전자투표에서의 선관위 부정방지에 관한 연구

박희운[0], 오형근, 이임영
순천향대학교 공과대학 컴퓨터학부

A Study on Illegal Act of Central Tabulating Agency on Electronic Elections

Hee-Un Park[0], Hyung-Geun Oh, Im-Yeong Lee
Department of Computer Science, College of Engineering
Soonchunhyang University

요 약

네트워크의 발전과 관련해 많은 응용 분야들이 연구되고 있는데, 그 중에서도 암호학을 이용한 전자 투표의 비중이 증대되고 있다. 이러한 측면에서 살펴볼 때 선거관리위원회(선관위)는 전자 투표를 총괄하며, 동시에 투표 결과를 집계해서 공표하는 기능까지 가지고 있는 중요한 기관이다. 그러나 이러한 위치의 선관위가 부정을 저지를 경우 투표에 있어 치명적인 악영향을 미칠 것은 두 말할 나위도 없다. 따라서 본고에서는 선관위가 저지를 수 있는 부정의 요소를 파악하고, 기존의 방식을 고찰하여 보다 더 안전하고 효율적인 선관위의 부정 방지 방식을 제안한다.

1. 서론

인류 역사를 거슬러 살펴보면 많은 의사 결정을 직·간접적으로 투표에 의존해 왔었다. 뿐만 아니라, 현대와 같은 최첨단 사회에서도 인간이 존속하는 한 투표는 주요한 의사 결정 수단이 되어 오고있다. 우리는 여러 형태의 투표를 수행하여 오고 있는데, 소수 모임의 대표에서부터 대통령을 뽑는 일까지 여러 분야에 있어 투표는 빼놓을 수 없는 수단으로 존재하는 것이다. 한 예로 국회의원을 선출하는 선거 기간이 되었다고 가정하자. 우선 선관위에서는 투표인 명부를 만들어 선거 안내문을 발송한다. 투표일이 되면 투표자는 자신의 신분증을 가지고 투표소에 가서 신분 확인을 한 뒤에 투표 용지를 받아서 기표소에서 투표를 하고, 이를 투표함에 넣는다. 하지만 이런 유형의 투표는 날씨가 안좋다던가 개인적으로 다른 급한 일이 생기는 경우에는 매우 번거롭게 생각되었던 것이 사실이다. 그러나 요즘은 정보통신 분야의 핵심인 인터넷의 사용이 확대되고 있으며, 네트워크의 급속한 발전과 초고속 통신망의 구축을 통하여 새로운 정보 서비스를 우리의 생활 안밖에서 보급받게 될 것이다. 이러한 서비스 위에 앞에서 고려해 보았던 전자 투표를 실생활에 보급할 수 있다면, 궂은 날씨나 장소에 구애받을 필요 없이 투표를 할 수 있으므로, 우리의 생활에서 매우 편리함을 제공할 것이다.

현재 기존의 투표 방식은 집계 및 그 밖의 작은 부분에서 컴퓨터가 도입되어 사용되고 있기는 하지만, 투표, 개표 및 집계 작업은 아직도 많은 부분이 사람들에 의해 수행되고 있어 많은 시간과 비용이 소요되는 것이 사실이다. 그러나 네트워크 상에서 전자 투표를 행할 경우 모든 정보가 전자적으로 처리되므로 시간 및 비용의 측면에서 매우 신속하고 저렴하게 수행되는 장점을 가지게 될 것이다. 본고에서는 전자 투표 상에서의 요구 사항 및 기존의 방

식을 분석하고, 선관위의 부정을 막을 수 있는 안전하고 효율적인 전자 투표 방식을 제안한다.

2. 요구 사항

2.1 전자 투표의 요구사항

일반적인 투표의 특성들 중에서 가장 중요하게 여기는 것 중에 하나로서 '무기명 비밀 투표'를 들 수 있다. 이는 투표자가 어떠한 내용을 투표하였는지 그 연결성을 알아낼 수 없다는 개념을 함축한 말로서, 현행 투표 상에서는 제 3자가 보이지 않는 기표소에서 비밀스럽게 자신의 투표를 수행하도록 함으로서 이러한 비밀성을 유지하고 있다. 전자 투표의 경우 그 특성상 일반 투표의 성격을 그대로 보유해야 하며, 특히 전자적 무기명 투표를 위해 필요한 요구 조건이 갖추어져야 할 것이다. 다음은 현행의 일반적인 투표를 고려할 경우 전자 투표가 갖추어야 할 주요 특성들이다.

