그룹 서명을 적용한 실제적인 전자투표 시스템의 구현

김경원*, 이필중*

*포항공과대학교 정보통신대학원

An Implementation of Practical Electronic Voting Scheme Based on the Group Signature

Kyoung Weon KIM*, Pil Joong LEE*

*Department of Graduate School of Information Technology, POSTECH

요 약

전자투표 시스템은 유권자들이 온라인상에서 안전하게 투표할 수 있도록 하기 위한 프로토콜이다. 현재까지 대부분의 전자투표 시스템은 믿을 수 있는 서버로 하여금 투표를 모아서 선거의 결과를 공정하게 계산할 수 있도록 하고 있다. 이러한 전자투표 시스템은 전자 서명[7,8,13,14,19], mix-net[20,21], homorphic encryption schemes[23,24]등을 이용하여 제안되었다. 또한 그룹 멤버가 그룹을 대표하여 서명을 하는 그룹 서명의 개념을 적용[15]할 수 있다. 본 논문에서는 그룹 서명을 전자투표 시스템에 그대로 적용할 수 없기 때문에 변형된 그룹 서명을 제안하고, 그것을 이용하여 전자투표 시스템에 적용하고자 한다. 우리는 Camenisch 와 Michels가 제안한 그룹 서명[1]을 기초로 한다.

Ⅰ. 서론

그룹 서명은 그룹의 멤버만이 메시지를 서명할 수 있으며, 검증자는 서명 값이 유효한지의 여부는 알 수 있으나 그룹 멤버 중 누가 서명을 했는지 확인할 수 없다[9]. 서명을 검증하기 위해서는 하나의 그룹 공개키만 있으면 되기 때문에 다른 scheme에 비해 공개키 크기가 훨씬 작다는 장점이 있다.

그룹 서명은 초기화(Setup), 등록(Join), 서명(Signature), 검증(Verification), Open의 다섯 단계로 이루어져 있다. 하지만, 현재 그룹 서명은 분쟁이 발생할 경우 누가 서명을 했는지를 밝힐 수 있다. 따라서 전자투표 방식에 적용하기 위해서는 변형을 가하여야 한다.

그룹 서명은 Chaum 과 van Heyst [9]에 의해 1991년에 소개 되었으며, 이후 e-cash 시스템을 비롯하여 많은 응용분야에 적용되었다.

은닉 서명의 개념은 Chaum[10]에 의해 소개되었으며 이후 e-cash 시스템 및 e-voting 시스템 등의 응용분야에 적용되었다.

그룹 은닉 서명은 그룹 멤버가 문서의 내용을 알지 못한 채 그룹을 대표하여 서명하고자 하는 기법이다. 즉, 그룹 서명에 은닉성을 추가하고자 하는 것이다. 이러한 기법은 1998년 A. Lysyanskaya, Z. Ramzan.에 의해 소개 되었다[4,5,11].

기존에 그룹 서명을 적용한 전자투표 시스템[15]은 투표자가 여러 대의 서버에 여러 번 연결해야 한다는 것과, 저자가 제안한 연결가능한(linkable) 그룹 서명이 open될 수 있다는 단점이 있다. 본 논문에서는 이 논문의 단점을 극복하고, 더욱 효율적이고 실제적인 전자투표 시스템을 제안한다.

안전한 전자투표 시스템은 여러 가지 요구사항에 대하여 만족하여야 하며, 특히, 다음의 요구조건들을 고려하여야 한다[13,14,16].

□익명성(Anonymity): 모든 투표가 비밀로 되어야 한다는 것으로, 특히 개인의 익명성이 보장되며, 투표 내용으로부터 해당 투표자를 확인할 수 없어야 한다.

□부분적 결과산출 불가성(No partial results): 최종집계이전에 부분적인 집계결과를 산출하는 것이 불가능하다.

□대중적 검증(Public verifiability): 선거가 끝난 후에 어느 누구라도 DB서버의 투표 값을 검증할 수 있다.

□합법성(Democracy): 투표 권한을 가진 합법적인 유권자만이 투표 값에 대한 그룹 서명에 참여할 수 있다.

□이중 투표 불가성(Unreusability): 정당한 투표자가 두 번 이상 투표할 수 없다는 것으로 단지 한번만 투표할 수 있어야 한다.

본 논문은 다음과 같이 구성되어 있다.

