내용 은닉서명과 VIOT를 적용한 전자선거 프로토콜

김 상 춘[†] · 이 용 주[††] · 이 상 호[†††]

요 약

이 논문에서는 전자선거 프로토콜 중에서 무기명 비밀투표 방식에서 요구되는 안전요구사항을 만족시킬 수 있도록 RSA 공개키 암호 시스템과 내용 은닉서명 기법을 이용한 VIOT 프로토콜을 이용하여 투표자의 프라이버시를 제공하고, 투표자나 선거위원의 부정행위를 탐지할 수 있는 송수신 부인봉쇄 기능을 갖는 새로운 전자선거 프로토콜을 제안하였다.

Election Protocol using Verifiable Interactive Oblivious Transfer and Blind Signature

Sang-Choon Kim[†] · Yong-Ju Yi[††] · Sang-Ho Lee[†††]

ABSTRACT

In this paper, we propose an electronic election protocol based on VIOT protocol which utilizes public key cryptographic system and blind signature method to meet the security requirement in election systems. Our proposed electronic election protocol provide voter's privacy and non-repudiation functionality which detect any misdemeanors of voters or relevant personnels.

1. 서 론

대통령선거, 헌법개정 찬반투표, 신임투표 등 우리가 일상생활에서 겪는 선거에는 많은 종류가 있다. 그러나 이들 투표에 있어서 집계 등 일부에는 컴퓨터가 도입되고 있지만 선거의 투표나 개표 작업의 많은 부분이 아직도 사람의 손에 의존하고 있어 시간이나 경비가 엄청나게 소요되고 있다. 따라서 이러한 투표작업을 집이나 사무실에서 컴퓨터를 통해 수행하게 된다면 유권자의 수고를 크게 경감시키게 될 뿐만 아니라, 이러한 방법으로 투표된 내용을 컴퓨터를 이용하여 집계하게 되면 투표에 소요되는 시간이나 경비를 줄일 수 있을 것이다. 향후 정보통신의 발달로 인하여 유권자가 직접 투표소에 나가서 투표하는 번거러움을 거치지 않고, 통신망을 통하여 집안이나 사무실에 앉아서도 종전과 다름없는 투표를 실현하는 방법이 기대된다.

그러나 통신망에 의해 선거를 수행할 경우, 투표자의 투표 내용이 통신 시스템을 통과하므로, 개인의 프라이버시가 침해될 우려가 있으며, 컴퓨터의 복사기능 등에 의해 개표 및 집계과정에서 부정이 개입될 가능성이 있다. 따라서 통신망을 통한 선거에 있어서 투표에 따른 적절한 안전성 문제가 해결되어야 한다.

이러한 문제를 해결하는 프로토콜이 전자선거 프로토콜(Electronic Election Protocol)[1-6]이다.

† 정 회 원 : 한국전자통신연구원 정보보호기술연구본부 선임기술원
†† 준 회 원 : 충북대학교 대학원 전자계산학과
††† 종신회원 : 충북대학교 컴퓨터과학과 교수
논문접수 : 1999년 4월 19일, 심사완료 : 1999년 12월 27일

2. 기본 개념 소개

2.1 내용 은닉 서명(Blind Signature)

내용 은닉서명은 D. Chaum이 CRYPTO'82 에서 제안한 것으로, 메시지 내용은 상대방에게 알려주지 않으면서도 메시지에 대한 서명자의 서명을 얻게 되는 것으로 전자 화폐(electronic cash)나 전자 선거(electronic vote)등에서 사용자의 프라이버시(privacy)를 제공하고 사용자가 익명성을 가질 수 있게 하는 추적 불가능 서명 기법(untraceability signature technique)이다[7].

RSA암호를 이용한 내용 은닉 서명은 다음과 같다.

서명자(B)의 공개키(public key)를 e, 비밀키(secret key)를 d라고 하자.

(RSA 파라메타(n)=p · q는 공개 정보이고, m은 메시지이다.)

[단계 1] 송신자(A)는 난수(random number) r을 생성하여 서명자(B)에게 $C=r^e\ m \pmod n$을 계산하여 보낸다.

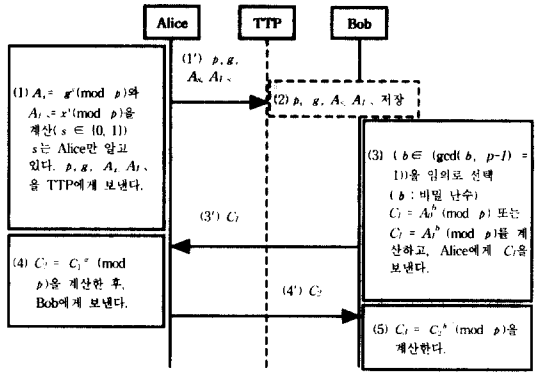
[단계 2] 서명자(B)는 송신자(A)로부터 수신한 C에 대하여 다음과 같이 계산하여, 송신자(A)에게 전송한다. $C^d = (r^e\ m)^d \pmod n$ 난수 r은 송신자만 알고 있으므로 서명자는 메시지의 내용을 알지 못한다.

