Journal of Network and Computer Applications (2002) **25**, 93–107
doi: 10.1006/jnca.2002.0132, available online at http://www.idealibrary.com on IDEAL®

An unlinkably divisible and intention attachable ticket scheme for runoff elections†

Chun-I Fan‡¶ and Chin-Laung Lei§*

‡ *Telecommunication Laboratories, Chunghwa Telecom Co., Ltd., 12, Lane 551, Min-Tsu Road Sec. 5, Yang-Mei, Tao-Yuan, Taiwan 326, R.O.C.*
§ *Department of Electrical Engineering, National Taiwan University, 1, Roosevelt Road Sec. 4, Taipei, Taiwan 107, R.O.C.*

(Received 11 June 2001; accepted 23 May 2002)

In a runoff election, the second round of voting must be performed to elect an absolute-majority winner when no candidate receives more than 50% of the votes in the first round of voting. Many states, such as France, Portugal, and Russia, have adopted this type of voting systems to elect their Presidents. In this paper, an unlinkably divisible and intention attachable ticket scheme is designed for runoff elections. A ticket in our scheme is composed of a main vote and a spare vote. The main vote containing some voter's intention can be extracted from the ticket for the first round of voting. If the second round of voting is required, the tally center enables the spare votes such that each voter can derive a spare vote from his ticket. A voter can then attach his intention to his spare vote for the second round of voting and, especially, the spare vote cannot be linked to the main vote by the tally center.

1. Introduction

Electronic voting makes it possible for voters to submit their votes to the tally center through communication networks. Compared to the traditional election systems, the technique of electronic voting shortens the time consumed by the election activities [13].

An anonymous electronic election protocol contains two types of participants, a tally center and a group of voters, and the protocol has three stages, i.e., initialization, registration, and voting. At the initialization stage, the tally center publishes some necessary information, such as the subject of the election and the list of candidates, for the election. At the registration stage, the voters are identified by the tally center through some secure identification mechanisms [15,22], and then

† A partial result of this paper was presented at International Computer Symposium, Workshop on Cryptology and Information Security, Tainan, Taiwan, R.O.C., December 17 – 19, 1998.
* Corresponding author: E-mail: lei@cc.ee.ntu.edu.tw;
¶ E-mail: chunifan@ms35.hinet.net

each identified voter obtains a vote with his intention for the election from the center by performing a secure blind signature protocol [3,6,9] between the voter and the center. At the voting stage, the voters submit their votes to the center through anonymous channels [5,7], and then, after receiving these votes, the center verifies and publishes them.

Typically, the candidate which receives the highest votes among all of the candidates is the winner of the election. This is called a *relative-plurality* election. In an *absolute-majority* election system, the winner must receive more than 50% of the votes in the election. *Runoff* elections are usually adopted to decide the winner in an absolute-majority election system [4]. In a runoff election, if an absolute-majority winner has been elected in the first round of voting, then the voting process terminates; otherwise the second round of voting must be performed to decide the exact winner from the two candidates who have received the highest votes among all of the candidates in the first round of voting. Many states, such as Austria, Brazil, Bulgaria, Chile, Colombia, Ecuador, Finland, France, Madagascar, Mali, Mozambique, Poland, Portugal, and Russia, have adopted the runoff election systems to elect their Presidents.

Ideally, the electronic voting protocols for runoff elections should possess the following properties:

1. *One-round registration.* In a runoff election, the second round of voting is usually performed shortly after the first round of voting when necessary. Re-registration actions for the second round of voting seem to be redundant since they are just performed in the same group of voters for the first round of voting. The cost of re-registration is usually high in a large-scale election. Hence, the unnecessary redundant re-registration for the second round of voting should be removed from the runoff election.
2. *Spare-votes enability.* To avoid some possible abuses of the spare votes for the second round of voting, such as the voters submit them to the center for the first round of voting, ideally, these spare votes for the second voting should not be enabled until they are really needed. In a runoff election, voters cannot obtain their spare votes until the second round of voting is about to be performed. This is the *spare-votes enability* property.
3. *Votes unlinkability.* In a runoff election, there are two sets V_1 and V_2 of votes where V_1 consists of all votes for the first voting and V_2 contains all votes for the second voting. For privacy consideration, given any two votes $v_1 \in V_1$ and $v_2 \in V_2$, (v_1, v_2) can be the two votes of any voter for the two rounds of voting from the center's point of view, that is, all of the votes in V_i for each $i \in \{1, 2\}$ are equally-likely form the center's point of view. This is called the *votes unlinkability* property in runoff elections.

