전자투표 신뢰성 향상을 위한 암호학적 영수증 발급기술†

이광우, 이윤호, 정한재, 김승주, 원동호*

성균관대학교 정보통신공학부 정보보호연구소

A Cryptographic Receipt for trustworthy e-Voting†

Kwangwoo Lee, Yunho Lee, Hanjae Jeong, Seungjoo Kim, and Dongho Won*

Information Security Group, School of Information and Communication Engineering, Sungkyunkwan University

요 약

최근 사회적 이슈가 되고 있는 전자투표는 관리적 측면에서는 유용하지만, 사회적으로 투표기의 동작에 대한 신뢰성을 확보하지 못하여 도입에 어려움을 겪고 있다. 본 논문에서는 전자투표기에 대한 신뢰성을 높이기 위하여 투표소 밖으로 가지고 나갈 수 있는 영수증 발급 기술을 제안한다. 이 방식은 기존 방식과 비교하여 특별한 용지나 프린터가 필요없고, 투표소 내의 기기나 관리자를 신뢰하지 않아도 되므로 실제 투표에 유용하게 사용될 수 있다.

I. 서론

현재의 종이투표 방식은 개표의 효율적인 업무 처리를 위하여 전자개표기를 도입하는 등의 노력을 하고 있지만, 광학 스캐닝 방식을 이용한 전자개표기의 경우 기기 특성상 인식 오류가 발생할 확률이 있기에 추가적인 인력이 배치되어야 하는 단점을 가지고 있다. 이와 비교하여 전자투표를 도입할 경우에는 투·개표에 소요되는 시간 및 인력을 현저하게 줄일 수 있으며, 정확한 집계가 가능할 것으로 기대하고 있다. 하지만, 이전의 연구를 통해 제안되었던 전자투표 시스템의 경우, 유권자에게 신뢰성을 제공하기 위해 밀폐된 유리창을 통해 투표 사실을 암호화하지 않고 투표기록지를 보여줌으로써, 투표기를 신뢰할 수 있도록 제안되고 있다. 투표소 내에서만 눈으로 확인 가능한 투표기록지를 보여주는 경우에는 재검표에 사용될 수 있으나, 투표자가 투표기록지를 확인하더라도 전자적인 기록은 검증할 수 없기 때문에 결과적으로 투표기록지에 대한 재검표가 반드시 수행되어야 하며, 이는 전자투표의 장점을 기대하기 어렵게 한다. 물론 전자투표기를 믿고 사용하기 위한 방안으로 오픈소스 방침이나 공인기관을 통한 투표기 검증 등의 정책적인 논의가 있었으나, 오픈소스에 따르는 공격위협과 공인기관에 대한 불신 등으로 인해, 투표 검증을 위해 사람이 개입되는 것은 최소화되어야 한다. 따라서 전자투표에 대한 신뢰성을 높이기 위하여 전자적인 기록 외에 투표자가 자신의 투표를 신뢰할 수 있도록 하기 위한 현실적인 대안으로 투표소 밖으로 가지고 나갈 수 있는 투표 검증용 영수증(Receipt)을 발급하는 것이 주목을 받고 있다[5][6]. 전자투표에 대한 신뢰는 크게 전자적인 기록에 대한 신뢰(Cast-as-intended)와 개표 결과에 대한 신뢰(Counted-as-cast)로 구분할 수 있으며, 전자는 개별 검증성(individual verifiability)이라고 하며, 후자를 전체 검증성(universal verifiability)이라 한다. 즉, 투표자는 자신이 의도한 투표값

* 교신저자 : 원동호(dhwon@security.re.kr)

† 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터(ITRC) 육성·지원사업의 연구결과로 수행되었음.

이 기록되었음을 개별적으로 확신할 수 있어야 하고, 이렇게 기록된 투표값으로부터 나온 개표 결과는 누구나 검증할 수 있어야 한다는 의미이다. 현재 전체 검증성은 읽기전용게시판(bulletin board)이나 믹스넷을 이용한 방법들이 제안되어 안전성이 입증되어 있지만, 공개 게시판에 등록된 투표 결과가 자신이 의도한 투표값을 암호화한 것임을 확신할 수 있도록 하기 위해 투표 영수증을 발급한다.

본 논문의 구성은 다음과 같다. 2장에서는 전자투표의 요소 기술이 되는 믹스넷과 확률적 암호화를 살펴보고 각각이 적용되는 경우를 설명한다. 3장에서는 기존에 연구되었던 투표소 밖으로 가지고 나갈 수 있는 투표 영수증 기술들을 살펴본다. 4장에서는 기존 기술들이 가지고 있는 단점을 보완하여 실제 투표에 활용할 수 있는 종이 영수증 발급 기술을 제안하며, 5장에서는 제안한 영수증 발급을 기존에 제안된 방식과 비교한다. 마지막으로 6장에서 결론을 맺는다.

