수신자 지정 그룹 서명 방식을 이용한 Magic Sticker형 전자투표 시스템

홍종국, 박희운, 이임영
순천향대학교 정보기술공학부

A Magic Sticker typed Electronic Voting System using the Digital Nominative Group Signature

Jong-Kook Hong, Hee-Un Park, Im-Yeong Lee
Division of Information Technology, Soon-chun-hyang University
E-Mail : siro1hope@hanmail.net, phu24@hotmail.com, imylee@sch.ac.kr

요 약

정보화 사회로 대변되는 현대사회는 컴퓨터 확산 및 네트워크의 급속한 발전과 더불어 이를 이용한 많은 응용분야들이 연구되고 있으며, 이중 전자투표에 관한 연구 또한 활발히 진행중이다. 이는 기존의 투표 방식을 전자화할 경우 시간 및 비용 측면에서 많은 절약효과를 얻을 수 있기 때문이다. 그러나 이런 효율성에도 불구하고 전자투표를 실제 적용하는데 있어서 투표 참여 요소의 부정 및 투표권 매매와 투표자 익명성 보장 등 아직 해결해야할 많은 문제점들이 산재해있다.

따라서 본 논문에서는 기존 투표를 전자투표로 적용시키는 과정에서 필요한 일반적 요구사항과 부정방지 및 매매방지를 위한 특수 요구사항을 살펴볼 것이다. 특히, 투표자 익명성 보장 및 매매방지를 위해 네트워크 상에서 투표내용이 공개되더라도 사용자 익명성을 보장할 수 있는 Magic Sticker 기법을 적용함과 동시에 사용자 인증 및 메시지 인증 부분에서는 자신을 밝히지 않은 상태에서 수신자를 지정하여 자신의 신분을 증명할 수 있는 수신자 지정 그룹 서명 방식을 이용함으로서 사용자 익명성을 제공하는 안전한 전자투표 방식을 제안한다.

1. 서론

컴퓨터 및 인터넷의 보급 확산은 기존의 오프라인 상에서 제공되던 많은 서비스들을 네트워크를 통해 제공하고 있다. 즉, 사용자들이 직접 상점에 가지 않고도 인터넷을 통해 상품을 검색하고 구매할 수 있으며, 편지 대신 E-mail을 통해 서신을 주고받을 수 있게 되었다. 이를 통해 사용자들은 상품을 사고 편지를 보내기 위해 드는 시간 및 비용 절약할 수 있게 되었다. 이외에 많은 인터넷 응용 서비스들이 제공되고 있으며, 이러한 서비스를 전제로 투표를 전자화 함으로서 실생활에 보급할 수 있다면 현행 투표 시스템이 안고 있던 많은 문제점들을 해결할 수 있을 것이다. 즉, 지정된 투표소에서만 수행 가능하던 투표 작업이 역이나 공항 등의 공공장소에 있는 컴퓨터를 이용하여 수행할 수 있다면, 투표자는 장소에 구애받을 필요 없이 투표를 할 수 있으므로 일상생활에 있어 편리함을 제공하게 될 것이다.

뿐만 아니라, 투표 절차에 있어 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 전자투표의 도입은 투표 제도에 있어 획기적인 전환을 맞을 수 있게 될 것이다.

이에 대해 본 논문에서는 전자투표를 위한 일반적인 요구사항과 투표 부정 및 매매방지를 위한 특수 요구사항에 대해 살펴본다. 동시에 네트워크 상에서 투표권의 매매방지를 위해 안전한 선택 기법인 "Magic sticker" 기법을 도입할 것이다. 또한 투표권자의 인증

본 연구는 2001년도 한국과학재단 지역대학 우수과학자 지원사업을 통해 수행된 것입니다.

