특집

인터넷 전자선거에서의 정보보호 기술동향

김건욱, 이동훈 (고려대학교)

I. 서 론

정보통신 기술의 발달과 유권자들의 의식 변화로 인해 최근 전자선거에 대한 관심이 높아지고 있다. 특히 인터넷을 이용한 인터넷 전자선거는 그 편리함과 유용성으로 인해 많은 연구가 이루어지고 있는 실정이다. 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 안정성을 요구하게 된다.

2008년에는 키오스크 방식의 전자선거를, 2012년부터는 인터넷 전자선거를 시행하겠다는 중앙선거관리위원회의 로드맵 발표로 인해 전자선거의 현실화에 대한 많은 관심이 쏟아지고 있다. 이미 세계 여러 나라에서는 전자선거를 시범서비스 중이고, 인터넷을 통한 전자선거에 대한 연구도 활발히 이루어지고 있다.

본고에서는 인터넷 전자선거를 위해 선결되어야 할 과제인 정보보호 기술 동향에 대해 살펴보고자 한다. 제 Ⅱ절에서는 인터넷 전자선거 시스템이 갖추어야 할 보안 요구사항에 대해 알아보고, 제 Ⅲ절에서는 인터넷 전자선거에 필요한 암호학적 기법들에 대해 간단히 소개한다. 제 Ⅳ절에서는 현재까지 제안된 여러 전자선거 기법들에 대해 살펴보고, 마지막으로 제 Ⅴ절에서 결론을 내린다.

II. 전자선거의 보안 요구사항

인터넷 전자선거는 투표와 관련된 일련의 과정들이 공정하고 안전하게 유지되도록 여러 가지 암호기법을 사용해서 이루어진다. 안전한 전자선거 시스템이 갖추어야 할 요구사항은 다음과 같다.[1,2,3,4]

• 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 누구나 투표 결과를 검증할 수 있는 전체검증(Universal Verifiability)이 있다.

• 매표방지(Receipt-free)

투표가 종료된 후, 투표자는 자신 이외에 다른 사람에게 자신의 투표 내용을 증명하는 것이 불가능해야 한다. 즉, 투표값을 매수, 매도하는 행위는 차단되어야 한다.

III. 암호학적 기법

전자선거를 위해서는 투표 과정에 대한 모든 메시지가 안전하게 전송되어야 한다. 만약 투표자에 의해 전송되는 투표값이 공격자에게 노출되었을 경우 익명성이 훼손됨은 물론 부정투표의 가능성도 일어나기 때문이다. 본 절에서는 암호학에서 사용되는 기본적인 기법에 대해 살펴본다.

1. 대칭키 암호시스템

대칭키 암호시스템이란 송신자와 수신자만이 알고 있는 동일한 대칭키를 이용하여 메시지를 암호화하고 복호화를 할 수 있는 시스템이다. 암호화를 위해서 송신자가 보유하고 있는 키와 복호화를 위해서 수신자가 가지고 있는 키가 동일하기 때문에 대칭형 암호시스템(Symmetric Cryptosystem)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 미국 연방정부 FIPS 46과 81에 정의된 DES(Data

Encryption Standard)와 2001년 FIPS 197로 제정된 AES(Advanced Encryption Standard)가 있다. 우리나라에서는 1999년 TTA에서 발표한 SEED와 2004년 KS표준으로 제정된 ARIA라는 대칭키 암호시스템을 만들어 사용하고 있다.

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 전자 서명과 같은 새로운 개념의 출현을 가능하게 하였다. 공개키 암호시스템은 암호화와 복호화에 사용되는 키가 서로 다르기 때문에 비대칭형 암호시스템(Asymmetric Cryptosystem)이라고도 부른다.

1) RSA 암호시스템

1978년 Rivest, Sharmir, Adleman에 의해서 제안된 암호시스템으로써, 현재 가장 널리 쓰이고 있는 공개키 암호시스템이다. RSA 암호시스템은 소인수분해(Factoring)의 어려움에 기반을 하고 있다.

