情報保護學會論文誌
第13券 第2號, 2003. 4

일방향 도청 불가능한 채널만을 이용하여 전체검증과 매표방지를 제공하는 새로운 전자선거 기법

조 진 현*, 김 상 진**, 오 희 국*

A New Universally Verifiable and Receipt-free Electronic Voting Scheme Using Only One-way Untappable Channels

Jinhyeon Cho*, Sangjin Kim**, Heekuck Oh*

요 약

공정하고 투명한 전자선거를 이루기 위해서는 비밀성(privacy), 선거권(eligibility) 등과 함께 전체검증(universal verifiability)과 매표방지(receipt-freeness) 속성이 반드시 제공되어야 한다. 그러나 매표방지와 전체검증은 상반되는 의미를 지니고 있어 두 가지 특성을 모두 만족시키는 것은 어렵다. 지금까지 제안된 전자선거 기법을 살펴보면 둘 중 한가지 특성만을 제공하거나 두 가지 특성을 제공하는 경우 계산량이 많아 실용적이지 못하다. 이 논문에서는 매표방지와 전체검증을 제공하면서 효율적인 전자선거 기법을 제안한다. 이 기법은 최소한의 물리적 가정인 일방향 도청 불가능한 채널(one-way untappable channel)을 가정하고, 준동형 암호화(homomorphic encryption) 기법을 이용한다. 유권자는 HR(Honest Randomizer)과 대화를 통해서 투표지를 구성하고, 이것이 유효하다는 증명과 함께 투표지를 게시판에 게시한다. 제안하는 기법은 일방향 도청 불가능한 채널을 가정하는 기법 중에서 계산량이 가장 적으며, 기존의 전체검증과 매표방지를 제공하는 기법보다 약한 물리적 가정을 사용한다. 새 시스템의 안전성 분석과 관련 시스템과의 성능 비교분석도 다룬다.

ABSTRACT

Electronic voting schemes must provide universal verifiability and receipt-freeness, as well as basic properties such as privacy, eligibility, to make the election fair and transparent. But it is difficult to provide both universal verifiability and receipt-freeness because they are mutually contradictory in their objective. To date, most electronic voting schemes provide only one of these properties and those few that provide both properties are not practical due to heavy computational load. In this paper, we present an efficient electronic voting scheme that provides both properties. The proposed scheme uses a trusted third party called HR(Honest Randomizer) and requires only one-way untappable channels from HRs to voters. Among the schemes that assume only one-way untappable channel this scheme requires the least amount of computation. Among the schemes that provide both properties, this scheme uses the weakest physical assumption. We also discuss the security of the system and compare our scheme with other realted schemes.

Keyword : *electronic voting, receipt-freeness, universal verifiability, homomorphic encryption*

Ⅰ. 서 론

선거는 민주주의를 실현하는데 가장 중요한 도구 중 하나이다. 국민들은 선거를 통해 국가의 대소사에 참여하게 된다. 그러나 현행 선거방식은 그 낙후성으로 인해 자원낭비가 심하고, 거대해진 현대사회에서

* 한양대학교 컴퓨터공학과 분산컴퓨팅연구실({jhjo, hkoh}@cse.hanyang.ac.kr)
** 한국기술교육대학교 인터넷미디어공학부(sangjin@kut.ac.kr)

국민들의 의견을 정확하고 신속하게 반영하기에 부족한 면이 많다. 또한 시간과 공간상의 제약으로 인하여 많은 사람들이 선거에 참여하지 않아, 전 세계적으로 저조한 선거 참여율이 문제가 되고 있다. 인터넷을 통한 전자선거가 실현되면 지역적인 제한없이 인터넷에 연결된 컴퓨터만 있다면 언제, 어디서나 선거에 참여할 수 있게 된다. 따라서 현재 문제가 되고 있는 저조한 선거 참여율을 어느 정도 해결할 수 있을 것으로 전망된다. 또한 투표와 개표하는 시간이 짧아지며 집계에 드는 시간과 비용도 절감된다.

전자선거가 현재 사용되고 있는 선거방식을 대체하기 위해서는 비밀성, 선거권 등과 같은 선거가 기본적으로 만족해야하는 요구사항[1]을 모두 만족해야 하며, 선거를 전자적으로 구성하였을 때 생길 수 있는 문제점[1-4]들을 정확히 파악하고 해결해야 한다. 전자선거가 실행되었을 때 문제가 될 수 있는 것 중 하나는 선거에 사용된 데이터가 변경되거나 삭제되는 것이다. 선거가 전자적으로 구성되면 모든 것이 디지털 정보 형태로 표현되고 통신망을 통해 전달된다. 이러한 경우 악의적인 외부 공격자나 선거관리자에 의해 선거에 사용된 데이터가 변경되거나 삭제될 수 있다. 또한 선거관리자가 고의로 유효한 표를 집계에서 누락시킬 수도 있다. 따라서 전자선거 기법은 선거가 올바르게 진행되었는지를 확인할 수 있도록 검증절차(verifiability)를 제공해야 한다. Sako와 Kilian[3]은 Fujioka[1] 등이 정의한 검증을 개별검증(individual verifiability)과 전체검증(universal verifiablitiy)으로 세분화하였다. Fujioka 등이 정의한 검증은 개별검증으로 투표한 유권자만이 자신의 표가 집계에 포함되었는지를 확인할 수 있다. 전체검증에서는 누구나 개별 투표지의 유효성과 집계결과의 유효성을 확인할 수 있다. 투명한 선거가 되기 위해서는 전자선거 기법이 전체검증을 제공하여 부정선거에 대한 의혹이 발생하지 않도록 해야 한다.

선거를 전자적으로 구성할 때 생기는 또 다른 문제는 매표행위[2]이다. 현재의 선거방식은 밀폐된 투표소를 사용하므로 유권자가 어떤 후보자에게 투표하였는지 확인할 수 없어 표를 사고 파는 것이 어렵다. 그러나 선거를 전자적으로 구성하면 선거에 사용된 모든 데이터를 유권자가 저장할 수 있고, 특정 후보자에게 투표했다는 증거를 남길 수 있다. 유권자는 이러한 증거를 구매자에게 제시하고 표를 팔 수 있으며, 구매자는 증거를 확인한 후 표를 살 수 있다. 매표행위를 방지하기 위해서는 유권자가 특정 후보자에게 투표했다는 증거를 남길 수 없거나, 유권자가 증거를 남길 수 있어도 구매자가 증거를 통해 유권자가 특정 후보자에게 투표했는지 확신할 수 없어야 한다.

공정하고 투명한 전자선거를 이루기 위해서 매표방지와 전체검증은 반드시 제공되어야 하지만 두 가지 특성이 상반되는 의미를 지니고 있어 동시에 만족시키기는 어렵다. 지금까지 제안된 전자선거 기법을 살펴보면 둘 중 한 가지 특성만을 제공하거나[5,6] 두 가지 특성을 모두 제공하는 경우 계산량이 많아 실용적이지 못하다[3,7].

