투표-취소가 가능한 1-out-of-L 전자투표 시스템

정회원 양 형 규*, 안 영 화*

1-out-of-L Electronic Voting System with Ballot-Cancellation

HyungKyu Yang*, YounHwa An* *Regular Members*

요 약

최근 들어, 국내외에서는 투표용지 대신에 전자적 투표 장치를 이용하는 전자투표 시스템들을 개발하고 있으나 이러한 전자투표 시스템은 전자투표의 초기 단계로서 온라인 투표시스템은 아니다. 따라서 많은 암호학자들은 암호기술을 기반으로 하는 온라인 전자투표에 대한 연구를 하고 있다. 기존의 1-out-of-L 전자투표는 ElGamal 암호 기법을 기반으로 하고 있다. 본 논문에서는 계산복잡도를 줄이기 위해, r차 잉여암호를 이용하고, ElGamal 암호 기반의 1-out-of-L 전자투표의 계산복잡도와 제안한 1-out-of-L 전자투표의 계산복잡도를 비교 분석하였으며, 제안한 전자투표 방식이 보다 효율적임을 보여준다. 또한, 새로운 형태의1-out-of-L 전자투표의 투표-취소 기법을 제안한다. 기존의 전자투표 시스템들은 투표 후의 투표-취소 기법에 대해서 간과해 왔다. 본 논문에서는 제안한 투표-취소 기법을 위해, 기존의 r차 잉여암호의 준동형성을 확장한다. 확장된 준동형성은 프라이버시와 전체검증성을 유지하면서 투표를 취소할 수 있다.

Key Words : E-voting, Privacy, Security, Ballot-cancellation

ABSTRACT

In this paper, we present an electronic voting system based on cryptographic techniques. Recently, some countries have used e-voting systems using an electronic voting device instead of a voting sheet. These e-voting systems are the early stage which is not online voting. Many cryptographers have studied on-line e-voting systems based on cryptographic techniques. The existing 1-out-of-L e-voting systems are based on ElGamal cryptosystem. To reduce computational complexity, we use r-th residue encryption scheme and compare the computational complexity of our 1-out-of-L e-voting system with that of the 1-out-of-L e-voting system based on ElGamal cryptosystem. Moreover, we extend the proposed 1-out-of-L e-voting system to ballot-cancellation property. The existing e-voting systems had been overlooked the ballot-cancellation property. There is the reason that the ballot is cancelled according to an election law. For our e-voting system with ballot-cancellation property, we extend the homomorphic property based on r-th residue encryption. The extended homomorphic property is used to cancel votes with guaranteeing privacy and universal verifiability.

Ⅰ. 서 론

투표는 민주주의사회에서 가장 중요한 의사결정의 방식이다. 기존의 투표방식은 많은 인적, 시간적, 비용적인 손실을 야기 시키고 있다. 이러한 문제점을 개선하기 위해, 암호기술을 기반으로 하는 전자투표 시스템들이 제안되고 있다. 그러나, 제안된 전자투표의 방식은 대부분이 찬반 전자투표 (Yes-No

※ 본 논문은 2005년도 강남대학교 교내 연구비 지원에 의한 것임
* 강남대학교 컴퓨터미디어공학부 ({hkyang, yhan}@kangnam.ac.kr)
논문번호 : KICS2006-10-466, 접수일자 : 2006년 10월 24일, 최종논문접수일자 : 2007년 1월 12일

e-voting)이며 단지 몇몇 프로토콜만이 1-out-of-L 전자투표에 응용할 수 있다. 1-out-of-L 전자투표의 의미는 L개의 후보자 또는 안건에 대해 투표자는 하나만 선택할 수 있는 전자투표 방식이다. 실제로, 투표에서는 찬반 투표보다는 1-out-of-L 투표의 방식이 많이 필요하다. 기존의 1-out-of-L 전자투표는, 모두 ElGamal 암호를 이용하였으며 이는 ElGamal 암호가 준동형성을 만족하기 때문에 투표 집계의 계산에서 효율적으로 이용할 수 있기 때문이라 할 수 있다.

r차 잉여암호도 준동형성을 만족하지만, ElGamal 암호 기법보다 계산량이 많다고 알려져 있었다. 그러나, Yamaguchi[11]등은 r차 잉여암호를 찬반 전자투표에 활용하면서 r차 잉여암호의 계산량이 ElGmal 암호방식에 비해 효율이 떨어지지 않는 다는 것을 증명하였다.

