A New Receipt-Free Voting Scheme Based on Linkable Ring Signature for Designated Verifiers*

Guomin Chen[1], Chunhui Wu[1], Wei Han[2], Xiaofeng Chen[1],
Hyunrok Lee[3], and Kwangjo Kim[3]
[1]School of Information Science and Technology,
Sun Yat-sen University, Guangzhou 510275, P.R.China
[2]Department of Computer Science and Engineering,
Shanghai Jiao Tong University, Shanghai 200240, P.R.China
[3]International Research center for Information Security (IRIS)
Information and Communications University(ICU), Taejon 305-714, KOREA
Email: isschxf@mail.sysu.edu.cn; {tank,kkj}@icu.ac.kr

Abstract

Receipt-freeness is an essential security property in electronic voting to prevent vote buying or coercion. In this paper, we propose a new approach to construct receipt-free electronic voting schemes. We first introduce the notion of linkable ring signature for designated verifiers which preserves all properties of a normal linkable ring signature while only the designated verifiers can verify the correctness of the signature. We then use this notion to construct a new receipt-free voting scheme. Furthermore, we prove that our voting scheme can achieve the desired security requirements.

1. Introduction

Electronic voting (e-voting) is one of the most significant applications of cryptographic protocol. It offers a number of advantages which can not be achieved by traditional voting such as convenience and efficiency. Plenty of research on e-voting has been done during the last two decades. Previous e-voting schemes can be categorized into three main types by their research approaches: schemes using blind signatures [9, 18, 19]; schemes using mix-nets [1, 2, 7, 14, 20, 12, 21]; and schemes using homomorphic encryptions [3, 4, 5, 6, 8, 11, 15, 22].

The concept of receipt-freeness was firstly introduced by Benaloh and Tuinstra [3] to solve the misbehavior of vote buying or coercion in electronic voting. Based on the assumption of a voting booth, they also proposed two voting schemes using homomorphic encryptions. The first one is a single authority voting scheme and fails to maintain vote secrecy. The second scheme is extended to a multi-authority scheme achieving vote secrecy. However, Hirt and Sako [11] proved that the scheme could not satisfy the property of receipt-freeness and proposed the first practical receipt-free voting scheme based on homomorphic encryption.

Receipt-free voting protocol based on a mix-net channel was first proposed by Sako and Kilian [21], which only assumes one-way secret communication from the authorities to the voters. However, a significant disadvantage of this protocol is the heavy processing load required for tallying.

The receipt-free voting schemes using blind signatures were proposed by Okamoto [19]. However, the first scheme requires the help of voting commission and the second one needs a stronger physical assumption of voting booth.

Recently, Linkable Ring Signature(LRS) is introduced to construct practical voting schemes. A linkable ring signature allows anyone to determine if two ring signatures are signed by the same group member. The first linkable ring signature was presented by Liu *et al.* [17] in 2004. Later, some simple discussion of constructing voting systems using linkable ring signature was proposed in [16, 23], where the linkability is used to achieve the uniqueness for the e-voting.

In this paper we first introduce the notion of the linkable ring signature for designated verifiers and then use it to propose a new solution to construct receipt-free voting schemes. In our voting scheme, a voter is allowed to cast a new vote later if the victim is controlled by the coercer during the voting stage. Moreover, only the latest vote is counted in the tally, so the uniqueness and receipt-freeness

*Supported by National Natural Science Foundation of China (No. 60503006) and NSFC-KOSEF Joint Research Project (No. 60611140543).

978-0-7695-3288-2/08 $25.00 © 2008 IEEE
DOI 10.1109/ICESS.Symposia.2008.54

can be achieved simultaneously.

The rest of the paper is organized as follows: The model and definitions for electronic voting are given in Section 2. Some preliminaries are provided in Section 3. The linkable ring signature for designated verifiers required in our voting scheme is presented in Section 4. The proposed receipt-free voting scheme and its security analysis are given in Section 5. Finally, the conclusions will be made in Section 6.

2. Model and Definitions

In this section, we briefly describe the model and security requirements of electronic voting.

2.1 Model

- **Entities:** The entities involved in a voting scheme include voters, administrator (bulletin board), and tally authorities.
- **Physical Assumptions:** The general physical assumptions for voting consist of anonymous channel and bulletin board.

