사용자 중심의 전자선거에 적합한 부인봉쇄 다중서명 기법

윤성현†

요 약

본 논문에서는 이산 대수 문제에 기반 한 부인봉쇄 디지털 다중서명 기법을 제안한다. 제안한 다중서명 기법은 부인봉쇄 성질을 만족하며 메시지 변조, 서명자들에 의한 다중서명 부정과 같은 능동적 공격에 안전하다. 여러 명의 선거관리자를 두는 전자선거 기법에 적용될 수 있으며, 부인봉쇄 성질을 만족하기 때문에 투표자와 선거관리자들 간의 분쟁을 해결할 수 있다. 제안한 기법은 선거관리 센터의 역할을 분산함으로써 기존의 전자선거보다 공정하며 사용자 중심의 전자선거를 가능하게 한다.

키워드 : 부인봉쇄 서명, 부인봉쇄 다중서명, 전자선거 기법

The Undeniable Digital Multi-Signature Scheme Suitable for User-Oriented Electronic Election

Sung-Hyun Yun†

ABSTRACT

In this study, the undeniable digital multi-signature scheme based on the discrete logarithms is proposed. The proposed multi-signature scheme satisfies undeniability and is secure against active attacks such as fabrication and denial of multi-signature by signers. It is suitable for electronic election scheme in which several administrators are required. Especially in case of dispute among voters and administrators, the proposed scheme can resolve it due to the undeniable property. It can provide fair electronic election by minimizing the role of voting center, and can enable user-oriented electronic election.

Keywords : Undeniable Signature, Undeniable Multi-Signature, Electronic Voting Scheme

1. 서 론

디지털 서명 기법은 전자 문서에 대한 서명을 생성하는 방법이다. 디지털 서명이 법적 구속력을 갖기 위해서는 서명자가 서명한 사실에 대해서 부인할 수 없고 문서 수신자를 포함한 모든 사용자가 올바르게 서명된 전자 문서의 정당함을 부인할 수 없어야 한다. 따라서 디지털 서명 기법은 서명 위조 및 메시지 변조를 할 수 없도록 하는 암호학적 인증 기법이 적용된다[6,7].

Chaum이 처음 제안한 부인봉쇄 디지털 서명 기법(undeniable digital signature scheme)은 서

† 정 회 원: 천안대학교 정보통신학부 조교수(교신저자)
논문접수: 2005년 3월 10일, 심사완료: 2005년 5월 18일

명자의 동의 없이는 서명을 검증할 수 없는 기법으로 많은 응용 분야를 갖는다[1,5]. 기업 내의 기밀 전자 문서와 같은 경우에 서명된 문서가 복제에 의해서 다른 사용자들에게 알려지게 되면 기업의 손익에 큰 영향을 미칠 수 있다. 원하는 수신자만 서명 검증을 할 수 있도록 하는 부인봉쇄 서명 기법의 적용이 필수적이다.

부인봉쇄 다중서명 기법은 모든 서명자들의 동의 없이는 서명 검증을 할 수 없는 기법이다. 본 논문에서는 이산대수 문제에 기반한 부인봉쇄 다중서명 기법을 제안한다. 제안한 방법은 다중서명 생성, 다중서명 확인 및 부인 프로토콜로 구성된다. 다중서명 생성 프로토콜은 동시 다중서명 방식으로 진행되며, 다중서명 확인 및 부인 프로토콜은 순차적으로 진행된다[8]. 제안한 방법의 부인봉쇄 성질 및 적극적 공격에 대한 안전성을 분석하며, 전자선거에의 응용에 대해서 기술한다. 여러 명의 선거관리자들을 이용함으로써 선거관리 센터의 역할을 최소화할 수 있고 부인봉쇄 성질을 통해서 선거관리자들 간의 분쟁을 해결할 수 있는 특성을 갖는다.

2 장에서는 이산대수 문제에 기반 한 기존의 다중서명 기법들에 대해서 살펴보고 3 장에서는 제안한 부인봉쇄 다중서명 기법에 대해서 기술한다. 4 장에서는 제안한 방법의 안전성을 분석하고 5 장에서는 사용자 중심의 전자선거를 위한 제안한 방법의 응용에 대해서 고찰한다. 6 장에서는 결론 및 향후 연구 과제를 제시한다.

2. 관련 연구

El-Gamal 서명 기법[2]에 기반한 대표적인 다중서명 기법에 대해서 살펴본다. 일반 서명 기법을 적용하여 여러 사람의 서명을 수용할 경우에 문서 당 서명 크기가 서명 참여자 수만큼 비례하여 커지게 된다. 2.1 절에서 Harn이 제안한 다중서명 기법은 서명 참여자 수에 관계없이 일반 서명과 똑 같은 크기를 갖는 다중서명을 생성한다. 2.2 절의 은닉 다중서명 기법은 Harn의 다중서명 기법에 기반하며 전자선거에서의 투표권 은닉 기술에 적용된다.

2.1 Harn의 다중서명 기법

메시지 기안자는 다중서명을 받을 메시지를 생성하고 서명자들에게 메시지를 동보 전송한다. 서명자들은 수신한 메시지에 대해서 서명자들의 공통키를 이용해서 각자의 서명을 생성하고 메시지 기안자에게 서명을 전송한다. 메시지 기안자는 서명자들의 서명을 검증하고 이를 조합하여 다중서명을 생성한다[3].

서명자들의 수는 전부 t 명이고 각각의 비밀키와 공개키는 다음과 같다고 가정한다.

