通信情報保護學會誌
第 10 券 第 1 號, 2000. 3

전자선거 프로토콜의 요구사항 연구

허 원 근*, 김 희 선**, 김 광 조**

요 약

본 연구는 전자선거 프로토콜의 요구사항을 규정해 보고, 컴퓨터 통신상에서 이를 충족시키기 위한 암호기법 들을 분석해 본다. 전자선거의 도입이 선거 비용을 절감시키고 투표 장소의 제약을 획기적으로 개선하지만 매표방지등의 문제로 아직은 완전한 이동성을 제공하지는 못한다. 그리고 투표결과의 정확성 검증과 매표방지는 서로 상충되는 요구사항이기도 하다. 실제선거에서는 효율성의 문제로 영지식증명기법등의 사용이 제약 받을 수도 있다. 이러한 문제들을 정리하고, 실제의 선거 절차와 선거 속성들이 전자선거 프로토콜로 어떻게 구현되었는지 비교 검토함으로써, 규정한 요구사항들의 선택적인 적용에 활용코자 한다.

Ⅰ. 서 론

전자선거란 최소한의 물리적 투표소를 이용하면서 안전성이 확보된 암호 알고리즘으로 프로토콜을 구성하여 실제 선거 과정들을 네트워크 상에서 구현한 가상 공간상의 전자적인 선거 행위로 투표의 비밀성, 완전성, 공정성, 검증성 등이 보장되는 것이다. 전자선거의 형태로는 투표 방식에 따라 찬반 투표(YES/NO voting)와 다수후보 투표(Multi-way voting)로 구분할 수 있고 선거 규모에 따라서는 소규모, 중규모, 대규모로 나눌 수 있다. 이러한 전자선거를 구성하는 개체들(participants)로는 유권자(또는 투표자), 선거관리자 및 공개게시판(또는 계수자)가 있다.

전자선거 프로토콜은 선거관리자와 투표자, 투표자와 공개게시판 또는 선거관리자와 공개게시판 사이에 투표 진행에 따른 결과들을 전송하는 규약으로 암호기법이 적용된다. 적용되는 암호기법들은 선거를 컴퓨터와 통신을 이용하여 구현할 때에도 선거가 지니는 속성을 만족시키고자 하는 목적을 갖는다. 전자선거 프로토콜의 요구사항 또는 속성은, [1]에서 비밀성, 건전성, 적임성 및 단일성등이 언급된 후, 1992년도 Fujioka 등의 연구[2]에서 본격적으로 다루기 시작했다. 이후의 연구들[3][4][5][6]에서는 추가적인 속성이 보완되었거나 선거 참가자들에 의한 불공정 행위를 방지하는 방법들이 강화되었다. 이 외에도 익명채널을 이용한 전체검증성을 제시한 연구[7], Publicly Verifiable Secret Sharing (PVSS) 기법을 전자선거에 도입한 연구[8] 등이 발표되었다.

이하의 제 2장에서는 전자선거 프로토콜에서 요구되는 사항들을 검토하고, 제 3장에서는 요구사항을 충족시키기 위해 사용되는 암호기법 들을 분석한다. 제 4장에서는 서로 상충되는 요구사항들을 비교 분석하여, 요구사항의 중요성과 현실적인 관점에서 선택적인 대안을 제시하도록 한다.

Ⅱ. 전자선거 프로토콜의 요구사항

선거의 구성요소에는 선거기관과 투표자들이 있다. 선거기관은 통상 정부라 할 수 있으며 유권자를 등록하고 선거시행 시 유권자를 확인하고 비밀이 보장되는 장소를 제공하여 선거를 하게 한다. 투표가 완료된 다음에는 투표지가 담긴 투표함을 봉인하여 취합하고 유효한 투표를 집계한 후 결과를 발표하게 된다.