에 있어서 자신의 신분을 밝히지 않은 상태에서 자신이 속한 그룹의 소속원이라는 것을 수신자를 지정하여 증명할 수 있는 수신자 지정 그룹 서명방식을 적용함으로서 사용자의 익명성을 보장할 것이다. 이를 통해 본 제안 방식은 일반적인 요구사항뿐 아니라 부정 및 매매를 방지함으로서 신뢰성과 안전성을 제공할 것이다.

2. 전자투표를 위한 요구사항

2.1 일반 요구사항

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

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

2.2 특수 요구사항

전자투표는 공개된 네트워크를 대상으로 한다. 따라서 투표자의 투표 결과를 확인하는 과정이 필수적으로 요구되며, 투표 결과들은 투표 수행 후 네트워크를 통해 선관위나 집계소로 전송된다. 이러한 일련의 과정들은 네트워크 특성상 중간 단계에서 투표 관리자들에 의한 부정이나, 투표자 사이의 매매가 가능함을 시사한다. 그러므로 전자투표 시스템은 이를 방지하기 위해서 다음과 같은 특수한 요구사항을 만족해야 한다.

- Receipt Free : 이 특성은 매매 방지를 위한 특성으로서, 어느 누구도 투표자의 개별 투표 결과를 검증할 수 있어서는 안된다[1][2][3][4].
- Robustness : 이 특성은 투표 관리 요소의 부정 방지를 위한 특성으로서, 누구나 각 참여자의 오류 또는 부정행위를 확인할 수 있어야 한다[5][6][7].

3. 기반 기술

3.1 수신자 지정 그룹 서명 방식

다음은 특정 수신자를 대상으로 서명자의 신원을 노출시키지 않으면서 자신의 신분을 인증할 수 있는 수신자지정 그룹 서명 방식에 대해 설명한다.

3.1.1 시스템 계수

- p : 소수 ≥512 bit
- q : 소수 ≥160 bit (q | p-1)
- g : 생성자
- k_1, k_2 : 랜덤 수 $\{k_1, k_2\} \in {}_RZ_P$
- X_Z : 수신자 Z의 비밀키
- Y_Z : 수신자 Z의 공개키
- H : 160bit 출력을 내는 안전한 일방향 해쉬 함수
- M : 메시지 M
- K_{PG} : 서명자의 소속 확인용 공개키 리스트
- K_{SU} : 서명자의 소속 서명 키 리스트
- S : 서명

3.1.2 소속 등록 및 키 분배 단계

소속의 등록은 TC(Trusted Center)가 관할하며, 소속에 등록 및 키를 분배받기 위해서는 다음과 같은 일련의 과정을 거친다.

(1) 서명자는 자신의 신상 정보 (서명자 이름, ID, 소속, 기타)를 TC에게 제공한다.

(2) TC는 서명자의 소속 확인이 끝난 후 비밀키 리스트를 안전한 방식으로 전달한다.

- $K_{SU} = K_{SL1}, \ldots, K_{SLn}$ (비밀키 리스트)
- $K_{SUk} = K_{SL1}, \ldots, K_{SLk}$ (단, $1 \le k \le n$)

(비밀키 리스트에서 k개의 키를 추출한 것)

서명자의 비밀키는 총 n개의 분할된 키를 갖게 된다. 이 키는 TC에서 만든다고 가정하며, 각 서명자의 공개키로 암호화해 분배되거나, IC카드와 같은 물리적인 형태로 분배된다. 각 서명자는 서명 수행을 위해 분배된 키 리스트 중에서, 날짜 또는 TC의 권고에 따라 k개를 선택해 서명 수행이 가능하다.

따라서 서명 확인을 위한 공개키는 수시로 변화되므로 안전성을 확보할 수 있으며, 별도의 키 생성을 위해 TC가 연산을 수행할 필요가 없기 때문에 효율적이다.

(3) TC는 서명자의 공개키들을 공개키 리스트에 등록한다.