이 논문에서는 신뢰할 수 있는 제3자인 HR(Honest Randomizer)과 최소한의 물리적 가정인 일방향 도청 불가능한 채널(one-way untappable channel)을 이용하여 매표방지와 전체검증을 제공하는 효율적인 전자선거 기법을 제안한다. 선거가 시작되면 HR은 암호화된 투표지를 암호화하여 섞은 다음 공개적으로 유효함을 증명하고, 도청 불가능한 채널을 통해 지정된 확인자 증명(designated verifier proof)으로 유권자에게 섞인 순서를 증명한다. 유권자는 투표하려는 후보자의 표를 선택하여 재암호화한 후 게시판에 게시하고, 투표지의 유효함을 공개적으로 증명한다. 이 기법은 일방향 도청 불가능한 채널을 가정하는 기법 중에서 계산량이 가장 적으며, 기존의 전체검증과 매표방지를 제공하는 기법보다 약한 물리적 가정을 사용한다.

이 논문의 구성은 다음과 같다. 2장에서는 기존의 전자선거 기법의 특성과 문제점을 분석하고, 3장에서는 제안하는 전자선거 기법에서 사용하는 기본 암호프로토콜을 설명한다. 4장에서는 제안하는 전자선거 기법을 서술하고, 5장에서는 이 기법의 안전성을 분석하고 기존 전자선거 기법과 비교하여 장단점을 논의한다. 끝으로 6장에서는 결론과 향후 연구 방향에 대해 서술한다.

II. 관련연구

전자선거 기법은 Chaum[8]이 1981년에 처음으로 제안한 이후 많은 발전을 거듭하여 오늘날까지 다양한 기법이 제안되었다. 지금까지 제안된 전자선거 기법들은 접근방법에 따라 크게 세가지로 분류할 수 있다.

- 준동형 암호화를 이용한 전자선거 기법[2,4,6,9,10,11]
- 믹스넷(mix-net)을 이용한 전자선거 기법[3,7,8,12]
- 은닉서명(blind signature)을 이용한 전자선거 기법[1,5,13,14]

Benaloh와 Tuinstra[2]는 선거관리자와 유권자 사이의 비밀통신을 물리적으로 보장하는 선거부스(voting booth)와 준동형 암호화 기법을 이용하는 두 가지 전자선거 기법을 제안하였다. 첫 번째 전자선거 기법은 단일 선거관리자를 이용하여 매표방지를 제공하였지만 유권자의 투표내용이 노출되는 단점이 있다. 두 번째 프로토콜은 다중 선거관리자를 두어 유권자의 투표내용이 노출되는 것을 방지하였다. 그러나 유권자가 cut-and-choose 기법으로 투표지의 유효성을 증명할 때, 임의의 문자열을 선택하여 해쉬한 값을 사용하면 매표행위가 가능해진다[7].

이병천과 김광조[11]는 정직한 확인자(Honest Verifier, HV)라고 하는 신뢰할 수 있는 제3자를 이용하여 매표방지와 전체검증을 제공하는 전자선거 기법을 제안하였다. 이 전자선거 기법에서 유권자는 자신이 구성한 첫 번째 투표지와 HV가 생성하는 임의의 쌍을 곱해서 최종 투표지를 구성하여 투표하게 된다. 유권자는 도청 불가능한 채널을 통해 HV에게 첫 번째 투표지를 전달하고, HV도 도청 불가능한 채널을 통해 임의의 쌍을 유권자에게 전달하기 때문에 유권자는 구매자에게 가짜 트랜스크립트를 제시할 수 있게 된다. 따라서 구매자는 유권자를 신뢰할 수 없게되어, 매표행위를 방지할 수 있다. Hirt[6]는 HV가 임의의 쌍에 대해서 유효성을 증명할 때 유권자가 선택하는 임의의 도전값을 특정 값으로 고정하면 유권자는 가짜 트랜스크립트를 생성할 수 없게 되어, 매표행위를 막을 수 없다는 것을 증명하였다. 그러나 HV가 유권자에게 임의의 쌍에 대해서 유효성을 증명할 때 일반적인 영지식 증명(zero-knowledge proof)를 이용하지 않고 지정된 확인자 증명으로 증명하면 매표행위를 방지할 수 있다.

Hirt는 이병천과 김광조의 기법을 확장한 새로운 전자선거 기법을 제안하였다[6]. 이 기법은 이병천과 김광조의 기법에서 이용한 HV와 비슷한 역할을 하는 신뢰할 수 있는 제3자인 HR을 이용한다. 유권자는 투표지를 구성하여 도청 불가능한 채널을 통해 HR에게 투표지를 전달한다. 그러면 HR은 이것을 재암호화하여 게시판에 게시하고 재암호화가 올바르게 이루어졌다는 것을 도청 불가능한 채널을 통해 지정된 확인자 증명으로 유권자에게 증명한다. 유권자는 지정된 확인자 증명을 통해 투표지의 유효성 증명을 받았기 때문에 구매자에게 가짜 트랜스크립트를 제공할 수 있고, 구매자는 유권자를 신뢰할 수 없어 매표행위가 방지된다. 그러나 Hirt가 제안한 전자선거 기법은 전체검증을 제공하지 않는다.

Sako와 Kilian[3]은 믹스넷을 이용하여 처음으로 매표방지와 전체검증을 제공하는 전자선거 기법을 제안하였다. 이 기법은 최소한의 물리적 가정인 일방향 도청 불가능한 채널을 가정한다. 그러나 믹스넷을 이용하여 유권자의 익명성을 보장하고 단일 표를 일일이 해독하여 집계하기 때문에 시간이 많이 걸리고 계산량이 많은 단점이 있다.

믹스넷을 이용하는 또 다른 전자선거 기법으로는 Hirt와 Sako[7]가 제안한 기법이 있다. 선거가 시작되면 첫 번째 믹스서버는 암호화된 투표지들을 재암호화하여 섞은 다음 두 번째 믹스서버에게 전달한다. 그런 다음 재암호화한 투표지들의 유효성을 공개적으로 증명하고, 도청 불가능한 채널을 통해 지정된 확인자 증명으로 유권자에게 섞인 순서를 증명한다. 이러한 과정을 마지막 믹스서버까지 반복하게 되면, 최종적으로 재암호화된 표가 어떤 후보자를 나타내고 있는지를 유권자만 알 수 있게 된다. 유권자는 마지막 믹스서버가 공개한 투표지 중 원하는 후보자의 표를 선택하여 게시판에 게시하여 투표를 한다. 선거관리자가 지정된 확인자 증명을 통해 유권자에게 섞인 순서를 증명하기 때문에 유권자는 구매자에게 섞인 순서를 거짓으로 증명할 수 있다. 또한 재암호화된 투표지의 유효성을 공개적으로 증명하기 때문에 선거가 올바르게 진행되었는지를 누구나 확인할 수 있다. 즉, 매표방지와 전체검증을 제공한다. 그러나 이 기법은 각각의 믹스서버(mix server)가 계산해야 하는 증명이 너무 많아 후보자가 여럿인 선거에는 적합하지 않다.

Okamoto[14]는 은닉서명과 트랩도어 비트위임(trapdoor bit-commitment)을 이용하여 매표방지를 제공하는 전자선거 기법을 제안하였다. 그러나 이 기법은 유권자가 비트위임에 사용되는 개인키를 모르는 상태에서 투표를 하면 매표행위가 가능해지는 단점이 있다. Okamoto[5]는 이 단점을 보안한 새로운 두 가지 전자선거 기법을 제안하였다. 첫 번째 기법에서는 PRC (Parameter Registration Committee)를 가정하고, PRC를 통해 유권자가 개인키를 알도록 한다. 두 번째 기법에서는 양방향 도청 불가능한 채널인 선거부스를 가정하고, 유권자가 개인키를 알고 있다는 것을 선거부스를 통해 선거관리자에게 증명한다. 그러나 Okamoto의 전자선거 기법은 매표방지는 제공하지만 전체검증은 제공하지 않는다.

