대규모 선거에 적합한 전자 선거 기법에 관한 연구

윤 성 현† · 김 태 윤††

요 약

컴퓨터의 보급과 통신망의 발전으로 인간의 많은 사회적 영역이 전자화 되고 있다. 전자 선거는 민주 사회에서의 가장 중요한 사회적 행위로 전자 민주주의 실현의 기반이며, 안전한 전자 선거를 위해서 정보 보호 기술의 접목은 필수적이다.

본 논문에서는 대규모 선거에 적합한 전자 선거 기법을 제안한다. 신뢰할 수 있는 선거 관리 센터와 Chaum이 제안한 추적할 수 없는 통신망을 가정함으로써 보다 실용적인 전자 선거가 가능하다. 투표자 등록 단계에서 개인의 ID에 기반한 투표권 인증을 수행하며, 투표 및 개표 과정에 부정할 수 없는 도전/응답 프로토콜(undeniable challenge/response protocol)을 적용하여 선거 중간에 투표 결과를 알 수 없도록 한다. 제안한 방법은 투표자의 비밀성, 선거 결과의 정확성, 선거의 공정성 등과 같은 대규모 선거에서 필요한 요구 사항을 만족한다.

A Study on the Electronic Voting Scheme Suitable for Large Scale Election

Sung-Hyun Yun † · Tai-Yun Kim ††

ABSTRACT

Many areas of human activities are computerized with the wide spread use of computers and communication networks. Electronic voting is an important social activity in democratic society. The realization of electronic democracy is based on the security of electronic voting scheme. Therefore, it is necessary to use the cryptographic technique for secure election.

In this study, an electronic voting scheme suitable for large scale election is proposed. In order to make practical voting scheme, we assume that the voting authorization center is trustful and the Chaum's anonymous communication channel[6] is prepared before the election day. The center authorizes the ballot of eligible voter by using the ID based digital signature scheme in the registration stage. During the voting stage, undeniable challenge/response protocol is performed between the center and the voters to ensure that the intermediate voting results should not affect the entire election. The proposed scheme fully conforms to the requirements of large scale election such as privacy of the voters, fairness, unreusability, unforgeability and eligibility.

1. 서 론

컴퓨터의 보급과 인터넷과 같은 개방형 통신망의 발전은 인간의 많은 사회적 영역을 전자적으로 처리될 수 있게 하였다. 많은 정보를 여러 사람이 공유함으로서 작업의 효율성 및 부가가치를 창출하게 되었지만 해커나 침입자로부터의 개인 정보 보호에 대한

† 준 회 원:고려대학교 컴퓨터학과
†† 종신회원:고려대학교 컴퓨터학과
논문접수:1996년 10월 4일, 심사완료:1997년 2월 11일

문제가 심각하게 제기되고 있다. 따라서 암호 및 인증 기법을 이용한 정보 보호 기술의 적용이 필수적이다. 보안 기술의 발전 및 적용은 선거, 현금 거래 등과 같은 인간의 보다 폭 넓은 사회적 영역을 컴퓨터화함으로서 생활의 편리함 뿐만 아니라 막대한 경제적 이익을 기대할 수 있다.

선거는 민주주의 사회에서 가장 중요한 사회적 활동 중의 하나이다. 일상 생활에서의 선거 방식을 전자화할 경우 투표 용지 제작, 운반, 선거 관리 인원 등 선거와 관련된 제반 경비를 줄일 수 있다. 전자 선거의 가장 큰 걸림돌은 개방형 컴퓨터 통신망의 특성상 개인의 비밀성 침해, 이중 투표, 침입자의 태핑(tapping)에 의한 부정 투표 등 많은 위험 요소가 존재한다는 것이다.

보안 기술이 접목된 안전한 전자 선거 기법의 실현으로 얻을 수 있는 장점은 다음과 같다. 기존 선거에 필요했던 물적·인적 제반 경비 및 부정 투표의 위험성을 줄일 수 있다. 개표 과정의 복잡한 절차를 단순화하여 전자적으로 처리함으로서 개표 즉시 결과를 알 수 있다. 전자 선거에 사용된 프로토콜과 보안 기술의 안전성이 공개적으로 증명되면 선거 후 개표 결과에 대한 시비를 방지할 수 있다.

안전한 전자 선거를 위한 요구 사항은 (표 1)과 같다[1, 3, 15].