서명자들 : $u_1, u_2, \ldots, u_t$

서명자 i의 비밀키 : $x_i \in Z_q$, $1 \le i \le t$

서명자 i의 공개키 : $y_i \equiv g^{x_i} \pmod{p}$, $1 \le i \le t$

(1) 서명자들의 공통키 생성

단계 1: 서명자 i는 Z_q 상에서 임의의 난수 k_i 를 선택하고 k_i에 대한 공개값 r_i 를 다음과 같이 생성한다.

$$k_i \in Z_q, \quad r_i \equiv g^{k_i} \pmod{p}$$

단계 2: 서명자 i는 서명에 참여하는 나머지 t-1 명의 서명자들에게 r_i 를 동보 전송한다.

단계 3: 서명자들은 동보 전송된 r_i 를 이용하여 공통키 r 을 생성한다.

$$r \equiv \prod_{i=1}^{t} r_i \equiv g^{k_1 + k_2 + \ldots + k_t} \equiv g^{\sum_{i=1}^{t} k_i} \pmod{p}$$

(2) 서명자들의 서명 생성

단계 1: 서명자 i는 공통키 r, 비밀키 x_i, 난수 k_i 를 이용하여 다음과 같이 메시지 m 에 대한 서명 s_i 를 생성한다.

$$s_i \equiv x_i \cdot (m + r) + k_i \pmod{p-1}$$

단계 2: 서명자 i는 메시지 기안자에게 서명 s_i 를 전송한다.

(3) 메시지 기안자의 다중서명 생성

단계 1: 메시지 기안자는 서명자들의 공통키 r 과 각 서명자의 공개키 y_i, 난수 정보 r_i, 서명

s_i를 이용해서 다음과 같이 t 개의 서명을 검증한다.

$$y_i^{m+r} \cdot r_i \equiv g^{x_i \cdot (m+r)} \cdot g^{k_i} \equiv g^{s_i} \pmod{p}$$

단계 2: t 개의 서명을 조합하여 메시지 m에 대한 다중서명을 생성한다.

$$s \equiv \sum_{i=1}^{t} s_i \pmod{p-1}$$

단계 3: 메시지 m에 대한 다중서명 (r, s)는 다음과 같이 검증된다.

$$y \equiv \prod_{i=1}^{t} y_i \pmod{p}, \quad y^{m+r} \cdot r \equiv g^s \pmod{p}$$

2.2 Horster가 제안한 은닉 다중서명 기법

Horster가 제안한 은닉 다중서명 기법은 은닉 서명 기법의 확장 개념으로 여러 명의 서명자들로부터 은닉 메시지에 대한 서명을 받아서 원본 메시지에 대한 다중서명을 생성하는 방법이다[4].

전부 t 명의 서명자들이 참여할 때 각 서명자의 공개키 및 비밀키는 다음과 같다.

서명자들 : $u_1, u_2, \ldots, u_t$

서명자 i의 비밀키 : $x_i \in Z_q$, $1 \le i \le t$

서명자 i의 공개키 : $y_i \equiv g^{x_i} \pmod{p}$, $1 \le i \le t$

(1) 공통키 생성

단계 1: 서명자들은 각각 Z_q 상에서 임의의 난수 k_i^-를 선택하고 k_i^-에 대한 공개값 r_i^-를 생성한다.

$$k_i^- \in_R Z_q, \quad r_i^- \equiv g^{k_i^-} \pmod{p}, \quad 1 \le i \le t$$

단계 2: 서명자들은 단계 1에서 생성한 r_i를 동보 전송한다.

단계 3: 서명자들의 은닉 공통키 r^-는 다음과 같이 생성된다.

$$r^- \equiv \prod_{i=1}^{t} r_i^- \pmod{p}$$

단계 4: 메시지 기안자는 은닉 공통키 r^-로부터 다음과 같이 공통키 r을 생성한다.

$$a, b \in Z_q, \quad y \equiv \prod_{i=1}^{t} y_i \pmod{p}$$

$$r \equiv r^{-a} \cdot y^b \pmod{p}$$

(2) 은닉 다중서명 생성

단계 1: 메시지 기안자는 메시지 m을 다음과 같이 은닉한다.

$$m^- \equiv (m + r + b) \cdot a^{-1} - r^- \pmod{q}$$

단계 2: 메시지 기안자는 m^-와 r^-를 서명자들에게 전송한다.

단계 3: 서명자들은 각자 은닉 메시지 m^-에 대한 서명 s_i^-를 생성한다.

$$s_i^- \equiv x_i \cdot (m^- + r^-) + k_i^- \pmod{q}$$

단계 4: 서명자들은 은닉 메시지에 대한 서명 s_i^-를 메시지 기안자에게 전송한다.

(3) 서명 검증 및 원본 메시지에 대한 서명 추출

단계 1: 메시지 기안자는 다음과 같이 은닉 메시지 m^-에 대한 각 서명자의 서명을 검증한다.

$$y_i^{m^- + r^-} \cdot r_i^- \equiv g^{s_i^-} \pmod{p}$$

단계 2: 원본 메시지 m에 대한 다중서명 (r, s)를 추출한다.

$$s^- \equiv \sum_{i=1}^{t} s_i^- \pmod{q}, \quad s \equiv s^- \cdot a \pmod{q}$$

단계 3: 메시지 m에 대한 다중서명 (r, s)는 다음과 같이 검증된다.

$$y^{m+r} \cdot r \equiv y^{m+r} \cdot (r^{-a} \cdot y^b)$$

$$\equiv y^{m+r+b} \cdot \left(\prod_{i=1}^{t} g^{s_i^- - x_i \cdot (m^- + r^-)}\right)^a$$

$$\equiv g^{a \cdot s^-} \cdot y^{-(m^- + r^-) \cdot a} \cdot y^{m+r+b} \equiv g^s \pmod{p}$$

3. 제안한 부인봉쇄 다중서명 기법

부인봉쇄 서명 기법의 확장 개념인 부인봉쇄 다중서명 기법에 대해서 제안한다. 전자선거 및 공동 저작권 보호 등과 같이 여러 서명자들의 서명이 요구되며, 부인봉쇄 성질이 필요한 응용에 적용될 수 있는 기법이다.

