情報保護學會論文誌
第16卷 第4號, 2006. 8

전자투표 신뢰성 향상을 위한 투표자 검증용 영수증 발급 기술*

이 광 우,† 이 윤 호, 원 동 호, 김 승 주‡
성균관대학교 정보통신공학부 정보보호연구소

A Voter Verifiable Receipt in Electronic Voting with Improved Reliability*

Kwangwoo Lee,† Yunho Lee, Dongho Won, Seungjoo Kim‡
Information Security Group School of Information and Communication Engineering Sungkyunkwan University

요 약

최근 전자투표 시스템에 대한 투표자의 신뢰성을 높이기 위하여, 투표자가 자신의 투표 결과를 확신할 수 있도록 하는 영수증 발급 기술에 대한 연구가 활발히 진행되고 있다. 전자투표 영수증은 투표소 밖에서도 검증할 수 있어야 하기 때문에 개별 검증성과 함께 매표방지에 대한 요구사항을 만족해야 한다. 기존의 연구에서는 특수한 용지와 프린터를 필요로 하거나 투표기가 올바로 작동하는 것을 수시로 검증해야 하는 관리상의 문제점을 가지고 있었다. 본 논문에서는 전자투표에 대한 신뢰성을 높이면서, 특수한 종이나 프린터 또는 스캐너가 필요 없고 투표소 내의 기기나 관리자를 신뢰하지 않아도 되는 영수증 발급 방식을 제안한다.

ABSTRACT

In order to improve voters' reliability in electronic voting system, voter verifiable receipt technique is being actively researched. Since the receipt should be verifiable not only inside but also outside a polling place, it satisfies the requirements, individual verifiability and receipt-freeness. In the previous researches, there are some problems that special paper and printer is necessary or frequent monitoring is needed to confirm the voting machine's trustworthiness. In this paper, we propose a new receipt issuing scheme. Our scheme does not require any special equipments such as special paper and printer or optical scanner. In addition to that it does not require voters to trust any devices in the polling station and there is no need of frequent observations to the voting machines.

Keywords : *Electronic Voting, Universal Verifiability, Probabilistic Encryption, Mix-net, Paper Receipt.*

Ⅰ. 서 론

대부분의 국가에서 실시되고 있는 현재의 종이투표 방식은 선거에 따른 비용 증가, 투표율 하락 및 부정확한 집계 결과로 인해 선거 신뢰도 저하라는 심각한 문제를 안고 있다. 이를 해결하기 위한 방안으로 전자투표에 대한 관심이 고조되고 있는데, 전자투표를 실시할 경우 투·개표에 소요되는 시간 및 인력을 현저하게 줄일 수 있으며, 정확한 집계가 가능할 것으로 기대하고 있다. 하지만, 현재의 선거 방식보

접수일: 2006년 5월 29일 : 채택일: 2006년 7월 12일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 IT학술기초연구 지원사업의 연구결과로 수행되었음.
† 주저자, kwlee@security.re.kr
‡ 교신저자, skim@security.re.kr

다 더 큰 혼란이 있을 것이라는 우려도 있다. 특히 투표의 전자적인 기록과 집계 과정을 신뢰할 수 없다는 것이 주요 문제로 지적되고 있다. 따라서 전자투표에 대한 신뢰성을 높이기 위하여 전자적인 기록 외에 투표자가 자신의 투표를 신뢰할 수 있도록 영수증을 발급하는 방법이 현실적인 대안으로 주목받고 있다[5,6].

전자투표에 대한 신뢰는 크게 전자적인 기록에 대한 신뢰(Cast-as-intended)와 개표 결과에 대한 신뢰(Counted-as-cast)로 나누어 생각할 수 있는데, 전자는 개별 검증성(individual verifiability)이라고 하며, 후자는 전체 검증성(universal verifiability)이라고 한다[14]. 즉, 투표자는 자신이 의도한대로 투표값이 기록되었음을 개별적으로 확신할 수 있어야 하고, 이렇게 기록된 전체 투표값으로부터 나온 개표 결과는 누구나 검증할 수 있어야 한다는 의미이다. 일반적으로 전체 검증성은 투표자가 자신의 암호화된 투표값을 확인할 수 있는 읽기 전용 공개 게시판과 익명성 보장을 위한 믹스넷을 이용하며 이미 많은 연구가 진행되어 안전성이 입증되어 있다. 하지만, 이 경우 공개 게시판에 등록된 투표 결과가 자신이 의도한 투표값을 암호화한 것임을 확신할 수 있도록 해야 하는데, 이를 위해 사용하는 것이 투표 영수증이다.

