情 報 保 護 學 會 誌
第 15 卷 第 5 號, 2005. 10

대규모 전자선거 기법 연구 동향 및 부인봉쇄 서명을 적용한 전자선거 기법

윤 성 현*

요 약

선거는 민주주의 사회에서 가장 중요한 사회적 행위 중의 하나이다. 여러 사회적 행위의 전자화를 위해서 정보보호 기술이 접목되고 있으며, 아직까지 개인의 익명성과 관련된 선거, 현금과 같은 분야는 매우 많은 요구사항으로 인하여 전자화 되지 못 하고 있는 실정이다. 본 논문에서는 규모가 큰 선거에서의 전자 선거 기법 도입을 위한 다양한 요구사항들을 분석하고, 전자선거 기법 구현시의 문제점 및 투표 및 개표 시스템의 전자화와 관련된 연구 동향을 알아본다. 또한, 부인봉쇄 서명 기법을 적용하여 전자선거에서의 투표자 중심의 요구사항을 만족하며 투표권에 대한 부인봉쇄 다중서명을 생성하도로 함으로써 보다 공정한 전자선거가 될 수 있는 인터넷 기반 전자선거 기법을 제안한다.

Ⅰ. 서 론

전자 선거는 선거의 모든 단계 또는 일부 단계를 전자화 하는 것을 의미한다. 국회의원 선거, 대통령 선거와 같은 대규모 전자선거 기법에 대한 연구는 부분 전자 선거와 인터넷 기반 전자선거의 두 가지로 구분된다. 선거의 모든 단계를 전자적으로 처리하는 것이 인터넷 기반 전자선거 이며 기존 선거 시스템의 투표 오류 및 개표의 신뢰성 확보를 위하여 투개표 시스템에 전자식 방식을 부분적으로 도입한 것이 부분 전자선거기법이다.[1-3]

선거는 민주주의 사회에서 가장 중요한 사회적 행위 중 하나로 막대한 예산과 비용이 소요되는 관리 절차가 필수적이다. 투표일, 투표 장소, 투표 시간, 후보자 및 유권자 등록에 대한 공고를 해야 하고 투표를 위한 용지 제작 및 운송, 공정한 선거를 위하여 정당별 선거관리인단을 구성하여 투표 및 개표 절차에 대한 감시 및 집계가 이루어져야 한다.

여러 가지 문제점에도 불구하고 전자선거에 대한 연구가 지속되는 이유는, 선거와 관련된 상기한 막대한 소요 경비를 절감할 수 있기 때문이다. 또한, 시간적/공간적 제약을 부분적으로 극복할 수 있으며, 이에 따른 투표 참여율을 높일 수 있다. 수작업에 의한 투개표 단계에서의 오류를 최소화함으로써 선거결과에 대한 신뢰성을 높일 수 있으며, 기타 인터넷을 통한 의견수렴의 용도로도 활용될 수 있다.

디지털 데이터는 원본과 복사본의 구분이 불가능하기 때문에 투표권 파일을 복제하여 이중으로 투표할 수 있다. 이 경우에 사용자 인증 또는 디지털 서명 기법 등을 이용하여 이중 투표를 방지할 수 있지만 투표자 개인의 익명성이 보장되지 않는 문제가 발생하게 된다. 민주주의 사회의 선거에서는 누가 누구에게 투표했는지 알 수 없어야 한다. 다양한 요구사항을 만족시켜야 하는 전자선거 기법의 구현을 위해서 정보보호 기술의 접목은 필수적이다.

본 논문에서는 대규모 전자선거기법에 대한 기존 요구사항 및 인터넷 기반 전자선거 방식의 문제점에 대해서 분석한다. 또한 부분 전자선거 방식과 관련된 최근의 연구동향과 투표자 중심의 요구사항에 대해서 알아본다. 부인봉쇄 서명을 적용하여 사용자 편의성, 선거의 공정성과 같은 특성을 갖는 전자선거 기법을 제안하고 부인봉쇄 서명 방식을 적용함으로써 얻을 수 있는 부가적인 특성에 대해서 분석한다.

Ⅱ. 대규모 전자선거 기법 요구사항 분석

2장에서는 대규모 전자선거 구현을 위해서 필요한 요구사항에 대해서 살펴본다. 먼저 기본적인 요구사항

* 천안대학교 정보통신학부 (shyoon@cheonan.ac.kr)

에 대해서 기술하고, 2.1절에서 투표자 중심의 요구사항, 2.2절에서 전자선거의 주요 문제점 및 최근의 연구 동향에 대해서 알아본다.