• $K_{PGk} = g^{KSUk} \bmod p$ (단, $1 \le k \le n$)
=> 공개 보드에 등록

3.1.3 서명 수행 단계

(1) 서명자는 다음과 같은 정보를 생성한다.
• 큰 소수 p와 q를 생성한 다음 공개한다.
• 생성자 g를 계산한다.
: $h \in \{1,...,p-1\}$를 선택한다.
: $g = h^{(p-1)/q} \bmod p$가 되는 g를 계산해 낸다.
: g를 공개한다.

(2) 수신자는 자신의 비밀키와 공개키를 생성한다.
• 자신의 일반 서명용 개인키를 생성한다.
: X_Z (단, $0 < X_Z < q$인 난수)
• 공개키는 다음과 같이 생성한다.
: $Y_Z = g^{XZ} \bmod p$

(3) 서명자는 다음과 같이 서명 정보를 생성하여 수신자 Z에게 전송한다.
• 랜덤 수 k_1, k_2를 다음과 같이 생성한 후 e를 계산한다.
: $\{k_1, k_2\} \in {}_RZ_P$
: $e = g^{k2-k1} \bmod p$
• 수신자 Z의 공개키를 이용하여 다음을 계산한다.
: $D = Y_Z^{k2} \bmod p$
• 해쉬 함수를 이용하여 다음을 계산한 다음 서명 정보를 생성한다.
: $R = H(g^{k1} \bmod p \,||\, M \,||\, e \,||\, D)$
: $S = k_1 - K_{SUk} * R \bmod q$
• 다음을 수신자에게 전송한다.
: (M, R, e, D, S) => 수신자

3.1.4 서명 검증 단계

(1) 수신자는 다음을 확인함으로서 서명자의 신분을 확인한다.
• 해쉬를 이용하여 R이 정확한지 확인한다.
: $H(g^S * K_{PG}{}^R \bmod p \,||\, M \,||\, e \,||\, D) = R$

(2) 확인된 R을 통해 다음 수식이 만족한다면 서명은 유효하다고 판단한다.
: $(g^S K_{PG}{}^R e)^{XZ} = D \bmod p$

3.2 안전한 선택을 위한 Magic Sticker 기법

다음은 물리적 매직 스티커 기법에 대한 설명이다. 매직 스티커는 2개 이상의 영상을 편광 각도가 다른 홀로그래피(holography) 필름에 2차원으로 합성시켜 광원의 각도에 따라 서로 다른 형체를 표현할 수 있도록 한 필름형 스티커를 의미한다. 그림 1은 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, 매직 스티커를 생성할 때 적용된 특수 정보를 아는 사람만이 확인 가능하다.

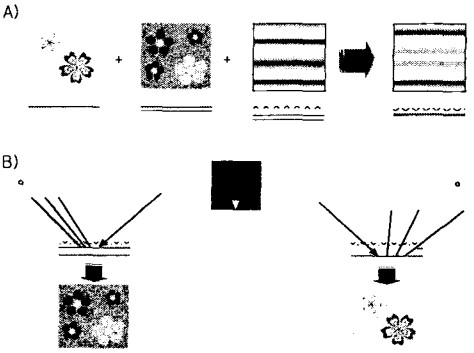

그림 1. 물리적 매직 스티커의 일반적인 형태

이러한 정보는 만약 특수 정보를 모르는 사람이 인위적으로 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 생성자가 2개의 영상 중 하나를 선택한 값이라면, 물리적으로 안전한 선택이 가능해 진다. 이러한 특성을 암호학적으로 접근할 경우 안전한 선택(secure selection) 서비스를 네트워크 상에서도 수행할 수 있게 된다[9].

4. 새로운 전자투표 방식 제안

본 방식은 상기 제시된 요구사항을 만족하기 위하여 Magic Sticker 기법과 수신자 지정 그룹 서명 방식을 적용한다.