$n = p\,q$(p, q: 2보다 큰 소수)
$ed \equiv 1 \bmod \phi(n)$, $\phi(n)$: 오일러 함수
공개키 : n, e
개인키 : d
메시지 : x
암호화 : $E_K(x) = x^e \bmod n$
복호화 : $D_K(y) = y^d \bmod n$

〈RSA 암호시스템〉

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 g, y, p를 알고 있어도 x를 구하는 것은 매우 어려운 문제라는 것이다.

$y \equiv g^a \bmod p$, p: 소수
공개키 : g, y, p
개인키 : a

암호화 : $E_K(m, r) = (C_1, C_2)$
메시지 : m, r: 임의의 값

$C_1 = g^r \bmod p$
$C_2 = y^r\, m \bmod p$

복호화 : $D_K(C_1, C_2) = C_2\, C_1^{-a} \bmod p$

〈ElGamal 암호시스템〉

현재 가장 널리 쓰이고 있는 공개키 암호시스템은 RSA 암호시스템이지만, 전자선거 기법에서는 ElGamal 암호시스템을 주로 사

용한다. 그 이유는 ElGamal 암호시스템에는 준동형 성질, 재암호화 성질 등 여러 유용한 성질들이 있기 때문이다. 자세한 내용은 Ⅳ 절에서 다루도록 하겠다.

3. 전자서명(Digital Signature)

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 서명자이외의 제3자에 의한 서명 위조는 일반적으로 불가능하고 또한 서명자가 나중에 자신이 서명한 내용을 부인할 수 없다는 것이다.

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 확인이나 투표자에 대한 인증, 투표자의 부인방지 등에 사용한다.

가장 널리 사용되는 RSA 서명기법은 다음과 같다. 파라미터의 구성은 RSA 암호시스템과 동일하다.

서명 : $Sig_K(x) = x^d \bmod n$
검증 : $Ver_K(y) = y^e \bmod n$

〈RSA 서명기법〉

4. 해쉬 함수(Hash Function)

메시지에 대한 무결성이 요구되어질 경우에는 해쉬값(Hash Value)을 메시지로부터 압축, 생성하여 메시지에 첨가하여야 한다. 또한, 그 메시지의 작성자에 대한 확인(Message Authentication)이 필요한 경우에는 해쉬값를 생성하는 과정에 메시지 작성자와 수신자만이 알고있는 비밀키가 포함되어져야 한다. 해쉬값를 생성하는 데에 사용되는 함수를 암호학적 해쉬 함수(Cryptographic Hash Function)라고 한다. 이 해쉬값를 통해서 수신자는 메시지에 대한 무결성 및 메시지를 보낸 작성자에 대한 확인을 할 수 있게 된다. 현재 미국 NIST에 의해 개발된 160 비트 길이의 SHA-1(Secure Hash Algorithm)이 여러 분야에 걸쳐 폭넓게 사용되고 있다.

Ⅳ. 전자선거 기법

전자선거에 사용되는 기법으로는 크게 3가지가 있다. 은닉서명을 이용한 기법[1], 준동형 암호화 기법[2], 믹스넷을 사용한 기법[3] 등이다. 각각의 전자선거 기법과 그 외에 사용되는 여러 암호화 기법들을 살펴보고, 이 기법들이 전자선거에 어떻게 사용되는지 알아본다.

1. 은닉 서명

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

A는 임의의 값 r을 선택한 후 다음을 계산하여 B에게 보낸다.
(n, e): B의 공개키, d: B의 개인키

$$x = r^e m \bmod n$$

B는 x값을 받더라도, r의 영향으로 m에 대한 어떠한 정보도 얻을 수 없다. B는 다음을 계산하여 A에게 보낸다.

$$x^d \bmod n$$

A는 다음을 계산하여 메시지에 대한 B의 서명을 얻게 된다.

$$r^{-1}x^d = r^{-1}(r^e m)^d = r^{-1} r m^d = m^d \bmod n$$

〈RSA 은닉서명기법〉

은닉서명을 사용한 전자선거 기법은 가장 간단하고 효율적이다. 첫 번째로, 투표자는 인증기관에 접속해 자신이 정당한 유권자임을 검증받는다. 두 번째로, 인증기관은 정당한 투표자에게 은닉된 투표값을 받고, 그 값에 서명을 하여 다시 재전송한다. 세 번째로, 투표자는 은닉서명기법을 이용해 투표값에 대한 인증기관의 서명값을 얻어낸다. 마지막으로, 투표자는 서명된 투표값을 개표기관으로 전송한다.

