based on blind signatures (Li, Hwang and Lai protocol [5]), based on mix-nets (Meng protocol [8]) and based on homomorphic encryption (EVIV protocol [11]). Also, we wanted to include at least one protocol used in real electoral processes and we found the protocol used in Estonian elections [23]. Thus, we chose the four Internet voting protocols cited in this paragraph. After protocol election, we established a notation to unify the way to describe the four protocols and their cryptographic operations. Table 1 shows the notation used in this paper.

Then, we describe the message sequence of each phase of the chosen protocols using the established notation and sequence diagrams (see Appendices in section 6). Finally, we count the number of cryptographic operations per phase and analysis the results obtained to determine: 1) if the computational cost is distributed among the phases, 2) if these protocols are suitable for large electoral processes, and 3) which of them has a better security level with a less number of cryptographic operations.

**Table 1.** Notation

| Notation | Description |
|---|---|
| $PK_i/SK_i$ | Public key/private key of entity i |
| $K_{i,j}$ | Secret key shared between entities i and j |
| Gen PK/SK | Asymmetric key pair generation |
| Gen K | Symmetric key generation |
| B | Blind signature of a message with factor r |
| $B^{-1}$ | Blinded removal |
| $E_{SK}$ | Encryption with private key |
| $D_{PK}$ | Decryption with public key |
| $E_{PK}$ | Encryption with public key |
| $D_{SK}$ | Decryption with private key |
| $E_K$ | Encryption with symmetric secret key |
| $E^{-1}_K$ | Decryption with symmetric secret key |
| h() | Hash operation |
| S | Secret sharing function |
| $S^{-1}$ | Secret sharing composing function |
| P | Proof of knowledge |
| vP | Verification of proof of knowledge |
| Σ | Homomorphic aggregation |
| Π | Homomorphic multiplication |
| Φ | Mix net operation |
| $CERT_i$ | Digital certificate of entity i |
| $PK_E/SK_E$ | Public key/private key of the election |
| ballot | Ballot without any mark |
| vote | Marked ballot |
| messages | Messages shared during the handshake of a SSL connection |
| rec | Voting receipt |
| N | Number of voters |
| k | Number of candidates |
| v | Number of votes (v≤N) |
| n | Number of authorities (trustees) |
| t | Threshold of trustees to decrypt a message using the shared private key |
| $ID_i$ | Identifier of entity i |
| $e\text{-mail}_i$ | E-mail of entity i |
| VL | Voters list |
| VVL | Voted voters list |
| VoL | Votes list |
| VVoL | Voters and votes list |
| CL | Candidates list |
| ReL | Results list |

## 4. Background

The protocols chosen for the analysis are described below in chronological order.

### 4.1 An Internet Voting Protocol with Receipt-Free and Coercion-Resistant by Meng

This voting protocol proposed in 2007 applies the encryption technologies: "*ElGamal cryptosystem, threshold ElGamal cryptosystem, mix net [24], homomorphic encryption, designated verifier proof [25], proof of knowledge that two cipher texts are encryption of the same plaintext [26], proofs of knowledge for equality of discrete logarithms [27], designated verifier proof of knowledge for equality of discrete logarithms [28]*" [8]. It has the properties of: privacy, completeness, soundness, fairness, invariableness, universal verifiability, receipt-free and coercion-resistant.

This protocol involves three entities:

- **Voter (V):** Person who wants to vote
- **Authorities (A1..n):** Entities that cooperate with the voter to construct an encryption of his/her vote and then computes the result of the election.
- **Bulletin Board (BB):** Place where the election information is published.

In addition, it includes four phases: preparation, registration, voting and tallying that are described in Appendix 6.1.

### 4.2 A Verifiable Electronic Voting Scheme over the Internet by Li, Hwang and Lai

This voting protocol was proposed in 2009. The authors "*use public cryptosystems to ensure the security of transmission on a public channel and blind signature technique to protect the private information*" [5]. It includes the features of: accuracy, simplicity, privacy, democracy, verifiability and uncoercibility. The responsibilities of the five participants are [5]:

- **Voter (V):** People who can participate in an election.
- **Certificate Authority (CA):** Registers each voter before the deadline of the election.
- **Authentication Centre (AC):** Verifies if each voter is registered with the CA or not. Then, it will transmit the receipt to the registered voters.
- **Supervisor Centre (SC):** Supervises all tasks of the election and verifies whether TC counts the ballots correctly or not.
- **Tally Centre (TC):** Collects the votes and tallies them. Only legal votes can be tallied.

This protocol comprises four phases: registering, authentication, voting and counting that are described in Appendix 6.2.

### 4.3 I-Voting System for Estonian Elections

The operation of this protocol was published in 2010 by Estonian National Electoral Committee (NEC) [29]. The properties that it includes are: eligibility, democracy, privacy, accuracy and fairness. According to [23], the roles of the system are fulfilled by three different servers:

- **Vote Forwarding Server (VFS):** Authenticates voters, distributes candidates' lists to voters and accepts the votes; VFS is available over the internet.
- **Vote Storing Server (VSS):** Stores votes and protects

their anonymity; VSS allows connections only from VFS.

- **Vote Counting Server (VCS):** Responsible for the tabulation process; VCS is offline all the time.

This protocol involves four phases: setup, voting, revocation and tabulation that are described in Appendix 6.3.

### 4.4 End-to-End Verifiable Internet Voting System (EVIV)

This protocol was proposed in 2013 and includes: completeness, accuracy, verifiability and privacy. The goal was to "*create a fully mobile End-to-End (E2E) verifiable Internet voting system that protects the voter's privacy from the vote casting PC*" [11]. To achieve this goal, EVIV combines a code voting protocol [30], to preserve the vote´s privacy from the vote casting PC, and the MarkPledge cryptographic voter's verifiable vote encryption technique [31] [32], to allow the voter can verify if his/her vote is cast and recorded-as-intended, performing a simple match of two small strings (4-5 alphanumeric characters). Additionally, EVIV uses verifiable homomorphic vote tally and a shared threshold ElGamal election key pair.

EVIV has four system players [11]:

- **Electoral Commission (EC):** Enrolls voters in the system and authenticates all election public data.
- **Voter (V):** Citizen with the right to vote.
- **Trustees (Tr):** Political parties and/or other authorized entity (e.g. a non-governmental organization).
- **Independent Organizations (IO):** Validates the correctness of the election public data.

This protocol is divided in four phases: voter enrolment, election registration, vote casting, and public verification and vote counting, that are described in Appendix 6.4.

In the Table 2, we summarize the features of the four protocols

**Table 2.** Features of the E-Voting Protocols

| Feature | Meng (2007) | Li, Hwang, Lai (2009) | I-Voting (2012) | EVIV (2013) |
|---|---|---|---|---|
| Democracy | | ✓ | ✓ | |
| Accuracy | | ✓ | ✓ | ✓ |
| Privacy | ✓ | ✓ | ✓ | ✓ |
| Completeness | ✓ | | | ✓ |
| Verifiability | ✓ | ✓ | | ✓ |
| Eligibility | | | ✓ | |
| Soundness | ✓ | | | |
| Fairness | ✓ | | ✓ | |
| Invariableness | ✓ | | | |
| Receipt-Free | ✓ | | | |
| Coercion Resistant | ✓ | ✓ | | |
| Simplicity | | ✓ | | |

## 5. Results and Discussion

Now, we are going to establish the number of cryptographic operations per phase of each voting protocol and analyse the results.

To determine the number of cryptographic operations, we consider all the operations carried out by each entity during the electoral process. Thus, although a voter carries out the process only once, the other entities can carry out their operations per voter. In addition, we take into account notation established in Table 1.

See in Table 3 the number of cryptographic operations per phase of the four Internet voting protocols, where the following abbreviations are used:

- **Ent:** Entity name
- **Op:** Type of cryptographic operation
- **#:** Number of operations

To establish how the number of cryptographic operations per phase changes with different number of voters (N), number of votes (v), number of candidates (k) and number of authorities (n), we elaborate Figure 8 to represent a small election (N=5,000, v=N/2, k=2, and n=2), Figure 9 to represent a medium election (N=500,000, v=N/2, k=10, n=5) and Figure 10 to represent a large election (N=50,000,000, v=N/2, k=100, n=10). In addition, to determine how the number of operations changes when the proportion of votes (v) increases respect to N, we elaborate Figure 11 with N=500,000, v=3N/4, k=10 and n=5. We establish v=N/2, because currently in Colombia, the abstentionism is around 50%.

In Meng protocol, the number of cryptographic operations depends on N, v and n (see Table 3). According to Figure 8, Figure 9 and Figure 10, registration (phase 2) and tallying (phase 4) involves the largest number of cryptographic operations, whereas preparation (phase 1) and voting (phase 3) implies less than 0.01% of the operations. In addition, the percentage of operations of the registration and tallying phases changes when the value of N, v and n increases. Thus, when N=5,000, v=N/2 and n=2 (see Figure 8), registration phase implies 60% of cryptographic operations whereas tallying phase involves 40% of them; when N=500,000, v=N/2 and n=5 (see Figure 9), registration phase implies 49.54% of cryptographic operations whereas tallying phase involves 50.46% of them; and when N=50,000,000, v=N/2 and n=10 (see Figure 10), registration phase implies 39.39% of cryptographic operations whereas tallying phase involves 60.61% of them. In addition, when N=500,000, v=3N/4 and n=5 (see Figure 11), registration phase implies 39.56% of cryptographic operations whereas tallying phase involves 60.44% of them. Therefore, in general, tallying phase implies more cryptographic operations than registration phase. In tallying phase, authorities carry out the most part of the cryptographic operations and $D_{PK}$ operations are the more numerous. Additionally, voting phase only implies that the voter carries out one $E_{PK}$ operation, so this is the least costly phase of all the four protocols. On the other hand, V (voter) participates in preparation, registration and voting phases and carries out the greatest number of its cryptographic operations in the registration phase.

