스마트카드를 이용하여 공개채널로 매표방지와 전체검증을 제공하는 전자선거기법†

김형석*, 김상진**, 오희국*

*한양대학교 컴퓨터공학과, **한국기술교육대학교 인터넷미디어공학부

A New Universally Verifiable and Receipt-free Electronic Voting Scheme Through Public Channel by Using Smartcard

Hyung-seok Kim*, Sang-jin Kim**, Hee-kuck Oh*

*Department of Computer Science and Engineering, Hanyang Univ.
**School of Internet-Media Engineering, Korea Univ. of Technology and Education

요 약

선거를 전자적으로 구성하기 위해서는 비밀성(privacy), 선거권(eligibility) 등과 함께 전체검증(universal verifiability)과 매표방지(receipt-freeness) 속성을 반드시 제공해야 한다. 지금까지 제안된 전자선거 기법은 매표방지와 전체검증을 제공하기 위해 도청 불가능한 채널이라는 물리적인 가정 하에 이루어지거나 하드웨어 장치를 이용하더라도 장치에 대한 신뢰가 가정되었다. 본 논문에서는 믹스 서버나 랜덤마이저의 역할을 스마트카드와 같은 안전한 하드웨어 장치가 하므로 물리적 가정 없이 효율적으로 구현한다. 제안한 시스템은 표를 섞는 과정에서 permutation matrix를 사용하여 증명하므로 증명의 회수가 적고 간단하여 효율적이다. 또한, 지금까지 제안된 대부분의 선거 기법은 ElGamal 암호시스템의 준동형 특성을 이용하여 모든 표를 결합한 다음 해독하여 집계를 계산하는데 이는 이산대수 문제를 효율적으로 해결할 수 있어야 가능했다. 이 논문에서는 ElGamal 암호시스템과 다차잉여 기반 암호알고리즘인 Naccacne 암호알고리즘을 결합하여 표를 인코딩 함으로써 유권자의 수가 많은 선거에 대해서도 다항 시간 내에 집계가 가능하다.

I. 서론

선거는 민주주의를 실현하는데 필요한 매우 중요한 방법 중에 하나이다. 국민들은 선거를 통해 국가의 정치, 사회의 많은 분야에 의견을 반영할 수 있다. 그러므로 전자 선거를 연구하는 것은 민주주의 증대에 매우 중요하다고 할 수 있다. 가까운 미래에 전자 선거는 가상 공간을 통해 많은 사람들의 의견을 쉽고 빠르게 모으는데 자주 사용될 것으로 기대된다. 암호학적인 측면에서 볼 때, 다양한 암호프로토콜 기술을 사용하는 전자선거는 중요한 응용분야 중에 하나이다.

전자선거가 현행 선거방식을 대체하기 위해서는 Fujioka 등[1]이 제안한 비밀성, 선거권 등의 기본적인 요구사항을 모두 만족해야 하며, 선거를 전자적으로 구성할 때 생길 수 있는 문제점들을 해결해야 한다. Sako와 Kilian[2]은 검증성을 선거에 참여한 유권자가 자신의 표가 집계에 올바르게 포함되었는지 확인할 수 있는 개별 검증성과, 선거의 참여 여부와 상관없이 누구나 개별 투표지의 유효성과 집계 결과의 유효성을 확인할 수 있는 전체 검증성으로 세분화하였는데 각 검증성을 모두 만족해야 한다. 또한 Benaloh와 Tuinstra[3]는 유권자가 자신이 투표한 내용에 대한 증거를 남길 수 있으면 이 증거를 제시하고 표를 팔 수 있으

† 이 논문은 2003년도 한국학술진흥재단의 지원에 의하여 연구되었음 (KRF-2003-003-D00445)

며, 구매자는 증거를 확인한 후에 표를 살 수 있다는 것을 발견하였다. 따라서 이런 증거를 남길 수 없도록 하거나 남길 수 있어도 구매자가 이 증거를 통해 확신을 가질 수 없도록 해야 한다. 이러한 요구사항을 매표방지(receipt-freeness)라 하는데 매표방지를 위해서는 증거를 남길 수 없어야 하고 위에서 언급한 전체 검증을 위해서는 증거를 남겨야 한다. 따라서 이 두 가지 특성은 상반되는 의미를 지니고 있어 두 가지 다 동시에 만족시키는 것은 어렵다.