그러나 은닉서명을 사용한 전자선거 기법은 익명채널(Anonymous Channel)이 필요하다는 단점이 있다. 마지막 단계에서 어떤 투표자가 투표값을 행사하였는지에 대한 정보를 개표기관이 알 수 없어야 하기 때문이다. 만약 익명채널이 존재하지 않는다면 개표 시 투표자의 투표값을 각각 복호화 하기 때문에 투표자의 익명성이 지켜지지 못하는 결과가 나타나게 된다.

2. 준동형 암호화

준동형 암호화 기법이란 암호화하기 전의 값을 연산을 한 후 암호화 한 값과 암호화한 각각의 값을 연산을 한 값이 같다는 성질을 이용한 것이다.

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

E( ): 준동형 암호화 알고리즘
m_1, m_2 : 임의의 메시지

〈RSA 은닉서명기법〉

은닉서명이나 믹스넷을 사용한 전자선거 기법은 개표 단계에서 투표값을 하나씩 복호화 하는 방법을 사용한다. 그러나 준동형 성질을 이용하면 개표 단계에서는 투표값들을 다 연산을 한 후, 한 번의 복호화 작업으로 모든 투표값을 집계할 수 있게 된다. 따라서 익명채널이 없더라도 투표자의 익명성은 보장된다. 또한 각각의 투표값을 복호화하는 것보다 계산량이 줄어들게 되므로 개표 단계에서는 다른 기법들보다 효율적이다.

그러나 준동형 암호화 기법에서는 투표자가 자신의 투표가 정당한 투표임을 증명해야 한다. 만약 한명의 투표자가 악의적인 오류표를 행사하였을 경우, 개표 단계에서 전체 투표값을 연산하기 때문에 전체 투표 시스템이 무효화 될 가능성이 있기 때문이다. 또한 후보자가 많을 경우 각각 값들을 연산하여 집계하는 과정이 복잡해지므로 준동형 암호화 기법을 사용하였을 때의 장점은 사라지게 된다.

준동형 성질을 이용한 기법은 ElGamal 암호시스템을 기반으로 하여 많이 이용하였는데, 최근에는 다차잉여 문제의 어려움에 기반한 Paillier 암호시스템[5] 또한 많이 응용되고 있다.

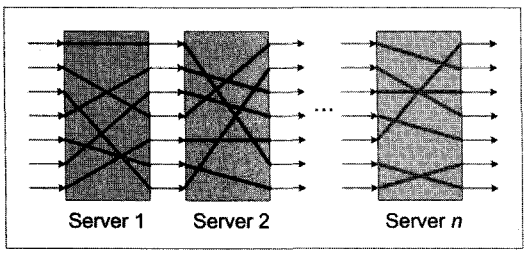
3. 믹스넷

1981년 Chaum이 처음 도입한 믹스넷[7]은 전자 메일과 전자선거에서 익명성을 보장하기 위한 것이었다.

믹스넷은 일련의 서버들을 필요로 하는데, 각 서버는 한 묶음의 메시지를 입력 받아서 그 묶음의 메시지 순서를 재배치하여 그 결과를 출력한다. 이런 믹스넷을 Shuffle Network라고도 한다.