대규모 전자 선거를 위한 기본 요구사항은 다음과 같다.[4,5,7,12,13]

· 재사용불가(unreusability)

등록된 유권자는 하나의 투표권만 행사할 수 있어야 한다. 즉, 투표권 복제에 의한 이중 투표가 불가능해야 한다.

· 익명성(privacy, untraceability)

구성원들이 누가 누구에게 투표했는지 알 수 없어야 하는 것으로 민주 선거에 있어서 가장 중요한 요구사항 중의 하나이다. 전자투표 결과로부터 투표자 신원과 투표권을 연결할 수 없어야 하며, 공중망을 이용하여 투표할 경우에 투표자의 투표권을 추적할 수 없어야 한다.

· 공정성(fairness)

투표 단계에서 선거결과를 미리 예측할 수 없어야 하는 것으로, 투표권은 개표 단계에서만 공개되어야 한다.

· 위조불가(unforgeability)

제 3자가 법적 효력을 갖는 투표권 파일을 만들 수 없어야 한다.

· 합법성(eligibility)

등록된 유권자만이 전자선거에 참여할 수 있다.

· 완전성(completeness)

모든 유효 표가 개표에 반영되어야 하는 것으로 전자선거 소프트웨어의 신뢰성과 관련이 있다. 소프트웨어는 버그가 없어야 하고, 해킹 위협이 없도록 안전하게 코딩되어야 하며 부정 투표 시비를 없애기 위해 소스가 완전히 공개되어야 한다.

· 강건성(robustness)

선거관리 센터의 부정을 최소화하는 것으로, 여러 명의 선거관리자를 두어 투/개표 시의 센터의 권한을 분산해야 한다.

2.1 투표자 중심의 요구사항

투표자 중심의 전자선거 요구사항은 기존 선거방식에서 제공할 수 없었던 전자선거에서만 가능한 특성들이다. 투표자가 직접 선거의 공정성과 신뢰성을 평가할 수 있으며, 투표자의 편의성이 고려되어야 하며 투표자에 대한 강압적 매표 행위가 없어야 한다.[2-4,13]

· 개별검증(individual verifiability)

투표자가 직접 자신의 투표권이 개표에 올바르게 반영되었는지 확인할 수 있어야 한다. 기존 선거에서는 투표함과 투표함 개봉 및 집계 절차를 전적으로 신뢰함으로써 투표자들이 선거 결과에 승복했지만, 전자선거에서는 투표자들이 직접 자신의 의견이 결과에 반영되었는지 확인할 수 있어야 한다.

· 전체검증(universal verifiability)

모든 구성원이 개별 투표권의 유효성과 전체 선거결과의 유효성을 확인할 수 있어야 한다.

· 매표 방지(receipt-freeness)

유권자가 다른 사람에게 투표권을 팔 수 없도록 하는 것으로, 자신의 투표권을 가지고 누구에게 투표했는지 증명할 수 없어야 한다.

· 강압적 투표 방지(uncoercibility)

유권자의 투표 행위가 독립적으로 수행되어야 하는 것을 뜻한다. 즉, 투표권 생성/등록/투표 단계에서 제3자가 참여 및 감시할 수 없어야 한다.

· 투표 취소 및 재투표(vote cancellation and re-voting)

투표 기간 중에 유권자의 마음이 변경되면 언제든지 이전 투표에 대한 취소와 재투표가 가능해야 한다. 기존 선거 시스템에서 실현하기 어려운, 전자 선거이기에 가능한 사용자 편의성을 고려한 요구사항이다.

매표 방지와 강압적 투표 방지 요구사항은 기존 선거 시스템에서 투표 장소와 기표소 그리고 투표함에 투표용지를 넣는 행위를 선거 관리인단이 한 자리에 모여 감시함으로써 실현하고 있다. 따라서 두 요구사항은 컴퓨터와 인터넷을 이용하는 전자선거에 있어서 요구되는 추가적 요구사항이라고 할 수 있다.

2.2 전자 선거의 문제점 및 최근 연구 동향[1-3]

전자선거 실현에 있어서 가장 중요한 문제점은 매표 행위 및 강압에 의한 투표를 근본적으로 차단할 수 있는가의 여부이다.

