Journal of Digital Contents Society Vol. 5. No. 1. March. 2004(pp.1-6)

컨텐츠 구입 시 고객의 익명성을 위한 은닉 서명 기법

이현주*, 이충세**

요 약

모바일 전자상거래 환경에서 컨텐츠를 구입하기 위한 지불 수단으로 전자화폐를 사용한다. 이때, 고객의 프라이버시를 보호하기 위해 서명의뢰자의 신원과 서명문을 연결시킬 수 없도록 익명성을 유지할 수 있는 서명 기법인 은닉 서명 기법을 이용하여 메시지의 서명을 생성한다. 본 논문에서는 GDHP기반의 타원곡선 알고리즘을 적용하여 통신횟수, 연산속도와 계산량 측면에서 기존의 은닉 서명 방식을 개선한 효율적인 은닉 서명 기법을 제안한다.

A Blind Signature Scheme for Customer Anonymity in Contents Purchase

Hyun-ju Lee*· Chung-Sei Rhee*

ABSTRACT

Electronic cash is used as a payment tool for contents purchase in mobile electronic commerce environment. In order to protect customer's privacy, we use blind signature. Blind signature has an anonymity property since it does not allow connection between customer's ID and customer's message. In this paper, we propose an blind signature scheme using elliptic curve algorithm based on Gap Diffie-Hellman Problem. Proposed scheme efficiently improved against existing blind signature scheme by reducing communication and computation time of the process.

Key words : Gap Diffie-Hellman Problem, Elliptic Curve, Blind Signature, Electronic cash

1. 서 론

최근 이동 전화의 급성장과 인터넷의 활용 증대로 국내 통신 시장의 무게 중심이 유선/음성 통신 위주에서 음성 및 대용량의 고속 데이터/멀티미디어 서비스를 이용할 수 있는 유/무선 통합 서비스 시대로 전환이 되고 있다. 이런 환경에서 컨텐츠의 복제와 무단 배포 방지를 위한 자료의 암호화뿐만 아니라, 전자지불 과정에서 무선 인터넷 활성화에 지대한 영향력을 행사하고 개인의 프라이버시를 보호할 수 있는 환경이 구축되어야 한다.

실제로 사용자가 전자화폐를 전자 은행으로부터 인출할 때 사용하는 일련번호는 사용자의 화폐에 대한 정보로써 이는 은행이 사용자 현금 사용 내역을 역추적하는 정보가 된다.

그러므로 전자 화폐는 물리적 화폐(지폐 또는 동전)와 달리 익명성이 제공되지 못하므로 그 결과 정보화 사회의 핵심인 사생활의 보호를 보장할 수 없게 된다. 이를 방지하기 위해 1982년 D.Chaum이 처음으로 RSA문제를 기반으로 하는 은닉서명 방식을 제안하였다[1]. 이 기법은 사용자가 인출할 화폐의 일련번호에 난수를 곱해서 은행으로 보내고 은행은 전달 받은 번호를 전자 현금화해서 사용자에게 넘겨주면 사용자는 사용된 난수로 나누게 되는데 이 경우 원래의 번호가 나타나지 않으므로 인출한 화폐의 일련번호의 익명성을 제공할 수 있다.

이 서명 기법은 사용자의 원래의 현금 번호를 은행이 알 수 없도록 하여 개인의 프라이버시와 익명성을 보장한다. 그러나 이 서명 기법은 사용자가 2개의 전자화폐로부터 은행의 승인 없이 다른 전자화폐를 만들 수 있다는 문제점이 있다. 또한, 다양한 방식의 은닉 서명 기법이 제안되었으나 복잡한 과정으로 구성되어 좁은 대역폭을 가지고 메모리 용량이 부족한 무선 환경에 적용하기에는 많은 어려움이 따른다. 따라서 무선 환경에

※ 제일저자(First Auther) : 이현주 , 주소 : 충북 청주시 흥덕구 개신동 충북대학교 컴퓨터과학과, 전화:043)261-2260,
E-mail: pinklee104@korea.com
접수일 : 2004년 2월 14일, 완료일 : 2004년 2월 27일
* 정회원, 충북대학교 컴퓨터과학과
** 충북대학교 전기전자 및 컴퓨터 공학부
(E-mail : csrhee@cbucc.chungbuk.ac.kr)

적합하도록 계산량을 줄일 수 있는 효과적인 은닉 서명 방식을 제안하고자 한다.

