情報保護學會論文誌
第11券 第5號, 2001. 10

Bit-Commitment를 이용한 전자투표 프로토콜에 관한 연구

김 대 엽*, 임 종 인**

A Study on Electronic Voting Protocol using Bit-Commitment

Dae-Youb Kim*, Jong-In Lim**

요 약

개인 컴퓨터와 네트워크의 급속한 보급 및 발전된 보안기술은 기존 투표형식의 많은 문제점들을 보완하면서 편리하고 안전한 전자투표의 비중을 증대시키고 있다. 그러나 이러한 비중의 증대에도 불구하고, 많은 취약점들이 산재해 있다. 특히, 투표자의 익명성과 투표결과의 정확성을 보장하는 문제는 전자투표 프로토콜이 실제 응용될 수 있는가를 판단하는 중요한 요소가 아닐 수 없다. 또한 투표권의 매매와 같은 문제들은 아직도 해결해야 될 과제로 남아 있다.

본 논문에서는 안전한 전자투표를 설계하기 위하여 고려해야 할 사항들을 살펴보고, [1]에서 발표되었던 전자투표 프로토콜의 취약점과 개선 방안을 제시한다. 개선된 프로토콜은 [1]에서 제시된 장점들을 유지하면서, 선거관리자와 집계자의 공모에 의한 투표권자의 익명성 훼손을 막고, 불법적인 선거개입을 원천적으로 봉쇄하도록 설계되었다.

ABSTRACT

Fast diffusion of personal computer and network, and developed security technology are augmenting specific gravity of convenient and safe electronic voting system supplementing much problems of existent off-line vote form. But in spite of enlargement of these weight, much limitations are extravagant. Specially, problem that secure voter's anonymousness and accuracy of poll can be important urea that judge if electronic voting system can be applied actually. Also, problems such as buying and selling of vote remain to subject that must solve yet.

In this paper, we introduce items that is considered to design the safe electronic voting system, and present limitation of electronic polling system announced in [1]. And we propose improvement way. Improved protocol keeping advantages that is presented in [1], designed to keep away voter's anonymousness defamation by conspiracy of Election Administration Committee and Totaling Committee, and block unlawful election intervention as original.

keyword : *전자투표, 전자서명, 암호프로토콜, Bit-Commitment*

Ⅰ. 서 론

민주적으로 운영되는 조직의 경우, 조직을 구성하고 운영하기 위한 대표를 선출하고 구성원의 의견을 수렴하기 위한 방법이 조직의 특성에 따라 운영되고 있다. 전통적으로 투표가 구성원의 의견을 공식적으로 표현하고 수렴하는 방법으로 사용되어졌다면, 여론조사는 그 결과에 있어서 비공식적이지만 의미 있는 대중의 의견으로 간주되어져 왔다.

이러한 투표와 여론조사는 안전성과 투표권자의

* (주) 시큐아이닷컴, 정보보호연구소(david_kdy@hanmail.net)
** 고려대학교 정보보호 대학원(jilim@tiger.korea.ac.kr)

익명성 등을 제공해야 된다. 그러나 이러한 조건을 모두 만족시키는 방법은 대부분 높은 비용문제가 제기된다. 뿐만 아니라, 안전성과 비밀 보장을 만족시키기 위한 새로운 시스템의 구성은 많은 시간 소요와 선거관리자가 부담해야 되는 비용, 그리고 투표권자에게 익숙하지 못한 투표절차 등의 문제가 제기될 수 있다. 특히, 투표권자들이 지역적으로 분산되어 있는 경우, 이러한 문제들은 더욱 크게 제기될 수 있다.

개인 컴퓨터와 컴퓨터 네트워크의 급속한 보급, 그리고 보안기술의 발전은 비정부 분야의 많은 부분에서 기존 off-line의 투표 시스템을 전자투표 시스템으로 대체하게 하는 기반이 되고 있다. 인터넷을 비롯한 컴퓨터 네트워크를 이용한 전자투표나 여론조사는 개인 컴퓨터의 보급이 확산될수록 투표권자에게 더욱 익숙한 시스템으로 자리 잡게 될 것이며, 투표를 하기 위하여 투표권자가 소요해야 되는 시간을 크게 줄일 수 있게 될 것이다. 또한, 기존에 구축된 네트워크를 이용하게 되므로 선거관리자의 추가 비용부담을 줄일 수 있다.

