재귀 대리 서명

김영설° 장직현
서강대학교 컴퓨터학과
{yskim°, jchang}@alglab.sogang.ac.kr

Self Proxy Signature Scheme

Young-seol Kim° Jik-hyun Chang
Dept. of Computer Science, Sogang University

요 약

대리서명은 원서명자의 서명 권한을 대리 서명자에게 위임하여 원서명자의 행위에 대해 서명할 수 있게 한 서명 방식이다. 이것은 일상생활에서 도장을 다른 사람에게 위임하는 것을 전자적으로 구현한 것이라 할 수 있다. 본 논문에서는 자기가 자신에게 서명 권한을 위임하는 방법을 통해 임시로 사용 할 수 있는 서명 키 쌍을 만들어내는 방법을 제안한다. 이 방법을 통해 원 서명 쌍을 보호할 수 있으며 동시에 여러 쌍의 키들을 사용할 수 있으므로 작업들과 키 쌍들을 구분하여 관리할 수 있다. 또한 임시 서명 키 쌍의 폐기는 원 서명 키 쌍의 폐기보다 쉽기 때문에 제안하는 재귀 대리 서명은 실제적이라 할 수 있다.

1. 서 론

대리서명은 1996년 Mambo, Usuda, Okamoto [1], [2]에 의해 처음으로 제안되었다. 대리서명 방식에서는 원서명자가 자신의 권한을 대리서명자에게 위임할 수 있으며 대리서명자는 위임받은 권한으로 서명할 수 있다. 검증자는 대리서명의 정확성을 검증 할 수 있으며 원서명자의 동의가 있었음을 확신 할 수 있다. 또한 일반적인 서명과 대리 서명을 구분 할 수 있다. 이것은 일상생활에서 도장을 다른 사람에게 위임하는 것을 전자적으로 구현한 것이라 할 수 있다. 대리서명 방식은 전자상거래, 이동 에이전트, 분산시스템 등 많은 응용 분야가 있다.

예를 들어 어떤 회사의 사장이 휴가를 가기 전에 비서에게 자신의 서명 권한을 위임할 수 있다. 비서는 결재되어야 하는 서류에 사장을 대신하여 서명을 할 수 있으며 서명을 검증하는 사람은 그 서명이 비서가 한 사장의 대리 서명이며 사장의 동의가 있었음을 확신 할 수 있다.

대리서명은 보통 다음과 같이 이루어진다. 원서명자는 대리서명자에게 특별한 메시지와 연결된 서명을 전달한다. 대리서명자는 이 정보를 이용하여 대리서명 비밀키를 만들어낸다. 대리서명자는 이 비밀키를 이용하여 특정 메시지에 일반적인 서명 알고리즘으로 서명할 수 있다. 이렇게 만들어진 메시지와 서명이 검증자에게 전달되면 검증자는 공개되어 있는 정보를 이용하여 대리서명 공개키를 복원하고 그것을 이용하여 대리서명을 검증할 수 있다. 역시 이 때에도 일반적인 서명 알고리즘의 검증 절차를 수행한다.

Mambo, Usuda, Okamoto [1], [2]의 대리 서명 이후 많은 대리 서명 방식이 연구되었으며 은닉 대리 서명, 검증자 지정 대리 서명 등의 특별한 대리 서명방식들도 연구되었다 [3], [4], [5], [6].

일상 생활에서 한 사람은 여러 개의 다른 도장들을 동시에 사용한다. 특별한 등록 절차를 거치고 중요한 일에만 사용하는 인감도장이 있고 인감도장이 아닌 일반 도장들도 여러 개를 사용할 수 있다. 어떤 특별한 작업에만 사용하는 도장을 한정할 수 있으며 인감도장의 사용을 남발하지 않음으로써 인감도장의 안전성도 보호할 수 있다.

본 논문에서는 일반적인 대리 서명을 이용하여 전자적인 임시 서명 키 쌍을 생성하는 방법을 제안한다. 이것은 자기가 자기 자신에게 재귀적으로 서명 권한을 위임하는 것으로 구현된다. 이 재귀 대리 서명을 통해 한 사용자는 자신의 원 서명 키 쌍으로부터 여러 개의 임시 서명 키 쌍을 생성하여 사용할 수 있으며 사용 후에는 쉽게 폐기할 수 있다.

2. 가정, 정의와 시스템 변수

2.1 가정

우리의 재귀 대리 서명은 안전성의 증명을 위해 다음

과 같은 알려져 있는 계산적으로 어려운 문제를 이용한다.

가정 1: 이산로그(Discrete Logarithm) 가정.
$G_q = < g >$를 위수가 q인 생성원 g에 의해 생성되는 순환적 곱셈군이라 하자. 그러면 입력 $(g, g^x) \in G_q^2$ $(x \in_R Z_q)$에 대해 무시할 수 없는 확률로 x를 계산하는 확률적 다항식 시간 알고리즘이 존재하지 않는다.

2.2 정의

정의 1. 재귀 대리 서명은 다음과 같은 단계를 거친다.

-준비 단계: 서명자의 비밀키, 공개키 쌍을 결정한다. 이 키들은 일반적인 전자서명 방식에서 사용되는 값이다.

-위임 단계: 서명자는 재귀적인 키 생성 단계를 통해 재귀 대리 서명 비밀키와 공개키 (x_p, y_p)를 만들어낸다. x_p는 오직 서명자만이 알아야 하며 y_p는 공개되거나 공개적으로 복원할 수 있어야 한다.

-재귀 대리 서명 생성 단계: 서명자는 메시지 m에 재귀 대리 서명 비밀키 x_p로 서명을 한 후 생성된 서명 σ를 메시지 m과 추가정보와 함께 검증자에게 전달한다.

-재귀 대리 서명 검증 단계: 검증자는 서명자로부터 받은 메시지 m과 σ를 정해진 검증식으로 검증한다.

정의 2. 안전한 재귀 대리 서명은 다음과 같은 요구사항들을 만족해야 한다.

-구분가능성: 재귀 대리 서명은 일반적인 서명과 구분 가능 해야 한다.

-부인방지: 서명자는 추후에 자신의 서명 행위를 부인할 수 없어야한다.

-검증가능성: 재귀 대리 서명은 누구나 검증할 수 있어야한다.

-위조불가능성: 오직 정당한 서명자만이 재귀 대리 서명을 생성할 수 있어야한다.

2.3 표기법

이후 제안하는 서명 방법의 편리한 표현을 위해 다음과 같은 기호들을 정의한다.

-p, q: 두 개의 큰 소수, $q \mid p-1$

-g: 위수가 q인 Z_p^*의 생성자

-x_u, y_u: 참가자 U의 비밀키와 공개키, $y_u = g^{x_u}$

-H(): 공개된 암호학적 해쉬 함수

-||: 문자열 결합

-m_w: 서명자의 신원 식별자, 위임기간, 서명 가능한 메시지 m에 대한 설명 등이 기록된 위임증서

3. 이전 연구

최초로 제안된 대리 서명은 Mambo, Usuda, Okamoto의 서명 스킴이다 [1], [2]. 이 대리 서명 스킴은 부분 위임 방식을 취하고 있으며 이산 대수 문제에 기반을 두고 있다.

시스템 변수로서 소수 p, p-1의 소인수 q, 그리고 위수가 q인 $g \in_R Z_p^*$ 가 있다. 원 서명자는 개인키 $x \in_R Z_q$와 공개키 $y = g^x \bmod p$ 를 가지고 있다. 각 단계의 세부 내용은 다음과 같다.

① 비밀 값의 생성

원 서명자는 랜덤 수 $k \in_R Z_q$ 를 선택하여 $r = q^k \bmod p$를 계산한다. 또한 $s = x + kr \bmod q$를 계산한다.

② 비밀 값의 전송

원 서명자는 안전한 통로를 통해 대리 서명자에게 (r, s)를 전달한다.

③ 비밀 값의 검증

대리 서명자는 원 서명자에게 받은 (r, s)로 다음 식을 확인한다.

$$g^s = yr^r \bmod p$$

만약 위의 식이 만족한다면 대리 서명자는 그것을 정당한 대리 서명 키로 받아들인다. 위 식이 만족하지 않는다면 프로토콜은 중지된다.

④ 대리 서명문 생성

대리 서명자는 서명문 원 서명자의 행위에 관한 메시지 m에 대해 s를 대리 서명 개인키로 삼아 일반적인 서명 방식으로 서명을 하여 서명 S_p를 생성한다. 그러면 검증자에게 전달할 대리 서명문은 (S_p, r)이 된다.

⑤ 대리 서명문의 검증

대리 서명자가 서명한 대리 서명문 (S_p, r)을 받으면 검증자는 먼저 $y' = yr^r \pmod p$로 y를 대치한다. 그 후 대리 서명자가 진행한 일반적인 서명의 검증 단계를 진행한다.

4. 재귀 대리 서명
(Self Proxy Signature Scheme)

우리는 이 장에서 일반적인 대리 서명을 이용하여 임시 서명 키 쌍을 만들어내는 재귀 대리 서명을 새롭게 제안한다. 이것은 자기가 자기 자신에게 서명권한을 재귀적으로 위임하는 방식으로 구현되었다. 서명자 A는 자신의 원 서명 키 쌍 (x_a, y_a)를 가지고 있다고 가정한다.

4.1 재귀 대리 서명 키 쌍 생성 단계

서명자 A는 자신의 원 서명 키 쌍 (x_a, y_a)을 이용해 다음과 같이 임시 서명 키 쌍을 만들어 낸다.

① 서명자 A는 임의의 값 $k, x_t \in_R Z_q^*$을 선택하고 $r = g^k \bmod p$와 $y_t = g^{x_t} \bmod p$를 계산한다.

② 그 후 서명자 A는 $x_p = k + (x_a + x_t)H(m_w) \bmod q$ 를 계산하여 자신의 임시 서명 비밀 키로 삼는다. 대응하는 임시 서명 공개 키는 $y_p = g^{x_p} \bmod p$ 가 된다.

③ 서명자 A는 y_t를 공개한다.

4.2 재귀 대리 서명 생성 단계

서명자 A는 메시지 m에 대해 재귀 대리 서명을 생성하기 위해 다음과 같은 절차를 수행한다.

① 서명자 A는 임의의 값 $k' \in_R Z_q^*$를 선택하고

$$r' = g^{k'} \mod p, \qquad (1)$$

$$s' = k' + x_p H(m) \mod q \qquad (2)$$

를 계산한다.

② 서명자 A 는 (m, (r′, s′), r, m_w)를 검증자에게 전달한다.

4.3 재귀 대리 서명 검증 단계

검증자 B는 먼저 공개된 m_w의 정보로 재귀 대리 서명의 서명자 신원과 위임 기간 메시지에 대한 제한 등을 확인한다. 정당한 서명자로 확인된다면 검증자는 다음과 같은 절차를 진행 한다.

① 먼저 검증자 B는 대리서명 공개키 y_p를 다음과 같이 복원한다.

$$y_p = r(y_a y_t)^{H(m_w)} \mod p$$

② 그 후 검증자 B는 다음과 같은 식을 검사하여 식이 만족한다면 (r′, s′)를 메시지 m에 대한 정당한 재귀 대리 서명으로 받아들인다.

$$g^{s'} = r' y_p^{H(m)} \mod p \qquad (3)$$

위임과 서명의 모든 단계가 올바르다면 위의 검증식은 다음과 같은 이유로 성립한다.

$$\begin{aligned} g^{s'} &= g^{(k' + x_p H(m))} \bmod p \\ &= g^{k'} (g^{x_p})^{H(m)} \bmod p \\ &= r' y_p^{H(m)} \bmod p \end{aligned}$$

5. 안전성 분석

5.1 위조 불가능성에 대한 분석

우리 서명 방식의 안전성은 가정 1의 이산 대수 문제에 기반을 둔다. 안전성 분석의 세부 내용은 다음과 같다.

정당하지 않은 공격자 C가 재귀 대리 서명을 위조하려 한다고 가정하자. 공격자는 두 가지 방법으로 공격할 수 있다. 첫 번째는 재귀 대리 서명 비밀 키 x_p를 위조하는 것이고 두 번째는 정당한 서명으로 검증될 수 있는 재귀 대리 서명을 키 없이 위조하는 것이다.

첫 번째 공격 방법에서 공격자 C가 x_p를 계산하기 위해서는 공개된 대리 서명 공개 키 y_p에서 x_p를 계산하거나 식 (1), (2) 그리고 서명자 A와 검증자 B 사이에서 전달되는 정보 (m, (r′, s′), r, m_w)를 통해 x_p를 계산해야 한다. 그런데 이 두 방법 모두 x_p를 계산하기 위해서는 이산 대수 문제를 해결해야 한다. 이것은 가정 1에 따라 계산적으로 매우 어렵다. 따라서 공격자 C가 x_p를 계산해 내는 것은 사실상 불가능하다고 할 수 있다.

두 번째 공격 방법에서 공격자 C는 재귀 대리 서명 비밀키 x_p 없이 식 (3)을 만족시키는 값 (r′, s′)를 위조해야 한다. 식 (3)에서 y_p와 m, p는 사실상 공개되어 있는 값이므로 미지수는 (r′, s′)이다. 그런데 s′가 지수승 부분에 위치하고 있기 때문에 이 방법으로도 역시 이산 대수 문제를 해결해야 한다. 역시 가정 1에 따라 이것도 계산적으로 매우 어려운 문제이다. 따라서 두 번째 공격 방법도 사실상 불가능하다고 할 수 있다.