투표 영수증은 투표소 밖으로 가지고 나갈 수 있는지 여부에 따라 두가지로 구분할 수 있다. 투표소 밖으로 가지고 나갈 수 있는 영수증은 매표를 방지하기 위해 투표값을 암호화해서 기록하지만 투표소 내에서만 사용되는 영수증은 암호화하지 않고 투표값을 기록하는데, 이 때 발급된 영수증은 투표자의 검증을 위해 사용되기도 하지만 (재)검표에 사용될 수도 있다. 하지만 이 경우 투표자가 영수증을 검증하더라도 전자적인 기록은 검증할 수 없기 때문에 결과적으로 영수증을 통한 재검표가 필연적이며 따라서 전자투표가 갖는 장점을 기대하기는 어렵다. 반면, 투표소 밖으로 가지고 나갈 수 있는 영수증은 재검표를 위해 발급하는 것이 아니고 전자적인 기록에 대한 신뢰를 위해 발급하게 된다.

투표소 밖으로 가지고 나갈 수 있는 영수증 발급 방식으로는 2002년에 발표된 Visual Cryptography를 응용한 Chaum의 방식[8][10]과 2003년에 발표된 Neff의 방식[7], 그리고 2005년에 Chaum이 발표한 방식[15]이 있다. Visual Cryptography를 이용한 방식은 두 장으로 분리할 수 있는 특수 용지에 투표 결과를 양면으로 인쇄하고 이를 분리하여 투표값을 알아볼 수 없도록 하는 방식으로서 투표 영수증이 가져야 할 여러 조건을 만족하지만, 특수한 프린터와 용지를 사용해야 하기 때문에 비용 측면에서 실용화하기 어려운 단점이 있다. 또한, 투표기는 투표자가 두 장의 용지 가운데 어느 것을 선택할지 예측해야만 부정 행위를 할 수 있기 때문에 1/2의 부정 행위 확률을 갖게 되지만 투표기의 영수증 인쇄 방법에 따라 이보다 높아질 수 있는 문제점이 있다.

Neff의 영수증 발급 방식은 사전에 유권자 수보다 많은 투표자에 대한 가능한 투표값을 모두 암호화하여 이를 코드북(codebook)으로 만들고, 투표기는 코드북을 참조하여 암호화된 투표값을 출력하는 방식으로서 일반 프린터를 이용할 수 있다는 장점이 있지만 코드북을 비밀리에 보관해야 하며 투표 기간 동안 투표기의 동작을 수시로 검증해야 하는 단점이 있다.

2005년에 발표된 Chaum의 방식은 사전에 전체 유권자 수보다 많은 투표용지를 만드는데, 이 때 후보자의 순서는 임의로 순환(rotate)되도록 하며, 순환 값은 암호화하여 투표용지에 함께 기록한다. 투표자는 임의로 투표용지를 선택하여 투표자의 순서와 암호화된 순환 값이 일치하는지 검증한다. 만약 검증되었을 경우에는 해당 투표용지는 폐기하며 새로운 투표용지를 이용하여 기표하고 후보자 부분과 기표 부분을 분리하여 기표 부분만 광학 스캐너 등을 이용하여 기록한 후 영수증으로 보관한다. 투표자는 공개 게시판에 자신의 영수증이 등록되었는지 확인한다. 개표할 때 어느 후보에 대한 투표값인지 확인하는 과정은 암호화된 순환 값을 복호화하여 진행한다. 이 방식의 장점으로는 투표기가 투표자의 투표값을 알 수 없다는 점이며, 단점으로는 투표소 내에서만 투표용지를 검증할 수 있다는 점과 검증을 위한 검증기를 신뢰해야 한다는 점, 그리고 투표용지에서 후보자 표시부분을 폐기하는 과정에서 투표값이 노출되거나 매표에 사용될 수 있다는 점 등이다.

