무선환경에 적합한 Gap Diffie-Hellman 그룹을 사용한 ID 기반 은닉서명 방식

(An ID-based Blind Signature Scheme using the Gap Diffie-Hellman Group in Wireless Environments)

김 현 주 † 김 수 진 †† 원 동 호 †††
(Hyun-Jue Kim) (Soo-Jin Kim) (Dong-Ho Won)

요 약 은닉서명(blind signature scheme)은 서명문의 내용을 숨기는 서명 방식으로 서명의뢰자의 신원과 서명문을 연결시킬 수 없는 익명성을 가지며 전자화폐나 전자투표 등 주로 행위자의 행동이 노출되어서는 안되는 보안서비스에 중요하게 활용된다. 본 논문에서는 GDH군에서의 ID 기반 은닉서명 방식을 제안한다. 제안한 방식의 안전성은 CDHP의 어려움에 기반을 두며, 효율성은 두 사용자간의 2회 통신만으로 서명을 생성함으로써 기존의 은닉서명 방식을 훨씬 개선하였다. 통신횟수와 계산량이 적으므로 제안한 은닉서명 방식은 무선 PKI 환경에서도 적용할 수 있다.

키워드 : ID 기반 은닉서명 방식, Gap Diffie-Hellman 문제, Weil-pairing

Abstract Blind signature is such a signature scheme that conceals the contents of signature itself and who is the user of the signature make user's anonymity possible. For this reason, they are used in security services such as electronic cashes and electronic votes in which the behavior of actor should not be exposed. In this paper we propose an ID-based blind signature scheme from Gap Diffie-Hellman group. Its security is based on the hardness of Computational Diffie-Hellman Problem. Proposed scheme efficiently improve against existing blind signature scheme by using two-pass protocol between two users and by reducing computation process. Therefore it can be used efficiently in wireless PKI environment.

Key words : ID-based blind signature scheme, Gap Diffie-Hellman Problem, Weil-pairing

1. 서 론

급속한 정보통신망의 발전에 힘입어 등장한 전자상거래는 시간적, 공간적 제약이 없는 새로운 시장으로 부각되고 있으며 세계 각국은 이러한 시장을 선점하기 위해 전자상거래를 활성화시킬 수 있는 다양한 사이버 서비스를 제공하고 있다. 사이버 서비스는 언제 어디서든지 접근 가능하여 사용자에게 편리하게 이용될 수 있는 반면 누구든지 접근가능하기 때문에 정보의 도청, 오남용, 변조 등 불법적인 행위가 발생할 위험을 배제할 수 없다.

† 학생회원 : 성균관대학교 전기전자및컴퓨터공학부
hjkim@dosan.skku.ac.kr
†† 비 회 원 : 성균관대학교 정보통신공학부
kimsj@dosan.skku.ac.kr
††† 종신회원 : 성균관대학교 정보통신공학부 교수
dhwon@dosan.skku.ac.kr
논문접수 : 2003년 6월 21일
심사완료 : 2003년 9월 18일

실제로 사용자가 전자화폐를 전자은행으로부터 인출할 때 사용하는 일련번호는 사용자의 화폐에 대한 정보로써 이는 은행이 사용자의 현금사용상황을 역추적하는 정보가 된다. 그리하여 전자화폐는 물리적 화폐(지폐 또는 동전)와 달리 익명성이 제공되지 못하므로 그 결과 정보화사회의 핵심인 사생활의 보호를 보장할 수 없게 된다. 이를 방지하기 위해 1982년 D. Chaum이 처음으로 RSA 문제를 기반으로 하는 은닉서명 방식을 제안하였다[1]. 이 방식은 사용자가 인출할 화폐의 일련번호에 불특정한 숫자를 곱해서 은행으로 보내고 은행은 전달받은 번호를 전자현금화해서 사용자에게 넘겨주면 사용자는 사용된 불특정한 숫자로 나누게 되는데 이 경우 원래의 번호가 나타나지 않으므로 인출한 화폐의 일련번호의 익명성을 제공할 수 있다. 이 서명 방식은 사용자의 원래의 현금번호를 은행이 알 수 없도록 하여 개인의 프라이버시와 익명성을 보장한다. 그러나 이 서명 방식은 사용자가 2개의 전자화폐로부터 은행의 승인 없

이 다른 전자화폐를 만들 수 있다는 문제점이 있다. 그 이후 다양한 문제에 기반을 둔 은닉서명 방식이 소개되어 왔으나 현재까지 소개된 은닉서명 방식들은 복잡한 과정을 거쳐서 구성되어지기 때문에 좁은 대역폭을 가지고 또한 메모리용량과 계산능력도 부족한 무선환경에 적용하기에는 여러 가지 어려움이 따른다. 따라서 무선환경에서 가장 큰 부담을 주는 계산량을 줄여 줄 수 있는 간단하면서도 효과적인 은닉서명 방식을 제안하고자 한다.