그러나 전자투표 시스템의 경우, 시스템 설계에서 발생할 수 있는 작은 오류로 인하여 투표결과가 잘못 집계되거나, 투표권자의 익명성이 훼손되는 문제가 발생할 수 있기 때문에 시스템 설계에 많은 주의가 요구된다.

본 논문에서는 1999년 한국통신정보보호학회 종합학술 발표회에서 발표된 전자투표 프로토콜[1]을 살펴보고, 해당 프로토콜의 취약점 및 보완방안을 제시한다.

II. 전자투표 프로토콜

이 절에서는 일반적인 전자투표 프로토콜의 구성요소와 안전성에 관한 정의를 살펴본다.

2.1 전자투표 프로토콜의 구성요소

전자투표 프로토콜의 구성요소는 시스템에 따라 다를 수 있다. 일반적으로 투표권자와 선거관리자의 두 요소로 구성되어 있거나, 투표권자, 선거관리자, 그리고 집계자의 세 요소로 구성된다. [5]에서 제안된 시스템에서는 실제 투표를 시작하기 전에 필요한 사항들을 준비해서 투표권자와 선거관리자, 그리고 집계자에게 각각 필요한 자료를 전달하는 Trusted Authority가 존재한다.

투표의 진행단계는 설계자의 설계원칙에 따라 다양한 모습으로 구성되어 있다. [5]에서 제안된 시스템의 경우는 Preparation, Registration, Voting, Opening의 네 단계로 구성되어 있고, [6]에서 제안된 시스템은 Preparation, Administration, Voting, Collection, Opening, Counting의 여섯 단계로 구성되어 있다. 이와 같이 시스템의 설계와 그 특성에 따라 투표 진행 단계의 구성은 다를 수 있으나, 크게 다음과 같은 네 단계로 요약될 수 있다.

(1) 준비 단계 : 투표에 필요한 data들을 생성하고 구성요소에 적절하게 전달한다.
(2) 등록 단계 : 투표권자는 자신의 투표권을 선거관리자에게 신고하고 인증을 받는다.
(3) 투표 단계 : 인증된 투표권자는 기표용지에 기표하고 집계자에게 전달한다.
(4) 개표 단계 : 집계자는 기표용지를 Open하고 결과를 집계한다.

각각의 단계에서는 안전성과 익명성을 보장하기 위하여 Bit-Commitment Scheme, Threshold Scheme, 전자서명, Blind Signature 등을 특성에 맞게 사용할 수 있다. [5]에서 제시한 Baraani의 프로토콜은 Threshold Scheme을 사용하여 구성요소의 부정을 최소화하는 방안을 제시하고 있다. Fujioka와 Okamoto등이 [6]에서 제안한 프로토콜은 Bit Commitment Scheme과 Blinding Scheme을 사용하여, 인증 및 투표권자의 익명성을 보호하는 방안을 제시하고 있다.

2.2 전자투표 프로토콜의 안전성

투표권자의 익명성과 투표결과의 유출을 막기 위한 적절한 프로토콜이 구성되지 않는다면 전자투표는 기존 off-line에서의 투표방식을 대체할 수 없다. 전자투표에 적합한 프로토콜이라면 적어도 다음과 같은 여섯 가지 요구사항[10]을 만족해야 된다.

(1) 투표권을 소유한 사람만이 투표에 참여할 수 있다.
(2) 투표권은 오직 한번만 행사할 수 있다.
(3) 다른 사람의 기표결과를 알 수 없다.
(4) 다른 사람의 기표용지를 복사할 수 없다.
(5) 기표된 용지가 불법적으로 변경되면, 그 결과는

항상 발견된다.
(6) 모든 투표권자는 자신의 투표결과가 정확하게 집계에 포함되었는지를 알 수 있다.

위의 요구사항들을 만족시키기 위한 익명성과 안전성을 제공하는 일반적인 전자투표 프로토콜에서의 기표용지는 다음과 같은 환경에서 집계자에게 제공된다.[2,3]

(1) 기표용지는 암호화된 상태에서 전달된다.
(2) Anonymous Communication Channel를 통해서 기표용지는 전달된다.

또한, 익명성을 보장하기 위하여 투표권자와 선거에 관련된 기관과의 모든 전송은 Anonymous Communication Channel를 통해서 전달되는 것을 원칙으로 한다.

이와 같은 통신 선로 상에서의 환경과 앞서 제시한 안전한 프로토콜의 몇 가지 요구사항을 바탕으로 전자투표 프로토콜의 안전성을 평가하기 위한 요소들은 다음과 같은 항목들이 있다.

