# 매개자를 이용한 변형된 Schnorr 기반의 대리서명 기법

서승현°, 이상호
이화여자대학교 컴퓨터학과
seosh@ewhain.net°, shlee@ewha.ac.kr

# A Modified Schnorr-based Proxy Signature Scheme By Using a Mediator

Seung-Hyun Seo°, Sang-Ho Lee
Dept. of Computer Science & Engineering, Ewha Womans University

요 약

대리서명은 원서명자가 대리서명자에게 서명 권한을 위임하여 대신 서명하게 하는 변형된 전자서명이다. 대부분의 대리서명 기법들은 위임장에 유효한 위임 기간을 명시함으로써, 대리서명자의 서명 권한을 제한한다. 그러나 누구도 대리서명자가 서명을 생성한 정확한 시간을 모르기 때문에, 정해진 위임 기간 내에 올바로 서명 권한을 수행했는지에 대해서 검증할 방법이 없다. 따라서 위임장에 위임 기간을 표시해 놓는 것만으로는 대리서명자의 서명 권한을 제한할 수 없다. 또한 기존의 대리 서명 기법들의 경우, 대리서명자가 악의적인 공격자와 결탁하여 서명 권한을 남용했을 때에도 원서명자가 대리서명자의 위임권한을 즉시 취소할 수 없는 문제점이 있다. 본 논문에서는 보안 매개자를 이용한 변형된 Schnorr 기반의 대리서명 기법을 제안하였다. 제안한 기법은 원서명자가 원하면 언제든지, 대리서명자의 서명권한을 취소할 수 있게 함으로써 기존의 대리서명 기법들의 취약성을 효율적으로 개선하였다.

## 1. 서 론

1996년, Mambo[1]등에 의해 처음 소개된 대리서명 기법은 위임받은 대리서명자가 원서명자를 대신하여 서명할 수 있는 전자서명 기법을 말하며, 위임의 형태에 따라 전체 위임과 부분 위임, 위임장에 의한 위임으로 분류된다. 이후, 김승주[2]등은 위임장의 내용을 직접 대리서명에 삽입시킴으로써 대리서명자에 의한 서명 권한의 오남용을 방지하는 기법을 제안하였다. 현재까지 대부분의 대리서명 기법은 김승주 등이 제안한 위임장에 의한 부분 위임 대리서명 기법에 초점을 맞추어 연구되어왔고, 유효한 위임기간을 위임장에 명시하는 것으로 대리서명자의 서명권한을 제한할 수 있다고 주장되었다.

그러나 기존의 방식[1,2,3,4]들은 대리서명자가 서명한 정확한 시간을 검증해낼 방법이 없기 때문에, 유효기간이 지난 후에 대리서명자가 서명을 생성하고서도 이전에 서명해놓았던 것이라고 주장할 수 있다. 또한, 기존의 방식들에서는 즉각적인 위임 취소 기능을 제공하지 않기 때문에, 위임기간이 종료되기 전에 대리서명자의 부정행위를 발견했다 하더라도, 원서명자가 대리서명자의 서명권한 위임을 취소할 수 없어서 문제가 되고 있다.

본 논문에서는 변형된 Schnorr 기반의 대리서명기법을 제안하였다. 제안된 기법은 보안 매개자(Security Mediator)[5]를 이용하여 이러한 문제점들을 해결하고, 원서명자가 원하면 즉시 위임권한을 취소할 수 있는 기능을 효율적으로 제공한다. 본 논문의 구성은 다음과 같다. 2장에서 용어 및 보안 요구사항을 기술하고, 3장에서 제안한 대리서명기법을 설명한다. 4장에서는 제안한 대리서명기법의 안전성 및 효율성을 분석하고, 5장에서 결론을 맺는다.

## 2. 용어 정의 및 보안 요구사항

이 장에서는 용어 정의와 대리서명기법들이 만족해야 하는 보안 요구사항[1,3]들을 기술한다.

