情報保護學會論文誌
第13券 第6號, 2003. 12

효율적인 ID 기반 부분은닉서명에 관한 연구

김 현 주*†‡, 오 수 현*, 원 동 호*

A Study on Efficient ID-based Partially Blind Signature

Hyun-Jue Kim*†‡, Soo-Hyun Oh*, Dong-Ho Won*

요 약

부분은닉서명은 서명자가 은닉서명을 발행할 때 그가 삽입하기를 원하는 어떠한 정보를 서명에 삽입할 수 있도록 하는 암호방식으로 전자화폐나 전자투표 등 주로 행위자의 행동이 노출되어서는 안되는 보안서비스에 중요하게 활용되며 전자화폐시스템에서 은행의 데이터베이스의 무제한적인 증가문제도 해결할 수 있는 암호방식이다. 본 논문에서는 GDH군에서의 ID 기반의 효율적인 부분은닉서명 방식을 제안한다. 제안한 방식은 Weil-pairing과 같은 bilinear 함수를 사용하며 CDHP의 어려움에 기반을 두고 있으며 기존의 부분은닉서명에 비하여 통신량, 통신횟수, 연산량을 줄여 무선 환경에 적용할 수 있는 효율적인 서명방식이다.

ABSTRACT

Partially blind signature scheme allows the signer to insert non-removable common information into his blind signature. Blind signatures providing with both users privacy and data authenticity are one of key parts of information systems, such anonymous electronic cash and electronic voting as typical examples. Partially blind signature, with which all expired e-cash but for still-alive can be removed from the banks database, copes well with the problem of unlimited growth of the banks' database in an electronic cash system. In this paper we propose an efficient ID-based partially blind signature scheme using the Weil-pairing on Gap Diffie-Hellman group. The security of our scheme relies on the hardness of Computational Diffie-Hellman Problem. The proposed scheme provides higher efficiency than existing partially blind signature schemes by using three-pass protocol between two participants, the signer and requesters also by reducing the computation load. Thus it can be efficiently used in wireless environment.

keyword : *ID-based partially blind signature scheme, Gap Diffie-Hellman Problem, Weil-pairing*

Ⅰ. 서 론

은닉서명은 서명의뢰자가 서명자로부터 메시지의 내용을 보여주지 않고 메시지에 대한 유효한 서명값을 얻는 서명방식이다. 즉, 서명의뢰자가 서명받고자하는 메시지를 은닉한 은닉 데이터를 서명자에게 전달하면 서명자는 전달받은 은닉 데이터에 서명을 해서 서명의뢰자에게 다시 전달하고 서명의뢰자는 서명된 은닉 데이터로부터 메시지에 대한 서명을 얻는 방식이다. 이 때, 서명자는 은닉서명 발행 프로토콜을 통해 생성한 메시지와 대응되는 서명 쌍에 대해 그 유효성을 검증할 수는 있으나, 메시지와 대응되는 서명 쌍을 서로 연결시킬 수는 없어야한다. 이와 같이 은닉서명은 서명의뢰자의 익명성을 보호하는 서명방식으로 개인의 프라이버시가 중시되는 현대사회에 필수적으로 요구되는 암호방식 중의 하나

* 성균관대학교 전기전자 및 컴퓨터 공학부 정보통신 보호연구실({hjkim, shoh, dhwon}@dosan.skku.ac.kr)
† 주저자, ‡ 교신저자, 논문접수일 : 2003년 9월 18일, 심사완료일 : 2003년 12월 1일

이다. 전자화폐나 전자투표 등 주로 행위자의 행동이 노출되어서는 안되는 보안서비스에 중요하게 활용된다.[1]

은닉서명방식은 1982년 D. Chaum[2]에 의해서 처음 소개되었다. 이 방식은 소인수분해 문제(IFP: Integer Factorization Problem)의 어려움에 기반한 RSA 서명방식[3]을 이용한 은닉서명방식이다. 그러나 1999년 J.S. Coron, D. Naccache와 J.P. Stern[4]등은 2개의 서명으로부터 정당하지 않은 서명을 만들 수 있다는 RSA 서명방식의 문제점을 발견했다. 이 후, 2000년 C. I. Fan, W. K. Chen와 Y. S. Yeh[5]은 랜덤화 특성을 가지는 RSA 암호 방식에 기반한 은닉서명 방식을 제안하여 D. Chaum의 은닉서명 방식을 개선하였다. 유한체 상에서의 이산 로그를 찾는 문제에 기반한 서명 방식을 이용한 ElGamal[6] 유형의 은닉서명 방식으로 대표적인 것은 1992년 T. Okamato[7]가 제안한 Schnorr[8]기반의 은닉서명 방식이 있다. 이산대수 문제에 기반한 은닉서명의 또 다른 예로는, 1994년 J. Camenish, J-M Piveteau와 M. Stadler[9]이 미국 표준인 DSA[10] 및 메시지 복원형 전자서명인 Nyberge-Ruppel 서명방식[11]을 기반으로 한 은닉서명방식이 있으며, 같은 해인 1994년 P. Horter, M. Michels과 H. Petersen[12]도 이산대수 문제에 기반한 일반적인 형태의 은닉서명 방식을 제시하였다. 그 후, 1997년 D. Pointchevel과 J. Stern[13]은 이차잉여 이론에 기반한 은닉서명방식을 제시하였다.

은닉성과 불추적성을 제공하는 은닉서명은 사용자의 익명성이 요구되는 전자 투표나 전자화폐 등에 사용된다. 그러나 전자화폐시스템은 전자적 특성상 쉽게 위조될 수 있다는 문제점이 있다. 전자화폐의 이중사용을 방지하기 위하여 은행은 전자화폐 자체가 특수한 구조를 가지도록 함으로써 매 지불시 마다 등록되는 데이터가 거의 동시에 모든 데이터베이스에 기록되도록 하여 이중 사용을 검출할 수 있다. 그러나 이미 사용된 모든 전자화폐들에 대한 데이터베이스를 구축해야 한다는 사실은 데이터베이스의 크기가 무제한적으로 증가하게 되며 또한 이에 대한 막대한 비용이 소요됨을 암시한다. 은행의 데이터베이스의 무제한적인 증가 문제를 해결하기 위하여 부분은닉서명방식이 제안되었다.

부분은닉서명방식이란 서명자(은행)가 은닉서명을 발행할 때 그가 삽입하기를 원하는 어떠한 공통정보를 서명에 삽입할 수 있도록 하는 암호방식이다. 서명에 삽입되는 공통정보를 이용하여 위의 문제를 해결할 수 있다. 예를 들어, 부분은닉서명을 사용하여 은행은 모든 전자화폐에 만료부(expiration data)와 같은 합의된 공통정보를 삽입하여 사용자(서명의뢰자)에게 발행한다. 은행은 전자화폐에 삽입된 공통정보를 통하여 후에 사용자가 사용하여 기간 만료된 전자화폐는 데이터베이스에서 제거하고 만료일이 지나지 않은 유효한 전자화폐만을 데이터베이스에 보관함으로써 방대한 데이터베이스 구축에 대한 부담을 해소하고 전자화폐의 이중사용문제도 해결할 수 있다. 그러므로 효과적이고도 안전한 부분은닉서명방식을 시급히 요구되고 있다.