(1) Completeness : 정당하게 투표된 결과는 정확하게 집계되어야 한다.
(2) Soundness : 정당하지 못한 투표권자가 투표를 방해하게 해서는 안 된다.
(3) Privacy : 투표권자의 기표결과는 비밀을 유지해야 한다. 기표내용은 기표한 당사자와 집계자를 제외한 다른 사람이 알 수 없어야 하며, 투표의 구성요소들(예를 들어, 집계자와 선거관리자)이 공모하더라도, 투표자와 기표내용 사이의 관계를 예측할 수 없어야 한다.
(4) Unreusability : 투표권자의 투표권은 한번만 행사될 수 있어야 한다.
(5) Eligibility : 정당한 투표권이 있는 투표권자만이 투표에 참여할 수 있어야 한다.
(6) Fairness : 투표 과정에서 중간 집계 결과를 알 수 없어야 한다. 즉, 중간 집계 결과가 투표권자의 투표 의사 결정에 영향을 끼칠 수 없어야 한다.
(7) Verifiability: 집계결과는 위조될 수 없다.

위와 같은 조건들을 만족할 때, 제안된 전자투표 프로토콜은 안전하다고 평가된다.[5~8]

Ⅲ. 기존 프로토콜

[1]에서는 두 종류의 전자투표 프로토콜이 제안되었다. 이 절에서는 그 중 Bit Commitment를 이용한 두 번째 프로토콜을 소개한다. 프로토콜은 투표권자(투표자), 선거관리자, 집계자의 세 부분으로 구성된다. 또한 투표는 크게 준비단계, 등록단계, 투표단계, 그리고 개표단계로 구분된다.

3.1 프로토콜의 요소

이 절에서는 [1]에서 제안한 프로토콜에서 사용된 기호들을 설명한다.

(1) $ps1$, $ps2$: 투표권자의 익명에 사용될 난수
(2) sk : bit commitment에 사용된 난수:

$$usk = sk^{-1} \tag{1}$$

(3) bk : blinding scheme을 위한 난수
(4) pe, pd : 투표권자의 공개키, 비밀키 쌍
(5) ce, cd : 선거관리자의 공개키, 비밀키 쌍
(6) te, td : 집계자의 공개키, 비밀키 쌍
(7) V : 기표된 투표용지
(8) $R-List$: 등록된 투표자의 리스트
(9) $C-List$: 투표결과 리스트

3.2 제안된 프로토콜

이 절에서는 [1]에서 제시한 프로토콜의 각 단계를 간략하게 설명한다.

3.2.1 등록단계

(a) 투표권자

- 집계자의 공개키를 사용하여 익명 ID로 사용할 $ps2$와 인증에서 사용할 난수 usk를 암호화한다 :

$$\langle ps2 \| usk \rangle_{te} . \tag{2}$$

- Bit Commitment Scheme :

$$m = (ps2 \| V)^{sk} \pmod{p} . \tag{3}$$

- Blinding Signature :

$B = m \times bk_{ce} \pmod{p}$,
$s = B_{pd} \pmod{p}$. (4)

- $\langle id, ps1 \rangle_{ce}$, $\langle\langle ps2 \| usk \rangle_{te} \rangle_{ce}$, B, s를 선거관리자에게 전송한다.

(b) 선거관리자
- $\langle\langle ps2 \| usk \rangle_{te} \rangle_{ce}$와 $\langle id, ps1 \rangle_{ce}$를 복호화 한다.
- 해당 투표권자의 서명을 확인한다.
- 해당 투표권자가 이전에 투표했는가를 확인한다.
- 게시판 R-List l번째에 id와 $ps1$을 공개한다.
- $\langle ps2 \| usk \rangle_{te}$와 B에 서명한다.
- 동일한 l번째에 서명한 결과를 공표 없이 저장한다.
- $\ll ps2 \| usk \rangle_{te} \rangle_{cd} \rangle_{pe}$와 B_{cd}를 해당 투표권자에게 전송한다.

3.2.2 투표단계

(a) 투표권자
- $\ll ps2 \| usk \rangle_{te} \rangle_{cd} \rangle_{pe}$를 자신의 비밀키로 복호화해서 그 값을 확인한다.
- B_{cd}의 값을 확인한다.
- Blinding을 제거한다:

$$m_{cd} = \frac{B_{cd}}{bk} \pmod{p}. \quad (5)$$

- m, m_{cd}, B_{cd}, $\langle ps2 \rangle_{te}$를 집계자에게 전송한다.