* 한국정보통신대학원대학교(ICU) 암호와 정보보안 연구실(abcxyz@icu.ac.kr) 졸업, 현재 삼성SDS(주)에 근무.
** 한국정보통신대학원대학교(ICU) 암호와 정보보안 연구실(sezsez@icu.ac.kr, kkj@icu.ac.kr)

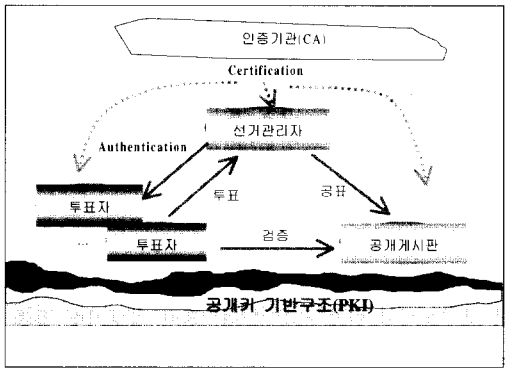

그림 1. 전자선거 개념도

투표의 이 과정을 대략 살펴보면 유권자의 명부를 작성하는 유권자 등록단계, 유권자가 본인임을 확인받는 단계, 투표하는 단계, 각 투표지를 취합하는 수집 단계, 투표 내용을 공개하는 개표 단계, 후보자에 대한 기표별로 더하는 계수단계와 결과의 발표 단계로 구분할 수 있다. 투표자는 이러한 일련의 과정에서 유권자로 등록하고 자신의 결정을 투표지에 표기하여 비밀하게 제시한다(그림 1 참조).

전자선거는 이러한 일련의 과정이 공정하고 안전하게 유지되도록 암호기법을 사용하여 프로토콜을 구성한다. 구성된 전자선거 프로토콜은 선거가 갖는 요구사항을 충족해야 하며, [2]에서는 전자선거 프로토콜이 충족해야할 요구사항을 분류하여 다음의 7가지로 정의하였다.

1. 완전성(Completeness) : 모든 유효 투표가 정확하게 집계되어야 한다는 것으로, 최종 집계에서 정당한 투표가 제거되는 일이 없어야 한다.
2. 건전성(Soundness) : 부정한 투표자에 의해 선거가 방해되는 일이 없어야 한다는 것으로, 최종 집계에서 부정 투표가 집계되어 선거에 영향을 끼치지 않아야 한다.
3. 비밀성(Privacy) : 모든 투표가 비밀로 되어야 한다는 것으로, 특히 개인의 투표내용으로부터 그 개인을 확인할 수 없어야 한다.
4. 단일성 또는 이중투표불가성(Unreusability) : 정당한 투표자가 두 번 이상 투표할 수 없다는 것으로 단지 한 번만 투표할 수 있어야 한다.
5. 적임성 또는 선거권(Eligibility) : 투표 권한을 가진 자만이 투표할 수 있는 것으로 투표가 허락되지 않은 사람은 투표할 수 없어야 한다.
6. 공정성(Fairness) : 투표에 영향을 미치는 어떤 것이 없어야 한다는 것으로 투표 중에 일부분 결과를 알게 되어 투표에 영향을 미치는 상황 등이 없어야 한다.
7. 검증성(Verifiability) : 선거 결과를 속일 수 없도록 누구라도 투표 결과를 확인하여 검증해 볼 수 있어야 한다.

이 후에 [2]에서는 거론되지 않았던 유권자의 매표방지에 관한 연구[4][9][5]이 발표되어 ⑧매표방지성(Receipt-freeness)이 전자선거의 중요한 요구사항으로 대두되었다. 비밀성을 폭 넓게 해석할 경우에 매표방지성을 포함할 수 있지만 별도로 다루고 있다. 매표방지성은 검증성과 상충되는 특성을 갖게 되는데 이에 대한 언급은 4장에서 다루기로 한다. 또한 전자선거에서는 선거관리자가 핵심적인 역할을 하기 때문에, 선거관리자의 부정한 행위 또는 장애방지를 위한 ⑨강인성(Robustness) 확보 또한 중요한 이슈이다. [2]에서 분류한 일곱번째 속성인 검증성의 요구조건은 자신의 투표결과를 검증하는 개별검증성(Locally verifiability)과 누구나 유효성을 검증할 수 있는 전체검증성(Universally verifiability)으로 구분할 수 있다.

