情報保護學會論文誌
第15券 第2號, 2005. 4

RSA와 소인수 분해 문제에 기반한 대리서명 기법의 안전성 분석*

박 제 홍,[1†‡] 강 보 경,[2] 한 재 우[1]
[1]국가보안기술연구소, [2]한국과학기술원

Security analysis of proxy signature schemes based on RSA and integer factorization problems

Je Hong Park,[1†‡] Bo Gyeong Kang,[2] Jae Woo Han[1]
[1]NSRI, [2]KAIST

요 약

최근 Zhou, Cao 그리고 Lu는 강한 위조 불가능성을 만족하는 RSA와 소인수 분해 문제 기반의 세 가지 대리서명 기법을 제안하면서 각각의 대리서명 기법들이 랜덤 오라클 모델하에서 증명가능한 안전성을 제공한다는 주장을 하였다. 본 논문에서는 이 기법들이 원 서명자로부터 위임받지 않은 사용자도 유효한 대리서명을 생성할 수 있게 한다는 점을 보임으로써 대리서명이 만족해야 하는 기본적인 안전성을 만족하지 않는다는 것을 보인다.

ABSTRACT

Quite recently, Zhou, Lu and Cao proposed a proxy-protected signature scheme based on the RSA assumption and two proxy-protected schemes based on the hardness of integer factorization. They also provided a security proof for each signature scheme in the random oracle model. In this paper, we show that their schemes do not satisfy a security requirement necessary for proxy signature schemes. This results in generating proxy signatures without any permission from an original signer.

Keywords : *Proxy signature schemes, Security analysis, Public key cryptosystem*

Ⅰ. 서 론

대리서명 기법은 원 서명자와 대리서명자, 그리고 검증자들로 구성되며 원 서명자가 대리서명자에게 자신의 서명 권한을 안전하게 위임함으로써, 대리서명자가 메시지에 대한 서명을 생성할 수 있도록 하는 방식이다. 이러한 대리서명 기법의 개념은 1996년 Mambo, Usuda, 그리고 Okamoto에 의해 처음 소개되었고, 이후 다양한 기법들이 제안되고 있다.[1-6]

대리서명 기법은 그 위임 방법에 따라 전체위임 (full delegation), 부분위임 (partial delegatIon), 그리고 보증위임 (delegation by certificate (warrant))으로 나눌 수 있다[1,4,5]. 대리자 보호 대리서명 (proxy-protected signature)은 일종의 부분위임 대리서명 기법으로, 위임받은 대리서명자 이외에는 원 서명자라도 유효한 대리서명을 생성하는 것이 불가능한 방법이다. 최근의 대리서명 연구에 있어서 이러한 성질은 기본적으로 만족해야 할 안전성 중 하나로 인정받고 있으며 이를 강한 위

접수일 : 2004년 12월 7일 ; 채택일 : 2005년 3월 30일
† 주저자 : jhpark@etri.re.kr
‡ 교신저자 : jhpark@etri.re.kr

조 불가능성으로 정의하고 있다. 참고로 대리서명 기법이 만족해야 할 기본적인 안전성은 다음과 같다.[4]

- 검증 가능성 (Verifiability): 주어진 대리서명으로부터, 검증자는 서명된 메시지에 대한 원 서명자의 동의를 확인할 수 있다.
- 강한 위조 불가능성 (Strong unforgeability): 대리서명자를 제외한 누구도 유효한 대리서명을 생성할 수 없다.
- 강한 신원 확인성 (Strong identifiability): 누구나 주어진 대리서명으로부터 서명을 생성한 대리서명자의 신원을 확인할 수 있다.
- 강한 부인 방지성 (Strong undeniability): 대리서명자는 자신이 생성한 대리서명을 부인할 수 없다.
- 오용 방지 (Prevention of misuse): 대리서명키는 유효한 대리서명을 생성하는 것 이외의 용도로 사용될 수 없다. 대리서명키의 오용이 확인될 경우, 대리서명자의 책임이 정확하게 결정되어야 한다.