II. 요소 기술

전자투표 영수증 발급 기술에 사용되는 요소 기술에는 믹스넷과 확률적 암호화 방식이 있다. 믹스넷(Mix-net)은 1981년 Chaum[1]에 의해 소개되었으며, 입력값과 출력값 사이의 연결정보를 알 수 없도록 섞는 방식이다. 전자투표에서는 유권자의 투표값에 익명성을 제공하기 위해 필수적으로 사용된다. 믹스넷은 다수 개의 믹스 서버로 구성되며, 각각의 믹스 서버는 초기입력 정보 또는 이전 믹스 서버의 출력값을 입력 정보로 하여 임의로 순환(rotate)되도록 하며, 이때 각 믹스서버는 순환이 올바르게 수행되었음을 증명해야 하는데, 영지식 증명, RPC (Randomization Parity Check) 등이 사용된다. 믹스넷은 크게 복호화 믹스넷과 재암호화 믹스넷이 있으며, 본 논문에서는 재암호화가 가능한 ElGamal 암호 시스템을 사용하여 믹스넷을 구성한다고 가정한다[4][10].

확률적 암호화는 암호화 과정에서 임의의 난수 r을 파라미터로 사용하여 평문 m_1와 m_2가 동일해도 이에 대한 암호문 $c_1=E(m_1)$과 $c_2=E(m_2)$는 같지 않다는 특성은 같지 않다는 특성이 있다[2][8]. 이는 전자투표와 같이 평문 공간이 한정된 유한 집합(후보자 기호)인 경우, 암호화된 투표값이 노출되더라도 난수 r을 알지 못하는 경우, 해당 평문을 알지 못하므로 매우 중요하다. 만약 전자투표에 결정적 암호 알고리즘을 사용할 경우에는 암호문에 대한 평문을 추측할 수가 있으므로 매표가 가능할 수 있다.

III. 관련 연구

전자 투표 방식 중 종이 영수증을 투표소 밖으로 가지고 나갈 수 있는 방식에는 A.Neff 방식[9]과 D.Chaum 방식[7]이 있다. 2004년 제안된 A.Neff 방식[11]의 경우, 투표자 i는 신원확인을 통해 고유한 투표번호(BSN_i)가 들어있는 스마트카드를 발급 받는다. 투표기는 스마트 카드를 인식하여 BSN_i에 해당되는 후보자 명단과 각 후보를 사전에 암호화한 코드북(codebook)에서 투표값을 화면에 출력한다. 투표자가 원하는 후보자를 선택하면, 투표기는 BSN_i와 암호화된 투표값, 그리고 서명값을 영수증에 출력한다. 발급된 영수증은 투표소 밖으로 가지고 나갈 수 있으며, 투표 결과를 확인하기 위해서는 검증 기관의 게시판(bulletin board)을 통하여 자신의 투표가 집계 결과에 제대로 반영되었는지를 확인할 수 있다. 이 방식은 영수증에 자신이 선택한 후보자의 투표값 번호를 확인함으로서 자기 검증이 가능하며, 다른 사람에게는 자신의 투표 결과를 증명할 수 없으므로 매표 방지가 가능하다. 하지만, 신뢰기관에 의해 미리 생성되는 코드북에 대한 검증을 수행하기 위해서 투표 중간에 감시자가 수시로 투표 과정을 확인해야 하는 단점이 있다.

D.Chaum은 2002년 Visual Cryptography를 이용한 발급 방식을 제안하였다. 이 방식은 투표자가 선택한 결과를 두 개의 투명한 레이어(top 또는 bottom layer)로 구성된 특수 용지에 나누어 출력하여 투표소 내에서 투표 결과를

가시적으로 확인할 수 있도록 하며, 투표소를 나갈 때에는 임의로 선택한 레이어만을 가지고 나갈 수 있도록 한다. 선택하지 않은 레이어는 선거관리자가 폐기한다. 본 방식의 특징은 한 장의 레이어만으로는 어느 후보자를 선택했는지 시각적으로 확인이 불가능하기 때문에 매표가 불가능하지만, 두 개의 레이어 모두 암호학적인 픽셀로 구성되어 어느 레이어를 선택하더라도 투표자의 투표값을 복호화 할 수 있다는 것이다. 하지만 영수증 출력을 위해 특수한 용지 및 프린터가 필요하다는 점과 영수증을 구성하는 레이어 두 개가 투표소 밖으로 유출될 경우에 발생할 수 있는 매표를 막기 위해 선거관리자가 모든 투표자의 투표용지 중 한 장을 반드시 수거해야 하는 관리상의 어려움이 있다

