Bilinear-pairing을 이용한 대리서명, ID 기반 부분은닉서명과 대리부분은닉서명 방식

(Proxy Signature, ID-based Partially Blind Signature and Proxy Partially Blind Signature using Bilinear-pairing)

김 현 주 † 여 상 희 †† 원 동 호 †††
(Hyunjue Kim) (Sanghee Yeo) (Dongho Won)

요 약 대리서명은 대리서명자로 하여금 원서명자를 대신해서 서명하도록 하는 암호방식이고, 부분은닉서명은 서명자가 은닉서명을 발행할 때 그가 삽입하기를 원하는 어떠한 정보를 서명에 삽입할 수 있도록 하는 암호방식으로, 부분은닉성과 익명성(또는 불추적성)을 제공하기 때문에 전자상거래에서 전자화폐나 전자투표 등과 같은 사용자의 프라이버시 보호나 보안을 요구하는 응용분야에 중요하게 적용되는 기술이다. 본 논문에서는 bilinear-pairing을 이용한 대리서명 방식과 ID 기반 부분은닉서명 방식을 제안한다. 그리고 두 방식을 결합한 대리부분은닉서명 방식을 제안한다. 제안하는 방식들은 GDH군에서 성립하며 CDHP의 어려움에 기반을 두고 있다. 제안하는 ID 기반 부분은닉서명 방식과 대리부분은닉서명 방식에서 공통정보를 제거하면 두 서명 방식은 각각 ID 기반 은닉서명 방식과 대리은닉서명 방식이 된다.

키워드 : 대리서명 방식, ID 기반 부분은닉서명 방식, 대리부분은닉서명 방식, Gap Diffie-Hellman 문제, Bilinear-pairing

Abstract Proxy signature scheme allow a designated proxy person to sign a message on behalf of the original signer. Partially blind signature scheme allows the signer to insert non-removable common information into his blind signature. Proxy signature and partially blind signature are very important technologies in secure e-commerce. In this paper we propose new proxy signature scheme and ID-based partially blind signature scheme using bilinear pairing. Further combining them, we propose a proxy partially blind signature scheme. The security of our schemes relies on the hardness of Computational Diffie-Hellman Problem. If we removing common information form propose ID-based partially blind signature scheme and proxy partially blind signature scheme, then they become variants of ID-based blind signature scheme and proxy blind signature scheme of Zhangs respectively.

Key words : Proxy signature, ID-based Partially Blind Signature scheme, Proxy Partially Blind Signatur scheme, Gap Diffie-Hellman Problem, Bilinear-pairing

1. 서 론

대리서명 방식은 원서명자가 자신의 부재중에 자신을 대신해서 서명을 할 수 있는 대리 서명자를 지정하여 대신 서명하도록 하는 서명 방식으로 기업의 대표가 과도한 업무나 또는 출장 등과 같은 이유로 제한된 기간 내에 반드시 서명을 해야하는 계약서나 문서에 서명을 못하게될 상황에 대한 해결책으로 유용하게 활용되고 있다. 대리서명 방식은 1996년 M. Mambo, K. Usuda와 E. Okamoto[1]에 의해서 처음 소개되었고, 그 후 많은 사람들에 의해서 연구되었다[2-7].

M. Mambo, K. Usuda와 E. Okamoto[1]는 대리서명 방식을 위임의 형태에 따라서 완전 위임(full delegation), 부분 위임(partial delegation)과 보증 위임(delegation by warrant)으로 분류하였고 S. Kim, S. Park와 D. Won[2]은 부분 위임의 장점과 보증 위임의 장점을 결합한 보증부분위임(partial delegation with warrant)이라는 새로운 개념을 제안하였다. 본 논문에서 제안한 대리서명 방식은 보증부분위임방식이다.

· 본 연구는 2004년도 정보통신부 지원 대학 IT 연구센터 육성지원사업 (C1090-0403-0005)의 연구비 지원으로 수행하였습니다.
† 학생회원 : 성균관대학교 정보통신공학부
hjkim@dosan.skku.ac.kr
†† 비 회 원 : 성균관대학교 정보통신공학부
yeosh72@hanmail.net
††† 종신회원 : 성균관대학교 정보통신공학부 교수
dhwon@dosan.skku.ac.kr
논문접수 : 2003년 10월 27일
심사완료 : 2004년 9월 2일

대리서명은 다른 특수서명과 결합하여 또 다른 형태의 특수서명 방식을 생성한다[8-11]. 최근 F. Zhang은 ID 기반 은닉서명 방식과 F. Hess[12]의 ID 기반 서명 방식을 기초로 한 대리서명 방식을 제안하였고[13], 이 두 방식을 이용한 대리은닉서명 방식을 제안하였다[9].

