대리 서명방식에 관한 연구 (II)
- 제 2부 : 역치 위임에 의한 대리 서명방식 -

김승주*, 박상준**, 정권성*° 원동호*
*성균관대학교 정보공학과, **한국전자통신연구소

A Study on the Proxy Signatures (II)
- Part 2 : Proxy Signatures with Threshold Delegation -

Seungjoo Kim*, Sangjoon Park**, Kwonsung Chung*°, Dongho, Won*
*Sung Kyun Kwan Univ., **ETRI

요 약

1996년 Mambo가 처음 제안한 대리 서명방식은 원서명자가 지정한 사람이 원서명자를 대신해서 서명을 하는 방법이다. "대리 서명방식에 관한 연구 (I) - 제 1부 : 보증 부분위임에 의한 대리 서명방식"에서는 대리 서명자에게 제공하는 대리 서명용 키의 공개키와 대리 서명용 키의 유효기간을 포함하는 메시지에 원서명자가 서명함으로써 만들어진 보증서를 사용하여 부분 보증 위임을 실현시키는 방법을 제안하였다. threshold 위임은 원서명자가 n명의 대리 서명자를 지정하고 n명의 대리 서명자중 t명 이상의 대리 서명자가 협조하여야 대리 서명을 할 수 있는 개념으로 본 논문에서는 threshold 위임에 의한 대리 서명 방식을 제시하였다.

Abstract

By proxy signatures, proposed by Mambo, a designated signer can sign original's signature instead of original signer. This paper presents new types of digital proxy signatures called partial delegation with threshold delegation. In proxy signatures for partial delegation with threshold delegation, the proxy signer's power to sign messages is shared. In conclusion, we construct proxy signature schemes satisfying our conditions.

1. 서 론

Mambo가 처음 제안한 대리 서명방식(proxy signatures)[1]은 원서명자(original signer)가 지정한 사람(이하 대리 서명자(proxy signer))이 원서명자를 대신해서 서명을 하는 방법으로 다음과 같은 조건을 갖는다.

(1) 위조 불능 : 원서명자가 지정한 대리 서명자만이 원서명자의 정당한 대리 서명을 생성할 수 있다.

(2) 검증 가능성 : 검증하고자 하는 대리 서명이 원서명자로 부터 지정받은 대리 서명자에 의해 서명된 것임을 검증자가 확인할 수 있다.

이러한 방식의 서명은 원서명자의 메시지에 서명하는 능력을 제3자에게 전달하는데 사용될 수 있다. 원서명자가 데이타 통신을 수행할 수 경우 즉, 네트워크에 접촉할 수 없는 상황에 있는 경우 원서명자는 어떠한 디지털 서명도 수행할 수 없게 될 것이다. 이경우 자신의 서명 능력을 제 3자에게 전달하여 제 3자가 원서명자 대신 서명을 수행한 다면 문제는 해결될 것이다.

Mambo는 대리 서명방식을 완전 위임(full delegation), 부분 위임(partial delegation)으로 분류하였으며 이는 대리서명자가 전달 받는 원서명자의 비밀정보의 형태에 따라 구분된다.[1][2][3]

본 논문에서는 여러 명의 대리 서명자를 지정하여 대리 서명시 지정된 서명자들의 상호 협조에 의하여 대리 서명하는 역치 위임(threshold delegation)에 의한 대리 서명방식을 제안한다. threshold 위임에 의한 대리 서명은 원서명자의 서명 능력을 n명의 사람에게 분산 위임하고 n명의 대리 서명자중 t명 이상이 서로 협조하여야 대리 서명할 수 있는 서명방식으로 대리 서명자에 의한 서명의 남용을 방지할 수 있다.

본 논문은 모두 4개의 절로 구성된다. 2절에서는 본 논문에서 제안되는 threshold 위임을 정의하였고, 3절에서는 역치 위임 방식을 구성하는 방법을 제안하였고 제안된 방식을 구성하기 위한 필요 조건과 구체적인 구현 방법을 제시하였다. 4절은 본 논문의 결론부이다.

