An anonymous and flexible $t$-out-of-$n$ electronic voting scheme

Chin-Chen Chang$^{1,2}$

Jung-San Lee$^2$

$^1$Department of Information Engineering and Computer Science
Feng Chia University
100 Wenhwa Rd., Seatwen
Taichung 40724
Taiwan
R.O.C.

$^2$Department of Computer Science and Information Engineering
National Chung Cheng University
Chiayi
Taiwan, 621
R.O.C.

Abstract

Voting is always considered as the most important hallmarks in the democratic society. However, there are plenty of problems of the traditional election such as inconvenience, non-mobility, unfairness, non-anonymity, and so on. Furthermore, the cost of the traditional voting often places a heavy burden on the nation. To solve the problems of the traditional election, the concept of “electronic voting” is proposed, where people are allowed to vote over the Internet. The properties of mobility and convenience are the most significant reasons why people may adopt the electronic voting mechanism in the future. In this article, we are going to present an efficient and flexible voting scheme which allows the voter having at most $t$ out of $n$ choices at the same time by employing Chaum’s blind signature scheme and the concept of an oblivious transfer protocol, where $n$ is the number of candidates. Our proposed electronic voting scheme not only achieves lots of essential requirements of general electronic voting schemes but also possesses better efficiency than that of other related works.

Keywords: Electronic voting, blind signature, oblivious transfer, anonymity.

$^*$E-mail: ccc@cs.ccu.edu.tw

$^†$E-mail: ljs@cs.ccu.edu.tw

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 9 (2006), No. 1, pp. 133–151
© Taru Publications
1. Introduction

With the rapid development of computer networks, the Internet has become a necessary in people's daily life. More and more routines are handled electronically, and voting is no exception. In 1981, Chaum first proposed the electronic voting mechanism [1,4,5,6]. People can consider the electronic voting as a procedure to make the voters be able to cast their ballots through the Internet. In other words, people can cast their ballots at any time and in any place if they can access the network. The traditional election not only has a lot of problems but also results in the waste of time and money. Most of the problems which the traditional elections suffer from can be resolved by the electronic voting mechanism. Generally speaking, mobility and convenience are the most important properties which make electronic voting become more and more popular. However, most of the electronic voting schemes are designed for permitting each voter to have single choice. And it is not flexible enough for common voting conditions. In this article, we are going to present a novel anonymous electronic voting scheme which allows the voter having $t$ out of $n$ choices at most at the same time by employing Chaum's blind signature scheme and the concept of an oblivious transfer protocol [19], where $n$ is the number of candidates and $t$ is the maximum choices the voter can select. To achieve the goal of anonymity, a proxy server is also adopted in our scheme to help conceal the original network address of a valid voter.

In general, the electronic voting scheme that satisfies more properties and less limits can be adopted in the real world with higher probability [8,9,10,13]. The following are nine requirements that could be achieved in our proposed scheme.

Requirement 1.  **Convenience**

The precise definition of convenience is that “the voter needs not to learn too many sophisticated techniques, and no additional equipment is needed”. Convenience is one of the important reasons why traditional elections may be replaced with electronic voting in the future [16].

Requirement 2.  **Mobility**

The precise definition of mobility is that “the voter will not be restricted by the physical location to cast his/her ballot”. This requirement
allows voters to vote in any place instead of in some particular voting booths. Therefore, the rate of voting will also be highly increased [16, 17, 18].

Requirement 3. **Anonymity**

The precise definition of anonymity is that “no one can link a ballot to the voter who casts it”. In order to protect the privacy of the voter, the electronic voting mechanism has to conceal the choice of the voter. In other words, no one can trace the link between the marked ballot and the corresponding voter [11, 12, 16, 17, 18].

Requirement 4. **Robustness**

The precise definition of robustness is that “no malicious intruder can disturb the procedure of voting”. Robustness is always considered the main concern of the electronic voting scheme. There are no electronic voting scheme can be applied in the real world without achieving this requirement [11, 16, 17].