현행 선거 방식은 유권자 등록을 마친 투표자가 투표를 하기 위해서는 선거관리인단의 감시 하에 기표소로 혼자 들어가 기표를 하고 투표권을 투표함에 넣음으로써 매표방지 및 강압적 투표를 예방하고 있다. 전자선거의 경우에 등록 및 투표 단계가 컴퓨터와 인터넷을 이용하여 모두 전자적으로 수행되기 때문에 유권자들의 투표 행위를 선거관리 센터가 감시할 수 없다.

결국 모든 구성원이 투표자의 투표권 생성 및 투표 행위를 바로 옆에서 지켜보아도 누구에게 투표 했는지 알 수 없어야만 매표방지 및 강압에 의한 투표를 예방할 수 있다. 이는 매우 어려운 가정이며, 따라서 완전한 전자선거 방식보다는 기존 선거 방식의 투개표 시스템의 전자화를 위한 부분 전자선거 방식에 대한 연구가 보다 실질적인 접근이 되고 있다.

부분 전자선거 방식에서는 사용자 등록 및 투표 행위는 기존의 선거 시스템의 신뢰성 확보 방법과 동일하며(매표 방지 및 강압적 투표 예방), 투표 및 개표 과정의 전자화를 통해서 기존 선거 방식의 신뢰성과 효율성을 높여줄 수 있다.

2000년 미국 대통령 선거에서의 플로리다 주 대규모 무효표 발생 사건과 더불어 최근 HAVA 프로젝트를 중심으로 선거 시스템의 전자화와 관련된 주요 연구 동향에 대해서 살펴본다. 미국은 주마다 서로 다른 선거 방식을 도입하여 사용하고 있으며, 2000년 대선에서의 주요 이슈는 투표 시스템에 대한 신뢰성 문제였다.

· 종이 투표 방식

비용이 많이 들지만 투표자의 투표권 확인 및 재검표가 가능한 장점이 있다. 하지만 기표시의 오류 발생률이 높아(무효표 발생) 선거 시스템의 신뢰성을 저하시킨다.

· 기계 방식

투표/개표 기능을 수행하는 기계를 이용하는 것으로, 투표자는 투표 기계에 대해서 전적으로 신뢰해야 한다는 단점이 있다. 선거 비용이 저렴하지만, 재검표가 불가능하여 투표자의 신뢰성을 저하시킨다.

· DRE Voting Machine

2000년 미국 대선에 가장 많이 사용된 방식으로 투표자의 투표 오류율을 감소할 수 있도록 전자적으로 투표할 수 있는 시스템이다. 하지만, 투표 및 개표 결과에 대해서 업체 제작 소프트웨어의 신뢰성에만 의존해야 하며, 재검표가 불가능하고 투표자에 의한 개별/전체 검증이 불가능하다.

HAVA Project는 플로리다 주의 대규모 무효투표 발생을 계기로, 오류를 최소화하고 쉽게 유권자의 의사를 표기할 수 있는 투표 방법이 필요하다는 인식 하에 만들어 지게 되었다. HAVA funding (US$3.86 billion)을 받게 되는 주는 기존의 선거 방식을 모두 전자 시스템으로 변경해야 하며 DRE voting machine을 비롯하여, 전자 선거를 위한 투/개표 시스템 개발 및 연구 사업이 활성화되고 있다.

투개표 시스템의 전자화와 관련된 최근의 연구 동향 및 논의되고 있는 이슈는 대략 다음과 같다.

· 전자선거 소프트웨어의 무결성이 보장되어야 한다.[1,3]
  - 소프트웨어 공학에 근거한 안전한 코딩 기법이 전제되어야 한다.
  - 전자선거 소프트웨어는 소스가 공개되어야 한다. 민주주의 선거에서는 부정이 없어야 하므로 의심이 갈만한 사항은 선거 시스템 및 절차에 포함되어서는 안 된다.
  - 하지만 소프트웨어 무결성에만 의존하는 것은 매우 위험한 방법이기 때문에, 프로그램에 독립적인 안전한 선거 방식 및 절차가 필요하다.

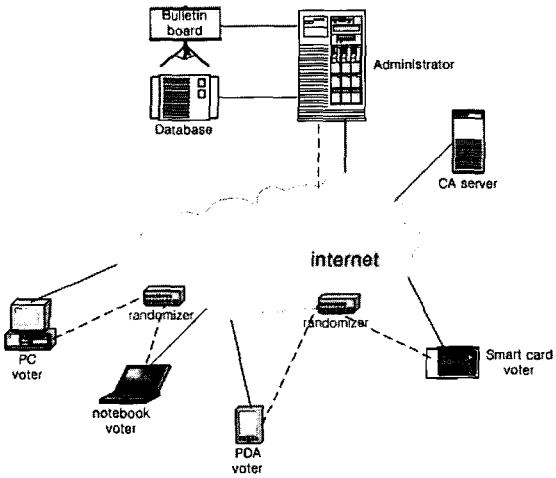
· 투표자 검증과 매표 방지를 동시에 만족하여야 한다.[2]
  - Receipt 생성 및 투표 행위의 확인
  - 투표자에 의한 개표결과 확인
  - Receipt은 제 3자가 투표자의 의사를 확인할 수 없도록 생성되어야 한다.