IV. 제안하는 영수증 발급 기술

본 논문에서는 Chaum의 방식과 달리 특수한 용지나 프린터가 없이도 투표자가 자신의 투표값이 의도대로 반영되었음을 높은 확률로 검증할 수 있으며, Neff 방식과 달리 전체 유권자에 대해 사전에 코드북을 만들 필요가 없으며 별도의 감시자가 필요없는 효율적인 영수증 발급 방식을 제안한다. 또한, 투표자는 투표소 밖에서 자신이 신뢰할 수 있는 검증 기관을 이용하거나 자신이 직접 검증기를 만들어 언제든지 투표값이 유효함을 검증할 수 있다.

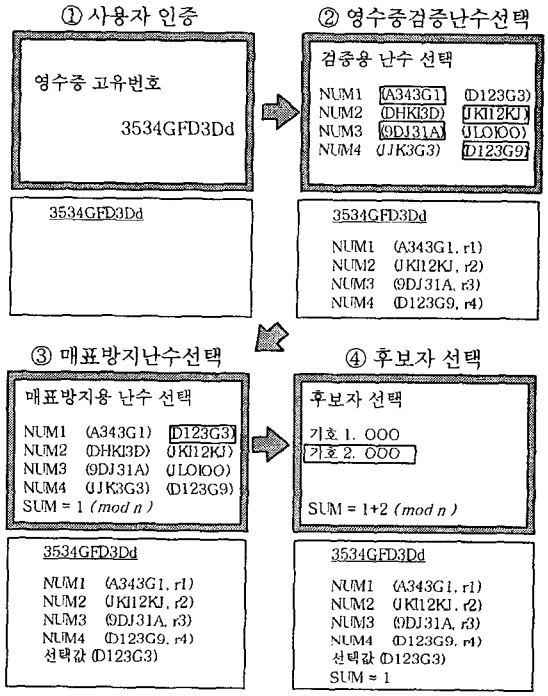
본 논문에서 제안하는 프로토콜에서 n은 후보자 수를, i는 투표자 고유번호를, $E(\cdot,\cdot)$는 ElGamal 암호화를, $H(\cdot)$는 해쉬함수를, 그리고 v_i는 선택한 후보($1 \le v_i \le n$)를 나타낸다.

제안방식의 투표 영수증을 발급 절차는 다음과 같다(그림 1참조).

① 투표기는 $j=1,...,t(n<t, n|t)$에 대해 난수 r_{j1}, r_{j2}을 이용하여 ElGamal 암호화를 수행하고 암호화된 결과를 화면에 표시한다.

$$(e_{j1}, e_{j2}) = (E(j, r_{j1}), E(j, r_{j2}))$$

② 투표자는 $j=1,...,t$에 대해 $e_j \in_R \{e_{j1}, e_{j2}\}$를 선택하고 투표기는 선택된 t 개의 e_j 및 암호화에 사용한 난수 $w_j (e_j = E(j, w_j))$를 영수증에 출력한다.



<그림 1> 제안 방식의 화면출력 및 투표 영수증 $(n=2, t=4)$

③ 투표자는 임의의 $R(1 \le R \le t)$을 선택하고 투표기는 단계 ②에서 선택되지 않은 e_R을 영수증에 출력한다. 그리고 화면에는 합계를 나타내는 $S_i = R(\mathrm{mod} n)$를 출력한다.

④ 투표기는 n 명의 후보자를 표시하고 투표자는 원하는 후보 v_i를 선택한다. 이 때 투표기는 화면에 표시된 S_i를 갱신하고 투표자는 계산된 S_i가 맞는지 검증한다.

$$S_i = (R + v_i)(\mathrm{mod} n)$$

⑤ 투표기는 최종적으로 S_i와 전체 영수증에 대한 서명값을 출력한다.

⑥ 투표자는 투표소 밖에서 영수증에 출력된 e_R 값의 유효성을 다음과 같이 검증한다.

$$E(j, w_j) = e_j (j = 1,...,t)$$

⑦ 투표자는 영수증에 출력된 (BSN_i, e_R, S_i)가 공개 게시판에 등록된 것과 일치하는지 확인한

다.

