그룹화와 은닉서명을 이용하여 익명성을 강화한 전자 투표 방법 설계

이광희[0] , 이충세
충북대학교 전자계산학과
khlee@algo.chungbuk.ac.kr csrhee@cbucc.chungbuk.ac.kr

A Design of Anonymity Enhanced Electronic Voting Mechanism Using Grouping and Blind Signature

Kwang-Hee Lee[0] Chung-Sei Rhee
Dept. of Computer Science, Chungbuk National University

요 약

인터넷의 급속한 보급과 초고속정보통신망의 구축으로 인해 여러 분야에서 전자투표가 실현될 수 있으며, 그에 따라서 선거 비용이 절감되고 투표 장소의 제약이 개선될 것으로 예상된다. 그러나 전자투표의 실용화를 위해서는 공정성과 안전성 등의 문제가 해결되어야하며, 이를 위해 각종 암호 기법을 사용하여 프로토콜을 구성한다. 이 논문에서는 투표 과정에서 투표자를 그룹화하며, 은닉 서명 기법을 이용하는 전자투표 방법을 제안한다. 이 방법은 복잡한 익명 통신로를 사용하지 않으면서도 투표자의 익명성을 보장한다. 또한 투표자가 자신의 투표 결과를 제3자에게 증명할 수 없으므로 최근에 심각한 문제로 대두되고 있는 투표의 매매를 방지할 수 있다.

1. 서 론

인터넷이 급속하게 보급되고 초고속정보통신망이 구축됨에 따라 새로운 정보 서비스가 등장하고 생활에 많은 변화가 있을 것으로 보인다. 이러한 차원에서 고려될 수 있는 새로운 정보 서비스 분야중의 하나가 바로 전자투표이다. 전자 투표는 신임이나 정책 결정에 대한 의사 표현, 대통령, 국회의원, 지방 자치 단체장 등의 선출, 그리고 각종 선거나 여론 조사 등 다양한 분야에서 사용될 수 있다.

투표의 과정을 살펴보면, 유권자 등록단계, 유권자가 본인임을 확인하는 단계, 투표하는 단계, 수집 단계, 개표 단계, 계수 단계와 결과의 발표 단계로 구분할 수 있다. 투표자는 이러한 일련의 과정에서 유권자로 등록하고 자신의 결정을 투표지에 표기하여 제시한다.

전자선거는 이러한 일련의 과정이 공정하고 안전하게 유지되도록 암호기법을 사용하여 프로토콜을 구성한다. 구성된 전자선거 프로토콜은 선거자가 갖는 요구사항을 충족해야 하며 Fuijioka등의 연구에서는 전자선거 프로토콜이 충족해야할 요구사항을 분류하여 다음과 같이 정의하였다.[1]

- 완전성(Completeness) : 투표 결과의 정확한 집계가 이루어져야 한다.
- 건전성(Soundness) : 부정 투표자에 의한 선거 방해를 견뎌내야 한다.
- 비밀성(Privacy) : 투표 결과와 투표자의 관계는 비밀 유지가 되어야 한다.
- 단일성 또는 이중투표 불가성(Unreusability) : 투표자는 단 1회만 투표 가능해야 한다.
- 적임성 또는 선거권(Eligibility) : 투표 권한이 없는 자의 투표 행위는 방지되어야 한다.
- 공정성(Fairness) : 투표 도중 집계 결과가 나머지 투표에 영향을 주지 않아야 한다.
- 검증성(Verifiability) : 누구도 투표 결과를 위조할 수 없어야 한다.

이 외에도 유권자들 사이의 투표 매매를 막기 위한 매표방지성이 전자선거의 중요한 요구사항으로 대두되고 있으며, 이를 위해서 영지식증명기법(Zero Knowledge Interactive Protocol)등을 이용한 연구[5]가 이루어지고 있으나 효율성의 문제로 실제 선거에서는 사용이 제약을 받을 수 있다. 이에 대해 이 논문에서는 투표자의 그룹화 및 은닉 서명 기법을 이용하여 익명성을 강화하는 동시에 매표방지성을 제공하는 전자투표 방법을 제안하고자한다.

논문의 구성은 2장에서는 기존에 발표된 관련 연구에 대해서 특징과 문제점을 살펴보고, 3장에서는 설계한

프로토콜을 기술하고 성능을 분석한다. 마지막으로 4장에서 결론을 맺는다.

2. 관련 연구

전자투표의 실용화를 위해서 암호를 이용하는 안전하고 신뢰성 높은 연구가 은닉 서명을 이용한 전자투표 방식, 다자간 프로토콜을 이용한 전자투표 방식, 익명 통신로를 이용한 전자투표 방식 등을 중심으로 행하여져 오고있다.

