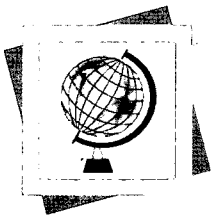
| 특집 04 |



전자선거 암호보안기술에 관한 동향 연구

김건욱 · 홍종욱 · 변진욱 · 구재형 · 이동훈
(고려대학교)

목 차

1. 서 론
2. 요구사항
3. 암호화와 전자서명 기법
4. 은닉 서명(Blind Signature)
5. 준동형 암호화(Homomorphic Encryption)
6. 믹스넷(Mixnet)
7. 기타 기술
8. 결 론

1. 서 론

2008년 총선부터 전자선거를 도입하겠다는 중앙 선거관리 위원회의 발표가 있은 후, 전자선거에 대한 관심이 높아지고 있다. 무효표 방지, 투표율 제고, 빠른 집계 등 전자선거의 장점들을 누리기 위해서는, 해킹, 부정투표, 악의적인 공격 등에 대한 보안 요소들이 선결되어야만 한다. 많은 사람들이 참여하는 전자선거가 특정 공격에 취약하다면 사회적으로 큰 혼란을 불러 올 수 있기 때문이다. 그러므로 전자선거는 가장 높은 수준의 암호학적 안전성을 요구하게 된다.

본 논문에서는 안전하고 효율적인 전자선거를 위한 여러 암호학적 기술들에 대해 살펴본다. 약 20여 년 전부터 연구되어온 전자선거 관련 연구내용과, 암호학적인 요구사항, 그리고 크게 3가지로 나눌 수 있는 암호학적 기법과 그 외에 필요한 기술들에 대해 알아본다.

2. 요구사항

전자선거는 투표와 관련된 일련의 과정들이 공정하고 안전하게 유지되도록 여러 가지 암호기법을 사용해서 이루어진다. 안전한 전자선거 시스템이 갖추어야 할 요구사항은 다음과 같다.

- **완전성(Completeness)** : 모든 유효 투표는 정확하게 집계되어야 한다. 최종 집계에서 정당한 투표가 제거되는 일은 없어야 한다.
- **건전성(Soundness)** : 부정 투표자에 의해서 투표가 방해되거나 중지되어서는 안 되며, 부정 투표가 집계되어 선거에 영향을 끼치지 않아야 한다.
- **익명성(Privacy)** : 투표 결과로부터 투표자를 구별할 수 없어야 한다.
- **이중 투표 불가성(Uniqueness)** : 정당한 투표자가 두 번 이상 투표할 수 없다.

- **권한성(Eligibility)** : 투표 권한을 가진 자만이 투표할 수 있다.
- **공정성(Fairness)** : 투표가 진행되는 시점에는 어떤 누구도 투표 결과에 대한 정보를 얻을 수 없다.
- **검증성(Verifiability)** : 선거 결과를 변경할 수 없도록 투표 결과를 검증할 수 있어야 한다. 검증성에는 투표자 개개인이 검증할 수 있는 개별검증(Individual Verifiability)과 전체검증(Universal Verifiability)이 있다.
- **매표방지(Receipt-free)** : 투표가 종료된 후, 투표자는 자신 이외에 다른 사람에게 자신의 투표 내용을 증명하는 것이 불가능해야 한다. 즉, 투표권을 매수/매도하는 행위는 차단되어야 한다.

3. 암호화와 전자서명 기법

전자선거는 투표자의 정보를 어떤 누구도 알 수 없어야 한다. 그러므로 투표자의 정보는 암호화 되어 전송되어야 한다. 여기서는 전자선거에서 쓰이는 기본적인 암호화 기법들을 살펴본다.

3.1 대칭키 암호시스템

대칭키 암호시스템이란 송신자와 수신자만이 알고 있는 동일한 대칭키를 이용하여 메시지를 암호화하고 복호화 할 수 있는 시스템이다. 암호화를 위해서 송신자가 보유하고 있는 키와 복호화를 위해서 수신자가 가지고 있는 키가 동일하기 때문에 대칭형 암호시스템(Symmetric Crypto-system)이라고 부른다. 따라서 대칭형 암호시스템에서는 송신자와 수신자 간에 키의 사전 분배가 선행되어야 한다.