이상의 속성 외에도 기존의 선거처럼 실용적인 전자선거는 기권이 가능하여야 하고 기권자와 관계없이 투표가 진행되어야 한다. 불특정 다수를 대상으로 하는 대규모 선거에서의 투표완료는 시간이 기준이 되어야 하겠으나 유권자가 권리를 행사함에 있어서 시스템이나 통신상의 문제로 방해받지 않아야 한다. 개표하는 키가 있는 경우에 키의 오류 시 오류의 원인이 투표자에게 있는지 선거관리자에게 있는지도 밝힐 수 있어야 한다.

Ⅲ. 암호기법의 적용

앞서 살펴본 전자선거 프로토콜의 요구사항들은 전자 투표의 진행 단계인 준비단계나 투표 및 개표 단계, 또는 사후 검증 단계에서 만족되어야 한다. 각 단계의 프로토콜에는 다양한 암호기법들이 사용된다. 그림 2와 같이 전자선거 프로토콜에 사용되는 암호 기법들은 기법 자체의 제한성과 계산의 복잡성

등으로 실용적이지 않거나 실제상황에는 적용하기 어려운 가정들과 함께 사용되기도 한다. 다음에서는 전자선거 프로토콜에 사용되는 기본적이고도 중요한 암호 기법들의 특성과 용도를 분석하고, 요구사항별로 적용여부를 분류한다.

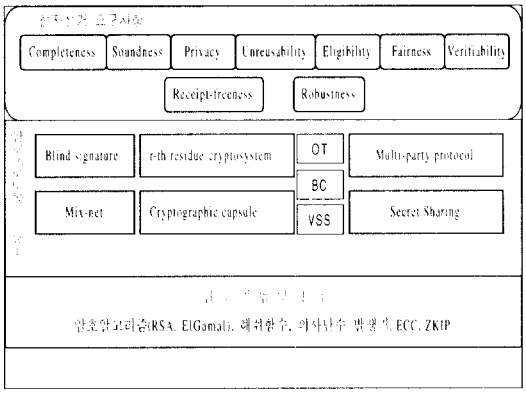

그림 2. 전자선거와 암호기술

1 암호기법

1.1 RSA

구별되는 2개의 큰 소수의 곱을 이용한 기법으로, 큰 소수 p와 q의 곱 n(=pq)의 소인수분해가 어렵다는 성질에 근거하고 있다. $n=pq$ 일 때, $\Phi(n)=(p-1)(q-1)$ 은 Euler Phi 함수로 $\gcd(\Phi(n), e)=1$ 인 난수 e 를 선택한다. 그리고 $ed=1 \bmod \Phi(n)$ 인 d 를 찾아 e, n 을 공개하고 d 는 비밀키로 삼는다. 메시지 M 의 암호화는 $C=M^e \bmod n$ 이고 복호화는 $D=C^d \bmod n$ 이다.

1.2 ElGamal

이산대수문제(Discrete Logarithm Problem)의 어려움에 근간한 공개키 암호 기법이다. 우선, 곱셈군 Z_p^* 상의 생성자 g 를 선택한다. $1 \le a \le p-2$ 인 임의의 정수 a 를 선택하여 $g^a \bmod p$ 를 계산한다. 이 때 (p, g, g^a) 이 공개키가 되고 a 는 개인키가 된다. 메시지 m 의 암호화는 $1 \le k \le p-2$ 인 임의의 정수 k 를 선택하여 $\gamma = g^k \bmod p$ 와 $\delta = m(g^a)^k \bmod p$ 를 계산한다. 복호화는 (γ, δ) 로부터 $(\gamma^{-a})\delta \bmod p$ 를 계산하여 메시지 m 을 얻는다.

1.3 은닉서명 (Blind Signature)

A가 B에게 메시지의 내용을 모르게 하면서 메세지에 대한 서명을 받는 방식으로 A의 익명성을 보장하기 위하여 사용된다. A는 $2 \le k \le n-2$ 이고 $\gcd(n, k)=1$ 인 임의의 수 k 를 선택하고, B의 공개키 b로 $m^* = m k^b \bmod n$ 을 하여 B에게 보낸다. B는 자신의 개인키 a로 서명하여 $s^* = (m^*)^a \bmod n$ 를 A에게 다시 보낸다. A는 $s = k^{-1} s^* \bmod n$ 하여 메세지 m에 대한 B의 서명을 획득한다.