Requirement 5. **Uniqueness**

The precise definition of uniqueness is that “each legal voter could vote exactly only once”. Both in the traditional election and in the electronic election, the requirement that no one can vote more than once is always regarded as an important rule which must be obeyed by all voters [10, 11, 15, 18].

Requirement 6. **Completeness**

The precise definition of completeness is that “only the eligible voter is allowed to vote”. The voter has to pass a serial of authentication procedures in person before he/she is permitted to cast his/her ballot in traditional voting [3, 10, 11, 12, 14, 18], and so does he/she in electronic voting. However, it is more difficult to achieve this requirement in electronic voting because of the gap of networks.

Requirement 7. **Correctness**

The precise definition of correctness is that “each valid ballot must be tallied correctly”. Undoubtedly, the vote of an eligible voter should not be altered, removed, and duplicated [16, 17, 18]. Otherwise, the voting result can not be confirmed.
Requirement 8. **Efficiency**

The precise definition of efficiency is that “the computation loads of the whole voting procedure must be light enough to have the voting result obtained within a reasonable period of time”. Efficiency is always an important concern of electronic voting. The better efficiency can make the voting scheme become a practical one with higher probability [7, 16, 17].

Requirement 9. **t-out-of-n choices**

The precise definition of t-out-of-n choices is that “the voter has at most t choices out of n candidates at the same time”. This requirement makes the electronic voting scheme more flexible such that it could be applied to more regions.

The rest of this paper is organized as follows. In Section 2, we will introduce the electronic voting scheme proposed by Chen et al [17]. The preliminaries are described in Section 3, and our proposed scheme is shown in Section 4. Next, some discussions on and analyses of our proposed scheme and the comparisons between our proposed scheme and other related works are given in Section 5. Finally, some conclusions are made in Section 6.

2. Related works

In the following, we are going to describe the blind signature scheme proposed by Chaum and the electronic voting scheme presented by Chen et al [17], in Subsections 2.1 and 2.2, respectively.

2.1 Chaum’s Blind Signature

In order to conceal the link between the ballot and the corresponding voter who casts it, not only a proxy server is adopted but also Chaum’s blind signature mechanism is used in our scheme. In 1983, Chaum first proposed the main concept of blind signature [2, 4, 5]. In Chaum’s blind signature scheme, there are two main participants, the signer and the client, where the signer can generate a digital signature for the client without knowing the content of the signed message. Before describing the details of Chaum’s blind signature scheme, we first define the notations used throughout this scheme. Let \( M \) denote the message that needs to be signed, \((e, n)\) denote the public key pair of the signer, and \( d \) denote
the private key of the signer. Let $s$ represent the signature of the message $m$, and $r$ be a random number generated by the client, where $\gcd(n, r) = 1$. The details of Chaum’s scheme are shown as follows.

**Step 1.** The client computes

$$M' = M \cdot r^e \mod n$$

and then sends the computation result to the signer.

**Step 2.** Upon receiving the message sent by the client, the signer computes

$$s' = (M')^d \mod n$$

and then sends the computation result to the client.

**Step 3.** While receiving the message sent by the signer, the client can get $s$ by computing the following equation,

$$s = s' \cdot r^{-1} \mod n = ((M \cdot r^e \mod n)^d \mod n) \cdot r^{-1} \mod n$$

$$= M^d \mod n.$$  

2.2 A review of Chen et al.’s electronic voting scheme

In this subsection, we are going to review Chen et al.’s electronic voting scheme proposed in 2004 [17]. There are six participants in their scheme listed as follows.

*The Voter:* the person who has the right to vote.

*Certificate Authority (CA):* a website provides all enrolled voters certificate services.

*Authentication Center (AC):* a website takes the responsibility of authenticating the validity of each voter.

*Proxy Server:* a server which is responsible for replacing the network address of the voter with another IP address.

*Tally Center (TC):* a website takes the responsibility of tallying the voting result.

