사용자 중심의 인터넷 기반 대규모 전자선거 기법

윤 성 현*

◈ 목 차 ◈

1. 서 론

컴퓨터의 보급과 인터넷과 같은 개방형 통신망의 발전은 인간의 많은 사회적 영역을 전자적으로 처리될 수 있게 하였다. 많은 정보를 여러 사람이 공유함으로써 작업의 효용성 및 부가가치를 창출하게 되었지만 해커나 침입자로부터의 개인 정보보호에 대한 문제가 심각하게 대두되고 있다.

사회적 영역의 전자화를 위해서 암호 및 인증 기법과 같은 정보보호 기술의 적용은 필수적이다. 정보보호 기술의 발전 및 적용은 선거, 현금 거래 등과 같은 인간의 보다 폭 넓은 사회적 영역을 전자화 함으로써 생활의 편리함 뿐만 아니라 막대한 경제적 이익을 기대할 수 있게 한다.

선거는 민주주의 사회에서 가장 중요한 사회적 행위 중의 하나이다. 오프라인 형태의 일반 선거 방식을 전자화하게 되면, 선거와 관련된 상당수의 제반 경비를 줄일 수 있다. 하지만, 전자선거의 구현에 있어서 가장 큰 걸림돌은 인터넷과 같은 공중 통신망의 특성상 개인의 익명성 침해, 이중 투표, 해커의 태핑(tapping)에 의한 부정 투표 등 많은 위험 요소가 존재한다는 것이다.

디지털 데이터는 그 특성상 원본과 복제본의 구분이 불가능하다. 부정 투표자에 의해서 합법적인 투표권을 복제 양산할 수 있으며, 공중망을 이용할 경우에 태핑 또는 모니터링 툴 등을 이용한 패킷 감시가 가능하다. 인터넷과 같은 공중망을 이용하는 대규모 전자선거에서 패킷의 원본 주소를 조사함으로써 누가 누구에게 투표했는지 알 수 있게 된다. 상기한 문제점들을 해결하고 전자 민주주의 실현을 위해서 정보보호 기술이 접목된 안전한 전자선거 기법의 개발이 필수적이다.

보안 기술이 접목된 안전한 전자선거 기법의 실현으로 얻을 수 있는 장점은 다음과 같다. 기존 오프라인 방식의 선거에 필요했던 물적·인적 제반 경비 및 부정 투표의 위험성을 줄일 수 있다. 개표 과정의 복잡한 절차를 단순화하여 전자적으로 처리함으로써 개표 결과를 실시간으로 확인할 수 있다. 전자선거에 사용된 프로토콜과 정보보호 기술의 안전성이 공개적으로 증명되면, 선거 후 개표 결과에 대한 시비를 방지할 수 있다.

전자 민주주의 실현의 기반이 되는 전자선거의 중요성과 함께 많은 연구가 진행되었다. 특히 인터넷의 폭 넓은 보급으로 대규모 선거에 적합한 선거 프로토콜의 개발이 주요 이슈로 등장하고 있다. [1, 2, 3]은 대규모 선거에 적합한 대표적인 전자선거 기법이다. 표 1은 대규모 전자선거에 적합한 보안 요구사항이다 [1, 3, 16].

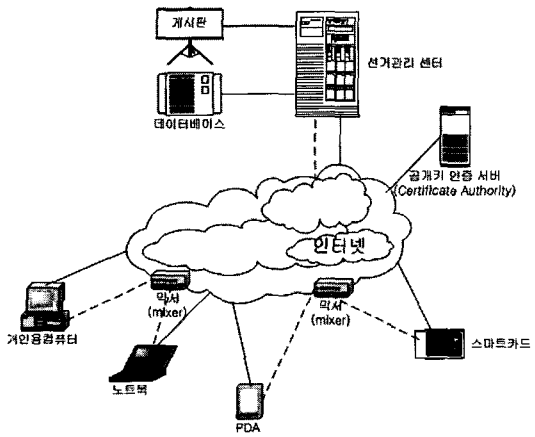
기존의 전자선거 기법들의 특징은 실용적인 프로토콜을 위해서, 적어도 하나 이상의 신뢰할 수 있는 선

* 천안대학교 정보통신학부 전임강사

거관리 센터의 존재를 가정한다. 또한 투표자의 익명성을 보장하기 위해서 chaum이 제안한 추적할 수 없는 통신망[6]과 같은 IP 추적이 불가능한 통신채널이 준비되어 있음을 가정한다.