본 논문에서는 계산적 Diffie-Hellman 문제의 어려움에 기반하면서 RSA기반의 은닉서명처럼 서명의뢰자가 서명자에게 은닉서명을 의뢰하면 추가적인 통신 없이 바로 서명을 생성해주는 효율적인 은닉서명 방식을 제안한다. 제안한 서명 방식은 Gap Diffie-Hellman 군에서 성립하고 bilinear성질을 가진 함수를 이용한다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 본 논문에서 제안한 새로운 은닉서명 방식에 사용된 안전성 기반 문제와 서명 검증에 사용된 함수에 대하여 설명하고, 3장에서는 기존의 은닉서명 방식을 설명하고, 4장에서는 본 논문에서 제안하는 새로운 ID 기반의 은닉서명 방식을 소개하고 제안한 방식의 안전성에 대해서 살펴본다. 5장에서는 제안한 은닉서명 방식의 효율성에 대하여 살펴보고 기존의 은닉서명 방식들과 본 논문에서 제안한 은닉서명 방식을 비교한다. 마지막으로 6장에서 결론을 도출한다.

2. Gap Diffie-Hellman Group과 Weil-pairing

본 장에서는 본 논문에서 제안한 새로운 은닉서명 방식에 사용된 안전성 기반 문제와 서명 검증에 사용된 함수에 대하여 설명한다. 2.1절에서는 제안한 은닉서명 방식에 사용된 안전성 기반 문제 즉, 계산적인 Diffie-Hellman 문제와 결정적인 Diffie-Hellman 문제 관계에서 나온 Gap Diffie-Hellman 문제를 다루고 2.2절에서는 서명 후에 검증과정에 사용되는 bilinear함수와 Weil-pairing에 대해서 설명한다.

2.1 Gap Diffie-Hellman 군

이산대수문제를 이용한 암호 및 서명 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)
  : g, $g^x \pmod p$와 $g^y \pmod p$으로부터 $g^{xy} \pmod p$를 계산하는 문제
- 결정적 Diffie-Hellman 문제(DDHP : Decisional Diffie-Hellman Problem)
  : g, $g^x \pmod p$, $g^y \pmod p$와 w으로부터 $w \equiv g^{xy} \pmod p$ 인지를 결정하는 문제

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. Pointcheval은 CDHP와 DDHP 해결의 어려움에 차이가 있을 경우, 이 차이에 기반한 서명 방식의 존재가능성을 제시하였다[2]. 그들은 CDHP의 해결은 어려우면서, DDHP의 해결은 쉬운 군(Group)을 Gap Diffie-Hellman(GDH)군이라고 정의하고 이러한 문제를 GDH 문제라고 정의하였다. 즉,

- Gap Diffie-Hellman 문제(GDHP : Gap Diffie-Hellman Problem)
  : g, $g^x \pmod p$와 $g^y \pmod p$으로부터 DDH Oracle을 이용하여 $g^{xy} \pmod p$를 계산하는 문제

이 후 2001년 D. Bonech, B. Lynn와 H. Shacham은 타원곡선상에서의 이산대수문제(DLP : Discrete Logarithm Problem)의 공격에 이용되었던 Weil-pairing을 암호에 응용하여, GDH군에서 실제로 구현 가능한 새로운 서명 방식을 제안하였다[3]. 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. Franklin은 Weil-pairing을 이용한 ID 기반의 암호 방식도 제안하였다[4]. GDH군을 이용한 새로운 형태의 암호 방식은 최근 활발히 연구되고 있다. 2003년에는 J. Cha와 J. Cheon이 GDH군에서의 ID 기반 서명 방식을 제안하였다[5]. 또 다른 GDH군을 찾기 위해 많은 학자들의 연구가 이루어지고 있지만, Weil-pairing과 같은 bilinear함수를 적용한 (초특이)타원곡선을 제외하고는 현재까지 알려진 GDH군은 존재하지 않는다.

2.2 The Weil-pairing

G_1과 G_2는 위수가 소수 ℓ인 순환군이다. G_1은 타원곡선 F_ℓ 위의 점들로 이루어진 군이며 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.

Bilinearity를 만족하는 함수 e를 bilinear함수라고 정의한다.

타원곡선 위의 점 P, aP, bP, cP가 주어졌을 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 사용하면 $e(aP,bP)=e(P,cP)$가 성립하는지를 확인함으로써 쉽게 해결할 수 있다. 식이 성립하면 (P, aP, bP, cP)은 DDH쌍이 된다. 따라서 이들은 GDHP 특성을 만족하는 예로써 암호 방식 등에 사용할 수 있다.