In this paper, we propose an unlinkably divisible and intention attachable voting ticket scheme for runoff elections. In the scheme each identified voter can obtain an unlinkably dividable and intention attachable ticket (*UDIA*-ticket) from the center at the registration stage of the election. A *UDIA*-ticket is composed of a main vote and a spare vote. The main vote containing some voter's intention for the election can be extracted from the ticket and it is submitted to the tally center in the first round of voting. The spare vote contains all possible intentions of the voter for the possible second round of voting. If the second round of voting is required, the center enables the spare votes such that the voter can derive a spare vote from his ticket, and then the voter just needs to attach his intention to his spare vote and submits it to the center without the second round of registration. Because of two candidates only, an absolute-majority winner can be elected in the second round of voting. In the proposed scheme the center cannot know the exact correspondence between the main vote and the spare vote derived from the same ticket. This is the votes unlinkability property.

This paper focuses on the unlinkable division of the tickets and the intention attachability of the spare votes for runoff elections. To simplify the presentation, we adopt a basic anonymous election protocol which possesses the tally correctness and anonymity properties to explain our idea. There are some other properties, such as receipt freeness [2], fairness [10], open objection [20], and so on, of anonymous electronic election protocols which have been discussed in the literature. Certainly, they are also interesting research topics to consider these properties in runoff elections. However, they are beyond the scope of the paper.

The rest of the paper is organized as follows. We review some fundamental techniques related to the research in Section 2. In Section 3, an anonymous electronic election scheme tailored for runoff elections 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 review some related techniques for anonymous electronic elections. Three underlying techniques are usually adopted to build an anonymous electronic election protocol, that is, secure identification schemes [15,22], blind signatures [3,6,9,12,16,17], and anonymous channels [5,7]. First, an identification scheme is always used to identify voters in an electronic election system through computers and communication networks [15,22]. 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 each published vote and the instance of the registration protocol producing that vote [3,6,9,12,16,17]. Finally, anonymous channels or untraceable electronic mails can protect the voters' identities when sending their votes to the tally center in most of the electronic election schemes proposed in the literatures [5,7].

2.1 *A typical anonymous electronic election scheme*

In the subsection, we present a typical anonymous electronic election protocol based on Chaum's blind signature scheme [6]. The protocol consists of three stages, initialization, registration, and voting, and the 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, such as the subject of the election and the list of candidates, of this election. In addition, let H be a public one-way hash function [8,18,23].
2. *Registration.* At the registration stage, the center identifies voters through an identification protocol [15,22]. Each 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 vote of the voter.
3. *Voting.* At the voting stage, the voter submits his vote (m, s) to the center through an anonymous channel [5,7].|| The center verifies the vote by checking if

$$s^e \equiv H(m) (\bmod n) \tag{1}$$

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

Owing to the unlinkability property of Chaum's blind signature scheme [6] and the anonymity of sender untraceable channels [5,7], 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 runoff elections*

If the second round of voting is required in a runoff election, we can repeat the entire election processes again. A straight-forward solution to deal with a runoff election is described below.

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

|| It is usually assumed that each registered voter has to submit his vote to the center in a typical anonymous electronic election protocol.

2. *Registration.* Voters are identified by the tally center, and then each identified voter obtains a blinded vote with his intention for the election from the center.
3. *Voting.* Voters unblind their blinded votes and submit their votes to the center by anonymous channels. After receiving all of the votes, the center computes and publishes the result of the election. If there is an absolute-majority winner, then the protocol terminates.
4. *Re-registration.* The tally center identifies all of the voters again, and then each identified voter obtains a blinded vote with his intention for the second round of voting from the center.
5. *Re-voting.* Voters unblind their blinded votes obtained at the re-registration stage and submit their votes to the center by anonymous channels. After receiving all of the votes, the center computes and publishes the result of the second round of voting.

In the protocol, the tally center cannot link the two votes together of any voter for the two rounds of voting because they are produced by two independent rounds of registration, respectively. This is the votes unlinkability property. Besides, it satisfies the spare-votes enability property, but it does not satisfy the one-round registration property.

2.3 *An intention attachable ticket scheme for runoff elections*

In a typical electronic voting protocol, such as the scheme of Section 2.1, the voters have to decide their intentions and put them in the messages *before* they submit the messages to the tally center for registration. If the voters can put their intentions in their votes *after* they receive the blinded votes from the center at the registration stage, then the votes are said to be *intention attachable*.

