전체검증과 매표방지가 가능한 전자선거 기법

조진현*, 김상진*, 오희국*

*한양대학교, 컴퓨터공학과

Universally Verifiable and Receipt-free Electornic Voting Scheme

Jinhyeon Cho*, Sangjin Kim*, Heekuck Oh*

*Department of Computer Science and Engineering, Hanyang University

요 약

공정하고 투명한 선거를 이루기 위해서는 비밀성(privacy), 선거권(eligibiligy) 등과 더불어 전체검증(*universally verifiability*)과 매표방지(receipt-freeness) 속성이 반드시 제공되어야 한다. 그러나 전체검증은 누구나 투표내용을 확인할 수 있는 방법을 제공하는 것이고 매표방지는 투표내용과 투표자를 연결할 수 있는 방법을 차단하는 것으로 두가지 특성은 상호표리적 관계에 있어서 두가지 특성을 동시에 만족시키기가 어렵다. 이 논문에서는 신뢰할 수 있는 제3자인 정직한 랜덤마이저(Honest Randomizer, HR)와 최소한의 물리적 가정인 HR에서 유권자로 가는 도청 불가능한 채널(untappable channel)을 이용하여 전체검증과 매표방지를 제공하는 효율적인 전자선거 기법을 제안한다.

I. 서론

선거는 민주주의를 실현하는데 가장 중요한 도구 중 하나이다. 국민들의 잡다한 이해는 선거를 통하여 표명된다. 그러나 현행 선거방식은 그 낙후성으로 인해 자원의 낭비가 심하고 거대해진 현대사회에서 국민들의 의견을 정확하고 신속하게 반영하기에는 부족한 면이 많다. 또한 시간적, 공간적 제약으로 인하여 전 세계적으로 저조한 투표율이 문제가 되고 있다.

인터넷을 통한 전자선거를 실현하면 지역적인 제한없이 인터넷에 연결된 컴퓨터만 있다면 전 세계 어디에서나 투표할 수 있고 투표와 개표하는 시간이 짧아지며 집계에 드는 시간과 비용도 절감할 수 있다. 특히 현재 문제가 되고 있는 저조한 투표율 문제를 해결하는데 크게 기여할 것으로 기대되고 있다.

전자선거 기법은 1981년 Chaum[1]이 처음 소개한 이후로 많은 기법이 제안되었다[2-7]. 1992년 Fujioka 등[2]은 전자선거 기법이 가져야할 7가지의 요구사항을 다음과 같이 정의하였다.

- 선거권(eligibility): 인가된 유권자만이 투표할 수 있어야 한다.
- 단일성 또는 이중투표 방지(unreusability): 모든 유권자는 한 표만 투표할 수 있다.
- 완전성(completeness): 모든 유효한 투표는 정확하게 집계되어야 한다. 즉, 최종 집계 결과에 정당한 표가 빠지는 일이 없어야 한다.
- 건전성(soundness): 누구도 표를 추가, 변경, 삭제할 수 없어야 한다. 건전성은 이런 불법적인 행위를 정정할 수 없더라도 최소한 발견할 수 있어야 한다.
- 공정성(fairness): 투표에 영향을 미칠 수 있는 것이 없어야 한다.
- 비밀성(privacy): 누구도 유권자의 투표내용을 알 수 없어야 한다.
- 검증성(verifiability): 선거 결과를 속일 수 없도록 누구라도 투표 결과를 확인하고 검증할 수 있어야 한다.

Fujioka 등이 정의한 검증성은 투표한 유권자만이 자신의 투표지가 집계에 포함되었는지를 확인할 수 있는 개별검증(individual verifiability)임에 반해 Sako와 Kilian[3]은 투표에 참여한 유권자와 투표에 참여하지 않는 관찰자들도 투표와 집계가 올바르게 이루어졌는지를 확인할 수 있는 전체검증을 처음으로 소개하였다. 또한 Benaloh와 Tuinstra[4]는 매표방지에 대한 개념을 처음으로 소개하였다. 현재의 선거방식은 밀폐된 투표소를 사용하기 때문에 유권자가 어떤 후보자에게 투표하였는지를 확신할 수 없다. 따라서 표를 팔거나 살 수 없다. 그러나 전자선거에서는 유권자가 선거에 사용된 모든 데이터를 기록할 수 있기 때문에 특정 후보에게 투표하였다는 증거를 가질 수 있어 매표행위와 강요가 가능해 진다. 선거과정에 부정이 없다는 것을 모든 사람에게 확신시키기 위해서 전자선거 기법은 매표방지와 전체검증을 반드시 제공해야 하지만 이 두 특성은 상호표리적 관계에 있어서 두 가지 특성을 동시에 만족시

키기가 어렵다.