대칭키 암호시스템의 문제점이라고 하면 새로운 사용자가 추가될 때마다 사용자만큼의 대칭키가 필요하다는 것이다. 그러므로 사용자가 늘어남에 따라 필요한 대칭키의 개수는 기하급수적으로 증가하게 되어 이러한 대칭키를 생성하여 분배하는 작업은 시스템의 효율성을 크게 저하시키게 된다. 특히, 모든 사용자들이 그렇게 많은 대칭키를 유지, 관리하는 것 역시 어렵다.

현재 가장 보편적으로 사용되고 있는 대표적인 대칭키 암호시스템은 1977년 미국에서 연방 정보처리 표준 46으로 채택된 DES(Data Encryption Standard)를 들 수 있다. 우리나라에서는 SEED와 ARIA라는 대칭키 암호시스템을 만들어 사용하고 있다.

3.2 공개키 암호시스템

1976년에 미국 스탠포드 대학의 Diffie와 Hellman에 의하여 공개키 암호시스템(Public-Key Cryptosystem)이라는 새로운 개념의 암호시스템이 제안되었다. 그들의 제안은 서로 연관이 있는 상이한 두 개의 키를 각각 암호화와 복호화에 이용하는 것이다. 이러한 개념은 키의 사전 분배문제를 자연스럽게 해결하였고 디지털 서명과 같은 새로운 개념의 출현을 가능하게 하였다. 공개키 암호시스템은 암호화와 복호화에 사용되는 키가 서로 다르기 때문에 비대칭형 암호시스템(Asymmetric Cryptosystem)이라고도 부른다.

전자선거 기법에서는 기본적으로 공개키 암호시스템을 사용한다. 만약 대칭키 암호시스템을 사용한다면, 모든 투표자들과 투표 관리자사이에 키를 모두 공유하고 있어야 하기 때문에 키 교환의 문제점이 생긴다. 전자선거에서는 투표자가 많기 때문에 공개키 암호시스템을 사용하여 이러한 문제점을 해결한다.

3.2.1 RSA 암호시스템

RSA 암호는 미국 M.I.T. 대학의 Rivest, Sharmir, Adleman에 의해서 1978년에 고안된 암

호로서 Diffie와 Hellman이 제안한 공개키 암호 시스템에 대한 개념을 가장 충실히 반영한 공개키 암호다. RSA 암호는 소인수분해(Factoring)의 어려움에 기반을 하고 있다.

$n = p \cdot q$ (p, q : 2보다 큰 소수)
$e \cdot d \equiv 1 \pmod{\phi(n)}$ $\phi(n)$: 오일러 함수

공개키 : n, e
개인키 : d
메시지 : x

암호화 : $e_K(x) = x^e \pmod{n}$
복호화 : $d_K(y) = y^d \pmod{n}$

〈RSA 암호시스템〉

3.2.2 ElGamal 암호시스템

ElGamal 암호시스템은 이산대수 문제(Discrete Logarithm Problem)에 기반을 하고 있다. 이산대수 문제란 p가 큰 소수일 때, $y = g^x \pmod{p}$에서 y, g, p를 알고 있어도 x를 구하는 것은 매우 어려운 문제라는 것이다.

$\beta \equiv \alpha^a \pmod{p}$ p: 소수
공개키 : p, α, β
개인키 : a
메시지 : x

암호화 :
$e_K = (x, k) = (y_1, y_2)$ (k: 임의의 수)

$$y_1 = \alpha^k \pmod{p}$$
$$y_2 = x\beta^k \pmod{p}$$

복호화 :
$d_K = (y_1, y_2) = y_2(y_1^a)^{-1} \pmod{p}$

〈ElGamal 암호시스템〉

3.3 전자서명 기법

전자서명은 전자문서에 종이 문서의 도장과 같은 역할을 할 수 있도록 하는 기술이다. 종이 문서에 행하는 일반적인 서명의 특징은 서명자에 의한 서명 생성작업과 그 서명에 대한 확인 작업은 용이하게 이루어질 수 있는 반면에 서명자 이외의 제3자에 의한 서명 위조는 일반적으로 불가능하고 또한 서명자가 나중에 자신이 서명한 내용을 부인할 수 없다.