1982년 D. Chaum[14]에 의해서 처음 소개된 은닉서명 방식은 은닉성과 익명성(또는 불추적성)을 제공하기 때문에 전자 투표나 전자화폐 등과 같은 보안을 요구하는 응용분야에 사용된다. 그러나 전자화폐는 전자적 특성상 쉽게 위조가 가능하여 이중사용의 문제점이 발생한다. 이에 대한 해결책으로, 전자화폐 자체가 특수한 구조를 가지도록 하여 매 지불시 마다 등록되는 데이타가 거의 동시에 모든 데이타베이스에 기록되도록 함으로써 이중 사용을 검출하는 방법이 있다. 그러나 이미 사용된 모든 전자화폐들에 대한 데이타베이스를 구축해야 한다는 사실은 데이타베이스의 크기가 무제한적으로 증가하게 됨을 암시하며 따라서 이에 대한 막대한 비용이 소요되는 문제를 야기한다. 이에 대한 해결책으로 부분은닉서명 방식이 제안되었다.

1996년 M. Abe와 E. Fujisaki[15]에 의해 소개된 부분은닉서명 방식은 서명자(은행)가 은닉서명을 발행할 때 그가 삽입하기를 원하는 어떠한 정보를 서명에 삽입할 수 있도록 하는 암호방식이다. 이때, 서명자는 자신이 삽입하고자 하는 정보가 서명에 삽입되었는지 확신할 수 있어야 한다. 또한 서명의뢰자가 그 정보를 제거하거나 변형할 수 없어야 한다. 부분은닉서명을 사용하여 은행은 모든 전자화폐에 만료부(expiration data)를 삽입하여 사용자(서명의뢰자)에게 발행하고, 사용자가 사용하여 기간 만료된 전자화폐에 관련된 기록은 은행의 데이타베이스에서 지워지도록 함으로써 데이타베이스의 무제한적인 증가 문제를 해결할 수 있다. 부분은닉서명 방식은 부분은닉성과 익명성을 제공하기 때문에 전자상거래에서 사용자의 프라이버시 보호나 보안을 요구하는 많은 응용분야에 유용하게 적용되는 암호방식으로 많은 사람들에 의해 연구되었다[16-19].

본 논문에서는 J. Cha와 J. Cheon[20]이 제안한 ID 기반 서명 방식을 기초로 한 새로운 대리서명 방식과 ID 기반 부분은닉서명 방식을 제안한다. 제안하는 대리서명 방식은 Zhang의 대리서명 방식에 비하여 서명 생성 시에 사용되는 계산량을 크게 줄인 효율적인 서명 방식이다. 그리고 제안하는 대리서명 방식과 ID 기반 부분은닉서명 방식을 결합한 대리부분은닉서명 방식을 제안한다. 제안하는 서명 방식들은 모두 GDH군에서 성립하며 CDHP의 어려움에 기반을 두고 있으며 서명검증에 bilinear-pairing을 사용한다. 제안하는 ID 기반 부분은닉서명 방식과 대리부분은닉서명 방식에서 공통정보를 제거하면 두 서명 방식은 각각 ID 기반 은닉서명 방식과 대리은닉서명 방식이 된다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 본 논문에서 제안하는 서명 방식에 사용된 안전성 기반 문제인 GDHP와 서명 검증에 사용된 bilinear-pairing에 대하여 설명하고, 3장에서는 Zhang의 대리서명 방식, ID 기반 은닉서명 방식과 대리은닉서명 방식들을 살펴본다. 4, 5 그리고 6장에서는 각각 본 논문에서 제안하는 새로운 대리서명 방식, ID 기반 부분은닉서명 방식 그리고 대리부분은닉서명 방식에 대하여 설명하고 분석하며, 마지막으로 7장에서 결론을 도출한다.