〈표 1〉 안전한 전자 선거를 위한 요구 사항 명세
〈Table 1〉 A description of requirements for secure electronic voting

요구사항	명 세
재사용 불가 (Unreusability)	· 등록된 투표자가 두 번 이상 투표할 수 없다. · 인증된 투표권은 한 번만 사용할 수 있다.
비밀성 (Privacy)	· 누가 누구에게 투표했는지 몰라야 한다. · 투표자에 대한 추적이 불가능해야 한다.
공정성 (Fairness)	· 선거 관리 센터는 투표 진행 중 전체 선거에 영향을 미칠 수 있는 중간 투표 결과를 알 수 없어야 한다.
위조 불가 (Unforgeability)	· 합법적 등록자는 인증된 투표권을 하나만 만들 수 있다. · 센터의 인증을 받은 투표권을 임의로 생성할 수 없다.
합법성 (Eligibility)	· 합법적인 절차를 거쳐서 등록된 투표자만 선거에 참여할 수 있다.

전자 민주주의 실현의 기반이 되는 전자 선거의 중요성과 함께 많은 연구가 진행되었다. 특히 인터넷의 폭 넓은 보급으로 대규모 선거에 적합한 전자 선거 기법의 개발이 주요 이슈로 등장하고 있다[1, 2, 3]. 특징은 실용적인 프로토콜을 위해서, 적어도 하나 이상의 신뢰할 수 있는 선거 관리 센터의 존재를 가정한다는 것이다. 또한 투표자의 비밀성을 보장하기 위해서 익명을 생성하고 Chaum이 제안한 추적할 수 없는 통신망[6]의 존재를 가정한다.

본 연구에서는 투표자 등록 및 개표 과정을 개선한 실용적인 전자 선거 기법을 제안한다. Baraani의 전자 선거 기법에서 투표자의 익명은 신뢰할 수 있는 선거 관리 센터에 의해 생성되며 안전한 통신망을 통해서 투표자에게 분배 된다[1]. 따라서 선거 준비 단계에서 위험 부담이 많이 따르며 실용적이지 못하다. 본 연구에서는 투표자 등록 단계에서 투표자가 자신의 익명을 생성하도록 함으로서 인터넷과 같은 불안전한 공중망을 통해서 보다 실용적이고 안전한 전자 선거 기법을 실현한다.

투표 및 개표 단계에서 선거 관리 센터와 투표자 간에 부정할 수 없는 도전/응답(undeniable challenge/response) 기법[10]을 적용하여 투표 단계에서 선거 관리 센터가 중간 투표 결과를 알 수 없도록 한다. 투표권에 대한 분쟁 발생시 기존의 전자 선거 기법에서는 등록 단계에서 사용된 디지털 서명을 근거로 제시해야 한다. 이 경우, 투표자의 신분이 밝혀지게 되는 단점이 있다. 제안한 전자 선거 기법은 투표 및 개표 단계에 부정할 수 없는 도전/응답 기법을 응용하여 익명적으로 분쟁을 해결할 수 있는 특성을 갖는다.

2장에서는 전자 선거 기법과 관련된 현재까지의 주요 연구 방향을 살펴본다. 3장에서는 Baraani의 전자 선거 모형[1]에 기반한 제안한 전자 선거 기법을 설명하고, 4장에서는 선거 요구 사항에 따른 안전성 분석을 한다. 5장에서 결론 및 향후 연구 과제를 제시한다.

2. 관련 연구

대규모 전자 선거에 적합한 기존의 전자 선거 기법들은 다음과 같은 두가지 가정에 기반한다. (가정 1과 2)는 실용적인 전자 선거를 위해서 필수적이다.

(가정 1) 추적 불가능한 통신망(Anonymous Com-

munication Channel)

투표자들과 선거 관리 센터 간에 Chaum이 제안한 추적 불가능한 통신망[6]이 존재한다.

인터넷과 같은 개방형 공중망은 특성상 외부 해커에 의한 능동적 공격이 가능하다. 인증된 익명을 획득한 투표자들의 투표권 행사시에 어느 곳으로부터 투표권이 전송되었는 지 역추적될 경우 투표자들의 비밀성은 보장될 수 없다. 전자 선거 기법에서 투표자의 비밀성은 가장 중요한 요구 사항 중의 하나이기 때문에 투표자의 익명과 더불어 추적할 수 없는 통신망이 존재한다는 가정 하에서만 실현될 수 있다.

(가정 2) 신뢰할 수 있는 선거 관리 센터

합법적 투표자 등록 및 투표권 인증을 수행하는 신뢰할 수 있는 선거 관리 센터가 적어도 하나 이상 존재한다.