The number of cryptographic operations of Li, Hwang and Lai protocol depends on N and v (see Table 3) and, according to Figure 8, Figure 9 and Figure 10, the authentication phase (phase 2) implies a larger number of cryptographic operations (50.01%) than the other phases (registering phase: 9.09%, voting phase: 36.36%, counting phase: 4.54%). However, when the proportion of votes increases to 3N/4 (see Figure 11), the percentage of cryptographic operations per phase changes slightly (registering phase: 6.25%, authentication phase: 51.56%, voting phase: 37.50% and counting phase: 4.69%). In authentication phase, AC (Authentication Centre) executes

the most part of the cryptographic operations of which $D_{PK}$ and $E_{SK}$ operations are the most numerous. In addition, V executes cryptographic operations in authentication and voting phases and carries out the greatest number of them in the authentication phase.

In I-voting protocol, the number of cryptographic operations also depends on N and v (see Table 3). Figure 8, Figure 9 and Figure 10 show that setup (phase 1) and voting (phase 2) involve a larger number of cryptographic operations (setup phase: 44.44%, voting phase: 44.45%) than the other phases (revocation phase: 7.41%, tabulation phase: 3.70%). When the proportion of votes increases to 3N/4 (see Figure 11), the percentage of cryptographic operations per phase changes (setup phase: 34.78%, voting phase: 52.17%, revocation phase: 8.70% and tabulation phase: 4.35%). Thus, voting phase implies the largest number of cryptographic operations. In this phase, VFS (Vote Forwarding Server) carries out the most part of the cryptographic operations of which Gen K, $E_K$ and $E^{-1}_K$ operations are the most numerous. In addition, V carries out cryptographic operations only in voting phase.

Finally, the number of cryptographic operations of EVIV protocol depends on N, v, n and k (see Table 3). Thus, the percentage of operations of the phases changes when the value of N, v, k and n increases. When N=5,000, v=N/2, k=2 and n=2 (see Figure 8), voter enrolment phase implies 8.33% of cryptographic operations, election registration phase 47.22%, vote casting phase 26.39% and public verification and vote counting phase 18.06%; when N=500,000, v=N/2, k=10, and n=5 (see Figure 9), voter enrolment phase implies 3.26% of cryptographic operations, election casting phase 27.72% and public verification and vote counting phase 33.15%; and when N=50,000,000, v=N/2, k=100, and n=10 (see Figure 10), voter enrolment phase implies 0.42% of cryptographic operations, election registration phase 29.50%, vote casting phase 28.46% and public verification and vote counting phase 41.62%. Therefore, whereas the percentage of voter enrolment (phase 1) and election registration (phase 2) phases tends to decrease, the percentage of vote casting (phase 3) and public verification and vote counting (phase 4) phases tends to increase. In addition, when N=500,000, v=3N/4, k=10 and n=5 (see Figure 11), voter enrolment phase implies 2.73% of cryptographic operations, election registration phase 30%, vote casting phase 34.77% and public verification and vote counting phase 32.50%. In this case, only the number of operations of vote casting phase tends to increase, and the others to decrease, compared to Figure 9. Even so, although the phase with the greatest growth is public verification and vote counting phase, on average, the phase that involves the largest number of cryptographic operations is election registration phase.

In this phase, the election registrar service of electoral commission (EC (ER)) executes the most part of the cryptographic operations of which $D_{PK}$ and vP operations are the most numerous. In addition, V participates in election registration, vote casting and public verification and vote counting phases, and carries out the greatest number of its cryptographic operations in the election registration phase.

## 6. Appendices

The phases of the four protocols are explained through sequence diagrams.

### 6.1 An Internet Voting Protocol with Receipt-Free and Coercion-Resistant by Meng

Meng protocol [8] includes three types of entities: Voter (V), Authorities ($A_{1..n}$), and Bulletin Board (BB); and four phases: Preparation (see Figure 12), Registration (see Figure 13), Voting (see Figure 1) and Tallying (see Figure 2).

We use the following notation to describe the phases of this protocol:

- **$A_i$:** ith authority
- **$c_{Ai}$:** Credential share generated by $A_i$ for voter
- **CV:** Credential of voter V
- **$PK_C/SK_C$:** Public and private key of threshold cryptosystem to encrypt and decrypt $c_{Ai}$
- **$PK_b/SK_b$:** Public and private key of threshold cryptosystem to encrypt and decrypt ballot and $c_{Ai}$
- **$PV_{Ai}$:** Non-interactive proof of knowledge that $E_{PKb}(c_{Ai})$ is encryption of the same $c_{Ai}$ produced by $A_i$ for V.
- **$A_{..n}$:** Other authorities
- **$()_{1..n}$:** Messages of all the authorities
- **$Re_{Ai}$:** Final tally of authority $A_i$
- **VoT:** Votes table
- **VT:** Voters table
- **VVoT:** Voters and votes table

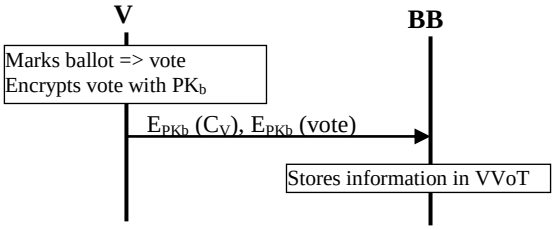


**Figure 1.** Meng Protocol: Voting Phase

### 6.2 A Verifiable Electronic Voting Scheme over the Internet by Li, Hwang and Lai

Li, Hwang and Lai protocol [5] includes five entities: Voter (V), Certificate Authority (CA), Authentication Centre (AC), Supervisor Centre (SC) and Tally Centre (TC) and four phases: Registering (see Figure 3), Authentication (see Figure 14), Voting (see Figure 15) and Counting (Figure 4).

The following notation is used to describe the phases of this protocol:

- **a:** Random number or fictitious name chosen by the voter
- **b:** Random number or identity name chosen by SC

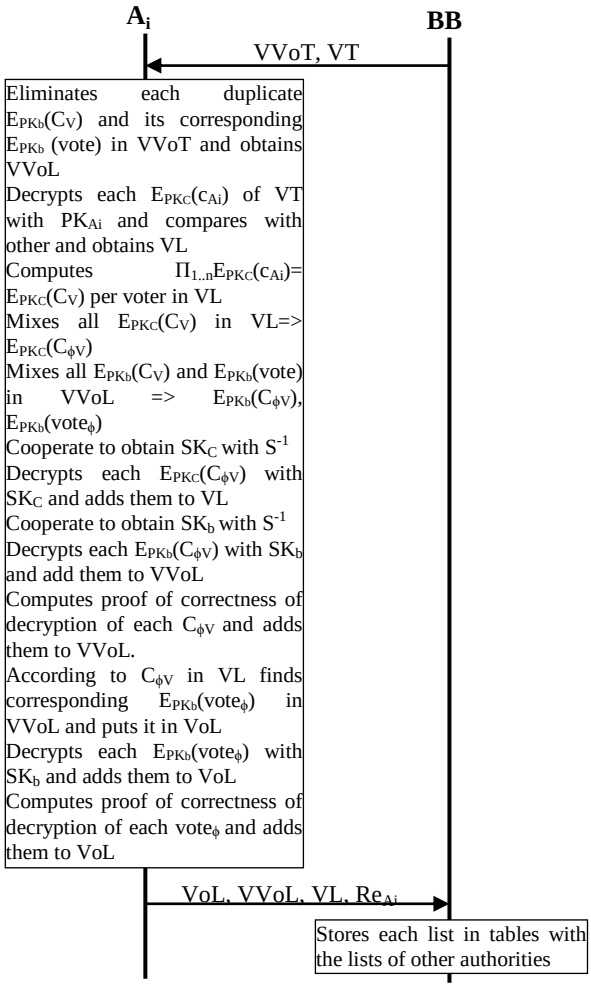


**Figure 2.** Meng Protocol: Tallying Phase

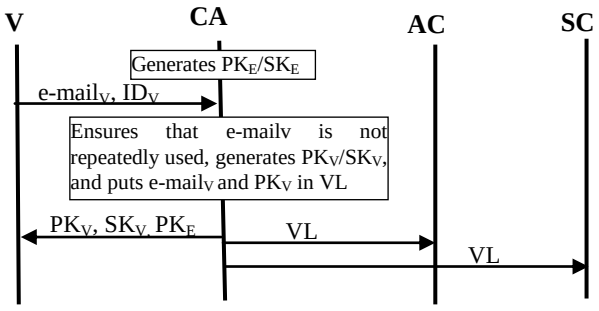


**Figure 3.** Li, Hwang and Lai Protocol: Registering Phase

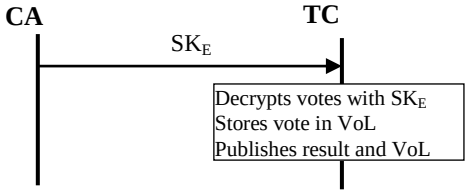


**Figure 4.** Li, Hwang and Lai Protocol: Counting Phase

### 6.3 I-Voting System for Estonian Elections

I-Voting protocol [23] includes three servers: Vote Forwarding Server (VFS), Vote Storing Server (VSS) and Vote Counting Server (VCS); and four phases: Setup (see Figure 16), Voting (see Figure 17), Revocation (see Figure 5) and Tabulation (see Figure 6).

"*Each voter belongs to one of 12 electoral districts. Each candidate has a unique candidate number and is registered to one electoral district. Only voters from the same district can vote for the candidate*" [23].

The system uses the following lists [29]:

- **CL:** It contains: constituency (electoral district), party (candidate number) and candidate (candidate name).
- **VL:** It contains: voter name, identity code ($ID_V$), constituency, polling division, certificate ($CERT^1_V$)
- **ReL:** It contains: constituency, party, candidate, votes (number of votes per candidate).
- **VVoL:** It contains: identity code ($ID_V$), constituency, polling division, encrypted and signed vote, certificate ($CERT^2_V$).
- **PVL:** Paper voters list. It contains: voter name, identity code ($ID_V$), constituency and polling division
- **VVL:** It contains: identity code ($ID_V$), constituency, polling division and digital signature of encrypted vote.