본 논문에서는 계산적 Diffie-Hellman 문제의 어려움에 기반하는 서명자와 서명의뢰자간의 3-pass 프로토콜로 서명이 생성되는 효율적인 ID 기반 은닉서명 방식과 ID 기반 부분은닉서명 방식을 제안한다. 제안하는 ID 기반 부분은닉서명 방식은 기존의 부분은닉서명방식에 비하여 연산량과 통신량이 작아서 이동통신환경이나 스마트카드 등에 적용할 수 있는 효율적인 서명방식이다. 제안하는 서명 방식은 Gap Diffie-Hellman 군에서 성립하고 bilinear성질을 가진 함수를 이용하여 서명을 검증한다. 제안하는 ID 기반 부분은닉서명 방식에서 공통정보와 그에 연관된 해쉬값을 제거하면 ID 기반 은닉서명 방식이 된다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 기존의 부분은닉서명 방식들을 설명하고, 3장에서는 본 논문에서 제안하는 서명 방식에 사용된 안전성 기반 문제와 서명 검증에 사용된 함수에 대하여 설명하고 본 논문에서 제안하는 새로운 ID 기반 부분은닉서명방식과 ID 기반 은닉서명방식을 설명한다. 4장에서는 본 논문에서 제안한 ID 기반 부분은닉서명방식을 분석하고 안전성과 효율성에 대해서 살펴보고 기존의 부분은닉서명 방식들과 본 논문에서 제안한 부분은닉서명 방식을 서로 비교한다. 마지막으로 5장에서 결론을 도출한다.

II. 부분은닉서명 방식

부분은닉서명방식이란 서명자가 은닉서명을 발행할 때 그가 삽입하기를 원하는 어떠한 공통정보를 서명에 직접 삽입할 수 있도록 하는 암호방식이다. 부분은닉서명 방식은 서명자가 메시지와 그 서명 값을 제시받은 경우에 서명자는 서명 값의 정당성 여부를 검증 할 수 있어야 하지만 서명 방식 수행과정에서 얻은 정보로부터 은닉부분을 추측할 수 없고

메시지와 대응되는 서명을 서로 연관시키는 것이 계산적으로 불가능하다. 그러나 일반 은닉서명에서 서명자는 서명 내용을 전혀 알 수 없지만 부분 은닉서명에서는 서명자가 자신이 삽입한 정보가 서명에 포함된다는 것을 확신할 수 있어야 한다. 또한 서명의뢰자가 그 삽입된 공통정보를 제거하거나 변형할 수 없어야 한다. 공통정보는 전자화폐의 유효기간, 전자화폐의 금액, 티켓(anonymous ticket)의 가치(액)와 유효기간 등을 나타내는 정보로 활용할 수 있다. 공통정보는 서명의뢰자와 서명자가 사전에 서로 합의한 내용일수도 있고 서명의뢰자가 서명자에게 전달하거나 또는 서명자가 은닉서명에 포함시키기 위해 서명의뢰자에게 전달하는 내용일수도 있다. 본 논문에서 사용된 공통정보는 사전에 사용자와 서명자간에 서로 합의된 내용으로 가정한다.

부분은닉서명방식은 다음의 두 가지 성질을 만족한다.

- 부분은닉성(Partial Blindness): 서명의뢰자는 서명자로부터 메시지의 내용을 보여주지 않고 메시지에 대한 유효한 서명 값을 얻을 수 있고 서명자는 삽입하고자 하는 정보를 서명에 삽입할 수 있다.
- 익명성(Anonymity, Untraceability): 서명자는 공개되는 정보로부터 은닉부분을 추측할 수 없고 서명방식 수행과정에서 얻은 정보와 서명검증을 위해 수신한 메시지-서명 쌍을 서로 연결시킬 수 없다.

부분은닉서명방식은 암호 프로토콜 참가자의 익명성이 요구되어지는 암호 응용분야에 있어서는 필수적으로 요구되어지는 기본적인 암호 기법으로 전자투표나 전자화폐 등에 이용되고 있다.

부분은닉서명방식은 다음의 세 단계로 구성된다.

1. 초기화단계: 서명자가 시스템 파라미터를 생성, 등록(공개)하는 단계이다.
2. 서명생성단계: 서명의뢰자가 은닉서명을 받고자하는 메시지를 암호화해서 서명자에게 전달하고 서명자가 전달받은 은닉된 메시지에 그가 삽입하려는 정보를 삽입하여 서명을 해서 서명의뢰자에게 다시 전달하면 서명의뢰자는 전달받은 결과로부터 서명을 획득하는 단계이다.
3. 서명검증단계: 서명의뢰자가 서명자로부터 전달받은 결과로부터 획득한 서명이 정당한지를 검증하는 단계이다.

부분은닉서명방식은 1996년 M. Abe와 E. Fujisaki[14]에 의해 소개되었다. 이 방식은 RSA를 이용한 서명방식으로 소인수분해 문제(IFP: Integer Factorization Problem)의 어려움에 기반한 부분은닉서명방식이다. 이산대수 문제(DLP: Discrete Logarithm Problem)의 어려움에 기반한 부분은닉서명 방식으로 대표적인 것은 1997년 M. Abe와 Jan Camenisch[15]가 제안한 Schnorr 기반의 서명방식이 있다. 1998년 C. I. Fan과 C. L. Lei[16]는 이차잉여(QR: Quadratic Residues)에 기반한 부분은닉서명 방식을 발표하였다. 이들은 Rabin암호방식[17]을 사용하였다. 이후, 2001년 H. Y. Chien, J. K. Jan와 Y. M. Tseng[18]은 RSA 암호방식에 기반한 부분은닉서명 방식을 발표하였다.

본 장에서는 기존에 발표되었던 부분은닉서명 방식들에 대하여 약술한다.

2.1 Abe-Fujisaki 부분은닉서명

[초기화단계]

서명자 B는 RSA암호 방식과 같은 방법으로 p, q, $n=pq$, $\lambda=(p-1)(q-1)$와 공개 일방향 해쉬함수 H를 설정한다. c는 부분은닉서명에 삽입할 공통정보로 사전에 서명의뢰자와 서명자간에 서로 합의된 내용이다. 공통정보는 전자화폐의 유효기간, 전자화폐의 금액, 티켓의 가치(액)와 유효기간등을 나타내는 정보로 활용할 수 있다.

[서명생성단계]

서명의뢰자 A는 메시지 M에 대한 부분은닉서명을 의뢰하기 위해 난수 $r \in {}_RZ_n^*$을 선택하고 소수생성함수 τ를 이용하여 $e_c=\tau(c)$를 계산한다. $Z \equiv H(M)r^{e_c} \bmod n$을 계산하여 서명자 B에게 Z을 전송한다. 서명의뢰자 A로부터 Z를 전송 받은 서명자 B는 소수생성함수 τ를 이용하여 $e_c=\tau(c)$를 계산하고 $e_c d_c \equiv 1 \bmod \lambda$를 만족하는 비밀값 d_c를 구한다. d_c를 이용하여 $T \equiv Z^{d_c} \bmod n$를 계산하고 T를 서명의뢰자 A에게 전송한다. 서명자 B로부터 T를 전달받은 서명의뢰자 A는 자신이 처음 선택한 난수 r로 T를 나누어 메시지 M에 대한 서명 $S \equiv \frac{T}{r} \equiv H(M)^{d_c} \bmod n$를 획득한다.

[서명검증단계]

메시지 M의 서명 $S \equiv H(M)^{d_c} \bmod n$의 검증은 $S^{e_c} \equiv H(M) \bmod n$이 성립하는지 확인함으로써 이루어진다.

서명의뢰자(A)		서명자(B)
$r \in_R Z_n^*$을 선택 $e_c = r(c)$ $Z \equiv H(M) r^{e_c} \bmod n$ $S \equiv \frac{T}{r}$ $\equiv H(M)^{d_c} \bmod n$	--- Z ---> <-- T ---	$e_c = r(c)$ $e_c d_c \equiv 1 \bmod \lambda$ $T \equiv Z^{d_c} \bmod n$

〔그림 1〕 Abe-Fujisaki 부분은닉서명 생성단계

2.2 Abe-Camenisch 부분은닉서명

[초기화단계]

Schnorr 암호방식과 같은 시스템 파라미터 p, q, g와 공개 일방향 해쉬함수 H를 사용하며 서명자 B는 비밀키 $x_1, x_2 \in Z_q^*$에 대응되는 공캐키 $y_1 = g^{x_1}$, $y_2 = g^{x_2}$를 설정한다. c는 부분은닉서명에 삽입할 공통정보로 사전에 서명의뢰자와 서명자간에 서로 합의된 내용이다. 공통정보는 전자화폐의 유효기간, 전자화폐의 금액, 티켓의 가치(액)와 유효기간등을 나타내는 정보로 활용할 수 있다.

