PVSS를 이용한 검증가능한 다중 전자선거와 검증성을 제한한 매표방지 다중 전자선거

허원근, 김광조

한국정보통신대학원대학교

Universally Verifiable and Limited Verifiable Receipt-free Multi-way Electronic Elections with PVSS

Weonkeun Huh, Kwangjo Kim

Information and Communications University

요 약

전자선거에 이용되는 (t,n)-threshold 비밀공유기법은 비밀을 n명이 나누어 공유함으로써 안전성을 높이고 t명이 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 PVSS를 이용하여 투표 결과의 정확성 검증을 쉽게 할 수 있으며 동시에 전자선거의 강인성도 만족시킨다. 본 논문에서는 PVSS를 이용한 전체검증성을 갖는 다중 전자선거와 검증성을 제한한 매표방지형 다중 전자선거를 제시하고 논의한다.

I. 개 요

전자선거는 안전성, 편리성, 공간성, 시간성 및 이동성 등에서 장점이 많다. 반면에 개표에 사용되는 선거관리자용 비밀키의 분실이나 훼손등은 선거전체를 중단시킨다. 이러한 장애에 대비하기 위하여 사용하는 기법이 비밀 공유(secret sharing : SS)[Sha79, Bla79] 기법이다. 비밀공유 기법은 비밀을 분산하여 보관하고 필요 시 모아서 비밀을 복원하는 형식이다. 방법은 비밀을 조각(shares)들로 쪼개어 참여자들에게 분배한다. 참여자들은 비밀을 복원할 수 있는 권한이 부여된 단체 또는 사람들이다. (t,n)-threshold 방식으로 비밀 공유를 함으로써 일부 비밀공유자의 장애에도 비밀을 복원할 수 있게 한다.

이 방식의 문제는 분배자가 배분하는 비밀 조각이 유효한지와 비밀 복원 시 참여자가 제출하는 비밀 조각이 유효한지를 판단할 수 없다는 것이다. 이에 대한 해결책을 [CGMA85]에서는 검증 가능한 비밀 공유(Verifiable Secret Sharing : VSS) 개념으로 제시하였다. VSS에서는 참여자가 자신의 비밀조각이 유효한지 검증해 볼 수 있으며 또한 정직한 참여자들에 의해서 비밀이 복원될 수 있다.

참여자뿐만 아니라 누구나 비밀조각의 유효성을 검증할 수 있는 개념이 [CGMA85]에서 제시되었으나, 제시된 구조가 공개적으로 검증가능하지는 않았다. Stadler는 참여자들의 공개키를 비밀 공유에 사용하여 공개적으로 검증가능한 비밀공유(publicly verifiable secret sharing : PVSS) 구조를 제시하였다[Sta96].

[FO98]과 [Sch99]에서는 Stadler의 PVSS 방식을 개선하여 효율성을 증대시키고 비밀의 분배 및 복원이 정당하게 행하여졌음을 증명하였다. [Sch99]에서는 또한 PVSS의 준동형(homomorphic)한 성질을 이용한 응용의 예로 찬반 전자선거를 제안 하였으며, 제안된 전자선거는 전체검증성(universally verifiability)을 만족하고 있다. 하지만 참여자인 분배자(Dealer)와 투표자(Voter) 및 선거관리자(Administrator)등이 서로 구별되지 않고, 준동형 성질의 적용으로 인하여 찬반 투표로 제한되고 있다. 제안된 전자선거에서는 0과 1로 제시되는 투표값을 계산하는 것이 이산대수 문제로 투표자 수가 적어야 하는 제약도 따른다.

본 논문에서는 [Sch99]의 전자선거를 확장하여 참여하는 주체들이 구분되며 검증 가능한 다중(multi-way) 전자선거를 제안한다. 또한 실제 선거에서 처럼, 간접적으로 검증성을 제공하고 선거의 중요한 성질인 매표방지성(receipt-freeness)을 충족하는 전자선거 방식을 함께 제시한다. 제안하는 2가지 전자선거는 (t,n)-threshold 에 기반함으로 강인성(robustness)을 함께 지닌다.