Ⅲ. 기본 프로토콜

이 논문에 있는 모든 수학 연산은 군(group)의 위수(order)가 매우 큰 소수 q인 G_q군에서 이루어진다. 이 군은 먼저 큰 소수 p를 선택하고, $p-1$의 소인수 중 하나인 q를 선택하여 구성한다. G_q군은 곱셈군 Z^*_p의 부분군(subgroup)으로 1을 제외한 모든 원소는 법 p에서 G_q군의 생성자가 된다. G_q의 생성자를 g 또는 g_i와 같이 g에 아래첨자를 사용하여 표현한다. 이 논문에서 지수 요소와 관련된 연산은 법 q에서 이루어지고 나머지 군 연산은 모두 법 p에서 이루어진다. 이후, 논문에서는 법 p와 q에 대한 연산 표기를 생략한다.

3.1 Threshold ElGamal 암호프로토콜

Threshold ElGamal 암호프로토콜에서는 개인키 $x \in Z_q$를 한 명이 소유하지 않고, n개의 비밀조각(secret share) $x_i, i=1,\ldots,n$로 나눈 다음 n명의 참여자에게 분산한다. 암호화된 메시지를 해독하기 위해서는 $t \le n$명의 정직한 참여자가 협력해야 한다. Threshold ElGamal 암호프로토콜은 키 생성 프로토콜(key generation protocol), 암호 알고리즘, 해독 프로토콜(decryption protocol)로 구성된다[15]. 암호 알고리즘은 일반 ElGamal 암호 알고리즘[16]과 같다.

- 키 생성 프로토콜 : 참여자는 Pedersen이 제안한 키 생성 프로토콜[15]을 실행한다. 키 생성 프로토콜이 끝나면 n명의 참여자는 개인키 x의 비밀조각 $x_i \in Z_q, 1 \le i \le n$를 소유하게 된다. 참여자는 x_i를 고정하기 위해서 $y_i = g^{x_i}$를 계산하고 공개한다. $t \le n$명 이상의 정직한 참여자 집합을 Λ라고 하면 다음 식에 의해서 개인키 x를 재구성할 수 있다.

$$x = \sum_{i \in \Lambda} x_i \lambda_{i,\Lambda}, \qquad \lambda_{i,\Lambda} = \prod_{l \in \Lambda \setminus \{i\}} \frac{l}{l-i}$$

  공개키 $y = g^x$는 시스템의 모든 참여자에게 공개된다. t보다 적은 참여자만으로는 개인키 x를 재구성할 수 없고, 개인키 x는 계산적으로 보호된다.
- 해독 프로토콜 : 개인키 x를 재구성하지 않고 암호문 $(a, b) = (g^a, y^a m)$을 해독하기 위해서 참여자는 다음의 프로토콜을 실행한다.

  1. 각각의 참여자는 $w_i = a^{x_i}$를 계산하여 다른 참여자들에게 브로드캐스트하고 다음을 영지식으로 증명한다.

$$\log_g y_i = \log_a w_i$$

  2. 영지식 증명을 통과한 $t \le n$명의 참여자 집합을 Λ라고 하면, 다음과 같이 평문 m을 얻을 수 있다.

$$m = b / \prod_{i \in \Lambda} w_i^{\lambda_{i,\Lambda}}$$

3.2 준동형 암호화

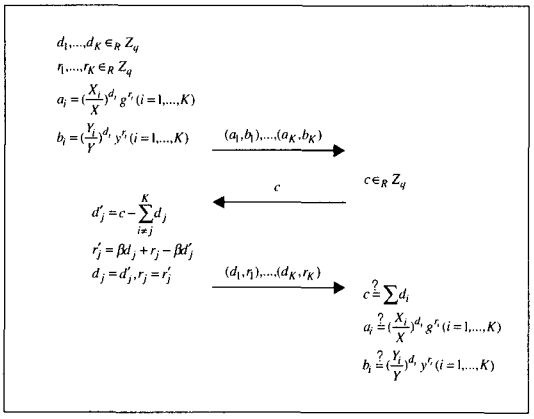
ε은 확률적 암호화 기법이고, 군 M은 어떤 $\oplus$연산에 대해서 닫혀있는 메시지 공간이며, 군 C는 어떤 $\otimes$연산에 대해서 닫혀있는 암호문 공간이라 하자. ε의 모든 인스턴스 E에 대해 $c_1 = E_{r_1}(m_1)$과, $c_2 = E_{r_2}(m_2)$가 주어졌을 때, 다음을 만족하는 r이 존재하면, ε을 $(\oplus, \otimes)$ 준동형(homomorphic) 암호화 기법이라 한다.

$$c_1 \oplus c_2 = E_r(m_1 \oplus m_2)$$

ElGamal 암호화 알고리즘은 준동형 속성을 만족한다. 평문 m_1을 암호화한 암호문이 (a_1, b_1)이고, 평문 m_2를 암호화한 암호문이 (a_2, b_2)일 때, 평문 $m_1 m_2$를 암호화한 암호문은 $(a_1 a_2, b_1 b_2)$가 된다. 평문 m이 Z_q군에 속하는 경우에는 고정된 생성자 $g \in G_q$를 이용하여 g^m으로 만든 다음에 ElGamal 암호화를 할 수 있다. 이 경우에도 준동형 속성을 만족한다. 즉, 평문 m_1을 암호화한 암호문이 $(a_1, b_1) = (g^{\alpha_1}, y^{\alpha_1} g^{m_1})$이고, 평문 m_2를 암호화한 암호문이 $(a_2, b_2) = (g^{\alpha_2}, y^{\alpha_2} g^{m_2})$라고 할 때, 두 암호문 (a_1, b_1)과 (a_2, b_2)를 곱한 것은 평문 $m_1 + m_2$를 암호화한 것과 같다.

3.3 K중 하나 암호화 증명

(X, Y)를 암호화한 암호문이 K개의 암호문 $(X_1, Y_1), \cdots, (X_K, Y_K)$ 중에 있다는 것을 암호화에 사용된 비밀값을 밝히지 않으면서 증명하는 프로토콜은 [그림 1]과 같다[7]. [그림 1]의 프로토콜에서 (X, Y)를 암호화한 암호문을 (X_j, Y_j)라 가정하고, 암호화에 사용된 비밀값을 $\beta \in Z_q$라고 가정한다. 즉, $(X_j, Y_j) = (g^\beta X, y^\beta Y)$가 된다.



〔그림 1〕 K중 하나 암호화 증명

1. 증명자는 임의로 $d_1,\cdots,d_K$와 $r_1,\cdots,r_K$를 선택하고, 다음을 계산하여 확인자에게 전송한다.

$$a_i=(\frac{X_i}{X})^{d_i} g^{r_i},\quad b_i=(\frac{Y_i}{Y})^{d_i} y^{r_i}$$

$i=j$인 경우를 제외한 모든 d_i와 r_i는 고정된다. $a_j=g^{\beta d_j+r_j}$이고, $b_j=y^{\beta d_j+r_j}$이므로 비밀값 β를 알고 있는 증명자는 나중에 d_j와 r_j를 변경할 수 있다.