근래에는 암호 기술을 사용하여 매표방지 및 전체검증을 제공하는 시스템에 대한 연구가 이루어지고 있지만 여전히 안전한 통신채널이라는 물리적 가정을 배제하지 못하고 있다. 지금까지 제안된 전자선거 기법은 둘 중 한 가지 특성만을 제공하거나 두 가지 특성을 모두 제공하는 경우 계산량이 많아 실용적이지 못하다. 따라서 본 논문에서는 스마트카드를 이용하여 도청 불가능한 채널없이 스마트카드가 랜더마이저 역할을 하도록 시스템을 설계한다.

스마트카드는 마이크로프로세서, COS(Chip Operating System), EEPROM(Electronically Erasable Programmable Read Only Memory)을 갖추고 있어 하나의 카드에서 다양한 애플리케이션을 구현할 수 있고 IC칩에 보안프로그램을 작동할 수 있기 때문에, 스마트카드를 사용하여 공개채널로 전자선거를 한다는 것은 표 구성을 신뢰기관과 프로토콜을 수행하여 구성하지 않고 스마트카드와 프로토콜을 수행하여 구성한다는 것이다. 따라서 스마트카드를 개인 컴퓨터에 연결하여 사용하므로 표를 구성하는 동안 외부로 데이터가 유출되지 않는다.

이 논문에서는 스마트카드를 이용한 공개채널만을 사용하여 선거를 할 수 있도록 함에 있어서 가장 안전한 형태의 프로토콜을 제안한다. 선거가 시작되면 스마트카드는 투표지들을 암호화하여 섞은 다음 유권자에게 섞인 표들의 정확성을 증명한다. 유권자는 투표하려는 후보자의 표를 선택하여 게시판에 게시하고, 투표지의 유효성을 증명한다. 이 기법은 지금까지 제안된 전체검증과 매표방지를 제공하는 기법들과 비교하였을 때, 물리적인 가정이 없어 현실적인 구현이 가능하며 계산량이 적어서 효율적이다.

이 논문의 구성은 다음과 같다. 2장에서는 기존의 전자선거 기법의 특성과 문제점을 분석하고, 3장에서는 제안하는 선거기법을 서술하고, 끝으로 4장에서는 이 기법의 안전성 분석과 함께 향후 연구 과제를 제시한다.

II. 관련연구

지금까지 많은 전자선거 기법이 제안되어 왔는데 접근방법에 따라 크게 다음과 같이 세 가지로 나누어 볼 수 있다.

- 은닉서명(blind signiture)을 이용한 전자선거 기법
- 믹스넷(mix-net)을 이용한 전자선거 기법
- 준동형 암호화(homomorphic encryption)를 이용한 전자선거 기법

은닉서명 기법은 비교적 간단한 프로토콜로 구성되고 계산량이 효율적이지만 유권자의 은닉요소가 표의 증거로 사용될 수 있으므로 유권자는 구매자에게 자신의 표를 증명하고 매표행위를 할 수 있다. 따라서 receipt-freeness가 제공되지 않는다.

믹스넷을 이용한 기법은 다중 믹서(mixer)가 표를 섞고, 섞은 것에 대한 정확성 증명을 해야 하므로 계산량이 많아서 일반적으로 효율적이지 못하다. 특히, 후보자의 수가 많은 선거에 대해서는 적합하지가 않다.

최근에는 HR(Honest Randomizer)이라는 신뢰할 수 있는 제3자와 도청 불가능한 채널을 이용하여 준동형 특성을 만족하는 암호화된 표를 전달하여 매표방지와 전체검증을 제공하는 기법들이 연구되었는데, 도청 불가능한 채널이라는 물리적인 가정은 현실적인 구현이 어렵다.

III. 제안하는 전자선거 기법

이 장에서는 매표방지와 전체검증을 제공하는 전자선거 기법을 제안한다. 이 기법은 랜더마이저와 도청 불가능한 채널의 역할을 하는 스마트카드를 이용한다.