*Supervision Center (SC):* a website which is responsible for supervising TC.

Chen et al.’s scheme consists of four phases: Initialization Phase, Authentication Phase, Voting Phase and Counting Phase. Before introducing these phases, we first define some notations used in their scheme.
\((p_x, q_x)\) : a pair of large primes

\(N_x\) : a large prime that satisfies \(N_x = p_x q_x\), and

\(\phi(N_x) = (p_x - 1)(q_x - 1)\)

\(PK_x\) : X’s public key

\(SK_x\) : X’s private key

\(v_i\) : the pseudonym of the voter \(i\)

\(h(\cdot)\) : a public one-way hash function

\(ID_x\) : the identification of \(X\)

\(BG_i\) : the signature of \(h(v_i)\)

\(S_{TC}, S_{SC}\) : two secret shadows generated by CA

Initialization phase:

**Step 1.** CA generates a pair of large primes \((p_{AC}, q_{AC})\), and computes \(N_{AC} = p_{AC} \times q_{AC}\). Then, CA randomly selects a public key \(PK_{AC}\) for AC, where \(PK_{AC}\) and \(\phi(N_{AC})\) are relative primes to each other. Then, the corresponding private key \(SK_{AC}\) is computed as follows

\[PK_{AC}SK_{AC} \equiv 1 \pmod{\phi(N_{AC})}.\]

CA then sends \(PK_{AC}\) and \(SK_{AC}\) to AC.

**Step 2.** CA generates a pair of two large primes \((p_\pi, q_\pi)\), and computes \(N_\pi = p_\pi \times q_\pi\). Then, CA computes TC and SC’s common key pair \((PK_\pi, SK_\pi)\) as follows

\[PK_\pi SK_\pi \equiv 1 \pmod{\phi(N_\pi)}.\]

Next, CA computes the key pairs of TC and SC, \((PK_{TC}, SK_{TC})\) and \((PK_{SC}, SK_{SC})\), as follows,

\[PK_{TC}SK_{TC} \equiv 1 \pmod{\phi(N_\pi)};\]
\[PK_{SC}SK_{SC} \equiv 1 \pmod{\phi(N_\pi)}.\]

Then, CA constructs the following polynomial,

\[f(x) = ax + SK_\pi(\mod \phi(N_\pi)),\]

where \(a \in [1, \phi(N_\pi)]\).
CA employs $f(x)$ to generate two secret shadows, $S_{TC}$ and $S_{SC}$, as follows

$$S_{TC} = f(ID_{TC}) \frac{-ID_{SC}}{ID_{TC} - ID_{SC}} \mod \phi(N_\pi),$$

$$S_{SC} = f(ID_{SC}) \frac{-ID_{TC}}{ID_{SC} - ID_{TC}} \mod \phi(N_\pi),$$

where $ID_{TC}$ is the identification of TC and $ID_{SC}$ is the identification of SC. Finally, CA sends $(PK_{TC}, PK_\pi, S_{TC})$ and $(PK_{SC}, PK_\pi, S_{SC})$ to TC and SC, respectively.

**Step 3.** CA issues each enrolled voter a personal certificate. Besides, CA generates a pair of two large primes $(p_i, q_i)$ and computes $N_i = p_i \times q_i$. Then, CA randomly selects a public key $PK_i$ for the voter $i$, where $PK_i$ and $\phi(N_i)$ are relative primes. The corresponding private key $SK_i$ is computed as follows

$$PK_i SK_i \equiv 1 \mod \phi(N_i),$$

where $N_i$ must satisfy that $N_{AC} < N_i < N_\pi$.

**Authentication phase:**

**Step 1.** The voter $i$ selects a random number $r_i \in [1, N_{AC} - 1]$ and selects a pseudonym $v_i \in [1, \phi(N_\pi)]$. Next, the voter $i$ computes as follows

$$C = h(v_i)^{r_i} \mod N_{AC},$$

and sends the computation result to AC along with his/her certificate $CERT_i$.