2. GDHP와 Bilinear-pairing

CDHP(Computational Diffie-Hellman Problem)가 해결되면 DDHP(Decisional Diffie-Hellman Problem)가 해결됨을 알 수 있다. 그러나 그 역의 성립에 대하여는 알려진 사실이 없다. 이에 대하여 2001년 T. Okamoto와 D. Pointcheval[21]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. 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
- Gap Diffie-Hellman 문제 (GDHP: Gap Diffie-Hellman Problem)
  : P, aP와 bP로부터 DDH Oracle을 이용하여 abP를 계산하는 문제

G은 타원곡선 F_ℓ 위의 점들로 이루어진 군으로 생성원 P를 갖는 순환군(cyclic group)이고 $a, b, c \in Z/\ell$이다. GDHP 특성을 만족하는 예로는 Weil-pairing이나 Tate-pairing과 같은 bilinear-pairing이 있다. GDH군을 찾기 위해 많은 학자들의 연구가 이루어지고 있지만, bilinear-pairing을 적용한 초특이 타원곡선을 제외하고는 현재까지 알려진 GDH군은 존재하지 않는다. bilinear-pairing의 정의는 다음과 같다.

G_1과 G_2는 위수가 소수 ℓ인 순환군이고 P는 G_1의 생성원이다. G_1은 타원곡선 F_ℓ 위의 점들로 이루어

진 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 bilinear-pairing이라고 한다.

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

- Bilinearity : $e(aP, bQ) = e(P, Q)^{ab}$ 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.
- Non-degeneracy : $e(P, Q) = 1$ 이면 P는 무한원점(O)이다.
- Efficiency : $e(P, Q)$의 계산이 효율적인 알고리즘이 존재한다.

타원곡선 위의 점 P, aP, bP, cP가 주어졌을 때 abP를 구하는 문제는 쉽게 해결되지 않지만 $abP = cP$가 성립하는지 결정하는 문제는 bilinear-pairing을 사용하여 $e(aP, bP) = e(P, cP)$가 성립하는지를 확인함으로써 쉽게 해결할 수 있다. 2001년 D. Bonech은 bilinear-pairing을 암호에 응용하여, GDH군에서 실제로 구현 가능한 새로운 ID 기반 암호 방식[22]과 서명 방식[23]을 제안하였다. 최근, bilinear-pairing을 이용한 새로운 형태의 암호 방식은 활발히 연구되고 있다[9,12,13,20, 22,24,25].

3. 기존 방식

1984년 Shamir[26]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. 이 후 ID 기반 암호 방식이 제안되어왔으며[27-29], 최근에는 bilinear-pairing을 이용한 새로운 ID 기반의 암호방식 및 서명 방식이 활발히 연구되고 있다[12,13,20,22,24, 25].

2003년 F. Zhang과 K. Kim[13]은 bilinear-pairing을 이용한 대리서명 방식과 ID 기반 은닉서명 방식을 제안하였다. 그리고 F. Zhang, R. Safavi-Naini과 C. Y. Lin[9]은 대리서명 방식과 ID 기반 은닉서명 방식을 결합하여 대리은닉서명 방식을 제안하였다. 이 장에서는 bilinear-pairing을 이용한 Zhang의 서명 방식들에 대하여 살펴본다.

3.1 Zhang의 대리서명 방식

*F. Zhang, R. Safavi-Naini*과 *C. Y. Lin*[9]는 Hess의 ID 기반 서명 방식[12]을 이용한 대리서명 방식을 제안하였다. Zhang의 대리서명 방식의 키 설정, 위임장 생성 및 전달, 위임장 검증과 대리서명 키 생성, 대리서명 생성, 대리서명 검증과정은 다음과 같다.

[키 설정]

- G_1 : 소수 ℓ을 위수로 가지는 GDH군
- P : G_1의 생성원
- e : $G_1 \times G_1 \rightarrow G_2$: bilinear pairing
- $H_1: \{0,1\}^* \times G_2 \rightarrow Z/\ell$, $H_2: \{0,1\}^* \rightarrow G_1$: 충돌회피 해쉬함수
- a ($\in Z/\ell$) : 서명자 A의 비밀키
- b ($\in Z/\ell$) : 대리서명자 B의 비밀키
- $P_A = aP$: 서명자 A의 공개키
- $P_B = bP$: 대리서명자 B의 공개키
- $(G_1, G_2, e, \ell, P, H_1, H_2)$: 시스템 파라미터
- W: 위임장

[위임장 생성 및 전달]

원서명자 A는 Bonech의 서명 방식[23]을 이용하여 W에 대한 서명을 생성한다. 즉, 원서명자 A는 해쉬값 $H_2(W)$을 계산하고 W에 대한 서명 $S_W = aH_2(W)$을 생성하여 대리서명자 B에게 S_W, W를 전달한다.