본 논문의 구성은 다음과 같다. 2장에서는 요소 기술로서 믹스넷과 확률론적 암호화를 살펴보고 각각이 적용되는 경우를 설명한다. 3장에서는 기존에 연구되었던 투표소 밖으로 가지고 나갈 수 있는 종이 영수증 기술들을 살펴본다. 4장에서는 기존 기술들이 가지고 있는 단점을 보완하여 실용적으로 활용될 수 있는 종이 영수증 발급 기술을 제안하며, 5장에서는 제안한 영수증 발급 기술의 안전성을 분석한다. 6장에서는 향후 연구를 살펴보고, 마지막으로 7장에서는 결론을 맺는다.

Ⅱ. 요소 기술

전자투표 영수증 발급 기술에 사용되는 요소 기술에는 믹스넷과 확률론적 암호화가 있다. 믹스넷은 투표값을 섞어 투표자와 투표값의 연결 정보를 끊음으로서 프라이버시를 보장한다. 또한 확률론적 암호화는 동일한 평문을 암호화 하였을지라도, 암호문 생성 인수로 난수를 사용하기 때문에 암호문이 매번 다르게 나오는 암호화 방식이다.

1. 믹스넷(Mix-net)

믹스넷은 1981년 D. Chaum[1]에 의해 소개된 방법으로 입력값과 출력값 사이의 연결 정보를 알 수 없도록 섞는(suffle) 것으로서, 출력값을 통해서는 입력값의 순서를 알 수 없도록 한다. 믹스넷은 다수개의 믹스 서버로 구성되며, 각각의 믹스 서버는 초기 입력값 또는 이전 믹스 서버의 출력값을 입력받아 섞기를 수행한다. 이때 각 믹스서버는 자신의 동작이 올바름을 증명해야 하는데, 증명 방법으로는 영지식 증명, RPC(Randomization Parity Check) 등이 사용된다. 믹스넷은 크게 복호화 믹스넷(decryption mix-net)과 재암호화 믹스넷(re-encryption mix-net)으로 구분하며 재암호화가 가능한 ElGamal 암호 시스템 등을 주로 이용한다[11,13].

전자투표에서 믹스넷은 유권자와 투표값이 매칭되어 공개될 경우에 발생할 수 있는 프라이버시 문제를 해결하기 위해 사용된다. 본 논문에서는 투표자와 투표값을 분리하고, 순서를 알 수 없도록 하기 위하여 믹스넷을 사용하는 것으로 가정한다.

2. 확률론적 암호화(Probabilistic Encryption)

확률론적 암호화는 암호화 과정에서 임의의 난수를 이용하는 방식으로서 평문 m_1과 m_2가 동일해도 이를 암호화한 결과인 $c_1 = E(m_1)$과 $c_2 = E(m_2)$는 같지 않다는 특성이 있다[9]. 이러한 특성은 전자투표와 같이 평문의 공간이 매우 작은 유한 집합으로 한정되어 있을 때 특히 중요하다. 만약 전자투표에 결정적(deterministic) 암호 알고리즘을 사용하게 된다면, 공격자는 CPA(Chosen Plaintext Attack)나 CCA(Chosen Ciphertext Attack)와 같은 방법을 사용하여 투표 내용을 확인할 수 있으므로 매표가 가능할 수 있다[12]. 이러한 공격을 방지하기 위하여 공개키 암호 방식에 난수 r 값을 포함하는 확률론적 암호화 방식을 사용하며, 본 논문에서는 ElGamal 암호 시스템[2]을 적용한다.

Ⅲ. 관련 연구

전자투표 영수증 발급 기술은 재검표를 위한 영수증과 투표기 검증을 위한 영수증이 있는데, 투표자가 투표기의 오작동 여부를 검증을 위한 영수증에는 대표적으로 Neff 방식과 Chaum 방식이 있다.

