情報保護學會論文誌
第13券 第2號, 2003. 4

Bilinear 함수를 이용한 ID 기반 대리서명 기법

이 정 연*, 천 정 희**, 김 태 성***, 진 승 헌***

ID-based Proxy Signature Scheme from the Bilinear Map

Jung-Yeun Lee*, Jung Hee Cheon**, Tae-sung Kim***, Seung-hun Jin***

요 약

대리서명은 원서명자가 대리인에게 서명 권한을 위임하여 대신 서명하게 하는 변형된 전자서명이다. 본 논문에서는 bilinear 함수를 이용한 ID 기반 인증 모델에서의 대리서명 기법을 제안한다. 기존에 제안된 ID 기반 인증 모델에서의 대리서명 기법은 대리인에 의한 오남용을 막을 수 없고, ID 기반 인증 모델에서의 대리서명임에도 불구하고 공개키 인증서가 필요하다[1]. 하지만 우리가 제한하는 기법은 대리인의 서명권한을 규정한 위임장을 대리서명에 삽입함으로서 대리인에 의한 서명 권한의 오남용을 막을 수 있을 뿐만 아니라 공개키 인증서도 필요 없다. 효율성 측면에서, 제안하는 대리서명 기법은 서명 권한 위임 시 보안채널 설정의 필요성을 제거함으로써 기존의 대리서명보다 효율성을 훨씬 개선 할 수 있으며, ID 기반 인증모델에서의 공개키 습득과정의 단순화를 통한 효율성 향상이 가능하다.

ABSTRACT

Proxy signatures are signature schemes in which an original signer delegates her signing capability to a proxy entity, who signs a message on behalf of the original signer. In this paper we propose the ID-based proxy signature schemes using a bilinear map. In the previous ID-based proxy signature scheme, the proxy signer can misuse the right of the signing capacity and the public key directory is required. However, by inserting the warrant information such as the identity of the proxy signer and the limit of the signing capacity to the proxy signature, our scheme can prevent the misuse of the proxy key pair by the proxy signer and does not require a public key certificate. Furthermore, our scheme dose not need a secure channel to deliver the warrant. Consequently, the proposed scheme is more efficient and useful than the previous proxy signature schemes.

Keyword : *대리서명, 원서명자, 대리인, bilinear 함수, ID 기반 인증모델*

Ⅰ. 서 론

기업의 대표는 각종 문서에 서명을 하는 일 뿐만 아니라 많은 할 일이 있다. 너무 많은 일로 인해 필요한 서류에 제때 서명을 하지 못하거나 타 지역으로의 출장이나 온라인 상의 문제로 인해 서명을 할 수 없는 상황은 빈번하게 일어날 수 있다. 그럼에도 불구하고 대표로서 반드시 서명을 해야 하는 계약서나 사내 문서가 있을 수 있다. 이런 상황에 대한 해결책으로 그는 하급 직원에게 일부 문서에 대해 서명 할 수 있는 권한을 위임하고 하급직원이 대표를 대신하여 서명하는 것이다.

Mambo 등에 의해 처음 소개된 대리서명 기법은 위임의 형태에 따라 전체 위임과 부분 위임 그리고

* 한국정보통신대학원대학교(ICU) 공학부 국제정보보호연구소(IRIS)(bushman@icu.ac.kr)
** 서울대학교(SNU) 자연과학대학 수리과학부(jhcheon@math.snu.ac.kr)
*** 한국전자통신연구원(ETRI) 정보보호연구본부 인증기반연구팀({taesung, jinsh}@etri.re.kr)

위임장에 의한 위임으로 분류된다(MUO 대리서명 기법)[2]. 여기에서 부분 위임은 원서명자의 대리서명 생성 능력에 따라 대리인만이 대리서명을 생성할 수 있는 대리인 보호 대리서명과 원서명자와 대리인 모두 대리서명을 생성할 수 있는 대리인 비보호 대리서명으로 나뉜다. 이 후 김승주, 박상준, 원동호는 위임장의 내용을 직접 대리서명에 삽입시킴으로서 대리인에 의한 서명 능력의 오남용을 방지하는 기법이 소개하였다(KPW 대리서명 기법)[3].

기본적인 대리서명 생성 방법은 다음과 같다. 먼저 원서명자가 대리인의 신상정보(ID등)를 포함한 대리서명 권한을 규정한 위임장에 공개키 시스템에서 사용하는 개인키를 이용하여 서명을 생성하고 위임장과 서명 값을 대리인에게 전달한다. 그러면 대리인은 서명 값과 자신의 개인키를 이용하여 대리서명에 사용될 대리서명 키 쌍을 생성하고 그 중 개인키를 이용하여 대리서명을 생성한다. 검증자는 원서명자와 대리인의 공개키를 이용하여 대리서명을 검증한다. 여기에서 검증자는 위임장의 내용과 대리서명된 문서의 내용을 검토하여 대리인의 위임된 권한의 행사에 대한 유효성을 확인한다. 만약 이 두 가지 검증 절차가 모두 유효하면 검증자는 검증과정에서 사용된 원서명자의 공개키를 통해 대리서명에 대한 원서명자의 동의를 확인할 수 있고, 또한 위임된 권한의 오남용도 막을 수 있을 것이다. 이와 같은 대리서명이 갖추어야 할 보안 요구사항은 다음과 같다[2,4].

