Filling the Gap between Voters and Cryptography in e-Voting

Wei Han, Dong Zheng, Ke-fei Chen
Dept. of Computer Sci. & Eng., Shanghai Jiaotong University

Abstract: Cryptography is an important tool in the design and implementation of electronic voting schemes for it provides the property of verifiability, which is not provided in the traditional voting. But in the real life, neither can most voters understand the profound theory of cryptographic e-voting nor can they perform the complicated cryptographic computation. An e-voting system is presented in this paper to leverage the use of cryptography between theory and practice. It combines the advantages of Moran-Naor's voting scheme and voting schemes based on homomorphic encryption. It makes use of cryptographic techniques, but it hides the details of cryptographic computation from voters. Voters can be convinced that the ballot is cast as intended. The tally can be verified in public. Compared with Moran-Naor's voting scheme, the new system has three advantages: the ballots can be recovered when the voting machine breaks down, the costly cut-and-choose zero-knowledge proofs for shuffling votes made by the voting machine are avoided and the partial tally result in each voting machine is kept secret.

Key words: electronic voting, homomorphic commitment, homomorphic encryption, threshold decryption

1. Introduction

Electronic voting will replace the traditional paper-based voting in the near future. There has been a large amount of research in this area. Some experts focus on the design of the reliable voting machine, which is often called "Direct Recording Electronic" (DRE) machine. Others engage in the design of e-voting protocols by using cryptographic tools. The cryptographic e-voting schemes can be mainly classified into three categories: voting based on anonymous channels such as mix-net [1][2][3], voting based on blind signature [4] and voting based on homomorphic encryption [5][6][7]. Voting based on homomorphic encryption does not need the complicated construction of anonymous channels so it is the most efficient.

Although many cryptographic voting schemes have been proposed, they only guarantee that the ballots are counted as cast. To guarantee that the ballot is cast as intended, voters must verify that each step of the complicated cryptographic protocol is strictly executed. However, most voters are not familiar with cryptography, and they only have highly constrained computation ability. So it is difficult for average voters to perform the verification. To solve this problem, Chaum presented a voting scheme based on visual cryptography [8]. Mix-net is employed so his scheme is not efficient. In addition, special print device is required. Neff presented a voting scheme called "MarkPledge" [9]. In this scheme the verification work is separated into two parts. The voter only needs to compare some strings in the voting booth, and the rest of complicated cryptographic computation can be carried out by any third party outside the voting booth. The voter is ensured that her ballot is cast as intend and the tally is counted as cast if both parts of the verification succeed. Inspired by Neff's scheme, Moran and Naor presented a simpler voting scheme [10] with the same advantage. In Moran-Naor's scheme[1] when a voter enters the voting booth, she chooses a candidate on the DRE. The DRE makes commitments to the candidate chosen by the voter. If the voting machine is honest, it can always open the commitments according to the challenge given by the voter. To hide the voter's choice the voting machine and the voter jointly simulate pairs of challenges and answers for other candidates. When the voter leaves the voting booth, the DRE prints a receipt for the voter. The voter only has to make sure that she gave the challenge for the real candidate after the DRE committed, and the challenges printed on the receipt match what she gave. The rest of verification can be made according to information on the receipt by any trusted third party outside the voting booth. The voter is convinced that her ballot is cast as intended after the receipt passes the verification. When the tally begins the DRE shuffles ballots stored in the memorizer and discloses the content. The receipts in Neff's scheme and Moran-Naor's scheme leaks no information on the voter's choice, since the receipts are both constructed on the idea that a simulated zero-knowledge proof is indistinguishable from a real zero-knowledge proof.

In this paper a voting system is designed to combine the advantages of Moran-Naor's scheme and voting schemes based on homomorphic encryption. It solves the hard problem of the ballot restoration in Moran-Naor's scheme. It also improves the efficiency and simplifies the design of the DRE.

The rest of the paper is organized as follows: in section 2 some building blocks of the new voting system are introduced. In section 3 the implementation of the voting system is presented. In section 4 the voting system is analyzed and compared to Moran-Naor's scheme. In section 5 some concluding remarks is given.

2 Preliminaries

Security requirements. A voting protocol should satisfy the security requirements below:

Eligibility: Only eligible voters can participate in the election, and each eligible voter can cast a single vote.