[서명생성단계]

서명의뢰자 A가 서명자 B에게 메시지 M에 대한 부분은닉서명을 요청하면 서명자 B는 난수 $k \in_R Z_q$를 선택하고 $Z \equiv g^k \bmod p$를 계산하여 Z를 서명의뢰자 A에게 전송한다. Z를 전달받은 서명의뢰자 A는 난수 $a, b \in_R Z_q$를 선택하고 $t \equiv Zg^a (y_1^c y_2)^b \bmod p$, $w = H(c \| M \| t)$, $r = w - a \bmod q$을 계산하여 서명자 B에게 r을 전송한다. 서명의뢰자 A로부터 r를 전송 받은 서명자 B는 $s' = \frac{k - r}{cx_1 + x_2} \bmod q$을 계산하여 서명의뢰자 A에게 s'을 전송한다. 서명자 B로부터 s'을 전달받은 서명의뢰자 A는 $s \equiv s' + b \bmod q$을 계산하여 메시지 M에 대한 서명 $Sig = (c, w, s)$를 획득한다.

[서명검증단계]

메시지 M의 서명 $Sig = (c, w, s)$의 검증은 $w = H(c \| M \| g^w (y_1^c y_2)^s)$이 성립하는지 확인함으로써 이루어지며 식 성립과정은 다음과 같다.

$$
\begin{aligned}
& g^w (y_1^c y_2)^s \\
&= g^w (y_1^c y_2)^{s'+b} \\
&= g^w (y_1^c y_2)^{s'} (y_1^c y_2)^b \\
&= g^w (g^{x_1 c s'} g^{x_2 s'}) (y_1^c y_2)^b \\
&= g^{w + s'(x_1 c + x_2)} (y_1^c y_2)^b \\
&= g^{w + \frac{k-r}{cx_1 + x_2}(x_1 c + x_2)} (y_1^c y_2)^b \\
&= g^{w+k-r} (y_1^c y_2)^b \\
&= g^{w+k-w+a} (y_1^c y_2)^b \\
&= g^{k+a} (y_1^c y_2)^b \\
&= g^k g^a (y_1^c y_2)^b \\
&= Z g^a (y_1^c y_2)^b \\
&= t
\end{aligned}
$$

이므로

$$
\begin{aligned}
w &= H(c \| M \| t) \\
&= H(c \| M \| g^w (y_1^c y_2)^s)
\end{aligned}
$$

2.3 Fan-Lei 부분은닉서명

시스템 파라미터는 Rabin 암호방식과 같다. 서명자 B는 $p \equiv q \equiv 3 \bmod 4$를 만족하는 서로 다른 큰 소수 p, q를 선택하고 $n = pq$를 계산한다. H는 일방향 해쉬 함수이고, c는 부분은닉서명에 삽입할 공통정보로 사전에 서명의뢰자와 서명자간에 서로 합의된 내용이다. 공통정보는 전자화폐의 유효기간, 전자화폐의 금액, 티켓의 가치(액)와 유효기간등을 나타

서명의뢰자(A)		서명자(B)
$a, b \in_R Z_q$를 선택 $t \equiv Zg^a (y_1^c y_2)^b \bmod p$ $w = H(c \| M \| t)$ $r = w - a \bmod q$ $s \equiv s' + b \bmod q$ 서명 $Sig = (c, w, s)$ 획득	<---------- Z ---------- ---------- r ----------> <---------- s' ----------	$k \in_R Z_q$을 선택 $Z \equiv g^k \bmod p$을 계산 $s' = \frac{k - r}{cx_1 + x_2} \bmod q$

〔그림 2〕 Abe-Camenisch 부분은닉서명 생성단계

서명의뢰자(A)		서명자(B)
$u, v \in {}_RZ_n^*$ 선택 $\alpha \equiv H(M)(u^2+v^2) \bmod n$	---------- α ---------->	
	<---------- x ----------	$x \in {}_RZ_n^*$ 선택 s.t $H(c)(\alpha(x^2+1))^3 \bmod n$은 이차잉여
$b \in {}_RZ_n^*$ 선택 $\delta = b^4 \bmod n$ $\beta = \delta(u-vx) \bmod n$	---------- β ---------->	
		$\lambda = \beta^{-1} \bmod n$ $t^8 \equiv H(c)(\alpha(x^2+1))^3\lambda^6 \bmod n$ t^8의 근 중의 하나인 t를 선택
$w = \delta\lambda(ux+v) \bmod n$ $s = b^3 t \bmod n$ 서명 $Sig = (c, w, s)$ 획득	<--------- t, λ ----------	

〔그림 3〕 Fan-Lei 부분은닉서명 생성단계

내는 정보로 활용할 수 있다.

[서명생성단계]

서명의뢰자 A는 메시지 M에 대한 부분은닉서명을 의뢰하기 위해 난수 $u, v \in {}_RZ_n^*$를 선택하여 $\alpha \equiv H(M)(u^2+v^2) \bmod n$를 계산하고 서명자 B에게 α를 전송한다. α를 전송받은 서명자 B는 Z_n^*상에서 $H(c)(\alpha(x^2+1))^3 \bmod n$가 QR이 되는 난수 $x \in {}_RZ_n^*$을 선택하여 서명의뢰자 A에게 x를 전송한다. x를 전송받은 서명의뢰자 A는 난수 $b \in {}_RZ_n^*$를 선택하고 $\delta = b^4 \bmod n$, $\beta = \delta(u-vx) \bmod n$를 계산하여 서명자 B에게 β를 전송한다. β를 전송받은 서명자 B는 $\lambda = \beta^{-1} \bmod n$를 계산한다. 서명자 B는 $t^8 \equiv H(c)(\alpha(x^2+1))^3\lambda^6 \bmod n$를 계산하고 t^8의 근 중의 하나인 t를 선택하여 λ와 t를 서명의뢰자 A에게 전송한다. λ와 t를 전송받은 서명의뢰자 A는 $w = \delta\lambda(ux+v) \bmod n$와 $s = b^3 t \bmod n$를 계산하여 메시지 M에 대한 서명 $Sig = (c, w, s)$를 획득한다.

[서명검증단계]

메시지 M의 서명 $Sig = (c, w, s)$의 검증은 $s^8 \equiv H(c)(H(M)(w^2+1))^3 \bmod n$이 성립하는지 확인함으로써 이루어지며 식 성립과정은 다음과 같다.

$$
\begin{aligned}
w &= \delta\lambda(ux+v) \\
&= \delta\beta^{-1}(ux+v) \\
&= \delta\delta^{-1}(u-vx)^{-1}(ux+v) \\
&= (ux+v)(u-vx)^{-1}
\end{aligned}
$$

이므로

$$
\begin{aligned}
s^8 &= (b^3 t)^8 = (b^4)^6 t^8 \\
&= \delta^6 H(c)(\alpha(x^2+1))^3\lambda^6 \\
&= H(c)[\alpha(x^2+1)\delta^2\lambda^2]^3 \\
&= H(c)[H(M)(u^2+v^2)(x^2+1)\delta^2\beta^{-2}]^3 \\
&= H(c)[H(M)(u^2+v^2)(x^2+1)\delta^2\delta^{-2}(u-vx)^{-2}]^3 \\
&= H(c)[H(M)(u^2x^2+v^2x^2+u^2+v^2)(u-vx)^{-2}]^3 \\
&= H(c)\{H(M)[(ux+v)^2+(u-vx)^2](u-vx)^{-2}\}^3 \\
&= H(c)\{H(M)[(ux+v)^2(u-vx)^{-2}+1]\}^3 \\
&= H(c)\{H(M)[((ux+v)(u-vx)^{-1})^2+1]\}^3 \\
&= H(c)[H(M)(w^2+1)]^3 \mod n
\end{aligned}
$$

2.4 Chien-Jan-Tseng 은닉서명

[초기화단계]

서명자 B는 RSA암호 방식과 같은 방법으로 비밀키 d, 공개키 e를 설정한다. H는 일방향 해쉬 함수이고, c는 부분은닉서명에 삽입할 공통정보로 사전에 서명의뢰자와 서명자간에 서로 합의된 내용이다. 공통정보는 전자화폐의 유효기간, 전자화폐의 금액, 티켓의 가치(액)와 유효기간등을 나타내는 정보로 활용할 수 있다.