[단계 3] 송신자(A)는 서명문(S) = C^d / r =$(r^{e\ d}\ m^d)$ /r = $m^d \pmod n$을 계산하여 서명자(B)의 메시지(m)에 대한 서명문(S)을 획득하게 된다.

2.2 검증가능한 대화형 불확정 전송 프로토콜 (Verifiable Interactive Oblivious Transfer Protocol)

검증가능한 대화형 불확정 전송 프로토콜은 L. Harn 등이 ASIACRYPTO'91에서 제안한 것으로, RSA 공개키 암호 시스템과 이산 대수 문제의 어려움에 근거한 방식이다. 이 프로토콜에서 수신자는 1/2의 확률로 송신자의 비밀을 얻거나, 얻지 못한다. 송신자와 수신자는 상대방이 비밀정보의 수신여부를 알지 못한다[10].

- p, p' : 소수($p = 4 \cdot p' + 1$, $p \equiv 1 \pmod 4$) • p : 공개 정보
- g : GF(p)의 원시근(공개 정보)
- x : Alice의 비밀키
  ($x \rightarrow \gcd(x,\ p-1) = 1$, $x \in QNR_p$ (p의 평방 비잉여))
- s : Alice이 선택한 값 • b : Bob가 선택한 값
- S_0, S_1 : Alice가 Bob에게 보내고자 하는 비밀 정보



(그림 1) 검증 가능한 대화형 불확정 전송 프로토콜

<프로토콜 분석>

[단계 5]에서 $C_3 = g$라면 Bob은 Alice의 비밀 정보에 대해서는 아무 것도 알지 못한다. $C_3 \neq g$이면 Bob이 $A_s = g^{C_3} \pmod p$($s \in \{0, 1\}$) 인지를 확인하여 Alice의 비밀 정보($x = C_3$)를 알게 된다. 그것이 아니라면 Bob은 Alice의 부정행위를 알 수 있다. 이 프로토콜의 그 특성은 다음과 같다.

(1) 공평성(fairness) : 양쪽 당사자가 프로토콜을 충실히 따른다면 불확정 전송 프로토콜의 기본 조건들이 공평하게 충족된다.
(2) 검증 가능성(verifiability) : 서로의 부정행위는 거의 1에 가까운 확률로 탐지 될 수 있다.
(3) 안전성(security) : 양쪽 당사자가 프로토콜을 충실히 따르지 않는다면 서로의 비밀 정보를 1/2 이상의 확률로 취할 수 없다.

2.3 전자 선거 프로토콜(Election Protocol)

전자선거 프로토콜이란, 통신망을 통해 투표 및 개표 등을 가능하게 하는 통신 프로토콜로써, 이들 선거 행위시 각 투표 종류마다 요구되는 안전성 문제를 암호 기술을 채용, 효율적으로 해결하는 알고리즘이다.

2.4 안전 요구사항(Security Requirement)

전자선거 프로토콜에서 요구되는 안전성 문제는 선거의 종류에 따라 다소 차이는 있겠지만 오늘날 가장 대표적인 무기명 비밀 투표 방식에 대한 안전 요구사항의 조건은 크게 다음과 같이 5가지 조건으로 요약할 수 있다.

(조건 1) 유권자의 투표 내용에 대한 비밀을 보장해야 한다.

(조건 2) 각 유권자는 단 1회의 기회만이 보장되어야 한다.

(조건 3) 투표권이 있는 자만 투표 행위를 할 수 있어야 한다.

(조건 4) 투표 내용이나 집계 결과에 대해서 수정이나 위조가 방지되어야 한다.

(조건 5) 다른 사람의 투표 결과에 따라 투표의 내용이 변경되지 않도록 공평성이 보장되어야 한다.

2.5 프로토콜의 구성(The composition of protocol)

1명의 선거위원(EC), N명의 유권자와 선거관리위원회(Trusted Third Party : TTP)로 구성된다. 유권자의 명단은 디지털 서명을 복호화 하기 위해 공개된 명부에 기록하며, 이 명부는 모든 관계자의 승인을 받게 하며, 선거관리위원회(Trusted Third Party : TTP)에서 관리한다.

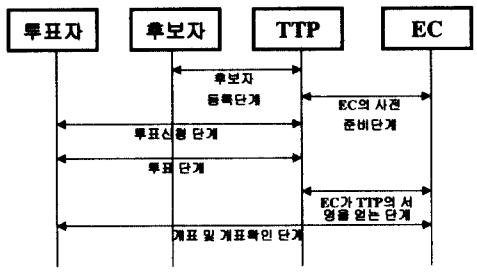
D. Chaum이 제안한 내용은닉 서명의 송신자 불추적성을 적용하여 송신자 익명 네트워크를 고려한다. 메시지의 수신자 또는 도청자는 그 메시지가 누구로부터 송신된 것인지 알 수 없다. 이 네트워크에서는 메시지의 전송을 방해하거나 전송 중에 메시지를 변경할 수 없다고 가정한다.