2. 역치 위임 대리 서명방식의 정의

본 논문에서는 Mambo의 대리 서명방식을 기반으로 한 새로운 형태의 대리 서명방식으로 역치 위임(threshold delegation)이 가능한 대리 서명 방식을 정의하고자 한다. 원서명자는 지정된 그룹에 속한 n명의 대리인에게 대리 서명 능력을 나누어주고 n명중 t명 이상이 서로 협조하여 대리 서명을 만들 수 있으나 t-1명 이하가 협조할 경우에는 대리 서명을 할 수 없도록 하고자 한다고 하자. 만일 원서명자의 권한이 책무가 막중하다면 특정한 한 사람에게 자신의 권한을 주는 것 보다 이와 같은 방식을 원할 수 있을 것이다. 이 경우 대리 서명자에 의한 대리 서명의 남용을 방지할 수 있기 때문이다.

정의 1. 역치 위임이란 n명의 서명자에게 대리 서명 능력을 분산시키는 것으로 n명의 서명자중 t명 이상의 서명자가 서로 협조하여 대리 서명을 생성한다. 다음은 (t, n)-역치 위임이 가져야 할 조건이다.

(1) n명의 대리 서명자중 t명 이상의 서명자가 서로 협조하면 대리 서명을 생성할 수 있다.
(2) 어떤 t-1명 이하의 서명자도 서명을 위조할 수 없다.

역치 위임은 대리 서명자에 의하여 서명이 남용될 가능성을 줄여준다. 다음절에서는 역치 위임에 의한 대리 서명의 구체적인 구성 방법들이 기술되었다.

3. 역치 대리 서명방식

본 절에서는 이러한 특성을 만족하는 Schnorr 서명방식에 의한 (t, n)-역치 대리 서명방식

을 제안하고자 한다. 역치 서명을 만들기 위하여 Ceredo의 Schnorr형 역치 서명방식을 사용한다.[10] 표현의 용이성을 위하여 PG = {P_i | i = 1, 2, ···, n)은 원서명자가 지정한 그룹의 회원들을 나타낸다. 소수 p는 p-1이 160비트 소수 q를 인수로 가지며 (즉, q|p-1), g는 위수 q를 갖는다.

난수 r을 n명의 그룹원에게 분산시켜 나누어 줄 경우, 딜러(dealer)는 랜덤한 다항식 $f(x) = r + a_1x + \cdots + a_{t-1}x^{t-1} \pmod p$를 선택하여 모든 회원 P_i에게 $s_i = f(i) \pmod p$를 비밀리에 전달한다 (i = 1, 2, ···, n). 이 경우 n명중 t명 이상이 모이면 딜러가 생성한 난수 r을 복구할 수 있다. 그러나 딜러는 난수 r을 이미 알 고 있으므로 다른 그룹원이 협조가 필요 없다. 다음의 프로토콜은 어떤 특정 딜러에 의지하지 않고 각 참가자 P_i가 서로 협조하여 t명 이상이 모여야만 공통의 난수 r을 복구할 수 있도록 해주는 난수 생성 프로토콜이다.

[난수 생성 프로토콜] [11][12]