3.1 부인봉쇄 다중서명 생성 프로토콜

그림 1은 제안한 다중서명 기법에서 다중서명을 생성하는 과정이다. 메시지 기안자는 메시지

와 해쉬 파라미터를 서명자들에게 전송한다. 서명자들은 다중서명을 위한 공통키를 생성하고 메시지 m 에 대한 부인봉쇄 서명을 만들어서 메시지 기안자에게 전송한다. 메시지 기안자는 서명자들의 부인봉쇄 서명을 조합하여 부인봉쇄 다중서명을 생성한다.

[정의 1] 암호학적으로 안전한 유한체 $GF(p)$ 와 군 G_q

p 는 큰 소수로 유한체 $GF(p)$ 상에서 모듈라 p 에 대한 이산 대수를 구하는 것이 계산상 불가능할 때 $GF(p)$ 를 암호학적으로 안전한 유한체라 정의한다. $p-1$ 의 인수 중 큰 소수를 q 라 가정하면, 군 G_q 는 $GF(p)$ 의 부분 집합 군으로 위수 q 를 갖는다.

암호학적으로 안전한 유한체 $GF(p)$ 는 정의 1과 같다. g 는 모듈라 p 에 대한 위수(order) $p-1$ 을 갖는 생성자(generator)이다. 서명자들의 수가 n 명일 때 각 서명자의 비밀키 및 공개키는 다음과 같이 정의된다.

서명자들: $u_1, u_2, \ldots\ldots, u_n$, 메시지: m

서명자 i의 비밀키: $x_i \in Z_{p-1},\ 1 \le i \le n$

서명자 i의 공개키: $y_i \equiv g^{x_i} \pmod{p}, 1 \le i \le n$

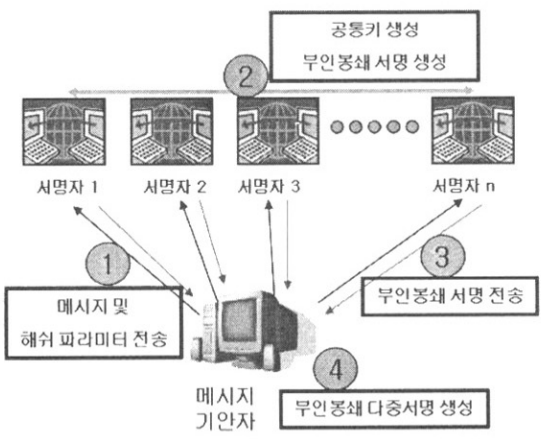

그림 1. 제안한 부인봉쇄 다중서명 생성 프로토콜의 도해

(1) 첫번째 서명자의 공통키 생성

단계 1: 메시지 기안자는 메시지 m 과 해쉬 파라미터 hpr 을 서명자들에게 전송한다. 메시지 m 에 대한 해쉬값 m_h 가 모듈라 p 에 대한 원시근(primitive root)이 되도록 hpr 을 설정한다.

$$m_h = h(m, hpr)$$

단계 2: 첫번째 서명자는 Z_{p-1} 상에서 임의의 난수 k_1 를 선택하고 k_1 에 대한 공개값 r_1 를 생성한다.

$$k_1 \in Z_{p-1},\ \gcd(k_1, p-1) = 1$$

$$m_h = h(m, hpr),\ r_1 \equiv m_h^{k_1} \pmod{p}$$

단계 3: 첫번째 서명자는 서명자들의 대표 공개키 Y 를 생성하기 위해서 Y_1 을 다음과 같이 설정한다.

$$Y_1 = y_1$$

단계 4: 첫번째 서명자는 단계 2와 3에서 생성된 (r_1, Y_1) 을 두번째 서명자에게 전송한다.

(2) 서명자 i의 공통키 생성

단계 1: 서명자 i는 서명자 i-1로부터 (r_{i-1}, Y_{i-1}) 을 수신한다.

$$r_{i-1} \equiv r_{i-2}^{k_{i-1}} \pmod{p} \equiv m_h^{\prod_{j=1}^{i-1} k_j} \pmod{p}$$

$$Y_{i-1} \equiv Y_{i-2}^{x_{i-1}} \pmod{p} \equiv g^{\prod_{j=1}^{i-1} x_j} \pmod{p}$$

단계 2: 서명자 i는 Z_{p-1} 상에서 임의의 난수 k_i 를 선택하고 k_i 에 대한 공개값 r_i 를 생성한다.

$$k_i \in_R Z_{p-1},\ \gcd(k_i, p-1) = 1$$

$$r_i \equiv r_{i-1}^{k_i} \equiv m_h^{k_1 \cdot k_2 \cdots k_i} \equiv m_h^{\prod_{j=1}^{i} k_j} \pmod{p}$$

단계 3: 서명자 i는 자신의 비밀키 x_i 를 이용하여 다음과 같이 Y_i 를 생성한다.

$$Y_i \equiv Y_{i-1}^{x_i} \equiv g^{x_1 \cdot x_2 \cdots x_i} \equiv g^{\prod_{j=1}^{i} x_j} \pmod{p}$$

단계 4: 서명자 i는 서명자 i+1에게 (r_i, Y_i) 를 전송한다.

