Receipt-Free Electronic Voting Schemes for Large Scale Elections

Tatsuaki Okamoto

NTT Laboratories
Nippon Telegraph and Telephone Corporation
1-1 Hikarinooka, Yokosuka-shi, Kanagawa-ken, 239 Japan
Email: okamoto@sucaba.isl.ntt.co.jp
Tel: +81-468-59-2511
Fax: +81-468-59-3858

Abstract

This paper proposes practical receipt-free voting schemes which are suitable for (nation wide) large scale elections. One of the proposed scheme requires the help of the voting commission, and needs a physical assumption, the existence of an untappable channel. The other scheme does not require the help of the commission, but needs a stronger physical assumption, the existence of a voting booth. We define receipt-freeness, and prove that the proposed schemes satisfy receipt-freeness under such physical assumptions.

1 Introduction

Various types of electronic secret voting schemes have been proposed in the last ten years [BGW88, BT94, CCD88, CFSY96, Cha88, FOO92, GMW87, Ive92, JSI96, Oka96, SK94, SK95], and recently *receipt-free* voting schemes are attracting many researchers [BT94, JSI96, Oka96, SK95]. The receipt-free property means that voting system generates no receipt (evidence) of whom a voter voted for, where the receipt of a vote, which proves that a voter has voted for a candidate, could be used by another party to coerce the voter.

Benaloh and Tuinsra [BT94] introduced the concept of the receipt-free voting based on the framework of the voting scheme using higher degree residue encryption [BY86, CF85]. They used a physical assumption, the existence of a *voting booth*. Their scheme allows voters only yes/no voting and is very impractical for large scale elections, since a lot of communication and computation overhead is needed to prevent the dishonesty of voters by using zero-knowledge (like) protocols.

Sako and Kilian [SK94] and Cramer, Franklin, Schoenmaker and Yung [CFSY96] improved the efficiency of the underlying zero-knowledge protocols by using discrete logarithm encryption in place of the higher degree residue encryption used in [BY86, CF85, BT94]. However, their schemes do not satisfy receipt-freeness. Moreover, their scheme allows voters only yes/no voting, and if it is extended to multiple bit voting, their schemes are still inefficient in practice.

Sako and Kilian [SK95] proposed a receipt-free voting scheme based on the Mixnet framework [Cha81]. Their scheme uses a weaker physical assumption, the existence of an *untappable channel*, than the physical assumption, a voting booth, of [BT94]. Their solution also satisfies universal verifiability. However, their scheme allows voters only yes/no voting, and if it is extended to multiple bit voting, their scheme is very inefficient in practice, especially when it is used for a large scale voting system.

Here, an *untappable channel* for V is a physical apparatus by which only voter V can send a message to a party, and the message is perfectly secret to all other parties. A *voting booth* is a physical apparatus for V in which only voter V can interactively communicate with a party, and the communication is perfectly secret to all other parties.

Another practical approach for realizing electronic voting involves the schemes using blind signatures and anonymous channels [Cha88, FOO92, Oka96]. This approach is considered to be the most suitable and promising for large scale elections, since the communication and computation overhead is fairly small even if the number of voters is large. Moreover, this type of scheme naturally realizes multiple value voting, and is also very compatible with the framework of existing physical voting systems.

In addition, this type of scheme is universally acceptable, and this is the most important property in election systems, since otherwise many people should be suspicious about the voting result. We now explain the reason why this framework is universally acceptable. The procedures consist of four stages; the authorizing stage, voting stage, claiming stage, and counting stage. In the authorizing stage, the administrators issue blind signatures. In the voting stage, the voters send their votes with the administrator's signatures to the bulletin board (or counter) through anonymous channels. In the claiming stage, each voter can publicly claim if his/her vote is not found in the board, and in the counting stage, the votes on the board are verified and counted. Here, in the claiming stage, everyone has the chance to raise a claim if he/she is suspicious about the contents of the board, and anyone (e.g., judge) can clearly determine whether the claim is valid or not, by checking the validity of the administrator's signature included in the claim. Thus, at the end of the claiming stage, everyone should be satisfied with the contents of the board (otherwise he/she should have raised a claim and had it resolved), and should be satisfied with the voting result, since all can count the voting result from the contents of the board.