(1) **검증 가능성:** 대리서명으로부터 검증자는 권한위임에 대한 원서명자의 동의를 확인할 수 있어야 한다.
(2) **강한 위조 방지:** 지명된 대리인만이 유효한 대리서명을 생성할 수 있어야 한다. 즉, 원서명자와 제 3자는 유효한 지명된 대리인을 가장하여 유효한 대리서명을 생성할 수 없어야 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.

본 논문에서는 ID 기반 인증 모델에서의 대리서명 기법을 제안한다. 1984년에 Shamir가 소개한 이 모델은 각 사용자의 ID(전자우편 주소 등)를 공개키로 사용함으로서 서명의 검증이나 암호화 과정에서 필요한 공개키의 습득과정을 단순화한 인증모델이다[5]. 이 모델의 단점으로는 사용자의 ID에 대응하는 개인키를 생성하는 개인키 생성자(PKG)가 모든 사용자의 개인키를 알고 있기 때문에 이 모델의 안전성을 개인키 생성자의 도덕성에 의존해야 한다는 것이 지적되고 있다. 이런 단점에도 불구하고 대리서명은 검증 과정에서 검증자가 원서명자와 대리인의 공개키를 모두 필요로 하기 때문에 이 인증모델의 사용은 효율성을 향상시키는데 큰 역할을 할 것이다.

기존의 ID 기반 대리서명 기법은 서명 기법을 직접 사용하여 대리서명을 생성하는 기법이다(DQ 서명 기법)[1]. 그들의 서명 기법은 사용자가 서명할 수 있는 횟수를 제한하는 'bounded-life span' 서명 기법인데, 그 제한된 횟수의 일부분을 대리인이 사용할 수 있도록 함으로서 대리서명을 생성하는 방법이다. 여기에서 원서명자가 대리인에게 전달하는 위임장은 대리인의 신상정보나 서명권한 사용의 한계에 대한 정보를 담고 있지 않기 때문에 대리인에 의한 서명권한의 오남용이나 위임된 권한을 제3자에게 전달하는 것을 막을 수 없다. 그렇기 때문에 위임장의 전달은 원서명자와 대리인 사이의 보안채널을 이용하여 전달되어야 한다. 무엇보다 이 기법이 가지는 가장 큰 단점은 ID 기반 모델에서의 대리서명 기법임에도 불구하고 검증자가 대리서명의 검증 과정에서 원서명자가 지급한 위임장의 유효성을 확인하기 위해 원서명자가 제공하는 위임장에 대한 인증서를 온라인 상태로 확인해야 한다는 것이다.

이에 반해 우리가 제안하는 ID 기반 대리서명 기법은 안전성이 증명된 ID 기반 서명기법[6]를 기존 인증서 기반 인증모델에서의 대리서명기법에 적용한 것으로, 위임장을 대리서명에 삽입함으로서 기존 ID 기반 대리서명 기법이 가지는 단점들을 모두 극복할 수 있었다. 또한 지금까지 제안되고 있는 대리서명 기법들이 위임장 전송 시 보안채널을 설정해야 하는 어려움이 있었으나 우리의 대리서명 기술은 이런 보안 채널 설정의 필요성을 제거했기 때문에 효율성에 있어서 기존 대리서명 기술들보다 훨씬 뛰어나다고 할 수 있다.

이 논문의 나머지 부분은 다음과 같이 구성되어 있다. 먼저 2장에서는 기존에 발표된 대리서명 기법을 소개하고 각 기법들이 가지는 단점을 정리하였다.

3장에서 ID 기반 대리서명 기법을 제안하고 4장과 5장에서 각각 제안하는 기법의 안전성과 기존 기법들과의 비교를 다룬다. 마지막으로 6장에서 결론을 정리한다.

Ⅱ. 기존 대리서명 기법

이 장에서는 지금까지 제안된 인증서 기반 대리인 보호 대리서명 기법인 MUO 기법과 KPW 기법을 정리하고, ID 기반 서명 기법 중 대리서명의 기능을 제공할 수 있는 DQ 서명 기법 을 소개한다. 그리고 각 기법이 제공하는 기능과 문제점을 정리한다. 이 논문을 통해 다음의 내용은 중복하여 정의하지 않고 사용한다.