지금까지 제안된 거의 모든 대리서명 기법들은 위의 기본적인 안전성들을 각각 독립적으로 증명하였으며 이로 인하여 대리서명 기법에서 충분히 발생할 수 있는 복합적인 공격 모델에서의 안전성은 정확히 검증되지 못하였다.[6] 하지만 최근 Boldyreva, Palacio 그리고 Warinschi는 보증위임 대리서명에 대한 안전성 개념을 형식화하고 이 형식 모델에 맞춘 증명가능한 안전성을 가지는 기법들을 제안함으로써 이러한 문제점을 해결하고자 하였다.[4]

최근 Zhou, Cao 그리고 Lu는 RSA와 소인수 분해 문제에 기반한 세 가지 대리자 보호 대리서명 기법을 제안하고 랜덤 오라클 모델에서의 안전성 증명을 제시하였다.[7,8] 그러나 이들은 자신들이 제안한 대리서명 기법의 안전성 증명에 있어서 논문 [4]에서와 같이 전체적인 안전성 개념에 대한 형식화 없이 단지 일반적인 서명기법의 안전성 개념인 능동 선택 평문 공격에 대한 존재 위조불가 (existentIal unforgeable under the adaptive chosen message attack)에 따른 증명을 제시하였다. 이러한 일반적인 서명기법의 안전성을 대리서명 기법에서 맞춰보면 대리서명자가 생성한 서명에 대한 위조 불가능성과 부인 방지성에만 해당한다. 결국 이들이 제시한 증명은 대리자 보호라는 특정 성격에만 초점을 맞춘 것으로, 궁극적으로는 기존의 대리서명 기법들과 마찬가지로 안전성 요구조건 각각에 대한 증명을 제시한 것과 다를 바 없다. 본 논문에서는 이들이 제시한 세 가지 대리서명 기법들이 명확한 증명이 제시되지 않은 검증 가능성 측면에서 실제로 안전하지 않음을 보인다. 본 논문에서 제안하는 공격방법은 일종의 가장 공격 (Impersonating attack)[9]으로 유효한 대리서명이 주어졌을 때, 이를 이용하여 누구나 자신의 개인키로 원 서명자의 동의나 인증과는 상관없이 유효한 대리서명을 생성할 수 있음을 보여준다. 본 논문에서는 특히 [7]에서 제안된 대리서명 기법의 경우 유효한 대리서명이 없이도 누구나 대리서명을 생성할 수 있음을 보인다. 이러한 성질은 Zhou등이 제안한 기법들이 대리서명으로부터 원 서명자의 동의를 확인할 수 있어야 한다는 검증 가능성을 만족하지 않는다는 것을 보여주며 이는 강한 부인 방지성, 강한 신원 확인성, 그리고 오용 방지 측면에서도 취약하다는 것을 의미한다.

II. 세 가지 대리서명 기법

Zhou, Cao 그리고 Lu는 논문 [8]에서 RSA 기반과 Rabin 기반 대리서명 기법을 제안하였고 [7]에서는 변형된 형태의 Rabin 기반 대리서명 기법을 제안하였다. 이 대리서명 기법들의 전체적인 구조는 동일하다고 볼 수 있는데, 원 서명자가 대리서명자에게 위임장과 그에 대한 서명[1] (m_w,σ)을 전송하면, 대리서명자는 인증서 σ의 유효성을 확인한 후, σ를 대리서명키로 사용한다. 각 서명 기법들의 자세한 구조를 설명하기에 앞서 공통적으로 사용하는 기호를 나열하면 다음과 같다.

- U_o: 원 서명자
- U_p: 원 서명자로부터 위임받은 대리서명자
- U: 원 서명자로부터 위임받지 않은 사용자
- p, q: 비슷한 크기의 서로 다른 소수
- N: p와 q를 곱한 값, 즉 $N=pq$
- $\phi(N)$: Euler 함수, $\phi(pq)=(p-1)(q-1)$
- e, d: RSA의 암호화 지수와 복호화 지수, $ed \equiv 1 \bmod \phi(N)$
- m_w: 대리서명자 U_p의 위임장

1) 이하 인증서라 하자.

- m_U: U가 직접 생성한 위임장
- s_o: 위임장에 대한 인증서

2.1 RSA 기반 대리서명 기법

우선 RSA 기반의 공개키 기반구조 (RSA based Public Key Infrastructure (PKI))를 가정하며 각 사용자는 공개키 $(N=pq, e)$와 개인키 (p,q,d)를 가진다.