본 논문에서는 GDHP의 어려움에 기반한 타원곡선상의 알고리즘을 적용함으로써 연산속도, 계산량, 키의 길이 측면에서 효율적이며 무선 환경에도 적합한 은닉 서명 기법을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 컨텐츠의 컨텐츠의 종류 및 특성에 대해 설명하고, 3장에서는 기존 은닉 서명 기법을 소개한다. 4장에서는 제안하는 GDHP 은닉 서명 기법을 설명하고, 5장에서는 제안한 은닉 서명 기법의 효율성 및 안전성을 비교한다. 6장에서는 결론을 제시한다.

2. 컨텐츠의 종류 및 특성

2.1 컨텐츠의 종류

멀티미디어 컨텐츠는 매우 다양한 영역을 대상으로 제작할 수 있는데 컨텐츠의 종류를 내용에 따라 분류하면 다음과 같다[2].

▸ **정보형**

전자 백과사전, 전자 매뉴얼, 관광안내등과 같이 사용자가 자주 필요로 하는 정보를 제공할 목적으로 개발된 컨텐츠로 어떤 특정 분야에 대해 자세하고 유용한 정보를 제공한다.

▸ **홍보형**

기업 홍보나 제품 광고와 같이 특정 기업이나 기관 또는 제품에 관한 정보를 제공하는 컨텐츠를 의미한다.

▸ **교육형**

교육 정보를 각종 미디어를 통해 제공하며, 상호 대화식 학습을 유도할 수 있도록 구성된 컨텐츠이다.

▸ **오락(Entertainment)**

게임, 영화등 주로 오락 분야의 내용물을 다양한 멀티미디어 요소들을 통해 표현하고, 사용자로 하여금 새로운 경험을 하게 하거나 상호 작용 방식으로 반응할 수 있는 기능들을 제공해 사용자의 흥미를 유발시키거나 저작물에 몰입감을 느낄 수 있도록 제작한 컨텐츠가 이 영역에 속한다.

▸ **첨단 영상물**

디지털 영화, 만화, 광고, 홍보영상 시뮬레이션(건축, 문화재 등) 및 그 외 기타 컴퓨터 영상 제작 기법이 도입된 영상물 등이 여기에 속한다. 그림1은 완전한 3차원 디지털 영화를 위한 데모 실사나 합성 셀 애니메이션 등 기존의 기법으로는 표현이 불가능한 영상을 얻기 위해, 캐릭터, 배경등을 모두 3차원 그래픽으로 처리한 첨단 영상물 분야 멀티미디어 컨텐츠의 예이다.

▸ **통신 컨텐츠**

통신 서비스를 통해 제공되고 있거나 제공될 수 있는 멀티미디어 정보 상품이다. VOD(Video on Demand), NOD(News on Demand)등 각종 웹 사이트에서 제공하는 음악 관련 서비스, 그리고 푸시(Push) 기술을 이용하여 시시각각으로 변하는 주식 정보등을 사용자에게 제공하는 컨텐츠 개발 분야가 여기에 속한다.

그림1. 디지털 영화 제작을 위한 3차원 컴퓨터 그래픽 'ARK'

http://www.mcc.or.kr/contest/industrial/industrial.html

2.2 컨텐츠의 특성

디지털 데이터의 문제점은 원본과 복사본의 구별이 어렵고 대량 복제가 가능하다는 것이다. 따라서 지적 소유권(원본)을 판별하기가 어렵다. 이러한 복사 방지 시스템으로 워터마킹과 핑거프린팅 기법을 사용하여 보안성을 확보한 후 저장매체에 저장되어 안전한 채널로 디지털 TV나 PC, 단말기를 사용하는 사용자에게 전송된다. 컨텐츠가 사용되어지는 과정에서 사용자와 컨텐츠 제공자, 그리고 은행사이에는 사용자의 프라이버시를 보호하고 거래 내역을 추적할 수 없는 은닉 서명 방식을 적용한 전자 지불이 이루어져야 한다.