1.4 영지식 증명 (Zero-Knowledge Proofs)

소유한 정보를 드러내지 않으면서 상대방에게 그 정보를 알고 있음을 증명하는 방법으로 인지증명, 유효성 증명 등에 사용된다. 다양한 방식의 ZKP가 제시되고 있으며, 완전성(completeness property), 건전성(soundness property) 및 영지식성(zero knowledge property)을 만족해야 한다.

1.5 비트위임 (Bit-Commitment)

A와 B가 있어서 A가 어떤 값을 B에게 위탁할 때, A는 이 값을 바꿀 수 없어야 하고 B는 일정시점까지는 이 값을 알 수 없어야 할 때 사용한다. 이차 잉여류를 이용한 방법은 잉여류가 아닌 $y \in Z_n^*$ 에 대하여, 0인 경우 $x^2 \bmod n$ 을 1인 경우 $y x^2 \bmod n$ 을 보낸다. 이산 대수를 이용한 방법은 소수 p , 생성자 $g \in Z_p^*$, 그리고 $s \in Z_p^*$ 를 선택하고 0인 경우 $g^x \bmod p$ 를 1인 경우 $s g^x \bmod p$ 을 보낸다.

1.6 전자서명 (Digital Signature)

공개키 암호 시스템의 개인키를 이용하여 메시지를 암호화하여 보내는 방법으로 상대는 서명자의 공개키로 수신된 메시지를 검증해 봄으로써 서명자를 유일하게 확인할 수 있다.

1.7 다자간 프로토콜 (Multi-party Protocol)

다수가 비밀을 분산 유지하여 모두가 모여 연산을 행하면 원하는 비밀 값을 얻을 수 있는 방식으로 (t,n) Threshold scheme 의 경우 비밀 정보를 n명이 분산 보관하고 t(<n)명이 협력하면 비밀정보를 복원하여 암호문을 복호화 할 수 있다.

1.8 검증가능 비밀공유 (Verifiable Secret Sharing)

비밀 정보를 분산시켜 보호하는 것으로, 각 참여자가 받은 비밀 조각이 정당한 것인지를 모든 참가자가 검증할 수 있는 구조이다. 비밀은 참여자 모두가 비밀의 재구성에 협조할 때만 재결합이 가능하다.

1.9 익명채널(Anonymous Channel or MIX-NET)

송신자와 그 메시지간의 관계를 숨기는 것으로, 모든 개인이 정직한 경우에 입력 메시지와 출력이 일치하면서 어느 경우에도 송신자와 그 메시지의 관계가 숨겨지는 방법으로, k개의 Mix 서버를 사용하여 일부 MIX의 부정을 방지하는 방법을 함께 사용한다.

1.10 기타 (Others)

이차 잉여류 (Quadratic Residues)인 $y = x^2 \bmod n$, 다차 잉여류 (R-th residue) 인 $z = x^r \bmod n$, 둘 이상에서 참(true)인 것을 비밀의 노출없이 상대에게 확신시키는 기법인 암호캡슐(Cryptographic Capsule), 그리고 비밀을 보증하면서 정보를 전달하는 Oblivious Transfer 등이 사용된다.

2. 요구사항별 암호기법 적용

이론적인 측면에서 전자선거 요구사항들이 충족됨을 증명하는 것은 중요하다. 하지만 실세계 선거는 물리적인 장소에 제약이 있으며, 유권자는 수만, 수십만, 또는 수백만에서 수천만 명까지 되기도 한다. 이러한 현실 때문에 전자선거의 장점인 이동성에서는 매표방지에 따른 제한이 가해지며, 영지식증명과 같이 효율성에 문제가 있는 암호기법들은 통신량 때문에 적용이 어려울 수도 있다. 즉, 전자선거를 도입하더라도 자신의 집이나 사무실에서 투표를 하는 대신에 기존의 선거처럼 물리적으로 한정된 기표소에서 투표를 해야 하는 것은 비슷한 상황이 될 수 있다.