In [11], we have proposed an election protocol for runoff elections with only one round of registration. Instead of embedding a voter's intention into his vote at the registration stage in an election protocol, we design an intention attachable ticket (*IA*-ticket) such that each voter can attach his intention to his voting ticket after the registration stage of the election protocol. The intention attachability property is one of the key techniques for performing a runoff election by only one registration stage. We briefly review the proposed scheme of [11] below.

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 other necessary information of this election. Let k be the possibly maximal amount of candidates, say $k = 100$, and these candidates are numbered from 1 to k. In addition, F, G, and H are three public one-way hash functions [8,18,23]. Let $F^i(w) = F(F^{i-1}(w))$ and $G^i(y) = G(G^{i-1}(y))$ for each input w and y, where i is a positive integer, $F^0(w) = w$, and $G^0(y) = y$. We define that $w_i = F^{k-i}(w)$ and $y_i = G^{k-i}(y)$ for each input w and y where $i \in \{1, 2, \ldots, k\}$.

2. *Registration.* At the registration stage, the center identifies each voter through an identification protocol. Each identified voter chooses a message m_1 containing his intention of the election. The voter then randomly chooses three integers r, w, and y, and computes $\delta = (F^k(w) \| G^k(y))$ 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.* At the voting stage, the voter submits his vote (m_1, s, δ) to the center through an anonymous channel. The center verifies the vote by checking if

$$s^e \equiv H(m_1 \| \delta) (\bmod\, n) \tag{2}$$

   and then publishes (m_1, s, δ). In addition, the center publishes all of the other votes, and computes the result of the election. If there is an absolute-majority winner, then the protocol terminates.
4. *Re-voting.* If the second round of voting is required, each voter just needs to perform another round of voting without an extra round of registration. First, the voter determines his intention $m_2 \in \{1, 2, \ldots, k\}$ 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 the 4-tuple, the center verifies it by checking if

$$s^e \equiv H(m_1 \| F^{m_2}(w_{m_2}) \| G^{k-m_2}(y_{k-m_2})) (\bmod\, n). \tag{3}$$

   Finally, the center publishes all of the votes it receives at the stage, and publishes the result of the re-voting.

The election protocol can perform the second round of voting without an extra registration stage. However, if the re-voting stage of the protocol is performed, one can link the voter's intention m_1 at the voting stage to the voter's intention m_2 at the re-voting stage after both of them are published. It turns out that the votes unlinkability property is not satisfied in the election protocol.

2.4 *An enhanced intention attachable ticket scheme for runoff elections*

In this subsection we propose a simple enhanced version of the election protocol shown in Section 2.3 to cut off the link between the two intentions m_1 and m_2 of a voter. We describe it below.

1. *Initialization.* The tally center selects four distinct large primes p_1, p_2, p_3, and p_4 at random. It computes $n_1 = p_1 p_2$ and $n_2 = p_3 p_4$. The center randomly chooses four distinct large integers e_1, e_2, d_1, and d_2 such that $e_1 d_1 \equiv 1$ $(\bmod\, (p_1 - 1)(p_2 - 1))$ and $e_2 d_2 \equiv 1$ $(\bmod\, (p_3 - 1)(p_4 - 1))$. It then publishes (e_1, e_2, n_1, n_2) and the necessary information of this election. Let k be the possibly

maximal amount of candidates, and these candidates are numbered from 1 to k. In addition, F, G, and H are three public one-way hash functions.

2. *Registration.* At the registration stage, the center identifies voters, and each identified voter chooses m_1 containing his intention of the election. The voter then randomly chooses four integers r_1, r_2, w, and y, and computes $\alpha_1 = (r_1^{e_1} H(m_1) \bmod n_1)$, $\delta = H(F^k(w) \,||\, G^k(y))$, and $\alpha_2 = (r_2^{e_2}\delta \bmod n_2)$. The voter submits (α_1, α_2) to the center. After receiving (α_1, α_2), the center derives $t_1 = (\alpha_1^{d_1} \bmod n_1)$ and $t_2 = (\alpha_2^{d_2} \bmod n_2)$, and sends (t_1, t_2) to the voter. After receiving $(t_1,\ t_2)$, the voter computes $s_1 = (r_1^{-1} t_1 \bmod n_1)$ and $s_2 = (r_2^{-1} t_2 \bmod n_2)$.
3. *Voting.* At the voting stage, the voter submits his vote $(m_1,\ s_1)$ to the center through an anonymous channel. The center verifies the vote by checking if

$$s_1^{e_1} \equiv H(m_1) (\bmod\, n_1) \tag{4}$$

and then publishes $(m_1,\ s_1)$. In addition, the center publishes all of the other valid votes, and computes the result of the election. If there is an absolute-majority winner, then the protocol terminates.

