A Privacy Enhanced Election Scheme with Spare Votes for Simplifying Possible Re-Voting Process

Chun-I Fan
Telecommunication Laboratories
Chunghwa Telecom Co., Ltd.
12, Lane 551, Min-Tsu Road Sec. 5
Yang-Mei, Tao-Yuan, Taiwan, R.O.C.
TEL: +886-3-424-5081
FAX: +886-3-424-4920
E-mail: chunifan@ms35.hinet.net

Chin-Laung Lei
Department of Electrical Engineering
National Taiwan University
1, Roosevelt Road Sec. 4
Taipei, Taiwan, R.O.C.
TEL: +886-2-2363-5251 ext. 343
FAX: +886-2-2363-8247
E-mail: lei@cc.ee.ntu.edu.tw

Abstract

In many daily election activities, it is quite often that we have to perform a re-voting process shortly after the previous one to make a decision on an additional subject, such as to resolve ties or to vote on a subject further than the previous one. With a typical election scheme, we usually have to repeat the entire election process again to finish the re-voting activity. This paper presents a new anonymous election scheme to simplify the possible re-voting process such that every voter can participate in the re-voting activity without a redundant re-registration action and the unlinkability between the two voting activities is preserved.

Keywords: Electronic voting, Blind signatures, Security and privacy, Quadratic Residues, Cryptography

1 Introduction

Electronic elections make it possible for voters to submit the tally center their digitalized votes through communication networks. Comparing with the traditional election systems, the technique of electronic voting not only makes the voters in remote sites be able to participate in elections through communication networks but shortens the time required for the election activities [1, 2, 7, 8, 14, 15, 16, 17, 26, 27, 28, 31].

Typically, an electronic election scheme consists of two types of participants, a tally center and a group of voters. Basically, an electronic election protocol has three stages, i.e., initialization, registration, and voting. At the initialization stage, the tally center publishes some necessary information of the election, such as the subject of the election and the list of candidates. At the registration stage, voters are identified by the tally center through some secure identification mechanisms [19, 29], and then every identified voter obtains a vote with his intention of the election from the center by performing secure blind signature protocols [3, 5, 11] between the voter and the center. At the voting stage, voters submit their votes to the center through secure anonymous channels [4, 6], and after receiving the votes, the center verifies and publishes them and computes the result of the election.

In many daily election activities, it is quite often to perform a re-voting activity shortly after the previous one. For examples,

(1). A re-voting activity is performed to make a decision on a subject further than that of the previous one such as we hold a voting to decide what to do on Sunday, and if the decision is excursion, then we perform a re-voting process to decide where to visit.

(2). A re-voting is performed to resolve the problem of ties which occurs in the previous voting, such as several candidate professors may receive the same highest votes when electing the chairman of a department, or several candidate players may tie for the last available position of a national basketball team elected by a group of coaches.

The re-voting activity has two features,

(1). The voters' intentions of the re-voting partially or totally depend on the result of the previous one.

(2). Both the voting and the re-voting activities are performed in the same group of voters.

With typical electronic election schemes proposed in the literatures [1, 2, 7, 8, 14, 15, 16, 17, 26, 27, 28, 31], it is necessary to repeat the entire election process again to finish the re-voting activity.

The simplification of re-voting was first discussed in [12]. In [12], we have presented an intention attachable ticket scheme for electronic elections to avoid the redundant re-registration action of the re-voting process. In the scheme of [12], every identified voter can obtain an intention attachable ticket (*IA*-ticket) from the center at the registration stage of the election. The *IA*-ticket consists of two parts, the main part and the spare part, where the former contains the voter's intention of the election and the latter contains all possible intentions of the voter for the possible re-voting. The main part along with the format of the *IA*-ticket is submitted to the center by the voter at the voting stage of the election, and then the center verifies and publishes them at the stage. If a re-voting stage is required, the voter just needs to attach his new intention to the spare part of his published *IA*-ticket by submitting appropriate information to the center at the re-voting stage without a re-registration action. Although the intention attachability property makes it possible to perform a re-voting process without an extra round of registration actions between every voter and the center, people can derive the link of the two intentions embedded in the main part and the spare part, respectively, of the same *IA*-ticket when both of them are published. It affects the unlinkability property which anonymous elections should possess. Hence, only the intention attachability property is not enough to resolve the problem. Ideally, it is necessary to solicit an efficient method to unlinkably divide an *IA*-ticket into a main vote and a spare vote to preserve the unlinkability property in anonymous elections.

