문턱 은닉 서명을 이용한 전자투표 프로토콜

김 진 호, 김 광 조

국제정보보호기술연구소, 한국정보통신대학원대학교

An Electronic Voting Protocol using Threshold Blind Signature

Jinho Kim, Kwangjo Kim

International Research center for Information Security(IRIS)

Information and Communications Univ.(ICU), Korea

{kman,kkj}@icu.ac.kr

요 약

단일 선거관리자로부터 은닉 서명을 생성하는 프로토콜은 부정한 선거관리자에 의한 투표위조의 문제점이 나타날 수 있으므로 그에 대한 보완이 필요하다. 본 논문은 은닉 서명을 사용하는 전자투표 프로토콜에 문턱 은닉 서명을 적용시켜 다중 선거관리자로부터 유효한 은닉 서명을 생성하는 투표 프로토콜을 제안한다. 효과적인 문턱 은닉 서명을 설계하기 위해서 Schnorr 은닉 서명을 이용했으며, 이를 적용한 다중 선거관리자에서의 전자투표 프로토콜을 설계했다. 제안한 방식에서 은닉서명은 n명의 선거관리자중 t명 이상의 합의에 의해서만 생성 가능하므로, 부정한 단일 선거관리자에 의한 투표위조의 문제점을 해결할 수 있다.

I. 서론

전자투표 프로토콜은 암호학의 중요한 응용분야로 안전하고 실용적인 프로토콜을 구현하기 위해서 다양한 연구들이 진행되어 왔다. 전자투표 프로토콜은 크게 믹스서버(Mix-net)를 이용하는 방식[1,2,11,13], 준동형(Homomorphism) 암호를 이용하는 방식[3,4,9], 그리고 은닉서명을 이용하는 방식[5,10]으로 나눌 수 있다.

믹스 서버를 이용하는 방식은 모든 입력 자료에 대해서 서버의 처리가 정당하다는 것을 증명해야 하기 때문에 실용적이지 못하다. 준동형 암호를 이용하는 방식은 두 후보가운데 하나를 선택할 때는 효과적이나 여러 후보가운데 하나를 선택할 때는 투표자가 자신의 투표값이 정당하다는 것을 증명하기 위해서 여러 번의 영지식 증명을 수행해야 하므로 효과적이지 못하다. 은닉 서명을 사용하는 방식은 계산량적 측면에서 가장 효과적이므로 대용량 투표에 적합한 해결책을 제공할 수 있으나, 익명통신로와 정직한 단일 선거관리자를 가정한다는 문제점이 있다.

1992년 Fujioka, Ohta, Okamoto가 제안한 은닉 서명을 이용한 전자투표 방식 FOO92[5]는 위에서 제기한 문제점과 투표자가 개표 시 참여해야한다는 문제점(No walk-away)을 가지고 있으며, 이는 은닉 서명 방식 투표 프로토콜을 비현실적으로 만든 점이다. OMAFO99[10]에서는 문턱암호를 사용해서 투표 재 참여 문제를 해결했으며, 믹스서버를 사용해서 익명 통신로를 구축하였다. 그러나, 여전히 부정한 선거관리자에 의한 투표위조의 문제점을 가지고 있다.

본 논문에서는 문턱 은닉 서명을 OMAFO99에 적용시켜 다중 선거관리자를 통한 은닉 서명 생성이 가능하도록 했다. 투표자는 다중 선거관리자로부터 유효한 은닉 서명을 얻기 위해서 t명의 선거관리자와 통신을 수행해야 한다. 이는 기존의 단일 선거관리자가 은닉 서명을 생성할 수 있는 문제점을 개선한 것으로 부정한 단일 선거관리자에 의한 투표위조의 문제점을 해결할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 전자

투표의 요구사항과 OMAFO99에 대해 설명하고, 3장에서는 Schnorr 은닉 서명을 이용한 문턱 은닉 암호에 대해서 기술하겠다. 4장에서는 문턱 은닉 암호를 적용한 전자투표 방식에 대해서 기술하겠으며 5장에서 결론을 맺는다.

II. 관련연구

1. 전자투표 프로토콜 요구사항

FOO92는 전자투표 프로토콜이 만족시켜야 되는 7가지 요구사항을 아래와 같이 정의하였다[5].

① 완전성(Completeness) : 모든 유효 투표가 정확하게 집계되어야 한다.