1. Andrew Neff 방식

Andrew Neff 방식[7]의 경우 투표자 i는 신원확인을 거쳐 고유의 투표 번호(BSN_i)가 들어있는 스마트카드를 발급 받는다. 투표기는 BSN_i에 해당되는 후보자 명단과 각 후보를 암호화한 투표값을 화면에 출력한다. 투표자가 원하는 후보자를 선택하면, 투표기는 BSN_i, 암호화된 투표값 및 투표기의 서명값을 영수증에 담아 출력한다(그림 1. 참조).

발급된 영수증은 투표소 밖으로 가지고 나갈 수 있으며, 읽기 전용 공개 게시판을 통하여 자신의 투표가 정확하게 기록되었는지 확인한다. 이 방식은 영수증에 출력된 암호화된 투표값이 투표기 화면에 표시된 그것과 일치하는지 확인함으로써 영수증의 유효성을 검증할 수 있지만, 투표소 밖에서는 자신의 투표 내용을 증명할 수 없어 매표는 불가능하다. 화면에 출력되는 암호화된 투표값은 투표기가 계산하지 않고 사전에 신뢰할 수 있는 기관이 생성한 코드북(codebook)을 이용하는데, 투표기는 단지 BSN_i를 코드북에서 참조하여 해당되는 투표값을 표시하게 된다. 이 때 투표기가 검증된 코드북에 의해 투표값을 표시하는지 검증해야 하는데, 이는 투표 기간 동안 감시자가 투표자인 것처럼 투표과정을 진행하여 해결한다.

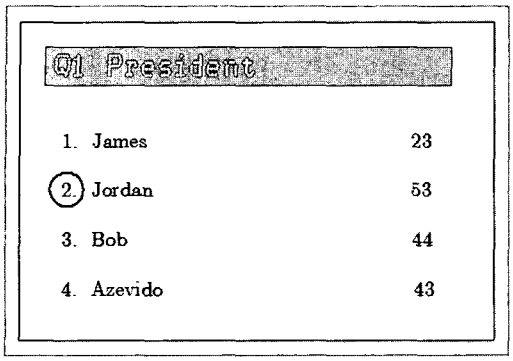
Neff 방식에서 투표의 경우 부정행위가 발생할 수 있는 확률은 다음과 같다(식 1. 참조).

$$\text{부정발생확률} = 1 - \frac{k}{m+k} \quad (1)$$

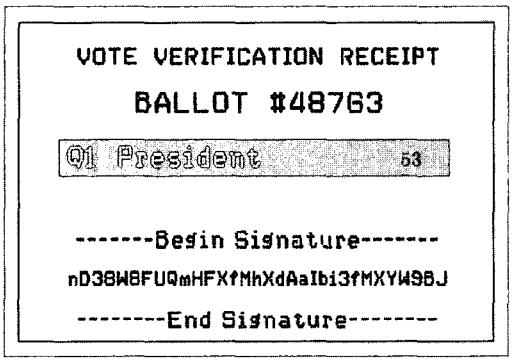
(m: 투표자 수, k: 검증 횟수)

전자투표 시스템에서는 선거관리자의 역할이 최소화 되어야 선거의 중립성을 보장할 수 있으므로, 이

러한 점은 투표기 도입에 있어 안전성과 편의성의 문제가 제기될 수 있다.



