Screw 기법을 이용한 Magic Sticker 전자 투표 방식

박희운[0] 이임영
순천향대학교 정보기술공학부
phu24@hotmail.com imylee@sch.ac.kr

The Magic Sticker Electronic Voting Scheme using the Screw Method

Hee-Un Park[0] Im-Yeong Lee
Division of Information Technology Eng. Soonchunhyang Univ.

요 약

정보 사회의 급속한 발전을 통해 유·무선 환경에서 다양한 응용 분야들이 창출되고 있다. 그 중에서 전자 투표는 그 효용성 측면에서 새로이 관심을 가지는 분야이다. 그러나, 아직까지는 공개 네트워크를 이용하여 투표를 수행할 경우 보안 측면에서 여러 고려 사항들이 존재하며, 이들이 만족되지 않을 경우 투표의 신뢰성을 떨어뜨리게 된다.

본 논문은 전자 투표를 위해 필수적으로 요구되는 보안 사항들을 일반 요구 사항과 특수 요구 사항으로 분류하고, 이들 요구사항을 만족하는데 필요한 Screw method와 Magic Sticker 방식을 제안한다. 동시에 이들을 기초로 새로운 전자 투표 기법을 제안하고, 요구 사항을 만족하는지 평가할 것이다.

1. 서 론

정보 사회를 거치면서 네트워크의 발전과 관련된 다양한 응용 분야들이 연구되고 있는데, 그 중에서도 암호학을 이용한 전자 투표의 비중이 증대되고 있다. 이러한 전자 투표는 시간 및 장소의 한계를 극복하고 있으며, 비용의 절감을 제공한다는 측면에서 이용 가치가 매우 높다. 그러나, 그 중요성에도 불구하고 전자 투표는 아직까지 많은 취약점이 산재하고 있다. 특히, 전자 투표에 참여하는 각 개체들이 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 요구되는 보안 사항들을 확인해 보고, 이들을 만족하는데 필요한 "Magic Sticker" 및 "Screw method" 기법을 제안한다. 동시에 이들에 기초한 새로운 전자 투표 기법을 제시하고, 요구 사항 만족도 및 기존 방식과의 비교 결과를 살펴보도록 하겠다.

2. 요구 사항

2.1 일반 요구 사항

전자 투표 시스템은 성격상 기존의 일반적인 투표가 갖는 주요 특성들 즉, '비밀 투표'나 '무기명 투표' 등등을 만족해야 한다. 이는 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.

- 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 투표 결과를 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 요구 사항

전자 투표는 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 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[1][2][3][4].
- Robustness : 이 특성은 투표 관리 요소의 부정 방지를 위한 특성으로서, 누구나 각 참여자의 오류 또는 부정 행위를 확인할 수 있어야 한다[5][6][7].

3. 새로운 기반 기술 방식

3.1 Magic Sticker

Magic Sticker는 2개 이상의 영상을 편광 각도가 다른 홀로그래피(Holography) 필름에 2차원으로 합성 시켜 광원의 각도에 따라 서로 다른 영상을 볼 수 있는 한 필름형 Sticker를 의미한다. 그림 1은 이에 대한 간단한 구조를 그림으로 표현한 것이다. A)는 2개의 영상과 필름을 합성한 형태를 보이고 있으며, B)는 빛의 편광 각도 θ에 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 θ 및 위치(특수 정보)를 아는 사람만이 확인 가능하다.

이러한 정보는 만약 특수 정보를 모르는 사람이 인위적으로 필름을 벗겨낼 경우에는 저장된 정보 및 영상의 내용을 확인할 수 없게된다. 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, 투표 매매로부터 안전한 프로토콜이 가능해진다[8].

본 연구는 2001년도 한국과학재단 지역대학 우수과학자 지원 연구에 의해 수행된 것입니다.

그림 1. 물리적 Magic Sticker의 일반적인 형태

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].

3.2 Screw Method

일반적인 나사 구조를 고려해 보자. 이 구조는 정확한 암나사가 없을 경우 결합이 불가능하며, 순차적으로 암·수나사를 결합하는 방법 외에는 결코 완전한 결합체를 얻을 수 없다. 이러한 모델을 전자적인 프로토콜 상으로 적용할 경우, 특정한 순서가 정해지면 그 순서를 위반하고서는 결과가 나올 수 없음을 보여주고 있다. 즉, 네트워크 상에서 ordered issue화 된 프로토콜이 생성될 수 있는데, 이를 Screw Method 기법이라 한다. 이 기법을 전자 투표에 적용시킬 경우 시스템 상의 관리자들로부터 투표 결과에 대한 안전성을 획득할 수 있으며, 관리자 상호간의 부정을 방지할 수 있게 된다.

