석사 학위논문

비밀공유 방식과 익명통신로를 이용한 전자선거 프로토콜에 관한 연구

A Study on Electronic Election Protocols Using Secret Sharing Scheme and Anonymous Channels

허 원 근 (□ □ 根)

공학부

한국정보통신대학원대학교

2000

비밀공유 방식과 익명통신로를 이용한 전자선거 프로토콜에 관한 연구

A Study on Electronic Election Protocols Using Secret Sharing Scheme and Anonymous Channels

A Study on the Electronic Election Protocols Using Secret Sharing Scheme and Anonymous Channels

Advisor : Professor Kwangjo Kim

by

Weonkeun Huh
School of Engineering
Information and Communications University

A thesis submitted to the faculty of Information and Communications University in partial fulfillment of the requirements for the degree of Master of Science in the School of Engineering.

Taejon, Korea
December 14, 1999
Approved by

Professor Kwangjo Kim
Major Advisor

비밀공유 방식과 익명통신로를 이용한 전자선거 프로토콜에 관한 연구

허 원 근

위 논문은 한국정보통신대학원대학교 석사학위논문으로 지도교수위원회의 논문심사에 통과되었음을 인정합니다.

1999 년 12 월 14 일

지도교수위원회 위원장 김 광 조 인

위 원 이 영 희 인

위 원 유 찬 수 인

MS Weonkeun Huh

A Study on Electronic Election Protocols Using Secret Sharing Scheme and Anonymous Channels

1998112 허원근

비밀공유 방식과 익명통신로를 이용한 전자선거 프로토콜에 관한 연구

School of Engineering, 1999, 64 Pages
Advisor: Prof. Kwangjo Kim
Text in Korean

Abstract

The requirements of the electronic election protocols are built with lots of cryptographic techniques. The anonymous channels using the secret sharing have an advantage of improving the security as the basic tools satisfying the privacy. In this paper, we propose that the “t mixes by user’s selection” randomly distributes the load by t mix servers parallel doing the randomization and permutation and decryption of the messages. The “t mixes by user’s selection” has the secret dealer take the minimized participation so that the fairness is increased in electronic elections. Also as the works of the mix servers are managed by the quorum data the total workflow will not be stopped when a mix server may occurs an error.

The secret sharing is the useful technique increasing the security, but the means is needed to justify that if the secret shares are valid and if the shares are valid to construct the secret. It is possible for anyone to verify the validity of the shares in PVSS because of using the public key. And because the function of secret sharing is done well even though the administrator does not know the shares, the secret key of an administrator remains secretly after the opening the votes in the application like the electronic election. In this paper, using the PVSS we propose the universally verifiable multi-way electronic elections and the limited verifiable receipt-freeness multi-way electronic elections. Those methods are suitable for the large scale electronic voting with lots of voters and several candidates.

Contents

List of Figures

List of Tables

Ⅰ. 서론

1.1 연구 배경 및 목적

전자선거란 최소한의 물리적 투표소를 이용하면서 안전성이 확보된 암호 알고리즘으로 프로토콜을 구성하여, 실제 선거과정들을 네트워크상에서 구현한 가상 공간상의 전자적인 선거 행위로 투표의 비밀성, 완전성, 공정성, 검증성 등이 보장되는 것이다. 전자선거의 형태로는 투표 방식에 따라 찬반 투표(YES/NO voting)와 다수후보 투표(multi-way voting)로 구분할 수 있고 선거 규모에 따라서는 소규모, 중규모, 대규모로 나눌 수 있다. 전자선거는 통상 유권자(또는 투표자), 선거관리자 및 공개게시판(또는 계수자)으로 불리는 참여자들로 구성된다. 전자선거 프로토콜은 선거관리자와 투표자, 투표자와 공개게시판 또는 선거관리자와 공개게시판 등 참여자들 간에 주고 받는 투표 진행에 따른 결과들을 전송하는 규약으로 암호기법들을 적용하여 구성된다.

암호기법에 의한 전자선거는 안전성, 편리성, 공간성, 시간성 및 이동성 등에서 우수하다. 반면에 개표에 사용되는 선거관리자용 비밀키의 도난이나 훼손 등은 선거전체를 중단시킨다. 이러한 장애에 대비하기 위하여 사용하는 기법이 비밀 공유(secret sharing)[Sha79][Bla79] 기법이다. t-1차 다항식을 이용하여 n명의 참여자들에게 비밀을 분산하여 보관하고, 필요 시 t명이 모여서 비밀을 복원한다. 참여자들에게는 비밀을 복원할 수 있는 권한이 부여된다. 이 방식은 (t,n)-threshold 기법으로써 일부 참여자의 장애 발생에도 비밀을 복원할 수 있으므로 안전성이 향상된다.

전자선거 프로토콜에서 안전성과 더불어 가장 중요한 사항은 투표자의 프라이버시 보호이다. 투표자의 투표값이 암호화되어 전달되더라도 통신상의 트래픽 분석으로 투표자와 메시지의 관계가 노출되면 개표결과와 투표자의 연결이 가능해지므로 프라이버시 보호를 위한 별도의 방법이 필요하다. 믹스-넷[Cha81] 일명 익명통신로[PIK93]가 그 대안으로써 메시지의 입력과 출력의 관계에서 크기, 순서, 시간 및 값에 의한 연관성을 찾을 수 없게 한다. 익명통신로는 메시지의 송신자와 수신자 그리고 믹스서버들로 구성된다. 믹스서버에서 입력과 출력의 연관성을 찾을 수 없도록 하는 방법으로는 다단계 암호화 또는 복호화 및 임의 조합의 방법들이 사용된다.

익명통신로를 이용하는 전자선거에서는 믹스서버가 선거관리자의 역할을 대신한다. 그러므로 선거관리자용 비밀키의 분배의 경우와 같이 (t,n)-threshold 비밀공유기법을 이용하여 일부 믹스서버의 장애나 속임에 대한 대비를 할 수 있어야 된다.

본 연구는 비밀공유방식을 적용한 익명통신로에서 난수화, 조합, 그리고 복호화를 행할 t 믹스를 형성하는 방법과, 비밀공유기법의 공개검증 방식인 PVSS를 이용한 다중(multi-way) 전자선거를 제안함을 목표로 한다. 제안하는 전자선거는 검증성을 제공하는 방식과 실제 선거에서처럼 검증성을 제한하는 대신에 선거의 중요한 성질인 매표방지성(receipt-freeness)을 제공하는 방식을 함께 제시함을 목표로 한다.

1.2 연구 내용 및 범위

본 논문에서는 사용자 선택에 의한 t믹스-넷 방식을 제안하였다. 사용자가 메시지를 믹스-넷으로 송신할 때 선택한 t개의 믹스서버들로 구성된 정족수 데이터를 함께 보낸다. 이 데이터에 포함된 믹스서버들은 메시지에 대한 난수화 및 조합을 행하고 정족수 데이터를 수정한다. 그리고 정족수중 아직 작업을 수행하지 않은 믹스서버들 중 하나에게로 전송한다. 임의 순서로 t개 믹스서버들이 메시지의 난수화 및 조합을 수행함으로써 부하가 분산된다. 사용자에 의한 정족수 구성은 비밀분배자의 관여를 최소화하여 전자선거의 공정성을 향상시키기도 한다. 또한 정족수 데이터에 의해 믹스서버들의 작업 과정이 관리됨으로써 믹스서버의 장애 시에 전체 작업의 중단없이 해당 메시지를 재처리 할 수 있도록 한다.

전자선거 프로토콜이 선거로써의 기능을 수행하기 위해서는 충족해야 할 요구사항들이 있다. 본 논문에서는 이들을 분류하고 이의 충족에 사용되는 암호기법들을 요구사항별로 정리하였다. 현재까지의 주요 전자선거 프로토콜들을 분석함으로써 암호기법들이 요구사항 충족에 어떻게 적용되었으며 해결되지 못한 문제점들이 무엇인지를 함께 기술하였다.

암호기법들중 비밀공유기법은 안전성을 증진하는 유익한 기법이지만 분배자가 배분하는 비밀 조각이 유효한지와 비밀 복원 시 참여자가 제출하는 비밀 조각이 유효한지를 판단할 수 없다는 것이다. 이에 대한 해결책으로 검증 가능한 비밀 공유(verifiable secret sharing : VSS) 기법이 제시되었다[CGMA85]. VSS는 참여자가 자신의 비밀조각이 유효한지 검증해 볼

수 있으며 또한 정직한 참여자들에 의해서 비밀이 복원될 수 있는 개념이다. [CGMA85]에서 제시된 VSS 구조의 예는 공개적으로 검증가능하지는 않았다. Stadler는 참여자들의 공개키를 비밀 공유에 사용하여 공개적으로 검증가능한 비밀공유(publicly verifiable secret sharing : PVSS) 구조를 제시하였다[Std96]. Schoenmaker는 Stadler의 PVSS에 개선된 효율성과 비밀복원시의 유효성 증명을 추가하고, PVSS의 준동형 성질을 이용한 응용의 예로 찬반 전자선거를 제안 하였다[Sch99].

본 논문에서는 [Sch99]의 전자선거의 단점들인 분배자, 투표자 및 선거관리자가 구별되지 않는 점, 찬반 투표로 국한된 점, 0 또는 1로 제시되는 투표값 계산이 이산대수 문제이므로 투표자 수가 적어야 하는 점등을 개선한 전자선거 프로토콜을 제안하였다. 제안된 전자선거는 PVSS를 이용한 다중 전자선거로 2개 방식이다. 첫번째는 분배자 대신에 사용자(투표자)가 비밀을 선택하고 선거관리자들에게 분배하는 모델을 도입하여 전자선거 프로토콜의 요구사항인 전체검증성이 구현되도록 하였다. 둘째는 분배자가 관여하는 모델로 사용자(투표자)가 보내는 메시지를 분배자가 재 암호화하도록 하여 매표방지성을 구현하도록 하였다.

1.3 논문 구성

본 논문은 총 4개장으로 구성된다. 2장에서는 전자선거 프로토콜의 기반기술로 사용되는 비밀공유방식 및 익명통신로를 기술하고, 사용자 선택에

의한 t 믹스-넷 방식을 제안하고 분석한다. 3장의 앞 부분은 전자선거 프로토콜의 요구사항과 적용되는 암호기법에 관하여 기술하고 현재까지의 주요 전자선거 프로토콜을 분석한다. 뒷 부분은 비밀공유기법의 일종인 PVSS를 이용한 다중 전자선거 방식에 대하여 제안하고 분석한다. 4장에서는 결과와 향후 연구 방향을 기술함으로서 끝맺음을 한다.

Ⅱ. 비밀공유방식 및 익명통신로

비밀공유방식은 암호화에 사용되는 비밀키등의 안전성을 향상하기 위한 기법으로 사용자의 프라이버시 보호에 사용되는 익명통신로(또는 믹스-넷) 구성 기술과 함께 사용된다. 본 장에서는 비밀공유방식의 유형과 익명통신로 구성 방식에 대하여 알아보고, 익명통신로상에서 믹스서버가 입력과 출력의 관계를 숨기기 위하여 행하는 난수화 및 조합, 그리고 메시지의 복호화에 대한 방법을 제안하고 분석한다.

2.1 비밀공유 방식

2.1.1 (t,n)-threshold 비밀공유 방식

비밀공유(secret sharing : SS) 구조는, 사용자 집합 U 와 U 중에서 권한이 부여된 부분집합을 A라 할 때, A에 속하는 어떠한 부분집합도 비밀을 복원할 수 있는 단일 접근 구조(monotone access structure)를 사용한다. 널리 사용되는 Shamir의 (t,n)-threshold 구조는 $t-1$차 다항식을 이용하는 단일 접근 구조이다:

$$p(x)=\sum_{j=0}^{t-1}\alpha_j x^j \quad , \quad s=\alpha_0 . \tag{2-1}$$

분배자가 비밀하게 선택한 식 (2-1)의 다항식 $p(x)$를 이용하여 n명의 참여자들에게 비밀 조각 $p(i)$를 분배한다. 비밀복원은 n명의 참여자중

임의의 t 명이 모여 Lagrange interpolation 공식[MOV96]으로 식 (2-2)와 같이 $p(x)$를 구하면 비밀 s를 복원하게 된다:

$$p(x) = \sum_{i=1}^{t} p(i) \prod_{1 \le j \le t, j \ne i} \frac{x - x_j}{x_i - x_j}, \quad (2\text{-}2)$$

즉, $p(0) = \alpha_0 = s$ 이다. 비밀 값 s는 다음 식으로도 구할 수 있다.

$$s = \sum_{i=1}^{t} p(i)\lambda_i, \quad (\lambda_i = \prod_{1 \le j \le t, j \ne i} \frac{x_j}{x_j - x_i}) \quad (2\text{-}3)$$

이 방식에서의 문제점은 분배된 비밀의 유효성을 확인할 방법을 제공하고 있지 않다는 점이다. 즉, 분배된 비밀 조각이 정당한지에 대하여 검증할 방법이 제공되어야 하겠다. [CGMA85]에 검증 가능한 비밀공유방식(verifiable secret sharing : VSS)의 개념을 제시하고 그 구조를 제안하였으나, 제안된 구조가 검증가능하지 않음이 밝혀졌다.

2.1.2 공개적으로 검증가능한 비밀공유(PVSS) 방식

Stadler는 참여자들의 공개키를 비밀 공유에 사용하여 공개적으로 검증가능한 비밀공유(publicly verifiable secret sharing : PVSS) 구조를 제시하였다[Std96]. [FO98]과 [Sch99]에서는 Stadler의 PVSS 방식을 개선하여 효율성을 증대시키고 비밀의 분배 및 복원이 정당하게 행하여졌음을 증명하였다. PVSS는 비밀공유에 공개키를 사용하는 방식으로 비밀조각에

대해서는 직접적으로 알지 않더라도 비밀공유 기능을 수행할 수 있는 방식이다. 이러한 장점으로 전자선거에 응용되는 경우 선거관리자의 비밀키를 노출시키지 않게 되고, 비밀키의 재 사용이 가능하게 된다. [Sch99]에서 제시된 PVSS는 다음과 같다.