선거가 시작되면 스마트카드는 모든 표에 대해서 빠짐없이 암호화하고 임의로 섞은 다음, 유권자에게 중복된 것이 없다는 것을 증명한다. 기존의 연구에서 보면 randomness의 선택이 매표방지에서의 증거와 밀접한 관련이 있는데 Hirt[4]의 기법을 확장하여 스마트카드를 이용한 이병천과 김광조[5]의 기법은 유권자가 자신이 선택한 후보의 표를 스마트카드에 전달하고 스마트카드는 이것을 암호화한 다음 유권자에게 전달한다. 여기서 유권자가 선택한 초기표를 스마트카드가 알고 있으므로 스마트카드가 이 정보를 누설하지 않아야 한다는 것을 신뢰해야 매표방지를 만족할 수 있다. 따

라서 제안하는 논문에서는 스마트카드를 사용하여 공개채널만으로 선거를 할 수 있도록 함으로써 스마트카드가 모든 후보의 표를 암호화하여 각 표의 유효성 증명과 함께 유권자에게 전달하는 방식을 취한다. 따라서 스마트카드를 반납하더라도 스마트카드 내에는 유권자가 선택한 값에 대한 어떠한 정보도 남아있지 않아 매표방지를 제공한다.

1. 시스템 모델

1) 참여자

이 전자선거 기법은 N명의 선거관리자 $(A_1,...,A_N)$, L명의 유권자$(V_1,...,V_L)$, 각 유권자에게 선거관리자가 발행한 랜더마이저 역할을 하는 스마트카드, K명의 후보자로 구성된다. 스마트카드는 인가된 유권자에게 선거 관리자가 발행한 조작불가능한 하드웨어 장치이다. 선거가 진행되는 동안 정직한 상태로 남아있어야 하는 최소한의 선거관리자의 수는 (t, N)-threshold 기법에서의 t명이다. 만일 t명 이상의 부정한 선거관리자들이 공모한다면 해독 프로토콜을 수행하여 선거 중간에 부분적인 결과를 알 수 있게 된다.

2) 통신모델

선거에 사용되는 데이터를 저장하기 위해 게시판(bulletin board)이라고 하는 메모리를 가지는 공개채널을 사용한다. 선거 참여자는 게시판 상에 자신의 지정된 영역을 가지며, 이 영역에 메시지를 게시할 수 있다. 게시판에 게시된 메시지는 누구나 읽을 수 있지만 삭제할 수는 없다. 유권자는 게시판 상에 자신의 지정된 영역을 가지며, 이 영역은 [표 1]과 같이 4개의 영역으로 나누어진다. 각 영역에 메시지를 게시하기 위해서는 안전한 인증절차를 거쳐야 하며, 어떤 특정 영역에 메시지를 게시할 권한이 있는 참여자만이 그 영역에 메시지를 게시할 수 있다. 유권자는 또한 자신의 개인 PC에 연결할 수 있는 스마트카드를 소유함으로써 스마트카드와 공개채널로 표를 구성하는 프로토콜을 수행한다.

2. 시스템 설정

시스템을 설정하기 위해서 우선 $q \mid p-1$인 두 개의 매우 큰 소수 p, q를 선택하여 Z_p^*의 부분군이며 위수가 q인 G_q군을 설정하고, [표 2]와 같이 3개의 G_q군의 생성자를 임의로 선택한다. 선거관리자들은 threshold ElGamal 암호프로토콜[7]의 키 생성 프로토콜을 실행하여 개인키 x_A의 비밀조각 x_i, $i=1,...,N$ 소유하고, $y_i=g^{x_i}$를 계산하고 공개하여 x_i를 고정한다. 선거 관리자가 공유하는 개인키 x_A에 대한 공개키는 $y_A=g_A^{x_A}$이다. 각각의 유권자도 개인키와 공개키를 갖는다. 유권자의 개인키는 x_V이고, 공개키는 $y_V=g_V^{x_V}$이다.