그러므로 전자서명은 그 문서를 작성한 사람만이 생성할 수 있어야 하고 그 사람만이 알고 있는 정보가 적용되어야 하며, 그 전자서명에 대한 확인 작업은 공개된 방식에 의해 누구나 확인 할 수 있어야 한다. 전자선거 기법에서는 전자서명 기법을 본인이 투표한 값에 대한 값을 확인하거나 본인임을 확인하는 데 사용된다.

$n = p \cdot q$ (p, q : 2보다 큰 소수)
$e \cdot d \equiv 1 \pmod{\phi(n)}$ $\phi(n)$: 오일러 함수
공개키 : n, e
개인키 : d
메시지 : x

서 명 : $Sig_K(x) = x^d \pmod{n}$
확 인 : $Ver_K(y) = y^e \pmod{n}$

〈RSA 서명 기법〉

3.4 해쉬함수(Hash Function)

메시지에 대한 무결성이 요구되어질 경우에는 인증자(Authenticator), 또는 해쉬 값(Hash Value)으로 명명되는 특수한 형태의 데이터 구조를 메시지로부터 압축, 생성하여 메시지에 첨가하여야 한다. 또한, 그 메시지의 작성자에 대한 확인(Message Authentication)이 필요한 경우에는 인증자를 생성하는 과정에 메시지 작성자와 수신자만이 알고있는 비밀키(Secret Key)가

포함되어져야 한다. 인증자를 생성하는 데에 사용되는 함수를 암호학적 해쉬함수(Cryptographic Hash Function)라고 한다. 이 인증자를 통해서 수신자는 메시지에 대한 무결성 및 메시지를 보낸 작성자에 대한 확인을 할 수 있게 된다.

4. 은닉 서명(Blind Signature)

Chaum[6]에 의해 처음 소개된 은닉 서명(Blind Signature)은 서명자(Signer)에게 메시지의 내용을 알려주지 않으면서 서명을 받는 기법이다. RSA 서명 기법을 이용하여 은닉 서명을 하는 방법은 다음과 같다.

- B에게 서명을 받고자 하는 A는 랜덤한 숫자 r을 선택한 후 다음을 계산하여 B에게 보낸다.((n, e)는 B의 공개키, d는 B의 개인키)

  $x = r^e m \bmod n$

- B는 x값을 받더라도, r의 영향으로 m에 대한 어떠한 정보도 얻을 수 없다. B는 $x^d \bmod n$을 계산하여 A에게 보낸다.
- A는 다음을 계산하여 메시지에 대한 B의 서명을 얻게 된다.

  $r^{-1}x^d = r^{-1}(r^e m)^d = r^{-1}r^{ed}m^d =$

  $r^{-1}rm^d = m^d \bmod n$

은닉 서명을 사용한 전자선거 기법[7, 15]은 가장 간단하고 효율적이나 익명 채널이 필요하다는 단점이 있다. 투표자는 인증기관으로부터 은닉 서명을 이용해 자신의 비밀 투표지에 서명을 받고, 비밀 투표를 개표 기관에 전송한다. 정당한 투표자만이 서명을 받을 수 있기 때문에 전자선거의 권한성이 지켜지나, 익명성을 보장하기 위해서 투표자와 개표 기관 사이에 익명 채널이 형성되어야만 한다. 은닉 서명을 이용했을 경우 5장에서 설명할 준동형 암호화를 이용한 전자선거와 비교하여, write-in ballot이 가능하다. write-in ballot은 투표자가 어떠한 형태의 투표도 가능하게 한다는 것으로, 투표자가 직접 후보자의 이름을 쓰는 등 자신이 직접 선택한 메시지를 투표하게 하는 개념이다.