Benaloh와 Tuinstra[4]는 선거관리자와 유권자 사이의 비밀통신을 물리적으로 보장하는 선거부스(voting booth)와 준동형 암호화(homomorphic encryption)를 이용하는 두 가지 선거기법을 제안하였다. 첫 번째 선거기법은 단일 선거관리자를 이용하여 매표방지를 제공하였지만 유권자의 투표내용이 노출되는 단점이 있다. 두 번째 프로토콜은 다중 선거관리자를 두어서 유권자의 투표내용이 노출되는 것을 방지하였다. 그러나 유권자가 cut-and-choose 기법으로 투표지의 유효성을 증명할 때, 임의의 문자열을 선택하여 해쉬한 값을 사용하면 매표행위가 가능해진다[5].

Hirt와 Sako[5]는 믹스넷(mix-net)을 기반으로 하는 전자선거 기법을 제안하였다. 이 전자선거 기법은 매표방지와 전체검증을 제공한다. 그러나 그들의 전자선거 기법은 각각의 믹스서버(mix server)가 계산해야 하는 증명이 너무 많아 다수 후보자 선거에는 적합하지 않다.

이병천과 김광조[6]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 전달하기 때문에 유권자는 구매자에게 가짜 트랜스트립트를 제시할 수 있게 된다. 따라서 구매자는 유권자를 신뢰할 수 없고 매표행위가 가능해진다. Hirt는 HV가 임의의 쌍에 대한 유효성을 증명할 때 도전값을 어떤 값으로 고정하면 유권자는 가짜 트랜스크립트를 생성할 수 없게 되고 매표방지가 이루어지지 않는다는 것을 증명하였다[7]. 그러나 HV가 유권자에게 임의의 쌍에 대한 유효성을 증명할 때 지정된 확인자 증명(designated verifier proof)으로 증명하면 매표방지를 제공할 수 있게된다.

Hirt[7]는 이병천과 김광조의 전자선거 기법을 확장한 새로운 전자선거 기법을 제안하였다. Hirt의 전자선거 기법은 이병천과 김광조의 전자선거 기법에서 이용한 HV와 비슷한 역할을 하는 정직한 랜덤마이저(Honest Randomizer, HR)를 이용한다. 유권자는 투표지를 구성하여 도청 불가능한 채널을 통해서 HR에게 투표지를 전달한다. 그러면 HR은 이것을 재암호화하여 게시판에 투표하고 재암호화가 올바르게 이루어졌다는 증명을 도청 불가능한 채널을 통해서 지정된 확인자 증명으로 유권자에게 증명한다. Hirt의 전자선거 기법은 매표방지는 제공하지만 전체검증은 제공하지 않는다.

이 논문에서는 신뢰할 수 있는 제3자인 정직한 랜덤마이저(Honest Randomzier, HR)와 최소한의 물리적 가정인 일방향 도청 불가능한 채널을 이용하여 매표방지와 전체검증을 제공하는 전자선거 기법을 제안한다. 선거가 시작되면 HR은 투표지를 재암호화하여 섞은 다음 공개적으로 증명하고, 도청 불가능한 채널을 통해 지정된 확인자 증명으로 유권자에게 섞인 순서를 증명한다. 유권자는 투표하려는 후보자의 표를 선택하여 재암호화한 후 게시판에 게시하고, 투표지의 유효성을 공개적으로 증명한다. 제안하는 기법은 매표방지와 전체검증을 제공하는 기존 기법들과 비교하였을 때 가장 약한 가정을 사용하고, 같은 가정을 하는 기법들 중에서는 계산량이 가장 적다.

이 논문의 구성은 다음과 같다. 2장에서는 제안하는 새로운 전자선거 기법을 설명하고, 그것의 장단점을 분석한다. 끝으로 3장에서는 결론과 향후 연구방향에 대해 서술한다.