[용어 정의]

- $A$ : 원서명자
- $B$ : 대리서명자
- $SEM$ : 보안 매개자(Security Mediator)
- $p, q$ : $q|p-1$을 만족하는 암호학적으로 강한 소수
- $g$ : 곱셈군 $Z_p^*$의 생성자
- $H(.)$: 암호학적 해쉬함수

[보안 요구사항]

① 검증 가능성: 대리서명으로부터 검증자는 권한위임에 대한 원서명자의 동의를 확인할 수 있어야 한다.
② 강한 위조 방지: 지명된 대리인만이 유효한 대리 서명을 생성할 수 있어야 한다.
③ 강한 확인: 대리서명으로부터 대리인의 신분을 확인할 수 있어야 한다.
④ 부인 방지: 한번 유효한 대리서명이 생성되면 대리인은 자신의 대리서명 생성에 대한 사실을 부인할 수 없어야 한다.
⑤ 오남용 방지: 대리인은 자신에게 위임된 권한 내에서 대리서명을 생성해야 한다.

### 3. 제안한 대리서명기법

이 장에서는 매개자를 이용한 변형된 Schnorr 기반의 대리서명기법을 제안한다. 제안한 대리서명기법은 위임장을 검증하고, 대리서명 토큰을 발행하는 SEM(SEcurity Mediator)를 사용한다. 기존의 대리서명기법들과 달리, 원서명자가 SEM과 대리서명자에게 위임키를 나누어주고, SEM과 대리서명자가 메시지에 대한 대리서명을 함께 생성해나가는 형태이다. 즉, 대리서명자 $B$가 메시지 $m$에 대리서명을 하려면, 반드시 SEM으로부터 위임권한 검증을 받고, 대리서명토큰을 받아야 한다.

SEM은 대리서명자가 대리서명을 하기 위해서 대리서명 토큰을 요청할 경우, 대리서명자의 위임기간이 유효한지 아닌지를 판단하고, 대리서명자의 ID가 위임권한취소 리스트에 있는지를 확인해서 올바른 경우에만 토큰을 발행한다. 이 토큰이 없으면, 대리서명자가 어떤 메시지에도 서명할 수 없기 때문에, 위임기간이 종료된 후에 대리서명 권한을 남용할 수 없다. 또한, 원서명자가 위임기간 종료이전에 대리서명자의 서명권한을 취소하고 싶을 때에, SEM에게 대리서명자의 토큰발행을 중지하라고 요청하면 되기 때문에, 제안된 기법은 즉시 위임권한을 취소할 수 있는 기능을 효율적으로 제공한다.

(1) 위임키 생성단계

원서명자 $A$는 임의의 난수 $k_B, k_S \in_R Z_q$를 선택하고, $k_A = k_B + k_S$, $r_A = g^{k_A} \bmod p$를 계산한다. 자신의 ID와 대리서명자 $B$의 ID, $SEM$의 ID, 위임기간 및 위임권한에 대한 정보를 조합하여 위임장 $m_W$를 생성한다. 그런 후에 $B$와 $SEM$를 위한 부분적인 위임키, $\sigma_B = k_B + x_A \cdot h(m_W \mid r_A) \bmod q$, $\sigma_S = k_S + x_A \cdot h(m_W \mid r_A) \bmod q$를 생성한다.

(2) 위임키 전송단계

$A$는 $(m_W, r_A, \sigma_B)$를 $B$에게, $(m_W, r_A, \sigma_S)$를 $SEM$에게 각각 전송한다.

(3) 위임키 검증 및 대리 서명키로의 변경단계

위임키들의 유효성을 검증하기 위해서, $B$는 $R_B = g^{\sigma_B} \bmod p$를 계산하여 $(m_W, R_B)$을 $SEM$에게 전송하고, $SEM$은 $R_S = g^{\sigma_S} \bmod p$를 계산하여 $(m_W, R_S)$를 $B$에게 전송한다. $B$와 $SEM$은 각각 다음을 계산하여, $R_B \cdot R_S = r_A \cdot y_A^{2h(m_W \mid r_A)} \bmod p$ 만족되는지에 대해서 검증한다. 유효성이 올바르게 검증되고 나면, $B$는 $\sigma_{P_B} = \sigma_B + x_B h(m_W \mid r_A) \bmod q$를 계산하고, $SEM$은 $\sigma_{P_S} = \sigma_S + x_S h(m_W \mid r_A) \bmod q$을 계산하여 각자의 위임키를 대리 서명키로 변경한다.