- 대리서명 준비과정: 원 서명자 U_o는 자신의 개인키 (p_o, q_o, d_o)와 공개키 (N_o, e_o)를 가지고 대리서명자 U_p는 자신의 개인키 (p_p, q_p, d_p)와 공개키 (N_p, e_p)를 가진다. 또한 $H_o: \{0,1\}^* \rightarrow Z_{N_o}$와 $H_p: \{0,1\}^* \times Z_{N_o} \rightarrow Z_{N_p}$를 각각 원 서명자와 대리서명자가 사용하는 안전한 해쉬함수로 한다.

- 대리서명 위임과정: 원 서명자 U_o의 서명 권한을 대리서명자 U_p에게 위임하기 위해 다음의 절차를 수행한다.
  1. U_o는 권한의 제한이나 유효 기간과 같은 대리 서명과 관련된 정보를 포함하는 위임장 m_w을 생성하고 이를 공개한다.
  2. U_o는 위임장 m_w을 다음과 같이 서명한다.

     $$s_o = H_o(m_w)^{d_o} \bmod N_o.$$

     그리고 (m_w, s_o)를 U_p에게 안전한 경로 (secure channel)로 전송한다.
  3. U_p는 다음의 식이 성립하는지 확인함으로써 이 서명을 검증한다.

     $$s_o^{e_o} \equiv H_o(m_w) \bmod N_o.$$

     만일 이 서명이 유효하다면, 인증서 s_o를 대리서명키로 사용한다.

- 대리서명 서명과정: 원 서명자 U_o를 대신해서 메시지 m을 서명하기 위해, U_p는 임의로 정수 $r \in Z_{N_o}$를 선택하고 다음을 계산한다.

$$R = r^{e_w} \bmod N_o,$$
$$r_1 = s_o \cdot r \bmod N,$$
$$r_2 = H_p(m,R)^{d_p} \bmod N_p.$$

메시지 m에 대한 대리서명은 $p\sigma = (r_1, r_2)$이다.

- 대리서명 검증과정: 메시지 m에 대한 대리서명 $p\sigma = (r_1, r_2)$을 검증하기 위해, 검증자는

$$R' = r_1^{e_w} \cdot H_o(m_w)^{-1} \bmod N_o \quad (1)$$

를 계산하고서 다음 식이 성립하는지 확인한다.

$$r_2^{e_p} \equiv H_p(m, R') \bmod N_p.$$

2.2 Rabin 기반 대리서명 기법

지금부터 설명하는 두 개의 대리서명 기법들은 소인수 분해 문제에 기반한 것들로 Rabin 서명 기법을 사용한다. 먼저 소인수 분해 문제의 어려움에 기반한 공개키 기반구조를 가정하자. 그러면 각 사용자는 개인키 (p,q)와 공개키 $(N=pq, a)$를 가진다. 여기서 p와 q는 임의로 생성된 큰 소수들로 $p \equiv q \equiv 3 (\bmod 4)$를 만족하며, a는 Jacobi symbol $\left(\frac{a}{N}\right) = -1$인 값이다.

- 대리서명 준비과정: 원 서명자 U_o의 개인키와 공개키는 각각 (p_o, q_o)와 (N_o, a_o)이며, 대리서명자 U_p의 개인키와 공개키는 각각 (p_p, q_p)와 (N_p, a_p)이다. 또한 $H_o: \{0,1\}^* \rightarrow Z_{N_o}$는 U_o가 사용하는 안전한 해쉬함수, 그리고 $H_p: \{0,1\}^* \times Z_{N_o} \rightarrow Z_{N_p}$는 U_p가 사용하는 안전한 해쉬함수라 하자.

- 대리서명 위임과정: 원 서명자 U_o의 서명 권한을 대리서명자 U_p에게 위임하기 위해 다음의 절차를 수행한다.
  1. U_o는 위임장 m_w을 생성하고 다음과 같이 서명한다.

$$c_1^o=\begin{cases}0, & \text{if}\left(\dfrac{H_o(m_w)}{N_o}\right)=1\\ 1, & \text{if}\left(\dfrac{H_o(m_w)}{N_o}\right)=-1\end{cases},$$

$$c_2^o=\begin{cases}0, & \text{if}\left(\dfrac{a_o^{c_1^o}\cdot H_o(m_w)}{p_o}\right)=1\\ 1, & \text{if}\left(\dfrac{a_o^{c_1^o}\cdot H_o(m_w)}{p_o}\right)=-1\end{cases},$$

$$s_o^2=(-1)^{c_2^o}\cdot a_o^{c_1^o}\cdot H_o(m_w)\ \bmod N_o.$$

위의 계산으로 얻어진 위임장과 그에 대한 인증서 (m_w, s_o, c_1^o, c_2^o)를 U_p에게 안전한 경로(secure channel)로 전송한다.