Privacy: The content of an individual ballot is kept secret. Only the final tally result is published.

Verifiability: The validity of the individual ballot and the tally process can be verified. When any passive third party can also verify the ballot cast and the tally, this property is called universal verifiability. Voting based on blind signature is not universal verifiable, but the other two categories of voting protocols satisfy the universal verifiability.

Robustness: The voting protocol can tolerate corrupt voters and dishonest authorities to some extent.

Fairness: The partial results of the tally should not be exposed prior to the end of the voting phase.

Receipt-freeness: The voter cannot convince others how she casts a ballot. This property is

[1] The authors of [10] presented a generic voting protocol and a concrete implementation based on Pedersen commitment. They claimed that the security proof of the generic protocol would be published in the full version. The full version is not published yet. So in this paper when we talk about Moran-Naor's scheme we only indicate the concrete implementation in [10].

crucial to thwart voting buying and coercion.

System model. Our voting system is designed to be used in a traditional setting, in which voters cast their ballots in a private voting booth. We assume a 1-out-of-L election, that is, the voter chooses one candidate from a setting of L candidates. In the election there are four entities: voter, DRE, registration authority and tallying authority. Before the election starts the voter must go to a registration authority to register her identity. Then the voter enters a voting booth, and casts her ballot on a DRE. The DRE encrypts the ballot and publishes the ciphertext on the bulletin board. There are l tallying authorities. We assume that at least t of them remain honest. When the voting phase ends, t tallying authorities jointly aggregate and decrypt the final tally result.

Encoding votes. We denote by M a strict upper bound on the number of voters. We represent candidates with numbers $0,...,L-1$ and encode a vote on candidate i as M^i. Tallying such encoded votes gives us an M-addic representation of the result, $\sum_{i=0}^{L-1} v_i M^i$, where v_i is the number of votes on candidate i.

System parameters. We assume that the message space of the threshold homomorphic encryption used in our voting system is Z_N for a suitable $N > M^L$ to avoid overflow. We define l_V as the maximal bit length of a vote. We assume that the distribution of the randomizer space of the cryptosystem is to pick a random l_R-bit randomizer. Similarly for the integer commitment we pick a random l_r-bit number as the randomizer. We need some extra security parameters. We use a cryptographic hash function that outputs an l_e-bit number e. l_e=160 may be sufficient. We use a security parameter l_s, such that for any value a we have that $a + r_a$ and r_a are indistinguishable, where r_a is a random $|a| + l_s$ -bit number. In practice l_s=80 will be fine.

Homomorphic integer commitment. Examples of homomorphic integer commitment can be found in [11], [12] and [13]. The homomorphic property is $com(m_1 \oplus m_1^{'},...,m_n \oplus m_n^{'}; r \odot r^{'}) = com(m_1,...,m_n; r) \otimes com(m_1^{'},...,m_n^{'}; r^{'})$, Where $\oplus$, $\odot$, $\otimes$ are the binary operations for messages, randomizers and ciphertexts respectively. For notational convenience, we will in the rest of paper use + for the message and randomizers, and · for the ciphertexts. In this paper we use the following variant of the Damgard-Fujisaki commitment scheme. We choose a moduls n as a product of two safe primes and random generators $g, g_1, ...g_k, h$ of QR_n. A commitment to an integer m using randomizer $r \in_R \{0,1\}^{l_r}$ is $c = g^m h^r \bmod n$. To commit to integers $m_1,...,m_k$ using randomizer $r \in_R \{0,1\}^{l_r}$ we compute $c = g_1^{m_1} ... g_k^{m_k} h^r \bmod n$. This commitment scheme satisfies the root extraction property ([14] [15]).

Homomorphic encryption. In this paper we make use of a semantically secure homomorphic threshold cryptosystem. The encryption algorithm E takes as input a message and a randomizer and output a ciphertext. The homomorphic property is $E(m \oplus m'; r \odot r') = E(m;r) \otimes E(m';r')$. Again, for notational convenience, we will in the rest of paper use $+$ for the message and randomizers, and $\cdot$ for the ciphertexts. Examples of homomorphic cryptosystems are the additive version [5] of ElGamal [16] and Paillier [17]. They both are semantically secure, have the root extraction property ([14] [15]) and have threshold variants ([18] [19] [7]).