In addition, the following notation is used:

- **IVCA:** I-Voting Client Application
- **NCA:** National Certification Authority
- **HSM:** Hardware Security Module

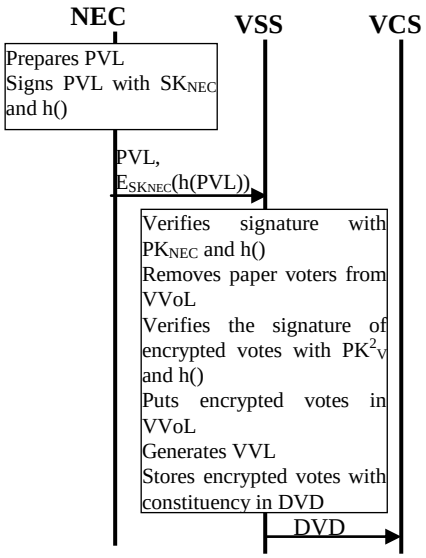


**Figure 5**. I-voting Protocol: Revocation Phase

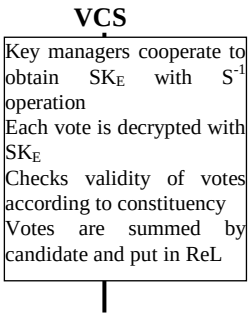


**Figure 6.** I-voting Protocol: Tabulation Phase

### 6.4 End-to-End Verifiable Internet Voting System (EVIV)

EVIV protocol [11] includes four system players: Electoral Commission (EC), voter (V), Trustees (Tr), Independent Organizations (IO) and four phases: Voter Enrolment (see Figure 7), Election Registration (see Figure 18), Vote

Casting (see Figure 19) and Public Verification and Vote Counting (see Figure 20).

Election registration phase is divided into two stages: election setup and ballot registration; vote casting phase is divided into two stages: vote casting initialization and vote casting; and public verification and vote counting phase is divided into three stages: election data verification, vote tally and vote tally verification.

According to [11], the EVIV architecture is constituted by:

- "***Enrolment Service (ES):*** *Responsible for the enrolment process of every voter.*
- ***Election Registrar (ER):*** *Allows voters to register for voting online on a particular election.*
- ***Ballot Box (BaB):*** *Provides the vote casting service on Election Day.*
- ***Bulletin Board (BB):*** *Responsible for the publication of all election public data.*
- ***Verification Service (VS):*** *Verifies the correction and validity of votes and receipts.*
- ***Voter Security Token (VST):*** *Responsible for the vote encryption and the voter's authentication by means of digital signature (the voter's private key is inside the VST).*
- ***Client Platform (PC):*** *PC or any other kind of interaction machine with a VST reader (e.g. mobile phone, PDA) together with the corresponding operating system and programs used by the voter during the vote protocol*".

In addition, in the description of the protocol, the following notation is used:

- **VL:** Electoral Roll or list of all voters´ certificates
- **BL:** Ballots list
- **RL:** Receipts list
- **Date:** Election date
- **p, q, g:** Election key pair parameters of ElGamal
- **codecard:** Card containing one vote code for each candidate and a single vote confirmation code.
- **RN:** Random number generated by trustees
- **eCh:** Election challenge generated by electoral commission
- **rec:** Verification codes for each candidate encryption
- **ballot:** Is comprised of k candidate vote encryptions ($cvote_{i,}$ i=1…k), in a random order, and the corresponding voteValidity proofs (generated with P function), where k is the number of candidates. Additionally, the ballot has a sumValidity data proving that there is only one YESvote entry in the ballot (ballot = $cvote_i|_1^k$ || $voteValidity|_1^k$ || sumValidity )
- **recVal:** Proofs of correct generation of the verification code of each candidate (receipt)
- **decProof:** Decryption proof of homomorphic vote aggregation

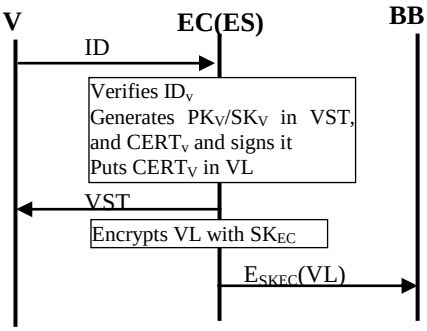


**Figure 7.** EVIV Protocol: Voter Enrolment Phase

## 7. Conclusions

Comparing the phases, we can see that all the protocols has four phases and the phases of registration, voting and counting are present in all of them, although the name of the phases changes slightly from one protocol to another.

The number of cryptographic operations of all the chosen protocols depends on N and v. In Meng protocol also depends on n and in EVIV protocol also depends on n and k.

In general, there is not a particular phase where the number of cryptographic operations of the four protocols is higher than the others, this depends on each protocol. Thus, in Meng protocol, the tallying phase involves, on average, 53% of cryptographic operations; in Li, Hwang, Lai protocol, the authentication phase implies approximately 50% of cryptographic operations; in I-Voting protocol, the voting phase involves, on average, 46% of cryptographic operations; and in EVIV protocol, the election registration phase implies, on average, 36% of cryptographic operations.

The entity in charge of the most part of cryptographic operations of the costliest phase of each protocol is always an authority ($A_i$ in Meng protocol; AC in Li, Hwang, Lai protocol; VFS in I-Voting protocol; and EC(ER) in EVIV protocol), that must have the enough computational and storage capacities to carry out all the operations in the shortest possible time.

Regarding to the distribution of computational load among the phases, in Meng protocol, the computational load is concentrated in the registration and tallying phases, and this increases in the tallying phase as N, v and n are increasing; while the cost of preparation and voting phases is insignificant; in Li, Hwang, Lai protocol, the authentication and voting phases are in charge of the most part of cryptographic operations although authentication phase implies more computational load, while counting phase is the least costly; in I-Voting protocol, setup and voting phases have distributed the most part of the computational load and tabulation phase implies the least computational cost; and in EVIV protocol, the computational load is distributed almost uniformly among election registration, vote casting and, public verification and vote counting phases, whereas voter enrolment phase implies the least computational load.

With regard to the type of cryptographic operations carried out in the costliest phases, in three of the protocols, $D_{PK}$ operations are among the most numerous.

In addition, the protocols that imply a less number of cryptographic operations are Li, Hwang and Lai protocol and I-Voting protocol, of which Li, Hwang, and Lai protocol has

the least number of cryptographic operations. On the other hand, the protocols that imply a larger number of cryptographic operations and are not suitable for big electoral processes are EVIV protocol and Meng protocol, of which EVIV protocol has the largest number of cryptographic operations.

Since in Colombia, the authentication, voting and counting phases must be carried out the same day of the election, we are interested in protocols where these phases imply a less number of cryptographic operations. Therefore, although of the four protocols, Li, Hwang and Lai protocol is the least costly, the authentication, voting and counting phases imply more than 90% of the cryptographic operations and includes democracy, accuracy, privacy, verifiability, coercion-resistant and simplicity features. On the other hand, we have I-Voting, used in Estonian Elections, where voting and tabulations phases imply between 48% and 56% of cryptographic operations and includes democracy, accuracy, privacy, eligibility and fairness features. Thus, of these two protocols, Li, Hwang and Lai protocol gives a better level of security although its phases are costliest. Therefore, we found that none of the protocols meets the requirements that a protocol should have for elections in Colombia, so we must design a new protocol with all the security features but the least possible number of cryptographic operations in authentication, voting and counting phases.

## 8. Acknowledgements

This work was supported by Universidad Antonio Nariño (Colombia) and belongs to the project "Auditable Secure Electronic Voting System Through Internet (ASEVSTI)".

## References

[1] Corporación Colombia Digital, "¿Estamos Cerca de Contar con el Voto Electrónico en Colombia?," https://colombiadigital.net/actualidad/noticias/item/9765-estamos-cerca-de-contar-con-el-voto-electronico-en-colombia.html, accessed 5 August 2017.

[2] N. Asghar, "A Survey on Blind Digital Signatures," University of Waterloo, pp. 1-31, 2012.

[3] J.-K. Jan, Y.-Y. Chen, Y. Lin, "The Design of Protocol for E-Voting on the Internet", IEEE 35th International Carnahan Conference on Security Technology, England, pp. 180-189, 2001.

[4] F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, A. Vaccarelli, "SEAS, A Secure E-Voting Protocol: Design and Implementation," Computers & Security, Vol 24, pp. 642-652, 2005.

[5] C.-T. Li, M.-S. Hwang, Y.-C. Lai, "A Verifiable Electronic Voting Scheme Over the Internet," 6th International Conference on Information Technology: New Generations, USA, pp. 449-454, 2009.

[6] O. Pereira, R. L. Rivest, "Marked Mix-Nets," Workshop on Advances in Secure Electronic Voting, Malta, pp. 1-17, 2017.

[7] M. Jakobsson, A. Juels, R. L. Rivest, "Making Mix Nets Robust for Electronic Voting by Randomized Partial Checking," 11th USENIX Security Symposium, USA, pp. 1-15, 2002.

[8] B. Meng, "An Internet Voting Protocol with Receipt-Free and Coercion-Resistant," IEEE 7th Int. Conf. on Computer and Information Technology, Japan, pp. 721-726, 2007.

[9] A. Acar, H. Aksu, , A. S. Uluagac, M. Conti., "A Survey on Homomorphic Encryption Schemes: Theory and Implementation," https://arxiv.org/abs/1704.03578, accessed 11 November 2017

[10] A. Huszti, "A Homomorphic Encryption-Based Secure Electronic Voting Scheme," Math. Debrecen, Vol. 79, No. 3-4, pp. 479-496, 2011.

[11] R. Joaquim, P. Ferreira, C. Ribeiro, "EVIV: An End-to-End Verifiable Internet Voting System," Computers & Security, Vol. 32, pp. 170-191, 2013.