2. 확인자는 임의의 도전값 $c\in Z_q$를 선택하여 증명자에게 전송한다.
3. 증명자는 $c=d_1+\cdots+d'_j+\cdots+d_K$가 되도록 d_j를 d'_j로 변경하고, $\beta d_j+r_j=\beta d'_j+r'_j$가 되도록 r_j를 r'_j로 변경한다. 그런 다음, $d_1,\cdots,d'_j,\cdots,d_K$와 $r_1,\cdots,r'_j,\cdots,r_K$를 확인자에게 전송한다.
4. 확인자는 다음을 확인한다.

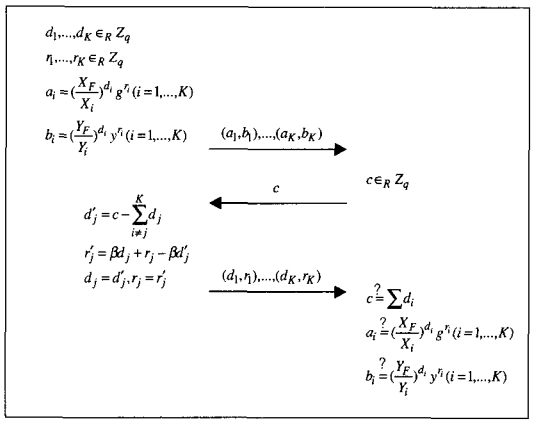
$$c?=\sum d_i$$

$$a_i?=(\frac{X_i}{X})^{d_i} g^{r_i}(i=1,\cdots,K)$$

$$b_i?=(\frac{Y_i}{Y})^{d_i} y^{r_i}(i=1,\cdots,K)$$

[그림 1]에 기술된 프로토콜은 도전과 응답을 통해 이루어지지만 Fiat와 Shamir가 제안한 기법[17]을 이용하면 비상호작용 증명으로 변환할 수 있다.

1. 증명자는 상호작용 증명과 동일하게 a_i와 b_i를 계산한다.



〔그림 2〕 변형된 K중 하나 암호화 증명

2. 증명자는 도전값 $c=H(E\|a_1\|\cdots\|a_K\|b_1\|\cdots\|b_K)$를 계산한다. 이때, E는 다음과 같다.

$$E=(X\|Y\|X_1\|X_2\|\cdots\|X_K\|Y_K)$$

3. 계산한 도전값 c에 맞게 $d_i, r_i(i=1,\cdots,K)$를 변경하고, $(d_1,r_1),\cdots,(d_K,r_K)$를 확인자에게 전송한다.
4. 확인자는 다음을 확인한다.

$$d_1+\cdots+d_K\ ?=$$
$$H(E\|(\frac{X_1}{X})^{d_1} g^{r_1}\|\cdots$$
$$\|(\frac{X_K}{X})^{d_K} g^{r_K}$$
$$\|(\frac{Y_1}{Y})^{d_1} y^{r_1}\|\cdots$$
$$\|(\frac{Y_K}{Y})^{d_K} y^{r_K})$$

앞에서 설명한 프로토콜을 약간만 변형하면 K개의 $(X_1,Y_1),\cdots,(X_K,Y_K)$ 중 하나인 (X_j,Y_j)를 암호화한 암호문이 (X_F,Y_F)라는 것을 증명하는 프로토콜로 바꿀 수 있다. 이 프로토콜은 [그림 2]와 같고 암호화에 사용된 비밀값을 $\beta\in Z_q$라고 가정한다. 즉, $(X_F,Y_F)=(g^{\beta}X_j, y^{\beta}Y_j)$가 된다.

이 프로토콜도 [그림 1]에 기술된 프로토콜과 마찬가지로 Fiat와 Shamir가 제안한 기법을 이용하면 비상호작용 증명으로 변환할 수 있다.

3.4 지정된 확인자 증명

K개의 $(X_i,Y_i), i=1,\cdots,K$를 암호화하고 임의

의 순서로 섞은 K개의 암호문 $(X'_1, Y'_1), \cdots, (X'_K, Y'_K)$가 있을 때, 섞인 순서를 지정된 확인자만 알 수 있도록 증명하는 프로토콜은 [그림 3]과 같다[6]. 이 프로토콜에서 임의의 (X_j, Y_j)를 암호화한 암호문을 $(X'_j, Y'_j) = (g^{\beta} X_j, y^{\beta} Y_j)$ 라고 가정하고, 암호화에 사용된 비밀값을 $\beta \in Z_q$라고 가정한다. 확인자의 개인키는 $x_A \in Z_q$이고, 공개키는 $y_V = g^{x_V}$이다. 증명자는 암호화에 사용되는 비밀값 β를 밝히지 않으면서 (X'_j, Y'_j)가 (X_j, Y_j)를 암호화한 암호문이라는 것을 다음의 절차에 따라 지정된 확인자에게 증명한다.

1. 증명자는 임의로 $w, s_2, c_2 \in Z_q$를 선택하고 다음을 계산해서 확인자에게 전송한다.

$$a = g^w, b = y^w, d = g^{s_2} / y_V^{c_2}$$

이 경우 w, s_2, c_2는 고정된다. 그러나 개인키 x_V를 알고 있는 확인자는 $s_2 - x_V c_2 = s'_2 - x_V c'_2$를 만족하는 s'_2, c'_2를 선택하여 원하는 대로 d를 공개할 수 있다.

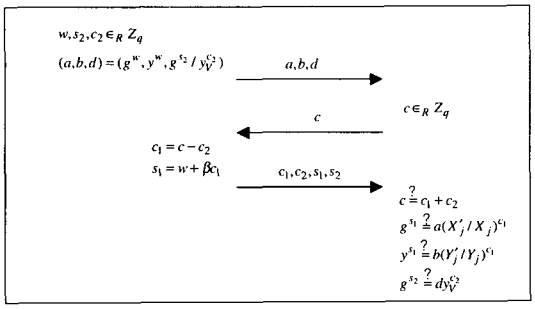
2. 확인자는 임의의 도전값 $c \in Z_q$를 선택하여 증명자에게 전송한다.
3. 증명자는 $c_1 = c - c_2$와 $s_1 = w + \beta c_1$을 계산하고, c_1, c_2, s_1, s_2를 확인자에게 전송한다.
4. 확인자는 다음을 확인한다.

$$c \stackrel{?}{=} c_1 + c_2$$

$$g^{s_1} \stackrel{?}{=} a (X'_j / X_j)^{c_1}$$

$$y^{s_1} \stackrel{?}{=} b (Y'_j / Y_j)^{c_1}$$

$$g^{s_2} \stackrel{?}{=} d y_V^{c_2}$$



〔그림 3〕 지정된 확인자 증명

증명자는 트랩도어 비트위임을 이용하여 섞인 순서를 증명한다. 개인키 x_V를 알고 있는 확인자만 증명의 유효성을 확인할 수 있다. 또한 개인키 x_V를 알고 있는 확인자는 증명을 자신이 원하는 형태로 바꾸어서 공개할 수 있다. 따라서 제3자는 확인자가 공개하는 증명을 신뢰할 수 없다. 공개키 $y_V = g^{x_V}$를 만족하는 개인키 x_V를 알고 있는 확인자는 암호문 (X, Y)의 재암호문이 (X', Y')이 아닌 임의의 암호문 $(\tilde{X}, \tilde{Y})$라고 제3자에게 거짓으로 증명할 수 있다. 확인자는 임의로 $\tilde{c}_1, \tilde{s}_1, \tilde{s}_2 \in Z_q$를 선택하고 다음을 계산하여 $(\tilde{X}, \tilde{Y})$를 만족하는 가짜 트랜스크립트를 쉽게 만들 수 있다.

