通信情報保護學會論文誌
第 8 卷 第 4 號, 1998. 12

전자투표상에서의 부정 행위 방지에 관한 연구

박 희 운*, 이 임 영*

A Study on Preventing Illegal Acts in Electronic Elections

Hee-Un Park, Im-Yeong Lee

요 약

정보화 사회를 거치면서 네트워크의 발전과 관련해 많은 응용 분야들이 연구되고 있는데, 그 중에서도 암호학을 이용한 전자 투표의 비중이 증대되고 있다. 이러한 전자 투표는 그 중요성에도 불구하고, 아직까지 취약한 점이 많이 산재해 있다. 특히, 전자 투표를 총괄하는 선거 관리 위원회가 부정을 저지를 경우 투표 자체의 신뢰성은 무너지게 되며, 투표권의 매매가 성립할 경우에는 전자 투표에 있어 치명적인 악영향을 미치게 된다.

따라서 본 논문에서는 기존의 투표를 전자 투표로 적용시키는 과정에서 어떠한 요소들이 필요한지 확인해 보고, 선거 관리 위원회의 부정 방지 및 투표 매매 방지를 위한 요구 조건을 살펴볼 것이다. 그리고 기존의 전자 투표 방식들이 이러한 위협 요소들에 대해 어떻게 대처하고 있는지를 고찰한 뒤에 더욱 효율적이고 안전한 전자 투표 방식을 제안한다.

Abstract

In our modern information society, many subjects related to computer networks are studied. The electronic election system based on cryptology is one of such subject, and the importance of the system is increasing rapidly. However, there are many issues to be resolved before the system can be applied in practice. Especially, when the central tabulating agency that controls the election system illegally manipulates the voting process, the outcome of the election will not be trusted. Also, if buying of votes is not prevented, the reliability of the system will be in question.

In this paper, we look into various elements involved in implementing the electronic election system. We especially focus on the requirements for making the system secure against various illegal attempts such as buying of votes and voting process manipulations. We investigate how the

본 연구는 98년 정보통신부 대학기초연구사업의 연구비 지원에 의해 수행되었음.
* 순천향대학교 공과대학 컴퓨터학부

conventional election system deals with the security problems, and then propose a safer and more efficient scheme for implementing the electronic election system.

Key word : Electronic Election, Central Tabulating Agency, Buying of Votes, Preventing Illegal Act, Cryptology

I. 서 론

인류 문명의 발생과 함께 인간은 끝없는 변화와 발전을 추구해 오고 있다. 인간은 사회라는 틀 안에서 모든 생활을 영위하며, 자신의 의사를 반영하기 위한 수단으로서 직·간접적으로 투표를 수행하여 왔다.

민주주의는 이러한 투표 방식을 모태로 인류 문명의 발전과 보조를 맞추어 왔으며, 인간은 자신의 개성과 의사를 반영하는 여러 가지 형태의 '투표'를 통해 더욱 성숙된 사회의 일원이 되는 것이다. 투표는 일상 생활에 있어 작게는 소수 모임의 대표에서부터 크게는 대통령을 뽑는 일 까지 다양한 분야에 걸쳐 현대 사회에 없어서는 안될 주요 수단으로 존재하고 있다.

한 예로 국회의원을 뽑는 투표를 가정하자. 우선 선거 관리 위원회(이하 선관위라 함)에서는 투표인 명부를 만들고, 투표 안내문을 발송한다. 투표일이 되면 투표자는 자신의 신분증을 가지고 투표소에 가서 자신이 투표권이 있음과, 이 투표구에 사는 사람이라는 것을 확인한다. 그런 다음에 투표자는 투표 용지를 받아 다른 사람의 간섭이 없는 기표소에서 투표를 수행하고, 이를 투표함에 넣는다. 하지만 이런 유형의 투표는 투표자가 투표소에까지 가서 직접 투표를 수행해야 한다는 전제 조건을 가지고 있다. 이것은 선거인 명부가 하나로 갖추어져 있어서 이를 복수화 할 경우 이중 투표를 막을 방법이 없기 때문에 만들어진 하나의 방편이다. 따라서, 날씨가 안좋다던가 개인적으로 급한 용무가 생겨 자신의 투표구 외의 장소로 이동해야 할 경우 현행의 투표 방식은 매우 번거로운 일로 취급되었던 것이 사실이다.