[위임장 검증과 대리서명 키 생성]

대리서명자 B는 bilinear-pairing e를 사용하여 S_W가 위임장 W에 대한 정당한 서명인지를 확인한다. 즉, $e(P_A, H_2(W)) = e(P, S_W)$ 인지 확인한다. 등식이 성립하면 대리서명자 B는 대리서명에 사용될 비밀키 $D_P = s_W + bH_2(W) = (a+b)H_2(W)$와 공개키 $P_P = P_A + P_B = (a+b)P$를 생성한다.

[대리서명 생성]

대리서명자 B는 메시지 M에 대한 대리서명을 생성하기 위해 난수 $k \in Z/\ell$을 선택하고 $U = e(P, P)^k$, $h = H_1(M, U)$와 $V = hD_P + kP$를 계산한다. 대리서명자 B는 서명요청자 C에게 메시지 M에 대한 대리서명 $sig = (W, h, V)$를 전송한다.

[대리서명 검증]

서명요청자 C는 수신된 메시지 M의 대리서명 $sig = (W, h, V)$를 검증하기 위해 원서명자의 공개키 P_A와 대리서명자의 공개키 P_B를 이용하여 대리서명에 사용된 공개키 $P_P = P_A + P_B$를 생성하고 위임장 W에 대한 해쉬값 $H_2(W)$을 계산한다. 생성한 P_P, $H_2(W)$와 bilinear-pairing e를 사용하여 $R = e(V, P)\{e(H_2(W), P_P)\}^{-h}$를 계산하고 해쉬값 $H_1(M, R)$을 생성한다. 마지막으로 서명요청자 C는 식 $h = H_1(M, R)$이 성립하는지 확인함으로써 메시지 M에 대한 대리서명 $sig = (W, h, V)$의 정당성을 검증한다.

3.2 Zhang의 ID 기반 은닉서명 방식

F. Zhang과 K. Kim[13]은 Cha의 ID 기반 서명 방식[20]을 기초로 한 ID 기반 은닉서명 방식을 제안하였다. Zhang의 ID 기반 은닉서명 방식의 키 설정, 서명 생성, 서명 검증과정은 다음과 같다.

[키 설정]

- G_1 : 소수 ℓ을 위수로 가지는 GDH군
- P : G_1의 생성원
- e : $G_1 \times G_1 \rightarrow G_2$: bilinear pairing
- $H_1 : \{0,1\}^* \times G_1 \rightarrow Z/\ell$, $H_2 : \{0,1\}^* \rightarrow G_1$: 충돌 회피 해쉬함수
- ID_B : B의 ID
- b ($\in Z/\ell$) : 서명자 B가 선택하는 난수로 마스터키로 사용된다.
- $Q_B = H_2(ID_B)$: B의 ID와 관련된 공개키
- $D_B = b \cdot H_2(ID_B) = bQ_B$: B의 ID와 관련된 비밀키
- $P_B = bP$: 공개
- $(G_1, G_2, e, \ell, P, H_1, H_2)$: 시스템 파라미터
- M : 서명될 메시지

[은닉서명생성]

서명자 B는 난수 $t \in Z/\ell$를 선택하여 $T = tQ_B$를 계산하고 서명의뢰자 A에게 T를 전달한다. 서명의뢰자 A는 난수 $r_1, r_2 \in Z/\ell$를 선택하고 $U = r_1 T + r_1 r_2 Q_B$, $h = H_1(M, U)$와 $X = r_1^{-1} h + r_2$를 계산하여 서명자 B에게 X를 전송한다. 서명자 B는 $Y = (t + X) D_B$를 계산하여 서명의뢰자 A에게 Y를 전송한다. 서명의뢰자 A는 $V = r_1 Y$를 계산하여 서명 $sig = (U, V)$를 획득한다.

[은닉서명검증]

서명 $sig = (U, V)$가 메시지 M에 대한 정당한 서명인지를 검증하기 위하여 식 $e(P_B, U + hQ_B) = e(P, V)$이 성립하는지 확인한다.

3.3 Zhang의 대리은닉서명 방식

F. Zhang, R. Safavi-Naini과 C. Y. Lin[9]는 3.1절의 대리서명 방식과 3.2절의 ID 기반 은닉서명 방식을 이용하여 대리은닉서명 방식을 제안하였다. Zhang의 대리은닉서명 방식의 키 설정, 대리서명 키 생성, 대리은닉서명 생성, 대리은닉서명 검증과정은 다음과 같다.