Continuing our previous research [12], we make a deeply research on the unlinkable division of an *IA*-ticket. We propose a new election scheme to achieve not only the intention attachability but the unlinkable division properties which are strongly required to resolve the problem of re-voting in anonymous elections. In the proposed election scheme, every identified voter obtains an unlinkably dividable and intention attachable ticket (*UDIA*-ticket) in the registration stage of an election. A *UDIA*-ticket contains a main vote and a spare vote. A main vote can be used as an ordinary vote in a typical electronic election. The main vote contains a voter's intention of the election and it is submitted to the tally center in the voting stage. If a re-voting stage is needed, every voter derives the spare vote from his *UDIA*-ticket and sends it to the center in the re-voting stage. Owing to the intention attachability and the unlinkable division properties, respectively, every voter can attach his new intention to his spare vote without a redundant re-registration action, and anyone else cannot link the spare vote to its main vote even when both of them are published, respectively.

The rest of the paper is organized as follows. We review several fundamental techniques related to the research in section 2. In section 3, an anonymous election scheme with unlinkable spare votes for re-voting is presented, and the security of the scheme is examined in section 4. Finally, we make a conclusion of this paper in section 5.

2 Preliminary

In this section we briefly describe several concepts related to anonymous electronic elections. Three underlying techniques are usually adopted to build a typical anonymous election protocol, that is, secure identification schemes [19, 29], blind signatures [3, 5, 11, 13, 21, 22], and anonymous channels [4, 6]. First, an identification scheme is always used to identify voters in an electronic election system through computer and communication networks [19, 29]. In addition, due to the unforgeability and the unlinkability properties, blind signatures are the key techniques to digitalize votes and to cut off the link between every published vote and the instance of the registration protocol producing that vote [3, 5, 11, 13, 21, 22]. Finally, anonymous channels or untraceable electronic mails are usually adopted to protect the voters' identities when sending their votes to the tally center in many election schemes proposed in the literatures [4, 6].

2.1 A Typical Anonymous Election Scheme

In the subsection we present a typical anonymous election protocol based on Chaum's blind signature scheme [5]. The protocol consists of three stages, initialization, registration, and voting, whose details are described as follows.

(1) **Initialization.** Initially, the tally center randomly selects two distinct large primes p_1 and p_2, and then computes $n = p_1 p_2$ and $\phi(n) = (p_1 - 1)(p_2 - 1)$. The center chooses two large integers e and d at random such that $ed \equiv 1 \pmod{\phi(n)}$. Thus, it publishes (e, n) and the necessary information of this election, such as the subject of the

election and the list of candidates. In addition, let H be a public one-way hash function [10, 23, 30].

(2) **Registration.** In the registration stage, the center identifies voters through identification protocols [19, 29]. Every identified voter chooses a message m which contains his own intention of the election, and randomly selects an integer r in Z_n^* which is the set of all positive integers less than and relatively prime to n. The voter submits $\alpha = (r^e H(m) \bmod n)$ to the center. After receiving α, the center sends $t = (\alpha^d \bmod n)$ to the voter. After receiving t, the voter performs the unblinding process to obtain $s = (r^{-1}t \bmod n)$. The tuple (m, s) is a valid vote of the voter.

(3) **Voting.** In the voting stage, the voter submits his vote (m, s) to the center through an anonymous channel [4, 6].[1] The center verifies the vote by checking if

$$s^e \equiv H(m) \pmod{n}$$

and then it publishes (m, s). In addition, the center publishes all of the other valid votes received from the voters, and computes the result of the election.

Owing to the unlinkability property of Chaum's blind signature scheme [5] and the anonymity of sender untraceable channels [4, 6], given a vote (m, s), it is computationally infeasible for the center to derive the identity of its owner in the election protocol.

2.2 A Straight-Forward Solution for Re-Voting

In the followings, we show a straight-forward method, repeating the entire election process again, to finish the re-voting activity. The protocol is described below.

(1) **Initialization.** The tally center publishes the necessary information of an election, such as the subject of the election, the list of candidates, and the public keys of the center.

(2) **Registration.** Voters are identified by the tally center, and then every identified voter obtains a vote with his intention of the election from the center.

[1] It is assumed that every registered voter submits his vote to the center in the voting stage.

(3) **Voting.** Voters submit their votes to the center. After receiving all of the votes, the center computes and publishes the result of the election.

(4) **Re-Registration.** If a re-voting activity is required, the tally center identifies the voters again, and then every identified voter obtains a vote with his intention for the re-voting from the center.

(5) **Re-Voting.** Voters submit their votes obtained at stage (4) to the center. After receiving all of the votes, the center computes and publishes the result of the re-voting.

2.3 A Partial Solution for Re-Voting Without Re-Registration

In [12], we have proposed an election protocol with only one round of registration action for a voting and a re-voting processes. Instead of embedding a voter's intention into his vote during the registration stage of a typical election protocol, we design an intention attachable ticket (IA-ticket) such that every voter can attach his intention to his vote after the registration stage of the election protocol. The intention attachability property is one of the key techniques to perform a voting and a re-voting processes with only one registration stage in the election protocol. We review the proposed scheme of [12] as follows.