(b) 집계자
- td로 $\langle ps2 \rangle_{te}$를 복호화 한다.
- ce로 m_{cd}를 확인한다.
- m_{cd}에 서명한다: $\langle m_{cd} \rangle_{td}$.
- 게시판 C-List의 j번째에 m, m_{cd}, B_{cd}, $\langle ps2 \rangle_{te}$를 게시한다.
- $\langle m_{cd} \rangle_{td}$를 해당 투표권자에게 전송한다.

(c) 투표권자
- $\langle m_{cd} \rangle_{td}$를 확인하여, 자신의 기표내용이 정확한가를 확인한다.

3.2.3 개표단계

(a) 선거관리자
- $\langle\langle ps2 \| usk \rangle_{te} \rangle_{cd}$가 수록된 리스트를 집계자에게 전송한다.

(b) 집계자
- $\langle\langle ps2 \| usk \rangle_{te} \rangle_{cd}$를 선거관리자의 공개키와 자신의 비밀키를 사용해서 복호화 한다.
- 집계자의 게시판에 게시된 익명의 $ps2$와 비교하여 투표용지를 개봉한다:

$$m^{usk} = (ps2 \| V)^{sk^{-} usk} \pmod{p} = ps2 \| V. \quad (6)$$

- C-List 를 갱신하고 결과를 발표한다.

Ⅳ. 프로토콜의 취약점

[1]에서 제안된 프로토콜은 다음과 같은 취약점이 있다.

(1) 투표 때마다 사용되는 선거관리자의 비밀키와 공개키의 쌍 (cd, ce)가 동일하다고 가정하면, 등록단계에서 투표권자가 선거관리자에게 전달하는 $\langle\langle ps2 \| usk \rangle_{te} \rangle_{ce}$, $\langle id, ps1 \rangle_{ce}$, B, s를 공격자가 도청하여 보관하고 있다가, 다음 선거에서 투표권자보다 먼저 선거관리자에게 동일한 자료를 전송하여 등록함으로서 정당한 투표권자의 투표를 방해할 수 있다. 즉 Soundness에 취약점을 갖고 있다.

(2) 등록단계에서 선거관리자는 보관된 자료로부터 투표권자의 $\langle\langle ps2 \| usk \rangle_{te} \rangle_{cd}$와 $\langle id, ps1 \rangle$의 관계를 알 수 있다. 또한 개표단계에서 집계자는 $\langle\langle ps2 \| usk \rangle_{te} \rangle_{cd}$와 개표용지 V의 관계를 알 수 있다. 그러므로 선거관리자와 집계자가 공모한다면, 투표권자의 id와 기표용지 V 사이의 관계를 알 수 있게 됨으로서 투표권자의 익명성, 즉 Privacy에 취약점을 갖고 있다. 특히, [1]에서는 Privacy의 평가를 공개키 기반 알고리즘과 블라인딩 기법의 안전성에만 근거를 두고 있기 때문에, 공모에 의한 Privacy의 침해가 고려되지 않고 있다.

(3) 선거관리자와 집계자가 공모하면 등록단계에서 선거관리자가 획득한 $\langle ps2 \| usk \rangle_{te}$를 이용하여 투표가 마감되기 전에 투표권자의 투표결과를 복호화 할 수 있다. 즉, 선거관리자와 집계자가 공모한다면 중간집계 결과를 알 수 있기 때문에 Fairness에 취약점을 갖고 있다.

V. 개선 안

5.1 기본논리 및 기호

앞 절에서 지적한 취약점에 대한 개선 안의 기본 논리는 다음과 같다.

(1) 투표 때마다 사용되는 선거관리자의 키 쌍이 같을 수 있다면, 선거관리자는 투표 때마다 다른 난수 R을 생성해서 개시한다. 투표자는 등록단계에서 등록을 위해 선거관리자에게 보내는 메시지 생성에 난수 R을 사용한다.
(2) 선거관리자와 집계자가 투표자에 대한 공통의 정보를 보유하지 못하도록 설계한다. 이를 위하여 개표단계에서 사용되는 투표권자의 익명 ID와 기표용지의 복호화 키에 대한 선관위의 서명을 획득할 때, Blinding Scheme을 사용한다.
(3) Fairness를 보완하기 위해서, 투표결과의 복호화에 필요한 $\langle\langle ps \| usk\rangle_{te}\rangle_{cd}$ 는 투표가 마감된 후 투표권자가 집계자에게 직접 전송한다.