[서명생성단계]

서명의뢰자 A는 메시지 M에 대한 부분은닉서명을 의뢰하기 위해 난수 $r, u \in {}_RZ_n^*$를 선택하여 $\alpha \equiv r^e H(M)(u^2+1) \bmod n$를 계산하고 서명자 B에게 α를 전송하고 서명자 B는 난수 $x \in {}_RZ_n^*$을 선택하여 서명의뢰자 A에게 x를 전송한다. x를 전송받은 서명의뢰자 A는 난수 $r' \in {}_RZ_n^*$를 선택하고 $b = r \cdot r'$, $\beta = b^e(u-x) \bmod n$를 계산하여 서명자 B에게 β를

서명의뢰자(A)		서명자(B)
$r, u \in {}_R\mathbb{Z}_n^*$를 선택		
$a \equiv r^e H(M)(u^2+1) \mod n$	---------- a --------->	$x \in {}_R\mathbb{Z}_n^*$
	<--------- x ----------	
$r' \in {}_R\mathbb{Z}_n^*$		
$b = r \cdot r'$		
$\beta = b^e(u-x) \mod n$		
	---------- β --------->	$\lambda = \beta^{-1} \mod n$
$w = (ux+1)\lambda b^2 \mod n$	<-------- t, λ ---------	$t = H(c)^d(a(x^2+1)\lambda^2)^{2d} \mod n$
$s = t r^2 r'^4 \mod n$		
서명 $Sig = (c, w, s)$ 획득		

〔그림 4〕 Chien-Jan-Tseng 부분은닉서명 생성단계

전송한다. β를 전송받은 서명자 B는 $\lambda = \beta^{-1} \mod n$와 $t = H(c)^d(a(x^2+1)\lambda^2)^{2d} \mod n$를 계산하여 λ와 t를 서명의뢰자 A에게 전송한다. λ와 t를 전송받은 서명의뢰자 A는 $w = (ux+1)\lambda b^2 \mod n$와 $s = t r^2 r'^4 \mod n$를 계산하여 메시지 M에 대한 서명 $Sig = (c, w, s)$를 획득한다.

[서명검증단계]

메시지 M의 서명 $Sig = (c, w, s)$의 검증은 $s^e \equiv H(c)\,H(M)^2(w^2+1)^2 \mod n$이 성립하는지 확인함으로써 이루어지며 식 성립과정은 다음과 같다.

$$
\begin{aligned}
w &= (ux+1)\lambda b^2 \\
&= (ux+1)\, b^{-e}(u-x)^{-1} b^e \\
&= (ux+1)\,(u-x)^{-1}
\end{aligned}
$$

이므로

$$
\begin{aligned}
s^e &= (t r^2 r'^4)^e \\
&= \{H(c)^d[a(x^2+1)\lambda^2]^{2d} r^2 r'^4\}^e \\
&= \{H(c)^d[r^e H(M)(u^2+1)(x^2+1) \\
&\qquad b^{-2e}(u-x)^{-2}]^{2d} r^2 r'^4\}^e \\
&= \{H(c)^d[r^e H(M)(u^2+1)(x^2+1) \\
&\qquad r^{-2e} r'^{-2e}(u-x)^{-2}]^{2d} r^2 r'^4\}^e \\
&= \{H(c)^d[H(M)(u^2+1)(x^2+1) \\
&\qquad (u-x)^{-2}]^{2d} r^2 r'^{-4} r^2 r'^4\}^e \\
&= H(c)[H(M)(u^2+1)(x^2+1)(u-x)^{-2}]^2 \\
&= H(c)[H(M)(u^2x^2+x^2+u^2+1)(u-x)^{-2}]^2 \\
&= H(c)\{H(M)[(ux+1)^2+(u-x)^2](u-x)^{-2}\}^2 \\
&= H(c)\{H(M)[(ux+1)^2(u-x)^{-2}+1]\}^2 \\
&= H(c)[H(M)(w^2+1)]^2 \\
&= H(c)H(M)^2(w^2+1)^2 \mod n
\end{aligned}
$$

Ⅲ. 새로운 ID 기반의 부분은닉서명

제안한 ID 기반 부분은닉서명방식을 설명하기에 앞서 우선 제안한 방식에 사용된 안전성 기반 문제와 서명 검증에 사용된 함수에 대하여 먼저 3.1절에서 설명하고 3.2절에서는 본 논문에서 제안한 방식의 기반이 되는 Cha-Cheon의 ID 기반 서명 방식을 설명한다. 그리고 3.3절에서는 본 논문에서 제안한 새로운 ID 기반 부분은닉서명방식을 소개한다.

3.1 GDHP와 Weil-pairing

관용 암호 방식에서의 키 관리 문제 등을 해결하기 위하여 1976년 W. Diffie와 M. Hellman[19]이 공개키 암호 방식의 개념을 제안한 이후 IFP나 DLP에 기반한 여러 공개키 암호 방식들이 제안되었다. DLP를 이용한 암호 방식의 안전성은 Diffie-Hellman 시스템의 어려움에 기반하고 있다. Diffie-Hellman 문제는 계산적 Diffie-Hellman 문제, 결정적 Diffie-Hellman 문제, Gap Diffie-Hellman 문제로 분류되며 본 논문에서 사용하는 Diffie-Hellman 문제를 정리하면 다음과 같다.

- 계산적 Diffie-Hellman 문제(CDHP : Computational Diffie-Hellman Problem)
  : P, aP와 bP로부터 abP를 계산하는 문제
- 결정적 Diffie-Hellman 문제(DDHP : Decisional Diffie-

Hellman Problem)

: P, aP, bP와 cP로부터 $c = ab \in Z/\ell$ 인지를 결정하는 문제

G은 타원곡선 F_ℓ 위의 점들로 이루어진 군으로 생성원 P를 갖는 순환군(cyclic group)이고 $a, b, c \in Z/\ell$ 이다. 위 문제들 사이의 관계를 살펴보면 CDHP가 해결되면 DDHP가 해결됨을 알 수 있다. 그러나 이들의 동치관계에 대하여 수많은 노력이 있었지만 그 역의 성립에 대하여는 알려진 사실이 없다. 이에 대하여 2001년 T. Okamoto와 D. Pointcheval[20]은 CDHP와 DDHP 해결의 어려움에 차이가 있을 경우, 이 차이에 기반한 서명 방식의 존재가능성을 제시하였다. 그들은 CDHP의 해결은 어려우면서, DDHP의 해결은 쉬운 군(Group)을 Gap Diffie-Hellman(GDH)군이라고 정의하고 이러한 문제를 GDH 문제라고 하였다. 즉,

- Gap Diffie-Hellman 문제(GDHP : Gap Diffie-Hellman Problem)

: P, aP와 bP로부터 DDH Oracle을 이용하여 abP를 계산하는 문제

GDHP 특성을 만족하는 예로는 Weil-pairing이 있다. GDH군을 찾기 위해 많은 학자들의 연구가 이루어지고 있지만, Weil-pairing과 같은 bilinear 함수를 적용한 초특이 타원곡선을 제외하고는 현재까지 알려진 GDH군은 존재하지 않는다. Weil-pairing은 초특이 타원곡선상에서 정의되는 bilinear 함수로써 정의는 다음과 같다.[21]

G_1과 G_2는 위수가 소수 ℓ인 순환군이다. G_1은 타원곡선 F_ℓ 위의 점들로 이루어진 군이고 G_2는 F_{ℓ^2}의 부분군으로 G_1은 덧셈군이며 G_2는 곱셈군이 된다. 함수 $e: G_1 \times G_1 \rightarrow G_2$가 다음 조건을 만족하면 e를 Weil-pairing이라고 한다.