(1) **Initialization.** The tally center selects two distinct large primes p_1 and p_2 at random. It computes $n = p_1 p_2$ and $\phi(n) = (p_1 - 1)(p_2 - 1)$. The center randomly chooses two large integers e and d such that $ed \equiv 1 \pmod{\phi(n)}$. Then, it publishes (e, n) and the necessary information of this election, such as the subject of the election and the list of candidates. Let all of the possible candidates or intentions of voters be numbered from 1 to k where k is a published small positive integer, say $k = 100$. In addition, F, G, and H are three public one-way hash functions [10, 23, 30]. Let $F^i(w) = F(F^{i-1}(w))$ and $G^i(y) = G(G^{i-1}(y))$ for every input w and y where i is a positive integer, $F^0(w) = w$, and $G^0(y) = y$. We define $w_i = F^{k-i}(w)$ and $y_i = G^{k-i}(y)$ for every input w and y where $i \in \{1, 2, ..., k\}$.

(2) **Registration.** In the registration stage, the center identifies voters through an identification protocol. Every identified voter chooses a message m_1 containing his intention of the election. Then the voter randomly chooses

three integers r, w, and y, and computes both $\delta = (F^k(w)||G^k(y))$ and $\alpha = (r^e H(m_1||\delta) \bmod n)$ where $||$ is the string concatenation operator. The voter submits α to the center. After receiving α, the center derives $t = (\alpha^d \bmod n)$ and sends t to the voter. After receiving t, the voter computes $s = (r^{-1}t \bmod n)$. The 4-tuple (m_1, s, w, y) is an IA-ticket of the voter.

(3) **Voting.** In the voting stage, the voter submits his vote (m_1, s, δ) to the center through an anonymous channel, where $\delta = (F^k(w)||G^k(y))$. The center verifies the vote by checking if

$$s^e \equiv H(m_1||\delta) \pmod{n}$$

and then publishes (m_1, s, δ). In addition, the center publishes all of the other valid votes, and computes the result of the election.

(4) **Re-Voting.** If a re-voting stage is required, every voter just needs to perform another round of voting without an extra round of registration actions. First, the voter determines his intention $m_2 \in \{1, 2, ..., k\}$ for the re-voting stage. Then the voter computes $w_{m_2} = F^{k-m_2}(w)$ and $y_{k-m_2} = G^{m_2}(y)$, and sends his vote $(m_2, s, w_{m_2}, y_{k-m_2})$ to the center through an anonymous channel. After receiving $(m_2, s, w_{m_2}, y_{k-m_2})$, the center verifies the vote by checking if

$$s^e \equiv H(m_1||F^{m_2}(w_{m_2})||G^{k-m_2}(y_{k-m_2}))$$

(mod n). Finally, the center publishes all of the valid votes it receives in the stage, and computes the result of the re-voting stage.

The advantages and disadvantages of the election protocol are summarized below.

Advantage: The election protocol can perform a re-voting process without a re-registration stage.

Disadvantage: If the re-voting stage (stage 4) of the protocol is required, everyone can link a voter's intention m_1 in the voting stage to the voter's intention m_2 in the re-voting stage after both of them are published. The unlinkability property is not preserved in the election protocol.

3 A Privacy Enhanced Solution for Re-Voting Without Re-Registration

In this section we introduce an election scheme with unlinkable spare votes for re-voting. The proposed scheme not only finish the re-voting process without re-registration but anyone else cannot link the two intentions of a voter in the two rounds of voting together.

3.1 The Proposed Election Scheme

The proposed election protocol for simplifying the re-voting process consists of four stages shown as follows.

(1) **Initialization.** The tally center publishes the necessary information of an election, such as the subject of the election, the list of candidates, and the public keys of the center.

(2) **Registration.** Voters are identified by the tally center, and then every identified voter obtains an unlinkably dividable and intention attachable ticket ($UDIA$-ticket) from the center. The $UDIA$-ticket can be unlinkably divided into a main vote and a spare vote where the main vote contains the voter's intention of the voting stage and the spare vote is intention attachable for the re-voting stage.

(3) **Voting.** Every voter derives the main vote from his $UDIA$-ticket, and submits the vote to the tally center through an anonymous channel. After receiving all of the main votes submitted by the voters, the tally center verifies and publishes them along with the result of the election.

(4) **Re-Voting.** If a re-voting stage is required, every voter computes the spare vote from his $UDIA$-ticket, and then puts his intention into the vote and submits it to the tally center through anonymous channels. After receiving all of the spare votes, the tally center verifies and publishes them along with the result of the re-voting stage.