2.2 Security Requirements

We present the security requirements as follows:

- *Completeness*: A vote cannot be forged or altered, and the valid votes are counted correctly.
- *Soundness*: All the eligible votes should be counted.
- *Privacy*: There is no association between the voter's identity and a marked vote.
- *Eligibility*: Only eligible voters are permitted to cast their votes.
- *Fairness*: Nothing can affect the voting.
- *Verifiability*: Voters can verify that their votes are counted correctly.
- *Receipt-freeness*: Anyone, even if the voter himself, must not be able to construct a receipt proving the content of his vote.
- *Uniqueness*: A voter can only have one vote to be counted.

3 Preliminaries

We briefly review the notions of linkable ring signature and designated verifier protocol in this section.

3.1 Linkable Ring Signature

Linkable ring signatures are ring signatures with linkability: anyone can determine whether two signatures are signed by the same group member. The first practical linkable ring signature scheme is introduced by Liu *et al.* [17]. We briefly review the scheme here.

- **Key Generation**

  Let $G = \langle g \rangle$ be a group of prime order q such that the underlying discrete logarithm problem is intractable. Let $H_1 : \{0,1\}^* \rightarrow Z_q$ and $H_2 : \{0,1\}^* \rightarrow G$ be some statistically independent cryptographic hash functions. For $i = 1, ..., n$, each user has a distinct public key y_i and a private key x_i such that $y_i = g^{x_i}$. Let $L = \{y_1, ..., y_n\}$ be the list of n public keys.

- **Signature Generation**

  Given a message $m \in \{0,1\}^*$, the list of public keys $L = \{y_1, y_2, ..., y_n\}$, private key x_π corresponding to $y_\pi (1 \leq \pi \leq n)$, the following algorithm generates a linkable ring signature.

  1. Compute $h = H_2(L)$ and $\hat{y} = h^{x_\pi}$.
  2. Select $u \in_R Z_q$, and compute
  $$c_{\pi+1} = H_1(L, \hat{y}, m, g^u, h^u).$$
  3. For $i = \pi + 1, ..., n, 1, ..., \pi - 1$, select $s_i \in_R Z_q$ and compute
  $$c_{i+1} = H_1(L, \hat{y}, m, g^{s_i} y_i^{c_i}, h^{s_i} \hat{y}^{c_i}).$$
  4. Compute $s_\pi = u - x_\pi c_\pi \mod q$.

  The signature is $\delta_L(m) = (c_1, s_1, ..., s_n, \hat{y})$.

- **Signature Verification**

  Check the signature $\delta_L(m) = (c_1, s_1, ..., s_n, \hat{y})$ on the message m and the list of public keys as follows.

  1. Compute $h = H_2(L)$ and for $i = 1, ..., n$, compute $z'_i = g^{s_i} y_i^{c_i}$, $z''_i = h^{s_i} \hat{y}^{c_i}$ and then $c_{i+1} = H_1(L, \hat{y}, m, z'_i, z''_i)$ if $i \neq n$.
  2. Check whether $c_1 = H_1(L, \hat{y}, m, z'_n, z''_n)$. If yes, accept. Otherwise, reject.

3.2 Designated Verifier Proof

The concept of designated verifier proof was first introduced by Jakobsson, Sako and Impagliazzo [13], where a prover can non-interactively designate a proof of a statement to a designated verifier, while the verifier can simulate

the proof by himself with his secret key and thus cannot transfer the proof to convince anyone else.

The designated verifier proof can be used to construct a non-interactive undeniable signature scheme as follows:

- **Constructing a proof:**

  The prover, Alice, selects $w, r, t \in_u Z_q$ and calculates

$$\begin{cases} c = g^w y_B^r \mod p \\ G = g^t \mod p \\ M = m^t \mod p \\ h = hash_q(c, G, M) \\ d = t + x_A(h + w) \mod q \end{cases}$$

  where $hash_q : \{0,1\}^* \rightarrow Z_q$. The prover sends (w, r, G, M, d) to the verifier, Bob.