4. *Re-voting.* The voter determines his intention $m_2 \in \{1, 2, \ldots, k\}$ 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 spare vote $(m_2, s_2, w_{m_2}, y_{k-m_2})$ to the center through an anonymous channel. After receiving the 4-tuple, the center verifies it by checking if

$$s_2^{e_2} \equiv H(F^{m_2}(w_{m_2}) \,||\, G^{k-m_2}(y_{k-m_2}))(\bmod\, n_2). \tag{5}$$

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

The election protocol performs only one round of registration, too. Also, it is computationally infeasible for anyone else to derive the link between the main vote (m_1, s_1) and the spare vote $(m_2, s_2, w_{m_2}, y_{k-m_2})$ of a voter when both of them are published. However, the protocol of Section 2.4 does not satisfy the spare-votes enability property.

3. A *UDIA*-ticket scheme for runoff elections

In an electronic runoff election system, a voting ticket issued by the center consists of the message and the signature parts where the former contains the intentions of a voter and the latter is the center's signature on the message part. If the message part m of a voting ticket can be divided into m_1 and m_2 and the corresponding signature part s can be divided into s_1 and s_2 by performing some computations such that (m_1, s_1) and (m_2, s_2) are two valid votes for the two rounds of voting, respectively, and s, s_1, and s_2 are of the same size, then the voting ticket is *divisible*. Furthermore, if it also satisfies the votes unlinkability property, then the voting ticket is *unlinkably divisible*.

In this section, we present an electronic election protocol with *UDIA*-tickets. The protocol requires only one round of registration, and satisfies both the votes unlinkability and spare-votes enability properties for runoff elections. The proposed protocol contains four stages shown below.

1. *Initialization.* The tally center publishes the necessary information, such as the subject of the election, the list of candidates, and the public keys of the center, of the election.
2. *Registration.* The voters are identified by the tally center, and then each identified voter obtains a *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 for the first round of voting and the spare vote is intention attachable for the possible second round of voting.
3. *Voting.* Each voter derives his 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. If an absolute-majority winner has been elected, then the protocol terminates.
4. *Re-voting.* The second round of voting is performed to elect an absolute-majority winner from the two candidates with the highest votes among all of the candidates in previous stage. The center enables the spare votes by publishing some messages such that each voter can derive his spare vote from his *UDIA*-ticket. The voter then puts his intention into the vote and submits it to the tally center through an anonymous channel. After receiving all of the spare votes, the tally center verifies and publishes them along with the result of the second round of voting.

The details of the above four stages are described in the following subsections, respectively.

3.1 *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 $ed \equiv 1 \pmod{\phi(n)}$. It then publishes (e, n), the subject of the election, the list of candidates, and an integer k where k is the amount of the candidates in the election and these candidates are numbered from 1 to k. In addition, F, G, and H are three public one-way hash functions.

3.2 *Registration*

At the registration stage, the center identifies the voters through secure identification protocols. Each identified voter chooses a message m_1 which contains his own intention for the election. The voter then randomly selects four integers u, v, w, and y, and computes $\delta = H(F^k(w) \,||\, G^k(y))$ 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 chooses x such that $(\alpha(x^2+1) \bmod n)$ is a quadratic residue in Z_n^* [19,23], i.e., there exists an integer a in Z_n^* such that $a^2 \equiv \alpha(x^2+1) \pmod{n}$. The center sends the integer x to the voter.

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

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

$$t^4 \equiv (\alpha(x^2+1)\beta^{-2})^d \pmod{n} \tag{6}$$

by some efficient algorithms [19,23]. 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

$$\begin{cases} c_1 = (ux+v)(u-vx))^{-1} \bmod n \\ s \ \ = bt \bmod n. \end{cases} \tag{7}$$

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

3.3 *Voting*

At the voting stage, the voter computes $s_1 = (\delta^{-1}s^e \bmod n)$, and then forms and submits the main vote (c_1, m_1, s_1) to the center through an anonymous channel. The center verifies the vote by checking if

$$s_1^4 \equiv H(m_1)(c_1^2+1) \pmod{n} \tag{8}$$

and then the center publishes (c_1, m_1, s_1). The center publishes all of the other main votes it receives and the result of the voting. If a candidate has received more than 50% of the main votes, then the candidate is the winner and the election protocol ends; otherwise all voters keep their *UDIA*-tickets in their computers or devices for the second round of voting.

