情 報 保 護 學 會 誌
第 15 卷 第 5 號, 2005. 10

인터넷선거 정보보호기술 동향 연구

홍 종 욱*, 김 건 욱*, 이 동 훈**, 임 종 인***

요 약

중앙선거관리위원의 2012년부터 인터넷선거를 시행하겠다는 발표 후, 인터넷선거에 대한 관심이 증대하고 있다. 인터넷선거가 현재 사용되는 종이선거방식을 대체하기 위해서는 비밀성, 완전성등과 같은 기본적인 요구사항을 만족해야 하며, 선거를 전자적으로 구성하였을 때 발생할 수 있는 문제점 역시 정확하게 파악하고 해결해야 한다. 흔히 인터넷선거는 다양한 정보보호 기술이 사용되므로 정보보호 기술의 종합 예술이라고 불리운다. 본 논문에서는 인터넷선거에 사용되는 여러 정보보호 기법들을 살펴본다.

Ⅰ. 서 론

선거가 전자적으로 구성되면 무효표 방지, 투표율 제고, 빠른 집계 등 장점을 누릴 수 있지만, 해킹, 부정 투표, 악의적인 공격 등이 발생할 수 있다. 그러므로 인터넷선거 기법은 선거가 올바르게 진행되었는지 확인할 수 있도록 전체검증(Universal Verifiability)을 제공해야 한다. 또한 인터넷선거의 경우 발생하는 문제점으로 매표행위가 있다. 현재의 선거방식은 밀폐된 투표소를 사용하기 때문에 유권자가 어떤 후보자에게 투표하였는지 확인할 수 없어 표를 사고 파는 것이 어렵지만, 인터넷선거를 사용하면 선거에 사용된 모든 데이터를 유권자가 저장할 수 있고, 특정 후보자에게 투표했다는 것을 남길 수 있으므로, 이러한 증거를 구매자에게 제시하여 표를 팔 수 있게 된다. 매표행위를 방지하기 위해서는 유권자가 특정 후보자에게 투표했다는 증거를 남길 수 없거나, 유권자가 증거를 남길 수 있어도 구매자가 증거를 통해 유권자가 특정 후보자에게 투표했는지 확신할 수 없어야 한다. 그러므로 인터넷선거는 정보보호 기술의 종합예술이라고 불리울 만큼 여러 기술을 사용하며, 높은 수준의 안전성을 요구하게 된다.

본 논문에서는 안전하고 효율적인 인터넷선거를 위해 여러 암호학적 기술들에 대해 살펴본다. 약 20여년 전부터 연구되어 온 인터넷선거 관련 연구내용과 암호학적인 요구 사항, 암호학적 기법과 그 외에 필요한 기술들에 대해 알아본다.

Ⅱ. 관련 연구

인터넷선거에서 사용되는 암호화 기법은 크게 3가지 방법으로 분류될 수 있다. 믹스넷을 이용한 방법, 은닉서명을 이용한 방법, 준동형 암호화 기법을 이용한 것이다. 이 3가지 유형들은 각각 특별한 성질을 가지고 있다.

인터넷선거는 Chaum[5]의 믹스넷을 기반으로 한 기법을 시작으로 오늘날까지 다양한 기법으로 발전하였다. Chaum이 제안한 믹스넷 기법은 복호화 서버를 여러대 두어 복호화 하면서 순서를 섞는 기법이였지만, 후보자가 많은 선거에서는 효율성이 떨어져, 최근에는 재암호화 믹스넷 기법으로 분리함으로서 좀 더 유연성과 효율성에 중점을 두었다.

다른 접근 방법으로 Chaum[6]의 은닉서명 기법을 이용한 방법이 제안되었다. Benaloh[3]는 인터넷선거를 하면 투표자의 투표값이 남는다는 문제점을 발견하였다. 이후 Fujioka, Okamoto[7]가 제안된 기법은 이 단점을 보안하여 만든 것이였는데, 은닉서명 기법의 단점인 도청불가능 채널을 사용해야만 한다는 단점

* 고려대학교 정보보호대학원 석사과정 ({jwhong, aches}@cist.korea.ac.kr)
** 고려대학교 정보보호대학원 교수 (donghlee@korea.ac.kr)
*** 고려대학교 정보보호 대학원 원장 (jilim@korea.ac.kr)

이 있었다.