개선된 프로토콜을 설명하기 위하여 [1]에서 사용한 기호를 동일하게 사용하며, 추가적으로 다음과 같은 기호들을 정의한다.

(1) id : 투표권자의 ID
(2) ps : 투표권자의 익명 ID로 사용 할 난수
(3) R : 선거관리자가 게시하는 난수

5.2 개선된 프로토콜

이 절에서는 [1]에서 제시한 프로토콜의 기본 안을 바탕으로 취약점을 보안하기 위해 개선된 프로토콜을 제시한다.

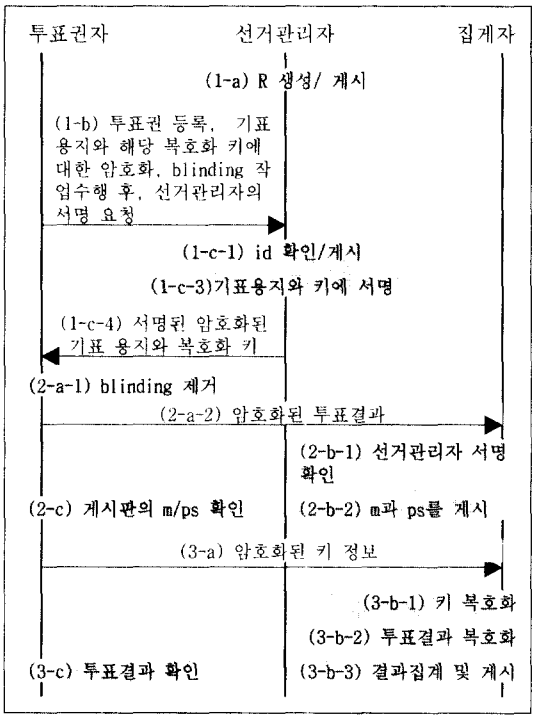
5.2.1 등록단계

(a) 선거관리자

- 시행되는 선거에서 사용할 난수 R을 생성/게시한다.

(b) 투표권자

- 집계자의 공개키를 사용하여 익명 ID로 사용할 ps와 인증에 사용할 난수 usk를 암호화한다:



[그림 1] 개선된 프로토콜 흐름도

$$K = \langle ps \| usk\rangle_{te} \| R \ . \tag{7}$$

- K를 선거관리자가 저장한 후, 집계자와 공모하는 것을 막기 위하여 Blinding Scheme을 사용한다:

$$BK = K \times bk_{ce} \pmod{p} \ . \tag{8}$$

- Bit-Commitment Scheme을 사용해서 투표결과를 암호화한다:

$$m = (ps \| V)^{sk} \pmod{p}. \tag{9}$$

- Blinding Scheme 과 서명:

$$B = m \times bk_{ce} \pmod{p}. \tag{10}$$

$$s = \ll id, R\rangle_{pd}\rangle_{ce} \| BK \| B\rangle_{pa}. \tag{11}$$

- id, $\langle\langle id, R\rangle_{pd}\rangle_{ce}$, BK, B, s를 선거관리자에게 전송한다.

(c) 선거관리자

- cd를 사용하여 전송된 $\langle\langle id, R\rangle_{pd}\rangle_{ce}$를 복호화 한다.
- 해당 투표권자의 공개키를 사용하여 $\langle id, R\rangle_{pd}$를 복호화해서 난수 R의 값을 확인한다.
- 해당 투표권자의 서명 s를 확인한다.
- 해당 투표권자가 이전에 투표했는가를 R-List와 id를 비교해서 확인한다.
- 게시판 R-List에 id와 $\langle id, R\rangle_{pd}$를 공개한다.
- BK와 B를 비밀키 cd로 서명한다.
- $\langle BK\rangle_{cd}$와 B_{cd}를 해당 투표권자에게 전송한다.

5.2.2 투표단계

(a) 투표권자

- $\langle BK\rangle_{cd}$와 B_{cd}에 첨부된 선거관리자의 서명을 확인한다.
- B에서 Blinding을 제거한다:

$$m_{cd} = \frac{B_{cd}}{bk} \pmod{p}. \tag{12}$$

- BK에서 Blinding을 제거한다:

$$\langle\langle ps||usk\rangle_{te}||R\rangle_{cd} = \frac{BK_{cd}}{bk} \pmod{p}. \tag{13}$$

- m, m_{cd}, $\langle ps\rangle_{te}$를 집계자에게 전송한다.