표 1: 게시판 상의 유권자의 지정된 영역

영 역	게시내용
암호화된 투표지 영역	유권자가 스마트카드로부터 받은 재암호화한 투표지를 게시
암호화된 투표지의 유효성 증명 영역	유권자가 재암호화한 투표지에 대한 유효성 증명을 게시
최종 투표지 영역	유권자가 최종 투표지를 게시
최종 투표지의 유효성 증명 영역	유권자가 최종 투표지에 대한 유효성 증명을 게시

제안하는 기법은 이병천과 김광조[5]가 제안한 인코딩 방식과 Naccache 암호시스템[8]을 결합하여 표를 구성한다. 이 방식에서는 L이 전체 유권자 수일 때, i, $1 \le i \le K$번째 후보자는 $g_N^{L^{i-1}}$로 표현된다. 선거가 시작되기 전에 선거관리자는 각 후보자 $i=1,...,K$ 나타내는 표를 $(X_i, Y_i)=(1, g_N^{L^{i-1}})$로 표현하여 공개한다. 누구나 각 후보자의 표가 유효한지 확인할 수 있다.

표 2: 시스템 설정을 위한 G_q군의 생성자

생성자	용 도
g_A	threshold ElGamal 공개키 암호 프로토콜의 공개키 $y_A=g_A^{x_A}$를 위한 G_q의 생성자
g_N	후보자의 표를 인코딩하기 위한 G_q의 생성자
g_V	유권자의 개인키가 x_V일 때, 공개키 y_V를 생성하기 위한 G_q의 생성자

3. 선거단계

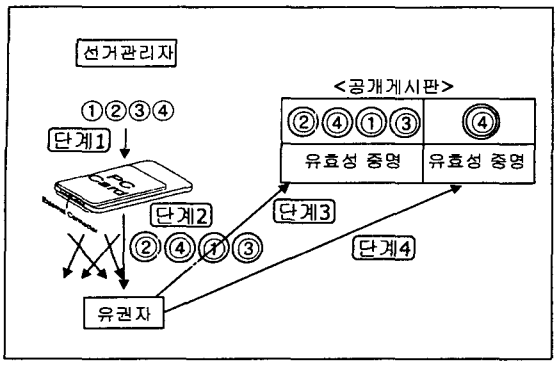

그림 1: 제안하는 전자선거 기법의 선거단계

스마트카드는 유권자에게 각 후보자에 대한 표를 암호화하여 전달하고 암호화된 표의 유효성을 증명한다. 유권자는 스마트카드가 암호화한 투표지 중에서 투표하려는 것을 선택하여 암호화하고 게시판에 게시하여 투표를 마친다. 선거 단계에 대한 전체적인 구성은 [그림 1]과 같이 4단계로 이루어지고, 각 단계에 대한 자세한 설명은 다음과 같다.

단계 1. 선거가 시작되면 인가된 유권자는 선거관리자로부터 스마트카드를 지급 받는다.

단계 2. 스마트카드는 임의의 $\alpha_i,\ i=1,\ldots,K$를 선택하고, 선거관리자가 공개한 후보자의 표 $(X_i, Y_i)=(1, g_c^{L_i})$를 $(X'_i, Y'_i)=(g_A^{\alpha_i}X_i,\ y_A^{\alpha_i}Y_i)$로 암호화하고 유권자에게 모든 $(X_i,\ Y_i)$를 빠짐없이 암호화하였고, 중복된 것이 없다는 것을 K중 하나 암호화 증명[7]을 K번 수행하여 지정된 확인자 증명으로 증명한다. 이 증명은 스마트카드와 유권자 사이의 공개채널을 통해서 유권자에게 전달하는데 증명 내용을 도청 가능한 채널이 아님에도 불구하고 지정된 확인자 증명을 하는 것은 나중에 제3자에게 전달되더라도 스마트카드가 증명한 내용을 제3자가 확신하지 못하도록 하기 위함이다. 유권자는 이 증명을 통해서 어떤 $(X'_i,\ Y'_i)$이 어떤 $(X_i,\ Y_i)$를 암호화하고 있는지 알 수 있게 된다. 지정된 확인자 증명의 특성상 개인키 x_V를 알고 있는 유권자만 스마트카드로부터 받은 증명의 유효성을 확인할 수 있다. 개인키 x_V를 알고 있는 유권자는 증명을 여러 가지 형태로 보일 수 있기 때문에 제3자는 유권자가 제시하는 증명을 신뢰할 수 없다. 그리고 스마트카드는 유권자에게 Furukawa와 Sako[8]가 제안한 shuffle의 정확성 증명을 한다. 이 증명은 permutation matrix를 사용하여 한 번의 증명으로 모든 표가 빠짐없이 암호화되고 섞였다는 것을 증명할 수 있다.