1) 비밀성 : 투표자와 투표내용의 대응은 당사자만이 안다.[1]
2) 투표권의 단일성 : 한 명의 투표자는 단 한번의 투표권만 가진다.
3) 투표권 인증 : 투표권이 있는 사람만이 투표를 수행할 수 있다.
4) 공평성 : 어느 누구도 다른 사람의 투표 결과를 통해 자신의 투표결과를 결정할 수 없어야 한다.
5) 투표 매매 방지성 : 투표권 매매로부터 투표자를 보호할 수 있어야 한다. [13]
6) 위조 불가능성 : 제 3자에 의한 투표 결과의 위·변조는 불가능하여야 한다.
7) 복사 불가능성 : 누구도 다른 사람의 투표를 복사할 수 없어야 한다.
8) 정확성 : 투표 결과의 집계는 정확해야 한다.

물론 이 외에도 많은 부분이 더 필요할 수 있다. 그러나 이중에서 특히 중요한 사항을 언급한다면, 비밀 투표를 보장해야 하며, 복사 및 매매가 가능해서는 안되고, 집계가 정확해야 한다는 점이다. 이는 기존의 투표에서도 필히 요구되는 사안이기에 전자 투표 구현시 깊은 통찰이 요구된다. 그렇다면 전자 투표가 이루어 질 경우 어떤 문제점을 고려해야 하는지 살펴보자.

2.2 선관위의 부정 방지를 위한 요구 사항

현행 일반 투표 방식들은 투표 안내, 투표, 투표 집계, 투표 감독 등의 기능들이 분할되어져 있다. 이와 같이 나누는 목적은 투표의 부정적인 요소들을 제거하는데 있다. 즉 서로를 감시함으로서 누군가의 부정적인 행위가 있을 때, 이들을 제어하여 안전한 투표를 이룰 수 있기 때문이다. 이를 전자 투표로 구현할 경우, 시간과 비용을 줄이기 위해 통일된 기관이 존재하게 되는데 바로 이것이 선관위가 된다. 따라서 선관위의 역할은 방대해 지는데 다음은 선관위의 역할을 기술한 것이다.

1) 투표 안내 : 투표의 일시 및 투표권자의 리스트를 공표한다.
2) 투표자 인증 : 투표권이 있는 사람들을 확인함으로서 일인 일투표가 가능하게끔 한다.
3) 투표 결과 확인 : 전송되어 온 투표값을 확인하여 위조 및 복사에 대응한다.
4) 집계 : 투표 결과를 확인하여 집계하는 것을 관할 한다.
5) 투표 결과 공표 : 집계 결과를 공표한다.

이상과 같이 전자투표 상에서는 선관위의 기능이 강화되었으며, 이에 따라 선관위가 부정을 저지를 경우 전자 투표는 아무런 의미가 없게 된다. 따라서 전자 투표에 있어 이러한 선관위의 부정이 발생하지 않도록 하는 것이 무엇보다 중요한 부분일 것이다. 다음은 전자투표 상에서 선관위의 부정을 방지하기 위한 요구조건이다.

1) 투표자는 자신의 투표 결과를 확인 할 수 있어야 한다.
2) 선관위는 미등록 투표자의 투표권을 행사할 수 없어야 한다.
3) 선관위는 투표자의 투표결과를 수정할 수 없어야 한다.
4) 선관위에서는 투표자와 투표내용을 대응할 수 없어야 한다.
5) 선관위는 독립적이며, 투표의 집계는 정확하게 수행해야 한다.

3. Park- Itoh-Kurosawa 방식

현재 안전하고 효율적인 전자 투표를 위해 많은 프로토콜 및 방식들이 나와 있는 상황이다.[2][3][4][5][6][7][8][9] 그 중에서도 Park -Itoh -Kurosawa[2]방식(이하 PIK 방식)은 익명 통신로를

전제로 하고 있으며, 다중 프로토콜에 기초하고 있다. 또한 안전한 투표를 위해서 다수의 선관위를 가지고 있다. 투표의 부정적인 요소나 행위가 발견되면, 투표를 멈추거나 완료시킬 수 있게 되어 있으며, 선관위들 중에서 1/2정도가 부정하지 않을 경우에는 투표를 정확히 계수할 수 있게끔 되어 있다.

3.1 시스템 계수

PIK방식에서 사용되는 시스템 계수는 다음과 같다.

