대리 서명 방식의 확장에 관한 연구

김소진 °, 이명희 †, 최재귀 ‡, 박지환 °
부경대학교 전자계산학과 °, 전산정보학과 †, 정보보호학(협) ‡

A Study on Extended Proxy Signature

So-Jin Kim, Myoung-Hee Lee, Jae-Gwi Choi, Ji-Hwan Park
Dept. of Computer Science, PuKyong Nat'l University

요 약

Araki[5]등은 Mambo[1]의 대리 서명 방식을 확장하여 대리 서명자의 부재시 또 다른 대리 서명자가 원 서명자를 대신해서 서명을 생성할 수 있는 다단계(multi-level) 대리 서명 방식을 제안하였다. 그러나 그들이 제안한 방식은 검증자가 전송받은 서명이 타당한 서명자들로부터 생성된 것인지 확신할 수 없는 문제점과 다단계 환경(예를 들어 위임 서명 유효기간 재설정)에 적합한 위임 서명 키 생성이 어렵다는 문제점이 있다. 따라서 본 논문에서는 전자적 처리 환경에 좀 더 안전하고 융통성있는 응용을 위해 보증 위임 대리 서명 방식과 proxy-signcryption 방식을 확장한 다단계 대리 서명 방식을 제안하고자 한다.

1. 서론

대리 서명방식은 원 서명자가 지정한 사람이 원 서명자를 대신해서 서명을 하는 방식으로 다음과 같은 조건을 가져야 한다.

- 위조 불능
  원 서명자가 지정한 서명자만이 원 서명자의 정당한 대리서명을 생성할 수 있다. 제 3자는 위임서명을 생성할 수 없어야 한다.
- 검증 가능성
  위임 서명을 확인하는 검증자는 대리 서명이 원 서명자가 인정한 대리 서명자에 의하여 서명되었음을 확인할 수 있어야 한다.

예를 들어 어떤 회사의 간부가 정보 통신망에 접속할 수 없는 지역으로 출장을 간다고 생각해 보자. 그는 출장 기간동안 어떤 문서에 결재하거나 메일등에 응답할 수 있는 권한을 다른 사람에게 부여해야 한다.

Mambo등은 이런 상황에서 본인이 부재시 대신 서명을 할 수 있는 대리 서명 방식을 최초로 제안하였다[1].

다시 앞의 예를 생각해보자. 만약에 대리 서명을 위임받은 대리인도 출장을 가야 할 상황이 발생한다면 그도 역시 서명 생성 능력을 위임해야만 할 것이다.

이에 본 논문에서는 기존의 보증 위임 대리 서명 방식을 확장하여 다단계 대리서명 방식을 제안하고, 나아가 디지털 서명과 암호 시스템의 기능을 동시에 제공하는 proxy-signcryption 방식을 확장하고자 한다.

2. 관련연구

대리 서명 방식을 처음 제안한 Mambo등은 [1]에서 위임 유형에 따라 완전 위임, 부분 위임, 보증 위임 방식으로 대리 서명을 분류하였다.

KPW[2]는 서명 정보와 대리 서명용 키의 유효기간을 포함하는 메시지에 대한 서명 결과인 보증서를 통해 대리 서명을 실행시키는 방식을 제안함으로서 Mambo의 기법을 확장하였다.

그 후 Gamage등은 Mambo가 제안한 부분 위임 대리 서명 방식과 Zheng의 signcryption 방식[3]의 장점을 이용하여 proxy-signcryption 방식을 제안하였다[4]. Proxy-signcryption이란 사용자가 지정한 대리인이 자신을 대신하여 정당한 signcryption 메시지를 생성할 수 있도록 하는 방식으로 signcryption을 생성하는데 요구되는 계산을 상대적으로 계산 능력이 뛰어난 proxy agent에 의존하는 것이다. 그러나 그들이 제안한 방식을 실제 응용에 적용할 경우 사용자가 proxy agent를 대신하여 정당한 서명을 생성할 수 있을 뿐만 아니라 자신이 전송한 메시지에 대해 부인할 수 있는 문제점이 있다. 이를 해결하기 위해 오수현 등[6]은 대리인 보호형 proxy-signcryption을 제안함으로 해결하였다.