1장에서는 이 논문에서 사용되는 표기법과 몇 가지의 정의에 관하여 설명한다. 2장에서는 전자 투표 시스템 적용을 위한 그룹서명에 대하여 설명한다. 3장에서는 제안하고 있는 새로운 전자 투표 시스템에 대하여 설명한다. 4장에서는 본 프로토콜의 안전성 분석에 관하여 설명하고, 마지막으로 결론에 관하여 서술할 것이다.

II. 본문

1. 표기법과 정의

이 장에서는 몇몇 표기법과, 지식 증명(proofs of knowledge)의 정의에 관하여 설명할 것이다.

1.1 표기법

• x=?y는 x와 y가 같은지, 다른지를 의미한다.

· $N=\{n \mid n=pq, p<q, p=2p'+1, q=2q'+1\}$,

· $[a,b]$ 은 $\{a, a+1, \ldots, b-1, b\}$ 를 가리킨다.

· $x \in_R E$ 은 집합 E로부터 임의로 선택되는 것을 말한다.

· ε, l_g, l_1, l_2, k, l_t 은 매개변수이다. 여기서 k는 일방향 함수 $H(\cdot)$: $\{0,1\}^* \rightarrow \{0,1\}^k$ 의 고정된 출력 길이이며, l_g는 그룹의 위수의 길이이며, $\varepsilon>1$, k, $l_1, l_2 \square l_g$, $l_t = \varepsilon(l_2+k)+1$이다.

1.2 정의

제안된 시스템에서 사용될 세 가지 정의에 대하여 소개한다. [2]에 따르면, 이 세 가지 정의는 통계적 영지식(statistical zero-knowledge)으로부터 유도된 서명이며, 지식 증명에 관한 서명(SPK)이라 불린다.

Fujisaki 와 Camenisch는 몇몇 가정 하에서 (예: Modified Strong RSA Assumption, Diffie-Hellman Decision Assumption[2]) 이 정의에 관하여 증명하였다[3].

우리는 [2,3]으로부터 다음의 정의들을 소개한다.

정의2.2.1과 정의2.2.2는 어떠한 구간에 있는 이산 대수의 지식(knowledge)을 보여준다.

정의2.2.3은 그룹 멤버가 그룹의 서명을 어떻게 발생하는가를 보여주는 그룹 서명에 관한 것이다.

1.2.1 정의 1

g에 관한 y의 이산 대수의 지식 증명은 $c=H(g \| y \| g^{s-c2^{l_1}} y^c \| m)$을 만족하는 $(c,s) \in \{0,1\}^k \times [-2^{l_2+k}, 2^{\varepsilon(l_2+k)}]$이며, 또한 $log_g y$의 값이 $[2^{l_1}, 2^{l_1}+2^{l_2}]$에 있다는 것을 증명한다. 이러한 proof of knowledge(지식 증명)은 다음과 같이 표기된다.

$$SPK\{(a): y = g^a \wedge (2^{l_1}-2^{\varepsilon(l_2+k)+1} < a < 2^{l_1}+2^{\varepsilon(l_2+k)+1}))(m)$$

만약 y=g^x이기 위한 이산대수 $x \in [2^{l_1}, 2^{l_1}+2^{l_2}]$이 알려진다면, 우리는 다음과 같이 proof를 계산할 수 있다.

- $r \in_R \{0,1\}^{\varepsilon(l_2+k)}$를 선택하고, t := g^r를 계산한다.

- $c := H(g \| y \| t \| m)$와 $s := r - c(x - 2^{l_1})$(in Z)을 계산한다.

-검증자는 식 $c = ?H(g \| y \| g^{s-c2^{l_1}} y^c \| m)$를 검사하고, proof를 받아들일 수 있는지를 결정하기 위해 $s \in [-2^{l_2+k}, 2^{\varepsilon(l_2+k)}]$를 확인한다.

2.2.2 정의 2

g에 관한 y_1의 이산 대수의 지식 증명과 h에 관한 y_2의 이산 대수의 지식 증명은 $(c, s_1, s_2) \in \{0,1\}^k \times [-2^{l_2+k}, 2^{\varepsilon(l_2+k)}] \times Z$ 이며, 또한 $log_g y$의 값이 $[2^{l_1}, 2^{l_1}+2^{l_2}]$에 있다는 것을 증명한다. 이러한 지식 증명은 다음과 같이 표기된다.

$$SPK\{(a): y_1 = g^a \wedge y_2 = h^a \wedge (2^{l_1}-2^{\varepsilon(l_2+k)+1} < a < 2^{l_1}+2^{\varepsilon(l_2+k)+1})\}(m)$$

우리는 정의 2.2.1에서 한 것처럼 (c, s_1, s_2)의 값을 구성할 수 있다.