따라서 본 논문에서는 r차 잉여암호를 1-out-of-L 전자투표에 응용하였으며, ElGamal 암호방식 기반의 1-out-of-L 전자투표의 계산량을 비교하였다.

기존에 제안된 전자투표 시스템들은 투표-취소(*Ballot-cancellation*)에 대한 문제들을 간과해 왔다. 많은 연구자들이 전자투표에서는 투표-취소의 문제가 발생하지 않을 것이라 주장하고 있으나, 각국의 선거법이나 전자투표 시스템에 따라 투표-취소 문제는 충분히 발생할 수 있다. 다음은 투표-취소 문제가 발생 할 수 있는 이유에 대해서 정리한 것이다.

경우 1. 투표권의 기준이 선거일일 때, 만약에 부재자가 투표를 한 후에, 선거일 전에 사망하거나 투표권을 손실한 경우에, 부재자의 투표는 취소되어야 한다 (일본의 선거법).

경우 2. 전자투표 시스템에서 다른 투표자에 의한 대리, 불법 투표가 발생할 수 있다.

경우 3. 투표진행 도중에 투표자가 투표를 포기할 때, 악의 있는 관리자에 의한 대리, 불법투표가 발생할 수 있다.

경우 1의 경우는 각 나라의 선거법에 의해 발생될 수 있는 문제라 할 수 있으며, 경우 2와 경우 3은 전자투표 시스템의 취약점에 의해 발생될 수 있는 문제라 할 수 있다. 실제로 경우 2와 경우 3과 같은 대리, 불법 투표를 막기 위해서 투표자는 자신의 투표의 유효성 증명(Proof of validity of the ballot)을 하고, 전자투표의 관리자(또는 시스템)는 암호화된 투표의 내용의 계산에 대한 유효성 증명(Proof of validity of encryption or decryption)을 하여야 한다. 그러나, 전자투표에서 투표-취소를 고려하지 않을 경우, 투표를 취소해야 할 경우가 발생할 시에는 전자투표 시스템 자체를 중단해야 하는 문제를 가지고 있다. 특히, 경우 3을 방지하기 위해서 몇몇의 전자투표 시스템[4, 7]이 제안되었으며, 이러한 시스템은 쓰레숄드 비밀분산 스킴(threshold secret sharing schemes)을 사용하고 있다. 그러나, 이러한 방식을 사용한 전자투표 시스템은 계산량이 다른 시스템 보다 비효율적이라 할 수 있다[11].

또한, 경우 1은 선거법의 투표권과 관련이 있다고 할 수 있으며, 투표권의 기준은 각 나라의 선거법에 따라 다르다 할 수 있다. 선거법의 투표권 기준은 크게 두 가지로 나눌 수 있으며, 그 기준은 투표하는 시점(한국의 경우)과 다른 하나는 선거일(일본의 경우)이다. 선거일이 투표권의 기준인 경우에는, 안전하고 공평한 부재자 전자투표를 위해서 투표-취소 기법이 반드시 필요하다. 현재 투표-취소 기법은 전자투표가 방식이 이미 도입되어 있는 일본의 전자투표 방식에서 유용하게 사용될 수 있을 것으로 기대되며, 향후 국내의 전자투표 방식 도입에 따른 문제점을 해소하기 위해서도 반드시 필요한 방식이라 할 수 있다.

2.1 전통적인 투표 방식 - 부재자 투표의 방식

본 절에서는 전통적인 투표 방식에 의한 일본의 부재자 투표 방식과 투표-취소의 방식을 설명한다. 부재자는 부재자 투표를 위해 미리 등록하여야 하며, 다음과 같은 절차를 따라야 한다.

(1) 부재자의 자격은 각 나라의 선거법에 따른다.
(2) 선거일 전에 부재자는 투표용지와 두 개의 봉투를 받는다.
(3) 부재자는 선거일 이전에 지정된 투표소에 가서, 투표를 하고, 첫 번째 봉투에 기표한 투표용지를 넣는다.
(4) 그리고, 두 번째 봉투에 첫 번째 봉투를 넣고, 자신의 서명을 한다.
(5) 부재자의 투표내용은 우체국에 의해, 해당 지역의 선거관리위원회로 배송된다.
(6) 선거일에 투표 종료 후에, 부재자의 투표권을 체크 한 후에, 부재자가 선거일 전에 사망했거나, 투표권을 상실한 경우에는, 선거관리위원회는 두 번째 봉투에 작성된 부재자의 서명을 보고, 부재자의 투표를 제외한다. 부재자의 투표

내용은 공개되지 않고, 그대로 파기시킨다.