3. 내용은닉과 VIOT를 적용한 전자선거 프로토콜

이 논문에서 제안한 내용은닉과 VIOT를 적용한 전자선거 프로토콜은 RSA 공개키 암호시스템과 내용 은닉 서명 프로토콜[7]과 공평한 비밀정보 교환을 위한 불확정전송 프로토콜[8-20] 중 검증가능한 불확정 전송 프로토콜을 적용하였다.

이는 은닉서명과 불확정 전송 프로토콜의 안전성과 검증 가능성을 도입하여 발생 가능한 부정을 사전에 제거하여 보다 강력한 보안성(security)과 개인의 프라이버시(privacy)를 제공할 수 있도록 설계하였다.

제안한 전자선거 프로토콜은 보안성에 초점을 맞추었으므로 다소 계산량이 많으나 보다 강력한 안전성이 요구되는 전자선거 시스템에 적합하며, <후보자 등록 단계>, <EC의 사전 준비단계>, <신원확인 및 투표신청 단계>, <투표단계>, <EC가 TTP의 서명을 얻는 단계>, <개표 및 개표 확인 단계>로 구성된다.



(그림 2) 내용은닉과 VIOT를 적용한 전자선거 프로토콜 구성

<전제조건>

[조건 1] 자격을 갖춘 유권자 중에서 어떤 사람도 후보자에 등록할 수 있어야 한다.

[조건 2] TTP는 신청자에게 서명한 내용을 보관하고 있어야 한다.

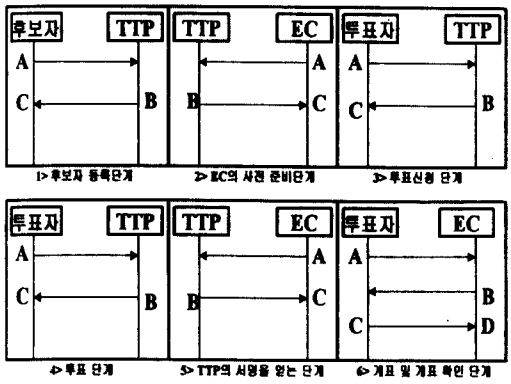
[조건 3] TTP로부터 은닉서명을 받은 자만이 검증 가능한 대화형 불확정 전송 프로토콜을 이용한 전자선거에 참여할 수 있도록 한다.

[조건 4] RSA 공개키 암호 시스템을 이용하는 TTP는 $n_T = p \cdot q$, $\gcd(T_E, \Phi(n_T)) = 1$, $T_E \cdot T_D \equiv 1 \pmod{\Phi(n_T)}$ 라고 한다.

<파라메타 정의>

- TTP : 두 당사자 모두가 신뢰하는 선거 관리 위원회
- T_{D_A} : TTP가 유권자(Alice)에게 서명하는 서명 함수(signature function)
- T_{E_A} : TTP가 유권자(Alice)에게 서명하는 서명 함수의 역함수(공개)
- T_{EC_D} : TTP가 선거위원(EC)에게 서명하는 서명 함수
- T_{EC_E} : TTP가 선거위원(EC)에게 서명하는 서명 함수의 역함수(공개)
- $T_{ID_{N_D}}$: TTP가 후보자(ID_N)에게 서명하는 서명 함수
- $T_{ID_{N_E}}$: TTP가 후보자(ID_N)에게 서명하는 서명 함수의 역함수(공개)
- ID_A : TTP가 유권자 명단에 포함된 Alice의 고유한 식별자
- ID_{EC} : TTP가 선거위원 명단에 포함된 EC의 고유한 식별자
- ID_{N_D} : 후보자(ID_N)의 서명 함수
- ID_{N_E} : 후보자(ID_N)의 서명 함수의 역함수(공개)
- EC_D : EC의 서명 함수

- EC_E : EC의 서명 함수의 역함수(공개)
- A_D : 유권자(Alice)의 서명 함수
- A_E : Alice의 서명 함수의 역함수(공개)
- B_D : 선거위원(Bob)의 서명 함수
- B_E : Bob의 서명 함수의 역함수(공개)
- $R(x)$: 서명 요청자가 TTP의 도움 없이는 서명을 할 수 없도록 검증 하는 값
- x_A : 유권자(Alice)의 비밀 정보 ($\gcd(x_A, p_A-1) = 1$, $x_A \in QNR_{p_A}$(p_A의 평방 비잉여))
- p, p' : 소수($p=4 \cdot p'+1$, $p \equiv 1 \pmod 4$))
- g : GF(p)의 원시근(primitive element)
- p_A, g_A : 공개 정보
- s : 유권자(Alice)의 비밀 정보
- b : 선거위원(EC)의 비밀 정보
- $M_{EC}(G)$: 후보 등록 신청자들의 정보($V_N \parallel ID_N$)
- G : 후보자 수($G \in \{1, 2, ..., n\}$)
- M_A : TTP가 보유하고 있는 투표용지(A는 고유 번호)
- M'_A : Alice가 투표한 결과 값
- N : 유권자 수($N \in \{1, 2, ..., n\}$)
- ID_N : 유권자 N에 대한 개인 식별자
- EC : 선거위원



(그림 3) 투표 단계 별 Moves

[단계 1] 후보자 등록단계 <후보 신청자(ID_N) <==> TTP>

후보신청을 원하는 자격을 갖춘 유권자는 [단계 A~C]의 절차를 통하여 선거관리위원회(TTP)에 후보 신청을 할 수 있다.