전자 선거는 특성상 부정 투표와 투표자의 비밀성 간의 상반 관계가 존재한다. 부정 투표는 등록되지 않은 투표자가 투표하는 것으로 부정 투표를 방지하기 위한 가장 확실한 방법은 디지털 서명 기법을 직접 적용하는 것이다. 이 경우, 누가 누구에게 투표했는지 투표자는 부인할 수 없고 모든 사용자가 투표권의 정당성을 확인할 수 있다. 부정 투표는 막을 수 있지만 투표자의 비밀성을 보장할 수 없기 때문에 민주주의 사회에서의 선거로는 적용될 수 없다.

투표자의 비밀성을 보장하기 위해서는 투표자는 자신의 이름 대신에 익명을 사용하여 투표해야 한다. 이 경우 누가 누구에게 투표했는 지 알 수 없기 때문에, 부정 투표의 위험성이 매우 크다. 따라서 등록된 투표자 만이 익명으로 전자 선거에 참여할 수 있도록 관리해 주는 신뢰할 수 있는 선거 관리 센터가 반드시 존재해야 한다.

(가정 2)는 전자 선거의 실용성과 밀접한 관계가 있다. 신뢰할 수 있는 센터 없이 투표자의 비밀성을 보장하는 전자 선거 기법의 경우에 각 투표자의 통신 단계 수와 연산량이 선거에 참여한 투표자들의 수에 비례해서 증가한다[15]. 열 명 내외의 투표자들이 참가하는 소규모 전자 선거에 적용될 수 있다. 인터넷을 이용한 대규모 전자 선거에는 과도한 연산량과 통신 복잡도로 실현될 수 없다. 따라서 대규모 전자 선거에 적합한 대표적인 전자 선거 기법들은 일상 생활에서의 중앙 선거 관리 위원장과 같은 신뢰할 수 있는 선거 관리 센터의 존재를 가정한다.

Boyd가 제안한 전자 선거 기법[4]은 이산 대수 문제의 어려움에 근거한 복수키 암호 방법의 안전성에 기반한다. 투표자 등록 과정에서 투표자의 비밀성을 보장하며 투표 과정의 비밀성은 Chaum이 제안한 추적 불가능한 통신망에 기반한다. 단점은 선거 관리 센터가 투표 단계에서 중간 투표 결과를 알 수 있기 때문에 선거의 공정성을 실현하지 못한다는 것이다.

Fujioka, Okamoto, Ohta가 제안한 전자 선거 기법[3]은 비트 도전 기법(bit commit- ment scheme)을 적용하여 투표 단계에서 선거 관리 센터가 중간 투표 결과를 알 수 없도록 함으로서 선거의 공정성을 실현한다. 단점은 등록된 투표자가 도중에 투표권 행사를 포기할 수 없기 때문에 대규모 전자 선거를 위한 기법으로는 실용적이지 못하다.

Baraani는 대규모 전자 선거에 적합하도록 Fujioka가 제안한 전자 선거 기법[3]을 개선하여 좀 더 실용적인 기법을 제안하였다[1]. 등록된 투표자가 중도에 선거에 불참하더라도 전체 선거 결과에 영향을 미치지 않으며 threshold 개념을 적용하여 투표자, 후보자 및 선거 관리자들의 부정을 최소화 하고자 하였다. 단점은 전자 선거 준비 단계에서 신뢰할 수 있는 센터가 각 투표자에게 안전한 통신망을 통해서 익명을 제공해야 하는 부담이 따른다는 것이다. 또한 등록된 투표자가 투표를 하지 않을 경우 선거 관리자(administrator)들에 의한 부정이 가능하다.

Horster가 제안한 전자 선거 기법은 신뢰할 수 있는 센터의 역할을 최소화하기 위해서 선거 관리자를 여러 명 두는 방식이다[2]. 온닉 다중 서명 기법(blind multisignature scheme)을 적용하여 적어도 한 명의 선거 관리자를 신뢰할 수 있다면 전자 선거의 공정성을 실현할 수 있다. 단점은 투표자에 의해서 전자 선거의 공정성을 실현할 수 없고, 선거 관리자의 신뢰성에 의존한다는 것이다. 따라서 선거 관리자들이 결탁할 경우 투표 단계에서 중간 투표 결과를 알 수 있고, 전체 선거 결과에 영향을 미칠 수 있다. 특히 투표 등록을 위한 통신 복잡도가 투표자 개인당 선거 관리자 수 만큼 배가하기 때문에 대규모 전자 선거에 적합하지 않다.

