Magic Sticker 기법을 이용한 안전한 전자투표 시스템

박 희 운† · 이 임 영††

요 약

정보 사회를 거치면서 네트워크의 발전과 관련한 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 될 것이다. 따라서 본 논문은 기존의 투표를 전자 투표로 적용시키는 과정에서 어떠한 요소들이 필요한지 확인해 보고 선거 관리 위원회의 부정 방지 및 매매방지를 위한 요구 조건을 살펴볼 것이다. 또한 매매방지를 위해 네트워크 상에서 익명성을 제공하는 안전한 선택 기법인 "Magic Sticker" 기법을 사용하여, 투표자의 투표 내용이 공개되더라도 투표 결과를 안전하게 보호할 수 있는 전자 투표 시스템을 제안한다.

The Secure Electronic Voting System using the Magic Sticker

Hee-Un Park† · Im-Yeong Lee††

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. So, we look into various elements involved in implementing the electronic voting system. We especially focus on the requirements that the receipt free and robustness for making the system secure against various illegal attempts such as buying of votes and voting process manipulations. Also we present a secure electronic voting system, although the voting result has been published on network board, using "Magic Sticker" scheme that offers the untraceability for receipt free on open network.

키워드 : Electronic Voting System(전자투표시스템), Receipt Free(매매 방지), Robustness(부정 방지), Magic Sticker(매직 스티커)

1. 서 론

현대 사회는 산업 혁명과 시민 의식의 발전을 통해 인류에게 평등권을 보장해 주었으며, 각 개인의 의사를 존중하기 위한 수단으로서 직·간접적으로 '투표'를 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 될 수 있었다. 투표는 일상 생활에 있어 작게는 소수 모임의 대표에서부터 크게는 대통령을 뽑는 일 까지 다양한 분야에 걸쳐 현대 사회에 없어서는 안될 주요 수단으로 존재하고 있다.

일반적으로 우리가 수행하는 투표의 모습을 살펴보면 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 지역 투표구에 사는 사람이라는 것을 확인한다. 그런 다음 투표자는 투표 용지를 받아 다른 사람의 간섭이 없는 기표소에서 투표를 수행하고 이를 투표함에 넣게 된다.

하지만 이런 유형의 투표는 투표자가 직접 지정된 투표소에 가야 한다는 전재 조건을 내포하고 있다. 따라서, 개인적으로 급한 용무가 생겨 자신의 투표구 외의 장소로 이동해야 할 경우 현행의 투표 방식은 매우 번거로운 일로 취급되었던 것이 사실이다.

그러나 요즘은 컴퓨터 및 네트워크의 발전을 통해 새로운 정보 서비스를 생활 안·밖에서 보급 받게 됨으로서 우리의 일상생활에서 많은 변화를 실감하고 있다. 이러한 서

※ 본 논문은 2001년도 한국과학재단 지역대학 우수과학자 지원연구 사업에 의해 수행되었습니다.
†준 회 원 : 순천향대 전자계산학과 대학원
††종신회원 : 순천향대학교 정보기술공학부 교수
논문접수 : 2001년 1월 9일, 심사완료 : 2001년 4월 3일

비스를 전제로 전자 투표를 실생활에 보급할 수 있다면 현행 투표 시스템이 안고 있던 많은 문제점들을 해결 할 수 있을 것이다. 즉, 투표소에서 수행 가능하던 투표 작업이 자신의 사무실이나 역 그리고 공항 등의 공공 장소에 있는 컴퓨터를 이용하여 수행될 수 있다면, 투표자는 날씨나 장소에 구애받을 필요 없이 투표를 할 수 있으므로 투표자의 불편함은 개선될 것이며, 일상 생활에 있어 매우 편리함을 제공하게 될 것이다.

뿐만 아니라, 전자 투표를 도입하게 된다면 개표 및 집계 시 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.

이에 대해 본 고에서는 전자 투표를 위한 일반적인 사항과 투표 부정 및 매매방지를 위한 특수 요구 사항에 대해 살펴본다. 동시에 네트워크 상에서 투표자의 자유 의지로 안전하게 투표를 수행하고, 투표자에 대한 익명성을 보장할 수 있도록 "Magic sticker" 기법을 도입할 것이다. 이를 통해 본 제안 방식은 일반적인 요구 사항뿐 아니라 부정 및 매매를 방지함으로서 신뢰성과 안전성을 제공할 것이다.

2. 전자 투표의 발전 현황 및 분류

2.1 전자 투표의 발전 현황

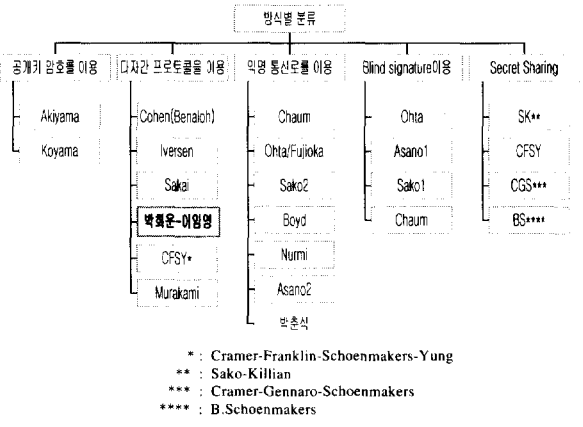
현재 전자 투표를 추진하고 있는 나라로는 미국, 일본, 스위스, 프랑스 등의 선진국들이 있다. 미국의 경우에는 1892년에 투표 용지를 사용하지 않고 투표기를 이용해 투표를 수행한 것을 필두로 1960년에는 펀치 카드 시스템을 투표에 도입했으며, 1980년에는 D.R.E(Direct Recording Election)버튼식 전자 투표기를 설치한 상태이다. 1997년도에는 뉴욕 전 투표소에서 버튼식 전자 투표기를 설치해 운용하고 있다.