$\sum -$***proofs.*** $\sum -$proofs [20] are a type of 3-move honest verifier zero-knowledge proofs that work in the following way: the prover and verifier know a common input x and the prover knows a witness w such that $(x,w) \in R$ where R is some relation. The prover sends an initial message a to the verifier, receives a random challenge e and responds with an answer z. On the basis of (a,e,z) the verifier decides whether to accept the claim that $x \in L$ where L is the language specified by the relation R. Using Fiat-Shamir heuristic [21] $\sum -$proofs can be made non-interactive by using a cryptographic hash function and letting the challenge be created as $e = hash(x,a)$. In the random oracle model [22] the resulting hash value is completely random.

3 The new voting system

The new voting system works as follows:

Step 1. Voting preparation

A bulletin board is constructed for the DREs, the registration authority and tallying authorities to publish certified messages. The messages posted on the bulletin board cannot be tampered with. Before the election starts all voters must go to the registration authority to register their identities. Tallying authorities jointly create the public key of the homomorphic commitment and the public key of the homomorphic threshold cryptosystem. The secret key of the cryptosystem is shared among l tallying authorities by a (t,l) secret sharing algorithm where t is the threshold. The public keys are posted on the bulletin board and fixed into the firmware of the DREs. The registration authority publishes the list of all eligible voters' identity information and places DREs into all polling stations.

Step 2. Casting a ballot

(1) A voter enters the voting booth after her identity is verified. Assume that she wants to vote for the k-th candidate ($k \in \{0,1,...,L-1\}$). The DRE receives her choice, picks $r \in_R \{0,1\}^{l_r}$ and computes the commitment $c = com(M^k; r)$.

(2) The DRE asks the voter to input random challenges for other $L-1$ candidates. Each challenge is a T-bit string. In practice the T-bit string can be composed of 4 alphanumeric characters.

(3) The DRE computes an $L \times T$ matrix $H = (h_{i,j})$, $i = 0,...,L-1$; $j = 1,...,T$. The element in the k-th row of the matrix is defined as $h_{k,j} = c \cdot com(0, r_{k,j})$,

$j = 1,...,T$, $r_{k,j} \in_R \{0,1\}^{l_r}$. Denote by $bit_{i,j}$ the j-th bit of the challenge for the i-th candidate ($i = 0,...,L-1$; $j = 1,...,T$). The element in the i-th ($i = 0,...,L-1$, $i \neq k$; $j = 1,...,T$) row of the matrix is defined as follows:

$$h_{i,j} = com(M^i; r + r_{i,j}) \text{ if } bit_{i,j} = 0 ,$$

$$h_{i,j} = c \cdot com(0; r_{i,j}) \quad \text{ if } bit_{i,j} = 1 . \qquad r_{i,j} \in_R \{0,1\}^{l_r} .$$

(4) The DRE computes a commitment to everything it has calculated so far: $x = com(c, H; r_x)$, $r_x \in_R \{0,1\}^{l_r}$. It prints x in the first two lines of the receipt. We require the actual printed information is hidden behind a shield. The voter can verify that two rows are actually printed but she cannot learn the exact content.

(5) The voter enters a random T -bit string as the challenge for her chosen candidate k .

(6) The DRE computes an $L \times T$ matrix $S = (s_{i,j})$, $i = 0,...,L-1$; $j = 1,...,T$. The element of the matrix S is defined as follows:

$$s_{i,j} = r + r_{i,j} \text{ if } bit_{i,j} = 0 ,$$

$$s_{i,j} = r_{i,j} \quad \text{ if } bit_{i,j} = 1 .$$

(7) The DRE prints each candidate’s name and its corresponding challenge on the receipt. The voter verifies that the challenges printed on the receipt are identical to the challenges she input. If everything is in order she presses “OK” button to finalize the vote. If something is wrong she presses “ESC” button to restart the voting.

(8) The DRE prints the voter’s identity information and a “Receipt Certified” message on the final two lines of the receipt. The voter takes her receipt and leaves the voting booth.