[Oka96] proposed a *receipt-free* voting scheme based on this framework. To our best knowledge, this scheme is the only receipt-free voting scheme that is based on this framework and is considered to be practical for large scale elections.

However, in this paper, we show a security flaw in the receipt-free property of this scheme, and propose some new voting schemes to overcome this security flaw. One scheme requires the help of a group of the voting commission, called the "parameter registration committee" (PRC), and needs the physical assumption of an *untappable channel*. Another scheme does not require the help of such a committee, but needs the stronger physical assumption of a *voting booth*. Since both solutions are still practical, the proposed receipt-free voting schemes are suitable for practical (nation wide) large scale elections.

One of the reasons why [Oka96] had such a flaw in receipt-freeness is that no formal definition and proof of receipt-freeness have been given in [Oka96]. Although Benaloh and Tuinstra [BT94] have defined receipt-freeness, their definition is specific to their framework, and cannot be used in our framework. Therefore, it is very important to define receipt-freeness based on our framework, and to prove that a voting scheme satisfies this definition.

This paper defines receipt-freeness based on our framework, and proves that our modified schemes satisfy receipt-freeness under physical assumptions (i.e., an untappable channel or a voting booth).

This paper is organized as follows: Section 2 introduces the previous voting scheme [Oka96], Section 3 shows a security flaw in [Oka96], and Section 4 gives the definition of receipt-freeness. In sections 5, 6 and 7, our voting schemes are presented and are proven to be receipt-free under physical assumptions.

2 Brief description of the previous scheme

This section briefly introduces [Oka96].

2.1 Participants of the proposed scheme

The participants of this scheme are voters, V_i $(i = 1, 2, \ldots, I)$, and voting commission, which consists of multiple administrators, multiple privacy commission members, and multiple timeliness commission members. Note that this scheme assumes no anonymous channel through the use of the Mixnet method [Cha81] with the multiple privacy commission members.

However, to simplify the explanation of this scheme, hereafter we assume that the voting commission consists of a single administrator, A, and a single timeliness commission member, T. In addition, we assume an anonymous channel but no privacy commission members.

2.2 Procedures

[Authorizing stage]

Several parameters, p, q, g, h, are generated and published by the system, where p and q are prime, $q|p-1$, g and h are in Z_p^*, and $q = \text{order}(g) = \text{order}(h)$. Here, α such that $h = g^\alpha \bmod p$ is not known to any party.

1. V_i randomly generates $\alpha_i \in Z_q$, and calculates $G_i = g^{\alpha_i} \bmod p$. We then define $BC(v_i, r_i) = g^{v_i} G_i^{r_i} \bmod p$. Here, $BC(v_i, r_i)$ is a *trap-door bit-commitment*, since V_i can open this bit-commitment in many ways, (v_i, r_i), (v_i', r_i'), etc., using α_i such that $v_i + \alpha_i r_i \equiv v_i' + \alpha_i r_i' \pmod q$.
   V_i makes his/her vote v_i and computes
   $$m_i = BC(v_i, r_i) = g^{v_i} G_i^{r_i} \bmod p,$$
   using random number r_i. V_i computes
   $$x_i = H(m_i \| G_i) {t_i}^e \bmod n,$$
   where t_i is a random number in Z_n, and (e, n) is the RSA public key of A for signatures, and H is a hash function. (x_i is a blind message for the RSA blind signature.) V_i generates his/her signature $z_i = S_{V_i}(x_i)$ for x_i. V_i also computes
   $$E_A(x_i \| z_i \| ID_{V_i}),$$
   where E_A is public-key encryption using A's public-key, and $\|$ denotes concatenation.
2. V_i sends $E_A(x_i \| z_i \| ID_{V_i})$ to A.
3. A decrypts the message, and checks that voter V_i has the right to vote, by using the voters' list. A also checks whether or not V_i has already applied. If V_i doesn't have the right or V_i has already applied, A rejects. If V_i is accepted, A checks the signature z_i of message x_i. If they are valid, then A generates signature
   $$y_i = {x_i}^{1/e} \bmod n.$$
   A sends y_i to V_i.
4. V_i gets A's signature $s_i = H(m_i \| G_i)^{1/e} \bmod n$ of message m_i by $s_i = y_i / t_i \bmod n$ (i.e., unblinding procedure).