그룹 $G_q \ (q : prime)$, 생성자 g와 G, 그리고 참여자 $P_i \ (1 \le i \le n)$가 있다. P_i의 개인 키를 $x_i \in Z_q^*$, 공개키는 $y_i = G^{x_i}$라 하자. 이 때, 분배자는 비밀 s의 조각 s_i인 $p(i) \ (1 \le i \le n)$를 참여자의 공개키 y_i를 이용하여 식 (2-4)와 같이 분배한다:

$$Y_i = y_i^{p(i)} \tag{2-4}$$

다항식의 계수 α_j를 $C_j = g^{\alpha_j}$로 공지하고, $X_i = \prod_{j=0}^{t-1} C_j^{i^j}$라 한다. 비밀의 분배자는 식 (2-5)를 만족하도록 유일한 $p(i)$의 proof of knowledge를 생성함으로써 비밀 분배를 옳게 했음을 보일 수 있다.

$$X_i = g^{p(i)}, \quad Y_i = y_i^{p(i)} \tag{2-5}$$

비밀의 복원 과정은 우선 P_i가 자신의 개인키 x_i로 $Y_i^{1/x_i} = G^{p(i)}$를 계산한다. $S_i = G^{p(i)}$와 식 (2-6)을 만족하는 proof of knowledge를 함께 공지한다.

$$y_i = G^{x_i}, \quad Y_i = S_i^{x_i} \tag{2-6}$$

복구하고자 하는 비밀 s의 지수승한 $S = G^s$를 식 (2-7)과 같이 누구나 구할 수 있게 된다.

$$\prod_{i=1}^{t} S_i^{\lambda_i} = \prod_{i=1}^{t} (G^{p(i)})^{\lambda_i} = G^{\sum_{i=1}^{t} p(i)\lambda_i} = G^{p(0)} = G^s \tag{2-7}$$

$S = G^s$는 비밀 조각 $p(i)$를 모르고서도 구할 수 있으며, 참가자 P_i는 자신의 비밀키 x_i를 노출시키지 않고서도 S를 생성할 수 있도록 하였다.

2.2 익명통신로

입력 항목으로부터 어떤 출력 항목을 만들어 낼 때 둘 간의 관계를 숨겨야 할 응용들이 존재한다. 예를 들어, 전자선거를 비밀투표에 이용할 경우에 투표자와 투표 값을 연결하는 방법을 차단해야 한다. 즉, 통신로를 누구나 도청할 수 있다고 가정한다면 값의 암호화만으로는 메시지와 그 송신자와의 관계를 숨기지는 못한다. D.L. Chaum[Cha81]이 암호기법을 이용하여 이 문제를 해결한 믹스-넷(익명통신로)을 처음으로 제시하였다

2.2.1 암호시스템의 적용

Chaum은 RSA 암호시스템을 사용하여 믹스-넷을 구성하였다. Chaum 방식은 송신자, 믹스서버 및 수취인으로 구성된다. 송신자는 K_1 (믹스서버의 공개키), A(수취인의 주소), K_a(수취인의 공개키)과 난수 R_1 및 R_0를 이용하여 메시지 M을 식 (2-8)의 왼편과 같이 암호화 하여 믹스서버에 보낸다. 믹스서버는 자신의 개인키로 복호화를 행하여 얻은 식 (2-8)의 오른편 값을 수취인에게 보낸다. 믹스서버가 정직하다면 RSA 암호시스템의 안전성과 동등하게 입력과 출력의 관계는 숨겨진다.

$$K_1(R_1, K_a(R_0, M), A) \rightarrow K_a(R_0, M), A \qquad (2\text{-}8)$$

이를 $K_n(R_n,\ldots, K_2(R_2, K_1(R_1, M))\ldots)$과 같이 n 믹스 서버 모델로 확장할 수 있다. Chaum의 믹스-넷 방식의 단점은 믹스 서버의 수에 비례하여 메시지가 확장되며 하나의 믹스 서버의 장애로 인하여 전체 진행이 중단될 수 있다. Park, Itoh, Kurosawa는 ElGamal 암호시스템[ElG85]을 도입하여 메시지 확장의 문제를 해결하고 있다[PIK93].

ElGamal 암호시스템은 그룹 G_q(q는 큰 소수), 그룹에서의 생성자 g가 있을 때, g를 기저로 하는 이산대수 문제를 계산하는 것이 어렵다는 사실을 이용한다. ElGamal 암호에서 어떤 사용자의 비밀키가 $s \in_R Z_q^*$일 때 공개키는 $H = g^s$이다. 메시지 m의 암호화는 임의의 난수 r을 사용하여 $(x, y) = (g^r,\ H^r m)$으로 한다. 복호화는 y를 x의 s승한 값으로 나누면 $y/x^s = (H^r m)/(g^r)^s = g^{sr} m / g^{rs} = m$이 되어 원래의 메시지 m을 얻을 수 있다.

ElGamal 암호시스템을 사용한 [PIK93]의 믹스-넷 방식을 살펴보면, 믹스서버의 개인키 X_i, 공개키 $Y_i(1 \le i \le k)$ 일 때 송신자는 난수 R을 선택하여 식 (2-9)의 첫번째 줄과 같이 계산하여 첫번째 믹스서버에게 보낸다. 믹스서버들은 식 (2-10)의 함수를 이용하여 식 (2-9)의 둘째 줄부터 마지막까지의 계산을 차례로 한다. k 번째 믹스서버는 결과 $B_i \, o E_{B_i}(m_i)$를 얻고 공개게시판(수취인에 해당)에 게시한다.

$$
\begin{aligned}
(C_{0i}, \quad C_{1i}) &= (g^R, \quad (B_i \, o E_{B_i}(m_i)) \times (Y_1 \cdots Y_k)^R) \\
&\rightarrow (g^{R_1}, \quad (B_i \, o E_{B_i}(m_i)) \times (Y_2 \cdots Y_k)^{R_1}) \\
&\qquad\qquad \vdots \\
&\rightarrow (g^{R_{k-1}}, \quad (B_i \, o E_{B_i}(m_i)) \times (Y_k)^{R_{k-1}}) \\
&\rightarrow B_i \, o E_{B_i}(m_i)
\end{aligned}
\tag{2-9}
$$

$$
f_j(t,u,r) \equiv \left\{ \begin{array}{ll} (t \times g^r, u \times (Y_{j+1} \cdots Y_k)^r / t^{X_j}) & if \;\; 1 \le j \le k-1 \\ u / t^{X_k} & if \;\; j = k \end{array} \right\}
\tag{2-10}
$$

[PIK93]의 믹스-넷에서도 Chaum의 방식과 마찬가지로 하나의 믹스서버의 장애에 의해 복호화가 중단되는 문제는 그대로 존재한다. 또한 ElGamal 암호시스템의 단점인 malleability 공격에도 취약하다.

2.2.2 비밀공유기법의 적용

일부 믹스서버의 장애 또는 공모로 믹스-넷이 중단되는 것을 방지하기 위하여 비밀공유기법이 사용된다. 즉, 믹스-넷을 구성함에 있어서 일부 믹스의 장애나 부정 행위에 대하여 안전성을 확보할 필요가 있다. [Abe98]에서 제시된 비밀공유기법의 임계치(threshold) 믹스-넷은 난수화와 조합 및 임계치 ElGamal 복호화를 행하는 방식으로 다음과 같다.

난수화와 조합

비밀 x를 [Sha79]의 방식으로 n믹스서버들이 공유하고 암호화 키 $y = g^x$가 공개된다. 각 믹스서버의 비밀조각 x_i는 $y_i = g^{x_i}\ (1 \le i \le n)$로 공개된다. 사용자에 의해 보내진 공개게시판상의 암호화된 메시지 목록은 $(C_{0,j}, G_{0,j})$로 $C_{0,j} = v_j y^{t_{0,j}}$이고 $G_{0,j} = g^{t_{0,j}}\ (1 \le j \le L)$이다. v_j는 메시지이고 $t_{0,j}$는 난수로 [Pfi94]의 공격을 방지하기 위하여 사용자는 $t_{0,j}$의 인지증명을 한다.

믹스서버들은 식 (2-11)과 같이 난수화 및 조합을 수행하여 입력과 출력의 관계를 숨긴다. L개의 메시지들의 모든 가능한 조합은 Π_L으로 표기하고 $\pi_i \in \Pi_L$이다.

$$
\begin{aligned}
, &:= {}_{-1,\pi_i(\ )}{}^{t_{i,\pi_i(j)}} \\
, &:= {}_{-1,\pi_i(\ )}g^{t_{i,\pi_i(j)}}\ (1 \le i \le n),\ (1 \le j \le L) \qquad \text{(2-11)}
\end{aligned}
$$

n 믹스서버들이 차례로 난수화 및 조합을 수행하여 얻어진 결과가 식 (2-12)이며, 식 (2-12)의 $(C_{n,j}, G_{n,j})\ (1 \le j \le L)$는 인지증명에 의해 유효성이 증명된 입력과 출력의 관계가 감추어진 메시지 목록이다..

$$, := \quad 0,\pi(\ ) \quad \hat{t}_{n,j}$$

$$, := \quad 0,\pi(\ ) \quad g^{\hat{t}_{n,j}}\ (\hat{t}_{n,j} = \sum_{i=1}^{n} t_{i,\pi_i(j)}) \qquad (2\text{-}12)$$

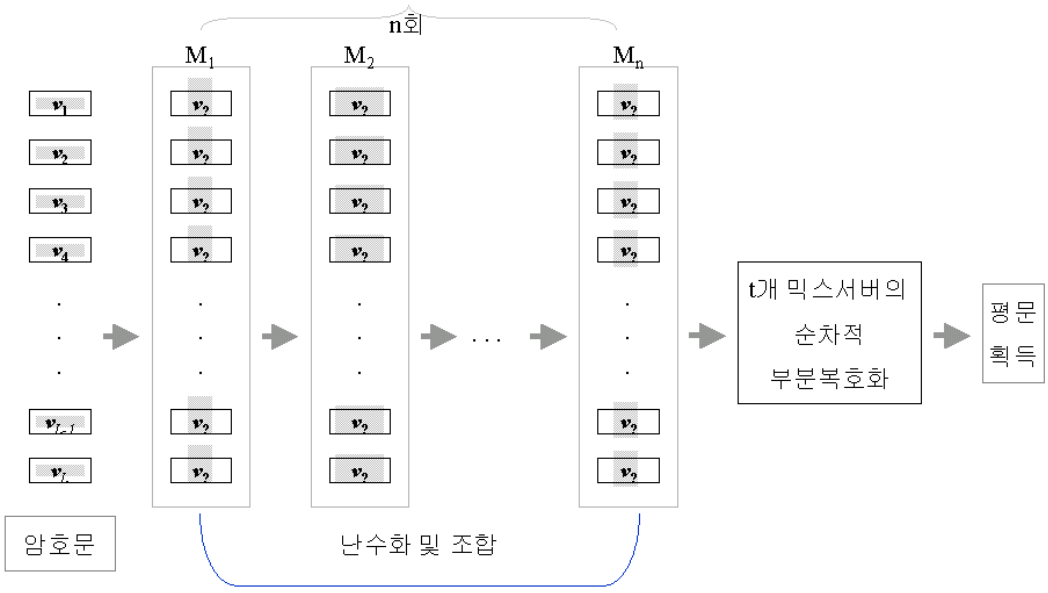

그림 2-1: [Abe98] 믹스-넷의 순차처리 난수화 및 조합

임계치 ElGamal 복호화

최종적으로 메시지 v_j를 얻기 위하여 정족수 $Q=\{1,...,t\}$에 속하는 믹스서버들이 협조한다. 믹스서버 $i\in Q$는 $(C_{n,j},G_{n,j})$에 대한 복호화를 $W_{i,j}:=W_{i-,j}G_{n,j}^{x_i\lambda_i}$ $(W_{0,j}=1)$ $(\lambda_i=\prod_{1\le k\le t,k\neq i}\frac{x}{x-x_i})$과 같이 하고 모든 $W_{i,j}$를 다음 차례의 믹스서버에게 보낸다. 마지막 믹스서버가 $W_{t,j}$를 공지하면 $C_{n,j}/W_{t,j}$를 계산하여 v_j를 얻는다.

모든 t 믹스서버들이 옳게 작업한다면 식 (2-13)의 결과를 얻을 수 있으며, 인지증명에 의해 작업의 유효성을 증명한다.

$$W_{,}=\prod_{=1}G_{,}^{x_i\lambda_i}=G_{,}^{\sum_{i=1}^{t}x_i\lambda_i}=G_{,}^{x} \qquad (2\text{-}13)$$

[Abe98]의 믹스-넷은 모든 믹스서버들이 순차적인 방법으로 작업을 하는 형태를 제시하고 있다(그림 2-1 참조). 믹스서버의 장애에 대한 관리 방법이 제시되어 있지 않기 때문에 장애 발생시에는 재작업을 하여야 한다. 또한 복호화를 행할 믹스서버들의 정족수 구성 방법에 대한 언급도 없다.

2.3 사용자 선택에 의한 t 믹스-넷 방식 제안

앞 절에서 언급한 비밀공유기법을 이용하는 [Abe98]의 믹스-넷에서 유효한 t 믹스서버들을 결정하는 문제를, [CGS97]에서는 분배자(dealer)가

결정토록 했다. 이 경우에 공유된 비밀의 복원(복호화)에 분배자가 관여하는 (t,n)-threshold 형태가 됨으로써 분배자에게 모든 역할이 집중된다. 그리고 분배자가 유효한 t 믹스서버들을 선정하더라도 어떤 장애가 t 믹스서버들 중에서 일어날 가능성은 항상 존재함으로 t 믹스서버들의 작업과정을 관리하는 방법이 제시되어야 한다. [Abe98]에서 믹스서버들의 난수화 및 조합, 그리고 t 믹스서버들에 의한 복호화는 순차적으로 진행되도록 구성되었다. 따라서 하나의 믹스서버의 처리가 끝난 후 다음 믹스서버가 복호화를 하기 때문에 작업의 부하가 작업중인 믹스서버에 집중된다. 이 같은 문제를 다음에 제안하는 사용자 선택에 의한 t 믹스-넷 방식에 의해서 해결한다.