· 투표 단계에서의 오류에 대한 정정이 가능하도록 취소 및 재투표 기능이 있어야 한다.[2]

Ⅲ. 부인봉쇄 서명을 적용한 인터넷 기반 전자선거

3장에서는 인터넷 기반 전자선거 구성요소 및 전자선거 단계에 대해서 살펴보고 부인봉쇄 서명을 적용한 인터넷 전자선거 기법 절차와 이로 인하여 얻을 수 있는 특성에 대해서 알아본다.

그림 1은 인터넷 기반 전자선거에 필요한 전형적인 구성 요소들을 보여준다. 선거관리 센터는 전자선거와 관련된 제반 관리 업무를 수행하며, CA server는 유권자 등록의 신뢰성을 높이기 위해서 각 유권자와 센



〔그림 1〕 인터넷 기반 전자선거 구성요소

터의 공개키에 대한 인증서를 발급하는 업무를 한다. 유권자들은 인터넷 연결이 가능하고, 투표 프로그램 적재가 가능한 장비들을 이용하여 투표에 참여하며, 그림 1에서 믹서(randomizer)는 실제 투표권 전송 시 추적이 불가능하도록 해 주는 역할을 하게 된다.[9]

기존의 인터넷 기반 대규모 전자선거 기법은 다음과 같이 세 가지 가정에 기반을 둔다.[5-8,12,13]

가정 1. 유권자 등록, 투표권 인증 및 개표 업무를 수행하는 선거관리 센터를 전적으로 신뢰하며, 선거관리 센터가 여러 개인 경우에는 적어도 하나의 센터를 신뢰할 수 있어야 한다.

가정 2. D.Chaum이 제안한 익명 통신 채널(Anonymous Communication Channel)이 존재한다. 투표자와 선거관리 센터 간에 익명적으로 메시지를 전송할 수 있는(IP 추적이 불가능한) 채널이 존재해야 한다.

가정 3. 유권자에 대해서 강압적으로 투표권 매표 또는 투표 행위가 이루어지지 않아야 한다. 선거관리 센터는 투표자의 투표 행위를 감시할 수 없기 때문에 컴퓨터와 인터넷을 이용한 투표행위가 공정하게 이루어졌는지 확인할 수 없기 때문이다.

디지털 다중 서명은 여러 서명자들이 법적 구속력을 갖는 서명을 전자문서에 대해서 수행하는 것으로, 선거관리 센터의 권한을 분산하기 위해서 사용된다. 정당 별로 선거관리 센터를 두어서 투표자와 정당에게 투/개표 결과의 신뢰성을 보장하며 유권자 등록 및 투/개표 단계에 적용될 수 있다.[13]

부인봉쇄 서명(Undeniable Signature)은 서명자의 동의 없이는 서명을 검증할 수 없는 기법으로, 사용자 편의성 및 매표방지를 위해서 사용될 수 있다. 부인봉쇄 서명된 투표권은 제 3자에게 공개되어도 적법한 투표권인지 아닌지 확인할 수 없기 때문에, 투표자에게 선거의 신뢰성 확보를 위하여 제공하는 receipt로 활용 가능하다.[11,12]

제안한 전자선거 기법은 부인봉쇄 서명 및 부인봉쇄 다중 서명 기법을 적용하여 등록 단계에서 투표권 취소 및 재투표가 가능하며 정당 별로 선거관리자들을 두어 투표권에 대한 부인봉쇄 다중서명을 수행함으로써 모든 정당들의 동의 하에서만 투표권에 대한 개봉 및 검증이 가능하도록 함으로써 공정한 전자선거가 될 수 있도록 한다.[13]

인터넷 기반 전자선거는 준비단계, 등록단계, 투표단계 그리고 개표단계로 구성된다. 준비단계에서 선거관리 서버는 각 후보자에 대한 고유 식별 난수 값을 생성한다. 선거관리자들과 유권자들은 고유한 암호학적 파라미터들을 생성하고 공개키 인증 센터를 통해서 공개키를 등록한다. 등록 및 투표 단계에서 각 유권자는 자신의 익명값(pseudonym)과 해당 후보자에 대한 투표권(ballot)을 생성한다. 각 유권자는 투표권 등록을 위해서 선거관리자들과 부인봉쇄 다중서명 기법[13]을 이용해서 서명한다. 투표 및 개표 단계에서 인증된 투표권 검증 및 투표권 개봉을 위해서 다중서명 확인 프로토콜[13]이 수행된다.