또한, 일본의 경우에는 투표율 및 신속한 처리를 위해 민간 차원에서 많은 연구가 진행되어 오고 있다. 1989년도에 전자 투표 시스템 연구회가 발족한 이래 on-line식 D.R.E 방식을 통해 네트워크 암호화에 따른 안전 대책 수립, 첨단 전자 기술의 활용으로 1993년에는 각 현별로 시스템 도입 검토 및 전자 투표 모의 실험을 실시한 상태이다.

그러나, 우리 나라의 경우에는 선거 관리 업무와 투·개표 단계의 자동화에 대한 연구와 검토가 이루어지고 있으나, 아직 암호를 이용한 안전하고 실용적인 전자 투표 시스템의 도입 검토는 이뤄지고 있지 않은 실정이다. 전자 투표에 대한 연구는 전자 선거 구현 시 수반되는 안전성 문제를 해결하기 위해 암호 응용 분야의 확대를 통해 많은 연구가 진행되고 있다.

2.2 전자 투표의 분류

현재까지의 국내외 전자 투표 연구 현황은 다음과 같이 분류되며, 간략히 그 기술들을 설명한다.



(그림 1) 전자 투표의 방식별 분류

전자 투표 프로토콜로서 최초로 제안된 것은 1981년 Chaum에 의해서지만, 이는 익명 통신로를 기본 전제로 하여 RSA의 안전성을 기반으로 한 것으로서 투표 용지로부터 특정 유권자를 추적할 수 있다는 단점이 있었다[1]. 또한 1985년 Cohen과 Fischer에 의해 제안된 다자간 프로토콜을 이용한 선거 방식의 경우 투표 용지의 비밀성을 보장할 수 없다는 문제점을 가지고 있었다[2].

1985년 일본의 Koyama는 RSA 공개키 암호를 이용한 안전한 무기명 투표 방식을 제안하였다. 그러나 이 방식은 투표자 다수가 결탁하거나 혹은 위원 이외에 단독으로 부정 행위를 시도할 경우, 이를 방지할 수 없는 단점이 있다[3].

1986년 Cohen과 Benaloh는 r차 잉여 암호계에 있어서 각각 대화형 영지식 증명 혹은 Secret Sharing을 응용하여 유권자의 프라이버시를 보호하는 투표 방식을 제안하고 있으나, Cohen의 방식은 부정 검출을 위해 통신량이 많은 반면, Benaloh의 방식은 센터와의 통신량이 보다 적은 장점을 갖고 있다. Benaloh의 방식을 개선한 전자 선거 프로토콜로서 1990년 Sakai, Murakami 등에 의해 제안된 방식을 들 수 있으며, 이는 Secret Sharing에 의한 투표 내용의 보호 방식에 있어서 보다 효과적으로 부정을 감시하는 것이 가능한 방식이다[4, 5].

Chaum등은 한 사람의 위원만으로 blind 서명을 사용하여 무기명성을 보증하는 투표 방식을 제안하였으나, 유권자의 공평성을 제공할 수는 없었다. 그 후 Asano등은 통신에 있어서 blind 서명과 함께 공개 게시판을 이용함으로서 유권자의 공평성까지 만족하는 방식을 제안하였다[6].

1993년에 제안된 Park-Itho-Kurosawa(PIK) 방식은 익명 통신로를 그 전제로 하고 있으며, 투표가 잘못되었을 경우 모든 투표자가 알 수 있도록 구성함으로서 선관위들의 부정을 방지하려 하고 있다. 그러나 선관위가 반수 이상 부정

을 저지를 경우 부정을 확인할 방법이 없으며 제 3자와의 결탁을 통해 투표 미등록자의 투표권을 행사할 가능성이 있기 때문에 완벽한 안전성을 확보했다고는 말할 수 없다[7]. 또한 1994년에 제안된 Sako 방식은 partially compatible homomorphism을 이용해 효율적인 MIX형 전자 투표 방식을 제안하였으나, 모든 투표 결과의 정당성을 투표자들이 확인할 수 없다는 문제가 있다[8].

1996년에 Niemi-Renvall은 투표의 매매 가능성을 지적하고, 이에 대한 대책을 제안하였다. 즉, 투표 결과 공개시 나타내는 각 투표자의 식별자를 생성할 때 위원회의 비밀 값을 결합해 생성함으로서 결코 제 3자에게 투표자가 자신의 식별자임을 증명 못하게 하는 방식을 제안했다. 그러나, 이 방식은 투표자가 투표 결과를 확인하지 못한 상태에서 식별자를 요구당할 경우 아무런 대책이 없다는 문제점을 안고 있다[9].

그 외에도 [10-13] 등 다양한 형태의 전자 투표 방식들이 제안되고 있다. 그러나, 각 방식별 특성상 매매 방지와 참여 요소간 부정에 대해서 아직은 완벽한 안전성을 제공하고 있지는 못한 실정이다.