4.1 시스템 계수

• CTA(Central Tabulating Agency): 선거관리위원회
• V_i, Q_i, G_i: 투표자, 집계소, 투표소 (i = 1, 2, 3, ... , n : n은 각 요소의 수)
• K_{GSi}, K_{GVi}: CTA가 생성한 수신자 지정 그룹 서명

키 및 확인 키

- 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: 투표자의 투표 선택 확인값 ($l \in \{0, 1\}$)
- k_i: 투표자가 선택한 투표결과 확인용 키 값
- ID_i: 투표자 i의 가명 식별자
- r_i: 투표자 i가 선택한 값 ($r \in \{0, 1, \ldots, n\}$, n은 선택할 항목의 개수)
- T : Time-Stamp

4.2 프로토콜

4.2.1 준비 단계

(1) 선관위

(가) 투표 대상자를 확인하여 투표자 명부를 작성하고 투표자에게 투표 안내문을 발송한다.

(나) 선관위는 투표자에게 제공할 가명 식별자 ID_i와 수신자 지정 그룹 서명에 사용할 서명용 키 K_{GSi} 및 서명 확인용 키 K_{GVi}를 생성한다.

(다) ID_i에 서명을 수행한 다음, ID_i와 수신자 지정 그룹 서명키 K_{GSi}를 연접해 투표용지를 구성한 후 투표소의 공개키로 암호화하여 투표소에 전달한다.

- $Pk_{gi}(Sk_a(ID_i)||ID_i||K_{GSi})$

(라) 수신자 지정 그룹 서명 확인 키 K_{GVi}를 선관위의 서명을 수행한 후 집계소의 공개키로 암호화하여 집계소에 전송한다.

- $Pk_{qi}(Sk_a(K_{GVi}))$

4.2.2 투표 단계

(1) 투표자

(가) 투표일이 되면 투표소에서 자신을 물리적으로 확인하고 입장한다. 이때 물리적 확인은 선관위를 통해서 하게되며, 등록 list에 투표자 자신의 서명을 하게 된다.

- $Sk_{vi}(list)$
- 이때 등록 list는 확인 과정에서 선관위에 의해 투표 참여 인원수와 집계소에서 집계한 투표 인원수를 비교하기 위해 사용된다.

(2) 투표소

(가) 선관위로부터 받은 투표용지 중 하나를 랜덤하게 선택하여 투표자에게 발급한다.

- $Sk_a(ID_i)||ID_i||K_{GSi}$

(나) 투표 과정을 기술하기 이전에 투표자가 사용할 전자투표용지는 다음 사항을 만족하야 한다.

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

(3) 투표자

(가) 투표자는 v_{i1}, v_{i2}를 결정한다.

(나) 투표 확인값 $l_i \in \{0, 1\}$을 선택한다.

(다) 0을 선택할 경우 투표값 v_{i1}이 집계에 반영되고 1을 선택하면 투표값 v_{i2}가 집계에 반영된다.

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

(라) 투표값을 결정하고 난 다음, 랜덤 값 r_i와 투표값 확인을 위한 키 k_i를 선택한다.

(마) 다음과 같이 l_i에 따라 집계될 투표값을 결정하고 다음과 같이 투표용지를 구성한다. 이때 실제 집계에 반영되는 투표값은 키 값의 왼쪽에 놓이게 된다.

- l_i값이 0일 경우
  : $(v_{i1}||k_i)||v_{i2}||l_i$
- l_i값이 1일 경우
  : $(v_{i2}||k_i)||v_{i1}||l_i$

(바) 투표결과 값과 $Sk_a(ID_i)$ 및 투표 시간을 나타내는 타임스탬프(T) 값을 이용하여 다음을 계산한다.

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

(사) 투표 결과 값 Z_i를 집계소의 공개키로 암호화한 후 투표소로부터 받은 수신자 지정 그룹 서명용 키를 이용하여 서명을 수행한다.

- $K_{GSi}(Pk_{qi}(Z_i))=R_i$

(아) 투표 완료 후 투표자가 선택한 v_{il}값은 다음과

같이 계산하여 선관위로 전송한다.