3.1 준비 단계

제안한 기법에서 사용되는 파라미터들은 다음과 같다.

- 선거관리자들 : $a_1, a_2, \ldots, a_n$
- 투표권 : $ballot$
- 은닉 투표권 : $ballot'$
- 선거관리자 i 의 비밀키 :
  $X_i \in Z_{p-1},\ 1 \le i \le n$
- 선거관리자 i 의 공개키 :
  $Y_i \equiv g^{X_i} \pmod{p},\ 1 \le i \le n$

단계 1: 선거관리 서버는 표 1과 같은 후보자 리스트를 인터넷상의 선거관리 게시판에 공고한다. 익명 값은 고유한 난수 값으로 각 후보자 별로 선거관리 서버에서 생성한다.

단계 2: 선거관리자들은 공통으로 사용하게 될 암호학적으로 안전한 Galois Field $GF(p)$, 생성자 g 그리

〔표 1〕 후보자 이름과 고유 익명 값

후보자 이름	고유 익명 값
C1	cps1
C2	cps2
…	…
Cn-1	cpsn-1
Cn	cpsn

고 공통 공개키 Y를 생성한다. 공개키 Y는 다음 프로토콜을 통해서 구한다.

단계 2.1: 선거관리 서버는 첫 번째 선거관리자 a_1에게 공통 공개키 Y에 대한 생성을 요청한다.

단계 2.2: 첫 번째 선거관리자 a_1은 두 번째 선거관리자 a_2에게 공개키 Y_1을 전송한다.

단계 2.3: 선거관리자 $a_i(2 \leq i \leq n)$는 이전 단계의 선거 관리자 a_{i-1}로부터 다음과 같은 이전 선거관리자들의 공개키 정보를 수신한다.

$$Y_{i-1} \equiv Y_{i-2}^{X_{i-1}} \pmod{p}$$

단계 2.4: 선거관리자 a_i는 다음과 같이 공통 공개키를 계산한다.

$$Y_i \equiv Y_{i-1}^{X_i} \equiv g^{\prod_{j=1}^{i} X_j} \pmod{p}.$$

단계 2.5: 선거관리자 a_i는 Y_i를 다음 선거관리자 a_{i+1}에게 전송한다. 만약 a_i가 마지막 선거관리자라면, 공통 공개키 Y는 다음과 같이 계산된다. a_n은 공통 공개키 Y를 선거관리 서버와 더불어 모든 선거관리자들에게 전송한다.

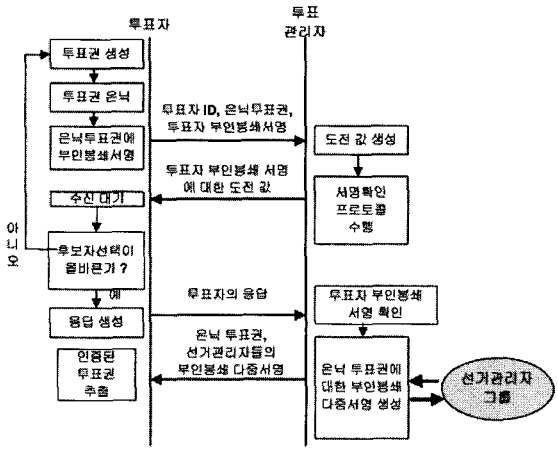
$$Y \equiv Y_{n-1}^{X_n} \equiv g^{\prod_{j=1}^{n} X_j} \pmod{p}$$

단계 3: 각 유권자의 공개키 y와 비밀키 x는 다음과 같이 생성한다.

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

3.2 등록 단계

그림 2는 제안한 투표권 등록 절차를 보여준다. 유권자와 투표권은 선거관리자 그룹에 의해서 등록된다.



〔그림 2〕 제안한 투표권 등록 단계

그림 2에서와 같이 등록단계에서 만약 유권자가 후보를 변경하고자 하는 경우에 등록단계를 재실행할 수 있다.