사용자 선택에 의한 믹스-넷 개념

(t,n)-threshold 믹스-넷 구조에서는 시스템 변수를 설정하는 분배자의 역할이 중요하다. 분배자는 비밀을 분배할 다항식을 선정하고 다항식을 이용하여 믹스서버들에게 비밀조각을 분배한다. 비밀에 대응하는 공개키는 모두에게 공개한다(준비단계). 준비가 완료된 후 사용자들은 자신의 메시지를 공개키로 암호화하여 믹스-넷으로 보낸다(암호송신단계). 그림 2-2와 같이 믹스서버들은 메시지의 송신자와 메시지의 관계를 단절시키기 위하여 난수로 재 암호화를 수행한다(난수화 단계). 믹스-넷에 보내진 메시지를 복호화 하기 위해서는 우선 t 믹스서버들을 선정하여야 하며, 이 단계(복호 단계)에 분배자가 다시 개입하게 된다[CGS97][Abe98][Jak98]. 결국 분배자는 전 과정에 영향을 미치게 되므로, 이러한 역할을 하는 분배자는 지극히 공정하고

신뢰할 만하다고 가정할 수 밖에 없다. 하지만 분배자의 거짓 또는 장애는 전 과정을 중단시킬 수 있으므로 암호송신이 시작되기 전인 준비단계까지만 관여하는 모델을 고려해 볼 가치가 있다. 그러면, 준비단계에서는 비밀이 분배되고 믹스들의 이상유무가 확인될 것이므로, 정상적으로 (t,n)-threshold 믹스-넷이 설정되었다고 가정할 수 있다.

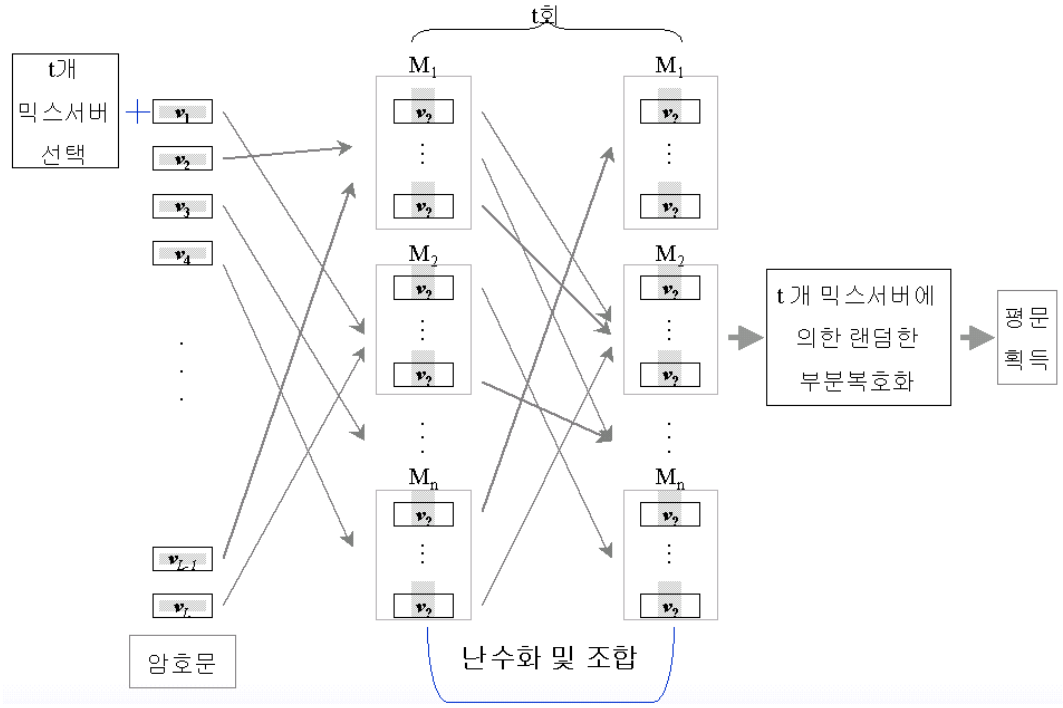

그림 2-2: 사용자 선택에 의한 t믹스-넷의 랜덤처리

기본 아이디어는, 분배자가 믹스서버들을 선정하는 대신에, 사용자가 t 믹스서버들을 선택하게 하는 것이다. 사용자는 n 개의 믹스서버들 중 t 개를 임의로 선택한다고 하자. 그러면 메시지 당 ${}_nC_t (t \le n)$ 가지의 처리 형태가 있을 것이다. 이러한 방식에는 다음과 같은 장점을 고려할 수 있겠다.

- 분배자의 개입을 제한하여 분배자의 부정을 최소화한다.
- 메시지 처리를 ${}_nC_t (t \le n)$ 경우로 난수화 할 수 있다.
- n 개의 믹스서버들로 부하를 분산하는 병렬 처리 믹스-넷을 구성한다.
- 사용자에 의한 (t,n)-threshold 방식을 구성할 수 있다.

이 방식에서 고려해야 할 사항으로는 장애가 발생한 믹스서버에 대한 대책이다. 네트웍상에서 장애 발생 믹스서버는 곧 파악이 되며 나머지 믹스서버들에게 공지된다. 장애 믹스서버를 거치는 메시지들은 별도로 처리하거나 $(n-t)$ 개 믹스서버들 중에서 대체할 수 있을 것이다. 사용자가 t 믹스서버들을 선정하는 믹스-넷에 대한 상세한 설명은 다음과 같다.

사용자 선택에 의한 믹스-넷 상세 모델

[준비 단계]

- 분배자는 비밀 x 를 [Sha79]의 방식으로 n 믹스서버들에게 분배하고 암호화 키 $y = g^x$ 를 공개한다. 각 믹스서버의 비밀 조각 x_i 는 $y_i = g^{x_i} \ (1 \le i \le n)$ 로 공개된다.
- 각 믹스서버들 $M_i \ (1 \le i \le n)$ 의 비밀 조각 $s_i = p(i)$ 를 개인키시스템 D_{M_i} 이라 하고, 이에 대응하는 공개키시스템을 E_{M_i} 이라 한다. 이 때 생성자는 α 를 사용한다.

[암호송신 단계]

- 사용자는 메시지를 믹스-넷의 공개키(암호화 키)로 암호화한다. 즉, 사용자 $A_j\,(1 \le j \le L)$의 메시지는 $(C_{0,j}, G_{0,j})$로 $C_{0,j} = v_j y^{t_{0,j}}$이고 $G_{0,j} = g^{t_{0,j}}$이다. $t_{0,j}$는 난수로 [Pfi94]의 공격을 방지하기 위하여 사용자는 $t_{0,j}$의 인지 증명을 한다.
- 사용자 A_j는 복호화를 수행할 t 믹스서버들(정족수 Q)을 선정하여 서명한 후 함께 보낸다. 선택한 t 믹스서버들을 표현하는 데이터 구조는 n비트 길이로써 t개의 1과 $n-t$개의 0으로 구성된다. 표 2-1의 데이터구조의 값의 범위는 $2^{t-1} + \cdots + 2^0 \le$ 값 $\le 2^{n-1} + \cdots + 2^{n-t}$. 예를 들어, (3,4)-threshold인 경우 7(0111)과 14(1110)의 범위에 있는 값들이다.

표 2-1: 메시지별 데이터구조의 2진 전개

비트 / 메시지	n^{th}	$n\text{-}1^{th}$	$n\text{-}2^{th}$	$\ldots i^{th} \ldots$	2^{nd}	1^{st}
v_1	1	0	1	…0…1 …	1	0
…	…	…	…	…	…	…
v_j	0	1	0	…1…0…	0	0
…	…	…	…	…	…	…
v_L	1	1	0	…0…0…	0	1

- 사용자 A_j는 데이터구조, 데이터구조에 대한 자신의 서명 값, 그리고 난수 r_j를 결합한 후 0이 아닌 비트(1로 설정된 비트)에 해당되는 믹스의 공개키로 암호화 한다. 데이터구조와 암호화된 메시지를 결합하여 공개게시판과 해

당 믹스서버에게 송신 한다. 표 2-1 의 예는 다음과 같다(→:전송).

$$v_1 \ : \ E_{M_n}(Sign_{A_1}(101\cdots10) \| (101\cdots10) \| r_1) \rightarrow M_n$$

$$v_j \ : \ E_{M_{n-1}}(Sign_{A_j}(010\cdots00) \| (010\cdots00) \| r_j) \rightarrow M_{n-1}$$

$$v_L \ : \ E_{M_{n-1}}(Sign_{A_L}(110\cdots01) \| (110\cdots01) \| r_L) \rightarrow M_{n-1}$$

[난수화 단계]

- 데이터구조에 명시된 믹스서버들(Q)은 식 (2-14)와 같이 난수화 및 조합을 한다. L 개의 메시지들이 n 믹스서버들로 균등 분배된다고 가정하면, 한 믹스서버에서의 모든 가능한 조합을 $\Pi_{L/n}$ 으로 표기하고 $\pi_i \in \Pi_{L/n}$ 이다.

$$\begin{aligned} &, \ := \ _{-1,\pi_i(\ )}{}^{t_{i,\pi_i(j)}} \\ &, \ := \ _{-1,\pi_i(\ )}g^{t_{i,\pi_i(j)}} \ (i \in Q), \ (1 \le j \le L) \end{aligned} \qquad (2\text{-}14)$$

- 난수화 및 조합을 수행한 믹스서버는 자신에 해당하는 비트를 0 으로 설정하고 서명한 후, 서명된 데이터구조와 원래의 데이터구조를 결합하여 나머지 t 믹스서버들 중 하나를 선택한다. 선택된 믹스의 공개키로 결합된 데이터구조를 암호화하고 메시지와 함께 보낸다.

- 식 (2-15)의 $(C_{Q,j}, G_{Q,j})\ (1 \le j \le L)$는 Q 에 속하는 마지막 믹스서버가 난수화 및 조합을 완료한 메시지이다.

$$\begin{aligned} &, \ := \ _{0,\pi(\ )}{}^{\hat{t}_{n,j}} \\ &, \ := \ _{0,\pi(\ )}g^{\hat{t}_{n,j}} \ (\hat{t}_{n,j} = \textstyle\sum_{i \in Q} t_{i,\hat{\pi}_i(j)}) \end{aligned} \qquad (2\text{-}15)$$

- 마지막 믹스서버는 사용자가 송신한 데이터구조를 공개한다.

[복호화 단계]

- $(C_{Q,j}, G_{Q,j})$의 복호화는 공개된 데이터구조에 속하는 믹스서버들이 자신들의 비밀조각과 $\lambda_i = \prod_{1 \le k \le t, k \ne i} \frac{x}{x - x_i}$ 값을 사용하여 계산한다. 계산 $W_{i,j} := W_{i-1,j} G_{Q,j}^{x_i \lambda_i}$ $(W_{0,j} = 1)$를 한 후 모든 $W_{i,j}$를 다음 차례의 믹스서버에게 보낸다. 마지막 믹스서버가 $W_{t,j}$를 공지하면 $C_{Q,j} / W_{t,j}$를 계산하여 v_j를 얻는다.

2.4 분석

[Abe98]의 믹스-넷 방식을 정리해 보면 모든 믹스서버가 참여하여 순차적으로 난수화 및 조합을 한다. 최종 믹스서버가 난수화 및 조합의 결과를 공개하면 정족수 Q의 믹스서버들이 협조하여 다시 순차적인 복호화로 원하는 메시지를 얻게 된다.

[Abe98]의 방식의 문제점들을 짚어보면 일부 믹스서버의 장애 시 관리 방법이 없으므로 재작업을 하여야 한다. 또한 순차적인 처리로 부하가 한 믹스서버에 집중되어 효율적인 작업처리가 되지 않는다. 그리고 정족수

구성에 분배자의 관여가 필요하게 된다. 이에 대한 해결책으로 제시된 사용자 선택에 의한 t 믹스-넷 방식을 정리해 보면 다음과 같다.

- 사용자가 t 믹스서버들의 선택에 관한 데이터구조를 만들고 암호화된 메시지와 함께 믹스-넷에 보낸다.
- t 믹스서버들의 작업사항이 데이터구조로 관리된다.
- 데이터구조에 의해 t 믹스서버들이 난수화 및 조합을 랜덤하게 수행한다.
- t 믹스서버들 중에서 발생하는 장애에 대한 처리는 별도로 규정한다.

t 믹스-넷 방식에서 고려할 사항은 믹스서버가 데이터구조를 변경할 가능성에 관한 것이다. 믹스서버가 정직하다면, 난수를 선택하여 메시지의 난수화 및 조합을 수행하고 데이터구조상에 자신의 비트를 0으로 설정한 후 서명을 하여 다음 차례의 믹스서버에게로 보낼 것이다. 정직하지 않다면, 난수화 및 조합을 옳게 행하지 않거나 사용자가 보낸 데이터구조를 변경할 것이다. 이 문제에 대한 대책은 다음과 같이 고려해 볼 수 있다.

- 메시지에 대한 난수화 및 조합을 옳게 했음은 proof of knowledge[Abe98]로 해결된다.
- 데이터구조 검증은 송신자의 데이터 구조에 대한 서명과 믹스서버들의 데이터구조에 대한 서명을 비교 검토함으로써 검증된다. 이 과정은 사전 준비단계에서 분배자가 배분한 $D_{M_i}\ (1 \le i \le n)$ 이 사용된다.

사용자로부터 메시지를 수신한 믹스서버는 난수화 및 조합을 수행하고 t-1 개의 믹스서버들 중 하나에게 메시지와 데이터구조를 전송하면 된다. 즉,

사용자가 t 믹스서버들을 랜덤하게 선택하는 것과 동일하게 t 믹스서버들 중에서의 다음 믹스서버 선택도 랜덤하게 진행된다. 다음으로는 믹스서버에 장애가 발생했을 경우의 처리방법에 대하여 고찰해 보자. 통상 네트워크 상에서 장애가 발생한 서버를 감지해 낼 수 있듯이, 믹스서버의 장애는 나머지 믹스서버들에게 알려진다는 가정을 채택한다.

