通信情報保護學會論文誌
第 10 券 第 4 號, 2000. 12

실용적이고 안전한 전자투표 프로토콜에 관한 연구*

김 순 석**, 이 재 신***, 김 성 권**

A Proposal for the Practical and Secure Electronic Voting Protocol

Soon-Seok Kim**, Jae-Shin Lee***, Sung-Kwon Kim**

요 약

각종 컴퓨터의 보급 및 네트워크 기술의 발달로 현재 컴퓨터 응용분야에 많은 발전이 이루어지고 있다. 그 중에서도 암호학을 이용한 전자투표는 전자화 되어 가는 민주 사회에서 필수적인 요소로 부각되고 있다. 그러나, 지금까지의 전자 투표는 그 중요성에도 불구하고 많은 문제점이 지적되고 있다. 본 논문에서는 신뢰할 수 있는 선거관리센터를 가정함으로써 전자 투표의 요구사항인 안전성, 공정성, 투표자의 비밀성, 선거 집계의 정확성 등을 만족하는 대규모적이고 실용적인 전자투표 프로토콜을 제안한다. 블라인딩기법(Blinding Technique)을 이용하여 투표자의 투표내용을 노출시키지 않고 투표권을 획득하며, 부정할 수 없는 도전 및 응답프로토콜(Challenge and Responsible Protocol)을 사용하여 투표자와 집계자 사이의 부정을 확인할 수 있으며, 투표자나 집계자의 부정으로 인한 전자 투표의 무결성과 투표자의 프라이버시를 보호하기 위해 투표자의 익명을 기반으로 한 안전한 전자투표를 방식을 제안한다.

ABSTRACT

We have seen a lot of developments on computer application areas with the wide spread use of computers and the rapid growth of communication network. It is necessary to use a cryptographic technique for electronic voting, but, at present, despite of its importance electronic voting protocols so far have many shortcomings. In this paper, with the assumption of a trustable voting centers we propose a large-scale and practical electronic voting protocol satisfying protocol requirements, such as secureness, fairness, privacy of voter and correctness. Voters are able to get a vote without revealing their voted information by using the blinding technique. We can find the injustice between a voter and the tallier by using undeniable challenge and responsible protocol. Also, we proposes a secure protocol that compensates a integrity of electronic voting and protects a privacy of voter from outer attacks as using a anonymity of voter.

keyword : *Electronic Voting Protocol, Cryptographic Protocol*

Ⅰ. 서 론

시대가 변하고 정보 통신 기술이 발달함에 따라 인간의 생활도 많은 변화와 발전을 겪어 오고 있다. 미디어 보급의 확대와 쌍방향 통신의 발달로 인하여 현대 사회는 산업 사회의 대중성, 대량성, 일방향성을 특징으로 하는 통신에서 정보화 사회의 새로운 매체들의 상호작용성, 탈대량화, 비동시성을 특징으로 전환을 하고 있다.

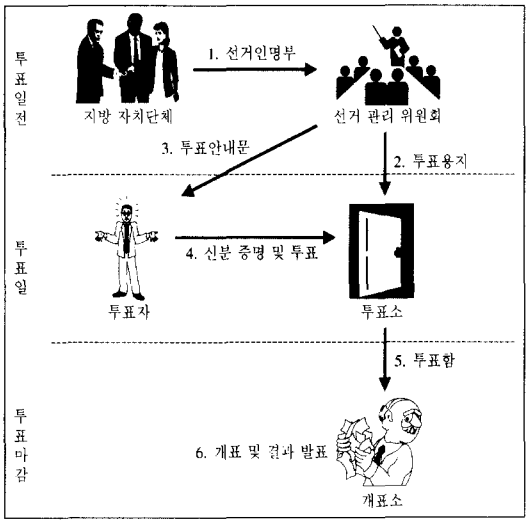
인간은 사회라는 테두리 내에서 생활을 영위하며,

* 본 연구는 한국과학재단 목적기초연구(2000-1-51200-001-3)지원으로 수행되었음.
** 중앙대학교 컴퓨터공학과 알고리즘 및 정보보호연구실(sskim@alg.cse.cau.ac.kr, skkim@cau.ac.kr)
*** (주)이니텍(jslee@initech.com)

투표라는 행위를 통하여 자신의 의사를 표출하는 데 사용하고 있다. 투표는 작은 모임에서의 의사 결정에서부터 넓게는 대통령선거에까지 생활 전반에 걸쳐 여러 분야에서 없어서는 안될 필요수단으로 존재하고 있다.

예로 현실에서 대통령을 뽑기 위한 투표를 한다고 가정하자. 실세계에서는 다음과 같은 방법으로 투표가 이루어진다. 투표는 단기무기명 투표, 직접 또는 우편투표, 자유투표제로, 먼저 선거인명부 작성기준일 현재의 주민등록표에 의하여 구·시·읍·면의 장이 직권으로 작성하여, 구·시·군위원회가 세대별로 선거인명부 등재번호·투표소의 위치 등을 기재하여 선거인명부 확정일의 다음날까지 책자형 소형인쇄물과 함께 투표안내문을 각 가정집에 발송한다. 투표일에 투표자는 해당 투표소에 자신의 신분증을 지참 지정 투표소에 입소하여 선거인명부 및 신분증명서에 의해 본인여부를 확인한 후 투표용지를 수령하고 일련번호지를 분리·투입하여 외부와는 단절된 기표소에서 기표한 후 준비된 투표함에 투입하고 퇴소를 하면 모든 투표 과정을 마치게 된다. 모든 투표가 끝나고 참관인 참관하에 위원전원이 투표함의 투입구와 자물쇠를 봉쇄·봉인하고, 투표구위원장이 투표참관인(10인이내)을 동반하여 투표함 및 관계서류를 개표소에 송부한다.

도착된 투표함들은 먼저 우편투표함 개함 후 일반투표함의 전부 또는 2/3이상 도착시 개표를 개시하며, 개표 진행은 투표구별로 투표함 이상유무 확인 후 투표함을 개함하여 투표용지의 유·무효를 구분,



〔그림 1〕 실세계 투표 흐름도

후보자별 득표를 집계·공표함으로써 모든 투표과정이 마치게 된다.