1. 각 참가자 P_i는 난수 k_i를 선택하고, $y_i = g^{k_i} \pmod p$를 계산한다.
2. 난수 k_i를 참가자들에게 나누어주기 위하여 각 P_i는 다음과 같은 $f_i(0) = k_i$인 t-1차 다항식을 만든다.
$$f_i(x) = k_i + a_{i,1}x + a_{i,2}x^2 + \cdots + a_{i,t-1}x^{t-1} \pmod q \quad (a_{i,j} \in Z_q)$$
3. P_i는 $f_i(j)$를 P_j에게 비밀리에 전달하고 다음의 값들은 모든 참가자들에게 알려준다 (i = 1, 2, ···, n).
$$y_i, \ g^{a_{i,1}}, \cdots, \ g^{a_{i,t-1}}, F_{i,1}, \cdots, F_{i,n} \ (F_{i,j} = g^{f_i(j)} \pmod p)$$
4. 이제 모든 참가자 P_i는 다음의 관계식을 확인한다 (i = 1, 2, ···, n).
$$g^{f_j(i)} = y_j \cdot (g^{a_{j,1}})^{i^1} \cdots (g^{a_{j,t-1}})^{i^{t-1}} \pmod p \ (j = 1, 2, \cdots, n)$$
$$F_{j,k} = y_j \cdot (g^{a_{j,1}})^{k^1} \cdots (g^{a_{j,t-1}})^{k^{t-1}} \pmod p \ (k = 1, 2, \cdots, n, \ j = 1, 2, \cdots, n)$$
5. 모든 참가자 는 난수 $r = k_1 + k_2 + \ldots + k_n \pmod p$에 대한 자신의 부분 비밀 정보 $r_i = f_1(i) + f_2(i) + \cdots + f_n(i) \pmod p$를 계산하고 난수 r에 대한 공개 정보 y와 다음의 정보를 계산한다.
$$y = \prod_j y_j, \ g^{a_1} = \prod_j g^{a_{j,1}}, \cdots, \ g^{a_{t-1}} = \prod_j g^{a_{j,t-1}} \ (a_i = \sum_{j=1}^{n} a_{j,i} \pmod q)$$

$f(x) = f_1(x) + f_2(x) + \cdots + f_n(x) \pmod p$라 하면 $f(0) = r \pmod p$이고 $f(x) = r + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1} \pmod q$이며, $r_i = f(i) \pmod q$이다. 따라서, 난수 r은 t명 이상의 참가자의 협조할 경우 Lagrange interpolation에 의하여 구할 수 있으나 t-1명 이하의 참가자들이 협조하는 경우에는 계산할 수 없다. 이제 이와 같은 난수 생성 프로토콜을 사용하여 대리 서명을 하는 방법을 설명하고자 한다.

3.1 대리인 비보호형 역치 대리 서명방식

먼저 원서명자가 대리 서명을 가장할 수 있는, 대리인 비보호형 역치 대리 서명방식을 제안한다. 원서명자가 지정한 그룹의 각 회원들에게 대리 서명용 비밀키를 분산 위임하는 프로토콜은 다음과 같다.

[대리 서명용 키 생성 프로토콜]

1. (원서명자에 의한 키 생성) 원서명자는 난수 k를 생성하여 $K = g^k \pmod p$를 계산하고,

m_w와 K의 해쉬값 $e = h(m_w, K)$를 계산한다.

2. (역치 방식) 원서명자는 (t, n)-역치 방식으로 대리 서명용 키를 나누어주기 위하여 다음과 같은 랜덤한 t-1차 다항식 $f'(x)$을 생성한다.

$$f'(x) = \sigma + b_1x + b_2x^2 + \cdots + b_{t-1}x^{t-1} \pmod q,\ \sigma_i = f'(i) \pmod q$$

3. (키 분배) 이제 $B_j = g^{b_j} \pmod p$, $S_j = g^{\sigma_j} \pmod p$ $(j = 1, \cdots, t-1)$와 (m_w, K)를 모든 참가자에게 공개적으로 나누어주고, σ_i는 각 참가자 P_i에게 비밀리에 전달한다.
4. (부분 키 정보 검증) 각 P_i는 해쉬값 $e = h(m_w, K)$를 계산하고 자신이 받은 키 정보가 σ_i가 올바른 키 정보인지 다음의 관계식으로 확인한다.

$$g^{\sigma_i} = (v_o^e \cdot K) \cdot \prod_{j=1}^{t-1} B_j^{(i^j)} \pmod p,$$

$$S_j = (v_o^e \cdot K) \cdot \prod_{l=1}^{t-1} B_l^{(j^l)} \pmod p \ (j \neq i)$$

이제 그룹 PG에 속하는 참가자중에서 t명 이상이 모여서 메시지 m에 대한 대리 서명을 만드는 과정을 설명한다. 다음의 대리 서명 프로토콜에서 H는 참가하는 참가자들의 집합이다.