. S_m : 다수로 구성된 선관위 (m = 1, 2,..., k)
. X_m , Y_m : 각 선관위의 비밀키와 공개키
. P_i : 투표자 (i = 1, 2,..., n)
. k_i, k_i^{-1} : 투표자의 공개키와 비밀키
. V_i : 투표값
. h : 일방향 해쉬 함수
. $\{d_i\}$, $\{e_i\}$: 랜덤 수
. z : 변수
. || : 연접 연산
. 0^l : 0이 l개 연속되어 있는 것
. P_L : 공개 보드상의 최신 리스트

3.2 투표 프로토콜

● **Main protocol**

<Initial Phase>

0) 각 S_m는 자신의 비밀키 X_m을 VSS(verifiable secret sharing scheme)을 이용해 다른 $\{S_j\}$에게 분배한다.[7] 만약 k/2 이상의 $\{S_j\}$가 모이면, 그들은 X_m을 복구할 수 있다. (단, k는 S_j의 수)

1) 각 투표자 P_i는 자신의 공개키와 비밀키를 선택한다. (k_i, k_i^{-1}) 그리고 자신의 공개키를 공개한다.

2) 공개키 리스트가 공개 보드에 사전 편찬순으로 저장된다. $\{k_i\} = (k_1, k_2,...)$

<Claiming phase>

3) 각 투표자는 공개 보드에서 자신의 공개키[12]를 확인한다. 만약 이상이 있으면, 투표자는 이의를 신청하고 투표는 중지된다. 그렇지 않을 경우에는 다음 단계로 넘어간다.

<Voting phase>

4) 투표자 P_i는 두 개의 랜덤수를 만들어 X-OR하여 투표값을 생성한다.

$$V_i = R_{i1} \oplus R_{i2}$$

5) 각 투표자는 익명 통신로를 이용해 다음을 전송한다.

$$a_i = (k_i||k_i^{-1}(R_{i1}||0^l)$$
$$b_i = (k_i||k_i^{-1}(R_{i2}||0^l)$$

6) Subprotocol 1이 수행된다.

<Testing phase>

$$A_{z(i)} = (g^{di}, k_i||k_i^{-1}(R_{i1}||0^l)(Y_1...Y_k)^{di})$$
$$B_{z(i)} = (g^{ei}, k_j||k_i^{-1}(R_{i2}||0^l)(Y_1...Y_k)^{ei})$$ 일 때 공개 보드에는 (A_1, B_1), (A_2, B_2)... 과 같은 리스트가 존재한다.

7) A_i 또는 B_i가 랜덤하게 선택된다.

8) subprotocol 2에 의해 선택되어진 것은 공개되며 그 결과값은 $u_i = t_i||w_i$가 된다.

9) 모든 사람들은 $t_i = k_i$, $t_i(w_i) = 0^l$인지 확인한다.

10) 9단계에서 이상이 없으면, 다음 단계로 가고 그렇지 않으면 멈춘다.

<Opening phase>

11) 남은 각 i에 대해 8, 9단계를 수행한다.

12) 아무 이상도 발견되지 않으면, $\{V_i\}$ 리스트를 수용한다.

● **Optional Protocol**

$(q, g, Y_m, a_1,...,a_n, Z_{1m},...Z_{nm})$가 공개 보드에 등록되어 있을 때 X_m를 참고하여 다음 식이 나온다. [11]

$$Y_m = g^{Xm} \bmod q$$
$$Z_j^i = a_j^{Xm} \bmod q \quad (j = 1,...,n)$$

1) 각 선관위는 영지식 증명(ZKIP)을 이용해 위의 수식을 확인한다.

2) 각 선관위는 subprotocol 1에서 사용했던 랜덤수를 확인한다.

3) 만약 S_m이 잘못된 것으로 판명되면 진정한 S_js가 VSS를 이용해 X_m을 복구한다.

4) X_m을 이용해 모든 V_is가 복구된다.

● **Subpotocol 1**

1) 공개 보드상의 최신 리스트가 다음과 같을 때 선관위는 랜덤수 $r_1,...,r_n$을 선택한 다음 각각의 j에 대해 $h(a_j, b_j, r_j)$를 계산한다.

$$(a_1, b_1), (a_2, b_2),...(a_n, b_n)$$

2) 선관위는 사전 편찬순으로 다음을 공표한다.

$$h(a_j, b_j, r_j) \quad (j = 1,...,n)$$

● **Subpotocol 2**

1) 각 선관위는 다음을 계산한다.