1.2.3 정의 3

μ에 관한 메시지 $m \in \{0,1\}^*$의 그룹 서명은 $c=H(g \| h \| y \| z \| a \| b \| d \| z^c b^{s_1-c2^{l_1}} / y^{s_2} \| a^{s_1-c2^{l_1}} / g^{s_2} \| a^c g^{s_3} \| d^c g^{s_1-c2^{l_1}} h^{s_3} \| m)$을 만족하는 $(c, s_1, s_2, s_3, a, b, d) \square \{0,1\}^k \times [-2^{l_2+k}, 2^{\varepsilon(l_2+k)}] \times [-2^{l_2+l_1+k}, 2^{\varepsilon(l_2+l_1+k)}] \times [-2^{l_2+k}, 2^{\varepsilon(l_2+k)}] \times G^3$ 이며, 다음과 같이 표기할 수 있다.

$$SPK\{(\eta, \vartheta, \zeta): z = b^\eta / y^\vartheta \wedge a^\eta / g^\zeta = 1 \wedge a = g^\zeta \wedge d = g^\eta h^\zeta \wedge (2^{l_1}-2^{\varepsilon(l_2+k)+1} < \eta < 2^{l_1}+2^{\varepsilon(l_2+k)+1}$$

그룹의 멤버로서 그룹을 대신하여 다음과 같이 메시지 $m \in \{0,1\}^*$을 서명할 수 있다.

①. $w \in \{0,1\}^{l_t}$을 선택하고, $a := g^u, b := u r^u, d := g^e h^u$을 계산한다.

②. $r_1 \in \{0,1\}^{\varepsilon(l_2+k)}$, $r_2 \in \{0,1\}^{\varepsilon(l_t+l_1+k)}$,

$r_3 \in \{0,1\}^{\epsilon(l_1+k)}$를 선택하고, 다음을 계산한다.

③. $t_1 := b^{r_1}(1/r)^{r_2}$, $t_2 := a^{r_1}(1/g)^{r_3}$,

$t_3 := g^{r_3}$, $t_4 := g^{r_1} h^{r_3}$

④ $c := H(m \| g \| h \| r \| z \| a \| b \| d \| t_1 \| t_2 \| t_3 \| t_4)$

⑤. $s_1 := r_1 - c(e - 2^{l_1})$, $s_2 := r_2 - cew$,

$s_3 := r_3 - cw$, $s_1, s_2, s_3 \in Z$

결과적으로 m의 서명 값은 $(c, s_1, s_2, s_3, a, b, d)$ 이다.

2. 전자투표 시스템 적용을 위한 그룹 서명

이번 장에서는 전자투표 시스템에 적용하기 위해서 기존에 제안한 그룹 서명[1,12]의 변형된 형태에 관하여 설명한다.

본 논문에서 제안하고 있는 전자투표 시스템은 다중의 서버를 수반하고 있으며, 온라인 투표에 적용하기 위한 것이다.

2.1 초기화(Setup)

우리의 시스템 초기화 과정은 [1,5]와 유사하며, 다음과 같다.

-그룹 매니저(G.M.)는 cyclic group G=<g>을 선택한다. 그룹의 위수의 길이는 l_g이다.

-임의의 원소 $z, g, h, r, k \in {}_R G$을 선택한다.

-충돌 회피 해쉬 함수 H(•)과 매개변수 l, l_1, l_2, ε을 선택한다. ex) $\varepsilon = 9/8$, $l_g = l = 1200$, $l_1 = 860$, $l_2 = 600$

-그룹 매니저는 z, g, h, r, k, G, l_g를 공개한다.

-그룹 매니저는 두개의 임의 소수 p, q를 선택한다. 여기서 $n = pq$, $p, q \neq 1 \pmod 8$, $p \neq q \pmod 8$, $p = 2p^0 + 1$, $q = 2q^0 + 1$을 만족한다. 그룹 매니저는 n을 공개한다.

2.2 등록

모든 사용자들(Ui)은 인증서(group license)를 얻기 위해서 그룹 매니저에 등록을 해야 한다.

U_i: ① 다음의 조건을 만족하는 e'와 e_i를 선택한다.