[서명 프로토콜]

1. H에 속하는 참가자들 P_i는 '**난수 생성 프로토콜**'을 사용하여 난수 r의 부분 정보를 나누어 갖고 다음과 같은 정보를 H에 속한 모든 참가자에게 준다 (이 경우 '**난수 생성 프로토콜**'의 n은 |H|가 된다).

$$y = g^r \pmod p,\ g^{a_1}, \cdots, g^{a_{t-1}} \pmod p \ \left(a_i = \sum_{j=1}^{n} a_{j,i} \pmod q\right)$$

또한, 각 참가자 P_i에게 $f(i)$를 비밀리에 전달한다 $(f(i) = r + a_1 i + \cdots + a_{t-1} i^{t-1} \pmod q)$.

2. H에 속한 각 참가자 P_i는 $e' = h(y, m)$, $\gamma_i = f(i) + \sigma_i e' = f(i) + f'(i)\, e' \pmod q$를 계산하고 γ_i를 H에 속한 참가자간에 비밀리에 주고받는다.
3. H에 속한 각 참가자 P_i는 다음의 관계식을 확인한다.

$$g^{\gamma_i} = \left(y \prod_{j=1}^{t-1} (g^{a_j})^{i^j}\right) \cdot \left((v_o^e K) \prod_{j=1}^{t-1} (g^{b_j})^{i^j}\right)^{h(y,m)} \pmod p \ (\text{모든 } P_l \in H \text{에 대하여})$$

4. 이제 각 $P_i \in H$는 집합 $\{\gamma_l \mid P_l \in H\}$와 Lagrange interpolation을 사용하면 공통의 비밀정보 $t = r + \sigma e' = f(0) + f'(0)\, e' \pmod q$를 얻을 수 있다. 이제 (m, t, e', K, m_w)를 H가 생성한 대리 서명으로 하고 서명 수신자에게 전달한다.
5. 서명 수신자는 (m, t, e', K, m_w)이 대리 서명임을 다음의 관계식에 의하여 확인한다.

$$y = g^t \cdot (v_o^{h(m_w,K)} K)^{-e'} \pmod p,\ e' = h(y, m)$$

제안된 방식은 원서명자가 H가 생성한 난수 r을 알 수 없기 때문에 t값을 계산할 수 없다. 그러나, r을 확인할 수 있는 어떤 정보도 서명 수신자가 가지고 있지 않기 때문에 원서명자도 임의의 난수 r'을 생성하여 대리 서명 $t' = r' + \sigma e'$을 만들 수 있다.

3.2 대리인 보호형 역치 대리 서명방식

대리인 비보호형 역치 대리 서명은 원서명자가 대리 서명을 위조할 가능이 있는 문제점을

갖는다. 이러한 문제점을 해결하기 위하여 대리 서명자들의 그룹 PG는 자신들이 대리 서명하였음을 수신자가 검증할 수 있도록 그룹 PG를 위한 검증용 비밀키 s_{PG}와 공개키 v_{PG}를 '**난수 생성 프로토콜**'을 사용하여 나누어 갖는다.

[대리 서명용 키 생성 프로토콜]

1. (PG에 의한 대리 서명 검증용 비밀키 생성) 먼저 PG는 '**난수 생성 프로토콜**'을 사용하여 비밀키 s_{PG}와 다음과 같은 공개 정보를 생성한다.

$$v_{PG} \ (= g^{s_{PG}} \pmod p), \ g^{c_1}, \cdots, \ g^{c_{t-1}} \pmod p$$

   특히 v_{PG}는 그룹 PG의 공개키 정보로서 후에 대리 서명자 그룹 PG가 생성한 대리 서명임을 확인하는 데 사용한다. 또한, PG의 어떤 누구도 s_{PG}를 알 수 없으며 비밀키 s_{PG}를 구하기 위해서는 t명 이상이 서로 협조하여야 한다. 생성 과정에서 각 PG의 참가자 P_i에게는 다음과 같은 비밀키 정보 $s_{PG,i}$를 얻게된다.

$$s_{PG} = f''(0), \ s_{PG,i} = f''(i) = s_{PG} + c_1 i + \cdots + c_{t-1} i^{t-1} \pmod q$$

