부정 행위 방지를 위한 전자 투표에 관한 연구

박희운°, 이임영
순천향대학교 공과대학 컴퓨터학부

A Study on Preventing Illegal Acts in Electronic Elections

Hee-Un Park, Im-Yeong Lee
Department of Computer Science, College of Engineering
Soonchunhyang University

요 약

네트워크의 발전과 더불어 많은 응용 분야들이 연구되고 있다. 이 중에서도 특히 암호학을 이용한 전자 투표의 중요성이 증대되고 있다. 그러나 전자 투표는 그 필요성에도 불구하고, 아직까지 취약한 점이 많이 산재해 있다. 투표권의 매매가 성립할 경우 전자 투표에 있어 치명적인 악영향을 미침과 동시에 전자 투표를 총괄하는 선거 관리 위원회가 부정을 저지를 경우 투표 자체의 신뢰성은 무너지게 된다.

본 논문에서는 기존의 일반 투표를 전자 투표로 적용시키는 과정에서 어떠한 요소들이 필요한지 확인해 보고, 투표 매매 방지 및 선거 관리 위원회의 부정 방지를 위한 요구 조건을 살펴볼 것이다. 또한 기존의 전자 투표 방식들에 대해 고찰한 다음 더욱 효율적이고 안전한 전자 투표 방식을 제안한다.

I. 서 론

인류 문명의 발생과 함께 인간은 자신의 의사를 반영하기 위한 수단으로서 직·간접적으로 투표를 수행하여 왔다. 민주주의의 테두리 속에 사는 우리는 자신의 개성과 의사를 반영하는 여러 가지 형태의 '투표'를 통해 그 이상을 실현하고 있는 것이다. 일상 생활에서 투표는 작게는 일반 단체의 대표에서부터 크게는 대통령을 선출하는데 까지 광범위한 분야에 걸쳐 중요한 의사 결정 수단으로 사용되고 있다.

현행 투표 방식을 고려하면, 투표자가 소속된 투표소에까지 가서 직접 투표를 수행해야 한다는 전제 조건을 가지고 있다. 이것은 이중 투표를 막기 위한 하나의 방편으로서, 날씨가 안좋다던가 개인적으로 급한 용무가 생겨 자신의 투표구 외의 장소로 이동해야 할 경우에는 매우 번거로운 일로 취급되었던 것이 사실이다.

그러나 요즘은 인터넷과 같이 개방된 네트워크의 급속한 발전을 통해 우리의 실생활에 많은 변화를 가져오고 있다. 이러한 서비스를 전제로 앞에서 고려해 보았던 전자 투표를 실생활에 보급할 수 있다면 매우 유용하게 될 것이다. 즉, 투표소에서 수행하는 투표 작업이 자신의 사무실이나 역 그리고 공항 등의 공공 장소에 있는 컴퓨터를 이용하여 투표를 수행함으로서, 날씨나 장소에 구애받을 필요가 없기 때문에 일상 생활에 있어 매우 편리함을 제공하게 될 것이다.