그러나, 전통적인 투표 방식에 의한 부재자 투표에서는 다음과 같은 문제가 발생할 수 있다.

- 배송지연(Delivery delay): 우체국에 의해 선거 종료 후에 배송될 수 있다.
- 배송누락(Delivery omission): 부재자의 투표가 해당 선거구에 제대로 배송되지 않고, 누락될 수 있다.

또한, 안전한 투표-취소를 위해 아래와 같은 조건이 필요하다.

- 프라이버시(Privacy) : 투표가 취소될 때, 어느 누구도 투표의 내용은 알 수 없다.
- 전체 검증성(Universal Verifiability) : 투표의 취소가 정확하게 이루어졌는지를 모든 사람이 확인할 수 있어야 한다.

Ⅱ. 암호 기반 기술

본 장에서는 본 논문에서 제안하는 방식의 기반을 이루고 있는 암호기술들에 대하여 설명한다.

2.1 준동형성 (Homomorphic property)

Cohen과 Fischer [3]는 처음으로 전자투표에 준동형성(Homomorphic property)을 이용했다. 최근까지, 제안된 많은 전자투표 시스템[4,7,11]이 투표 집계의 계산량 감소와 전체 검증성(Universal Verifiability)을 위해서 준동형성을 이용하고 있다.

ξ를 확률적 암호 기술(Probabilistic encryption scheme)로 정의한다고 하자. M을 메세지 공간(message space), C를 암호 메세지 공간(ciphertext space)으로 가정하고, M은 $\oplus$의 연산 하에서 동작하는 그룹이고, C는 $\otimes$의 연산 하에서 동작하는 그룹으로 가정한다. $c_1 = E_{r_1}(m_1)$과 $c_2 = E_{r_2}(m_2)$가 있을 때, 아래의 식을 만족하는 r이 존재한다.

$$c_1 \otimes c_2 = E_r(m_1 \oplus m_2)$$

이때, ξ는 $(\oplus, \otimes)$의 준동형성을 만족한다고 하며, 준동형 암호기법(Homomorphic Encryption Scheme) 이라고 한다.

다음으로 먼저 r-차 잉여암호 (r-residue encryption)에 대하여 간단하게 정리하면,

비밀키(Secret key): 두 개의 큰 소수: p_T, q_T

공개키(Public key): $N_T(=p_T q_T), y_T$(y_T는 난수)

평문(Plaintext): $v_i (0 \le v_i \le r)$

암호화(Encryption): $Z_i = y_T^{v_i} x^r \bmod N_T$(x는 난수)

[r: 홀수]

$\gcd\ (p_T - 1, r) = e_1$

$\gcd\ (q_T - 1, r) = e_2$

$r = e_1 e_2$

$\gcd\ (e_1, e_2) = 1$

[r: 짝수]

$\gcd\ (p_T - 1, r) = e_1$

$\gcd\ (q_T - 1, r) = e_2$

$2r = e_1 e_2$

$\gcd\ (e_1, e_2) = 2$

복호화(Decryption)

$\bmod p_T$

$$Z_i^{(p_T-1)/e1} = (y_T^{v_i} x^r)^{p_T-1/e_1} = (y_T^{(p_T-1)/e1})^{v_i} (x^{r/e1})^{(p_T-1)} = (y_T^{(p_T-1)/e1})^{v_i}$$

$\bmod q_T$

$$Z_i^{(q_T-1)/e2} = (y_T^{v_i} x^r)^{q_T-1/e_2} = (y_T^{(q_T-1)/e2})^{v_i} (x^{r/e2})^{(q_T-1)} = (y_T^{(q_T-1)/e2})^{v_i}$$

$i, (1 < i < r)$를 선택하고, 아래의 수식과 비교한다.

$(y_T^{(p_T-1)/e_1})^i \bmod p_T$ 과 $(y_T^{(q_T-1)/e_2})^i \bmod q_T$

2.2 r차 잉여암호의 준동형성

r-차 잉여암호는 아래와 같은 준동형성을 만족한다.

$$E(m+n) = E(m)E(n)x^r \bmod N$$

예를 들어 $E(m)$과 $E(n)$을 아래와 같이 정의하고,

$$E(m) = y^m x^r \bmod N, \quad E(n) = y^n x^r \bmod N$$

이때,

$$E(m+n) = y^{m+n} x^r \bmod N,$$
$$E(m)E(n) = (y^m x^r \bmod N)(y^n x^r \bmod N) = y^{m+n} x^r \bmod N$$

그러므로, $E(m+n)=E(m)E(n)x^r \bmod N$이 성립한다.