마지막으로 준동형 암호화 기법을 이용한 것인데, Benaloh와 Yung이 처음으로 준동형 암호를 이용한 방식을 제안하였다. 이 후 Cramer[20]가 제안한 방식은 좀 더 효율적이고 단순한 방식으로 이 분야가 커다란 발전을 이루게 되었다. 이후 [21]는 Cramer가 제안한 기법보다는 비효율적이지만 작은 위원회 정도의 선거에서는 보다 효율적인 방법이였다. 선거관리위원사이의 상호 작용은 초기단계에서 시스템을 셋업할 때 외에는 필요하지 않았기 때문이다.

이 후 매표방지에 대한 연구가 활발하게 이루어 졌는데 [13]의 결과는 유권자와 정직한 검증자의 협력으로 영수증이 필요 없는 성질을 만족하고 있다.

Ⅲ. 요구사항

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

1. 완전성(Completeness)
   모든 유효 투표는 정확하게 집계되어야 한다. 최종 집계에서 정당한 투표가 제거되는 일은 없어야 한다.
2. 건전성(Soundness)
   부정 투표자에 의해서 투표가 방해되거나 중지되어서는 안되며, 부정 투표가 집계되어 선거에 영향을 끼치지 않아야 한다.
3. 익명성(Privacy)
   투표 결과로부터 투표자를 구별할 수 없어야 한다.
4. 이중 투표 불가성(Uniqueness)
   정당한 투표자가 두 번 이상 투표할 수 없어야 한다.
5. 권한성(Eligibility)
   투표 권한을 가진 자만이 투표할 수 있어야 한다.
6. 공정성(Fairness)
   투표가 진행되는 동안에는 어떤 누구도 투표 결과에 대한 정보를 얻을 수 없어야 한다.
7. 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.
8. 매표방지(Receipt-Free)
   투표가 종료된 후, 투표자는 자신외에 다른 사람에게 자신의 투표 내용을 증명하는 것이 불가능해야 한다. 즉, 투표권을 매수, 매도하는 행위는 차단되어야 한다.

Ⅳ. 인터넷 투표 기법

인터넷선거에 사용되는 인터넷 투표 기법으로는 크게 3가지가 있다. 준동형 암호화 기법, 믹스넷을 사용한 기법, 은닉서명을 이용한 기법이다. 각각의 인터넷 투표 기법과 그 외에 사용되는 여러 암호화 기법들을 살펴보고, 이 기법들이 인터넷선거에 어떻게 사용되는지 알아본다.

4.1 준동형 암호화 기법(Homomorphic Encryption)

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 성질을 가지고 있는 함수
m_1, m_2 : 임의의 메시지

〈준동형 암호화 기법〉

준동형 성질을 이용하면 투표 종료 후 개표 단계에서는 투표 과정에서 암호화된 값들을 다 연산을 한 후, 한 번의 복호화 작업으로 모든 투표 값을 집계할 수 있게 된다. 준동형 성질을 이용하지 않는다면, 투표 과정에서 암호화된 값들을 모두 다 복호화 하여야 하므로 계산 량도 증가하게 된다. 또한, 각각 값들이 복호화 될 경우 어떤 유권자가 어떤 후보자를 선택하였는지 들어나기 때문에 준동형 성질을 이용하면 모든 값들이 다 합쳐져서 연산된 후에 복호화를 하므로 복호화 되어 진 값이 들어난다고 해서 어떤 선택을 하였는지 알 수 없게 된다. 준동형 성질을 이용한 기법은 ElGamal암호시스템을 기본으로 하여 많이 이용하였는데, 최근에는 Paillier[16] 암호시스템을 이용하는 추세이다.

4.1.1 Paillier 암호화 기법

$n = pq$ (p,q : 소수)

$g \in Z^*_{n^2}$

$\lambda(n) = lcm((q-1)(p-1))$

$S_n = u > n^2 | u = 1 \bmod n$

$L(u) = (u-1)/n$ 이라고 놓으면,

암호문 $c = g^m r^n \bmod n^2$ (r : 임의의 수)

복호화

$m = \dfrac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$ 이 된다.