[Voting stage]

V_i sends $(m_i \| G_i, s_i)$ to the bulletin board through an anonymous channel. V_i also sends (v_i, r_i, m_i) to timeliness commission member T through an untappable anonymous channel.

[Claiming stage]

V_i checks that his/her ballot is listed on the bulletin board (ballot list). If his/her vote is not listed, then V_i claims this by showing $(m_i \| G_i, s_i)$.

[Counting stage]

In this stage, T publishes the list of votes, v_i, in random order on the board, and also shows a non-interactive modification of zero-knowledge proof, σ, to prove that the list of v_i contains only correct open values of the list of m_i without revealing the linkage between m_i and v_i. In other words, T publishes $(v'_1, \ldots, v'_I)$, which is a random order list of v_i. That is, $v'_i = v_{\pi(i)}$ $(i = 1, \ldots, I)$, where π is a random permutation of I elements. Given $(m_1, \ldots, m_I)$ and $(v'_1, \ldots, v'_I)$, T proves that T knows (π, r_i) such that

$$m_i = BC(v_i, r_i), \quad v'_i = v_{\pi(i)},$$

without revealing (π, r_i).

Here, we omit the description of how to calculate σ.

3 A security flaw in the receipt-freeness of the scheme

In [Oka96], the trapdoor bit-commitment is essential for satisfying receipt-freeness. If the value of α_i is generated by voter V_i as specified, then the scheme satisfies the receipt-freeness.

However, if α_i is generated by a coercer C, and C forces V_i to use $G_i = g^{\alpha_i} \bmod p$ for V_i's bit-commitment, then V_i cannot open $m_i = BC(v_i, r_i)$ in more than one way, since V_i does not know α_i. Hence, the voting scheme is not receipt-free and C can coerce V_i. (Here, we assume that C will pay V_i money or release a hostage, if C gets the receipt indicating that V_i voted in C's favor.)

4 Definition of receipt-freeness

This section defines the receipt-freeness based on the above-mentioned framework of voting schemes.

Definition 1. Given published information, X, (public parameters and information on the bulletin board), adversary (coercer) C interactively communicates with voter V_i in order to force V_i to cast C's favorite vote v^*_i to T, and finally C decides whether to accept $View_C(X : V_i)$ or not, and T decides whether T accepts v^*_i or not. Here, C gets message x_b from the bulletin board immediately after x_b is put on the board. $View_C(X : V_i)$ means C's view through communicating with V_i and getting information from the bulletin board, that is, $View_C(X : V_i)$ includes published information X, C's coin flips, v_i^*, and the messages that C receives from V_i.

A voting system is receipt-free, if there exists a voter, V_i, such that, for any adversary C, V_i can cast v_i ($v_i \neq v_i^*$) which is accepted by T, under the condition that $View_C(X : V_i)$ is accepted by C.

Note: In the above-mentioned definition, we assume that the final voting result (total number of votes for each candidate) does not affect the decision of whether C accepts $View_C(X : V_i)$ or not. That is, the total number of votes for v_i^* changes by 1 depending on whether V_i casts v_i^* or v_i ($v_i \neq v_i^*$). We assume that C is insensitive to such change in the total number of votes. (This assumption is very reasonable, since at least the voting result must be published in any voting system.)

5 Modified voting scheme using untappable channels (Scheme A)

Here, we assume an untappable channel and the parameter registration committee (PRC).

5.1 Untappable channel

Definition 2. A physical apparatus is called an "untappable channel" for voter V_i, if only V_i can send out a message, m, to recipient R, and all others can know (information theoretically) nothing about m.

Let $R_1, \ldots, R_N$ be PRC members.

5.2 Procedures

[Authorizing stage]

Public parameters are the same as the original scheme.