[단계 A] 후보신청을 원하는 유권자(ID_N)는 자신의 신분을 TTP로부터 확인 받고 후보자 등록을 하기 위하여 후보자등록신청원($V_N = g_N^{x_N} \pmod{p_N}$)과 자신의 식별자($ID_N$)를 자신의 서명 함수($ID_{N_D}$)와 TTP가 ID_N에게 서명하는 서명 함수의 역함수($T_{ID_{N_E}}$)로 암호화한다.

$F = T_{ID_{N_E}}(ID_{N_D}(ID_N \parallel V_N))$ 결과 값(F, V_N, g_N, p_N)을 TTP에게 전송하고 자신의 비밀키(x_N)는 비밀리에 보관한다.

[단계 B] TTP는 ID_N으로부터 받은 결과 값(F, V_N, g_N, p_N)을 자신이 ID_N에게 서명하는 서명 함수($T_{ID_{N_E}}$)와 ID_N의 서명 함수의 역함수(ID_{N_E})로 복호화한다.

$F_1 = T_{ID_{N_E}}(ID_{N_E}(F)) = T_{ID_{N_E}}(ID_{N_E}(T_{ID_{N_E}}(ID_{N_D}(ID_N \parallel V_N)))) = (ID_N \parallel V_N)$ 결과 값($F_1 = ID_N \parallel V_N$)이 유권자 명단에 포함된 ID_N의 고유한 식별자(ID_N)와 같다고 판단되면 (F_1)에 자신이 ID_N에게 서명하는 서명함수($T_{ID_{N_E}}$)와 ID_N의 서명함수의 역함수(ID_{N_E})로 암호화한다.

$F_2 = ID_{N_E}(T_{ID_{N_E}}(ID_N \parallel V_N))$의 결과 값($F_2$)을 ID_N에게 전송하고 후보 등록 명단에 (ID_N, V_N, g_N, p_N) 저장한다.

[단계 C] ID_N은 TTP로부터 받은 결과 값(F_2)을 자신의 서명 함수(ID_{N_D})와 TTP가 ID_N에게 서명하는 서명 함수의 역함수($T_{ID_{N_E}}$)로 복호화한다. $F_3 = T_{ID_{N_E}}(ID_{N_D}(F_2))) = T_{ID_{N_E}}(ID_{N_D}(ID_{N_E}(T_{ID_{N_E}}(F_1)))) = (F_1) = ID_N \parallel V_N$ 를 확인한다.

[단계 2] EC의 사전 준비단계<TTP <==> EC>

[단계 A] EC는 TTP로부터 자신의 신원을 확인 받고 후보자의 명단을 받기 위하여 공개된 자신의 식별자(ID_{EC})를 자신의 서명 함수(EC_D)와 TTP가 EC에게 서명하는 서명 함수의 역함수(T_{EC_E})로 암호화한다. $EC = T_{EC_E}(EC_D(ID_{EC}))$를 계산한 후, 결과 값($EC$)을 TTP에게 전송한다.

[단계 B] TTP는 EC로부터 받은 결과 값(EC)을 자

신이 EC에게 서명하는 서명 함수(T_{EC_D})와 EC의 서명 함수의 역함수(EC_E)로 복호화한다.

$EC_1 = T_{EC_D}(EC_E(EC)) = T_{EC_D}(EC_E(T_{EC_E}(EC_D(ID_{EC}))) = ID_{EC}$

결과 값($EC_1 = ID_{EC}$)이 선거위원 명단에 포함된 EC의 고유한 식별자 (ID_{EC})와 같으면 후보자등록신청원($V_N = g_N{}^{x_N} (\mathrm{mod}\ p_N)$) 들이 TTP 에게 의뢰한 정보가 들어 있는 메세지($M_{EC}(G)$)와 (EC_1)에 자신이 EC에게 서명하는 서명 함수(T_{EC_D})와 EC의 서명 함수의 역함수 (EC_E)로 암호화한다.

$EC_2 = EC_E(T_{EC_D}(M_{EC}(G) \| EC_1))$의 결과 값(EC_2)을 EC에게 전송한다.

[단계 C] EC는 TTP로부터 받은 결과 값(EC_2)을 자신의 서명 함수(EC_D)와 TTP가 EC에게 서명하는 서명 함수의 역함수(T_{EC_E})이용하여 $EC_3 = EC_D(T_{EC_E}(EC_2)) = EC_D(T_{EC_E}(EC_E(T_{EC_D}(M_{EC}(G) \| EC_1)))) = (M_{EC}(G) \| EC_1)$를 계산하고 확인한 후 M_{EC}의 내용인 후보자 명단을 공개 게시판에 공개한다. ($M_{EC}(G) = ID_N, V_N, g_N, p_N$)($N \in 1, 2, ..., N$)

[단계 3] 신원확인 및 투표신청 단계 <Alice <==> TTP>

[단계 A] Alice는 TTP로부터 자신의 신원을 확인 받고 투표용지를 신청하기 위하여 자신의 식별자(ID_A)를 자신의 서명 함수(A_D)와 TTP가 Alice에게 서명하는 서명 함수의 역함수 (T_{E_A})로 암호화한다.