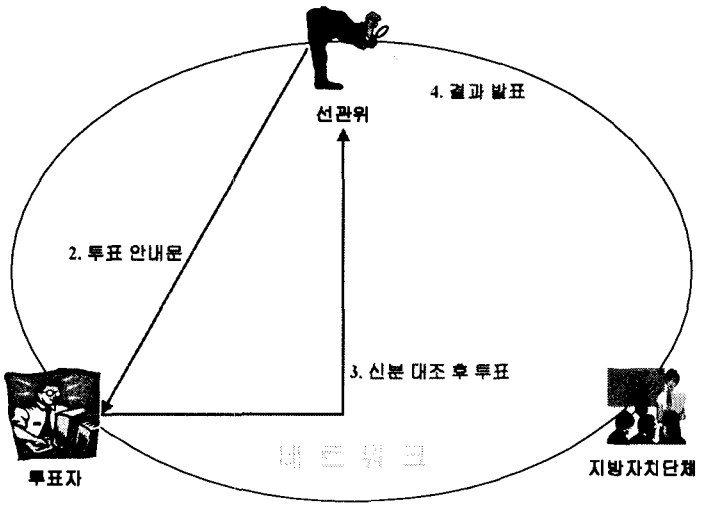

그림 1. 전자 투표에 대한 흐름도

물론 기존의 투표 방식에도 적은 부분에서 컴퓨터가 도입되고 있기는 하지만, 대다수의 모든 투·개표 작업이 인력을 통해 이뤄지므로 매우 비효율적이었다. 그러나 앞에서 고려해 보았던 전자 투표를 도입하게 된다면 투·개표 및 집계시 많은 부분들이 전자적으로 수행되므로 저렴하면서도 빠르고 정확하게 투표를 수행할 수 있다. 따라서 향후 이러한 전자 투표의 도입을 통해 투표 제도에 있어 획기적인 전환을 맞을 수 있게 될 것이다.

본 고에서는 전자 투표 상에서 요구되는 사항이 무엇이 있는지 살펴보고, 투표권 매매와 선관위 부정과 같이 안전한 전자 투표에 대해 위협이 되는 부정행위를 막기 위한 요구사항이 무엇인지 살펴본다. 또한 기존의 방식이 이러한 부정행위에 대해 어떻게 대처하고 있는지 알아 본 다음에 기존 방식이 안고 있던 몇몇 문제점을 고려하여 이를 해결할 수 있는 새로운 전자 투표 방식을 제안하려 한다.

II. 요구사항

전자 투표는 네트워크를 이용한다는 전제하에 암호 프로토콜의 주요 응용 분야가 되고

있다. 현재 훌륭한 전자 투표 프로토콜 [1]~[8]이 제시되어 있는 상황이다. 물론 안전성의 수준이나 효율성에는 많은 차이가 있지만 투표의 비밀성이나 결과의 정확한 집계 등과 같이 중요한 요구 조건을 만족하고 있다. 그러나, 이들 프로토콜은 투표 매매 및 선관위 부정과 같은 일부 사항에 대하여 완전하게 만족하지 않았으며, 이러한 측면에서 우리는 필히 확인을 해 보아야 할 것이다.

2.1 전자 투표의 요구사항

투표에 있어 가장 중요한 요소는 "비밀성"의 보장이다. 이는 투표자와 투표 내용의 연결성을 찾을 수 없다는 개념을 함축한 말로서, 기존 투표 형식에서는 '무기명 투표'를 통해 이를 보장하고 있다. 전자 투표의 경우에도 역시 일반 투표의 안전성은 보유해야 하며, 특히 비밀성, 투표권의 단일성, 투표권 인증성, 공평성, 위조 불가능성, 정확성, 투표 매매 방지성 그리고 선관위 부정 방지 기능이 보장되어져야 할 것이다.[13],[14]

물론, 이 외에도 많은 부분이 더 필요할 수 있다. 그러나 전자 투표를 고려할 경우, 특히 이중 투표 및 매매가 발생되어서는 안되며 비밀 투표를 보장하고 정확한 집계를 위해서 선관위의 부정을 방지해야 할 것이다. 다음은 전자 투표가 이루어 질 경우 어떤 문제점을 고려해야 하는지 살펴본 것이다.

2.2 전자 투표 매매 방지를 위한 요구 사항

전자 투표 시스템을 구현함에 있어 기존의 전자 투표 방식들은 투표자가 자신의 투표 결과를 다시 확인할 수 있게끔 하고 있다. 물론 이러한 절차는 자신의 투표 결과에 불법적인 변조가 없었다는 것을 확인하는 차원에서 꼭 필요한 요소가 될 것이다. 그러나, 전자적 매체의 특성상 확인 과정을 통해 투표자는 제 3자에게 자신의 투표 결과를 쉽게 확인시킬 수 있게 되고, 이를 통해 투표 매매를 부추길 수 있는 소지가 발생한다. 따라서 자신의 비밀 투표성을 보장하고, 투표 매매를 예방할 수 있는 방안이 필요하게 된다. 다음은 전자 투표 매매 방지를 위한 요구 사항들을 기술한 것이다. [11],[13]

1) 투표자는 자신의 투표 결과를 확인 할 수 있어야 한다.
2) 투표자 이외의 어느 누구도 투표자와 투표내용을 대응시킬 수 없다.
3) 제 3자는 투표자의 도움없이는 결코 투표 결과를 확인 할 수 없다.