- Bilinearity

: 임의의 $P, Q, R \in G_1$와 $a, b \in Z/\ell$에 대하여

$e(aP, bQ) = e(P, Q)^{ab}$ 또는

$e(P+Q, R) = e(P, R) \cdot e(Q, R)$,

$e(P, Q+R) = e(P, Q) \cdot e(P, R)$를 만족한다.

- Identity

: 임의의 $P \in G_1$에 대하여 $e(P, P) = 1$를 만족한다.

- Alternation

: 임의의 $P, Q \in G_1$에 대하여

$e(P, Q) = e(Q, P)^{-1}$를 만족한다.

- Non-degeneracy

: 임의의 $Q \in G_1$에 대하여 $e(P, Q) = 1$ 이면 P는 무한원점 (O)이다.

- Efficiency

: $e(P, Q)$의 계산이 효율적인 알고리즘이 존재한다.

타원곡선 위의 점 P, aP, bP, cP가 주어졌다고 가정하자. 이 때, CDHP 즉, P, aP, bP가 주어졌을 때 abP를 구하는 문제는 쉽게 해결되지 않는다. 그러나 DDHP 즉, P, aP, bP, cP가 주어졌을 때 $abP = cP$가 성립하는지 결정하는 문제는 Weil -pairing을 사용하여 $e(aP, bP) = e(P, cP)$가 성립하는지를 확인함으로써 쉽게 해결할 수 있다. 식 $e(aP, bP) = e(P, cP)$이 성립하면 (P, aP, bP, cP)은 DDH 쌍이 된다. 따라서 이들은 GDHP 특성을 만족하는 예로써 암호 방식 등에 사용할 수 있다.

2001년 D. Bonech, B. Lynn와 H. Shacham[22]은 타원곡선상에서의 이산대수문제(DLP: Discrete Logarithm Problem)의 공격에 이용되었던 Weil-pairing을 암호에 응용하여, GDH군에서 실제로 구현 가능한 새로운 서명 방식을 제안하였다. 그들은 서명을 수신한 사람은 누구든지 수신된 서명의 정당성을 쉽게 확인할 수 있어야 하지만, 서명의 생성자 이외에는 누구도 서명을 생성할 수 없어야한다는 사실에 착안하여 GDHP 특성을 만족하는 예를 찾았다. 그리고 같은 년도에 D. Boneh와 D. Franklin[23]은 Weil-pairing을 이용한 ID 기반의 암호 방식도 제안하였으며 2003년에는 J. Cha와 J. Cheon[24]이 GDH군에서의 ID 기반 서명 방식을 제안하였다. GDH군을 이용한 새로운 형태의 암호 방식은 최근 활발히 연구되고 있다.

3.2 Cha-Cheon ID 기반 서명

[초기화단계]

- G : 소수 ℓ을 위수로 가지는 GDH군
- P : G의 생성원
- e : bilinear 함수
- $H_1: \{0,1\}^* \times G \rightarrow Z/\ell$, $H_2: \{0,1\}^* \rightarrow G$: 충돌 회피 해쉬함수
- ID_B : B의 ID
- b ($\in Z/\ell$) : 서명자 B의 마스터키

서명의뢰자(A)		서명자(B)
난수 $r \in Z/\ell$ 선택 $U = r(T + Q_B)$ $h_1 = H_1(M, U)$ $h_2 = H_3(C)$ $X = (r^{-1}h_1 + h_2)Q_B$ $V = rY$ 서명 $sig = (C, U, V)$ 획득	<---------- T ---------- ---------- X ---------->\n<---------- Y ----------	난수 $t \in Z/\ell$ 선택 $T = tQ_B$ $h_2 = H_3(C)$ $Y = (bX + th_2D_B)$

〔그림 5〕 제안하는 ID 기반 부분은닉 서명생성단계

- $Q_B = H_2(ID_B)$: B의 ID와 관련된 공개키
- $D_B = b \cdot H_2(ID_B) = bQ_B$
  : B의 ID와 관련된 비밀키
- $P_B = bP$: 공개
- M : 서명될 메시지

[서명생성단계]

서명자 B는 난수 $r \in Z/\ell$를 선택하고 $U = rQ_B$, $h = H_1(M, U)$와 $V = (r+h)D_B$를 계산하여 $sig = (U, V)$을 메시지 M에 대한 서명으로 정의한다.

[서명검증단계]

메시지 M의 서명 sig의 검증은 bilinear 함수 e를 사용하여 $e(P_B, U + hQ_B) = e(P, V)$인지 확인함으로써 이루어진다. 식 성립과정은 다음과 같다.

$$
\begin{aligned}
& e(P_B, U + hQ_B) = e(bP, rQ_B + hQ_B) \\
& = e(P, (r+h)Q_B)^b \\
& = e(P, (r+h)bQ_B) \\
& = e(P, (r+h)D_B) \\
& = e(P, V)
\end{aligned}
$$

3.3 제안하는 ID 기반 부분은닉서명

1984년 Shamir[25]는 가입자의 개인 신분정보를 일방향 함수(one-way function)로 하여 공개키를 형성하는 ID 기반 시스템 개념을 제안하여 기존의 인증서(certification) 기반 공개키 기반구조(PKI: Public Key Infrastructure)의 키 관리 절차를 간단히 하였다. 이후 ID 기반의 암호 방식 및 서명 방식은 대부분 IFP를 기반으로 하여 제안되었다. Y. Desmedt와 J. Quisquater[26]는 일방향 함수의 계산 복잡성을 이용하는 대신에 장치의 tamperfreeness에 기반하는 방식을 제안하고 H. Tanaka[27]는 DLP와 IFP 둘 다를 기반으로 하는 혼합된 형태로써 threshold 방식을 이용하여 제안하였다. DLP를 기반으로 한 암호 방식은 S. Tsujii, T. Itho와 K. Kurosawa[28]에 의해 제안되었다. 최근 D. Boneh와 D. Franklin[23]은 Weil-pairing을 이용한 새로운 ID 기반의 암호 방식을 제안하고 이를 기초로 하여 J. Cha와 J. Cheon[24]는 ID 기반의 서명 방식을 제안하였다.

본 논문은 [24]의 서명 방식을 토대로 한 ID 기반 은닉서명방식과 ID 기반 부분은닉서명 방식을 제안한다. 본 논문에서 제안하는 방식들은 기존 방식과 달리 GDHP를 기반으로 하고 있으며 서명검증과정은 Weil-pairing과 같은 bilinear함수를 사용하여 이루어진다. 다음은 제안하는 ID 기반 부분 은닉 서명 방식의 초기화단계, 서명생성단계, 서명검증단계이다.