3. 제안한 전자 선거 기법

본 논문에서는 Baraani의 기법[1]을 개선한 실용적인 전자 선거 기법을 제안한다. 제안한 방법은 대규모 전자 선거에 적합하도록 (가정 1, 2)에 정의된 Chaum의 추적할 수 없는 통신망과 신뢰할 수 있는 선거 관리 센터의 존재에 기반한다.

〈표 2〉 제안한 전자 선거 기법의 구성
〈Table 2〉 The electronic voting steps of the proposed scheme

준비 단계	1. 유한체 GF(p)와 생성자 g 공개 2. 선거일과 후보자 공고 3. 센터의 공개키 Y 공개 4. 투표자들의 ID 공개
등록 단계	1. 투표자의 은닉 투표권 생성 및 서명 2. 센터의 은닉 투표권 인증 3. 투표자의 인증된 투표권 획득
투표 단계	1. 투표자의 인증된 투표권 전송 2. 선거 관리 센터의 투표권 공고
개표 단계	1. 투표자 확인 및 익명 전송 2. 센터의 개표

(표 2)는 제안한 전자 선거 기법의 절차로 준비 단계, 등록 단계, 투표 단계, 개표 단계로 구성된다. 등록 단계에서 개인의 ID 정보에 기반한 디지털 서명 기법[11, 12]을 적용하여 은닉 투표권(blinded ballot)에 대한 디지털 서명을 생성한다. 개인 정보에 바탕을 둔 서명 기법을 적용함으로서 전자 주민증 시대의 지자제 선거나 국회 의원 투표와 같은 대규모 선거에 적합하며 실제 투표 과정의 투명성을 반영한다. 투표자의 익명은 등록 단계에서 투표자가 직접 결정함으로서 센터에 대한 의존도 및 외부 해킹에 대한 위험 요소를 줄였다.

투표 및 개표 단계에서 부정할 수 없는 도전/응답 기법을 적용하여 전자 선거의 공정성 실현과 더불어 분쟁 발생시 투표자의 비밀성을 보장하면서 투표권의 위조 여부를 밝힐 수 있는 특징이 있다. (가정 1, 2)와 더불어 등록 단계에 사용된 디지털 서명 기법이 안전하면 제안한 방법은 투표자 및 외부 해커로부터의 공격에 대해서 안전하다.

3.1 준비 단계

단계 1:선거 관리 센터는 안전한 전자 선거를 위한 파라미터를 공개한다. 법 p에 대한 이산 대수 문제가 계산상 불가능 하도록 암호학적으로 안전한 유한체 $GF(p)$와 생성자 g를 선택한다. 센터의 공개키 Y와 함께 게시판에 공고한다. 선거 관리 센터의 비밀키 X와 공개키 Y는 다음과 같다.

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

〈표 3〉 후보자 이름과 익명
〈Table 3〉 Candidate's name and corresponding pseudonym

후보자 이름	익명
C_1	$cdname_1$
C_2	$cdname_1$
⋮	⋮
C_{n-1}	$cdname_{n-1}$
C_n	$cdname_n$

단계 2:선거 관리 센터는 선거일과 후보자 인적 사항을 게시판에 공고한다. 후보자 이름과 익명은 (표 3)과 같다.

$$cdname_i \in Z_{p-1}$$

단계 3:투표 참여자의 ID를 게시판에 공고한다.

3.2 등록 단계

등록 단계에서는 게시판에 공고된 유권자들이 합법적인 절차를 통해서 선거 관리 센터의 인증을 받은 투표권을 생성한다. 투표자가 투표 단계에서 사용할 투표권은 센터가 등록 단계에서 인증한 투표권과 달라야 투표자의 비밀성을 보장할 수 있다. 은닉 기법(blinding technique)을 적용하여 투표자는 선거 관리 센터로부터 은닉 투표권에 대한 인증을 받는다. 인증된 은닉 투표권으로부터 은닉 값(blinding factor)을 해제하여 인증된 투표권을 생성한다.

(1) 투표자 i의 투표권 생성 및 서명

단계 1:의사 난수 발생기(pseudo random number generator)를 사용해서 사용자 ID 대신 투표에 사용할 익명을 만든다. 선거 관리 센터에서 공고한 후보자들 중 한 명을 선택한다. 두 값을 곱해서 투표권을 생성한다. 투표자 i는 익명 Ps_i 값을 조정하여 투표권 $Ballot_i$이 법 p에 대한 원시근(primitive root of mod p)이 되도록 한다.