2.3 선관위의 부정 방지를 위한 요구 사항

전자 투표 방식에서 선관위는 투표 안내, 투표, 투표 집계, 투표 감독 등의 기능들을 수행하며, 이를 통해 비용 및 시간의 효율성을 높이게 된다. 이것을 또 다른 의미로 해석

한다면, 선관위가 부정을 저지를 경우 전자 투표는 무용지물이 됨을 의미한다. 따라서 전자 투표에 있어 이러한 선관위의 부정이 발생하지 않도록 하는 것이 무엇보다 중요한 부분일 것이다. 다음은 전자투표 상에서 선관위의 부정을 방지하기 위한 요구조건을 기술한 것이다. [1],[14]

1) 투표자는 자신의 투표 결과를 확인 할 수 있어야 한다.
2) 선관위는 미등록 투표자의 투표권을 행사할 수 없어야 한다.
3) 선관위는 투표자의 투표결과를 수정할 수 없어야 한다.
4) 선관위에서는 투표자와 투표내용을 대응할 수 없어야 한다.
5) 선관위는 독립적이며, 투표의 집계는 정확하게 수행되어야 한다.

III. 기존 방식의 분석

3.1 Niemi - Renvall 방식 분석[11],[13]

Niemi - Renvall방식은 실제 사용하기에 이상적인 조건들을 부가적으로 기술하고 있다. 또한, 투표자 자신의 식별자를 생성할 때 투표 확인자의 비밀 랜덤 수가 삽입됨으로서, 그 어느 누구에게도 자신의 식별자를 확인하지 못하게 하는 투표 매매 방지책을 제시하고 있다. 그러나, 이 방식에서는 한가지 중요한 점을 놓치고 있다. 다음은 그에 대한 문제를 기술하고 있다.

투표 매매가 성립되었다고 가정할 경우, 매매자는 투표자가 투표를 마친 후 식별자를 정직하게만 얻는다면 투표자의 투표 결과를 믿을 수 있을 뿐만 아니라, 매매가 이루어 질 수도 있다. 즉, 투표자가 투표소를 나오자마자, 자신의 식별자를 매매자에게 제공하기로 계약을 맺을 경우 투표자는 자신의 식별자가 정확히 어떻게 만들어 졌는지를 증명할 수는 없지만, 자신의 식별자를 정직하게 매매자에게 알려 주게 됨으로서 매매자는 쉽게 투표자의 투표내용을 확인하게 된다. 이러한 사실은 투표 결과에 대한 식별자가 공표 되므로, 투표자가 매매자와의 계약을 어쩔수 없이 따라야 하는 취약성을 제공한다 하겠다.

3.2 Park-Itoh-Kurosawa 방식[1],[14]

Park -Itoh -Kurosawa방식(이하 PIK 방식)은 익명 통신로를 전제로 하고, 다중 프로토콜에 기초하고 있다. 또한 안전한 투표를 위해서 다수의 선관위를 둔다. 투표의 부정적인 요소나 행위가 발견되면, 투표를 멈추거나 완료시킬 수 있게 되어 있으며, 선관위들 중에서 1/2정도가 부정을 저지르지 않을 경우에는 투표를 정확히 계수할 수 있게끔 구성되어 있다.