- **Verifying a proof:**

  The designated verifier can verify a proof by calculating

$$\begin{cases} c = g^w y_B^r \mod p \\ h = hash_q(c, G, M) \end{cases}$$

  and verifying that

$$\begin{cases} G y_A^{h+w} = g^d \mod p \\ M s^{h+w} = m^d \mod p \end{cases}$$

- **Simulating transcripts:**

  The designated verifier can simulate correct transcripts by selecting $d, \alpha, \beta \in_u Z_q$ and calculate

$$\begin{cases} c = g^\alpha \mod p \\ G = g^d y_A^{-\beta} \mod p \\ M = m^d s^{-\beta} \mod p \\ h = hash_q(c, G, M) \\ w = \beta - h \mod q \\ r = (\alpha - w) x_B^{-1} \mod q \end{cases}$$

4 Linkable Ring Signature for Designated Verifier

In this section we introduce a new notion named linkable ring signature for designated verifiers. More precisely, it is a linkable ring signature while the signature can only be verified by the designated verifiers. In particular, the designated verifiers can not convince any third party of the fact.

The scheme is similar to the one in [17] described in section 3.1. We use the same notations and let $E_V(m)$ denote the encryption of m using the verifier V's public key y_V.

- **Signature Generation**

  Given a message $m \in \{0,1\}^*$, the list of public keys $L = \{y_1, y_2, ..., y_n\}$, private key x_π corresponding to $y_\pi (1 \leq \pi \leq n)$, the following algorithm generates a linkable ring signature for designated verifiers.

  1. Compute $h = H_2(L)$ and $\tilde{y} = h^{x_\pi}$.
  2. Select $u \in_R Z_q$, and compute
$$c_{\pi+1} = H_1(L, \tilde{y}, m, g^u, h^u).$$
  3. For $i = \pi + 1, ..., n, 1, ..., \pi - 1$, select $s_i \in_R Z_q$ and compute
$$c_{i+1} = H_1(L, \tilde{y}, m, g^{s_i} y_i^{c_i}, h^{s_i} \tilde{y}^{c_i}).$$
  4. Compute $s_\pi = u - x_\pi c_\pi \mod q$.
  5. Compute g^{s_n} and h^{s_n}, then compute
$$E = E_V(\tilde{y} || g^{s_n} || h^{s_n} || DV\text{-}ZKP(w, r, G_1, G_2, d)),$$
     where $DV\text{-}ZKP(w, r, G_1, G_2, d)$ is a non-interactive designated-verifier zero-knowledge proof on (g^{s_n}, h^{s_n}), and can be constructed as follows:
     Select $w, r, t \in_u Z_q$ and compute
$$\begin{cases} c = g^w y_V^r \mod p \\ G_1 = g^t \mod p \\ G_2 = h^t \mod p \\ h^* = hash_q(c, G_1, G_2) \\ d = t + s_n(h^* + w) \mod q \end{cases}$$
     where y_V is the public key of the designated verifier. The prover sends (w, r, G_1, G_2, d) to the verifier.

  The signature is $\delta_L(m) = (c_1, s_1, ..., s_{n-1}, E)$.

- **Signature Verification**

  The designated verifier V checks $\delta_L(m) = (c_1, s_1, ..., s_{n-1}, E)$ on a message m and a list of public keys as follows:

  1. Compute $h = H_2(L)$, and then decrypt E with his private key x_V to obtain $\tilde{y}$, g^{s_n}, h^{s_n}, and $DV\text{-}ZKP(w, r, G_1, G_2, d)$.
  2. Verify the zero-knowledge proof on (g^{s_n}, h^{s_n}) as follows:
     Compute
$$\begin{cases} c = g^w y_V^r \mod p \\ h^* = hash_q(c, G_1, G_2) \end{cases}$$

and verify that

$$\begin{cases} G_1(g^{s_n})^{h^*+w} = g^d \mod p \\ G_2(h^{s_n})^{h^*+w} = h^d \mod p \end{cases}$$

3. For $i = 1, ..., n$, compute $z'_i = g^{s_i} y_i^{c_i}$, $z''_i = h^{s_i} \tilde{y}^{c_i}$ and then $c_{i+1} = H_1(L, \tilde{y}, m, z'_i, z''_i)$ if $i \neq n$.
4. Check whether $c_1 = H_1(L, \tilde{y}, m, z'_n, z''_n)$. If yes, accept. Otherwise, reject.