• $Pk_a(ID_i||Pk_a(r_i)*(v_{il}))$

(4) 투표소

(가) 투표자가 선택한 r_i값과 투표 정보 R_i를 투표소의 DB에 저장한다.

• r_i, R_i

(나) 투표 시간이 마감되면 DB에 저장된 투표 정보에 다음과 같이 계산하여 각각 집계소와 선관위로 전송한다.

• R_i를 집계소로 전송한다.

• $Pk_a(Sk_{gi}(ID_i||r_i))$를 선관위로 전송한다.

4.2.3 확인 단계

(1) 집계소

(가) 선관위로부터 전송된 수신자 지정 그룹 서명 확인키를 이용하여 그룹 서명을 확인한다.

• $K_{GVi}(R_i) = Pk_{qi}(Z_i)$

(나) 서명 확인 후 집계소의 개인키로 투표값을 복호화하고 타임스탬프를 확인한다. 키 값 k_i의 왼쪽에 있는 투표결과 값을 집계에 반영한다.

• $Sk_{qi}(Pk_{qi}(Z_i)) = (v_{i1}||k_i)||v_{i2}||l_i||Sk_a(ID_i)||$ T

• v_{i1} 값을 집계에 반영한다.

(다) 투표자의 ID_i와 키 값 k_i 및 투표값을 집계소의 DB에 저장한다.

(라) 집계 완료 후 집계에 반영된 투표값을 공개보드 상에 저장한다.

(2) 선관위

(가) 투표 정보를 복호화 한다. 그런 다음 r_i와 관련된 정보에서 투표소의 서명을 확인하고 자신의 개인키로 복호화 한다.

• $Sk_a(Pk_a(ID_i||Pk_a(r_i)*v_{il})) = ID_i||Pk_a(r_i)*v_{il}$

• $Pk_{gi}(Sk_a(Pk_a(Sk_{gi}(ID_i||r_i)))) = ID_i||r_i$

(나) 추출된 r_i값과 자신의 개인키를 이용하여 선관위 서명 투표 결과를 공개한다.

• $(Sk_a(Pk_a(r_i)*v_{il}))r_i = Sk_a(v_{il})$

(다) 다음의 수식을 이용하여 공개보드 상에 저장된 집계 내용과 투표소에서 전송되어온 투표 정보가 일치하는지 확인한다.

• $Pk_a(Sk_a(v_{1l}))*\cdots*Pk_a(Sk_a(v_{il}))$ mod n

<=> $v_{1i}*\cdots*v_{ni}$ mod n

(라) 투표자 등록 list에 서명된 투표자 수와 공개보드 상에 저장된 투표자 인원수가 일치하는지 확인한다. (다) 및 (라)를 만족하면 투표결과는 accept 된다.

(3) 투표자

(가) 투표자는 자신이 생성한 키 값 k_i를 이용하여 집계소에 저장된 자신이 선택한 투표결과를 확인한다. 집계소에서는 키 값이 일치한다면 실제 집계에 반영된 투표값을 확인시켜주고 일치하지 않는다면 투표자가 선택한 다른 투표값을 보여준다. 만약 집계에 반영된 투표값이 v_{il}이라면,

• k_i 값 일치

: v_{i1}

• k_i 값 불일치

: v_{i2}

(나) 공개보드 상에 저장된 집계 내용과 선관위 투표정보가 일치하는지 확인한다.

• $Pk_a(Sk_a(v_{1l}))*\cdots*Pk_a(Sk_a(v_{il}))$ mod n

<=> $v_{1i}*\cdots*v_{ni}$ mod n

4.2.4 공표 단계

선관위는 투표 결과를 확인하고 이상이 없을 경우 확인된 결과를 공표한다.