(b) 집계자

- $\langle ps\rangle_{te}$를 복호화 한다.
- ce로 m_{cd}를 확인한다.
- 게시판 C-List에 ps와 m을 게시한다.

(c) 투표권자

- 게시판 C-List에서 ps와 m을 확인한다.

5.2.3 개표단계

(a) 투표권자

- 투표가 마감된 후, 집계자에게 $\langle\langle ps||usk\rangle_{te}||R\rangle_{cd}$를 전송한다.

(b) 집계자

- $\langle\langle ps||usk\rangle_{te}||R\rangle_{cd}$를 선거관리자의 공개키와 자신의 비밀키를 사용하여 복호화하고 R을 확인한다.
- 집계자의 게시판에 게시된 익명 ID ps와 비교하여 투표권을 개봉한다:

$$m^{usk} = (ps||V)^{sk \times usk} \pmod{p} = ps||V\ . \tag{14}$$

- C-List를 갱신하고 결과를 발표한다.

(c) 투표권자

- C-List에서 자신의 ps와 결과를 확인한다.

5.3 안전성에 관한 평가

개선된 프로토콜은 [1]에서 제안한 프로토콜의 기본골격을 유지하면서, [1]에서 고려하지 못한 사항에 관하여 추가적으로 기능을 보강한 것이다. 그러므로 [1]에서 평가한 프로토콜의 안전성은 기본적으로 유지된다.

- Completeness/Verifiability : 선거관리자와 집계자의 게시판을 통해서, 투표권자는 등록 및 투표 결과를 확인할 수 있다. 그러므로, 자신의 투표가 정확하게 집계되었는가를 확인할 수 있다. 또한, 자신의 투표가 위조/변조되었다면 그 사실을 항상 발견할 수 있다.
- Unreusability : 투표에 참여하기 위해서는 선거관리자에게 등록을 해야 하기 때문에 이중 투표를 막을 수 있다.
- Eligibility : 투표에 참여하기 위해서는 투표권자의 비밀키를 알고 있어야 선거관리자에게 등록을 할 수 있기 때문에, 본인 이외의 사람은 투표에 참여할 수 없다. 또한, 선거관리자와 집계자가 공모하고 미등록자에 대한 대리 투표를 시도하기 위해서는 R-List에 미등록자의 id와 $\langle id, R\rangle_{pd}$를 공개해야 된다. 그러나, 투표권자의 비밀키를 알 수 없기 때문에, $\langle id, R\rangle_{pd}$를 생성할 수 없다. 또한 $\langle id, R\rangle_{pd}$은 매 투표마다 다른 R을 사용하기 때문에, 과거 등록된 데이터의 재사용이 불가능하다. 그러므로, 미등록자에 대한 대리 투표는 불가능하다.

이 절에서는 보강된 Privacy, Soundness, 그리고 Fairness에 관한 안전성만을 평가한다. 또한 Privacy의 경우, [1]에서 Blinding Scheme의

안전성을 증명했기 때문에, 본 논문에서는 선거관리자와 집계자의 공모에 대한 안전성만을 평가한다.

[정리1(Privacy)]

투표자를 제외한 모든 구성요소들이 공모하더라도 투표자의 익명성은 보장된다.

[증 명]

기표용지와 투표권자의 관계를 알기 위해서는 기표용지 V와 투표권자의 id 사이의 관계를 알아야 한다. 선거관리자가 획득할 수 있는 투표권자의 정보는 등록단계에서 전송된 투표권자의 id, 그리고 $\langle ps||usk\rangle_{te}$ 정보의 blinding된 결과인 BK, 그리고 m의 blinding 된 결과 B 등이 있다. 집계자가 보유할 수 있는 정보는 암호화된 투표 결과 m과 복호화 된 결과 V, 그리고 blinding이 제거된 $\langle ps||usk\rangle_{te}$가 있다. 투표과정에 사용된 모든 전송이 Anonymous Communication Channel을 통해서 이뤄졌고, 사용된 Blinding Scheme이 안전하다고 가정한다면, BK와 $\langle ps||usk\rangle_{te}$의 관계, 그리고 B와 m의 관계를 예측할 수 없다. 그러므로 선거관리자와 집계자가 공모하더라도 투표결과 V와 투표권자 id 사이의 관계를 추측할 수 있는 정보를 공유할 수 없다. 즉, 투표권자의 익명성이 보장된다.