Ps_i:투표자 i의 익명, $Ballot_i$:투표자 i의 투표권

$Ballot_i: Ps_i \cdot cdname_i$

단계 2:다음 조건을 만족하는 임의의 난수 bf, ubf를 생성해서 $Ballot_i$를 은닉(blind) 한다.

bf:은닉값(blinding factor),

ubf:은닉 해제값(unblinding factor)

$B(,)$:은닉 함수(blinding function), $B(ballot_i, bf)$:투표자 i의 은닉 투표권

$bf \cdot ubf \equiv 1 \pmod{p-1}$, $B(ballot_i, bf) \equiv ballot_i^{bf} \pmod{p}$

단계 3:은닉 투표권 $B(ballot_i, bf)$에 대한 디지털 서명을 생성한다. 개인의 ID 정보에 기반한 서명 기법을 적용한다. 디지털 서명은 투표자의 은닉 투표권과 신분을 인증하는 수단이므로 합법적인 투표자 등록을 위해서 필수적이다.

$S(,)$:ID 기반 디지털 서명 생성 함수

$V(,)$:ID 기반 디지털 서명 검증 함수

KEY_i:투표자 i의 비밀키

$S(KEY_i, B(Ballot_i, bf))$:투표자 i의 은닉 투표권에 대한 디지털 서명

단계 4:선거 관리 센터로 $(ID_i, B(Ballot_i, bf), S(KEY_i, B(Ballot_i, bf)))$를 전송한다.

(2) 선거 관리 센터의 은닉 투표권 인증

단계 1:선거 관리 센터는 투표자가 두 번 이상 등록하지 못하도록 센터로부터 투표권을 인증 받은 투표자들의 ID와 투표자 i의 ID를 비교해서, 투표자 i가 처음으로 등록한 경우에만 다음의 투표권 인증 프로토콜을 수행한다.

단계 2:투표자 i의 은닉 투표권 $B(Ballot_i, bf)$에 대한 디지털 서명을 검증한다. 투표자 i가 은닉 투표권에 올바르게 서명한 경우 (단계 3)을 수행한다. 그렇지 않을 경우 선거 관리 센터는 투표자 i에게 서명이 잘못됐음을 알리고 투표권 인증 프로토콜을 취소한다.

$V(ID_i, S(KEY_i, B(Ballot_i, bf))) = B(Ballot_i, bf)$:올바른 서명이다.

$V(ID_i, S(KEY_i, B(Ballot_i, bf))) \neq B(Ballot_i, bf)$:잘못된 서명이다.

단계 3:투표자 i의 ID를 저장하고 은닉 투표권 $B(Ballot_i, bf)$를 인증한다. 등록된 투표자 ID를 저장함으로서 투표자가 두 번 이상 등록하지 못하게 한다.

$S_A(,)$:선거 관리 센터의 인증 함수

$S_A(X, B(Ballot_i, bf)) \equiv B(Ballot_i, bf)^X \pmod{p}$

단계 4:인증된 은닉 투표권 $S_A(X, B(Ballot_i, bf))$을 투표자 i에게 전송한다.

(3)인증된 은닉 투표권으로부터 인증된 투표권 획득

단계 1:투표자 i는 선거 관리 센터로부터 인증받은 은닉 투표권을 수신한다.

$$S_A(X, B(Ballot_i, bf)) \equiv B(Ballot_i, bf)^X \pmod{p}$$
$$\equiv Ballot_i^{bf \cdot X} \pmod{p}$$
$$\equiv (Ps_i \cdot cdname_i)^{bf \cdot X} \pmod{p}$$

단계 2:인증된 은닉 투표권으로부터 은닉값 bf가 제거된 투표권(unblinded ballot)을 추출한다.