3. 은닉 서명 기법

은닉 서명(blind signature)은 서명문의 내용을 숨기는 서명 방식으로 서명의뢰자의 신원과 서명문을 연결시킬 수 없는 익명성을 유지할 수 있는 서명 방식이다. D.Chaum이후 여러 은닉 서명 방식이 발표되었지만 현재 안전성을 인정 받고 있는 암호 방식은 RSA와 Diffie-Hellman 방식이 거의 대부분이다. 본장에서는 먼저 일반 RSA서명 방식과 대표적인 은닉 서명 방식으로 D.Chaum이 제안한 RSA암호 방식에 기반한 은닉 서명 방식과 T.Okamoto가 제안한 Schnorr기반의 은닉 서명 방식에 대하여 살펴본다.

3.1 RSA 서명

서명자는 메시지 m에 대한 RSA 서명 $S = m^d \bmod n$을 생성하여 서명 의뢰자에게 서명 (m, S)를 안전하게 전송한다. 서명 의뢰자는 (m, S)를 전자화폐로써 사용한다. 원하는 컨텐츠를 구매하기 위해 (m, S)를 지불한다. 이렇게 전자 서명된 전자화폐는 지폐 또는 동전을

대신하여 사용할 수 없다. 전자서명 과정에서 서명자는 서명의뢰자의 신원과 발급 받은 전자화폐의 일련 번호를 알고 있으므로 서명자(은행)와 판매자가 결탁하게 되면 서명의뢰자(고객)의 구매에 관한 정보인, 언제, 어디서, 무엇을 사는지에 대한 개인의 프라이버시 관련 정보가 쉽게 노출되게 된다[3].

3.2 Chaum 은닉 서명

RSA 암호 방식에 기반한 은닉 서명 방식은 D.Chaum에 의해 처음 제안되었다[4]. 은닉 서명 방식의 안전성은 소인수분해문제(IFP: Integer Factorization Problem)의 어려움에 기반하고 있다. 그러나 이 서명 방식의 문제점은 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 $m_1 m_2$에 대한 부정한 서명 $S_1 S_2 = (m_1 m_2)^e$ 를 생성할 수 있다. 이러한 문제점은 서명문과 함수가 주어졌을 때 메시지를 알아내기 어려운 일방향 해쉬 함수 $h(\cdot)$를 도입하여 은닉 서명을 만들면 쉽게 해결할 수 있다. 키 설정과정, 서명 생성과정, 서명 검증과정은 다음과 같다.

▸ **키 설정**

서명자 B는 RSA 방식과 같은 방법으로 비밀키 d, 공개키 e를 설정한다[5].

▸ **서명 생성**

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. B는 $K_2 \equiv K_1^d \bmod n$를 계산하여 A에게 전송한다. A는 전달 받은 K_2를 자신이 처음 선택한 난수 r로 나누어 서명 $S \equiv \frac{K_2}{r} \equiv m^d \bmod n$ 을 획득한다.

▸ **서명 검증**

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

3.3 Okamoto 은닉 서명

Schnorr 암호 방식에 기반하고 서명 방식의 안전성을 이산대수문제(DLP: Discrete Logarithm Problem)의 어려움에 두고 있는 이 서명 방식은 T.Okamoto에 의해 제안되었다[6]. 그러나 이 서명은 RSA에 기반한 서명 방식에 비하여 프로토콜도 복잡하고 계산량도 많은 단점이 있다. 키 설정과정, 서명 생성과정, 서명 검증과정은 다음과 같다.

▸ **키 설정**

서명자 B는 Schnorr 방식과 같은 방법으로 비밀키 x, 공개키 $y = g^x$를 설정한다[7].

▸ **서명 생성**

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

▸ **서명 검증**

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.

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

4. GDHP 기반 은닉 서명 기법

개인 신분 정보를 일방향 함수(one-way function)로 하여 공개키를 형성하는 ID 기반 시스템은 1894년 Shamir에 의해 처음 제안되었다[8]. 기존의 인증서(certificaton)기반 공개키 기반구조(PKI: Public Key Infrastructure)의 키 관리 절차를 간단히 하였다. 이후 ID 기반의 암호 방식 및 서명 방식은 대부분 IFP를 기반으로 제안되었다. 최근 D.Boneh와 D.Franklin은 Weil-pairing을 이용한 타원곡선에 bilinear 함수를 적용한 새로운 ID 기반의 암호 방식을 제안하였다[9]. 4.1절에서는 CDHP와 DDHP 문제에서 정의되는 GDHP 문제를 다루고 4.2절에서는 서명 후에 검증 과정에 사용되는 Weil-pairing과 bilinear 함수에 대해 설명한다. 본 논문에서는 4.3절에서 GDHP를 기반으로 하는 은닉 서명 기법을 제안한다.