(a) DRE 화면



(b) 종이 영수증

그림 1. Neff 방식에서의 DRE 화면과 발급되는 종이 영수증

2. Chaum 방식

D.Chaum은 2002년 Visual Cryptography를 이용한 발급 기술을 제안하였다. 이 방식은 투표자로 하여금 투표소 내부에서는 영수증을 통하여 자신의 투표 결과를 가시적으로 확인할 수 있게 함과 동시에 투표소를 나가게 되면 투표 결과를 증명할 수 없도록 함으로써 매표 행위를 방지하고 있다. 즉 투표기는 투표자가 선택한 후보를 두 개의 투명한 레이어로 구성된 특수 용지에 나누어 출력하여 투표 결과를 확인하도록 하고 투표자로 하여금 하나의 레이어(top layer 또는 bottom layer)만 임의로 선택하도록 한다. 이 때 두 개의 레이어는 모두 암호학적인 픽셀로 구성되어 어느 레이어를 선택하더라도 투표자의 투표값을 복호화할 수 있다. 선택되지 않은 레이어는 관리자와 함께 폐기하는데, 하나의 레이어 만으로는 어느 후보자를 선택했는지 시각적으로 확인할 수 없기 때문에 투표소 밖에서 자신의 투표를 증명하는 것 불가능하다[8](그림 2 참조).

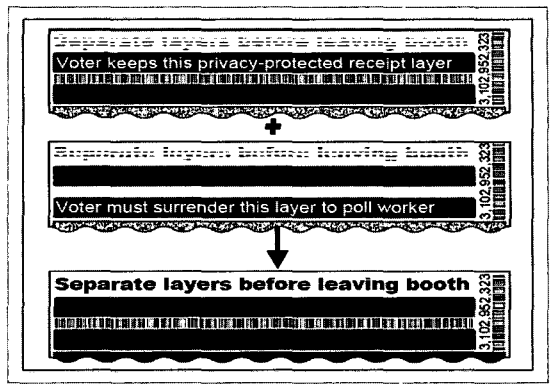


그림 2. Chaum 방식의 영수증 발급 기술

Chaum 방식의 단점은 영수증 출력을 위해 특수한 프린터가 필요하다는 것과 투표기의 부정 행위를 감지할 확률이 각 투표자마다 1/2이라는 점이다. 물론 20명의 투표자에 대한 투표를 조작할 수 있는 확률은 $\frac{1}{2^{20}}=\frac{1}{1{,}048{,}576}$이며 이는 현실적으로 매우 낮지만 불과 몇 표 차이로 인해 당락이 결정될 수도 있다고 보면 무시할 수 있는 확률은 아니다. 또한 영수증을 구성하는 레이어 두 개가 투표소 밖으로 유출될 경우에는 매표가 발생할 수 있으므로 관리자가 모든 투표자의 투표용지 중 한 장을 수거하여 폐기해야 하는 관리상의 어려움이 존재한다.

Ⅳ. 제안하는 영수증 발급 기술

Neff와 Chaum의 방식은 모두 투표자가 투표소 밖으로 영수증을 가지고 나갈 수 있기 때문에 투표 과정에 대한 투표자의 신뢰를 높일 수 있는 장점이 있다. 하지만, 두 방식 모두 투표소 내에서만 영수증에 기록된 내용이 정확함을 확률적으로 확신할 수 있고 투표소 밖에서는 영수증의 내용과 공개 게시판에 등록된 내용이 같은지 여부만을 확인할 수 있다.

본 논문에서는 Chaum의 방식과 같은 특수한 장비 없이 투표자 개인이 자신의 투표 결과가 자신의 의도대로 반영되었음을 비교적 높은 확률로 검증할 수 있고, Neff 방식과는 달리 전체 유권자에 대해 사전에 암호화된 투표값(codebook)을 만들 필요가

없으며 별도의 감시자가 필요 없는 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 방식의 전체적인 프로토콜은 다음과 같다(그림 3. 참조).

본 논문에서 제안하는 프로토콜에 사용될 용어와 표기법은 다음과 같다.

n	후보자 수
i	투표자 고유번호
$E(\cdot,\cdot)$	ElGamal 암호화
$H(\cdot)$	Hash 함수
v_i	선택한 후보 $(1 \le v_i \le n)$

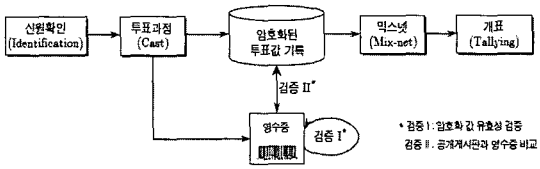


그림 3. 제안하는 영수증 발급 방식의 전체적인 절차

1. 영수증 발급 절차(그림 4. 참조)

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 $j=1,...,t(n<t, n|t)$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.