Step 3. Publishing the vote

The DRE picks $R \in_R \{0,1\}^{l_R}$ and computes the encryption of the ballot $C = E(M^k; R)$. It uses the following $\sum -$proof to prove that the commitment c and the encryption C hold the same element m modulo N :

Common input: Commitment c , Encryption C and public keys.

Private input for the prover: Message m and randomizer $r \in \{0,1\}^{l_r}$, $R \in \{0,1\}^{l_R}$ so $c = com(m; r)$, $C = E(m; R)$.

Initial message: Choose $R_m \in_R \{0,1\}^{l_V + l_e + l_s}$, $R_R \in_R \{0,1\}^{l_R + l_e + l_s}$ and $r_r \in \{0,1\}^{l_r + l_e + l_s}$. Set $C_R = E(R_m; R_R)$ and $c_r = com(R_m; r_r)$.

Challenge: $e = hash(C, c, C_R, c_r)$.

Answer: Set $\boxed{m} = em + R_m$, $\boxed{R} = eR + R_R$ and $\boxed{r} = er + r_r$. The answer is ($\boxed{m}$, $\boxed{R}$, $\boxed{r}$).

Verification: The verifier computes e as above, and verifies that $C^e C_R = E(\boxed{m}; \boxed{R})$ and $c^e c_r = com(\boxed{m}, \boxed{r})$.

Next the DRE makes a non-interactive zero-knowledge proof to prove that the encryption of the voter's ballot is correctly formed. The techniques for such proofs have been investigated in ([5][6][7][14][15]). In appendix an efficient zero-knowledge proof is given. It may be helpful to design a DRE.

The DRE publishes the encryption of the ballot, the two non-interactive zero-knowledge proofs made as above and the voting information of the voter on the bulletin board. The voting information including the following data: the copy of the voter's receipt, the commitment c, the matrix H, the randomizer r_x and the matrix S.

Step 4 Verifying the individual vote outside the voting booth

The voter checks that a copy of her receipt appears on the bulletin board. The voter does not need to participate in the next verification. She can ask any third party she trusts, such as a helper organization, to perform the left verification. The third party carries out the verification as follows: ① verifies $x = com(c, H; r_x)$; ② verifies $h_{i,j} = com(M^i; s_{i,j})$ if $bit_{i,j} = 0$, or $h_{i,j} = c \cdot com(0; s_{i,j})$ if $bit_{i,j} = 1$; for all $i = 0, ..., L-1$; $j = 1, ..., T$. If the DRE made the commitment $c = com(M^k; r)$ to some value other than the voter's choice in the voting booth, the DRE will be caught with probability at least $1 - 2^{-T}$. ③verifies the proof that a commitment c and an encryption C hold the same element; ④verifies the proof that the encryption of the ballot is correctly formed. The voting schemes based on homomorphic encryption are vulnerable to malformed encrypted ballots. A sender who sends $E(-100)$ may take 100 yes-votes out of the ballot box. We use the zero-knowledge proof for correct encryption of a ballot to guarantee that even if a malformed encrypted ballots can escape the former verification, the damage it can do is only limited to casting a ballot for another candidate. Note this zero-knowledge proof and its corresponding verification are performed by the DRE and the third party respectively. The overhead of the voter is not increased. Since the data published on the bulletin board is publicly accessible, even a passive third party interested in the election can participate in the verification. If the verification fails, the verifier can appeal to the legal authority for arbitration. The incorrect votes are excluded from the tallying.

Step 5. Tallying

When the voting phase ends, the tallying authorities multiply all the ciphertexts of the ballots.

By the homomorphic property of the cryptosystem they get a new ciphertext $E(\sum_{i=0}^{L-1} v_i M^i)$. The tallying authorities threshold decrypt this ciphertext and give the zero-knowledge proof that the decryption is correctly performed. It is straightforward to extract the voting result from the plaintext.

Step 6. Verifying the tally

Any passive third party interested in the election can re-compute the ciphertext $E(\sum_{i=0}^{L-1} v_i M^i)$ and verify the zero-knowledge proof of correct decryption.

4 Security analysis and discussion

The proposed voting system satisfies all security requirements presented in Section 2.

Eligibility: The voter's identity must be registered and checked before she can enter the voting booth. Everyone can verify that the voter who has cast a ballot is included in the list of all eligible voters.