이 후 Araki 등은 Mambo의 대리 서명 방식을 확장한 다단계(Multi-level) 대리 서명 방식을 제안하였다[5]. Araki 등이 제안한 다단계 대리 서명 방식은 다음과 같다.

(1) 대리 서명용 키 생성

- 원 서명자 U_0는 아래와 같이 대리 서명용 키를 생성하여 대리 서명자 U_1에게 전송한다.
  1. U_0은 난수 $k_0 \in Z_{p-1}$을 선택한 후 $K \equiv g^{k_0} \pmod{p}$을 계산한다.
  2. U_0은 대리 서명용 키 $\sigma_0 \equiv x_o + k_0 K_0 \pmod{p-1}$ 를 계산한다.
  3. U_0은 대리 서명용 키 σ_0는 안전한 채널을 통해 U_1에게 전송하고, K는 신뢰센터에 보낸다.

- i번째 대리 서명자 U_i $(i>0)$가 다른 대리 서명자 U_{i+1}에게 원 서명자 U_0의 서명 생성 능력을 위임하고자 한다면 다음의 단계를 수행한다.
  1. U_i은 서명 생성 키 $\lambda_i \equiv \sigma_i + x_i y_i \pmod{p-1}$ 를 계산한다.
  2. U_i은 난수 $k_i \in Z_{p-1}$ 을 선택한 후 $K_i \equiv g^{k_i} \pmod{p}$을 계산한다.
  3. U_{ii}은 대리 서명용 키 $\sigma_i \equiv (\sigma_{i-1} + x_i) y_i + k_i \pmod{p-1}$ 를 계산하고 , K_i는 신뢰센터에 등록한다.
  4. U_{ii}는 대리 서명용 키 σ_i를 U_{i+1}에게 전송한다.

(2) 대리 서명용 키 검증

대리 서명자 U_i는 U_{i-1}에게 받은 σ_i와 U_{i-1}의 공개키 y_{i-1}와 대리 서명용 공개키 σ_{i-1}를 이용하여 다음을 계산하여 대리 서명용 키를 검증한다.

$$g^{\sigma_{i-1}} \equiv (((y_0 K_0^{K_0} y_1)^{y_1} K_1) \cdots y_{i-1})^{y_{i-1}} K_{i-1} \pmod{p}$$

위 식이 검증되면, U_i는 U_0의 대리 서명용 키 λ_i, σ_i 를 생성할 수 있다. 여기에서 λ_i는 서명키이고, σ_i는 다른 대리인에게 보내는 대리 서명용 키이다.

(3) 서명 생성 및 검증

U_i는 일반 서명 방식을 이용하여 $SIG_{U_i}(m, \lambda_i)$ 대리 서명을 생성할 수 있다. 또한 이 서명을 받은 검증자도 다음 식과 같이 대리 서명 공개키를 검증할 수 있다.

$$\rho_i \equiv g^{\lambda_i} \pmod{p}$$
$$\equiv (((y_0 K_0^{K_0} y_1)^{y_1} K_1 \cdots y_{i-1})^{y_{i-1}} K_{i-1}) y_i^{y_i}$$

그리고 $Ver(Sig_{U_i}(m, \lambda_i), \rho_i)$을 이용하여 대리 서명을 검증할 수 있다.

위의 방식은 원 서명자가 지정한 대리인이 아닌 다른 사람이 원 서명자를 대신해서 서명할 수 있는 문제가 발생하여 결국 검증자는 타당하지 않은 대리 서명자가 생성한 서명도 원 서명자의 서명이라고 확신할 수 있게 된다. 또한 대리 서명을 다단계로 확장함으로써 생길 수 있는 상이한 위임환경에도 적합하지 않다. 이 문제점을 해결하기 위하여 대리 서명자와 유효 기간을 지정한 보증 위임 대리 서명 방식을 확장한 방식과 대리인 보호형 proxy-signcryption을 확장한 방식을 제안한다.