Chaum이 원래 제안했던 것은 믹스넷의 각 서버들이 각각의 공개키, 비밀키 쌍을 갖고 있다. 한 묶음의 메시지가 각 서버를 통과할 때 해당 서버의 공개키로 암호화되어 입력되고 서버 내에서 순서가 재배치된 후 출력된다. 출력된 후 복호화되고 다시 다음서버에 통과하기 위해 그 서버의 공개키로 암호화된다. 이런 과정을 반복 시행하여 한 묶음의 메시지는 완전히 재배치될 수 있다.

믹스넷의 실행과정에서 각각의 믹스 서버는 올바르게 섞는 과정이 수행되었다는 것을 증명해야 한다. 이는 하나의 믹스서버가 공격하여 아무도 모르게 투표값을 바꾸는 것에 대비하기 위해서이다. 그러나 이 증명을 통해 입력값과 출력값에 대한 어떠한 정보도 알려지면 안된다.



〈믹스넷〉

1) 복호화 믹스넷

믹스서버 : $M_1, M_2, \ldots, M_n$
믹스서버 M_i의 공개키 : pk_i

1. 투표자는 각각 믹스서버의 공개키로 자신의 투표값을 암호화한다.
   $E_{pk1}(E_{pk2}(\ldots E_{pkn}\{\}(m)))$
2. 투표자는 암호화한 값을 첫 번째 믹스서버에 보낸다.
3. 값을 받은 믹스서버는 그 값을 복호화한 후 순서를 섞은 후 다음 서버에 보낸다.
4. n개의 믹스서버를 거치면 최종 믹스서버는 m값을 얻을 수 있게 된다.

〈복호화 믹스넷(Decryption Mixnet)〉

전자선거 시스템에서 믹스넷을 사용하면 투표값을 보고 어떤 투표자가 투표하였는지 알 수 없게 되어 익명성이 보장된다.

2) 재암호화 믹스넷

재암호화 믹스넷(Re-encryption Mixnet)에 각각의 믹스 서버는 복호화 믹스넷과는 다르게, 복호화 과정을 하는 대신 재암호화 과정을 수행한다. 이때 ElGamal 암호 시스템이나 Paillier 암호 시스템 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, $s \in {}_R Z^*_p$)

〈ElGamal의 재암호화 과정〉

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.

3) 전체 재암호화

재암호화 믹스넷이 암호문을 암호화 하는데 쓰인 공개키를 알아야 하는 단점이 있다면 전체 재암호화(Universal Re-encryption)[8]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 전체 암호시스템은 다음과 같다.

· 키 생성
$(PK, SK) = (y=g^x, x),\ x \in {}_U Z_q$

· 암호화
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.

· 복호화
y로 암호화된 암호문 $C=[(\alpha_0, \beta_0);(\alpha_1, \beta_1)]$을 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.

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

〈전체 재암호화〉

믹스넷의 믹스서버들이 전체 재암호화 방식을 사용할 경우, 각각의 믹스 서버들은 최종 믹스서버의 공개키를 알지 못하더라도 입력값에 대한 재암호화 출력값을 출력할 수 있게 된다. 이는 공개키를 얻을 때 요구되는 인증 등의 부하들이 없어짐을 뜻하므로, 믹스넷을 좀 더 효율적으로 운영할 수 있게 된다.

4) 비밀 분산 기법

Shamir가 처음 제안한 비밀 분산 기법(Secret Sharing)[9]은 어떤 비밀값 s를 n개의 기관에서 나누어 보관하는 것이다. Threshold

t값을 사용하여 t개 이하의 기관이 모였을 때는 s값을 얻을 수는 없지만, t+1개 이상의 기관이 모일 경우 Lagrange interpolation formula를 이용해 s값을 유일하게 복원할 수 있다. 비밀값 s를 분산하는 방법은 다음과 같다.

1. 임의의 $a_1,\cdots,a\in Z_p$를 선택하고 이를 이용해 $f(x)=s+a_1x+a_2x^2+$ CDOTS $+a_tx^t$을 생성한다.
2. $s_i=f(i)$ mod p, $i=1,\cdots,n$. s_i를 n개의 기관이 나누어 보관한다.
   t+1개의 기관이 모일 경우 유일하게 $f(x)$를 복원할 수 있으므로 비밀값 s를 얻을 수 있다.