[초기화단계]

- G : 소수 ℓ을 위수로 가지는 GDH군
- P : G의 생성원
- e : bilinear 함수
- $H_1 : \{0,1\}^* \times G \rightarrow Z/\ell$,
  $H_2 : \{0,1\}^* \rightarrow G$, $H_3 : \{0,1\}^* \rightarrow Z/\ell$
  : 충돌 회피 해쉬함수
- ID_B : B의 ID
- b ($\in Z/\ell$) : 서명자 B의 마스터키
- $Q_B = H_2(ID_B)$: B의 ID와 관련된 공개키
- $D_B = b \cdot H_2(ID_B) = bQ_B$
  : B의 ID와 관련된 비밀키
- $P_B = bP$: 공개
- C : 부분은닉서명에 삽입할 공통정보로 사전에 서명의뢰자와 서명자간에 서로 합의된 내용이다. 공통정보는 전자화폐의 유효기간, 전자화폐의 금액, 티켓의 가치(액)와 유효기간등을 나타내는 정보로 활용할 수 있다.
- M : 서명될 메시지

[서명생성단계]

서명의뢰자 A에게 서명요청을 받은 서명자 B는 난수 $t \in Z/\ell$를 선택하여 $T = tQ_B$를 계산하고 서명의뢰자 A에게 T를 전달한다. T를 전달받은 서명의뢰자 A는 메시지 M을 은닉하기 위해 난수 $r \in Z/\ell$을 $U = r(T + Q_B)$, $h_1 = H_1(M, U)$, $h_2 = H_3(C)$와 $X = (r^{-1}h_1 + h_2)Q_B$를 계산하여 서명자 B에게 X를 전송한다. X를 전송 받은 서명자 B는 $h_2 = H_3(C)$와 $Y = (bX + th_2D_B)$를 계산하여 서명의뢰자 A에게 Y를 전송한다. 서명의뢰자 A는 전달받은 Y를 자신이 처음 선택한 난수 r로 곱하여 $V = rY$를 계산하고 서명 $sig = (C, U, V)$를 획득한다.

[서명검증단계]

메시지 M의 서명 $sig = (C, U, V)$의 검증은 $(P, P_B, h_1Q_B + h_2U, V)$가 DDH쌍인지 확인함으로써 이루어진다. 즉, bilinear 함수 e를 사용하여 $e(P_B, h_1Q_B + h_2U) = e(P, V)$인지 확인한다. 식 성립과정은 다음과 같다.

$$
\begin{aligned}
& e(P_B, h_1Q_B + h_2U) \\
&= e(bP, h_1Q_B + h_2r(T + Q_B)) \\
&= e(P, h_1Q_B + h_2rtQ_B + h_2rQ_B)^b \\
&= e(P, br(r^{-1}h_1Q_B + h_2tQ_B + h_2Q_B)) \\
&= e(P, r(b(r^{-1}h_1 + h_2)Q_B + h_2tbQ_B)) \\
&= e(P, r(bX + th_2D_B)) \\
&= e(P, rY) \\
&= e(P, V)
\end{aligned}
$$

제안하는 ID 기반 부분은닉서명 방식에서 공통정보 C와 그에 연관된 값 $h_2 = H_3(C)$를 제외하면 본 논문에서 제안하는 방식은 ID 기반 은닉서명 방식이 된다. 제안하는 ID 기반 은닉서명 방식의 안전성은 ID 기반 부분은닉서명 방식과 같다.

Ⅳ. 제안하는 ID 기반 부분은닉서명 분석

본 장에서는 제안하는 ID 기반의 부분은닉서명 방식이 전자서명요구조건인 유일성, 위조 불가능성, 진위 확인의 용이성, 거부의 불가능성의 조건을 만족함을 보인다. 그리고 제안하는 서명방식이 랜덤성을 제공하고 있음을 보이고 부분은닉서명이 갖추어야 할 부분은닉성과 익명성의 조건을 만족함을 보인다. 또한 제안하는 서명방식의 안전성과 효율성에 대하여 살펴보고 기존에 발표되었던 부분은닉서명방식들과 본 논문에서 제안하는 ID 기반 부분은닉서명방식을 서로 비교한다.

4.1 전자서명조건

제안하는 서명 방식은 전자 서명이 갖는 요구 조건인 유일성, 위조 불가능성, 진위 확인의 용이성, 거부의 불가능성의 조건을 모두 만족한다. 서명 $sig = (C, U, V)$에는 서명자 B의 마스터키 b가 삽입되었기 때문에 서명자 B이외의 어느 누구도 서명을 생성할 수 없고 또한 서명 $sig = (C, U, V)$에는 서명의뢰자 A의 난수 r이 삽입되었기 때문에 서명을 위조할 수도 없다. 그리고 제안하는 서명방식은 bilinear 함수를 이용하여 누구든지 서명의 진위 여부를 쉽게 확인할 수 있으며, 서명생성단계에서 서명자 B의 마스터키 b가 사용되기 때문에 사용자 B만이 합법적인 서명을 생성할 수 있다. 만약 서명자 B가 후에 자신이 서명한 사실을 부인할 경우 특수서명인 부인 방지 서명을 이용해서 서명의 부인을 방지할 수 있다.

4.2 랜덤성

제안하는 서명 방식은 랜덤화 특성을 갖는다. 서명자 B는 서명생성단계에서 서명을 생성하기 전에 서명의뢰자 A로부터 전달받은 은닉된 데이터 X에 비밀난수 t를 삽입한다. 서명의뢰자 A가 서명에 삽입된 난수 t를 제거하거나 수정하려고 하더라도 $T = tQ_B$이나 $Y = (bX + th_2D_B)$로부터 t를 구하는 것은 이산대수문제이므로 난수 t를 구하는 것은 계산적으로 불가능하다. 이러한 랜덤화 특성으로 인하여 선택평문공격(chosen plaintext attacks)으로부터 제안한 부분은닉서명은 안전하다.

4.3 부분은닉성

서명자 B가 서명의뢰자 A로부터 전달받은 X는 서명의뢰자 A가 선택한 비밀 난수 r을 곱한 U와 메시지 M을 함께 해쉬함수 H_1으로 적용한 다음 그 값을 다시 난수 r의 역원과 Q_B로 곱한 결과값이기 때문에 서명자 B는 자신이 서명할 메시지 M에 대한 내용을 전혀 알 수가 없다. 그러나 서명자 B는 서명

$sig=(C, U, V)$에 그가 삽입하고자하는 정보 C를 삽입할 수는 있다. 그러므로 제안하는 서명방식에서는 서명의뢰자가 서명자에게 메시지의 내용을 보여주지 않고 메시지에 대한 유효한 서명을 얻을 수 있고, 서명자는 비록 서명 내용을 전혀 알 수 없더라도 공통정보를 은닉서명에 포함시킬 수 있다. 그리고 서명자 B가 공통정보 C를 자신이 직접 서명에 삽입하므로 서명자 B는 삽입한 정보 C가 서명에 포함된다는 것을 확신할 수 있다. 또한 서명 $sig=(C, U, V)$의 $V=rY=r(bX+th_2D_B)$ 값은 공통정보 C에 대한 해쉬함수 H_3의 값 $h_2=H_3(C)$와 서명자 B의 마스터키 b와 비밀 난수 t로 이루어진 값이기 때문에 서명의뢰자 A는 서명 $sig=(C, U, V)$에 삽입된 공통정보 C를 제거하거나 변형할 수 없다.

4.4 익명성

서명 $sig=(C, U, V)$에는 서명의뢰자 A의 신원을 연관시킬 정보가 아무것도 존재하지 않고 $U=r(T+Q_B)$나 $V=rY$로부터 은닉정보 r을 구하는 것은 DLP이므로 계산상 불가능하다. 그러므로 서명자 B는 부분은닉서명방식을 통한 자신의 서명생성단계 수행과정에서 얻은 정보와 서명검증을 위해 수신한 메시지-서명 쌍을 서로 연결시키는 것은 불가능하다. 따라서 제안하는 서명방식은 서명의뢰자의 익명성을 보호하며 서명의뢰자의 신원을 추정하거나 추적하는 것이 불가능하다.