3.2.1 은닉투표권 생성 및 부인봉쇄 서명

단계 1: 유권자는 익명 값 ps를 생성하고 후보자 i의 익명 값 cps_i를 선택한다. 이 정보를 가지고 투표권을 다음과 같이 생성하고 은닉한다.

$$ballot \equiv (cps_i \cdot ps)^{ps} \pmod{p}$$
$$ballot' \equiv ballot^{bf} \pmod{p},$$
$$(bf \cdot bf^{-1} \equiv 1 \pmod{p-1})$$

단계 2: 유권자는 은닉 투표권에 대한 부인봉쇄 서명을 한다. 본 논문에서는 〔11〕의 부인봉쇄 서명 기법을 다음과 같이 은닉 투표권에 대해서 적용한다. 은닉 투표권 $ballot'$에 대한 서명 (s,r)은 다음과 같다.

$$r \equiv ballot'^{k} \pmod{p}, \quad k \in Z_{p-1}$$
$$k \cdot (ballot' + s) \equiv x \cdot r \pmod{p-1}$$

단계 3: 유권자는 신분 식별 정보, 은닉 투표권 그리고 부인봉쇄 서명을 선거관리 서버로 전송한다.

3.2.2 유권자 등록

단계 1: 선거관리 서버는 서명 확인 프로토콜〔11〕을 수행하여 유권자의 서명을 검증한다. 만약 서명이 유효하지 않다면 선거관리 서버는 투표권 등록을 취소한다. 그렇지 않다면, 선거관리 서버는 유권자 ID를 조사하여 해당 유권자가 이미 등록되어 있는지 검증한

다. 유권자 ID가 이미 등록되어 있다면 선거관리 서버는 투표권 등록을 취소한다. 같은 유권자가 합법적인 투표권을 여러 개 만들 수 없도록 하기 위해서이다. 그렇지 않다면, 단계 2가 수행된다. 또한, 유권자가 후보자를 변경하고자 하면 이 단계에서 서명 확인 프로토콜을 거부함으로써 투표권 등록 절차를 재시도할 수 있다. 부인봉쇄 서명은 서명자의 도움 없이는 서명을 검증할 수 없기 때문이다. 투표권 인증을 위한 선거관리 서버의 서명 확인 도전 값에 대해서 유권자가 응답하지 않으면, 유권자의 서명은 검증될 수 없다.

단계 2: 선거관리 서버는 유권자 식별 정보인 ID를 데이터베이스에 기록한다.

단계 3: 선거관리 서버는 유권자의 은닉 투표권을 등록하기 위해서 모든 선거관리자들에게 은닉 투표권을 전송한다.

3.2.3 은닉투표권에 대한 부인봉쇄 다중서명 생성

단계 1: 선거관리 서버는 첫 번째 선거관리자 a_1에게 부인봉쇄 다중서명 생성을 위해서 필요한 공통 난수 값 R의 생성을 요청한다.

단계 1.1: 선거관리자 a_1은 Z_{p-1}상에서 임의의 난수 k_1을 선택한다. a_1은 난수 k_1과 은닉투표권을 이용하여 다음과 같이 R_1을 생성하고 선거관리자 a_2에게 전송한다.

$$R_1 \equiv ballot'^{\,k_1} \pmod{p}$$

단계 1.2: 선거관리자 $a_i(2 \le i \le n)$는 선거관리자 a_{i-1}로부터 R_{i-1}을 수신한다.

$$R_{i-1} \equiv R_{i-2}^{k_{i-1}} \pmod{p}$$

단계 1.3: a_i는 다음과 같이 R_i를 계산한다.

$$R_i \equiv R_{i-1}^{k_i} \equiv ballot'^{\,\prod_{j=1}^{i} k_j} \pmod{p}$$

단계 1.4: a_i는 R_i를 선거관리자 a_{i+1}에게 전송한다. 만약 a_i가 마지막 선거관리자이면 공통 난수 값 R을 다음과 같이 생성하고 선거관리 서버를 비롯한 모든 선거관리자들에게 전송한다.

$$R \equiv R_{n-1}^{k_n} \equiv ballot'^{\,\prod_{j=1}^{n} k_j} \pmod{p}$$

단계 2: 선거관리자 $a_i(1 \le i \le n)$는 부인봉쇄 서명 s_i를 생성하고 선거관리 서버로 전송한다. k_i와 $p-1$은 서로소이기 때문에 다음 식을 만족하는 해 s_i가 존재한다.

$$k_i \cdot s_i \equiv x_i \cdot R - k_i \cdot ballot' \pmod{p-1}$$

단계 3: 선거관리 서버는 부인봉쇄 다중서명 S를 다음과 같이 생성한다.

$$S \equiv \prod_{j=1}^{n} (ballot' + s_j) \pmod{p}$$

단계 4: 선거관리 서버는 부인봉쇄 다중서명 (S,R)을 유권자에게 전송한다.