2. U_p는 다음의 식이 성립하는지 확인함으로써 이 서명을 검증한다.

$$s_o^2\equiv(-1)^{c_2^o}\cdot a_o^{c_1^o}\cdot H_o(m_w)\ \bmod N_o.$$

- 대리서명 서명과정: 원 서명자 U_o를 대신해서 메시지 m을 서명하기 위해, U_p는 임의로 정수 $r\in Z_{N_o}$를 선택하여 $R=r^2 \bmod N_o$를 계산하고 다음의 계산을 수행한다.

$$c_1^p=\begin{cases}0, & \text{if}\left(\dfrac{H_p(m,R)}{N_p}\right)=1\\ 1 & ,\text{if}\left(\dfrac{H_p(m,R)}{N_p}\right)=-1\end{cases},$$

$$c_2^p=\begin{cases}0, & \text{if}\left(\dfrac{a_p^{c_1^p}\cdot H_p(m,R)}{p_p}\right)=1\\ 1, & \text{if}\left(\dfrac{a_p^{c_1^p}\cdot H_p(m,R)}{p_p}\right)=-1\end{cases},$$

$$r_1=s_o\cdot r\ \bmod N_o,$$

$$r_2^2=(-1)^{c_2^p}\cdot a_p^{c_1^p}\cdot H_p(m,R)\ \bmod N_p.$$

이렇게 얻어진 메시지 m에 대한 대리서명은 $p\sigma=(c_1^o, c_2^o, c_1^p, c_2^p, r_1, r_2)$이다.

- 대리서명 검증과정: 메시지 m에 대한 대리서명 $p\sigma=(c_1^o, c_2^o, c_1^p, c_2^p, r_1, r_2)$을 검증하기 위해, 검증자는 다음을 계산한다.

$$R_1=r_1^2 \bmod N_o,$$

$$R_2=r_2^2 \bmod N_p,$$

$$W=(-1)^{c_2^o}\cdot a_o^{c_1^o}\cdot H_o(m_w)\ \bmod N_o.$$

이 값들로부터 서명에 사용된 난수요소를 다음과 같이 계산한다.

$$R'=R_1\cdot W^{-1} \bmod N_o. \qquad (2)$$

이후 다음 식이 성립하는지 확인한다.

$$R_2\equiv(-1)^{c_2^p}\cdot a_p^{c_1^p}\cdot H_p(m,R')\ \bmod N_p.$$

2.3 변형된 Rabin 기반 대리서명 기법

서명기법의 기반구조 및 대리서명 준비과정과 대리서명 위임과정은 2절의 알고리즘과 동일하다. 그러므로 여기서는 대리서명 생성과 검증 알고리즘에 대해서만 정리하도록 한다.

- 대리서명 서명과정: 원 서명자 U_o를 대신해서 메시지 m을 서명하기 위해, U_p는 임의로 정수 $t\in Z_{N_oN_p}$를 선택하고 $T\equiv t^2 \bmod N_oN_p$를 계산한 후 다음의 절차를 수행한다.

$$c_1^p=\begin{cases}0, & \text{if}\left(\dfrac{H_p(m,T)}{N_p}\right)=1\\ 1, & \text{if}\left(\dfrac{H_p(m,T)}{N_p}\right)=-1\end{cases},$$

$$c_2^p=\begin{cases}0, & \text{if}\left(\dfrac{a_p^{c_1^p}\cdot H_p(m,T)}{p_p}\right)=1\\ 1, & \text{if}\left(\dfrac{a_p^{c_1^p}\cdot H_p(m,T)}{p_p}\right)=-1\end{cases},$$

$$s_p^2=(-1)^{c_2^p}\cdot a_p^{c_1^p}\cdot H_p(m,T)\ \bmod N_p,$$

$$r_o=s_o\cdot t\ \bmod N_o, \qquad r_p=s_p\cdot t\ \bmod N_p.$$

이렇게 얻어진 메시지 m에 대한 대리서명은 $p\sigma=(m,T,r_o,r_p,c_1^o,c_2^o,c_1^p,c_2^p)$이다.