**Step 2.** Upon receiving the message sent by the voter $i$, AC checks if the certificate of the voter $i$ is legal. If it does not hold, the connection is terminated; otherwise, CA computes as follows

$$BG'_i = C^{SK_{AC}} \mod N_{AC},$$

$$= (h(v_i)^{r_i})^{PK_{AC}} SK_{AC} \mod N_{AC},$$

$$= h(v_i)^{SK_{AC} r_i} \mod N_{AC}.$$

Finally, AC sends $SG'_i$ to the voter $i$. Note that AC only generates the blind signature for the voter $i$ once.
Step 3. While receiving the message sent by AC, the voter \( i \) then computes the signature of \( h(v_i) \) as follows

\[
BG_i = BG'_i \cdot r_i^{-1} = h(v_i)^{SK_{AC}r_i} \cdot r_i^{-1} \mod N_{AC}
\]

\[
= h(v_i)^{SK_{AC}} \mod N_{AC}.
\]

Voting phase:

Step 1. While the voter \( i \) makes his/her decision, he/she then encrypts the marked ballot \( m \) as follows

\[
B = (w \oplus m)^{PK_{\pi}} \mod N_{\pi},
\]

where \( w \) is a random number. Next, the voter \( i \) casts \( (v_i, BG_i, B, w) \) to TC and SC through a trusted proxy server.

Step 2. After receiving the message sent by the voter \( i \), TC and SC check the validity of the voter \( i \) as follows

\[
h(v_i) = (BG_i)^{PK_{AC}} \mod N_{AC}.
\]

If the above equation holds, they will store \( (v_i, BG_i, B, w) \) in their databases; otherwise, the ballot will be destroyed.

Counting phase:

While the voting deadline, TC and SC compute as follows

\[
C_{TC} = (B)^{S_{TC}} \mod N_{\pi} = (B)^{f(ID_{TC})[-ID_{SC}/(ID_{TC} - ID_{SC})]} \mod N_{\pi},
\]

and

\[
C_{SC} = (B)^{S_{SC}} \mod N_{\pi} = (B)^{f(ID_{SC})[-ID_{TC}/(ID_{SC} - ID_{TC})]} \mod N_{\pi}.
\]

Note that only with the cooperation of TC and SC, the marked ballot \( m \) can be revealed as follows

\[
(C_{TC}C_{SC}) \oplus w \mod N_{\pi} = (B)^{SK_{\pi}} \oplus w \mod N_{\pi}
\]

\[
= ((w \oplus m)^{PK_{\pi}})^{SK_{\pi}} \oplus w \mod N_{\pi} = m.
\]

3. The proposed scheme

In this section, we are going to present a novel anonymous electronic voting scheme which allows each voter having at most \( t \) out of \( n \) choices, where \( n \) is the number of candidates. There are five participants listed as follows in our scheme.
Certificate Authority (CA): CA takes the responsibility for issuing each voter a personal certificate.

Monitor Center (MC): MC is a trusted website which is responsible for authenticating the validity of each voter and generating the corresponding blind signature for the voter.

Announcement Center (AC): AC is a trusted website which is responsible for tallying the valid votes and announcing the final voting result.

Proxy Server (PS): PS takes the responsibility for replacing the original network address of a ballot with another address such that the property, anonymity, can be achieved in our proposed scheme.

Voter: the person who has the right to vote.