단계 3. 유권자는 스마트카드로부터 받은 모든 $(X_i,\ Y_i)$를 빠짐없이 암호화하였고, 중복된 것이 없다는 것을 K중 하나 암호화 증명[8]을 공개게시판의 암호화된 투표지 영역에 게시하고 shuffle의 정확성 증명으로 투표지의 유효성 증명을 한다. 따라서 누구나 모든 표가 빠짐없이 암호화되었다는 것을 확인할 수 있다.

단계 4. 유권자는 임의의 $\beta\in Z_q$를 선택하여 투표하려는 후보자의 투표지 $(X'_i,\ Y'_i)$를 $(X_F,\ Y_F)=(g_A^{\beta}X'_i,\ y_A^{\beta}Y'_i)$로 재암호화하고 게시판 상에 있는 유권자의 최종 투표지 영역에 게시한다. 게시된 최종 투표가 스마트카드가 공개한 암호화된 투표지 $(X'_i,\ Y'_i)$중 하나를 선택하여 재암호화하였다는 것을 K중 하나 암호화증명을 변형한 변형된 K중 하나 암호화 증명을 이용해서 증명한다. 이 증명은 게시판 상에 있는 유권자의 최종 투표지의 유효성 증명 영역에 게시된다. 따라서 누구나 유권자가 올바르게 투표하였다는 것을 확인할 수 있고 전체검증성이 만족된다.

4. 집계단계

투표가 끝나면 지정된 선거관리자는 유효한 투표지를 모으고, 다음을 계산한다.

$$(X_T,\ Y_T)=\left(\prod_{i=1}^{l}X_{F,i},\ \prod_{i=1}^{l}Y_{F,i}\right)$$

이때, l은 투표한 총 유권자의 수이다. 모든 투표지가 게시판에 게시되기 때문에 누구나 $(X_T,\ Y_T)$를 계산하여 선거관리자가 계산한 값이 올바른지 확인해 볼 수 있다. 이것은 threshold ElGamal 암호시스템의 준동형 특성을 이용하므로 암호해독에 사용되는 개인키 x_A는 N명의 선거관리자 중 t명 이상이 협력해야만 $(X_T,\ Y_T)$를 해독하여 W를 얻을 수 있다. 선거관리자는 해독 프로토콜을 실행하여 $W=(Y_T/X_T^{x_A})$를 계산한다. 투표결과를 집계할 때 개인키 x_A를 재구성하여 각각의 표를 해독하는 것이 아니라 $X_T^{x_A}$를 계산하여 결과를 한꺼번에 계산한다.

선거관리자가 협력하여 해독 프로토콜을 실행하면 다음의 결과를 얻을 수 있다.

표 3: 전자선거 기법 비교

		Hirt의 기법	이병천과 김광조의 기법	조진현 등의 기법	제안하는 기법
기본 요구사항		○	○	○	○
매표방지		○	○	○	○
전체검증		×	○	○	○
유권자의 계산량	K중 하나 암호화 증명	1번	1번	1번	1번
	유효성 확인	1번	1번	1번	1번
HR 또는 스마트카드의 계산량	K중 하나 암호화 증명	없음	없음	K번	K번
	지정된 확인자 증명	1번	1번	K번	K번
통신채널에 대한 가정		양방향 도청 불가능한 채널	스마트카드 이용	일방향 도청 불가능한 채널	스마트카드 이용
Randomness의 선택 (표의 암호화 흐름)		유권자가 먼저선택	유권자가 먼저선택	신뢰기관이 먼저선택	스마트카드가 먼저선택
최종 게시자		신뢰기관	스마트카드	유권자	유권자

$$W = g_N^{r_1 L^0 + r_2 L^1 + \cdots r_K L^{K-1}}$$

이 값은 Naccache 암호시스템으로 인코딩한 표값이므로 해독할 때 중국인의 나머지 정리를 이용하여 개인키를 알고있는 사람만이 기저 g에 대한 c의 이산대수를 계산할 수 있다. 모든 집계가 이루어진 다음에만 계산을 할 수 있으므로 선거가 끝나기 전에 중간결과를 알 수 없으며, 개별 표에 대한 해독이 불가능하여 선거의 비밀성 및 강건성을 만족시킨다. 또한 기존의 ElGamal 암호시스템을 이용한 표의 인코딩과 비교하여 이산대수를 풀어야 하는 어려운 문제에서 투표자의 수가 많은 큰 규모의 선거에 대해서도 다항시간 내에 집계가 가능하다.

