무선 PKI 환경에 적합한 타원곡선 기반 은닉 서명 제안

윤 이 중[†] · 한 대 완[††] · 한 재 우[†††] · 류 재 철[††††]

요 약

본 논문에서는 무선 PKI 환경에 적합한 은닉 서명을 제안한다. 제안하는 방식은 [5]에서 제안한 Gap problem을 이용한 시스템으로 이에 대한 예로는 타원곡선 기반의 Weil pairing을 이용한 서명 방식등이 될 수 있다. 특히 Weil pairing을 이용한 서명 방식은 작은 키 크기로 높은 안전성을 제공할 수 있으며, Diffie-Hellman 문제에 기반한 실용적인 은닉 서명으로는 최초의 방식이라고 할 수 있다.

A proposal for blind signature scheme based on the elliptic curves suitable for wireless PKI

E-Joong Yoon[†] · Daewan Han[††] · Jaewoo Han[†††] · Jae-Cheol Ryou[††††]

ABSTRACT

In this paper we propose the efficient blind signature scheme based on Gap problem. We can find the short signature schemes for Weil pairing as the example of signature schemes based on Gap problem. Since short signature scheme is based on elliptic curve, our proposed signature scheme can be used in wireless PKI environment.

키워드 : 은닉 서명(Blind signature), Gap problem, Weil pairing, 무선 PKI(Wireless PKI)

1. 서 론

은닉 서명은 서명 의뢰자가 서명 생성자에게 서명을 의뢰하면 서명 생성자는 서명 내용에 대한 정보를 전혀 모르는 상태에서 서명을 하는 기법으로 전자 화폐 등에서 필수적인 서명 방식이다[3]. 즉, 일반 전자 화폐 사용자는 자신의 전자 화폐 사용 내역을 은행에 공개하지 않고, 은행으로부터 현재 전자 화폐가 올바른 화폐이며, 은행이 이 전자 화폐에 대하여 책임을 진다는 서명을 받아낼 수 있다.

그러나 현재까지 소개된 은닉 서명은 RSA 기반의 서명 방식만이 간단한 방식으로 만들 수 있으며, 타원곡선 암호 등의 Diffie-Hellman 문제에 기반한 시스템은 다소 복잡한 과정을 거쳐야만 은닉 서명 방식이 구성되어지기 때문에 무선 PKI 환경 등에 적용하기에는 여러 가지 어려움이 따른다.

본 논문에서는 먼저 Diffie-Hellman 문제에 기반하면서도 RSA 기반 은닉 서명과 같이 효율적인 은닉 서명을 구성하는 방법을 제안하며, 이를 바탕으로 타원곡선 기반의 효율적인 은닉 서명 방식을 제안한다. 즉, 서명 의뢰자가 서명 생성자에게 은닉 서명을 의뢰하면 추가적인 통신이 없이도 바로 은닉 서명을 생성해주는 시스템을 제안한다.

본 논문에서 제안하는 서명 방식은 기본적으로 T. Okamoto와 D. Pointcheval[5]이 제안한 Gap Diffie-Hellman 군에서 성립한다. Gap problem을 사용하여 제안된 서명 방식의 예로는 D. Boneh, B. Lynn, H. Shacham이 제안한 Weil pairing을 이용한 서명 방식[1] 등이 될 수 있다.

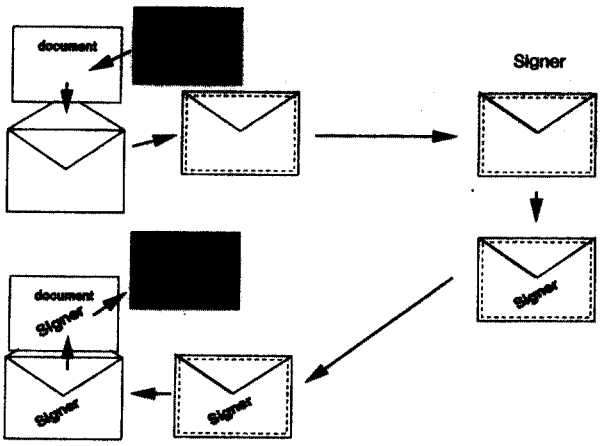
2장에서는 은닉 서명에 대한 정확한 의미와 함께 현재까지 제안된 은닉 서명에 대하여 간단하게 살펴보고, 3장에서는 이산대수문제, Diffie-Hellman 계산 문제 및 Diffie-Hellman 판별 문제에 대한 정의와 함께 이들 문제의 어려움의 차이로부터 파생되는 Gap problem과 함께 이를 사용한 서명 방식에 대하여 살펴본다. 4장에서는 이 문제의 직접적인 예제가 되는 Weil pairing에 대하여 살펴보고, 5장에서 본 논문이 주장하는 Gap problem을 사용한 은닉 서명과 함께 Weil pairing을 이용한 서명 방식을 소개하며, 본 은닉 서명의 안전성에 대한 간단한 증명과 함께 효율성에 대하여 분석한다.