3. 기존 은닉서명 방식

은닉서명은 서명문의 내용을 숨기는 서명 방식으로 서명의뢰자의 신원과 서명문을 연결시킬 수 없는 익명성을 가지며 전자화폐나 전자투표 등 주로 행위자의 행동이 노출되어서는 안 되는 보안 서비스에 중요하게 활용된다. D. Chaum이후 여러 은닉서명 방식이 발표되었지만 현재 안전성을 인정받고 있는 암호 방식은 RSA와 Diffie-Hellman 방식에 거의 한정되어 있다. 본 장에서는 먼저 기존에 제안된 방식들 중 대표적인 은닉서명 방식으로 D. Chaum이 제안한 RSA 암호 방식에 기반한 은닉서명 방식과 T. Okamato가 제안한 Schnorr기반의 은닉서명 방식에 대하여 3.1절과 3.2절에서 각각 살펴보고, 3.3절에서는 최근에 제안된 C. I. Fan, W. K. Chen and Y. S. Yeh의 RSA 암호 방식에 기반한 은닉서명 방식에 대하여 살펴본다.

3.1 Chaum 은닉서명 방식

1982년 D. Chaum은 RSA 암호 방식에 기반한 은닉서명 방식을 처음으로 제안하였다[1]. 서명 방식의 안전성은 소인수분해문제(IFP : Integer Factorization Problem)의 어려움에 따른다. 그러나 이 제안한 서명 방식은 2개의 서명으로부터 정당하지 않은 서명을 만들 수 있다는 문제점이 있다. 즉, 서명의뢰자 A가 서명자 B로부터 받은 메시지 m_1, m_2에 대한 정당한 서명 $S_1=m_1^e$, $S_2=m_2^e$를 가지고 또 다른 메시지 m_1m_2에 대한 정당하지 않은 서명 $S_1S_2=(m_1m_2)^e$를 생성할 수 있다.

키 설정과정, 서명 생성과정, 서명 검증과정은 다음과 같다.

[키 설정과정]

서명자 B는 RSA암호 방식과 같은 방법으로 비밀키 d, 공개키 e를 설정한다[6].

[서명 생성과정]

A는 m에 대한 서명을 의뢰하기 위해 난수 $r\in_R Z_n$을 선택하고 $K_1\equiv r^e m \bmod n$을 계산하여 B에게 K_1을 전송한다. K_1을 전송 받은 B는 $K_2\equiv K_1^d \bmod n$을 계산하여 A에게 전송한다. A는 전달받은 K_2를 자신이 처음 선택한 난수 r로 나누어 서명 $S\equiv\frac{K_2}{r}\equiv m^d \bmod n$를 획득한다.

[서명 검증과정]

메시지 m의 서명 S를 검증하기 위해 서명자 B의 공개키 e를 이용해 $S^e\equiv m \bmod n$이 성립하는지 확인한다.

의뢰자(A)		서명자(B)
$r\in_R Z_n$을 선택		
$K_1\equiv r^e m \bmod n$을 계산	------ K_1 ----->	
$S\equiv\frac{K_2}{r}$	<----- K_2 ------	$K_2\equiv K_1^d \bmod n$을 계산
$\equiv m^d \bmod n$		

그림 1 Chaum 은닉서명 생성과정

3.2 Okamato 은닉서명 방식

1992년 T. Okamato는 Schnorr 암호 방식에 기반한 은닉서명 방식을 제안하였다[7]. 이 서명 방식의 안전성은 이산대수문제(DLP : Discrete Logarithm Problem)의 어려움에 따른다. 그러나 이 서명 방식은 RSA에 기반한 서명 방식에 비하여 프로토콜도 복잡하고 계산량도 많은 단점이 있다.

키 설정과정, 서명 생성과정, 서명 검증과정은 다음과 같다.

[키 설정과정]

서명자 B는 Schnorr암호 방식과 같은 방법으로 비밀키 x, 공개키 $y=g^x$를 설정한다[8].

[서명 생성과정]

A가 m에 대한 서명을 의뢰하기 위해 B에게 서명요청을 하면 B는 난수 $r \in_R Z_q$을 선택하고 $T^* \equiv g^r \bmod p$을 계산하여 A에게 T^*을 전송한다. T^*를 전달받은 A는 난수 $u, d \in_R Z_q$를 선택하고 $T \equiv g^u y^d T^* \bmod p$, $e \equiv h(T, m)$, $e^* \equiv e - d \bmod q$을 계산하여 B에게 e^*를 전송한다. e^*를 전달받은 B는 $S^* \equiv r - e^* x \bmod q$를 계산하여 A에게 S^*를 전송한다. S^*를 전달받은 A는 $S \equiv S^* + u \bmod q$을 계산하고 서명 $\sigma = (e, S)$를 획득한다.