PIK 방식은 공개 보드를 사용하기 때문에 선관위가 투표자의 투표값를 위조하거나 변

경할 수 없다는 장점을 가지고 있다. 또한 익명 통신로를 사용하기 때문에 투표값과 투표자를 연결시킬 수 없다는 특징을 가지고 있다. 그러나 이 방식은 선관위의 1/2이상이 결탁 할 경우, 투표 결과값을 인증할 방법이 없기 때문에 투표의 공정성은 무너지게 된다. 뿐만 아니라 투표자들은 자신의 공개키와 투표값만을 알 수 있기 때문에, 투표 미등록자에 대해서 선관위가 투표권을 행사할 경우 그 부정을 확인할 수 있도록 하는 방안이 필요하다.

Ⅳ. 새로운 부정 행위 방지 전자 투표 방식 제안

본 고에서 제안하려는 방식은 앞에서 살펴보았던 두 가지 방식들이 안고 있었던 취약점들을 극복하기 위하여 다음과 같은 특징을 갖는다.[13],[14]

첫째로, 일인당 투표 공란을 두 개 만들어 매매자에게 투표자 자신의 식별자와 투표 결과 모두를 알려 준다 하여도, 투표자가 어떤 공란에 투표를 하였는지 모르게 함으로서 투표 매매를 방지할 수 있다.

둘째로, 투표소의 기능을 강화하여 선관위가 집계시 저지를 수 있는 부정을 감시하도록 함으로서 선관위의 부정을 방지할 수 있다.

4.1 시스템 계수

본 방식에서 사용하는 시스템 계수는 다음과 같다.

- r_{i1}, r_{i2} : 은닉 서명 비밀 계수들($r_{i1} * r_{i1}' = 1 \bmod n$, $r_{i2} * r_{i2}' = 1 \bmod n$)[9]
- A_1, A_2, ... A_n : 선관위
- V_i : 투표자 i (i = 1, 2, ..., n)
- A_s, A_p : 선관위의 비밀키와 공개키
- A_{sj}, A_v : 선관위의 투표 확인용 분배 비밀키들과 공개키(Secret Sharing 사용, j = 1, 2, ..., k)
- G_s, G_p : 투표소의 비밀키와 공개키
- v_{i1}, v_{i2} : 투표자가 선택 가능한 두 개의 투표값 (집계시에는 둘 중에 하나만이 등록된다.)
- R_{i1}, R_{i2} : 투표자가 생성하는 랜덤 수
- ID_i : 투표자 i의 세션 ID
- H : 일방향 해쉬 함수
- $H(Sig_i)$: 투표자 i의 서명을 해쉬한 값

4.2 제안 프로토콜

• Registration Phase

1) 선관위는 투표 대상자들을 확인하여 선거인 명부를 만들고, 투표자 및 투표소에 공표한다.

2) 각 투표자는 등록과정을 통해 선관위 및 투표소로부터 자신을 인증하고, 랜덤한 세션 ID를 등록한다. (은닉 서명 사용)[9]

· 투표자는 은닉 서명 비밀 계수 r_{i1} 및 r_{i2}를 선택해 세션 ID를 숨겨서 선관위 및 투표소에 보낸다.

: $r_{i1}(ID_i)$를 생성해 선관위에 전송한다.

: $r_{i2}(ID_i)$를 생성해 투표소에 등록한다.

3) 전송되어온 데이타에 대하여 선관위는 공동으로 인증을 수행한 후, 대표 비밀키로 서명한 뒤 투표자에게 전송하며, 투표소 역시 인증을 수행한 후 자신의 비밀키로 서명한 다음 투표자에게 제공한다.

· $A_s(r_{i1}(ID_i))$, $G_s(r_{i2}(ID_i))$ ==> 투표자

4) 투표자는 선관위와 투표소로부터 받은 서명들을 확인한다.