II. 새로운 전자선거 기법

1. 시스템 설정

이 전자선거 기법은 n명의 선거관리자($A_1,\ldots,A_n$), m명의 유권자($V_1,\ldots,V_m$), K명의 HR, L명의 후보자로 구성된다. 유권자가 투표할 때는 한 명의 HR과 상호작용을 한다. 여러 명의 HR을 두는 것은 결함을 허용하기 위함이다. 특히

생성자	용도
g_A	threshold ElGamal 공개키 암호 프로토콜의 공개키 $y_A=g_A^x$를 위한 G_q의 생성자
$G_1,\ldots,G_L$	각 후보자를 나타내기 위한 G_q군의 생성자
g_V	유권자의 개인키가 x_V일 때, 공개키 y_V를 생성하기 위한 G_q군의 생성자

표 1: 시스템 설정을 위한 G_q군의 생성자

DOS(Denial Of Service) 공격에 대한 방어 수단이다. 선거가 이루어지고 있는 동안 정직한 상태로 남아있어야 하는 최소한의 선거관리자는 t명이다.

선거관리자들은 시스템을 설정하기 위해 우선 $q|p-1$인 두 개의 매우 큰 소수 p, q를 선택하여 Z_p^*의 부분군이며 위수가 q인 G_q군을 설정하고, 표 1과 같이 G_q군의 생성자를 임의로 선택한다.

2. 투표 및 집계

선거가 시작되면 HR은 $\alpha_i \in_R Z_q$를 선택하고, (x_i, y_i)를 $(x'_i, y'_i)=(g_A^{\alpha_i}, y_A^{\alpha_i} G_i)$로 재암호화하여 임의로 순서를 섞은 다음 유권자의 게시판 영역에 공개한다. HR은 각각의 재암호화된 투표지에 대해서 그림 1의 증명을 통하여 선거관리자가 공개한 투표지를 올바르게 재암호화하였다는

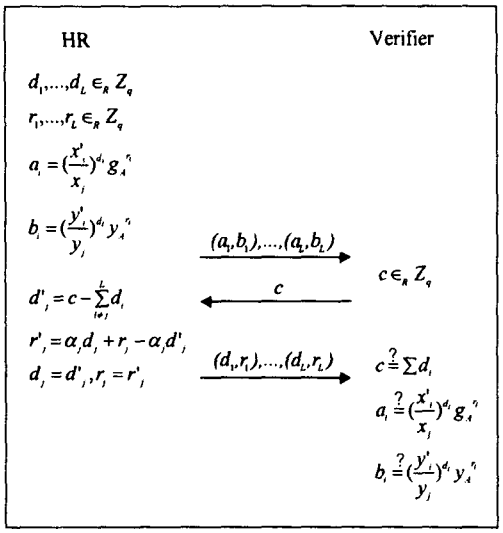

그림 1: 재암호화한 투표지의 유효성 증명

것을 재암호화에 사용된 비밀값 α_i와 섞은 순서를 밝히지 않으면서 공개적으로 증명한다. 이 증명을 통하여 누구나 HR이 올바르게 재암호화하였다는 것을 확인할 수 있게된다. HR은 도청 불가능한 채널을 통해 유권자에게 그림 2의 지정된 확인자 증명으로 재암호화된 표가 섞인 순서를 증명한다.

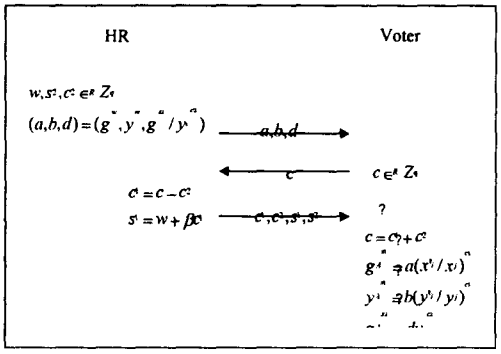

그림 2: 지정된 확인자 증명

유권자는 지정된 확인자 증명의 유효성을 확인한 다음 자신이 투표하고자 하는 k번째 후보자의 투표지를 $(x_f, y_f)=(x_k' g_A^{\beta}, y_k' y_A^{\beta})$로 재암호화하고 게시판에 투표한다. 유권자가 최종적으로 구성한 투표지의 유효성을 그림 3의 증명을 통해서 공개적으로 증명한다.