그러나 현실 투표상의 문제점을 열거해보면, 일단 투표자들은 투표를 위해 지정 투표소까지 가야하고, 개인적인 용무 등의 필요에 의해 다른 투표소에서 투표를 하고자 할 경우 선거인 명부가 단지 하나만 존재하므로 번거로운 과정을 거쳐야 하며, 그렇지 않을 경우 이중 투표의 문제점이 존재한다. 또한 선거 용지 제작, 운반, 보관에 많은 비용이 소요되며, 투표를 위해 다수의 선거 관리 인원이 필요하고, 많은 투표 장소 및 시간이 소요된다.

인터넷의 폭넓은 보급과 초고속 통신망 등의 통신 매체를 통해 이러한 실세계의 투표 방식을 컴퓨터를 이용한 전자적인 투표방식으로 전환한다면 상기 열거된 문제점들을 상당히 줄일 수 있을 것이다. 즉, 투표소에서만 행해지던 투표과정이 네트워크를 통하여 전자 투표소의 단말기뿐만 아니라 자신의 회사내 사무실 또는 집안에서, 선박이나 항공기내에서 자신의 노트북을 통하여 또는 공공장소의 컴퓨터를 이용하여 동일한 투표의 목적을 이룰 수 있다면 투표자의 편리성을 제공한다. 뿐만 아니라, 물적, 인적의 경비 감소 및 투표용지의 전달에 따른 주위의 산재된 운반상의 문제점들을 없애며, 투표 및 개표가 전자적으로 이루어져 정확하고 빠른 시간 내에 결과를 알 수 있어 투표의 시비를 줄일 수 있는 등의 장점을 얻을 수 있어 투표 방식에 변화를 갖게 될 것이다.

이를 위해서는 해커나 부정한 침입자로부터 자신의 개인 정보를 보호하며, 올바른 정보의 전송 및 확인이 필요하다. 따라서 암호 및 인증을 기반으로 정보보호 기술이 필수 요소로 사용되고 있다. 암호학의 발전과 정보보호 및 보안 기술의 발전은 전자투표, 전자화폐, 전자지불, 전자지갑, 전자상거래 등의 요소기술[1]로서 일상 생활의 편리성과 경제성에 막대한 영향을 주고 있다.

본 논문에서는 투표 및 개표 과정을 개선한 전자투표 프로토콜을 제안한다. 투표 단계에서는 익명을 통하여 불완전한 네트워크 상에서 자신의 ID노출에 대한 프라이버시(Privacy) 침해 위험 부담을 감소시켰으며, 블라인딩기법(Blinding Technique)을 이용하여 투표자 이외에는 누구도 투표 내용을 알 수 없이 투표권에 대한 인증(Authentication)을 받을 수 있도록 하였고, 투표자, 선거관리센터와 집계자 사이에 블라인딩기법을 이용한 인증서를 통해 시스템의 오류나 부정에 의한 투표 프로토콜의 불완

전한 종료를 방지하였다. 그리고 부정할 수 없는 도전/응답(Undeniable Challenge and Response) 기법을 이용하여 투표자와 집계자간에 익명으로써 부정을 검증 할 수 있으며, 또한 중간 투표의 결과를 알 수 없도록 하였고, 투표 마감 후 선거 관리 센터가 투표 용지를 개표할 수 있는 인자(Parameter)를 집계자에게 전달함으로써 투표자는 한 번의 세션에 모든 투표 과정이 종료될 수 있도록 하였다.

Ⅱ장에서는 전자투표 프로토콜에서의 요구사항 무엇인지 알아보고, Ⅲ장에서는 전자 투표와 관련, 기존에 제안된 투표 프로토콜 및 각각의 요구사항과 특징들을 살펴본다. Ⅳ장에서는 도전/응답 기법을 사용하여 제안한 투표 프로토콜을 기술하고 안전성을 분석하며, Ⅴ장에서는 영수증을 사용하여 제안한 프로토콜 기술 및 안전성을 분석한다. 그리고 Ⅵ장에서는 결론 및 향후 발전 방향을 제시한다.

Ⅱ. 요구사항

실세계에서의 투표 방식 중에서 주로 사용되는 투표는 자기 자신이 누구에게 투표를 했는지를 아무도 알 수 없는 무기명, 비밀 투표이다. 일반 투표가 갖는 성질을 만족하면서 전자적인 투표형태로 전환되었을 때 갖추어야 할 특징들을 알아볼 필요가 있다. 그래서 전자 투표가 갖추어야하는 요구사항들을 열거해 보면 다음과 같다.[2,3,4]

- 정확성(Accuracy) : 시스템이 투표용지를 수정, 삭제할 수 없고, 유효한 투표용지가 투표 기록에 올바로 카운트되며, 유효하지 않는 투표 용지가 투표 기록에 카운트되지 않아야 한다, 즉 집계결과가 정확해야 한다.
- 비밀성(Privacy) : 시스템이 투표권을 행사하는 투표자에게 연결되어있지 않고, 어떠한 방법으로도 투표자가 누구에게 투표를 했는지를 증명할 수 없어야 한다. 또한 투표자와 투표자 자신이 투표한 내용은 해당 투표자만이 알 수 있어야 한다.
- 위조 불가능성(Unforgeability) : 선거관리센터로부터 인증을 받은 투표권은 제 3자에 의해 위조가 불가능해야 한다.
- 단일성(Singularity) : 합법적인 투표자는 단지 한 번의 투표권만 행사 할 수 있어야 한다.
- 합법성(Eligibility) : 합법적인 절차를 통하여 투표권을 얻은 사람만이 투표에 참여할 수 있다.
- 공정성(Fairness) : 투표 진행 과정에서 다른 사람의 투표권 행사에 의해 자신의 투표권 행사가 전체 투표에 영향을 줄 수 없어야 한다. 즉 전체 투표에 영향을 줄 수 있는 중간 투표 결과를 알 수 없어야 한다.
- 확인성(Verfiability) : 투표자가 올바르게 자신의 투표용지가 카운트되었는지를 확인 할 수 있어야 한다.
- 투표권 매매 방지(Untradability) : 투표권을 타인에게 매매할 수 없으며, 매매에 따른 결과는 투표권을 소유하는 인증된 투표자만이 알 수 있어야 한다.
- 완전성(Completeness) : 투표자들이나 집계자의 부정에 의해 투표 시스템의 모든 투표 진행이 중단되거나 불완전한 결과를 초래하지 않아야 한다.

이상의 요구 사항은 전자 투표 방식에서 기본적으로 만족해야 하는 내용이며, 반드시 만족해야 하는 것은 아니지만, 보다 효율적이고 투표율을 높이기 위해서는 다음의 요구사항을 충족해야 한다.