$Ballot_i^X$:투표자 i의 인증된 투표권

$$B(S_A(X, B(Ballot_i, bf)), ubf) \equiv B(Ballot_i, bf)^{X \cdot ubf} \pmod{p}$$
$$\equiv Ballot_i^{bf \cdot ubf \cdot X} \pmod{p}$$
$$\equiv (Ballot_i)^X \pmod{p} \ (\because bf \cdot ubf \equiv 1 \pmod{p-1})$$

3.3 투표 단계

투표자는 부정할 수 없는 도전/응답 프로토콜을 이용하여 인증된 투표권을 선거 관리 센터로 전송한다. 투표자의 비밀성은 등록 단계에서 사용된 은닉 기법과 Chaum이 제안한 추적할 수 없는 통신망에 기반한다. 등록 단계에서 선거 관리 센터의 인증을 받기 위해 사용된 은닉 투표권과 투표자가 추출한 인증된 투표권은 서로 다르기 때문에 선거 관리 센터를 포함한 투표 참여자들은 누가 누구에게 투표했는지 알 수 없다. 투표 단계에서 투표자는 인증된 투표권을 Chaum의 추적할 수 없는 통신망을 이용하여 선거 관리 센터로 전송하므로 투표권이 어느 곳으로부터 전송되

었는 지 역추적할 수 없다.

(1)투표자 i의 투표권 행사

단계 1:선거의 공정성을 실현하기 위해서 투표자는 다음 조건을 만족하는 임의의 난수 a, b를 선택해서 부정할 수 없는 도전/응답 프로토콜을 진행한다.

CV_i:투표자 i의 도전(challenge),
$a, b \in_R Z_{p-1}$:도전값(challenge value)
$CV_i \equiv Ballot_i^{X \cdot a} \cdot Y^b \pmod{p}$

단계 2:Chaum이 제안한 추적할 수 없는 통신망을 이용하여 선거 관리 센터로 Ps_i와 CV_i를 전송한다.

(2)선거 관리 센터의 투표권 공고

단계 1:투표자 i의 도전 CV_i에 대한 응답(response)을 생성한다.

RP_i:투표자 i의 도전에 대한 선거 관리 센터의 응답

$$RP_i \equiv CV_i^{X^{-1}} \pmod{p}$$
$$\equiv (Ballot_i^{X \cdot a} \cdot g^{X \cdot b})^{X^{-1}} \pmod{p}$$
$$\equiv Ballot_i^a \cdot g^b \pmod{p}$$

단계 2:선거 관리 센터는 (Ps_i, CV_i, RP_i)를 게시판에 공고한다.

3.4 개표 단계

투표자는 게시판에 공고된 자신의 익명을 확인하고 인증된 투표권의 도전에 대한 선거 관리 센터의 응답이 올바른지 검증한다. 응답이 잘못된 경우 두 번째 도전을 생성하여 선거 관리 센터가 부정하는 것인지 투표권이 잘못된 것인지 확인한다. 기존의 전자 선거 기법과 달리 분쟁 발생시 투표자는 추적할 수 없는 통신망을 이용하여 익명적으로 분쟁을 해결할 수 있는 특성을 갖는다.

(1)투표자 i의 투표권 검증 및 도전값 전송

단계 1:투표자 i는 공고된 (Ps_i, CV_i, RP_i)로부터 CV_i에 대한 응답 RP_i를 인증한다.

$RP_i \equiv Ballot_i^a \cdot g^b \pmod{p}$:올바른 투표권

$RP_i \neq Ballot_i^a \cdot g^b \pmod{p}$:잘못된 투표권 또는 선거 관리 센터가 부정을 하는 경우

단계 2:선거 관리 센터로 개표에 필요한 도전값 a, b를 전송한다.

(2)선거 관리 센터의 개표

단계 1:선거 관리 센터는 투표자 i로부터 전송 받은 도전값 a, b를 이용하여 투표권을 개봉하고 해당 후보자의 표 수를 하나 증가시킨다.

$$cdname_i \equiv (RP_i \cdot g^{-b})^{a^{-1}} \cdot Ps_i^{-1} \pmod{p}$$
$$\equiv (Ballot_i^a \cdot g^b \cdot g^{-b})^{a^{-1}} \cdot Ps_i^{-1} \pmod{p}$$
$$\equiv (Ballot_i \cdot Ps_i^{-1} \pmod{p}$$
$$\equiv cdname_i \cdot Ps_i \cdot Ps_i^{-1} \pmod{p}$$
$$\equiv cdname_i \pmod{p}$$

단계 2:선거 관리 센터는 $(Ps_i, CV_i, PR_i, a, b, Ballot_i, cdname_i)$를 게시판에 공고한다.