(표 1) 대규모 선거에 적합한 보안요구사항

재사용불가	등록된 투표자가 두 번 이상 투표할 수 없다
익명성	누가 누구에게 투표했는지 알 수 없어야한다
공정성	투표 단계에서 전체 선거 결과에 영향을 미치는 중간 투표 결과를 알 수 없어야한다
위조불가	합법적인 등록자 외에 인증 투표권을 만들 수 없다
합법성	합법적인 절차를 거쳐서 등록된 투표자만 선거에 참여할 수 있다



(그림 1) 제안한 전자선거 기법의 전체 구성도

그림 1은 제안한 전자선거 기법의 전체 구성도로 구성원들 간의 인터페이스를 보여준다. 선거관리 센터는 투표자 등록, 개표 결과 공지 등과 같은 선거와 관련된 업무를 수행한다. 공개키 인증 서버(Certificate Authority)는 선거관리 센터, 투표자들의 공개키를 인증 및 관리 한다. 투표자들은 인터넷 연결이 가능하고 투표 프로그램을 실행할 수 있는 PC, 노트북, PDA 또는 스마트카드와 같은 장비를 사용할 수 있다. 그림 1에서 믹서의 역할은 IP 추적이 불가능하게 투표자들의 투표권을 섞어서 선거관리 센터로 보내주는 역할을 담당한다.

본 논문에서는 투표 단계에서의 투표자 및 투표권 등록 절차를 개선한 실용적인 프로토콜을 제안한다. 투표 단계에서 투표자는 익명성 보장을 위하여 직접 투표권을 은닉하며, 부인봉쇄 서명 기법을 투표자 등록 절차에 적용함으로써 투표 단계 동안 투표자가 본인의 의사에 따라서 투표권을 재생성하여 투표할 수 있도록 투표자의 의사를 최대한 반영한 투표자 중심의 전자선거 기법이다. 또한, 투표 및 개표 단계에서 선거관리 센터와 투표자 간에 도전/응답 기법이 내포된 서명확인 프로토콜을 진행함으로써 선거의 공정성을 실현한다.

제안한 방법은 전자선거 기법에 은닉 부인봉쇄 서명 기법을 접목하여 전자선거와 같은 복잡한 사회적 영역의 전자화를 위한 보안 요구사항을 만족시킨다. 신뢰할 수 있는 선거관리 센터와 IP 추적이 불가능한 통신 채널이 준비되어 있다는 가정 하에서 침입자 및 내부자로부터의 위협에 대해서 안전하다.

2 장에서는 대규모 전자선거 기법과 관련된 기존의 대표적인 연구 동향을 살펴본다. 3 장에서는 제안한 전자선거 기법을 설명하고 4 장에서는 대규모 전자선거의 보안 요구사항에 따른 안전성 분석을 한다. 5 장에서 결론 및 향후 연구 과제를 논한다.

2. 관련 연구

대규모 선거에 적합한 기존의 전자선거 기법을 살펴보면 크게 두 가지 가정에 기반을 둔다. 첫째는 투표자의 익명성을 보장하기 위해서 Chaum이 제안한 추적 불가능한 통신망의 존재를 가정한다[6]. 둘째는 일상생활의 선거에서의 선거관리 위원장과 같은 선거관리 센터의 안전성에 기반을 둔다. 센터의 주요 역할은 투표자를 등록하고 합법적인 투표권을 부여하고 개표의 책임을 맡는다.

[4]는 Boyd가 제안한 전자 선거 기법으로 이산대수 문제의 어려움에 근간 한 복수키 암호 방법의 안전성에 기반을 둔다. 투표자 등록 과정에서 투표자의 익명성을 보장하며 투표 과정의 익명성은 Chaum이 제안한 추적 불가능 한 통신망에 기반을 둔다. 단점은 선거관리 센터의 권한 및 역할이 많아서 선거관리 센터

에 의한 부정 투표 또는 중간 선거 결과의 유출이 가능하다는 것이다.