Privacy: The receipt leaks no information about the voter's choice. Due to the hiding property of the commitment, the semantic security property of the encryption algorithm and the zero-knowledge property of the $\sum -$proofs, no information about the content of the vote can be inferred from the public data posted on the bulletin board. The single encrypted ballot will never be decrypted if the number of honest tallying authorities is more than the threshold. Only the final tallying result is jointly decrypted and revealed.

Universal Verifiability: The receipts, the tallying process and all zero-knowledge proofs are posted on the bulletin board. Any third party can act as a verifier.

Robustness: The DRE must provide the voter a receipt to prove that it has correctly recorded the voter's choice. The encryption of the ballot made by the DRE and the joint decryption made by the tallying authorities are proved by corresponding $\sum -$proofs. So failure of the participants in the election can be detected. The threshold cryptosystem can tolerate $l-t$ dishonest tallying authorities. The corruption of the DRE does not influence the data recovery. This will be discussed later.

Fairness: When t tallying authorities remain honest, they will never cooperate to decrypt any of the partial tallying results.

Receipt-freeness: Interestingly, although the voter receives a receipt in the voting booth, any adversary can gain no information about the voter's choice from the receipt. Only the voter knows the order of the input challenges for candidates. On the receipt the real zero-knowledge proof for the candidate chosen by the voter is indistinguishable from any other zero-knowledge proof simulated by the DRE. The voter has no idea about the randomizers used by the DRE. Although she is convinced that the DRE correctly encrypts her ballot by the $\sum -$proofs, she cannot prove to others how she casts a ballot. So the proposed voting system satisfies the receipt-free property.

The new voting system retains the advantage of Moran-Naor's scheme, that is, the voter only needs to remember and compare some strings and she can let any third party she trusted complete the left verification. There are some differences between the new voting system and Moran-Naor’s scheme:

A special vote encoding is used in the new voting system. In Moran-Naor’s scheme, the vote is simply encoded as the hash value of the candidate’s name.

A homomorphic integer commitment scheme is used in the new system, whereas, Pedersen commitment [23] is used in Moran-Naor’s scheme.

The DRE is required to do more work and the tallying authorities are introduced in the new system. The DRE encrypts the ballot and gives two relative non-interactive zero-knowledge proofs. The tallying authorities jointly decrypt the ciphertext of the final result.

Compared with Moran-Naor’s scheme, the new voting system has the following advantages:

Firstly, Moran-Naor’s scheme has the property of everlasting privacy. They use Pedersen commitment and the commitment is perfect hiding. Although the commitment to the vote is published on the bulletin board, the secrecy of the commitment is in the information-theoretic sense. This property is good in theory, however, may be too strong in practice. If the DRE breaks down, the ballot stored in it cannot be recovered and will be everlasting lost. In the new voting system the encryption of the ballot is published on the bulletin board. The failure of the DRE will not have a significant impact on the election.

Secondly, in the tallying phase of Moran-Naor’s scheme, the ballot is stored in the DRE on the form of plaintext. In order to hide the content of the individual ballot, the DRE shuffles the ballots and gives a cut-and-choose zero-knowledge proof to prove the correctness of the shuffle. In the new voting system the ballots are specially encoded to allow a homomorphic aggregation on the form of ciphertexts. The fact that the DRE does not store ballots on the form of plaintext provides a higher security level. The $\sum -$proofs made by the DRE are more efficient than the costly cut-and-choose shuffle proof, and the design of the DRE is greatly simplied.

Finally, in Moran-Naor’s scheme the tallying is separately performed on each DRE. So the tallying result on each DRE is disclosed. Although the tally is counted after the voting phase ends and the fairness property is not violated, additional information about voters’ choices on each DRE is exposed. This is not desirable. In the new voting system the tallies on all DREs are combined on the form of ciphertext by the homomorphic property of the cryptosystem. The partial tallies are always hidden if t tallying authorities remain honest.