- 대리서명 검증과정: 메시지 m에 대한 대리서명 $p\sigma=(m,T,r_o,r_p,c_1^o,c_2^o,c_1^p,c_2^p)$을 검증하기 위해, 검증자는 다음을 계산한다.

$$R_o=r_o^2 \bmod N_o,$$
$$R_p=r_p^2 \bmod N_p,$$
$$S_o=(-1)^{c_2^o}\cdot a_o^{c_1^o}\cdot H_o(m_w) \bmod N_o,$$
$$S_p=(-1)^{c_2^p}\cdot a_p^{c_1^p}\cdot H_p(m,T) \bmod N_p,$$
$$T_o=R_o\cdot S_o^{-1}\equiv t^2 \bmod N_o,$$
$$T_p=R_p\cdot S_p^{-1}\equiv t^2 \bmod N_p.$$

검증자는 중국인의 나머지 정리 (Chinese Remainder Theorem)를 이용하여

$$T'\equiv T_o \bmod N_o, \quad T'\equiv T_p \bmod N_p$$

를 계산하고 다음을 확인한다.

$$T\equiv T' \bmod N_oN_p.$$

III. 안전성 분석

본 절에서는 II장에서 제시한 세 가지 대리서명 기법들이 모두 안전하지 않다는 것을 보인다. 이러한 문제점은 이들 대리서명 기법들이 원 서명자가 생성한 인증서 자체를 대리서명키로 사용하는 구조에서 발생한다. 논문 [8]에서 제시한 두 가지 기법들에 대해서는 대리서명자로부터 생성된 대리서명이 주어진 경우, 이를 이용하여 위임을 받지 않은 사용자가 유효한 대리서명을 생성할 수 있음을 보이고, 논문 [7]에서 제시한 기법의 경우 사전에 획득한 대리서명 없이 누구나 유효한 대리서명을 생성할 수 있음을 보인다.

3.1 논문 [8] 서명 기법에 대한 공격

먼저 RSA 기반 대리서명 기법을 살펴보자. 원 서명자 U_o로부터 위임받은 대리서명자를 U_p라 하고 위임받지 않은 사용자를 U라 하자. U_o와 U_p의 공개키/개인키 쌍은 서명 기법 설명에서 제시한 기호를 사용하며 U의 키 쌍은 각각 (p,q,d)와 (N,e)라 하고 $H_U:\{0,1\}^*\times Z_{N_o}\rightarrow Z_N$를 자신이 사용하는 해쉬 함수라 하자. 만일 U가 U_p에 의해 생성된 메시지 m에 대한 대리서명 $p\sigma=(r_1,r_2)$를 받았을 때, 일반성을 잃지 않고 U_p에 대한 위임장 m_w도 같이 얻는다고 가정할 수 있다. 그러면 U는 주어진 서명에서 난수요소 R를 식 (1)을 사용하여 복구할 수 있다.

$$R=r_1^{c_w}\cdot H_o(m_w)^{-1} \bmod N_o.$$

다음으로 U는 자신의 공개키가 포함되어 있는 새로운 위임장 m_U을 생성하고 새로운 메시지 m'에 대해 다음을 계산한다.

$$R_U=R\cdot H_o(m_w)\cdot H_o(m_U)^{-1} \bmod N_o,$$
$$r'_2=H_U(m',R_U)^d \bmod N.$$

그러면 메시지 m'에 대한 위조 대리서명 (r_1,r_2')은 다음의 식을 만족하기 때문에 유효한 것으로 검증된다.

$$r_1^{c_w}\cdot H_o(m_U)^{-1}\equiv R\cdot H_o(m_w)\cdot H_o(m_U)^{-1}$$
$$\equiv R_U \bmod N_o.$$

즉, U로부터 위임장 m_U와 메시지 m', 그리고 대리서명 (r_1,r'_2)을 받은 검증자는 먼저 $r_1^{c_w}\cdot H_o(m_U)^{-1} \bmod N_o$를 계산하여 난수요소 R_U를 찾고 $r'^e_2 \bmod N$과 $H_U(m',R_U) \bmod N$이 서로 같은지 비교한다. 물론 $r'_2=H_U(m',R_U)^d \bmod N$ 이기 때문에 서로 같음을 확인할 수 있고 결국 이 대리서명이 유효하다는 검증을 하게 된다.