† 정 회 원 : 국가보안기술연구소 기반기술연구부장
†† 정 회 원 : 국가보안기술연구소 기반기술연구부 연구원
††† 정 회 원 : 국가보안기술연구소 기반기술연구부 선임연구원
†††† 종신회원 : 충남대학교 정보통신공학부 교수

논문접수 : 2001년 12월 12일, 심사완료 : 2001년 12월 26일

2. 은닉 서명 기법

은닉 서명 기법(Blind signature scheme)이란 서명을 하는 행위자가 서명되는 메시지와 서명 값에 대하여 어떠한 정보도 얻을 수 없는 전자 서명 기법을 말한다[3]. 은닉 서명 기법은 현대 암호학의 중요한 요소로서, 전자화폐나 전자 투표 등 주로 행위자의 행동이 노출되어서는 안되는 보안 서비스에 활용된다. 은닉 서명의 개념을 그림으로 표현하면 (그림 1)과 같다.



(그림 1) 은닉 서명의 개념도

D. Chaum이 RSA 문제를 기반으로 하는 은닉 서명을 처음 제시한 이래로, 다양한 문제에 기반을 둔 은닉 서명들이 제안되었다.

본 절에서는 기존에 제안된 은닉 서명 기법들 중 대표적인 RSA와 Schnorr 은닉 서명 기법에 대하여 살펴본다.

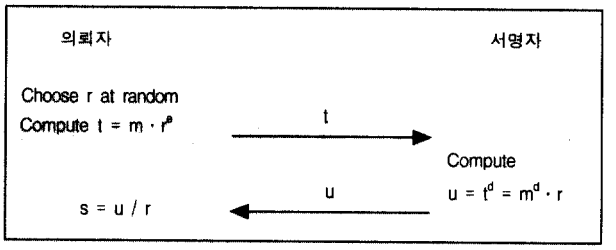
2.1 RSA 은닉 서명 기법

본 소절에서는 D.Chaum이 제안한 RSA 기반 은닉 서명기법에 대하여 살펴본다.

일반적으로 은닉 서명의 프로토콜은 서명 의뢰(requesting), 은닉 서명(signing), 서명 추출(extraction)의 세 단계로 이루어진다. RSA 은닉 서명 기법의 프로토콜을 각 단계별로 설명하면 다음과 같다.

- 키 생성 : 키 생성은 일반적인 RSA 기반 서명에서의 키 생성 절차와 같다. 즉, 서명자가 임의의 소수 p, q를 선택하고, $n = pq$와 $\phi(n) = (p-1)(q-1)$을 계산한다. 서명자는 임의의 정수 d를 선택하고, $ed = 1 \bmod \phi(n)$이 되는 e를 계산한다. 서명자의 공개키는 (n, e)이고, 비밀키는 d이다.
- 서명 의뢰 : 서명 의뢰자는 메시지 M에 대한 서명을 의뢰하기 위하여, M의 해쉬값 $m = h(M)$과 난수 r을 선택하여 $t = mr^e$을 계산한 다음 t를 서명자에게 전송한다.
- 서명 생성 : t를 전송받은 서명자는 $u = t^d = m^d \cdot r$을 계산한 후, u를 의뢰자에게 전송한다.
- 서명 추출 : u를 전송받은 후, 의뢰자는 $s = m^d = u/r$을 계산한다. M에 대한 서명값은 s가 된다.