[3]은 Fujioka, Okamoto, Ohta가 제안한 선거 기법으로 선거 도중 선거 결과에 영향을 미칠 수 있는 중간 투표 결과를 발표할 수 없도록 함으로써 선거의 공정성을 실현한다. 단점은 등록된 투표자가 도중에 투표권 행사를 포기할 수 없다는 것이다. 따라서 대규모 선거에 실용적이지 못하다.

[1]은 [3]에서 제안한 선거 기법을 개선하여 좀 더 실용적인 전자 선거 기법을 제안하였다. 등록된 투표자가 중도에 선거에 불참하더라도 전체 선거 결과에 영향을 미치지 않으며 투표 진행 단계에 threshold 개념을 적용하여 투표자, 후보자들, 선거 관리자의 부정을 최소화 하고자 하였다. 단점은 선거 준비 단계에서 신뢰할 수 있는 센터가 각 투표자에게 안전한 통신망을 통해서 투표권 생성에 사용되는 투표자 별 난수 값(pseudonym)을 제공해야 하는 부담이 따른다. 또한 등록된 투표자가 투표를 하지 않을 경우 선거 관리자(administrator)에 의한 부정이 가능하다.

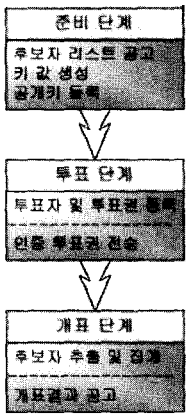
[2]는 신뢰할 수 있는 센터의 역할을 최소화하기 위해서 선거 관리자를 여러 명 두는 선거 기법이다. 은닉 다중 서명 기법(blind multisignature scheme)을 적용하여 적어도 한 명의 선거 관리자가 신뢰할 수 있다면 선거의 안전성이 보장된다. 단점은 선거 관리자들이 모두 결탁할 경우 중간 투표 결과를 유출할 수 있고, 전체 선거 프로토콜이 붕괴된다는 것이다. 특히 투표 등록을 위한 통신 복잡도가 일반 선거 기법에서보다 투표자 개인당 선거 관리자수 만큼 배가하기 때문에 대규모 선거에 적합하지 않다.

3. 사용자 중심의 대규모 전자선거 기법

본 논문에서는 대규모 전자선거에 적합한 실용적인 전자선거 기법을 제안한다. 그림 2는 제안한 전자선거 기법의 각 단계별 구성 및 특징을 보여준다. 제안한 기법은 준비 단계, 투표 단계 그리고 개표 단계로 구성된다.

준비 단계에서 선거관리 센터는 선거일 이전에 각 후보자의 이름과 투표권 생성에 사용될 해당 후보자별 난수 값을 게시판에 공고한다. 각 후보자를 대표하는 난수 값은 투표자들이 투표권을 임의로 변조할 수 없도록 충분히 큰 값을 갖게 한다. 투표자들과 선거관리 센터는 투표에 사용될 암호학적 파라미터들을 생성하며 각자의 공개키를 공개키 인증 센터에 등록한다.

투표 단계에서 각 투표자는 투표권 은닉을 위한 난수 값을 생성하고 해당 후보에 대한 은닉 투표권을 생성한다. 투표자 및 투표권 등록을 위해서 센터와 투표자 간에 부인봉쇄 서명 기법이 적용되며, 투표자는 투표 및 개표 단계에서 IP 추적이 불가능한 통신 채널을 이용하여 익명적으로 선거관리 센터에 투표권을 전송한다. 개표 단계에서 선거관리 센터는 각 후보자별 투표권을 개수하고 개표 결과를 게시판에 공고한다.



(그림 2) 전자선거 단계 별 구성도

3.1 가정 및 용어정의

기존의 전자선거 기법과 마찬가지로 제안한 기법은 다음과 같은 가정에 기반을 둔다.

(가정 1) 선거관리 센터는 신뢰할 수 있으며 합법적인 투표자의 투표권 등록, 투표 및 개표 결과에 대한 책임을 맡는다.