2.3 r차 잉여암호의 준동형성의 확장

준동형성 확장에서 $E(m-n)$을 아래와 같이 정의할 수 있으며,

$$E(m-n)=\{E(m)/E(n)\}x^r \bmod N$$

여기서 $E(m)$과 $E(n)$을 아래와 같이 정의하면,

$$E(m)=y^m x^r \bmod N$$
$$E(n)=y^n x^r \bmod N,\ (m>n)$$

다음과 같은 수식이 정립하게 된다.

$$E(m-n)=y^{m-n}x^r \bmod N,$$
$$E(m)/E(n)=(y^m x^r \bmod N)/(y^n x^r \bmod N)$$
$$=y^{m-n}x^r \bmod N$$

그러므로, $E(m-n)=\{E(m)/E(n)\}x^r \bmod N$이 성립한다.

Ⅲ. 제안하는 1-out-of-L 전자투표

3.1 L possibilities의 비교

다음으로 L possibilities의 기법을 비교 설명하면, 앞에서 언급한 것과 같이 기존에 제안된 전자투표의 대부분은 찬반 전자투표 (Yes-No E-voting) 이었으며, 몇몇 개의 1-out-of-L 전자투표[4,10]가 제안되었다. 제안된 1-out-of-L 전자투표는 ElGamal 암호와 Publicly Verifiable Secret Shaing(PVSS)를 사용하였다. 1-out-of-L 전자투표에서는 투표자가 L개의 후보자(또는 안건) 중에서 하나를 선택했다는 것을 증명하여야 한다. 이 증명방법을 L possibilities 기법이라고 한다. 본 장에서는 ElGamal 암호기법에서의 L possibilities 기법과 우리가 사용하는 r차 잉여암호의 L possibilities 기법을 비교한다.

1) ElGamal 암호의 L possibilities

- 투표자 V_i 는 그의 투표 v_i를 투표내용의 집합 $\{M^0, M^1, \ldots, M^{L-1}\}$으로부터 선택한다. 여기에서, M은 투표자의 수이다.
- 그는 투표내용을 관리자의 수로 나누고, 나누어진 암호화된 투표내용의 조각 g^{s_i} 을 관리자들에게 분배하고, $U_i=g^{s_i+v_i}$을 공개한다.
- L possibilities 의 증명은 아래와 같다.

$$\log_G(GC_0)=\log_g U_i \vee \log_G(G^M C_0)$$
$$=\log_g U_i \ldots \vee \log_G(G^{M^{L-1}}C_0)=\log_g U_i$$

여기에서, $C_0=G^{S_i}$는 분배되어진 투표내용의 조각이다. 여기서 관리자들이 모여서 준동형성을 이용해서, $\sum v_i$을 계산하면, 원래의 투표 내용으로 복호화 할 수 있다.

2) r차 잉여 암호의 L possibilities

본 논문에서 제안하는 1-out-of-L전자투표를 위해서 r차 잉여암호를 위한 L possibilities를 아래와 같은 방법으로 제안한다.

- 투표자는 투표내용 m_i을 투표내용 $\{G_1, \ldots, G_L\}$의 집합으로부터 선택한다. 투표내용 $\{G_1, \ldots, G_L\}$은 N_2의 생성기에 의해 생성되었고, 범위는 $0 \le G_1, \ldots, G_L < r$이다.
- 생성된 투표내용은 r차 잉여암호에 의해 $Z_i=y^{m_i}x_i^r \bmod N_2$를 생성한다.
- 투표자는 자신이 선택한 투표내용이 $\{G_1, \ldots, G_L\}$중의 하나의 값이라는 것을 아래의 수식으로 증명한다.

$$\log_y(Z_i S/R)=\log_y(Z_1 S/R)\vee,\ldots,\vee\log_y(Z_L S/R)$$

이때, $S=s_i^r$, $R=X_i^r \bmod N_2$, $S_i(\in N_2)$는 난수이다.

- 투표자는 자신의 투표내용을 공개하지 않고, 그의 투표의 유효성을 표1의 방법에 의해서 증명할 수 있다.