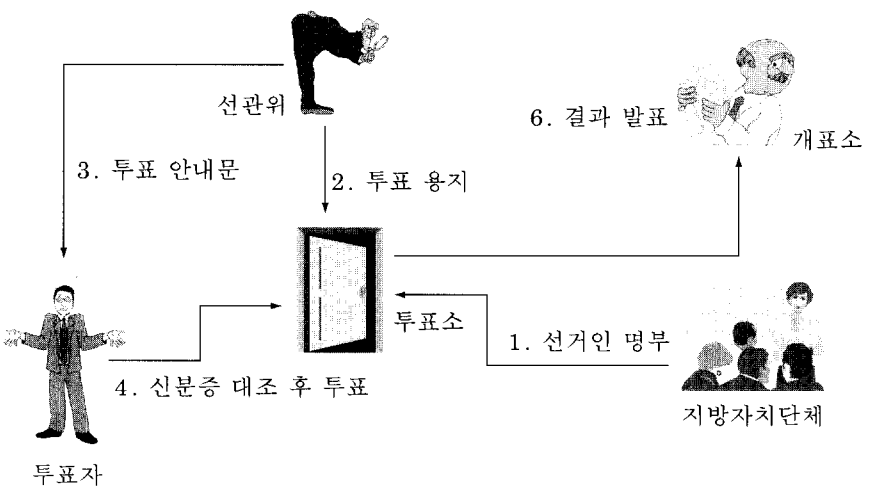


그림 1. 현행 투표에 대한 흐름도
Fig 1. Flowchart about conventional election

그러나 요즘은 인터넷과 같이 개방된 네트워크가 매우 급속한 발전을 하고 있으며, 초고속 통신망과 같은 고속화된 통신 매체가 구축되고 있다. 또한, 이러한 통신 매체의 발전을 통해 새로운 정보 서비스를 생활 안밖에서 보급받게 됨으로서 우리의 실생활에 많은 변화를 가져오게 될 것이다. 이러한 서비스를 전제로 앞에서 고려해 보았던 전자 투표를 실생활에 보급할 수 있다면 현행 투표 시스템이 안고 있던 많은 문제점들을 해결할 수 있을 것이다. 즉, 투표소에서 수행하는 투표 작업이 자신의 사무실이나 역 그리고 공항 등의 공공 장소에 있는 컴퓨터를 이용하여 전자투표로 행하여 질 수 있다면, 투표자는 날씨나 장소에 구애받을 필요 없이 투표를 할 수 있으므로 투표자의 불편함은 개선될 것이며, 일상 생활에 있어 매우 편리함을 제공할 것은 말할 나위도 없다.

뿐만 아니라, 현행 투표 방식에 있어 아주 적은 부분에서 컴퓨터가 도입되어 사용되고 있기는 하지만 아직까지는 선거의 투표, 개표 작업의 대부분이 사람의 손에 의존하고 있기 때문에 시간 및 비용 측면에 있어 비효율적으로 운용된 것이 사실이다. 그러나, 앞에서 고려해 보았던 전자 투표를 도입하게 된다면 투표와 개표 및 집계시 많은 부분들이 전자적으로 수행되므로 시간적인 측면에서 빠르면서도 정확하게 수행할 수 있고, 비용 측면에 있어 저렴하게 수행할 수 있는 장점이 생긴다. 따라서 향후 이러한 전자 투표의 도입은 투표 제도에 있어 획기적인 전환을 맞을 수 있게 될 것이다.

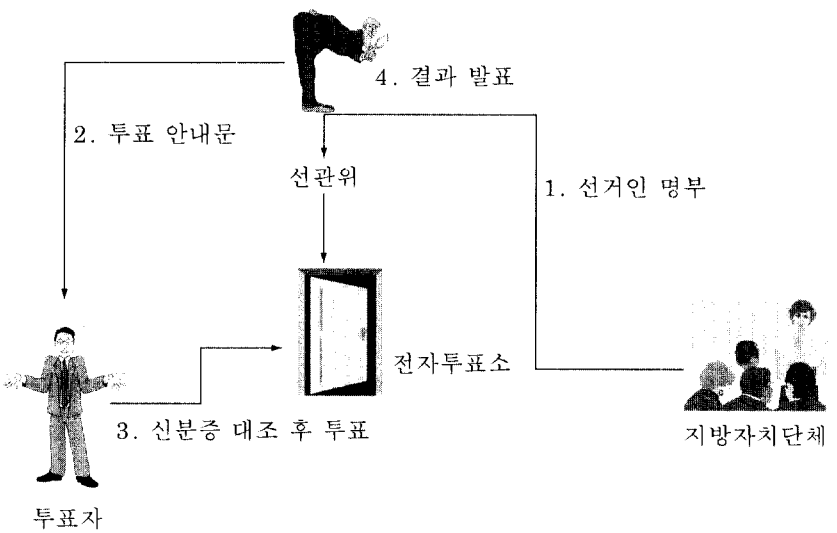


그림 2. 전자 투표에 대한 흐름도
Fig 2. Flowchart about electronic election

이에 대해 본 고에서는 전자 투표 상에서 요구되는 사항이 무엇이 있는지 살펴보고, 투표권 매매와 선관위 부정과 같이 안전한 전자 투표에 대해 위협이 되는 부정행위를 막기 위해 무엇이 필요한지 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

2.1 전자 투표의 요구사항

기존의 일반적인 투표 형식이 갖는 특성 중에서 특히 강조되는 요건을 하나 꼽는다면 '비밀 투표'를 들 수 있다. 이는 투표자와 투표 내용의 연결성을 찾을 수 없다는 개념을 함축한 말로서, 기존의 투표상에서는 '무기명 투표'를 통해 비밀성이 보장된 투표를 수행하고 있다. 전자 투표의 경우 그 특성 상 일반 투표의 성격을 그대로 보유하여야 하며, 특히 비밀성이 보장된 전자적 무기명 투표를 위해 필요한 요구 조건이 갖추어져야 할 것이다. 다음은 일반 투표를 고려할 때 전자 투표가 갖추어야 할 요구사항을 기술한 것이다.