5. Conclusion

Cryptography is an important tool in the implement of e-voting. But most voters have little knowledge about the theory, and it is unreasonable to assume that voters can perform complicated computation. To address the issue, Neff designed the first e-voting scheme that greatly reduced the computation cost needed by the voter. Moran and Naor designed a simpler e-voting scheme by using the similar idea. In this paper we present a new voting system combining the advantages of Moran-Naor’s voting scheme and voting schemes based on homomorphic encryption. The voter is free of complicated computation and more advantages are given: the ballots can be recovered when the voting machine breaks down, the costly cut-and-choose zero-knowledge proofs made by the voting machine are avoided and the partial tally result in each voting machine is kept secret.

Acknowledgement

The first author would like to thank Tal Moran for helpful comments, and thank some anonymous comments. (The fact that they provided helpful comments does not necessarily mean that they agree with everything in this paper. The authors take full responsibility for any errors or oversights here.)

References

[1] D. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”, Communications of the ACM, Vol. 24, No. 2, pp. 84-88, 1981.

[2] J. Furukawa and K. Sako, “An Efficient Scheme for Proving a Shuffle”, CRYPTO 2001, LNCS Vol. 2139, Springer-Verlag, pp. 368-387, 2001.

[3] C. A. Neff, “A verifiable secret shuffle and its application to E-voting”, In Proceedings of 8th ACM Conference on Computer and Communications Security-CCS 2001, ACM Press, pp. 116-125, 2001.

[4] A. Fujioka, T. Okamoto and K. Ohta, “A Practical Secret Voting Scheme for Large Scale Elections”, AUSCRYPT 1992, LNCS Vol. 718, Springer-Verlag, pp. 244-251, 1992.

[5] R. Cramer, R. Gennaro and B. Schoenmakers, “A Secure and Optimally Efficient Multi-Authourity Election Scheme”, EUROCRYPT 1997, LNCS Vol. 1233, Springer-Verlag, pp. 103-118, 1997.

[6] O. Baudron, P. A. Fouque, D. Pointcheval, G. Poupard and J. Stern, “Practical Multi-candidate Election System”, PODC 2001, ACM Press, pp. 274-283, 2001.

[7] I. Damgard and M. Jurik, “A Generalisation, a Simplification and Some Applications of Paillier’s Probabilistic Public-key System”, PKC 2001, LNCS Vol. 1992, Springer-Verlag, pp. 119-136, 2001.

[8] D. Chaum, “Secret-Ballot Receipt: True Voter-Verifiable Elections”, IEEE Security and Privacy, Vol.2, No.1, pp.38-47, 2004.

[9] C. A. Neff. “Practical High Certainty Intent Verification for Encrypted Votes”, October 2004. Available from: http://www.votehere.net/vhti/documentation/vsv-2.0.3638.pdf.

[10] T. Moran and M. Naor. “Receipt-Free Universally-Verifiable Voting with Everlasting Privacy”, CRYPTO 2006, LNCS Vol. 4117, Springer-Verlag, pp. 373-392, 2006.

[11] E. Fujisaki and T. Okamoto, “Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations”, CRYPTO 1997, LNCS Vol.1294, Springer-Verlag, pp. 16-30, 1997.

[12] I. Damgard and E. Fujisaki, “A Statistically-Hiding Integer Commitment Scheme Based on Groups with Hidden Order”, ASIACRYPT 2002, LNCS Vol.2501, pp. 125-142, 2002.

[13] Jens Groth, “Cryptography in Subgroup of Z_n^* ”, TCC 2005, LNCS Vol.3378, Springer-Verlag, pp. 50-65, 2005.

[14] I. Damgard, J. Groth and G. Salomonsen, “The theory and implementation of an electronic voting system”, In D. Gritzalis, editor, Secure Electronic Voting, pp. 77-100. Kluwer Academic Publishers, 2003.

[15] J. Groth, “Non-interactive Zero-knowledge Arguments for Voting”, ACNS 2005, LNCS

Vol.3531, Springer-Verlag, pp. 467-482, 2005. Full version available from: http://www.brics.dk/~jg/ACNS05VoteProofFull.pdf.

[16] T. ElGamal. “A Public key cryptosystem and a signature scheme based on discrete logarithms”, CRYPTO’84, LNCS Vol. 196, pp. 10-18, 1984.

[17] P. Paillier, “Public-Key Cryptosystems Based on Composite Degree Residuosity Class”, EUROCRYPT 1999, LNCS Vol.1592, Springer-Verlag, pp. 223-239, 1999.