〈Paillier 암호화 기법〉

이 암호화 기법은 다음과 같은 유용한 성질들을 제공한다.

재암호화하기 위해 임의의 수 r을 뽑는다.

$D(E(m)g^{nr} \bmod n^2) = m$

으로 만든다.

〈Self-Blinding Encryption〉

2개의 평문을 m_1, m_2라고 하면

$D(E(m_1)E(m_2) \bmod n^2) = m_1 + m_2 \bmod n$

$D(E(m_1)^m_2 \bmod n^2) = m_1 m_2 \bmod n$

〈준동형 암호화〉

준동형 암호화 기법을 이용한 인터넷투표는 찬반투표나 후보자가 적은 시스템에서 효율적으로 사용될 수 있다. 후보자가 많을 경우, 각각 값들을 연산하여 집계하는 과정이 복잡하여 지므로 준동형 암호화 기법을 이용하였을 때의 장점은 사라지게 된다.

4.2 믹스넷(Mix-net)

1981년 Chaum이 처음 도입한 믹스넷은 전자 메일과 인터넷선거에서 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 안 된다.

4.2.1 복호화 믹스넷(Decryption Mixnet)

믹스서버 : $M_1, M_2, \ldots M_n$

믹스서버 M_i의 공개키 : E_i

믹스서버 M_i의 개인키 : D_i

1. 투표자는 각각 믹스서버의 공개키로 자신의 투표값을 암호화한다. $E_1(E_2(\ldots E_n(m)))$
2. 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 m 값을 가지게 된다.

〈복호화 믹스넷〉

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

4.2.2 재암호화 믹스넷(Re-Encryption Mixnet)

재암호화 믹스넷에 각각의 믹스 서버는 복호화 믹스넷과는 다르게, 복호화 과정을 하는 대신 재암호화 과정을 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 보

장하기 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 재암호화한 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.

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

〈전체 재암호화〉

4.3 은닉서명(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.

1. B에게 서명을 받고자 하는 A는 임의의 숫자 r을 선택한 후 다음을 계산하여 B에게 보낸다. ((n, e)는 B의 공개키, d는 B의 개인키)
   $$x = r^e m \bmod n$$
2. B는 x값을 받더라도, r의 영향으로 m에 대한 어떠한 정보도 얻을 수 없다. B는
   $x^d \bmod n$을 계산하여 A에게 보낸다.
3. A는 다음을 계산하여 메시지에 대한 B의 서명을 얻게 된다.
   $$r^{-1} x^d = r^{-1} (r^e m)^d = r^{-1} r^{ed} m^d = r^{-1} r m^d = m^d \bmod n$$

〈은닉서명〉

은닉 서명을 사용한 인터넷선거 기법[7,14]은 가장 간단하고 효율적이나 익명 채널이 필요하다는 단점이 있다. 투표자는 인증기관으로부터 은닉 서명을 이용해 자신의 비밀 투표지에 서명을 받고, 비밀 투표를 개표기관에 전송한다. 정당한 투표자만이 서명을 받을 수 있기 때문에 인터넷선거의 권한성이 지켜지나, 익명성을 보장하기 위해서 투표자와 개표 기관 사이에 익명 채널이 형성되어야만 한다. 은닉 서명을 이용했을 경우 앞에서 설명한 준동형 암호화를 이용한 인터넷선거와 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.

4.4 기타 암호화 기법

앞에서 설명한 3가지 암호화 기법과 더불어 인터넷 선거에 필요한 암호화 기법은 다음과 같다.

4.4.1 상호증명(Interactive Proof)

인터넷선거에서는 영지식 증명을 이용하여 상호증명을 한다. 영지식 증명이란 클라이언트와 서버간의 절대적인 신뢰할 수 없는 상황에서 단지 자신의 신분만을 서버에게 밝히기를 원하는 경우에 사용된다.

인터넷선거 시스템의 매표방지와 전체검증을 만족하기 위해 영지식 증명을 사용하는데, 자신이 투표한 값을 밝히지는 않으면서 정당하게 투표하였는지 검증할 때 사용되는 방식이다. 그러나 영지식 증명을 사용하게 되면 계산량과 통신량이 증가하게 되는 단점도 있다.