[정리2(Soundness)]

정당한 투표권이 없는 사람의 투표참여는 항상 발견되며, 부정한 목적에 의해서 투표과정을 방해할 수 없다.

[증 명]

과거에 행해진 투표에서 투표자가 등록단계에서 선거관리자에게 보낸 메시지를 도청하여 보관하고 있다 하더라도, 매 번의 투표마다 새로운 난수 R이 선거관리자에 의해서 게시되고, 투표권자가 난수 R을 메시지 생성에 이용하기 때문에 방해자가 보관하고 있는 사용된 메시지는 비록 정당한 투표권자의 ID와 서명이 있다 하더라도, R의 값이 틀리기 때문에 무시된다. 또한, 투표단계에서 투표권자가 집계자에게 전송하는 메시지는 모두 선거관리자의 서명을 정당하게 획득한 메시지들이다. 그러므로 이 단계에서 투표를 방해하기 위하여 투표과정에 불법적으로 참여하는 시도들은 항상 발견된다. 그러므로 Soundness는 보존된다.

[정리3(Fairness)]

투표의 중간집계 결과를 투표 마감 전에 알 수 없다.

[증 명]

암호화된 기표용지 m의 복호화에 사용되는 투표권자의 익명 ID와 복호화 키, 그리고 난수 등의 정보 $\langle\langle ps||usk\rangle_{tc}||R\rangle_{cd}$는 투표가 마감된 후 투표권자가 직접 집계자에게 전송한다. 그러므로, 투표의 중간집계 결과를 투표 마감 전에 알 수 없다.

〔표 1〕은 〔1〕에서 제시한 프로토콜과 개선된 프로토콜의 안전성을 비교한 결과를 나타낸다. Fairness를 보완하기 위해 투표권자는 익명의 ID인 ps와 투표결과의 복호화에 사용할 usk를 개표단계에서 집계자에게 전송해야 되기 때문에, 투표의 전 과정에 참여해야 되는 단점이 있다. 투표를 하기 위해서 투표권자는 모두 3번의 세션 과정을 수행해야 된다. 또한 투표의 전 과정에서 구성요소 간에 총 4회의 데이터 전송이 필요하다. 〔표 2〕는 〔1〕과 〔6〕에서 제시한 프로토콜과 개선된 프로토콜의 세션 수와 데이터 전송 수에 대한 비교표이다. 세션 수는 구성요소간에 통신 연결을 시도한 회수를 의미하며, 데이터 전송 수는 연결된 세션을 통해서 등록에서부터 집계까지 데이터를 전송하는 회수를 의미한다.

〔표 1〕 〔1〕의 프로토콜과 개선된 프로토콜의 안전성 비교

	〔1〕의 프로토콜	개선된 프로토콜
Completeness	게시된 투표결과로 확인 가능	
Soundness	집계자에게 전송되는 투표권자의 모든 메시지는 선거관리자의 정당한 서명이 첨부된 것이므로, 확인가능	
	선거 때마다 선관위의 키가 동일하다면, 침해 가능	**불가능**
Privacy	Blinding 기법 사용으로 투표결과와 투표권자와의 관계를 추측할 수 없음	
	공모에 의한 익명성 침해 가능	**공모에 의한 익명성 침해 불가능**
Unreusablility	투표권자의 (실명)id와 R-List를 사용해서, 투표권은 한번만 행사할 수 있음	
Eligibility	등록단계에서 인증된 투표권자만이 투표에 참여할 수 있음	
Fairness	**공모에 의해 중간집계결과를 알 수 있음**	**중간 집계 결과를 알 수 없음**
Verifiability	게시된 투표결과로 확인 가능	

〔표 2〕 세션 연결 및 데이터 전송 회수 비교

		〔1〕 안	〔6〕 안	개선 안
세 션 연결 수	선거관리자	1	0	0
	집계자	0	0	0
	투표권자	2	3	3
데이터 전송 수		5	4	4

VI. 결 론

전자투표가 실생활에 적용되기 위해서는 편리성뿐만 아니라 투표자의 익명성과 개표의 정확성, 그리고 투표과정의 안전성 등이 보장되어야 한다. 개선된 프로토콜은 〔1〕에서 제시한 프로토콜의 취약점을 개선하여, 부정한 목적으로 투표에 참여하는 정당하지 못한 시도를 즉각 발견할 수 있도록 설계되었으며, 선관위와 집계자가 공모하더라도 투표자의 익명성을 보장할 수 있도록 설계되었다. 또한 투표가 마감되기 전에 중간 집계결과를 알 수 없도록 개표에 필요한 복호화 키를 투표 마감 후에 투표권자가 직접 전달하는 방법을 사용했다. 이와 같은 방법은 Bit-Commitment를 사용한 전자투표 프로토콜에서 일반적으로 사용되는 방법이다. 그러나 투표권자가 투표의 전 과정에 참여해야 되기 때문에, 투표권자에게 많은 시간을 요구한다는 단점이 있다.