② 건전성(Soundness) : 부정한 투표자에 의해 선거가 방해되는 일이 없어야 한다.

③ 기밀성(Privacy) : 모든 투표의 비밀은 보장되어야 한다.

④ 단일성 또는 이중투표불가성(Unreusability) : 정당한 투표자가 두 번 이상 투표할 수 없다.

⑤ 적임성 또는 선거권(Eligibility) : 투표 권한을 가진 자만이 투표할 수 있다.

⑥ 공정성(Fairness) : 투표에 영향을 미치는 것이 없어야 한다.

⑦ 검증성(Verifiability) : 선거 결과를 변경할 수 없도록 누구라도 투표 결과를 확인하여 검증해 볼 수 있어야 한다.

익명통신로와 정직한 선거관리자를 가정한다면 FOO92는 위의 요구사항을 모두 만족시키지만, 투표자가 개표 시 다시 참여해야한다는 문제점은 여전히 가지고 있다. OMAFO99에서는 이런 문제점을 문턱암호와 믹스서버를 적용시켜 해결했으나, 여전히 정직한 선거관리자를 가정하고 있기 때문에 부정한 선거관리자에 의한 투표위조의 문제점을 가지고 있다.

2. OMAFO99 프로토콜

1) 기호 정의

A : 선거관리자, V_i : 투표자 i, C : 개표자, M : 믹스서버, BB : 공개 게시판

E() / D() : 공개키/개인키를 이용한 암호화/복호화 함수. S() : 서명생성 함수.

B() : 은닉 함수 , UB() : 비은닉 함수

ID_i : V_i 의 식별정보

v_i : V_i 의 투표값

2) 등록단계(Registering stage)

Step 1 : V_i는 투표값 v_i를 선택한 후 C의 공개키를 이용해서 암호화하여 x_i=E (v_i) 을 얻는다. x_i를 난수 r_i를 이용해서 은닉해서 e_i=B (x_i, r_i)를 얻는다. e_i에 대한 서명을 생성해서 s_i=S (e_i)를 얻는다. 마지막으로 〈 ID_i, e_i, s_i〉를 선거관리자 A에 전송한다.

Step 2 : A 는 V_i가 투표권한, 이중투표, 서명의 정당성이 있는지를 검사해서 투표자격이 없다면 A는 인증을 거부한다. 모든 과정을 통과하면 A는 e_i에 서명 d_i=S (e_i)를 생성해서 V_i에게 전송한다.

Step 3 : V_i는 x_i에 대한 서명 y_i=UB (d_i, r_i)를 추출한다. y_i가 x_i에 대한 A의 서명인지를 검증한 후 검증이 실패하면, 〈 x_i, y_i〉가 유효하지 않다고 주장한다.

3) 투표단계(Voting stage)

Step1 : V_i는 〈 x_i, y_i〉를 M의 공개키로 암호화해서 c_i=E(〈 x_i, y_i〉)를 얻는다. c_i에 대한 서명 s_i=S (c_i)를 생성한 후 BB에 〈 c_i, s_i〉전송한다. BB는 서명확인 후 게시한다.

4) 개표단계(Counting stage)

Step1 : M은 BB에 있는 c_i를 복호화한 후 무작위 순서로〈 x_i, y_i〉를 출력한다.

Step2 : C는 x_i에 대해서 y_i가 정당한 A의 서명인지 검증한다. 검증에 실패하면 〈 x_i, y_i〉를 공개한다. 개표자중 정직한 t명 이상이 〈 x_i, y_i〉와 같은 값이 이미 존재한다고 주장하면 M은 영지식 증명기법을 이용해서 〈 x_i, y_i〉가 c_i를 복호화한 값이라는 것을 증명한다. 각각의 개표자는 증명의 정당성을 검증한다. 검증이 실패하면 M의 부정 행위임으로 해당 M을 믹싱 과정에서

제외시킨다. 검증이 성공하면 M은 정직하나, 투표자가 유효하지 않은 정보를 보낸 것이 되므로 투표값을 개표에서 제외시킨다.

Step3 : 모든 개표자는 문턱암호를 이용해서 x_i를 복호한 후 v_i=D (x_i)를 BB에 공개한다. 검증자는 투표수와 투표자 수가 일치하고, 개표자가 정확히 개표했는지 검사한다. 검증이 실패하면 무효를 주장한다.