(가정 2) 투표자와 선거관리 센터 간에 익명적으로 투표권을 전송할 수 있는 IP 추적이 불가능한 통신 채널이 존재한다.

다음은 본 논문에서 사용된 용어에 대한 정의이다.

ps : 투표권생성에 필요한 투표자의 난수정보
C : 후보자들 집합
C_i : 후보자 i , $C_i \in C$
cps_i : 투표권생성에 필요한 후보자i의 난수정보
$ballot$: 투표자에 의해 생성된 투표권
$ballot'$: 투표자에 의해 은닉된 은닉 투표권
$S_A(ballot)$: 선거관리센터가 서명한 인증투표권

3.2 준비 단계

□ 선거관리 센터

선거관리 센터는 다음과 같이 큰 소수 p, 생성자 g, 비밀키 X 그리고 공개키 Y와 같이 전자선거에 사용될 암호학적 파라미터들을 생성하고 게시판에 비밀키 X를 제외한 값들을 공고한다. 일반적으로 큰 소수 p를 법으로 하는 이산대수 문제는 계산상 불가능하며 본 전자선거 기법의 안전성은 이에 기반을 둔다[13,14].

$$Y \equiv g^X \pmod{p}$$

(표 2) 후보자 리스트

후보자 이름	투표권 생성에 사용될 난수 값
C_1	Cps_1
C_2	Cps_2
…	…
C_{n-1}	cps_{n-1}
C_n	cps_n

표 2는 후보자 이름과 투표권 생성에 사용될 각 후보자에 대응하는 난수 값으로 선거관리 센터에 의해서 게시판에 공고된다. 난수 값은 투표권 생성 시에 위조가 불가능하도록 충분히 큰 값을 생성한다. 기타, 선거와 관련된 공지 사항을 게시판에 공고한다.

□ 투표자

투표자는 다음과 같이 전자선거에 사용될 비밀키 x와 공개키 y를 생성한다.

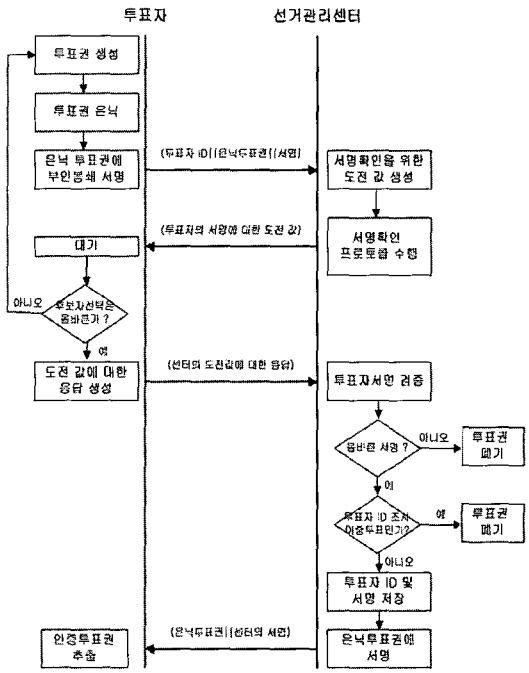
$$y \equiv g^x \pmod{p}$$

선거관리 센터와 투표자들은 선거일 이전에 자신의 공개키를 온라인 또는 오프라인으로 CA와 같은 공개키 인증기관에 등록한다.

3.3 투표 단계

투표 단계는 투표권 등록과 투표권 전송의 두 가지 절차로 구성된다. 투표권 등록 절차에서 투표자와 투표자의 투표권은 선거관리 센터에 의해서 등록된다. 투표권 전송 절차에서 투표자는 익명적으로 투표권을 선거관리 센터로 전송한다.

그림 3은 투표 단계에서의 투표자 및 투표권 등록 절차를 보여준다. 부인봉쇄 서명 기법을 적용함으로써, 투표자는 투표권 확인을 위한 그림 3의 서명확인 프로토콜에서 선거관리 센터의 도전에 응답하지 않음으로써 투표권을 재생성하여 등록할 수 있는 특징이 있다.