- **Linkability**

  For a fixed list of public keys L, given two signatures associating with L, namely $\delta'_L(m') = (c'_1, s'_1, ..., s'_{n-1}, E')$ and $\delta''_L(m'') = (c''_1, s''_1, ..., s''_{n-1}, E'')$, where m' and m'' are some messages. Due to the encryption of (g^{s_n}, h^{s_n}) using designated verifier's public key, only the designated verifier can verify the linkability and correctness of the signatures. After decryption, the verifier checks if $\tilde{y}' = \tilde{y}''$. If the equation holds, the verifier concludes that the signatures are created by the same signer. Otherwise, the verifier concludes that the signatures are generated by two different signers.

We could extend the scheme for multiple designated verifiers. Due to the consideration of space, we omit it here.

5 The Proposed Receipt-free Voting Scheme

In this section we present a new receipt-free voting scheme based on linkable ring signature for designated verifiers.

5.1 Our Voting Scheme

The participants of our scheme include l eligible voters $V_i (1 \leq i \leq l)$, an administrator A, and n tally authorities $T_i (1 \leq i \leq n)$. We assume that V_i and A are connected by an anonymous channel. Moreover, we assume that each voter V_i has a public/private key pair (y_i, x_i) and the public key of each voter is publicly known in a bulletin board. Let L denote the set of public keys of all eligible voters. Define a cryptographic hash function $H : \{0,1\}^* \rightarrow \{0,1\}^k$. Let (PK, SK) be the public/private key pair used in an (n, t) threshold encryption scheme $\varepsilon_{\mathrm{PK}}(\cdot)$, where $\mathrm{SK} = (\mathrm{SK}_1, \mathrm{SK}_2, \cdots, \mathrm{SK}_n)$ and SK_i is given to T_i. Let (y_T, x_T) be the public/private key pair used in a linkable ring signature scheme for designated verifiers δ_L, where $x_T = (x_{T_1}, x_{T_2}, \cdots, x_{T_n})$ and x_{T_i} is given to T_i. Generally, we can use Gennaro *et al*'s distributed key generation (DKG) protocol [10] to generate these key pairs.

We denote by $\mathcal{S}$ the set of votes, by $Sign_A(m)$ a signature on the message m generated with A's private key x_A, and by $DV\text{-}LRingSign_{B,L}(m)$ a linkable ring signature for designated verifiers on message m generated using B's private key and the public keys in L.

The proposed voting scheme consists of the following two stages:

- **Voting stage:**
  - A publishes the information $\mathcal{I}$ which contains the details of the voting event.
  - V_i selects $s \in_R \{0,1\}^k$, $m \in \mathcal{S}$, and computes $m' = \varepsilon_{\mathrm{PK}}(m)$, $c = H(s, m', \mathcal{I})$. He then sends c to A.
  - A computes $S = Sign_A(c, \mathcal{I}, Time)$ and then sends $(S, Time)$ to V_i, where $Time$ is a timestamp.
  - If S is not a valid signature of A, terminates the protocol. Otherwise, V_i computes the linkable ring signatures for designated verifiers $R = DV\text{-}LRingSign_{V_i,L}(S, c, \mathcal{I})$, then sends $\{s, m', c, Time, S, R\}$ to the bulletin board.
- **Tallying stage:** The tally stage is performed by the tally authorities T_i.
  - At least t tally authorities $T_i (1 \leq i \leq n)$ together decrypt the ciphertext E to obtain $\tilde{y}$, g^{s_n}, h^{s_n}, and $DV\text{-}ZKP(w, r, G_1, G_2, d)$. T_i then together recover the secret key x_T and verify all signatures S and R on the public bulletin. All invalid values are discarded.
  - If there are two or more linkable ring signatures having the same $\tilde{y}$, then T_i discard the ones which have the earlier timestamps.
  - T_i obtain the vote m. Similarly, the ciphertext $\varepsilon_{\mathrm{PK}}(m)$ can only be decrypted by at least t tally authorities $T_i (1 \leq i \leq n)$. Each decrypted vote m is verified to be in $\mathcal{S}$. If $m \notin \mathcal{S}$, the vote is discarded. Finally, T_i counts all valid votes and announce the result.

5.2 Security Analysis

Theorem 1. *The proposed scheme satisfies the properties of completeness, privacy, soundness, eligibility, fairness, verifiability, receipt-freeness, and uniqueness.*

Proof. We show that our scheme satisfies all the security properties listed in section 2.2.