3.4 *Re-voting*

Since no candidate received more than 50% of the main votes in the first round of voting, the second round of voting starts. The center publishes $\theta = (s_1^{-d} \bmod n)$ for each main vote (c_1, m_1, s_1) published in the previous stage.

The voter determines his intention $m_2 \in \{\hat{i}, \hat{j}\} \subset \{1, 2, \ldots, k\}$ with $\hat{i} \neq \hat{j}$ for the second round of the voting where the two candidates numbered $\hat{i}$ and $\hat{j}$ have received the highest votes among all of the candidates in the previous 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 forms and

** Since there are only two candidates in the second round of voting, we can take $k = 2$ in the protocol. However, if we do so, the tally center must re-number the two candidates from 1 to 2 and publish them again at the re-voting stage.

Table 1 *Properties comparison*

	Section 2.2	Section 2.3	Section 2.4	Section 3
One-round registration	No	Yes	Yes	Yes
Spare-votes enability	Yes	No	No	Yes
Votes unlinkability	Yes	No	Yes	Yes

sends his spare vote $(m_2, s_2, w_{m_2}, y_{k-m_2})$ to the center through an anonymous channel. After receiving the 4-tuple, the center verifies the spare vote by checking if

$$s_2^e \equiv H(F^{m_2}(w_{m_2}) \,||\, G^{k-m_2}(y_{k-m_2})) \pmod{n}. \tag{9}$$

Finally, the center publishes all of the spare votes it receives, and then computes and publishes the result of the re-voting. Because of only two candidates in the second round of voting, an absolute-majority winner can be elected and the protocol ends.

3.5 *Summary*

We summarize the properties of the proposed election protocol as follows.

1. The proposed election protocol of Section 3 can perform a re-voting process for the second round of voting without re-registration.
2. The tally center does not enable the spare votes until the second voting is needed since the center does not publish $\theta = (s_1^{-d} \bmod n)$ for each main vote (c_1, m_1, s_1) until the re-voting stage of the election protocol.
3. It is information-theoretically impossible for anyone else to derive the link between the main vote and the spare vote derived by some voter from his *UDIA*-ticket even when both of them are published in the proposed election protocol. This will be proved in Section 4.3.

The properties of the schemes shown in Section 2 and Section 3 are compared at Table 1.

4. Discussions

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

4.1 *Protocol correctness*

We examine the correctness of the proposed election protocol of Section 3 below.

Theorem 1. *If (c_1, m_1, s_1) is the voter's main vote derived from his UDIA-ticket produced by the election protocol of Section 3, then (8) is satisfied.*

Proof Since $(\alpha(x^2+1) \bmod n)$ is a quadratic residue in Z_n^*, we have that

$$\begin{aligned}
&(\alpha(x^2+1)\beta^{-2})^d \pmod n\\
&\quad\equiv (\delta^4 H(m_1)(u^2+v^2)(x^2+1)(b^{-4})^e(u-vx)^{-2})^d \pmod n\\
&\quad\equiv (b^{-4})^{ed}(\delta^4 H(m_1)(u^2+v^2)(x^2+1)(u-vx)^{-2})^d \pmod n\\
&\quad\equiv b^{-4}(\delta^4 H(m_1)((ux+v)^2+(u-vx)^2)(u-vx)^{-2})^d \pmod n\\
&\quad\equiv b^{-4}(\delta^4 H(m_1)((ux+v)^2(u-vx)^{-2}+1))^d \pmod n\\
&\quad\equiv b^{-4}(\delta^4 H(m_1)(c_1^2+1))^d \pmod n
\end{aligned}$$

is a quadratic residue in Z_n^*, too. Thus, the center can derive t such that $t^4 \equiv (\alpha(x^2+1)\beta^{-2})^d \equiv b^{-4}(\delta^4)^d(H(m_1)(c_1^2+1))^d \pmod n$. Since $s = (bt \bmod n)$ and $s_1 = (\delta^{-1}s^e \bmod n)$, $s_1^4 \equiv \delta^{-4}(s^4)^e \equiv \delta^{-4}(b^4)^e(t^4)^e \equiv H(m_1)(c_1^2+1) \pmod n$. □