서명의 검증은 일반적인 RSA 기반 서명의 검증과 동일하게 수행한다. 즉, 검증자는 서명자의 공개키 e를 이용해, $s^e = h(M)$이 성립하는지를 검증한다.

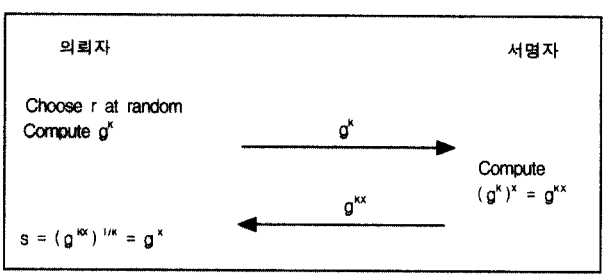


(그림 2) RSA 은닉 서명 기법

2.2 Schnorr 은닉 서명 기법

Schnorr 기반 은닉 서명 기법은 T.Okamoto에 의해서 처음 제안되었다[4]. Okamoto가 제안한 은닉 서명의 프로토콜은 다음과 같다.

- 키 생성 : 키 생성은 일반적인 Schnorr 서명 기법과 같다. 즉, G의 크기가 소수 q인 그룹이고 g를 G의 생성원이라고 하자. 서명자는 임의의 정수 x를 선택한 후, $y = g^x \bmod q$를 계산한다. 서명자의 공개키는 y, 비밀키는 x가 된다.
- 서명 의뢰 : 서명 의뢰 과정은 다음 세 단계로 세분된다.
  ① 서명 의뢰자는 먼저 서명자에게 서명 요청을 한다.
  ② 서명 요청을 받은 서명자는 난수 r을 선택한 후, $t' = g^r$을 계산하여 의뢰자에게 전송한다.
  ③ t'를 전송받은 후, 서명자는 난수 a, b를 선택한 후, $t = t'g^a y^b$와 $c = h(M \| t)$, $c' = c - b$를 차례로 계산한 후, c'를 서명자에게 전송한다.
- 서명 생성 : c'를 전송받은 서명자는, $s' = r - c'x$를 계산한 후, 의뢰자에게 전송한다.
- 서명 추출 : 의뢰자는 전송받은 s'로부터, $s = s' + a$를 계산한다. 메시지 M에 대한 서명값은 $(c.s)$가 된다.



(그림 3) Schnorr 은닉 서명 기법

서명의 검증은 서명값 (c,s)와 공개키 y로부터 $c=h(m\|(g^s y^c))$이 성립하는지를 확인하면 된다.

3. Gap-problem

이산대수문제의 어려움에 기반한 암호 및 서명 방식들은 현재까지 많이 제안되었다. Diffie-Hellman 키공유 시스템, ElGamal 암호 시스템, 타원곡선 암호 시스템 등의 암호 시스템과 DSA, Schnorr 서명, KCDSA 및 이들 시스템의 타원곡선 버전 등의 서명시스템 등이 소개되었다. 현재까지 소개된 이산대수문제를 이용한 암호 및 서명 방식의 안전성은 Diffie-Hellman 문제에 기반하고 있다. 즉, 이산대수문제의 어려움에 기반하고 있다고 하는 시스템도 정확하게는 Diffie-Hellman 시스템의 어려움에 기반하고 있다. 그러나 서명 방식의 검증과정은 주어진 서명문이 올바른 값인지를 판단하는 부분에서는 변형된 형태의 판별문제를 사용함으로 검증과정을 수행하게 된다.

이러한 과정을 통하여 이산대수문제와 관련된 문제들을 다음과 같이 정리할 수 있다.