· 투표자는 자신의 비밀 계수를 제거하여 선관위의 서명이 붙은 자신의 식별자 S_A와 투표소의 서명이 붙은 S_G를 얻는다.

$$r_{i1}'(A_s(r_{i1}(ID_i))) = A_s(ID_i) = S_A,$$

$$r_{i2}'(G_s(r_{i2}(ID_i)) = G_s((ID_i)) = S_G$$

· 선관위의 공개키 A_p과 투표소의 공개키 G_p을 이용하여 서명을 확인하고, 자신의 식별자가 정확히 등록되었는지 확인한다.

$$A_p(S_A) = A_p(A_s(ID_i)) = ID_i, \quad G_p(S_G) = G_p(G_s((ID_i)) = ID_i$$

• Voting Phase

5) 투표일이 되면 투표자는 투표소에서 물리적으로 자신을 확인하고 투표를 수행한다. (선관위 및 투표소의 공개키를 이용해 내용을 암호화한다.)

· 1차 선택만을 투표값으로 선택할 경우

: 투표자는 2차 선택을 하지 않으므로 자신의 1차 선택 값 FIR와 Dummy값 DUM을 다음과 같이 생성한다.

$(v_{i1}||R_{i1})$ = FIR, $(ID_i||R_{i2})$ = DUM (단, R_{i1}, R_{i2}는 투표자가 선택한 랜덤값이다.)

: 해쉬 함수 H를 이용해 다음을 계산한다. (단, $H(Sig_i)$는 투표자의 서명을 해쉬한 값이다.)

$H(FIR||DUM||H(Sig_i)) = J$

: 투표자는 자신의 1차 선택값 FIR, Dummy값 DUM 그리고 자신의 서명을 해쉬한 값 $H(Sig_i)$를연접해 선관위의 공개키로 암호화한다.

$A_v(FIR||DUM||H(Sig_i)) = E$

- 2차 선택을 투표값으로 선택하는 경우

: 투표자는 1차 선택값 FIR와 2차 선택값 SEC를 다음과 같이 생성한다.

: $(v_{i1}||R_{i1})$ = FIR, $(v_{i2}||R_{i2})$ = SEC (단, R_{i1}, R_{i2}는 투표자가 선택한 랜덤값이다.)

: 해쉬 함수 H를 이용해 다음을 계산한다.

$H(FIR||SEC||H(Sig_i)) = K$

: 투표자는 1차 선택값 FIR, 2차 선택값 SEC 그리고 자신의 서명을 해쉬한 값 $H(Sig_i)$를 연접해 선관위의 공개키로 암호화한다.

$A_v(FIR||SEC||H(Sig_i)) = E'$

- 투표자는 투표소와 선관위의 서명을 암호 결과값(E 또는 E')과 연접해 전송한다.

: 투표자가 1차 선택만 수행했을 경우에는 $S_A||E$를 선관위에게 전송하고, $S_G||J$를 투표소의 DB에 저장한다. 2차 선택을 수행했을 경우에는 $S_A||E'$을 선관위에 전송하고, $S_G||K$를 투표소의 DB에 저장한다.

- **Conviction Phase**

6) 선관위 및 투표소는 자신들의 비밀키를 이용해 복호화 한 뒤, 서명을 확인함으로 투표 결과를 확인한다.

- 선관위 및 투표소는 자신들의 공개키로 서명을 확인한다.

$A_p(S_A) = ID_i$, $G_p(S_G) = ID_i$

- 선관위는 자신들의 분배 비밀키들로 투표 정보를 복호화 한다.

$A_{sj}(E) = A_{sj}(A_p(FIR||DUM||H(Sig_i)))$

$= FIR||DUM||H(Sig_i)$ (투표자가 1차 선택을 수행하여 전송한 경우)

$A_{sj}(E') = A_{sj}(A_p(FIR||SEC||H(Sig_i)))$

$= FIR||SEC||H(Sig_i)$ (투표자가 2차 선택을 수행하여 전송한 경우)

- 선관위는 결과를 투표소의 공개키로 암호화해 전송한다. 투표소는 선관위로부터 수신된 투표 정보를 다음과 같이 자신들의 비밀키로 확인한 후 해쉬를 취한다. 그런 다음 DB에 저장된 내용과일치하는지 비교한다.