- $\hat{e} \square_R 2^{l-1}, \ldots, 2^l - 1$

- $e_i \square_R 2^{l_1}, \ldots, 2^{l_1} + 2^{l_2} - 1$

- $e', e_i \neq 1 \pmod 8$, $\hat{e} \neq e_i \pmod 8$

② 다음을 계산한다.

- $\varepsilon := \hat{e} e_i \pmod n$

- $z := z^{\hat{\varepsilon}} \pmod n$

③ 계산된 ε, z를 그룹 매니저에게 보내고 그룹 매니저와 함께 다음의 쌍방의 프로토콜(interactive protocol)를 수행한다.

$SPK\{(?, \bar{}): z' = z^{?} \wedge z = z^{\bar{}} \wedge (2^{l_1} - 2^{\varepsilon(l_2+k)+1} \square ? \square 2^{l} + 2^{\varepsilon(l_2+k)+1})\}(z)$

G.M.: ① $?_i, \bar{}_i \square_R \frac{1}{2}2^{l-1}, \ldots, 2^l - 1\frac{3}{4}$을 선택한다.

② $?_i$와 $\bar{}_i$를 사용자에게 보낸다.

U_i: ① $x_i = (?_i \hat{e} + \bar{}_i) \pmod{2^l}$를 계산한다.

② $\circ = k^{x_i} \pmod n$를 계산하고 그룹 매니저에게 $\circ$ 값을 보내고, 그룹 매니저와 함께 다음의 쌍방의 프로토콜을 수행한다.

$SPK\frac{1}{2}(?): \circ = k^{?} \wedge -2^{l} \square ? \square 2^{l}\frac{3}{4}$

G.M.: ① $u_i = (z \square \circ)^{1/e}$를 계산하고 사용자에게 u_i를 보낸다.

② (u_i, ε, z)를 저장한다.

U_i: ① $k^{x_i} \square z \equiv u_i^{\varepsilon} \pmod n$을 검증한다.

② 인증서로서 (u_i, e_i)를 저장하며, 각 사용자의 비공개키는 x_i가 된다.

2.3 서명

서명과정 역시 [1,12]와 유사하며, 서명의 기본적인 개념은 정의2.2.3의 그룹 서명을 따를 것이다. 그러나 그 자체로 전자투표에 적용하기엔 부적합하므로, 투표절차 중에 투표 값을 open할 수 없도록 하기 위해서 약간의 변형을 필요로 한다.

합법적인 투표자의 이중투표를 방지하기 위해서 그룹 멤버의 비공개키로 서명을 한, 유일한 값 η가 서명 값에 포함된다. 이 값을 통해, 투표자가 동일인에 대하여 이중 투표한 것을 막을 수 있다.

이 장에서 적용되는 메시지 m은 *3장. 새로운 전자투표 시스템*에서 제시한 그림에서의 $\frac{1}{2}$값과 일치한다. 즉 서명과정에서 입력은 ID 성분과 투표 값(m_i)을 암호화한 $\frac{1}{2}$값이 된다. 이 장에서는 그룹 서명의 이해를 돕기 위해서 *2장. 정의*에 따

라 메시지 m의 표기로 한다.

$^{2}, l_1, l_2$은 매개변수이며, ^{2} □ 1, l_2 □ l_1 □ l_g, l_2 □ $\frac{l_g - 2}{2} - k$의 조건을 만족한다.

메시지 m □ 0,1 □의 그룹 서명은 $(c, s_1, s_2, s_3, a, b, d)$ □ 0,1 □× $-2^{l_2+k}, \ldots, 2^{\wedge(l_2+k)}$ × $-2^{l_g+l_1+k}, \ldots, 2^{\wedge(l_g+l_1+k)}$ × $-2^{l_g+k}, \ldots, 2^{\wedge(l_g+k)}$ × G^{3}이며, $T_1 = z^{c} b^{s_1 - c2^{l_1}} / r^{s_2}$, $T_2 = a^{s_1 - c2^{l_1}} / g^{s_2}$

$T_3 = a^{c} g^{s_3}$, $T_4 = d^{c} g^{s_1 - c2^{l_1}} h^{s_3}$

$c = H(m \| g \| h \| r \| z \| a \| b \| d \| T_1 \| T_2 \| T_3 \| T$ 을 만족한다.

서명과정을 수행하기 위해 그룹 멤버는 다음의 단계를 따른다.