[12] X. Zou, H. Li, Y. Sui, W. Peng, F. Li, "Assurable, Transparent and Mutual Restraining E-Voting Involving Multiple Conflicting Parties," IEEE Conference on Computer Communications (INFOCOM 2014), Canada, pp. 136-144, 2014.

[13] V. Cortier, D. Galindo, R. Küsters, J. Müller, T. Truderung, "SoK: Verifiability Notions for E-Voting Protocols," IEEE Symposium on Security and Privacy, USA, pp. 779-798, 2016.

[14] J. Dreier, L. Pascal, Y. Lakhnech, "A Formal Taxonomy of Privacy in Voting Protocols," 1st IEEE International Workshop on Security and Forensics in Communication Systems, Canada, pp. 6710- 6715, 2012.

[15] N. S. Miramirkhani, R. Jalili, M. Yarmohamadi, "FOO e-Voting Protocol: Inductive Analysis of the Eligibility Property," 9th International ISC Conference on Information Security and Cryptology, Iran, pp. 128-134, 2012.

[16] K. Sampigethaya, R. Poovendran, "A Framework and Taxonomy for Comparison of Electronic Voting Schemes," Computer & Security, Vol. 25, pp. 137-153, 2006.

[17] L. Langer, A. Schmidt, J. Buchmann,, M. Volkamer, A. Stolfik, "Towards a Framework on the Security Requirements for Electronic Voting Protocols," 1st International Workshop on Requirements Engineering for E-Voting Systems (Re-Vote'09), USA, pp. 1-8, 2009.

[18] B. Smyth, "Formal Verification of Cryptographic Protocols with Automated Reasoning," PhD Thesis, University of Birmingham, 2011.

[19] K. Butterfield, H. Li, X. Zou, F. Li, "Enhancing and Implementing Fully Transparent Internet Voting," 24th International Conference on Computer Communications and Networks (ICCCN), USA, pp. 1-6, 2015.

[20] P. Danielis, S. T. Kouyoumdjieva, G. Karlsson, "DiVote: A Distributed Voting Protocol for Mobile Device-to-Device Communication," 28th International Teletraffic Congress – The 1st International Conference in Networking Science &Practice, Germany, pp. 70-77, 2016.

[21] G. S. Grewal, M. D. Ryan, L. Chen, M. R. Clarkson, "Du-Vote: Remote Electronic Voting with Untrusted Computers," IEEE 28th Computer Security Foundations Symposium, Italy, pp. 155-169, 2015.

[22] Y. Zhou, Y. Zhou, S. Chen, S. S. Wu, "MVP: An Efficient Anonymous E-Voting Protocol," IEEE Global Communications Conference, USA, pp. 1- 7, 2016.

[23] S. Heiberg, P. Laud, J. Willemson, "The Application of E-Voting for Estonian Parliamentary Elections of 2011," Lecture Notes in Computer Science, Vol. 7187, pp. 208-223, 2012.

[24] C. Park, K. Itoh, K. Kurosawa, "Efficient Anonymous Channel and All/Nothing Election Scheme," Advances in Cryptology- EUROCRYPT'93, pp. 248-259, 1993.

[25] M. Jakobsson, K. Sako, R. Impagliazzo, "Designated Verifier Proofs and Their Applications," Lecture Notes in Computer Science, Vol. 1070, pp. 143-154, 1996.

[26] A. Acquisti, "Receipt-Free Homomorphic Elections and Write-in Voter Verified Ballots," https://eprint.iacr.org/2004/105.pdf, accessed 15 August 2017.

[27] G. R. Blakley, "Safeguarding Cryptographic Keys", International Workshop on Managing Requirements Knowledge AFIPS, Vol. 48, USA, pp. 313-317, 1979.
[28] J. Goulet, J. Zitelli, "Surveying and Improving Electronic Voting Schemes," http://www.seas.upenn.edu/~cse400/CSE400_2004_2005/34 writeup.pdf, accessed 10 August 2017
[29] Estonian National Electoral Committee (NEC), "E-Voting System, General Overview," http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf, accessed 23 August 2017
[30] R. Oppliger, "How to Address the Secure Platform Problem for Remote Internet Voting," 5th Conference on Sicherheit in Informationssystemen (SIS'02), Austria, pp. 153-173, 2002.
[31] C. A. Neff, "Practical High Certainty Intent Verification for Encrypted Votes," http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.134.1006&rep=rep1&type=pdf, accessed 6 September 2017.
[32] R. Joaquim, C. Ribeiro, "An Efficient and Highly Sound Voter Verification Technique and Its Implementation," Lecture Notes in Computer Science, Vol. 7187, pp. 104-121, 2012.

**Table 3** Number of Cryptographic Operations per Phase

| Protocol | Phase 1 | | | Phase 2 | | | Phase 3 | | | Phase 4 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Preparation | | | Registration | | | Voting | | | Tallying | | |
| | Ent | Op | # | Ent | Op | # | Ent | Op | # | Ent | Op | # |
| Meng (2007) | V | Gen PK/ SK | 1 | V | $E_{SK}$ | 1 | V | $E_{PK}$ | 1 | $A_i$ | $D_{PK}$ | nv |
| | | $D_{PK}$ | 1 | | $E_{PK}$ | 1 | | | | | $\Pi$ | v |
| | $A_{1..n}$ | Gen PK/ SK | 2+n | | $D_{SK}$ | n | | | | | $\phi$ | 3 |
| | | $E_{SK}$ | 1 | | vP | n | | | | | $D_{SK}$ | 3v |
| | | S | 2 | | $\Pi$ | 1 | | | | | P | 2v |
| | | | | $A_i$ | $D_{SK}$ | N | | | | $A_{1..n}$ | $S^{-1}$ | 2 |
| | | | | | $D_{PK}$ | N | | | | $A_{..n}$ | $D_{PK}$ | (n-1) nv |
| | | | | | $E_{PK}$ | 3N | | | | | $\Pi$ | (n-1)v |
| | | | | | P | N | | | | | $\phi$ | 3(n-1) |
| | | | | | $E_{SK}$ | N | | | | | $D_{SK}$ | 3(n-1) v |
| | | | | $A_{..n}$ | $E_{PK}$ | 3(n-1) N | | | | | P | 2(n-1) v |
| | | | | | P | (n-1) N | | | | | | |
| | | | | | $E_{SK}$ | (n-1) N | | | | | | |
| **TOTAL** | | | **7+n** | | | **3+2N+5 nN+2n** | | | **1** | | | **$2+n^2v$ +6nv+3 n** |
| | **Registering** | | | **Authentication** | | | **Voting** | | | **Counting** | | |
| | **Ent** | **Op** | **#** | **Ent** | **Op** | **#** | **Ent** | **Op** | **#** | **Ent** | **Op** | **#** |
| Li, Hwang, Lai (2009) | CA | Gen PK/ SK | 1+N | V | $E_{PK}$ | 3 | TC | $D_{PK}$ | 4v | TC | $D_{SK}$ | v |
| | | | | | B | 3 | | $D_{SK}$ | v | | | |
| | | | | | $E_{SK}$ | 2 | | $E_K$ | v | | | |
| | | | | | h() | 1 | | $E^{-1}{}_K$ | 2v | | | |
| | | | | | $D_{SK}$ | 1 | V | $D_{PK}$ | 1 | | | |
| | | | | | $B^{-1}$ | 3 | | h() | 1 | | | |
| | | | | | $D_{PK}$ | 4 | | Gen K | 1 | | | |
| | | | | AC | $D_{SK}$ | v | | $E_{PK}$ | 1 | | | |
| | | | | | $D_{PK}$ | 2v | | $E^{-1}{}_K$ | 1 | | | |
| | | | | | $E_{SK}$ | 2v | | $E_K$ | 2 | | | |
| | | | | | $E_{PK}$ | v | | | | | | |
| | | | | SC | $D_{SK}$ | v | | | | | | |
| | | | | | $D_{PK}$ | v | | | | | | |
| | | | | | $E_{SK}$ | 2v | | | | | | |
| | | | | | h() | v | | | | | | |
| **TOTAL** | | | **1+N** | | | **17+ 11v** | | | **7+8v** | | | **v** |
| | **Setup** | | | **Voting** | | | **Revocation** | | | **Tabulation** | | |
| | **Ent** | **Op** | **#** | **Ent** | **Op** | **#** | **Ent** | **Op** | **#** | **Ent** | **Op** | **#** |
| I-Voting (2010) | NCA | Gen PK/S K | 2N | V | $D_{PK}$ | 2 | NEC | $E_{SK}$ | 1 | VCS | $S^{-1}$ | 1 |
| | | $E_{SK}$ | 2+2N | | h() | 3 | | h() | 1 | | $D_{SK}$ | v |
| | | h() | 2+2N | | Gen K | 2 | VSS | $D_{PK}$ | 1+v | | | |
| | NEC | Gen PK/S K | 2 | | $E_{PK}$ | 2 | | h() | 1+v | | | |
| | | S | 1 | | $D_{SK}$ | 1 | | | | | | |
| | | $E_{SK}$ | 1 | | $E_K$ | 2 | | | | | | |
| | | h() | 1 | | $E^{-1}{}_K$ | 2 | | | | | | |
| | VFS | Gen PK/S K | 1 | | $E_{SK}$ | 1 | | | | | | |
| | | | | VFS | $D_{PK}$ | v | | | | | | |
| | | | | | h() | v | | | | | | |
| | | | | | $D_{SK}$ | v | | | | | | |
| | | | | | Gen K | 2v | | | | | | |
| | | | | | $E_{PK}$ | v | | | | | | |
| | | | | | $E^{-1}{}_K$ | 2v | | | | | | |