$$\tilde{a} = g^{\tilde{s}_1} (\tilde{X} / X)^{-\tilde{c}_1}$$

$$\tilde{b} = y^{\tilde{s}_1} (\tilde{Y} / Y)^{-\tilde{c}_1}$$

$$\tilde{c}_2 = c - \tilde{c}_1$$

$$d = g^{\tilde{s}_2 - x_V \tilde{c}_2}$$

[그림 3]에 기술된 프로토콜은 도전과 응답을 통해 이루어지는 프로토콜이지만 도전값 C를 다음과 같이 계산하여 사용하면 비상호작용 증명으로 바꿀 수 있다.

$$c = H(E \| a \| b \| d), E = (X \| Y \| X' \| Y')$$

Ⅳ 제안하는 전자선거 기법

이 장에서는 매표방지와 전체검증을 제공하는 전자선거 기법을 제안한다. 이 기법은 신뢰할 수 있는 제3자인 HR과 일방향 도청 불가능한 채널을 가정한다.

4.1 시스템 모델

4.1.1 참여자

이 전자선거 기법은 N명의 선거관리자 $(A_1, \cdots, A_N)$, L명의 유권자 $(V_1, \cdots, V_L)$, M명의 HR, K의 후보자로 구성된다. 유권자는 한 명의 HR과의 상호작용을 통해 투표지를 구성하지만, 실패할 경우를 대비하여 M명의 HR을 둔다. 특히, DOS(Denial Of Service) 공격에 대한 방어수단으로 사용한다. 선거가 진행되는 동안 정직한 상태로 남아있어야 하는 최소한의 선거관리자의 수는 t명이다. 만일 t명 이상의 부정한 선

거관리자가 공모하면 암호해독 프로토콜을 실행하여 선거 중간에 부분적인 결과를 알 수 있게 된다.

4.1.2 통신모델

게시판. 선거에 사용되는 데이터를 저장하기 위해 게시판(bulletin board)이라고 하는 메모리를 가지는 공개채널을 사용한다. 선거관리자와 유권자는 게시판 상에 자신의 지정된 영역을 가지며, 이 영역에 메시지를 게시할 수 있다. 게시판에 게시된 메시지는 누구나 읽을 수 있지만 삭제할 수는 없다. 게시판에서 유권자의 영역은 [표 1]과 같이 4개로 나누어진다. 각 영역에 메시지를 게시하기 위해서는 안전한 인증 절차를 거쳐야 하며, 어떤 특정 영역에 메시지를 게시할 권한이 있는 참여자만이 그 영역에 메시지를 게시할 수 있다.

일방향 도청 불가능한 채널. 우리는 HR로부터 유권자로 가는 채널이 도청 불가능함을 가정한다. HR만이 이 채널을 통해서 유권자에게 메시지를 보낼 수 있으며, 유권자를 제외한 누구도 어떤 메시지가 채널을 통해 전달되었는지 알 수 없어야 한다. 채널의 안전성은 물리적으로 보장되어야 한다.

4.2 시스템 설정

시스템을 설정하기 위해서 우선 $q \mid p-1$인 두 개의 매우 큰 소수 p와 q를 선택하여 Z^*_p의 부분군이며 위수가 q인 G_q군을 설정하고, [표 2]와 같이 3개의 G_q군의 생성자를 임의로 선택한다. 각각의 선거관리자는 threshold ElGamal 암호프로토콜의 키 생성 프로토콜을 실행하여 개인키 x_A의 비밀조각 $x_i, i=1,\cdots,N$를 소유하고, $y_i=g_A^{x_i}$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.

제안하는 전자선거 기법은 이병천과 김광조[18]가 제안한 인코딩 방식을 이용한다. 이 인코딩 방식에서는 이 전체 유권자 수일 때, $i, 1\le i\le K$번째 후보자는 $g_C^{L^{i-1}}$로 표현된다. 선거가 시작되기 전에 선거관리자는 각 후보자 $i=l,\cdots,K$를 나타내는 표를 $(X_i, Y_i)=(1, g_C^{L^{i-1}})$로 표현하여 공개한다. 누구나 각 후보자의 표가 유효한지 확인할 수 있다.

[표 1] 게시판 상의 유권자의 지정된 영역

게시순서	영 역	게시자	게시내용
1	암호화된 투표지 영역	HR	HR이 암호화한 투표지를 게시한다.
2	암호화된 투표지의 유효성 증명 영역	HR	HR이 암호화한 투표지에 대한 유효성 증명을 게시한다.
3	최종 투표지 영역	유권자	유권자가 최종 투표지를 게시한다.
4	최종 투표지의 유효성 증명 영역	유권자	최종 투표지에 대한 유효성 증명을 게시한다.

4.3 선거단계

유권자가 HR을 통해서 투표지를 구성하는 것은 크게 두 단계로 나누어진다. 먼저 HR이 선거관리자가 공개한 각 후보자를 나타내는 표 $(X_i, Y_i)=(1, g_C^{L^{i-1}})$를 암호화하여 유권자에게 전달한다. 그러면 유권자는 HR에게서 받은 암호화된 표를 재암호화하여 최종 투표지를 구성하여 투표하게 된다. 선거단계에 대한 전체적인 구성은 [그림 4]와 같이 4단계로 이루어지고, 각 단계에 대한 자세한 설명은 다음과 같다.

단계 1. 선거가 시작되면 유권자는 임의의 HR을 선택하고 투표하겠다는 의사를 밝힌다.

단계 2. HR은 임의의 $a_i, i=1,\cdots,K$를 선택하고, 선거관리자가 공개한 후보자의 표 $(X_i, Y_i)=(1, g_C^{L^{i-1}})$를 $(X'_i, Y'_i)=(g_A^{a_i}X_i, y_A^{a_i}Y_i)$로 암호화하고 임의로 섞은 다음, 게시판 상에 있는 유권자의 암호화된 투표지 영역에 공개한다. HR은 모든 (X_i, Y_i)를 빠짐없이 암호화하였고, 중복된 것이 없다는 것을 [그림 1]에 기술된 K중 하나 암호화 증명을 K번 수행하여 증명한다. 이 증명은 [그림 4]에나타난 것과 같이 게시판 상에 있는 유권자의 암

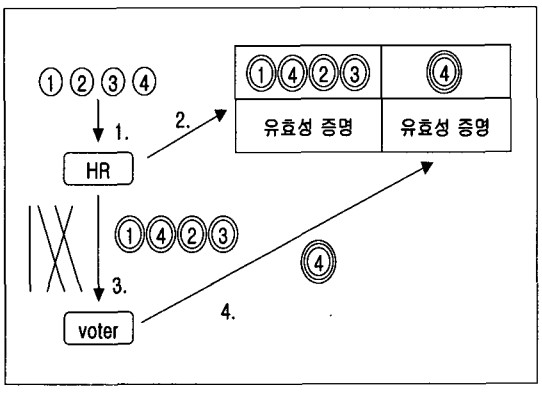
[표 2] 시스템 설정을 위한 G_q군의 생성자

생성자	용 도
g_A	threshold ElGamal 공개키 암호 프로토콜의 공개키 $y_A=g_A^{x_A}$ 를위한 G_q 의 생성자
g_C	후보자의 표를 인코딩하기 위한 G_q 의 생성자
g_V	유권자의 개인키가 x_V 일 때, 공개키 y_V 를 생성하기 위한 G_q 의 생성자

호화된 투표지의 유효성 증명 영역에 공개된다. 따라서 누구나 HR이 올바르게 (X_i, Y_i)를 암호화했는지 확인할 수 있다. [그림 1]에 기술된 프로토콜은 상호작용 증명이지만 실제 HR이 이 프로토콜을 수행할 때는 비상호작용 증명으로 변환하여 수행한다.