표 1. 투표의 유효성 증명

Prover P		Verifier V
$C_i=G^{Z_i} \bmod p_0$ where $Z_i=y^{m_i}x_i^r \bmod N_2$		
$T\equiv y^{-m_i}t^r \bmod N_2$, $\tilde{T}=G^T \bmod p_0$, $W=TZ_i \bmod N_2$	t ← $\tilde{T}$, W →	$t\in_R Z_{N_2}^*$ $G^W \stackrel{?}{=} C_i\tilde{T}$

3.2 1-out-of-L 전자투표

표 2와 표 3은 본 논문에서 사용하는 notations과 게시판의 내용에 대하여 각각 정리한 것이다. 그리고 표4에서는 본 논문에서 제안하는 1-out-of-L 전자투표 방식을 정리한 것이다.

1-out-of-L 전자투표는 2개의 센터(Center1과 Center2)와 게시판(Bulletin Board)으로 구성되어 있으며, 투표-취소를 위해서 Cancellation-center를 정의한다. 각 센터의 역할은 다음과 같다.

Center1
- Center1은 투표 종료 후에, 투표자에 의해 이중 암호화된 투표내용을 첫 번째로 복호화 하고, 복호화된 투표내용의 곱을 다시 게시판에 송부한다.
- 투표자의 커미트먼트의 값과 자신에 의해 복호화된 커미트먼트의 값을 비교하여, 자신의 계산에 대한 유효성 증명을 한다.
- Center2에 의해 계산된 최종 투표집계의 유효성을 확인할 수 있다.

표 2. Notations

	서명을 위해	
	비밀키	공개키
투표자 r	$d_{v_i}, p_{v_i}, q_{v_i}$	$e_{v_i}, N_{v_i}(=p_{v_i}q_{v_i})$
Center1	$d_{C_1}, p_{C_1}, q_{C_1}$	$e_{C_1}, N_{C_1}(=p_{C_1}q_{C_1})$
Center2	$d_{C_2}, p_{C_2}, q_{C_2}$	$e_{C_2}, N_{C_2}(=p_{C_2}q_{C_2})$

	암호화/복호화를 위해	
	비밀키	공개키
투표자 r	$d'_{v_i}, p'_{v_i}, q'_{v_i}$	$e'_{v_i}, N'_{v_i}(=p'_{v_i}q'_{v_i})$
Center1	d_1, p_1, q_1	$e_1, N_1(=p_1q_1)$
Center2	p_2, q_2	$r, y, N_2(=p_2q_2)$ $(N_1>N_2)$

표 3. 게시판의 내용

Ballots		Commitment data for multiplication	Ballot-cancellation or not	Final tally in encrypted form		Finally tally	
Voter's own designated section A'	Accepted mark section B'	Center1's own designated section C'	CC's own designated section D'	Center1's own designated section E'	Valid mark section F'	Center2's own designated section G'	Valid mark section H'

Center2
- Center1에 의해 복호화된 투표내용을, 다시 복호화 하여, 최종 투표집계의 계산을 한다.
- 자신의 투표집계의 계산의 유효성은 Center1의 암호화된 투표내용의 곱을 이용해서 확인하여 비교할 수 있다.

Cancellation-center
- Cancellation-center는 투표내용의 암호화와 복호화, 계산 등에 관여하지 않고, 단지, 투표자의 투표권만을 확인하여, 발표한다.

Bulletin Board (게시판)

모든 사람이 게시판의 내용을 볼 수 있지만, 게시판의 내용을 삭제하거나, 변경할 수 없다. 단지, 게시판의 내용은, 해당 센터만이 해당 부분에 기입할 수 있다. 게시판은 유효성의 증명하기 위해, 계산된 값을 공개하거나, 투표-취소를 위해 투표권을 손실한 유권자를 표시하는데 사용된다.

3.3 최종 투표의 집계 계산

본 절에서는 ElGamal기반의 1-out-of-L 전자투표의 최종 투표 집계의 계산량과 제안하는 1-out-of-L 전자투표의 계산량을 비교한다. ElGamal기반의 1-out-of-L 전자투표의 최종 투표 집계의 계산방법은 아래와 같다[4].

$$W = G_1^{k_1} G_2^{k_2} \ldots G_L^{k_L}$$

W로부터 각 후보자의 득표값 $k_i (i=1, \ldots, L)$을 얻기 위해 아래와 같이 계산을 한다[5].

- $\sum_{i=1}^{L} k_i = m$, $m \le M$으로 가정한다. 이때, m은 실제로 투표를 한 투표자의 수이다.

- 아래의 수식으로부터 $k_1, \ldots, k_{L-1}$의 값을 계산한다.

$$W / G_L^m = (G_1/G_L)^{T_1} (G_2/G_L)^{T_2} \ldots (G_{L-1}/G_L)^{T_{L-1}}$$

- 득표값 $k_i (i=1, \ldots, L)$를 계산하기 위한 계산량은 $O(m^{L-1})$이다.