투표자는 단계 ⑥과 ⑦의 검증 과정을 통해 자신이 선택한 대로 투표되었음을 확신할 수 있지만, e_R을 복호화할 수는 없고 v_i가 기록되어 있지 않기 때문에 투표 내용을 증명할 수는 없다. 개표 단계에서는 v_i를 계산하기 위해 e_R을 복호화하면 되는데, 투표값 v_i는 다음의 식으로 간단히 계산할 수 있다.

$$v_i = S_i - E^{-1}(e_R) (\mathrm{mod} n)$$

이 방식의 안전성은 안전성 파라미터 t에 의해 결정되는데, t는 후보자 수 n의 배수로 정해야 한다. 이는 모든 후보자가 확률적으로 동일한 분포를 갖게 하기 위해서이다.

V. 안전성 분석 및 비교

전자투표에서 발급하는 영수증은 전자투표에 대한 신뢰성을 향상시키기 위해 사용된다. 따라서 전자투표 영수증에 대한 안전성은 전자투표기의 부정행위 확률과 매표 가능성으로 분석할 수 있다[3].

[표 1] 제안하는 방식과 기존 발급 기술의 비교

	제안하는 방식	Neff 방식	Chaum 방식
탐지확률(1)	$1-\frac{1}{2^t}$	$1-\frac{k}{m+k}$	$\frac{1}{2}$
특수장비	불필요	불필요	필요
코드북 사전생성	불필요	필요	불필요
감시자	불필요	필요	불필요
매표 가능성	없음	코드북 노출시	영수증 미수거시

t : 안전성파라미터($2 \le t$), m : 투표자 수, k : 검증 횟수
(1) : 투표자 1인당 투표기의 부정 행위 탐지 확률

제안 방식은 Neff와 Chaum의 방식과 비교하여 투표자 1인당 투표기 부정행위 탐지 확률이 안전성 파라미터 t에 따라 높은 신뢰도를 갖으며 관리상의 부실로 인한 매표 가능성을 배제하였다. 또한 특수한 출력 용지나 장치를 사용하지 않아도 되므로 비용절감 효과가 있으며, 투표 중간에 기기의 올바른 작동을 점검할 필요가 없어 효과적이다.

VI. 결론

본 논문에서는 전자투표에서 유권자가 자신의 투표 결과에 대한 확신을 가질 수 있도록 하면서 동시에 투표기에 의해 발생할 수 있는 부정을 최소화 시킬 수 있는 투표 영수증 발급 기술을 제안하였다. 향후 연구를 통해서는 전자투표 시스템으로 실용화하기 위하여 t번의 무작위 선택 과정을 효과적인 인터페이스를 구성하여 해결할 것이다.

[참고문헌]

[1] David L. Chum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM*, vol.24 , no.2, pages 84-88, Feb 1981.

[2] T.ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. on Information Theory, vol.IT-31, no-4, pages 469-472, 1985.

[3] Yunho Lee, Kwangwoo Lee, Seungjoo Kim and Dongho Won, "Efficient Voter Verifiable E-Voting Schemes with Cryptographic Receipts," Cryptology ePrint Archive, http://eprint.iacr.org/, Report 2006/167, 2006.

[4] C.A.Neff, "A Verifiable Secret Shuffle and Its Application to E-Voting," Proc. of the 8th ACM Conference on Computers and Communications Security(CCS-8), pages 116-125, 2001.

[5] R.Mercuri, "Rebecca Mercuri's Statement on Electronic Voting," http://www.notatlesoftware.com/RMstatement.html, 2001.

[6] T.Kohno, A.Stubblefield, A.D.Rubin, and D.S.Wallach, "Analysis of an Electronic Voting System," Proc. of IEEE Symposium on Security and Privacy, page 27, 2004.

[7] D.Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections," IEEE Security and Privacy Magazine, vol.2, no.1,pages 38-47, Jan. 2004.

[8] S.Goldwasser and S.Micali, "Probabilistic Encryption," Journal of Computer System Sciences(JCSS), vol.28, no.2, pages 270-299, Apr. 1984.

[9] C.A.Neff and J.Adler, "Verifiable e-Voting," IEEE Security and Privacy Magazine, vol.2, no.1, pages 38-47, Jan. 2004.

[10] P.Golle, M.Jakobsson, A,Juels, and P.Syverson, "Universal Re-Encryption for Mixnets," CT-RSA 2004, LNCS 2964, pages 38-47, Jan. 2004.

[11] C.A.Neff and J.Adler, "Verifiable e-Voting," IEEE Security and Privacy Magazine, vol.2, no.1, pages 38-47, Jan. 2004.