[18] T. P. Pedersen, “A threshold cryptosystem without a trusted third party”, EUROCRYPT 1991, LNCS Vol.547, Springer-Verlag, pp. 522-526, 1991.

[19] P. A. Fouque, G. Poupard and J. Stern, “Sharing Decryption in the Context of Voting or Lotteries”, Financial Cryptography 2000, LNCS Vol.1962, Springer-Verlag, pp. 90-104, 2001.

[20] R. Cramer, I. Damgard and B. Schoenmakers, “Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols”, CRYPTO 1994, LNCS Vol.839, Springer-Verlag, pp. 174-187, 1994.

[21] A. Fiat and A. Shamir, “How to prove yourself: Practical Solutions to Identification and Signature Problems”, CRYPTO’86, LNCS Vol.263, Springer-Verlag, pp. 186-194, 1986.

[22] M. Bellare and P. Rogaway, “Random oracles are practical: A paradigm for designing efficient protocols”, ACM Conference on Computer and Communications Security 1993, ACM Press, pp. 62-73, 1993.

[23] T. Pedersen, “Non-Interactive and Information Theoretic Secure Verifiable Secret Sharing”, CRYPTO’91, LNCS Vol. 576, Springer-Verlag, pp. 129-140, 1991.

Appendix

1. How to prove that a commitment c and an encryption C hold the same element m modulo N.

In this paper we use a $\sum -$proof to prove that a commitment c and an encryption C hold the same element m modulo N. The $\sum -$proof is presented in [14]. But the authors of [14] do not prove that the proof satisfies the criteria of the special honest verifier zero-knowledge proof. Here we give the complete proof.

Common input: Commitment c, Encryption C and public keys.

Private input for the prover: Message m and randomizer $r \in \{0,1\}^{l_r}$, $R \in \{0,1\}^{l_R}$ so $c = com(m;r)$, $C = E(m;R)$.

Initial message: Choose $R_m \in_R \{0,1\}^{l_V+l_e+l_s}$, $R_R \in_R \{0,1\}^{l_R+l_e+l_s}$ and $r_r \in \{0,1\}^{l_r+l_e+l_s}$. Set $C_R = E(R_m;R_R)$ and $c_r = com(R_m;r_r)$.

Challenge: $e = hash(C, C_R, c, c_r)$.

Answer: Set $\boxed{m} = em + R_m$, $\boxed{R} = eR + R_R$ and $\boxed{r} = er + r_r$. The answer is ($\boxed{m}$, $\boxed{R}$,

$\boxed{r}$).

Verification: The verifier computes e as above, and verifies that $C^e C_R = E(\boxed{m};\boxed{R})$ and $c^e c_r = com(\boxed{m},\boxed{r})$.

Theorem 1. In the random oracle model, the protocol above is a non-interactive special honest verifier zero-knowledge argument. If the commitment scheme is statistically hiding, the protocol is statistically special honest verifier zero-knowledge argument. If the commitment scheme is statistically binding, the protocol is a special honest verifier zero-knowledge proof.

Proof. It is straightforward to verify that the protocol is complete. It remains to argue zero-knowledge and special soundness.

To argue zero-knowledge we pick e at random. We choose $\boxed{m} \in_R \{0,1\}^{l_V + l_e + l_s}$, $\boxed{R} \in_R \{0,1\}^{l_R + l_e + l_s}$ and $\boxed{r} \in_R \{0,1\}^{l_r + l_e + l_s}$. We set $C_R = E(\boxed{m};\boxed{R})C^{-e}$ and $c_r = com(\boxed{m},\boxed{r})c^{-e}$. Finally, we program the random oracle to output e on input (C, C_R, c, c_r). The simulated argument is statistically indistinguishable from a real argument if the commitment scheme is statistically hiding.

To argue special soundness, we suppose an adversary produces a valid proof. We wish to extract a witness (m, r, R). To do so we can rewind the adversary to the point where it queries the random oracle with C, C_R, c, c_r , we then give it random challenges until we get a new acceptable proof. Let us call the two acceptable arguments ($C_R, c_r, e, \boxed{m}, \boxed{R}, \boxed{r}$) and ($C_R^{'}, c_{\ r}^{'}, e^{'}, \boxed{m}^{'}, \boxed{R}^{'}, \boxed{r}^{'}$).