4.1 Gap Diffie-Hellman 군

이산대수문제를 이용한 암호 및 서명 방식의 안전성은 Diffie-Hellman 시스템의 어려움에 기반하고 있다.

Diffie-Hellman 문제는 계산적 Diffie-Hellman 문제(CDHP), 결정적 Diffie-Hellman 문제(DDHP), Gap Diffie-Hellman 문제로 구분된다[10].

- CDHP(Computational Diffie-Hellman Problem): $g, g^x \bmod p$와 $g^y \bmod p$ 로부터 $g^{xy} \bmod p$를 계산하는 문제
- DDHP(Decisional Diffie-Hellman Problem): $g, g^x \bmod p, g^y \bmod p$와 w 로부터 $w \equiv g^{xy} \bmod p$ 인지를 결정하는 문제

위 문제들 사이의 관계를 살펴보면 CDHP가 해결되면 DDHP가 해결됨을 알 수 있다. CDHP의 해결은 어려우면서, DDHP의 해결은 쉬운 군(Group)을 Gap Diffie-Hellman(GDH)군이라 정의하고 이러한 문제를 GDH문제라고 정의한다.

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

4.2 The Weil-pairing

G_1과 G_2는 위수가 소수 l인 순환군이다. G_1은 타원곡선 F_l위의 점들로 이루어진 군이며 G_2는 F_{l^2}의 부분군으로 G_1은 덧셈군이며 G_2는 곱셈군이 된다. 함수 $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 가 다음 조건을 만족하면 $\hat{e}$를 Weil-pairing 이라고 한다.

- Bilinearity: 임의의 $P, Q, R \in G_1$와 $a, b \in Z/l$ 에 대하여
  $\hat{e}(P+Q, R) = \hat{e}(P, R) \cdot \hat{e}(Q, R)$
  $\hat{e}(P, Q+R) = \hat{e}(P, Q) \cdot \hat{e}(P, R)$
  $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ 를 만족한다.
- Identity: 임의의 $P \in G_1$에 대하여 $\hat{e}(P, P) = 1$을 만족한다.
- Alternation: 임의의 $P, Q \in G_1$에 대하여 $\hat{e}(P, Q) = \hat{e}(Q, P)^{-1}$를 만족한다.
- Non-degeneracy: 임의의 $Q \in G_1$에 대하여 $\hat{e}(P, Q) = 1$이면 P는 무한원점 O 이다.
- Efficient: $\hat{e}(P, Q)$의 계산이 효율적인 알고리즘이 존재한다.

Bilinearity를 만족하는 함수 $\hat{e}$를 bilinear함수라고 정의한다. 타원곡선 위의 점 P, aP, bP, cP 가 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 $\hat{e}(aP, bP) = \hat{e}(P, cP)$가 성립하는지 확인함으로써 쉽게 해결할 수 있다. 식이 성립하면 (P, aP, bP, cP)은 DDH쌍이 된다. 따라서 이들은 GDHP 특성을 만족하는 예로써 서명 검증 암호 방식 등에 사용할 수 있다.

4.3 GDHP 기반 은닉 서명 기법

제안하는 GDHP 기반 은닉 서명 방식의 키 설정과정, 서명 생성과정, 서명 검증과정이다.

·키 설정

- G: DDHP가 해결되는 소수 l을 위수로 가지는 군
- P: G의 생성원
- $H_1: \{0,1\}^* \times G \rightarrow Z/l$: 충돌회피 해쉬함수
- $H_2: \{0,1\}^* \rightarrow G$: 충돌회피 해쉬함수
- ID_B : B의 아이디
- $Q_B = H_2(ID_B)$: B의 공개키
- $D_B = bQ_B$: B의 비밀키
- $b \in Z/l$:서명자가 생성한 난수로 비밀키로 사용
- $P_B = bP$: 공개

·서명 생성

A는 m에 대한 서명을 의뢰하기 위해 난수 $r \in Z/l$을 선택하고 $U = rQ_B$, $h = H_1(m, U)$, $X = (r+h)$를 계산하여 B에게 X를 전송한다. B는 $V = (r+h)D_B$를 계산하여 A에게 전송한다. A는 서명 $\sigma = (U, V)$를 획득한다.