〈비밀 분산 기법〉

안전한 전자선거를 위해서는 선거관리위원회의 권한을 분산할 필요가 있다. 하나의 선거관리위원회가 투표와 개표의 모든 과정을 총괄할 경우, 부정행위가 발생할 가능성이 있기 때문이다. 따라서 투표자가 투표값을 암호화 할 때 쓰이는 공개키의 대응하는 개인키는 하나의 기관이 소유할 것이 아니라, 여러 기관에 분산되어 보관되어야 한다. (t, n)-threshold 기법을 사용해 n개의 기관에 비밀키를 분산하고, 개표 과정에서 t+1개 이상의 기관이 모여 개표작업을 할 경우, 부정행위의 가능성은 현저히 줄거들게 된다.

V. 결론

이상과 같이 인터넷 전자선거에 필요한 암호화 기법과 3가지의 전자선거 기법에 대해 살펴보았다. 그러나 안전한 전자선거를 위해서는 앞에서 살펴본 내용 외에 네트워크 보안, 데이터베이스 보안, 웹 보안 등 여러 보안 기술들과의 융합이 필요하다. 그리고 또한 재검표 문제, 종이영수증 문제, 매표방지 문제 등 현재 이슈화 되고 있는 여러 문제들도 해결되어야 한다.

현재 미국, 스위스, 영국 등 세계 여러 나라에서는 전자선거의 현실화를 위해 여러 노력을 하고 있다. 특히 한해에 여러 번의 투표가 이루어지는 스위스의 경우, 이미 예전부터 일반 국민들에게 우편투표를 실시했었고 일부 지역에서는 인터넷 전자선거를 성공적으로 치러내었다. 이는 우편투표를 통한 원격투표에 익숙해진 국민들이 인터넷 전자선거 또한 거부감 없이 받아들였기 때문이다.

우리나라의 경우 올해 3월 국회의원, 행정부서, 관련 연구기관, 학계, 시민단체 등 각계 인사들이 참여한 가운데 '전자선거추진협의회'를 공식 발족하였다. 과거 부정투표로 얼룩졌던 과거 때문에 우리나라에서는 아직 전자선거에 대한 불안감을 깨끗이 털어낼 수 없는 것이 사실이다. 전자선거에 대한 공학적인 연구뿐만 아니라, 사회 구성원 전체에 대한 합의가 이루어질 때 인터넷 전자투표는 시행될 수 있을 것이다.

참고 문헌

[1] A. Fujioka, T. Okamoto, and K. Ohta. "A practical secret voting scheme for large scale elections". In Auscrypt'92, pages 244-251. Springer-Verlag, LNCS 718, 1992.

[2] J. Benaloh and D. Tuinstra. "Receipt-free Secret-ballot Elections". Proc. of the 26th ACM Symp. on Theory of Computing, pp. 544-553, ACM Press, 1994.

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

[4] 정보처리학회지. 제 12권 제 4호. 2005. 7.

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

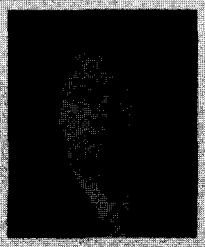
[6] David Chaum. "Blind signatures for untraceable payments". In Advances in Cryptology - Crypto'82, pages 199-203. Plenum Press, 1983.

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

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

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

저자소개



김 건 욱

2004년 고려대학교 수학과, 컴퓨터학과 학사
2004년 – 현재 고려대학교 정보보호대학원 석사과정
주관심 분야 보보호, 암호응용, 프로토콜, 전자선거, 웹 보안

이 동 훈

1992년 단국대학교 전자계산학과 전임강사
1993년 – 1997년 고려대학교 전산학과 조교수
1997년 – 2001년 고려대학교 전산학과 부교수
2001년 – 현재 고려대학교 정보보호대학원 교수
주관심 분야 정보보호, 암호이론, 프로토콜, 정보이론