논문의 구성은 공개적으로 검증 가능한 비밀공유 구조와 전자선거 응용 예를 2장에서 소개한다. 3장에서는 PVSS를 이용하여 검증가능한 다중 전자선거와 전체검증성을 제한한 매표방지형 다중 전자선거를 제안한다. 4장에서는 제시한 방식들에 대한 특징을 살펴본다.

II. 공개적으로 검증 가능한 비밀 공유

비밀 공유 구조는, 사용자 집합 U와 U중에서 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:

$$p(x) = \sum_{j=0}^{t-1} a_j x^j, \quad s = a_0. \tag{1}$$

분배자가 비밀하게 선택한 다항식 $p(x)$를 이용하여 n명의 참여자들에게 비밀 $p(i)$를 분배한다. 비밀복원은 n명의 참여자중 임의의 t 명이 모여 Lagrange interpolation 공식[MOV96]으로 구하면 된다:

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

$p(0) = a_0 = s$ 이다. 비밀 값 s는 다음 식으로 구할 수도 있다.

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

비밀의 분배뿐만 아니라 분배된 비밀이 유효한지를 검증하는 것 또한 중요하다. [Scha79, Bla79]의 SS, [CGMA85]의 VSS, 그리고 [Sta96]의 PVSS로 발전한 비밀공유기법에 Schoenmaker는 비밀분배와 비밀복원이 유효함을 증명하는 효율적인 proof of knowledge를 도입하였다. 다음에서는 Schoenmaker가 제안하고 있는 PVSS 기법을 기술하고 전자선거에 응용한 예를 분석한다.

■ Schoenmaker의 PVSS 모델

그룹 G_q $(q : prime)$, 생성자 g와 G, 그리고 참여자 P_i $(1 \le i \le n)$가 있다. P_i의 개인키를 $x_i \in Z_q^*$, 공개키는 $y_i = G^{x_i}$라 하자. 이 때, 분배자는 비밀 s의 조각 s_i인 $p(i)$ $(1 \le i \le n)$를 다음과 같이 분배한다:

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

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

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

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 (6)를 만족하는 proof of knowledge를 함께 공지한다.

$$y_i = G^{x_i}, \; Y_i = S_i^{x_i} \tag{6}$$

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

있게 된다.

$$\prod_{i=1}^{t} S_i^{l_i} = \prod_{i=1}^{t} (G^{p(i)})^{l_i} = G^{\sum_{i=1}^{t} p(i) l_i} = G^{p(0)} = G^{s} \qquad (7)$$

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

■ Schoenmaker가 예시한 찬반 전자선거

식 (7)에서 보듯이 이 PVSS는 준동형(homomorphism)의 성질이 있다. 이를 찬반 전자선거에 응용하여 전체검증성을 갖도록 한 예를 [Sch99]에서 제안하고 있다. 이 전자선거는 투표자와 선거관리자가 동일하고, 투표자가 비밀 분배자가 되는 이사회 의결(board-room elections)과 같은 작은 규모의 투표의 예로 다음과 같다.

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

② 투표자는 비밀 s는 m명의 투표자에게 분배

③ $Y_i^* = \prod_{j=1}^{m} Y_{ij} = y_i^{\sum_{j=1}^{m} p_j(i)}$ 를 계산

④ Y_i^*를 공개키 y_i에 대응하는 비밀키 x_i 로 decryption

⑤ 각 투표자의 비밀 G^{s_j}를 복원

⑥ 준동형 성질로 $\prod_{j=1}^{m} U_j = G^{\sum_{j=1}^{m} s_j + v_j}$ 계산

⑦ $G^{\sum_{j=1}^{m} s_j}$는 m명 투표자들의 비밀 값이므로 $G^{\sum_{j=1}^{m} v_j}$의 계산이 가능

⑧ v_j는 0또는 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.