2. (원서명자에 의한 키 생성) 원서명자는 난수 k를 생성하여 $K = g^k \pmod p$를 계산하고, m_w와 K의 해쉬값 $e = h(m_w, K)$를 계산한다 (m_w는 원서명자의 ID, 대리 서명 그룹을 나타내는 ID, 위임 기간 등을 명시한다).
3. (역치 방식) 원서명자는 (t, n)-역치 방식으로 대리 서명용 키를 나누어주기 위하여 다음과 같은 랜덤한 t-1차 다항식 $f'(x)$을 생성한다.

$$f'(x) = \sigma + b_1 x + b_2 x^2 + \cdots + b_{t-1} x^{t-1}, \ \sigma_i = f'(i) \pmod q, \ \sigma = f'(0) \pmod q$$

4. (키 분배) 이제 $B_j = g^{b_j} \pmod p$, $S_j = g^{\sigma_j} \pmod p$ $(j = 1, \cdots, t-1)$와 (m_w, K)를 모든 참가자에게 공개적으로 나누어주고, σ_i는 각 참가자 P_i에게 비밀리에 전달한다.
5. (부분 키 정보 검증 및 서명 키 변환) 각 P_i는 해쉬값 $e = h(m_w, K)$를 계산하고 자신이 받은 키 정보가 σ_i가 올바른 키 정보인지 다음의 관계식으로 확인한다.

$$g^{\sigma_i} = (v_0^e \cdot K) \cdot \prod_{j=1}^{t-1} B_j^{(i^j)} \pmod p,$$

$$S_j = (v_0^e \cdot K) \cdot \prod_{l=1}^{t-1} B_l^{(j^l)} \pmod p \ (j \neq i)$$

   이제 원서명자가 비밀키 정보를 알 수 없도록 하기 위하여 각 참가자 P_i는 다음과 같이 비밀키 정보를 변환하여 $\sigma_{p,i}$를 역치 대리 서명의 비밀키로 사용한다.

$$\sigma_{p,i} = \sigma_i + s_{PG,i} = f(i) + f''(i) \pmod q$$

[서명 프로토콜]

1. H에 속하는 참가자들 P_i는 '**난수 생성 프로토콜**'을 사용하여 난수 r의 부분 정보를 나누어 갖고 다음과 같은 정보를 H에 속한 모든 참가자에게 준다 (이 경우 '**난수 생성 프로토콜**'의 n은 |H|가 된다).

$$y = g^r \pmod p, \ g^{a_1}, \cdots, g^{a_{t-1}} \pmod p \ \left(a_i = \sum_{j=1}^{n} a_{j,i} \pmod q\right)$$

   또한, 각 참가자 P_i에게 f(i)를 비밀리에 전달한다 $(f(i) = r + a_1 i + \cdots + a_{t-1} i^{t-1} \pmod q)$.
2. H에 속한 각 참가자 P_i는 $e' = h(y, m)$, $\gamma_i = f(i) + \sigma_{p,i} e' = f(i) + (f'(i) + f''(i))e' \pmod q$를 계산하고 γ_i를 H에 속한 참가자간에 비밀리에 주고받는다.
3. H에 속한 각 참가자 P_i는 다음의 관계식을 확인한다.

$$\left(y \prod_{j=1}^{t-1} (g^{a_j})^{i^j}\right) \cdot \left(\left((v_0^e K) \prod_{j=1}^{t-1} (g^{b_j})^{i^j}\right) \cdot \left(v_{PG} \prod_{j=1}^{t-1} (g^{c_j})^{i^j}\right)\right)^{e'}$$
$$= g^{f(i)+(f'(i)+f''(i))e'}$$

$= g^{\gamma_i} \pmod p$ (모든 $P_i \in H$에 대하여)

4. 이제 각 $P_i \in H$는 집합 $\{\gamma_i \mid P_i \in H\}$와 Lagrange interpolation을 사용하면 공통의 비밀정보 $t = r + (\sigma + s_{PG})e' = f(0) + (f'(0) + f'(0))e' \pmod q$를 얻을 수 있다. 이제 (m, t, e', K, m_w)를 H가 생성한 대리 서명으로 하고 서명 수신자에게 전달한다.
5. 서명 수신자는 (m, t, e', K, m_w)이 대리 서명임을 다음의 관계식에 의하여 확인한다.

