通信情報保護學會論文誌
第 8 卷 第 2 號, 1998. 6

보증 부분 위임과 역치 위임에 의한 대리 서명방식

김 승 주*, 박 상 준**, 원 동 호*

Proxy Signatures for Partial Delegation with Warrant and Threshold Delegation

Seungjoo Kim*, Sangjoon Park**, Dongho Won*

요 약

Mambo, Usuda, Okamoto에 의하여 최초로 제안된 대리 서명은 원서명자가 지정한 서명자가 원서명자를 대신하여 서명하는 것을 허용한다. 본 논문에서는 이러한 대리 서명 중에서 보증서를 이용하여 부분 위임이 가능한 대리 서명과 역치 위임이 가능한 대리 서명을 제안하였다. 보증 부분 위임은 Mambo가 제안한 부분 위임과 Neuman의 보증 위임의 장점을 결합한 것으로 암호 효율성 또한 좋다. 역치 위임은 원서명자가 n명의 대리 서명자를 지정하고 n명의 대리 서명자중 t명 이상의 대리 서명자가 협조하여야 대리 서명을 할 수 있는 개념으로 본 논문에서 threshold 위임에 의한 대리 서명 방식을 제시하였다..

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 two new types of digital proxy signatures called partial delegation with warrant and threshold delegation.

Proxy signatures for partial delegation with warrant combines the benefit of Mambo's partial delegation and Neuman's delegation by warrant, and then in threshold delegation the proxy signer's power to sign messages is shared. Moreover, we also propose straightforward and concrete proxy signature schemes satisfying our conditions.

키워드 : 공개키 방식, 디지틀 서명, 특수 서명, 대리 서명, threshold cryptography

*성균관대학교, 전기 · 전자 및 컴퓨터공학부
**한국전자통신연구원

1. 서 론

Mambo가 처음 제안한 대리 서명방식(proxy signatures)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 서명자만이 원서명자의 정당한 대리 서명을 생성할 수 있다.

검증 가능성 : 검증자는 대리 서명이 원서명자가 인정한 대리 서명자에 의하여 서명되었음을 확인할 수 있다.

이와 같은 서명방식은 하드웨어 장치의 도움 없이 메시지에 서명하는 능력을 제3자에게 전달하는데 사용될 수 있다. 회사에 종사하는 사람이 컴퓨터 네트워크가 구성되지 않은 장소를 여행하는 경우 긴급한 결재 사항을 처리할 수 없게 될 것이다. 이 경우 이 사람은 자신의 비서에게 자신을 대신해서 대리 서명할 수 있도록 한다면 긴급한 결정 사항을 원만하게 처리하는 것이 가능할 것이다.

Mambo는 원서명자가 대리 서명자에게 제공하는 형태에 따라 완전 위임(full delegation), 부분 위임(partial delegation), 보증 위임(delegation by warrant)으로 분류하였다. 본 논문에서는 Mambo의 부분 위임과 보증 위임의 개념을 통합한 보증 부분 위임(partial delegation with warrant)을 제안하였다. 보증 부분 위임에 의한 대리 서명방식은 부분 위임과 보증 위임이 갖는 장점을 모두 수용하였을 뿐 아니라, 제안된 방식은 Mambo의 방식에 비하여 서명의 효율성이 높다. 본 논문에서는 또한 여러 명의 대리 서명자를 지정하여 대리 서명시 지정된 서명자들의 상호 협조에 의하여 대리 서명하는 역치 위임(threshold delegation)에 의한 대리 서명방식을 제안한다. 역치 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 6개의 절로 구성된다. 2절에서는 Mambo에 의한 대리 서명의 분류에 따른 서명 방식들을 기술하고, 또한 본 논문에서 제안되는 보증 부분 위임과 역치 위임을 정의하였다. 3절에서는 Mambo의 부분 위임에 의한 대리 서명방식을 소개하고, 4절에서는 보증 부분 위임 방식을 구성하는 구체적인 방법을, 5절에서는 역치 위임 방식을 구성하는 방법을 제안하고 제안된 방식의 안전성과 효율성을 기술하였다. 6절은 본 논문의 결론 부이다.