$G_s(G_p(FIR||DUM||H(Sig_i)))$ = $FIR||DUM||H(Sig_i)$(투표자가 1차 선택을 수행했을 경우)

==> $H(FIR||DUM||H(Sig_i)) = J$ (같다면 정당한 투표값으로 인정한다)

$G_s(G_p(FIR||SEC||H(Sig_i))) = FIR||SEC||H(Sig_i)$(투표자가 2차 선택을 수행했을 경우)

==> $H(FIR||SEC||H(Sig_i)) = K$ (같다면 정당한 투표값으로 인정한다)

- 투표자가 1차 선택만을 수행했을 경우 R_{i1}을 생략한 뒤 v_{i1}과 $H(Sig_i)$가 연접되어 집계에 들어간다. 그리고, 투표자의 투표 결과를 제 3자에게 노출시키지 않기 위하여 $ID_i||R_{i2}$를 해쉬하여 연접한다.

  $ID_i||v_{i1}||H(Sig_i)||H(ID_i||R_{i2})$

- 투표자가 2차 선택까지 수행하게 되면, v_{i2}가 집계에 들어간다. 그리고, 결과를 다음과 같이 작성한다. 이때 1차 선택 결과는 2차 선택 결과와 내용이 같아서는 안되며, 제 3자로부터 투표자의 투표결과를 노출시키지 않기 위해서 다음과 같이 작성한다.

  $ID_i||v_{i1}||H(ID_i||H(Sig_i)||H(v_{i2}||R_{i2}))$

- **Opening Phase**

7) 선관위에서는 투표자의 투표 결과를 저장하고, 공개 보드 상에 공표한다.

- 1차 선택만 수행했을 경우

  : $ID_i||v_{i1}||H(Sig_i)||H(ID_i||R_{i2})$가 저장되고, 투표값 v_{i1}이 집계 결과가 된다. 이 때 공개 보드 상에는 투표자의 투표값에 따라 후보자의 득표수가 Counting되어 공표된다.

- 2차 선택을 수행했을 경우

  : $ID_i||v_{i1}||H(ID_i||H(Sig_i)||H(v_{i2}||R_{i2}))$가 저장되며, 투표값 v_{i2}가 집계 결과가 된다. 이 때 공개 보드상에는 투표자의 투표값에 따라 후보자의 득표수가 Counting되어 공표된다.

8) 투표자는 자신의 투표 결과를 확인한다.

- 1차 선택만을 수행한 경우에는 v_{i1}만 확인하면 되며, 투표 매매에 대한 방지책을 사용한 투표자는 2차 선택까지 수행했기 때문에 자신의 식별자와 2차 선택값 그리고, 자신이 생성한 랜덤수를 결합해 해쉬한 값을 투표 결과 list와 비교함으로써 자신의 투표 결과 v_{i2}가 집계되었음을 확인한다.

  $ID_i||v_{i1}||\mathbf{H(ID_i||H(Sig_i)||H(v_{i2}||R_{i2}))}$==> $H(ID_i||H(Sig_i)||H(v_{i2}||R_{i2}))$

4.3 제안 방식 고찰

본 제안 방식은 은닉 서명을 이용한 예비 등록 절차를 통해 자신의 식별자를 등록하게 끔 함으로서 투표자와 ID_i를 연결시킬 근거를 없애고 있다. 또한 투표소에서 투표를 수

행함으로서 물리적 확인을 통해 1인 1투표가 가능하며, 제 3자가 대리 투표를 하거나, 위조와 같은 부정적인 방해를 수행할 수 없다는 장점을 가지고 있다. 그와 함께, 투표가 끝난 후에 투표 결과를 공표함으로써 제 3자로부터 투표 결과에 따라 자신의 투표를 결정할 아무런 근거도 갖지 못한다. 그리고 투표를 관할하는 선관위를 보조하는 투표소들의 기능을 강화함으로써, 집계의 공정성을 확보하였으며 제 3자와의 결탁을 방지할 수 있다.

본 제안 방식은 이와 함께, 다음과 같은 부정 유형에 대해 대응함으로서 선관위의 부정한 시도 및 전자 투표 매매에 대한 방지책을 제시하고 있다.