V_i randomly generates $\alpha_i \in Z_q$, and splits α_i into N pieces, $\alpha_{i,1}$ …, $\alpha_{i,N}$ such that $\alpha_i = \alpha_{i,1} + \cdots \alpha_{i,N} \bmod q$. V_i then calculates $G_i = g^{\alpha_i} \bmod p$, and $G_{i,j} = g^{\alpha_{i,j}} \bmod p$ $(j = 1, \ldots, N)$.

The other procedure in this stage is the same as the original except

$$x_i = H(m_i \| G_i \| G_{i,1} \| \cdots \| G_{i,N}) {t_i}^e \bmod n.$$

Therefore, finally V_i gets A's blind signature s_i of $(m_i \| G_i \| G_{i,1} \| \cdots \| G_{i,N})$.

[Voting stage]

V_i sends $(m_i \| G_i \| G_{i,1} \| \cdots \| G_{i,N}, s_i)$ to the bulletin board through an anonymous channel. V_i also sends (v_i, r_i, m_i) to timeliness commission member T through an untappable anonymous channel.

In addition, V_i sends $\alpha_{i,j}$ to R_j $(j = 1, \ldots, N)$ along with G_i through an untappable anonymous channel.

R_j calculates

$$G_{i,j} = g^{\alpha_{i,j}} \bmod p,$$

and sends $G_{i,j}$ along with G_i to the bulletin board.

[Claiming stage]

V_i checks that his/her ballot is listed on the bulletin board (ballot list). If his/her vote is not listed, then V_i claims this by showing $(m_i \| G_i \| G_{i,1} \| \cdots \| G_{i,N}, s_i)$.

In addition, V_i checks that all $G_{i,j}$ $(j = 1, \ldots, N)$ are listed on the board by R_j. If $G_{i,j}$ is not listed, then V_i claims this and sends again $\alpha_{i,j}$ to R_j $(j = 1, \ldots, N)$ along with G_i through an untappable anonymous channel.

[Counting stage]

T (and others) checks whether all $G_{i,j}$ of $(m_i \| G_i \| G_{i,1} \| \cdots \| G_{i,N})$ with s_i are the same as $G_{i,j}$ sent by R_j, and $G_i = \prod_{j=1}^{N} G_{i,j} \bmod p$. If this check fails, the corresponding vote v_i is removed from the list of votes.

The other procedure is the same as the original one.

5.3 Proof of receipt-freeness

In this subsection, we prove that the above-mentioned modified scheme satisfies receipt-freeness, if all PRC members are honest.

Theorem 3. *Let T follow the protocol. Let σ (T's proof) be the interactive version (i.e., perfect zero-knowledge interactive proof). Assume that untappable channels are available and that all PRC members, R_j $(j = 1, \ldots, N)$ follow the protocol. Then the modified voting scheme A satisfies receipt-freeness.*

Proof. Suppose that all procedures for V_i are done by adversary C, except for the procedure of sending messages to R_j and T through untappable channels. That is, the only role of V_i is sending (v_i, r_i, m_i) to T and $\alpha_{i,j}$ to R_j $(j = 1, \ldots, N)$ through untappable channels.

Such adversary C is universal since if a voting scheme is receipt-free for this type of adversary C, then the voting scheme is also receipt-free for any other type of adversary C^+. This is because: Suppose that for any adversary C of this type, there exists a voter, V_i, such that V_i can cast v_i $(v_i \neq v_i^*)$ accepted by T, under that $View_C(X : V_i)$ is accepted by C. Then for any other type of adversary C^+ with more limited view than C, we can construct voter V_i^+ which follows V_i's strategy and adopts any strategy for the part that C^+ does not execute but C executes in place of V_i. Then for any adversary C^+, there exists a voter, V_i^+, such that V_i^+ can cast v_i $(v_i \neq v_i^*)$ accepted by T, under that $View_{C^+}(X : V_i^+)$ is accepted by C^+.

Here, w.l.o.g., we can assume that C accepts $View_C(X : V_i)$ only if the messages sent out by V_i through untappable channels are compatible with $View_C(X : V_i)$ (more precisely C's view except $G_{i,j}$ sent by R_j $(j = 1, \ldots, N)$). That is, we can assume that C accepts $View_C(X : V_i)$ only if $G_{i,j}$ sent by R_j are exactly the same as $G_{i,j}$ authorized by A's signature in the authorizing stage.