단계 5: 서명자 i가 마지막 서명자일 때 까지 단계 1부터 단계 4를 반복한다. 마지막 서명자는 다음과 같이 서명자들의 공통키 R 과 대표 공개키 Y 를 구해서 서명자들 및 메시지 기안자에게

동보 전송한다.

$$R \equiv r_{n-1}^{k_n} \equiv m_h^{k_1 \cdot k_2 \cdot \cdots \cdot k_n} \equiv m_h^{\prod_{j=1}^{n} k_j} \pmod{p}$$

$$Y \equiv Y_{n-1}^{x_n} \equiv g^{x_1 \cdot x_2 \cdot \cdots \cdot x_n} \equiv g^{\prod_{j=1}^{n} x_j} \pmod{p}$$

(3) 다중서명 생성

단계 1: 서명자들은 각자 공통키 R 을 이용하여 다음 식을 만족하는 s_i 를 구한다. k_i 와 $p-1$은 서로소이므로 s_i 에 대한 유일한 해가 존재한다.

$$k_i \cdot s_i \equiv x_i \cdot R - k_i \cdot m_h \pmod{p-1},\ 1 \le i \le n$$

단계 2: 서명자들은 s_i 를 메시지 기안자에게 전송한다.

단계 3: 메시지 기안자는 서명자들로부터 전송받은 s_i 를 다음과 같이 조합하여 부인봉쇄 다중서명 S 를 생성한다.

$$S \equiv \prod_{j=1}^{n} (m_h + s_j) \pmod{p}$$

3.2 부인봉쇄 다중서명 확인 프로토콜

메시지 기안자는 (R, S) 가 메시지 m 에 대한 올바른 다중서명인지 확인하기 위해서 그림 2와 같은 다중서명 확인 프로토콜을 수행한다.

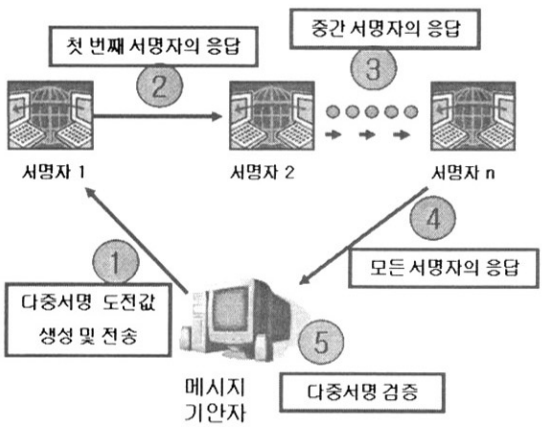

그림 2. 제안한 부인봉쇄 다중서명 확인 프로토콜의 도해

(1) 메시지 기안자의 도전 생성

단계 1: 메시지 기안자는 임의의 난수 (a, b)를 Z_{p-1} 상에서 선택하고 도전 ch 를 다음과 같이 생성해서 첫번째 서명자에게 전송한다.

$$ch \equiv R^{S \cdot a} \cdot Y^{R^n \cdot b} \equiv m_h^{a \cdot \prod_{j=1}^{n} k_j (m_h + s_j)} \cdot g^{b \cdot R^n \cdot \prod_{j=1}^{n} x_j}$$

$$\equiv m_h^{a \cdot R^n \cdot \prod_{j=1}^{n} x_j} \cdot g^{b \cdot R^n \cdot \prod_{j=1}^{n} x_j} \pmod{p}$$

단계 2: 첫번째 서명자는 다음과 같이 응답 rsp_1 을 생성해서 두번째 서명자에게 전송한다. x_1^{-1} 는 모듈라 $p-1$ 에 대한 x_1 의 모듈라 곱셈의 역이다.

$$rsp_1 \equiv ch^{x_1^{-1}} \equiv m_h^{a \cdot R^n \cdot \prod_{j=2}^{n} x_j} \cdot g^{b \cdot R^n \cdot \prod_{j=2}^{n} x_j} \pmod{p}$$

(2) 서명자 i의 응답 생성

단계 1: 서명자 i는 서명자 i-1로부터 응답 rsp_{i-1} 를 수신한다.

$$rsp_{i-1} \equiv rsp_{i-2}^{x_{i-1}^{-1}} \equiv ch^{\prod_{j=1}^{i-1} x_j^{-1}}$$

$$\equiv m_h^{a \cdot R^n \cdot \prod_{j=i}^{n} x_j} \cdot g^{b \cdot R^n \cdot \prod_{j=i}^{n} x_j} \pmod{p}$$

단계 2: 서명자 i는 x_i^{-1} 를 이용하여 다음과 같이 응답 rsp_i 를 생성한다. x_i^{-1} 는 모듈라 $p-1$ 에 대한 x_i 의 모듈라 곱셈의 역이다.

$$rsp_i \equiv rsp_{i-1}^{x_i^{-1}} \equiv m_h^{a \cdot R^n \cdot \prod_{j=i+1}^{n} x_j} \cdot g^{b \cdot R^n \cdot \prod_{j=i+1}^{n} x_j} \pmod{p}$$

단계 3: 서명자 i는 서명자 i+1에게 응답 rsp_i 를 전송한다.

단계 4: 서명자 i가 마지막 서명자일 때까지 단계 1부터 단계 3을 반복한다. 마지막 서명자는 도전 ch 에 대한 전체 서명자의 응답 rsp_n 을 메시지 기안자에게 전송한다.