[키 설정]

- G_1 : 소수 ℓ을 위수로 가지는 GDH군
- P : G_1의 생성원
- e : $G_1 \times G_1 \rightarrow G_2$: bilinear pairing
- $H_1 : \{0,1\}^* \times G_1 \rightarrow Z/\ell$, $H_2 : \{0,1\}^* \rightarrow G_1$: 충돌 회피 해쉬함수
- a ($\in Z/\ell$) : 서명자 A의 비밀키
- b ($\in Z/\ell$) : 대리서명자 B의 비밀키
- $P_A = aP$: 서명자 A의 공개키
- $P_B = bP$: 대리서명자 B의 공개키
- $(G_1, G_2, e, \ell, P, H_1, H_2)$: 시스템 파라미터
- W : 위임장
- M : 서명될 메시지

[대리서명 키 생성]

3.1절에서와 같이 원서명자 A는 Bonech의 서명 방식을 이용하여 대리서명에 사용될 비밀키 $D_P = S_W + bH_2(W) = (a+b)H_2(W)$와 공개키 $P_P = P_A + P_B = (a+b)P$를 생성한다.

[대리은닉서명 생성]

서명의뢰자 C에게 서명요청을 받은 대리서명자 B는 난수 $t \in Z/\ell$를 선택하여 $T = tH_2(W)$를 계산하고 서명의뢰자 C에게 위임장 W와 T를 전달한다. 서명의뢰자 C는 난수 $r_1, r_2 \in Z/\ell$를 선택하고 $U = r_1 T + r_1 r_2 H_2(W)$, $h = H_1(M, U)$와 $X = r_1^{-1} h + r_2$를 계산하여 서명자 B에게 X를 전송한다. 서명자 B는 $Y = (t + X) D_P$를 계산하여 서명의뢰자 A에게 Y를 전송한다. 서명의뢰자 C는 $V = r_1 Y$를 계산하고 서명 $sig = (W, U, V)$를 획득한다

[대리은닉서명 검증]

서명요청자 C는 수신된 메시지 M의 대리은닉서명 $sig = (W, U, V)$를 검증하기 위해 원서명자의 공개키 P_A와 대리서명자의 공개키 P_B를 이용하여 대리서명에 사용된 공개키 P_P를 생성하고 위임장 W에 대한 해쉬값 $H_2(W)$와 $h = H_1(M, U)$를 생성한다. 생성한 P_P, $H_2(W)$, $h = H_1(M, U)$와 bilinear-pairing e를 사용하여 식 $e(P_P, U + hH_2(W)) = e(P, V)$이 성립하는지 확인하여 서명의 정당성을 검증한다.

4. 대리서명 방식 제안

이 장에서는 Cha의 ID 기반 서명 방식[20]을 이용한 새로운 대리서명 방식을 제안한다. 제안하는 방식의 안전성은 GDHP를 기반으로 하고 있으며 서명 검증과정은 bilinear-pairing을 사용하여 이루어진다. 4.1절에서 새로운 대리서명 방식을 제안하고, 4.2절에서는 제안하는 방식의 안전성에 대하여 살펴보고 기존의 대리서명 방식과 서로 비교한다.

4.1 제안하는 대리서명 방식

제안하는 대리서명 방식의 키 설정, 위임장 생성 및 전달, 위임장 검증과 대리서명 키 생성, 대리서명 생성, 대리서명 검증과정은 다음과 같다.

[키 설정]

- G_1 : 소수 ℓ을 위수로 가지는 GDH군
- P : G_1의 생성원
- e : $G_1 \times G_1 \rightarrow G_2$: bilinear pairing
- $H_1 : \{0,1\}^* \times G_1 \rightarrow Z/\ell$, $H_2 : \{0,1\}^* \rightarrow G_1$: 충돌 회피 해쉬함수
- a ($\in Z/\ell$) : 서명자 A의 비밀키
- b ($\in Z/\ell$) : 대리서명자 B의 비밀키
- $P_A = aP$: 서명자 A의 공개키
- $P_B = bP$: 대리서명자 B의 공개키
- $(G_1, G_2, e, \ell, P, H_1, H_2)$: 시스템 파라미터
- W: 위임장

[위임장 생성 및 전달]

원서명자 A는 Bonech의 서명 방식[23]을 이용하여 대리서명자 B에 대한 정보와 위임되는 권한에 대한 정보를 담은 W에 대한 서명을 생성한다. 즉, 원서명자 A는 W에 대한 해쉬값 $H_2(W)$에 비밀키 a를 곱하여 W에 대한 서명 $S_W = aH_2(W)$을 생성하여 대리서명자 B에게 S_W, W를 전달한다.