3. 제안 방식

3.1 보증 위임 대리 서명 방식의 확장

- 시스템 설정
  - p : 512비트 이상의 큰 소수
  - q : $q|p-1$인 큰 소수

- g : 위수가 q인 Z_p상의 원소
- x_i : 각 대리자(*i-th proxy signer*)의 비밀키
- y_i : 각 대리자의 공개키
- h : 해쉬함수

(1) 대리 서명용 키 생성

· 원 서명자 U_0는 아래와 같이 대리 서명용 키를 생성하여 대리 서명자 U_1에게 전송한다.

1. U_0은 난수 $k_0 \in Z_{p-1}$ 을 선택한 후 $K_0 \equiv g^{k_0} \pmod p$을 계산한다.
2. U_0은 자신 ID와 대리 서명자 ID, 유효 기간등을 포함한 보증서 m_0와 K_0을 가지고 $e_0 \equiv h(m_o, K_0) \pmod q$ 을 계산한다
3. U_0은 대리 서명용 키 $s_0 \equiv x_o e_0 + k_0 \pmod q$를 계산한다.
4. U_0은 s_0, e_0, m_0를 안전한 채널을 통해 U_1에게 전송한다.

· i번째 대리 서명자 $U_i\,(i>0)$가 다른 대리 서명자 U_{i+1}에게 원 서명자 U_0의 서명 생성 능력을 위임하고자 한다면 다음 단계를 수행한다.

1. U_i은 난수 $k_i \in Z_{p-1}$ 을 선택한 후 $K_i \equiv g^{k_i} \pmod p$을 계산한다.
2. U_i은 $e_i \equiv h(m_0 \| m_1 \| \cdots \| m_i, K_i) \pmod q$ 를 계산한다. 이 때 이전에 받은 $m_0, m_1, \cdots, m_{i-1}$의 내용과 m_i (다음 대리 서명자의 ID와 유효기간 명시)을 연결하여 해쉬함수를 적용한다.
3. U_i은 대리 서명 생성 키 $s_i \equiv s_{i-1} + x_i e_i + k_i \pmod q$를 계산한다.
4. U_i는 $s_i, (e_0, e_1, \cdots, e_i), (m_0, m_1, \cdots, m_i)$를 U_{i+1}에게 전송한다.

(2) 대리 서명용 키 검증

대리 서명자 U_i는 U_{i-1}에게 받은 정보와 U_{i-1}의 공개키 y_{i-1}와 대리 서명용 공개키를 이용하여 다음과 같이 대리 서명용 키를 검증한다.

1. $e_{i-1}' \equiv h(m_0 \| m_1 \| \cdots \| m_{i-1}, K_{i-1})$을 계산한 후 e_{i-1}과 같은 지 확인한다.
2. 위 식이 성립하면 $g^{s_{i-1}} \equiv y_0^{e_0} y_1^{e_1} \cdots y_{i-1}^{e_{i-1}} K_0 K_1 \cdots K_{i-1} \pmod p$을 확인한다.

위 식이 검증되면, U_i는 U_0의 대리 서명용 키 s_i, r_i 를 생성할 수 있다. 여기에서 r_i는 서명키이고, s_i는 다른 대리인에게 보내는 대리 서명용 키이다.

$$r_i \equiv s_{i-1} + e_{i-1} x_i \pmod q$$

(3) 서명 생성 및 검증

U_i는 일반적인 서명 방식을 이용하여 $SIG_{U_i}(m, r_i)$대리 서명을 생성할 수 있다. 또한 이 서명을 받은 검증자도 다음 식과 같이 대리 서명 공개키를 검증할 수 있다.

$$R_i \equiv g^{r_i} \pmod p$$
$$\equiv y_0^{e_0} y_1^{e_1} \cdots y_{i-1}^{e_{i-1}} y_i^{e_{i-1}} K_0 K_1 \cdots K_{i-1} \pmod p$$

그리고 $Ver(Sig_{U_i}(m, r_i), R_i)$을 이용하여 대리 서명을 검증할 수 있다.