· 은닉 서명(Blind Signature) 이용방식

메시지의 내용은 알려주지 않으면서 메시지에 대한상대방의 서명을 얻게 되는 것으로 전자현금이나전자투표 등 프라이버시를 제공해야 하는 곳에 활 용될 수 있는 추적이 불가능한 서명이다. Chaum에 의해 처음으로 제안되었으며, 전자현금인 경우 서명을 해주는 곳은 은행이고 전자투표인 경우는 선거 관리자가 될 수 있다. 서명을 받고자하는 메시지를 m, B의 공개키를 (e,n), 비밀키를 d라고 할 때, RSA 은닉 서명은 다음과 같다.

1. A는 난수 r을 생성하여 B에게 $C=mr^e mod\ n$을 계산하여 보낸다.
2. B는 수신한 C에 대한 서명문 $C^d=(mr^e)^d mod\ n$을 계산하여 A에게 제시한다.
3. A는 $S=C^d/r=m^d r^{ed}/r=m^d mod\ n$을 계산하여 B의 메시지 m에 대한 서명문으로 S를 얻게 된다.

· 다자간 프로토콜(Multy-Party Protocol) 이용방식

이 방식은 여분의 센터나 집계자를 사용하지 않고, 임의의 함수의 값을 얻기 위해 투표 참가자들 사이에 메세지를 주고받는 규칙이다. n명의 투표 참가자 $i(i=1,2,\cdots,n)$의 비밀입력 $x_i \in \{0,1\}$를 신임한다면 1,불신임한다면 0으로 한다. 이 때 $f(x_1,\cdots,x_n)=\sum x_i$로해서 다자간 프로토콜을 구성한다면, 각 투표자의 투표내용 x_i를 비밀로 한 채 몇 명이 신임했는가를계산할 수 있다.[2]

· 익명 통신로(Anonymous Channel) 이용방식

익명 통신로는 투표자가 지신의 정보를 임의의 통 신로에 보냈을 경우, 제 3자에 의해 자신과 자신이보낸 메시지와의 대응 관계가 노출되지 않아 프라 이버시가 보장되는 통신로이다. Chaum에 의해서 mix형 익명 통신로가 처음으로 제안되었으며, k개 의 mix센터를 사용하는 방식은 다음과 같다. n명의송신자를 $A_1,\ldots,A_n$라하고 수신자 B_i의 공개키를E_{Bi}, 센터 S_i의 공개키를 E_i라 한다.

1. 각 송신자 A_i는 난수 R을 발생하여 $E_1(R_1 \circ E_2(R_2 \cdots E_k(R_k \circ B_i \circ E_{Bi}(m_i))\cdots))$와 같은 암호문을 계산한 후 공개 게시판에 전송한다.
2. 처음 mix 센터는 수신한 암호문들을 복호화하 고, 그 내용 중에서 난수 R_1을 제거한 후, 남은 내용들을 알파벳순으로 나열하여 공개 게시판에 전송한다.
3. 마지막 mix 센터를 제외한 나머지 mix들 $S_2,\ldots,S_{k-1}$는 차례로 뒤의 단계를 반복한다.
4. 마지막으로, S_k는 $\{B_i \circ E_{Bi}(m_i)\}$를 알파벳순으로 나열하여 공개 게시판에 전송한다.[3]

다자간 프로토콜을 이용하는 방식은 많은 통신량과 계산량을 필요로 하며, 찬반 투표가 아닌 전자투표 시에는 실용성 면에서 많은 문제점이 있다. 그러나 안전성 측면에서는 우수하다. 익명 통신로를 이용한 전자투표는 효율성 면에서는 다자간 프로토콜 방식보다 우수하나 안전성 측면에서 다소 부족하다. 또한 번잡한 절차를 필요로 하기 때문에 대규모의 투표에는 부적당하다. Fuijioka나 Sensus 등의 연구에서도 투표의 비밀성을 위해 익명 통신로를 전제로 한 프로토콜을 제안하고 있지만 현실적으로 인터넷 상에서 익명성을 보장하기는 어렵다는 단점이 있다.[1][4]

또 한가지 고려해야 할 사항으로, 전자 투표의 매매에 관한 연구가 필요하다. 기존에 제안된 방식들은 투표 수행 과정에서 자신의 투표결과를 다시 확인할 수 있게 하고 있다. 이러한 검증 절차는 자신의 투표결과가 정확하게 집계되었는지를 확인하는 차원에서 필요하지만, 이 과정을 통해서 투표자는 불법적인 제3자에게 자신의 투표 결과를 쉽게 증명할 수 있게 된다. 결국 이러한 확인 절차로 인해 전자 투표의 매매가 발생할 위험이 있기 때문에 투표자의 비밀 투표성을 보장하면서 동시에 전자투표 매매를 예방할 수 있는 방안이 필요하다.