2. 대리 서명방식의 정의와 분류

Mambo는 대리 서명방식에서 원서명자의 서명 능력을 위임하는 형태에 따라 완전 위임(full delegation), 부분 위임(partial delegation)으로 나누었으며, Neuman, Varadharajan등은 원서명자에 만든 보증서를 사용하여 대리 서명을 실현하는 보증 위임(delegation by warrant)의 개념을 제안하였다. 각 위임 형태에 대한 정의는 다음과 같다.

정의 1. 완전 위임 (full delegation) 완전 위임이란 원서명자(original signer)가 대리 서명자(proxy signer)에게 자신의 서명용 비밀키 s를 주는 경우를 말한다. 따라서, 대리 서명자에 의한 서명과 원서명자에 의한 서명은 구분되지 않는다.

정의 2. 부분 위임 (partial delegation) 부분 위임이란 원서명자가 대리 서명용 비밀키 σ를 자신의 비밀키 s를 이

용하여 생성한다. 이때 비밀키 s는 σ로부터 계산 불가능하여야 한다. 부분 위임의 형태는 다시 다음과 같은 두 가지 형태로 분류된다.[1][2][3]

대리인 비보호형 대리 서명방식 (proxy-unprotected proxy signatures) : 대리 서명자는 원서명자를 대신하여 서명할 수 있으나, 대리 서명자 이외에 원서명자 또한 정당한 대리 서명자를 가장하여 대리 서명할 수 있다. 그러나 대리 서명자로 지정 받지 않은 제3자는 대리 서명을 생성할 수 없다.

대리인 보호형 대리 서명방식 (proxy-protected proxy signatures) : 정당한 대리 서명자만이 대리 서명이 가능하다. 따라서, 원서명자 또한 정당한 대리 서명자를 가장하여 대리 서명할 수 없다.

정의 3. 보증 위임 (delegation by warrant) 보증 위임이란 원서명자가 대리 서명자에게 보증서(warrant)를 발행함으로서 대리 서명을 구현하는 방식을 말하며 다음과 같이 두 가지 형태로 구분된다.[4][5]

보증서 기반 대리 서명방식 (delegation proxy) : 지정한 사람을 대리 서명자로 선언하는 서류에 원서명자가 일반적인 디지털 서명을 통하여 서명한 후, 그 서명된 보증서를 이용하여 대리 서명을 실현한다.

소지자 기반 대리 서명방식 (bearer proxy) : 지정한 서명자를 위한 비밀키와 공개키를 생성하고 생성된 공개키에 대하여 원서명자가 보증서를 만들어 지정된 대리 서명자 준다. 이때 생성된 비밀키는 대리 서명자에게 비밀리에 전달된다.

완전 위임에서는 원서명자의 비밀키 정보가 완전히 노출되기 때문에 대리 서명자가 원서명자를 가장하여 서명을 생성하는 것이 가능하다. 따라서, 부분 위임은 완전 위임 보다 안전하다. 또한, 보증 위임에서는 보증서를 검증하는 과정이 추가적으로 요구되기 때문에 부분 위임에 비하여 처리 속도가 느린 단점이 있으나 일반적인 서명 방식들도 어떠한 변경 없이 보증 위임에 의한 대리 서명을 실시할 수 있다는 장점이 있다. 본 논문에서는 이러한 부분 위임과 보증 위임의 장점만을 취하여 보증 부분 위임에 의한 대리 서명 방식을 제안한다. 다음은 본 논문에서 제안하는 보증 부분 위임(partial delegation with warrant)의 정의이다.