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

4.2 *Tally correctness*

The proposed election protocol is based on Chaum's blind signature scheme [6] and Fan-Lei's blind signature protocol [9]. 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, and the difficulty of forging a triple (s_2, w, y) such that $s_2^e \equiv H(F^k(w)\,||\,G^k(y)) \pmod n$ relies on the security of Chaum's blind signatures. Besides, if $(m_2, s_2, w_{m_2}, y_{k-m_2})$ is the voter's spare vote published at the re-voting stage, it is intractable for anyone else to derive $(m_2', s_2, w_{m_2'}, y_{k-m_2'})$ with $m_2 \neq m_2'$ such that $(F^{m_2}(w_{m_2})\,||\,G^{k-m_2}(y_{k-m_2})) \equiv (F^{m_2'}(w_{m_2'})\,||\,G^{k-m_2'}(y_{k-m_2'})) \pmod n$ unless F or G is invertable. Hence, if F and G are strong and 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 because they are submitted by the same voter.

In addition, each registered voter has to submit his main vote and spare vote (if the re-voting stage is required) to the tally center, so that the center cannot publish a vote formed by itself without being detected by the voters.

From the above, the tally correctness of the election protocol depends on the security of Chaum's blind signatures [6], Fan-Lei's blind signatures [9], and one-way hash functions [1,14].

4.3 *Privacy protection*

For each 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 who communicated with the center 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 each view (α_i, β_i, x_i) such that

$$\begin{cases} c_{1_A} \equiv (ux_i + v)(u - vx_i)^{-1} \text{ (mod } n) \\ \alpha_i \equiv H(F^{m_{2_B}}(w_{m_{2_B}})||G^{k-m_{2_B}}(y_{k-m_{2_B}}))^4 H(m_{1_A})(u^2 + v^2) \text{ (mod} \, n) \\ \beta_i \equiv (b^2)^e (u - vx_i) \text{ (mod } n). \end{cases} \tag{10}$$

Proof If $c_{1_A} \equiv (ux_i + v)(u - vx_i)^{-1}$ (mod$\,n$), we have that $u \equiv v(c_{1_A}x_i + 1) \times (c_{1_A} - x_i)^{-1}$(mod n). For each quadratic residue r in Z_n^* we define that ($r^{1/2}$ mod$\,n$) is a square root of r in Z_n^* where ($r^{1/2}$ mod$\,n$) has four different values in Z_n^* because n is the product of two distinct primes [19,22]. By Section 4.1, $s_{1_A}^4 \equiv H(m_{1_A}) \times (c_{1_A}^2 + 1)$ (mod n) and $s_{2_B}^e \equiv H(F^{m_{2_B}}(w_{m_{2_B}}) \,||\, G^{k-m_{2_B}}(y_{k-m_{2_B}}))$ (mod n).

If $\alpha_i \equiv H(F^{m_{2_B}}(w_{m_{2_B}}) \,||\, G^{k-m_{2_B}}(y_{k-m_{2_B}}))^4 H(m_{1_A})(u^2 + v^2)$ (mod n), then we have the following derivations,

$$\begin{aligned} &\alpha_i \equiv \delta_B^4 H(m_{1_A})(u^2 + v^2) \text{ (mod } n) \\ &\alpha_i \equiv \delta_B^4 H(m_{1_A})(v^2(c_{1_A}x_i + 1)^2(c_{1_A} - x_i)^{-2} + v^2) \text{ (mod } n) \\ &\alpha_i \equiv \delta_B^4 H(m_{1_A})v^2((c_{1_A}x_i + 1)^2(c_{1_A} - x_i)^{-2} + 1) \text{ (mod } n) \\ &\alpha_i \equiv \delta_B^4 H(m_{1_A})v^2((c_{1_A}x_i + 1)^2 + (c_{1_A} - x_i)^2)(c_{1_A} - x_i)^{-2} \text{ (mod } n) \\ &\alpha_i \equiv \delta_B^4 H(m_{1_A})v^2(c_{1_A}^2 + 1)(x_i^2 + 1)(c_{1_A} - x_i)^{-2} \text{ (mod } n) \\ &\alpha_i \equiv \delta_B^4 v^2 s_{1_A}^4 (x_i^2 + 1)(c_{1_A} - x_i)^{-2} \text{ (mod } n) \\ &v^2 \equiv \delta_B^{-4} s_{1_A}^{-4} \alpha_i (x_i^2 + 1)^{-1}(c_{1_A} - x_i)^2 \text{ (mod } n) \\ &v^2 \equiv \delta_B^{-4} s_{1_A}^{-4} \alpha_i (x_i^2 + 1)(x_i^2 + 1)^{-2}(c_{1_A} - x_i)^2 \text{ (mod } n) \\ &\;\, v \equiv \delta_B^{-2} s_{1_A}^{-2} (\alpha_i(x_i^2 + 1))^{\frac{1}{2}}(x_i^2 + 1)^{-1}(c_{1_A} - x_i) \text{ (mod } n). \end{aligned}$$