(3) 메시지 기안자의 다중서명 검증

메시지 기안자는 다음과 같이 전체 서명자들의 응답을 검증한다.

$$rsp_n \equiv m_h^{R^n \cdot a} \cdot g^{R^n \cdot b} \pmod{p} \quad (3.1)$$

$$rsp_n \not\equiv m_h^{R^n \cdot a} \cdot g^{R^n \cdot b} \pmod{p} \quad (3.2)$$

식 3.1이 성립하면 메시지 기안자는 (R, S) 가 메시지 m 에 대한 올바른 다중서명임을 확인한다. 식 3.2는 다중서명이 잘못된 경우와 서명자들 중 적어도 한 서명자 이상이 부정을 하는 경우이다. 메시지 기안자는 3.3 절의 부인 프로토콜

을 이용해서 다중서명이 잘못된 것인지 서명자들이 부정하는 것인지 확인한다.

3.3 부인 프로토콜

메시지 기안자는 3.2 절의 다중서명 확인 프로토콜에서 응답 rsp_n에 대한 인증에 실패할 경우에 부인 프로토콜을 통해서 서명자들이 부정하는 것인지 다중서명이 잘못된 것인지 확인한다.

(1) 메시지 기안자의 두번째 도전 생성

단계 1: 메시지 기안자는 다음 조건을 만족하는 임의의 난수 c, d를 선택해서 첫번째 서명자에게 전송할 도전 ch'을 생성한다.

$$c,\ d \in Z_{p-1},\ a \cdot d \neq b \cdot c \pmod{p-1}$$

$$ch' \equiv R^{S \cdot c} \cdot Y^{R^n \cdot d} \equiv m_h^{c \cdot R^n \cdot \prod_{j=1}^{n} x_j} \cdot g^{d \cdot R^n \cdot \prod_{j=1}^{n} x_j} \pmod{p}$$

단계 2: 첫번째 서명자는 다음과 같이 응답 rsp_1'을 생성해서 두번째 서명자에게 전송한다.

$$rsp_1' \equiv ch'^{x_1^{-1}} \equiv m_h^{c \cdot R^n \cdot \prod_{j=2}^{n} x_j} \cdot g^{d \cdot R^n \cdot \prod_{j=2}^{n} x_j} \pmod{p}$$

(2) 서명자 i의 응답 생성

단계 1: 서명자 i는 서명자 i-1로부터 응답 rsp_{i-1}'을 수신한다.

$$rsp_{i-1}' \equiv m_h^{c \cdot R^n \cdot \prod_{j=i}^{n} x_j} \cdot g^{d \cdot R^n \cdot \prod_{j=i}^{n} x_j} \pmod{p}$$

단계 2: 서명자 i는 x_i^{-1}를 이용하여 다음과 같이 응답 rsp_i'를 생성한다.

$$rsp_i' \equiv rsp_{i-1}'^{x_i^{-1}} \equiv m_h^{c \cdot R^n \cdot \prod_{j=i+1}^{n} x_j} \cdot g^{d \cdot R^n \cdot \prod_{j=i+1}^{n} x_j} \pmod{p}$$

단계 3: 서명자 i는 다음 서명자에게 응답 rsp_i'을 전송한다.

단계 4: 서명자 i가 마지막 서명자일 때 까지 단계 1부터 단계 3을 반복한다. 마지막 서명자는 도전 ch'에 대한 전체 서명자의 응답 rsp_n'을 메시지 기안자에게 전송한다.

(3) 메시지 기안자의 다중서명 검증

단계 1: 메시지 기안자는 다음과 같이 전체 서명자들의 응답을 검증한다.

$$rsp_n' \equiv m_h^{R^n \cdot c} \cdot g^{R^n \cdot d} \pmod{p}$$

$$rsp_n' \not\equiv m_h^{R^n \cdot c} \cdot g^{R^n \cdot d} \pmod{p}$$

단계 2: 단계 1에서 다중서명 검증에 실패할 경우에 메시지 기안자는 rsp_n와 rsp_n'을 이용해서 다음 식을 만든다.

$$R_1 \equiv (rsp_n \cdot g^{-R^n \cdot b})^c \pmod{p}$$

$$R_2 \equiv (rsp_n' \cdot g^{-R^n \cdot d})^a \pmod{p}$$

단계 3: R_1과 R_2를 비교함으로써 서명자들의 부정인지 다중서명이 잘못된 것인지 확인한다.

$R_1 = R_2$: 다중서명이 잘못된 것이다.

$R_1 \neq R_2$: 서명자들 중 적어도 한 서명자 이상이 올바른 다중서명에 대해서 부인하는 경우이다.

4. 부인봉쇄 성질 분석

제안한 부인봉쇄 다중서명 기법의 부인봉쇄 성질을 분석한다. 정리 4.1은 잘못된 다중서명에 대해서 메시지 기안자가 올바른 응답을 생성하는 도전값을 둘 이상 생성할 수 없음을 보여 준다. 정리 4.1에 기반하여 제안한 부인 프로토콜의 정당성을 정리 4.2와 4.3에서 보여 준다. 정리 4.2는 서명자들의 부정을 4.3은 다중서명이 잘못됐음을 입증한다.