Since the proofs are acceptable we have $C^e C_R = E(\boxed{m};\boxed{R})$ and $C^{e'} C_R = E(\boxed{m}^{'};\boxed{R}^{'})$. This gives us $C^{e-e'} = E(\boxed{m} - \boxed{m}^{'};\boxed{R} - \boxed{R}^{'})$. With overwhelming probability we have $e \neq e'$ and using the root extraction property of the cryptosystem we can extract $\mu = (\boxed{m} - \boxed{m}^{'})/(e - e') \bmod N$ and $\rho = (\boxed{R} - \boxed{R}^{'})/(e - e')$ so $C = E(\mu;\rho)$. In a similar way by the root extraction property of the commitment we can extract $\gamma = (\boxed{m} - \boxed{m}^{'})/(e - e')$ and $\lambda = (\boxed{r} - \boxed{r}^{'})/(e - e')$ so $c = com(\gamma;\lambda)$. We can see $\mu = \gamma \mod N$.

If the commitment scheme is statistically binding, even an unbounded adversary cannot change its mind about the value it has committed to. We actually have a special honest verifier zero-knowledge proof.

2. How to prove the encryption of the ballot is correctly formed

In voting based on homomorphic encryption, the encrypted ballot is cast with a proof that the encryption of the ballot is correctly formed. The proof techniques have been developed in ([5][6][7][14][15]). Groth suggested non-interactive zero-knowledge arguments for four types of voting: limited vote, approval vote, divisible vote and Borda vote in [15]. To the best of our knowledge, his arguments are the most efficient. Following his idea, we give a NIZK argument suitable for our voting system. It is a simplified version of Groth's argument for limited vote.

Recall that we represent candidates with numbers $0,...,L-1$ and encode a vote on candidate i as M^i. We select $M = p^2$ where p is a prime. Assume that the voter chooses candidate j ($j \in \{0,...,L-1\}$) and give her choice to the DRE. The DRE encrypts M^j and gives a non-interactive zero-knowledge argument for the encryption as follows:

Common input: Ciphertext C and public keys.

Prover's input: $R \in_R \{0,1\}^{l_R}$ such that $C = E(V;R) = E(M^j;R)$. We prove correctness of the encryption of the vote by producing the proof of knowledge: [(v,ρ,α,β): $C = E(v;\rho)$, $v = \alpha^2$ and $p^L = p\alpha\beta$].

Argument: Let $V = M^j$, choose $R_V \in_R \{0,1\}^{l_V+l_e+l_s}$, $R_R \in_R \{0,1\}^{l_R+l_e+l_s}$, and set $C_R = E(R_V;R_R)$.

Let $a = p^j$, $b = p^{L-j-1}$. Choose $r_a, r_b \in_R \{0,1\}^{l_V/2+l_e+l_s}$. Let $\Psi = par_b + pbr_a$, $\Delta = 2ar_a - R_V$.

Set $c = com(a,b,\Psi,\Delta,r)$. Set $c_r = com(r_a, r_b, pr_a r_b, r_a^2, r_r)$.

Compute the challenge as $e = hash(C, C_R, c, c_r)$.

Set $\boxed{V} = eV + R_V = eM^j + R_V$ and $\boxed{R} = eR + R_R$.

Set $\boxed{a} = ea + r_a = ep^j + r_a$, $\boxed{b} = eb + r_b = ep^{L-j-1} + r_b$ and $\boxed{r} = er + r_r$.

The argument is ($C_R, c, c_r, \boxed{V}, \boxed{R}, \boxed{a}, \boxed{b}, \boxed{r}$).

Verification: Compute e as above. Let $\boxed{\Psi} = p\boxed{a}\boxed{b} - e^2 p^L$, $\boxed{\Delta} = \boxed{a}^2 - e\boxed{V}$.

Verify that $C^e C_R = E(\boxed{V};\boxed{R})$ and $c^e c_r = com(\boxed{a},\boxed{b},\boxed{\Psi},\boxed{\Delta},\boxed{r})$.