[정상적인 믹스서버에서의 장애처리 방법]

- 정상적인 믹스서버들은 데이터구조로부터 장애 발생 믹스서버와 관계되는 메시지들을 파악한다. 즉, 현재 보유중인 메시지들의 데이터구조상의 비트를 검사함으로써 장애 발생 믹스서버가 작업을 수행했는지를 확인할 수 있다.
- 장애 믹스서버가 이미 처리한 메시지는 관계없이 진행된다.
- 장애 믹스서버를 포함하는 메시지를 장애 믹스서버가 처리하지 않은 경우에는, 현재 메시지를 유지하고 있는 믹스서버가 다음과 같이 새로운 데이터구조를 구성한다.

> [새로운 데이터구조 구성] : $n-t$ 개 믹스서버 중 하나를 장애 믹스서버와 교체하여 데이터구조를 구성한다. 새롭게 구성된 데이터구조와 데이터구조에 대한 서명 값을 다음 믹스서버의 공개키로 암호화 하여 게시한다. 사용자가 보낸 데이터구조도 함께 게시한다.

[장애 믹스서버의 장애 처리 방법]

- 장애 발생 믹스서버는 나머지 믹스서버들에게 인지됨으로 장애 믹스서버에서 처리 중이던 메시지의 이전 믹스서버와의 연결은 데이터베이스에서의

triggering 기법과 유사한 방법으로 해결이 가능하다. 즉, 장애 믹스서버에서 메시지의 난수화 및 조합이 완료되어 다음 차례의 믹스서버로 작업이 넘어가기 전에 장애가 발생하면 triggering 에 의해 이전 믹스서버로 되돌려 진다. 그러면 앞서의 정상적인 믹스서버에서의 장애 처리 방법과 같이 새로운 데이터 구조를 구성하여 처리한다.

표 2-2는 [Abe98]의 믹스-넷과 "사용자 선택에 의한 t 믹스-넷" 방식을 비교한 것으로, 사용자의 선택정보는 n 비트 크기의 데이터구조를 사용한다.

표 2-2: [Abe98]의 믹스-넷과 사용자 선택에 의한 t 믹스-넷의 비교

항목	[Abe98]의 믹스-넷	사용자 선택에 의한 t 믹스-넷
접근 방식	비밀분배자 중심	사용자 중심
분배자개입	준비단계 및 복호화 단계	준비단계
메시지의 난수화 방법	1 가지 방식	${}_nC_t$ 가지 방식
메시지의 복호화	정족수에 의한 순차처리	정족수에 의한 랜덤처리
작업 형태	순차 처리	랜덤 처리
작업 부하	1개 믹스서버에 부하 집중	n개 믹스서버로 부하 분산
장애 관리	장애관리 방법 제시하지 않음	n 비트 데이터구조와 믹스상호간 작업처리비트로 관리

Ⅲ 전자선거 프로토콜

전자선거 프로토콜은 실제 선거를 대체하기 위한 요구사항들을 가지고 있으며, 이를 충족시키는 방법으로 다양한 암호기법들이 사용된다. 암호기법의 적용에는 안전성과 효율성이 고려되어야 하며 만족시키고자 하는 요구사항중 상호 배타적인 속성에 관하여는 현실적인 선거와의 관계를 고려하여 적용을 검토한다.

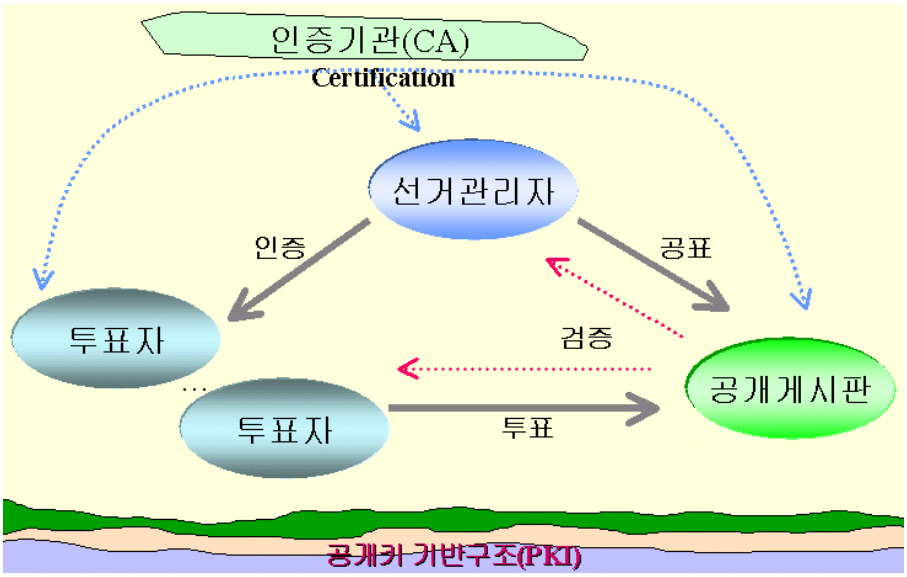

그림 3-1: 전자선거 개념도

3.1 전자선거 프로토콜의 요구사항

전자선거 프로토콜에서 선거기관은 통상 정부라 할 수 있으며 유권자를 등록하고 선거시행 시 유권자를 확인하고 비밀이 보장되는 장소를

제공하여 선거를 하게 한다. 투표가 완료된 다음에는 투표지가 담긴 투표함을 봉인하여 취합하고 유효한 투표를 집계한 후 결과를 발표하게 된다. 투표의 이 과정을 대략 살펴보면 유권자의 명부를 작성하는 유권자 등록단계, 유권자가 본인임을 확인 받는 단계, 투표하는 단계, 각 투표지를 취합하는 수집 단계, 투표 내용을 공개하는 개표 단계, 후보자에 대한 기표별로 더하는 계수단계와 결과의 발표단계로 구분할 수 있다. 투표자는 이러한 일련의 과정에서 유권자로 등록하고 자신의 결정을 투표지에 표기하여 비밀하게 제시한다.

전자선거는 이러한 일련의 과정이 공정하고 안전하게 유지되도록 암호기법을 사용하여 프로토콜을 구성한다. 구성된 전자선거 프로토콜은 선거가 갖는 요구사항을 충족해야 하며, [FOO92]에서는 전자선거 프로토콜이 충족해야 할 요구사항을 분류하여 다음의 7가지로 정의하였다.

- 완전성(completeness) : 모든 유효 투표가 정확하게 집계되어야 한다는 것으로, 최종 집계에서 정당한 투표가 제거되는 일이 없어야 한다.
- 건전성(soundness) : 부정한 투표자에 의해 선거가 방해되는 일이 없어야 한다는 것으로, 최종 집계에서 부정 투표가 집계되어 선거에 영향을 끼치지 않아야 한다.
- 비밀성(privacy) : 모든 투표가 비밀로 되어야 한다는 것으로, 특히 개인의 투표내용으로부터 그 개인을 확인할 수 없어야 한다.
- 단일성 또는 이중투표불가성(unreusability) : 정당한 투표자가 두 번 이상 투표할 수 없다는 것으로 단지 한 번만 투표할 수 있어야 한다.

- 적임성 또는 선거권(eligibility) : 투표 권한을 가진 자만이 투표할 수 있는 것으로 투표가 허락되지 않은 사람은 투표할 수 없어야 한다.
- 공정성(fairness) : 투표에 영향을 미치는 어떤 것이 없어야 한다는 것으로 투표 중에 일부분 결과를 알게 되어 투표에 영향을 미치는 상황 등이 없어야 한다.
- 검증성(verifiability) : 선거 결과를 속일 수 없도록 누구라도 투표 결과를 확인하여 검증해 볼 수 있어야 한다.

이 후에 [FOO92] 에서는 거론되지 않았던 유권자의 매표방지에 관한 논문[NR94][BT94][SK95]이 발표되어 매표방지성(receipt-freeness)이 전자선거의 중요한 요구사항으로 대두되었다. 또한 전자선거에서는 선거관리자가 핵심적인 역할을 하기 때문에, 선거관리자의 부정한 행위 또는 장애 방지를 위한 강인성(robustness) 확보 또한 중요한 이슈이다. [FOO92] 에서 분류한 일곱번째 속성인 검증성의 요구조건은 자신의 투표결과를 검증하는 개별검증성(locally verifiability)과 누구나 유효성을 검증할 수 있는 전체검증성(universally verifiability)으로 구분할 수 있다.

이상의 속성 외에도 기존의 선거처럼 실용적인 전자선거는 기권이 가능하여야 하고 기권자와 관계없이 투표가 진행되어야 한다. 불특정 다수를 대상으로 하는 대규모 선거에서의 투표완료는 시간이 기준이 되어야 하겠으나 유권자가 권리를 행사함에 있어서 시스템이나 통신상의 문제로 방해 받지 않아야 한다. 개표하는 키가 있는 경우에 키의 오류 시 오류의 원인이 투표자에게 있는지 선거관리자에게 있는지도 밝힐 수 있어야 한다.

3.2 암호기법 적용

앞서 살펴본 전자선거 프로토콜의 요구사항 들은 전자 투표의 진행 단계인 준비단계나 투표 및 개표단계, 또는 사후 검증 단계에서 만족되어야 한다. 각 단계의 프로토콜에는 다양한 암호기법 들이 사용된다. 전자선거 프로토콜에 사용되는 암호 기법들은 기법 자체의 제한성과 계산의 복잡성 등으로 실용적이지 않거나 실제상황에는 적용하기 어려운 가정들을 하기도 한다. 다음에서 주요 암호 기법들의 특성과 용도를 분석해 보고자 한다.

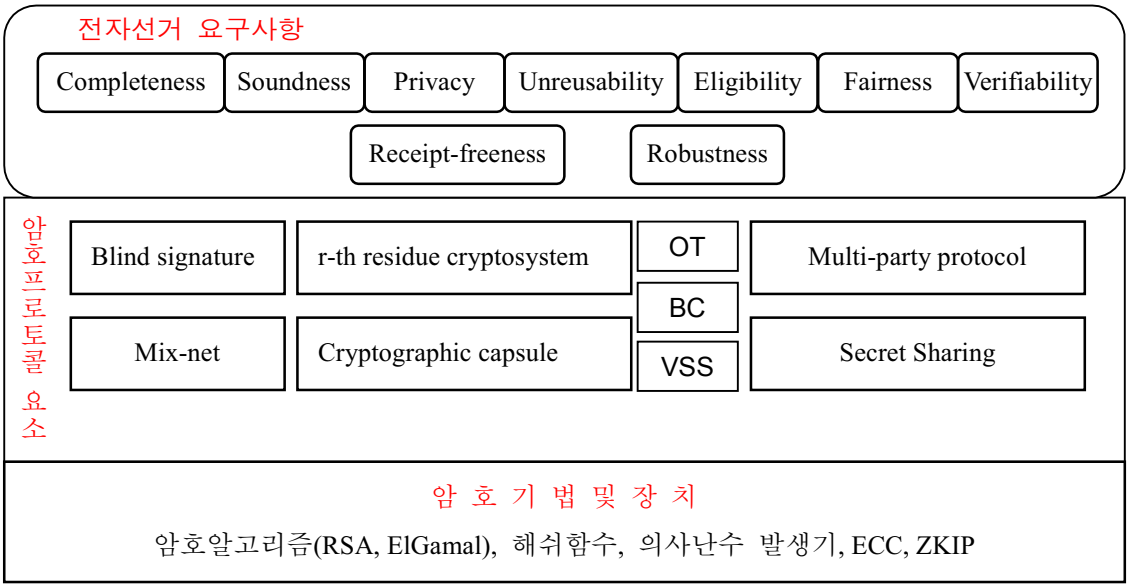

그림 3-2: 전자선거와 암호기술

3.2.1 암호기법

전자선거 프로토콜은 공개키 암호를 기반으로 하여 영지식 증명, 다자간 프로토콜, 전자서명 및 은닉서명을 이용하여 구성하게 된다.

- RSA 암호 : 구별되는 2 개의 큰 소수의 곱을 이용한 기법으로 큰 소수 p 와 q 의 곱 n(=pq)의 소인수분해가 어렵다는 성질에 근거하고 있다. $n = pq$ 일 때, $\Phi(n) = (p-1)(q-1)$ 은 Euler Φ 함수로 $\gcd(\Phi(n), e) = 1$ 인 난수 e 를 선택한다. 그리고 $ed = 1 \bmod \Phi(n)$ 인 d 를 찾아 e, n 을 공개하고 d 는 비밀키로 삼는다. 메시지 M 의 암호화는 $C = M^e \bmod n$ 이고 복호화는 $D = C^d \bmod n$ 이다.
- ElGamal 암호 : 이산대수문제의 어려움에 근간한 공개키 암호 기법이다. 우선, 곱셉군 Z_p^* 상의 생성자 g 를 선택한다. $1 \le a \le p-2$ 인 임의의 정수 a 를 선택하여 $g^a \bmod p$ 를 계산한다. 이 때 (p, g, g^a) 이 공개 되고 a 는 개인키가 된다. 메시지 m 의 암호화는 $1 \le k \le p-2$ 인 임의의 정수 k 를 선택하여 $\gamma = g^k \bmod p$ 와 $\delta = m(g^a)^k \bmod p$ 를 계산한다. 복호화는 (γ, δ) 로부터 $(\gamma^{-a})\delta \bmod p$ 를 계산하여 메시지 m 을 얻는다.
- 은닉서명(blind signature) : A 가 B 에게 메시지의 내용을 모르게 하면서 메시지에 대한 서명을 받는 방식으로 A 의 익명성을 보장하기 위하여 사용된다. A 는 $2 \le k \le n-2$ 이고 $\gcd(n, k) = 1$ 인 임의의 수 k 를 선택하고,

$m^* = mk^b \bmod n$ 을 하여 B 에게 보낸다. B 는 자신의 개인키 a 로 서명하여 $s^* = (m^*)^a \bmod n$ 를 A 에게 다시 보낸다. A 는 $s = k^{-1}s^* \bmod n$ 하여 메시지 m 에 대한 B 의 서명을 획득한다.