5. 준동형 암호화(Homomorphic Encryption Scheme)

준동형 암호화 기법이란 하나의 연산에 대해, 두 개의 메시지들 각각의 암호화한 값을 연산한 값이 같은 성질을 이용한 기법이다.

$$E(m_1 m_2) = E(m_1)E(m_2)$$

$E()$: 준동형 성질을 가지고 있는 함수
m_1, m_2 : 임의의 메시지

〈준동형 암호화 기법〉

대표적인 준동형 성질을 만족하는 RSA 암호화 알고리즘은 평문 m_1을 암호화 한 암호문이 a_1이고, 평문 m_2를 암호화한 암호문이 a_2일 때, 평문 $m_1 m_2$를 암호화 한 암호문은 $a_1 a_2$가 된다.

Benaloh와 Tuinstra[3]는 선거관리자와 유권자 사이의 비밀통신을 물리적으로 보장하는 선거부스(voting booth)와 준동형 암호화 기법을 이용하는 두 가지 전자선거 기법을 제안하였다.

준동형 성질을 이용하면 투표 종료 후 개표 단계에서는 투표 과정에서 암호화된 값들을 다 연산을 한 후, 한 번의 복호화 작업으로 모든 투표값을 집계할 수 있게 된다. 준동형 성질을 이용하지 않는다면, 투표 과정에서 암호화된 값들을 모두 다 복호화하여야 하므로 계산량도 증가하게 된다. 또한, 각각 값들이 복호화될 경우 어떤 유권자가 어떤 후보자를 선택하였는지 밝

혀지기 때문에 준동형 성질을 이용하면 모든 값들이 다 합쳐져서 연산된 후에 복호화를 하므로 복호화되어진 값이 밝혀진다고 해서 어떤 선택을 하였는지 알 수 없게 된다.

준동형 암호화 기법을 이용한 전자투표는 찬반 투표나 후보자가 적은 시스템에서 효율적으로 사용될 수 있다. 후보자가 많을 경우, 각각 값들을 연산하여 집계하는 과정이 복잡해지므로 준동형 암호화 기법을 이용하였을 때의 장점은 사라지게 된다.

6. 믹스넷(Mixnet)

믹스넷은 Chaum[5]에 의해 처음 소개되었고, 그 이후 여러 연구를 통해 발전되어 왔다[1, 12, 18]. 믹스넷은 투표자들의 투표값에 익명성을 부여함으로써 전체 시스템의 익명성을 제공한다(그림 1참조). 믹스넷은 크게 복호화 믹스넷(decryption mixnet)과 재암호화 믹스넷(re-encryption mixnet)으로 나눌 수 있다. Chaum이 처음 제안한 믹스넷은 복호화 믹스넷이었지만, 최근 연구에서는 재암호화 믹스넷을 많이 다루고 있다. 왜냐하면 재암호화 믹스넷은 믹스 과정과 복호화 과정을 분리함으로써 좀 더 유연하고 효율적인 결과를 보여주기 때문이다.

믹스넷의 실행 과정에서 각각의 믹스 서버는 올바르게 믹스 과정을 수행하였다는 것을 증명해야 한다. 이는 하나의 믹스 서버가 공격하여 아무도 눈치 채지 못하게 투표값을 바꾸는 것에 대해 대비하기 위해서이다. 그러나 이러한 증명을 통해 입력값과 출력값에 대한 어떠한 정보도 알려지면 안 된다. 증명 기법에는 영지식 증명, RPC(Randomized Partial Checking) [9], Proof-of-Subproduct 등이 있다.

6.1 복호화 믹스넷(Decryption Mixnet)

믹스넷은 입력값을 섞어 다음 서버에게로 전달하는 역할을 하는 여러 개의 믹스 서버로 구성되어 있다. 투표자는 각각의 믹스 서버의 공개키로 암호화한 투표값 $E_{p_1}(E_{p_2}(E_{p_3}(\cdots E_{p_t}(m))))$을 첫 번째 믹스 서버에게 보낸다. 첫 번째 믹스 서버는 투표자로부터 받은 값들을 모두 복호화한 후 순서를 뒤섞어 다음 믹스 서버에게 보낸다. 이 과정이 t개의 믹스 서버를 통해 모두 이루어지면, 최종 믹스 서버는 모두 복호화된 m의 값을 얻게 된다.