(1) p와 q는 매우 큰 소수이며, q는 $p-1$의 약수이다. p는 적어도 512비트 이상이어야 하며, q는 160비트 이상이어야 한다.
(2) g는 곱셈 $(Z_p^*,*)$ 의 위수가 q인 부분군의 생성원이다.
(3) $h()$는 충돌 회피 해쉬 함수이다.
(4) m_d는 대리인에 대한 정보와 위임되는 권한에 대한 정보를 담은 문서이다.
(5) m_w는 m_d와 이에 대한 원서명자의 서명을 권한 위임에 필요한 내용 일체를 말한다.
(6) m_p는 m_d에서 제한하고 있는 대리인의 서명 권한에 의해 정당하게 서명될 수 있는 문서이다.
(7) Alice는 공개키 암호 시스템에서 사용되는 키 쌍 $(x_A, y_A(=g^{x_A} \bmod p))$을 소유하고 있는 원서명자이며 Bob은 키 $(x_B, y_B(=g^{x_B} \bmod p))$ 을 소유하고 있는 대리인이다.

2.1 MUO 대리서명 기법[2]

〔1단계〕 위임장 생성 및 전송

원서명자 Alice는 임의의 난수 $k \in Z_q^*$를 생성하고 $K=g^k \bmod p$를 계산한다. 그후 $s_A=(x_A+k\cdot K) \bmod q$를 구하고 (s_A, K)를 위임장 m_w로 정의한다. Alice는 위임장 m_w를 대리인 Bob에게 보안채널을 이용하여 안전하게 전송한다.

〔2단계〕 위임장 검증과 대리서명 키 생성

Bob은 먼저 $g^{s_A}=y_A\cdot K^K \bmod p$ 인지를 확인하여 위임장의 진위를 파악하고 유효하다면 다음과 같이 대리서명을 위한 개인키를 생성한다.

$$x_P=s_A+x_B\cdot y_B.$$

〔3단계〕 대리서명 생성

Bob은 문서 m_p에 대해 대리서명을 생성하기 위해 개인키로 x_P를 사용하고 이산대수 문제의 어려움에 기반한 서명기법 ($Sign_\sigma$)을 활용하여 대리서명 σ를 생성한다.

$$\sigma=(m_p,\ Sign_\sigma(m_p), K, y_A, y_B).$$

〔4단계〕 대리서명 검증

대리서명 σ를 검증하기 위해 먼저 검증자는 대리서명 생성에 사용된 개인키 (x_P)에 대응하는 공개키를 생성한다.

$$y_P=g^{x_P}=y_A\cdot K^K\cdot y_B^{y_B}.$$

그 후 대리서명 생성과정에서 사용된 서명 기법의 검증과정을 수행하여 대리서명의 유효성을 확인한다.

〔문제점〕

이 기법이 가지는 단점으로 다음과 같은 사항들이 지적되었다[4].

(1) 위임되는 권한의 사용에 대한 제약이 없다. 즉, 대리인에 의한 오남용이 가능하다.
(2) 대리인이 위임장을 원서명자의 동의 없이 제 3자에게 전달하여 대리서명을 생성할 수 있다.
(3) 위임장 전송 시 보안채널을 확보 해야한다. 만약 보안 채널이 확보되지 못하면 위 두 번째 문제점을 이용하여 m_w를 확보한 공격자에 의해 서명권한이 사용될 수 있기 때문이다.

2.2 KPW 대리서명 기법[3]

김승주 등은 위 대리서명 기법의 문제점들을 극복하기 위해 대리인과 위임되는 권한에 대한 정보를 담은 m_d를 대리서명에 삽입함으로서 위임된 권한의 오남용이나 제3자에게로의 서명 권한 전달을 막을 수 있는 방법을 제시하였다.

〔1단계〕 위임장 생성 및 전송

원서명자 Alice는 대리인에 대한 정보와 위임되는 권한에 대한 정보를 담은 m_d에 Schnorr 서명기법을 이용하여 서명을 생성한다. 자세히 살펴보면, Alice는 임의의 난수 k_A를 생성하고 $r_A = g^{k_A} \bmod p$를 계산한 후 서명 값 s_A를 다음과 같이 생성한다.

$$s_A = k_A + x_A \cdot h(m_d, r_A).$$

위임장 m_w을 (m_d, s_A, r_A)로 정의하고 보안 채널을 이용하여 대리인에게 전달한다.