(4) 위임권한 검증 및 대리서명 토큰발행 단계

$B$는 난수 $l_B \in_R Z_q$를 선택하고, $L_B = g^{l_B} \bmod p$를 계산한 후에, 메시지 $m$에 대한 대리서명 토큰 요청 메시지 $(m_W, m, r_A, R_B, L_B)$을 $SEM$에게 전송한다. $SEM$은 아래와 같은 과정을 거쳐 $B$의 위임권한의 유효성을 검증한다.

① 위임장 $m_W$에 명기된 위임기간이 유효한지를 검증한다.

② $r_A$가 $SEM$에 의해 유지되고 있는 위임권한취소목록에 있는지를 확인한다. 만약, 취소목록에 있다면 $r_A$를 가지고 있는 대리서명자 $B$의 위임권한이 취소된 것이므로 토큰발행을 하지 않는다.

유효성이 검증되면, $SEM$은 난수 $l_S \in_R Z_q$를 선택하고, $L_S = g^{l_S} \bmod p$, $L_A = g^{l_S} \cdot g^{l_B} \bmod p$, $S_S = l_S + \sigma_{P_S} h(m \mid L_A) \bmod q$를 계산하여, 대리서명토큰 $(L_A, S_S, L_S)$을 $B$에게 전송한다.

(5) 대리서명 생성단계

$B$는 $g^{S_S} = L_S \cdot (R_S \cdot y_S^{h(m_W \mid r_A)})^{h(m \mid L_A)} \bmod p$임을 계산하여, $SEM$에게 받은 대리서명토큰 $(L_A, S_S, L_S)$을 검증한다. 토큰 검증이 성공하면, 아래와 같이 $m$에 대한 대리서명 $S$을 생성하고, 검증자에게 대리서명 메시지 $(m, m_W, r_A, S, L_A)$를 전송한다.

$$S = S_S + l_B + \sigma_{P_B} h(m \mid L_A) \bmod q$$
$$= l_S + l_B + (\sigma_{P_B} + \sigma_{P_S}) \cdot h(m \mid L_A) \bmod q$$

(6) 대리서명 검증단계

검증자는 $m$에 대한 대리서명 $S$을 검증하기 위해서, 다음의 계산식이 올바른지를 확인한다.

$$g^S = L_A \cdot (r_A \cdot (y_A^2 y_B y_S)^{h(m_W \mid r_A)})^{h(m \mid L_A)} \bmod p$$
$$= g^{l_S + l_B} \cdot (g^{k_A} \cdot (g^{2x_A} \cdot g^{x_B} \cdot g^{x_S})^{h(m_W \mid r_A)})^{h(m \mid L_A)} \bmod p$$
$$= g^{l_S + l_B + (k_A + (2x_A + x_S + s_B) h(m_W \mid r_A)) h(m \mid g^{l_S + l_B})} \bmod p$$

### 4. 안전성 및 효율성 분석

이 장에서는 제안한 대리서명 기법의 안전성을 2장에서 기술한 보안요구사항에 따라 분석하고, 기존의 대리서명기법들과의 효율성을 비교분석한다.

#### 4.1 안전성 분석

(1) 검증 가능성: 제안한 대리서명 기법에서 대리서명 메시지는 $(m, m_W, r_A, S, L_A)$로 구성된다. 위임장 $m_W$을 통해서, 검증자는 원서명자, 대리서명자, $SEM$의 신원을 확인할 수 있다. 또한 대리서명 검증단계에서 원서명자의 비밀키가 대리서명메세지에 포함되어있음을 확인함으로써, 원서명자의 동의를 확신할 수 있다.

(2) 강한 위조 방지: 이산대수문제의 어려움에 근거하여, 대리서명자 $B$의 비밀키를 알아낼 수 없기 때문에, 원서명자의 위임키를 도청했다하더라도, $B$의 대리서명키를 만들어낼 수 없다. 또한, 이산대수문제의 어려움에 근거하여 $SEM$의 비밀키도 알아낼 수 없기 때문에, 악의적인 대리서명자나 원서명자라 하더라도, $SEM$이 생성한 대리서명토큰을 위조할 수 없다. 따라서, 정당하게 위임받은 $B$만이 대리서명을 생성할 수 있으며, 위임기간이 지났을 때에는 $SEM$으로부터 토큰을 받지 못하기 때문에, 더 이상 대리서명을 생성할 수 없다.

(3) 강한 확인: 대리서명자의 식별정보 $B$가 공개키 형태로 위임장에 명확히 포함되어있어, 누구든지 대리서명 메시지를 생성한 대리서명자를 확인할 수 있다.