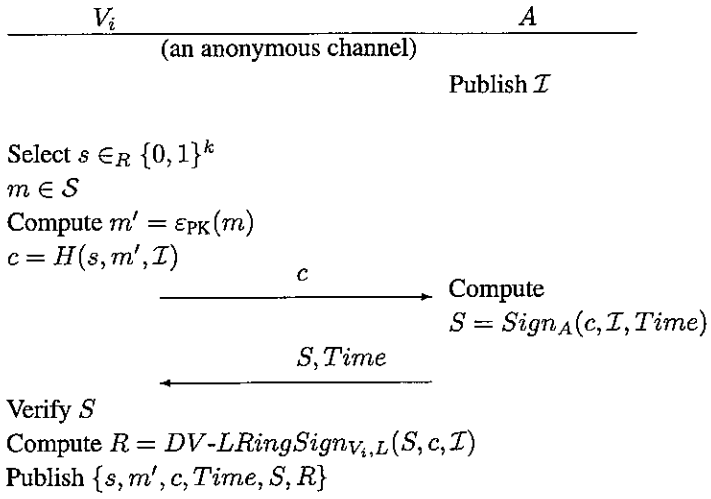

Figure 1. The Voting Stage

- *Completeness*: In our proposed scheme, each encrypted vote is signed by a voter using a linkable ring signature which is unforgeable. No one can corrupt a voter's vote. And the voter can check whether his/her vote is listed on the bulletin board, any valid vote is counted correctly.
- *Privacy*: In the voting stage, the voter communicates with administrator through an anonymous channel. Therefore, no one can trace the communication and violet the privacy of the voter. Also, due to the linkable ring signature for designated verifiers, no one except the tally T_i can verify the correctness of the signature.
- *Soundness*: In the tally stage, tally T_i can check the validity of vote by verifying whether the linkable ring signature for designated verifiers is valid. So, all the eligible votes can be counted in the result of the voting.
- *Eligibility*: Eligibility can be easily achieved in our scheme using a linkable ring signature, because any ineligible voter can not generate a valid signature.
- *Fairness*: The tallying stage is done after the voting stage and V_i provides a knowledge proof that his/her vote is correct, no one can affect the result of voting.
- *Verifiability*: In our proposed scheme, all linkable ring signatures are published in the bulletin board and the voters can verify their votes.
- *Receipt-freeness*: The reason why some existing voting schemes can not achieve receipt-freeness is simple: after the encrypted vote is published, the voter himself can prove the content of his vote by revealing the random number that he used in the scheme. Our proposed scheme can easily achieve receipt-freeness by allowing the voters to vote multi-times. Note that, when a voter-buyer C wants to buy a voter of V_i, even if the voter V_i gives all his information to C, including his private key, C still can not trust him because V_i can cast another ballot in private and revoke the previous one. Moreover, our scheme can still be receipt-free even if the coercer C colludes with some tally authorities T_i to verify share of credentials received from the voter V_i. Though the tally authority T_i can present a proof to convince the coercer C that the voter casted a specific vote, the coercer C can not trust the tally authorities T_i due to the designated verifier protocol, *i.e.*, T_i can simulate a proof with his private key as follows:

$$(w, r, G_1, G_2, d) \begin{cases} c = g^{\alpha} \mod p \\ G_1 = g^d (g^{s_n})^{-\beta} \mod p \\ G_2 = h^d (h^{s'_n})^{-\beta} \mod p \\ h^* = hash_q(c, G_1, G_2) \\ w = \beta - h^* \mod q \\ r = (\alpha - w) x_T^{-1} \mod q \end{cases}$$

- *Uniqueness*: Though voters are allowed to vote multi-times, uniqueness is ensured by counting only the latest one, eliminating the earlier votes linked to the same voter.

□

6 Conclusion

Receipt-freeness is an essential security property in electronic voting to prevent vote buying or coercion. In this paper, we introduce the notion of linkable ring signature for designated verifiers and then use it to propose a new receipt-free electronic voting scheme. Moreover, we prove that our scheme can achieve the desired security notions.

References

[1] M. Abe, *Mix-networks on permutation networks*, Advances in Cryptology-ASIACRYPT 1999, LNCS 1716, pp. 258-273, Springer-Verlag, 1999.

[2] R. Aditya, B. Lee, C. Boyd, and E. Dawson, *An efficient mixnet-based voting scheme providing receipt-freeness*, Advances in Trustbus 2004, LNCS 3184, pp. 152-161, Springer-Verlag, 2004.