[정의 2] 메시지 m에 대한 올바른 다중서명 (R, S)와 잘못된 다중서명 (R', S)를 다음과 같이 정의한다.

m_h는 메시지 m에 대한 해쉬값이고 X는 전체 서명자들의 비밀키를 모듈라 $p-1$에 대해서 모듈라 곱셈한 결과이다.

$$m_h = h(m, hpr),\ X \equiv \prod_{j=1}^{n} x_j \pmod{p-1}$$

· 올바른 다중서명 (R, S)

$$R \equiv m_h^{\prod_{j=1}^{n} k_j} \pmod{p},\ S \equiv \prod_{j=1}^{n} (m_h + s_j) \pmod{p-1}$$

$$\prod_{j=1}^{n} k_j (m_h + s_j) \equiv R^n \cdot X \pmod{p-1}$$

· 잘못된 다중서명 (R', S)

$$R' \equiv m_h^{\prod_{j=1}^{n} k_j} \pmod{p}$$

$$\prod_{j=1}^{n} k_j(m_h + s_j) \not\equiv R'^{n} \cdot X \pmod{p-1} \quad (4.1)$$

식 4.1은 잘못된 다중서명에 대한 관계식으로 다음 식 4.2를 만족하는 X'을 정의한다.

$$\prod_{j=1}^{n} k_j(m_h + s_j) \equiv R'^{n} \cdot X' \pmod{p-1},\ X \neq X' \quad (4.2)$$

[정리 4.1] 잘못된 다중서명에 대해서 올바른 응답을 생성하는 도전값은 둘 이상 존재할 수 없다.

(증명) Z_{p-1} 상에서 정의되는 도전값 (a, b) 와 (a', b') 이 동일한 도전과 올바른 응답을 생성한다고 가정한다. 메시지 기안자가 잘못된 다중서명에 대해서 올바른 응답을 생성하는 도전값을 둘 이상 생성할 수 없으면 서명자들은 잘못된 다중서명에 대해서 올바른 응답을 할 수 없다.

잘못된 다중서명 (R', S) 에 대해서 도전값 (a, b) 와 (a', b') 을 이용하여 생성한 도전과 응답은 다음과 같다.

· (a, b) 를 이용한 도전 ch 와 응답 rsp_n

$$ch \equiv R'^{S \cdot a} \cdot Y^{R'^{n} \cdot b} \pmod{p}$$

$$\equiv m_h^{a \cdot R'^{n} \cdot X} \cdot g^{b \cdot R'^{n} \cdot X} \pmod{p}$$

$$rsp_n \equiv m_h^{R'^{n} \cdot a} \cdot g^{R'^{n} \cdot b} \pmod{p}$$

· (a', b') 을 이용한 도전 ch' 과 응답 rsp_n'

$$ch' \equiv R'^{S \cdot a} \cdot Y^{R'^{n} \cdot b} \pmod{p}$$

$$\equiv m_h^{a \cdot R'^{n} \cdot X} \cdot g^{b \cdot R'^{n} \cdot X} \pmod{p}$$

$$rsp_n' \equiv m_h^{R'^{n} \cdot a} \cdot g^{R'^{n} \cdot b} \pmod{p}$$

도전값 (a, b) 와 (a', b') 이 동일한 도전을 생성한다고 가정했으므로 다음 식 4.3과 4.4를 유도할 수 있다.

$$m_h^{(a-a') \cdot R'^{n} \cdot X} \equiv g^{(b-b') \cdot R'^{n} \cdot X} \pmod{p} \quad (4.3)$$

$$m_h^{(a-a') \cdot R'^{n}} \equiv g^{(b-b') \cdot R'^{n}} \pmod{p} \quad (4.4)$$

식 4.4를 식 4.3에 대입하면 다음과 같이 식 4.5가 유도된다.

$$m_h^{(a-a') \cdot R'^{n} \cdot X} \equiv m_h^{(a-a') \cdot R'^{n} \cdot X} \quad (4.5)$$

정의 2에서 $X \neq X'$ 이므로 식 4.5는 성립될 수 없다. 따라서 잘못된 다중서명에 대해서 동일한 도전을 생성하는 도전값은 둘 이상 존재할 수 없다. Q.E.D.

[정리 4.2] 서명자들의 부정

올바른 다중서명에 대해서 서명자들 중 적어도 한 서명자 이상이 부인하는 경우에 부인 프로토콜을 통해서 서명자들의 부정을 입증할 수 있다.

(증명) m_h 에 대한 올바른 서명 (R, S) 는 정의 2와 같다. 서명자들 중 적어도 한 서명자 이상이 부정할 경우에 응답 생성 과정에서 도전 ch 에 대한 모듈라 지수 곱셈의 역이 변하게 된다. 올바른 모듈라 지수 곱셈의 역은 X^{-1} 이고 잘못된 역은 X'^{-1} 라 가정한다.

$$X^{-1} \equiv \prod_{j=1}^{n} x_j^{-1} \pmod{p-1},\ x_j \neq x_j'$$

$$X'^{-1} \equiv \prod_{j=1}^{n} x_j'^{-1} \pmod{p-1},\ X^{-1} \neq X'^{-1}$$

메시지 기안자는 다음과 같이 서명 (R, S) 에 대한 도전을 생성한다.

$$ch \equiv R^{S \cdot a} \cdot Y^{R'^{n} \cdot b} \pmod{p}$$

$$\equiv m_h^{a \cdot R'^{n} \cdot X} \cdot g^{b \cdot R'^{n} \cdot X} \pmod{p}$$

전체 서명자들의 응답 rsp_n 은 다음과 같다.

$$rsp_n \equiv ch^{X^{-1}} \pmod{p}$$

$$\equiv m_h^{a \cdot R'^{n} \cdot X \cdot X^{-1}} \cdot g^{b \cdot R'^{n} \cdot X \cdot X^{-1}} \pmod{p}$$

$$rsp_n \not\equiv m_h^{a \cdot R'^{n}} \cdot g^{b \cdot R'^{n}} \pmod{p} \quad (4.6)$$