[서명 검증과정]

메시지 m의 서명 S의 검증은 서명 $\sigma = (e, S)$와 B의 공개키 y를 이용해 $e \equiv h(g^S y^e, m)$이 성립하는지 확인함으로써 이루어지며 다음과 같다.

$$\begin{aligned} h(g^S y^e, m) &= h(g^{S^*+u} g^{xe}, m) \\ &= h(g^{u-e^*x+r} g^{xe}, m) \\ &= h(g^{u+xe-e^*x+r}, m) \\ &= h(g^u g^{x(e-e^*)} g^r, m) \\ &= h(g^u y^d T^*, m) \\ &= h(T, m) \\ &= e \end{aligned}$$

3.3 Fan-Chen-Yeh 은닉서명 방식

2000년 C. I. Fan, W. K. Chen and Y. S. Yeh은 랜덤화 특성을 가지는 RSA 암호 방식에 기반한 은닉서명 방식을 제안하여 D. Chaum의 은닉서명 방식을 개선하였다[9]. 이들이 제안한 은닉서명 방식은 서명의뢰자 A가 마음대로 메시지 m을 선택할 수 없기 때문에 선택적 메시지 공격이 불가능하다.

키 설정과정, 서명 생성과정, 서명 검증과정은 다음과 같다.

[키 설정과정]

서명자 B는 RSA암호 방식과 같은 방법으로 비밀키 d, 공개키 e를 설정한다.

[서명 생성과정]

A는 m에 대한 서명을 의뢰하기 위해 난수 $r \in_R Z_n^*$과 $u \in_R Z_n$를 선택하고 $a \equiv r^e h(m)(u^2+1) \bmod n$를 계산하여 B에게 a를 전송한다. a를 전송 받은 B는 난수 $x \in_R Z_n$를 계산하여 A에게 전송한다. A는 난수 $b \in_R Z_n^*$를 선택하고 $\beta \equiv b^e(u-x) \bmod n$를 계산하여 B에게 전송한다. B는 $t \equiv \{a(x^2+1)\beta^{-2}\}^d \bmod n$를 계산하여 A에게 전송한다. A는 $C \equiv (ux+1)(u-x)^{-1} \bmod n$를 계산하고 B로부터 전달받은 t를 이용하여 $S \equiv r^{-1} b^2 t \bmod n$를 계산하여 서명 $\sigma = (C, S)$를 획득한다.

[서명 검증과정]

메시지 m의 서명검증은 서명 $\sigma = (C, S)$와 B의 공개키 e를 이용해 $S^e \equiv h(m)(C^2+1) \bmod n$이 성립하는지 확인함으로써 이루어지며 다음과 같다.

$$\begin{aligned} a(x^2+1)\beta^{-2} &= r^e h(m)(u^2+1)(x^2+1)b^{-2e}(u-x)^{-2} \\ &= r^e b^{-2e} h(m)(u^2+1)(x^2+1)(u-x)^{-2} \\ &= r^e b^{-2e} h(m)[\{(ux+1)(u-x)^{-1}\}^2+1] \\ &= r^e b^{-2e} h(m)(C^2+1) \end{aligned}$$

의뢰자(A)		서명자(B)
$u, d \in_R Z_q$를 선택		$r \in_R Z_q$을 선택
$T \equiv g^u y^d T^* \bmod p$	<------ T^* ------	$T^* \equiv g^r \bmod p$을 계산
$e \equiv h(T, m)$		
$e^* \equiv e - d \bmod q$	------- e^* ------>	
	<------ S^* ------	$S^* \equiv r - e^* x \bmod q$
$S \equiv S^* + u \bmod q$		
$\sigma = (e, S)$ 서명 획득		

그림 2 Okamato 은닉서명 생성과정

의뢰자(A)		서명자(B)
$r \in_R Z_n^*$		
$u \in_R Z_n$를 선택		
$\alpha \equiv r^e h(m)(u^2+1) \mod n$	------ α ----->	
	<----- x ------	$x \in_R Z_n$
$b \in_R Z_n^*$을 선택		
$\beta \equiv b^e(u-x) \mod n$	------ β ----->	
$C \equiv (ux+1)(u-x)^{-1} \mod n$		
$S \equiv r^{-1}b^2 t \mod n$	<----- t ------	$t \equiv \{\alpha(x^2+1)\beta^{-2}\}^d \mod n$
서명 $\sigma = (C, S)$ 획득		