$Z_j^i = a_j^{Xi}(=Y_i^{dj}) \bmod q \ (j = 1,...,n)$

2) 각 선관위는 공개보드에 다음을 공표한다.

$(Z_j^i,...,Z_n^i)$

3) 모든 사람들이 다음을 확인한다.

$u_j = b_j(Z_j^1,...,Z_n^k)$

$(=n_{z(j)}*(Y_1...Y_k)^{dj}/Y_1^{dj}...Y_k^{dj}= P_{Lz(j)}$

3.3 기존 방식의 고찰

PIK 방식은 공개 보드를 사용하기 때문에 선관위가 투표자의 투표값를 위조하거나 변경할 수 없다는 장점을 가지고 있다. 또한 익명 통신로를 사용하기 때문에 투표값과 투표자를 연결시킬 수 없다. 그러나 이 방식은 선관위의 1/2정도가 결탁 할 경우, 투표 결과값을 인증할 방법이 없기 때문에 투표의 공정성은 무너지게 된다. 뿐만 아니라 투표자들은 자신의 공개키와 투표값만을 알 수 있기 때문에, 투표 미등록자에 대해서 선관위가 투표권을 행사할 경우 그 부정을 확인할 수 있도록 하는 방안이 필요하다.

4. 새로운 방식 제안

현행의 투표 절차를 살펴보면 투표함의 개표 및 집계원이 집계를 수행할 경우 참관인이 대동해 그들이 부정을 저지르는지에 대해 감사를 하게끔 되어 있다. 본고에서 제안하는 방식에서는 바로 '참관인'과 같은 기능을 수행하는 감사 기구를 구성하여 선관위의 부정을 감시하도록 구성하였다.

4.1 요구 조건

본 제안 방식에서는 선관위의 부정을 방지하기 위해 다음과 같은 사항을 부가한다.

1) 감사 기구 및 선관위는 투표자의 신뢰를 획득하기 위해 예비등록을 통하여 투표자 확인을 수행한다.[11]

2) 투표 매매와 같은 부정적인 사고에 대비하여 별도의 투표소들을 운용한다.[13]

3) 감사 기구와 선관위의 결탁을 방지하기 위해 감사기구는 선관위와는 독립적이며, 다수로 구성한다.

4) 투표 결과에 대한 확인의 공정성을 기하기 위하여 감사 기구는 개표 수행에 참여한다.

4.2 시스템 계수

본 제안 방식에서 사용되는 시스템 계수는 다음과 같다.

. ID_s : 투표자의 세션 ID (단, $S = A_s(ID_s)$

. $G_1, G_2, ... G_n$: 감사 기구들

. A : 선관위

. V_i : 투표자

. V : 투표값

. G_s, G_p : 감사 기구들의 대표 비밀키와 공개키

. G_{si}, G_v : 감사 기구들의 투표 확인용 분배 비밀키들과 공개키(Secret Sharing 사용)

. N_i : 감사 기구들이 부여하는 시리얼 번호

. A_s, A_p : 선관위의 비밀키와 공개키

. r : 은닉 서명 비밀 계수 (단 $r*r' = 1 \bmod n$)

. H : 일방향 해쉬 함수

4.3 제안 투표 프로토콜

● **Registration Phase**

1) 선관위는 투표 대상자들을 확인하여 선거인 명부를 만들고, 투표자와 감사 기구에 공표한다.

2) 각 투표자는 등록 과정을 통해 자신을 인증하고, 랜덤한 세션 ID를 등록한다. (은닉서명 사용)[2]

. 투표자는 은닉 서명 비밀 계수 r를 선택하여 세션 ID를 숨겨서 선관위 및 감사 기구에 보낸다.

$r(ID_s)$

3) 전송되어온 데이타에 대하여 선관위는 대표 비밀키로 서명한 뒤 투표자에게 전송하며, 감사 기구 역시 공동으로 확인한 후 시리얼 번호를 부여하여 자신들의 대표 비밀키로 서명한 뒤 투표자에게 전송한다. (감사 기구와 선관위의 결탁을 방지하기 위해 시리얼 번호를 부여한다.)

. $A_s(r(ID_s))$, $G_s(r(ID_s)||N_i)$ ==> 투표자

4) 투표자는 선관위와 감사 기구로부터 전송된 서명들과 시리얼 번호를 확인한다.[1]

. 투표자는 자신의 비밀 계수를 제거한다.

$A_{sr'}(r(ID_s)) = A_s(ID_s) = S_A$,

$G_{sr'}(r(ID_s)||N_i) = G_s((ID_s)||N_i) = S_G$

. 서명을 확인한다.