〔2단계〕 위임장 검증과 대리서명 키 생성

대리인은 m_w가 유효한 위임장인지를 Schnorr 서명 기법의 검증 과정을 통해 확인하고, 유효하면 그것을 이용하여 다음과 같이 대리서명을 위한 개인키 (x_P)를 생성한다.

$$x_P = h(m_d, r_A) \cdot x_B + s_A.$$

〔3단계〕 대리서명 생성

대리인 Bob은 m_p에 대리서명을 생성하기 위해 안전성을 이산대수 문제의 어려움에 바탕을 둔 서명 기법을 이용하여 x_P로 서명한다. 여기에서는 Bob이 Schnorr 서명 방법을 이용하여 서명 (s_P, r_P)을 생성한다고 하자. 서명과정이 끝나면 Bob은 다음의 수열을 문서 m_P에 대한 대리서명으로 정의한다.

$$(m_P, r_P, s_P, m_w)$$

〔4단계〕 대리서명 검증

대리서명의 유효성을 검증하기 위해 먼저 대리서명을 위한 개인키 (x_P)에 대응하는 공개키를 다음과 같이 생성하여 대리서명을 검증한다.

$$y_P = g^{x_P} = (y_A \cdot y_B)^{h(m_d, r_A)} \cdot r_A.$$

〔문제점〕

이 대리서명 기법의 단점으로는 대리서명 내에 원서명자와 대리인의 역할이 동일하기 때문에 m_d에 그들의 역할을 분명히 하지 않는다면 그들의 역할이 바뀔 수 있다는 것이다.

2.3 DQ 서명 기법을 이용한 ID 기반 대리서명[1]

Oliver Delos와 Jean-Jacques Quisquater는 서명하는 횟수를 제한할 수 있는 ID 기반 서명 기법을 제안하였다[1]. 그리고 제한된 서명횟수의 일부를 대리인이 수행할 수 있는 방법을 소개하였다. 이 장에서는 그들의 서명 기법을 소개하고 제안하는 대리서명 방법을 정리한다.

ID 기반 인증 모델에서는 각 사용자의 ID에 대응하는 개인키를 생성해 주는 신뢰기관의 구축이 필요하다. 따라서 ID 기반 서명 기법은 시스템 파라미터와 각 사용자의 개인키를 생성하는 초기화 과정과 그것들을 이용하여 서명을 생성 및 검증하는 과정으로 구성되어 있다.

2.3.1. 초기화

사용자의 ID를 I*라고 하고 이에 대응하는 공개키를 J라고 하자. 여기에서 I*로부터 J를 얻는 과정은 해쉬 함수를 사용하여 누구나 할 수 있다.

(1) 시스템은 강한 소수 p와 q를 선택하고 공개되는 합성수 n을 p와 q의 곱으로 구한다. 여기에서 p와 q는 외부에 노출하지 않고 안전하게 관리한다.

(2) 시스템은 ID의 불법적 전용을 막기 위해 I*로부터 J를 추출한 후 아래의 성질을 만족하는 개인키(D)를 생성한다.

$$J \cdot D^v \equiv 1 (\bmod n)$$

여기에서 v는 공개되는 소수이다.

(3) $F()$를 $F(x) = x^v \bmod n$인 일방향 해쉬 함수라 할 때 각 사용자는 x_0로부터 $F()$를 이용하여

$$i = 1, 2, \ldots, k \text{에 대하여 } x_i = F(x_{i-1})$$

를 구한다. 여기에서 $x_i = (x_0)^{v^i}$라는 사실은 명백하다.

(4) 각 사용자는 처음에 x_k를 공개키 디렉토리에 공개하고 서명이 끝날 때마다 그 색인을 1씩 감소시켜 공개키 디렉토리를 갱신한다. 이 방법을 사용함으로서 사용자는 k번 서명할 수 있다.

2.3.2. 서명 생성 및 검증

여기에서 우리는 $x_k, x_{k-1}, \ldots, x_{m+1}, x_m$은 사용자에 의해 이미 사용되었다고 가정하자.

〔1단계〕 입력

$$(J, x_{m+1}, v, n)$$

〔2단계〕 서명

(1) (J, x_m)을 공개한다.

(2) 난수 r_m에 대하여 $T_m = r_m^v \bmod n$을 구한다.

(3) 서명할 문서 M에 대하여 $d_m = h(T_m, M|I*)$ 과 $t_m = r_m \cdot (D \cdot x_{m-1})^{d_m}$ 을 각각 구하고 $(T_m, t_m, M|I*)$를 M에 대한 서명으로 정의하여 검증자에게 보낸다.

〔3단계〕 검증

(1) 검증자는 (J, x_{m+1}, v, n)과 x_m을 이용하여 다음 두 사항을 검증한다.

$$x_{m+1} = x_m^v \bmod n$$
$$d_m = h(t_m^v \cdot (J \cdot x_m^{-1})^{d_m} \bmod n,\ M|I*)$$

(2) 마지막으로 다음 사항을 검증하여 서명자가 x_{m-1}를 이미 알고 있음을 확인할 수 있다.

$$\begin{aligned} & t_m^v \cdot (J \cdot x_m^{-1})^{d_m} \\ &= (r_m \cdot D^{d_m v} \cdot x_{m-1}^{d_m v}) \cdot J^{d_m} \cdot x_m^{-d_m} \bmod n \\ &= r_m^v \cdot (D^v J)^{d_m} \cdot (x_{m-1}^v \cdot x_m^{-1})^{d_m} \bmod n \\ &= r_m^v \bmod n \end{aligned}$$

검증이 끝난 후 검증자는 서명을 사용하여 공개키 디렉토리에 $x_m \rightarrow x_{m-1}$으로 갱신한다.