$$y = g^t \cdot (v_o^{h(m_w, K)} \cdot K \cdot v_{PG})^{-e'} \pmod p,\ e' = h(y, m)$$

수신된 서명의 검증 과정에서 원서명자의 공개키 v_o뿐 아니라 그룹 PG의 공개키 v_{PG}를 사용하여 서명을 검증하기 때문에 공개키 v_{PG}에 대응되는 비밀키 s_{PG}를 갖고 있지 못한 원서명자 조차도 대리 서명을 위조할 수 없다.

4. 결 론

본 논문에서는 새로운 형태의 대리 서명방식인 역치 위임에 의한 대리 서명방식을 제안하였다. 최근의 그룹 지향의 사회에서 적용될 수 있는 방식으로 원서명자는 n명의 지정 서명자 그룹을 지정하고 n명 중 t명 이상이 서로 협조할 경우 대리 서명을 할 수 있다. 또한 제안된 방식을 구성하기 위한 필요 조건과 구체적인 구현 방법을 제시하였다.

참고 문헌

[1] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: Delegation of the power to sign messages," IEICE Trans. Fundamentals, vol.E79-A, no.9, 1996, pp.1338-1354.

[2] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," Proc. Third ACM Conf. on Computer and Communications Security, 1996, pp.48-57.

[3] K. Usuda, M. Mambo, T. Uyematsu, and E. Okamoto, "Proposal of an automatic signature scheme using a compiler," IEICE Trans. Fundamentals, vol.E79-A, no.1, 1996, pp.94-101.

[4] V. Varadharajan, P. Allen, and S. Black, "An analysis of the proxy problem in distributed systems," Proc. 1991 IEEE Computer Society Symposium on Research in Security and Privacy, 1991, pp.255-275.

[5] B.C. Neuman, "Proxy-based authorization and accounting for distributed systems," Proc. 13th International Conference on Distributed Computing Systems, 1993, pp.283-291.

[6] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory, vol.IT-31, no.4, 1985, pp.469-472.

[7] B.S. Kaliski, "A response to DSS," Nov. 1991.

[8] C.P. Schnorr, "Efficient signature generation by smart cards," Journal of Cryptology, vol.4, no.3, 1991, pp.161-174.

[9] T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes," Proc. Crypto'92, Lecture Notes in Computer Science, LNCS 740, Springer--Verlag, 1993, pp.31-53.

[10] M. Cerecedo, T. Matsumoto, and H. Imai, "Efficient and secure multiparty generation

of digital signatures based on discrete logarithms," IEICE Trans. Fundamentals, vol.E76-A, no.4, 1993, p.532-545.

[11] T.P. Pedersen, "A threshold cryptosystem without a trusted party," Proc. Eurocrypt'91, Lecture Notes in Computer Science, LNCS 547, Springer--Verlag, 1991, pp.522-526.

[12] T.P. Pedersen, "Distributed provers with applications to undeniable signatures," Proc. Eurocrypt'91, Lecture Notes in Computer Science, LNCS 547, Springer--Verlag, 1991, pp.221-238.

[13] A. Shamir, "How to share a secret," Commun. ACM, vol.22, no.11, 1979, pp.612-613.

[14] Y. Desmedt and Y. Frankel, "Shared generation of authenticators and signatures," Proc. Crypto'91, Lecture Notes in Computer Science, LNCS 576, Springer--Verlag, 1991, pp.457-469.

[15] C. Park and K. Kurosawa, "New ElGamal type threshold digital signature scheme," IEICE Trans. Fundamentals, vol.E79-A, no.1, 1996, pp.86-93.

[16] S.J. Park, S.J. Kim and D.H. Won, "Proxy signature, revisited," Proc. of ICICS'97, International Conference on Information and Communications Security, Springer, Lecture Notes in Computer Science, 1997, to appear.