정의 4. 보증 부분 위임 (partial delegation with warrant) 보증 부분 위임이란 원서명자가 대리 서명용 비밀키 σ를 자신의 비밀키 s와 유효기간과 대리 서명자와의 관계 등이 언급된 보증서 m_w를 이용하여 생성하는 경우를 말한다. 이때 원서명자의 비밀키 s는 σ와 m_w로부터 계산 불가능하여야 한다. 보증 부분 위임의 형태는 다음과 같은 두 가지 형태로 분류된다.[6]

대리인 비보호형 대리 서명방식 : 대리 서명자는 원서명자를 대신하여 서명할 수 있으나, 대리 서명자 이외에 원서명자 또한 정당한 대리 서명자를 가장하여 대리 서명을 생성할 수 있다. 그러나 대리 서명자로 지정 받지 않은 제 3자는 대리 서명을 생성할 수 없다.

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

부분 위임의 경우에는 대리 서명자가 대리 서명을 할 수 있는 기간 등을 명시할 수 없기

때문에 대리인을 철회하고자 하는 경우에 대리 서명 철회 과정(proxy revocation protocol)이 요구되나, 제안된 방식에서는 보증서에 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.

이제 본 논문에서 제안하는 다른 형태의 대리 서명방식으로 역치 위임(threshold delegation)이 가능한 대리 서명 방식을 정의하고자 한다.

정의 5. 역치 위임 (threshold delegation)
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.[6]

(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. 본 논문의 4절에서는 보증 부분 위임에 의한 대리 서명의 구체적인 구성 방법이 기술되었으며, 5절에서는 역치 위임에 의한 대리 서명의 구체적인 구성 방법들이 기술되었다.

3. Mambo의 부분 위임에 의한 대리 서명방식

본 절에서는 Mambo가 제안한 부분 위임에 의한 대리 서명 방식을 소개하고자 한다. 본 논문에서 p는 $2^{511} < p < 2^{512}$인 큰 소수이고 g는 Z_p^*상의 원시원소이다. s는 원서명자의 비밀키이고 $v_O = g^s \pmod p$는 공개키이다. 대리 서명 과정은 다음과 같다.

1. (대리 서명용 키 생성) 원서명자는 대리 서명자에게 다음과 같은 서명용 키 σ를 생성하여 (σ, K)를 대리 서명자에게 비밀리에 전달한다.

$$k \in Z_{p-1} - \{0\},$$
$$K = g^k \pmod p,$$
$$\sigma = s_O + k \cdot K \pmod{p-1}$$

2. (대리 서명용 키의 검증) 대리 서명자는 자신이 받은 (σ, K)이 정당한 키인지 다음의 관계식에 의하여 확인한다.

$$g^\sigma = v_O K^K \pmod p$$

3. (대리 서명자에 의한 서명) 대리 서명자는 비밀키 σ를 사용하여 임의의 메시지 m에 대한 ElGamal 형태의 서명 $\mathrm{Sign}_\sigma(m)$을 생성하고 (m, $\mathrm{Sign}_\sigma(m)$, K)를 서명 수신자에게 전달한다.

4. (대리 서명의 검증) 서명 수신자는 먼저 $v' = v_O \cdot K^K \pmod p$를 계산한다. 이제 v'을 사용하여 σ를 사용하여 만들어진 서명 $\mathrm{Sign}_\sigma(m)$을 검증한다. 이때 검증 방법은 ElGamal 형태의 서명 방식에 의한다.

4. 보증 부분 위임에 의한 대리서명방식

본 절에서는 대리 서명자에게 제공하는 대

리 서명용 키의 공개키와 대리 서명용 키의 유효 기간을 포함하는 메시지에 원서명자가 서명함으로서 만들어진 보증서를 사용하여 부분 위임을 실현시키는 방법을 제안하고자 한다. 제안되는 방식을 대리인 비보호 방식과 대리인 보호 방식으로 나누어 설명하고자 한다.