2.3.3. 서명권한 위임 방법

위 ID 기반 서명 기법은 서명할 수 있는 권한이 k번으로 제한되는 기법이다. 특히 k번의 권한 중 일부를 위임하기 위해 대리인에게 $x_i\ (0 \le i < t)$를 보안채널을 이용하여 전달한다. 그러면 대리인은 자신이 생성할 수 있는 몇 개의 x_i와 자신의 ID에 대응하는 개인키를 이용하여 서명을 생성한다. 생성된 대리서명의 검증을 위해 검증자는 사용된 x_i의 유효성을 검사하고 유효하면 대리인의 ID와 x_i를 이용하여 서명을 검증한다.

〔문제점〕

이 기법의 가장 큰 단점은 ID 기반 인증 모델에서의 서명 기법임에도 불구하고 x_i의 유효성 확인을 위해 원서명자나 신뢰기관이 제공하는 x_i에 대한 인증서를 사용해야 한다. 그래서 ID 기반 인증 모델의 단점, 즉 시스템이 각 사용자의 개인키를 알고 있다는 것과 인증서 기반 인증 모델의 단점, 서명자의 공개키에 대한 신뢰기관의 인증서를 받아야 한다는 것을 모두 가지게 된다. 또한, 단순한 횟수의 제한을 제외하고 권한의 사용에 대한 아무런 제약이 없기 때문에 [2]에서 소개한 대리서명 기법이 가지는 문제점을 모두 갖는다.

Ⅲ. Bilinear 함수를 이용한 ID 기반 대리서명 기법

이 장에서 우리는 ID 기반 인증 모델에서의 대리서명 방법을 제안한다. 제안하는 방법의 기본 과정은 2.2 에서 정리한 대리서명 기법과 같다. 즉, 먼저 원서명자는 m_d에 ID 기반 서명 방법을 이용하여 서명을 생성하여 위임장을 발행하면 대리인은 위임장을 이용하여 대리서명을 생성한다. 여기에서 우리는 안전한 ID 기반 서명 기법으로 [6]에서 소개되는 기법을 사용한다.

3.1 ID 기반 서명 기법

우리는 차재춘과 천정희의 ID 기반 전자서명을 소개하기 전에 그들의 기법이 사용하고 있는 bilinear 함수와 안전성 기반문제의 정의를 간단히 정리한다.

G_1과 G_2를 위수가 소수 q인 순환군이며 G_1은 덧셈군이며 G_2는 곱셈군이라 하자. G_1과 G_2에서 이산대수 문제는 어렵다.

〔정의1〕 (bilinear 함수)

우리는 함수 $e: G_1 \times G_1 \rightarrow G_2$가 임의의 $P_1,\ P_2 \in G_1$과 $Q_1, Q_2 \in G_2$에 대하여 다음 조건을 만족하면 bilinear 함수라 한다.

(1) [Bilinearity] $a,\ b \in F_q$에 대하여
$e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$,
$e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$ 또는

$e(aP, bQ) = e(P, Q)^{ab}$ 를 만족한다.

(2) [Non-degenerate]

$e(P, Q) \neq 1$인 P와 Q가 존재한다.

(3) [Efficiency]

$e(P, Q)$의 계산이 효율적인 알고리즘이 존재한다.

우리는 여기에서 Weil과 Tate pairings 이 초특이 타원곡선에 적용되면 위와 같은 bilinear 함수를 생성할 수 있다는 사실을 지적한다.

우리는 다음으로 암호 프로토콜의 안전성기반 문제로 사용되고 있는 네 가지 문제를 묘사한다.

(1) 이산 대수 문제 (DLP) : 주어진 두 개의 원소 P와 Q에 대하여 $Q = nP$인 n을 찾아라.

(2) 결정적 디피-헬만 문제 (DDHP) : 주어진 P, aP, bP, cP에 대하여 $c \equiv ab \bmod q$인지를 결정하라.

(3) 계산적 디피-헬만 문제 (CDHP) : 주어진 P, aP, bP에 대하여 abP를 계산하여라.

(4) 결선형 디피-헬만 문제 (BDHP) : bilinear 함수 e를 사용하여 주어진 $aP, bP, cP \in G$에 대하여 $e(P, P)^{abc}$를 구하라.

차재춘과 천정희가 제안한 ID 기반 서명 기법은 bilinear 함수의 연산이 다항식 시간 내에 쉽게 이루어지나 BDHP의 해결은 어려운 임의의 군 위에서 서명 생성과 검증이 이루어진다[6]. 그러한 군을 gap Diffie-Hellman Group(GDH군)이라 부른다. 여기에서 BDHP의 어려움은 전자서명에 대한 existential forgery 공격을 막기 위해 사용되며 bilinear 함수의 사용은 서명의 검증에 사용된다.