- 부정 유형 1) 선관위가 투표자의 투표 결과를 위조하거나 수정하려 시도할 경우
  => 투표자가 투표를 수행한 후에 투표자의 투표값 v_{i1} 또는 v_{i2}가 집계 결과로서 저장되게 된다. 따라서, 투표값이 변경된다면, 투표자는 투표 결과에 따른 자신의 투표값을 확인함으로써 선관위의 부정을 방지할 수 있다.

- 부정 유형 2) 선관위 및 투표소에서 투표 미등록자의 투표권을 행사하려 시도할 경우
  => 모든 투표자는 투표 수행시 자신의 서명을 해쉬하여 연접하기 때문에, 선관위가 임의의 제 3자를 통해 투표 미등록자의 투표권을 행사하려 한다 해도 투표자의 서명 값을 생성하지 못하기 때문에 투표 집계시 부정을 검출할 수 있다.

- 부정 유형 3) n-1개의 선관위와 투표소가 결탁할 경우
  => 투표자의 식별자 ID_i에 대해 선관위들이 모두 동의한 상태에서 확인 서명을 부여하게 되므로 이러한 부정은 힘들게 된다.

- 부정 유형 4) 투표 매매자가 투표자의 식별자 ID_i를 요구하여 결과를 확인할 경우
  => 투표자는 2차 선택을 수행한 후에 ID_i를 매매자에게 제공하게 되면, 매매자는 v_{i1}이외의 어떤 정보도 알 수 없으므로 매매가 성립한 것으로 간주한다.

- 부정 유형 5) 투표 매매자가 투표자의 2차 선택 유무를 의심할 경우
  => 투표자는 1차 투표에서 사용되는 랜덤값 R_{i1}대신에 $H(v_{i2}||R_{i2})$를 적용함으로서 자신은 1차 선택만 수행했다고 주장할 수 있다.

- 부정 유형 6) 투표 매매자가 투표자의 모든 시스템 계수를 다 요구할 경우
  => 투표자는 1차 선택에서 사용되는 랜덤값 R_{i1}대신에 $H(v_{i2}||R_{i2})$의 결과값을 매

매자에게 제공함으로서 계산상으로 투표 매매자는 2차 투표를 수행했는지에 대한 아무런 이상을 느끼지 못한다.

• 부정 유형 7) 투표 매매자가 투표자에게 2차 선택을 요구하면서, 자신의 의뢰인을 부탁할 경우

=> 투표자는 1차 선택만을 수행하면서, R_{i1}대신에 요구된 $H(v_{i2}||R_{i2})$를 계산하여 연접한다. 이때 집계시에는 자신이 의도한 1차 선택 결과를 얻으면서, 매매자는 마치 2차 선택이 이루어진 것으로 생각하기 때문에 아무런 이상을 발견하지 못하게 된다.

이상과 같이 투표소의 기능을 강화함으로서 선관위의 위조나 결탁을 통한 부정은 무의미하게 되므로 선관위의 부정을 예방할 수 있다. 뿐만 아니라 매매자가 투표자에게 투표 매매를 의뢰한다 할 지라도, 투표 결과는 투표자의 의사에 달려 있으므로, 투표 매매 의뢰는 무의미하게 되고 이를 통해 투표 매매를 예방할 수 있겠다.

V. 결론

현재 의사 결정의 수단으로서 제시되어진 투표는 그 성격상 매우 미묘한 문제가 되기 때문에 그 어떤 상황에서도 부정의 소지가 있어서는 않된다. 전자 투표의 경우도 예외는 아니며, 사람과 사람이 직접 만나지 않고 프로토콜이 수행되기 때문에 그만큼 투표의 안전성은 무엇보다 중요하게 된다. 이에 대해 본고에서는 다가올 미래에 사용 가능성이 매우 높은 전자 투표에 대해서 그 필요성과 요구사항을 제시하였다.