3. 전자 투표를 위한 요구사항

3.1 일반적 요구사항

전자 투표 시스템은 성격상 기존의 일반적인 투표가 갖는 주요 특성들을 만족해야 한다. 일 예로 '비밀 투표'나 '무기명 투표'는 투표자의 비밀성과 안전성을 보장하기 위한 특성들을 대표하는 용어들로서, 전자 투표 시스템 구현 시 필수적으로 만족되어야 할 부분이다. 다음은 전자 투표 시스템 구현 시 갖추어야 할 일반적인 요구사항을 기술한 것이다.

- 비밀성 : 투표자와 투표내용의 대응은 당사자만이 안다.
- 공정성 : 투표자는 오직 하나의 투표권으로 한번 투표한다.
- 인증성 : 투표권이 있는 사람만이 투표를 수행할 수 있다.
- 공평성 : 누구도 다른 사람의 투표 결과를 통해 자신의 투표결과를 결정할 수 없다.
- 무결성 : 제 3자에 의한 투표 결과의 변경은 불가능하다.
- 검증성 : 투표가 끝난 다음 누구나 투표가 정당하게 수행되었는지를 확인할 수 있어야 한다.

3.2 특수 요구 사항

전자 투표는 기존의 일반 방식들과는 달리 공개된 네트워크를 통해 수행되게 된다. 따라서 투표자의 투표 결과를 확인시키는 과정이 필수적으로 요구되어 진다. 또한 투표 수행 후 집계를 위해 투표 결과들은 네트워크를 통해 선관위나 집계소로 전송되게 된다. 이러한 일련의 과정들은 네트워크 특성상 중간 단계에서 투표 관리자들에 의해 부정이 생길 가능성이 있으며, 투표자 사이에서는 매매가 가능할 수 있게 된다. 그러므로 전자 투표 시스템은 이를 방지하기 위해서 다음과 같은 특수한 요구 사항을 만족해야 한다.

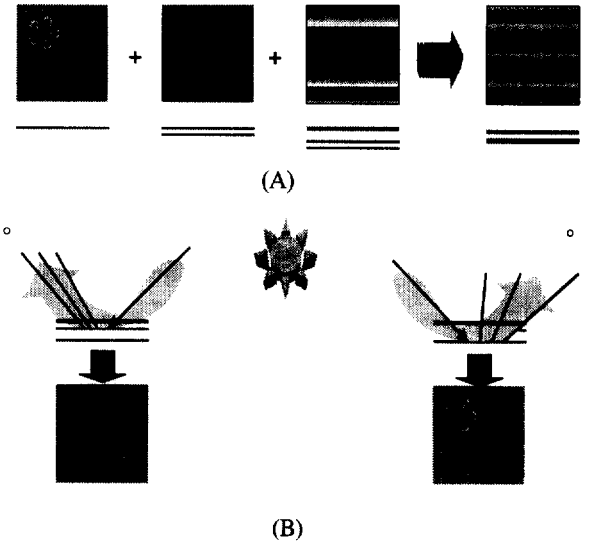
- Receipt Free : 이 특성은 매매 방지를 위한 특성으로서, 어느 누구도 투표자의 개별 투표 결과를 확인할 수 있어서는 안 된다[4, 8, 9, 14].
- Robustness : 이 특성은 투표 관리 요소의 부정 방지를 위한 특성으로서, 누구나 각 참여자의 오류 또는 부정 행위를 확인 할 수 있어야 한다[7, 13, 15].

4. Magic Sticker 기법

본 방식은 전자 투표 상에서 안전성과 신뢰성을 보장하고 매매 방지를 위하여 다음에서 기술하는 Magic Sticker 기법을 적용한다[16].

4.1 물리적 Magic Sticker개념

Magic Sticker는 2개 이상의 영상을 편광 각도가 다른 홀로그래피(Holography) 필름에 2차원으로 합성 시켜 광원의 각도에 따라 서로 다른 형체를 표현할 수 있도록 한 필름형 Sticker를 의미한다. (그림 2)는 이에 대한 간단한 구조를 그림으로 표현한 것이다. (A)는 2개의 영상과 필름을 합성한 형태를 보이고 있으며, (B)는 빛의 각도에 따라 각기 다른 영상이 보여지는 것을 표현한 것이다. 이때 각 영상의 어느 위치에나 눈에 보이지 않는 정보를 저장할 수 있으며, Magic Sticker를 생성할 때 적용된 특수 정보를 아는 사람만이 확인 가능하다.



(그림 2) 물리적 Magic Sticker의 일반적인 형태

이러한 정보는 만약 특수 정보를 모르는 사람이 인위적

으로 필름을 벗겨낼 경우에는 저장된 정보 및 영상 모두가 파괴된다. 또한 저장 정보 확인을 위해서는 특수 정보가 필요하게 되므로 인위적인 편법을 통해 이를 확인하는 것은 불가능하게 된다. 이때 저장 정보의 내용이 투표자의 의사를 반영하는 '투표 결과'일 경우, 물리적으로 안전한 투표가 가능해 진다. 이러한 특성을 암호학적으로 접근할 경우, 사용자가 자신의 자유 의지로 선택을 수행하고 이에 대한 안전한 신원 보장을 이룰 수 있는 안전한 선택(Secure Selection) 서비스를 네트워크 상에서도 수행할 수 있게 된다[16].