1) 비밀성 : 투표자와 투표내용의 대응은 당사자만이 안다.
2) 투표권의 단일성 : 한 명의 투표자는 단 한번의 투표권만 가진다.
3) 투표권 인증 : 투표권이 있는 사람만이 투표를 수행할 수 있다.
4) 공평성 : 어느 누구도 다른 사람의 투표 결과를 통해 자신의 투표결과를 결정할 수 없다.
5) 위조 불가능성 : 제 3자에 의한 투표 결과의 변경은 불가능하다.
6) 정확성 : 투표 결과의 집계는 정확해야 한다.
7) 투표 매매 방지성 : 투표권 매매로부터 투표자를 보호할 수 있어야 한다.[11][13]
8) 선관위 부정 방지 : 선관위가 부정을 예방할 수 있는 안전한 장치가 있어야 한다.[11][13]

물론, 이 외에도 많은 부분이 더 필요할 수 있다. 그러나, 이들 요구 사항 중에서 더욱 중요한 사항을 꼽으라 한다면, 이중 투표 및 매매가 발생되어서는 안되며, 비밀 투표를 보장하고 정확한 집계를 위해서 선관위의 부정을 방지해야 할 것이다. 이는 기존의 투표에서도 필히 요구되는 사안이기에 전자 투표 구현시 깊은 통찰이 요구된다. 본고에서는 특히 전자 투표가 이루어 질 경우 매매 및 선관위의 부정을 방지하기 위해 어떠한 요구 사항이 필요한지 분석하였으며, 기존의 방식들이 이러한 요구 사항에 대해 어떻게 대처하는지 살펴 본 다음에 이들 부정 행위를 차단할 수 있는 새로운 방식을 제안한다. 그렇다면 전자 투표가 이루어 질 경우 어떤 문제점을 고려해야 하는지 살펴보자.

2.2 전자 투표 매매 방지를 위한 요구 사항

전자 투표는 네트워크를 이용한다는 전제하에 암호 프로토콜의 주요 응용 분야가 되고 있다. 현재 여러가지 훌륭한 전자 투표 프로토콜이 제시되어 있는 상황이다.[1]-[8] 물론 안전성의 수준이나 효율성에는 많은 차이가 있지만 투표의 비밀성이나 결과의 정확한 집계 등과 같이 앞에서 언급했던 중요한 요구 조건을 만족하고 있다. 그러나, 이들 프로토콜은 다음과 같은 사항을 고려하지 않았으며, 이러한 측면에서 우리는 필히 확인을 해보아야 할 것이다.

기존의 일반 투표 형식을 전자 투표 형식으로 전이시키면서 기존의 방식들은 투표 수행 과정에서 자신의 투표결과를 다시 확인할 수 있게끔 하고 있다. 물론 이러한 절차는 전자 투표를 수행함에 있어 자신의 투표 결과에 불법적인 변조가 없었다는 것을 확인하는 차원에서 꼭 필요한 요소가 될 것이다. 그러나, 전자적 매체의 특성상 확인 과정을 통해서 투표자는 제 3자에게 자신의 투표 결과를 쉽게 증명할 수 있게 되고, 이를 통해 비밀 투표성을 해칠 우려가 발생한다. 결국, 이러한 확인 절차는 전자 투표 매매를 부추길 수 있는 소지가 될 수 있기 때문에 자신의 비밀 투표성을 보장하면서도, 전자 투표 매매를 예방할 수 있는 방안이 필요하다. 다음은 전자 투표 매매 방지를 위한 요구 사항들을 기술한 것이다.[11][13]

1) 투표자는 자신의 투표 결과를 확인 할 수 있어야 한다.
2) 제 3자는 투표자의 도움 없이는 결코 투표 결과를 확인 할 수 없다.
3) 선관위에서는 투표자와 투표내용을 대응시킬 수 없다.
4) 선관위는 독립적이며, 투표에 관련된 어떠한 부정도 저질러서는 않된다.

2.3 선관위의 부정 방지를 위한 요구 사항

현행 일반 투표 방식들은 투표 안내, 투표, 투표 집계, 투표 감독 등의 기능들이 분할되어져 있다. 이와 같이 나누는 목적은 투표 상에서 부정적인 요소들을 제거하는데 있다. 즉 투표 관리 기구를 분할하여 서로를 감시함으로서 누군가의 부정적인 행위가 발생했을 때 이들을 제어할 뿐만 아니라 안전한 투표를 이룰 수 있기 때문이다. 이를 전자 투표로 구현할 경우, 시간과 비용을 줄이기 위해 통일된 기관이 존재하게 되는데 바로 이것이 선관위가 된다. 따라서 선관위의 역할이 방대해지는데 다음은 전자투표 상에서 선관위의 역할을 기술한 것이다.

1) 투표 안내 : 투표의 일시 및 투표권자의 리스트를 공표한다.
2) 투표자 인증 : 투표권이 있는 사람들을 확인함으로서 1인 1투표가 가능하게끔 한다.
3) 투표 결과 확인 : 전송되어 온 투표값을 확인하여 위조 및 복사에 대응한다.
4) 집계 : 투표 결과를 확인하여 집계하는 것을 관할한다.
5) 투표 결과 공표 : 집계 결과를 공표한다.

이상과 같이 전자투표 상에서 선관위의 기능이 상당히 강화되었음을 알 수 있다. 이것을 또 다른 의미로 해석한다면, 선관위가 부정을 저지를 경우 전자 투표는 아무런 소용이 없게 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.[10][11]

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 수행해야 한다.

III. 기존 방식의 분석

3.1 Niemi - Renvall 방식[11]

이 방식은 부분적인 제약 사항을 통해 투표자가 투표 결과에 따르는 식별자를 다른 사람에게 증명할 수 없게 함으로써 투표 매매를 방지하는 형식을 취하고 있다. 본 장에서는 Niemi-Renvall 방식에서 요구하는 부가적 사항을 기술하고, 투표 프로토콜을 살펴본 뒤 그 문제점을 지적하려 한다.