①. $w \in \{0,1\}^{l_g}$을 선택하고,

$a := g^{w}, b := u_i r^{w}, d := g^{e_i} h^{w}$,

$\pm := m^{x_i} (mod n)$을 계산한다.

② . $r_1 \in \{0,1\}^{\wedge(l_2+k)}$, $r_2 \in \{0,1\}^{\wedge(l_g+l_1+k)}$, $r_3 \in \{0,1\}^{\wedge(l_g+k)}$, $r_4 \in \{0,1\}^{\wedge(l_g+l_2+k)}$ 를 선택하고, 다음을 계산한다.

③. $t_1 := b^{r_1} (1/r)^{r_2}$, $t_2 := a^{r_1} (1/g)^{r_2}$,

$t_3 := g^{r_3}$, $t_4 := g^{r_1} h^{r_3}$,

$t_5 = m^{r_4} (mod n)$

④. $c := H(m \| g \| h \| r \| z \| a \| b \| d \| t_1 \| t_2 \| t_3 \| t_4 \| t_5)$.

⑤. $s_1 := r_1 - c(e_i - 2^{l_1})$, $s_2 := r_2 - c e_i w$,

$s_3 := r_3 - cw$, $s_4 := r_4 - c(x_i - 2^{l_1})$, s_1, s_2, s_3, s_4를 Σ

결과적으로 m의 서명 값은 $(c, s_1, s_2, s_3, s_4, a, b, d, \pm)$ 이다.

2.4 검증

메시지 m의 서명 값 $(c, s_1, s_2, s_3, s_4, a, b, d, \pm)$은 다음의 단계로 검증될 수 있다.

① 다음의 값을 계산한다.

$T_1 = z^{c} b^{s_1 - c2^{l_1}} / r^{s_2}$ $T_2 = a^{s_1 - c2^{l_1}} / g^{s_2}$

$T_3 = a^{c} g^{s_3}$ $T_4 = d^{c} g^{s_1 - c2^{l_1}} h^{s_3}$

$T_5 = m^{s_4} (\pm / m^{2^{l_1}})^{c}$

$c' = H(m \| g \| h \| r \| z \| a \| b \| d \| T_1 \| T_2 \| T_3 \| T_4 \| T_5)_{PKc}$ $(\square_i \| T_i)$을 받게 되며, 이 N개의 값과 □

② 다음의 조건을 만족하면 서명을 받아들인다.

$c = c^{0}$, s_1 □ $-2^{l_2+k}, \ldots, 2^{\wedge(l_2+k)}$,

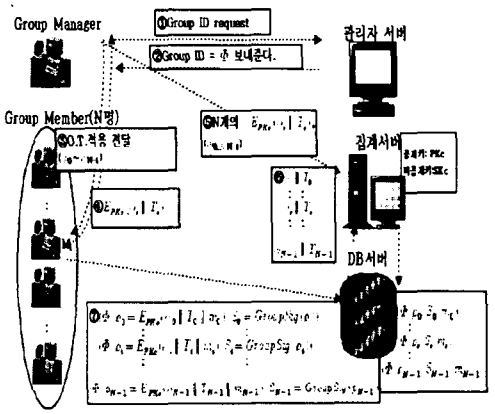
s_2 □ $-2^{l_g+l_1+k}, \ldots, 2^{\wedge(l_g+l_1+k)}$,

s_3 □ $-2^{l_g+k}, \ldots, 2^{\wedge(l_g+k)}$,

s_4 □ $-2^{l_g+l_2+k}, \ldots, 2^{\wedge(l_g+l_2+k)}$

3. 새로운 전자투표 시스템

투표에 참가하는 모든 개체는 투표자, 유효한 투표자를 등록하기 위한 관리자서버, 투표 값의 집계를 실시하는 집계서버, 투표자의 ID성분과 투표 값에 관한 정보, 서명 값을 등록하는 DB서버로 나눌 수 있다. 투표절차를 그림으로 간단하게 나타내면 다음과 같다.



위의 그림에서 보는 바와 같이 세부절차는 다음과 같다.

①그룹 매니저는 관리자서버에게 그룹 ID를 요청한다.

②관리자서버는 그룹 매니저에게 그룹 ID = □를 보내준다.