If $G_{i,j}$ $(j = 1, \ldots, N))$ are sent by R_j, then R_j receives $\alpha_{i,j}$ from V_i through an untappable channel, under the condition that R_i follows the protocol. Then, V_i must send out $\alpha_{i,j}$ to R_j, under an untappable channel assumption. This means V_i can calculate $\alpha_i = \alpha_{i,1} + \cdots \alpha_{i,N} \bmod q$, and then calculate (v_i, r_i) $(v_i \neq v_i^*)$ such that $m_i = BC(v_i^*, r_i^*) = BC(v_i, r_i)$ by using α_i with $v_i + \alpha_i r_i \equiv v_i^* + \alpha_i r_i^* \pmod q$. Therefore, if V_i can send out messages to R_j which are compatible with $View_C(X : V_i)$, then V_i can calculate (v_i, r_i) $(v_i \neq v_i^*)$ such that $m_i = BC(v_i^*, r_i^*) = BC(v_i, r_i)$.

Let V_i^* be V_i who follows C's coercion (i.e., V_i^* casts v_i^* to T). Let V_i cast v_i to T $(v_i \neq v_i^*)$ under the condition that V_i sends out messages to R_j which are compatible with $View_C(X : V_i)$. W.l.o.g., we can suppose that C accepts $View_C(X : V_i^*)$.

Now we assume that C does not accept $View_C(X : V_i)$. The only difference between $View_C(X : V_i^*)$ and $View_C(X : V_i)$ is the voting result and T's proof (say $(Res_{V_i}, \sigma_{V_i})$ with V_i and $(Res_{V_i^*}, \sigma_{V_i^*})$ with V_i^*). This means C can distinguish between the $(Res_{V_i}, \sigma_{V_i})$ and $(Res_{V_i^*}, \sigma_{V_i^*})$. Since $\sigma_{V_i})$ and $\sigma_{V_i^*})$ are perfectly indistinguishable, C should distinguish Res_{V_i} and $Res_{V_i^*}$. This contradicts the assumption described in the definition of receipt-freeness.

Hence C accepts $View_C(X : V_i)$ when V_i casts v_i $(v_i \neq v_i^*)$ to T who accepts v_i.

6 Modified voting scheme using untappable channels (Scheme B)

In the above-mentioned modified voting scheme, α_i is simply split into N pieces. Therefore, if even one PRC member, R_j, does not follow the protocol, then the receipt-freeness cannot be guaranteed.

In this section, we propose a scheme proof against some faulty PRC members. The scheme uses Feldman-Pedersen's VSS directly [Fel87, Ped91a].

6.1 Procedures

Almost all procedures are similar to the previous scheme except the following part:

Let $K \leq N$. V_i randomly generates $\alpha_i \in Z_q$, and $a_k \in Z_q$ $(k = 1, \ldots, K-1)$. Let $f(x) = \alpha_i + a_1 x + \cdots + a_{K-1}x^{K-1}$, and $\alpha_{i,j} = f(j) \bmod q$ $(j = 1, \ldots, N)$. V_i then calculates $G_i = g^{\alpha_i} \bmod p$, $G_{i,j} = g^{\alpha_{i,j}} \bmod p$ $(j = 1, \ldots, N)$, $F_{i,k} = g^{a_k} \bmod p$ $(k = 1, \ldots, K-1)$.

In the voting stage, V_i sends $(m_i \| G_i \| G_{i,1} \| \cdots \| G_{i,N} \| F_{i,1} \| \cdots \| F_{i,K-1}, s_i)$ to the bulletin board through an anonymous channel. V_i also sends $\alpha_{i,j}$ to R_j $(j = 1, \ldots, N)$ along with G_i through an untappable anonymous channel. R_j calculates

$$G_{i,j} = g^{\alpha_{i,j}} \bmod p,$$

and sends $G_{i,j}$ along with G_i to the bulletin board.