본 논문에서 제안하는 최종 집계의 계산방법은 아래와 같다.

$$W = k_1 G_1 + \ldots + k_L G_L$$

위의 수식에서 우리는 각 투표내용 $\{G_1, \ldots, G_L\}$의 상수를 계산하면, 각 후보자의 투표값을 계산할 수 있다. 이때의 계산량은 $O(M)$이다.

Ⅳ. 제안하는 1-out-of-L 전자투표를 위한 투표-취소 기법

4.1 투표-취소 기법

본 절에서는 3장에서 제안한 1-out-of-L전자투표의 투표-취소 기법에 대하여 설명한다. 본 논문에서는 투표-취소 기법을 위해서 2.3장에서 기존의 r차 잉여 암호의 준동형성을 확장하고, 1-out-of-L 전자투표에 활용하기 위해 투표의 유효성 증명(표1 참조)을 제안했다. 3장에서 제안한 1-out-of-L전자투표에서 투표-취소를 위해 별도의 Cancellation - center을 두고, 아래의 방법으로 투표를 취소한다.

- 투표가 종료된 후에, center 1은 전체 암호화된 투표값의 곱 (Z)과 취소되어야 할 암호화된 투표값의 곱 (Z_b)을 다음과 같이 계산한다.

$$Z = y^{M} x^{r} \bmod N_2, \quad M = k_1 G_1 + \ldots + k_L G_L$$

$$Z_b = y^{M_b} x^{r} \bmod N_2, \quad M_b = k_1{}' G_1 + \ldots + k_L{}' G_L$$

- Center1은 유효 투표값의 곱 Z_v을 아래와 같이

표 4. 1-out-of-L 전자투표

Phase 1. 투표자(V) 1-1. $Voting - list_{i=1}^{L} G_i$ 1-2. $V \leftarrow m_i (i = 1, \ldots, L)$ from the set $G_1, \ldots, G_L$	L 생성기 ($(0 \le G_1, \ldots, G_L \le r)$ 투표내용
1-3. $Z_i = y^{m_i} x_i^{r} \bmod N_2$ (by C_2의 공개키 y, N_2)	투표내용의 첫 번째 암호문
1-4. $E_i \equiv Z_i^{e_i} \bmod N_1$ (by C_1의 공개키 e_1, N_1)	투표내용의 두 번째 암호문
1-5. $C_i = G^{Z_i} \bmod p_0$	커미트먼트 데이터(Commitment data)
1-6. $V \rightarrow Verifier$(투표내용의 유효성 증명)	r차 잉여 암호로부터의 L possibilities
1-7. $(H_i)^{d_{v_i}} \bmod N_{v_i} \leftarrow H_i = hash(E_i, C_i, MSG_{v_i})$	투표자의 서명
1-8. $(ID_{v_i}, E_i, C_i, MSG_{v_i})^{d_{v_i}} \bmod N_{v_i} \rightarrow BB$	투표
Phase 2. Center1 (C_1) 2-1. $Z_i \equiv E_i^{d_i} \bmod N_1$	두 번째 암호문을 복호화
2-2. $G^{Z_i} \bmod p_0$을 계산한 후에, 투표자가 계산한 $G^{Z_i} \bmod p_0$와 비교한다.	암호화된 투표내용의 유효성 증명
2-3. $C_{(j,i)} = G^{Z_j, Z_i} \bmod p_0 \rightarrow BB$	Multiplication of the commitment data (Z_j : 앞서 계산한 커미트먼트의 곱, Z_i : 현재의 커미트먼트의 값)
2-4. $(c_j, c_i, c_{(j,i)}) \rightarrow BB$	커미트먼트의 값을 게시판에 송부
2-5. $(ID_{C_1}, Z, MSG_{C_1}, H_{v_i})^{d_{C_1}} \bmod N_{C_1} \rightarrow BB$	암호화된 투표내용의 값을 게시판에 송부
2-6. $Z = \Pi_{i=1}^{l} Z_i = y^{M} X^{r} \bmod N_2$, l은 전체 투표의 수	암호화된 투표내용의 값
Phase 3. Center2 (C_2) 3-1. Verify $(C_j, C_i, C_{(j,i)})$	Center1의 서명
3-2. $Z = \Pi_{i=1}^{l} Z_i = y^{M} X^{r} \bmod N_2$, $M = k_1 G_1 + k_2 G_2 + \ldots + k_L G_L$, $X = \Pi_{i=1}^{l} x_i$	암호화된 투표내용을 복호화
3-3. $M = k_1 G_1 + k_2 G_2 + \ldots + k_L G_L$, $k_i (i = 1, \ldots, L)$는 각 후보자의 득표수	최종 투표값을 계산(3.3장 참고)