③그룹 매니저는 □를 비밀 공유(sectet sharing) 개념을 적용하여,

□ = $\square_0 x^{0} + \square_1 x^{1} + \ldots + \square_{N-1} x^{N-1}$와 같이 N개로 나누고, Oblivious Transfer를 적용[17,18]하여 그룹 멤버에게 ($\square_0 \sim \square_{N-1}$)의 값을 보낸다. 즉, 그룹 매니저는 그룹 멤버가 어떤 값을 받았는지 모르게 된다.

④그룹 멤버 M_i는 $E_{PKc}(\square_i \| T_i)$을 생성하고, 이 값을 그룹 매니저에게 전달한다. 여기서, T_i는 시점확인(time stamp)이다.

⑤그룹 매니저는 N명의 그룹 멤버로부터 $E_{PKc}(\square_i \| T_i)$을 받게 되며, 이 N개의 값과 □를 N개로 나눈 값($\square_0, \ldots \square_{N-1}$)을 집계서버에게 보낸다.

⑥집계서버는 비공개키를 이용하여 $\square_i \| T_i$로

복호화 한다.

⑦그룹에 속해 있는 그룹 멤버(M_i)는 $(\square, \frac{1}{2_i} = E_{PKc}(\square, \| T_i \| m_i), S_i = GroupSig(\frac{1}{2_i}))$을 DB서버에 올린다.

⑧집계서버는 $\frac{1}{2_i}$를 복호화한 값 중 $\square_i \| T_i$에서 $\square_i$가 그룹 매니저로부터 받은 값 ($\square_0 \sim \square_{N-1}$)에 속했는지의 여부를 판단하여 그룹 $\square$의 멤버인지를 판단할 수 있다. 그리고, 집계서버에 저장된 $\square_i \| T_i$와 $\frac{1}{2_i}$를 복호화하여 얻은 값 $\square_i \| T_i$을 비교하여 이중투표를 막을 수 있다.

4. 분석

본 논문은 서론에서 제시한 다음의 요구조건을 만족하고 있다.

□익명성(Anonymity): 투표용지는 익명의 채널을 통해서 전달되며, 그룹 서명을 적용하였기 때문에 투표자의 익명성이 보장된다. 특히, 그룹 매니저와 그룹 멤버 사이에 Oblivious Transfer를 적용한 값에, 시점 확인값을 추가하여 집계서버의 공개키로 암호화한 값을 이용하기 때문에, 그룹 멤버가 어떤 값을 가졌는지 알 수 없게 된다. 따라서 본 프로토콜에서는 익명성이 더욱 보장된다.

□부분적 결과산출 불가성(No partial results): 최종 집계는 모든 개표 검사원이 모였을 때만 가능한 것으로 한다. 개표 검사원 중 적어도 한 사람이 정직하다고 가정하면 부분적 결과산출은 불가능하다.

□대중적 검증(Public verifiability): 선거가 끝난 후에 집계서버의 비공개키 SKc를 공개하기 때문에 어느 누구라도 DB서버의 투표 값을 검증할 수 있다.

□합법성(Democracy): 외부 사용자가 그룹 멤버에 등록하기 위해서 오프라인을 통해 등록 프로토콜을 사용하여 인증서 (u_i, e_i)를 받게 되며, 투표를 하고자 하는 그룹 멤버는 (u_i, e_i)값을 가지고 그룹 서명을 하게 된다.

□이중투표 불가성(Unreusability): 서명 값 중 $\dashv$의 값이 투표에 대한 개인의 서명 값이므로, 각 투표자마다 유일하다. 따라서, 이중투표의 여부를 판단하기 위해서 DB서버에 등록되는 투표자의 서명 값 중 $\dashv$값을 확인하면 된다. 그리고, 한 명의 유권자가 이미 투표했는지를 검사하기 위해서 개표 검사원들은 현재의 서명 값과 이전의 서명 값들을 비교하면 된다. 집계서버는 6번 과정에서 얻은 값과, 투표자가 DB서버에 올린 7번 값을 복호화한 값을 비교하여 이중투표를 막을 수 있다.

III. 결론

본 논문에서는 그룹 서명의 개념을 전자투표 시스템에 적용하기 위해서 변형된 그룹 서명을 제안하였다. 또한, 본 논문에서는 그룹 서명의 개념을 적용하고 있기 때문에, 투표 값에 대한 서명을 검증하기 위해서 하나의 그룹 공개키만으로 검증이 가능하며, 그룹 서명을 적용한 기존의 전자투표 시스템[15]의 단점을 극복하였다.