- 영지식 증명(zero-knowledge proofs) : 소유한 정보를 드러내지 않으면서 상대방에게 그 정보를 알고 있음을 증명하는 방법으로 인지증명, 유효성 증명 등에 사용된다. 다양한 영지식 증명 방법이 제시되고 있으며, 완전성(completeness property), 건전성(soundness property) 및 영지식성(zero knowledge property)을 만족해야 한다.
- 비트위임(bit commitment) : A 와 B 가 있어서 A 가 어떤 값을 B 에게 위탁할 때, A 는 이 값을 바꿀 수 없어야 하고 B 는 일정시점까지는 이 값을 알 수 없어야 할 때 사용한다. 이차 잉여류를 이용한 방법은 잉여류가 아닌 $y \in Z_n^*$ 에 대하여 0 인 경우 $x^2 \bmod n$ 을 1 인 경우 $yx^2 \bmod n$ 을 보낸다. 이산 대수를 이용한 방법은 소수 p, 생성자 $g \in Z_p^*$, 그리고 $s \in Z_p^*$ 를 선택하고 0 인 경우 $g^x \bmod p$ 를 1 인 경우 $sg^x \bmod p$ 를 보낸다.
- 전자서명(digital signature) : 공개키 암호 시스템의 개인 키를 이용하여 메시지를 암호화하여 보내는 방법으로 상대는 서명자의 공개키로 수신된 메시지를 검증해 봄으로써 서명자를 유일하게 확인할 수 있다.
- 다자간 프로토콜(multi-party protocol) : 다수가 공통의 비밀을 분산 유지하다가 필요 시 모두가 모여 연산을 행하면 원하는 비밀 값을 얻을 수 있는 방식으로, (t,n)-threshold scheme 의 경우 비밀 정보를 n 명이 분산 보관하고 k(<n)명이

협력하면 비밀정보를 복원하여 암호문을 복호화 할 수 있다.

- 검증가능 비밀공유(verifiable secret shares) : 비밀 정보를 분산시켜 보호 시, 각 참여자가 받은 비밀 조각이 정당한 것인지를 모든 참가자가 검증할 수 있는 구조이다. 비밀은 참여자 다수(임계치 이상)가 비밀의 재구성에 협조할 때만 재결합이 가능하다.
- 익명채널(anonymous channel or mix-net) : 송신자와 그 메시지간의 관계를 숨기는 것으로, 모든 개인이 정직한 경우에 입력 메시지와 출력이 일치하면서 어느 경우에도 송신자와 그 메시지의 관계가 숨겨지는 방법으로, 다자간 프로토콜인 비밀공유기법을 이용하여 일부 믹스서버의 부정을 방지하는 방법을 함께 사용한다.
- 기타 : 이차 잉여류(quadratic residues)인 $y = x^2 \bmod n$, 다차 잉여류(r-th residues)인 $z = x^r \bmod n$, 둘 이상에서 참(true)인 것을 비밀의 노출없이 상대에게 확신시키는 기법인 암호캡슐(cryptographic capsule), 그리고 비밀을 보증하면서 정보를 전달하는 oblivious transfer 등이 사용된다.

3.2.2 요구사항별 암호기법

전자선거 프로토콜의 각 요구사항들을 만족시키기 위하여 사용된 암호기법들을 표 3-1로 정리하였다.

표 3-1: 전자선거 프로토콜 요구사항의 암호기법 적용

요구사항	암호기법	비 고
완전성 (completeness)	전자서명[FOO92], 은닉서명, 익명채널 등	유효투표의 정확한 집계
건전성 (soundness)	비트위임[FOO92], 다자간 프로토콜[PIK93][Abe98][Jak98]	부정 투표의 선거 방해 불가
비밀성 (privacy)	은닉서명[FOO92]과 RSA[Cha81], ElGamal[PIK93][Abe98][Jak98] 등의 암호기법으로 익명채널[Cha81] 을 구성	투표의 비밀 유지, 투표와 개인 연결 불가
단일성 (unreusability)	전자서명, 은닉서명[FOO92]	단 한번의 투표
적임성 (eligibility)	전자서명[FOO92]	투표 권한자만 투표
공정성 (fairness)	비트위임[FOO92], threshold ElGamal	어떠한 요인도 투표중에 영향을 미치지 못함
검증성 (verifiability)	전자서명[FOO92], 비트위임[FOO92], Threshold ElGamal[Abe98], 은닉서명	투표 결과의 정확성 검증
매표방지성 (receipt-freeness)	영지식증명[Ben87][BT94][NR94][SK95]	매표행위 불가
강인성 (robustness)	비밀분산, threshold의 다자간 프로토콜[DF89][Ped91][CGS97]	일부 시스템 장애 또는 부정행위에 영향 받지 않음

표 3-1에서 알 수 있듯이 암호기법들이 여러 요구사항에 공통적으로 사용되고 있으며 암호기법들을 종합적으로 사용하기도 한다. 선거의 가장 중요 속성인 비밀성을 만족함으로써 [FOO92] 에서 정의한 요구사항 7가지는 대부분 만족될 수 있다. 반면에 강인성은 (t,n)-threshold 기법을 사용하며, 매표방지성에는 영지식증명기법을 사용하여 구현하고 있다. 위 9가지 속성중 매표방지성의 구현이 가장 난해하여, 매표방지성을 포함하는 전자선거 프로토콜을 제시하는 논문[BT94] [NR94] [SK95]은 강한 가정을 사용한다.

3.2.3 검증성과 매표방지성 검토

앞서 논의한 아홉가지 요구사항 중 검증성과 매표방지성은 기본적으로 중요한 속성이지만 표리적인 특성으로 인하여 동시에 만족시키기가 어렵다. 검증성은 자신의 투표 결과가 올바르게 게시되었는지를 확인하는 개별 검증성과 게시된 투표결과의 정확성을 누구나가 확인할 수 있는 전체 검증성으로 구성된다. 검증성은 투표내용을 확인할 수 있는 어떤 방법을 투표자나 제삼자에게 제공하는 것이고, 매표방지성은 투표의 내용과 투표자를 연결할 수 있는 방법을 차단하는 것으로 상호 표리적인 관계에 있다.

매표방지성을 제시한 논문들[BT94] [NR94] [SK95]을 보더라도 전체검증성을 제공하지 않거나 매표방지 방법에서 투표자의 정보가 누출될 수 있는 가능성을 내포하고 있다. 전체검증성을 제시하고 있는 논문들[CGS97] [Abe98]은 매표방지성을 제시하지 않고 있다. 이처럼

현재까지는 두가지 요구사항을 충족시키는 방법이 제시되지 못하고 있는 실정이다. 즉, 검증성과 매표방지성은 속성 상 동시 만족이 불가하다고 볼 수 있다. 그렇다면 두가지 요구사항중 하나를 선택하거나, 둘 중 하나는 간접적으로 확인하는 방법을 채택하는 것이 현실적이라 하겠다.

투표자, 선거관리자, 공개게시판이 전자선거를 구성하고 있다. 이 중 선거관리자는 삼권분립이 잘 되어있고 민주주의가 성숙한 나라의 정부기구로써 공정하고 신뢰할 만하다고 가정하자. 공개게시판은 공적인 게시판으로써 누구나가 열람할 수 있다. 투표자는 선거관리자의 역할하에서 자신의 결정을 투표지로 표기하여 공개게시판에 게시한다. 이 과정에서 투표와 개표 결과의 정확성 또는 유효성을 우선 시 한다면 검증성을 필히 제공하여야 한다. 반면에 투표자의 매표 가능성 방지를 우선 시 한다면 매표방지성을 제공하여야 한다.

민주주의 사회에서 의사결정을 위하여 사용하는 투표라는 도구의 기능을 중시한다면 검증성보다는 매표방지성을 제공하는 것이 우선이라 하겠다. 매표방지성을 제공하더라도 검증성은 간접적으로 확인할 수 있는 방법이 제시될 수 있다. 반면에 검증성을 제공하는 경우에는 매표방지성을 제공할 뾰족한 대안이 없는 실정이다.

간략하게 예를들면, 투표자가 $(x, y) = (g^{\alpha}, vh^{\alpha})$와 같이 v라는 투표내용을 암호화하여 게시하면 선거관리자는 자신의 공개키 $h(= g^{s})$에 대응하는 개인키 s로 복호화하여 투표를 집계할 수 있다. 하지만 투표자는 자신의 투표를 강압자에게 증명할 수 있게 된다. 반면에 선거관리자가 투표자의 메시지 $(x, y) = (g^{\alpha}, vh^{\alpha})$를, 난수 β를 사용하여 $(x', y') =$

$(g^{\alpha}g^{\beta}, vh^{\alpha}h^{\beta})$ 와 같이 재암호화(re-encryption)하여 게시한다. 그러면 투표자는 선거관리자의 도움없이는 자신의 투표를 주장할 수 없게 된다. 즉, 선거관리자와 무관한 독립적인 검증 방법이 존재하지 않는다. 만약 이를 독립적으로 검증할 수 있다면, 이는 이산대수문제의 어려움에 근간한 ElGamal 암호방식을 해독할 수 있다는 것과 동일하게 된다. 고로 매표방지기능을 제공할 수 있게 된다. 반면에 검증성은 간접적인 방법으로 제공한다.

이러한 간접적인 검증성의 제공은 현행의 투표방식과 동일하다고 할 수 있겠다. 현재의 선거제도에서 투표 후, 선거관리기관에서 개표한 투표결과의 정확성을 확인할 수 있는 방법이 독립적으로 제공되지 않는다. 다만 이의신청을 법원에 제기하면 개표된 투표지들을 재 검토하는 과정을 다시 할 수 있게 되는 것이다. 이는 공개게시판의 $(x', y') = (g^{\alpha}g^{\beta}, vh^{\alpha}h^{\beta})$ 을 검증하는 과정으로 볼 수 있다.

3.3 기존 전자선거 프로토콜 분석

전술한 전자선거의 요구사항들과 암호기법들이 전자선거 프로토콜 구성에 어떻게 적용되었고 해결되지 않은 문제점들은 무엇인지를 분석하고자 한다. 전자선거 프로토콜의 중요한 개념들을 제시한 논문들과 최근의 연구현황을 중심으로 살펴봄으로써 앞으로의 연구방향을 정할 수 있겠다.

3.3.1 Fujioka, Okamoto, Ohta 의 방식

[FOO92]에서는 일곱가지 전자선거 프로토콜의 요구사항인 완전성(completeness), 건전성(soundness), 비밀성(privacy), 단일성(unreusability), 적임성(eligibility), 공정성(fairness), 검증성(verifiability)을 정의했다. 투표자, 관리자, 공개게시판을 구성요소로 익명통신로를 가정한 전자선거 형태이다. 사용된 암호기법들로는 비트위임, 전자서명, 은닉서명 및 RSA 암호방식 등이며 대규모 선거에 맞는 전자선거 방식으로 다음과 같다.

- 표기
  - V_i : 투표자 i
  - A : 관리자
  - C : 계수자
  - $\xi(v,k)$: 키 k를 사용하여 메시지 v에 대한 비트위임
  - $\sigma_i(m)$: 투표자의 서명
  - $\sigma_A(m)$: 관리자의 서명
  - $\chi_A(m,r)$: 메시지 m과 난수 r에 대한 은닉 기법
  - $\delta_A(s,r)$: 은닉서명의 복구 기법
  - ID_i : 투표자의 ID
  - v_i : 투표자의 투표

- 준비단계 : 투표자 V_i는 투표 v_i를 선택하고 난수 k_i로 $x_i=\xi(v_i,k_i)$를 생성, 은닉기법 $e_i=\chi(x_i,r_i)$를 사용하여 메시지 e_i를 계산, e_i에 서명 $s_i=\sigma_i(e_i)$를 하고 관리자에게 $<ID_i,e_i,s_i>$를 전송

- 관리단계 : 관리자 A는 투표자 V_i의 투표권리를 검사하고 V_i의 서명검사로 기 투표 여부도 검사한다. e_i의 서명 s_i를 검사하고 $d_i=A(e_i)$로 서명하여 d_i를 V_i에게 전송한다. 관리자는 서명한 투표자들의 $<ID_i,e_i,s_i>$를 포함하는 목록으로 공지

- 투표단계 : 투표자 V_i는 $y_i=\delta_A(d_i,r_i)$로 투표지 v_i의 서명 y_i를 검사한다. 관리자의 서명이 잘못되었을 때 $<x_i,y_i>$를 보여 주장하고, V_i는 익명통신로로 $<x_i,y_i>$를 계수자에게 전송

- 집계단계 : 계수자 C는 관리자의 검증 키를 사용하여 투표지 x_i의 서명 y_i를 검사한다. 검사가 성공이면 C는 번호 l 을 갖는 $<l,x_i,y_i>$를 목록 상에 등재하고 모든 투표자가 투표를 완료한 후에 목록을 공지

- 공개단계 : 투표자 V_i는 목록 상의 투표지 숫자와 투표자의 숫자가 같은 지를 검사한다. 검사에 실패하면 투표자는 암호에 사용되었던 r_i를 공개하여 주장한다. 목록 상에 자신의 투표지가 열거된 것을 검사하여 열거되지 않았으면 유효한 투표지와 서명인 $<x_i,y_i>$를 공개하여 주장한다. 숫자 l의 $<l,k_i>$인 k_i를 계수자 C에게 익명통신로로 전송

- 계수단계 : 계수자 C는 투표지 x_i의 위임을 공개하고 목록상에 k_i와 v_i를 더한다. v_i가 유효한 투표인지를 검사하여 C는 투표를 계수하고 투표 결과를 공지

[FOO92]의 전자선거 프로토콜은 몇 가지 가정을 전제로 자신의 일곱가지 요구사항을 만족한다. 투표자가 illegal key를 보내는 경우에는 투표자와 관리자중 누가 부정한지 판별이 불가하다. 익명통신로의 사용을 전제로 하기 때문에 익명통신로의 안전성과 효율성에 종속적이며 실제적인 접목 방법이 추가적으로 제시되어야 한다. 또한 기권자가 없음을 가정하고 있기 때문에 실질적인 선거와의 괴리가 있고 투표완료 시점을 판단할 적절한 수단이 없다. 검증성에 있어서도 전체 검증성은 제공되지 않고 있다. 그리고 [FOO92]의 방식 이후에 나온 요구사항인 매표방지 기능이 충족되지 않으며, 하나의 선거관리자로 인한 장애와 부정에 대처할 방법이 없다. 하지만 이러한 단점에도 불구하고 실제적인 선거의 구현 모델로써 가장 많이 참조된다.