The details of every stage of the proposed election protocol are described in the following subsections, respectively.

3.1.1 Initialization Initially, the tally center randomly selects two distinct large primes p_1 and p_2 where $p_1 \equiv p_2 \equiv 3 \pmod 4$. The center computes $n = p_1 p_2$ and $\phi(n) = (p_1 - 1)(p_2 - 1)$. The center randomly chooses two large integers e and

d such that $ed \equiv 1 \pmod{\phi(n)}$. Then, it publishes (e, n) and the necessary information of this election, such as the subject of the election and the list of candidates. Let k be the possibly maximal amount of candidates or intentions of voters, say $k = 100$, and these candidates or intentions are numbered from 1 to k. In addition, F, G, and H are three public one-way hash functions.

3.1.2 Registration In the registration stage, the center identifies voters through identification protocols. Every identified voter chooses a message m_1 which contains his own intention of the election. Then the voter randomly chooses four integers u, v, w, and y in Z_n^*, and computes both $\delta = (F^k(w)||G^k(y))$ and $\alpha = (\delta^4 H(m_1)(u^2 + v^2) \bmod n)$. The voter submits α to the center.

After receiving α, the center randomly selects x such that $(\alpha(x^2+1) \bmod n)$ is a quadratic residue in Z_n^* [24, 30], and then sends the integer x to the voter.

After receiving x, the voter randomly chooses an integer b in Z_n^*, and then submits $\beta = (b^{2e}(u - vx) \bmod n)$ to the center.

After receiving β, the center derives an integer t in Z_n^* such that

$$t^4 \equiv (\alpha(x^2 + 1)\beta^{-2})^d \pmod{n}$$

since the center knows d, p_1, and p_2 [24, 30]. Hence, the integer t is one of the 4th roots of $((\alpha(x^2+1)\beta^{-2})^d \bmod n)$ in Z_n^*. The center sends t to the voter.

After receiving t, the voter computes

$$\begin{cases} c_1 = (ux + v)(u - vx)^{-1} \bmod n \\ s = bt \bmod n. \end{cases}$$

The 5-tuple (c_1, m_1, s, w, y) is a *UDIA*-ticket of the voter.

3.1.3 Voting In the voting stage, the voter computes $s_1 = (\delta^{-1} s^e \bmod n)$, and then submits the main vote (c_1, m_1, s_1) derived from his *UDIA*-ticket (c_1, m_1, s, w, y) to the center through an anonymous channel. The center verifies the vote by checking if

$$s_1^4 \equiv H(m_1)(c_1^2 + 1) \pmod{n}$$

and then the center publishes (c_1, m_1, s_1). In addition, the center publishes all of the other valid main votes and the result of the election.

3.1.4 Re-Voting If a re-voting stage is required, the center publishes $\theta = (s_1^{-d} \bmod n)$ for every main vote (c_1, m_1, s_1) published in the voting stage. The voter determines his intention $m_2 \in \{1, 2, ..., k\}$ for the re-voting stage. The voter computes $w_{m_2} = F^{k-m_2}(w)$, $y_{k-m_2} = G^{m_2}(y)$, and $s_2 = (s\theta \bmod n)$. He sends his spare vote $(m_2, s_2, w_{m_2}, y_{k-m_2})$ to the center through an anonymous channel. After receiving $(m_2, s_2, w_{m_2}, y_{k-m_2})$, the center verifies the vote by checking if

$$s_2^e \equiv (F^{m_2}(w_{m_2})||G^{k-m_2}(y_{k-m_2})) \pmod{n}.$$

Finally, the center publishes all of the valid spare votes it receives, and then computes and publishes the result of the re-voting stage.

3.2 Summary

We briefly summarize the features of the proposed election protocol in the followings.

Advantage 1: The proposed election protocol of section 3 can perform a re-voting process without an extra round of registration actions between every voter and the tally center.

Advantage 2: It is computationally infeasible for anyone else to derive the link between the main vote and the spare vote derived by a voter from his *UDIA*-ticket even when both of them are published in the proposed election protocol. This feature will be discussed in section 4.3.

4 Discussions

In this section we examine the correctness, security, and privacy of the election protocol proposed in section 3.

4.1 Protocol Correctness

First, we examine the correctness of the proposed election protocol of section 3 in the followings.