3.2.4 선거관리자들이 서명한 인증 투표권 추출

단계 1: 투표자는 부인봉쇄 다중서명 (S,R)로부터 인증 투표권 $S_A(ballot)$을 다음과 같이 추출한다.

$$\begin{aligned} R^{S \cdot bf^{-1} \cdot R^{n-1}} &\equiv ballot'^{\,bf^{-1} \cdot R^{n-1} \cdot \prod_{j=1}^{n} k_j \cdot (ballot' + s_j)} \\ &\equiv (cps_i \cdot ps)^{ps \cdot \prod_{j=1}^{n} X_j} \\ &\equiv ballot^{\prod_{j=1}^{n} X_j} \pmod{p} \\ &\equiv S_A(ballot) \end{aligned}$$

3.3 투표 단계

단계 1: 투표자는 인증투표권 $S_A(ballot)$에 대한 도전(challenge) ch를 생성한다. (a,b)는 Z_{p-1}상에서 선택된 임의의 난수이고 Y는 선거관리자들이 생성한 공통 공개키이다.

$$ch \equiv S_A(ballot)^a \cdot Y^b \pmod{p}$$

단계 2: 투표자는 $(S_A(ballot),ch)$를 추적 불가능한 통신망[9]을 이용하여 선거관리 서버로 전송한다.

단계 3: 선거관리 서버는 $(S_A(ballot),ch)$를 첫 번째 선거관리자 a_1에게 전송한다. 선거관리자들은 다음 단계들을 통해서 순차적으로 투표자의 도전 값에 대한 응답을 생성한다.

단계 3.1: 선거관리자 i는 선거관리자 i-1로부터 인증

투표권과 응답을 수신한다.

$$S_A(ballot)^{\prod_{j=1}^{i-1} X_j^{-1}} \equiv ballot^{\prod_{j=i}^{n} X_j} \pmod{p}$$

$$rsp_{i-1} \equiv ch^{\prod_{j=1}^{i-1} X_j^{-1}}$$

$$\equiv ballot^{a \cdot \prod_{j=i}^{n} X_j} \cdot g^{b \cdot \prod_{j=i}^{n} X_j} \pmod{p}$$

단계 3.2: 선거관리자 i는 자신의 비밀키 X_i를 이용하여 인증 투표권과 응답에 대해서 다음과 같은 연산을 한다.

$$(S_A(ballot)^{\prod_{j=1}^{i-1} X_j^{i-1}})^{X_i^{-1}}$$

$$\equiv ballot^{\prod_{j=i+1}^{n} X_j} \pmod{p} \; rsp_i \equiv (ch^{\prod_{j=1}^{i-1} X_j^{-1}})^{X_i^{-1}}$$

$$\equiv ballot^{a \cdot \prod_{j=i+1}^{n} X_j} \cdot g^{b \cdot \prod_{j=i+1}^{n} X_j} \pmod{p}$$

단계 3.3: 선거관리자 i는 단계 3.2의 결과물들을 다음 선거관리자 i+1에게 전송한다. 마지막 선거관리자는 투표자의 투표권을 추출하고 모든 선거관리자들의 응답을 다음과 같이 생성한다.

$$S_A(ballot)^{\prod_{j=1}^{n} X_j^{-1}}$$

$$\equiv ballot^{\prod_{j=1}^{n} X_j \cdot X_j^{-1}} \equiv ballot \pmod{p}$$

$$rsp_n \equiv ch^{\prod_{j=1}^{n} X_j^{-1}} \equiv ballot^a \cdot g^b \pmod{p}$$

단계 4: 선거관리 서버는 다음과 같은 결과물을 게시판에 공고한다.

$$(S_A(ballot), ballot, rsp_n)$$

3.4 개표 단계

단계 1: 투표자는 선거관리자들의 응답 rsp_n이 정확한지 검증한다. 만약 응답이 잘못되었다면 부인 프로토콜(disavowal protocol)[13]을 실행하여 부인봉쇄 다중서명이 잘못된 것인지 아니면 몇몇 선거관리자들이 부정하는 것인지 식별한다. 응답이 정확하다면 투표권 개봉을 위하여 투표자는 자신의 익명 값 ps를 선거관리 서버에 전송한다.