The integer ($\alpha_i(x_i{}^2 + 1)$ mod n) is a quadratic residue in Z_n^*, so that $((\alpha_i(x_i^2 + 1))^{1/2}$ mod n) exists in Z_n^* and v also has four different values in Z_n^*. Thus, if $\beta_i \equiv (b^2)^e \times (u - vx_i)$ (mod n), we have that

$$\begin{aligned} \beta_i \equiv (b^2)^e (&\delta_B^{-2} s_{1_A}^{-2} (\alpha_i(x_i^2 + 1))^{\frac{1}{2}}(x_i^2 + 1)^{-1}(c_{1_A}x_i + 1) \\ &- \delta_B^{-2} s_{1_A}^{-2} (\alpha_i(x_i^2 + 1))^{\frac{1}{2}}(x_i^2 + 1)^{-1}(c_{1_A} - x_i)x_i) \text{ (mod } n) \end{aligned}$$

$$\beta_i \equiv (b^2)^e \delta_B^{-2} s_{1_A}^{-2} (\alpha_i(x_i^2+1))^{\frac{1}{2}} (x_i^2+1)^{-1} ((c_{1_A} x_i + 1) - (c_{1_A} - x_i) x_i) \pmod{n}$$

$$\beta_i \equiv (b^2)^e \delta_B^{-2} s_{1_A}^{-2} (\alpha_i(x_i^2+1))^{\frac{1}{2}} (x_i^2+1)^{-1} (x_i^2+1) \bmod n)$$

$$\beta_i \equiv (b^2)^e \delta_B^{-2} s_{1_A}^{-2} (\alpha_i(x_i^2+1))^{\frac{1}{2}} \pmod{n}$$

$$(b^2)^e \equiv \beta_i \delta_B^2 s_{1_A}^2 (\alpha_i(x_i^2+1))^{-\frac{1}{2}} \pmod{n}$$

$$b^2 \equiv (\beta_i \delta_B^2 s_{1_A}^2 (\alpha_i(x_i^2+1))^{-\frac{1}{2}})^d \pmod{n}.$$

Since there must exist exactly one value among the four different values of $((\alpha_i(x_i{}^2+1))^{-1/2} \bmod n)$ such that $((\beta_i \delta_B^2 s_{1_A}^2 (\alpha_i(x_i^2+1))^{-1/2})^d \bmod n)$ is a quadratic residue in Z_n^* [22], we can derive four different values of b in Z_n^* from the congruence $b^2 \equiv (\beta_i \delta_B^2 s_{1_A}^2 (\alpha_i(x_i^2+1))^{-1/2})^d \pmod{n}$. □

In the proposed scheme, the tally center cannot obtain the identity of any voter from the anonymous channel on which the voter's main and spare votes are transmitted to the center. In addition, by Theorem 2, the center cannot derive the link between a main vote (or a spare vote, respectively) divided from a *UDIA*-ticket and the instance of the registration protocol which produces that ticket. Moreover, the integer $\theta = (s_1^{-d} \bmod n)$ is published by the tally center for each main vote (c_1, m_1, s_1), so that the center cannot link a given main vote to its corresponding spare vote. Therefore, all of the main votes or the spare votes are equally likely from the center's point of view. This is the votes unlinkability property for runoff elections.

5. Conclusions

We have designed a *UDIA*-ticket scheme for an electronic runoff election with only one round of registration. The ticket can be unlinkably divided into two votes when the second round of voting is required, and the second vote is intention attachable such that the voter can attach his intention to the vote at the re-voting stage.