대리인 비보호형 서명 프로토콜

1. (대리 서명용 키 생성) 원서명자는 대리 서명자에게 다음과 같은 서명용 키 σ를 생성한다. 이때, m_w에는 원서명자의 ID, 대리 서명자의 ID, 위임 기간 등이 명시된다. 따라서, σ는 m_w와 K에 대한 원서명자의 서명이다 (단, h(·)는 안전한 해쉬 함수이다). 이제 (m_w, σ, K)를 대리 서명자에게 비밀리에 전달한다.

$$k \in Z_{p-1} - \{0\},$$
$$K = g^k \pmod p,$$
$$e = h(m_w, K),$$
$$\sigma = e\, s_O + k \pmod{p-1}$$

2. (대리 서명용 키의 검증) 대리 서명자는 자신이 받은 (m_w, σ, K)로부터 이 m_w, K에 대한 원서명자의 서명임을 확인한다.

$$e = h(m_w, K),$$
$$g^\sigma = v_O^e\, K \pmod p$$

3. (대리 서명자에 의한 서명) 대리 서명자는 비밀키 σ를 사용하여 임의의 메시지 m에 대한 ElGamal 형태의 서명 $\mathrm{Sign}_\sigma(m)$을 생성하고 (m, $\mathrm{Sign}_\sigma(m)$, m_w, K)를 서명 수신자에게 전달한다.

4. (대리 서명의 검증) 서명 수신자는 먼저 $e=h(m_w, K)$와 $v' = v_O^e\, K \pmod p$를 계산한다. $v' = g^\sigma \pmod p$이므로 v'을 사용하여 서명 $\mathrm{Sign}_\sigma(m)$을 검증할 수 있다. 이때 검증 방법은 ElGamal 형태의 서명방식에 의한다. 관계식 $v' = v_O^e\, K \pmod p$는 원서명자가 v'에 대응되는 σ를 만들어서 대리인에게 주었음을 의미한다. 왜냐하면 대리인은 이러한 관계식을 만족시키는 σ를 만들 수 없기 때문이다. 따라서, 서명 $\mathrm{Sign}_\sigma(m)$이 원서명자를 대신한 대리 서명임을 확인할 수 있다.

논문[3]에서 Usuda는 보증서 m_w를 사용하지 않고 관계식 $g^\sigma = v_O^{h(K)} \cdot K \pmod p$에 의하여 부분 위임에 의한 대리 서명을 제안하였다. 따라서, 이 경우에는 대리인 위임 기간이 지날 경우 원서명자는 대리인 철회를 위한 별도의 철회 과정을 수행하여야 한다.

대리인 비보호형에서는 원서명자가 대리인을 가장하여 대리 서명을 할 수 있다. 따라서, 제3자는 원서명자가 서명한 것을 대리 서명자가 서명한 것으로 오인할 수 있다. 그러므로 대리 서명자를 보호하기 위한 방안이 요구된다. 대리인 보호형 대리 서명방식에서는 이러한 문제점을 해결할 수 있다. 다음의 프로토콜에서 S_P는 대리 서명자의 비밀키이고 $v_P = g^{S_P} \pmod p$는 대리 서명자의 공개키이다.

대리인 보호형 서명 프로토콜

1. (원서명자에 의한 대리 서명용 키 생성) 대리인 비보호형 프로토콜과 동일하다.

$$k \in Z_{p-1} - \{0\},$$
$$K = g^k \pmod p,$$
$$e = h(m_w, K),$$
$$\sigma = e\, s_O + k \pmod{p-1}$$

2. (키의 검증) 대리인 비보호형 프로토콜

과 동일하다.

$$e = h(m_w, K),$$
$$g^{\sigma} = v_O^{e} \cdot K \ (mod\ p)$$

3. (대리 서명키의 변환) 대리 서명자는 원서명자가 서명용 키를 알 수 없도록 다음과 같이 변환하여 대리 서명용 키 σ′를 생성한다.

$$\sigma' = \sigma + S_P\, h(m_w, K)\ (mod\ p\text{-}1)$$

4. (대리 서명자에 의한 서명) 대리 서명자는 비밀키 σ′를 사용하여 임의의 메시지 m에 대한 ElGamal 형태의 서명 $Sign_{s'}(m)$을 생성하고 $(m, Sign_{s'}(m), m_w, K)$를 서명 수신자에게 전달한다.