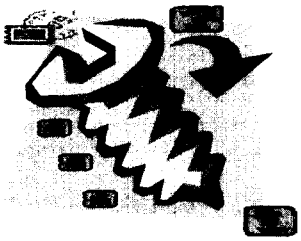

그림 2. Ordered Issue화된 Screw method 모델

4. 새로운 전자투표 기법 제안

본 장에서는 2장에서 요구되었던 일반 및 특수 요구사항을 만족하는 새로운 전자투표 기법을 제안한다. 본 방식은 특수 요구사항을 만족하기 위해 새로이 제안한 Magic Sticker 기법과 Screw Method 기법을 암호학적으로 적용한다.

4.1 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수를 기술한 것이다.

- V_i, G_i, T_i, CTA : 투표자, 투표소, 집계소, 선관위
- v_i, $V_{\_result}$: 투표자 i의 투표 값 및 투표 결과 정보
- $r_{\_MSi}$, $r_{\_salti}$, $r_{\_seed}$: 투표자의 매직 스티커 θ, 선관위의 salt 값, 집계소의 seed 값
- ID_i : 선관위가 생성한 투표자의 가명 식별자
- $EK_{P(S)\_*}$, $DK_{P(S)\_*}$: *의 공개키 또는 개인키로의 암호화 및 복호화
- f, h : 대칭형 투표 함수 및 일방향 해쉬 함수

4.2 프로토콜

1) 준비 단계

가) 선관위 CTA

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

(2) 선관위는 투표자에게 제공할 가명 식별자 ID_i와 Salt 값 $r_{_salti}$을 생성한다. 이때, $r_{_salti}$는 투표 용지에 저장되게 되며, 해당 투표자 및 투표소만이 이 정보를 확인한다.

(3) ID_i에 서명을 수행하고, ID_i와 투표시 사용될 Salt 값을 연접해 투표 용지를 구성한 다음, 투표소의 공개키로 암호화하여 투표소에 전달한다. 단, 투표 용지의 개수는 해당 투표구의 선거인 명부 인원에 근거해 발송되게 된다.

- $EK_{P\_Gi}(ID_i \| r_{\_salti})$

나) 집계소 T_i

T_i는 Seed 값 $r_{_seed}$에 기초한 투표 함수 f를 구성하여, 투표소의 공개키로 암호화하여 전송한다. 이때 만들어진 Seed 값은 오직 집계소만이 소유한다.

2) 투표 단계

가) 투표자 V_i

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.

- $EK_{S\_Vi}(list)$

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

나) 투표소 G_i

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

다) 투표자 V_i

(1) Magic Sticker의 θ값 $r_{_MSi}$를 선택한다.

(2) 투표자는 투표 값 v_i를 결정한다.

(3) 투표 함수 f를 이용하여, 다음과 같이 투표 결과 $V_{_result}$를 생성한다.

- $V_{\_resulti} = f(v_i \oplus r_{\_seed}) \| f(r_{\_salti}(v_i \oplus r_{\_MSi}) \oplus r_{\_seed}) \| \ldots \| f(v_k \oplus r_{\_seed})$

(단, $V_{\_n}=\{후보자_1, \ldots, 후보자_n\}$, $v_i \in V_{\_n}$, $V_{\_s} \subset V_{\_n}$, $v_j, v_k \in V_{\_s}$)

(4) 투표가 완료되면, 다음의 정보를 투표소에 저장한다.

- $EK_{P\_Gi}(ID_i \| V_{\_resulti} \| r_{\_salti})$ --> 투표소

라) 투표소 G_i

투표소는 다음의 정보를 선관위 및 집계소로 전송한다.

- 선관위 : $V_{Ci}' = EK_{P\_CTA}(EK_{S\_Gi}(ID_i \| V_{\_resulti}))$
- 집계소 : $V_{Ci} = EK_{P\_Ti}(EK_{S\_Gi}(ID_i \| V_{\_resulti}))$

3) 확인 단계

가) 선관위 CTA 및 집계소 T_i

(1) 투표 시간이 종료되면, 선관위와 집계소는 자신들이 생성했던 ID_i, r_salt_i와 r_seed를 각각의 공개키를 이용해 교환한다.

(2) 자신의 개인 키와 투표소의 공개키를 이용해 수신된 투표 정보를 복호한다.