$C = T_{E_A}(A_D(ID_A))$를 계산한 후 결과 값 (C)을 TTP에게 전송한다.

[단계 B] TTP는 Alice로부터 받은 결과 값(C)을 자신이 Alice에게 서명하는 서명 함수(T_{D_A})와 Alice의 서명 함수의 역함수(A_E)로 복호화한다.

$C_1 = T_{D_A}(A_E(C)) = T_{D_A}(A_E(T_{E_A}(A_D(ID_A)))) = ID_A$

결과 값($C_1 = ID_A$)이 유권자 명단에 포함된 Alice의 고유한 식별자 (ID_A)와 같으면 고유 번호가 있는 투표용지(M_A)와 (C_1)에 자신이 Alice에게 서명하는 서명 함수(T_{D_A})와 Alice의 서명 함수의 역함수 (A_E)로 암호화한다.

$C_2 = A_E(T_{D_A}(M_A \| C_1))$의 결과 값(C_2)을 Alice에게 전송한다.

같지 않으면 프로토콜을 중지한다.

[단계 C] Alice는 TTP로부터 받은 결과 값(C_2)을 자신의 서명 함수(A_D)와 TTP가 Alice에게 서명하는 서명 함수의 역함수(T_{E_A})로 복호화한다.

$C_3 = T_{E_A}(A_D(C_2)) = T_{E_A}(A_D(A_E(T_{D_A}(M_A \| C_1))))$

$= (M_A \| C_1) = (M_A \| ID_A)$를 계산함으로써 TTP로부터 투표 용지(M_A)를 받는다.

[단계 4] 투표단계 <Alice <==> TTP>

[단계 A] Alice는 TTP로부터 받은 투표용지(M_A)에 공개 게시판에 공개된 $M_{EC}(G)$의 정보를 보고 후보자를 선택한 후 투표한 내용을 노출시키지 않고 TTP에게 은닉 서명을 받기 위하여 $R_A(x)$에서 x의 값을 임의로 선택하고 (x_A), $M'_{A,S} = (V_N)^{x_A} (\mathrm{mod}\ p_A)$, $M'_{A,1-S} = (V_N \| x_A)^{x_A} (\mathrm{mod}\ p_A)$을 계산하여 투표한 결과 값 ($M'_{A,S} \| M'_{A,1-S}$)에 자신의 서명 함수(A_D)와 TTP가 Alice에게 서명하는 서명함수의 역함수(T_{E_A})를 이용하여 $R_A(x) = T_{E_A}(A_D(M'_{A,S} \| M'_{A,1-S})$를 계산한 후 TTP에게 서명을 의뢰한다($S \in \{0, 1\}$).

[단계 B] TTP는 Alice로부터 받은 결과 값($R_A(x)$)로부터 Alice의 서명함수의 역함수(A_E)와 자신이 Alice에게 서명하는 서명함수(T_{D_A})를 이용하여 계산하여 저장하고 Alice의 투표 결과 값($M'_{A,S} \| M'_{A,1-S}$)을 공개한다. TTP는 자신이 Alice에게 서명하는 서명함수(T_{D_A})와 Alice의 서명함수의 역함수 (A_E)를 이용하여 $R'_A(x) = T_{D_A}(A_E(M'_{A,S} \| M'_{A,1-S}))$를 계산하고 서명된

결과 값 $R'_A(x)$을 Alice에게 보낸다.

[단계 C] Alice는 TTP로부터 받은 결과 값을 자신의 서명 함수(A_D)를 이용하여 $R'_A(x) = A_D(R'_A(x)) = A_D(T_{D_A}(A_E(M'_{A,S} \| M'_{A,1-S}))) = T_{D_A}(M'_{A,S} \| M'_{A,1-S})$를 계산함으로써 TTP의 서명($R'_A(x)$)을 얻는다.

위와 같은 투표단계를 이용하여 전자선거에 참여하는 당사자들은 TTP로부터 자신이 투표용지에 투표 결과의 내용을 TTP에게 노출시키지 않고 서명을 얻을 수 있다.

[단계 5] EC가 TTP의 서명을 얻는 단계 <EC <==> TTP>

[단계 A] EC는 TTP로부터 은닉 서명을 받기 위하여 ($R_{EC}(x)$)에서 x의 값을 임의로 선택하고 (x_B), 자신의 식별자(ID_{EC})와 함께 자신의 서명 함수(EC_D)와 TTP가 EC에게 서명하는 서명함수의 역함수($T_{E_{EC}}$)를 이용하여 $R_{EC}(x) = T_{E_{EC}}(EC_D(x_B \| ID_{EC})$를 계산 한 후 결과 값($R_{EC}(x)$)을 TTP에게 서명을 의뢰한다.