5. (대리 서명의 검증) 서명 수신자는 먼저 $e = h(m_w, K)$와 $v' = (v_O\, v_P)^{e} \cdot K\ (mod\ p)$를 계산한다. $v' = g^{\sigma}\ (mod\ p)$이므로 v'을 사용하여 서명 $Sign_{s'}(m)$을 검증할 수 있다. 이때 검증 방법은 ElGamal 형태의 서명방식에 의한다. 관계식 $v' = (v_O\, v_P)^{e} \cdot K\ (mod\ p)$에서는 원서명자의 공개키 v_O뿐 아니라 대리 서명자의 공개키 v_P도 사용되므로 이러한 관계식을 만족하는 v'에 대응되는 σ′을 원서명자 또는 대리 서명자 혼자서는 만들 수 없음을 의미하며, 이러한 관계식을 만족시키는 σ′은 둘의 협조로 만들었음을 확인할 수 있다. 따라서, 서명 $Sign_{s'}(m)$이 원서명자를 대리하여 대리인이 대리 서명한 것임을 확인할 수 있다.

성능 분석

만일 대리 서명방식으로 ElGamal 서명방식[7]을 사용한다고 하면 보증 위임에 의한 대리 서명방식보다 제안된 보증 부분 위임에 의한 대리 서명방식에서 소요되는 계산량이 적다. 보증 위임방식의 계산량은 2956 + 2WI(512)이나, 제안된 방식의 대리인 비보호형 방식의 계산량은 2156 + 2WI(512) + 2WH($|m_w|$)이고 대리인 보호형 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.[8] 상수는 512비트 모듈러 곱셈의 개수를 의미하며 WI(b)는 b비트 모듈러 역원 계산의 개수를 나타내고, WH(b)는 b비트 입력을 갖는 해쉬 함수의 계산량을 의미한다 (논문 [1] 참조).

부분 위임에 의한 대리 서명방식과의 비교에서, 제안된 방식은 대리 서명용 비밀키 σ(σ′)를 계산하는 과정에서 641 + WH($|m_w|$) (642 + WH($|m_w|$))의 계산량이 요구되며, 서명 생성과정에서는 642 + WI(512) (642 + WI(512)), 서명 검증과정에서는 875 + WH($|m_w|$) (876 + WH($|m_w|$))의 계산량이 요구된다 (괄호 내는 대리인 보호형 방식의 계산량을 의미한다). 반면에 부분 위임방식의 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′는 다음과 같이 만드는 것도 가능하다.

$$\sigma' = \sigma + S_P\, V_P\ (mod\ p\text{-}1)$$

그러나, 위와 같이 σ′를 생성하는 경우에는 대리 서명 검증과정에서 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[9], Okamoto 서명방식[10]에서도 같은 유사한 결과를 얻을 수 있다.

5. 역치 대리 서명방식

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. 본 절에서는 이러한 특성을 만족하는 Schnorr 서명방식에 의한 (t, n)-역치 대리 서명방식을 제안하고자 한다. 역치 서명을 만들기 위하여 Ceredo의 Schnorr형 역치 서명방식을 사용한다.[11] 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 $f(x)=r+a_1x+\cdots+a_{t-1}x^{t-1}\ (mod\ p)$를 선택하여 모든 회원 Pi에게 $s_i=f(i)\ (mod\ p)$를 비밀리에 전달한다 ($i=1, 2, \cdots, n$). 이 경우 n명중 t명 이상이 모이면 딜러가 생성한 난수 r을 복구할 수 있다. 그러나 딜러는 난수 r을 이미 알고 있으므로 다른 그룹원의 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[12][13]