- 이산대수문제 : g와 $g^x \bmod p$로부터 x를 구하는 문제
- Diffie-Hellman 계산 문제(CDHP : Computational Diffie-Hellman Problem) : g, $g^x \bmod p$와 $g^y \bmod p$로부터 g^{xy}를 계산하는 문제
- Diffie-Hellman 판별 문제(DDHP : Decisional Diffie-Hellman Problem) : g, $g^x \bmod p$, $g^y \bmod p$ 및 h로부터 $g^{xy} \bmod p$가 h인지 판별하는 문제

위의 문제들의 난이도를 살펴보면 이산대수문제가 해결이 되면, Diffie-Hellman 계산 문제가 해결이 되고, Diffie-Hellman 계산 문제가 해결이 되면 Diffie-Hellman 판별 문제가 해결이 된다. 그러나 이 역들에 대하여는 많은 노력이 있었지만 아직까지 주목할만한 연구 결과물은 발표되지 않았다. 이에 대하여 2001년 T. Okamoto와 D. Pointcheval은 PKC 2001에서 Diffie-Hellman 계산 문제와 Diffie-Hellman 판별 문제의 어려움에 차이가 있을 경우, 이 어려움의 차이에 기반한 서명 방식을 설계할 수 있음을 보였다[5]. 그러나 이 논문에서는 단지 이러한 시스템의 존재 가능성만을 논하였을 뿐, 실재적인 시스템은 제안하지 못하였다. 즉, 이 때까지는 Diffie-Hellman 계산 문제는 어려우면서 Diffie-Hellman 판별 문제는 쉬운 군을 찾지 못하였다. 이 후 D.Boneh 등은 Asiacrypt 2001에서 실제로 Weil pairing을 이용하면 초특이 타원곡선 위에서의 Diffie-Hellman 계산 문제는 어려우면서 Diffie-Hellman 판별 문제는 쉬운 사실을 이용하여 실제로 사용할 수 있는 서명 방식을 제안한다[1]. 이에 대한 내용은 다음 장에서 소개하기로 하고 본 장에서는 Okamoto와 Pointcheval이 제안한 Diffie-Hellman 계산 문제가 어려우면서 Diffie-Hellman 판별 문제가 쉬운 경우의 서명 방식의 구성에 대하여 알아본다.

- 키 생성 : 서명자는 위수가 소수 q인 군에 대하여, 생성자 g와 난수 x를 선택하여 공개키로 (g, g^x)를 공개하고, 비밀키로 x를 보관한다.
- 서명 생성 : 메시지 M의 해쉬값 m에 대한 서명값 s는 m^x이다.
- 서명 검증 : Diffie-Hellman 판별 문제((g, g^x, m, s)가 주어졌을 때 m^x이 s인지 판별하는 문제))를 풀어서 올바른 서명값인지 판단한다.

위의 서명 방식은 서명값은 만들기 어려우며, 이에 대한 판단은 쉬워야 한다는 사실을 응용하여 제안된 시스템이다. 그러나 이러한 군은 찾기가 쉽지 않으며, Diffie-Hellman 계산 문제가 어려우면서, Diffie-Hellman 판별 문제가 쉬운 군은 특별히 GDH(Gap Diffie-Hellman)군이라고 정의하였고 이러한 문제를 GDH 문제라고 정의한다.

4. Weil pairing

Weil pairing은 타원곡선 이산대수문제의 공격에 사용되어 왔으나, 2001년에 몇 편의 논문을 통하여 암호 응용 프로토콜에도 사용이 될 수 있다는 사실이 알려지기 시작했다. 이러한 이유는 Weil pairing을 이용하면 3자 키 공유 시스템의 구성도 가능하며, Diffie-Hellman 계산 문제는 여전히 어려우면서도 Diffie-Hellman 판별 문제도 쉽게 해결이 될 수 있기 때문이다.

Weil pairing은 초특이 타원곡선 상에서 정의되는 쌍선형사상(bilinear map)으로 E가 초특이 타원곡선 위의 점으로 이루어진 군이고, F_{p^2}이 크기가 p^2인 유한체라고 할 때, 쌍선형사상 e는 다음과 같이 정의된다.

$$e : E \times E \rightarrow F_{p^2}$$

이 때, 쌍선형사상은 다음과 같은 성질을 만족한다.

$$e(aP, bQ) = e(P, Q)^{ab}$$

Weil pairing에 대한 엄밀한 정의 및 수학적인 결과는 [7]을 통하여 살펴볼 수 있다.