| Protocol | Phase 1 | | | Phase 2 | | | Phase 3 | | | Phase 4 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | $E_K$ | 2v | | | | | | |
| | | | | VSS | $D_{PK}$ | v | | | | | | |
| | | | | | h() | v | | | | | | |
| **TOTAL** | | | **10+ 6N** | | | **15+ 12v** | | | **4+2v** | | | **1+v** |
| | **Voter Enrolment** | | | **Election Registration** | | | **Vote Casting** | | | **Public Verification and Vote Counting** | | |
| | **Ent** | **Op** | **#** | **Ent** | **Op** | **#** | **Ent** | **Op** | **#** | **Ent** | **Op** | **#** |
| | EC (ES) | Gen PK/SK | N | V | $D_{SK}$ | 1 | V | $D_{SK}$ | 1 | EC | ∑ | 1 |
| | | h() | N | | $E_K$ | 2 | | $E_K$ | 2 | | $E_{SK}$ | 2 |
| | | $E_{SK}$ | 1+N | | $E^{-1}{}_K$ | 3 | | $E^{-1}{}_K$ | 3 | | $D_{PK}$ | 1 |
| | | | | | $D_{PK}$ | 4 | | $D_{PK}$ | 4 | | vP | 1 |
| | | | | | $E_{PK}$ | 2k | | P | k | IO (VS) | $D_{PK}$ | 2 |
| | | | | | P | k | | $E_{SK}$ | 1 | | $E_{PK}$ | kN+ kv |
| | | | | | $E_{SK}$ | 1 | EC (BaB) | $D_{PK}$ | 2v+n | | $E_{SK}$ | 2+v |
| **EVIV (2013)** | | | | EC (ER) | $E_{SK}$ | 4+N | | h() | 1+v+n | | vP | 1+kN+k v |
| | | | | | $D_{PK}$ | 4N+n | | $E_{SK}$ | 2+v | | ∑ | 1 |
| | | | | | h() | N | | Gen K | v | Tr | $D_{PK}$ | 1 |
| | | | | | Gen K | N | | $E_{PK}$ | v+2kv | | $S^{-1}$ | 1 |
| | | | | | $E_{PK}$ | N | | $E^{-1}{}_K$ | 2v | | $D_{SK}$ | 1 |
| | | | | | $E^{-1}{}_K$ | 2N | | $E_K$ | 3v | | P | 1 |
| | | | | | $E_K$ | 3N | | vP | 2kv | | $E_{SK}$ | 1 |
| | | | | | vP | 2kN | Tr | h() | 2n | V | $D_{PK}$ | 1 |
| | | | | Tr | $D_{PK}$ | 1 | | $E_{SK}$ | 2n | | | |
| | | | | | Gen PK/SK | 1 | | $D_{PK}$ | n | | | |
| | | | | | S | 1 | | | | | | |
| | | | | | $E_{SK}$ | n | | | | | | |
| **TOTAL** | | | **1+3N** | | | **18+ 13N +2kN +2n +3k** | | | **14+ 11v+ 4kv +7n +k** | | | **17+ 2kN +v +2kv** |