3.3.2 Park, Itoh, Kurosawa 의 방식

[PIK93]에서는 Chaum의 Mix-net이 믹스서버의 수에 비례하여 메시지가 확장되는 문제를, ElGamal 암호시스템과 믹스서버들의 공개키를 메시지 암호화에 사용하는 방식으로 해결하고 있다.

● 표기

- q : 큰 소수
- g : $GF(q)$상의 생성자
- S_i : 믹스서버
- X_i : 믹스서버들의 비밀키($X_i \in \{1,...,q-1\}$)
- Y_i : 믹스서버들의 공개키($Y_i = g^{X_i} \bmod q$)
- P_j : 투표자
- V_j : 투표 값
- K_j : 투표자의 공개키
- K_j^{-1} : 투표자의 비밀키
- h : 해쉬 함수

● 준비단계 : 각 믹스서버 S_i에 비밀키를 분배한다. 투표자 P_j는 K_j 및 K_j^{-1}를 선택하고 공개키를 공개게시판에 공개

● 투표단계 : 투표자 P_j는 난수 R_{j1}과 R_{j2}를 선택하여 투표 값 $V_j = R_{j1} \oplus R_{j2}$을 생성한다. 난수 r_{j1}과 r_{j2}으로

$$(a_{j1}, b_{j2}) = E(K_j \parallel K_j^{-1}(R_{j1} \parallel 0^l), r_{j1})$$
$$(a_{j2}, b_{j1}) = E(K_j \parallel K_j^{-1}(R_{j2} \parallel 0^l), r_{j2})$$

을 계산하고 공개게시판에 기록한다.

$((a_{11},b_{11})(a_{12},b_{12})(a_{21},b_{21})(a_{22},b_{22}),...)$ 이 공개게시판의 공개된 목록이다.

각 믹스서버 S_i 는 $\begin{array}{l}(\overline{\alpha}_{j1},\overline{\beta}_{j1}) = h(a_{j1},b_{j1},e_{j1}) \\ (\overline{\alpha}_{j1} = a_{j1} * e_{j1}, \overline{\beta}_{j1} = b_{j1} * (Y_1 \cdots Y_k)^{e_{j1}}) \\ (\overline{\alpha}_{j2},\overline{\beta}_{j2}) = h(a_{j2},b_{j2},e_{j2}) \\ (\overline{\alpha}_{j2} = a_{j2} * e_{j2}, \overline{\beta}_{j2} = b_{j2} * (Y_1 \cdots Y_k)^{e_{j2}})\end{array}$ 를 계산한다.

$((\overline{\alpha}_{11},\overline{\beta}_{11})(\overline{\alpha}_{12},\overline{\beta}_{12})(\overline{\alpha}_{21},\overline{\beta}_{21})(\overline{\alpha}_{22},\overline{\beta}_{22}),...)$ 이 공개게시판 상의 목록이다.

- 테스트단계 : $(\overline{\alpha}_{i1},\overline{\beta}_{i1})$ 을 선택한 경우에, 믹스서버 $S_1,...,S_k$ 는 $((\overline{\alpha}_{i1},\overline{\beta}_{i1}) = E(\overline{K}_i \parallel \overline{K}_i^{-1}(\overline{R}_{i1} \parallel 0^l), x_{i1}))$ 를 복호화 한다. $(\overline{\alpha}_{i2},\overline{\beta}_{i2})$ 을 선택한 경우에, 믹스서버 $S_1,...,S_k$ 는 $((\overline{\alpha}_{i2},\overline{\beta}_{i2}) = E(\overline{K}_i \parallel \overline{K}_i^{-1}(\overline{R}_{i2} \parallel 0^l), x_{i2}))$ 를 복호화 한다. 각자 0^l 의 형태를 확인하여 이상이 있으면 멈추고 없으면 다음 단계를 진행한다.

- 개표단계 : 남아 있는 각 i 에 대하여 테스트 단계를 수행한다. 이상이 없으면 투표 값 V_i 목록을 채택한다.

[PIK93]의 방식은 투표자의 투표값을 변조할 수 없고 투표자와 투표값을 연결할 수 없기 때문에 투표자의 익명성이 보장된다. 반면에 매표방지 행위, 전체 투표의 유효성 검증, 미등록자에 대한 관리자의 부정 행위를 차단할 방법이 제공되지 않는다. [Pfi94]에 언급된 공격을 방지하기 위해선 non-malleability 방법을 고려해야 한다.

3.3.3 Sako, Kilian 의 방식

[SK95]은 매표방지성(receipt-freeness)을 제시한 전자선거 프로토콜로써 영지식 비트 위임 기법을 사용하여 투표자와 믹스서버의 공모에 의한 부정을 방지하고자 했다.

- 준비단계 : 믹스-넷 프로토콜을 초기화 한다. 각 투표자 i는 난수 문자열 위임에 사용되는 카멜레온 비트 위임 구조에 대한 키 쌍 $(a_i, \alpha_i = g^{a_i} \bmod p)$을 소유한다
- 1 단계 : 마지막 믹스-센터 n은 길이 $l+1$ 비트의 난수 문자열 $\pi^{(i,n)}$을 공개키 α_i를 사용하는 투표자 i에게 위임한다. 난수 r_{2n-1}, $r_{2n} \in Z_p^*$를 선택하고, $w_0 = \prod_{i=1}^{n} y_i \bmod p$로 다음을 계산한다.

  $v_0 = (\overline{G}_n, \overline{M}_n) = (g^{r_{2n}} \bmod p, m_0 * w_0^{r_{2n}} \bmod p)$

  $v_1 = (\overline{G}'_n, \overline{M}'_n) = (g^{r_{2n-1}} \bmod p, m_1 * w_0^{r_{2n-1}} \bmod p)$

  만약 $\pi^{(i,n)}$의 첫 번째 비트가 0이면 (v_0, v_1), 아니면 (v_1, v_0)으로 놓는다.

  v_0, v_1이 적절하게 구성되었음을 영지식으로 증명한다.

  $\pi^{(i,n)}$의 첫번째 비트를 제외한 난수 스트링은 영지식 프로토콜에 사용된다.
- 2 단계 : 믹스-센터 n은 투표자에게 도청 되지 않는 채널로 $\pi^{(i,n)}$을 위임 해제한다. 단지 투표자만이 v_0, v_1의 순서를 알게 된다 .

- 3 단계 : 다음의 믹스-센터 $j(j=n-1,...,1)$는 투표자 i에 대하여 믹스-센터 $j+1$로부터 $((\overline{G}_{j+1},\overline{M}_{j+1}),(\overline{G}'_{j+1},\overline{M}'_{j+1}))$ 또는 $((\overline{G}'_{j+1},\overline{M}'_{j+1}),(\overline{G}_{j+1},\overline{M}_{j+1}))$을 얻고, 투표자에게 $l+1$ 비트 스트링 $\pi^{(i,n)}$을 위임하며 그리고 난수 r_{2n-1}, $r_{2n} \in Z_p^*$를 선택한다.

  첫 번째 경우에는,

  $(\overline{G}_j,\overline{M}_j) = (\overline{G}_{j+1} * g^{r_{2j}} \bmod p, \overline{M}_{j+1} * w_0^{r_{2j}} \bmod p)$

  $(\overline{G}'_j,\overline{M}'_j) = (\overline{G}'_{j+1} * g^{r_{2j-1}} \bmod p, \overline{M}'_{j+1} * w_0^{r_{2j-1}} \bmod p)$

  두 번째 경우에는,

  $(\overline{G}_j,\overline{M}_j) = (\overline{G}'_{j+1} * g^{r_{2j}} \bmod p, \overline{M}'_{j+1} * w_0^{r_{2j}} \bmod p)$

  $(\overline{G}'_j,\overline{M}'_j) = (\overline{G}_{j+1} * g^{r_{2j-1}} \bmod p, \overline{M}_{j+1} * w_0^{r_{2j-1}} \bmod p)$

  을 계산한다.

  비트스트링의 첫 번째 비트의 값이 0 이면 $((\overline{G}_j,\overline{M}_j),(\overline{G}'_j,\overline{M}'_j))$으로, 반대이면 $((\overline{G}'_j,\overline{M}'_j),(\overline{G}_j,\overline{M}_j))$으로 위치한다. 비트스트링의 첫 번째 사용하지 않는 비트 값에 따라 각 라운드에서 λ를 선택하여 올바르게 프로토콜을 따랐음을 증명할 수 있다. 단지 2 가지 순서만이 가능하기 때문에 λ에 대하여 2 가지 선택만이 존재한다. 고로 λ는 비트스트링의 임의의 비트 값에 의해 완전하게 결정된다

- 4 단계 : 비트스트링을 위임 해제함으로써 믹스-센터의 출력의 순서는 투표자

에게만 노출된다.

- 5 단계 : 단계 2 와 3 은 모든 믹스-센터에 대하여 반복된다. $(z_1,...,z_t) \in \{0,1\}^t$ 가 있어서 투표자는 다음의 쌍을 얻는다.

$$(\overline{G}_1, \overline{M}_1) = (g^{\sum_{t=1}^{n} r_{2t-z_t}} \bmod p, m_0 * w_0^{\sum_{t=1}^{n} r_{2t-z_t}} \bmod p)$$

$$(\overline{G}_1', \overline{M}_1') = (g^{\sum_{t=1}^{n} r_{2t+z_t-1}} \bmod p, m_1 * w_0^{\sum_{t=1}^{n} r_{2t+z_t-1}} \bmod p)$$

- 6 단계 : 투표자는 어떤 쌍이 어떤 투표인지 알고 믹스-센터 1 에 그의 선택을 보낸다.이 쌍은 믹스-넷을 통하여 믹스-센터 n 에게 보내진다. 믹스-센터 n 은 이 투표자의 투표를 복구할 수 있다. 랜덤한 $\sum_{t=1}^{n} r_{2t-z_t}$ 또는 $\sum_{t=1}^{n} r_{2t+z_t-1}$ 을 가지고 투표자에 의해 암호화된 투표로서 해석될 수 있다. 고로 위에 기술한 믹스-넷 프로토콜을 통하여 쉽게 보내질 수 있다.
- 7 단계 : 마지막 믹스-센터는 투표를 공개하고 모든 사람은 계수를 계산할 수 있다.

[SK95]의 방식은 매표방지성을 제공하고 있다. 그러나 [PIK93]의 방식에 근거함으로 인해서 검증자는 각 서버가 cut-and-choose로 올바르게 행위를 했는지 검사해야 하는 부담으로 효율성에 문제가 있다. [MH96]에서 지적했듯이 익명성이 위반될 수 있다.

3.3.4 Cramer, Gennaro, Schoenmaker 의 방식

[CGS97]은 임계치 비밀공유기법을 이용한 전자선거 프로토콜로써, 준동형의 성질을 사용하여 투표의 결과를 한번에 복호화 할 수 있도록 한 효율성이 향상된 방식이다.

- 준비단계
  - A_j : 선거관리자$(j = 1,...,n)$
  - V_k : 유권자$(k = 1,...,m)$
  - 선거관리자는 공개키 h를 생성하고 그에 해당하는 비밀키 s_j를 재분배하고 공개게시판에 게시
  - 후보자 l명에 대한 독립적인 생성자 G_i $(i = 1,...,l)$를 생성하고 공개게시판에 게시
  - m명의 유권자들을 공개게시판에 등록
- 투표단계 : 각 유권자 V_k는 후보자를 선택한 후 해당 생성자 G_i로 투표 값 $(x, y) = (g^{\alpha}, h^{\alpha} G_i)$를 생성하고 유효성 증명과 함께 공개게시판에 게시한다.
- 개표단계
  - 선거관리자는 공개게시판에 게시된 각 투표의 유효성을 검증하고 유효한 투표값을 곱하여 $(X, Y) = (\prod_{k=1}^{m} x_k, \prod_{k=1}^{m} y_k)$을 계산한다.
  - 선거관리자들은 X^s으로부터 $W = Y / X^s$를 계산한다.

– 이산대수 문제인 $W = G_1^{T_1} G_2^{T_2} \cdots G_l^{T_l}$ 을 만족하는 $T_1, T_2, \cdots, T_l$ 를 계산하면 후보자별 집계를 얻게 된다.

[CGS97]의 전자선거 프로토콜은 임계치 비밀공유기법을 사용하여 선거관리자의 장애에 대한 대비를 하였다. 투표 값 전체를 곱하여 한 번의 복호화 작업으로 결과를 집계할 수 있도록 효율성도 개선하였다. 하지만 결과 계산이 이산대수 문제에 근간함으로써 어느 정도 큰 규모에 대해서는 투표 값을 나누는 과정이 필요함으로 이점이 축소된다. 또한 후보자 수에 따라 유효성증명의 계산량이 증가하고 투표자가 사용한 난수를 제시하여 자신의 투표 내용을 증명할 수 있기 때문에 매표방지성은 충족하지 않는다.

3.3.5 Schoenmaker 의 PVSS 를 이용한 찬반 전자선거

[Sch99]는 PVSS의 준동형(homomorphism) 성질을 이용하여, 전체검증성을 갖는 찬반 전자선거를 제안하였다. 이 전자선거는 투표자와 선거관리자가 동일하고, 투표자가 비밀 분배자가 되는 이사회 의결(board-room elections)과 같은 작은 규모의 투표의 예로 다음과 같다. 그룹 $G_q \ (q : prime)$, 생성자 G, 그리고 투표자 $P_i \ (1 \le i \le m)$가 있다. P_i의 개인키를 $x_i \in Z_q^*$, 공개키는 $y_i = G^{x_i}$라 하자.