3.1.1 요구 사항

이 방식은 기존의 전자투표에서 요구하는 것 외에도 여러 가지 부가적인 사항을 요구하는데, 다음은 그 중 특징적인 것들을 정리한 것이다.

1) 각 투표자는 예비 등록을 수행해야 한다.
2) 투표소와 같이 물리적으로 통제된 환경하

에서 실시해야 한다.

3) 투표의 정확성은 안전한 등록 투표소에서 ZKIP으로 증명되어 진다.

4) 투표 확인의 공정성을 위해 투표를 관할하는 센터는 n개로 분할한다.

3.1.2 시스템 계수

이 방식에서 사용하는 시스템 계수는 다음과 같다.

- Vi : 투표자 (i = 1, ..., n)
- $[v_i]$: 투표자의 투표값
- f(x) : 투표자의 식별 정보
- vi = ($[v_i]$, f(x)) : 투표 결과
- s_i : 투표 확인자(선관위)가 생성하는 랜덤수
- $s = s_1 ... s_n$: 투표 확인자의 비밀 세션 키
- x : $x = z_1 ... z_{4n}$ 에 속하는 정수로서 투표 확인자(선관위)가 생성 (단, i = {n+1, n+2, ... 3n} 일 때 z_i는 0 비트가 되어야 함)
- f : $x \rightarrow x^e \pmod p$: zero-way permutation함수 (단, p는 솟수.)
- e, d : 투표 확인자의 공개키와 비밀키
- C_j : 투표 확인자(선관위) (j = 1, ..., n)

3.1.3 프로토콜

1) 투표 준비
   - 투표 확인자 C_j(j = 1, ..., n)는 사용 알고리즘을 결정하고, 랜덤수 s_{kj}와 비밀 세션 키 $s = s_1 ... s_n$을 생성한 후, 자신의 공개키와 비밀키를 생성한다.
     : (e, d) (단, e는 공개키이며, d는 비밀키이다.)

2) 투표를 수행하기 위해 투표소에서는 투표자 인증을 실시한다.
   - 투표자는 물리적으로 식별되어야만 투표소에 입장 할 수 있게 된다.

3) 투표 확인자는 투표자에게 식별자를 부여한다.
   - 투표자는 다음과 같이 식별자 f(x)를 만드는데, s의 값은 오직 투표 확인자만이 알고 있으므로 투표자는 결코 어느 누구에게도 부여된 식별자가 어떻게 생성되었는지 그 유효성을 증명할 수 없다.
     $f(x) = x^e \pmod p$[5]

4) 투표 수행
   - 투표자 Vi는 투표 결과 vi를 다음과 같이 생성해 투표 확인자의 공개키로 암호화해 전송한다.
     vi = ($[v_i]$, f(x)) ($[v_i]$는 투표 결과를 의미하며, f(x)는 투표자의 식별자이다.)
     $e(vi) = e([v_i], f(x))$[10]

5) 투표 집계 단계
   - 투표 확인자는 자신의 비밀키로 투표 내용을 복호화 하여 투표 결과를 공개 보드상에 공표한다.
     $d(e[v_i]) = d(e([v_i], f(x))) = ([v_i], f(x))$

3.1.4 Niemi - Renvall 방식 고찰

기존에 제안된 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 논문에서는 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 나오자 마자 자신의 식별자를 매매자에게 제공하기로 계약을 맺을 경우, 투표자는 자신의 식별자가 정확히 어떻게 만들어 졌

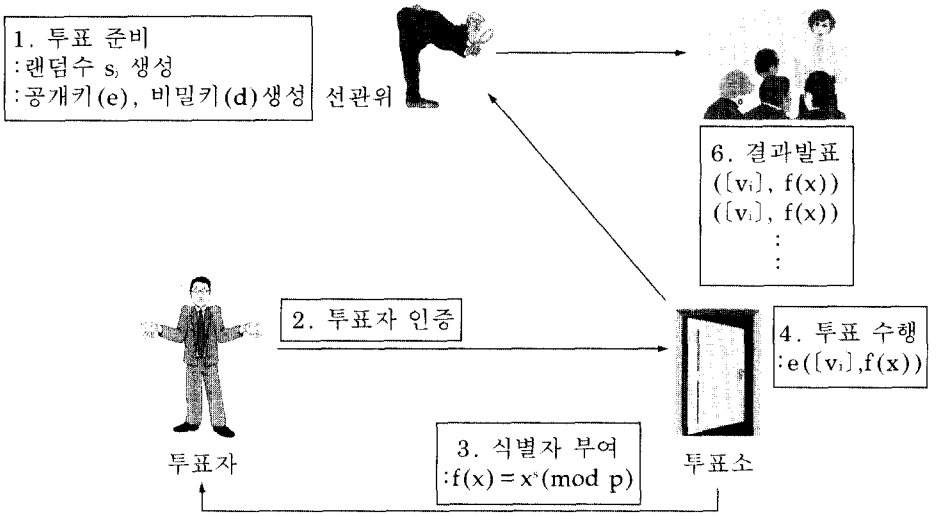


그림 3. Niemi-Renvall 방식
Fig 3. Niemi-Renvall method

는지를 설명할 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 어쩔 수 없이 따라야 하는 취약성을 제공한다 하겠다.