6.2 재암호화 믹스넷(Re-Encryption Mixnet)

재암호화 믹스넷에 각각의 믹스 서버는 복호화 믹스넷과는 다르게, 복호화 과정을 하는 대신 재암호화과정을 수행한다. 이때 ElGamal 암호 시스템과 같은, 암호문에 대한 재암호화를 지원하는 공개키 암호 기법을 사용한다. 어떤 주어진 공개키에 대해서 C와 C'이 복호화했을 때 같은 평문이 나온다면, C'는 C의 재암호화를 나타낸다고 한다. 이 때 익명성을 보장하기 위해서는 실제 암호문의 쌍 (C, C')과 난수를 암호화한 R과의 쌍인 (C, R)이 구별 불가능해야 한다. 재암호화 과정은 복호화 과정에 영향을 끼치지 않으며, 또한 비밀키를 모르더라도 가능하다. ElGamal 암호 시스템의 재암호화는 다음과 같다.

$ReEnc(c_1, c_2) = (c_1 * g^s, c_2 * y^s) =$
$(g^{(r+s)}, my^{(r+s)})$
(c_1, c_2: 기존의 암호문, y: 공개키, $s \in {}_R Z_p^*$)

〈재암호화 믹스넷〉

투표자는 암호화된 투표값들을 첫 번째 믹스 서버로 입력하고, 믹스 서버는 각각의 입력값을 재암호화 한 후 그 결과를 섞어서 두 번째 믹스

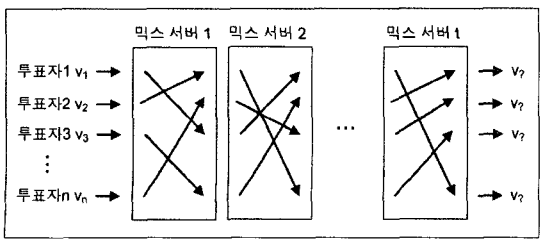
서버로 전송한다. 두 번째 믹스 서버 역시 이 과정을 수행하고, 이 과정이 마지막까지 반복된 후, 믹스 서버들에 분산되어 있는 비밀키를 혼합하여 모든 입력값을 복호화할 수 있다.

6.3 전체 재암호화(Universal Re-Encryption)

재암호화 믹스넷이 암호문을 암호화 하는데 쓰인 공개키를 알아야 하는 단점이 있다면 전체 재암호화(universal re-encryption)는 공개키에 대한 정보가 없이도 재암호화를 수행할 수 있다. 따라서 좀 더 효율적인 믹스넷의 설계가 가능해진다.

$E[m]$을 기존의 ElGamal 암호시스템 하에서 암호화라고 한다면, 전체 암호시스템에서의 암호문은 $[E[m]; E[1]]$이 된다(ElGamal 암호 시스템의 준동형 성질을 사용). ElGamal 암호 시스템의 전체 암호시스템은 다음과 같다.

- **키 생성**: $(PK,\ SK) = (y = g^x,\ x)$ for $x \in {}_UZ_q$
- **암 호 화**: 메시지 m과 공개키 y, 랜덤 암호화 요소 $r=(k_0,\ k_1) \in Z_q^2$ 을 입력값으로 받는다. 출력값은 암호문 $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)] = [(my^{k_0}, g^{k_0}); (y^{k_1}, g^{k_1})]$이다.
- **복 호 화**: 공개키 y로 암호화된 암호문 $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$을 입력값으로 받아서, $m_0 = \alpha_0/\beta_0^x$, $m_1 = \alpha_1/\beta_1^x$을 각각 계산한다. 만약 $m_1 = 1$이라면 m_0을 출력하고, 그렇지 않으면 $FAIL$을 출력한다.



(그림 1) 믹스넷(Mixnet)

- **재암호화**(Re-encryption): 암호문 $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$와 랜덤 재암호화 요소 $r' = (k_0', k_1') \in Z_q^2$을 입력값으로 받는다. 암호문 $C' = [(\alpha_0', \beta_0'); (\alpha_1', \beta_1')] = [(\alpha_0\alpha_1^{k_0'}, \beta_0\beta_1^{k_0'}); (\alpha_1^{k_1'}, \beta_1^{k_1'})]$, $k_0, k_1 \in {}_UZ_q$ 이 출력값이다.