Theorem 1 *If (c_1, m_1, s_1) is a voter's main vote derived from his UDIA-ticket produced by the election protocol of section 3, then*

$$s_1^4 \equiv H(m_1)(c_1^2 + 1) \ (mod\ n).$$

Proof. By the Chinese remainder theorem [30], every integer g in Z_n^* can be represented by $< g_1, g_2 >$ where $g_1 = (g \bmod p_1)$ and $g_2 = (g \bmod p_2)$. For convenience, $< g_1, g_2 >$ is denoted by $< g >$ sometimes. For every $< g > = < g_1, g_2 >$ and $< h > = < h_1, h_2 >$ in Z_n^*, $< gh \bmod n > = < g_1 h_1 \bmod p_1, g_2 h_2 \bmod p_2 >$, and $< g^{-1}$

mod n $>=<$ g_1^{-1} mod p_1, g_2^{-1} mod $p_2>$. In addition, for every $<g_1,g_2>$ and $<h_1,h_2>$ in Z_n^*, $<g_1,g_2>=<h_1,h_2>$ if and only if $g_1 \equiv h_1 \pmod{p_1}$ and $g_2 \equiv h_2 \pmod{p_2}$. If g is a quadratic residue in Z_n^*, then there are totally four different square roots of g in Z_n^* [30].

Since $(\alpha(x^2+1) \bmod n)$ is a quadratic residue in Z_n^*, we have that $(\alpha(x^2+1)\beta^{-2})^d$
$\equiv (\delta^4 H(m_1)(u^2+v^2)(x^2+1)b^{-4e}(u-vx)^{-2})^d$
$\equiv b^{-4}(\delta^4 H(m_1)(u^2+v^2)(x^2+1)(u-vx)^{-2})^d$
$\equiv b^{-4}(\delta^4 H(m_1)((ux+v)^2+(u-vx)^2)(u-vx)^{-2})^d$
$\equiv b^{-4}(\delta^4 H(m_1)((ux+v)^2(u-vx)^{-2}+1))^d$
$\equiv b^{-4}(\delta^4 H(m_1)(c_1^2+1))^d \pmod n$
is a quadratic residue in Z_n^*. As both $(b^{-4} \bmod n)$ and $(\delta^4 \bmod n)$ are quadratic residues in Z_n^*, the integer $(H(m_1)(c_1^2+1) \bmod n)$ is also a quadratic residue in Z_n^*. If $<z_1,z_2>$ is one of the 4th roots of the integer $(H(m_1)(c_1^2+1) \bmod n)$ in Z_n^*, then the four 4th roots of the integer in Z_n^* are $<\pm z_1, \pm z_2>$. Thus, the four 4th roots of $(b^{-4}\delta^{4d}(H(m_1)(c_1^2+1))^d \bmod n)$ in Z_n^* are $<\pm b_1^{-1}\delta_1^d z_1^d, \pm b_2^{-1}\delta_2^d z_2^d>$. As $t^4 \equiv b^{-4}\delta^{4d}(H(m_1)(c_1^2+1))^d \pmod n$, t belongs to $\{<\pm b_1^{-1}\delta_1^d z_1^d, \pm b_2^{-1}\delta_2^d z_2^d>\}$. Since $s_1 = (\delta^{-1}s^e \bmod n) = (\delta^{-1}b^e t^e \bmod n)$, s_1 is an element in $\{<\pm\delta_1^{-1}b_1^e b_1^{-e}\delta_1 z_1, \pm\delta_2^{-1}b_2^e b_2^{-e}\delta_2 z_2>\} = \{<\pm z_1, \pm z_2>\}$. It follows that s_1 is a 4th root of the integer $(H(m_1)(c_1^2+1) \bmod n)$ in Z_n^*. Hence, $s_1^4 \equiv H(m_1)(c_1^2+1) \pmod n$. □

In addition, if $(m_2, s_2, w_{m_2}, y_{k-m_2})$ is a voter's spare vote derived from his $UDIA$-ticket produced by the election protocol of section 3, then we have that $s_2^e \equiv (s\theta)^e \equiv s^e\theta^e \equiv \delta s_1 s_1^{-1} \equiv \delta \equiv (F^k(w)||G^k(y)) \equiv (F^{m_2}(w_{m_2})||G^{k-m_2}(y_{k-m_2})) \pmod n$.

4.2 Tally Correctness

The proposed election protocol is based on Chaum's blind signature scheme [5] and Fan-Lei's blind signature protocol [11]. The difficulty of forging a main vote (c_1, m_1, s_1) such that $s_1^4 \equiv H(m_1)(c_1^2+1) \pmod n$ depends on the security of Fan-Lei's blind signature scheme. Since every registered voter has to submit his vote to the tally center, the center cannot publish a vote other than these main votes of the voters in the voting stage without being detected by them. Hence, the tally correctness of the voting stage in the proposed protocol is guaranteed if Fan-Lei's blind signatures are unforgeable.