(3)분쟁 해결 프로토콜

제안한 전자 선거 기법에서 투표권에 대한 분쟁이 발생할 경우 익명적인 분쟁 해결이 가능하다. 투표 및 개표 단계에 부정할 수 없는 도전/응답 기법[10]을 적용함으로써 선거 관리 센터가 올바른 투표권에 대해서 부인할 수 없는 특성을 갖는다. 분쟁이 발생한 경우 투표자는 추적할 수 없는 통신망을 이용해서 두 번째 도전을 전송하고 선거 관리 센터는 이에 대한 응답을 공고한다. 투표자는 첫 번째 응답 RP_i와 두번째 응답 RP_i'을 이용하여 다음 판단식을 생성하고 선거 관리 센터의 부정을 검증한다.

c, d:두번째 도전 값
$R_1 \equiv (RP_i \cdot g^{-b})^c \pmod{p}$, $R_2 \equiv (RP_i' \cdot g^{-d})^a \pmod{p}$
$R_1 = R_2$:투표자의 투표권이 잘못된 경우이다.
$R_1 \neq R_2$:선거 관리 센터가 올바른 투표권에 대해서 부인하는 경우이다.

4. 안전성 분석

신뢰할 수 있는 선거 관리 센터와 Chaum의 추적할 수 없는 통신망이 존재한다는 가정 하에서 제안한 전자 선거 기법은 내·외적인 공격으로부터 안전하다.

안전한 전자 선거에 요구되는 선거 요구 사항별로 제안한 전자 선거 기법에 대한 안전성을 분석한다.

(정리 1) 재사용 불가(Unreusability)

투표자는 투표자 등록 단계에서 획득한 인증된 투표권을 이용하여 두 번 이상 투표할 수 없다.

(증명) 먼저 합법적인 투표자가 두 번 이상 등록할 수 없음을 보이고 인증된 투표권을 재사용할 수 없음을 보인다. 선거 관리 센터는 투표자 등록 단계에서 투표권을 부여한 투표자 ID를 보관하고 점검함으로서 투표자가 두 번 이상 등록할 수 없도록 한다. 투표자가 인증된 투표권을 재사용하기 위해서는 익명이 달라야 하므로 (식 4.1)을 만족하는 익명 Ps_i'을 만들어야 한다.

$$cdname_i \cdot Ps_i = cdname_i \cdot Ps_i' \tag{4.1}$$

Ps_i, Ps_i'은 1보다 크고 $p-1$ 보다 작은 정수이다. Ps_i와 다른 값을 갖으면서 (식 4.1)을 만족하는 Ps_i'은 없다.

(정리 2) 비밀성(Privacy)

투표자의 비밀성은 투표권 은닉 기법의 안전성과 (가정 1)에 기반한다. 선거 참여자는 누가 누구에게 투표했는지 알 수 없다.

(증명) 선거 참여자가 누가 누구에게 투표했는지 알기 위해서는 은닉 투표권과 인증된 투표권의 상관관계를 유추해낼 수 있어야 한다.

$$\begin{aligned} &Ballot_i' \equiv Ballot_i^{bf} \pmod p \\ &T = Ballot_i, \qquad T' \equiv T^{bf} \pmod p \\ &bf \equiv \log_T T' \pmod p \end{aligned} \tag{4.2}$$

은닉 값 bf를 구하는 것은 $GF(p)$ 상에서의 이산 대수 문제가 된다. 따라서 투표자 ID와 익명과의 관계를 유추할 수 있는 파라미터 bf를 찾는 문제는 계산상 불가능하다[13, 14].

투표자들은 투표 및 개표 단계에서 투표권을 (가정 1)에 정의된 Chaum의 추적할 수 없는 통신망을 이용하여 선거 관리 센터로 전송한다. 따라서 투표권에 대한 추적이 불가능하기 때문에 선거 참여자는 누가 누구에게 투표했는지 알 수 없다.

(정리 3) 공정성(Fairness)

선거 관리 센터는 전체 선거 결과에 영향을 미칠 수 있는 중간 투표 결과를 투표 단계에서 알 수 없다.

(증명) 투표자는 투표 단계에서 투표권에 대한 도전을 생성하여 선거 관리 센터로 전송한다. 선거 관리 센터는 투표자의 도전에 대한 응답을 생성하고 게시판에 공고한다. 투표자는 응답을 검증하여 올바르면 투표 종료 후에 개표를 위한 도전 값을 전송한다.

선거 관리 센터가 투표 단계에서 중간 투표 결과를 알기 위해서는 다음과 같이 인증된 투표권에 대한 도전으로부터 도전 값 a, b를 유추해내야 한다.

$$CV_i \equiv Ballot_i^{Y \cdot a} \cdot Y^b \pmod p \tag{4.3}$$

(식 4.3)에서 도전 값 a, b를 구하는 문제는 법 p에 대한 이산 대수 문제로 계산상 불가능하다. 따라서 선거 관리 센터는 투표 단계에서 투표자들의 투표권을 개봉할 수 없다.