다음은 Rabin 기반 대리서명 기법을 살펴보자. 이 기법에 대한 공격 방법은 RSA 기반 대리서명 기법에 대한 공격과 매우 유사하다. 그러므로 여기서는 핵심적인 부분에 대해서만 간략하게 소개하도록 한다. 먼저 위임 받지 않은 사용자 U에 대한 개인키와 공개키를 각각 (p,q)와 (N,a)라 하자. 만일

U가 U_p에 의해 생성된 메시지 m에 대한 대리서명 $p\sigma=(c_1^o, c_2^o, c_1^p, c_2^p, r_1, r_2)$을 안다면, U는 우선 식 (2)을 이용하여 commitment R'을 계산할 수 있다. 다음으로 U는 자신의 공개키 정보가 들어간 새로운 위임장 m_U을 생성하고 다음을 계산한다.

$$R_U = R' \cdot H_o(m_w) \cdot H_o(m_U)^{-1} \bmod N_o.$$

이어서 새로운 메시지 m'에 대한 해쉬값 $H_U(m', R_U)$을 계산한 후, 대리서명 알고리즘의 절차에 따라 c_1^p, c_2^p 그리고 r_2대신 사용할 c_1, c_2 그리고 r'_2를 계산할 수 있다. 그러면 메시지 m'에 대한 위조서명 $(c_1^o, c_2^o, c_1, c_2, r_1, r'_2)$은 다음의 식을 만족하기 때문에 유효한 것으로 판정된다.

$$R_1 \cdot W^{-1} \equiv H_o(m_w) \cdot R' \cdot H_o(m_U)^{-1} \equiv R_U \bmod N_o.$$

이를 자세히 살펴보면, 앞의 RSA 기반의 대리서명 기법과 마찬가지로 공격자 U로부터 위임장 m_U와 메시지 m', 그리고 대리서명 $(c_1^o, c_2^o, c_1, c_2, r_1, r'_2)$을 받은 검증자는 먼저

$$R_1 = r_1^2 \bmod N_o \text{ 와}$$
$$W = (-1)^{c_2^o} \cdot a^{c_1^o} \cdot H_o(m_U) \bmod N_o$$

를 계산하여

$$R_U = R_1 \cdot W^{-1} \bmod N_o$$

를 얻는다. 위조서명의 생성 과정에서

$$r'^2_2 \equiv (-1)^{c_2} \cdot a^{c_1} \cdot H_U(m', R_U) \bmod N$$

인 r'_2, c_1, c_2를 계산하였으므로 검증자는

$$R_2 \equiv (-1)^{c_2} \cdot a^{c_1} \cdot H_U(m', R_U) \bmod N$$

임을 확인하게 된다.

3.2 논문 [7]의 서명 기법에 대한 공격

먼저 U는 자신의 공개키가 포함되어 있는 새로운 위임장 m_U를 생성하고 임의로 선택한 $A \in Z_{N_o}$에 대해, $r_o \equiv A \bmod N_o$라 하자. 그리고 Jacobi symbol $\left(\frac{H_o(m_U)}{N_o}\right)$에 따라 c_1을 다음과 같이 정하자.

$$c_1 = \begin{cases} 0, & \text{if} \left(\frac{H_o(m_U)}{N_o}\right) = 1 \\ 1, & \text{if} \left(\frac{H_o(m_U)}{N_o}\right) = -1 \end{cases}$$

다음으로, U는 임의의 값 $Q \in Z_N$를 선택하고, 임의의 값 $c_2 \in \{0,1\}$에 대해

$$S_o = (-1)^{c_2} \cdot a_o^{c_1} \cdot H_o(m_U) \bmod N_o$$

를 계산하고, 다음 값들을 정하자.

$$T_o := \equiv r_o^2 \cdot S_o^{-1} \bmod N_o, \quad T_U := \equiv Q^2 \bmod N.$$

중국인의 나머지 정리를 사용하여 다음을 만족하는 commitment $T^* \bmod N_o N$를 찾을 수 있다.

$$T^* \equiv T_o \bmod N_o, \quad T^* \equiv T_U \bmod N.$$

이 값을 이용하여 새로운 메시지 m'에 대한 해쉬값 $H(m', T^*)$을 계산한 후, (c_1^U, c_2^U, s_U, r_U)를 다음과 같이 계산한다.