1. 각 참가자 P_i는 난수 k_i를 선택하고, $y_i=g^{k_i}\ (mod\ p)$를 계산한다.
2. 난수 k_i를 참가자들에게 나누어주기 위하여 각 P_i는 다음과 같은 $f_i(0)=k_i$인 t-1차 다항식을 만든다.

$$f_i(x)=k_i+a_{i,1}x+a_{i,2}x^2+\cdots+a_{i,t-1}x^{t-1}\ (mod\ q)\ (a_{i,j}\in Z_q)$$

3. P_i는 $f_i(j)$를 P_j에게 비밀리에 전달하고 다음의 값들은 모든 참가자들에게 알려준다 ($i=1, 2, , n$).

$$y_i, g^{a_{i,1}}, \ldots, g^{a_{i,t-1}}, F_{i,1}, \ldots, F_{i,n}(F_{i,j}=g^{f_i(j)}\ (mod\ p))$$

4. 이제 모든 참가자 P_i는 다음의 관계식을 확인한다 ($i=1, 2, , n$).

$$g^{f_j(i)}=y_j\cdot(g^{a_{j,1}})^{i}\cdots(g^{a_{j,t-1}})^{i^{t-1}}\ (mod\ p)\ \ (j=1,2,,n)$$
$$F_{j,k}=y_j\cdot(g^{a_{j,1}})^{k}\cdots(g^{a_{j,t-1}})^{k^{t-1}}\ (mod\ p)\ (k=1,2,,n, j=1,2,,n)$$

5. 모든 참가자 는 난수 $r=k_1+k_2+\cdots+k_n\ (mod\ p)$에 대한 자신의 부분 비밀 정보 $r_i=f_1(i)+f_2(i)+\cdots+f_n(i)\ (mod\ p)$를 계산하고 난수 r에 대한 공개 정보 y와 다음의 정보를 계산한다.

$$y=\prod_j y_j g^{a_j}=\prod_j g^{a_{j,i}}, \cdots g^{a_{j,t-1}}=\prod_j g^{a_{j,t-1}}\ (a_i=\sum_{j=1}^{n}a_{j,i}\ (mod\ q))$$

$f(x)=f_1(x)+f_2(x)+\cdots+f_n(x)\ (mod\ p)$라 하면 $f(0)=r\ \ (mod\ p)$이 고 $f(x)=r+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}\ (mod\ q)$이며, $r_i=f(i)\ (mod\ q)$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.

5.1 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 $e = h(m_w, K)$와 $s = e \cdot s_O + k \pmod q$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.

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

3. (키 분배) 이제 $B_j = g^{b_j} \pmod p$, $S_j = g^{\sigma_j} \pmod p$ $(j = 1, \cdots, t\text{-}1)$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.

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

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

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).

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

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

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

4. 이제 각 $P_i \in H$는 집합 $\{\gamma_i \mid P_i \in H\}$와 Lagrange interpolation을 사용하면 공통의 비밀 정보 $t = r + \sigma \cdot e' = f(0) + f'(0) \cdot e' \pmod q$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.

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

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 $t'=r'+\sigma\cdot e'$을 만들 수 있다.

5.2 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.

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

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.

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

2. (원서명자에 의한 키 생성) 원서명자는 난수 k를 생성하여 $K=g^{k}\ (mod\ p)$를 계산하고, m_w와 K의 해쉬값 $e=h(m_w, K)$와 $\sigma=e\cdot s_O+k\ (mod\ q)$를 계산한다 ($m_w$는 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.

$$f'(x)=\sigma+b_1x+b_2x^2+\cdots+b_{t-1}x^{t-1},\ \sigma_i=f'(i)\ (mod\ q),\ \sigma=f'(0)\ (mod\ q)$$

4. (키 분배) 이제 $B_j=g^{b_j}\ (mod\ p)$, $S_j=g^{\sigma_j}\ (mod\ p)$ $(j=1,\cdots, t\text{-}1)$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 정보 σ_i가 올바른 키 정보인지 다음의 관계식으로 확인한다.