계산할 수 있다.

$$Z_v = Z / Z_b$$

- Center2는 최종 유효 투표값 M_v를 아래와 같이 계산할 수 있다.

$$Z_v = y^{M_v} x^r \bmod N_2,\ M_v = k_1'' G_1 + \ldots + k_L'' G_L$$

이때,

$$M_v = M - M_b = (k_1 G_1 + \ldots + k_L G_L) - (k_1' G_1 + \wedge + k_L' G_L) = k_1'' G_1 + \ldots + k_L'' G_L$$

이다. 여기서 $k_i''\{i=0,\ldots,L\}$는 각 후보자가 얻은 유효 득표수이다.

4.2 안전성 분석

본 절에서는 본 논문에서 제안한 1-out-of-L 전자투표의 투표-취소 기법의 안전성을 분석한다.

Privacy

프라이버시를 위해 몇 가지의 프라이버시의 레벨이 제안되었으며, 정리하면 다음과 같다. [5].

- Privacy 1: 투표의 내용은 볼 수 있지만, 투표자를 추적할 수는 없다.
- Privacy 2: 실제 투표의 내용은 보는 것과 계산하는 것은 어렵지만, 투표자의 ID은 알 수 있다.
- Privacy 3: 투표자의 내용과 투표자의 ID는 알 수 있지만, 둘 사이의 관계를 알거나, 계산할 수는 없다.

본 논문에서 제안한 1-out-of-L 전자투표의 투표-취소 기법의 프라이버시는 privacy 2에 해당된다. 투표-취소를 위해서는 누군가는 투표의 내용과 투표자의 관계를 알고 있어야 한다. 본 논문에서 제안한 기법에서는 Cancellation-center가 본 역할을 담당한다. 그러나, Cancellation-center는 투표내용의 암호화에 사용된 Center 1과 Center 2의 비밀키를 모르기 때문에, 투표의 내용을 알 수는 없다. Cancellation-center는 단지 선거 종료 후에 부재자의 투표권만 체크하고, 투표권을 상실한 부재자만을 게시판에 공개한다.

Universal Verifiability

모든 사람이 투표권을 상실해서, 투표를 취소해야 하는 부재자에 대해 검증할 수 있어야 하고, 납득이 되어야 한다. 따라서, Cancellation-center에 의해 결정된 투표권의 상실자의 ID는 게시판에 공개되고, 그들의 투표값은 커미트먼트 데이터 C_i에 의해서 정확히 계산되었는 지를 판별할 수 있다.

V. 계산량 분석

본 논문에서는 Cramer[4]가 제안한 ElGamal 암호기반의 1-out-of-L 전자투표의 계산량과 본 논문에서 제안한1-out-of-L 전자투표의 계산량을 비교한다. 표 5는 두 개의 기법의 계산량을 보여준다.

표 5에서, l과 M은 유효투표자의 수와 후보자의 수를 각각 나타낸다. 본 논문에서 제안한 시스템에서는 r차 잉여암호를 사용하기 때문에, 난수 q는 투표자의 수 l보다 두 배 이상이라는 것을 가정한다. Cramer의 기법에서는 안전성의 비밀 파라미터 k때문에 l이 $q/2$보다 작다고 가정한다. 후보자의 수 M이 5와 10에서의 계산량에 대한 시뮬레이션의

표 5. 계산량 분석

	제안기법	Cramer의 기법[4]
암호화	$O(l)$	$O(l)$
복호화	$O(l)$ $MO(l)+O(l^{1/2})$	$O(l^{M-1})$
증명	$O(l)$	$O(l+M):(l>m)$
총 계산량	$(M+3)O(l)+O(l^{1/2})$	$2O(l)+O(l^{M-1})$

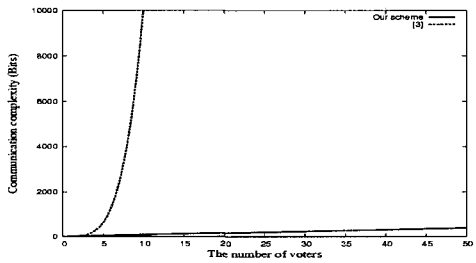

그림 1. M=5일 때의 계산량 비교

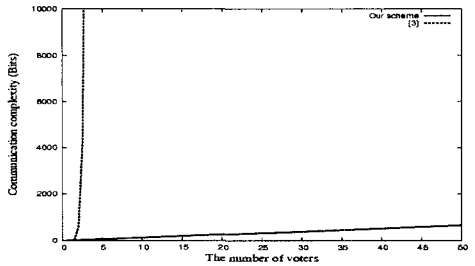

그림 2. M=10일 때의 계산량 비교

결과를 그림 1과 그림 2에서 보여 준다.