- 세션성(Sessionality) : 투표를 모든 위한 행위 및 연산은 투표자가 한 세션에 완료할 수 있어야 한다.
- 편리성(Conveniency) : 투표 시스템이 최소한의 장비와 기술로 투표를 빠른 시간에 마칠 수 있어야 한다.
- 유동성(Flexibility) : 투표자를 위해 투표 용지 형식이 다양하게 사용될 수 있어야 한다.

위의 모든 요구 사항들을 만족하기 위한 특징으로 안전한 전자 투표를 위해서는 신뢰할 수 있는 선거관리 센터를 두어야 하며, ID 기반이 아닌 익명으로 투표가 진행되어야 한다.

Ⅲ. 기존 투표 프로토콜 연구

기존 제안된 프로토콜은 많이 있지만 본 논문에서는 다음의 세 가지 프로토콜을 살펴보고 각각의 문제점을 알아본다.

Fujioka, Okamoto, Ohta 프로토콜[2] 기법은 비트 도전 기법(Bit Commitment Scheme)을 사용하였으며 블라인딩기법을 사용하여 인증 및 투표자의 비밀을 보호하였다. 하지만 투표자가 중간에

투표권을 포기할 수 없고, 투표용지 전송 및 키 전송을 위해 두 번의 세션 작업을 필요로 한다. 그리고 투표자 또는 제 삼자에 의해 투표 용지가 수정되거나 삭제된다면 다시 투표해야하기 때문에 전체 시스템에 큰 영향을 준다. 또한 네트워크상에서 프로토콜을 완료하기 위해서는 투표자 당 4회의 전송 패스를 필요로 한다.

Baraani 프로토콜[3]은 Threshold기법을 적용하여 참가자들간의 부정을 최소화하고 후보자들의 다수가 정직하다라는 가정에서 투표 프로토콜이 진행된다. 이 프로토콜은 선거 전에 센터가 투표자에게 익명을 제공해야 하는 과정이 필요하고, 등록된 투표자가 투표하지 않을 경우 선거 관리자들에 의한 부정이 가능하며, 투표 단계에서 통신 복잡도가 개인 당 후보자수 만큼 배로 증가한다. 또한, 투표 후 투표자는 투표용지를 복호화하기 위해 키를 재 전송해야 한다.

SENSUS 프로토콜[4]은 Fujioka, Okamoto, Ohta 프로토콜에 기반을 둔 프로토콜이다. 이 프로토콜은 프라이버시를 노출시키지 않기 위해 메시지 다이제스트(Message Digest)기법 및 블라인딩기법을 이용하고, 전자서명(Digital Signature)기법을 이용하여 투표자 자신임을 증명하였다. 투표자는 집계자로부터 영수증을 받음으로서 집계자의 부정을 방지하게 하였다. 투표용지 전송 및 키 전송을 위해 두 번의 세션 작업을 필요로 하며 투표 과정 중 부정이 있을 경우 전체 투표 시스템이 불완전할 가능성이 있고 프로토콜을 완료하기 위해서는 5회의 전송 패스를 필요로 한다.

Ⅳ. 제안한 프로토콜(Ⅰ)

제안한 프로토콜은 신뢰하는 선거관리센터를 가정한다. 또한 블라인딩기법을 이용하여 투표자의 투표용지 내용을 알 수 없도록 하여 프라이버시를 보호하였으며, Chaum의 부정할 수 없는 도전 및 응답 기법(Undeniable Challenge and Response Technique)[5]을 이용하여 투표자와 집계자 사이의 부정을 증명할 수 있도록 하였다. 이전의 투표 프로토콜들은 한 번의 세션에 투표를 완료하기 위해서는 중간투표의 결과를 알 수 있었으며, 중간투표의 결과를 알 수 없도록 하기 위해서는 두 번의 세션(투표용지 전송, 키 전송)이 필요하였으므로 사용자의 편리성 측면에서 한 세션에 모든 투표를 마칠 수 있도록 하였다. 그리고 이전 투표 프로토콜은 투표자, 집계자 또는 제 3자에 의해 부정이 있을 경우 전체 투표 시스템에 커다란 영향을 줄 수 있다. 이러한 단점을 보완하여 투표자, 집계자 사이의 부정이 있더라도 투표 과정에서 부정을 증명할 수 있으며, 전체 시스템에 줄 수 있는 영향을 최소화하도록 하였다. 전체 투표 과정은 준비, 등록, 투표, 개표단계로 구성되어진다. 그리고 선거관리센터 및 집계자는 게시판을 사용하는데, 게시판은 누구든지 사용 가능하지만, 선거관리센터 게시판은 선거관리센터만, 집계자의 게시판은 집계자만 입력 및 수정, 삭제가 가능하다.

4.1 프로토콜 요소

- ps1, ps2 : 투표자가 익명에 사용될 랜덤수
- a, b : 투표자가 생성한 도전/응답 기법의 랜덤수
- bk : 블라인딩기법을 위한 랜덤수
- $bk^*ubk=1 \pmod{p-1}$
- pe, pd : 투표자의 키 쌍
- V : 기표된 투표용지
- $m=V^*ps2$
- ce, cd : 선거관리센터의 키 쌍
- $B=m^{bk} \pmod{p}$: 블라인드 된 투표용지
- Reg_List : 등록된 투표자의 리스트(아이디, 공개키 포함)
- te, td : 집계자의 키 쌍
- || : 연접연산
- T : 투표 결과 리스트

4.2 프로토콜

4.2.1 준비단계(선거 전)

〈선거관리센터〉

- $y=g^x \pmod{p}$를 생성
  - y, g, p를 게시
  - 1/x를 집계자의 공개키인 te로 암호화하여 전송

4.2.2 등록단계

〈투표자〉

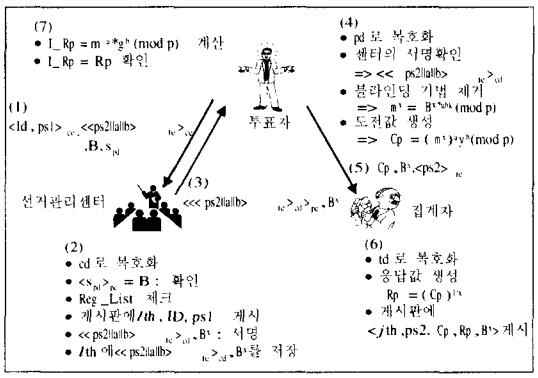
- $\langle ps2||a||b\rangle_{te}$: 투표자의 익명 아이디와 도전 및 응답 기법의 랜덤 수를 집계자의 공개키로 암호화