3. 제안한 방식

이번 장에서 제안하는 전자 투표 프로토콜은 선거 관리자, 투표자, 개표자, 공개 게시판으로 구성되며 사용된 기호는 다음과 같다.

- A : 선거 관리자, C : 개표자, B : 공개 게시판
- u : 투표자, V_u : u의 투표값

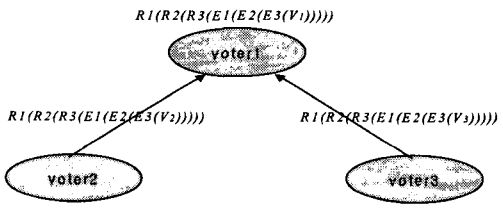
- E_u, D_u : 투표자의 첫 번째 암호화, 복호화 함수
- R_u, Q_u : 투표자의 두 번째 암호화, 복호화 함수
- $blind()$: 은닉 함수, $unblind()$: 비은닉 함수
- m : 그룹의 투표값, r : 난수
- $sign()$: 서명 함수
- A_e, A_d : 선거관리자의 공개키, 비밀키
- C_e, C_d : 개표자의 공개키, 비밀키

- 그룹 설정 및 투표용지 배부 단계

1. 투표자가 선거관리자에게 login하고 투표 의사를 밝히면, 투표자를 대기자 리스트에 추가한다.
2. 해당 투표에 미리 정의된 수의 투표자가 대기자 리스트에 들어오면 선거관리자는 그룹을 설정하고, 그 그룹의 정보와 그룹 내의 투표자들의 정보를 각각 RGL(Registered Group List)와 RVL(Registered Voter List)에 기록한다.
3. 그룹내의 각각의 투표자에게 투표용지를 배부한다. 이때 그룹 대표(대기자 리스트 상의 마지막 투표자)의 공개키에 대한 선거 관리자의 전자서명을 나 누어서 전달한다.

- 투표 단계

1. 각각의 투표자는 투표값을 자신의 공개키로 암호화한 후, 그룹 내의 모든 투표자의 공개키로 암호화 한다. random string을 추가하여 다시 한번 이중암호화하고 voter1에게 전달한다.



[그림 1] 그룹내의 투표 시작

2. voter1은 자신의 비밀키를 이용하여 복호화 한 다음 voter2에게 전달한다. voter2도 같은 방법으로 한 단계 더 복호화해서 voter3에게 전달한다. voter3는복호화를 수행하고 자신의 전자서명을 덧붙여서 다시 voter1에게 보낸다. 이 과정에서 voter1과 voter2에게도 전자 서명을 전달한다.

$$Q_1[R_1(R_2(R_3(E_1(E_2(E_3(V_u))))))]=R_2(R_3(E_1(E_2(E_3(V_u)))))$$
$$Q_2[R_2(R_3(E_1(E_2(E_3(V_u)))))]=R_3(E_1(E_2(E_3(V_u))))$$
$$Q_3[R_3(E_1(E_2(E_3(V_u))))]=E_1(E_2(E_3(V_u)))$$

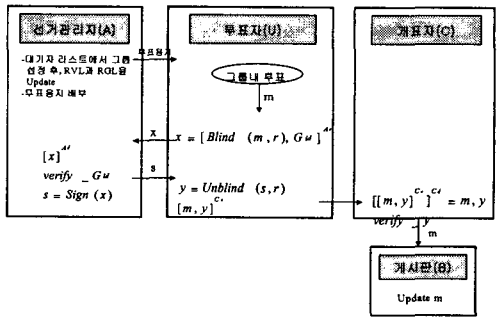
3. 위의 과정과 마찬가지로, 투표자는 자신의 또 다른 키로 복호화 한 다음 자신의 전자서명으로 sign해서 다음 투표자에게 전달한다. 동시에 그룹 내의다른 모든 투표자에게 서명을 전달한다.
4. voter3가 마지막으로 복호화해서 결과(V_1, V_2, V_3) 를 얻는다.

$$D_1[E_1(E_2(E_3(V_u)))]=E_2(E_3(V_u))$$
$$D_2[E_2(E_3(V_u))]=E_3(V_u)$$
$$D_3[E_3(V_u)]=V_u$$

5. 각각의 투표자들의 서명을 이용해 검증한다.