본 논문에서는 전자투표의 안전성에 초점을 둔 프로토콜을 제시했다. 그러나 본 논문에서 다루지 못한 투표자의 투표권 매매와 같은 부정행위는 off-line의 기존 투표 제도를 on-line 상의 전자투표로 대체하는데 커다란 걸림돌이 되고 있다.[2~4] 또한 Bit-Commitment Scheme을 이용할 때, 투표권자에게 많은 시간을 요구함으로 인하여 발생하는 투표율 저하 등의 문제도 해결해야 될 과제이다. 전자투표가 실생활에 적용되기 위해서는 안전성, 효율성, 그리고 투표권 매매 등의 부정방지를 위한 대책이 지속적으로 연구되어져야 한다.

참 고 문 헌

〔1〕 이재신, 홍영기, 김순석, 김성권, "효율적인 전자투표 프로토콜에 관한 연구", *한국통신정보보학회 종합학술발표회 논문집*, Vol. 9. No. 1, 1999.

〔2〕 허원근, 김광조, "PVSS를 이용한 검증가능한 다중 전자선거와 검증성을 제한한 매표방지 다중 전자선거", 한국통신정보보호학회 종합학술발표회 논문집, Vol. 9. No. 1. 1990.

〔3〕 이병천, 김광조, "매수행위 방지 가능한 전자투표 시스템", *대한민국특허청, 공개특허공보*, 특 2001-0000030. 2001. 1.

〔4〕 박희운, 이임영, "전자투표상에서의 부정행위 방지에 관한 연구", *통신정보보호학회 논문지*, 제8권, 제4호, 1998. 12.

〔5〕 Ahmad Baraani-Dastjerdi, Josef Pieprzyk, Reihaneh Safaci-Naini, "A Practical Electronic Voting Protocol Using Threshold Schemes".

〔6〕 Atsushi Fujioka, Tatsuaki Okamoto, Kazuo Ohta, "A Practical Secret Voting Scheme for Large Scale Elections".

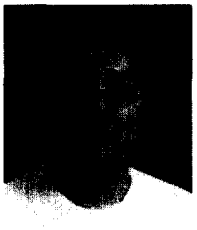
〔7〕 Wei-Chi Ku, Sheng-De Wang, "A secure and practial electroinc voting schem (80e", *Computer Communication 22*, 1999.

〔8〕 Lorrie Faith Cranor, Ron K. Cytron, "Design and Implementation of a Practical Security-Conscious Electronic Polling System".

〔9〕 Lorrie Faith Cranor, Ron K. Cytron, "Sensus: A Security-Conscious Electronic Polling System for the Internet".

〔10〕 Bruce Schneier, "Applied Cryptography", *John Wiley & Sons, Inc.*, 1996.

〈著者紹介〉



김 대 엽 (Dae-Youb Kim) 정회원
1994년 2월 : 고려대학교 수학과 졸업
1996년 8월 : 고려대학교 수학과 석사 (대수학 전공)
2000년 2월 : 고려대학교 수학과 박사 (대수학 전공)
1997년 8월~2001년 3월 : (주)텔리맨, 위성통신 연구소 선임연구원
2001년 4월~현재 : (주)시큐아이닷컴 정보보호 연구소 선임연구원
〈관심분야〉 CAS, Smart Card, PKI, 유/무선 보안프로토콜

임 종 인 (Jong-In Lim) 정회원
1980년 2월 : 고려대학교 수학과 졸업
1982년 2월 : 고려대학교 수학과 석사 (대수학 전공)
1986년 2월 : 고려대학교 수학과 박사 (대수학 전공)
1986년 2월~현재 : 고려대학교 수학과 정교수
2000년10월~현재 : 고려대학교 정보보호 대학원 원장
〈관심분야〉 블록암호 및 스트림 암호의 분석 및 설계, 암호 프로토콜, 공개키 암호 알고리즘의 분석