III. 문턱 은닉 서명

문턱 은닉 서명이란 n명의 서명자가 있을 때 사용자 B는 t명으로부터 은닉 서명을 얻어낼 수 있으며, t명보다 작은 수의 서명자로부터는 은닉 서명 생성이 불가능한 서명 방식이다. 이 방식은 Juang과 Lei에 의해서 처음 제안[7] 됐으며, 안전하고 효과적인 방식이 [8]에서 제안되었다. 본 논문에서는 이를 좀 더 단순화한 Schnorr 은닉 서명 [12]에 기반한 문턱 은닉 서명을 사용한다.

1. 키 생성

큰 소수 p와 p-1을 나누는 소수 q가 있을 때 G를 위수가 q인 Z_p^* 의 부분 군이라고 하고, g를 G의 생성자라고 하자. 즉 G=<g> 가 된다. 이때 $x_i \in Z_p^*$ 와 $y_i = g^{x_i} \bmod p$를 서명자 P_i의 개인키와 공개키가 된다. 문턱암호에 사용될 분산키는 DKG[6]에 의해서 얻어지며 이때 사용되는 비밀 분산(Secret share)을 s_i 라 한다.

2. 문턱 은닉 서명

사용자 B는 문서 m에 대한 은닉 서명을 얻기 위해서 n명의 서명자 $P_1, \ldots, P_n$ 중 t명을 선택해서 은닉 서명에 필요한 값을 요청한다.

- 요청을 받은 P_i는 난수 $k_i \in Z_q$를 생성한 후 $a_i = g^{k_i} \bmod p$를 계산해서 B에게 보낸다.

- B는 모든 a_i를 받은 후, $a = \prod_{i=1}^{t} a_i \bmod p$를 계산하고, 난수 $\beta, \gamma \in Z_q$를 생성한 후 $\alpha = a g^{\beta} h^{\gamma} \bmod p$를 계산한다. $\varepsilon = H(m, \alpha)$와 $e = \varepsilon - \gamma \bmod q$를 계산해서 P_i에게 e를 전송한다.

- P_i는 e를 받은 후, 부분 은닉 서명 $R_i = k_i - e s_i \omega_i \bmod q$를 B에게 보낸다.

- B는 R_i를 받은 후 $a_i = g^{R_i} y_i^{e\omega_i} \bmod p$인지 검증한다. 검증이 통과하면 $\rho = \beta + \sum_{i=1}^{t} R_i \bmod q$를 계산해서 문턱 은닉 서명 (ε, ρ)를 생성한다.

3. 서명 검증

서명 검증자는 $\alpha = g^{\rho} y^{\varepsilon} \bmod p$를 계산한 후 ε와 $H(m, \alpha)$가 같은지 비교한다. 두 값이 같으면 서명은 유효하다.

IV. 문턱 은닉 암호를 적용한 전자 투표 프로토콜

제안한 방식은 n명의 다중 선거관리자를 기본 모델로 하며 문턱 은닉 서명방식을 OMAFO99에 적용시켜 투표자는 t명의 선거관리자로부터 은닉 서명을 받는다. 프로토콜을 단순화하기 위해서 투표자는 선거관리자 $A_1, \ldots, A_t$로부터 서명을 받는다고 가정한다. 문턱 은닉 서명은 앞장에서 설명한 방식을 따른다. 투표단계와 개표단계는 OMAFO99와 같으므로 생략하겠다.

- 등록단계(Registering stage)

Step 1 : V_i는 투표값 v_i를 선택한 후 C의 공개키를 이용해서 암호화하여 x_i=E (v_i)을 얻는다. V_i는 t명의 선거관리자에게 은닉 서명 생성에 필요한 값 a_i를 요청한다.

Step2 : V_i는 a_i를 받아서 $a = \prod_{i=1}^{t} a_i \bmod p$를 계산하고, 난수 $\beta, \gamma \in Z_q$를 생성해서 x_i를 은닉한 e_i=B (x_i, a, β, γ)를 구한다. e_i에 대한 서명 s_i=S (e_i)을 생성한 후 〈 ID_i, e_i, s_i〉를 A_j에게 전송한다.

Step3 : A_j는 V_i가 투표권한, 이중투표, 서명의 정당성이 있는지를 검사해서 투표자격이 없다면 인증을 거부한다. 위의 모든 과정을 통과하면 A_j는 e_i에 은닉 서명 R_j = S (e_i)를 생성해서 V_i에게 전송한다.