그와 함께, 전자 투표상에서 발생할 수 있는 선관위의 부정에 관하여 기존의 방식 중에 하나인 PIK 방식이 어떻게 대처하는지에 대해 살펴보았다. 동시에 전자 투표에서 발생할 수 있는 투표 매매에 관해서 Niemi - Renvall이 제안한 투표 매매 방지책을 분석하였으며, 본 고에서는 선관위의 부정을 방지하면서 투표 매매를 예방할 수 있는 새로운 방식을 제안하였다.

본 제안 방식은 투표소가 물리적으로 안전하고, 투표소의 독립성이 보장될 경우 선관위가 투표자의 투표 결과를 위조하는 것을 막을 뿐만 아니라, 투표 미수행자들의 투표권을 이용해 부정을 저지를 수 없도록 구성하고 있다. 또한 제 3자의 강요 및 매수에 의해 투표를 수행하여야 할 경우 자신의 의사를 그대로 반영하면서도, 결코 그들이 자신의 투표 결과를 알지 못하도록 수행하고자 할 때 매우 유용하게 사용할 수 있는 방법을 제시하였다. 다음은 기존 방식들과 제안 방식을 비교 분석한 것이다.

표 1. 전자 투표 방식별 안전성 비교 분석

	비밀성	단일성	정확성	공평성	투표 미등록자 부정 방지	위조 불가능성	선관위 부정방지	매매 방지
Niemi-Renvall 방식	O	O	O	O	X	O	△	△
PIK방식	O	O	O	O	△	O	△	X
제안방식	O	O	O	O	O	O	O	O

* 본 연구는 정보통신부 98 대학기초연구사업의 연구비 지원에 의해 수행되었음.

VI. 참고 문헌

[1] C. Park, K. Itoh and K. Kurosawa, "Efficient anonymous channel and all/nothing election scheme," Proc. EUROCRYPT '93, Springer LnCS 765, pp.248-259, 1994.

[2] D. Chaum, "Elections with Unconditionally Secret Ballots and Disruptions Equivalent to Breaking RSA," Advances in Cryptology, Proceedings of EUROCRYPT '88, pp.177-181, 1988.

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

[4] H. Nurmi, A. Salomaa and L. santean, "Secret ballot elections in computer networks," Computers and Security 10, pp.553-560, 1991.

[5] J. Cohen and M. Fischer, "A Roubust and Verifiable Cryptographically Secure Election Scheme ," Proceedings of the 26th Annual IEEE symposium on the Foundations of Computer Scirence, pp.372-382, 1985.

[6] J. Benaloh, "Secret Sharing homomorphism : Keeping shares of a Secret," Advances in Cryptology, Proceedings of Crypto '86, pp.251-260, 1986.

[7] J. Benaloh, "Verifiable secret-ballot elections," Ph.D.thesis, Yale university,

Technical report 561, 1987.

[8] K. Iversen, "A cryptographic scheme for computerized general elections," Proc. CRYPTO '91, Springer LNCS 576, pp.405-419, 1992.

[9] D. Chaum, "Blind Signature for Untraceable Payments," Advances in Cryptology Proceedings of CRYPTO '82, pp.199-203.

[10] R. Rivest, A. shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the Association for Computing machinery, Vol, 21, No.2, pp120-126, 1978.

[11] V. Niemi and A. Renvall, "how to prevent buying of votes in computer elections," ASIACrypto '94 pp.164-170, 1994.

[12] W. Diffie and M. hellman, "New directions in cryptography," IEEE Transaction on Information Theory, Vol.22 No.6, pp.644-654, 1976.

[13] 박희운, 이임영, " 전자 투표 매매 방지에 관한 연구," 제 9회 한국정보처리학회 춘계 학술 발표 대회 논문집, 제 5권, 제 1호, 1998. 4.

[14] 박희운, 오형근, 이임영, " 전자투표에서의 선관위 부정방지에 관한 연구," 제 1회 멀티미디어학회 춘계 학술 발표 논문집, 제 1권, 제 1호, pp163-168, 1998. 6.