그러므로 전자선거를 실제 국회의원 선거나 대통령 선거에 적용했다고 가정했을 때 발생할 수 있는 상황들을 예측하는 작업이 필요하고, 이론적으로는 가능하지만 현실적으로는 가능하지 않거나 제한적으로 적용될 수 밖에 없는 요구사항과 암호기법의 한계를 인식하여야 한다. 이는 전자선거 관련 연구들의 프로토콜을 상세히 비교 분석함으로써 얻어질 수 있으며 본 연구에서는 다루지 않는다.

표 2. 전자선거 프로토콜 요구사항의 암호기법 적용 예

요구사항	암호기법	비 고
완전성 (Completeness)	전자서명[2], 은닉서명, 익명채널 등 사용	유효투표의 정확한 집계
건전성 (Soundness)	비트위임, 다자간 프로토콜 사용	부정 투표의 선거 방해 불가
비밀성 (Privacy)	은닉서명[2]과 RSA[10], ElGamal[3][7][11] 등의 암호기법으로 익명채널[10]을 구성하여 사용	투표의 비밀 유지, 투표와 개인 연결 불가
단일성 (Unreusability)	전자서명, 은닉서명 사용	단 한번의 투표
적임성 (Eligibility)	전자서명 사용	투표 권한자만 투표
공정성 (Fairness)	비트위임 사용	어떠한 요인도 투표에 영향을 미치지 못함
검증성 (Verifiability)	비트위임[15], 난수, Threshold ElGamal[7], 은닉서명[2], 공개키비밀분산[8] 사용	투표 결과의 정확성 검증
매표방지성 (Receipt-freeness)	영지식증명[12][14][9][15] 사용	매표행위 불가
강인성 (Robustness)	비밀분산, Threshold의 다자간 프로토콜[13][6] 사용	일부 시스템 장애 또는 부정행위에 영향 받지 않음

표 1은 전자선거 프로토콜에서의 요구사항 충족을 위하여 사용되거나 사용가능한 암호기법 들을 정리한 표이다. 암호기법들은 하나의 요구사항을, 또는 여러 다른 요구사항들을 동시에 만족시키기도 한다. 더 상세한 내용들은 참고문헌의 연구들을 참조하면 될 것이다.

표 1에서 알 수 있듯이 암호기법들이 여러 요구사항에 공통적으로 사용되고 있으며 암호기법들을 종합적으로 사용하기도 한다. 선거의 가장 중요 속성인 비밀성을 만족함으로써 [2]에서 정의한 요구사항 7가지는 대부분 만족될 수 있다. 반면에 강인성은 (t,n)-threshold 기법을 사용하며, 매표방지성에는 영지식증명기법을 사용하여 구현하고 있다.

위 9가지 속성중 매표방지성의 구현이 가장 난해하다. 또한 매표방지성은 검증성과 상충되는 특성 - 제 4장에서 언급 - 으로 인하여, 매표방지성을 포함하는 전자선거 프로토콜을 제시하는 연구[4][9][5]이 드물며 강한 가정을 사용하고 있다.

Ⅳ. 검증성과 매표방지성

2장에서 논의한 9가지 요구사항중 검증성과 매표방지성은 기본적으로 중요한 속성이지만 표리적인 특성으로 인하여 동시에 만족시키기가 어렵다. 검증성은 자신의 투표 결과가 올바르게 게시되었는지를 확인하는 개별 검증성과 게시된 투표결과의 정확성을 누구나가 확인할 수 있는 전체 검증성으로 구성된다. 검증성은 투표내용을 확인할 수 있는 어떤 방법을 투표자나 제삼자에게 제공하는 것이고, 매표방지성은 투표의 내용과 투표자를 연결할 수 있는 방법을 차단하는 것으로 상호 표리적인 관계에 있다.