그림 3 Fan-Chen-Yeh 은닉서명 생성과정

이므로

$$\begin{aligned} t &= \{\alpha(x^2+1)\beta^{-2}\}^d \\ &= \{r^e b^{-2e} h(m)(C^2+1)\}^d \\ &= r b^{-2}\{h(m)(C^2+1)\}^d \end{aligned}$$

$$\begin{aligned} S &= r^{-1}b^2 t \\ &= r^{-1}b^2 r b^{-2}\{h(m)(C^2+1)\}^d \\ &= \{h(m)(C^2+1)\}^d \end{aligned}$$

그러므로

$$S^e \equiv h(m)(C^2+1) \mod n$$

4. 새로운 ID 기반의 은닉서명 방식 제안

1984년 Shamir는 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[10]. 이 후 ID 기반의 암호 방식 및 서명 방식은 대부분 IFP를 기반으로 하여 제안되었다. Y. Desmedt와 J. Quisquater는 일방향 함수의 계산 복잡성을 이용하는 대신에 장치의 tamperfreeness에 기반하는 방식을 제안하고 H. Tanaka는 DLP와 IFP 둘 다를 기반으로 하는 혼합된 형태로써 threshold 방식을 이용하여 제안하였다[11,12]. DLP를 기반으로 한 암호 방식은 S. Tsujii, T. Itho와 K. Kurosawa에 의해 제안되었다[13]. 최근 D. Boneh와 D. Franklin은 Weil-pairinig을 이용한 타원곡선에 bilinear 함수를 적용한 새로운 ID 기반의 암호 방식을 제안하고 이를 기초로 하여 J. Cha와 J. Cheon는 ID 기반의 서명 방식을 제안하였다[4,5].

본 논문은 [5]에서 제안하는 서명 방식을 사용한다. 4.1절에서 새로운 ID 기반 은닉서명 방식을 제안하고, 4.2절에서는 제안한 방식의 안전성에 대하여 살펴본다.

4.1 새로운 ID 기반 은닉서명 방식

본 논문에서 제안하는 ID 기반 은닉서명 방식은 기존의 은닉서명 방식과 달리 GDHP를 기반으로 하고 있으며 서명 검증과정은 bilinear함수를 사용하여 이루어진다. 다음은 제안하는 ID 기반 은닉서명 방식의 키 설정과정, 서명 생성과정, 서명 검증과정이다.

[키 설정과정]

- G : DDHP가 해결되는 소수 ℓ을 위수로 가지는 군
- P : G의 생성원
- e : bilinear 함수
- $H_1 : \{0,1\}^* \times G \rightarrow Z/\ell$, $H_2 : \{0,1\}^* \rightarrow G$: 충돌회피 해쉬함수
- ID_B : B의 ID
- $Q_B = H_2(ID_B)$: B의 ID와 관련된 공개키
- $D_B = b \cdot H_2(ID_B) = bQ_B$: B의 ID와 관련된 비밀키
- b ($\in Z/\ell$) : 서명자 B가 선택하는 난수로 마스터키로 사용된다.
- $P_B = bP$: 공개

[서명 생성과정]

A는 m에 대한 서명을 의뢰하기 위해 난수 $r \in Z/\ell$을 선택하고 $U = rQ_B$, $h = H_1(m, U)$, $X = hQ_B$를 계산하여 B에게 X를 전송한다. X를 전송 받은 B는 $Y = b(X + Q_B)$를 계산하여 A에게 전송한다. A는 전달받은 Y를 자신이 처음 선택한 난수 r로 곱하여 $V = rY = r(1+h)D_B$를 계산하고 서명 $\sigma = (U, V)$를

획득한다.

[서명 검증과정]

메시지 m의 서명 $\sigma=(U, V)$를 검증하기 위해 non-degenerated bilinear 함수 e를 사용하여 $(P, P_B, (1+h)U, V)$가 DDH쌍인지 확인한다. 즉, $e(P_B, (1+h)U) = e(P, V)$인지 확인한다.

$$\begin{aligned} e(P_B, (1+h)U) &= e(bP, (1+h)rQ_B) \\ &= e(P, r(1+h)Q_B)^b \\ &= e(P, r(1+h)bQ_B) \\ &= e(P, r(1+h)D_B) \\ &= e(P, V) \end{aligned}$$

제안한 은닉서명 방식은 사용자 보호와 익명성의 두 가지 조건을 모두 만족한다. 서명의뢰자 A가 서명자 B에게 메시지 m에 대한 서명을 의뢰할 때 보내는 메시지 m은 U와 함께 해쉬함수를 적용한 다음 그 값을 Q_B로 곱하여 나온 값을 전송하기 때문에 개인의 프라이버시를 보호할 수 있으며, 서명 $\sigma=(U, V)$에는 의뢰자의 신원을 연관시킬 정보가 아무것도 존재하지 않기 때문에 서명의뢰자 A의 익명성을 제공할 수 있다.