4.2 Magic Sticker형 투표 용지 구성

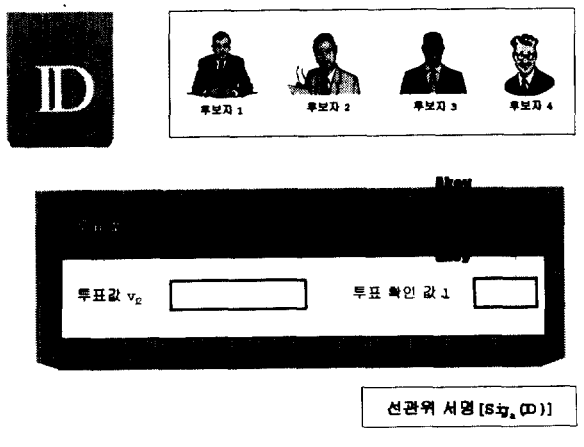
4.2.1 일반 투표 용지 구성 형태

기존의 투표용지를 보면 후보자 기호와 성명 및 후보자 선택란이 칸으로 구성되어 있으며, 투표용지가 정당하다는 것을 보장하기 위해서 선관위의 도장이 찍혀있다. 투표자는 자신이 선택하고자 하는 후보자의 성명 옆에 있는 선택란에 도장을 찍게된다. 그러나 전자 투표의 경우 모든 것이 전자적으로 안전하게 수행되어야 하므로 투표용지의 구성과 투표 수행에 있어서 차이점을 가지고 있다.

4.2.2 전자 투표 용지 구성

전자 투표용지의 구성은 선관위의 서명, 투표자 가명 ID 및 투표 값 선택란(공란 두 개)과 투표 값 확인란, 마지막으로 후보자들의 정보가 포함된다. 선관위의 확인은 기존의 선관위 도장대신 디지털 서명이 사용되며, 후보자 선택 또한 투표자가 후보자 번호를 직접 선택하게 된다.

본 방식은 Receipt Free 특성을 만족하기 위하여 투표 값 확인란에는 두 개의 투표 값 중 하나를 선택하여 자신의 투표 값으로 결정한다. 이때 투표자의 선택 정보는 신뢰성을 보장하여야 하지만 결코 제 3자에게 노출되어서는 안된다. 이를 위해 두 개의 Magic Sticker Ekey와 Akey를 투표자에게 제공한다. (그림 3)은 제안된 전자 투표 용지 구성도를 나타낸 것이다.



(그림 3) 전자 투표용지 구성도

투표자는 투표 값 v_{i1}과 투표 값 v_{i2}를 모두 작성해야하며, 이 두 값이 같아서는 안 된다. 또한 투표 확인란에 0과 1중 하나를 선택하여 자신의 투표 값을 결정해야하며, 오직 집계소에서만 이들 값을 알 수 있다. 만약 상기 두 개의 Magic Sticker 및 투표 확인 정보를 모르는 사람이 인위적으로 투표 내용을 알아내려 할 경우에는 확인이 불가능하게 된다. 또한 저장 정보 확인을 위해서는 Akey 및 Ekey가 필요하게 되므로 인위적인 편법을 통해 이를 확인하는 것은 불가능하게 된다. 이렇게 함으로써 투표 선택 결과의 익명성을 보장하고 있다.

5. 새로운 방식 제안

5.1 시스템 계수

다음은 신뢰된 전자 투표 시스템을 구성하는데 필요한 시스템 계수를 기술한다.

- CTA(Central Tabulating Agency) : 선거관리 위원회
- V_i : 투표자 i (i = 1, 2, 3, …, n : n은 투표자의 수)
- Q_i : 집계소 i (i = 1, 2, 3, …, j : j는 집계소의 수)
- G_i : 투표소 i (i = 1, 2, 3, …, m : m은 투표소의 수)
- Mkey : CTA가 생성한 통신 및 인증을 위한 마스터 키
- H : 128비트 결과를 내는 안전한 일방향 해쉬 함수
- ID_i : 투표자 i의 가명 식별자
- $Akey_i$: 투표값 인증 Magic Sticker, $Akey_i$ = $H(ID_i||$ Mkey)의 상위 64비트
- $Ekey_i$: 투표값 암호 Magic Sticker, $Akey_i$를 만들고 난 나머지 64비트
- Sk_a, Pk_a : CTA의 개인키 및 공개키
- Sk_{qi}, Pk_{qi} : 집계소 i의 개인키 및 공개키
- Sk_{gi}, Pk_{gi} : 투표소 i의 개인키 및 공개키
- Sk_{vi}, Pk_{vi} : 투표자 i의 개인키 및 공개키
- v_{i1}, v_{i2} : 투표자 i의 투표값
- l_i : 투표자 i의 투표 선택 확인 값 ($l \in \{0, 1\}$)
- r_i : 투표자 i가 선택한 은닉 계수용 랜덤 값
- T : Time-Stamp

5.2 프로토콜

5.2.1 준비 단계

가) 선관위

① 투표 대상자를 확인하여 투표자 명부를 작성하고 투표자에게 투표 안내문을 발송한다.

② 선관위는 투표자에게 제공할 가명 식별자 ID_i와 Mkey를 생성한다.