- $m=V^{*}ps2$: 투표자의 기표된 투표용지와 투표자의 익명 아이디와 곱셈연산
- $B=m^{bk} \pmod p$: 블라인딩기법 연산 결과
- $s=B_{pd} \pmod p$: 투표자의 서명 결과
- $\langle ID||ps1||\langle ps2||a||b\rangle_{te}||B||s\rangle_{ce}$를 선거관리센터에 전송

〈선거관리센터〉
- cd로 암호화된 $\langle ID||ps1||\langle ps2||a||b\rangle_{te}||B||s\rangle_{ce}$를 복호화
- $B=s_{pe} \pmod p=(B_{pd})_{pe} \pmod p$: 투표자의 서명 확인
- 투표자가 이전에 투표했는지 Rev_List 체크
- 게시판 1 번째에 ID, ps1 공표
- $\langle\langle ps2||a||b\rangle_{te}\rangle_{cd}$, B^{x} : $\langle ps2||a||b\rangle_{te}$에 선거관리센터의 서명 및 B 투표용지에 선거관리센터가 인증하는 서명
- 동일한 1 번째에 $\langle\langle ps2||a||b\rangle_{te}\rangle_{cd}$, B^{x}를 공표없이 저장.
- $\langle\langle\langle ps2||a||b\rangle_{te}\rangle_{cd}||B^{x}\rangle_{pe}$를 투표자에게 전송

4.2.3 투표단계
〈투표자〉
- $\langle\langle\langle ps2||a||b\rangle_{te}\rangle_{cd}||B^{x}\rangle_{pe}$를 자신의 비밀키 pd로 복호화 및 확인
- $m^{x}=B^{x*ubk} \pmod p$: 블라인딩기법 제거
- $Cp=(m^{x})^{a}y^{b} \pmod p$: 도전값 생성
- $\langle Cp||B^{x}||ps2\rangle_{te}$를 집계자에게 전송

〈집계자〉
- td로 $\langle Cp||B^{x}||ps2\rangle_{te}$를 복호화



〔그림 2〕 제안한 프로토콜(Ⅰ) : 등록 및 투표단계

- $Rp=(Cp)^{1/x} \pmod p$: 응답값 생성
- 집계자는 게시판의 j번째에 ps2, Cp, Rp, Bx을 게시

〈투표자〉
- $I\_Rp=m^{a*}g^{b} \pmod p$: 자신의 응답값 생성
- I_Rp=Rp 이면 자신의 올바른 투표용지임을 증명

4.2.4 I_Rp와 Rp가 같지 않을 경우(부정이 있는 경우)
〈투표자〉
- a, b를 대신하는 c, d를 생성, 등록단계의 과정과 동일하게 수행하여 $(B')^{x}$를 획득한 후 도전값 Cp′를 계산
- 집계자에게 $\langle Cp'\rangle_{te}$를 전송

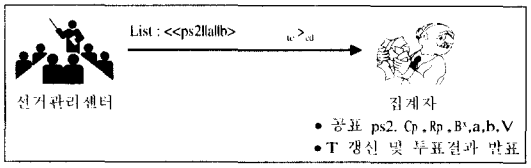
〈집계자〉
- td로 $\langle Cp'\rangle_{te}$를 복호화
- $Rp'=(Cp')^{1/x} \pmod p$: 두 번째 응답값 생성
- Rp′와 Cp′를 게시판에 게시

〈투표자〉
- Rp와 Rp′를 가지고 $(Rp*g^{-b})c=(Rp'*g^{-d})a$를 계산 : 만일 두 값이 같다면 투표자의 기표가 잘못된 경우이고, 같지 않다면 집계자가 올바른 투표 용지에 대해 부정을 저지른 것이다.

4.2.5 개표단계(투표 완료 후)
모든 투표자가 투표를 완료한 후 수행한다.

〈선거관리센터〉
- 리스트 $\langle\langle\langle ps2||a||b\rangle_{te}\rangle_{cd}\rangle_{te}$를 집계자에게 전송

〈집계자〉
- $\langle\langle\langle ps2||a||b\rangle_{te}\rangle_{cd}\rangle_{te}$를 자신의 복호키와 선거관리센터의 ce 서명 검증키로 복호화
- 게시판에 게시된 익명의 ps2와 비교하여 투표용지를 개봉



〔그림 3〕 제안한 프로토콜(Ⅰ) : 올바른 투표가 완료된 이후의 개표단계

$V=(Rp^{*}g^{1/b})^{1/a*}(1/ps2) \pmod p$
$=(m^{a*}g^{b*}g^{1/b})^{1/a*}(1/ps2) \pmod p$
$=m^{*}(1/ps2) \pmod p$
$=(V^{*}ps2)^{*}1/ps2 \pmod p = V$

- T 갱신 및 결과 발표

4.3 제안한 프로토콜(I) 분석

제시된 투표 프로토콜의 요구사항에 대해 제안한 본 논문의 프로토콜(I)의 안전성을 분석한다.

4.3.1 단일성(Singularity)

합법적인 투표자는 선거관리센터로부터 등록단계에서 Reg_List에 의해 체크가 가능하므로 동일한 투표자가 두 번 이상 투표할 수 없다. 또한 다른 투표자의 투표권을 행사하려고 할 경우 다른 투표자의 전자서명키를 알 수 없으므로 투표가 불가능하다

4.3.2 비밀성(Privacy)

선거에 참여하는 어느 누구도 투표자가 누구에게 투표했는지를 알 수 없어야 한다. 투표 내용을 알기 위해서는 블라인딩 된 투표 용지와 이 용지에 선거관리센터가 서명한 투표 용지와의 관계로부터 다음과 같은 계산을 하여야 한다.