참고문헌

[1] J. Camenisch, M. Michels. "A group signature scheme with improved efficiency," *Asiacrypt'98,* LNCS vol. 1514, Springer-Verlag, pp. 160-174, 1998.

[2] J. Camenisch, M. Michels. "A group signature scheme based on am rsa-variant," BRICS Technical Report RS-98-27(A prelininary version of this paper appeared *Asiacrypt'98*), Nov 1998.

[3] E. Fujisaki, T. Okamoto. "Statistical zero-knowledge protocols to prove modular polynomial relations," *CRYPTO'97*, volume 1294 of LNCS, pp. 16-30. Springer Verlag, 1997.

[4] A. Lysyanskaya, Z. Ramzan. "Group blind signature: A scalable solution to electronic cash," *Financial Cryptography(FC'98)*, volume 1465 of LNCS, pp. 184-197 Springer-Verlag, 1998

[5] C. Popescu. "An efficient group blind signature scheme based on the strong RSA assumption," *Romanian Journal of Information Science and Technology*, Volume 3, Number 4, pp.365-374, 2000

[6] Fujioka, Okamoto, Ohta, "A practice secret Voting Scheme for Large Scale Elections," *Asiacrypt'92*, 1992

[7] A. Fujioka, M. Abe, M. Ohkubo, F. Hoshino, "An Implementation and an Experiment of a Practical and Secure Voting Scheme," *SCIS2000*

[8] K. Kim, J. Kim, B. Lee, and G. Ahn, "Exprimental Design of Worldwide Internet Voting System using PKI," *SSGRR2001*, L'Aquila, Italy, Aug.6-10, 2001

[9] D. Chaum, E. van Heyst. "Group Signatures," In D. W. Davies, editor, *EUROCRYPT'91*, volume 547 of LNCS, pages 257-265. Springer-Verlag, 1991.

[10] D. Chaum. "Blind signature system," In D. Chaum, editor, Proc. *CRYPTO 83*, New York, Plenum. press, 1984.

[11] Z. Ramzan. "Group Blind Digital

Signature: Theory and Applications." master's thesis, http://theory.lcs.mit.edu/~cis/theses/ramzanms.pdf

[12] G. Ateniese, J. Camenisch, M. Joye, G. Tsudik. "A Practical and Provably Secure Coalition-Resistant Group Signature Scheme," In L. Bellare, editor, *CRYPTO'2000,* volume 1880 of LNCS, pp. 255-270. Springer-Verlag, 2000

[13] M. Ohkubo, F.Miura, M.Abe, A. Fujioka, T. Okamoto: "An Improvement on a Practical Secret Voting Scheme," *ISW.* 225-234, 1999:

[14] A. Fujioka, T. Okamoto, K. Ohta. "A Practical Secret Voting Scheme for Large Scale Elections," *AUSCRYT '92,* LNCS 718, Springer-Verlag, Berlin, pp.244-251 1993.

[15] T. Nakanishi, T. Fujiwara, H. Watanabe. "A Linkable Group Signature and Its Application to Secret Voting," Trans. *IPS.* Japan. Vol.40, No.7, pp. 3085-3096, July 1999.

[16]http://210.107.131.31/cipher/purpose/overview.jsp

[17] L. Harn and H. Lin, "Non-Interactive Oblivious Transfer," *Electronic Letters,* Vol. 26, No.10, pp. 635 - 636, 1990.

[18] L. Harn and H. Lin, "An Oblivious Transfer Protocol and its Application for the Exchange of Secrets," *Asiacrypt'91,* pp. 187 - 190, 1991.

[19] D. Chaum, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA," *EUROCRYPT '88,* LNCS 330, Springer-Verlag, Berlin, pp.177-182, 1988.

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

[21] M. Abe, "Universally Verifiable Mix-Net with Verification Work Independent of The Number Of Mix-Servers," *EUROCRYPT '98,* LNCS 1403, Springer-Verlag, Berlin, pp.437-447, 1998.

[23] J. Benaloh and M. Yung, "Distributing the Power of a Government to Enhance the Privacy of Votes," *Proceedings of the 5th ACM Symposium on Principles of Distributed Computing,* pp. 52-62, Aug. 1986.

[24] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung, "Multi-Authority Secret-Ballot Elections with Linear Work," *EUROCRYPT '96,* LNCS 1070, Springer-Verlag, Berlin, pp. 72-83, 1996.