- 투표 값 $v \in \{0,1\}$ 와 비밀 값 $s \in_R Z_q$ 를 사용하여 $U = G^{s+v}$를 생성

- 투표자는 비밀 s 는 m 명의 투표자에게 분배
- $Y_i^* = \prod_{j=1}^{m} Y_{ij} = y_i^{\sum_{j=1}^{m} p_j(i)}$ 를 계산
- Y_i^* 를 공개키 y_i 에 대응하는 비밀키 x_i 로 복호화
- 각 투표자의 비밀 G^{s_j} 를 복원
- 준동형 성질로 $\prod_{j=1}^{m} U_j = G^{\sum_{j=1}^{m} s_j + v_j}$ 계산
- $G^{\sum_{j=1}^{m} s_j}$ 는 m 명 투표자들의 비밀 값이므로 $G^{\sum_{j=1}^{m} v_j}$ 의 계산이 가능
- v_j 는 0 또는 1 이므로 투표결과 $T = \sum_{j=1}^{m} v_j \ (0 \le T \le m)$ 가 얻어짐

이 전자선거는 매우 제한적이다. 준동형 성질을 이용한 효율적인 전체검증성을 구현하고자 찬반 전자투표에 국한하게 되었으며, 투표 결과를 얻기 위해서는 이산대수를 계산하여야 함으로 투표자의 수가 적어야 한다. 또한 준동형 성질을 적용함은 투표자와 계수자 또는 비밀 분배자와 투표자가 동일한 형태인 전자선거로 제한되게 하고 있다.

3.4 PVSS 를 이용한 다중 전자선거 방식 제안

[Sch99]에서의 제한 사항을 개선하고 PVSS의 장점을 활용하는 두가지 형태의 전자선거를 다음에 제시한다. 제시하는 전자선거는, PVSS를 이용한 검증가능한 대규모의 다중(multi-way) 전자선거와 검증성을 제한하여 간접적인 검증성을 제공하는 매표방지(receipt-freeness)형 전자선거로 준동형 성질은 사용하지 않는다.

3.4.1 검증가능한 다중 전자선거

PVSS를 이용하여 전체검증성을 만족하는 다중 전자선거 방식은 투표자, 선거관리자 및 공개게시판으로 구성된다. 선거관리자는 비밀키를 선택하고 비밀키에 대응하는 공개키를 공개게시판에 등록한다. 투표자는 투표 값을 암호화하는 비밀 값과 다항식을 선택한다. 다항식을 이용하여 생성한 비밀조각으로 선거관리자들의 공개키에 지수 승을 하고 암호화된 투표 값과 함께 공개게시판에 게시한다. 선거관리자들은 자신의 개인키로 공개키의 지수승 된 값을 복호화한다. 투표자가 선거관리자의 공개키에 지수승하여 배분한 비밀 조각이 복호화되었음으로 누구나가 투표 결과를 검증해 볼 수 있게 된다. 선거관리자는 투표 값들을 계수하여 결과를 공표한다. 이를 상세히 기술하면 다음과 같다.

- 표기
  - 그룹 G_q 에서의 생성자 g, G
  - 투표자 V_i
  - 선거관리자 A_j 의 개인키 $x_j \in_R Z_q^*$, 공개키 $y_j = G^{x_j}$
- 투표자 V_i 의 투표
  - 임의의 t-1 차 다항식 p 선택
  - $p(x) = \sum_{j=0}^{t-1} \alpha_j x^j$ 를 이용하여 비밀 분배 ($s_i = \alpha_0,\ \ s_{ij} = p(i)$)
  - 투표 $(G^{s_i} v,\ \ y_j^{s_{ij}})$ $\begin{Bmatrix} i = 1,...,m \\ j = 1,...,n \end{Bmatrix}$ 생성
- 선거관리자 A_j 의 복호화
  - $(G^{s_i} v,\ \ y_j^{s_{ij}})$ 의 $(y_j^{s_{ij}})^{1/x_j} = G^{s_{ij}}$ 로 복호화
- 결과 집계 (Any one)
  - $\prod_{j=1}^{t} (G^{s_{ij}})^{\lambda_j} = G^{\sum_{j=1}^{t} s_{ij}\lambda_j} = G^{s_i}$
  - $(G^{s_i} v,\ \ y_j^{s_{ij}})$ 의 $G^{s_i} v$ 로부터 $G^{s_i} v / G^{s_i} = v$ 얻음
  - v 를 후보자별로 더하여 투표 결과 공표

투표자가 선택한 임의의 $t-1$차 다항식의 계수 α_j를 $C_j = g^{\alpha_j}$로 공지하고, $X_i = \prod_{j=0}^{t-1} C_j^{i^j}$ 라 하면, V_i 는 식 (3-1)을 만족하도록 유일한 $s_{ij} = p(j)$의 proof of knowledge를 생성하여 비밀 분배를 옳게 했음을 보일 수 있다.

$$X_i = g^{s_{ij}}, \quad Y_i = y_i^{s_{ij}} \tag{3-1}$$

증명자가 식 (3-1)과 같은 형태의 $h_1 = g_1^r$와 $h_2 = g_2^r$를 만족하는 어떤 난수 r을 알고 있음을 증명하는 과정은 다음과 같다.

- 증명자
  - 임의의 난수 $v \in Z_q$ 선택
  - $c_1 = g_1^v$과 $c_2 = g_2^v$ 계산
  - c_1과 c_2를 검증자에게 전송
- 검증자(도전 과정)
  - 임의의 난수 $\alpha \in Z_q$ 선택하여 증명자에게 전송
- 증명자(응답 과정)
  - $\beta = v - r\alpha (\mathrm{mod}\, q)$를 검증자에게 전송임
- 검증자(검증 과정)
  - $c_1 = g_1^{\beta} h_1^{\alpha}$이고 $c_2 = g_2^{\beta} h_2^{\alpha}$ 인지를 검사

이 방식은 전체검증성은 만족하지만 매표방지성(receipt-freeness)은 충족하지 못한다. 선거관리자가 투표자의 투표값을 재암호화(re-encryption)하는 방식으로 매표방지성을 만족시킨 전자선거를 다음에서 제안한다.

3.4.2 검증성이 제한된 매표방지 다중 전자선거

매표방지가 가능한 전자선거는 검증성을 제한하는 것으로 검증성은 간접적으로만 제공한다. 이 방식에서는 분배자(dealer)를 도입하여 투표자의 투표를 암호화하여 게시하도록 설정한다. 이를 상세히 기술하면 다음과 같다.

- 표 기
  - 그룹 G_q에서의 생성자 g, G
  - 투표자 V_i
  - 선거관리자 A_j 의 개인키 $x_j \in_R Z_q^*$, 공개키 $y_j = G^{x_j}$
- 투표자 V_i의 투표
  - 임의의 t-1 차 다항식 p 선택
  - $p(x) = \sum_{j=0}^{t-1} \alpha_j x^j$ 를 이용하여 비밀 분배 ($s_i = \alpha_0$, $s_{ij} = p(j)$)
  - 투표 $(G^{s_i} v,\ y_j^{s_{ij}}) \begin{Bmatrix} i = 1,...,m \\ j = 1,...,n \end{Bmatrix}$ 생성
- 분배자의 재암호화 및 게시

– 임의의 $t-1$차 다항식 q 선택

– $q(x)=\sum_{j=0}^{t-1}\beta_j x^j$ 를 이용하여 비밀 분배 ($\delta_i=\beta_0,\ \delta_{ij}=q(j)$)

– 투표 값을 $(G^{\delta_i}G^{s_i}v,\ \ y_j^{\delta_{ij}}y_j^{s_{ij}})\begin{Bmatrix}i=1,...,m\\ j=1,...,n\end{Bmatrix}$ 로 재암호화하여 게시

- 선거관리자 A_j 의 복호화

– $(y_j^{\delta_{ij}}y_j^{s_{ij}})^{1/x_j}=G^{\delta_{ij}+s_{ij}}$ 계산

- 결과 집계 (Any one)

  – $\prod_{j=1}^{t}(G^{\delta_{ij}+s_{ij}})^{\lambda_j}=G^{\sum_{j=1}^{t}(\delta_{ij}+s_{ij})\lambda_j}=G^{\delta_i+s_i}$

  – $G^{\delta_i}G^{s_i}v\ /\ G^{\delta_i+s_i}=v$ 얻음

  – v를 후보자별로 더하여 투표 결과 공표

본 방식도 첫번째 방식(검증가능한 다중 전자선거)처럼, 투표자는 식 (3-1)을 만족하는 proof of knowledge를 생성하여 비밀 분배를 옳게 했음을 분배자에게 보일 수 있다. 반면에 분배자는 proof of knowledge를 생성할 수 없다. 왜냐하면, 선택한 임의의 $t-1$차 다항식의 계수 β_j를 $D_j=g^{\beta_j}$ 로 공지하고, $X_i'=\prod_{j=0}^{t-1}D_j^{i^j}$ 라 하여, 식 (3-2)를 만족하도록 유일한 $\delta_{ij}=q(j)$ 의 proof of knowledge를 생성하면 투표자가 자신의 투표 값을 증명할 수 있게 되기 때문이다.

$$X_i' = g^{\delta_{ij}}, \quad Y_i' = y_i^{\delta_{ij}} \tag{3-2}$$

결과적으로, 투표 결과에 대한 정확성 검증은 간접적으로 행해질 수 밖에 없다. 현행의 선거에서 투표함에 자신의 투표지를 넣는 순간 투표 결과에 대한 직접적인 검증 방법이 없어지는 것처럼, 분배자가 투표자의 메시지를 재 암호화 함으로써 투표함을 대신한다.

3.5 분석

앞 장에서 제안한 2가지 방식(방식 1 : 검증가능한 다중 전자선거, 방식 2 : 검증성을 제한한 매표방지 다중 전자선거)의 특징을 전자선거 프로토콜의 요구사항별로 분석해 본다.

- 완전성(completeness)
  - 방식 1) 방식 2) : 참여자들이 정직하다면 투표의 결과는 신뢰할 수 있다.
- 건전성(soundness)
  - 방식 1) 방식 2) : 투표자에 대한 인증 방법이 필요하며, 제시한 투표 값에 대해서는 투표자가 값을 변경할 수 없다.
- 비밀성(privacy)
  - 방식 1) 방식 2) : PVSS 성질에 의하여 투표 값과 투표자를 연결할

수 없다. 하지만 메시지와 투표자를 연결할 수는 있으므로 익명통신로를 이용하여 트래픽 분석을 방지해야 한다.

- 단일성 또는 이중투표불가성(unreusability)
  - 방식 1) 방식 2) : 투표자에 대한 인증 방법이 필요하며, 투표권을 행사한 투표자는 다시 투표할 수 없다.
- 적임성 또는 선거권(eligibility)
  - 방식 1) 방식 2) : 투표자에 대한 인증 방법이 필요하며, 인증을 받은 투표자만이 투표할 수 있다.
- 공정성(fairness)
  - 방식 1) 방식 2) : n 명 중 t 명 이상의 선거관리자들이 공모하지 않는다면 투표를 개표할 수 없다. 고로 모든 투표가 완료된 후 개표를 진행할 수 있으므로 공정성을 만족한다.
- 검증성(verifiability)
  - 방식 1) : 투표자는 자신이 제시한 비밀 값의 확인으로 개별 검증할 수 있으며, 누구든지 PVSS 성질을 이용하여 전체 결과를 검증할 수 있다.
  - 방식 2) : 분배자가 투표자의 투표 값을 재 암호화 하였으므로 간접적인 검증만이 가능하다. 즉, 검증하기 위해서는 샘플링에 의해 일부의 투표자들을 선택한 후 분배자의 협조로 검증할 수 있을 것이다.
- 매표방지성(receipt-freeness)
  - 방식 1) : 투표자는 자신의 투표 값을 증명할 수 있으므로 매표방지

성이 없다.

- 방식 2) : 투표자의 투표 값을 분배자가 재 암호화하여 게시하였으므로 투표자는 자신의 투표 값을 증명할 수 없으며 매표방지성을 만족한다.

- 강인성(robustness)
  - 방식 1) 방식 2) : (t,n)-threshold 비밀공유기법의 적용으로 t 미만인 선거관리자의 부정에 대하여 안전하다. 또한 일부 장애에 대하여도 안전하다.

제안한 전자선거 프로토콜은 기능적인 측면에서 [Sch99]의 찬반 전자선거 방식과 비교할 때 다음과 같은 장점을 갖는다. 단 효율성 측면에서는 메시지의 양과 계산량이 늘어나는 단점이 있다.

- 투표 값의 암호화에 사용되는 비밀 값을 투표자가 선택함으로써 분배자의 관여를 최소화한다.
- 다수 후보자에 대한 선거를 실시할 수 있는 다중 전자선거 형태이다.
- 대규모 유권자를 대상으로 전자선거를 실시할 수 있다.

표 3-2과 표 3-3은 위의 분석 내용을 정리한 것으로 공개게시판을 사용하는 전자선거에서 투표자의 인증은 기본적으로 충족되는 것으로 가정한다.