(그림 3) 투표자/투표권 등록 절차

(1) 투표자의 은닉 투표권 생성 및 서명

단계 1: 투표자는 투표권 생성을 위해서 필요한 난수 값 ps를 직접 생성하고 특정 후보자 i를 선택한다. 표 2의 후보자 i에 해당하는 난수 값 cps_i와 자신이 생성한 ps를 이용하여 다음과 같이 투표권을 생성한다. 투표자는 ps를 조정하여 투표권이 법 p의 원시 근(primitive root)이 되도록 한다.

$$ballot \equiv (cps_i \cdot ps)^{ps} (\bmod p)$$

단계 2: 다음과 같이 투표권을 은닉한다.

$bf \cdot bf^{-1} \equiv 1 (\bmod p-1)$, bf : 은닉 값

$ballot' \equiv ballot^{bf} (\bmod\ p)$

단계 3: 투표자는 합법적인 투표자 등록을 위해서 서명자 신분을 보장할 수 있게 은닉 투표권 $ballot'$에 서명한다. 투표자의 투표권 서명은 다음과 같이 부인봉쇄 서명 기법이 적용되며, 서명 (s,r)은 다음과 같다[15].

$$r \equiv ballot'^{k} (\bmod\ p),\quad k \in Z_{p-1}$$

$$k \cdot (ballot' + s) \equiv x \cdot r (\bmod\ p-1)$$

단계 4: 투표자는 ID, 은닉 투표권 그리고 서명을 선거관리 센터로 전송한다.

(*ID*, *s*, *r*, ballot')

(2) 투표자 및 투표권 등록

단계 1: 선거관리 센터는 투표자의 서명 (s, r)을 검증하기 위해서 서명확인 프로토콜을 수행한다[15]. 서명확인 프로토콜은 검증자의 도전에 대해서 서명자가 응답을 함으로써 이루어진다. 만약 투표자가 다른 후보에게 투표하고자 마음이 변하면 선거관리 센터의 도전에 응답하지 않고 투표 단계를 재시작하면 된다. 부인봉쇄 서명은 서명자의 동의 없이는 검증할 수 없는 특성을 갖는다.

단계 2: 선거관리 센터는 투표자의 응답을 검증하여 서명이 유효한 지 확인한다. 잘못된 서명인 경우에 투표자의 투표권을 폐기한다. 서명이 올바르면, 선거관리 센터는 투표자가 두 번 이상 투표하는 것인지를 확인하기 위하여 투표자 ID를 확인한다. 투표자가 두 번 이상 투표하는 경우에, 마찬가지로 투표권을 폐기한다. 정상적인 경우에 다음 단계로 진행한다.

단계 3: 선거관리 센터는 투표자의 이중 투표(double voting)를 방지하기 위해서 투표자 ID와 서명을 저장한다.

단계 4: 선거관리 센터는 투표자의 은닉 투표권에 다음과 같이 서명 (S,R)을 생성한다.

$$R \equiv ballot'^{K} (\bmod\ p),\quad K \in Z_{p-1}$$

$$K \cdot (ballot' + S) \equiv X \cdot R (\bmod\ p-1)$$

단계 5: 선거관리 센터는 서명 (S,R)을 투표자에게 전송한다.

(3) 선거관리 센터가 서명한 인증 투표권 추출

단계 1: 투표자는 선거관리 센터의 서명으로부터 인증 투표권 $S_A(ballot)$을 다음과 같이 추출한다.

$$\begin{aligned} S_A(ballot) &\equiv R^{(ballot' + S) \cdot bf^{-1} \cdot R^{-1}} (\bmod\ p) \\ &\equiv ballot'^{K \cdot (ballot' + S) \cdot bf^{-1} \cdot R^{-1}} (\bmod\ p) \\ &\equiv ballot'^{X \cdot R \cdot bf^{-1} \cdot R^{-1}} (\bmod\ p) \\ &\equiv ballot'^{X \cdot bf \cdot bf^{-1} \cdot R^{-1}} (\bmod\ p) \\ &\equiv ballot'^{X} (\bmod\ p) \end{aligned}$$

$(\because bf \cdot bf^{-1} \equiv 1 \bmod p-1,\ R \cdot R^{-1} \equiv 1 \bmod p-1)$

(4) 인증 투표권 전송

□ 투표자

투표자는 선거관리 센터의 서명 (S,R)을 확인하기 위해서 인증 투표권에 대한 도전을 다음과 같이 생성하고 선거관리 센터로 전송한다.