[위임장 검증과 대리서명 키 생성]

S_W, W를 전달받은 대리서명자 B는 S_W가 위임장 W에 대한 정당한 서명인지를 확인한다. 서명검증은 non-degenerated bilinear 함수 e를 사용하여 $(P, P_A, H_2(W), S_W)$가 DDH쌍인지 확인함으로써 이루어진다. 즉, $e(P_A, H_2(W)) = e(P, S_W)$인지 확인한다. 등식이 성립하면 대리서명자 B는 대리서명에 사용될 비밀키 $D_P = S_W + bH_2(W) = (a+b)H_2(W)$와 공개키 $P_P = P_A + P_B = (a+b)P$를 생성한다.

[대리서명 생성]

대리서명자 B는 메시지 M에 대한 대리서명을 생성하기 위해 난수 $t \in Z/\ell$을 선택하고 $U = tH_2(W)$, $h = H_1(M, U)$와 $V = (h+t)D_P$를 계산한다. 대리서명자 B는 서명요청자 C에게 메시지 M에 대한 대리서명 $sig = (W, U, V)$를 전송한다.

[대리서명 검증]

서명요청자 C는 수신된 메시지 M의 대리서명 $sig = (W, U, V)$를 검증하기 위해 원서명자의 공개키 P_A와 대리서명자의 공개키 P_B를 이용하여 대리서명에 사용된 공개키 P_P를 생성하고 위임장 M에 대한 해쉬값 $H_2(W)$와 $h = H_1(M, U)$를 생성한다. 생성한 P_P, $H_2(W)$, $h = H_1(M, U)$와 bilinear pairing e를 사용하여 $(P, P_P, U + hH_2(W), V)$가 DDH쌍인지 확인한다. 즉, $e(P_P, U + hH_2(W)) = e(P, V)$인지 확인하여 서명의 정당성을 검증한다.

$$\begin{aligned} e(P_P, U + hH_2(W)) &= e((a+b)P, tH_2(W) + hH_2(W)) \\ &= e(P, (t+h)H_2(W))^{(a+b)} \\ &= e(P, (h+t)(a+b)H_2(W)) \\ &= e(P, (h+t)D_P) \\ &= e(P, V) \end{aligned}$$

4.2 제안하는 대리서명 방식 분석

제안하는 방식은 대리서명 방식이 가져야할 다음의 조건[7]을 모두 만족한다.

1) 구별가능성(Distinguishability): 서명 $sig = (W, U, V)$에는 위임장 W가 포함되어있고, 더구나 서명 검증시 위임장 W, 원서명자의 공개키 P_A와 대리서명자의 공개키 P_B가 모두 필요하다. 따라서 서명 $sig = (W, U, V)$는 원서명자가 지정한 대리인에 의해 서명된 대리서명임을 확신할 수 있다.
2) 검증가능성(Verifiability): 제안하는 방식은 원서명자가 대리서명자에게 위임장를 발행하는 보증 위임 방식(delegation with warrant)이다. 일반적으로 위임장 W에는 신원정보, 서명에 대한 권한등이 명시되어 있다. 따라서 대리서명 $sig = (W, U, V)$으로부터 검증자는 서명된 메시지에 대한 원서명자의 동의를 확인할 수 있다. 그리고 제안하는 대리서명 방식은 bilinear pairing을 이용하여 누구든지 서명의 진위를 쉽게 확인할 수 있다.
3) 강한 위조 방지(Strong non-forgeability): 제안하는 방식은 Cha의 ID 기반 서명 방식을 기반으로 한 대리서명 방식이므로 적응 가능한 선택 메시지 공격(adaptively chosen message attacks)에 대하여 안전하다[20]. 그리고 대리서명자가 위임장의 내용을 수

의뢰자(A)		대리서명자(B)
		난수 $t \in Z/\ell$ 선택
		$U = tH_2(W)$
		$h = H_1(M, U)$
서명 $sig = (W, U, V)$ 획득	$< \cdots W, U, V \cdots >$	$V = (h+t)D_P$

그림 1 제안하는 대리서명 생성 과정

정하려고 하더라도 위임장 W으로부터 생성되는 대리서명 비밀키 $D_P = S_W + bH_2(W)$는 원서명자의 서명 $S_W = aH_2(W)$으로 생성되기 때문에 대리서명자나 제3자의 위임장 수정도 불가능하다. 또한 대리서명 비밀키에는 대리서명자의 비밀키 b가 포함되어있기 때문에 원서명자도 대리서명을 생성하거나 위조하는 것은 불가능하다.