매표방지성을 제시한 연구들[12][4][9][5]를 보더라도 전체검증성을 제공하지 않거나 매표방지 방법에서 투표자의 정보가 누출될 수 있는 가능성을 내포하고 있다. 전체검증성을 제시하고 있는 연구들[6][7]은 매표방지성을 제시하지 않고 있다. 이처럼 현재까지는 두가지 요구사항을 충족시키는 방법이 제시되지 못하고 있는 실정이다. 즉, 검증성과 매표방지성은 속성 상 동시 만족이 불가하다고 볼 수 있다. 그렇다면 두가지 요구사항중 하나를 선택하거나, 둘 중 하나는 간접적으로 확인하는 방법을 채택하는 것이 현실적이라 하겠다.

투표자, 선거관리자, 공개게시판이 전자선거를 구성하고 있다. 이 중 선거관리자는 삼권분립이 잘 되어있고 민주주의가 성숙한 나라의 정부기구로써 공정하고 신뢰할 만하다고 가정하자. 공개게시판은 공적인 게시판으로써 누구나가 열람할 수 있다. 투표자는 선거관리자의 역할하에서 자신의 결정을 투표지로 표기하여 공개게시판에 게시한다. 이 과정에서 투표와 개표 결과의 정확성 또는 유효성을 우선 시 한다면 검증성을 필히 제공하여야 한다. 반면에 투표자의 매표 가능성 방지를 우선 시 한다면 매표방지성을 제공하여야 한다.

민주주의 사회에서 의사결정을 위하여 사용하는 투표라는 도구의 기능을 중시한다면 검증성보다는 매표방지성을 제공하는 것이 우선이라 하겠다. 매표방지성을 제공하더라도 검증성은 간접적으로 확인할 수 있는 방법이 제시될 수 있다. 반면에 검증성을 제공하는 경우에는 매표방지성을 제공할 뾰족한 대안이 없는 실정이다.

간략하게 예를들면, 투표자가 $(x,\ y) = (g^{\alpha},\ h^{\alpha}m)$ 와 같이 m이라는 투표내용을 암호화하여 게시하면 선거관리자는 자신의 공개키 $h\ (=\ g^{x})$ 에 대응하는 개인키 x 로 복호화하여 투표를 집계할 수 있다. 하지만 투표자는 자신의 투표를 강압자에게 증명할 수 있게 된다. 반면에 선거관리자가 투표자의 메세지 $(x,y)=(g^{\alpha},h^{\alpha}m)$ 를, g^{β} 와 h^{β} 를 사용하여, $(x',\ y') = (g^{\beta}g^{\alpha},\ h^{\beta}h^{\alpha}m)$ 와 같이 재암호화(re-encryption)하여 게시한다. 그러면 투표자는 선거관리자의 도움없이는 자신의 투표를 주장할 수 없게 된다. 즉, 선거관리자와 무관한 독립적인 검증 방법이 존재하지 않는다. 만약 이를 독립적으로 검증할 수 있다면, 이는 이산대수문제의 어려움에 근간한 ElGamal 암호방식을 해독할 수 있다는 것과 동일하게 된다. 고로 매표방지기능을 제공할 수 있게 된다. 반면에 검증성은 간접적인 방법으로 제공한다.

이러한 간접적인 검증성의 제공은 현행의 투표방식과 동일하다고 할 수 있겠다. 현재의 선거제도에서 투표 후, 선거관리기관에서 개표한 투표결과의 정확성을 확인할 수 있는 방법이 독립적으로 제공되지 않는다. 다만 이의신청을 법원에 제기하면 개표된 투표지들을 재 검토하는 과정을 다시 할 수 있게 되는 것이다. 이는 공개게시판의 $(x',\ y') = (g^{\beta}g^{\alpha},\ h^{\beta}h^{\alpha}m)$ 을 검증하는 과정으로 볼 수 있다.

결론적으로 선거에서 주도적인 역할을 맡고 있는 선거관리기관은 기본적으로 신뢰할 수 있는 기관이라는 가정이 현실적인 선거에서도 필요하며, 똑같이 전자선거에서도 필요하다. 이와 같은 가정이 바탕이 된다면 검증성보다는 매표방지성을 전자선거 프로토콜이 제공하는 것이 현재 선거의 기능에 가깝다고 할 수 있겠다.