표 3-2: 제안방식의 요구사항 분석

속성 / 특성	방식 1	방식 2
비밀성(privacy)	O	O
완전성(completeness)	O	O
건전성(soundness)	O	O
단일성(unreusability)	O	O
적임성(eligibility)	O	O
공정성(fairness)	O	O
검증성(verifiability)	O	∇
매표방지성(receipt-freeness)	X	O
강인성(robustness)	O	O

* 충족(o), 조건부 충족(∇), 불충족(X)

표 3-3: 제안방식의 기능비교

기능 \ 방식	제안 방식	[Sch99]의 방식
분배자의 관여	준비단계[방식1]/투표단계[방식2]	준비단계 및 투표단계
선거 규모	대규모 선거	소규모 선거
선거 방식	다중 선거	찬반 선거

Ⅳ. 결론 및 향후 과제

비밀공유기법은 안전성을 향상시킬 수 있는 가장 효과적인 방법으로, ElGamal 암호시스템의 비밀키를 분산 공유하게 하는 암호 기법으로 사용되어 익명통신로를 구성한다. 비밀공유기법에 의한 익명통신로에서 n개의 믹스서버들 중 비밀의 복원에 참여할 t개의 믹스서버들을 선정하는 명시적인 방법으로 사용자 선택에 의한 t믹스-넷 구성 방법을 제시하였다. 사용자 선택에 의한 t믹스-넷이 메시지의 난수화, 조합 및 복호화의 작업 부하를 분산시키고 믹스서버들의 장애를 관리하고자 하는 것을 목표로 하고 있다. 사용자 선택에 의한 t믹스-넷은 데이터구조를 사용하여 t믹스서버들을 관리하고, 이 데이터구조를 참조함에 의해 임의의 순서로 작업을 전달하는 것이 가능하며, 장애 시에 장애 믹스서버 내에 있는 메시지들의 작업을 재설정할 수 있다.

비밀공유기법의 또 다른 방법인 공개적으로 검증가능한 비밀공유(PVSS) 기법은 비밀공유에 공개키를 사용함으로써 누구나 비밀 조각의 유효성 검증이 가능하다. 또한 비밀 조각을 직접 알고 있지 않더라도 비밀공유 기능이 수행됨으로 전자선거와 같은 응용에서 선거관리자의 비밀키를 노출시키지 않을 수 있다. 이 PVSS를 이용하여 제안한 검증가능한 다중 전자선거는 다수 후보자들과 대규모 유권자로 구성되는 전자선거에서 검증성을 제공하며 사용자가 비밀을 선택하고 분배함으로서 비밀분배자의 관여를 최소화한 모델이다. 또한 검증성이 제한된 매표방지 다중 전자선거는 검증성을 제한하되 선거의 중요한 요구사항인 매표방지성을 갖도록 하였다.

앞으로의 연구 과제로는 투표자와 선거관리기관간의 인증 단계와 투표권 부여, 투표자와 공개게시판간의 투표 및 투표진행의 요구사항 충족 여부, 그리고 선거관리기관과 공개게시판간의 계수과정의 프로토콜들을 상세화하는 작업이 요구된다. 또한 검증성과 매표방지성이 모두 중요한 요구사항임에도 불구하고 상호 상충되는 특성으로 인하여 프로토콜 완성이 난해하지만 지속적인 연구가 필요하다.

국문요약

전자선거 프로토콜의 요구사항 충족은 다양한 암호기법들을 사용하여 이루어 진다. 비밀공유기법을 이용한 익명통신로는 전자선거 프로토콜의 비밀성을 만족시키는 기본적인 도구로서 안전성 향상에 강점이 있다. 본 논문에서 제안하는 사용자 선택에 의한 t믹스-넷 방식은 임의 순서로 t개 믹스서버들이 메시지의 난수화 및 조합을 수행하게 함으로써 부하를 분산시킨다. 사용자에 의한 t믹스-넷 구성은 비밀분배자의 관여를 최소화하여 전자선거의 공정성을 향상시키기도 한다. 또한 정족수 데이터에 의해 믹스서버들의 작업 과정이 관리됨으로써 믹스서버의 장애 시에 전체 작업의 중단없이 해당 메시지를 재처리 할 수 있도록 한다.

암호기법들중 비밀공유기법은 안전성을 증진하는 유익한 기법이지만 분배자가 배분하는 비밀 조각이 유효한지와 비밀 복원 시 참여자가 제출하는 비밀 조각의 유효성을 판단하는 수단이 필요하다. PVSS는 비밀공유에 공개키를 사용함으로써 누구나 비밀 조각의 유효성 검증이 가능하게 하였으며, 비밀 조각을 직접 알고 있지 않더라도 비밀공유 기능이 수행됨으로 전자선거와 같은 응용에서 선거관리자의 비밀키를 노출시키지 않을 수 있다. 본 논문에서는 이 PVSS를 이용하여 검증가능한 다중 전자선거와 검증성이 제한된 매표방지 다중 전자선거를 제안한다. 2개 방식 모두 다수 후보자들과 대규모 투표자들을 대상으로 하는 전자선거에 적합하다.

References

[Sha79] A. Shamir, “How to share a secret”, Communications of the ACM, 22(11): pp. 612-613, 1979.

[Bla79] G.R. Blakley, “Safeguarding cryptographic keys”, In Proceedings of the National Computer Conference 1979, Vol. 48 of AFIPS Conference Proceedings, pp. 313-317, 1979.

[Cha81] David L. Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms Communications of the ACM, Vol. 24, No.2, pp. 84-88, 1981.

[ElG85] T.ElGamal, “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”, IEEE Transactions on Information Theory, IT-31(4):469~472, July 1985.

[CGMA85] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, “Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults”, In Proceeding of the 26th IEEE Symposium on the foundations of Computer Science(FOCS), pp. 383-395, 1985.

[CF85] J. Cohen, M. Fisher, “A Robust and Verifiable Cryptographically Secure Election Scheme”, In Proceedings of the 26th IEEE Symposium on Foundations of Computer Science, pp. 372-382, IEEE Computer Society, 1985.

[Ben87] J.C.Benaloh, "Verifiable secret ballot elections", PhD

thesis, Yale University, TR561, 1987

[DF89] Y. Desmedt, Y. Frankel, "Threshold cryptosystems", Advances in Cryptology- Crypto89, LNCS Vol.435, pp.287-296, Springer-Verlag, 1989.

[Ive91] Kenneth R. Iversen, "A Cryptographic Scheme for Computerized General Elections", Advances in Cryptology - Crypto 91, LNCS Vol. 576, pp. 405-419, Springer-Verlag, 1991.

[Ped91] T. P. Pedersen, "A Threshold Cryptosystem Without A Trusted Party", Advances in Cryptology -EuroCrypt 91, LNCS Vol.547, pp. 522-526, Springer-Verlag, 1991.

[FOO92] A.Fujioka, T.Okamoto and K. Ohta, "A practical secret voting scheme for large scale election", Advances in Cryptology -Auscrypt92, LNCS Vol.718, pp. 244-251, Springer-Verlag, 1992.

[PIK93] C. Park, K. Itoh, K. Kurosawa, "Efficient Anonymous Channel and All/Nothing Election Scheme", Advances in Cryptology -Eurocrypt 93, LNCS Vol.765, pp. 248-259, Springer-Verlag, 1993.

[Pfi94] B. Pfitzmann, “Breaking an Efficient Anonymous channel”, Advances in Cryptology - Eurocrypt 94, LNCS Vol.950, pp. 332-340, Springer-Verlag, 1994.

[NR94] V.Niemi and A.Renvall, "How to prevent buying of voters in computer elections", Advances in Cryptology -Asiacrypt94,

LNCS Vol.917, pp.164-170, Springer-Verlag, 1994.

[BT94] J.C.Benaloh and D.Tuinstra, "Receipt-free secret ballot elections", Proc. of 26th ACM STOC, pp.544-553, 1994

[SK95] K.Sako and J.Killian, "Receipt-free Mix type voting scheme - a practical solution to the implementation of a voting booth", Advances in Cryptology -Eurocrypt95, LNCS Vol.921, pp.393-403, Springer-Verlag, 1995.

[MH96] M. Michels, P. Horster, “Some Remarks on A Receipt free and Universally Verifiable Mix-Type Voting Scheme”, Advances in Cryptology - Asiacrypt 96, LNCS Vol. 1163, pp. 125-132, Springer-Verlag, 1996.

[MOV96] “Handbook of d o a ”, CRC Press, September 1996.

[Std96] M. Stadler, "Publicly Verifiable Secret Sharing ", Advances in Cryptology- Eurocrypto96, LNCS Vol. 1070, pp.190-199, Springer-Verlag, 1996.

[CGS97] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers, "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology-EUROCRYPT'97, LNCS Vol. 1233, pp.103-118, Springer-Verlag, 1997.

[FO98] E. Fujisaki, T. Okamoto, "A Pratical and Provably Secure Scheme for Publicly Verifiable Secret Sharing and Its Applications ", Advances in Cryptology- Eurocrypto98, LNCS Vol. 1403, pp.32-46, Springer-Verlag, 1998.

[Abe98] M. Abe, Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers, Advances in Cryptology-Eurocrypt 98, LNCS Vol. 1403, pp.437-447, Springer-Verlag, 1998.

[Jak98] M. Jakobsson, A Practical Mix, Advances in Cryptology - Eurocrypt 98, LNCS Vol. 1403, pp. 449-461, Springer-Verlag, 1998.

[Sch99] B. Schoenmakers, "A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting", Advances in Cryptology- Crypto99, LNCS Vol.1666, pp.148-164, Springer-Verlag, 1999.

감사의 글

학문을 갈고 닦는 생활이 결코 쉽지 않음을 소중하게 주어진 기회만큼 무겁게 느끼며 2 년의 시간을 접으려 합니다. 20 대 젊은이의 마음으로 시작한 ICU 생활이 세월의 벽을 다시 깨닫게 했지만 열성적인 교수님과 주위의 동료 후배분들 덕에 부족하나마 한 권의 논문으로 마감하게 됨을 인연이 닿는 모든 분들께 감사의 말로 대신하고자 합니다.

먼저 삼성 SDS 의 서정묵 이사님과 임직원분들께 IMF 의 어려운 시기에 학업의 기회를 주신 것에 진심으로 감사한 마음을 전하고자 합니다. 그리고 ICU 의 정보공학부 교수님들과 총장님께 학생 일원으로 선발하고 지도 편달하여 주신 노고에 심심한 감사를 표합니다.

팀웍을 바탕으로 집중적이며 꾸준하고 다양한 연구활동을 강조하시면서 왕성하신 활동력으로 손수 앞서 이끌어 주신 김광조 교수님께 감사한 마음을 전합니다. 그리고 논문 심사를 맡아 주신 이영희 교수님과 유찬수 교수님께 무언의 격려를 해주신 점 깊이 감사드립니다. ETRI 의 자상하신 이대기부장님, 윤이중팀장께도 감사를 표합니다. 또한 암호와 정보보안 연구실에서 동고동락하면서 재치있고 앞선 지적 능력으로 도움을 준 서문석, 황규범, 김희선, 이병천, 백준상, 안국환, 고재승, 박현철, 송보연씨에게 고마움을 전합니다.

마지막으로 아직도 제대로 깨닫지 못했지만 항상 가없이 크신 사랑을 주시는 부모님께 감사 드립니다. 그리고 오늘 이 지면에 가득 담고 싶은 사랑하는 아내 운숙, 예쁜 솔지, 꿈돌이 정원이 모두에게 고마운 마음을 전합니다. 또한 함께 있음으로 든든한 세 동생들과 친구들에게도 고마움을 전합니다.

Curriculum Vitae

Name : Weonkeun Huh
Date of Birth : December 10, 1960
Place of Birth : Jeonbuk, Korea
Address : 388 Yangjae 2 Dong, Seocho-Gu, Seoul, 137-132, KOREA

Educations

1981 - 1987 : Yonsei University (B.S.)

Career

1993.6 – 1999.12: Human Resources Management Team, Samsung SDS Co., Ltd., Seoul, Korea

Papers

1. 허원근, 김광조, “전자선거 프로토콜의 요구사항 연구”, 한국통신정보보호학회 논문지, 제출(1999. 9. 18).

본 논문은 전자선거 프로토콜의 요구사항을 규정해 보고, 컴퓨터 통신상에서 이를 충족시키기 위한 암호기법 들을 분석해 본다. 전자선거의 도입이 선거 비용을 절감시키고 투표 장소의 제약을 획기적으로 개선하지만 매표방지등의 문제로 아직은 완전한 이동성을 제공하지는 못한다. 그리고 투표결과의 정확성 검증과 매표방지는 서로 상충되는 요구사항이기도 하다. 실제선거에서는 효율성의 문제로 영지식증명기법등의 사용이 제약 받을 수도 있다. 이러한 문제들을 정리하고, 실제의 선거 절차와 선거 속성들이 전자선거 프로토콜로 어떻게 구현되었는지 비교 검토함으로써, 규정한 요구사항들의 선택적인 적용에 활용코자 한다.

2. 허원근, 김광조, “PVSS 를 이용한 검증가능한 다중 전자선거와 검증성을 제한한 매표방지 다중 전자선거”, Proc. of CISC’99, 1999.

전자선거에 이용되는 (t,n)-threshold 비밀공유기법은 비밀을 n 명이 나누어 공유함으로써 안전성을 높이고 t 명이 비밀을 복원할 수 있게 함으로써 장애에 대비할 수 있게 한다. 특히 공개키 암호기법을 비밀공유에 적용한 PVSS(Publicly Verifiable Secret Sharing) 기법은 누구나가 비밀조각의 유효성을 검증할 수 있다. 전자선거에 PVSS 를 이용하여 투표 결과의 정확성 검증을 쉽게 할 수 있으며 동시에 전자선거의 강인성도 만족시킨다. 본 논문에서는 PVSS 를 이용한 전체검증성을 갖는 다중 전자선거와 검증성을 제한한 매표방지형 다중 전자선거를 제시하고 논의한다.

3. Weonkeun Huh, Kwangjo Kim, “*t* Mixes by User’s Selection”, SCIS’2000.

The mix-net decrypts a list of messages without revealing the relationships of sizes, orders, times and values between inputs and outputs. Using the (t,n)-threshold secret sharing, the mix-net assures high security and holds the robustness against some errors. For t mix servers to do the threshold decryption of the randomized messages, we must construct the quorum with t mixes in n ones. The previous works of the threshold mix-net describe vaguely a way to construct quorum. How to select quorum with t mixes to decrypt the messages and how to manage the order of decryption for t mixes. In this paper we propose that the user who sends the message selects the quorum respectively. Instead of decrypting all messages sequentially, it is possible to decrypt them randomly in our mix-net. The proposed mix-net holds the ${}_nC_t\,(t \le n)$ cases of decryption. The advantages of our method are that the load is distributed and the obstacles of decryption are managed.