[3] J. Benaloh and D. Tuinstra, *Receipt-free secret-ballot elections*, Proc. of 26th Symp. on Theory of Computing-STOC 1994, pp. 544-553, 1994.

[4] J. Benaloh and M. Fischer, *A robust and verifiable cryptographically secure election scheme*, Proc. 26th IEEE Symposium on the Foundations of Computer Science (FOCS), pp. 372-382, 1985.

[5] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung, *Multi-authority secret-ballot elections with linear work*, Advances in Cryptology-EUROCRYPT 1996, LNCS 1070, pp.72-83, Springer-Verlag, 1996.

[6] R. Cramer, R. Gennaro and B. Schoenmakers, *A secure and optimally efficient multi-authority election scheme*, Advances in Cryptology-EUROCRYPT 1997, LNCS 1233, pp.103-118, 1997.

[7] D. Chaum, *Untraceable electronic mail, return addresses, and digital pseudonyms*, Communications of the ACM, 24(2), pp.84-88, 1981.

[8] J. Benaloh and M.Yung, *Distributing the power of a government to enhance the privacy of voters*, Proc. 5th ACM Symposium on Principles of Distributed Computing (PODC), pp.52-62, ACM, 1986.

[9] A. Fujioka, T. Okamoto, and K. Ohta, *A practical secret voting scheme for large scale election*, Advances in Cryptology-AUSCRYPT 1992, LNCS 718, pp.244-260, Springer-Verlag, 1992.

[10] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, *Secure Distributed Key Generation for Discrete-Log Based Cryptosystems*, Journal of Cryptology, 20(1), pp.51-83, Springer-Verlag, 2007.

[11] M. Hirt and K.Sako, *Efficient receipt-free voting based on homomorphic encryption*, Advances in Cryptology-EUROCRYPT 2000, LNCS 1807, pp.393-403, Springer-verlag, 2000.

[12] M. Jakobsson, *A Practical Mix*, Advances in Cryptology-EUROCRYPT 1998, LNCS 1403, pp. 448-461, Springer-Verlag, 1998.

[13] M. Jakobsson, K. Sako and R. Impagliazzo, *Designated verifier proofs and their applications*, Advanced in Eurocrypt 1996, LNCS 1070, pp. 143-154, Springer-Verlag, 1996.

[14] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo, *Providing receipt-freeness in mixnet-based voting protocols*, ICISC 2003, LNCS 2971, pp.245-258, Springer-Verlag, 2003.

[15] B. Lee and K. Kim, *Receipt-free electronic voting scheme with a tamper-resistant randomizer*, ICISC 2002, LNCS 2587, pp.389-406, Springer-Verlag, 2002.

[16] Joseph K. Liu, Sherman S. M. Chow, and Duncan S. Wong, *A new approach to e-voting*, CISC 2005, 2pp.57-266, 2005.

[17] J. Liu, V. Wei, and D. Wong, *Linkable spontanrous anonymous group signature for ad hoc group (extended abstract)*, ACISP 2004, LNCS 3108, pp.325-335, Springer-Verlag, 2004.

[18] T. Okamoto, *An electronic voting scheme*, IFIP World Conference 1996, Advanced in IT Tools, pp.21-30, Chapman Hall, 1996.

[19] T. Okamoto, *Receipt-free electronic voting schemes for large scale elections*, Proceeding of Workshop on Security Protocols 1997, LNCS 1361, pp.25-35, Springer-Verlag, 1997.

[20] C. Park, K. Itoh, and K. Kurosawa, *Efficient anonymous channel and all/nothing election scheme*, Advances in Cryptology-EUROCRYPT 1993, LNCS 765, pp.248-259, Springer-Verlag, 1993.

[21] K. Sako and J. Kilian, *Receipt-free mix-type voting scheme: a practical solution to the implementation of a voting booth*, Advance in Cryptology-EUROCRYPT 1995, LNCS 921, pp.393-403, Springer-verlag, 1995.

[22] K. Sako and J. Kilian, *Secure voting using partially compatible homomorphisms*, Advances in Cryptology-CRYPTO 1994, LNCS 839, pp.411-424. Springer-Verlag, 1994.

[23] P. Tsang, V. Wei, *Short linkable ring signatures for e-voting, e-cash and attestation*, ISPEC 2005, LNCS 3439, pp.48-60, Springer-Verlag, 2005.