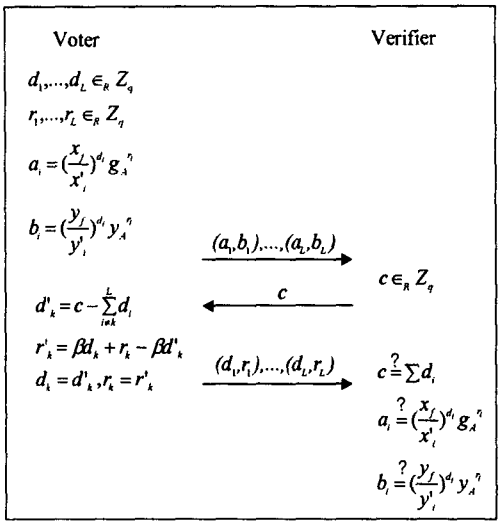

그림 3: 최종 투표지의 유효성 증명

선거가 끝나면 지정된 선거관리자는 유효한 투표지를 모으고, $(X, Y)=(\sum_{i=1}^{m} x_{f,i}, \sum_{i=1}^{m} y_{f,i})$를 계산한다. 모든 투표지가 게시판에 게시되기 때문에 누구나 (X, Y)를 계산하여 선거관리자가 계산한 값이 올바른지 확인해 볼 수 있다. 선거관리자들은 threshold ElGamal 암호프로토콜의 복호화 프로토콜을 실행하여 $W=Y/X^x$를 계산한다. $T_1,\ldots,T_K$가 선거결과일 때, $W=G_1^{T_1} G_2^{T_2} \cdots G_K^{T_K}$를 얻을 수 있고, 미리 계산한 W값과 비교하여 선거결과를 얻을 수 있다.

3. 안전성 분석

비밀성, 완전성 등과 같은 요구사항에 대한 분석은 생략하며 여기서는 매표방지와 전체검증에 대한 안전성만 분석한다.

매표방지: 유권자는 HR이 재암호화에 사용한 비밀값 α_i를 알지 못하기 때문에 (x_f, y_f)가 어떤 표를 암호화한 것인지를 구매자에게 직접적으로 증명할 수 없다. 또한 HR이 도청 불가능한 채널을 통해 지정된 확인자 증명으로 섞인 순서를 증명하기 때문에 유권자는 구매자에게 가짜 트랜스크립트를 제시할 수 있다. 따라서 구매자는 유권자를 신뢰할 수 없어 매표방지를 만족하게 된다.

전체검증: HR이 그림 1의 증명을 통해 재암호화한 투표지의 유효성을 공개적으로 증명하고 유권자는 그림 3의 증명을 통해서 재암호화한 투표

지의 유효성을 공개적으로 증명하기 때문에 누구나 올바르게 투표지가 투표되었다는 것을 확신할 수 있다. 또한 게시판에 게시된 표를 누구나 합산해서 결과를 확인해 볼 수 있다.

III. 결론

신뢰할 수 있는 제3자를 이용한 전자선거 기법을 이병천과 김광조가 제안하였지만, 그들의 기법이 매표방지를 제공하지 않는다는 것을 Hrit가 증명하였다. 이병천과 김광조가 제안한 전자선거 기법에서 HV가 유권자에게 임의의 쌍에 대한 유효성을 증명하는 프로토콜을 일반 영지식 증명이 아닌 지정된 확인자 증명으로 바꾸면 매표방지를 제공하게 된다. 그러나 그들의 전자선거 기법은 제안하는 기법보다 강한 물리적 가정인 양방향 도청 불가능한 채널을 사용한다. Hirt는 최소한의 계산량으로 매표방지를 제공하는 전자선거 기법을 제안하였지만 전체검증을 제공하지 않고 이병천과 김광조의 기법과 마찬가지로 양방향 도청 불가능한 채널을 사용하고 있다. 일방향 도청 불가능한 채널을 이용하여 매표방지와 전체검증을 제공하는 Hirt와 Sako의 전자선거 기법은 제안하는 기법보다 계산량이 월등히 많다.

이 논문에서는 Fujioka 등이 정의한 전자선거 기법이 갖추어야 할 요구사항을 모두 만족하면서 상반된 의미 때문에 동시에 구현하기 힘들다고 생각되었던 매표방지와 전체검증을 동시에 제공하는 전자선거 기법을 제안하였다. 이 기법은 매표방지와 전체검증을 제공하는 기존 기법들과 비교하였을 때 가장 약한 가정을 사용하며, 같은 가정을 하는 기법들 중에서는 계산량이 가장 적다.

참고문헌

[1] D. Chaum, "Untraceable Electronic Mail, Return Address, and Digital Pseudonyms," *Communications of the ACM*, pp. 84-88, ACM Press, 1981.

[2] A. Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Scheme for Large Scale Election," *Advances in Cryptology, AUSCRYPT '92*, LNCS 718, pp. 244-251, Springer, 1992.

[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] 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.

[5] 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.

[6] Byongcheon Lee and Kwangjo Kim, "Receipt-free Electronic Voting through Collaboration of Voter and Honest Verifier," *Proc. of the JWISC 2000*, pp. 101-108, 2000.

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