[단계 B] TTP는 EC로부터 받은 결과 값($R_{EC}(x)$)로부터 EC의 서명함수의 역함수 EC_E와 자신이 EC에게 서명하는 서명함수를 이용하여 ID_{EC}를 확인하고 정당하면 보관한다. 자신의 서명 함수($T_{D_{EC}}$)와 EC의 서명함수의 역함수(EC_E)를 이용하여 $R'_{EC}(x) = T_{D_{EC}}(EC_E(x_B))$을 계산하여 서명한 후 결과 값 ($R'_{EC}(x)$)을 저장하고 EC에게 보낸다.

[단계 C] EC는 TTP로부터 받은 결과 값($R'_{EC}(x)$)을 자신의 서명 함수 (EC_D)를 이용하여 ($R'_{EC}(x)) = EC_D(R'_{EC}(x)) = EC_D(T_{D_{EC}}(EC_E(x_B))) = T_{D_{EC}}(x_B)$를 계산함으로써 TTP의 서명을 얻는다.

[단계 6] 개표 및 개표 확인 단계 <Alice <==> EC>

[단계 A] Alice는 투표단계의 [단계 C]에서 TTP로부터 받은 서명 값($R'_A(x)$)을 EC의 서명 함수의 역함수(EC_E)와 자신의 식별자(ID_A)와 서명 함수 (A_D)를 이용하여 암호화하여 EC에게 전송한다.

$G = EC_E(A_D(ID_A \| R_A(x_A) \| R'_A(x)))$

[단계 B] EC는 Alice로부터 받은 결과 값(G)을 검증하기 위하여 Alice의 서명 함수의 역함수 (A_E)와 자신의 서명 함수(EC_D)를 이용하여 다음을 계산한다.

$G_1 = A_E(EC_D(G)) = A_E(EC_D(EC_E(A_D(ID_A \| R_A(x_A) \| R'_A(x))))) = (ID_A \| R_A(x_A) \| R'_A(x))$

ID_A와 TTP의 서명 값($R'_A(x)$)을 공개된 TTP의 서명 함수의 역함수(T_{E_A})를 이용하여 $G'_1 = T_{E_A}(T_{D_A}(R'_A(x)))$를 계산하여 서명 값($R_A(x_A)$)과 G'_1이 같은지를 확인한다. 만약 서명이 정당하다고 확인되면 [단계 B']로 진행하고, 정당하지 않으면 즉시 프로토콜을 중지한다.

[단계 B'] EC는 투표단계의 [단계 B]에서 TTP가 공개한 Alice의 결과 값($M'_{A,S} \| M'_{A,1-S}$)을 비밀 난수($b \in \{\gcd(b, p_B-1) = 1\}$)을 임의로 선택하여 $G_2 = (M'_{A,0})^b \pmod{p_B}$, $G_2 = (M'_{A,1})^b \pmod{p_B}$를 계산하고 결과 값(G_2)을 TTP로부터 서명 받은 서명값 ($R_{EC}(x)$)을 자신의 서명 함수(EC_D)와 Alice의 서명 함수의 역함수 (A_E)를 이용하여 $G_3 = A_E(EC_D(G_2 \| R_{EC}(x)))$를 계산하여 결과 값(G_3)을 저장하고, Alice에게 전송한다.

[단계 C] Alice는 EC로부터 받은 결과 값(G_3)을 자신의 서명 함수(A_D)와 EC의 서명 함수의 역함수(EC_E)를 이용하여 $G_4 = A_D(EC_E(G_3)) = A_D(EC_E(A_E(EC_D(G_2 \| R_{EC}(x))))) = (G_2 \| R_{EC}(x))$을 계산하고 TTP의 서명 값을 검증하기 위하여 TTP의 서명 함수의 역함수($T_{E_{EC}}$)를 이용하여 $G'_4 = T_{E_{EC}}(T_{D_{EC}}(R_{EC}(x)))$를 계산하여 서명 값($R_{EC}(x_B)$)과 G'_4가 같은지를 확인한다. 만약 정당하다고 확인되면 [단계 C'] 로 진행하고, 정당하지 않으면 즉시 프로토콜을 중지한다.

[단계 C'] Alice는 EC로부터 받은 결과 값(G_3)을 이용하여 $G_5 = G_4^{x_A^{-1}} \pmod{p_A} = G_2^{x_A^{-1}} \pmod{p_A}$를 계산하고 EC에게 전송한다.

[단계 D] EC는 Alice로부터 받은 결과 값(G_5)을 이용하여 $G_6 = G_5^{b^{-1}} \pmod{p_B}$를 계산한다.

만약 G_6 = g라면, EC는 Alice의 비밀에 대하여 아무것도 알지 못한다. $G_6 \neq g$이면, $M'_{A,S} = g^{G_6} \pmod{p_A}$ (S ∈ {0, 1})인지를 확인하여, Alice의 비밀정보($x_A = G_6$)를 알 수 있다. 그것이 아니라면, Bob은 Alice의 부정행위를 TTP에게 알린다.

[개표 확인 단계]

EC는 유권자들로부터 VIOT에 의해 투표결과를 확인하기 위해서는 후보자의 비밀키와 유권자의 비밀키가 있어야만 확인이 가능하기 때문에 부정행위를 할 수 없으며, 또한 유권자는 EC가 정확히 어떤 정보를 받았는지 알 수 없기 때문에 부정행위를 할 수가 없다. (그 이유는 OT 프로토콜의 특성상 상대방이 비밀정보를 정확히 받을 확률은 1/2이기 때문이다.)