The difficulty of forging a triple (s_2, w, y) such that $s_2^e \equiv (F^k(w)||G^k(y)) \pmod n$ in the proposed election protocol relies on the security of Chaum's blind signature scheme. In our protocol, if $(m_2, s_2, w_{m_2}, y_{k-m_2})$ is the spare vote of a voter published in the re-voting stage, it is infeasible for anyone else to compute $(m_2', s_2, w_{m_2'}, y_{k-m_2'})$ with $m_2 \neq m_2'$ such that $(F^{m_2}(w_{m_2})||G^{k-m_2}(y_{k-m_2})) \equiv (F^{m_2'}(w_{m_2'})||G^{k-m_2'}(y_{k-m_2'})) \pmod n$ because F and G are one-way. Hence, if the center receives two spare votes $(m_2, s_2, w_{m_2}, y_{k-m_2})$ and $(m_2', s_2, w_{m_2'}, y_{k-m_2'})$ with $m_2 \neq m_2'$, these two spare votes are considered to be invalid by the center since they are submitted by the same voter. In addition, every registered voter must submit his spare vote to the tally center in the re-voting stage. Therefore, the tally correctness at the re-voting stage of the proposed election protocol is also ensured if Chaum's blind signatures are unforgeable.

4.3 Privacy Protection

For every instance, numbered i, of the registration protocol in the proposed election scheme of section 3, the tally center can record the parameters (α_i, β_i) received from the voter communicating with it during the instance i of the registration protocol. The triple (α_i, β_i, x_i) is usually referred to as the *view* of the tally center to the instance i of the registration protocol. Thus, we have the following theorem.

Theorem 2 *Given the main vote $(c_{1_A}, m_{1_A}, s_{1_A})$ of a voter named A and the spare vote $(m_{2_B}, s_{2_B}, w_{m_{2_B}}, y_{k-m_{2_B}})$ of another voter named B, the tally center can derive b, u, and v for every recorded (α_i, β_i, x_i) such that*

$$\begin{cases} c_{1_A} \equiv (ux_i+v)(u-vx_i)^{-1} \ (mod\ n) \\ \alpha_i \equiv (F^{m_{2_B}}(w_{m_{2_B}})||G^{k-m_{2_B}}(y_{k-m_{2_B}}))^4 \\ \qquad H(m_{1_A})(u^2+v^2) \ (mod\ n) \\ \beta_i \equiv b^{2e}(u-vx_i) \ (mod\ n). \end{cases}$$

Proof. If $c_{1_A} \equiv (ux_i+v)(u-vx_i)^{-1} \pmod n$, we have that $u \equiv v(c_{1_A}x_i+1)(c_{1_A}-x_i)^{-1} \pmod n$. For every quadratic residue r in Z_n^*, we define that $(r^{\frac{1}{2}} \bmod n)$ is a square root of r in Z_n^* where $(r^{\frac{1}{2}} \bmod n)$ has four different values in Z_n^* because n is the product of two distinct primes [24, 30]. From section 4.1, $s_{1_A}^4 \equiv H(m_{1_A})(c_{1_A}^2+1) \pmod n$ and $s_{2_B}^e \equiv (F^{m_{2_B}}(w_{m_{2_B}})||G^{k-m_{2_B}}(y_{k-m_{2_B}})) \pmod n$. If $\alpha_i \equiv (F^{m_{2_B}}(w_{m_{2_B}})||G^{k-m_{2_B}}(y_{k-m_{2_B}}))^4 H(m_{1_A})(u^2+v^2) \pmod n$, then we have that α_i
$\equiv \delta_B^4 H(m_{1_A})(u^2+v^2)$
$\equiv \delta_B^4 H(m_{1_A})(v^2(c_{1_A}x_i+1)^2(c_{1_A}-x_i)^{-2}+v^2)$
$\equiv \delta_B^4 H(m_{1_A})v^2((c_{1_A}x_i+1)^2(c_{1_A}-x_i)^{-2}+1)$
$\equiv \delta_B^4 H(m_{1_A})v^2(c_{1_A}^2+1)(x_i^2+1)(c_{1_A}-x_i)^{-2}$
$\equiv \delta_B^4 v^2 s_{1_A}^4(x_i^2+1)(c_{1_A}-x_i)^{-2} \pmod n$, $v^2 \equiv \delta_B^{-4}s_{1_A}^{-4}\alpha_i(x_i^2+1)^{-1}(c_{1_A}-x_i)^2 \equiv \delta_B^{-4}s_{1_A}^{-4}\alpha_i(x_i^2+$