The flowchart of our proposed electronic voting scheme is illustrated in Figure 1. Our scheme consists of three phases: Initial Phase, Voting Phase and Announcing Phase. Before introducing these three phases, we first define the notations used throughout our scheme as follows.

\[ p \] : a large prime
\[ g \] : a primitive element in \( \text{GF}(p) \)
\[ e_M \] : the public key of MC
\[ d_M \] : the private key of MC
\[ e_A \] : the public key of AC
\[ d_A \] : the private key of AC
\[ V_i \] : the voter \( i \)
\[ CID_i \] : the identity number of candidate \( i \)
\[ CERT_i \] : the personal certificate of \( V_i \) generated by CA
\[ SN_i \] : the unique serial number of \( v_i \) generated by MC
\[ m_i \] : the marked ballot corresponding to \( CID_i \), where \( i = 1, 2, \ldots, n \)
\[ n \] : the number of candidates
\[ t \] : the maximum choices \( v_i \) can choose, \( t < n \)
\[ h(\cdot) \] : a public one-way hash function

Initial phase:

Step 1. At first, CA issues each enrolled voter a personal certificate and \( n \) marked ballots.
Figure 1
the flowchart of our proposed $t$-out-of-$n$ electronic voting scheme

**Step 2.** $V_i$ randomly chooses $t$ secret numbers $s_1, s_2, \ldots, s_t$, and then computes as follows

$$y_i = g^{s_i} \mod p,$$

where $s_i \in \mathbb{Z}_p$, $i = 1, 2 \text{ to } t$.

**Step 3.** $V_i$ then generates $t$ distinct random numbers $x_1, x_2, \ldots, x_t$, where $x_i \in \mathbb{Z}_p$, $i = 1, 2 \text{ to } t$. Here, $V_i$ has $t$ pairs of $(x_i, y_i)$'s. $V_i$ then can use these $t$ pairs of $(x_i, y_i)$'s to construct a polynomial $f(x)$ by Lagrange Interpolating Polynomial as follows,

$$f(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j \neq i}^{n} \frac{x - x_j}{x_i - x_j} \mod p = a_1 x + a_2 x^2 + \ldots + a_t x^t \mod p,$$

where $a_1, a_2, \ldots, a_t$ are coefficients of $f(x)$.

**Step 1.** Next, $V_i$ selects other $(n - t)$ distinct random numbers, $x_{i+1}, x_{i+2}, \ldots, x_n$, from $\mathbb{Z}_p$, and computes the corresponding $y_i$, where $i = t + 1, t + 2 \text{ to } n$, as follows,

$$y_{i+1} = f(x_{i+1}) = a_1 x_{i+1} + a_2 x_{i+1}^2 + \ldots + a_t x_{i+1}^t \mod p,$$

$$y_{i+2} = f(x_{i+2}) = a_1 x_{i+2} + a_2 x_{i+2}^2 + \ldots + a_t x_{i+2}^t \mod p,$$

$$\vdots$$

$$y_n = f(x_n) = a_1 x_n^2 + a_2 x_n^2 + \ldots + a_t x_n^t \mod p.$$
Voting phase:

**Step 1.** $V_i$ selects $n$ random numbers, $k_1, k_2, \ldots, k_n$, from $Z_p$, and computes as follows,

$$r_i = g^{k_i} \mod p$$

and

$$z_i = m_i^* y_i^{k_i},$$

where $i = 1, 2$ to $n$. Then, $v_i$ generates $(n - t)$ random numbers $s_{t+1}, s_{t+2}, \ldots, s_n$, from $Z_p$. Here, $V_i$ has $n$ triplets $(z_i, r_i, s_i)$, where $i = 1, 2$ to $n$. Next, $V_i$ generates a random number $\text{Ran} \in Z_p$ and computes as

$$\text{MSG} = M^{d_A} (\text{Ran})^{d_M} \mod p,$$

where $M = ((z_1, r_1, s_1), (z_2, r_2, s_2), \ldots, (z_n, r_n, s_n))$. Finally, $V_i$ sends $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n), \text{MSG}$ and $\text{CERT}_i$ to $MC$.