4.4.1.1. L개중 1개에 대한 재암호화 증명 (Existence of a 1-out-of-L Re-encryption proof)

(X, Y)를 암호화한 값이 다음 암호문 $(X_1, Y_1), (X_2, Y_2), ..., (X_L, Y_L)$ 중에 있다는 것을 자신의 정보를 밝히지 않으면서 증명하는 방법이다.

(X, Y)를 암호화한 암호문을 (X_j, Y_j)라 하고, 암호화에 사용된 비밀키를 $\beta \in Z_q$라고 가정하면 $(X_j, Y_j) = (g^{\beta}X, y^{\beta}Y)$가 된다.

인터넷선거 시스템의 완전성과 건전성을 만족하기 위해 L개중 1개에 대한 재암호화 증명을 사용한다. 그 이유는 자신이 투표한 값을 다른 사람에게 보이지 않으면서 개표된 표들 중 포함되어 있는지 확인하기 위해서이다.

4.4.1.2. 지정된 검증자의 재암호화 증명 (Designated-Verifier Re-encryption Proofs)

지정된 검증자의 재암호화 증명(DVRP)이란 재암호화의 결과가 옳음을 정해진 검증자만이 확인할 수 있는 방법이다.

투표값 m에 대해 공개키 $h = g^s$를 이용해 암호화한 값을 $(x, y) = (g^{\alpha}, h^{\alpha}m)$라고 하고, 재암호화된 값

1. 증명자는 임의로 $d_1, d_2, \dots, d_L$와 $r_1, r_2, \dots, r_L$를 선택하고, 다음을 계산하여 확인자에게 전송한다.

$$a_i = (\frac{X_i}{X})^{d_i} g^{r_i},\ b_i = (\frac{Y_i}{Y})^{d_i} y^{r_i}$$

$i = j$인 경우를 제외한 모든 d_i와 r_i는 고정된다. $a_j = g^{\beta d_i + r_i}$이고, $b_j = y^{\beta d_i + r_i}$이므로 비밀값 β를 알고 있는 증명자는 나중에 d_j와 r_j를 변경할 수 있다.

2. 검증자는 임의의 값 $c \in Z_q$를 선택하여 증명자에게 전송한다.
3. 증명자는 $c = d_1 + d_2 + \dots + d_j' + \dots + d_L$가 되도록 d_j를 d_j'으로 변경하고, $\beta d_j + r_j = \beta d_j' + r_j'$이 되도록 r_j를 r_j'으로 변경한다. 그 후, $d_1, \dots, d_j', \dots, d_L$와 $r_1, \dots, r_j', \dots, r_L$를 확인자에게 전송한다.
4. 검증자는 다음을 검증한다.

$$c\,? = \sum d_i$$

$$a_i\,? = (\frac{X_i}{X})^{d_i} g^{r_i}\ (i = 1, 2, \dots, L)$$

$$b_i\,? = (\frac{Y_i}{Y})^{d_i} y^{r_i}\ (i = 1, 2, \dots, L)$$

〈L개중 1개에 대한 재암호화 증명〉

1. 증명자는 $k, r, t \in_R Z_q$ 를 선택한다.
2. $(a, b) = (g^k, h^k), d = g^r h_V^t$를 계산한다.
3. $c = H(a, b, d, x_f, y_f), u = k - \beta(c + r)$을 계산한다.
4. (c, r, t, u)를 검증자에게 보낸다.
5. 검증자는 다음값이 같은지 확인한다.

$$\tilde{c} = ?\ H(g^u (x_f/x)^{c+r}, h^u (y_f/y)^{c+r}, g^r h_V^t, x_f, y_f)$$

〈지정된.검증자의 재암호화 증명〉

을 $(x_f, y_f) = (xg^{\beta}, yh^{\beta}m)$이라고 하면,
지정된 검증자는 5번째 단계를 통하여 (x, y)의 재암호화 결과가 (x_f, y_f)가 된다는 것을 확신할 수 있다. 그러나 이 확신을 제3자에게 전이하는 것은 불가능하

다. 제3자에게는 거짓증명이 가능하기 때문이다. 거짓 증명의 과정은 다음과 같다.