$B'=B^{x} \pmod p$
$x=\log_{B^{B'}} \pmod p$

하지만 GF(p) 상에서의 x를 찾는 이산대수 문제는 계산이 불가능하므로 투표자 외에 누구도 투표 내용을 알 수 없으며, $B=m^{bk} \pmod p$ 또한 이산대수문제로 계산이 불가능하다

4.3.3 합법성 (Eligibility)

합법적인 절차를 통하여 투표권을 얻은 사람만이 투표에 참여할 수 있다. 이를 위해서는 투표 전에 합법적인 투표자를 선별하여 각 선거관리센터와 집계자에게 리스트를 전송한다. 만약 합법적이지 못한 투표자가 투표를 하기 위해서는 합법적인 투표자의 전자 서명을 생성할 수 있어야 한다. 그러나, 전자 서명은 합법적인 투표자만이 생성하여, 투표자 인증에 사용되고 등록된 공개키로만 검증할 수 있기 때문에 비합법적인 투표자는 투표에 참가 할 수 없다.

4.3.4 정확성 (Accuracy)

집계결과가 정확해야 한다. 투표 완료 후 선거관리센터는 집계자에게 $\langle\langle ps2,\ a,\ b\rangle_{te}\rangle_{cd}$리스트를 전송함으로써 집계자가 투표 용지를 올바르게 카운트하는 지를 알 수 있다.

4.3.5 위조 불가능성(Unforgeability)

선거관리센터로부터 인증을 받은 투표권은 제3자에 의해 위조가 불가능하다.

$B^{x}=(m^{bk})^{x} \pmod p$

선거관리센터의 인증 값 cd를 계산 할 수 있어야 투표자가 기표한 투표 용지를 위조 할 수 있다. 하지만, x 값은 계산한다는 것은 GF(p) 상에서의 이산대수 문제이므로 투표 용지의 위조는 불가능하다. 만일 제 3자가 x 값을 안다는 것은 집계자가 부정을 했다는 것을 의미하며 또한 결탁한다 할지라도 투표 완료 후 선거관리센터는 집계자에게 $\langle\langle ps2||a||b\rangle_{te}\rangle_{cd}$ 리스트를 전송함으로써 대조에 의해 집계자의 부정을 알 수 있다.

4.3.6 공정성(Fairness)

투표진행과정에서 전체 투표에 영향을 줄 수 있는 중간투표 결과를 알 수 없어야 한다.

$Cp=(m^{x})^{a}y^{b} \pmod p$

중간투표 결과를 알기 위해서는 집계자는 a, b값을 알아야 한다. a, b를 구하는 문제는 이산대수 문제로 계산이 불가능하다. 또한 선거관리센터가 a, b를 알기 위해서는 $\langle ps2||a||b\rangle_{te}$ 에서 집계자의 비밀키를 알아야 한다. 그러므로 누구도 중간투표의 결과를 알 수 없다.

4.3.7 완전성(Completeness)

투표시스템은 투표자 또는 집계자의 부정을 통해 투표 진행이 중단되지 않아야 한다. 위의 3, 4단계 즉, 투표자가 투표를 한 후 자신의 투표 결과를 집계자의 게시판을 통해 확인하는 과정에서 만일, 투표자가 기표한 내용이 잘못된 경우라면 1인 1투표 원칙에 따라 현실세계와 마찬가지로 재투표가 불가능하다. 그러나, 투표자가 아닌 집계자의 실수나 혹은 부정을 통해 잘못된 결과가 발생했다면 위의 4단계 이후에 아래와 같은 해당 투표자의 재투표 과정

이 진행되어야 하며 또한, 이를 통해 본 프로토콜의 완전성을 증명할 수 있다.

〈집계자〉
- 투표자에게 집계자의 부정으로 인한 증거물, $\langle\langle ps2||Cp'||Rp'||B^x\rangle_{td}\rangle_{pe}$를 전송한다.
- 선거관리센터에게 $\langle\langle B^x\rangle_{td}\rangle_{ce}$를 전송함으로서 해당 투표 내용을 삭제할 것을 요청한다.
- 집계자 자신의 게시판에 게시된 해당 투표자의 투표 내용인 ps2, Cp', Rp', B^x을 게시판에서 삭제한다.

〈투표자〉
- 집계자로부터 받은 $\langle\langle ps2||Cp'||Rp'||B^x\rangle_{td}\rangle_{pe}$를 복호화하여 확인하고 이 중 Bx과 등록단계에서 사용한 랜덤수 ps1 즉, $\langle\langle B^x||ps1\rangle_{pd}\rangle_{ce}$를 선거관리센터에 전송한다.

〈선거관리센터〉
- 집계자로부터 받은 $\langle\langle B^x\rangle_{td}\rangle_{ce}$와 투표자로부터 받은 $\langle\langle B^x||ps1\rangle_{pd}\rangle_{ce}$를 각각 복호 및 검증하여 두 B^x 값을 비교한다. 만일 이 두 값이 동일하다면 ps1을 통해 게시판에서 1 번째의 투표 내용을 검색, 해당 투표 내용들을 삭제한 후, 투표자에게 본 프로토콜의 첫 단계부터 재투표할 것을 요청한다. 이때, 만일 두 값이 다를 경우는 투표자와 집계자에게 전송한 값의 재확인을 요청한다.

〈투표자〉
- 선거관리센터의 요청을 확인하고 본 프로토콜의 첫 단계부터 재투표를 진행한다.

제안한 프로토콜은 기존의 프로토콜에 비해 전체 투표 진행이 한번의 세션에 완료되고, 투표자당 전송패스 수의 감소로 대규모의 전자투표에 적용할 수 있으며, 또한 어느 누구도 중간투표 결과를 알 수 없다. 도전 및 응답 프로토콜에 의해 투표자나 혹은 집계자 사이의 부정을 증명할 수 있으며, 익명에 의한 투표로 투표자 프라이버시를 강화하였고, 투표자와 집계자 및 제 3자의 부정을 통해 진행된 투표를 다시 해야하는 불편함을 제거함으로써 시스템의 완전성을 만족하고 있다. 프로토콜에 대한 공격 및 해결은 투표자가 다른 사람의 아이디를 도용하여 투표할 경우 도용한 아이디 투표자의 비밀키를 알 수 없으므로 투표가 불가능하며, 투표한 투표자가 다른 투표권을 생성하여 선거관리센터에 전송시 선거관리센터의 Res_List에서 체크가 되기 때문에 이중 투표가 불가능하다. 집계자가 선거관리센터의 x 값을 알 수 있으므로 자신이 투표권을 생성하여 투표할 경우 투표 마감 후, 합법적인 투표자가 투표권을 행사했던 선거관리센터의 Res_List와 집계자의 T와 비교함으로써 방지할 수 있다.