**Step 2.** Upon receiving the messages sent by $V_i$, $MC$ then checks if $\text{CERT}_i$ is legal or not. If it holds, $MC$ then computes an $n \times (t + 1)$ matrix $A$ as follows,

$$A = \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} & y_1 \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} & y_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{t-1} & y_n \end{bmatrix},$$

where $y_i = y_i / x_i$ and $i = 1, 2$ to $n$. Next, $MC$ checks if $\text{Rank}(A)$ is less or equal to $(t + 1)$, where $\text{Rank}(A)$ is the rank of matrix $A$. If it does not hold, $MC$ will terminate the connection; otherwise, $MC$ will generate a unique serial number $SN_i$ for $V_i$ and computes as follows,

$$BG_i = \text{MSG}^{e_M} \mod p$$

$$= (M^{d_A} (\text{Ran})^{d_M})^{e_M} \mod p$$

$$= (M^{d_A e_M (\text{Ran})}) \mod p.$$  

Note that $MC$ only generates a unique serial number for $V_i$ once. Then, $MC$ sends $BG_i$ and $SN_i$ to $V_i$. 

Step 3. After receiving the messages sent by MC, $V_i$ computes as follows

$$SG_i = BG_i(Ran)^{-1} = M^{d_AeM} \mod p.$$ 

Finally, $V_i$ sends $(SG_i, h(SN_i))$ to AC through a secure proxy server $PS$ which will replace $V_i$’s original network address with another one.

Step 4. While receiving the messages from $PS$, AC will store $(SG_i, h(SN_i))$ in its database. Note that AC has to make sure that $h(SN_i)$ is stored in its database only once.

Announcing phase:

Step 1. After the deadline of voting, AC computes as follows to reveal $V_i$’s secret information, 

$$M = (SG_i)^{e_AdM} \mod p = (M^{d_AeM})^{e_AdM} \mod p.$$ 

Step 2. AC then can use the decrypted result $M = ((z_1, r_1, s_1), (z_2, r_2, s_2), \ldots, (z_n, r_n, s_n))$ to reveal the voting result as follows

$$m'_1 = \frac{z_1}{r_1} = ? m_1$$

$$m'_2 = \frac{z_2}{r_2} = ? m_2$$

$$\vdots$$

$$m'_n = \frac{z_n}{r_n} = ? m_n.$$ 

If $m'_i = m_i$ holds, $m_i$ will be counted; otherwise, it will be discarded. Note that only $t$ valid choices will be counted at most for each voter.

4. Security analyses

In this section, we are going to present that our proposed electronic voting scheme can achieve the essential requirements mentioned in Section 1 and show the comparisons between some related electronic voting schemes and ours in Subsections 5.1 and 5.2, respectively.
4.1 Requirements Analyses

In this subsection, we will gradually show that our proposed electronic voting scheme can achieve the nine requirements shown in Section 1.

Requirement 1. **Convenience**

In our proposed scheme, the voter needs not to learn too many complicated techniques. Instead, the voter only needs to have the ability of accessing the Internet. Because the Internet is very popular in the world, lots of people can access it at will. Hence, most of the legal voters can be a member of our proposed electronic voting scheme. What is more, no additional equipment such as smart cards and card readers is required in our scheme except for a proxy server \( PS \). As a result, this requirement is confirmed in our scheme.

Requirement 2. **Mobility**

Because our proposed scheme can be implemented over the Internet, it is so easy and convenient for voters to cast their ballots through the networks. That is, if voters can access the Internet, they will not be restricted to vote in some particular voting place. Therefore, the requirement of mobility can be ensured in our scheme.

Requirement 3. **Anonymity**

The blind signature signed by \( MC \) is used to cut off the link between the voter and the corresponding ballot. Furthermore, a proxy server is also adopted in our scheme to help replace the original network address of the ballot with another network address. Consequently, no one can trace the connection between the ballot and the corresponding voter who casts it. That is, our scheme can confirm this requirement.