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 n명의 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 공개게시판에 등록된 것과 일치하는지 확인한다.

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.

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

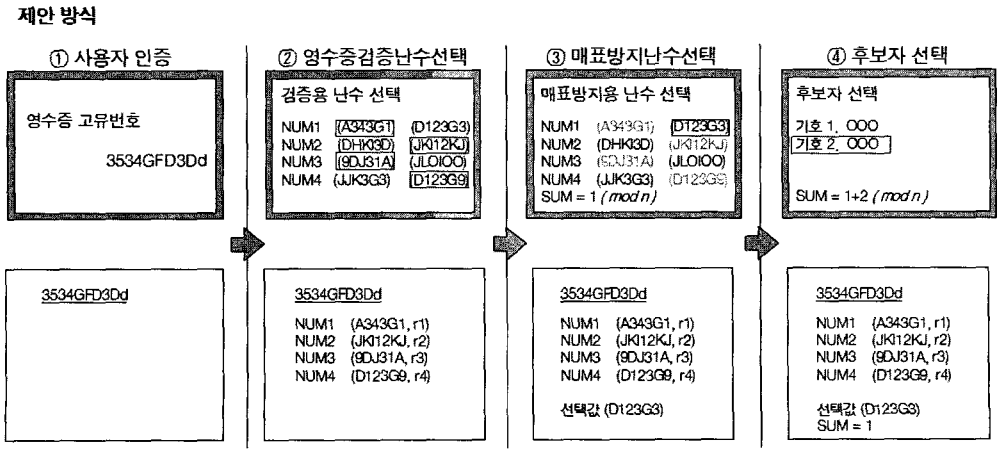


그림 4. 제안 방식 (투표 절차에 따른 화면 출력과 영수증, $n=2$, $t=4$인 경우)

이 방식의 안전성은 안전성 파라미터 t에 의해 결정되는데, t는 후보자 수 n의 배수로 정해야 한다. 이는 모든 후보자가 확률적으로 동일한 분포를 갖게 하기 위해서이다. 예를 들어, $n=2$, $t=3$일 경우, $S_i=0$으로 계산되었다고 가정할 때, 각각의 후보자가 선택되었을 확률이 다음과 같이 서로 동일하지 않음을 알 수 있다.

$$\Pr[v_i=1]=\frac{2}{3},\ \Pr[v_i=2]=\frac{1}{3}$$

표 1. 투표자 1인당 투표기의 부정 행위 탐지 확률

	제안하는 방식	Neff 방식	Chaum 방식
탐지 확률	$1-\frac{1}{2^{t-1}}$	$1-\frac{k}{m+k}$	$\frac{1}{2}$

t : 안전성파라미터($2 \le t$) m : 투표자 수 k : 검증 횟수

표 2. 효율성 비교

	제안하는 방식	Neff 방식	Chaum 방식
특수 프린터,용지	×	×	⊙
감시자	×	⊙	×
코드북	×	⊙	×
매표가능성	없음	코드북 노출시	영수증 미수거시

⊙ : 필요 × : 불필요

V. 안전성 분석

전자투표 과정에서 사용되는 종이 영수증은 전자투표에 대한 신뢰성을 높이기 위해 사용된다. 따라서 전자투표 영수증에 대한 안전성은 전자투표기의 부정행위 방지와 영수증을 이용한 매표 방지로 생각할 수 있다. 이외에도 구현의 용이성과 소요 비용, 그리고 영수증 발급 및 관리의 효율성 등을 생각할 수 있다.

제안한 방식은 Neff와 Chaum의 방식과 같이 출력된 영수증을 투표소 밖으로 가지고 나갈 수 있지만 자신의 투표를 다른 사람에게 증명할 수는 없다. 즉, 투표값을 계산하기 위해서는 e_R을 복호화해야 한다. 또한 e_R의 유효성 검증을 위해 출력된 t개의 암호화된 값 e_j에 대한 검증도 복호화를 통한 검증이 아니고 암호화를 통한 검증이기 때문에 e_j를 검증한다고 해도 e_R을 복호화할 수는 없다.