3.2 Park-Itoh-Kurosawa 방식[1]

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 1/2이상이 부정을 저지르지 않을 경우에는 투표를 정확히 계수할 수 있게끔 되어 있다.

3.2.1 시스템 계수

PIK방식에서 사용되는 시스템 계수는 다음과 같다.

- g : GF(q)상의 생성자 (단, q는 큰 소수)
- S_m : 다수로 구성된 선관위 (m = 1, 2, ..., k)
- X_m, Y_m : 각 선관위의 비밀키와 공개키
- P_i : 투표자 (i = 1, 2, ..., n)
- k_i, k_i^{-1} : 투표자의 공개키와 비밀키
- V_i : 투표값
- h : 일방향 해쉬 함수
- Z_i : 변수
- ‖ : 연접 연산
- 0^l : 0이 l개 연속되어 있는 것
- P_l : 공개 보드상의 최신 리스트

3.2.2 투표 프로토콜

- **Main protocol**

<Initial Phase>

1) 선관위 S_m은 자신의 비밀키 X_m을 VSS

(Verifiable Secret Sharing Scheme)를 이용해 다른 $\{S_i\}$에게 분배한다.[6] 만약 k/2 이상의 $\{S_i\}$가 모이면, 그들은 X_m을 복구할 수 있다. (단, k는 S_i의 수)

2) 투표자 P_i는 자신의 공개키와 비밀키(k_i, k_i^{-1})를 선택한다. 그리고 자신의 공개키를 공개한다.

3) 공개키 리스트가 공개 보드에 사전 편찬순으로 저장된다. $\{k_i\} = (k_1, k_2, ..., k_i)$

<Claiming phase>

4) 각 투표자는 공개 보드에서 자신의 공개키를 확인한다.[12] 만약 이상이 있으면, 투표자는 이의를 신청하고 투표는 중지된다. 그렇지 않을 경우에는 다음 단계로 넘어간다.

<Voting phase>

5) 투표자 P_i는 두 개의 랜덤수를 만들어 EXOR하여 투표값을 생성한다.
$V_i = R_{i1} \oplus R_{i2}$

6) 각 투표자는 익명 통신로를 이용해 다음을 전송한다.
$a_i = (k_i \| k_i^{-1}(R_{i1} \| 0^l))$
$b_i = (k_i \| k_i^{-1}(R_{i2} \| 0^l))$

7) Subprotocol 1이 수행된다.

<Testing phase>

Subprotocol 1이 수행된 후에 공개 보드에는 $(A_1, B_1), (A_2, B_2), ..., (A_n, B_n)$과 같은 리스트가 존재한다.

8) A_i 또는 B_i가 랜덤하게 선택된다. (단, i = 1, 2, ..., n)

9) subprotocol 2에 의해 선택되어진 것은 공개되며 그 결과값은 $u_i = (t_i \| w_i)$와 같은 형태를 취한다.

10) 모든 사람들은 $t_i = (k_i, t_i \| w_i)$의 마지막 부분이 0^l인지 확인한다.

11) 10)단계에서 이상이 없으면, 다음 단계로 가고 그렇지 않으면 멈춘다.

<Opening phase>

12) 남은 각 i에 대해 <Testing phase>의 9), 10) 단계를 수행한다.

13) 아무 이상도 발견되지 않으면, $\{V_i\}$ 리스트를 수용한다.

• Optional Protocol

$(q, g, Y_m, a_1, ..., a_n, Z_1, ..., Z_n)$가 공개 보드에 등록되어 있을 때 $X_m (m = 1, ..., k)$를 참고하여 다음 식이 나온다.

$Y_m = g^{X_m} \bmod q$

$Z_i = Y_m^{r_i} (=g^{r_i}) \bmod q \ (i = 1, ..., n)$

1) 각 선관위는 영지식 증명(ZKIP)을 이용해 위의 수식을 확인한다.

2) 각 선관위는 subprotocol 1에서 사용했던 랜덤수를 공개한다.

3) 만약 S_m이 오류를 범한 것으로 판명되면 나머지 선관위가 VSS를 이용해 X_m을 복구한다.

4) X_m을 이용해 오류가 발생되었던 모든 투표값이 복구된다.

• Subprotocol 1

1) 선관위는 각 투표자로부터 전송된 a_i, b_i를 다음과 같이 나열한다.
$(a_1, b_1), (a_2, b_2), ..., (a_n, b_n)$

2) 선관위는 랜덤수 $r_1, ..., r_n$을 선택한 다음 각각의 i(i = 1, 2, ..., n)에 대하여 다음을 생성한다.
$h(a_i, b_i, r_i) = (A_i, B_i)$
(단, $A_i = a_i * g^{r_i}$, $B_i = b_i * (Y_1...Y_k)^{r_i}$)

3) 선관위는 사전 편찬순으로 다음을 공개 보드 상에 공표한다.
$(A_i, B_i) \ (i = 1, ..., n)$

• Subprotocol 2

1) 각 선관위는 다음을 계산한다.
- A_i를 선택하였을 경우
$Z_i = g^{r_i} \bmod q$ (단, i = 1, ..., n)

- B_i를 선택하였을 경우
  $Z_i = Y_m^{r_i} \bmod q$ (단, i = 1, ..., n, m = 1, ..., k)