단계 2: 선거관리 서버는 다음과 같이 ps를 이용하여 투표권을 개봉하고 후보자 별로 계수한다.

$$cps_i \equiv \frac{ballot^{ps^{-1}}}{ps} \pmod{p}$$

$$\equiv \frac{(cps_i \cdot ps)}{ps} \equiv cps_i \pmod{p}$$

만약 cps_i가 표 1의 후보자 리스트에 있으면, 선거관리 서버는 해당 후보자에 대한 카운트를 하나 증가시키고 단계 3으로 이동한다. 그렇지 않다면, 선거관리 서버는 해당 투표권을 폐기한다.

단계 3: 선거관리 서버는 다음 결과물들을 게시판에 공고한다.

$$(ps, cps_i, S_A(ballot), ballot)$$

Ⅳ. 결 론

본 논문에서는 대규모 전자선거에 적합한 요구사항들을 분석하고 현재 진행 중인 부분 전자선거 방식에 대한 연구 동향을 살펴보았다. 인터넷 기반 전자선거 실현을 위한 가장 큰 걸림돌은 매표 방지와 강압적인 투표 방지를 어떻게 실현할 수 있느냐 하는 것이다. 또한 개별 검증, 전체 검증과 더불어 등록 및 투표 단계에서 투표권 취소 및 재투표가 가능한 투표자 중심의 요구사항도 만족할 수 있어야 한다.

국회의원 선거 또는 대통령 선거와 같이 정당별로 후보자를 공고하고 투표하는 대규모 전자선거 방식에 적합하도록 부인봉쇄 서명을 적용한 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 정당 별로 선거관리자들을 두어 투표권에 대한 부인봉쇄 다중서명을 수행함으로써 모든 정당들의 동의 하에서만 투표권에 대한 개봉 및 검증이 가능하도록 함으로써 공정한 전자선거가 될 수 있도록 한다.

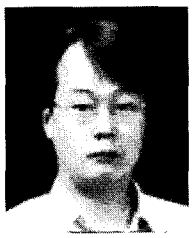
참 고 문 헌

[1] D.Evans, N.Paul, "Election Security: Perception and Reality," IEEE S&P Magazine Jan/Feb, pp.24-31, 2004.

[2] D.Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections,", IEEE S&P

Magazine Jan/Feb, pp.38-47, 2004.
[3] J.Bannet, D.W.Price, A.Rudis, J.Singer, S.Wallach, "Hack-a-Vote: Security Issues with Electronic Voting Systems," IEEE S&P Magazine Jan/Feb, pp.32-37, 2004.
[4] B.C.Lee, K.J.Kim, "Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer," ICISC 2002, LNCS 2587, Springer-Verlag, pp. 389-406, 2002.
[5] Ahmad Baraani-Dastjerdi, Josef Pieprzyk and Reihaneh Safavi-Naini, "A Secure Voting Protocol Using Threshold Schemes," Proceedings of COMPSAC'95, pp.143-148, 1995.
[6] Patrick Horster, Markus Michels and Holger Petersen, "Blind Multisignature Schemes and Their Relevance for Electronic Voting," Proceedings of COMPSAC'95, pp.149-155, 1995.
[7] 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.
[8] 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.
[9] D.Chaum, "Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms ," Communications of the ACM, Vol. 24, No. 2, pp.84-88, 1981.
[10] David Chaum, "Undeniable Signatures," Proceedings of CRYPTO'89, pp.212-216, 1989.
[11] S.H.Yun, H.W.Lee, "The Efficient Multipurpose Convertible Undeniable Signature Scheme," LNAI 3683, Springer-Verlag, pp.325-331, 2005.
[12] 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.
[13] S.H.Yun, H.W.Lee, "The Large Scale Electronic Voting Scheme Based on Undeniable Multi-signature Scheme," LNCS 3481, Springer-Verlag, pp.391-400, 2005.

〈著 者 紹 介〉



윤 성 현 (YUN SUNGHYUN)
정회원

1992년 : 고려대학교 컴퓨터학과 졸업
1994년 : 고려대학교 컴퓨터학과 석사
1997년 : 고려대학교 컴퓨터학과 박사
1998년 ~ 2002년 : LG 전자/정보통신 중앙연구소 선임연구원
2002년 ~ 현재 : 천안대학교 정보통신학부 조교수
〈관심 분야〉 정보보호, 전자상거래 보안, DRM, ATM 스위치