V. 제안한 프로토콜(II)

제안한 프로토콜(II)도 또한 신뢰하는 선거관리센터를 가정한다. 이 프로토콜의 기본 스킴은 앞서 제안한 Chaum의 부정할 수 없는 도전 및 응답 기법(Undeniable Challenge and Response Technique)을 사용하지 않고 비트 도전 기법을 이용하여 선거관리센터가 개표 단계에서 비트 도전 기법의 키를 전송함으로써 봉인된 투표 용지를 개봉할 수 있으며, 투표 단계에서 투표자가 선거관리센터로부터 투표용지에 대한 영수증을 받음으로써 투표자는 자신의 투표용지가 올바로 등록되었음을 인식한다.

5.1 프로토콜 요소

- ps1, ps2 : 투표자가 익명에 사용될 랜덤수
- sk : 비트 도전 기법의 랜덤수
  $usk = sk^{-1}$
- bk : 블라인딩기법을 위한 랜덤수
- pe, pd : 투표자의 키 쌍
- V : 기표된 투표용지
- $m = (ps2||V)^{sk} \pmod p$
- $B = m^* bk_{ce} \pmod p$: 블라인드 된 투표용지
- ce, cd : 선거관리센터의 키 쌍
- Reg_List : 등록된 투표자의 리스트(아이디, 공개키 포함)
- te, td : 집계자의 키 쌍
- || : 연접연산
- T : 투표 결과 리스트

5.2 프로토콜

5.2.1 등록단계

〈투표자〉
- $\langle ps2||usk\rangle_{te}$: 투표자의 익명 아이디와 비트도

전 기법의 랜덤 수를 집계자 공개키로 암호화

- $m=(ps2||V)^{sk} \pmod p$: 투표자의 기표된 투표 용지와 투표자의 익명을 연접한 후 비트 도전 기법 적용 결과
- $B=m^{*}bk^{ce} \pmod p$: 블라인딩기법 연산 결과
- $s=B_{pd} \pmod p$: 투표자의 서명 결과
- $\langle ID||ps1||\langle ps2||usk\rangle_{te}||B||s\rangle_{ce}$를 선거관리센터에 전송

〈선거관리센터〉

- cd로 암호화된 $\langle ID||ps1||\langle ps2||usk\rangle_{te}||B||s\rangle_{ce}$를 복호화
- $B=s_{pe} \pmod p=(B_{pd})_{pe} \pmod p$: 투표자의 서명 확인
- 투표자가 이전에 투표했는지 Rev_List 체크
- 게시판 l 번째에 ID, ps1 공표
- $\langle\langle ps2||usk\rangle_{te}\rangle_{cd}$, B_{cd} : $\langle ps2||usk\rangle_{te}$에 선거관리센터의 서명 및 B 투표용지에 선거관리센터가 인증하는 서명
- 동일한 l 번째에 $\langle\langle ps2||usk\rangle_{te}\rangle_{cd}$, B_{cd}를 공표없이 저장.
- $\langle\langle\langle ps2||usk\rangle_{te}\rangle_{cd}||B_{cd}\rangle_{pe}$를 투표자에게 전송

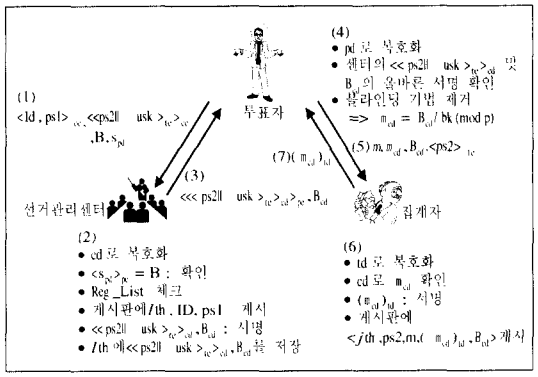
5.2.2 투표단계

〈투표자〉

- $\langle\langle\langle ps2||usk\rangle_{te}\rangle_{cd}||B_{cd}\rangle_{pe}$를 자신의 비밀키 pd로 복호화 및 확인
- $m_{cd}=B_{cd}/bk \pmod p$: 블라인딩기법 제거
- $\langle m||m_{cd}||B_{cd}||ps2\rangle_{te}$를 집계자에게 전송

〈집계자〉

- td로 $\langle m||m_{cd}||B_{cd}||ps2\rangle_{te}$를 복호화



〔그림 4〕 제안한 프로토콜(II) : 등록 및 투표단계

- ce로 m_{cd} 확인
- $(m_{cd})_{td}$: 집계자의 서명
- 집계자는 게시판의 j번째, m, m_{cd}, B_{cd}, $\langle ps2\rangle_{te}$를 게시
- $\langle\langle m_{cd}\rangle_{td}\rangle_{pe}$를 투표자에게 전송

〈투표자〉

- pd로 $\langle\langle m_{cd}\rangle_{td}\rangle_{pe}$를 복호화, $\langle m_{cd}\rangle_{td}$에서 자신이 보낸 투표용지의 정당성 확인

5.2.3 개표단계(투표 완료 후)

모든 투표자가 투표를 완료한 후 수행한다.

〈선거관리센터〉

- 리스트 $\langle\langle\langle ps2||usk\rangle_{te}\rangle_{cd}\rangle_{te}$를 집계자에게 전송

〈집계자〉

- $\langle\langle\langle ps2||usk\rangle_{te}\rangle_{cd}\rangle_{te}$를 td로 복호한 다음 선거관리센터의 ce 서명 검증키로 확인
- 게시판에 게시된 익명의 ps2와 비교하여 투표용지를 개봉

$$m^{usk}=(ps2||V)^{sk \cdot usk} \pmod p$$
$$=ps2 \,||\, V$$

- T 갱신 및 결과 발표

5.3 제안한 프로토콜(II) 분석

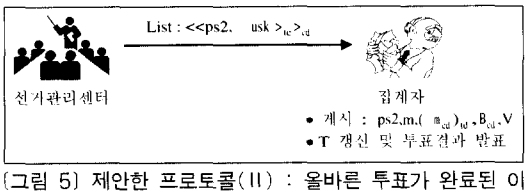
제시된 투표 프로토콜의 요구사항에 대해 제안한 본 논문의 프로토콜(II)의 안전성을 분석한다.

5.3.1 투표권의 공통성(Commonality)

합법적인 투표자는 선거관리센터로부터 등록단계에서 Reg_List에 의해 체크가 가능하므로 동일한 투표자가 두 번 이상 투표할 수 없다.