단계 3. HR은 [그림 3]에 기술된 지정된 확인자 증명을 통해서 유권자에게 암호화된 표들이 섞인 순서를 증명한다. 이 증명은 도청 불가능한 채널을 통해서 유권자에게 전달된다. 유권자는 이 증명을 통해서 어떤 (X'_i, Y'_i)이 어떤 (X_i, Y_i)를 암호화하고 있는지 알 수 있게 된다. 채널의 특성상 유권자를 제외한 누구도 채널을 통해 무엇을 수신하였는지 알 수 없고, 지정된 확인자 증명의 특성상 개인키 x_V를 알고 있는 유권자만 HR로부터 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. 이 증명도 각각의 (X_i, Y_i)에 대해서 한번씩 수행해야 하기 때문에 총 K을 수행해야 한다.

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 HR이 공개한 암호화된 투표지 (X'_i, Y'_i)중 하나를 선택하여 재암호화하였다는 것을 [그림 2]에 기술된 프로토콜을 이용하여 증명한다. 이 증명은 게시판 상에 있는 유권자의 최종 투표지의 유효성 증명 영역에 게시된다. 따라서 누구나 유권자가 올바르게 투표하였다는 것을 확인해 볼 수 있어 전체검증이 이루어진다.



[그림 4] 제안하는 전자선거 기법의 선거단계

4.4 집계단계

투표가 끝나면 지정된 선거관리자는 유효한 투표지를 모으고, 다음을 계산한다. 이 때, l은 투표한 총 유권자의 수이다.

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

모든 투표지가 게시판에 게시되기 때문에 누구나 (X_T, Y_T)를 계산하여 선거관리자가 계산한 값이 올바른지 확인해 볼 수 있다. 선거관리자는 해독 프로토콜을 실행하여 $W = (Y_T / X_T^{x_A})$를 계산한다. 암호해독에 사용되는 개인키 x_A는 N명의 선거관리자가 나누어 가지고 있고, N명의 선거관리자 중 t명 이상이 협력해야만 (X_T, Y_T)를 해독하여 M를 얻을 수 있다. 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.

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

이 때 $r_i, (i = 1, \ldots, K)$는 각 후보자 i가 얻은 득표수가 된다. 일반적으로 $r_i, (i = 1, \ldots, K)$를 계산하는 것은 이산대수 문제이고, 이것은 계산하기 어려운 문제이다. 그러나 Cramer[4] 등이 제안한 방법을 이용하면 $O(\sqrt{L}^{K-1})$의 복잡도를 가지고 각 $r_i (i = 1, \cdots K)$를 계산할 수 있다.

V 성능 분석

5.1 안전성

가정 1 (게시판의 안전성). 인가된 유권자는 게시판 상에 자신의 지정된 영역을 가지며, 이 영역은 [표 1]과 같이 4개의 영역으로 다시 나누어진다. 각 영역에 메시지를 게시하기 위해서는 안전한 인증 절차를 거쳐야 하며, 어떤 특정 영역에 메시지를 게시할 권한이 있는 참여자만이 그 영역에 메시지를 게시할 수 있다. 누구나 게시판에 게시된 메시지를 읽을 수 있지만 누구도 삭제할 수 없다.

가정 2 ((t,N)-treshold ElGamal 암호 프로토콜의 안전성). 선거관리자는 안전한 키 생성 프로토콜을 실행하여 선거에 사용하는 개인키 x_A를 다른 선거관리자와 공유하며, 선거관리자가 t명 이상 협력해야 암호문을 해독할 수 있다.

가정 3 (K중 하나 암호화 증명의 안전성). [그림 1]에 기술된 증명에서 (X, Y) 암호문이 K개의 암호문 $(X_1, Y_1), \ldots, (X_K, Y_K)$ 중에 없을 때, 거짓으로 증명하는 것은 계산적으로 어렵다. 마찬가지로 [그림 2]에 기술된 증명에서 (X_F, Y_F)가 K개의 $(X_1, Y_1), \ldots, (X_K, Y_K)$중 하나를 암호화한 것이 아닐 때, 거짓으로 증명하는 것은 계산적으로 어렵다. 정직하게 수행되었을 때, 확인자가 두 증명에서 특정 관계를 알 확률은 $1/K$이다.

가정 4 (지정된 확인자 증명의 안전성) [그림 3]에 기술된 증명에서 증명자가 지정된 확인자에게 섞인 순서를 거짓으로 증명하는 것은 계산적으로 어렵다.

정리 1 (비밀성). t명 이상의 선거관리자가 공모하지 않는 이상 누구도 유권자의 투표내용을 알 수 없다.

증명. ElGamal 암호 알고리즘의 안전성과 가정 2에 의해서 t명 이상의 선거관리자가 공모하지 않는 이상 누구도 유권자의 투표지를 해독할 수 없다. 또한 HR은 가정 4에 의해서 유권자에게 섞인 순서를 거짓으로 증명할 수 없고, 유권자가 어떤 표를 재암호화했는지 알 수 없다. 가정 3에 의해 HR도 유권자의 투표내용을 알 수 없다.

정리 2 (완전성(completeness)). 모든 유효한 투표지는 정확하게 집계된다.

증명. 가정 3에 의해서 HR은 [그림 1]에 기술된 증명을 거짓으로 통과할 수 없고, 암호화한 투표지의 유효성을 공개적으로 증명하기 때문에 누구나 유효성을 확인해 볼 수 있다. 마찬가지로 유권자도 [그림 2]에 기술된 증명을 거짓으로 통과할 수 없고, 재암호화한 투표지의 유효성을 공개적으로 증명하기 때문에 누구나 최종 투표지가 올바르게 구성되었는지 확인해 볼 수 있다. 최종 투표지는 모두 게시판에 게시되고, 가정 1에 의해 누구도 게시된 메시지를 지울 수 없기 때문에 선거관리자가 계산한 $(X_T, Y_T) = (\prod_{i=1}^{l} X_{F,i}, \prod_{i=1}^{l} Y_{F,i})$를 누구나 계산해서 올바른지 확인해 볼 수 있다. 선거관리자는 해독 프로토콜을 실행하여 계산한 $X_T^{x_A}$을 이용하여 $W = Y_T / X_T^{x_A}$가 올바른지 계산해 볼 수 있다. 따라서 모든 유효한 투표지는 올바르게 집계된다.

정리 3 (선거권). 인가된 유권자만이 선거에 참여할 수 있다.