4. 전자선거 프로토콜의 안전요구사항에 대한 안전성 분석

- (조건 1)를 만족시키기 위하여 유권자(Alice)는 TTP로부터 내용 은닉서명을 받음으로써, 투표 내용은 본인만이 알 수 있도록 프로토콜을 설계하였다.
- (조건 2)를 만족시키기 위하여 TTP는 고유번호가 있는 투표용지를 유권자의 신원을 확인한 후에 발급하도록 프로토콜을 설계하였다.
- (조건 3)를 만족시키기 위하여 TTP는 투표권이 있는 유권자의 명단을 보유하고, 투표용지를 신청하는 유권자의 서명을 받아 신원확인 절차를 거쳐 투표용지를 발급하도록 프로토콜을 설계하였다.
- (조건 4)를 만족시키기 위하여 유권자, 선거위원들이 TTP로부터 내용 은닉서명을 받음으로써, 투표 내용을 확인하기 위해서는 유권자의 비밀키와 TTP의 서명함수가 요구되도록 프로토콜을 설계하였다.
- (조건 5)를 만족시키기 위하여 투표가 종료된 후 TTP로부터 유권자의 비밀키와 후보자의 비밀키로 투표 내용을 확인할 수 있기 때문에 사전에 다른 유권자들의 선택 내용을 확인할 수 없도록 프로토콜을 설계하였다.

5. 기존의 전자선거 프로토콜과의 비교 분석

유권자, 선거위원, 제3자 누구라도 부정을 할 가능성이 있으며, 2명 이상의 사람이 결탁하여 부정을 행할 가능성도 고려하였다. Asano 등이 제안한 RSA Blind

비교항목	Asano 등이 제안한 RSA Blind 전자선거프로토콜	내용은닉서명과 VIOT를 이용한 전자선거 프로토콜
안전성	RSA 공개키 방식의 안전성에 의존	RSA의 안전성에 불확정 전송 프로토콜의 안전성까지 유지
무기명성	투표의 비밀이 유지되어 무기명성이 유지	투표내용을 확인하기 위해서는 유권자의 비밀키와 TTP의 서명함수가 요구되므로 안전하게 만족
부정조작의 가능성	유권자가 투표를 포기할 경우 부정조작 가능	TTP는 투표권이 있는 투표자의 명단과 투표결과를 보관하고 있으므로 선거관리위원회나 유권자 등 부정조작이 불가능하며 TTP역시 후보신청자의 비밀키를 모르므로 부정 조작 불가능
유권자의 부정투표 가능성	유권자의 2표 이상의 투표 및 비 유권자의 투표가 가능	TTP는 고유번호가 있는 투표용지를 유권자의신원을 확인한 후 발급하도록 설계되어 안전하게 만족
선거관리 위원회의 부정가능성	유권자와 선거관리위원회의 결탁으로 신원확인 과정에 부정가능	TTP가 개입되어 선거관리위원회와 유권자와 후보자가 모두 신원확인을 받고 결과를 보관하므로 부정 불가능
유권자의 공평성에 대한 안전성	모든 사람의 투표가 끝나기 전에는 타인의 투표 내용이 비공개 되므로 만족	투표가 종료된 후 TTP로부터 비밀키와 후보자의 비밀키로 투표내용을 확인할 수 있기 때문에 사전에 다른 유권자들의 선택내용을 확인할 수 없으므로 안전하게 만족
투표중간과정에서의 검증가능성	불가능하므로 비 만족	불확정 전송 프로토콜의 특성에 따라 중간 과정에서도 검증가능하며 부정이 발견되면 프로토콜을 즉시 중지할 수 있다.
사후 분쟁 해결 가능성	내용은 은닉이 되나 투표가 끝난 후 부정이 발견되면 해결 불가능	투표 종료 후 부정이 발견되면 비밀키를 요구해 확인 가능하므로 안전하게 만족
계산량 및 통신량	통신량은 11moves이며 계산량은 많지 않음	통신량은 13move이며 계산량 면에서 다소 시간이 걸림

전자선거프로토콜[18]과 이 논문에서 제안한 프로토콜과 안전성, 무기명성, 부정조작의 가능성 등에 대하여 비교분석 하였다.

6. 결 론

이 논문에서 제안한 전자선거 프로토콜은 RSA 공개키 암호 시스템과 내용 은닉서명을 사용함으로써, 기존의 VIOT의 공정성, 검증가능성, 안전성을 그대로 가지면서, 유권자와 선거위원은 TTP의 은닉서명을 받지 않고서는 이 프로토콜에 참여할 수 없으므로 송수신 사실을 후에 부인할 수 없게 된다. 또한 유권자와 선거위원이 신뢰하는 TTP로부터 내용 은닉서명을 받음으로써, 이 프로토콜을 정직하게 따르면 양자 부정행위 가능성, 프로토콜 중간과정에서의 검증가능성, 사후 분쟁 해결 가능성 면에서 우수하나, 통신량 및 계산량 면에서 다소 시간이 걸리는 단점이 있다. 앞으로 이를 해결하기 위한 연구가 필요하다.