Requirement 4. **Robustness**

In our proposed scheme, messages transmitted by the involved participants will be protected with the proper public key. Hence, no one can find or modify \( m_i \) without the knowledge of the corresponding private keys. As a result, this requirement can be completely achieved in our scheme.
Requirement 5. *Uniqueness*

Since the monitor center MC only issues a unique serial number \( SN_i \) to \( V_i \) once after \( V_i \) is authenticated, the voter \( V_i \) can not cast his/her ballot twice. Otherwise, AC will detect the duplications in its own database and will delete them. Therefore, this requirement can be achieved in our scheme.

Requirement 6. *Completeness*

Assume that no one can successfully mount attacks on Chaum’s blind signature scheme to forge \( M \). Therefore, only the eligible voter is allowed to vote. Furthermore, each enrolled voter is issued a unique serial number by MC. Hence, \( h(SN_i) = h(SN_j), \ i \neq j \), will never occur in our scheme. That is, our scheme can confirm this requirement.

Requirement 7. *Correctness*

To ensure the correctness of the voting, all ballots are protected from being removed, duplicated or altered by the public-key cryptosystem and an oblivious transfer protocol. Only AC can reveal the final voting result by the following computation.

\[
M = (SG_i)^{eA_dM} \mod p
\]
\[
= (M^{eA_dM})^{eA_dM} \mod p.
\]

Here, AC can use the decrypted result \( M = ((z_1, r_1, s_1), (z_2, r_2, s_2), \ldots, (z_n, r_n, s_n)) \) to compute \( m'_i \) as follows

\[
m'_i = \frac{z_i}{r_i^e}.
\]

If \( m'_i \) is not equivalent to \( m_i \), \( m_i \) is deleted; otherwise, \( m_i \) is counted. That is, the valid ballot must be tallied correctly. Hence, this requirement is also achieved in our scheme.

Requirement 8. *Efficiency*

Without loss of generality, the number of candidates should be quite small. Hence, the voter only needs to spend a little time on performing the voting procedure in our scheme. Most of the computation operations are performed by MC and AC. As a result, our proposed electronic voting scheme can be applied in the real world.
Requirement 9. *t-out-of-n* choices

After the voter $V_i$ generates the unique polynomial $f(x) = a_1x + a_2x^2 + \ldots + a_t x^t \mod p$ by Lagrange Interpolating Polynomial [20], he/she can compute $y_i = f(x_i)$ in terms of the given $x_i$, where $i = t + 1, t + 2$ to $n$. However, it is infeasible for him/her to compute the discrete logs of these values in polynomial time. To prevent the voter $V_i$ from making more than $t$ choices, MC will check if the rank of the matrix $A$ is larger than $(t + 1)$. If it holds, the vote is destroyed; otherwise, the voting process is carried on. To simplify the explanation, we take the case that the voter makes exact $t$ choices for instance [19, 21]. That is, if $V_i$ also pre-selects $y_i$, where $i = t + 1, t + 2$ to $n$, and then tries to figure out $a_1, a_2, \ldots$, and $a_n$ to form $f(x) = a_1x + a_2x^2 + \ldots + a_t x^t \mod p$, he/she must fail. Let us consider the following $n \times (t + 1)$ matrix

$$A = \begin{bmatrix}
1 & x_1 & x_1^2 & \cdots & x_1^{t-1} & y_1 \\
1 & x_2 & x_2^2 & \cdots & x_2^{t-1} & y_2 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
1 & x_n & x_n^2 & \cdots & x_n^{t-1} & y_n
\end{bmatrix},$$

where $\text{Rank}(A)$ is $(t + 1)$. Hence, we have

$$A = \begin{bmatrix}
a_1 \\
a_2 \\
\vdots \\
a_t \\
-1
\end{bmatrix} = \begin{bmatrix}
0 \\
0 \\
\vdots \\
0
\end{bmatrix}.$$