(정리 4) 위조 불가능(Unforgeability)

투표자는 인증된 투표권을 임의로 만들 수 없다.

(증명) 투표를 위조하기 위해서는 다음과 같이 익명과 인증된 투표권을 임의로 만들 수 있어야 한다.

$$Ps_i, (cdname_i \cdot Ps_i)^X \pmod p)$$

선거 관리 센터의 인증 값 X를 유추하는 것은 (정리 2, 3)에서와 같이 $GF(p)$ 상에서의 이산 대수 문제가 된다. 따라서 투표자에 의한 투표권 위조는 불가능하다.

(정리 5) 합법성(Eligibility)

투표자 등록 단계에서 사용된 디지털 서명 기법이 안전하면 합법적인 투표자만 선거에 참여할 수 있다.

(증명) 디지털 서명 기법은 전자 문서에 대한 서명

을 생성하는 기법으로 서명자는 자신이 서명한 전자 문서에 대해서 부인할 수 없는 특성을 갖는다. 디지털 서명은 서명자 만이 생성할 수 있기 때문에 투표자 등록 단계에서 투표자 신분 확인 및 은닉 투표권에 대한 인증에 사용된다. 등록되지 않은 투표자가 전자 선거에 참여하기 위해서는 등록된 투표자들의 공개키로 검증 가능한 디지털 서명을 생성할 수 있어야 한다. 전자 선거에 사용된 디지털 서명 기법이 안전하고 선거 관리 센터를 신뢰할 수 있으면 합법적인 투표자만 전자 선거에 참여할 수 있다.

5. 결 론

본 논문에서는 대규모 전자 선거에 적합한 전자 투표 방법을 제안하였다. 제안한 방법은 대규모 전자 선거에 적합하게 개인의 ID 정보에 기반하여 투표자 등록을 수행한다. 투표자에 의해 익명이 생성됨으로써 선거 준비 단계의 부정을 최소화한다. 투표 및 개표 과정에 센터와 투표자간의 부정할 수 없는 도전/응답 기법을 적용하여 선거의 공정성을 실현하였고, 분쟁 발생시 투표자가 익명적으로 분쟁을 해결할 수 있는 특성을 갖는다. 신뢰할 수 있는 선거 관리 센터와 추적 불가능한 통신망[6]이 존재한다는 가정하에 제안한 방법은 안전한 대규모 전자 선거를 위한 요구사항을 만족한다.

향후 연구 과제로는 모든 서명자들의 동의하에서만 서명 검증을 할 수 있는 디지털 다중 서명 기법(undeniable digital multisignature scheme)에 대한 연구이다. 여러 명의 선거 관리자들로 구성되는 대규모 전자 선거에 적용할 경우, 신뢰할 수 있는 선거 관리 센터의 역할을 최소화할 수 있다. 후보자 정당별로 선거 관리자를 두어서 모든 선거 관리자들의 동의 하에서만 투표자 등록 및 개표를 할 수 있고, 분쟁 발생시 익명적으로 분쟁을 해결할 수 있도록 함으로써 개인의 비밀성을 보장하면서 선거 관리 센터에 의한 부정을 최소화할 수 있다.

참 고 문 헌

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

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

[8] Torben 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 and 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 and 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] B. Schneier, Applied Cryptography, 2nd Edition, John Wiley&Sons Press, 1996.

[16] David M. Burton, Elementary Number Theory, 3rd Edition, Wm. C. Brown Publishers, 1994.

윤 성 현

1992년 고려대학교 컴퓨터학과 (학사)

1994년 고려대학교 컴퓨터학과 (석사)

1997년 고려대학교 컴퓨터학과 (박사)

1996년~현재 고려대학교 멀티미디어네트워크 연구실 연구원

관심분야:컴퓨터 통신 보안, EDI 시스템

김 태 윤

1981년 고려대학교 산업공학과 학사

1983년 미국 Wayne State University 전산과학과 석사

1987년 미국 Auburn University 전산과학과 박사

1988년~현재 고려대학교 컴퓨터학과 교수

관심분야:컴퓨터 그래픽스, 컴퓨터 네트워크, EDI 시스템, ISDN, 이동통신, 위성통신 등