5.3.2 비밀성(Privacy)

선거에 참여하는 어느 누구도 투표자가 누구에게



〔그림 5〕 제안한 프로토콜(II) : 올바른 투표가 완료된 이후의 개표단계

투표했는지를 알 수 없어야 한다. 투표 내용을 알기 위해서는 블라인딩 된 투표 용지의 내용을 알아야 하는데 블라인딩기법의 파라미터는 투표자만이 알고 있으므로 투표자 외에 누구도 투표 내용을 알 수 없다.

5.3.3 합법성 (Eligibility)

합법적인 절차를 통하여 투표권을 얻은 사람만이 투표에 참여할 수 있다. 투표 전에 합법적인 투표자를 선별하여 각 선거관리센터와 집계자에게 리스트를 전송하므로, 만약 비합법적이지 못한 투표자가 투표를 하기 위해서는 합법적인 투표자의 전자 서명을 생성할 수 있어야 한다. 그러나, 전자 서명은 합법적인 투표자만이 생성하여, 투표자 인증에 사용되고 등록된 공개키로만 검증할 수 있기 때문에 비합법적인 투표자는 투표에 참가 할 수 없다.

5.3.4 정확성 (Accuracy)

집계결과가 정확해야 한다. 투표 완료 후 선거관리센터는 집계자에게 $\langle\langle ps2, usk\rangle_{te}\rangle_{cd}$리스트를 전송함으로써 집계자가 투표 용지를 올바르게 카운트하는 지를 알 수 있다.

5.3.5 위조 불가능성(Unforgeability)

선거관리센터로부터 인증을 받은 투표권은 제3자에 의해 위조가 불가능하다.

$$B^{cd}=(m^{*}bk^{ce})^{cd} \pmod p$$

선거관리센터의 인증 값 cd를 계산 할 수 있어야 투표자가 기표한 투표 용지를 위조 할 수 있다. 하지만 cd 값을 계산한다는 것은 GF(p) 상에서의 이산대수 문제이므로 투표 용지의 위조는 불가능하다.

5.3.6 공정성(Fairness)

투표진행과정에서 전체 투표에 영향을 줄 수 있는 중간투표 결과를 알 수 없어야 한다.

$$m=(ps2||V)^{sk} \pmod p$$

중간투표 결과를 알기 위해서는 집계자는 usk 값을 알아야 한다. 또한 선거관리센터가 usk를 알기 위해서는 $\langle ps2||usk\rangle_{te}$ 에서 집계자의 비밀키를 알아야 한다. 그러므로 누구도 중간투표의 결과를 알 수 없다.

5.3.7 완전성(Completeness)

투표시스템은 투표자 또는 집계자의 부정을 통해 투표 진행이 중단되지 않아야 한다. 만일, 투표 단계에서 집계자가 투표자에게 투표내용의 확인을 위해 보낸 일종의 영수증, $(m_{cd})_{td}$값을 확인하는 과정에서 이 값이 투표자 자신이 보낸 값과 동일하지 않을 경우에 집계자의 실수나 혹은 부정이 밝혀진다. 따라서, 이 단계 이후에 앞서 제안한 프로토콜(Ⅰ)에서와 마찬가지로 B^{x}가 아닌 B_{cd} 값을 적용하여 아래와 같이 프로토콜의 완전성을 증명할 수 있다.

〈집계자〉

- 투표자와 선거관리센터에게 각각 $\langle\langle B_{cd}\rangle_{td}\rangle_{pe}$와 $\langle\langle B_{cd}\rangle_{td}\rangle_{ce}$를 전송함으로서 해당 투표 내용을 삭제할 것을 요청한다.
- 집계자 자신의 게시판에 게시된 해당 투표자의 투표 내용인 $\langle m, m_{cd}, B_{cd}, \langle ps2\rangle_{te}\rangle$를 게시판에서 삭제한다.

〈투표자〉

- 집계자로부터 받은 B_{cd}를 복호 및 확인하고, $\langle\langle B_{cd}||ps1\rangle_{pd}\rangle_{ce}$를 선거관리센터에 전송한다.

〈선거관리센터〉

- 집계자로부터 받은 $\langle\langle B_{cd}\rangle_{td}\rangle_{ce}$와 투표자로부터 받은 $\langle\langle B_{cd}||ps1\rangle_{pd}\rangle_{ce}$를 각각 복호 및 검증하여 두 B_{cd} 값을 비교한다. 만일 이 두 값이 동일하다면 ps1을 통해 게시판에서 1 번째의 투표 내용을 검색, 해당 투표 내용들을 삭제한 후, 투표자에게 본 프로토콜의 첫 단계부터 재투표할 것을 요청한다. 이때, 만일 두 값이 다를 경우는 투표자와 집계자에게 전송한 값의 재확인을 요청한다.

〈투표자〉

- 선거관리센터의 요청을 확인하고 본 프로토콜의 첫 단계부터 재투표를 진행한다.

제안한 프로토콜(Ⅱ)는 (Ⅰ)의 프로토콜과 동일하게 전체 투표 진행이 한번의 세션에 완료되나, 영수증을 주기 위해 통신 패스가 네 번으로 늘어난다. 그리고 어느 누구도 중간투표 결과를 알 수 없다. 또한 투표자와 집계자 및 제 3자의 부정을 통해 진행된 투표를 다시 해야하는 불편함을 제거하였다.

〔표 1〕 투표 프로토콜들의 요구사항에 대한 분석

프로토콜 / 요구사항	Fujioka, Okamoto, Ohta 프로토콜	Baraani 프로토콜	SENSUS 프로토콜	제안한 프로토콜(Ⅰ)	제안한 프로토콜(Ⅱ)
정확성	○	○	○	○	○
비밀성	○	○	○	○	○
위조 불가능성	○	○	○	○	○
단일성	○	○	○	○	○
합법성	○	○	○	○	○
공정성	○	×	×	○	○
확인성	○	○	○	○	○
투표권 매매방지	×	×	×	×	×
완전성	×	×	×	○	○
통신패스	4회	후보자들 수+3회	5회	3회	4회
세션성	두 세션	두 세션	두 세션	한 세션	한 세션
비고		공정성과 세션성은 상충됨	공정성과 세션성은 상충됨	제안한 프로토콜(Ⅱ)는 패스가 1회 증가하지만 소규모 투표에서 투표자에게 영수증을 보냄으로써 신뢰성 증가	

프로토콜에 대한 공격 및 해결은 투표자가 다른 사람의 아이디를 도용하여 투표할 경우 도용한 아이디 투표자의 비밀키를 알 수 없으므로 투표가 불가능하며, 투표한 투표자가 다른 투표권을 생성하여 선거관리센터에 전송시 선거관리센터의 Res_List에서 체크가 되기 때문에 이중 투표가 불가능하다. 또한, 영수증을 각 투표자들에게 전달함으로써 투표한 내용에 대한 확신을 줄 수 있으며 이는 향후 구현 측면에서도 고려될 수 있는 장점을 가지고 있다.