2) 각 선관위는 공개보드에 다음을 공표한다.
   $(Z_1, Z_2, ..., Z_n)$
3) 모든 사람들이 다음을 확인한다.
   - A_i가 선택된 경우 다음의 값만이 정확하게 확인된다.
     $u_i = A_i / Z_i$
   - B_i가 선택된 경우 다음의 값만이 정확하게 확인된다.
     $u_i = B_i / Z_i$

3.2.3 PIK 방식 고찰

PIK 방식은 공개 보드를 사용하기 때문에 선관위가 투표자의 투표값를 위조하거나 변경할 수 없다는 장점을 가지고 있다. 또한 익명 통신로를 사용하기 때문에 투표값과 투표자를 연결시킬 수 없다. 그러나 이 방식은 선관위의 1/2이상이 결탁할 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

본고에서 제안하려는 방식은 앞에서 살펴보았던 두 가지 방식들이 가지고 있었던 취약점들을 극복하기 위하여 다음과 같은 특징을 갖는다.[13][14]

첫째로, 1인당 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, 기존의 투표 절차에서 투표함의 개표 및 집계시 대동하는 '참관인 제도'를 전자 투표에 도입함으로서 선관위가 집계시 저지를 수 있는 부정을 감시하도록 한다. 이와 같은 감사 기구를 통해 선관위가 저지를 수 있는 부정들을 차단한다.

4.1 요구 조건

이 방식은 투표 매매 방지 및 선관위와 제 3자와의 결탁에 따르는 문제점들을 극복하기 위하여 다음과 같은 요구 사항들을 제시한다. 이렇게 함으로써 투표자 및 선관위의 신뢰도를 높일 수 있으며 만일에 발생할 수 있는 투표 매매 및 선관위의 부정에 대해 대처할 수 있는 유용한 장치가 구성되기 때문이다.

1) 감사기구 및 선관위는 투표자의 신뢰를 획득하기 위해 예비등록을 통하여 투표자 확인을 수행한다.
2) 투표 매매와 같은 부정적인 사고에 대비하여 물리적으로 통제된 별도의 투표소들을 운용한다.
3) 투표의 정확성은 안전한 등록 투표소에서 ZKIP으로 증명되어 진다.
4) 감사 기구와 선관위의 결탁을 방지하기 위해 감사기구는 선관위와는 독립적이며, 다수로 구성한다.
5) 투표 결과에 대한 집계의 공정성을 기하기 위하여 감사 기구는 개표 수행에 참여한다.

4.2 시스템 계수

이 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]

- $G_1, G_2, \ldots G_n$: 감사 기구들
- A : 선관위
- V_i : 투표자 i (i = 1, 2, ..., n)
- A_S, A_P : 선관위의 비밀키와 공개키
- G_S, G_P : 감사 기구들의 대표 비밀키와 공개키
- G_{Sj}, G_V : 감사 기구들의 투표 확인용 분배 비밀키들과 공개키(Secret Sharing 사용, j = 1, 2, ..., k)
- 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
- N_i : 감사 기구들이 투표자에게 부여하는 일련 번호

4.3 제안 프로토콜

- Registration Phase

1) 선관위는 투표 대상자들을 확인하여 선거인 명부를 만들고, 투표자와 감사기구에 공표한다.
2) 각 투표자는 등록과정을 통해 선관위 및 감사 기구로부터 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 감사기구에 보낸다.
  : $r_{i1}(ID_i)$를 생성해 선관위에 전송한다.
  : $r_{i2}(ID_i)$를 생성해 감사 기구에 전송한다.

3) 전송되어온 데이터에 대하여 선관위는 자신의 비밀키로 서명한 뒤 투표자에게 전송하며, 감사 기구 역시 공동으로 인증을 수행한 후 일련 번호를 부여하여 자신들의 대표 비밀키로 서명한 뒤 투표자에게 전송한다. (감사 기구는 선관위의 부정을 방지하기 위해 일련 번호를 부여한다.)
   $A_S(r_{i1}(ID_i))$, $G_S(r_{i2}(ID_i) \| N_i)$ ==> 투표자
4) 투표자는 선관위와 감사 기구로부터 전송된 서명들과 일련 번호를 확인한다.

- 투표자는 자신의 비밀 계수를 제거하여 선관위의 서명이 붙은 자신의 식별자 S_A와 감사 기구의 서명 이 붙은 S_G를 얻는다.
  $r_{i1}'(A_S(r_{i1}(ID_i))) = A_S(ID_i) = S_A$,
  $r_{i2}'(G_S(r_{i2}(ID_i) \| N_i)) = G_S((ID_i) \| N_i) = S_G$
- 선관위의 공개키 A_P와 감사 기구의 공개키 G_P를 이용하여 서명을 확인하고, 자신의 식별자가 정확히 등록되었는지 확인한다.
  $A_P(S_A) = A_P(A_S(ID_i)) = ID_i$, $G_P(S_G)$
  $= G_P(G_S((ID_i) \| N_i)) = ID_i \| N_i$

- **Voting Phase**

5) 투표일이 되면 투표자는 투표소에서 물리적으로 자신을 확인하고 투표를 수행한다. (선관위 및 감사 기구의 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.)
  : 감사 기구의 공개키를 이용해 다음을 계산한다.
  $G_V(FIR \| DUM \| N_i) = J$
  : 투표자는 J와 자신의 1차 선택값 FIR, Dummy값 DUM 그리고 일련 번호 N_i를 연접해 선관위의 공개키로 암호화한다.
  $A_P(FIR \| DUM \| N_i \| J) = E$
- 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.)
  : 감사 기구의 공개키를 이용해 다음을 계산한다.