1. 검증자는 $r'+s_V t'=r+s_V t$를 만족하는 임의의 r', t'을 선택한다.
2. 임의의 메시지 $(\tilde{x}, \tilde{y})$와 임의의 $(\tilde{\gamma}, \tilde{\delta}, \tilde{u})$를 선택한다.
3. 다음 각각의 값을 계산한다.
   $\tilde{r}=\tilde{\gamma}-\tilde{c}$, $\tilde{t}=(\tilde{\delta}-\tilde{t})/s_V$
4. 그러면 $(\tilde{c}, \tilde{r}, \tilde{t}, \tilde{u})$는 DVRP의 5번째 단계를 통과한다.

〈DVRP의 거짓증명〉

인터넷선거 시스템의 매표방지를 하기 위해 지정된 검증자의 재암호화 증명을 사용한다. 자신의 표가 집계되었다는 것은 확인하면서, 그 확인 결과를 제3자에게 증명할 수 없기 때문이다. 또한, (x,y)를 위조하여 $(\tilde{x}, \tilde{y})$를 만들어도 검증자를 쉽게 통과하게 되므로, 투표자는 제3자에게 임의의 표를 행사했다고 거짓증명을 할 수 있다. 따라서 표를 사는 사람은 투표자의 표에 대해 신뢰할 수 없으므로, 매표방지가 이루어진다.

4.4.1.3. 2개의 암호문이 같은 평문이라는 증명 (Proof of Knowledge that Two Ciphertexts are Encryption of the Same Plaintext)

Baudron[23]에서 제안된 영지식 증명을 사용한 이 기법은 하나의 평문이 두 개의 암호문으로 암호화 될 경우, 두 암호문이 같은 평문에서 암호화 되었다는 것을 복호화하지 않고 증명하는 것이다. 앞에서 설명한 Paillier 암호시스템을 이용하여 이 기법을 설명하면,

두 개의 암호문을

$f_V = g_V^m r_V^{n_V} \bmod n_V^2$

$f_C = g_C^m r_C^{n_C} \bmod n_C^2$

이라고 하면,

1. 증명자는 임의의 값 $\rho \in [0, 2^k]$, $s_C \in Z_{n_C^2}^*$를 뽑고, $u_C = g_C^{\rho} s_C^{n_C} \bmod n_C^2$ 을 계산한다.
   $u_V = g_V^{\rho} s_V^{n_V} \bmod n_V^2$
2. 확인자는 임의의 값 $d \in [o, A]$를 뽑아 확인자에게 보낸다.
3. 증명자는
   $z = \rho + cd$
   $w_C = s_C r_C^d \bmod n_C$
   $w_V = s_V r_V^d \bmod n_V$
   를 계산 후 확인자에게 보낸다.
4. 확인자는 $z \in [0, 2^k]$에서
   $g_C^z w_C^{n_C} = w_C f_C^d \bmod n_C^2$
   $g_V^z w_V^{n_V} = w_V f_V^d \bmod n_V^2$
   이 되는지 확인한다.

〈2개의 암호문이 같은 평문이라는 증명〉

이 된다. 위에서 본 것과 같이 두 개의암호문이 같은 평문을 암호화한 것인지 암호문을 복호화 해 보지 않고 알 수 있다.

4.4.2 비밀 분산(Secret Sharing)

Shamir[18]가 처음 제안한 비밀 분산 기법은 어떤 비밀값 s를 n개의 기관에서 나누어 보관하는 것이다. Threshold t값을 사용하여 t개 이하의 기관이 모였을 때만 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. 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.
2. $s_i = f(i) \bmod p$ 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.

〈비밀 분산 기법〉

이 외에 비밀 분산 기법에는 다항식을 이용한 Shamir의 기법을 t차원의 벡터공간으로 확장한 Vector Scheme과 CRT(Chinese Remainder Theorem)을 이용한 Asmuth와 Bloom의 기법이 있다. 또한 t차원의 열벡터를 사용한 Karnin, Greene, Hellman의

기법과 행렬을 이용한 Noar와 Shamir의 기법이 있다.

인터넷선거 시스템의 완전성과 건전성을 만족하기 위해서 중앙선거관리위원회의 권한을 분산할 필요가 있다. 하나의 선거관리위원회가 투표와 개표의 모든 과정을 총괄할 경우, 부정행위가 발생할 가능성이 있기 때문에 투표와 개표에 관련된 중요한 비밀정보를 여러기관에 분산해 놓고, 개표 과정에서 여러 기관이 모여 개표를 한다면 부정행위의 가능성을 줄일 수 있게 된다.