증명. 가정 1에 의해서 선거에 참여하는 유권자는 게시판 상에 자신의 지정된 영역을 가지고 있고, 안전한 인증절차를 거쳐야만 이 영역에 투표지를 게시할 수 있다. 따라서 인가된 유권자만이 선거에 참여할 수 있다.

정리 4 (이중투표 방지(unreusability)). 모든 유권자는 한 표만 투표할 수 있다.

증명. 가정 1에 의해서 유권자는 게시판 상에 자신의 지정된 영역을 제외한 다른 영역에 투표지를 게시할 수 없으므로 유권자는 단지 한 표만 투표할 수 있다.

정리 5 (견실성(soundness)). 정직하지 않은 유권자가 선거를 방해할 수 없다.

증명. 정리 3과 4에 의해서 인가된 유권자만이 투표에 참여할 수 있고, 한 표만 투표할 수 있다. 또한 가정 3에 의해서 올바르지 않은 투표지를 구성한 유권자가 [그림 2]의 증명을 성공적으로 통과하는 것은 계산적으로 어렵다. 따라서 정직하지 않은 유권자가 선거를 방해할 수 없다.

정리 6 (공정성(fairness)). t명 이상의 선거관리자가 공모하지 않는 이상 투표 중에 부분적인 투표결과를 알 수 없다.

증명. 가정 2에 의해서 t명 이상의 선거관리자가 협동해야만 해독 프로토콜을 진행하여 투표결과를 얻을 수 있다.

정리 7 (표의 복사 가능성(vote duplication)). 유권자는 게시판 상에 게시되어 있는 다른 유권자의 표를 복사하여 투표할 수 없다.

증명. 유권자는 다른 유권자의 최종 투표지와 유효성 증명을 복사하여 자신의 게시판에 게시할 수 있다. 그러나 유권자는 가정 1에 의해서 HR이 유권자의 암호화된 투표지 영역과 암호화된 투표지의 유효성 증명 영역에 게시하는 메시지를 복사하여 게시할 수 없다.

정리 8 (매표방지(receipt-freeness)). 구매자나 유권자가 HR과 공모하지 않는 이상 매표행위를 할 수 없다.

증명. 유권자는 HR이 암호화에 사용한 비밀값 $\alpha_i, 1 \le i \le K$를 알지 못하기 때문에 구매자에게 $(X_F, Y_F) = (g_A^{\alpha_i + \beta}, Y_A^{\alpha_i + \beta} g_i)$를 직접적으로 증명할 수 없다. HR은 도청 불가능한 채널을 통해 지정된 확인자 증명으로 암호화된 투표지가 섞인 순서를 유권자에게 증명한다. 채널의 안전성이 물리적으로 보

장되기 때문에 구매자는 이러한 증명을 관찰할 수 없다. 따라서 구매자는 유권자에게 도청 불가능한 채널을 통해서 수신한 증명과 유권자가 재암호화한 투표지의 증명을 요구해야 한다. 그러나 개인키 x_V를 알고 있는 유권자는 3.4절과 같이 섞인 순서를 거짓으로 증명할 수 있고, 자신이 투표한 것과 전혀 다른 것을 투표한 것처럼 증명할 수 있다. 결국 구매자는 유권자를 신뢰할 수 없어 매표행위가 이루어지지 않는다.

정리 9 (전체검증(universal verifiability)). 제안하는 기법은 전체검증을 제공한다.

증명. HR은 선거관리자가 공개한 초기 투표지를 암호화하고, 유효성 증명을 유권자의 게시판 상에 있는 유권자의 암호화된 투표지의 유효성 증명 영역에 공개한다. 가정 3에 의해서 이 증명을 거짓으로 생성하는 것은 계산적으로 어렵다. 유권자는 HR이 암호화한 투표지를 재암호화한 후 유효성 증명을 게시판 상에 있는 유권자의 최종 투표지의 유효성 증명 영역에 공개한다. 이 증명 또한 가정 3에 의해서 거짓으로 생성하는 것은 계산적으로 어렵다. 가정 1에 의해 게시판 상에 공개된 모든 메시지는 누구나 읽을 수 있으므로, HR과 유권자가 공개한 증명은 누구나 확인해 볼 수 있다. 따라서 유효하지 않은 투표지가 집계에 반영될 수 없으며, 집계과정의 특성상 누구나 집계결과의 정확성을 알 수 있다.

5.2 다른 전자선거 기법과 비교

신뢰할 수 있는 제3자를 이용한 전자선거 기법을 이병천과 김광조가 제안하였지만, 그들의 기법이 매표방지를 제공하지 못한다는 것을 Hirt[6]가 증명하였다. 그러나 이병천과 김광조가 제안한 기법에서 HV가 유권자에게 임의의 쌍에 대한 유효성을 증명할 때 일반 영지식 증명 대신 지정된 확인자 증명을 사용하면 매표방지를 제공할 수 있다. 이 기법은 유권자가 초기 투표지를 구성하고 유효성을 증명하기 위해서 1번의 K중 하나 암호화 증명이 필요하고, HV가 전체검증을 위해 공개하는 정보의 유효성을 증명하기 위해서 또 1번의 K중 하나 암호화 증명이 필요하다. 또한 HV가 임의의 쌍에 대한 유효성을 유권자에게 증명할 때, 1번의 영지식 증명 또는 1번의 지정된 확인자 증명이 필요하다. Hirt는 기존의 방법보다 적은 계산량으로 매표방지를 제공하는 전자선거 기법을 제안하였지만 전체검증을 제공하지 않는다. 이 기법에서는 유권자가 구성한 초기 투표지의 유효성을 증명하기 위해서 1번의 K중 하나 암호화 증명이 필요하다. 그리고 HR이 암호화한 투표지의 유효성을 증명하기 위해서 1번의 지정된 확인자 증명이 필요하게 된다. 이병천과 김광조의 기법과 Hirt의 기법은 이 논문에서 제안하는 기법보다 계산량이 적지만 물리적 가정이 양방향 도청 불가능한 채널이라는 단점이 있다.

Hirt와 Sako의 기법은 일방향 도청 불가능한 채널과 믹스넷을 이용하여 매표방지와 전체검증을 제공한다. 한 명의 유권자가 투표하기 위해서는 최대 N개의 믹스서버가 유권자와 통신해야 한다. 각각의 믹스서버는 이전 믹스서버에게 받은 투표지를 올바르게 재암호화했다는 것을 증명하기 위해 K번의 K중 하나 암호화 증명을 실행한다. 또한, 섞인 순서를 유권자에게 알려주기 위해서 K번의 지정된 확인자 증명을 실행한다. 이 기법은 믹스서버가 계산해야 하는 증명이 많아 다수 후보자 선거에 적합하지 않다.

이 논문에서 제안하는 전자선거 기법은 신뢰할 수 있는 제3자와 일방향 도청 불가능한 채널을 가정하고 있다. HR이 초기 투표지를 암호화하고 섞은 다음, 유효성을 증명하기 위해서 K번의 K중 하나 암호화 증명을 실행한다. 이 증명은 전체검증을 제공하기 위해서 실행하는 것이기 때문에 유권자가 확인할 필요가 없다. 또한 HR은 섞인 순서를 유권자에게 증명하기 위해서 K번의 지정된 확인자 증명을 실행한다. HR이 K개의 비상호작용 증명을 도청 불가능한 채널을 통해 유권자에게 보내지만 유권자는 K개의 증명을 모두 확인할 필요는 없다. 단지 유권자는 투표하려는 후보자의 표가 올바르게 구성되었는지 확인하면 된다. 유권자는 HR이 공개한 암호화한 투표지 중 하나를 선택하여 재암호화하고 유효성을 증명하기 위해 1번의 K 하나 암호화 증명을 실행한다.