메시지 기안자는 부인 프로토콜을 수행하여 (c, d) 에 대한 도전 ch' 을 생성하고 응답 rsp_n' 을 수신한다.

$$ch' \equiv R^{S \cdot c} \cdot Y^{R'^{n} \cdot d} \pmod{p}$$

$$\equiv m_h^{a \cdot R'^{n} \cdot X} \cdot g^{b \cdot R'^{n} \cdot X} \pmod{p}$$

$$rsp_n' \equiv ch'^{X^{-1}} \pmod{p}$$

$$\equiv m_h^{c \cdot R'^{n} \cdot X \cdot X^{-1}} \cdot g^{d \cdot R'^{n} \cdot X \cdot X^{-1}} \pmod{p}$$

$$rsp_n' \not\equiv m_h^{c \cdot R'^{n}} \cdot g^{d \cdot R'^{n}} \pmod{p} \quad (4.7)$$

식 4.6과 4.7에서 서명자들의 응답은 메시지 기안자가 생성한 검증 값과 다르다. 메시지 기안자는 rsp_n, rsp_n' 을 이용해서 다음 식을 계산한다.

$$R_1 \equiv (rsp_n \cdot g^{-R'' \cdot b})^c$$
$$\equiv m_h^{a \cdot c \cdot R'' \cdot X \cdot X^{-1}} \cdot g^{c \cdot (b \cdot R'' \cdot X \cdot X^{-1} - b \cdot R'')} (\mathrm{mod}\ p)$$
$$R_2 \equiv (rsp_n' \cdot g^{-R'' \cdot d})^a$$
$$\equiv m_h^{c \cdot a \cdot R'' \cdot X \cdot X^{-1}} \cdot g^{a \cdot (d \cdot R'' \cdot X \cdot X^{-1} - d \cdot R'')} (\mathrm{mod}\ p)$$

제안한 부인 프로토콜에서 서명자들이 부정을 하는 경우에 다음 식과 같이 R_1과 R_2는 다른 값을 갖게 된다.

$$m_h^{a \cdot c \cdot R'' \cdot X \cdot X^{-1}} \cdot g^{c \cdot b \cdot R'' \cdot (X \cdot X^{-1} - 1)}$$
$$\neq m_h^{c \cdot a \cdot R'' \cdot X \cdot X^{-1}} \cdot g^{a \cdot d \cdot R'' (X \cdot X^{-1} - 1)}$$
$$(\because\ b \cdot c \not\equiv d \cdot a\ (\mathrm{mod}\ p-1))$$

Z_{p-1} 상에서 선택된 도전 값 a, b, c, d는 메시지 기안자가 생성한 것으로 서명자들은 도전 값을 모르기 때문에 R_1과 R_2를 같게 할 수 없다. Q.E.D.

[정리 4.3] 잘못된 다중서명

다중서명이 잘못됐음을 부인 프로토콜을 통해서 입증한다.

(증명) m_h에 대한 잘못된 다중서명 (R', S)는 정의 2와 같다.

(R', S)에 대한 첫번째 도전과 응답은 다음과 같다.

$$ch \equiv R'^{S \cdot a} \cdot Y^{R'' \cdot b}\ (\mathrm{mod}\ p)$$
$$\equiv m_h^{a \cdot R'' \cdot X'} \cdot g^{b \cdot R'' \cdot X}\ (\mathrm{mod}\ p)$$
$$rsp_n \equiv m_h^{a \cdot R'' \cdot X' \cdot X^{-1}} \cdot g^{b \cdot R''}\ (\mathrm{mod}\ p)$$
$$\neq m_h^{a \cdot R''} \cdot g^{b \cdot R''}\ (\mathrm{mod}\ p)\quad (4.8)$$

(R', S)에 대한 두번째 도전과 응답은 다음과 같다.

$$ch' \equiv R'^{S \cdot c} \cdot Y^{R'' \cdot d}\ (\mathrm{mod}\ p)$$
$$\equiv m_h^{c \cdot R'' \cdot X'} \cdot g^{d \cdot R'' \cdot X}\ (\mathrm{mod}\ p)$$
$$rsp_n' \equiv m_h^{c \cdot R'' \cdot X \cdot X^{-1}} \cdot g^{d \cdot R''}\ (\mathrm{mod}\ p)$$
$$\neq m_h^{c \cdot R''} \cdot g^{d \cdot R''}\ (\mathrm{mod}\ p)\quad (4.9)$$

식 4.8과 4.9에서 서명자들의 응답은 메시지 기안자가 생성한 검증 값과 다르다. 메시지 기안자는 rsp_n, rsp_n'을 이용해서 다음 식을 계산한다.

$$R_1 \equiv (rsp_n \cdot g^{-R'' \cdot b})^c \equiv m_h^{a \cdot c \cdot R'' \cdot X \cdot X^{-1}} (\mathrm{mod}\ p)$$
$$R_2 \equiv (rsp_n' \cdot g^{-R'' \cdot d})^a \equiv m_h^{c \cdot a \cdot R'' \cdot X \cdot X^{-1}} (\mathrm{mod}\ p)$$

R_1과 R_2가 같기 때문에 다중서명이 잘못됐음을 알 수 있다. Q.E.D.

5. 부인봉쇄 다중서명 기법과 전자선거

전자선거에서 부인봉쇄 다중서명 기법의 필요성에 대해서 고찰한다. 먼저 안전한 전자선거를 위해서 꼭 필요한 부정 투표 방지와 개인의 익명성 보장 문제간의 상관관계를 살펴본다.