$A_p(S_A) = ID_s$, $G_p(S_G) = ID_s||N_i$

● **Voting Phase**

5) 투표일이 되면 투표를 수행하기 위해 자신을 확인한 뒤 투표를 수행한다. (선관위 및 감사 기구의 공개키를 이용해 내용을 암호화한다.)

. 일방향 해쉬 함수를 이용해 자신의 시리얼 번호, ID_s 및 투표값 V를 해쉬한다.

$H(ID_s||V||N_i) = R$

. 감사 기구의 공개키로 R을 암호화한 뒤, 자신의 시리얼 번호, ID_s 및 V를 연접해 선관위의 공개키로 암호화 한다.

$A_p(ID_s||V||N_i||G_v(R)) = E$

. 감사 기구와 선관위의 서명을 암호 결과값과 연접해 전송한다.

$S_A||S_G||E$

- **Conviction Phase**

6) 선관위 및 감사 기구는 자신들의 비밀키를 이용해 복호화 한 뒤, 서명을 확인함으로 투표 결과를 확인한다.

. 선관위 및 감사 기구는 자신들의 공개키들로 서명을 확인한다.[10][11]

$A_p(S_A) = ID_s$, $G_p(S_G) = ID_s||N_i$

. 선관위 및 감사 기구는 자신들의 비밀키들로 복호화 한다.

$A_s(E) = A_s(A_p(ID_s||V||N_i||G_v(R)))$

$= ID_s||V||N_i||G_v(R)$

$G_{si}(G_v(R)) = H(ID_s||V||N_i)$

. 선관위 및 감사 기구는 해쉬 함수를 이용해 R값과 비교하여 투표의 진위 여부를 판단한다.

$H(ID_s||V||N_i) = R$

- **Opening Phase**

7) 투표자의 투표 결과를 공개 보드 상에 공표한다.

. ID_s , V

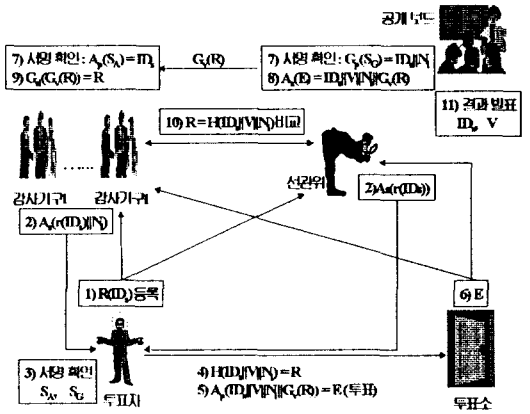

그림 1. 제안 방식

4.4 제안 방식 고찰

본 제안 방식은 은닉 서명을 이용한 예비 등록 절차를 통해 세션 ID를 선관위와 감사 기구에 등록하게끔 함으로서, 투표자와 ID_s를 연결시킬 근거를 없애고 있다. 또한 투표소에서 투표를 수행하게 함으로서 물리적으로 확인을 통해 일인 일투표가 가능하며, 제 3자의 대리투표나, 위조와 같은 부정적인 방해를 수행할 수 없다는 장점을 가지고 있다. 그와 함께 투표가 끝난 뒤 집계 결과를 공표함으로서 제 3자의 투표 결과에 따라 자신의 투표를 결정할 아무런 근거도 가지지 못할 뿐 아니라, 선관위의 투표 결과 수정이 불가능하게 된다.

본고에서는 이와 함께, 다음과 같은 부정 유형에 대해 대응함으로서 선관위의 부정한 시도에 대한 방지책을 제시하고 있다.

. 부정 유형 1) : 선관위가 투표자의 투표 결과를 위조하거나 수정하려 시도할 경우

=> 모든 투표 결과는 공개되어 있는 보드 상에 투표자의 ID_s와 투표값 V가 등록되게 된다. 투표자의 투표값이 변경이 된다면, 투표자는 이러한 경로를 통해 자신의 투표값을 확인하므로 선관위의 부정을 방지할 수 있다.

. 부정 유형 2) : 선관위가 투표 미등록자의 투표권을 행사하려 시도할 경우

=> 모든 투표자는 투표를 수행하기 전에 자신의 세션 ID를 선관위와 감사 기구에 등록하게 되어 있다. 감사 기구는 ID 등록시 시리얼 번호를 부여하게 되어 있기 때문에, 선관위가 임의의 제 3자를 통해 투표 미등록자의 투표권을 행사하려 한다 해도 감사 기구가 부여한 시리얼 번호를 알지 못하기 때문에 투표 확인시 부정을 검출할 수 있다.