$1)(x_i^2+1)^{-2}(c_{1_A}-x_i)^2 \pmod n$, and $v \equiv \delta_B^{-2}s_{1_A}^{-2}(\alpha_i(x_i^2+1))^{\frac{1}{2}}(x_i^2+1)^{-1}(c_{1_A}-x_i) \pmod n$. The integer $(\alpha_i(x_i^2+1) \bmod n)$ a quadratic residues in Z_n^*, so that $((\alpha_i(x_i^2+1))^{\frac{1}{2}} \bmod n)$ exist in Z_n^* and v also has four different values in Z_n^*. Thus, if $\beta_i \equiv b^{2e}(u-vx_i) \pmod n$, we have that $\beta_i \equiv b^{2e}(\delta_B^{-2}s_{1_A}^{-2}(\alpha_i(x_i^2+1))^{\frac{1}{2}}(x_i^2+1)^{-1}(c_{1_A}x_i+1)-\delta_B^{-2}s_{1_A}^{-2}(\alpha_i(x_i^2+1))^{\frac{1}{2}}(x_i^2+1)^{-1}(c_{1_A}-x_i)x_i) \equiv b^{2e}\delta_B^{-2}s_{1_A}^{-2}(\alpha_i(x_i^2+1))^{\frac{1}{2}}(x_i^2+1)^{-1}((c_{1_A}x_i+1)-(c_{1_A}-x_i)x_i) \equiv b^{2e}\delta_B^{-2}s_{1_A}^{-2}(\alpha_i(x_i^2+1))^{\frac{1}{2}}(x_i^2+1)^{-1}(x_i^2+1) \equiv b^{2e}\delta_B^{-2}s_{1_A}^{-2}(\alpha_i(x_i^2+1))^{\frac{1}{2}} \pmod n$, $b^{2e} \equiv \beta_i\delta_B^2 s_{1_A}^2(\alpha_i(x_i^2+1))^{-\frac{1}{2}} \pmod n$, and $b^2 \equiv (\beta_i\delta_B^2 s_{1_A}^2(\alpha_i(x_i^2+1))^{-\frac{1}{2}})^d \pmod n$.
Since there must exist exactly one value among the four different values of $((\alpha_i(x_i^2+1))^{-\frac{1}{2}} \bmod n)$ such that $((\beta_i\delta_B^2 s_{1_A}^2(\alpha_i(x_i^2+1))^{-\frac{1}{2}})^d \bmod n)$ is a quadratic residue in Z_n^* [30], we can also derive four different values of b in Z_n^* from the congruence $b^2 \equiv (\beta_i\delta_B^2 s_{1_A}^2(\alpha_i(x_i^2+1))^{-\frac{1}{2}})^d \pmod n$. □

Hence, given A's main vote $(c_{1_A}, m_{1_A}, s_{1_A})$ and B's spare vote $(m_{2_B}, s_{2_B}, w_{m_{2_B}}, y_{k-m_{2_B}})$, the tally center can always derive the three blinding factors b, u, and v for every recorded (α_i, β_i, x_i). It turns out that all of the main votes or the spare votes are indistinguishable from the center's point of view. Therefore, it is computationally infeasible for the center to derive the link between an instance i of the registration protocol and the main vote or the spare vote produced by that protocol. Besides, the integer $\theta = (s_1^{-d} \bmod n)$ is computed and published by the tally center for every main vote (c_1, m_1, s_1), so that it is computationally infeasible for the center to derive the link between a given main vote and its corresponding spare vote after both of them are published. Since the unlinkability is preserved and every voter submits his vote on an anonymous channel [4, 6], the privacy of voters is protected in the proposed election scheme.

5 Conclusions

With the proposed election protocol, we can simplify the possible re-voting process by eliminating the redundant re-registration action between every voter and the tally center. Furthermore, we have presented a method to unlinkably divide a ticket into two votes to successfully preserve the unlinkability property in the proposed scheme.

Acknowledgment

We would like to thank the anonymous referees of this paper for their valuable comments.

References

[1] J. Borrell and J. Rifa, "An Implementable Secure Voting Scheme," Computers & Security, Vol. 15, No. 4, pp. 327-338, 1996.

[2] C. Boyd, "A New Multiple Key Ciphers and an Improved Voting Scheme," Advances in Cryptology-EUROCRYPT'89, LNCS 434, Springer-Verlag, pp. 617-625, 1990.

[3] J. Camenisch, J. Piveteau, and M. Stadler, "Blind Signatures Based on the Discrete Logarithm Problem," Advances in Cryptology-EUROCRYPT'94, LNCS 950, Springer-Verlag, pp. 428-432, 1995.

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

[5] D. Chaum, "Blind Signatures for Untraceable Payments," Advances in Cryptology-CRYPTO'82, Springer-Verlag, pp. 199-203, 1983.

[6] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," Journal of Cryptology, Vol. 1, No. 1, pp. 65-75, 1988.