타원곡선 위의 점들 (P, aP, bP, cP)가 주어졌을 때, Diffie-Hellman 판별 문제는 Weil pairing을 사용하여 다음의 식이 만족하는지만 계산하면 쉽게 해결할 수 있다.

$$e(aP, bP) = e(P, cP)$$

위의 계산은 쉽게 할 수 있다. 따라서 Okamoto와 Point-

cheval이 소개한 Gap problem 특성을 만족하는 예가 될 수 있으며, Weil pairing을 이용하면 실재 구현 가능한 서명 방식의 구성이 가능하다[1]. 실재 [1]에서는 어떠한 방법을 통하여 서명 방식의 구성이 가능하며, 이 때 사용되는 파라미터 등을 어떻게 선택하는지에 관하여 다루고 있으며, 짧은 길이의 서명문을 만드는 시스템에 관하여 소개하고 있다.

5. GDH 기반 제안 은닉 서명

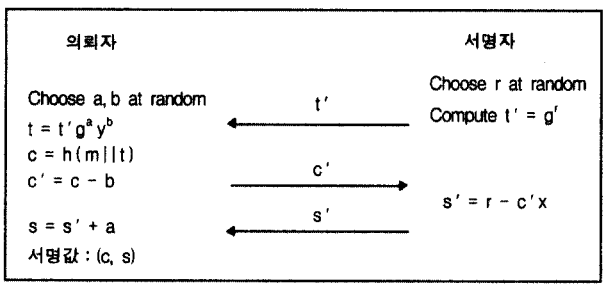
2절에서 살펴보았듯이, Schnorr 은닉 서명은 RSA에 비하여 프로토콜도 복잡하고, 계산량도 많은 단점이 있다. T. Okamoto의 방법 이후 변형된 Schnorr 은닉 서명 기법들이 몇몇 제시되고 있지만, 효율성 면에서 큰 진전은 없었다. 이에 본 절에서는 타원곡선 암호 체계에서 효율적으로 적용할 수 있는 은닉 서명 기법으로, GDH 문제에 기반한 은닉 서명 기법에 대하여 설명하고, 그 예로 Weil pairing을 이용한 은닉 서명 기법을 제시한다.

5.1 GDH 기반 은닉 서명의 프로토콜

일반적인 GDH 군에 적용할 수 있는 은닉 서명의 프로토콜은 다음과 같다.

- 키 생성 : 서명자는 임의의 난수 x를 선택한 후, $y = g^x$를 계산한다. 서명자의 공개키는 y, 비밀키는 x가 된다.
- 서명 의뢰 : 서명 의뢰자는 메시지 M에 대한 서명을 의뢰하기 위하여 난수 k를 선택하여 M에 대한 해쉬값 m과 m^k를 계산한 다음 m^k를 서명자에게 전송한다.
- 서명 생성 : m^k를 전송받은 서명자는 $(m^k)^x = m^{kx}$를 계산한 후, m^{kx}를 서명 의뢰자에게 전송한다.
- 서명 추출 : m^{kx}를 전송받은 후, 의뢰자는 $\sigma = (m^{kx})^{k^{-1}} = m^x$를 계산한다. M에 대한 서명 값은 σ가 된다.

서명 σ를 검증하기 위해서는, (g, y, m, σ)가 군 G상에서 올바른 DH 쌍인지를 확인하면 된다.



(그림 4) GDH 문제 기반 은닉 서명 기법

5.2 Weil pairing을 이용한 은닉 서명 기법

본 논문에서 제안하는 은닉 서명은 간단한 변경만으로 임의의 GDH 군에 적용 가능하다. 그 예로 본 소절에서는, [1]에서 제안된 GDH 군에 위에서 제안한 은닉 서명을 적용해 보기로 한다.

앞에서 설명한 타원 곡선 상의 Weil pairing을 이용하여 구성한 GDH 군에 본 은닉 서명 기법을 적용한 프로토콜은 다음과 같다.

- 키 생성 : F_{p^2} 위의 타원곡선 E를 택하고, 위수가 q인 점 $P \in E$를 생성한다. 서명자는 임의의 난수 x를 선택한 후, $R = xP$를 계산한다. 서명자의 공개키는 (l, q, P, R), 비밀키는 x가 된다.
- 서명 의뢰 : 서명 의뢰자는 메시지 M에 대한 서명을 의뢰하기 위하여 M에 해당하는 $\langle P \rangle$ 위의 점 Q를 계산한 후, 난수 k를 선택하여 kQ를 계산한 다음 서명자에게 전송한다.
- 서명 생성 : kQ를 전송받은 서명자는 $S' = x(kQ) = kxQ$를 계산한 후, S'을 서명 의뢰자에게 전송한다.
- 서명 추출 : S'을 전송받은 후, 의뢰자는 $S = k^{-1}(S') = xQ$를 계산한다. M에 대한 서명 값 σ는 S의 x 좌표 값이다.