이를 개선한 전자선거를 다음 장에서 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.

III. PVSS형 대규모 다중 전자선거 방식

1. PVSS형 전체검증 가능한 다중 전자선거

PVSS를 이용하여 전체검증성을 만족하는 다중 전자선거 방식은 투표자와 선거관리자로 구성된다. 선거관리자는 자신의 공개키를 등록한다. 투표자는 투표값을 암호화하는 비밀 값과 다항식을 선택하고 선거관리자들의 공개키를 이용하여 비밀 조각을 분배한다. 선거관리자는 자신의 개인키로 비밀 조각을 복호화 한다. 선거관리자는 투표 값들을 계수하여 결과를 공표한다. 투표자가 배분한 비밀 조각을 복호화하였으므로 누구나가 결과를 검증해 볼 수 있게 된다. 이를 상세히 기술하면 다음과 같다.

① 표기

- 그룹 G_q에서의 생성자 g, G
- 투표자 V_i
- 선거관리자 A_j 의 개인키 $x_j \in_R Z_q^*$, 공개키 $y_j = G^{x_j}$

② 투표자 V_i의 투표

- 임의의 t-1 차 다항식 p 선택
- $p(x) = \sum_{j=0}^{t-1} a_j x^j$ 를 이용하여 비밀 분배 ($s_i = a_0$, $s_{ij} = p(i)$)
- 투표 $(G^{s_i} v,\ y_j^{s_{ij}}) \begin{Bmatrix} i = 1,\ldots,m \\ j = 1,\ldots,n \end{Bmatrix}$ 생성

③ 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

④ 결과 집계 (Any one)

- $\prod_{j=1}^{t} (G^{s_{ij}})^{l_j} = G^{\sum_{j=1}^{t} s_{ij} l_j} = G^{s_i}$
- $(G^{s_i} v,\ y_j^{s_{ij}})$의 $G^{s_i} v$ 로부터 $G^{s_i} v / G^{s_i} = v$ 얻음
- v를 후보자별로 더하여 투표 결과 공표

투표자가 선택한 임의의 $t-1$차 다항식의 계수 a_j를 $C_j = g^{a_j}$로 공지하고, $X_i = \prod_{j=0}^{t-1} C_j^{i^j}$ 라 하면, V_i 는 식 (8)을 만족하도록 유일한 $s_{ij} = p(j)$의 proof of knowledge를 생성하여 비밀 분배를 옳게 했음을 보일 수 있다.

$$X_i = g^{s_{ij}}, \quad Y_i = y_i^{s_{ij}} \qquad (8)$$

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

2. 전체 검증성을 제한한 PVSS형 매표방지 다중 전자선거

검증성(또는 전체검증성)은 투표내용을 확인할 수 있는 어떤 방법을 투표자나 제삼자에게 제공하는 것이고, 매표방지성은 투표의 내용과 투표자를 연결할 수 있는 방법을 차단하는 것이다. 이는 상호 표리적인 관계로 동시에 만족시키기가 어렵다. 매표방지성을 제시한 논문들[Ben87, NR94, BT94, SK95]과 전체검증성을 제시한 논문들[CGS97, Abe98]이 두가지 조건을 충족하지 못하고 있음이 이를 반증한다.

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.

① 표 기

- 그룹 G_q에서의 생성자 g, G
- 투표자 V_i
- 선거관리자 A_j 의 개인키 $x_j \in_R Z_q^*$, 공개키 $y_j = G^{x_j}$

② 투표자 V_i의 투표

- 임의의 *t-1* 차 다항식 p 선택
- $p(x) = \sum_{j=0}^{t-1} a_j x^j$ 를 이용하여 비밀 분배 ($s_i = a_0$, $s_{ij} = p(j)$)
- 투표 $(G^{s_i} v, \ y_j^{s_{ij}}) \begin{Bmatrix} i = 1,\ldots,m \\ j = 1,\ldots,n \end{Bmatrix}$ 생성