Since the rank of the matrix $A$ is $(t + 1)$, by performing row transformations, we will have a nonsingular matrix $B$ such that

$$BA = \begin{bmatrix} C \\ 0 \end{bmatrix},$$

where $C$ is an $(t + 1) \times (t + 1)$ nonsingular upper triangle matrix. As a result,

$$BA = \begin{bmatrix}
 a_1 \\
 a_2 \\
\vdots \\
 a_t \\
-1
\end{bmatrix} = \begin{bmatrix} C \\ 0 \end{bmatrix} \begin{bmatrix}
 a_1 \\
 a_2 \\
\vdots \\
 a_t \\
-1
\end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix}.$$
And, it is equivalent to
\[
\begin{bmatrix}
a_1 \\
a_2 \\
\vdots \\
a_t \\
-1
\end{bmatrix}
= \begin{bmatrix}
0 \\
0 \\
\vdots \\
0
\end{bmatrix}.
\]

Next, we apply \(C^{-1}\) to the above equation. Thus, we have
\[
C^{-1} \begin{bmatrix}
a_1 \\
a_2 \\
\vdots \\
a_t \\
-1
\end{bmatrix} = C^{-1} \begin{bmatrix}
0 \\
0 \\
\vdots \\
0
\end{bmatrix} = \begin{bmatrix}
a_1 \\
a_2 \\
\vdots \\
a_t \\
-1
\end{bmatrix}.
\]

Since \(C^{-1}\) is also a nonsingular matrix, it implies that the equations with respect to \(a_i\) have no nonzero solution, where \(i = 1, 2, \ldots, t\). That is, if the voter pre-selects \(y_i\), where \(i = t + 1, t + 2, \ldots, n\), he/she can not find any nonzero solution. As a result, this requirement is confirmed in our scheme.

### Table 1
Comparisons between our scheme and other related works

<table>
<thead>
<tr>
<th></th>
<th>Ours</th>
<th>Chen et al.’s</th>
<th>Dini’s</th>
<th>Fjioka et al.’s</th>
<th>Liaw’s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymity</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Convenience</td>
<td>High</td>
<td>Mid</td>
<td>Low</td>
<td>X</td>
<td>Mid</td>
</tr>
<tr>
<td>Robustness</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mobility</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>X</td>
<td>Yes</td>
</tr>
<tr>
<td>Uniqueness</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Completeness</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Correctness</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Efficiency</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Mid</td>
</tr>
<tr>
<td>(t)-out-of-(n) choices</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### 4.2 Comparisons between electronic voting schemes

In this subsection, we are going to present the comparisons between our proposed scheme and other related works. At first, we define the notations used in Table 1. “High” denotes that the scheme can completely achieve the requirement, “Mid” means the scheme can only achieve the requirement medially, and “Low” means that it is hard to have
this requirement confirmed in the corresponding scheme. “Yes” means that this requirement is confirmed in the corresponding scheme while “No” represents that the corresponding scheme can not achieve the requirement. “X” denotes that this requirement is not mentioned in the scheme. In our proposed scheme, complicated techniques which the voter has to learn and lots of the demanded equipments are not needed but a proxy server. Hence, the convenience requirement is confirmed in our scheme with a higher degree than in others. As shown in Table 1, our proposed electronic voting scheme not only confirms all essential requirements but also allows the voter having at most $t$ out of $n$ choices at the same time.

5. Conclusions

People cast their ballots through the Internet is a good and practical idea. About twenty years ago, electronic voting has already been proposed. Later, more and more schemes are proposed to make the electronic voting scheme complete. However, most of them can not achieve all of the essential requirements mentioned in Section 1. In this article, we present an anonymous and flexible scheme for electronic voting, in which allows the voter having at most $t$ out of $n$ choices at the same time. Our proposed scheme adopts Chaum’s blind signature mechanism and the concept of an oblivious transfer protocol to confirm the requirements anonymity and correctness, respectively. Furthermore, a trusted proxy server is also applied to have the requirement anonymity achieved. As shown in Subsections 5.1 and 5.2, our proposed electronic voting scheme not only achieves all essential requirements mentioned in Section 1 but also has better performance than other related works. As a result, our proposed electronic voting scheme can be practically applied over the Internet in the real world.

References


Received March, 2005