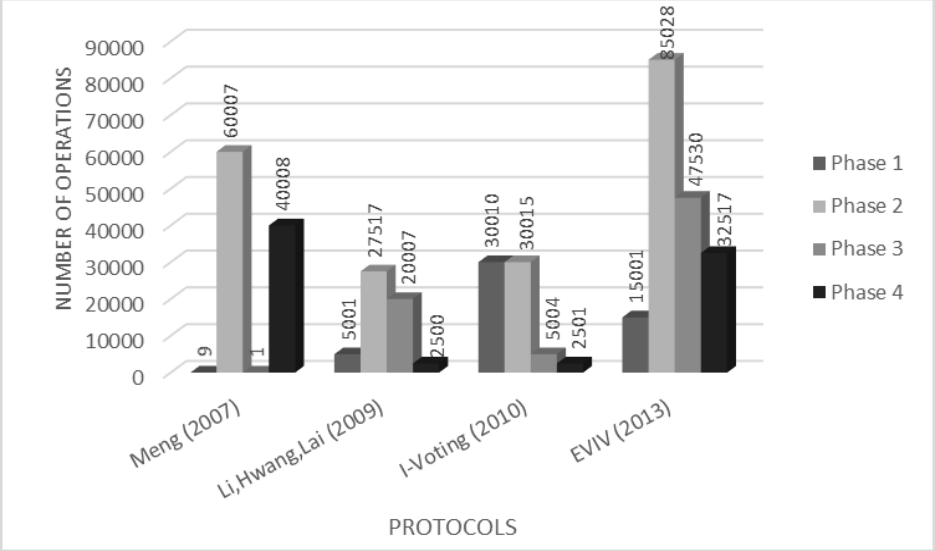


**Figure 8.** Number of Cryptographic Operations per Phase (N=5,000, v=N/2, k=2, n=2)

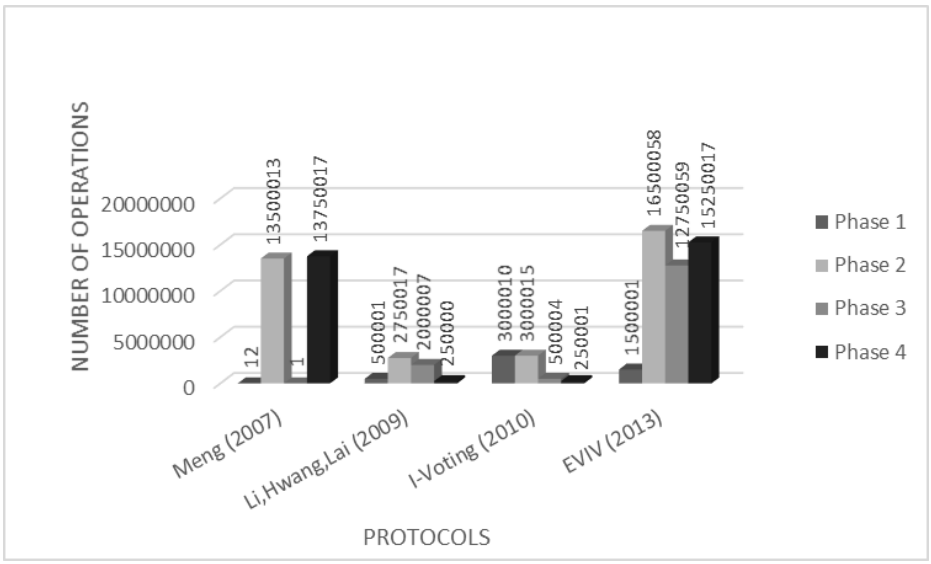


**Figure 9.** Number of Cryptographic Operations per Phase (N=500,000, v=N/2, k=10, n=5)

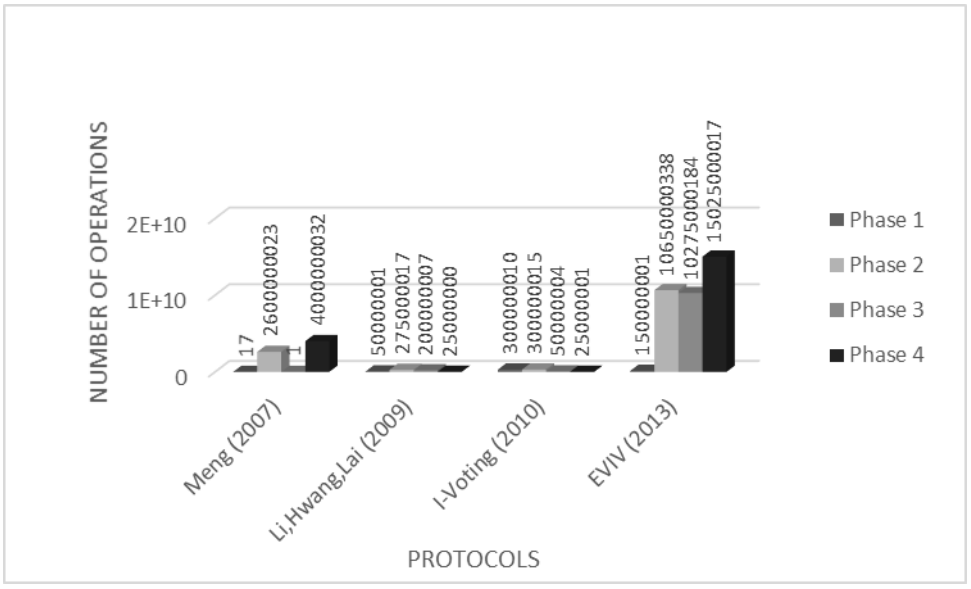


**Figure 10.** Number of Cryptographic Operations per Phase (N=50,000,000, v=N/2, k=100, n=10)

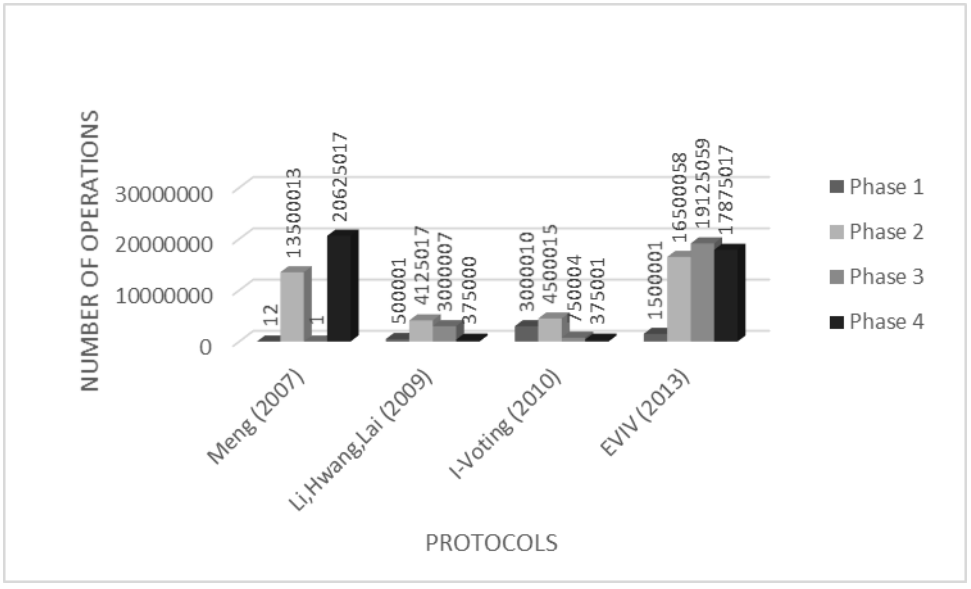