③ 분배자의 재암호화 및 게시

- 임의의 $t-1$차 다항식 q 선택

- $q(x)=\sum_{j=0}^{t-1} b_j x^j$ 를 이용하여 비밀 분배 ($d_i = b_0$, $d_{ij} = q(j)$)
- 투표 값을 $(G^{d_i} G^{s_i} v,\ y_j^{d_{ij}} y_j^{s_{ij}}) \begin{Bmatrix} i=1,...,m \\ j=1,...,n \end{Bmatrix}$ 로 재암호화하여 게시

④ 선거관리자 A_j 의 복호화

- $(y_j^{d_{ij}} y_j^{s_{ij}})^{1/x_j} = G^{d_{ij}+s_{ij}}$ 계산

⑤ 결과 집계 (Any one)

- $\prod_{j=1}^{t} (G^{d_{ij}+s_{ij}})^{l_j} = G^{\sum_{j=1}^{t}(d_{ij}+s_{ij}) l_j} = G^{d_i+s_i}$
- $G^{d_i} G^{s_i} v / G^{d_i+s_i} = v$ 얻음
- v를 후보자별로 더하여 투표 결과 공표

1의 방식(PVSS형 전체검증 가능한 다중 전자선거)처럼, 투표자는 식 (8)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 b_j를 $D_j = g^{b_j}$로 공지하고, $X_i' = \prod_{j=0}^{t-1} D_j^{i^j}$ 라 하여, 식 (9)를 만족하도록 유일한 $d_{ij} = q(j)$의 proof of knowledge를 생성하면 투표자가 자신의 투표값을 증명할 수 있게 되기 때문이다.

$$X_i' = g^{d_{ij}},\ Y_i' = y_i^{d_{ij}} \qquad (9)$$

결과적으로, 투표 결과에 대한 정확성 검증은 간접적으로 행해질 수 밖에 없다. 현행의 선거에서도 투표를 한 후, 자신의 투표 값이나 투표 결과를 직접적으로 검증할 방법은 없다. 단지 이의를 제기하는 방식으로 검증해 볼 수 있을 뿐이다. 이 장에서 제시한 방식의 전자선거도 투표자가 분배자의 협조를 얻는 간접적인 방식으로 검증성은 확인될 수 있다.

Ⅳ. 제안 방식의 특징

앞 장에서 제안한 2가지 방식의 특징을 전자선거 프로토콜의 요구사항별

로 관찰해 본다(방법 1 : PVSS형 전체검증 가능한 다중 전자선거, 방법 2 : 전체 검증성을 제한한 PVSS형 매표방지 다중 전자선거).

① 완전성(Completeness) : 모든 유효 투표가 정확하게 집계되어야 한다는 것으로, 최종 집계에서 정당한 투표가 제거되는 일이 없어야 한다.

방법 1) 방법 2) : 참여자들이 정직하다면 투표의 결과는 신뢰할 수 있다.

② 건전성(Soundness) : 부정한 투표자에 의해 선거가 방해되는 일이 없어야 한다는 것으로, 최종 집계에서 부정 투표가 집계되어 선거에 영향을 끼치지 않아야 한다.

방법 1) 방법 2) : 투표자에 대한 인증 방법이 필요하며 제시한 투표값에 대해서는 투표자가 값을 변경할 수 없다.

③ 비밀성(Privacy) : 모든 투표가 비밀로 되어야 한다는 것으로, 특히 개인의 투표내용으로부터 그 개인을 확인할 수 없어야 한다.

방법 1) 방법 2) : PVSS 성질에 의하여 투표값과 투표자를 연결할 수 없다. 하지만 메시지와 투표자를 연결할 수는 있으므로 익명통신로를 이용하여 트래픽 분석을 방지해야 한다.

④ 단일성 또는 이중투표불가성(Unreusability) : 정당한 투표자가 두 번 이상 투표할 수 없다는 것으로 단지 한 번만 투표할 수 있어야 한다.