서명의 검증 과정은 Weil pairing을 이용한 서명 기법에서의 검증 과정과 동일하다[1]. 즉, e가 타원곡선 E상에서 정의된 Weil pairing이라고 할 때, $e(xP, Q) = e(P, xQ)$가 성립하면 올바른 서명값으로 받아들이면 된다.

5.3 안전성

본 논문에서 제안한 은닉 서명 기법의 안전성은 다음의 세 가지 관점으로 접근할 수 있다.

- 키 복구 공격(Key recovery attack) : 공격자가 사용자의 비밀키를 복구하는 공격 방법
- 선택 위장 공격(Selectively forgery attack) : 공격자가 주어진 메시지에 대한 서명문을 위조하는 공격
- 단순 위장 공격(Existential forgery attack) : 공격자가 임의의 메시지에 대하여 서명문을 위조하는 공격

공격의 어려움은 키 복구 공격, 선택 위장 공격, 단순 위장 공격의 순이 됨은 쉽게 알 수 있다.

키 복구 공격이 성공하기 위해서는 공격자가 이산대수문제를 해결할 수 있어야만 한다. 이러한 사실은 키 복구 공격이 가능한 공격자가 존재한다고 하면 이 공격자를 사용하여 이산대수문제를 풀 수 있는 알고리즘을 설계할 수 있음을 보임으로 증명할 수 있으며, 이 증명 과정은 간단하다. 즉, 주어진 이산대수문제 g^x에 대하여 키 복구 공격이 가능한 공격자에게 g에 대한 서명값 g^x를 입력으로 주어서 주어진 키 x를 출력으로 받는다. 이렇게 하면 비밀키 x를 얻을 수 있으며, 이 x라는 값은 주어진 이산대수문제의 해답이다. 따라서 이

산대수문제가 안전하다면 주어진 시스템의 키 복구 공격도 안전하다는 결론을 얻을 수 있다.

다음으로 선택 위조 공격에 대한 안전성을 알아보자. 능동적 선택 메시지 공격 방법을 사용하면 주어진 은닉 서명 기법의 안전성은 해쉬함수의 안전성에 의존한다. 이에 대한 상세한 설명은 다음 문단에서 소개하기로 하고, 우선은 주어진 해쉬함수가 충분히 안전하다고 가정하기로 하자. 선택 위조 공격에 대한 안전성도 위와 비슷한 과정을 거치면, Diffie-Hellman 계산 문제가 안전하다면 주어진 서명 기법에 대한 선택 위조 공격도 안전하다는 결론을 얻을 수 있다.

다음으로 단순 위장 공격의 안전성을 살펴보자. 단순 위장 공격에 대한 안전성은 사용된 해쉬함수의 안전성과 깊은 관계가 있다. 우선 해쉬함수를 사용하지 않는 시스템을 살펴보자. 메시지 m_1에 대한 서명값 m_1^x과 메시지 m_2에 대한 서명값 m_2^x을 사용하여 메시지 m_1m_2에 대한 서명값 $(m_1m_2)^x$를 얻을 수 있다. 따라서 해쉬함수의 출력값이 작다면 단순 위장 공격에 대한 안전성은 전적으로 해쉬함수에 대한 안전성에 의존하며, 해쉬함수가 충분히 안전하다면 주어진 은닉 서명 기법의 안전성은 Diffie-Hellman 계산 문제의 어려움에 기반한다. 이에 대한 증명 또한 위의 방법과 비슷한 과정을 통하여 증명할 수 있다.

5.4 효율성

본 논문에서 제안한 은닉 서명 기법은 기존의 RSA기반 은닉 서명과 마찬가지로 단 한번씩의 통신과정을 거쳐 서명문을 생성할 수 있다. 따라서 기존의 Diffie-Hellman 문제 기반 서명 기법과 비교하여 매우 효율적이며, 계산량 역시 한 번의 지수승씩만으로 서명문을 생성하기 때문에 효율적이라고 할 수 있다. 이 때 사용되는 해쉬함수 연산량이나 역원 계산 연산량은 지수승 연산에 비하여 매우 작기 때문에 무시할 만한 양이다.