그리고 제안한 서명 방식은 전자 서명이 갖는 요구조건인 유일성, 위조 불가능성, 진위 확인의 용이성, 거부의 불가능성의 조건을 모두 만족한다. 생성된 서명 $\sigma=(U, V)$는 서명자 B의 비밀정보 b가 사용되기 때문에 서명자 B이외의 어느 누구도 서명을 만들 수 없고 또한 서명 $\sigma=(U, V)$에는 서명의뢰자 A의 난수 r이 삽입되었기 때문에 서명을 위조할 수는 없다. 그리고 제안한 서명방식은 bilinear 함수를 이용하여 누구든지 서명의 진위를 쉽게 확인할 수 있으며, 만약 서명자 B가 후에 자신이 서명한 사실을 부인하더라도 서명 $\sigma=(U, V)$에 서명자 B의 비밀정보 b가 사용되었기 때문에 서명의 진위를 확인할 수 있다.

4.2 제안한 ID 기반 은닉서명 방식의 안전성

제안한 방식은 GDH군에서의 ID 기반 은닉서명 방식으로 CDHP의 어려움에 기반하고 있으며 적응 가능한 선택 메시지(adaptively chosen message)와 주어진 ID에 대한 단순 위장 공격(existential forgery attack)에 대하여 안전하다.

다음의 게임을 수행하는 챌린저 C에 대항할 수 있는 무시할 수 없는 이익(advantage)을 가지고 있는 다항식 시간 알고리즘 A_0가 존재하지 않는다면, 서명 방식은 적응 가능한 선택 메시지와 주어진 ID에 대한 단순 위장 공격에 대하여 안전하고 말한다.

STEP 1 : 챌린저 C는 시스템 파라미터들을 A_0에게 제공한다.

STEP 2 : A_0는 다음과 같은 쿼리(query)들을 요청한다.

(a) 해쉬함수 (H_1, H_2) 쿼리

: 챌린저 C는 요청된 입력에 대한 해쉬함수 값을 계산하고 그 값을 A에게 보낸다.

(b) *Extract* 쿼리

: 챌린저 C는 주어진 ID에 관련된 비밀키를 반환한다.

(c) *Sign* 쿼리

: 챌린저 C는 주어진 ID와 메시지 m에 대한 서명을 반환한다.

STEP 3 : A_0는 (ID, m, σ)를 출력한다. 이때, ID와 (ID, m)는 각각 *Extract* 쿼리와 *Sign* 쿼리의 입력과 같지 않다.

만약 σ가 ID에 대한 m의 유효한 서명이라면 다항식 시간 알고리즘 A_0는 게임에서 이긴다.

[정리 1]

t_0의 수행시간과 이익 $\varepsilon_0 \left(\geq \frac{10(q_S+1)(q_S+q_{H_1})q_{H_2}}{\ell-1}\right)$를 갖는 제안한 은닉서명 방식에 대하여 적응 가능한 선택 메시지와 주어진 ID를 가지고 공격하는 알고리즘

의뢰자(A)		서명자(B)
난수 $r \in Z/\ell$ 선택		
$U = rQ_B$		
$h = H_1(m, U)$		
$X = hQ_B$	-------- X -------->	
$V = rY$ $= r(1+h)D_B$	<------- Y ---------	$Y = b(X+Q_B)$
$\sigma=(U, V)$ 서명 획득		

그림 4 제안하는 ID 기반 은닉서명 생성과정

A_0가 존재한다면, CDHP가 수행시간 $\frac{23 q_{H_1} q_{H_2} t_0}{\varepsilon_0(1-\frac{1}{\ell})}$ 이내에 풀릴 확률은 $\frac{1}{9}$이상이다.

[정리 2]

t_0의 수행시간과 이익 $\varepsilon_0 \left(\geq \frac{10(q_S+1)(q_S+q_{H_1})q_{H_2}}{\ell-1}\right)$를 갖는 제안한 은닉서명 방식에 대하여 적응 가능한 선택 메시지와 주어진 ID를 가지고 공격하는 알고리즘 A_0가 존재한다면, CDHP는 기대시간(expected time) $\frac{120686 q_{H_1} q_{H_2} t_0}{\varepsilon_0(1-\frac{1}{\ell})}$ 이내에 풀릴 수 있다.

q_{H_1}은 알고리즘 A_0가 H_1에게 요구하는 최대 쿼리(query) 수, q_{H_2}는 알고리즘 A_0가 H_2에게 요구하는 최대 쿼리(query) 수이고 q_S는 알고리즘 A_0의 *Sign*에 대한 최대 쿼리(query) 수이다.