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

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

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.

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

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).

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

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 $e' = h(y, m)$, $i = f(i) + \sigma_{p,i}$ $e' = f(i) + (f'(i) + f''(i))\, e' \pmod q$를 계산하고 i를 H에 속한 참가자간에 비밀리에 주고받는다.

3. H에 속한 각 참가자 P_i는 다음의 관계식을 확인한다.

$$(y \prod_{j=1}^{t-1} (g^{a_j})^{l_j}) \cdot ((v_o^{e'} \cdot K) \prod_{j=1}^{t-1} (g^{b_j})^{l_j}) \cdot (V_{PG} \prod_{j=1}^{t-1} (g^{c_j})^{l_j})^{e'}$$

$$= g^{f(i) + (f'(i) + f''(i))\, e'}$$

$$= g^{r_e} \pmod p \quad (\text{모든 } P_l \in H \text{에 대하여})$$

4. 이제 각 $P_i \in H$는 집합 $\{\gamma_l \mid P_l \in H\}$와 Lagrange interpolation을 사용하면 공통의 비밀 정보 $t = r + (\sigma + s_{PG}) e' = f(0) + (f'(0) + f''(0)) e' \pmod q$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.

결 론

우리는 본 논문에서 두 가지 새로운 형태의 대리 서명 방식을 제안하였다. 하나는 보증 부분 위임 대리 서명방식으로 Mambo가 제안한 부분 위임과 Neuman의 보증 위임의 장점을 결합하였다. 이는 보증서를 검증하는 과정이 별도로 요구되지 않으므로 기존의 단순 보증서 위임에 의한 대리 서명방식 보다 계산 효율이 좋으며, 또한 보증서에 대리 서명을 할 수 있는 기간을 명시할 수 있으므로 부분 위임에 의한 서명 방식에서와 같이 위임의 철회를 위한 철회 과정이 필요하지 않은 장점이 있다.

다른 하나는 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. 그러므로 역치 위임은 대리 서명자에 의하여 서명이 남용될 가능성을 줄여준다. 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] 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, 1997, pp.223-232

[7] 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.

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

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

[10] 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.

[11] 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.

[12] 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.

[13] 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.

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

[15] 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.

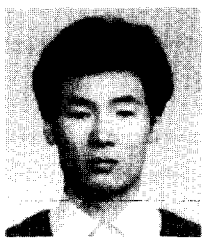
[16] C. Park and K. Kurosawa, "New ElGamal type threshold digital signature scheme," IEICE Trans. Fundamentals, vol.E79-A, no.1, 1996, pp.86-93.

□ 著者紹介

김 승 주

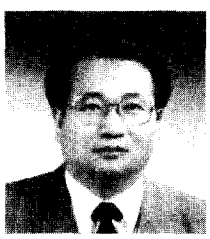
1994년 2월 성균관대학교 정보공학과 졸업(공학사)
1996년 2월 성균관대학교 대학원 정보공학과 졸업(공학석사)
1996년 3월 - 현재 성균관대학교 대학원 전기 · 전자 및 컴퓨터공학부 박사과정

※ URL : http//dosan.skku.ac.kr/~sjkim



\박 상 준

1984년 2월 한양대학교 수학과 졸업(이학사)
1986년 2월 한양대학교 대학원 수학과 졸업(이학박사)
1986년 1월 - 현재 한국전자통신연구원 책임연구원
1995년 3월 - 현재 성균관대학교 대학원 전기 · 전자 및 컴퓨터공학부 박사과정



원 동 호

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 3월 - 현재 성균관대학교 공과대학 전기 · 전자 및 컴퓨터공학부 교수
1991년 3월 - 한국통신정보보호학회 편집이사

※ 주관심분야 : 암호이론, 정보이론
URL : http//dosan.skku.ac.kr