(4) 부인 방지: 대리서명자는 원서명자로부터 받은 위임키에 자신의 비밀키 정보를 포함하여 대리서명을 생성하기 때문에, 유효한 대리서명 메시지가 일단 생성되면 부인할 수 없다.

(5) 오남용 방지: 비밀키 $x_B$를 알고 있는 대리서명자 $B$만이 대리서명을 생성할 수 있다. 따라서, 다른 용도로 대리서명을 남용한다면 그것은 $B$가 한 일임이 증명되기 때문에, 대리서명자의 오남용은 불가능하다.

### 4.2 효율성 분석

제안한 대리서명기법의 효율성을 분석하기 위해서, 암호학적 해쉬함수의 출력 길이를 160bits로 $p$의 길이를 1024 bits로, $q$의 길이를 160bits로 가정한다. Kaliski에 의해 사용된 방법을 이용해서 계산량을 측정하여, 기존의 위임취소기능을 갖는 대리서명기법들과 효율성을 비교한 결과는 아래의 표 1과 같다.

표1 위임취소기능을 갖는 대리서명기법들의 효율성비교

| | Lu[6] | Das[7] | 제안한 기법 |
|---|---|---|---|
| 대리서명생성 계산량 | 12807 | 10240 | 2007.1 |
| 대리서명검증 계산량 | 6404 | 3840 | 604.02 |
| 전체 계산량 | 19211 | 14080 | 2611.12 |

표 1에서 대리서명생성 계산량은 3장에서 제안한 기법의 (1)단계부터 (5)단계를 수행하는데 필요한 계산량을 의미하며, 대리서명검증 계산량은 (6)단계를 수행하는데 필요한 계산량을 의미한다. 비교된 기존 기법들의 계산량도 제안한 기법에서의 각 단계와 유사한 단계들의 계산량을 측정한 것이다. 기존의 위임취소기능을 갖는 대리서명 기법들은 인증서버를 이용하여, 대리서명자가 대리서명을 수행하려고 할 때마다 타임스탬프를 발행하고, 검증자는 대리서명자의 서명 뿐 아니라 인증서버의 타임스탬프 서명까지도 검증해야하기 때문에 비효율적이다. 제안한 기법은 기본 요구사항을 만족하면서 동시에, 기존의 기법들과 달리 대리서명자의 계산량 뿐 아니라 검증자의 계산량도 크게 줄였다.

## 5. 결론

본 논문에서는 보안매개자를 이용하여 즉각적인 위임취소기능을 제공하는 대리서명기법을 제안하였다. 제안한 서명기법은 기존의 대리서명기법들과 달리, 대리서명을 수행할 때 보안매개자는 대리서명자의 위임기간을 검증한 후 대리서명토큰을 발행하고, 대리서명자는 원서명자의 위임키와 함께 대리서명토큰을 이용해서 대리서명을 수행하게 하였다. 이로써, 유효한 위임기간 내에만 대리서명자가 대리서명을 수행할 수 있음이 검증된다. 또한, 정해진 위임기간 내에 대리서명자의 위임권한 남용이 발견 되었거나 원서명자가 대리서명권한 취소를 원하는 경우에 보안매개자로부터 토큰 발행 중지를 요청함으로써 효율적으로 즉각적인 위임권한취소를 할 수 있다.

## 6. 참고 문헌

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

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

[3] B.Lee, H.Kim and K.Kim, "Strong proxy signature and its applications," In Proc. of SCIS'2001, pp.603~608, 2001.

[4] H.-M.Sun, "Design of time-stamped proxy signatures with traceable receivers," IEE Proceedings of Comput.Digit.Tech., Vol.147, No.6, pp.462~466, 2000.

[5] D.Boneh, X.Ding, G.Tsudik and C.M.Wong, "A method for fast revocation of public key certificates and security capabilities," In 10th USENIX Security Symposium, pp.297~308, 2001.

[6] E.J.-L.Lu, M.-S.Hwang and C.-J.Huang, "A new proxy signature scheme with revocation," Applied Mathematics and Computation, Elsevier, in press, 2004.

[7] M.L.Das, A.Saxena and V.P.Gulati, "An efficient proxy signature scheme with revocation," International Journal Informatica, Vol.15, No.4, pp.455~464, 2004.