단계 1: 투표자는 임의의 두 난수 (a,b)를 생성하고 다음과 같이 도전 ch를 생성한다.

$$ch \equiv S_A(ballot)^{a} \cdot Y^{b} (\bmod\ p),\quad a, b \in Z_{p-1}$$

단계 2: 투표자는 도전 ch와 인증 투표권 S_A(ballot)을 선거관리 센터로 익명적으로 전송한다. 가정 2에서 언급한 IP 추적이 불가능한 통신 채널을 이용한다.

□ 선거관리 센터

선거관리 센터는 투표자의 도전에 대한 응답을 생성하고 투표자의 투표권을 추출한다.

단계 1: 선거관리 센터는 다음과 같이 응답을 생성한다.

$$rsp \equiv ch^{X^{-1}} \equiv ballot^{a} \cdot g^{b} (\mathrm{mod}\ p)$$

단계 2: 선거관리 센터는 인증 투표권으로부터 투표자의 투표권을 다음과 같이 추출한다.

$$S_A(ballot)^{X^{-1}} \equiv ballot^{X \cdot X^{-1}} \equiv ballot (\mathrm{mod}\ p)$$

단계 3: 선거관리 센터는 게시판에 인증 투표권, 투표자의 투표권, 응답을 게시한다. 투표자의 투표권은 투표자의 난수 값과 후보자의 난수 값으로 구성된다. 투표자의 난수 값을 알지 못하기 때문에, 선거관리 센터는 투표 단계 동안 투표권을 개봉할 수 없다.

$$(S_A(ballot),\ ballot,\ rsp)$$

□ 투표자

투표자는 선거관리 센터의 응답을 검증한다. 선거관리 센터의 응답이 올바르지 않을 경우에, 투표자는 부인 프로토콜을 수행하여 선거관리 센터가 부정을 했는지의 여부를 검증할 수 있다[15].

3.4 개표 단계

□ 투표자

투표자는 투표권 개봉을 위해서 자신이 생성한 난수 값 ps를 선거관리 센터로 전송한다.

□ 선거관리 센터

단계 1: 선거관리 센터는 다음과 같이 후보자 별 투표권을 개수한다.

$$\begin{aligned} cps_i &\equiv \frac{ballot^{ps^{-1}}}{ps} (\mathrm{mod}\ p) \\ &\equiv \frac{(cps_i \cdot ps)}{ps} (\mathrm{mod}\ p) \\ &\equiv cps_i (\mathrm{mod}\ p) \end{aligned}$$

cps_i가 표 1의 후보자 리스트에 존재하면 해당 후보자의 표수를 증가시키고, 그렇지 않으면 해당 투표권을 폐기한다.

단계 2: 선거관리 센터는 게시판에 투표자 별 개표 결과를 공고한다.

4. 안전성 분석

본 절에서는 대규모 전자선거에 적합한 보안 요구사항 별로 제안한 방법의 안전성을 분석한다.

(1) 재사용 불가

선거관리 센터는 투표자 등록 절차에서 투표권을 부여한 투표자 ID를 저장하고 중복 여부를 점검함으로써 투표자가 두 번 이상 등록할 수 없도록 한다. 투표자가 두 번 이상 등록 또는 투표하기 위해서는 센터가 인증한 투표권을 임의로 만들어 낼 수 있어야 한다. 다음과 같이 투표자는 센터의 비밀 키 X를 계산해야 한다.

$$\begin{aligned} &S_A(ballot) = ballot^{-X} (\mathrm{mod}\ p) \\ &X \equiv \log_{ballot} S_A(ballot) (\mathrm{mod}\ p) \end{aligned} \qquad \text{(식 1)}$$

(식 1)은 mod p에 대한 이산대수 문제로 p 값이 클 때 X를 구하는 것은 계산상 불가능하다[13, 14]. 따라서 투표자가 두 번 이상 투표할 수 없다. Q.E.D.