참 고 문 헌

[1] D. Chaum, "Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms," Communication of the ACM, Vol.24, No.24, pp.84-88, 1981.

[2] Cohen, Fischer, "A robust and verifiable cryptographically secure election scheme," Proceedings 26th FOCS, pp.372-382, 1985.

[3] Cohen, "Improving Privacy in Cryptographic Elections," TR-454, Yale University, Department of Computer Science, New Haven, CT, Feb. 1986.

[4] Benaloh, J., "Secret sharing homomorphism : Keeping Shares of a Secret Secret Crypto'86," 1986.

[5] Ryuichi SAKAI, Yasuyuki MURAKAMI, Masao KASAHARA, "A Note on Electric Election," Dept. of Electronics and Information Science, Kyoto Institute of Technology.

[6] Chaum, "Elections With unconditionally-secret ballots and disruption equivalent to breaking RSA," Porceedings of EUROCRYPTO '88, 1988.

[7] Chaum, "Blind Signatures for Untraceable Payments," Advances in Cryptology : Proceedings of CRYPTO'82, Plenum Press, pp.199-203, 1982.

[8] Halpern, J., Rabin. M., "A Logic to Reason about Likelihood," ACM Symposium on Theory of Computing, pp.310-319, May 1983.

[9] Crépeau C., "Verifiable Disclosure of Secrets and Application," Advances in Cryptology : Eurocrypt'89 Proceedings, Springer-Berlag, pp.181-191, 1989.

[10] Harn L., "Verifiable Oblivious Transfer Protocol and its Application," Advance in Cryptology, ASIACRYPTO'91, Proceedings, 1991.

[11] Sakurai, T., Itoh & K. Kurosawa, "Some Remarks on Zero-Knowledge Proofs Based on Oblivious Transfer," ISEC90-13, Japan, 1990.

[12] Rabin, "How to Exchange Secret by Oblivious Transfer," Harvard Center for Research in computer Technology, Cambridge, Mass., 1981.

[13] Tedrick, "Fair Exchange of Secrets," Proceedings of Crypto'84, pp.434-438, 1984.

[14] Yao, "How to Generate and Exchange Secrets," Proceedings of 28th Stoc or Fcs, pp.162-167, 1986.

[15] Beaver, "How to Break a 'Secure' Oblivious Transfer Protocol," Advances in Cryptology : EUROCRYPT'92 Procedings Springer-Berlag LNCS 658, pp.285-296, 1993.

[16] Even, Goldreich, Lempel, "A Randomized protocol for Signing Contracts," Communications of the ACM, Vol.28, 1985.

[17] W. Diffie & M. Hellman, "New Directions in Cryptography." IEEE Transactions on Information Theory IT-22, pp.644-654, November 1976.

[18] Tomoyuki ASANO, Tsutomu MATSUMONO, Hideki IMAI, A S. "Fair Electronic Secret Voting"

[19] SangChoon Kim & YoungSil O & SangHo Lee, "A Non-Interactive Oblivious Transfer containing

Verifiable Capability," ICAST'98, pp.179-183, June, 1998.

[20] SangChoon Kim & SangHo Lee, "An Oblivious Transfer containing Non-Repudiation Capability," ICOIN'13, pp.8D-1.1-1.5, January, 1999.

[21] 김상춘, 오영실, 이상호, "부인봉쇄 기능을 갖는 불확정 전송", 정보과학회 논문지 26권 3호(A), pp. 333-340, 1999.

김 상 춘

e-mail : kimsc@etri.re.kr

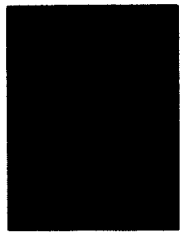
1986년 대전산업대학교 전자계산학과(학사)

1989년 청주대학교 전자계산학과(석사)

1999년 충북대학교 전자계산학과(이학박사)

1983년~2000년 현재 한국전자통신연구원 정보보호기술연구본부 선임기술원

관심분야 : 컴퓨터 네트워크, Network Security, 차세대 인터넷 정보보호, 전자상거래 정보보호 등



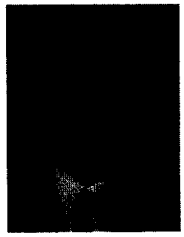
이 용 주

e-mail : yongjuyi@orgio.net

1999년 청주대학교 정보통신공학과(학사)

1999년~2000년 현재 충북대학교 대학원 전자계산학과(석사과정)

관심분야 : Cryptography, Network Security, Network Based Computing



이 상 호

e-mail : shlee@cbucc.chungbuk.ac.kr

1976년 숭실대학교 전자계산(공학사)

1981년 동대학원 시뮬레이션(공학석사)

1989년 동대학원 컴퓨터네트워크(공학박사)

1981년~현재 충북대학교 컴퓨터과학과 교수

1990년~1991년 호주 텔레콤 연구소 연구원

1992년~1993년 캐나다 UBC 방문연구원 Post Doc.

1994년~1998년 충북대학교 전자계산소 소장

관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture