논문 99-24-3A-13 한국통신학회논문지 '99-3 Vol.24 No.3A

보증 부분 위임에 의한 대리 서명에 관한 연구

김 승 주*, 박 상 준**, 양 형 규***, 원 동 호*

A Study on the Proxy Signatures for Partial Delegation with Warrant

Seungjoo Kim*, Sangjoon Park**, Hyungkyu Yang***, Dongho Won* *Regular Members*

요 약

Mambo, Usuda, Okamoto 등에 의하여 최초로 제안된 대리 서명방식은 원서명자가 지정한 대리 서명자가 원서명자를 대신하여 서명하는 것을 허용한다. 본 논문에서는 기존의 대리 서명방식에서 발생하는 대리 서명자의 유효 위임 서명기간과 위임을 한 원서명자의 탈법을 방지할 수 있는 새로운 보증 부분 위임에 의한 대리 서명방식을 제안하였다. 제안한 방식은 유효기간의 정보가 포함된 보증서를 해쉬 함수를 이용하여 대리 서명자에게 위임 정보로 제공하고 다시 대리 서명자는 원서명자로부터 받은 위임 정보에 자신의 정보를 부가하여 대리 서명 생성 정보로 사용토록 하였다.

ABSTRACT

Proxy signatures, introduced by Mambo, Usuda and Okamoto allow a designated person to sign on behalf of an original signer. This paper first presents a new type of digital proxy signatures called partial delegation with warrant. Proxy signatures for partial delegation with warrant combine the benefit of Mambo's partial delegation and Neuman's delegation by warrant. Moreover, we also propose straightforward and concrete proxy signature schemes satisfying our conditions.

I. 서 론

암호 시스템의 기능은 정보의 보호기능과 인증기능으로 나눌 수 있다. 정보보호기능은 정보가 노출된다고 해도 키를 알지 못하는 한 정보의 정확한 의미를 파악하지 못하게 하여 정보를 보호하는 것이고, 인증기능은 정보의 전달상태 또는 통신시의 송·수신자간의 상대방 확인기능을 갖춰 분쟁을 해결할 수 있는 기능을 제공하는 기능이다. 인증기능은 자신이 보낸 정보가 전송도중 변경되지 않고 상대방에게 정확하게 전달되었는가를 확신하는 메시지 인증기능과 정보의 생성, 보관, 처리 등의 행위에 관여한 사용자가 맞는가를 확인하는 사용자 인증기능으로 구분할 수 있다. 일상생활에서 우리가 사용하는 서명이나 인감과 같은 효과를 전자적으로 수행하는 디지털 서명(digital signatures)은 이러한 사용자 인증과 메시지 인증기능을 모두 만족하여야 한다.

일반적으로 서명이나 인감은 개인의 필요성에 의하여 언제든지 발급될 수 있고, 이 서명 또는 인감을 수신한 사람 역시 수신된 서명이나 인감의 정당성을 쉽게 확인할 수 있으며, 서명의 생성자나 인감의 소유자 이외에는 이 서명이나 인감을 발급할 수 없어야 한다. 따라서 디지털 서명에서도 서명자만이 서명을 생성할 수 있는 유일성, 위조가 불가능한 위조 불가능성, 서명의 진위를 쉽게 확인할 수 있는 진위의 확인의 용이성, 자신의 서명을 위조된 것이라고 거부하는 것이 불가능한 거부의 불가능성 등

* 한국정보보호센서 선임연구원(skim@kisa.or.kr)
** 성균관대학교 전기·전자 및 컴퓨터공학부
*** 강남대학교
논문번호 : 98251-0619, 접수일자 : 1998년 6월 19일

의 요구 사항을 만족하여야 한다.

이러한 디지털 서명은 사용목적에 따라 기능이 다른 특수한 서명들이 제안되었다. 본 논문에서는 M. Mambo와 E. Okamoto가 제안한 부분 위임(partial delegation)에 의한 대리 서명방식(proxy signatures)에서 위임기간의 불확실성에 따른 대리 서명의 유효기간과 위임을 한 원서명자(original signer)가 대리 서명자(proxy signer)를 가장한 대리 서명을 수행하였을 때에 발생할 수 있는 문제점을 해결할 수 있는 방식을 제안하였다.

대리 서명방식은 원서명자가 자신의 부재중에 자신을 대신해서 서명을 할 수 있는 대리 서명자를 지정하여 대신 서명토록 하는 서명방식이다. 따라서 대리 서명자로 지정 받은 자가 서명한 서명으로부터 원서명자의 대리서명기간등의 지정한 내용을 서명 검증자가 확인할 수 있어야 한다. 또한 대리 서명자임을 인정한다는 내용 등을 확인할 수 있어야 한다.

제안한 방식에서는 부분 위임방식에 유효기간 등의 정보가 포함된 보증서(warrant)를 해쉬 함수(hash function)를 이용하여 대리 서명정보에 포함시킴으로써, 대리 서명방식에 이 사실을 확인시킬 수 있는 방법을 구성하였다.

Ⅱ. 디지털 서명

2.1 디지털 서명의 개요

디지털 서명은 전자문서, 컴퓨터 파일, 혹은 일반 정보데이터에 대한 서명을 실행하는 알고리즘으로 이진 비트 열로 표시되며 기존의 종이문서의 수기 서명이나 인증에 해당된다. 그러나 기존의 서명은 사용자에 따라서 항상 일정하며 도용이나 위조 가능성이 크다. 디지털 서명은 동일한 서명자라도 각 문서에 따라 생성되는 서명의 모양이 달라지며 서명의 변경이나 위조도 용이하게 검출할 수 있다.

디지털 서명은 서명자의 인증과 문서의 변경여부를 확인하는 메시지 인증으로 구성된다. 즉, 디지털 서명의 참여자를 확인할 수 있고, 문서의 변경여부를 확인할 수 있으며, 통신망 상에서의 통신의 발신처 확인과 서명자의 서명 부인을 막을 수 있는 방식이다.

디지털 서명은 서명에 참여하는 참가자에 따라 직접 서명방식과 간접 서명방식으로 나눈다. 직접 서명방식은 서명자와 수신자간에 직접 문서와 서명을 전달하는 방법이며, 간접 서명방식은 서명자와 검증자 사이에 신뢰할 수 있는 제삼의 중재자를 개입시켜 서명의 정당성을 확인하는 방법이다. 이 두 방식은 사용하는 암호화 알고리즘에 따라 결정된다. 일반적으로 중재자를 갖는 간접 서명방식은 관용 암호방식을 이용하고, 직접 서명방식은 공개키 암호방식을 이용한다.

직접 서명방식은 제삼자를 필요로 하지 않으므로 서명 시스템 구성이 보다 간편하다. 공개키 암호방식을 이용하는 디지털 서명은 비밀 서명정보에 대한 공개 검증 정보를 분리하여 서명자는 비밀 서명정보로 문서의 서명을 생성하고, 검증자는 공개 검증정보로 서명을 확인한다. Diffie와 Hellman이 1976년 공개키 암호방식에 기반한 디지털 서명의 개념을 소개한 이후 여러 방식들이 제안되었다[1]. 그 대표적인 디지털 서명방식으로는 RSA방식, ElGamal방식, Schnorr방식, Nyberg-Rueppel 서명방식, DSS, GOST 등이 제안되었으며 국내에서도 KCDSA(Korean Certificate-based Digital Signature Algorithm)라는 디지털 서명방식이 한국표준으로 검토되고 있다[2,3,4,5,6,7].

디지털 서명의 사용목적에 따라 특수한 서명방식들(special digital signatures)이 제안되었다. 대표적인 특수 서명방식으로는 과다한 서명의 검증기능을 축소함으로써 서명자의 프라이버시(privacy)를 보호할 수 있는 부인방지 서명방식(undeniable digital signatures), 문서의 내용을 노출시키지 않고 서명할 수 있는 은닉 서명방식(blind Signatures), 서명문서를 수신한 자만이 서명의 진위를 검증할 수 있는 수신자 지정 서명방식(nominative signatures), 다수의 서명자가 참여하는 다중서명(multisignatures) 등, 많은 특수목적 서명들이 발표되었다[8,9,10,11].

특히 M. Mambo와 E. Okamoto는 최근 대리 서명방식이라고 하는 특수 서명방식을 제안하였다[12,13,14,15,16]. 이 서명방식은 제삼자에게 자신을 대신하여 서명할 수 있도록 서명을 위임하는 방식이다. 서명을 검증하는 사람은 대리 서명임을 검증과정에서 확인할 수 있다. 이 방식은 원서명자가 대리 서명자에게 비밀 서명정보를 자신의 일반 서명정보로부터 산출하여 전송한 다음 일반적인 서명방식으로 서명을 실행하게 되어 있으므로, 우선 기존의 일반적인 디지털 서명방식 하나를 설명하도록 한다.

2.2 일반적인 디지털 서명방식

앞절에서 설명한 바와 같이 일반적인 디지털 서명은 여러 사람에 의해 많이 제안되었으나, 본 절에

서는 이산대수문제(discrete logarithm problem)를 이용한 디지털 서명으로 효율성과 안전성이 우수한 것으로 알려진 Nyberg-Rueppel 방식을 소개한다[7].

〔초기화〕

(주) h, ‖를 제외한 기호는 음이 아닌 정수 값이다.

- g : $g=a^{(p-1)/q} \pmod p$; $1 < a < p-1$이고, $a^{(p-1)/q} \pmod p > 1$을 만족함.
- h : 해쉬 함수
- H : 해쉬 코드
- A : 난수값
- q : $q \mid p-1$, $q \geq 2160$
- R : 서명의 중간값
- $S_{x_A}(m)$: 서명자 A의 서명
- X_A : 서명자 A의 비밀 서명정보
- Y_A : 서명자 A의 공개 검증정보
- m : 문서

$Y_A = g^{X_A} \pmod p$의 X_A는 서명자 A의 비밀 서명정보로 서명자가 유일하게 X_A를 소유하고 있음을 검증자는 서명자 A의 공개 검증정보 Y_A로 확인한다. 따라서 서명자 A는 자신의 비밀 서명정보 X_A를 비밀리에 보관하고 Y_A는 검증자를 위해 공개한다.

〔서명 과정〕

문서 m에 대한 서명은 다음 단계를 거쳐 계산된다.

단계 1) $H = h(m)$을 계산한다.

단계 2) 난수값 $r \in_R Z_q$를 선택한다.

단계 3) $R = (g^r \bmod p) \bmod q$를 계산한다.

단계 4) $S_{X_A}(m) = r - R \cdot X_A \cdot H \pmod q$를 계산한다.

단계 5) 서명자 A는 m, R, $S_{X_A}(m)$을 검증자 B에게 전송한다.

〔검증 과정〕

서명자 A로부터 전송받은 m, R, $S_{X_A}(m)$을 서명자 A의 공개 검증정보 Y_A로 검증 절차를 실행한다.

단계 1) $H = h(m)$을 계산한다.

단계 2) $(g^{S_{x_A}(m)} Y_A^{RH} \bmod p) \bmod q \stackrel{?}{=} R$이 성립하는지 검증한다.

서명과정과 검증과정을 그림으로 나타내면 그림 1과 같다. 서명자 A는 자신이 비밀리에 보관하고 있는 비밀 서명정보 X_A로 서명한 $S_{X_A}(m)$을 검증자에게 전달하여 디지털 서명을 검증자 B로부터 확인 받는다. 서명과정에서의 $H = h(m)$은 문서 m을 해쉬하는 일방향 함수로 공개할 수 있다.

서명자 A	공개디렉토리 p, q, g, Y_A	검증자 B
$r \in_R Z_q$ $R = (g^r \bmod p) \bmod q$ $H = h(m)$ $S_{XA(m)} = r - RX_AH \pmod q$	m, R, $S_{XA(m)}$	$H = h(m)$ $g^{S_{x_A}(m)} \cdot Y_A^{RH} \bmod p) \bmod q$

그림 1. Nyberg-Rueppel의 디지털 서명방식

Ⅲ. 대리 서명방식

3.1 대리 서명방식의 개념

대리 서명방식이란 대리 서명자로 하여금 원서명자를 대신하여 서명을 할 수 있는 서명시스템을 말한다. 대리 서명방식의 조건은 두 가지로 나눌 수 있다. 첫째, 원서명자로부터 지정 받은 사람만 대리 서명을 생성할 수 있어야 하며, 대리 서명자로 지정 받지 못한 제삼자는 대리 서명을 생성할 수 없어야 한다. 또한 대리 서명을 검증하는 사람은 대리 서명으로부터 원서명자가 대리 서명자에게 대리 서명을 위임한 사실을 확인할 수 있어야 한다.

이와 같은 대리 서명방식은 다음과 같은 상황에서 유용하게 사용될 수 있다. 어떤 회사의 간부가 컴퓨터 네트워크가 없는 장소에 출장중, 본인 앞으로 도착한 전자문서에 대한 응답이 필요한 경우 사전에 다른 사람이 그 문서를 받아 답신을 할 수 있도록 해야 할 때 문서의 서명이 문제가 된다. 이때 사전에 대리 서명을 할 수 있도록 조치할 수 있다.

지금까지 제안된 대리 서명방식의 종류는 완전 위임(full delegation), 부분 위임(partial delegation) 그리고 보증 위임(delegation with warrant) 등 세 가지 방식이 있다.

1) 완전 위임방식

원서명자가 자신의 비밀 서명정보 X_A를 대리 서명자에게 알려주어 대리 서명자로 하여금 대리 서명하게 하는 방법으로 서명결과는 원서명자의 서명과 동일하게 된다. 이 경우는 원서명자의 비밀 서명정보X_A의 관리에 문제점이 생기게 되고, 대리 서명자의 절대적인 신뢰를 전제로 하지 않고는 사용이 불가능하다. 즉 대리 서명자의 부당한 X_A의 사용과 노출이 염려되는 방법으로 매우 제한적인 방식이다.

2) 부분 위임방식

부분 위임방식에서는 원서명자가 자신의 비밀 서명

정보 X_A로부터 새로운 비밀 서명정보 σ를 생성하여 비밀리에 대리 서명자에게 전달한다. 그러면 대리 서명자는 원서명자로부터 비밀리에 제공받은 σ를 자신의 대리 서명의 비밀 서명정보로 사용하게 된다. 물론 대리 서명을 생성하는 비밀 서명정보 σ로부터 원서명자의 비밀 서명정보 X_A를 구할 수 없어야 한다. 즉 원서명자는 완전 위임방식에서 발생하는 자신의 비밀 서명정보 X_A의 노출 위험성에 대해 안전하다[14,15,16].

부분 위임방식은 다음 두 가지로 나눌 수 있다.

① 대리인 비보호형 대리 서명방식(proxy-unprotected proxy signatures)

대리 서명자는 원서명자를 대신해서 대리 서명을 생성할 수 있으나, 대리 서명자 이외에 원서명자 또한 정당한 대리 서명자를 가장하여 대리 서명을 생성할 수 있다. 그러나, 대리 서명자로 지정 받지 않은 제삼자는 대리 서명을 생성할 수 있다.

② 대리인 보호형 대리 서명방식(proxy-protected proxy signatures)

정당한 대리 서명자만이 대리 서명이 가능하다. 따라서, 제삼자뿐만 아니라 원서명자 또한 정당한 대리 서명자를 가장하여 대리 서명을 생성할 수 없다.

3) 보증 위임방식

보증 위임방식은 원서명자가 문서로 대리 서명자임을 밝히는 방법으로 두 가지 방식이 있다[12,13].

① 보증서 기반 대리 서명방식(delegation proxy)

원서명자가 지정한 사람을 대리 서명자로 선언하는 서류에 일반적인 디지털 서명을 통하여 서명한 후, 그 서명된 보증서를 대리 서명자에게 전달한 다음 대리 서명자로 하여금 그 사실을 전제로 대리 서명을 시행토록 하는 방법이다.

② 소지자 기반 대리 서명방식(bearer proxy)

원서명자는 대리 서명자가 사용할 새로운 비밀 서명정보와 그에 대한 공개 검증정보를 생성하고, 생성된 공개 검증정보에 대한 서명을 하여 대리 서명자에게 준다. 이때 생성된 비밀키는 대리 서명자에게 비밀리에 전달된다.

대리 서명방식은 앞에서 설명한 세 방식을 이용하여 서명을 한다. 각자의 특징을 보면 완전 위임방식의 경우 원서명자 대리 서명자에게 직접 자신의 비밀 서명정보 X_A를 전달해 주므로해서 원서명자의 비밀 서명정보가 일반인에게 노출될 염려가 있을 뿐만 아니라 대리 서명자 선정에도 제한적이다. 즉, 대리 서명자로 선정된 사람의 X_A에 대한 비밀유지가 문제가 된다.

또한 보증 위임방식의 경우 보증서를 검증하는 추가적인 계산량과 전송량의 증가가 초래되므로 실용성 측면의 문제가 있으나, 보증서가 있어 대리 서명자의 통제기능이 가능하다.

부분 위임방식은 완전 위임방식에서와 같은 원서명자의 비밀 정보 누설을 방지할 수 있으며, 또한 보증서를 검증하는 과정이 별도로 요구되는 것이 아니라 대리 서명 검증시에 함께 검증 가능함으로 보증 위임방식에 비해 효율적이다. 그러나 보증서가 없어 대리 서명자로의 유효기간 등이 문제가 될 수 있다.

따라서 본 논문에서는 부분 위임방식의 장점과 보증 위임방식의 장점만을 취한 보증 부분 위임방식(partial delegation with warrant)을 제안한다. 부분 위임의 경우에는 대리 서명자가 대리 서명을 할 수 있는 기간을 명시할 수 없기 때문에 대리인을 철회하고자 하는 경우에 별도의 대리 서명 철회 과정(proxy revocation protocol)이 요구되나, 제안된 방식에서는 대리 서명자가 사용할 비밀 서명정보에 대리 서명을 할 수 있는 기간을 명시할 수 있으므로 이러한 과정이 필요 없다. 또한, 보증 위임에서와 같이 보증서를 검증하는 과정이 별도로 요구되는 것이 아니라 대리 서명 검증시에 보증서도 함께 검증 가능함으로 부분 위임과 같은 효율성을 갖는다.

3.2 Mambo의 부분 위임에 의한 대리 서명방식

M. Mambo와 E. Okamoto는 이산대수 문제를 이용하여 부분 위임에 의한 대리 서명방식을 제안하였다. 이 방식은 앞에서 설명한 바와 같이 원서명자의 비밀 서명정보 X_A를 포함시킨 새로운 대리 서명자의 비밀 서명정보를 생성시켜 비밀리에 대리 서명자에게 전달한다. 이 방식의 순서는 다음과 같다.

〔초기화〕

- p : 큰 소수 $p > 2^{512}$
- g : 원시 원소 $g \in Z_p$
- X_A : 원서명자의 비밀 서명정보 $X_A \in Z_{p-1}$
- Y_A : 원서명자의 공개 검증정보 $Y_A = g^{X_A} \pmod p$
- Sign(·) : 일반적인 디지털 서명방식

〔프로토콜〕

단계 1) (대리 서명용 키 생성) 원서명자는 다음을 계산한다.

$k \in_R Z_{p-1}$

$K = g^k \pmod p$

$\sigma = X_A + kK \pmod{p-1}$

단계 2) (대리 서명용 키의 분배) 원서명자는 자신이 계산한 대리 서명자의 비밀 서명정보 σ를 비밀리에

K와 같이 대리 서명자에게 전달한다.

단계 3) (대리 서명용 키의 검증) 대리 서명자로 지정 받은 사람은 원서명자가 생성한 대리 서명을 위한 비밀 서명정보 σ의 정당성을 원서명자의 공개 검증정보 Y_A를 이용하여 확인한다.

$g^{\sigma} \equiv Y_A K^K \pmod p$

단계 4) (대리 서명자에 의한 서명) 대리 서명자는 원서명자가 생성하여 비밀리에 제공한 비밀 서명정보 σ를 이용하여 일반적인 디지털 서명방식을 이용하여 문서 m의 대리 서명을 생성한다.

$(m, Sign_{\sigma}(m), K)$

단계 5) (대리 서명의 검증) 대리 서명자의 새로운 공개 검증 정보는 $V = Y_A K^K \pmod p$가 된다. 대리 서명을 검증하려는 사람은 V를 계산하는 과정에 Y_A가 포함되어 있으므로 원서명자의 위임 사실을 인지하게 되며 대리 서명의 검증은 일반적인 디지털 서명의 검증 순서를 따르게 된다.

Ⅳ. 보증 부분 위임에 의한 대리 서명방식의 제안

본 논문에서는 M. Mambo와 E. Okamoto가 제안한 부분 위임의 개념을 확장하여 보증 부분 위임에 의한 대리 서명방식을 제안하였다. 다음은 본 논문에서 제안하는 보증 부분 위임의 정의이다.

- 보증 부분 위임방식

보증 부분 위임이란 원서명자가 대리 서명용 비밀 정보 σ를 자신의 비밀 서명정보 X_A와 유효기간과 대리 서명자와의 관계 등이 언급된 보증서 m_w를 이용하여 생성하는 경우를 말한다. 이때 원서명자의 비밀 서명정보 X_A는 σ와 m_w로부터 계산 불가능하여야 한다. 보증 부분 위임의 형태는 다음과 같은 두 가지 형태로 분류된다.

① 대리인 비보호형 대리 서명방식

대리 서명자는 원서명자를 대신해서 대리 서명을 생성할 수 있으나, 대리 서명자 이외에 원서명자 또한 정당한 대리 서명자를 가장하여 대리 서명을 생성할 수 있다. 그러나, 대리 서명자로 지정 받지 않은 제삼자는 대리 서명을 생성할 수 없다.

② 대리인 보호형 대리 서명방식

정당한 대리 서명자만이 대리 서명이 가능하다. 따라서, 제삼자뿐만 아니라 원서명자 또한 정당한 대리 서명자를 가장하여 대리 서명을 생성할 수 없다.

제안하는 보증 부분 위임에 의한 대리 서명방식은 근본적으로 Mambo의 대리 서명방식과 기능은 유사하나, 보증서 기능을 추가하기 위해 공개 해쉬함수를 이용하였다. 대리 서명과 관련된 유효정보나 대리 서명자로 지정된 사실 등을 m_w으로 표시하여 $e = h(m_w, K)$를 계산한다.

한편 일반적으로 대리 서명자는 원서명자가 항상 정직하다는 전제로 대리 서명을 시행하게 된다. 그러나, 예를 들어, 원서명자가 대리 서명을 만들어 대리 서명자를 곤란하게 만들 경우가 있다. 이러한 경우를 방지하기 위해 대리 서명자 자신도 자신을 보호할 수 있는 기능이 있어야 한다. 앞에서 설명한 바와 같이 대리 서명자가 자신을 보호하기 위한 방식을 대리인 보호형 대리 서명방식, 그렇지 못한 경우를 대리인 비보호형 대리 서명방식이라 한다. 이 두 방식을 구별해서 본 논문에서는 제안을 하였다.

〔초기화〕

Mambo의 초기화 설정과정과 동일하다.

〔프로토콜 Ⅰ (대리인 비보호형 대리 서명방식)〕

단계 1) (대리 서명용 키 생성) 원서명자는 대리 서명자의 대리 서명을 생성할 수 있는 비밀 서명정보 σ에 유효기간과 대리 서명자의 관계 등이 언급된 보증서를 해쉬함수를 이용하여 포함시킨다. m_w가 보증서이고, ‖ 은 연접을 의미한다.

$k \in_R Z_q$

$K = g^k \pmod p$

$e = h(m_w \| K)$

$\sigma = eX_A + k \pmod q$

단계 2) (대리 서명용 키의 분배) 원서명자는 자신이 계산한 대리 서명자의 비밀 서명정보 σ를 비밀리에 m_w, K와 함께 대리 서명자에게 전달한다.

단계 3) (대리 서명용 키의 검증) 대리 서명자로 지정 받은 사람은 원서명자가 생성한 대리 서명 생성용 비밀 서명정보 σ의 정당성을 원서명자의 공개 검증정보 Y_A를 이용하여 확인한다.

$e = h(m_w \| K)$

$g^{\sigma} \equiv Y_A{}^e K \pmod p$

단계 4) (대리 서명자에 의한 서명) 대리 서명자는 원서명자가 생성하여 비밀리에 제공한 비밀 서명정보 σ를 가지고 일반적인 디지털 서명방식(예를 들면, Nyberg-Rueppel 서명방식)을 이용하여 문서 m의 대리 서명을 생성한다.

$(m, m_w, S_{\sigma}(m), K)$

단계 5) (대리 서명의 검증) 대리 서명자는 $e = h(m_w \| K)$를 계산하고, 대리 서명을 위한 공개 검증정보 $V = Y_A{}^e K \pmod p$를 계산한다. 대리 서명을 검증하려는 사람의 입장에서는 공개 검증정보 계산과정에 Y_A가 포함되는 사실로부터 원서명자의 위임 사실을 인지하게 된다. 대리 서명의 검증과정은 일반적인 디지털 서명의 검증순서와 동일하다.

위의 서명과정을 그림으로 나타내면 그림 2와 같다.

대리 서명자	공개디렉토리 p, q, g, Y_A	검 증 자
$r \in_R Z_q$ $R=(g^r \bmod p) \bmod q$ $H=h(m)$ $S_\sigma(m)=r-R\sigma H \pmod q$	m, m_w, R, $S_\sigma(m)$	$e=h(m_w \| K)$ $V=Y_A{}^eK \pmod p$ $R \doteq (g^{S_\sigma(m)} V^{RH} \bmod p) \bmod q$

그림 2. Nyberg-Rueppel형 '대리인 비보호형 대리 서명방식'

〔프로토콜 II (대리인 보호형 대리 서명방식)〕

지금까지 설명한 대리 서명방식은 원서명자의 신뢰성을 전제로 하는 방식이다. 그러나 원서명자의 정직하지 못한 행동 즉, 원서명자가 대리 서명자를 가장한 서명은 대리 서명자를 곤란하게 만들 수 있다. 원서명자의 부정 행위는 상기의 단계 3)-단계 5)를 다음 방식으로 바꾸면 간단히 방지할 수 있다. 〔프로토콜 I〕을 다음과 같이 바꾼다.

단계 3′) (대리 서명용 키의 검증 및 변환) 원서명자가 생성한 대리 서명용 비밀정보 σ와 m_w, K를 전달받은 대리 서명자는 대리 서명을 위한 비밀정보 σ의 정당성을 확인한 후 대리 서명자 자신이 비밀리에 보관하고 있는 일반 서명 비밀정보 X_B를 포함시킨다. 따라서 대리 서명 생성용 비밀 서명정보에 대리 서명자 자신의 비밀 서명정보 X_B가 포함되어 있어, 변환된 대리 서명용 비밀정보 σ_P를 만들 수 있는 사람은 대리 서명자 뿐으로 자신을 보호할 수 있다.

$e = h(m_w \| K)$

$g^{\sigma} \doteq Y_A{}^eK \pmod p$ 확인

$\sigma_P = \sigma + eX_B \pmod{p-1}$

단계 4′) (대리 서명자에 의한 서명) 대리 서명자는 자신이 재생성한 대리 서명용 서명 비밀정보 σ_P를 이용하여 일반적인 디지털 서명방식을 이용하여 문서 m의 대리 서명을 생성한다.

단계 5′) (대리 서명의 검증) 대리 서명자의 새로운 공개 검증정보 계산 절차는 먼저 $e=h(m_w \| K)$를 계산하고 $V_P=(Y_AY_B)^eK \pmod p$를 계산한다. 대리 서명의 검증 순서는 일반 디지털 서명의 검증 순서에 따라 검증한다. 검증을 위한 V_P 계산과정에서 Y_A와 Y_B가 포함되므로 원서명자와 대리 서명자의 신원을 확인할 수 있으며 특히, σ_P 계산과정에 X_B가 포함되므로 σ_P의 생성은 대리 서명자에 의해서만 계산이 가능하다.

대리인 보호형 대리 서명방식을 그림으로 나타내면 그림 3과 같다.

대리 서명자	공개디렉토리 p, q, g, Y_A	검 증 자
$r \in_R Z_q$ $R=(g^r \bmod p) \bmod q$ $H=h(m)$ $S_{\sigma_P}(m)=r-R\sigma_P H \pmod q$	m, m_w, R, $S_{\sigma_P}(m)$	$e=h(m_w \| K)$ $V_P=(Y_AY_B)^eK \pmod p$ $R \doteq (g^{S_{\sigma_P}(m)} V_P{}^{RH} \bmod p) \bmod q$

그림 3. Nyberg-Rueppel형 '대리인 보호형 대리 서명방식'

V. 성능 분석

만일 대리 서명방식으로, 논문 [15, 16]에서와 같이, ElGamal 서명 방식을[3] 사용한다고 하면 보증 위임에 의한 대리 서명방식보다 제안된 보증 부분 위임에 의한 대리서명 방식에서 소요되는 계산량이 적다. 보증 위임 방식의 계산량은 2956+2WI(512)이나, 제안된 방식의 대리인 비보호 방식의 계산량은 2156+2WI(512)+2WH(|m_w|)이고 대리인 보호 방식의 계산량은 2158+2WI(512)+2WH(|m_w|)이다. 따라서 제안된 방식이 보다 효율적임을 알 수 있다. 본 계산량 분석 방법에서는 Kaliski에 의한 측정 방법을 사용하였다.[18] 상수는 512 비트 모듈러 곱셈의 개수를 의미하며 WI(b)는 b비트 모듈러 역원 계산의 개수를 나타내고, WH(b)는 b비트 입력을 갖는 해쉬 함수의 계산량을 의미한다.

부분 위임에 의한 대리 서명방식과의 비교에서, 제안된 방식은 대리 서명용 비밀키 σ(σ_P)를 계산하는 과정에서 641+WH(|m_w|) (642+WH(|m_w|))의 계산량이 요구되며, 서명 생성 과정에서는 642+WI(512) (642+WI(512)), 서명 검증 과정에서는 875+WH(|m_w|) (876+WH(|m_w|))의 계산량이 요구된다(괄호 내는 대리인 보호 방식의 계산량을 의미한다). 반면에 부분 위임 방식의 경우에는 대리 서명용 비밀키를 계산하는 과정에서 641(642)의 계산량이 요구되며, 서명 생성과정에서는 642+WI(512) (642+WI(512)), 서명 검증과정에서는 875(906)의 계산량이 요구되며, 대리인을 철회하고자 하는 경우에 철회 과정을 위하여 1282의 계산량이 추가로 요구된다.

대리인 보호 방식의 3번째 단계 대리 서명키의 변환 과정에서 대리 서명용 키 σ_P는 다음과 같이 만드는 것도 가능하다.

$$\sigma_P = \sigma + s_pV_p \pmod{p-1}$$

그러나, 위와 같이 σ_P를 생성하는 경우에는 대리 서명 검증 과정에서 906+WH(|m_w|)의 계산량이 요구되어 비효율적이다.

결론적으로, 계산 효율성 측면에서, 제안된 보증 부분 위임방식은 단순 보증 위임방식 보다 계산량이 적다. 또한, 원서명자의 관점에서, 부분 위임방식에서 요구되는 대리인 철회 과정이 필요치 않다. 이러한 계산량 분석 결과는 Schnorr 서명방식[4], Okamoto 서명방식[6], 또한 본 논문에서 사용한 Nyberg-Rueppel 서명방식[7] 등에서도 같은 유사한 결과를 얻을 수 있다.

Ⅵ. 결 론

본 논문에서는 기존의 대리 서명방식에서 필요로 하는 보증서 기능을 포함시킨 보증 부분 위임에 의한 대리 서명방식을 제안하였다. 제안한 보증서 기능을 갖는 부분 위임 방식의 대리 서명은 기존의 보증 위임에 의한 대리 서명방식보다 계산량이 적으며 보통의 부분 위임에 의한 대리 서명방식보다 구조적으로 우수하다.

제안된 보증 부분 위임에 의한 대리 서명방식은 보증서 기능을 갖고 있어 위임을 한 원서명자의 위임기간 등의 유효정보를 설정할 수 있어 응용범위가 클 것으로 사료된다.

참 고 문 헌

[1] W. Diffie and M. Hellman, "New directions in cryptography," IEEE. Trans. on Information Theory IT-22, pp.644-654, 1976.

[2] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystem," communication of ACM vol 21, no.2, pp.120-126, 1978.

[3] T. ElGamal, "A public key cryptosystem and signature scheme based in discrete logarithm," IEEE. Trans. on Information Theory vol.31 no.4, pp.469-472, 1995.

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

[5] NIST FIPS PUB XX. "Digital Signature Standard, National Institute of Standards and Technology," U.S Department of commerce. Draft. 1 Feb. 1993.

[6] T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes," Proc. Crypto'92, pp.31-53, 1993.

[7] Kaisa Nyberg and Rainer A. Rueppel, "Message Recovery for signature schemes based on the discrete logarithm problem," Eurocrypt'94, pp. 175-190, 1994.

[8] D. Chaum and H. Antwerpen, "Undeniable signature," Crypto'89, pp.212-216.

[9] S.J. Park, K.H. Lee and D.H. Won "An entrusted undeniable signature" JW-ISC'95, pp.2.1-2.7, 1995.

[10] S.J. Kim, S.J. Park, and D.H. Won, "Nominative signature," Proc. of ICEIC'95, International Conference on Electronics, Informations and Communications, pp.II-68~II-71, 1995.

[11] S.J. Kim, S.J. Park, and D.H. Won "Zero-knowledge nominative signature," Pragocrypt '96, International Conference on the Theory and Applications of Cryptology, pp.38-392, 1996.

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

[13] B.C. Neuman, "Proxy-based authentication and accounting for distributed system" Proc. of 13th International Conference on Distributed Computing System. pp.283-291, 1993.

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

[15] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signature for delegating signing operation," Proc. of third ACM conference on computer and communication security, pp.48-57, 1996.

[16] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signature : Delegation of the power to sign message," IEICE Trans. Fundamentals, vo.E79-A, no.9, 1996.

[17] S.J. Kim, S.J. Park and D.H. Won, "Proxy signatures, revisited," Proc. of ICICS '97, International Conference on Information and Communications Security, Springer, Lecture Notes in Computer Science, LNCS 1334, pp.223-232,

1997.
[18] B.S. Kaliski, "A response to DSS," Nov. 1991.

김 승 주(Seungjoo Kim) 정회원
1971년 9월 22일생
1994년 2월 : 성균관대학교 정보공학과 졸업 (공학사)
1996년 2월 : 성균관대학교 대학원 정보공학과 졸업(공학석사)
1999년 2월 : 성균관대학교 대학원 정보공학과 졸업(공학박사)
1998년 2월 : 성균관대학교 대학원 정보공학과 졸업(공학박사)
※URL : http://dosan.skku.ac.kr/~sjkim

박 상 준(Sangjoon Park) 정회원
1960년 6월 25일생
1984년 2월 : 한양대학교 수학과 졸업 (이학사)
1986년 2월 : 한양대학교 대학원 수학과 졸업(이학석사)
1986년 1월~현재 : 한국전자통신연구원 책임연구원
1999년 2월 : 성균관대학교 대학원 정보공학과 졸업(공학박사)

원 동 호(Dongho Won) 정회원
1949년 9월 23일생
1976년 2월 : 성균관대학교 전자공학과 졸업 (공학사)
1978년 2월 : 성균관대학교 대학원 전자공학과 졸업(공학석사)
1988년 2월 : 성균관대학교 대학원 전자공학과 졸업(공학박사)
1978년 4월~1980년 3월 : 한국전자통신연구원 연구원
1985년 9월~1986년 8월 : 일본 동경공대 객원연구원
1996년 4월~1998년 4월 : 정보화추진위원회 자문위원
1982년 3월~현재 : 성균관대학교 공과대학 전기·전자 및 컴퓨터공학부 교수
1991년~현재 : 한국통신정보보호학회 편집이사
<주관심분야 : 암호이론, 정보이론>
URL : http://dosan.skku.ac.kr

양 형 규(Hyungkyu Yang) 정회원
1959년 7월 6일생
1983년 2월 : 성균관대학교 전자공학과 졸업(공학사)
1985년 2월 : 성균관대학교 대학원 전자공학과 졸업(공학석사)
1994년 2월 : 성균관대학교 대학원 정보공학과 졸업(공학박사)
1984년~1991년 : 삼성전자 컴퓨터부문 선임연구원
1995년~현재 : 강남대학교 전자계산학과 조교수