시뮬레이션의 결과에 의해, 제안하는 1-out-of-L 전자투표는 후보자의 수에 큰 영향을 받지 않고, 투표결과를 쉽게 집계할 수 있다는 것을 알 수 있다.

Ⅵ. 결 론

본 논문에서, r차 잉여암호를 이용한 1-out-of-L 전자투표 방식을 제안한다. 제안하는 1-out-of-L전자투표 시스템을 위해, r차 잉여 암호의 L possibilities와 투표내용의 유효성 증명 기법을 제안하였으며 또한 기존의 ElGamal 암호 기반의 1-out-of-L전자투표 보다 계산적 효율성을 가진다는 것을 증명하였다. 본 논문에서는 암호기술을 이용한 전자투표 방식에서 간과되어 온 투표 종료 후의투표-취소 기법을 제안하였다. 본 논문에서 제안한 투표-취소 기법은 부재자 투표에서 필요한 투표-취소 기법을 전자투표 방식에서도 응용이 가능할 것으로 기대된다.

참 고 문 헌

[1] Benaloh,J.C., and Tuinstra,D. "Receipt-free secret-vote elections.", Prof.26th ACM Symposium on the Theory of Computing, pp.544-553, 1994.

[2] Canor,L.F., and Cytron,R.K.,"Design and Implementation of a Practical Security-Conscious Electronic Polling System." WUCS-96-02, Department of Computer Science, Washington University, St. Louis, Jan, 1996.

[3] Cohen, J.D, Fischer, M.J., "A robust and verifiable cryptographically secure elelction schme." In Proc.26th IEEE Symp. on Foundation of Comp. Science, pages 372-382, Portland, 1985. IEEE.

[4] Cramer,R., Gennaro,R., Schoenmakers, B., "A secure and optimally efficient multi-authority election scheme." European Transactions on Telecommunication, 8:481-489, Eurocrypt 1997.

[5] P.Diplomová, "'Electronic Voting Schemes." April, 2002.

[6] Fujioka, A., Okamoto, T., Ohta, K., "A Practical Secret Voting Scheme for Large Scale Elections." in Advaces in Cryptology-AUSCRYPT '92, LNCS718, Springer-Verleg, Berlin, pp.244-251, 1993.

[7] Hirt,M , Sako,K., "Efficient receipt-free voting based on homomorphic encryption." Eurocrypt 2000, LNCS1807, pp539-556, 2000.

[8] Park,C., Itoh, K., Kurosawa, K., "Efficient Anonymous Channel and All Nothing Election Scheme." EUROCRYPT '93, LNCS765, Springer-Verlag, Berlin Heidelberg 1994.

[9] Sako,K., Kilian,J., "Receipt -Free Mix-Type Voting Scheme." EUROCRYPT '95, LNCS921, pp393-403, Springer-Verlag, Berlin Heidelberg 1995.

[10] Scheonmakers, B. "A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting." Advances in Cryptology-CRYPTO, LNCS1666, pp148-164, 1999.

[11] Yamaguchi, H., Kitazawa, A., Doi, H., Kurosawa, K., Tsuji, S., "An Electronic Voting Protocol Preserving Voter's Privacy" IEICE Trans. INF.&SYST., Vol.E86-D, No.9, September, 2003.

양 형 규 (HyungKyu Yang) 정회원

한국 통신학회 논문지 2006년 2월호 참조

현재 강남대학교 컴퓨터미디어공학부 정교수

안 영 화 (YoungHwa An) 정회원

1975년~1990년 성균관대학교 전자공학과(학사, 석사, 박사)

1983년 3월~1990년 2월 해군사관학교 전자공학과 교수

1999년 8월~2001년 7월 강남대학교 학술정보처장

2002년 3월~2003년 2월 Florida State University, 방문교수

1990년 3월~현재 강남대학교 컴퓨터미디어공학부 교수

<관심분야> 정보보호, 네트워크 보안