$G_V(FIR \| SEC \| N_i) = K$

: 투표자는 K와 1차 선택값 FIR, 2차 선택값 SEC 그리고 일련 번호 N_i을 연접해선관위의 공개키로 암호화한다.

$A_P(FIR \| SEC \| N_i \| K) = E'$

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

: 투표자가 1차 선택만 수행했을 경우에는 $S_A \| S_C \| E$를 선관위와 감사 기구에 각각 전송하며, 2차 선택을 수행했을 경우에는 $S_A \| S_C \| E'$를 선관위와 감사 기구에 각각 전송한다.

• Conviction Phase

6) 선관위 및 감사 기구는 자신들의 비밀키를 이용해 복호화 한 뒤, 서명을 확인함으로 투표 결과를 확인 한다.

- 선관위 및 감사 기구는 자신들의 공개키로 서명을 확인한다.

$A_P(S_A) = ID_i$, $G_P(S_C) = ID_i \| N_i$

- 선관위는 자신의 비밀키로 투표 정보를 복호화 한다.

$A_S(E) = A_S(A_P(FIR \| DUM \| N_i \| J)) = FIR \| DUM \| N_i \| J$ (투표자가 1차 선택을 수행하여 전송한 경우)

$A_S(E') = A_S(A_P(FIR \| SEC \| N_i \| K)) = FIR \| SEC \| N_i \| K$ (투표자가 2차 선택을 수행하여 전송한 경우)

- 선관위는 투표자가 1차 선택을 수행한 경우 J를 감사 기구에 전송하며, 2차 선택을 수행했을 경우에는 K를 감사 기구에 전송한다. 감사 기구는 선관위로부터 수신된 투표 정보를 다음과 같이 자신들의 비밀키들로 확인한 후 해쉬를 취한다.

$G_S(J) = G_S(G_V(FIR \| DUM \| N_i)) = FIR \| DUM \| N_i$(투표자가 1차 선택을 수행했을 경우)

==> $H(FIR \| DUM \| N_i) = J_H$

$G_S(K) = G_S(G_V(FIR \| SEC \| N_i)) = FIR \| SEC \| N_i$(투표자가 2차 선택을 수행했을 경우)

==> $H(FIR \| SEC \| Ni) = K_H$

- 선관위 및 감사 기구는 해쉬 함수를 이용해 다음과 같이 계산 및 비교하여 투표의 진위 여부를 판단한 다.

: 투표자가 1차 선택만을 수행했을 경우, 선관위는 투표자가 선택한 1차 선택값 FIR, Dummy값 DUM 그리고 일련 번호 N_i를 연접해 해쉬를 수행한 후 감사 기구에서 확인한 J_H와 비교한다. 만약 비교한 값이 같다면 정당한 투표값으로 인정한다.

$H(FIR \| DUM \| N_i) = J_H$

: 투표자가 2차 선택을 수행했을 경우, 선관위는 투표자가 선택한 1차 선택값 FIR, 2차 선택값 SEC 그리고 일련 번호 N_i를 연접해 해쉬를 취하여 감사 기구에서 확인한 K_H와 비교한다. 만약 비교한 값이 같다면 정당한 투표값으로 인정한다.

$H(FIR \| SEC \| N_i) = K_H$

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

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

- 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 투표 결과를 노출시키지 않기 위해서 다음과 작성한다.

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

• Opening Phase

7) 투표자의 투표 결과를 저장하고, 공개 보드상에 공표한다.

- 1차 선택만 수행했을 경우

: $ID_i \| v_{i1} \| H(ID_i \| R_{i2})$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
  : $ID_i \| v_{i1} \| H(ID_i \| H(v_{i2} \| R_{i2}))$가 저장되며, 투표값 v_{i2}가 집계 결과가 된다. 이 때 공개 보드 상에는 투표 자의 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 해쉬 한 값을 투표 결과 list와 비교함으로써 자신의 투표 결과 v_{i2}가 집계되었음을 확인한다.

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

4.4 제안 방식 고찰

본 제안 방식은 은닉 서명을 이용한 예비 등록 절차를 통해 자신의 식별자를 등록하게끔 함으로서 투표자와 ID_i를 연결시킬 근거를 없애고 있다. 또한 투표소에서 투표를 수행함으로서 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 감시하는 감사 기구들을 구성함으로서, 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) 선관위가 투표 미등록자의 투표권을 행사하려 시도할 경우
  => 모든 투표자는 투표를 수행하기 전에 자신의 식별자 ID_i를 선관위와 감사 기구에 등록하게 되어 있다. 감사 기구는 ID_i 등록시 일련 번호 N_i를 부여하게 되어 있기 때문에, 선관위가 임의의 제 3자를 통해 투표 미등록자의 투표권을 행사하려 한다 해도 감사 기구가 부여한 일련 번호를 알지 못하기 때문에 투표 집계시 부정을 검출할 수 있다.