4.5 안전성

제안하는 방식은 [24]의 서명방식을 토대로 한 ID 기반 부분은닉서명방식으로, G가 GDH군이라면, 즉, CDHP가 어렵다면, 제안하는 ID 기반 부분은닉서명 방식은 단순 위장 공격(existential forgery attack)에 대하여 안전하다.[24]

4.6 효율성

Abe-Fujisak의 부분은닉서명방식은 2회의 통신만으로 서명을 생성할 수 있다는 장점이 있지만 랜덤화 특성을 가지지 않는다는 단점이 있으며, C. I. Fan과 C. L. Lei가 제안한 부분은닉서명방식은 2002년 M. S. Hwang, C. C. Lee와 Y. C. Lai[29]에 의해서 부분은닉서명이 가져야할 추적불가능 성질을 만족하지 않음이 밝혀졌다. 본 논문에서 제안하는 부분은닉서명방식은 전자서명이 가져야할 조건, 랜덤성, 부분은닉성, 익명성을 모두 만족하며, 기존의 부분은닉서명방식과는 달리 ID 기반 인증 모델을 적용하였기 때문에 공개키 인증서가 필요 없으며, 타원곡선 암호방식을 적용하여 연산 속도를 향상시켰다. [표 1]에 기존 부분은닉서명방식들의 연산량과 본 논문에서 제안하는 서명방식의 연산량을 비교하였다. 일반적으로 타원곡선 이산대수는 이산대수에 비해 약 10배 이상의 성능향상이 있는 것으로 알려져 있다.[30] 타원곡선 암호방식은 기본적으로 키의 비트수가 유한체에서의 연산에 비해 작다. 예를 들면 타원곡선에서의 160비트는 RSA에서

〔표 1〕 제안하는 ID 기반 부분은닉서명 방식과 기존 부분은닉서명 방식 비교

			Abe-Fujisak 방식	Abe-Camenisch 방식	Fan-Lei 방식	Chien-Jan-Tseng 방식	제안하는 방식
수학적기반			RSA	DHP	Rabin	RSA	GDHP
공개키인증서			필요	필요	필요	필요	필요없음
랜덤화 특성			제공안함	제공	제공	제공	제공
추적가능성(익명성)			추적불가	추적불가	추적가능	추적불가	추적불가
익명성 제어			불가	불가	불가	불가	불가
통신횟수			2-pass	3-pass	4-pass	4-pass	3-pass
통신량			$2\|n\|$ (단, $n=1024$)	$3\|q\|$ (단, $q=160$)	$5\|n\|$ (단, $n=1024$)	$5\|n\|$ (단, $n=1024$)	$3\|\ell\|$ (단, $\ell=160$)
통신량 분석			제안하는 방식은 Abe-Fujisak방식에 비해 약 23% 제안하는 방식은 Fan-Lei방식과 Chien-Jan-Tseng방식에 비해 약 9%				
연산량	서명생성	의뢰자	2M+E+I+2H	3M+3E+H	13M+H	14M+2E	3A+I+2H
		서명자	E+I+H	M+E+I	9M+I+H	6M+2E+I+H	3A+H
	서명검증		E+2H	2M+3E+H	8M+2H	5M+E+2H	2A+P+2H

1024비트와 같은 안전성을 가진다. 그렇기 때문에 같은 연산을 하더라도 RSA 1024비트에서의 모듈라 지수승 연산과 ECC 160비트의 스칼라 곱셈 연산은 연산 자체보다는 키 비트수(약1/6) 때문에 타원곡선에서의 연산이 더 빠른 것이다. 짧은 키 길이를 갖는다는 것은 대역폭과 메모리가 작아짐을 의미한다. 그리고 타원곡선 알고리즘은 하드웨어 이식이 쉽다. 이로 인해 메모리와 처리능력이 제한된 스마트카드나 이동단말기나 호출기와 같이 휴대형 시스템에 적용하기 쉽다. 또한 타원곡선상에서의 DHP는 IFP나 유한체상의 DHP에 비해 효과적인 공격 방법이 현재까지 발견되지 않고 있다. 그러므로 본 논문에서 제안하는 ID 기반 부분은닉서명방식은 타원곡선상에서 연산이 이루어지므로 기존의 부분은닉서명방식에 비해 키의 크기를 줄여주고, 연산속도를 증가시킴으로써 서명을 생성, 검증하는데 걸리는 시간을 줄여준다. 따라서 제안한 방식은 적은 메모리 용량을 갖는 스마트카드나 휴대형 시스템에 적용할 수 있고 무선환경에서도 적용할 수 있는 간단하면서도 효과적인 서명 방식이다.

[표 1]은 본 논문에서 제안하는 ID 기반 부분은닉서명 방식과 기존의 부분은닉서명 방식을 비교한 것이다. 여기에서 M은 모듈라 곱에 대한 연산량, E는 모듈라 지수승에 대한 연산량, I는 모듈라 역원에 대한 연산량, H는 해쉬함수의 연산량, A는 타원곡선위에서 스칼라곱에 대한 연산량, P는 타원곡선위에서 pairing에 대한 연산량을 의미한다. 제안하는 ID 기반 부분은닉서명은 [표 1]에서 보듯이 기존의 부분은닉서명 방식들에 비하여 안전성을 강화시켰고 ID 기반 인증 모델을 적용하였기 때문에 기존의 부분은닉서명방식과는 달리 공개키 인증서가 필요 없으며 랜덤화 특성을 가지므로 선택평문공격으로부터 안전하다. 그리고 타원곡선상에서 연산이 이루어지므로 기존의 부분은닉서명방식에 비해 서명을 생성, 검증하는데 걸리는 시간을 줄여준다. 제안한 방식은 3번의 통신횟수로 부분은닉서명이 생성되며 기존방식에 비해 통신량을 크게 감소시킨 효율적인 서명방식이다. [표 1]의 통신량 분석에서 보듯이 제안한 방식은 Abe-Fujisak방식에 비해 약 77%의 통신량이 감소되었고 Fan-Lei방식과 Chien-Jan-Tseng방식에 비해서도 약 91%의 통신량이 감소되었다.

V. 결론 및 향후 연구방향

부분은닉서명은 은닉된 메시지에 어떠한 공통정보를 삽입할 수 있는 은닉서명방식으로, 은닉서명방식을 전자화폐시스템 등에 적용하였을 때 발생하는 데이터베이스의 무제한적인 증가 문제를 해결하여 전자상거래에 주요하게 활용된다. 그러나 최근 전자상거래가 유선통신환경에서 무선통신환경으로 이동되어감에 따라 낮은 성능의 CPU, 적은 메모리용량의 제약, 무선화로 인한 통신속도의 둔화, 통신 에러발생률의 증가 등 많은 제약조건을 갖는 무선환경에서도 적용할 수 있는 암호방식이 시급히 요구되고 있다.

본 논문에서 제안하는 ID 기반 인증 모델 부분은닉서명방식은 GDHP의 어려움에 기반하고 있으며 타원곡선상에서 연산이 이루어지므로 유한체상에서의 어느 연산보다 연산속도가 빠르고 짧은 길이의 키에 비해 동등한 안전성을 가진다. 그리고 기존의 부분은닉서명 방식에 비하여 통신량, 통신횟수, 연산량을 감소시켜 효율성을 높였다. 그러므로 제안하는 ID 기반 부분은닉서명은 낮은 연산처리 능력에 제약을 받는 무선 환경이나 스마트 카드 등과 같은 다양한 응용분야에 효과적으로 적용할 수 있다. 또한 제안하는 방식은 사용자의 정당성 확인과 동시에 사용자의 익명성을 제공하므로 전자상거래, 전자화폐, 전자투표 등의 응용분야에 적용할 수 있다. 그러나 제안한 방식은 사용자가 불법행위를 할 경우 익명성을 제어하는 기능을 수행하지는 못한다. 익명성의 제한없이 서비스를 제공하는 경우 익명성의 오용으로 인한 문제점 즉, 인터넷 범죄, 돈 세탁, 이중 투표 등의 역기능들이 발생한다. 제안한 ID 기반 부분은닉서명은 향후 연구를 통해 사용자가 익명성을 악용하는 경우 이를 추적할 수 있는 사용자 익명성 제어 기능을 추가하여 더욱 발전시킬 수 있을 것이다. 추가적으로 PSS(Provable signature scheme)을 적용한다면 위장 공격에 대한 안전성을 더욱 높일 수 있을 것이다.