최종적으로 두 가지 방법 모두 사실상 불가능하므로 정당하지 않은 공격자 C가 재귀 대리 서명을 위조하는 것은 계산적으로 매우 어렵다고 할 수 있다. 따라서 제안하는 재귀 대리 서명은 위조 불가능성을 만족시킨다.

5.2 부인 방지에 대한 분석

정당한 서명자 A가 재귀 대리 서명을 한 후 추후에 자신의 서명이 아니라고 부인하는 경우를 고려해보자. 검증자 B는 공개되어 있는 y_t와 서명자 A의 원 공개키 y_a 그리고 위임증서 m_w를 사용하여 재귀 대리 서명 공개키 y_p를 복원한다. 먼저 검증자 B는 위임증서 m_w에서 서명자의 신원을 확인할 수 있다. 또한 복원시 서명자 A의 원 공개키 y_a를 사용하기 때문에 정당한 서명이라면 반드시 검증이 되며 정당하게 검증되는 서명은 서명자 A가 한 것임을 확신 할 수 있다. 따라서 서명자 A는 자신의 정당한 서명에 대해 추후 부인할 수 없다. 따라서 제안하는 재귀 대리 서명은 부인방지 성질을 만족시킨다.

5.3 구분가능성에 대한 분석

정당한 재귀 대리 서명 (m, (r′, s′), r, m_w)을 검증하기 위해서 검증자는 재귀 대리 서명 공개 키 y_p를 복원하는 과정을 거친다. 위 과정을 거침으로 검증자는 위 서명이 일반적인 서명이 아니라 재귀 대리 서명임을 확인할 수 있다. 또한 위 재귀 대리 서명문에는 위임증서 m_w과 추가 정보 r이 포함되어 있기 때문에 검증자는 일반적인 서명과는 형태가 다름을 확인할 수 있다. 따라서 제안하는 재귀 대리 서명은 구분가능성을 만족시킨다.

5.4 검증가능성

정당한 재귀 대리 서명 (m, (r′, s′), r, m_w)을 검증하려는 누구나 공개되어 있는 정보 r, y_a, y_t, m_w를 통해 y_p를 복원할 수 있으며 정해진 검증식에 따라 서명 (r′, s′)를 검증할 수 있다. 따라서 제안하는 재귀 대리 서명은 검증가능성 성질을 만족시킨다.

6. 결 론

본 논문에서 우리는 재귀 대리 서명을 제안하였다. 재귀 대리 서명은 자기가 자신에게 서명 권한을 위임하는 형태로 되어 있으며 일반적인 대리 서명을 변형하여 구현할 수 있다. 재귀 대리 서명으로 한 사용자는 여러 쌍의 임시 서명 키 쌍들을 병행하여 사용할 수 있다. 또한 하나의 작업에 하나의 임시 서명 키 쌍을 한정하여 사용할 수 있으며 사용이 끝난 키 쌍은 원 서명 키 쌍보다 쉽게 폐기할 수 있다.

참 고 문 헌

[1] M. Mambo, K. Usuda and E. Okamoto. "Proxy Signatures: Delegation of the Power to Sign Message", IEICE Trans. Fundamentals, Vol. E79 A, No. 9, 1996

[2] M. Mambo, K. Usuda, E. Okamoto. Proxy signatures for delegating signing operation. In: 3rd ACM Conference on Computer and Communications Security(CCS'96), pp. 48-57. New York: ACM Press, 1996

[3] G. Wang. Designated-Verifier Proxy Signature Schemes. In: Security and Privacy in the Age of Ubiquitous Computing (IFIP/SEC 2005), pp. 409-423. Springer, 2005.

[4] Z. Tan, Z. Liu, C. Tang. Digital Proxy Blind Signature Schemes Based on DLP and ECDLP. In: MM Research Preprints, No. 21, MMRC, AMMS, Academia Sinica, Beijing, 2002, pp. 212-217

[5] S. Lal, A. K. Awasthi. Proxy Blind Signature Scheme. In: Journal of Information Science and Engineering. Cryptology ePrint Archive, Report 2003/072. Available at http://eprint.iacr.org/.

[6] Guilin Wang, Feng Bao, Jianying Zhou, and Robert H. Deng. Security Analysis of Some Proxy Signatures. In: Information Security and Cryptology - ICISC 2003, LNCS 2971, pp. 305-319. Springer-Verlag, 2004.