방법 1) 방법 2) : 투표자에 대한 인증 방법이 필요하다.

⑤ 적임성 또는 선거권(Eligibility) : 투표 권한을 가진 자만이 투표할 수 있는 것으로 투표가 허락되지 않은 사람은 투표할 수 없어야 한다.

방법 1) 방법 2) : 투표자에 대한 인증 방법이 필요하다.

⑥ 공정성(Fairness) : 투표에 영향을 미치는 어떤 것이 없어야 한다는 것으로 투표 중에 일부분 결과를 알게 되어 투표에 영향을 미치는 상황 등이 없어야 한다.

방법 1) 방법 2) : n명 중 t명 이상의 선거관리자들이 공모하지 않는다면 투표를 개표할 수 없다. 고로 모든 투표가 완료된 후 개표를 진행할 수 있으므로 공정성을 만족한다.

⑦ 검증성(Verifiability) : 선거 결과를 속일 수 없도록 누구라도 투표 결과를 확인하여 검증해 볼 수 있어야 한다.

방법 1) : 투표자는 자신이 제시한 비밀값의 확인으로 개별 검증할 수 있으며, 누구든지 PVSS 성질을 이용하여 전체 결과를 검증할 수 있다.

방법 2) : 분배자가 투표자의 투표값을 재 암호화 하였으므로 간접적인 검증만이 가능하다. 즉, 검증하기 위해서는 샘플링에 의해 일부의 투표자들을 선

택한 후 분배자의 협조로 검증할 수 있을 것이다.

⑧ 매표방지성(Receipt-freeness) : 투표자가 자신의 투표값을 증명할 수 없어야 한다.

방법 1) : 투표자는 자신의 투표값을 증명할 수 있으므로 매표방지성이 없다.

방법 2) : 투표자의 투표값을 분배자가 재 암호화하여 게시하였으므로 투표자는 자신의 투표값을 증명할 수 없다.

⑨ 강인성(Robustness) : 일부 선거관리자의 부정한 행위 또는 장애에도 영향을 받지 않아야 한다.

방법 1) 방법 2) : (t,n)-threshold 비밀공유기법의 적용으로 t 미만인 선거관리자의 부정에 대하여 안전하다. 또한 일부 장애에 대하여도 안전하다. 하지만 투표값의 복호화를 위하여는 최소한 t명의 선거관리자가 있어야 한다.

V. 결 론

누구나가 검증가능한 비밀공유기법인 PVSS를 이용한 2가지 전자선거 방식을 제안하였다. 방식 1에서는 투표자가 비밀 값을 선정하고 투표값을 암호화하고 선거관리자의 공개키를 사용하여 비밀을 분배하도록 하였다. 1의 방식으로는 검증성 및 강인성을 만족한다. 반면에 방식 2에서는 분배자가 투표자의 투표값을 재 암호화하여 게시함으로써 매표방지성은 구현되지만 검증성은 제한되었다.

PVSS 기법은 비밀공유에 공개키를 사용하는 방식으로 누구나가 공개적으로 비밀 조각의 유효성 검증이 가능하다. 또한 비밀 조각을 직접적으로 알지 않더라도 비밀공유의 기능이 수행된다. 그리고 전자선거에 응용되었을 때 선거관리자들은 자신의 비밀키를 노출하지 않고서도 복호화를 행할 수 있으므로 비밀키의 재 사용이 가능한 것이 특징이다.

이러한 PVSS 기법의 장점을 인증기법과 결합하여 전자선거 프로토콜의 요구사항을 만족시키데 대한 지속적인 연구가 필요하다고 생각된다

참고문헌

[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.

[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.

[Ben87] J.C.Benaloh, "Verifiable secret ballot elections", PhD thesis, Yale University, TR561, 1987

[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.

[MOV96] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, "Handbook of Applied Cryptography", 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. , 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.

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