(2) 익명성

투표자의 익명성은 은닉 프로토콜의 안전성과 가정 2에 기반을 둔다. 투표 단계에서 투표자는 투표권을 은닉하기 위해서 은닉 값 bf를 생성한다. 투표자는 은닉 투표권을 선거관리 센터로 전송한다. 선거관리 센터는 은닉 투표권에 대해서 서명하고 투표자에게 전송한다. 투표자는 서명된 은닉 투표권으로부터 센터의 서명이 있는 인증 투표권을 추출한다. 누가 누구에게 투표했는지 유추하기 위해서는 다음과 같이 투표권 은닉에 사용된 bf 값을 계산해야 한다.

$$ballot' \equiv ballot^{bf} (\mathrm{mod}\ p) \qquad \text{(식 2)}$$

식 2에서 bf를 구하는 것은 식 1에서와 같이 mod p에 대한 이산대수 문제가 된다. 또한 가정 2의 IP 추적이 불가능한 통신채널을 이용하여 인증 투표권을 전송하기 때문에 선거 참여자는 누가 누구에게 투표했는지 알 수 없다. Q.E.D.

(3) 공정성

공정성은 전체 선거 결과에 영향을 미칠 수 있는 중간 투표 결과를 투표 단계에서 알 수 없도록 하는 것이다. 투표자는 투표 및 개표 단계에서 서명확인 프로토콜을 수행하여 인증 투표권에 대해서 검증한다. 선거관리 센터의 서명이 올바르면, 투표권 생성 시 만들었던 투표자의 난수 값 ps를 선거관리 센터로 전송한다. 선거관리 센터는 투표자가 전송한 ps를 이용하여 투표권으로부터 후보자를 추출한다.

ps는 개표 단계에서 투표자에 의해 전송되므로 선거관리 센터는 투표자의 투표권을 투표 단계 동안 개봉할 수 없다. 선거관리 센터가 투표 단계 동안 후보자 추출을 위해서는 투표권에 내재되어 있는 투표자의 ps 값을 계산해야 한다.

$$S_A(ballot)^{X^{-1}} \equiv ballot^{X \cdot X^{-1}} (\mathrm{mod}\ p)$$
$$ballot(\mathrm{mod}\ p) \equiv (cps_i \cdot ps)^{ps}\ (\mathrm{mod}\ p) \qquad \text{(식 3)}$$
$$ps \equiv \log_{(cps_i,\ ps)} ballot(\mathrm{mod}\ p)$$

식 3에서 ps는 mod p에 대한 이산대수 문제가 되며, ps를 구하는 것은 계산상 불가능하다. Q.E.D.

(4) 위조불가

선거 참여자는 다른 사람의 투표를 위조할 수 없어야 한다. 투표권을 위조하기 위해서는 다음과 같이 인증 투표권을 임의로 만들 수 있어야 한다.

$$(ps,\ cps_i,\ (cps_i \cdot ps)^{ps}\ (\mathrm{mod}\ p),\ (cps_i \cdot ps)^{X \cdot ps}\ (\mathrm{mod}\ p))$$

선거관리 센터의 비밀키 X를 구하는 문제는 식 1, 2, 3과 마찬가지로 mod p에 대한 이산대수 문제가 되며, 가정 1과 같이 선거관리 센터를 신뢰할 수 있다면 투표권 위조는 불가능하다. Q.E.D.

(5) 합법성

투표자 등록 절차에서 사용된 서명 기법이 안전하면, 합법적인 투표자만 선거에 참여할 수 있다. 투표자 등록을 위해서 부인봉쇄 서명 기법이 적용된다[15]. 투표자들은 투표권을 센터로부터 인증 받기 위해서 은닉 투표권에 대한 부인봉쇄 서명을 생성한다. 선거 관리 센터는 투표자의 ID와 부인봉쇄 서명을 검증하여 투표자에 대한 합법성을 결정한다. 등록되지 않은 투표자가 선거에 참여하기 위해서는 센터로부터 검증 가능한 부인봉쇄 서명을 만들어내야 한다. 적용된 서명 기법이 안전하면, 해당 투표자가 선거관리 센터와 결탁을 해야만 가능하다. 이는 가정 1에 위배된다. Q.E.D.