이 논문에서 제안하는 기법은 신뢰할 수 있는 제3자를 가정하는 다른 기법과 비교하였을 때는 계산량은 많지만 보다 약한 물리적 채널을 가정하고 있고, 동일한 일방향 도청 불가능한 채널을 가정하는 기법들 중에서는 계산량이 가장 적다. [표 3]은 이병천과 김광조의 기법, Hirt의 기법, Hirt와 Sako의 기법과 제안하는 기법을 비교한 표이다.

Ⅵ. 결 론

전자선거의 최종 목표는 현재 사용되고 있는 선거

[표 3] 전자선거 기법 비교

		Hirt와 Sako의 기법	이병천과 김광조의 기법	Hirt의 기법	제안하는 기법
기본 요구사항		○	○	○	○
매표방지		○	△ (지정된 확인자 증명을 사용하면 가능)	○	○
전체검증		○	○	×	○
유권자의 계산량	K중 하나 암호화 증명	없음	1번	1번	1번
	유효성 확인	NK번	1번	1번	1번
HR 또는 믹스서버의 계산량	K중 하나 암호화 증명	NK번	1번	없음	K번
	지정된 확인자 증명	NK번	1번	1번	K번
가정		일방향 도청 불가능한 채널	양방향 도청 불가능한 채널	양방향 도청 불가능한 채널	일방향 도청 불가능한 채널
		믹스넷	신뢰할 수 있는 제3자	신뢰할 수 있는 제3자	신뢰할 수 있는 제3자

방식을 대체하는 것이다. 따라서 비밀성, 선거권 등과 같은 선거가 기본적으로 만족해야 하는 요구사항들을 모두 만족해야 하며, 선거를 전자적으로 구성하였을 때 생길 수 있는 매표행위를 방지하고, 선거가 올바르게 진행되었다는 것을 누구나 확인할수 있도록 전체검증을 제공해야 한다. 그러나 지금까지 제안된 전자선거 기법들은 매표방지나 전체검증 중 하나만을 제공하거나 둘 다 제공하더라도 계산량이 많아 실용적이지 못했다. 이 논문에서는 선거시스템이 기본적으로 만족해야 하는 요구사항을 모두 충족시키면서, 전자선거를 구성할 때 문제가 되는 매표행위를 방지하고 전체검증까지 제공하는 전자선거 기법을 제안하였다. 이 기법에서는 신뢰할 수 있는 제3자인 HR과 최소한의 물리적 가정인 일방향 도청 불가능한 채널을 가정하고, 준동형 암호화 기법을 이용한다. 이 기법은 매표방지와 전체검증을 제공하는 기존 기법들과 비교하였을 때 가장 약한 가정을 사용하며, 같은 물리적 가정을 사용하는 기법 중에서는 계산량이 가장 적다.

인터넷을 이용한 전자선거가 실행된다면 일반가정에서 웹 TV나 컴퓨터를 이용하여 쉽고 편하게 선거에 참여할 수 있다. 그러나, 현재까지 제안된 전자선거 기법들은 매표방지를 제공하기 위해서 물리적으로 안전성이 보장되는 채널을 가정하고 있다. 이러한 경우 현재의 선거방식과 마찬가지로 일정 장소에 투표소를 설치하고 유권자는 투표소까지 가서 투표해야 하는 불편함이 있다. 따라서, 향후 인터넷과 같이 안전성이 보장되지 않은 공개채널을 이용하여도 매표행위를 방지할 수 있는 방법에 대한 연구가 필요하다.

참 고 문 헌

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

[2] 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.

[3] 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.

[4] R. Cramer, R. Gennaro, and B. Schoenmakers, "A Secure and Optimally Efficient Multi-Authority Election

Scheme," *Advances in Cryptology, Eurocrypt '97*, LNCS 1233, pp. 103~118, Springer, 1997.

[5] T. Okamoto, "Receipt-Free Electronic Voting Schemes for Large Scale Elections," *Proc. of Workshop on Security Protocols '97*, LNCS 1361, pp. 25~35, Springer, 1998.

[6] M. Hirt, "Receipt-free Voting with Randomizers," Presentated at *the Workshop on Trustworthy Elections*, Aug. 2001.
http://www.vote.caltech.edu/wote01/

[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. Chuam, "Untraceable Electronic Mail, Return Address, and Digital Pseudonyms," *Communications of the ACM*, pp. 84~88, 1981.

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

[10] R. Cramer, M. K. Franklin, B. Schoenmakers, and M. Yung, "Multi-Authority Secret-Ballot Elections with Linear Work," *Advances in Cryptology, Eurocrypt '96*, LNCS 1070, pp. 72~83, Springer, 1996.

[11] B. Lee and K. Kim, "Receipt-free Electronic Voting through Collaboration of Voter and Honest Verifier," *Proc. of the JWISC 2000*, pp. 101~108, 2000

[12] M. Jakobsson, "A Practical Mix," Advances in Cryptology, Eurocrypt '98, LNCS 1403, pp. 448~461, Springer, 1998.

[13] K. Sako, "Electronic Voting Schemes allowing Open Objection to the Tally," *IEICE Trans. on Fundamentals*, Vol. E77-A, No. 1, Jan. 1994.

[14] T. Okamoto, "An Electronic Voting Scheme," *Proc. of IFIP '96*, Advanced IT Tools, pp. 21~30, Chapman and Hall, 1996.

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

[16] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme based on Discret Logarithms," *Advances in Cryptology, Crypto '84*, LNCS 196, pp. 10~18, Springer, 1985.

[17] A. Fiat and A. Shamir, "How To Prove Yourself: Practical Solutions to Identification and Signature Problems," *Advances in Cryptology, Crypto '86, LNCS 263*, pp. 186~194, Springer, 1987.

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

〈著者紹介〉

오 희 국 (Heekuck Oh) 종신회원
1983년 : 한양대학교 전자공학과(학사)
1989년 : 아이오와주립대학 전자계산학과(석사)
1992년 : 아이오와주립대학 전자계산학과(박사)
1993년~1994년 : 한국전자통신연구원 선임연구원
1995년~현재 : 한양대학교 전자컴퓨터공학부 부교수
<관심분야> 암호기술 응용, 분산컴퓨팅
URL: http://infosec.hanyang.ac.kr/~hkoh

조 진 현 (Jinhyeon Cho) 학생회원
1998년 : 한양대학교 전자계산학과(학사)
2003년 : 한양대학교 컴퓨터공학과(석사)
<관심분야> 암호기술 응용, 전자선거
URL: http://infosec.hanyang.ac.kr/~jhjo

김 상 진 (Sangjin Kim) 정회원
1995년 : 한양대학교 전자계산학과(학사)
1997년 : 한양대학교 전자계산학과(석사)
2002년 : 한양대학교 컴퓨터공학과(박사)
2003년~현재 : 한국기술교육대학교 인터넷미디어공학부 전임강사
<관심분야> 암호기술 응용, 전자화폐, 전자선거