V. 결 론

인터넷선거를 시행하면 지금까지 선거에서의 문제점으로 지적되어 온 투표율제고 및 무효표를 방지할 수 있다. 인터넷선거를 현재 사용되고 있는 선거방식을 대체하여 보다 편리하고 공정한 선거를 만들고자 한다. 그러나 인터넷선거를 시행할 경우 보안적으로 현행 선거에 비해 보다 많은 문제점이 생겨날 수 있다. 지금까지 살펴본 기법들은 인터넷선거 시스템의 보안적인 문제점을 해결하고, 안전하게 구축하기 위해 필요한 암호화 기법들이다.

안전한 인터넷선거 시스템을 구축하기 위해서는 지금까지 살펴 본 여러 암호보안기술과 시스템적인 보안기술들의 융합이 필요하다. 또한 종이영수증 문제, 매표방지 문제, 재검표 문제 등 현재 이슈가 되고 있는 여러 사항들도 해결되어야 한다. 앞에서 설명한 여러 암호 보안기술들이 적절하게 융합되어 안전성일 보일 때, 인터넷선거는 시행될 수 있을 것이다.

참 고 문 헌

[1] Masayuki Abe., Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers. In EUROCRYPT'98, LNCS 1403, pages 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, pages 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, pages 244-251. Springer-Verlag, LNCS 718, 1992.

[8] Philippe Golle, Markus Jakobsson, Ari Juels, and Paul Syverson. Universal Reencryption 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. Impagliazzo. Designated Verifier Proofs and Their Applications. Advances in Cryptography - EUROCRYPT'96, LNCS 1070, pages 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, pages 245-258, 2004

[13] Byoungcheon Lee and Kwangjo Kim. Receipt-free electronic voting scheme with a tamper-resistant randomizer. In ICISC2002, pages 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, pages 25-35. Springer-Verlag, LNCS 1361, 1997.

[16] Pascal Paillier. Public-keycryptosystems based on composite degree residuosity classes. In J. Stern, editor, EUROCRYPT '99, pages 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, pages 61-72, 2004.
[18] K. Sako and J. Kilian, Receipt-free Mix-Type Voting Scheme, In EUROCRYPT '95, pages 393-403. Springer-Verlag, LNCS 921, 1995
[19] Adi Shamir. How to share a secret. Communications of the ACM, 22 : 612-613, 1979
[20] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers, A Secure and optimally efficient multi-authoruty election scheme EUROCRYPT, 1997
[21] Berry Scheonmakers, A simple publicly verifiable secret sharing scheme and its application to electronic voting, CRYPTO, 148-164, 1999
[22] www.rsasecurity.com
[23] Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Guillaume Poupard, and Jacques Stern. Practical multi-candidate election system. PODC '01 274-283. ACM, 2001

〈著 者 紹 介〉

홍 종 욱
2003년 2월 : 한양대학교 수학과 (학사)
2004년 9월~현재 : 고려대학교 정보보호대학원 석사과정
관심분야 : 정보보호, 암호응용, 프로토콜, 인터넷선거

김 건 욱
2004년 2월 : 고려대학교 수학과, 컴퓨터학과(학사)
2004년 3월-현재 : 고려대학교 정보보호대학원 석사과정
관심분야 : 정보보호, 암호응용, 프로토콜, 인터넷선거

이 동 훈
1983년 : 고려대학교 경제학사
1987년 : Oklahoma 대학 전산학 석사
1992년 : Oklahoma 대학 전산학 박사
1993년~2001년 : 고려대학교 전산학과 부교수
2001년 2월-현재 : 고려대학교 정보보호대학원 교수
관심분야 : 정보보호, 암호이론, 프로토콜, 정보이론

임 종 인
1980년 : 고려대학교 수학과 졸업
1982년 : 고려대학교 수학과 석사
1986년 : 고려대학교 수학과 박사
1986년~현재 : 고려대학교 수학과 교수 2000년~현재 : 고려대학교 정보보호 대학원 원장
관심분야 : 정보보호, 암호이론, 프로토콜, 정보이론