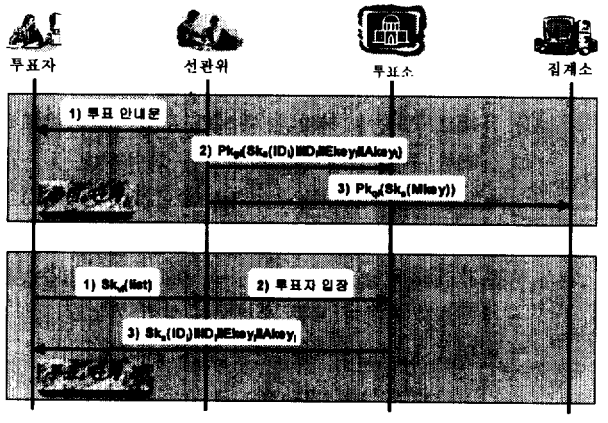
③ ID_i에 서명을 수행하고, ID_i와 투표시 사용될 Magic Sticker $Ekey_i$ 및 $Akey_i$를 연접해 투표 용지를 구

성한 다음, 투표소의 공개키로 암호화하여 투표소에 전달한다. 단, 투표 용지의 개수는 해당 투표구의 선거인 명부 인원에 근거해 발송되게 된다.

- $Pk_{gi}(Sk_a(ID_i)||ID_i||Ekey_i||Akey_i)$

④ 생성된 Mkey를 선관위의 서명을 수행한 후 집계소의 공개키로 암호화하여 집계소에 전송한다.

- $Pk_{qi}(Sk_a(Mkey))$



(그림 4) 준비 단계 및 투표자 인증 단계 흐름도

5.2.2 투표 단계

가) 투표자 V_i

① 투표일이 되면 투표자 V_i는 인터넷을 통해 자신을 인증하고 지정 투표소에 접속한다. 이때 인증은 선관위를 통해서 하게되며, 지정 투표구에 속한 선거인 명부(list)에 투표자 자신의 서명을 하게 된다.

- $Sk_{vi}(list)$

이때, 선거인 명부(list)는 확인과정에서 선관위에 의해 투표 참여 인원수와 집계소에서 집계한 투표 인원수를 비교하기 위해 사용된다.

나) 투표소 G_i

① 선관위로부터 받은 투표 용지 중 하나를 랜덤하게 선택하여 투표자 V_i에게 발급한다.

- $Sk_a(ID_i)||ID_i||Ekey_i||Akey_i$

② 투표 과정을 기술하기 이전에 투표자가 사용할 전자 투표 용지는 다음 사항을 만족해야 한다.

- 전자 투표 용지는 각기 다른 투표결과를 저장할 두 개의 공란과 투표 확인란으로 구성된다.
- 투표자는 두 개의 공란에 투표 값을 모두 선택하게 되고 투표 확인란은 두 공란의 투표 값 중 어떤 값을 집계 시에 반영할지 선택하게된다.
- 두 공란의 값은 같을 수 없으며, 투표 확인란에는 0과 1로 실제 집계에 반영될 값을 결정하게 된다.

다) 투표자 V_i

① 투표자는 투표 값 v_{i1}, v_{i2}를 결정한다.

② 투표 확인 값 $l_i \in \{0, 1\}$을 선택한다.

③ 투표자가 l_i 값으로 0을 선택할 경우 투표 값 v_{i1}이 집계에 반영되고 1을 선택하면 투표 값 v_{i2}가 집계에 반영된다.

- $v_{i1} \,||\, v_{i2} \,||\, l_i$ 은 투표자가 작성한 투표 값이다.

④ 투표 확인 값을 결정하고 난 다음, 랜덤 값 r_i를 선택한다.

⑤ 다음과 같이 l_i에 따라 집계될 투표 값을 결정하고, 신뢰성과 안전성을 보장하기 위해 Magic Sticker $Ekey_i$ 및 $Akey_i$를 이들 값에 부착한다. 즉, $Akey_i$는 l_i에 따른 투표자의 선택 결과가 무엇인지를 인증시키기 위해 사용되고, $Ekey_i$는 이들 값들의 기밀성을 제공하는데 사용된다.

- l_i값이 0일 경우

$$Ekey_i(Akey_i(v_{i1} \,||\, l_i)||\, v_{i2})$$

- l_i값이 1일 경우

$$Ekey_i(v_{i1}||Akey_i(v_{i2} \,||\, l_i))$$

⑥ Magic Sticker가 부착된 투표결과 값과 $Sk_a(ID_i)$ 및 투표 시간을 나타내는 타임스탬프(T) 값을 이용하여 다음을 생성한다.

- $Z_i = Ekey_i(Akey_i(v_{i1} \,||\, l_i)||\, v_{i2})||Sk_a(ID_i)||\, T$

⑦ Magic Sticker가 부착된 투표값과 l_i값을 연접하여 전송함으로서 Mkey를 모르는 이상 투표결과 값을 알 수 없으며, 이를 통해 투표값에 따라 투표자를 연관시킬 근거를 제거함으로서 투표자의 익명성을 보장하게 된다.

⑧ 투표가 완료되면 투표자는 선택한 v_{il}값을 다음과 같이 계산하여 선관위로 전송한다.

- $Pk_a(ID_i||Pk_a(r_i)*(v_{ik}))$

  (단, $k \in \{1, 2\}$)

또한, Z_i 및 r_i를 연접하여 투표소의 공개키로 암호화한 결과 $Pk_{gi}(Z_i||r_i)$를 투표소에 전송한다.

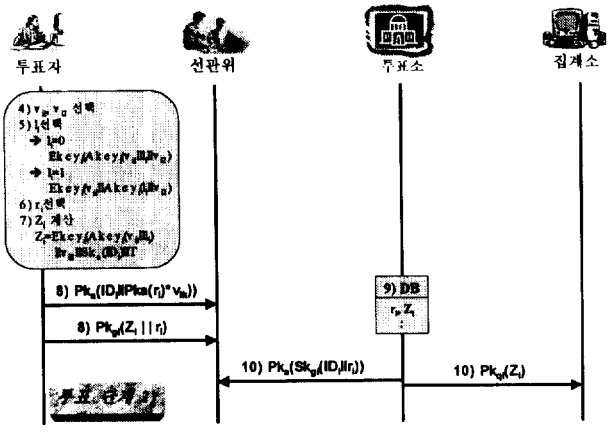
라) 투표소 G_i

① 전송된 $Pk_{gi}(Z_i||r_i)$의 복호화 과정을 통해 투표자 V_i가 선택한 r_i값과 투표 정보 Z_i를 투표소의 DB에 저장한다.