**Figure 11.** Number of Cryptographic Operations per Phase (N=500,000, v=3N/4, k=10, n=5)

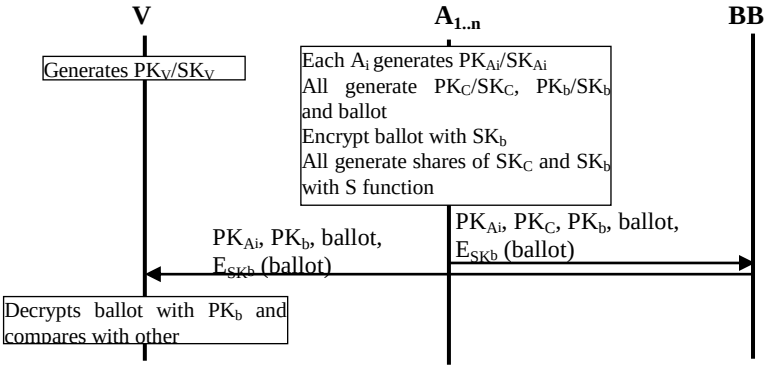


**Figure 12.** Meng Protocol: Preparation Phase

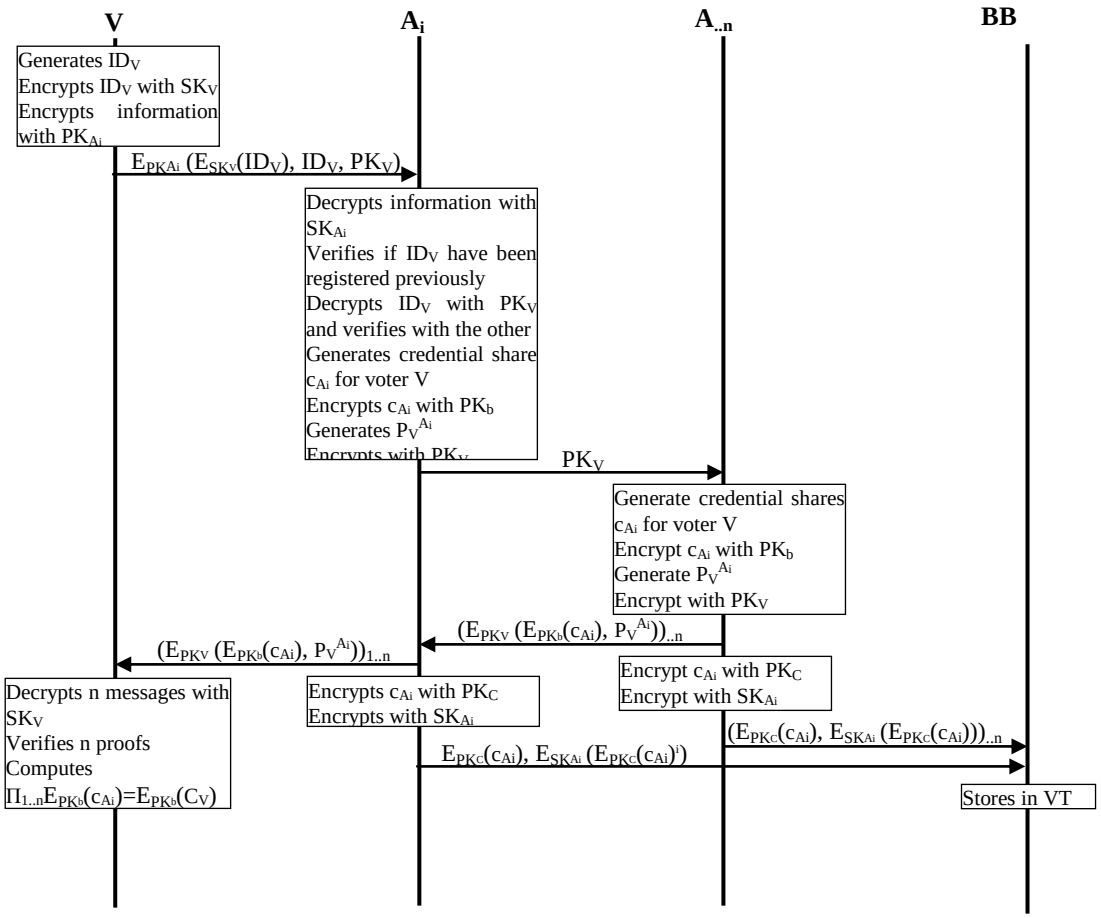


**Figure 13.** Meng Protocol: Registration Phase

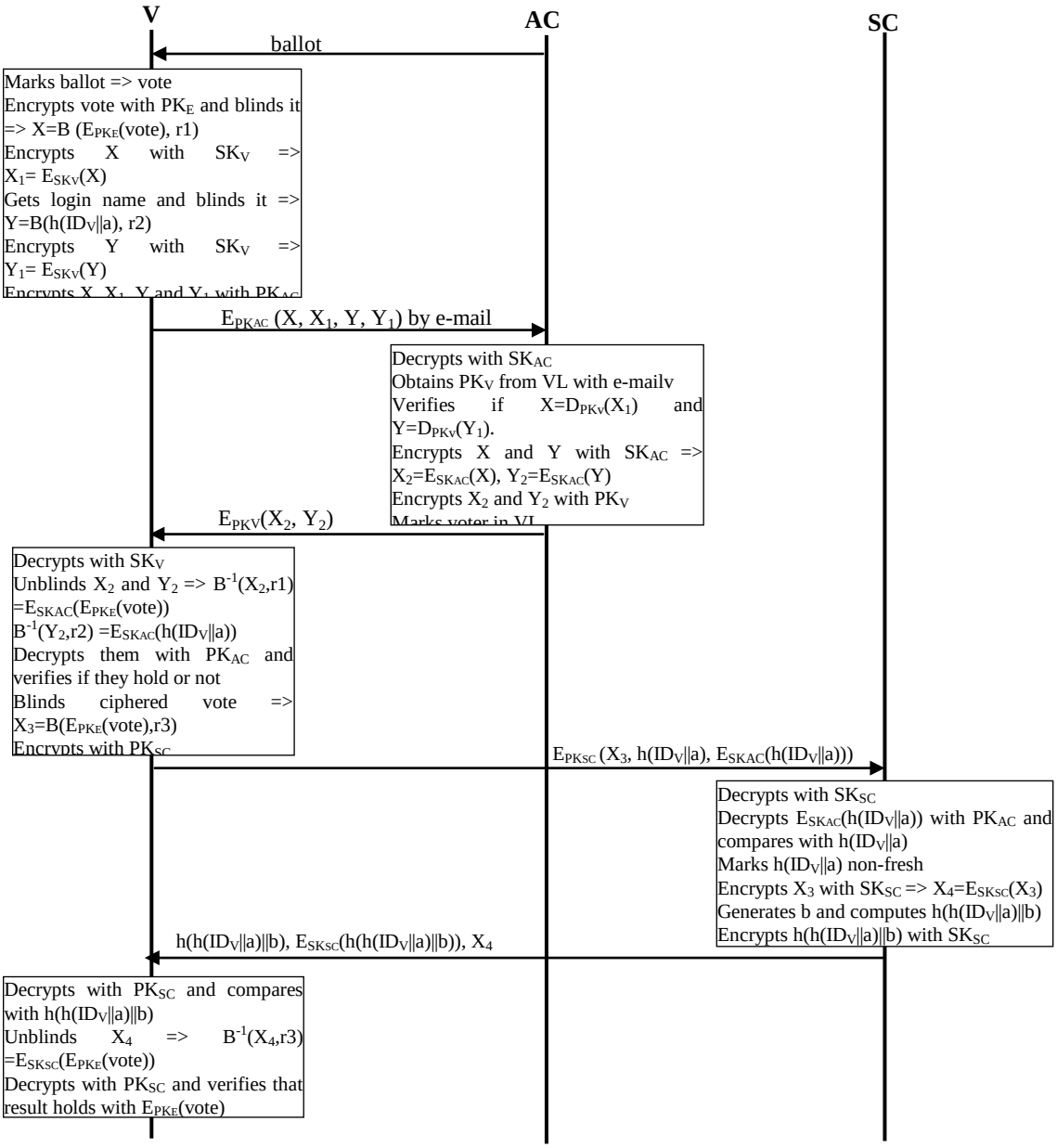


**Figure 14.** Li, Hwang and Lai Protocol: Authentication Phase

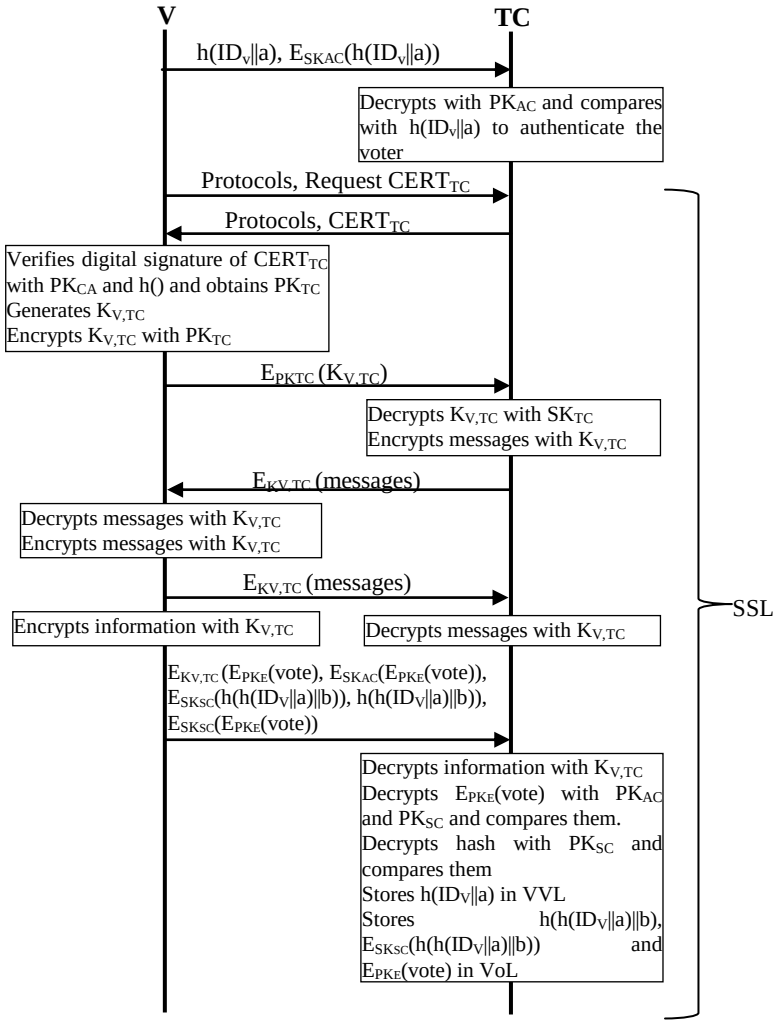


**Figure 15.** Li, Hwang and Lai Protocol: Voting Phase

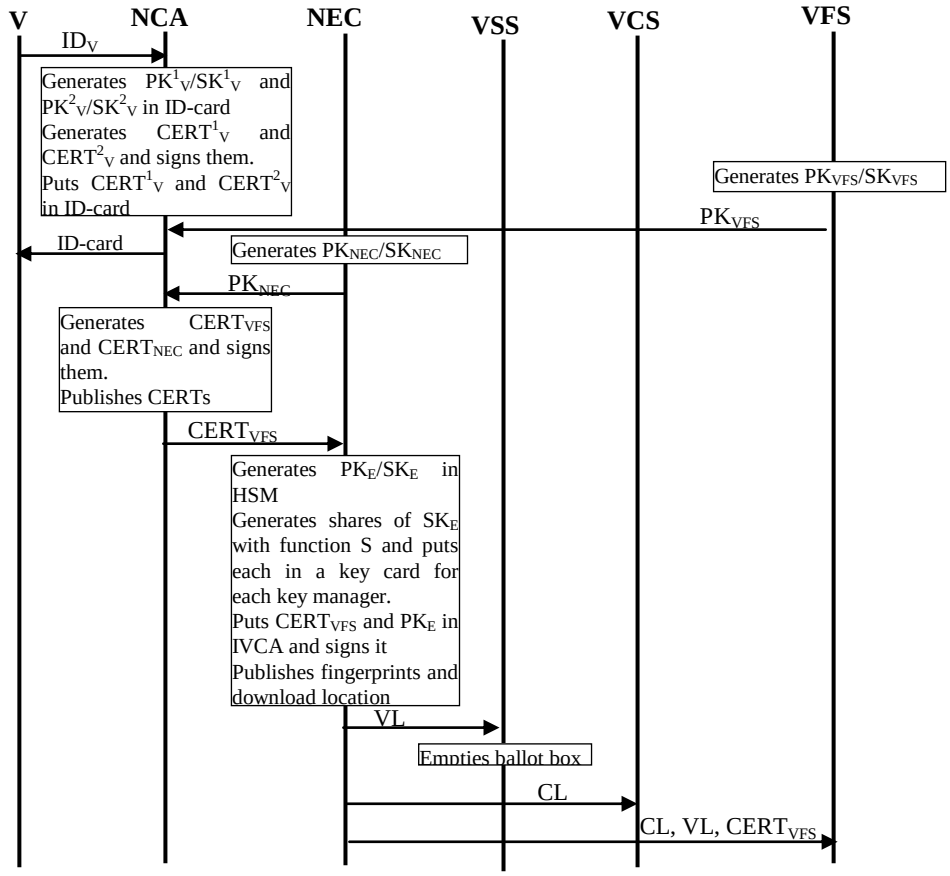