- 부정 유형 3) 선관위와 n-1개의 감사 기구가 결탁할 경우
  => 투표자의 식별자 ID_i에 대해 감사 기구들이 모두 동의한 상태에서 일련 번호를 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 자

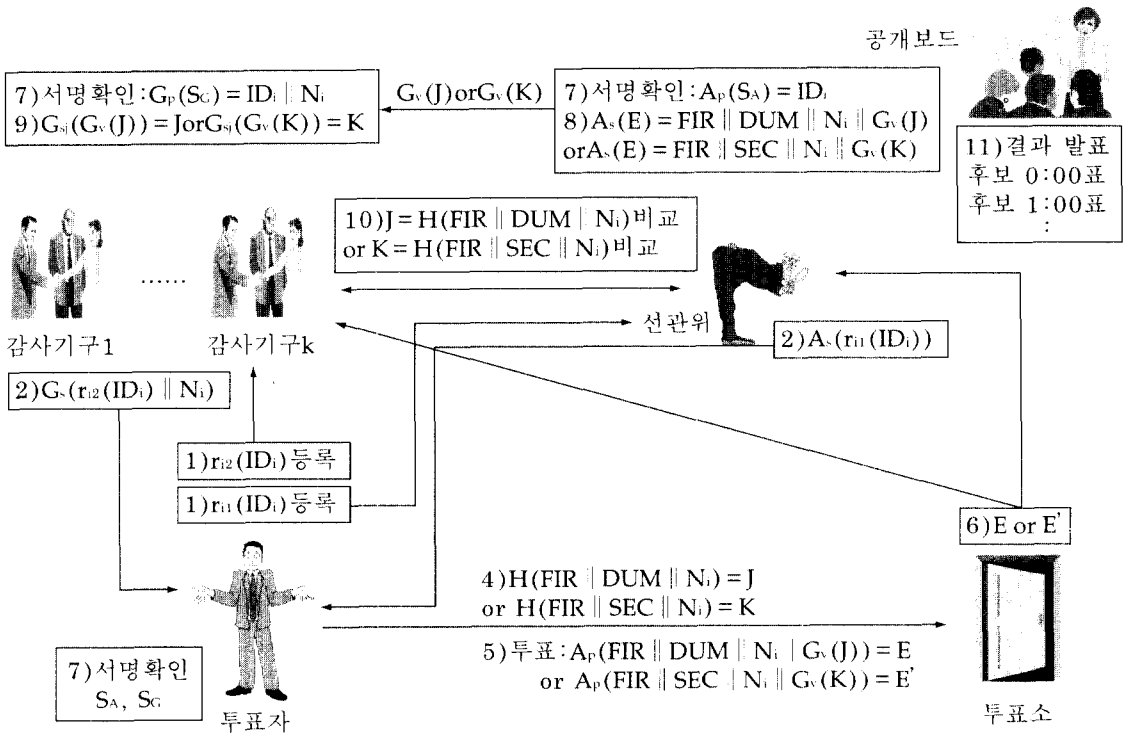


그림 4. 제안 방식 흐름도
Fig 4. Flowchart about proposed method

신은 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 매매자에게 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 감사 기구 시스템을 도입함으로서 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. 결 론

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, 투표를 총괄하는 선관위의 비중이 어느 정도가 되는지에 대해서 생각해 보았으며, 전자 투표상에서 발생할 수 있는 선관위의 부정에 관하여 기존의 방식 중에 하나인 PIK 방식이 어떻게 대처하는지에 대해 언급하였다. 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.

상기 기존의 방식들은 투표자와 선관위가 정직하다는 가정하에 수행 기능을 기술하고 있으며, 미등록 투표자에 대한 선관위의 부정에 대해 고려하고 있지 않았었다. 또한, 투표자가 제 3자에게 자신의 식별자를 확인시키지 못하게 함으로서 투표 매매를 제한하려 하였으나, 매매자가 식별자를 투표 후에 그대로 요구할 경우 투표자가 대응할 아무런 방법도 없다는 문제점을 가지고 있었다.

이에 대해 본 제안 방식은 투표소가 물리적으로 안전하고, 감사 기구의 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 투표결과를 알지 못하도록 수행하고자 할 때 매우 유용하게 사용할 수 있는 방법을 제시한다. 이들을 통해 소외된 계층에 접근하는 매수자들의 시도를 근원적으로 예방할 수 있을 뿐만 아니라, 향후 전자 투표 수행에 있어 좀더 안전하면서도, 편리하게 사용하는데 있어 많은 도움이 되리라 생각한다.

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.

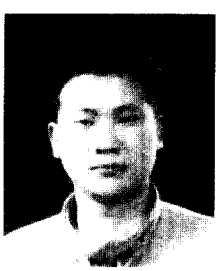
[11] V. Niemi and A. Renvall, "How to prevent buying of votes in computer elections," ASIACrypto '94 pp.164-170, 1994.

[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, pp.163-168, 1998. 6.

□ 著者紹介

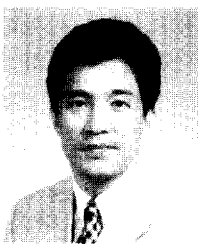


박 희 운

1997년 2월 순천향대학교 전산학과 졸업
1997년 ~ 현재 순천향대학교 전산학과 대학원

※ 주관심 분야 : 암호이론, 컴퓨터 보안

□ 著者紹介



이 임 영

1981년 홍익대학교 전자공학과 졸업
1986년 일본 오오사카대학 통신공학부(석사)
1989년 일본 오오사카대학 통신공학과(박사)
1992년 ~ 1994년 한국전자통신연구원 선임연구원
1994년 ~ 현재 순천향대학교 컴퓨터학부 교수

※ 주관심 분야 : 암호이론, 정보이론, 컴퓨터 보안