[정리 1]과 [정리 2]의 증명은 [5]에 자세히 기술되어 있다.

5. 효율성 및 기존 은닉서명 방식과의 비교

본 장의 5.1절에서는 본 논문에서 제안한 은닉서명 방식의 효율성에 대하여 살펴보고, 5.2절에서는 기존에 제안된 은닉서명 방식들과 본 논문에서 제안한 은닉서명 방식을 비교한다.

5.1 제안한 ID 기반 은닉서명 방식의 효율성

최근 급속한 정보통신망의 발전으로 무선통신 사용자가 급격히 증가하고 있다. 그로 인해 각 기업들은 전자상거래, 전자결제 등의 다양한 서비스를 무선 PKI 환경에서도 제공하기 위해서 많은 노력을 하고 있다. 그러나 무선환경은 낮은 성능의 CPU, 적은 메모리용량의 제약, 무선화로 인한 통신속도의 둔화, 통신 에러발생률의 증가 등 많은 제약조건을 가지고 있어 유선 환경에서의 계산능력에 미치지 못하고 있다. 그러므로 현재까지 소개된 은닉서명 방식들은 복잡한 과정을 거쳐서 구성되어지기 때문에 좁은 대역폭을 가지고 또한 메모리와 연산능력도 부족한 무선환경에 적용하기에는 여러 가지 어려움이 따른다. 본 논문에서 제안한 방식은 무선환경에서 가장 큰 부담을 주는 계산량을 줄여 주는 간단하면서도 효과적인 은닉서명 방식이다.

공개키 암호 방식의 효율성은 통신 횟수, 계산량, 공개키, 개인키 등의 키의 길이들에 의해 영향을 받는다. 이 중, 하드웨어의 급속한 발달로 인하여 공개키와 개인키 등 저장하여야 할 데이타의 길이는 예전에 비해 그 중요성이 감소하게 되었고 그 결과 암호 방식의 효율성은 주로 계산량의 다소에 의해 결정된다. 이러한 계산량은 모듈러(modular)에 대한 지수승 연산, 곱셈 연산, 역원 연산이 대부분을 차지한다. 일반적으로 모듈러 연산에서 모듈러 지수승과 모듈러 역원 연산은 거의 같은 계산량을 필요로 하는 것으로 알려져 있다. 그리고 지수승 연산에 비해 매우 작지만 해쉬함수의 연산등이 암호 방식의 효율성에 영향을 미친다.

본 논문에서 제안한 은닉서명 방식은 표 1에서 보듯이 기존의 은닉서명 방식보다 계산량이 크게 감소하였다. 그리고 서명의뢰자와 서명자 사이에 각각 한번씩의 통신만으로 서명을 생성하므로 통신 에러발생률에 있어서 보다 안전하다. 또한 타원곡선상에서 연산이 이루어지므로 유한체에서의 키의 길이가 다른 어느 연산보다도 작다. 타원곡선 알고리즘은 하드웨어 이식이 쉬워 스마트카드나 이동단말기나 호출기와 같이 휴대형 시스템에 적용하기 쉽고 타원곡선에서의 160비트는 RSA에서 1024비트와 같은 안전성을 가지며 주요 연산이 스칼라 곱이기 때문에 수행 시간이 많이 절약될 수 있다. 따라서 본 논문에서 제안한 은닉서명 방식은 타원곡선상에서 연산이 이루어지므로 연산속도, 계산량, 키의 길이 등에 있어 좋은 효율성을 가지고 있고 기존에 발표된 은닉서명 방식에 비해 훨씬 간단한 과정을 거쳐서 서명이 생성되며 서명의뢰자와 서명자간의 통신량과 통신횟수도 줄여 효율성을 높였다. 그러므로 전술한 제약조건을 갖는 무선환경에서도 적용할 수 있는 효율적인 은닉서명 방식이다.