$$c_1^U = \begin{cases} 0, & \text{if} \left(\frac{H(m', T^*)}{N}\right) = 1 \\ 1, & \text{if} \left(\frac{H(m', T^*)}{N}\right) = -1 \end{cases},$$

$$c_2^U = \begin{cases} 0, & \text{if} \left(\frac{a^{c_1^U} \cdot H(m', T^*)}{p}\right) = 1 \\ 1, & \text{if} \left(\frac{a^{c_1^U} \cdot H(m', T^*)}{p}\right) = -1 \end{cases},$$

$$s_U^2 = (-1)^{c_2^U} \cdot a^{c_1^U} \cdot H(m', T^*) \bmod N,$$
$$r_U = s_U \cdot Q \bmod N.$$

이러한 계산을 통해 새로운 메시지 m'에 대한 대

리서명 $p\sigma' = (T^*, r_o, r_U, c_1, c_2, c_1^U, c_2^U)$을 출력한다. 이 서명을 받은 검증자는

$$R_o = r_o^2 \equiv A^2 \bmod N_o,$$
$$R_U = r_U^2 \equiv s_U^2 \cdot Q^2 \bmod N,$$
$$S_o = (-1)^{c_2} \cdot a_o^{c_1} \cdot H_o(m_U) \bmod N_o,$$
$$S_U = (-1)^{c_2^U} \cdot a^{c_1^U} \cdot H(m', T^*) \bmod N,$$

를 계산하고 다음 식을 만족하는 $X \bmod N_o N$을 찾는다.

$$X \equiv R_o \cdot S_o^{-1} (\equiv T_o) \bmod N_o,$$
$$X \equiv R_U \cdot S_U^{-1} \equiv Q^2 (\equiv T_U) \bmod N.$$

그러면 $X \equiv T^* \bmod N_o N$을 만족하기 때문에, $p\sigma'$을 유효한 m'에 대한 대리서명으로 검증한다.

3.3 공격 방법에 대한 분석

앞 소절에서 제시한 공격 방법들은 결국 대리서명키 s_o가 실제 대리서명자의 서명절차에서 제 역할을 수행하지 못하기 때문에 발생한다. 대리서명 단계에서 원 서명자의 인증서인 s_o는 단지 난수요소 r을 숨기기 위한 용도로만 사용되는데, 문제는 실제 서명 생성에 필요한 난수요소의 역할은 commitment R이 담당하며, 이 값은 대리서명 검증단계의 절차로부터 쉽게 얻어질 수 있는 것이다. 앞의 대리서명 기법에서는 인증서가 직접 대리서명키로 사용되기 때문에 검증자에게 공개되지 않고 결국 검증자는 위임장에 대한 직접적인 검증을 할 수 없게 된다. 그러므로 위임받지 않은 사용자 U는 자신의 위임장을 스스로 생성해서 다른 commitment R_U를 만들어 내고 이를 이용한 자신의 대리서명을 생성할 수 있다. 이 대리서명을 받은 검증자는 원 서명자의 정보만으로 R_U를 복구한 다음 위조된 위임장 m_U에 기재된 대리서명자의 정보를 이용하여 서명의 유효성을 검증하게 된다. 또한 위임받은 대리서명자 U_p도 이러한 공격방법을 이용하면 위임장을 위조하여 사용할 수 있다. 이는 권한의 오용 방지 측면에서의 취약성을 나타낸다.

이러한 취약성을 제거하기 위한 기본적인 방법은 검증자가 원 서명자의 인증서의 유효성을 독립적으로 확인하는 것이다. 이를 위해서는 대리서명자가 인증서를 검증자에게 서명과 함께 전송해야 하기 때문에 위의 구조와는 다른 형태의 대리서명키를 사용해야 한다. 일반적인 보증위임 대리서명 기법에서처럼 대리서명자 자신의 개인키를 대리서명키로 이용하면 위임장과 인증서 (m_w, s_o)는 대리서명과 함께 검증자에게 전달될 수 있다. 대리서명을 받은 검증자는 먼저 인증서를 검증한 후 위임장에 명시되어 있는 대리서명자의 공개키로 대리서명의 유효성을 검증할 필요가 있으며 서명된 메시지가 위임장에 명시된 제한조건에 부합하는지 확인해야 한다.