- $Sk_{gi}(Pk_{gi}(Z_i||r_i)) = Z_i||r_i$

② 투표 시간이 마감되면 DB에 저장된 투표 정보에 다음과 같이 계산하여 각각 집계소 Q_i와 선관위로 전송한다.

- $Pk_{qi}(Z_i)$를 집계소 Q_i로 전송한다.
- $Pk_a(Sk_{gi}(ID_i||r_i))$를 선관위로 전송한다.



(그림 5) 투표 단계 흐름도

5.2.3 확인 단계

가) 집계소 (Ω_i)

① 전송 내용을 자신의 개인키로 복호화 한 다음, Z_i를 확인한다.

- $Sk_{qi}(Pk_{qi}(Z_i))$ = $Ekey_i(Akey_i(v_{i1} \| l_i)\| v_{i2})\|$ $Sk_a(ID_i)\|$ T

② 선관위 서명 및 타임스탬프를 확인하고 선관위로부터 전송된 Mkey와 투표자 i의 ID_i로부터 $Ekey_i$와 $Akey_i$를 생성하여 투표값을 복호화한 후 l_i값이 연접된 투표 값을 집계에 반영한다.

- $Akey_i$ = $H(ID_i||Mkey)$의 상위 64비트
- $Ekey_i$ = $Akey_i$를 만들고 난 나머지 64비트
- $Ekey_i(Ekey_i(Akey_i(v_{i1} \| l_i)\| v_{i2}))$
  = $Akey_i(Akey_i(v_{i1} \| l_i))\| v_{i2}$
  = $(v_{i1}||l_i) \| v_{i2}$

③ l_i값에 따라 v_{i1}값을 DB에 저장한다. 즉, l_i = 0일 경우 v_{i1}이 저장되고, l_i = 1일 경우 v_{i2}가 저장된다.

④ 확인된 투표결과 값은 l_i값을 제외하고 각각 $Ekey_i$와 $Akey_i$로 다시 숨긴다.

- $Akey_i(v_{i1})||Ekey_i(v_{i2})$

⑤ 집계가 완료되면 공개보드 상에 투표자의 ID_i와 은닉된 투표값을 저장한다.

- $ID_i||Akey_i(v_{i1})||Ekey_i(v_{i2})$

나) 선관위

① 투표 정보를 복호화 한다. 그런 다음 r_i와 관련된 정보에서 투표소의 서명을 확인하고 자신의 개인키로 복호화 한다.

- $Sk_a(Pk_a(ID_i||Pk_a(r_i)*(v_{ik})))$ = $ID_i||Pk_a(r_i)*(v_{ik})$
- $Pk_{gi}(Sk_a(Pk_a(Sk_{gi}(ID_i||r_i))))$ = $ID_i||r_i$

② 추출된 r_i값과 자신의 개인 키를 이용하여 선관위 서명 투표 결과를 공개한다.

- $(Sk_a(Pk_a(r_i)*(v_{ik})))/r_i$ = $Sk_a(v_{ik})$

③ 다음의 수식을 이용하여 공개보드 상에 저장된 집계 내용과 투표소에서 전송되어온 투표정보가 일치하는지 확인한다.

- $Pk_a(Sk_a(v_{1k}))*\cdots*Pk_a(Sk_a(v_{nk}))$ mod n
  ≡ $v_{1k}*\cdots*v_{nk}$ mod n

④ 투표자 선거인 명부에 서명된 투표자 수와 공개보드 상에 저장된 투표자 인원수가 일치하는지 확인한다. ③및 ④를 만족하면 투표 결과를 받아들인다.

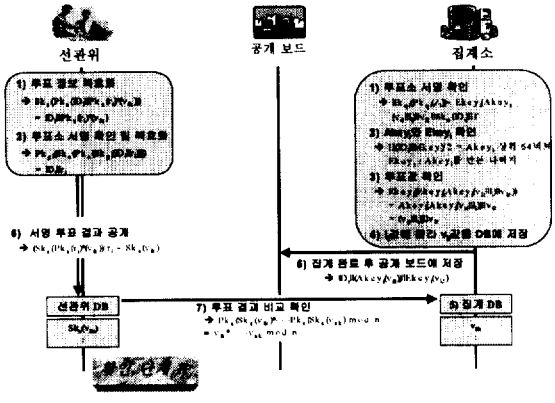
다) 투표자

① 공개보드 상에 저장된 자신의 투표 값과 자신이 선택한 투표 값이 일치하는지를 확인한다.

- $ID_i||Akey_i(v_{i1})||Ekey_i(v_{i2})$를 확인한다.

② 공개보드 상에 저장된 집계 내용과 선관위 투표정보가 일치하는지 확인한다. 단, 이 과정은 검증성을 제공하기 위하여 모든 사람들이 확인 가능하다.