7. 기타 기술

앞에서 설명한 3가지 기법과 더불어 전자선거에 추가적으로 필요한 암호기술들은 다음과 같다.

7.1 영지식 증명(Zero-Knowledge Proofs)

영지식 증명이란 클라이언트와 서버 간의 절대적인 신뢰할 수 없는 상황에서 단지 자신의 정당한 신분만을 서버에게 밝히기를 원하는 경우에 사용되는 프로토콜이다. 영지식 증명은 이러한 목적으로 고안된 클라이언트와 서버 간의 대화형(interactive) 프로토콜로서 클라이언트의 비밀정보를 서버에게 직접적으로 제공함이 없이 클라이언트가 단지 그 비밀정보를 실제로 알고 있다는 사실만을 서버에게 확신시켜 주는 정교한 프로토콜이다.

7.2 Designated-Verifier Proofs

Jakobsson[10]이 제안한 Designated-verifier proofs란 지정된 검증자만이 어떤 증명에 대해 확신하고, 다른 개체는 이 증명을 보고 확신을 가질 수 없음을 뜻하는 증명방법이다.

전자선거 시스템에서 전자선거 시스템의 매표방지와 전체검증을 만족하기 위해 영지식 증명과 함께 designated-verifier proofs를 사용하여 자신이 투표한 값을 밝히지는 않으면서 정당하게 투표하였는지를 증명한다. 투표자는 선거관리위원회를 지정해 자신의 투표가 올바른지를 증명할 수 있고, 매표행위를 하고자 하는 후보

자에게는 거짓 증명을 할 수 있게 된다. 따라서 후보자는 투표자의 표를 믿지 못하게 되고 매표 행위는 이루어지지 않게 된다.

7.3 비밀 분산(Secret Sharing)

Shamir[19]가 처음 제안한 secret sharing은 어떤 비밀값 s를 n개의 기관이 나누어 보관하는 것을 말한다. Threshold t값을 사용하여 t개 이하의 기관이 모였을 경우 s값을 얻을 수는 없지만, $t+1$개 이상의 기관이 모일 경우 s값을 유일하게 복원할 수 있다($0 < t < n$).

비밀값 s를 분산하는 방법은 다음과 같다.

- 랜덤값 $a_1, \cdots, a_t \in Z_p$ 를 선택하고 이를 이용해 $f(x) = s + a_1 x + a_2 x^2 + \cdots + a_t x^t$ 을 생성한다.
- $s_i = f(i) \bmod p$ for $i = 1, \cdots, n$. s_i를 n개의 기관이 나누어 보관한다.

$t+1$개의 기관이 모일 경우 유일하게 $f(x)$를 복원할 수 있으므로 비밀값 s를 얻을 수 있다.

전자선거 시스템의 완전성과 건전성을 만족하기 위해서 선거관리위원회의 권한을 분산할 필요가 있다. 하나의 선거관리위원회가 투표와 개표의 모든 과정을 총괄할 경우, 부정행위가 발생할 가능성이 있기 때문이다. 따라서 투표와 개표에 관련된 중요한 비밀정보를 여러 기관에 분산해 놓고, 개표과정에서 여러 기관이 모여 개표를 한다면 부정행위의 가능성을 없앨 수 있다.

8. 결 론

안전한 전자선거 시스템을 구축하기 위해서는 여러 보안기술들의 융합이 필요하다. 그리고 종이영수증 문제, 매표방지 문제 등 현재 이슈가 되고 있는 여러 사항들 또한 해결되어야 하겠다. 앞에서 설명한 여러 암호 기술들이 적절하게 융합되어 한 치의 틈도 없는 안전성일 보일 때, 전자선거는 시행될 수 있을 것이다.

참고문헌

[1] Masayuki Abe. Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers. In EUROCRYPT'98, LNCS 1403, pp.437-447, 1998.

[2] Alessandro Acquisti, Receipt-Free Homomorphic Elections and Write-in Ballots.