참 고 문 헌

[1] D. Chaum, A. Fiat, and M. Naor, "Untraceable Electronic Cash", *Advances in Cryptology - CRYPTO '88, LNCS* 403, Springer-Verlag, pp.319~327, 1990.

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

[3] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystem", *Commun. ACM*, Vol.21, pp.120

~126, 1978.

[4] J. S. Coron, D. Naccache and J. P. Stern, "On the Security of RSA Padding", *Advances in Cryptology - CRYPTO '99, LNCS,* Vol.1666, Springer-Verlag, pp.1~18, 1999.

[5] C. I. Fan, W. K. Chen and Y. S. Yeh, "A Randomization Enhanced Scheme for Chaum's Blind Signature", *Computer Communications*, Vol.23, No. 17, pp.1677~1680, Nov. 2000.

[6] T. ElGamal, "A Public-key Crypto- system and a Signature Scheme Based on Discrete Logarithms", *Advances in Cryptology - Proceeding of Crypto '84*, Springer-Verlag, pp.10~18, 1985.

[7] T. Okamoto, "Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes", *Advances in Cryptology - Proceeding of Crypto '92*, Springer-Verlag, pp.31~53, 1993.

[8] C. P. Schnorr, "Efficient Signature Generation by Smart Cards", *Journal of Cryptology*, Vol.4, No. 3, pp.161~174, 1991.

[9] J. Camenish, J-M Piveteau and M. Stadler, "Blind Signatures Based on the Discrete Logarithm Problem", *Advances in Cryptology - EUROCRYPT '94, LNCS,* Vol.950, Springer-Verlag, pp.428~432, 1994.

[10] NIST FIPSPUB 186, *Digital Signature Standard (DSS)*, National Institute of Standards and Technology, U.S. Department of Commerce, Nov. 1994.

[11] K. Nyberg and R. Ruppel, "A New Signature Scheme Based on the DSA Giving Message Recovery", *Proc. 1st ACM Conference on Computer and Communication Security*, Fairfax, Virginia, p.4, Nov.3~5, 1993.

[12] P. Horter, M. Michels and H. Petersen, "Meta-Message Recovery and Meta-Blind Signatures Schemes Based on the Discrete Logarithm Problem and Their Applications", *Advances in Cryptology - ASIACRYPT '94, LNCS* 917, Springer-Verlag, pp.224 ~237, 1994.

[13] D. pointchevel and J. Stern, "New Blind Signatures Equivalent to Factorization", *Proc. 4th ACM Conference on Computer and Communication Security*, pp.92~99. 1997.

[14] M. Abe and E. Fujisaki, "How to Date Blind Signatures", in K. Kim and T. Matsumoto, eds. *Advances in Cryptology - ASIACRYPT '96, LNCS* 1163, Springer-Verag, pp.244~251, 1996.

[15] M. Abe and J. Camenisch, "Partially Blind Signature Schemes", *Proc. of the 1997 Symp. on Cryptography and Information Security Workshop*, 1997.

[16] C. I. Fan and C. L. Lei, "Low-computation Partially Blind Signatures for Electronic Cash", *IEICE Trans. Fundamentals*, Vol.E-81-A, No.5, pp.818~824, May 1998.

[17] M. O. Rabin, "Digitalized Signatures and Public -key Functions as Intractable as Factorization", *Technical Report, MIT/LCS/TR212*, MIT Lab., Computer Science, Cambridge, Mass., Jan. 1979.

[18] H. Y. Chien, J. K. Jan, Y. M. Tseng, "RSA-Based Partially Blind Signature with Low Computation", *Proc. of the Eighth International Conference in Parallel and Distributed Systems (ICPADS 2001).* KyungJu, Korea. pp.385~389.

[19] W. Diffe and M. Hellman, "New Direction in Cryptography", IEEE *Tranctions on Information Theory*, Vol.IT-22(6), pp.644~654, 1976.

[20] T. Okamoto and D. Pointcheval, "The Gap- Problems: A New Class of Problems for the Security of Cryptographic Schemes", *4th International Workshop on Practice and Theory in Public Key Crypto-systems, PKC 2001*, Springer-Verlag, preprint, pp.104~118, 2001.

[21] J. H. Silverman. *The Arithmatic of Elliptic Curves*, Vol.106 of Graduate Texts in Mathematics. Springer-Verlag, 1986.

[22] D. Bonech, B. Lynn and H. Shacham, "Short Signatures from the Weil Pairing", *Advances in Cryptology-Proceeding of Asiacrypt 2001*, Springer-Verlag, preprint, 2001.

[23] D. Boneh and D. Franklin, "Identity-Based Encryption from the Weil Pairing", *Proc. of Crypto '01, LNCS.* Vol.2139, pp.213~229, Springer-Verlag, 2001.

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

[25] A. Shamir, "Identity-based Crypto-systems and Signature Schemes", *Proc. of Crypto '84, LNCS*, Vol. 196, pp.47~53, Springer-Verlag, 1984.

[26] Y. Desmedt and J. Quisquater, "Public-key Systems Based on the Difficulty of Tampering", *Proc. of Crypto '86, LNCS.* Vol.263, pp.111~117, Springer-Verlag, 1986.

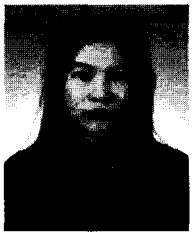
[27] H. Tanaka, "A Realization Scheme for the Identity Based Cryptosystem", *Proc. of Crypto '87, LNCS.* Vol.293, pp.341~349, Springer-Verlag, 1987.

[28] S. Tsujii, T. Itho and K. Kurosawa, "ID-based Cryptosystem using Discrete Logarithm Problem", *Electron. Lett.* Vol.23, pp.1318~1320, 1987.

[29] M. S. Hwang, C. C. Lee and Y. C. Lai, "Traceability on Low-computation Partially Blind Signatures for Electronic Cash", *IEICE Trans. Fundamentals*, Vol.E85-A, No.5, pp.1181~1182, May 2002.

[30] Certicom Corp., "Elliptic Curve Cryptosystem Tutorials and White Papers", available from http://www.certicom.ca/.

〈著者紹介〉



김 현 주 (Hyun-Jue Kim) 학생회원

1991년 2월 : 세명대학교 수학과 졸업(이학사)
1997년 2월 : 서강대학교 수학과 졸업(이학석사)
1999년 3월~현재 : 성균관대학교 전자전자 및 컴퓨터공학과 박사과정

오 수 현 (Soo-Hyun Oh)

1998년 2월 : 성균관대학교 정보공학과 졸업(공학사)
2000년 2월 : 성균관대학교 전자전자 및 컴퓨터공학과 졸업(공학석사)
2003년 8월 : 성균관대학교 전자전자 및 컴퓨터공학과 졸업(공학박사)

원 동 호 (Dong-Ho Won)

성균관대학교 전자공학과 졸업(학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구원 전임연구원
1985년~1986년 : 일본 동경공업대 객원연구원
1988년~1999년 : 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원
2002년~2003년 : 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, 정통부 지정 정보보호인증기술연구센터장, 성균관대학교 연구처장