In the counting stage, T (and others) check whether all $G_{i,j}$ of $(m_i \| G_i \| G_{i,1} \| \cdots \| G_{i,N} \| F_{i,1} \| \cdots \| F_{i,K-1})$ with s_i are the same as the $G_{i,j}$ sent by R_j, and

$$G_{i,j} = G_i \prod_{k=1}^{K-1} {F_{i,k}}^{j^k} \bmod p.$$

6.2 Receipt-freeness

Theorem 4. *Let T follow the protocol. Let σ (T's proof) be the interactive version (i.e., perfect zero-knowledge interactive proof). Assume that untappable channels are available and that at least K PRC members among $\{R_1, \ldots, R_N\}$ follow the protocol. Then the modified voting scheme B satisfies receipt-freeness.*

The proof uses the known results on Feldman-Pedersen's VSS and the same techniques used in the proof of the previous theorem.

This scheme can be extended to the unconditionally secure (for $G_{i,j}$ and $F_{i,k}$) version based on the unconditionally secure VSS by Pedersen [Ped91b].

7 Modified voting scheme using voting booths (Scheme C)

In this section, we assume a voting booth, which is a stronger physical assumption than an untappable channel, but we do not need the help of the voting commission.

7.1 Voting booth

Definition 5. A physical apparatus is called "voting booth" for voter V_i, if only V_i can interactively communicate with another party R through the booth, and all others can know (information theoretically) nothing about the communication.

We also require an additional property, anonymity for the voting booth, i.e., R does not know who V_i is.

7.2 Procedures

[Authorizing stage]

All procedures in this stage are the same as in the original.

[Voting stage]

The procedures in this stage are the same as in the original, except for an additional procedure as follows:

V_i proves to T through an anonymous voting booth that V_i knows α_i in a zero-knowledge manner [TW87] (or with a more efficient protocol such as [Sch91] in practice). If T accepts V_i's proof, then T accepts his vote, $(m_i \| G_i, s_i)$, under the condition that the vote is also valid.

[Claiming stage]

The procedures in this stage are the same as in the original, except for the claiming procedure as follows:

If V_i's vote is not listed on the bulletin board, V_i claims this by showing $(m_i \| G_i, s_i)$ and proving to T through the voting booth that V_i knows α_i in a zero-knowledge manner [TW87].

[Counting stage]

The procedure in this stage is the same as the original.

7.3 Receipt-freeness

Theorem 6. *Let T follow the protocol. Let σ (T's proof) be the interactive version (i.e., perfect zero-knowledge interactive proof). Assume that voting booths are available. Then the modified voting scheme C satisfies receipt-freeness.*

8 Remarks on the security of multiple timeliness commission members

This section shows some remarks for the case of using multiple timeliness commission members (Section 5 in [Oka96]):

- Each T_l ($l = 1, 2, \ldots, L$) sends each v_{il} to their private board (for T_l) and calculate $v_i = v_{i1} + \cdots + v_{iL} \bmod q$. In this stage, we assume that T_l sends $BC(v_{il})$ and then reveals v_{il} after all T_l sends $BC(v_{il})$. Here, BC is a standard bit-commitment in which only a unique value can be revealed after fixing $BC(v_{il})$.
- When the voting is tally, v_i should be multiple bits long with redundant bits for error detection. In other words, one bit ballot should be coded by an error correcting or detecting code.
- The random permutatios π and δ should be split to L timeliness commission members, T_l. That is, each T_l generates random permutatios π_l and δ_l individually, and $\pi = \pi_1 \circ \cdots \circ \pi_L$ and $\delta = \delta_1 \circ \cdots \circ \delta_L$. The basic idea is as follows: V_i splits $v_i = v_{i1} + \cdots + v_{iL} \bmod q$ and votes

  $$E_1(m_i \| (v_{i1}, r_{i1}) \| E_2((v_{i2}, r_{i2}) \| E_3(\cdots E_L(v_{i2}, r_{i2}) \cdots)$$

  to T_1. These messages are decrypted sequentially by T_1 through T_L in a Mixnet manner [Cha81]. The permutations in the Mixnet-like tramsmission from T_l to T_{l+1} corresponds to π_l and δ_l. Here, there are two paths for obtaining v_i and W_i. Then the interactive proof σ is generated by the collaboration of T_1 through T_L. The detailed description of this protocol will be given in the final version of this paper.