[3] J. Benaloh and D. Tuinstra, Receipt-free Secret-ballot Elections

[4] Dan Boneh, and Philippe Golle. Almost Entirely Correct Mixing With Applications to Voting. ACM CCS'02, 2002

[5] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2) : 84-88, 1981

[6] David Chaum. Blind signatures for untraceable payments. In Advances in Cryptology-Crypto'82, pp.199-203. Plenum Press, 1983

[7] Atshushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. A practical secret voting scheme for large scale elections. In Auscrypt'92, pp.244-251. Springer-Verlag, LNCS 718, 1992.

[8] Philippe Golle, Markus Jakobsson, Ari Juels, and Paul Syverson. Universal Re-encryption for Mixnets.

[9] Markus Jakobsson, Ari Juels, and Ronald L. Rivest. Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking. 2002.

[10] M. Jakobsson, K. Sako, and R. Impag-

liazzo. Designated Verifier Proofs and Their Applications. Advances in Cryptography-EUROCRYPT'96, LNCS 1070, pp.143-154, 1996.

[11] Aggelos Kiayias, and Moti Yung. The Vector-Ballot E-Voting Approach.

[12] Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, Jeongmo Yang, and Seungjae Yoo. Providing Receipt-Freeness in Mixnet-Based Voting Protocols. ICISC2003, LNCS 2971, pp.245-258, 2004.

[13] Byoungcheon Lee and Kwangjo Kim. Receipt-free electronic voting scheme with a tamper-resistant randomizer. In ICISC2002, pp.405-422, 2002.

[14] M. Ohkubo, F. Miura, M. Abe, A. Fujioka and T. Okamoto An Improvement on a Practical Secret Voting Scheme.

[15] Tatsuaki Okamoto. Receipt-free electronic voting schemes for large scale elections. In Security Protocols Workshop, pp.25-35. Springer-Verlag, LNCS 1361, 1997.

[16] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In J. Stern, editor, EUROCRYPT '99, pp.223-238. Springer-Verlag, LNCS 1592, 1999.

[17] Kun Peng, Riza Aditya, Colin Boyd, Ed Dawson, and Byoungcheon Lee. Multiplicative Homomorphic E-Voting. INDOCRYPT 2004, LNCS 3348, pp.61-72, 2004.

[18] K. Sako and J. Kilian, Receipt-free Mix-Type Voting Scheme, In EUROCRYPT'95, pp.393-403. Springer-Verlag, LNCS 921, 1995.

[19] Adi Shamir. How to share a secret. Communications of the ACM, 22 : 612-613, 1979.

[20] www.rsasecurity.com

[21] 이래, 이동훈 서비스 현실화에 중점을 둔 인터넷 전자 투표 시스템, 정보보호학회지, 2004.

저자약력

김 건 욱

2004년 고려대학교 수학과, 컴퓨터학과(학사)
2004년~현재 고려대학교 정보보호대학원 석사과정
관심분야 : 정보보호, 암호응용, 프로토콜, 전자선거

홍 종 욱

2003년 한양대학교 수학과(학사)
2004년~현재 고려대학교 정보보호대학원 석사과정
관심분야 : 정보보호, 암호응용, 프로토콜, 전자선거

변 진 욱

2001년 고려대학교 전산학과 졸업
2003년 고려대학교 정보보호대학원 석사 졸업
2003년~현재 고려대학교 정보보호대학원 박사 과정
관심분야 : 암호학, 응용 프로토콜, 키 교환, 프라이버시, DB 보안, 전자선거

구 재 형

2000년 고려대학교 전산학과 졸업
2002년 고려대학교 정보보호대학원 석사 졸업
2002년~현재 고려대학교 정보보호대학원 박사 과정
관심분야 : 암호학, 응용 프로토콜, 키 교환, 프라이버시, DB 보안, 전자선거

이 동 훈

1983년 고려대학교 경제학사
1987년 Oklahoma University 전산학 석사
1992년 Oklahoma University 전산학 박사
1992년 단국대학교 전자계산학과 전임강사
1993년~1997년 고려대학교 전산학과 조교수
1997년~2001년 고려대학교 전산학과 부교수
2001년~현재 고려대학교 정보보호대학원 교수
관심분야 : 정보보호, 암호이론, 프로토콜, 정보이론