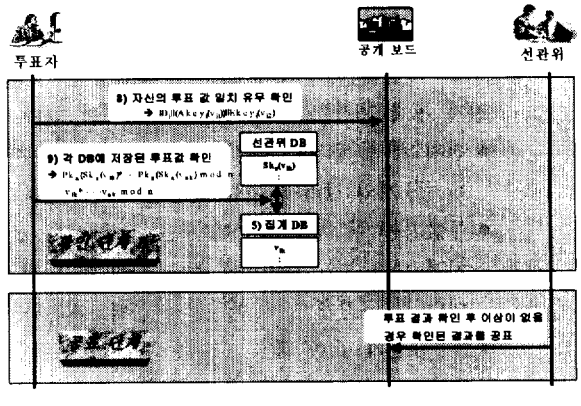
- $Pk_a(Sk_a(v_{1k}))*\cdots*Pk_a(Sk_a(v_{ik}))$ mod n
  ≡ $v_{1k}*\cdots*v_{nk}$ mod n



(그림 6) 선관위 및 집계소 투표 결과 확인 단계 흐름도

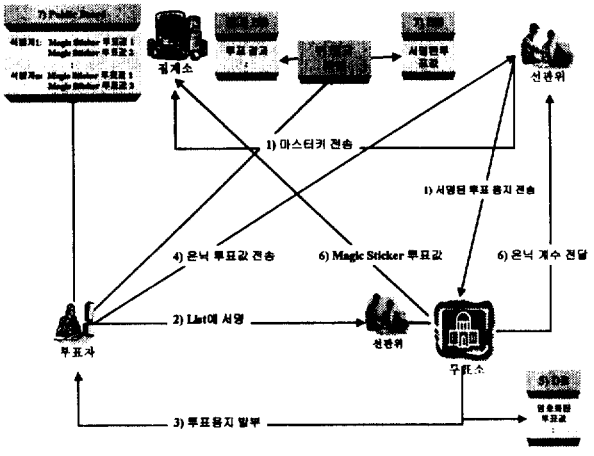
5.2.4 공표 단계

선관위에서는 투표 결과를 확인하고 이상이 없을 경우 확인된 결과를 공표한다.



(그림 7) 투표자 투표 확인 및 공표 단계 흐름도

다음의 (그림 8)은 제안 방식의 전체적인 흐름을 간략히 기술한 것이다.



(그림 8) 제안 방식 흐름도

6. 특징 및 비교 분석

본 장에서는 기존 방식과 제안 방식에 대해 요구 사항, 통신량 및 계산량 측면에서 비교 분석을 수행한다. 특히 통신량 및 계산량 측면의 비교 분석에서는 동일한 조건을 보장하기 위하여 특정 알고리즘을 가정하지 않았으며, 일반적 요구 사항을 그 대상으로 하였다.

6.1 요구 사항 만족도 비교 분석

본 제안 방식은 다음의 특징들을 통해 모든 전자 투표 요구 사항들을 만족하고 있다.

- 비밀성 : 송·수신되는 모든 투표 정보는 수신자의 공개키로 암호화되며, Magic Sticker 기법을 통해 제 3자는 투표 내용을 확인할 수 없다.
- 공정성 및 인증성 : 투표소 입실시 투표자는 선관위에 자신의 서명을 수행한 후 들어가게 되므로 하나의 투표권으로 한번 투표하게 된다.
- 공평성 : 모든 투표 결과는 투표가 완료된 다음에 공개된다.
- 무결성 : 투표 정보 전송시 무결성 보장을 위하여 인증 Magic Sticker 및 디지털 서명이 사용된다.
- 검증성 : 투표가 완료된 다음, 선관위와 집계소 정보를 통해 모든 사람들이 투표 결과들을 확인 할 수 있다.
- Receipt Free : Magic Sticker 기법을 이용하므로, 매매가 성립되었다 하더라도 l_i에 대한 정보를 모르는 한 투표 결과를 확인할 수 없게된다. 따라서 매매는 성립할 수 없다.
- Robustness : 투표 관리 요소들 간에 부정이 발생한다 하더라도, 결과 확인시 모든 요소가 확인 가능하므로 이 조건을 만족하고 있다.

다음의 <표 1>은 기존의 방식과 제안 방식을 요구 사항 측면에서 비교 분석한 결과이다.

〈표 1〉 각 방식별 요구 사항 만족도 비교 분석

	Niemi-Renvall 방식	PIK 방식	Sako	RMBM	Iversen	제안 방식
비밀성	○	○	○	○	○	○
공정성	○	○	○	○	○	○
검증성	△	○	×	△	×	○
공평성	○	○	○	○	○	○
인증성	×	△	△	△	×	○
무결성	○	○	○	○	○	○
Robustness	×	△	×	×	△	○
Receipt free	△	×	○	△	×	○

○ : 좋음 △ : 보통(환경 및 조건에 따라 부분적으로 취약) × : 나쁨

6.2 통신 및 계산 복잡도 분석

일반적으로 투표 생성 및 확인 과정은 전자 투표상의 효율성에 중요한 부분을 차지한다. 따라서 본 논문은 투표 생성 및 확인 과정상의 통신 및 계산 복잡도를 산출하여 비교 분석하는데 초점을 맞춘다. 다음은 일반적인 전자 투표 요구 사항을 대상으로 하였을 경우, 기존 방식과 제안 방식의 통신 및 계산 복잡도 분석 결과를 표로 작성한 것이다.