3.1.1 서명기법

위수가 l인 GDH 군 $(G, +)$의 생성원을 P라하고 그 위에서의 bilinear 함수를 e라 하자. 그들의 서명 기법은 다음의 네 단계로 구성되어 있다.

〔1단계〕 시스템 파라미터와 마스터키 생성

(1) 난수 $s \in Z/l$을 생성하고 $P_{pub} = s \cdot P$를 계산한다.

(2) 두 개의 충돌 회피 해쉬 함수를 사용한다.

$$H_1 : \{0,1\}^* \rightarrow Z/l \text{과} \quad H_2 : \{0,1\}^* \rightarrow G.$$

(3) 시스템 파라미터 (P, P_{pub}, H_1, H_2)를 공개하고 s를 마스터키로 사용한다.

〔2단계〕 ID에 대응하는 개인키 생성

시스템은 각 사용자가 생성한 ID에 대하여 $D_{ID} = s \cdot H_2(ID)$를 계산하고 그것을 그 ID에 대응하는 개인키로 발급한다. 사용자들은 H_2를 이용하여 ID로부터 쉽게 공개키 역할을 하는 $Q_{ID} = H_2(ID)$를 생성하여 사용할 수 있다.

〔3단계〕 서명 생성

자신의 개인키 D_{ID}를 이용하여 메시지 m에서명한다. 먼저 난수 $r \in Z/l$을 선택하고 다음을 계산한다.

$$U = r \cdot Q_{ID}$$
$$V = (r + H_1(m, U)) \cdot D_{ID}$$

그리고 $\sigma = (U, V)$를 m에 대한 서명으로 정의한다.

〔4단계〕 서명 검증

서명 $\sigma = (U, V)$ 검증을 위해 e를 사용하여 $h = H_1(m, U)$일 때, $(P, P_{pub}, U + h \cdot Q_{ID}, V)$가 결정적 Diffie-Hellman(DDH) 쌍인지 확인한다. 즉, $e(P_{pub}, U + h \cdot Q_{ID}) = e(P, V)$인지 확인하여 검증한다.

그들은 이 서명 기법이 existential forgery 공격에 대하여 안전함을 증명하였다.

3.2 ID 기반 대리서명 기법

Alice와 Bob은 각각 공개키와 개인키쌍 (Q_A, D_A)와 (Q_B, D_B)를 가지고 있다고 하자.

〔1단계〕 위임장 생성 및 전달

Alice는 난수 $r_A \in Z/l$를 생성하고,

$$U_A = r_A \cdot Q_A$$
$$V_A = (H_1(m_d, U_A) + r_A) \cdot D_A$$

를 계산하고 $m_w = (U_A, V_A, m_d)$를 대리인 Bob에게 전달한다.

〔2단계〕 대리서명 키 생성

Bob은 m_w에서 (U_A, V_A)가 m_d에 대한 올바른 서명인지 확인하고 유효한 서명이면 다음과 같이 대리서명을 위한 개인키와 이에 대응하는 공개키를 생성한다.

$$D_P = V_A + D_B$$
$$Q_P = U_A + H_1(m_w, U_A) \cdot Q_A + Q_B$$

여기에서 우리는 $D_P = s \cdot Q_P$임을 확인할 수 있다.

〔3단계〕 대리서명 생성

Bob은 위임장에서 명시한 권한 내에서 서명 가능한 문서 m_P에 대해서 대리서명을 위한 개인키를 이용하고 위 ID 기반 서명 기법으로 아래와 같이 대리서명을 생성한다.

(1) Bob은 난수 r_P를 선택하고 다음을 계산한다.
$U_P = r_P \cdot Q_P, \quad V_P = (r_P + H_1(m, U_P)) \cdot D_P$

(2) 순서쌍 $(U_P, V_P, U_A, m_d, m_P)$를 문서 m_P에 대한 대리서명으로 정의한다. 여기에서 U_A는 원서명자의 서명 권한 위임에 대한 동의를 나타낸다.

〔3단계〕 대리서명 검증

대리서명 검증자는 수신된 대리서명 $(U_P, V_P, U_A, m_d, m_P)$을 검증하기 위해 먼저 대리서명에 사용된 개인키에 대응하는 공개키를 생성한다.

$$Q_P = U_A + H_1(m_w, U_A) \cdot Q_A + Q_B.$$

그 후, Q_P를 이용하여
$(P, P_{pub}, U_P + H_1(m, U_P) \cdot Q_P, V_P)$가 유효한 DDH 쌍인지를 확인하여 검증한다.

Ⅳ. 안전성

위에서 언급한 바와 같이 우리가 제안하는 대리서명 기법은 existential forgery 공격에 대하여 안전한 서명 기법을 반복하여 사용하고 있기 때문에 그 안전성에 대하여 우리는 다음의 두 가지 경우에 대하여 고려하면 된다.