3.2 대리인 보호형 Proxy-signcryption 확장

· 시스템 설정

- p : 512비트 이상의 큰 소수
- q : $q|p-1$인 큰 소수
- g : 위수가 q인 Z_p상의 원소
- x_i : 각 대리자(*i-th proxy signer*)의 비밀키
- y_i : 각 대리자의 공개키
- y_v : 검증자의 공개키
- h : 해쉬함수
- $E(\ ), D(\ )$: 관용 암호/복호 알고리즘

(1) 대리 서명용 키 생성

· 원 서명자 U_0는 아래와 같이 대리 서명용 키를 생성하여 대리 서명자 U_1에게 전송한다.

1. U_0은 난수 $k_0 \in Z_{p-1}$ 을 선택한 후 $K_0 \equiv g^{k_0} \pmod p$을 계산한다.
2. U_0은 자신 ID와 대리 서명자 ID, 유효 기간 등

을 포함한 보증서 m_0와 K_0을 가지고 $e_0 \equiv h(m_o, K_0)$ (mod q) 을 계산한다

3. U_0은 대리 서명용 키 $s_0 \equiv x_o e_0 + k_0$ (mod q) 를 계산한다.
4. U_0은 s_0, e_0, m_0를 안전한 채널을 통해 U_1에게 전송한다.

- i번째 대리 서명자 $U_i\,(i>0)$가 다른 대리 서명자 U_{i+1}에게 원 서명자 U_0의 서명 생성 능력을 위임하고자 한다면 다음의 단계를 수행한다.

1. U_i은 난수 $k_i \in Z_{p-1}$ 을 선택한 후 $K_i \equiv g^{k_i}$ (mod p)을 계산한다.
2. U_i은 $e_i \equiv h(m_0 \| m_1 \| \cdots \| m_i, K_i)$ (mod q) 를 계산한다. 이 때 이전에 받은 $m_0, m_1, \cdots, m_{i-1}$의 내용과 m_i (다음 대리 서명자의 ID와 유효기간 명시)을 연결하여 해쉬 함수를 적용한다.
3. U_i은 대리 서명 생성 키 $s_i \equiv s_{i-1} + x_i e_i + k_i$ (mod q)를 계산한다.
4. U_i는 $s_i, (e_0, e_1, \cdots, e_i), (m_0, m_1, \cdots, m_i)$를 U_{i+1}에게 전송한다.

(2) 대리 서명용 키 검증

대리 서명자 U_i는 U_{i-1}에게 받은 $s_i, e_i, (m_0, m_1, \cdots, m_i)$와 U_{i-1}의 공개키 y_{i-1}와 대리 서명용 공개키를 이용하여 다음을 계산하여 대리 서명용 키를 검증한다.

$$g^{s_{i-1}} \equiv y_0^{e_0} y_1^{e_1} \cdots y_{i-1}^{e_{i-1}} K_0 K_1 \cdots K_{i-1} \quad (\text{mod } p)$$

위 식이 검증되면, U_i는 U_0의 대리 서명용 키 s_i, r_i 를 생성할 수 있다. 여기에서 r_i는 서명키이고, s_i는 다른 대리인에게 보내는 대리 서명용 키이다.

(3) 서명 생성

U_i는 비밀 랜덤 수 $k_i \in Z_{p-1}$을 선택하여 $IK \equiv y_v^{k_i}$ (mod p) 계산한다. $IK = IK_1 \| IK_2$로 나누고 다음과 같이 메시지 m 에 대한 signcryption을 생성한다.

$$H \equiv h_{IK_2}(m)$$

$$r \equiv \left(\frac{k_i}{H + x_i + s_{i-1}}\right)$$

$$C \equiv E_{IK_1}(m)$$

메시지 m에 대한 signcryptioned 메시지 $(C, r, H, (e_0, e_1, \cdots, e_i))$를 검증자에게 전송한다.

(4) proxy-signcryption의 검증

검증자는 자신의 비밀키를 이용하여 $IK \equiv (y_0^{e_0} y_1^{e_1} \cdots y_{i-1}^{e_{i-1}} y_i K_0 K_1 \cdots K_{i-1} g^H)^{rx_v}$ (mod p)를 구한다. $IK = IK_1 \| IK_2$로 나누고 다음과 같이 메시지를 복호한다.

$$m = D_{IK_1}(C)$$

단, $h_{IK_2}(m) = H$인 경우에만 정당한 signcryption으로 받아들인다.