Acknowledgments

The author would like to thank Kazue Sako and Markus Michels for pointing out the security flaws of the previous scheme and for invaluable discussions on the receipt-free voting schemes.

References

[BGW88] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation", Proc. of STOC'88, pp.1–10 (1988).

[BT94] J. Benaloh and D. Tuinstra, "Receipt-Free Secret-Ballot Elections", Proc. of STOC'94, pp.544–553 (1994).

[BY86] J. Benaloh and M. Yung, "Distributing the Power of a Government to Enhance the Privacy of Votes", Proc. of PODC'86, pp.52–62 (1986).

[Cha81] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, Vol.24, No.2, pp.84–88 (1981).

[Cha85] D. Chaum, "Security without Identification: Transaction systems to Make Big Brother Obsolete", Communications of the ACM, Vol.28, No.10, pp.1030–1044 (1985).

[Cha88] D. Chaum, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", Proceedings of Eurocrypt'88, LNCS 330, Springer–Verlag, pp.177–182 (1988).

[CCD88] D. Chaum, C. Crépeau, and I. Damgård, "Multiparty Unconditionally Secure Protocols", Proc. of STOC'88, pp.11–19 (1988).

[CF85] J. Cohen and M. Fisher, "A Robust and Verifiable Cryptographically Secure Election Scheme", Proc. of FOCS, pp.372–382 (1985).

[CFSY96] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung, "Multi-Authority Secret-Ballot Elections with Linear Work", Proc. of Eurocrypt'96, LNCS 1070, Springer–Verlag, pp.72–82 (1996).

[Fel87] P. Feldman, "A Practical Scheme for Non-interactive Verifiable Secret Sharing", Proc. of FOCS, pp. 427–437 (1987).

[FFS88] Feige, U., Fiat, A. and Shamir, A.: Zero-Knowledge Proofs of Identity, Journal of CRYPTOLOGY, Vol. 1, Number 2 pp.77–94(1988)

[FOO92] A. Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections", Proc. of Auscrypt '92, LNCS, Springer–Verlag, pp. 244–251 (1992).

[GMW87] O. Goldreich, S. Micali, and A. Wigderson, "How to Play Any Mental Game, or a Completeness Theorem for Protocols with Honest Majority", Proc. of STOC, pp.218–229 (1987).

[Ive92] K. R. Iversen, "A Cryptographic Scheme for Computerized General Elections", Proc. of Crypto '91, LNCS 576, Springer–Verlag, pp.405–419 (1992).

[JSI96] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated Verifier Proofs and Their Applications", Proc. of Eurocrypt '96, LNCS 1070, Springer–Verlag, pp.143–154 (1996).

[Oka96] T. Okamoto, "An Electronic Voting Scheme", Proc. of IFIP'96, Advanced IT Tools, Chapman & Hall, pp.21–30 (1996).

[TW87] Tompa, M. and Woll, H.: Random SelfReducibility and Zero Knowledge Interactive Proofs of Possession of Information, Proc. of FOCS'87, pp.472-482 (1987).

[Ped91a] Pedersen, T. P., "Distributed Provers with Applications to Undeniable Signatures", Proceedings of Eurocrypt 91 (1992).

[Ped91b] Pedersen, T. P., "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing", Proceedings of Crypto 91, pp. 129–140 (1992).

[Sch91] Schnorr, C.P., "Efficient Signature Generation by Smart Cards", Journal of Cryptology, Vol. 4, No. 3, pp.161-174 (1991).

[SK94] K. Sako, and J. Kilian, "Secure Voting Using Partially Compatible Homomorphisms", Proc. of Crypto'94, LNCS 839, Springer–Verlag, pp.411–424 (1994)

[SK95] K. Sako, and J. Kilian, "Receipt-Free Mix-type Voting Scheme", Proc. of Eurocrypt'95, LNCS 921, Springer–Verlag, pp.393–403 (1995)

This article was processed using the LaTeX macro package with LLNCS style