4) 강한 신원확인(Strong identifiability): 대리서명 $sig = (W, U, V)$에는 위임장 W가 포함되어있기 때문에 모든 사용자는 위임장 W로부터 대리서명자의 신원을 확인할 수 있다.

5) 강한 부인 방지(Strong non-deniability): 대리서명 $sig = (W, U, V)$의 위임장 W로부터 대리서명자의 신원을 쉽게 확인할 수 있으며, 만약 서명자가 후에 자신이 서명한 사실을 부인하더라도 서명 $sig = (W, U, V)$에는 서명자의 비밀정보 b가 사용되었기 때문에 대리서명자는 자신이 대리서명을 생성한 사실을 부인 할 수 없다.

6) 오남용 방지(Prevention of misuse): 원서명자가 대리서명자에게 발행하는 위임장 W에는 서명에 대한 권한 등이 명시되어있고, 위의 강한 위조 방지에 의해 대리서명자는 위임장의 내용을 수정하는 것이 불가능하므로 대리서명자는 자신에게 위임된 권한 내에서만 대리서명은 생성할 수 있다.

제안하는 대리서명 방식은 위임장 W, 원서명자의 비밀키 a와 대리서명자의 비밀키 b를 이용하여 대리서명에 사용될 비밀키 $D_P = (a+b)H_2(W)$를 생성하는 보증부분위임(partial delegation with warrant)방식으로 대리서명자가 사용할 비밀 서명정보에 대리 서명을 할 수 있는 기간을 명시할 수 있으므로 대리인을 철회하고자 하는 경우에 별도의 대리 서명 철회 과정(proxy revocation protocol)이 필요 없다. 또한 보증서를 검증하는 과정이 별도로 요구되는 것이 아니라 대리 서명 검증시에 보증서도 함께 검증 가능함으로 높은 효율성을 가진다. 그리고 제안하는 대리서명 방식은 Cha의 ID 기반 서명 방식을 이용한 대리서명 방식으로 Hess의 ID 기반 은닉서명 방식을 이용한 Zhang의 대리서명 방식에 비하여 서명생성과정에서의 계산량을 크게 줄여 효율성을 증대시켰다. 표 1은 본 논문에서 제안하는 대리서명 방식과 Zhang의 대리서명 방식을 비교한 것이다. 여기에서 H는 해쉬함수의 계산량, A는 타원곡선위에서 덧셈에 대한 계산량, M은 타원곡선위에서 스칼라곱에 대한 계산량, P는 타원곡선위에서 pairing에 대한 계산량을 의미한다.

5. ID 기반 부분은닉서명 방식 제안

F. Zhang은 [13]에서 ID 기반 은닉서명 방식을 제안하였다. 그러나 그는 은닉서명 방식만을 제안하였을 뿐 부분은닉서명 방식을 제안하지는 못했다. 본 논문에서는 Cha의 서명 방식[20]을 기반으로 하여 Zhang의 은닉서명 방식을 변형시킨 또 다른 형태의 ID 기반 은닉서명 방식을 제안한다. 제안하는 방식은 기존 Zhang의 은닉서명 방식과는 달리, 본 논문에서 제안하는 ID 기반 은닉서명 방식 그대로 단지 공통정보만을 추가적으로 삽입함으로써 간단히 ID 기반 부분은닉서명 방식으로 바뀌는 효율적인 서명방식이다.

제안하는 ID 기반 은닉서명 방식은 제안하는 ID 기반 부분은닉서명 방식에서 공통정보만을 제거하면 되므로 이장에서는 ID 기반 부분은닉서명 방식에 대하여 살펴본다.

5.1 제안하는 ID 기반 부분은닉서명 방식

제안하는 ID 기반 부분은닉서명 방식의 안전성은 GDHP를 기반으로 하고 있으며 서명 검증과정은 bilinear-pairing을 사용하여 이루어진다. 제안하는 방식에서 공통정보 C와 그와 관련된 해쉬값 $h_2 = H_3(C)$를 제거하면 ID 기반 은닉서명 방식이 된다. 제안하는 ID 기반 부분은닉서명 방식에서의 키 설정, 부분은닉서명 생성, 부분은닉서명 검증과정은 다음과 같다.