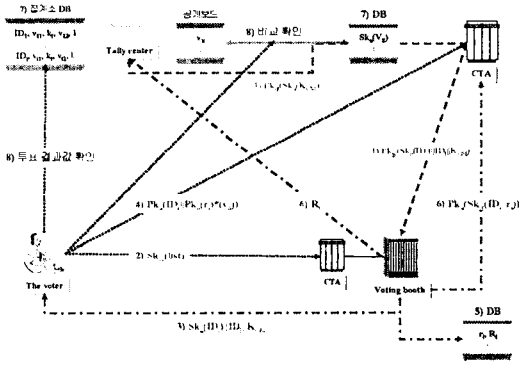

그림 2. 제안방식 흐름도

4.3 요구 사항 만족도 분석

본 제안 방식은 다음의 특징들을 통해 모든 전자투표 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 단 한번 투표하게 된다. 또한 투표값 전송에 있어서 수신자 지정 그룹 서명 방식을 통해 투표자의 소속 인증과 익명성을 제공하며, 오직 수신자만이 전송된 값을 확인할 수 있다.
- 공평성 : 모든 투표 결과는 투표가 완료된 다음에 공개된다.
- 무결성 : 투표 정보 전송시 무결성 보장을 위하여 투표소의 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 집계소를 통해 보여지는 메시지가 정당한 투표값인지를 검증할 수 없게 된다.
- Robustness : 투표 관리 요소들 간에 부정이 발생한다 하더라도, 투표 결과 확인 시 모든 요소가 확인 가능하므로 이 조건을 만족하고 있다.

따라서 Magic Sticker 기법과 수신자 지정 그룹 서명방식을 이용한 본 전자투표 방식은 익명성을 보장함과 동시에 안전한 선택이 가능한 방식이다.

5. 결론

인터넷의 보급 확산은 오프라인 상에서 제공되던 서비스들을 가상공간을 통해 제공하고 있다. 기존 투표 방식 또한 전자화하여 실생활에 적용한다면 투표 및 개표에 소요되는 인력 및 투표용지 제작과 투표함 운송에 드는 비용을 절약할 수 있으며, 집계에 있어서 전자적으로 수행됨으로 정확성 및 편리성을 제공할 것이다. 그러나 투표에 있어 투표자의 익명성은 필히 보장되어야하며, 투표 부정 방지 및 매매 방지 또한 제공되어야 할 것이다.

따라서 본 논문에서는 투표자의 익명성을 보장하는데 그 초점이 맞추었으며, 이를 위해 안전한 선택 기법인 Magic Sticker 기법을 적용함으로서 투표값이 공개되더라도 투표자의 익명성을 보장하고 있다. 또한 Receipt free 및 Robustness와 같은 특수 요구 사항을 만족함으로서, 각 요소간의 부정을 방지를 통한 안전한 선택이 가능하게 되었으며, 투표자 인증 및 전송되는 정보의 인증을 위한 수신자 지정 그룹 서명 방식의 적용은 자신이 누구라는 것을 밝히지 않은 상태에서 수신자를 지정하여 자신의 신분을 증명함으로서 익명성을 제공한다.

이들을 통해 향후 전자투표를 실생활에 적용함에 있어 안전성과 편리성을 제공할 것이다.

[참고문헌]

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

[2] J. Benaloh and D. Tuinstra, "Receipt Free Secret Ballot Elections," proceedings of the 26th ACM Symposium on the Theory of Computing, pp.544-553, 1994.

[3] 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.

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

[5] 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.

[6] K. Ohta, "An Electrical Voting Scheme Using a Single administrator," 1998 Spring National Convention Record, IEICE, A-294, 1988.

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

[8] 박희운, 오형근, 이임영, " 전자투표에서의 선관위 부정방지에 관한 연구," 한국멀티미디어학회 춘계학술발표대회, pp163-168, 1998. 6.

[9] 박희운, 이임영, "안전한 선택을 위한 Magic Sticker 기법," 한국멀티미디어학회 추계학술발표대회, 2000.