- 개표 단계

1. 그룹의 대표는 그룹설정 단계에서 받은 선거관리자의 서명을 이용해 권한을 확인 받고, 결과 용지를 배부 받아 작성한다.
2. 결과 값을 은닉하고 그룹 ID와 함께 선거 관리자의공개키로 암호화하여 선거 관리자에게 전달한다.
3. 선거관리자는 자신의 비밀키로 복호화하고 이전에투표 사실이 없는 지를 확인한 후, 은닉 서명을 수행하여 대표에게 전달한다.
4. 대표는 비은닉 함수를 수행하여 선거관리자의 서명을 얻는다. 선거관리자의 서명임이 검증되면 투표 값에 서명해서 개표자의 공개키로 암호화한 다음 개표자에게 전달한다.
5. 개표자는 자신의 비밀키로 복호화 하여 투표값을얻고선거관리자의 검증을 받은 것인지 확인한다.
6. 공개 게시판에 게시한다.
7. 투표자들은 자신이 속한 그룹의 투표값이 정확히집계되었는지 확인한다.
8. 투표 결과를 공표한다.



[그림 2] 프로토콜 구성도

이 방법에서 그룹내의 투표에는 Pfleeger가 제안한 방식[6]을 적용했다. 이 과정에서 투표값을 이중 암호화하여비밀로 한다. 개체들 사이에 메시지를 주고받

을 때는 공개키 암호 기법을 사용하므로 중간에 누군가가 투표값을 가로채더라도 수신자의 비밀키 없이는 결과를 얻어내거나 변조가 불가능하다. 또한 투표 용지 발급단계에서 투표자의 리스트를 작성하여 이중투표를 방지하였으며, 선거관리자의 서명이 있는 투표만 개표 시에 집계되므로 적임성을 만족한다.

검증성을 충족하기 위해서 투표 결과를 공개 게시판에 게시하여 투표자가 자신의 투표가 정확히 집계되었는지 확인할 수 있도록 하였다. 그러나 다른 방식과는 달리 그룹의 결과만을 확인하게 되므로 개개인의 투표자와 투표 결과를 추적하기는 거의 불가능하며, 투표자는 자신의 투표 결과를 제3자에게 증명할 수 없게된다. 따라서 익명성이 강화됨과 동시에 투표의 매매를 막는 효과가 있다.

4. 결론

이 논문에서는 투표 과정에서 투표자를 그룹화하며, 은닉 서명 기법을 이용하는 전자투표 방법을 제안하였다. 은닉 서명으로 투표자는 자신의 개인 정보를 누출하지 않고 선거관리자의 서명을 얻을 수 있으며, 그룹화를통해 마지막 검증 과정에서 개인의 투표 결과가 제3자에게 드러날 수 있는 위험을 방지했다. 그룹내의 투표에는 이중 암호화 방식을 적용하였으며, 공개키 시스템 등의 암호기법을 이용하여 전자투표의 기본적인 요구사항을 충족 시켰다. 이 방법은 복잡한 익명 통신로를 사용하지 않으므로 효율적으로 투표자의 익명성을 보장하며 더 나아가 매표 방지의 기능을 제공한다.

향후 과제로 투표자의 인증을 강화하고 프로토콜을 구성하는 각각의 개체들의 부정을 방지하기 위한 지속적인 연구가 필요하다.

[참 고 문 헌]

[1] A.Fuijioka, T.Okamito and K.Ohta, "A Practical secret voting scheme for large scale election", Advances in Cryptology -Auscrypt92, LNCS Vol.718, pp.244-251, Springer-Verlag, 1992

[2] S.Goldwasser, L.Levin, "Fair Computation of General Functions in Presence of Immoral Majority", Proc. of Crypto'90, LNCS 537, pp. 77-93, Springer-Verlag, 1992

[3] D.Chaum, "Untraceable Electronic Mail, Reurn Address, and Digital Pseudonyms", Communications of the ACM Vol.24, No.2, pp.84-88, 1981

[4] L.F.Cranor and R.K.Cytron, "Design and Implementation of a Practical Security-Conscious Electronic Polling System", WUCS-96-02, Dept. of CS, Washington University, St. Louls, 1996

[5] J.D.Cohen and M.J.Fischer, "A robust and verifiable cryptographically secure election scheme", In Proc. 26th IEEE Symp. on Foundations of Comp. Science, pp. 372-382, Portland, 1985

[6] Charles P.Pfleeger, Security in Computing, pp.151-154, Prentice Hall, 1997