(1) 대리인에 의한 서명 권한 오남용

(2) 대리서명에서 원서명자와 대리인의 역할분리 가능성

먼저 대리인에 의한 서명 권한의 오남용에 대하여 고려해 보면 우리의 대리서명 기법은 [3]에서의 기법과 같이 위임장의 내용을 대리서명에 포함시킴으로써 대리인의 오남용을 방지할 수 있다.

실질적으로 두 번째 고려사항이 대리서명의 안전성을 결정짓는 중요한 부분이다. 특히 우리의 기법은 과거 인증서 기반 대리서명 기법과 달리 위임장 전송시 보안채널의 확보가 필요 없는 대리서명이기 때문에 대리서명에서 원서명자와 대리인의 역할 분리는 다음과 같은 중요한 문제점을 낳을 수 있다.

(1) 대리서명 생성시 서명 기법을 두 번 반복하여 사용하기 때문에, 만약 대리서명에서 원서명자와 대리인의 역할이 분리된다면, 원서명자가 대리서명으로부터 자신의 역할을 분리하여 대리인의 유효한 서명을 생성할 수 있다.

(2) 위임장 전송 시 보안채널이 확보되어 있지 않기 때문에 특정인에게 전송되는 위임장을 모두 확보할 수 있다. 만약 원서명자와 대리인의 역할이 분리된다면 공격자에 의해 특정인이 생성한 대리서명의 원서명자를 마음대로 바꿀 수 있다. 뿐만 아니라, 대리서명에서 원서명자의 역할을 제거함으로써 대리인의 일반 서명을 얻을 수 있고, 역으로 일반 서명으로부터 대리서명을 얻어낼 수 있다.

이러한 문제점은 이전의 인증서 기반 대리서명에서 발견되어 위임장을 보안채널을 이용해서 전송해야 하는 문제점을 노출하였다. 하지만 우리는 [정리1]을 통해 원서명자와 대리인의 역할이 분리 될 수 없음을 확인할 수 있고, 따라서 보안 채널의 없이 안전한 대리서명을 생성할 수 있음을 보인다.

〔정리1〕

만약 공격자가 우리가 제안하는 기법에서 원서명자와 대리인의 역할을 분리할 수 있다면 그는 타원곡선 군에서 이산 로그 문제를 해결할 수 있다.

(증명)

공격자가 우리의 알고리즘에서 원서명자와 대리인의 역할을 분리하기 위해서는 $(U_P, V_P, U_A, m_d, m_P)$

의 U_P로 부터 $U_B(=r_P \cdot Q_B)$를 추출할 수 있어야 한다. 하지만 이를 위해서 공격자는 r_P를 구할 수 있어야 하고 만약 공격자가 r_P를 구할 수 있다면 이는 그가 타원곡선에서의 이산대수 문제를 해결할 수 있음을 의미한다.

V. 비 교

이 장에서는 본 논문에서 제안한 대리서명 기법과 기존에 제안된 여러 기법을 효율성과 기능 측면에서 비교한다[표 1].

먼저 효율성 측면을 살펴보면 우리의 기법이 갖는 장점은 크게 두 가지로 요약된다. 한가지는 ID 기반 인증 모델을 기반구조로 사용함으로써 자연스럽게 만들어지는 것이며 다른 한가지는 서명 기법상에서 발생하는 장점이다. 첫 번째 경우는 ID 기반 인증 모델을 적용한 대리서명 기법이기 때문에 사용자의 공개키 인증서의 필요성을 없앨 수 있다는 것인데, 특히 대리서명 기법에서는 그 검증 과정에서 원서명자와 대리인의 공개키를 모두 필요로 하기 때문에 공개키 인증서 습득과정의 생략은 인증서 기반 기법보다 훨씬 효율적일 것이다. 둘째로 서명 기법상에서 얻어지는 효율성은 위임장 전송 시 보안채널의 확보 필요성을 제거할 수 있다는 것이다. 이 부분은 특히 중요한 부분으로 기존 대리서명 기법들이 모두 보안채널의 필요성이 효율성을 현저히 떨어뜨리기 때문이다.

다음으로 우리가 제안하는 기법이 제공하는 기능을 살펴보자. 우리의 대리서명 기법은 [3]에서와 마찬가지로 m_w를 ID 기반 대리서명에 삽입함으로서 [3]의 기법이 가지는 모든 기능을 수행할 수 있다. 특히, m_w의 삽입은 기존 ID 기반 대리서명 기법이 제공하지 못하는 오남용 방지기능을 제공할 수 있다.