※ 연산 기호

• EXP	:	Exponential 연산
• MUL	:	Multiplication 연산
• EnP	:	공개키 암호화 연산
• EnS	:	대칭키 암호화 연산
• H	:	해쉬 연산
• S	:	서명 연산

〈표 2〉 각 방식별 통신 및 계산 복잡도 비교 분석

	통신회수	계산량
Niemi-Renvall	2n	EXP = n MUL = 1 EnP = 2n
PIK	2n + 3c + 1	EXP = n MUL = 1 EnP = c(c-1) + 2n H = n
Sako	4n + 4c	EXP = 11n + 3c + 4 MUL = n + c
RMBM	4n + c	EXP = (8n + 4) + 2c(c+1) MUL = 3n + 1
Iversen	6n+6	EXP = nc + 2kc + kc/2 MUL = nc + kc/2 H = nk + n + c + 3kc/2 S = 2c + n
제안방식	2n+k+2	EnP = 4n + t + b EnS = 6n MUL = n H = n S = n

n : 투표자 수, c : 선관위 수, t : 집계소의 수, b : 투표소의 수, k : 비밀 계수의 수

실제 효율성 분석에 있어 본 논문에서의 통신 및 계산 복잡도는 각 객체가 키 분배 및 투표값 전송, 확인 과정에

서 일어나는 통신회수와 계산량을 구하였다. Niemi-Renvall 방식의 경우 통신회수와 계산량 측면에서 가장 좋은 것으로 나타났으나, 이것은 단지 준비 단계 및 투표 과정에서 필요한 요소들의 생성 부분을 배제하고 실제 투표 부분에 관한 복잡도만을 측정한 것이다. 따라서 다른 방식들과의 비교 대상은 될 수 없는 것으로 판단된다. 이 방식을 제외하고 전반적인 사항을 고려해 볼 때 제안 방식이 다른 방식에 비해 통신회수와 계산 복잡도에 있어 효율적인 것을 볼 수 있다. 따라서 향후 실제 투표 시스템을 구현하는데 있어 효율적으로 적용 가능할 것이라 본다.

7. 결 론

현재 의사 결정의 수단으로서 제시되어진 투표는 그 성격상 매우 미묘한 문제가 되기 때문에 어떠한 상황에서도 부정의 소지가 있어서는 안 된다. 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 일반적인 요구사항을 제시하였다.

그와 함께, 전자 투표 상에서 발생할 수 있는 관리 요소 부정 및 투표 매매방지에 관하여 살펴보았으며, 이들 문제를 해결하기 위하여 "Magic Sticker"기법을 도입 적용하였다. 이를 통해 본 제안 방식은 안전성과 신뢰성을 확보할 수 있었으며, 특히 부정 및 매매 방지를 위한 효율적인 해결책을 제시할 수 있었다. 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.

참 고 문 헌

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

[2] 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 Science, pp.372-382, 1985.

[3] K. Koyama, "Secure Secret Voting System using the RSA Public-Key Cryptosystem," IEICE Trans., Vol.J68-D, No.11, pp.1956-1965, 1985.

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

[5] J. Benaloh, "Verifiable secret-ballot elections," Ph.D.thesis, Yale university, Technical report 561, 1987.

[6] T. Asano, T. Matsumoto and H. Imai, "A Scheme for fair Electronic Secret Voting," technical Report, IEICE Japan, ISEC 90-35, pp.21-31, 1990.

[7] 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.

[8] K. Sako, and J. Kilian, "Receipt Free Mix Type Voting Scheme-A Practical Solution to the Implementation of a Proceedings" of EUROCRYPT '95, pp.393-403, 1995.

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

[10] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung, "Multi-authority secret-ballot elections with linear work," LNCS 1233, Advances in Cryptology-EUROCRYPT '96, pp.72-83, 1996.

[11] K. Sako, and J. Killian, "Secure voting usint partially compatible homomorphisms," LNCS 839, Advances in Cryptology-CRYPTO '94, pp.411-424, 1991.

[12] R. Cramer, R. Gennaro, and B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme," LNCS 1233, Advances in Cryptology-EUROCRYPT '97, pp. 103-118, 1997.

[13] B. Schoenmakers, "A Simple publicly verifiable secret sharing scheme and its application to electronic voting," LNSC 1666, Adances in Cryptology-CRYPTO '99, pp.148- 164, 1999.

[14] 박희운, 이임영, "전자 투표 매매 방지에 관한 연구", 한국정보처리학회 춘계학술발표대회, 제5권, 제1호, 1998. 4.

[15] 박희운, 오형근, 이임영, "전자 투표에서의 선관위 부정방지에 관한 연구", 한국멀티미디어학회 춘계학술발표대회, 제1권, 제1호, pp.163-168, 1998. 6.

[16] 박희운, 이임영, "안전한 선택을 위한 Magic Sticker 기법", 한국멀티미디어학회 추계학술발표대회, 제3권, 제2호, pp.485-488, 2000. 11.

박 희 운

e-mail : heeun@cse.sch.ac.kr

1997년 순천향대학교 컴퓨터공학부 졸업 (학사)

1999년 순천향대학교 전산학전공 석사 (공학석사)

1999년~현재 순천향대 전산학전공 박사과정

관심분야 : 암호이론, 컴퓨터 보안

이 임 영

e-mail : imylee@sch.ac.kr

1981년 홍익대학교 전자공학과 졸업 (학사)

1986년 오사카대학 통신공학전공 석사 (공학석사)

1989년 오사카대학 통신공학전공 박사 (공학박사)

1989년~1994년 한국전자통신연구원 선임연구원

1994년~현재 순천향대학교 정보기술공학부 부교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안