4. 제안 방식의 특징

(1) 위임 환경 재설정

제안 방식은 대리 서명 방식을 다단계로 확장한 대리 서명 방식이다. 이를 전자 환경에 적용하기 위해서는 각 단계마다 서명자의 상황에 맞는 환경을 재설정할 수 있어야 할 것이다. 예를 들어 원 서명자가 위임 서명 생성 기간을 10일이라고 지정해서 대리 서명자에게 위임했다고 하자. 만약 지정된 대리 서명자가 10일 중에 5일동안만 그 역할을 수행할 수 없다면, 다음 대리 서명자에게는 5일간만 위임 능력을 위임시키고, 나머지 5일간은 자신이 원 서명자를 대신하면 된다.

이전의 방식[5]에서는 위임 정보 내용에 대리 서명용 키만 있으므로 이런 기능을 제공할 수가 없다. 본 제안 방식에서는 위임 정보에 유효 기간을 명시할 수 있을 뿐만 아니라, 각 단계마다 대리 서명자의 상황에 맞는 위임 내용을 추가할 수 있으므로, 더욱 융통성있게 응용될 수 있을 것이다.

(2) 타당한 서명자 인증

만약 원 서명자(A)가 지정한 대리 서명자(B)가 다른 사람(C)에게 원 서명자가 전송해 준 정보를 준다고 가정해보자. 이전의 방식[3]에서는 C도 같은 방식으로 타당한 대리 서명키를 생성할 수 있으므로, 검증자는 C가 타당한 서명자인지 아닌지 결정할 수 없을 것이다. 제안 방식에서는 위임 정보에 대리 서명자의

신원을 지정함으로서 검증자는 대리 서명자의 흐름이 타당한 지 아닌지 확인할 수 있을 것이다.

5. 결론

본 논문에서는 위임 정보 대리 서명 방식과 대리인 보호형 proxy-signcryption방식을 확장하였다. 이는 원 서명자가 지정한 대리 서명자가 그 역할을 수행할 수 없을 때 또 다른 사람에게 원 서명자의 서명 생성 능력을 위임할 수 있는 다단계 대리 서명 방식이다.

제안 방식은 기존 방식에 비해 위임 정보에 대리 서명자를 지정할 수 있을 뿐만 아니라 유효 기간을 명시할 수 있어 각 단계마다 대리 서명자의 상황에 맞는 환경을 설정할 수 있으므로 전자 환경 시스템에 더 안전하고 융통성있게 응용될 수 있을 것이다.

[참고문헌]

[1] M.Mambo, K.Usda and E.Okamoto, "Proxy signature : Delegation of the power to sign message", IEICE Transaction on Fundamentals, E79-A(9):1338-1354, 1996

[2] S.J.Kim, S.J.Park and D.H.Won, "Proxy signatures, revisited", Proc. of ICICS'97, LNCS 1334, pp.223-232, 1997

[3] Y.Zheng, "Signcryption and Its Applications in Efficient Public Key Solutions", Proc. of ISW'97, LNCS 1397, pp.291-312, 1998.

[4] C.Gamage, J.Leiwo and Y.Zheng, "An Efficient scheme for Secure Message Transmission using Proxy-Signcryption", Procedding of the Twenty Second Australasian Computer Science Conference, January. 1999.

[5] Shunsuke Araki and Kyoki Imamura, "An application of Mambo-Usuda-Okamoto Proxy Signature Schemes", Proc. of ISITA 2000.

[6] 오수현, 김현주, 원동호, " 이동 통신 환경에서의 전자 상거래에 적용할 수 있는 Proxy-signcryption 방식", 통신정보보호학회논문지 제10권 제2호. 2000. 6.

[7] B.C.Lee, H.S Kim, and K.G Kim, "Secure Mobile Agent using Strong Non-designated Proxy Signature", Proc. of ACISP2001, LNCS, Springer Verlag Vol.2119, pp.474-486, 2001