〔표 1〕 제안 대리서명 기법과 기존 기법의 비교

분 류		[6]	[3]	[1]	제안기법
효율성	보안채널	필 요	필 요	필 요	필요없음
	공개키인증서	필 요	필 요	필 요	필요없음
주요기능	오남용방지	제공못함	제 공	제공못함	제 공
	강한위조방지	제공못함	제 공	제공못함	제 공

VI. 결 론

대리서명은 한 사용자가 자신의 서명 권한을 위임할 필요가 있을 때 사용될 수 있는 매우 유용한 기술이다. 하지만 인터넷과 같은 분산환경에서 원서명자나 대리인을 신뢰하기는 매우 어려운 문제이기 때문에 안전한 대리서명 기법에 대한 연구는 중요하다.

우리는 이 논문에서 기존 대리서명 기법들이 기반하고 있는 환경과 전혀 다른 ID 기반 인증 모델에서의 대리서명 기법을 소개하고 있다. 우리가 제안하는 기법은 기존 대리서명 기법이 제공하는 모든 기능을 제공할 뿐만 아니라 훨씬 효율적이다. 또한 우리의 대리서명 기법은 최근 활발히 연구되고 있는 bilin-ear 함수를 이용한 것으로 그들과 함께 사용됨으로서 ID 기반 인증 모델에서의 공개키 암호 시스템의 구현에 이바지 할 수 있다.

참 고 문 헌

[1] O. Delos and J. J.Quisquater, "An Identity-Based Signature Scheme with Bounded Life-Span," Springer-Verlag, *Advances in Cryptology, Proceedings of CRYPTO '94,* LNCS 839, pp. 83~94, 1994.

[2] M. Mambo, K. Usuda and E. Okamoto, "Proxy Signature : Delegation of the Power to Sign Messages," In *IEICE Trans. Fundamentals*, Vol. E79-A, No. 9, Sep., pp. 1338~1353, 1996.

[3] S. Kim, S. Park, and D. Won, "Proxy Signatures, Revisited," Springer-Verlag, *Proceedings of ICICS '97,* LNCS 1334, pp. 223~232, 1997.

[4] Byoungcheon Lee, Heesun Kim, Kwangjo Kim, "Strong Proxy Signature and its Applications," *Proceedings of SCIS2001, vol 2/2,* pp. 603-608, 2001.

[5] A. Shamir, "Identity-based Crypto systems and Signature Schemes," Springer-Verlag, *Advances in Cryptology, Proceedings of Crypto '84, LNCS* 196, pp. 47~53, 1985.

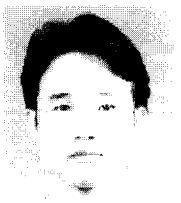
[6] J. Cha and J. Cheon, "An Identity-based Signature from Gap Diffie-Hellman Groups," Springer-Verlag, *Advances in Cryptology, Proceedings of PKC '03, LNCS* 2567, pp. 18~30, 2003.

[7] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," Springer-Verlag, *Advances in Cryptology, Proceedings of CRYPTO '01, LNCS* 2139, pp. 213~229, 2001.

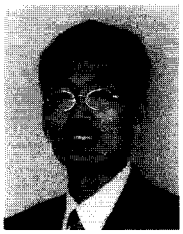
[8] Byoungcheon Lee, Heesun Kim, and Kwangjo Kim "Secure Mobile Agent using Strong Non-designated Proxy Signature," Springer-Verlag, *Proceedings of ACISP2001, LNCS* 2119, pp. 474~486, 2001.

[9] D. Pointcheval and J. Stern, "Security Proofs for Signatures,"Springer-Verlag, *Advances in Cryptology, Proceedings of Eurocrypt '96, LNCS* 1070, pp. 387~398, 1996

〈著者紹介〉



이 정 연 (Jung-Yeun Lee) 학생회원
2000년 2월 : 경희대학교 수학과 석사
2003년 2월 : 한국정보통신대학원대학교 석사
<관심분야> 대리서명, ID 기반 공개키 암호시스템, 공개키 인증서



천 정 희 (Jung Hee Cheon) 정회원
1997년 2월 : 한국과학기술원 수학과 박사
1997년 3월~2000년 1월 : 한국전자통신연구원 선임연구원
2000년 1월~2000년 12월 : Brown 대학 박사후 연구원
2000년 12월~2003년 2월 : 한국정보통신대학교 공학부 조교수
2003년 3월~현재 : 서울대학교 수리과학부 조교수
<관심분야> 응용정수론, 암호론, 응용암호론

김 태 성 (Tae-sung Kim)
2001년 2월 : 동국대학교 컴퓨터공학과 석사
2001년 3월 : 한국전자통신연구원 정보보호연구본부 인증기반연구팀 (ETRI)

진 승 헌 (Seung-hun Jin) 정회원
1995년 2월 : 숭실대학교 석사
1996년 4월 : (주)대우통신 종합연구소 연구원
1999년 5월 : (주)삼성전자 통신연구소 전임연구원
2003년 3월 : (주)한국전자통신연구원 정보보호연구본부 인증기반연구팀 팀장(ETRI)
<관심분야> 컴퓨터/네트워크 보안, 정보보호(PKI, 인증/인가 기술)