- 선관위 : $DK_{S\_CTA}(EK_{P\_Gi}(V_{Ci}')) = ID_i \| \| V\_result_i$
- 집계소 : $DK_{S\_Ti}(EK_{P\_Gi}(V_{Ci})) = ID_i \| \| V\_result_i$

(3) 양자간에 교환된 투표 생성 관련 정보를 통해 투표 결과를 복호한다.

- $f(V\_result_i) = v_j \| \| r\_salt_i(v_i \oplus r\_MSi) \| \| \ldots \| \| v_k$
- $r\_salt_i(v_i \oplus r\_MSi)/r\_salt_i = v_i \oplus r\_MSi$

나) 투표자 V_i

투표자는 자신의 θ 값 r_MSi, 자신의 ID_i 및 확인을 원하는 투표 결과를 연접하여 선관위 및 집계소의 공개키로 암호화하여 전송한다. 이때, 투표 확인 결과를 위한 값은 V_result_i 값 중에 임으로 선택하여도 무방하다.

- 선관위 : $EK_{P\_CTA}(ID_i \| \| f(r\_salt_i(v_i \oplus r\_MSi) \oplus r\_seed) \| \| r\_MSi)$
- 집계소 : $EK_{P\_Ti}(ID_i \| \| f(r\_salt_i(v_i \oplus r\_MSi) \oplus r\_seed) \| \| r\_MSi)$

다) 선관위 CTA 및 집계소 T_i

(1) 수신된 투표자의 r_MSi를 통해 투표 값을 복원한다.

- $(v_i \oplus r\_MSi) \oplus r\_MSi = v_i$

(2) 집계소는 복원된 정보를 다음과 같이 투표자에게 확인시킨다.

- $ID_i \| \| v_i$

(3) 집계소는 투표 확인이 끝나면 각 투표 결과를 공개한 다음, 선관위 명부의 선거인 수와 투표 결과 수를 비교한다.

- $v_{1k}, \ldots, v_{nk}$ (n = 투표자 수, k ∈ {투표 결과들})

(4) 선관위는 각 투표자의 투표 결과를 다음과 같이 해쉬 함수를 이용하여 공개한 다음, 투표 결과 개수와 선거인 명부 상의 투표인 수가 일치하는지 비교한다.

- $H = h(v_{1k} \oplus \ldots \oplus v_{nk})$

라) 모든 투표 관련 개체들

다음의 수식을 확인함으로서 최종 투표 결과를 확인한다.

- $h(v_{1k} \oplus \ldots \oplus v_{nk}) = H$

4) 공표 단계

선관위에서는 투표 결과를 확인하고 이상이 없을 경우 확인된 결과를 공표한다.

5. 요구 사항 만족도 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 단 한 번 투표하게 된다.
- 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 투표 값인지를 검증할 수 없게된다.
- Robustness : 투표 관리 요소들 간에 부정이 발생한다 하더라도, Screw 기법을 통해 투표 확인 절차는 순서를 가지게된다. 또한, 투표 결과 확인시 모든 요소가 확인 가능하므로 이 조건을 만족하고 있다.

6. 결론

정보 사회의 발전은 새로운 응용 서비스들을 요구하고 있으며, 특히 전자 투표에 대한 관심이 증가하고 있다. 전자 투표는 효용성 및 비용의 절감을 제공하는데 비해 아직까지 많은 보안적 문제점들이 야기되고 있다.

본 논문은 이들을 근거로 신뢰성을 제공하는 전자 투표를 위한 일반적 요구 사항들과 투표 매매 및 부정 방지를 위한 특수 요구 사항들을 기술하였다. 특히 특수 요구 사항들을 만족하기 위해 "Magic Sticker" 및 "Screw method" 개념 및 모델을 제시하였고, 이 두 방식을 근거로 새로운 전자 투표 기법을 제안하였다. 본 방식은 신뢰성을 제공하기 위한 모든 요구 사항들을 만족함으로서, 향후 안전한 전자 투표 시스템 개발의 밑거름이 되리라 판단된다.

참고 문헌

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

[2] 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.

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

[4] 박희운, 이임영, "전자 투표 매매 방지에 관한 연구," 한국정보처리학회 춘계학술발표대회, 제 5권, 제 1호, 1998. 4.

[5] 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.

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

[7] 박희운, 오형근, 이임영, "전자 투표에서의 선관위 부정방지에 관한 연구," 한국멀티미디어학회 춘계학술발표대회, 제 1권, 제 1호, pp.163-168, 1998. 6.

[8] 박희운, 이임영, "안전한 선택을 위한 Magic Sticker 기법," 한국멀티미디어학회 추계학술발표대회, 제 3권, 제 2호, pp.485-488, 2000. 11.