서론에서 언급한 바와 같이 위 대리서명 기법들을 제안한 논문에서는 대리서명 기법이 만족해야할 기본적인 안전성 조건을 전체적으로 고려하지 않고 단지 강한 위조 불가능성에 대한 안전성 증명만으로 이 기법들이 증명가능한 안전성을 가진다고 주장하였다. 하지만 주어진 대리서명 기법이 진정한 의미에서 안전하다는 것을 증명하기 위해서는, 이 기법에서 발생할 수 있는 다양한 공격들을 형식 모델로 정립한 후에 이에 대한 안전성을 측정, 증명하여야 할 것이다.

V. 결 론

본 논문에서는, Zhou, Cao 그리고 Lu가 제안한 세 가지 대리서명 기법에서 위임받지 않은 사용자가 원 서명자의 대리서명을 생성할 수 있는 공격방법을 제시하여 이 대리서명 기법들이 안전하지 않음을 보였다. 이러한 결과를 통해 볼 때, 암호 기법에서 부분적인 성질에 대한 안전성 증명만으로는 기법의 전체적인 안전성을 보장할 수 없다는 것을 유의해야 한다.

참 고 문 헌

[1] 김승주, 박상준, 원동호, "보증 부분 위임과 역치 위임에 의한 대리 서명방식," 정보보호학회논문지, 8(2), pp. 69-81, 1998.

[2] 이정연, 천정희, 김태성, 진승헌, "Bilinear 함수를 이용한 ID 기반 대리서명 기법," 정보보호학회논문지, 13(2), pp. 3-11, 2003.

[3] 박희운, 이임영, "이동 통신에서 적용 가능한 수신자 지정 대리 서명 방식," 정보보호학회논문지, 11(2), pp. 18-27, 2001.
[4] A. Boldyreva, A. Palacio, B. Warinschi, "Secure proxy signature schemes for delegation of signing rights," *Cryptology ePrint Archive*, Report 2003/096.
[5] S. Kim, S. Park, D. Won, "Proxy signatures, revisited," *Information and Communication Security - ICICS'97*, Lecture Notes in Comput. Sci. vol. 1334, pp. 223-232, 1997.
[6] J.-Y. Lee, J.H. Cheon, S. Kim, "An analysis of proxy signatures: Is a secure channel necessary?" *Topics in Cryptology - CTRSA 2003*, Lecture Notes in Comput. Sci. vol. 2612, pp. 68-79, 2003.
[7] R. Lu, Z. Cao, Y. Zhou, "A simple efficient proxy-protected signature scheme based on factoring," *Comp. Stand. Inter.*, withdrawn, 2004.
[8] Y. Zhou, Z. Cao, R. Lu, "Provably secure proxy-protected signature schemes based on factoring," *Appl. Math. Comput.* 164(1), pp. 83-98, 2005.
[9] G. Wang, F. Bao, J. Zhou, R.H. Deng, "Security analysis of some proxy signatures," *Information Security and Cryptology - ICISC 2003*, Lecture Notes in Comput. Sci. vol. 2971, pp. 305-319, 2004.

〈著者紹介〉

박 제 홍 (Je Hong Park) 정회원
1998년 2월: 경북대학교 수학과 졸업
2000년 2월: 한국과학기술원 수학과 석사
2004년 2월: 한국과학기술원 수학과 박사
2004년 3월~현재: 국가보안기술연구소 연구원
〈관심분야〉 암호론, 정수론

강 보 경 (Bo Gyeong Kang) 학생회원
1999년 8월: 서울대학교 수학교육학과 졸업
2001년 8월: 한국과학기술원 수학과 석사
2001년 9월~현재: 한국과학기술원 수학과 박사과정
2004년 9월~현재: Visiting Researcher, Univ. of Maryland at College Park
〈관심분야〉 암호론, 타원곡선, Complexity theory

한 재 우 (Jae Woo Han) 정회원
1991년 2월: 서강대학교 수학과 졸업
1993년 2월: 한국과학기술원 수학과 석사
1999년 8월: 한국과학기술원 수학과 박사
1999년 7월~2000년 1월: 한국전자통신연구원 선임연구원
2000년 1월~현재: 국가보안기술연구소 선임연구원
〈관심분야〉 암호 프로토콜, 스트림 암호, 매듭이론