Acknowledgements

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

References

1. M. Bellare & P. Rogaway 1993. Random oracles are practical: a paradigm for designing efficient protocols. *Proceedings of the first ACM Conference on Computer and Communications Security* 62–73.
2. J. Benaloh & D. Tuinstra 1994. Receipt-free secret-ballot elections. *Proceedings of the 26th ACM Symposium on the Theory of Computing* 544–553.

3. J. Camenisch, J. Piveteau and M. Stadler 1995. Blind signatures based on the discrete logarithm problem. *Advances in Cryptology-EUROCRYPT'94*, LNCS 950, Springer-Verlag, 428–432.
4. A. Carstairs 1980. *A Short History of Electoral Systems in Western Europe*. London: George Allen & Unwin.
5. D. Chaum 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM* **24**(2), 84–88.
6. D. Chaum 1983. Blind signatures for untraceable payments. *Advances in Cryptology-CRYPTO'82*, Springer-Verlag, 199–203.
7. D. Chaum 1988. The dining cryptographers problem: unconditional sender and recipient untraceability. *Journal of Cryptology* **1**(1), 65–75.
8. A. Evans, W. Kantrowitz and E. Weiss 1974. A user authentication scheme not requiring secrecy in the computer. *Communications of the ACM* **17**(8), 437–442.
9. C. Fan & C. Lei 1998. User efficient blind signatures. *Electronics Letters* **34**(6), 544–546.
10. C. Fan and W. Chen 2001. An efficient blind signature scheme for information hiding. *International Journal of Electronic Commerce* **6**(1), 93–100.
11. C. Fan, C. Lei & C. Chang 1998. An efficient election scheme for resolving ties. *International Computer Symposium, Workshop on Cryptology and Information Security* 95–100.
12. N. Ferguson 1994. Single term off-line coins. *Advances in Cryptology-EUROCRYPT'93*, LNCS 765, Springer-Verlag, 318–328.
13. C. Lei & C. Fan 1998. A universal single-authority election system. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **E81-A**(10), 2186–2193.
14. A. Menezes, P. van Oorschot & S. Vanstone 1997. *Handbook of Applied Cryptography*, CRC Press LLC.
15. T. Okamoto 1992. Provably secure and practical identification schemes and corresponding signature schemes. *Advances in Cryptology-CRYPTO'92*, LNCS 740, Springer-Verlag, 31–53.
16. D. Pointcheval & J. Stern 1996. Provably secure blind signature schemes. *Advances in Cryptology-ASIACRYPT'96*, LNCS 1163, Springer-Verlag, 252–265.
17. D. Pointcheval & J. Stern 1997. New blind signatures equivalent to factorization. *Proceedings of the 4th ACM Conference on Computer and Communication Security* 92–99.
18. G. Purdy 1974. A high security log-in procedure. *Communications of the ACM* **17**(8), 442–445.
19. M. Rabin 1979. Digitalized signatures and public-key functions as intractable as factorization. *Technical Report*, MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, MA.
20. K. Sako 1994. Electronic voting schemes allowing open objection to the tally. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **E77-A**(1), 24–30.
21. C. Schnorr 1990. Efficient identification and signatures for smart cards. *Advances in Cryptology-CRYPTO'89*, LNCS 435, Springer-Verlag, 235–251.
22. G. Simmons 1992. *Contemporary Cryptology: The Science of Information Integrity*, NY: IEEE Press.

Chun-I Fan was born in Tainan, Taiwan on October 15, 1967. He received his MS degree in computer science and information engineering from National Chiao Tung University, Taiwan, in 1993, and the PhD degree in electrical engineering at National Taiwan University in 1998. In 1999, he joined Telecommunication Laboratories, Chunghwa Telecom Co., Ltd, Taiwan, and he is now an associate researcher. He is an editor of Information Security Newsletter, and he also is a member of Chinese Cryptology and Information Security Association. His current research interests include information security, cryptographic protocols, electronic cash, electronic voting, and electronic commerce.

Chin-Laung Lei was born in Taipei, Taiwan on January 9, 1958. He received the BS degree in electrical engineering from National Taiwan University in 1980, and the PhD degree in computer science from the University of Texas at Austin in 1986. From 1986 to 1988, he was an assistant professor of the computer and information science department at the Ohio State University, Columbus, Ohio, USA. In 1988 he joined the faculty of the department of electrical engineering, National Taiwan University, where he is now a professor. His current research interests include network security, cryptography, parallel and distributed computing, design and analysis of algorithms, and operating system design. Dr Lei is a member of the Institute of Electrical and Electronic Engineers and the Association for Computing Machinery.