**Figure 16.** I-voting Protocol: Setup Phase

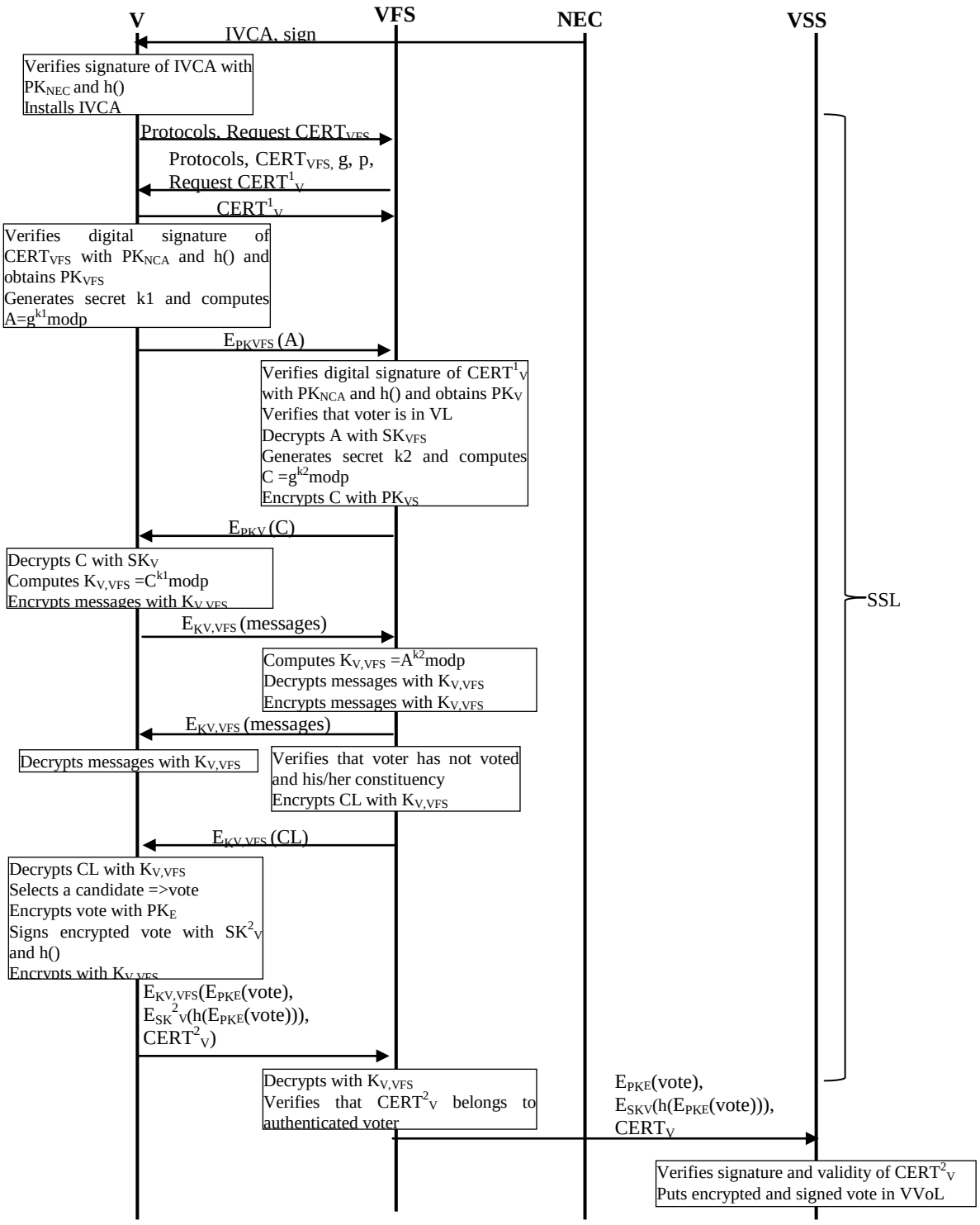


**Figure 17.** I-voting Protocol: Voting Phase

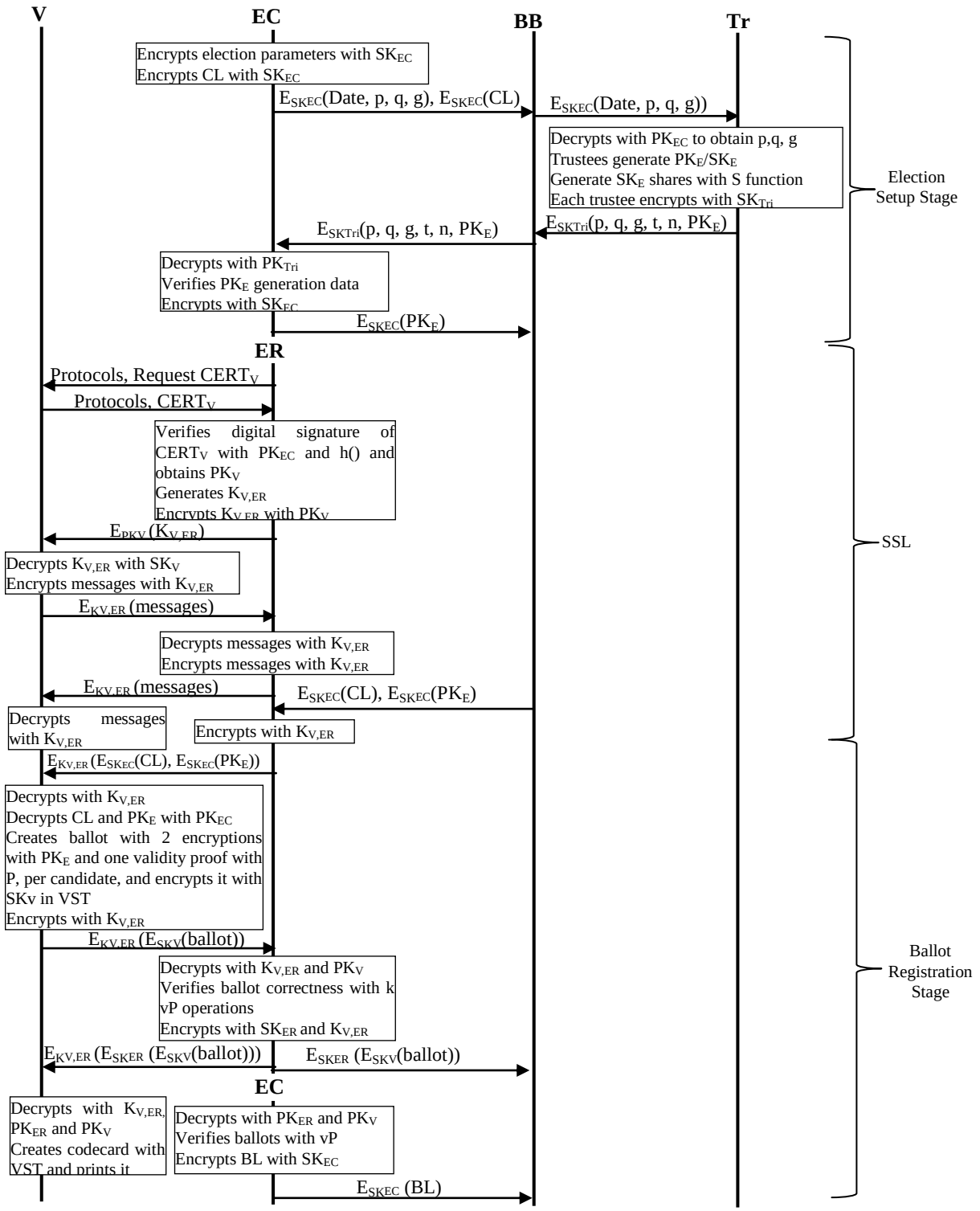


**Figure 18.** EVIV Protocol: Election Registration Phase

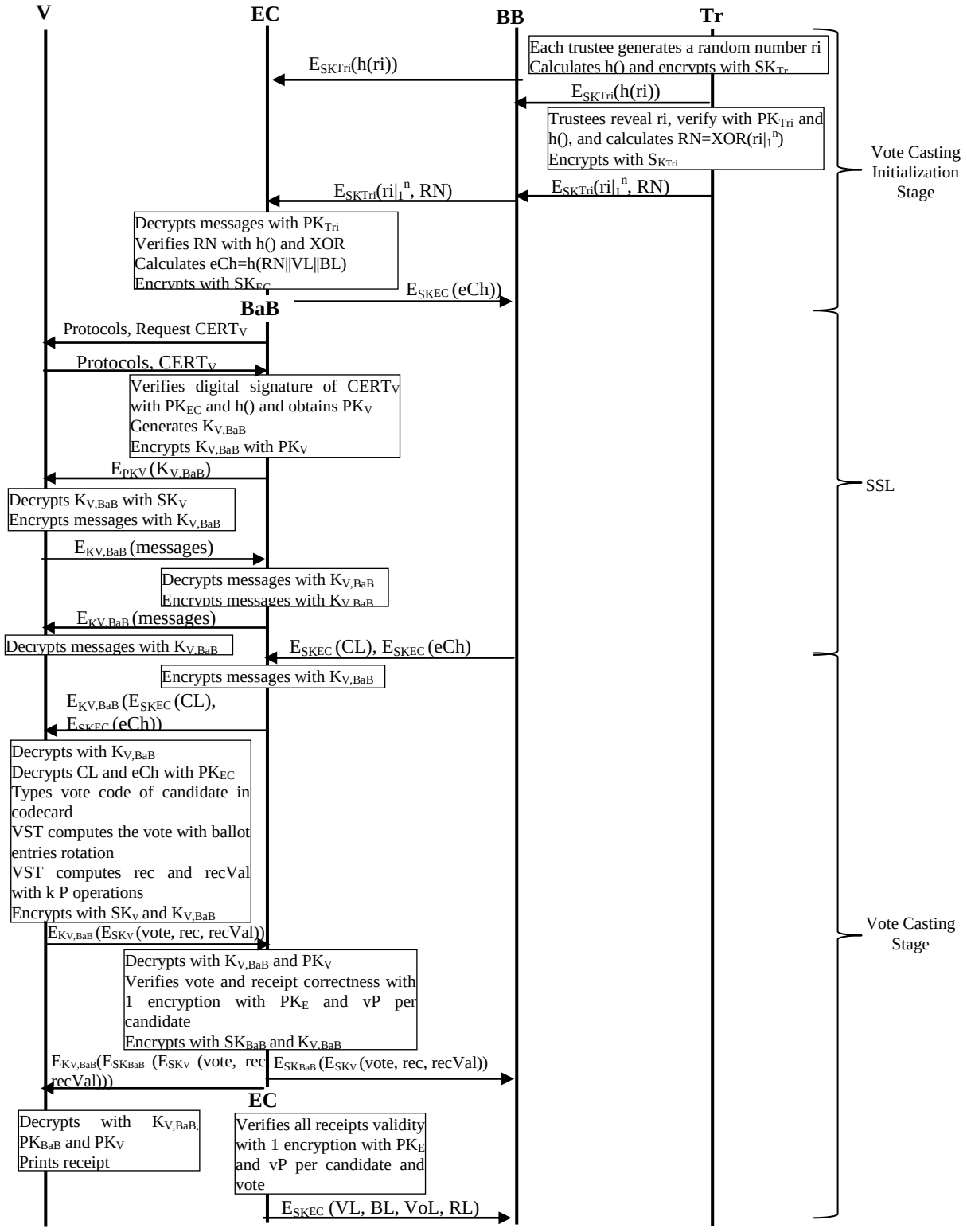


**Figure 19.** EVIV Protocol: Vote Casting Phase

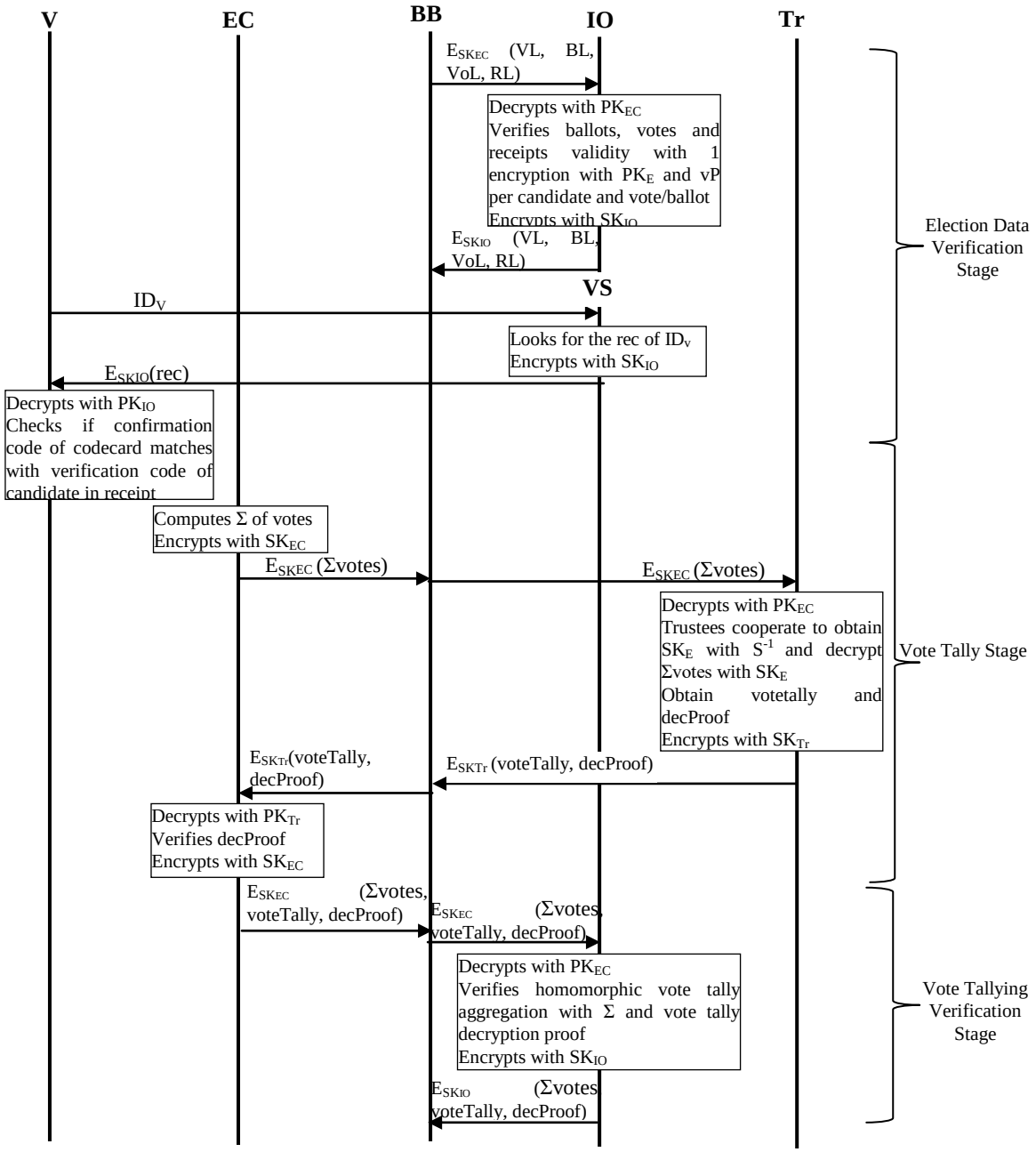


**Figure 20.** EVIV Protocol: Public Verification and Vote Counting Phase