[7] J. Cohen and M. Fisher, "A Robust and Verifiable Cryptographically Secure Election Scheme," Proceedings of the 26th IEEE Symposium on Foundations of Computer Science, pp. 372-382, 1985.

[8] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung, "Multi-Authority Secret-Ballot Elections with Linear Work," Advances in Cryptology-EUROCRYPT'96, Springer-Verlag, pp. 72-83, 1996.

[9] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol. 31, pp. 469-472, 1985.

[10] A. Evans, W. Kantrowitz, and E. Weiss, "A User Authentication Scheme Not Requiring Secrecy in the Computer," Communications of the ACM, Vol. 17, No. 8, pp. 437-442, 1974.

[11] C. Fan and C. Lei, "User Efficient Blind Signatures," Electronics Letters, Vol. 34, No. 6, pp. 544-546, 1998.

[12] C. Fan, C. Lei, and C. Chang, "An Efficient Election Scheme for Resolving Ties," International Computer Symposium, Workshop on Cryptology and Information Security, Tainan, Taiwan, R.O.C., pp. 95-100, 1998.

[13] N. Ferguson, "Single Term Off-Line Coins," Advances in Cryptology-EUROCRYPT'93, LNCS 765, Springer-Verlag, pp. 318-328, 1994.

[14] A. Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections," Advances in Cryptology-AUSCRYPT'92, LNCS 718, Springer-Verlag, pp. 244-251, 1992.

[15] K. Iversen, "A Cryptographic Scheme for Computerized General Elections," Advances in Cryptology-CRYPTO'91, LNCS 576, Springer-Verlag, pp. 405-419, 1991.

[16] M. Michels and P. Horster, "Some Remarks on a Receipt-Free and Universally Verifiable Mix-Type Voting Scheme," Advances in Cryptology-ASIACRYPT'96, LNCS 1163, Springer-Verlag, pp. 125-132, 1996.

[17] H. Nurmi, A. Salomaa, and L. Santean, "Secret Ballot Elections in Computer Networks," Computers & Security, Vol. 10, pp. 553-560, 1991.

[18] K. Nyberg and R. Rueppel, "A New Signature Scheme Based on the DSA Giving Message Recovery Schemes," The first ACM Conference on Computer and Communications Security, Fairfax, Virginia, pp. 58-61, 1993.

[19] T. Okamoto, "Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes," Advances in Cryptology-CRYPTO'92, Springer-Verlag, LNCS 740, pp. 31-53, 1992.

[20] S. Pohlig and M. Hellman, "An Improved Algorithm for Computing Logarithms over GF(p) and Its Cryptographic Significance," IEEE Transactions on Information Theory, Vol. 24, pp. 106-110, 1978.

[21] D. Pointcheval and J. Stern, "Provably Secure Blind Signature Schemes," Advances in Cryptology-ASIACRYPT'96, LNCS 1163, Springer-Verlag, pp. 252-265, 1996.

[22] D. Pointcheval and J. Stern, "New Blind Signatures Equivalent to Factorization," Proceedings of the 4th ACM Conference on Computer and Communication Security, pp. 92-99, 1997.

[23] G. Purdy, "A High Security Log-in Procedure," Communications of the ACM, Vol. 17, No. 8, pp. 442-445, 1974.

[24] M. Rabin, "Digitalized Signatures and Public-Key Functions as Intractable as Factorization," Technical Report, MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, Mass. Jan. 1979.

[25] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, pp. 120-126, 1978.

[26] K. Sako, "Electronic Voting Schemes Allowing Open Objection to the Tally," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E77-A, No. 1, pp. 24-30, 1994.

[27] K. Sako and J. Kilian, "Secure Voting Using Partially Compatible Homomorphisms," Advances in Cryptology-CRYPTO'94, LNCS 839, Springer-Verlag, pp. 411-424, 1994.

[28] K. Sako and J. Kilian, "Receipt-Free Mix-Type Voting Scheme," Advances in Cryptology-EUROCRYPT'95, Springer-Verlag, pp. 393-403, 1995.

[29] C. Schnorr, "Efficient Identification and Signatures for Smart Cards," Advances in Cryptology-CRYPTO'89, Springer-Verlag, LNCS 435, pp. 235-251, 1990.

[30] G. Simmons, Contemporary Cryptology: The Science of Information Integrity, IEEE Press, N.Y., 1992.

[31] P. Slessenger, "Socially Secure Cryptographic Election Scheme," Electronics Letters, Vol. 27, No. 11, pp. 955-957, 1991.

[32] H. Williams, "A Modification of the RSA Public-Key Encryption Procedure," IEEE Transactions on Information Theory, Vol. 26, No. 6, pp. 726-729, 1980.