제안한 프로토콜들은 모두 개인의 프라이버시를 보호하고, 중간투표 결과를 알 수 없지만, 첫 번째 제안한 프로토콜은 투표자의 수가 많은 대규모 전자투표에서 투표자당 전송 패스를 줄임으로써 시스템의 효율을 증가시킬 수 있으며, 두 번째 프로토콜은 전송패스는 1회 증가하지만, 사용자 측면에서 투표자는 집계자로부터 투표용지에 대한 영수증을 받음으로써 신뢰성을 향상시켰다.

위의 〔표 1〕은 기존 프로토콜들과 본 논문에서 제안한 프로토콜의 요구사항들에 대해 비교한 것이다.

Ⅵ. 결 론

투표는 민주 사회에서 개개인의 의사 표시를 위한 한 방법이므로 부정이 발생하지 않아야 한다. 게다가 실세계에서 이루어지지 않고 전자적으로 투표가 이루어진다면 더 많은 세밀한 부분까지도 염두 해 두어야 한다. 본 논문에서는 실용적이고 대규모 전자투표에 적합한 프로토콜을 제안하였다. 기존에 제안된 프로토콜들의 단점인 패스가 늘어남에 따라 전체 투표 시스템에 미치는 영향도 증가하므로 제안된 논문에서는 패스를 감소시킴으로써 시스템의 효율성을 높였으며, 중간투표 결과를 알 수 없도록 하기 위해서 투표자가 한번 더 투표에 참여해야 하는 불편함을 제거하였다.

제안된 첫 번째 프로토콜은 익명을 기반으로 도전 및 응답 프로토콜을 사용하여 투표자와 집계자사이의 부정을 방지하였으며, 개표 단계에 선거관리센터가 집계자에게 투표용지를 개봉할 수 있는 파라미터를 전송함으로써 어느 누구도 중간투표 결과를 알 수 없고, 한 번의 세션에 투표를 완료할 수 있다.

두 번째 제안된 프로토콜은 전송 패스가 한 번 더 추가되었지만, 비트 도전 기법을 이용하여 개표 단계에 선거관리센터가 비트 도전 기법의 비밀키를 전송함으로써 중간투표 결과를 알 수 없게 하였다. 그러나, 이러한 일련의 기법들(도전 및 응답 프로토콜이나 비트 도전기법 등)은 자칫 통신상에서 비용이나 효율성을 저하시킬 수 있는 소지가 있으므로 향후 여기에 대한 개선 방안을 강구할 필요가 있다.

그밖에 본 논문에서는 신뢰할 수 있는 선거관리센터를 가정하였는데, 만약 선거관리센터가 부정하거

나 집계자와의 결탁이 발생할 경우에는 투표에 대한 위조가 가능하며, 동시에 투표 미 수행자에 대한 투표권을 임의로 수행할 수 있다는 문제점을 안고 있다. 따라서, 이 부분은 [6]에서 언급되고 있는 감사기구를 둠으로서 선거관리센터를 감시하는 기능이나 혹은 새로운 개선 방법을 제안하는 등의 추가적인 연구를 통해 향후 이 문제 역시 보완할 필요가 있다.

또한 향후 프로토콜의 발전 방향은 많은 연구가 진행되고 있지만, 전자적으로 인터넷을 통한 투표에서 투표일 전에 매수자에 의해 투표권을 매수 당할 경우 이를 해결할 방법이 없다. 그러므로 투표자와 매수자 사이에 매매 방지를 위한 추가 연구가 필요로 하며, 제안한 투표시스템의 구현으로 실생활에 응용하기 위한 추가 연구가 필요하다.

참 고 문 헌

[1] B. Schneier, *Applied Cryptography*, John Wiley & Sons Inc., 1997

[2] A. Fujioka, T. Okamoto and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections", *In Advances in Cryptology-Proceedings of AUSCRYPT'92*, 1992

[3] A. Baraani-Dastjerdi, J. Pieprzyk and R. Safavi-Naini, "A Secure Voting Protocol Using Threshold Schemes," *Proceedings of COMPSAC'95*, pp. 143~148, 1995

[4] L. F. Cranor, R. K. Cytron, "Design and Implementation of a Security-Conscious Electronic Polling System", Washington University Computer Science Technical Report WUCS-96-02, February, 1996

[5] D. Chaum, "Undeniable Signatures," *Proceedings of CRYPTO'89*, pp. 212~216, 1989.

[6] 박희운, 이임영, "전자투표상에서의 부정행위 방지에 관한 연구", *통신정보보호학회논문지* 제8권, 제4호, 1998. 12

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

〈著者紹介〉

김 순 석 (Soon-Seok Kim)
1997년 2월 : 진주대학교 컴퓨터공학과 학사
1999년 2월 : 중앙대학교 컴퓨터공학과 석사
1999년 3월~현재 : 중앙대학교 컴퓨터공학과 박사과정
〈관심분야〉 암호프로토콜, 이동통신 보안, 정보보호

이 재 신 (Jae-Shin Lee)
1998년 2월 : 군산대학교 컴퓨터과학과 학사
2000년 2월 : 중앙대학교 컴퓨터공학과 석사
2000년 3월~현재 : 주식회사 이니텍 연구원
〈관심분야〉 전자투표 프로토콜, 전자지불시스템, 정보보호

김 성 권 (Sung-Kwon Kim) 정회원
1981년 2월 : 서울대학교 계산통계학과 학사
1983년 2월 : 한국과학기술원 전산학과 석사
1983년 3월~1985년 9월 : 목포대학교 재직
1990년 8월 : University of Washington 전산학과 박사
1991년 3월~1996년 2월 : 경성대학교 재직
1996년 3월~현재 : 중앙대학교 컴퓨터공학과 재직중
〈관심분야〉 정보보호, 알고리즘, 컴퓨터이론