V. 결 론

전자선거 프로토콜의 요구사항에 대하여 검토하고 요구사항을 충족시키기 위하여 사용되는 암호기법들에 관하여 분석하였다. 요구사항중 검증성과 매표방지성이 상호 모순되는 관계에 있음을 기술하였고 선진민주사회에 적용할 현실적인 전자선거에서는 매표방지성을 우선 부여하고 검증성은 간접적으로 제공하여야 함을 제시하였다.

앞으로, 개인키의 노출없이 Secret Shares 를 검증할 수 있는 PVSS(Publicly Verifiable Secret Sharing) 구조를 활용하여, 전체검증성과 제한적인 검증성을 지닌 매표방지성 성질을 제공하는 전자선거 프로토콜에 관한 연구가 필요하다.

참 고 문 헌

[1] Kenneth R. Iversen, "A Cryptographic Scheme for Computerized General Elections", Advances in Cryptology -Crypto 91, LNCS Vol., pp. 405-419, Springer-Verlag, 1991.

[2] A.Fujioka, T.Okamoto 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.

[3] 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, 1993.

[4] V.Niemi and A.Renvall, "How to prevent buying of voters in computer elections", Advances in Cryptology -Asiacrypt94, LNCS Vol.917, pp.164-170, Springer-Verlag, 1994.

[5] K.Sako and J.Killian, "Receipt-free Mix type voting scheme - a practical solution to the implementation of a voting booth", Advances in Cryptology -Eurocrypt95, LNCS Vol.921, pp.393-403, Springer-Verlag, 1995.

[6] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers, "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology-EUROCRYPT'97, LNCS Vol. 1233, pp.103-118, Springer-Verlag, 1997.

[7] 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.

[8] B. Schoenmakers, "A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting", Advances in Cryptology- Crypto99, LNCS Vol. , pp.148-164, Springer-Verlag, 1999.

[9] J.C.Benaloh and D.Tuinstra, "Receipt-free secret ballot elections", Proc. of 26th ACM STOC, pp.544-553, 1994.

[10] David L. Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms Communications of the ACM, Vol. 24, No.2, pp. 84-88, 1981.

[11] M. Jakobsson, A Practical Mix, Advances in Cryptology -Eurocrypt 98, LNCS Vol. 1403, pp. 449-461, Springer-Verlag, 1998.

[12] J.C.Benaloh, "Verifiable secret ballot elections", PhD thesis, Yale University, TR561, 1987.

[13] Y. Desmedt, Y. Frankel, "Threshold cryptosystems", Advances in Cryptology-Crypto89, LNCS Vol., pp.287-296, Springer-Verlag, 1989.

〈著者紹介〉

허 원 근 (許 元 根)

1987년 2월 : 연세대학교 물리학과 졸업(학사)
1987년 1월 ~ 1993년 6월 : 대림산업대덕연구소
1993년 6월 ~ 현재 : 삼성SDS(주)
2000년 2월 : 한국정보통신대학원대학교 졸업(석사)
〈관심분야〉 공개키기반구조, 전자상거래, 정보보호와 암호 이론 및 응용

김 희 선 (金 希 先)

1998년 2월 : 강원대학교 정보통신공학과 졸업(학사)
1998년 3월 ~ 현재 : 한국정보통신대학원대학교 석사과정
〈관심분야〉 전자화폐, 전자상거래

김 광 조 (金 光 兆)

1979년 2월 : 연세대학교 전자공학과(학사)
1983년 2월 : 연세대학교 전자공학부(석사)
1991년 2월 : 요꼬하마 국립대 전자정보공학부(공학박사)
1979년 12월 ~ 1997년 12월 : 한국전자통신연구원 부호1실장
1996년 3월 ~ 1997년 8월 : 충남대학교 컴퓨터 과학과 겸임 교수
1998년 1월 ~ 현재 : 한국정보통신대학원 공학부 교수, 본학회 학술(국외) 이사, 세계암호학회 회원, Asiacrypt 조정 위원회 위원
1999년 12월 ~ 2000년 2월 : 요꼬하마 국립대 방문교수
2000년 1월 ~ 현재 : 세계암호학회(IACR) 이사
〈관심분야〉 정보보호와 암호 이론 및 응용