5. 결 론

본 논문에서는 대규모 전자선거에 적합한 실용적인 전자선거 기법을 제안하였다. 제안한 방법은 투표단계의 투표자 등록 절차에서 투표자가 직접 투표권을 은닉하며 부인봉쇄 서명 기법을 적용함으로써 익명성 보장은 물론 투표 단계에서의 투표권 재생성이 가능한 투표자 중심의 전자선거 기법이다. 또한 투표 및 개표 단계에서 선거관리 센터와 투표자 간에 도전/응답 기법이 내포된 서명확인 프로토콜을 적용함으로써 선거의 공정성을 만족한다.

신뢰할 수 있는 선거관리 센터와 IP 추적이 불가능한 통신채널이 존재한다는 가정 하에 제안한 전자선거 기법은 재사용불가, 익명성, 공정성, 위조불가, 합법성 등과 같은 대규모 전자선거에서 요구되는 보안 요구사항을 만족한다.

참고문헌

[1] Ahmad Baraani-Dastjerdi, Josef Pieprzyk and Reihaneh Safavi-Naini, "A Secure Voting Protocol Using Threshold Schemes," Proceedings of

COMPSAC'95, pp.143-148, 1995.

[2] Patrick Horster, Markus Michels and Holger Petersen, "Blind Multisignature Schemes and Their Relevance for Electronic Voting," Proceedings of COMPSAC'95, pp.149-155, 1995.

[3] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta, "A Practical Secret Voting Scheme for Large Scale Elections," In Advances in Cryptology, Proceedings of AUSCRYPT'92, 1992.

[4] Colin Boyd, "A New Multiple Key Cipher and an Improved Voting Scheme," In Advances inn Cryptology, Proceedings of EUROCRYPT'89, LNCS 434, pp.617-625, 1990.

[5] M.Naor, "Bit Commitment using Pseudorandomness," In Advances in Cryptology, Proceedings of CRYPTO'89, LNCS 435, pp.128-136, 1990.

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

[7] Y.Desmedt, Y.Fraenkel, "Threshold Cryptosystems," In Advances in Cryptology, Proceedings of Crypto'89, LNCS 435, pp.307-315, 1990.

[8] Troben Pryds Pedersen, "Distributed Provers with Applications to Undeniable Signatures," In Advances in Cryptology, Proceedings of Eurocrypt'91, LNCS 547, ,pp.221-242, 1991..

[9] A.Shamir, "How to Share a Secret," Communications of the ACM, Vol. 22, No. 11, pp.612-613, 1979.

[10] David Chaum, "Undeniable Signatures," Proceedings of CRYPTO'89, pp.212-216, 1989.

[11] A.Shamir, "Identity-based cryptosystems and signature scheme," Proceedings of Crypto'84, LNCS 196, pp.47-53, 1985.

[12] A.Fiat, A.Shamir, "How to Prove Yourself: Practical Solution to Identification and Signature Problems," In Advances in Cryptology, Proceedings of CRYPTO'86, LNCS 263, pp.186-199, 1987.

[13] Whitfield Diffie, Martin E.Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol. IT-22, No. 6, pp.644-654, 1976.

[14] Taher Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp.469-472, 1985.

[15] S.H.Yun, T.Y.Kim, "Convertible Undeniable Signature Scheme," Proceedings of IEEE HPC ASIA'97, pp.700-703, 1997.

[16] S.H.Yun, S.J.Lee, "An Electronic Voting Scheme based on Undeniable Blind Signature Scheme," Proceedings of 37th IEEE Carnahan Conference on Security Technology, pp.163-167, 2003.

◐ 저 자 소 개 ◑

윤 성 현

1988년~1992년 고려대학교 컴퓨터학과(학사)
1992년~1994년 고려대학교 컴퓨터학과(석사)
1994년~1997년 고려대학교 컴퓨터학과(박사)
1998년~2002년 LG전자 중앙연구소 선임연구원
2002년~현재 천안대학교 정보통신학부 전임강사
관심분야 : 정보보호, 전자상거래 보안, DRM