·서명 검증

서명 $\sigma = (U, V)$를 검증하기 위해 bilinear 함수 $\hat{e}$를 사용하여 $(P, P_{pub}, (r+h)Q_B, V)$이 DDH쌍인지 확인한다.

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

5. 비교 분석

서명 $\sigma = (U, V)$에는 서명의뢰자의 난수 r를 포함하고 있기 때문에 서명을 위조할 수 없다. 만약, 서명자 B가 서명 사실을 부인하더라도 서명 $\sigma = (U, V)$에 서명자의 비밀 정보 b가 사용되었기 때문에 서명자를 판별할 수 있다. 또한, 서명 $\sigma = (U, V)$에는 서명의뢰자의 신원 정보가 존재하지 않기 때문에 사용자 보호와

표1. 통신량과 계산량 비교

		Chaum 기법	Okamoto 기법	제안 기법
통신횟수		2-pass	3-pass	2-pass
위조가능성		위조가능	위조불가능	위조불가능
계산량	서명의뢰자	2M+E+I	2M+E+H	A+H
	서명생성자	E	E+M	2A
	서명검증	E	2E+M+H	P

익명성을 제공한다. 또한 서명자의 비밀키 D_B가 사용되기 때문에 서명자 외에는 서명을 생성할 수 없다. 또한, 무선 통신 사용자의 증가로 무선 PKI 환경에서는 통신속도, 메모리 용량, CPU성능 등을 고려해야 한다. 지금까지 제안된 은닉 서명은 복잡한 과정을 통해 이루어지기 때문에 메모리와 연산 능력이 부족한 무선 환경에 적용하기에는 많은 제약이 따른다. 암호 방식의 효율성은 주로 계산량의 다소에 의해 결정된다. 지수승 연산에 비해 매우 작지만 해쉬 함수의 연산등이 암호 방식의 효율성에 영향을 미친다.

본 논문에서 제안한 은닉서명 기법은 GDHP의 어려움에 기반한 타원 곡선 상에서 연산이 이루어지기 때문에 연산속도, 계산량, 키의 길이 등에 있어 뛰어난 효율성을 가지고 있다. 따라서 서명을 생성, 검증하는데 걸리는 시간을 감소시킨다. 또한 서명의뢰자와 서명자 간의 통신량과 통신횟수의 감소로 효율성을 높였다. 표1에서 M은 모듈라 곱셈에 대한 계산량, E는 모듈라 지수승에 대한 계산량, I는 모듈라 역원에 대한 계산량, H는 해쉬함수의 계산량, A는 타원곡선위에서 Weil-pairing에 대한 계산량을 의미한다.

6. 결 론

본 논문에서는 Chaum과 Okamoto가 제시한 은닉 서명 기법의 문제점을 개선하여 GDHP에 기반한 은닉 서명 기법을 제안하였다. 은닉 서명은 전자 지불등과

같은 금융에 관련된 보안 서비스에 활용되는 서명 방식 중의 하나이다. 무선 환경에 적합한 GDH군에서 타원곡선상에서 연산이 이루어지므로 통신량, 통신횟수, 연산속도와 계산량을 감소시켰으며 또한, 사용자의 프라이버시 보호와 익명성을 제공한다. 향후 사용자가 익명성을 악용하는 경우 즉, 돈세탁, 이중사용 등을 추적할 수 있는 익명성 제어 기능에 대한 연구가 필요하다.

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] 최 윤철, 고견, "멀티미디어 배움터", 생능출판사, 2002.

[3] Douglas R.Stinson, "Cryptography: Theory and Practice", CRC Press.

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

[5] R.L.Riverst, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystem", Commun, ACM, Vol. 21, pp. 120-126, 1978.

[6] 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.

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

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

[9] 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.

[10] 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.

이 현 주

1990년 2월 청주대학교 수학과 이학사
1992년 2월 청주대학교 수학과 이학석사
2000년 8월 청주대학교 수학과 이학박사
2003년 2월 충북대학교 대학원 컴퓨터과학과 박사과정 수료
관심분야: M-Commerce, 정보보호, 멀티미디어

이 충 세

1989년 University of South Carolina, 전산학 박사
University of North Dakota 전산학과 조교수
1991년- 현재: 충북대학교 전기전자 및 컴퓨터공학부 교수
관심분야: 결함허용, 알고리즘 및 전문가 시스템, 정보보안