5.2 제안한 ID 기반 은닉서명 방식과 기존 은닉서명 방식과의 비교

D. Chaum이 제안한 RSA 기반 은닉서명 방식은 2회의 통신만으로 서명을 생성할 수 있다는 장점이 있지만 2개의 서명으로부터 정당하지 않은 서명을 만들 수 있다는 문제점이 지적되었다. 이러한 취약점을 개선하여 C. I. Fan, W. K. Chen와 Y. S. Yeh이 RSA에 기반한 은닉서명 방식을 제안하였으나 이들이 제안한 은닉서명 방식은 통신횟수와 계산량이 많고 프로토콜도 복잡하다. 특히, 서명의뢰자의 계산량이 D. Chaum의 은닉서명 방식에 비해 크게 증가되었다. T. Okamato가 제안한 Schnorr기반 은닉서명 방식은 DHP의 어려움에 기반을 하였지만 Fan-Chen-Yeh 은닉서명 방식과 마찬가지로 프로토콜도 복잡하고 계산량도 많은 단점을 가지고 있다.

본 논문에서 제안한 은닉서명 방식은 GDHP의 어려움에 기반하면서 Chaum 은닉서명 방식처럼 서명의뢰자가 서명자에게 은닉서명을 의뢰하면 추가적인 통신 없이 바로 서명을 생성하고 타원곡선상에서 연산이 이루어지므로 키의 크기를 줄여주고, 연산속도를 증가시킴으로써 서명을 생성, 검증하는데 걸리는 시간을 줄여준다. 또한 제안한 은닉서명 방식은 ID 기반 인증 모델을 적

표 1 제안한 ID 기반 은닉서명 방식과 기존 은닉서명 방식 비교

			Chaum방식	Okamato방식	Fan-Chen-Yeh방식	제안한 방식
통신횟수			2-pass	3-pass	4-pass	2-pass
공개키인증서			필요	필요	필요	필요없음
위조가능성			위조가능	안전	안전	안전
계산량	서명생성	의뢰자	2M+E+I	2M+2E+H	9M+2E+2I+H	3A+H
		서명자	E	E+M	4M+E+I	2A
	성명검증		E	2E+M+H	2M+E+H	P

용하였기 때문에 공개키 인증서가 필요 없다. 서명을 검증하는 과정에서 서명자의 공개키가 사용되기 때문에 공개키 인증서 습득과정의 생략은 암호 방식의 효율성을 증대시킨다.

표 1은 본 논문에서 제안한 은닉서명 방식과 기존의 은닉서명 방식을 비교한 것이다. 여기에서 M은 모듈라 곱에 대한 평균 계산량, E는 모듈라 지수승에 대한 평균 계산량, I는 모듈라 역원에 대한 평균 계산량, H는 해쉬함수의 계산량, A는 타원곡선위에서 스칼라곱에 대한 평균 계산량, P는 타원곡선위에서 pairing에 대한 평균 계산량을 의미한다.

6. 결론 및 향후 연구방향

은닉서명은 전자상거래나 금융 관련된 보안서비스에서 활용되는 암호 방식 중에 하나이다. 현재 전자상거래가 유선통신에서 무선통신으로 이동되어가고 있기 때문에 이에 적합하도록 빠른 연산을 수행하고 적은 통신량이 보장되어야 한다.

본 논문은 기존의 효율성을 훨씬 개선한 GDH군에서의 ID 기반 인증 모델 은닉서명 방식을 제안했다. 본 논문에서 제안한 방식은 전자서명의 요구조건을 그대로 가지고 있으면서 개인의 프라이버시와 익명성을 제공한다. 그리고 타원곡선상에서 연산이 이루어지므로 유한체에서의 키의 길이가 다른 어느 연산보다도 작다. 또한 DH문제에 기반한 기존의 은닉서명 방식에 비하여 통신량, 통신횟수, 연산속도와 계산량을 감소시켜 효율성을 높였으므로 낮은 연산처리 능력에 제약을 받는 무선 PKI 환경에서도 적용할 수 있다.

제안한 은닉서명 기법에 추가적으로 PSS(Provable signature scheme)기법을 사용한다면 위장 공격에 대한 안전성을 더욱 높일 수 있을 것이다.

참 고 문 헌

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

[2] 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 Cryptosystems, PKC '01, Springer-Verlag, preprint, pp. 104-118, 2001.

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

[4] 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.

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

[6] 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.

[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 Sinature Generation by Smart Cards," Journal of Cryptology, Vol. 4, No. 3, pp. 161~174, 1991.

[9] 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.

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

[11] 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.

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

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

김 현 주

1991년 세명대학교 수학과 졸업(학사) 1997년 서강대학교 수학과 졸업(석사) 1999년~현재 성균관대학교 전기전자 및 컴퓨터공학부 박사과정. 관심분야는 암호이론, 전자상거래 보안

김 수 진

2002년 성균관대학교 전기전자컴퓨터공학부와 수학과 졸업(학사, 복수전공) 2002년~현재 성균관대학교 정보통신공학부 석사과정. 관심분야는 암호이론, 전자상거래 보안

원 동 호

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. 관심분야는 암호이론, 정보시스템 보안