6. 결 론

본 논문에서는 타원곡선 등 Diffie-Hellman 문제의 어려움에 기반한 효율적인 은닉 서명 기법을 제안하였다. 이 서명 기법은 기존의 RSA 기반 은닉 서명만큼 효율적이며, 안전성 역시 현재까지 어렵다고 알려진 이산대수 문제와 Diffie-Hellman 계산 문제의 어려움에 기반하고 있다.

또한 제안한 은닉 서명 기법에 추가적으로 [6]에서 제안된 PSS(Provable signature scheme) 기법을 사용한다면 위장 공격에 대한 안전성을 더욱 높일 수 있으며, 제안한 은닉 서명 기법의 안전성도 [6]에서 증명한 방법을 통하여 안전성을 증명할 수 있다.

본 논문에서 제시한 방식은 현재 국내·외적으로 부각되고 있는 타원곡선 기반의 무선 PKI 환경에 별다른 부가 요인 없이 적용 가능하리라 예상된다.

참 고 문 헌

[1] D. Boneh, B. Lynn and H. Shacham, "*Short signatures from the Weil pairing*," Advances in Cryptology -Proceeding of Asiacrypt 2001, Springer-Verlag, preprint, 2001.

[2] J. Camenisch, J. Piveteau and M. Stadler, "*Blind signatures Based on the Discrete Logarithm Problem*," Advances in Cryptology, Proceedings of Eurocrypt'94, Springer-Verlag, pp.428-432, 1995.

[3] D. Chaum, "*Blind Signatures for Untraceable Payments*," Advances in Cryptology - Proceedings of Crypto'82, Springer -Verlag, pp.199-204, 1982.

[4] T. Okamoto, "*Provable secure and practical identification schemes and corresponding signature schemes*," Advances in Cryptology - Proceedings of Crypto'92, Springer-Verlag, pp.31-53, 1993.

[5] T. Okamoto and D. Pointcheval, "*The Gap-problem : A new class of problems for the security of cryptographic schemes*," 4th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2001, Springer-Verlag, preprint, pp.104-118., 2001.

[6] M. Bellare and P. Rogaway, "*The exact security of digital signatures -How to sign with RSA and Rabin*," Advaces in Cryptology -Proceedings of Eurocrypt'96, Springer-Verlag, pp.399-416, 1996.

[7] J. H. Silverman, "*The Arithematic of elliptic curves*," volume 106 of Graduate Texts in Mathematics, Springer-Verlag, 1986.

윤 이 중

e-mail : yej@etri.re.kr

1990년 인하대학교 전산과석사

1997년~현재 충남대학교 컴퓨터과학과 박사과정

1990년~2001년 한국전자통신연구원 정보보호시스템연구부장

2001년~현재 국가보안기술연구소 기반기술연구부장

관심분야 : 정보보호, PKI, 컴퓨터네트워크, 데이터베이스

한 대 완

e-mail : dwh@etri.re.kr

1995년 서울대학교 수학과(학사)

1997년 서울대학교 수학과(석사)

1998년~2001년 공군기상전대 수치예보개발장교

2001년~현재 국가보안기술연구소 연구원

관심분야 : 공개키 암호, 해쉬 함수

한 재 우

e-mail : jwhan@etri.re.kr
1991년 서강대학교 수학과(학사)
1993년 한국과학기술원 수학과(석사)
1999년 한국과학기술원 수학과(박사)
1999년~1999년 한국전자통신연구원 선임연구원
2000년~현재 국가보안기술연구소 선임연구원
관심분야 : 공개키 암호, 매듭이론

류 재 철

e-mail : jcryou@home.cnu.ac.kr
1985년 한양대학교 산업공학과 졸업
1988년 Iowa State Univ. 전산학석사
1990년 Northwestern Univ. 전산학박사
1991년~현재 충남대학교 정보통신공학부 부교수
관심분야 : 인터넷 보안, PKI, 스마트카드 보안