IV. 성능 분석 및 향후 과제

제안한 시스템은 선거시스템이 기본적으로 만족해야 하는 요구사항을 모두 충족시키면서 전자선거를 구성할 때 문제가 되는 매표방지 및 전체검증을 모두 제공한다. 기존의 기법과 비교하였을 때 통신채널에 대한 물리적 가정이 없어 보다 현실적이며, 이병천과 김광조[5]의 기법보다는 하드웨어 장치에 대한 신뢰성에 대한 의존이 보다 적은 편이다. 또한 표의 유효성 증명에서 후보자의 수가 K명일 때, K중 하나 암호화 증명을 K번 하던 것을 shuffle의 정확성 증명 한번으로 줄여서 효율성을 높였다. 또한 표의 인코딩을 준동형 특성을 만족하는 threshold ElGamal 암호시스템과 다차 잉여 기반 암호시스템인 Naccache 시스템을 결합하여 사용하므로 투표자의 수가 다수인 큰 규모의 선거에 대해서 다항시간내에 집계가 가능하도록 하였다. 그러나 스마트카드가 유권자에게 모든 표가 빠짐없이 암호화된 것을 증명할 때, shuffle의 정확성 증명을 지정된 확인자 증명으로 하면 K중 하나 암호화 증명을 할 필요 없이 더 효율적으로 할 수 있다. 이는 본 과제에서 효율성을 더 높이기 위한 하나의 방법이 될 수 있다.

앞으로 전자선거가 현재 사용되고 있는 선거를 완전히 대체하기 위해서는 보다 안전한 하드웨어 장치의 개발과, 사용자가 장치를 신뢰하지 않아도 암호 알고리즘을 이용하여 안전한 프로토콜을 수행할 수 있는 확신을 가질 수 있도록 하는 프로토콜을 개발에 대한 연구가 더욱 필요하다.

참고문헌

[1] A. Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections," *Advanced in Cryptology, AUSCRYPT* '92, LNCS 718, pp. 244-251, Springer, 1993.

[2] K. Sako and J. Kilian, "Receipt-free

Mix-Type Voting Scheme: A Practical Solution to the Implementation of a Voting Booth," *Advances in Cryptology, Eurocrypt* '95, LNCS 921, pp. 393-403, Springer, 1995.

[3] J. Benaloh and D. Tuinstra, "Receipt-free Secret-Ballot Elections," *Proc. of the 26th ACM Symp. on Theory of Computing*, pp. 544-553, ACM Press, 1994.

[4] M. Hirt, "Receipt-free Voting with Randomizers," Presentated at the *Workshop on Trustworthy Elections, Aug.* 2001.

[5] B. Lee and K. Kim, "Receipt-free electronic voting scheme with a tamper-resistant randomizer," *Pre-Proc. of ICISC2002*, pp. 405-422, 2002.

[0] 조진현, 김상진, 오희국, "일방향 도청 불가능한 채널만을 이용하여 전체검증과 매표방지를 제공하는 전자선거 기법," 한국정보보호학회 논문지, 제13권, 제2호, pp. 49-61, 2003년 4월.

[6] T. P. Pedersen, "A Threshold Cryptosystem without a Trusted Party," *Advances in Cryptology, Eurocrypt* '91, LNCS 547, pp. 522-526, Springer, 1991.

[7] M. Hirt and K. Sako, "Efficient Receipt-Free Voting Based on Homomorphic Encryption," *Advances in Cryptology, Eurocrypt* '00, LNCS 1807, pp. 539-556, Springer, 2000.

[8] D. Naccache and J. Stern, "A New Public Key Cryptosystem Based on Higher Residues," *Proc. of the 5th ACM Conf. on Computer and Communications Security*, pp. 59-66, ACM Press, 1998.

[9] J. Furukawa and K. Sako, "An Efficient Scheme for Proving a Shuffle," To appear in *CRYPTO 2001*.