Step 4 : 수신한 R_j를 검증한 후, V_i는 x_i에 대한 서명 y_i= UB ($R_1, \ldots, R_t, \beta$)을

추출한다. y_i가 x_i에 대한 A의 서명인지를 검증한 후 검증이 실패하면, $\langle x_i, y_i \rangle$가 유효하지 않다고 주장한다.

등록단계에서 투표자는 n명의 선거관리자중 t명에게 은닉 서명을 요청하며 요청받은 t명의 선거관리자는 투표자의 투표권한여부를 확인한 후 자신의 개인키를 이용해서 부분 은닉 서명을 생성한다. 이때 1명의 선거관리자라도 서명을 거부한다면 투표자는 R_j를 검증해서 어떤 선거관리자가 서명을 거부했는지 알 수 있으므로, 투표 검증자에게 증재를 요청할 수 있다.

제안한 방식은 문턱 은닉 서명을 OMAFO99에 적용시켜서 단일 선거관리자가 정직하다는 가정을 n명의 선거관리자중 t명 이상의 선거관리자가 정직하다는 가정으로 개선시켰으므로, OMAFO99가 만족시키는 7가지 요구사항을 모두 만족시킨다.

V. 결론 및 향후 과제

본 논문에서는 은닉 서명을 사용하는 전자투표 프로토콜에 문턱 은닉 서명을 적용시켜 다중 선거관리자로부터 유효한 은닉 서명을 생성하는 투표 프로토콜을 제안하였다. 제안한 문턱 은닉 서명은 Schnorr 은닉 서명에 기초해서 설계했으며, 이를 전자투표 프로토콜에 적용시켜 다중 선거관리자로부터 은닉 서명을 생성하는 것이 가능하도록 설계했다. 제안한 방식을 사용하면 투표자는 n명의 선거관리자중 t명의 선거관리자로부터 은닉 서명을 얻어야 한다는 복잡함이 있으나, 부정한 단일 선거관리자가 투표를 위조할 수 있는 문제점을 해결할 수 있다.

참고문헌

[1] M. Abe, "Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers", Advances in Cryptology-Eurocrypt 98, LNCS Vol. 1403, pp.437-447, Springer-Verlag, 1998

[2] D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Comm. ACM 24, pp.84-88, 1981.

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

[4] R. Cramer, R. Gennaro, B. Schoenmakers, "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology-Eurocrypt'97, LNCS Vol. 1233, pp.103-118, Springer-Verlag, 1997

[5] A. Fujioka, T. Okamoto, K. Ohta, "A Practical Secret Voting Scheme for Large Scale Election", Advances in Cryptology-Auscrypt'92, LNCS Vol. 718, pp. 248-259, Springer-Verlag, 1993

[6] R. Gennaro, S. Jarecki,H. Krawczyk, T. Rabin, "Secure Distributed Key Generation for Discrete-Log Based Cryptosystems", Advances in Cryptology-Eurocrypt'99, LNCS Vol.1592, pp.295-310, Springer-Verlag, 1999.

[7] W. S. Juang and C. L. Lei, "Blind Threshold Signatures Based on Discrete Logarithm", Proceedings of the 2nd Asian Computing Science Conference, Lecture Notes in Computer Science 1179, Springer-Verlag, pp. 172-181, 1996.

[8] J. Kim and K. Kim, "An Efficient and Provably Secure Threshold Blind Signature", submitted to ICISC'01

[9] B. Lee and K. Kim, "Receipt-free Electronic Voting through Collaboration of Voter and Honest Verifier", Proceeding of JW-ISC2000, pp.101-108, Jan. 25-26, 2000

[10] M. Ohkubo, F. Miura, M. Abe, A. Fujioka, T. Okamoto, "An Improvement on a Practical Secret Voting Scheme", Information Security'99, LNCS Vol.1729, pp.225-234, Springer-Verlag, 1999.

[11] C. Park, K. Itoh, K. Kurosawa, "Efficient Anonymous Channel and All/Nothing Election Scheme", Advances in Cryptology-Eurocrypt'93, LNCS Vol.765, pp.248-259, Springer-Verlag, 1994.

[12] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures", Journal of Cryptology, LNCS Vol. 13, pp. 361-396, Springer-Verlag, 2000

[13] K. Sako and J. Killian, "Receipt-free Mix Type Voting Scheme", Advances in Cryptology-Eurocrypt'95, LNCS Vol.921, pp.393-403, Springer-Verlag, 1995