. 부정 유형 3) 선관위와 n-1개의 감사 기구가 결탁할 경우

=> 투표자의 세션 ID에 대해 감사 기구들이 모두 합의한 상태에서 시리얼 번호를 부여하게 되므로 부정이 힘들게 된다.

이상과 같이 감사 기구 시스템을 도입함으로서, 선관위의 위조나 결탁을 통한 부정은 무의미하게 되므로 선관위의 부정은 예방될 수 있겠다.

5. 결론

현재 의사 결정의 수단으로서 제시되어진 투표는 그 성격상 매우 미묘한 문제가 되기 때문에 그 어느 상황에서도 부정의 소지가 있어서는 안된다. 전자 투표의 경우도 예외는 아니며, 사람과 사람이 직접 만나지 않고 프로토콜이 수행되기 때문에 그만큼 투표의 안전성은 무엇보다 중요하게 된다. 이에 대해 본고에서는 다가올 미래에 사용 가능성이 매우 높은 전자 투표에 대해서 그 필요성과 요구사항을 제시하였다. 그와 함께, 투표를 총괄하는 선관위의 비중이 어느 정도가 되는지에 대해서 생각해 보았으며, 전자 투표상에서 발생할 수 있는 선관위의 부정에 관하여 언급하였다.

기존의 방식은 투표자와 선관위가 정직하다는 가정하에 수행 기능을 기술하고 있으며, 미등록 투표자에 대한 선관위의 부정에 대해 고려하고 있지 않았었다. 이에 대해 본고에서는 투표소가 물리적으로 안전하고, 감사 기구의 독립성이 보장될 경우 선관위가 투표자의 투표 결과를 위조하는 것을 막을 뿐만 아니라, 투표 미수행자들의 투표권을 이용해 부정을 저지를 수 없도록 구성되어 있다. 그러므로, 향후 전자 투표 수행에 있어 좀더 안전하면서도, 편리하게 사용하는데 있어 많은 도움이 되리라 생각한다.

6. 참고 문헌

[1] D. Chaum, "Blind Signature for Untraceable Payments", Advances in Cryptology Proceedings of CRYPTO '82, pp.199-203.

[2] C. S. Park, K. Itoh and K. Kurosawa, "Efficient anonymous channel and All/Nothing election scheme", Advances in Cryptology, Proc. EUROCRYPT '93, pp.248-259, 1993.

[3] D. Chaum, "Elections with Unconditionally Secret Ballots and Disruptions Equivalent to Breaking RSA", Advances in Cryptology, Proceedings of EUROCRYPT '88, pp.177-181, 1988.

[4] D. Chaum, "Untraceble Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM Vol.24, No.2, pp.84-88, 1981.

[5] H. Nurmi, A. Salomaa and L. santean, " Secret ballot elections in computer networks", Computers and Security 10, pp.553-560, 1991.

[6] J.D. Cohen and M.H. Fischer, "A Roubust and Verifiable Cryptographically Secure Election Scheme ", Proceedings of the 26th Annual IEEE symposium on the Foundations of Computer Scirence, pp.372-382, 1985.

[7] J.C. Benaloh, "Secret Sharing Homomorphism : Keeping shares of a Secret", Advances in Cryptology, Proceedings of Crypto '86, pp.251-260, 1986.

[8] J.C. Benaloh, "Verifiable secret-ballot elections", Ph.D.thesis, Yale university, Technical report 561, 1987.

[9] K. Iversen, "A cryptographic scheme for computerized general elections", Proc. CRYPTO '91, Springer LNCS 576, pp.405-419, 1992.

[10] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the Association for Computing machinery, Vol, 21, No.2, pp120-126, 1978.

[11] T. ElGamal, "A public key cryptosystem and signature scheme based on discrete logarithms", IEEE Trans, Inform, Theory, Vol.31, No.4,p p.469-472, 1985.

[12] W. Diffie and M.E. Hellman, "New directions in cryptography", IEEE Transaction on Information Theory, Vol.22 No.6, pp.644-654, 1976.

[13] 박희운, 이임영, " 전자 투표 매매 방지에 관한 연구", 제 9회 한국정보처리학회 춘계 학술 발표대회, 제 5권 1호, 1998. 4.

[14] 최용락, 소우영, 이재광, 이임영, "통신망정보보호", 도서 출판 그린, 1996.