투표기의 부정행위 탐지를 고려해 보면, Neff 방식에서는 투표기의 부정 행위를 투표자가 직접 확인할 수는 없으며, 별도의 감시자가 투표 진행 과정 중에 수시로 점검해야 하는 불편이 있다. 하지만 제안하는 방식에서는 투표자가 직접 영수증을 이용하여 투표기의 부정을 높은 확률로 감지할 수 있다 (표 1 참조).

제안한 방식에서 투표기가 부정을 저지르기 위해서는 투표자가 선택할 t 개의 e_j를 예측해야만 한다. 즉, 투표자가 선택할 e_j는 정상적으로 $j=1,...,t$를 암호화하고 나머지는 투표기가 임의의 값을 사용한다면 투표 결과는 투표자의 의도와는 다르게 기록될 수 있다. 따라서 투표기의 부정행위가 탐지되지 않을 확률은 $\frac{1}{2^{t-1}}$이 된다. 안전성 파라미터 t 는 후보자의 수에 따라 결정되는데 예를 들어 후보자가 2명일 경우 $t=2,4,6,8,...$이 될 수 있으며, 3명일 경우 $t=3,6,9,12,...$가 될 수 있다. t를 크게 하면 안전성은 높아지지만, 투표자가 투표소 내에서 화면과 영수증을 비교해야 하기 때문에 너무 크지 않아야 한다. $t=6$이라고 했을 때 투표기가 발각되지 않고 5명의 투표값을 조작했을 확률은 $\left(\frac{1}{2^{6-1}}\right)^5=\frac{1}{33,554,432}$이 된다.

표 2에서와 같이 제안한 방식은 특별한 프린터나 종이를 필요로 하지 않으며, 투표 중간에 감시자에 의한 간섭을 필요로 하지 않아 투표의 공정성을 확보할 수 있다. 또한 Neff 방식에서 불편했던 코드북 생성 및 검증 단계가 불필요하며 매표는 불가능하다.

VI. 향후 연구

제안한 방식이 안전성 측면에서 기존 방식에 비해 높은 안전성을 보이지만, 심리학적인 측면과 실용적인지에 대한 분석이 필요하다. 심리학적으로 사람은 무작위 선택에 상당히 취약한 것으로 알려져 있다. 따라서 가능한 한 무작위 선택은 최소한으로 제한하는 것이 좋다. 하지만, 제안한 방식에서는 안전성 파라미터 t 번의 무작위 선택을 하도록 되어 있다. 이러한 t 번의 무작위 선택은 사용자 인터페이스를 효과적으로 구성하면 1번의 선택으로 줄일 수 있다. 즉, 각각의 선택이 이진 선택이기 때문에 $1\sim 2^t$ 사

이의 수를 임의로 고르는 것과 같다. 또한, 제안한 방식에서는 투표자가 모듈로 연산을 해서 합계가 맞는지 검증해야 한다(단계 ④). 이는 매우 간단한 모듈로 연산이지만 모든 투표자가 무리없이 연산을 할 수 있을 것이라고 기대할 수는 없다. 투표자의 모듈로 연산이 필요 없도록 제안한 방식을 수정하는 것도 가능하지만, 이는 안전성과 연계될 수 있기 때문에 후보자의 수를 고려하여 선택해야 한다. 심리학적으로 무리없는 효과적인 인터페이스 구성과 검증 연산의 범용성 확보는 향후 연구를 통해 개선할 것이다.

Ⅶ. 결 론

본 논문에서는 전자투표에서 유권자가 자신의 투표 결과에 대한 확신을 가질 수 있도록 하면서 동시에 투표기에 의해 발생할 수 있는 부정을 최소화 시킬 수 있는 영수증 발급 기술을 제안하였다. 제안하는 방식은 Chaum과 Neff 방식의 단점이었던 특별한 프린터나 감시자를 필요로 하지 않으므로 비용 측면에서 우수하며, 안전성 측면에서도 매우 높은 신뢰도를 갖는다. 이 방식은 기존의 투표기에 비하여 보다 효율적이고 안전하며, 소프트웨어나 하드웨어로의 구현이 용이하므로, 실제 투표에 실용적으로 활용될 수 있을 것이다.