부정 투표를 방지하기 위해서는 디지털 서명 기법을 적용해야 한다. 투표권에 대한 디지털 서명은 해당 투표권을 갖는 투표자만이 생성할 수 있기 때문에 제 3 자에 의한 부정 투표를 방지할 수 있다. 단점은 디지털 서명의 특성상 모든 사용자가 투표권의 서명을 검증할 수 있기 때문에 누가 누구에게 투표했는지 알 수 있으므로 투표자의 익명성을 보장할 수 없다. 따라서 민주주의 사회에서의 선거 기법으로는 적용될 수 없다.

개인의 익명성을 보장하기 위해서는 자신의 이름 대신 익명을 사용하여 투표를 해야 한다. 투표자는 투표권을 은닉하여 자신의 이름으로 은닉 투표권에 대한 선거관리 센터의 인증을 받고, 인증된 은닉 투표권으로부터 은닉값을 해제한 인증된 투표권을 획득한다. 이 경우 익명으로 투표를 하기 때문에 누가 누구에게 투표했는지 알 수 없게 된다. 개인의 익명성은 보장할 수 있지만 선거관리 센터에 전적으로 의존해야 하는 부담이 따른다.

전자선거는 앞서 살펴 본 바와 같이 개인의 익명성을 보장하려면 선거관리 센터의 신뢰성에 기반해야 하고, 부정 투표를 방지하려면 개인의 익명성을 보장할 수 없는 상반 관계가 존재한다[9]. 따라서 개인의 익명성을 보장하면서 선거관리 센터에 의한 부정을 최소화하는 방안에 대한 연구가 필요하다.

전자선거에 참여하는 후보자들이 공정한 표 대결을 하기 위해서는 각 후보자가 소속된 정당별로 선거관리자를 두어서 모든 선거관리자들의 동의 하에서만 인증된 은닉 투표권을 생성하고 개표할 수 있는 기법이 제공되어야 한다. 기존의

선거관리 센터의 역할을 여러 명의 선거관리자들로 분산하고, 전체 선거관리자들의 동의 하에서만 투표 및 개표가 가능하게 함으로써 부정 투표를 최소화할 수 있다.

부인봉쇄 다중서명 기법은 모든 서명자의 동의 없이는 서명 검증을 할 수 없는 기법으로 여러 명의 선거관리자들로 구성되는 전자선거에 응용될 수 있는 서명 기법이다. 또한 도전/응답 형식의 다중서명 확인 및 부인 프로토콜이 포함되기 때문에 투표 및 개표 단계에서의 선거의 공정성(fairness)[4,9] 실현에 응용될 수 있고, 부인봉쇄 성질을 만족하기 때문에 투표권에 대한 분쟁 발생시에 선거관리자들의 부정을 해결할 수 있는 특성을 갖는다.

6. 결론

본 논문에서는 이산 대수 문제에 기반한 부인봉쇄 다중서명 기법을 제안하였다. 부인봉쇄 다중서명 기법은 모든 서명자들의 동의 없이는 서명 검증을 할 수 없다. 제안한 방법은 다중서명 생성 프로토콜, 다중서명 확인 프로토콜 그리고 부인 프로토콜로 구성된다. 부인봉쇄 성질을 만족하며 서명 위조 및 서명 부인과 같은 능동적 공격에 대해서 안전하다. 제안한 방법을 전자선거 기법에 응용하게 되면, 기존의 선거관리 센터의 역할을 최소화할 수 있고 각 정당별로 선거관리자를 배정하여 모든 선거관리자들의 동의 하에서만 투표 및 개표를 수행할 수 있도록 함으로써 전자 선거의 신뢰성을 향상시킬 수 있다.

참 고 문 헌

[1] D.Chaum(1990). Undeniable Signatures. Advances in Cryptology, Proceedings of CRYPTO'89, Springer-Verlag, pp.212-216.

[2] T.Elgamal(1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp.469-472.

[3] L.Harn(1993). (t,n) Threshold Signature and Digital Multisignature. Workshop on Cryptography & Data Security, pp.61-73.

[4] P.Horster and H.Petersen(1995). Blind multisignature schemes and their relevance for electronic voting. Proceedings of COMPSAC'95, pp.149-155.

[5] T.P.Pedersen. Distributed provers with applications to undeniable signatures. Advances in Cryptology, Proceedings of Eurocrypt'91, LNCS 547, pp.221-242.

[6] F.Piper(1991). Digital Signatures. IFIP/SEC'91 Conference, Proceedings of the 7th International Conference and Exhibition on Information Security, pp.62-71.

[7] S.G.Akl(1983). Digital Signatures: A Tutorial Survey. IEEE Computer, pp.15-24.

[8] S.H.Yun and T.Y.Kim(1997). A Digital Multisignature Scheme Suitable for EDI Message. Proceedings of 11th International Conference on Information Networking, pp.9B3.1-9B3.6.

[9] S.H.Yun and S.J.Lee(2003). An electronic voting scheme based on undeniable blind signature scheme. Proceedings of IEEE 37th carnahan conference, pp.163-167.

윤 성 현

1992 고려대학교 컴퓨터학과 (이학학사)

1994 고려대학교 컴퓨터학과 (이학석사)

1997 고려대학교 컴퓨터학과(이학박사)

1998~2002 LG전자/정보통신 중앙연구소 선임연구원

2002~현재 천안대학교 정보통신학부 조교수

관심분야: 정보보호, 전자상거래, 광대역 통신

E-Mail: shyoon@infocom.cheonan.ac.kr