참 고 문 헌

[1] D.Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM*, vol.24, no.2, pp. 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, pp. 469-472, 1985.

[3] J.D.Cohen and M.J.Fischer, "A Robust and Verifiable Cryptographically secure Election Scheme," *Proc. of the 26th IEEE Symposium on the Foundations of Computer Science*, pp. 372-382, 1985.

[4] M.Naor and A.Shamir, "Visual Cryptography," *Proc. of Advances in cryptology (Eurocrypt' 94)*, LNCS 950, pp. 1-12, 1995.

[5] R.Mercuri, "Rebecca Mercuri's Statement on Electronic Voting," http://www.notatlesoftware.com/RMstatement.htm l, 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] C.A.Neff and J.Adler, "Verifiable e-Voting," *IEEE Security and Privacy Magazine*, vol.2, no.1, pp. 38-47, Jan. 2004.

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

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

[10] D.Chaum, P.Y.A.Ryan, and S,Schneider, "A Practical, Voter-Verificable Election Scheme," *Technical Report CS-TR-880*, University of Newcastle upon Tyne, 2004.

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

[12] P.Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," *Proc. of Advances in Cryptology (Eurocrypt'99)*, LNCS 1592, pp. 223-238, 1999.

[13] 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)*, pp. 116-125, 2001.

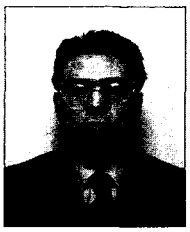
[14] Ryan, P. Y. A., Peacock, T., "CS-TR: 929 Prêt á Voter: a System Perspective", http://www.cs.ncl.ac.uk/research/

pubs/trs/papers/929.pdf, School of Computing Science, University of Newcastle, Sep 2005.
[15] David Chaum, Peter Y. A. Ryan, Steve A. Schneider, "A Practical Voter-Verifiable Election Scheme," *Proc. of ESORICS 2005*, LNCS 3679, pp. 118-139, Sep. 2005.

〈著者紹介〉

이 광 우 (Kwangwoo Lee) 학생회원
2005년 2월 : 성균관대학교 정보통신공학부(공학사)
2005년-현재 성균관대학교 대학원 컴퓨터공학과 석사과정 재학중
〈관심분야〉 암호이론, 전자투표, 정보보호제품 평가, 워터마킹, 정보보호 응용

이 윤 호 (Yunho Lee) 학생회원
1991년 2월 : 성균관대학교 정보공학과(공학사)
1993년 2월 : 성균관대학교 대학원 정보공학과(공학석사)
1993년 3월-2000년 4월 : 한국통신 연구개발본부 전임연구원
2000년 5월-2005년 1월 : KBS인터넷㈜ 기술지원팀장
2005년 3월-현재 : 성균관대학교 컴퓨터공학과 박사과정 재학중
2006년 6월-현재 : ㈜애니온소프트 기술이사
〈관심분야〉 암호이론, 정보보호 응용, 전자투표, 워터마킹



김 승 주 (Seungjoo Kim) 종신회원
1994년 2월-1999년 2월 : 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월-2004년 2월 : 한국정보보호진흥원(KISA) 팀장
2004년 3월-현재 : 성균관대학교 정보통신공학부 교수
2001년 1월-현재 : 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년 4월-현재 : 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년 6월-현재 : 교육인적자원부 유해정보차단 자문위원
2005년 7월-현재 : 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장
〈관심분야〉 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호 (Dongho Won) 종신회원
1976년-1988년 : 성균관대학교 전자공학과(학사, 석사, 박사)
1978년-1980년 : 한국전자통신연구원 전임연구원
1985년-1986년 : 일본 동경공업대 객원연구원
1988년-2003년 : 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년-1998년 : 국무총리실 정보화추진위원회 자문위원
2002년-2003년 : 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, IT보안성평가연구회 위원장
〈관심분야〉 암호이론, 정보이론, 정보보호