[키 설정]

- G_1 : 소수 ℓ을 위수로 가지는 GDH군
- P : G_1의 생성원
- e : $G_1 \times G_1 \rightarrow G_2$: bilinear pairing
- $H_1 : \{0,1\}^* \times G_1 \rightarrow Z/\ell$, $H_2 : \{0,1\}^* \rightarrow G_1$, $H_3 : \{0,1\}^* \rightarrow Z/\ell$: 충돌 회피 해쉬함수
- ID_B : B의 ID
- b ($\in Z/\ell$) : 서명자 B가 선택하는 난수로 마스터키로 사용된다.
- $Q_B = H_2(ID_B)$: B의 ID와 관련된 공개키

표 1 제안하는 대리서명 방식과 Zhang의 대리서명 방식 비교

		Zhang의 대리서명 방식	제안하는 대리서명 방식
기반한 서명 방식		Hess의 ID 기반 서명 방식	Cha의 ID 기반 서명 방식
계산량	대리서명생성	3M+A+P+H	2M+H
	대리서명검증	M+A+2P+2H	M+2A+2P+2H

- $D_B = b \cdot H_2(ID_B) = bQ_B$: B의 ID와 관련된 비밀키
- $P_B = bP$: 공개
- $(G_1, G_2, e, \ell, P, H_1, H_2, H_3)$: 시스템 파라미터
- M : 서명될 메시지
- C : 부분은닉서명에 삽입할 공통정보로 사전에 서명의뢰자와 서명자간에 서로 합의된 내용이다.

[부분은닉서명생성]

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 $r_1, r_2 \in Z/\ell$를 선택하고 $U = r_1T + r_2Q_B$, $h_1 = H_1(M, U)$, $h_2 = H_3(C)$와 $X = r_1^{-1}(h_1 + r_2h_2)Q_B$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 r_1로 곱하여 $V = r_1Y$를 계산하고 서명 $sig = (C, U, V)$를 획득한다.

[부분은닉서명검증]

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

$$\begin{aligned} e(P_B, h_1Q_B + h_2U) &= e(bP, h_1Q_B + h_2(r_1T + r_2Q_B)) \\ &= e(P, h_1Q_B + h_2r_1tQ_B + h_2r_2Q_B)^b \\ &= e(P, b(h_1Q_B + h_2r_1tQ_B + h_2r_2Q_B)) \\ &= e(P, r_1(br_1^{-1}(h_1 + r_2h_2)Q_B + th_2bQ_B)) \\ &= e(P, r_1(br_1^{-1}(h_1 + r_2h_2)Q_B + th_2D_B)) \\ &= e(P, r_1(bX + th_2D_B)) \\ &= e(P, r_1Y) \\ &= e(P, V) \end{aligned}$$

5.2 제안하는 ID 기반 부분은닉서명 방식 분석

제안하는 방식은 랜덤화 특성을 가지며, 부분은닉서명 방식이 가져야할 부분은닉성과 익명성 조건을 만족한다.

1) 랜덤화 특성(Randomness): 서명자는 서명생성과정에서 비밀 난수 $t \in Z/\ell$를 삽입한다. 서명의뢰자가 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 제안하는 부분은닉서명은 안전하다.
2) 부분은닉성(Partial blindness): 서명의뢰자는 서명자에게 메시지의 내용을 은닉하기 위하여 비밀 난수 $r_1, r_2 \in Z/\ell$를 선택하고 난수 r_1, r_2를 사용하여 생성된 $X = r_1^{-1}(H_1(M, U) + r_2H_3(C))Q_B$를 서명자에게 전달한다. X로부터 은닉정보 r_1, r_2를 구하는 것은 DLP이므로 계산상 불가능하다. 따라서 r_1, r_2를 모르는 서명자는 자신이 서명할 메시지 M에 대한 내용을 전혀 알 수가 없다. 그러나 서명자는 서명 $sig = (C, U, V)$의 $V = r_1(bX + th_2D_B)$에 그가 삽입하고자하는 정보 C의 해쉬값 $h_2 = H_3(C)$를 삽입할 수 있다. 그러므로 제안하는 서명 방식은 서명의뢰자가 서명자에게 메시지의 내용을 보여주지 않고 메시지에 대한 유효한 서명을 얻을 수 있고, 서명자는 비록 서명 내용을 전혀 알 수 없더라도 공통정보를 서명에 포함시킬 수 있다. 그리고 서명자가 공통정보 C를 자신이 직접 서명에 삽입하므로 서명자 B는 삽입한 정

서명의뢰자(A)		서명자(B)
난수 $r_1, r_2 \in Z/\ell$ 선택		난수 $t \in Z/\ell$ 선택
$U = r_1T + r_2Q_B$	<-------- T --------	$T = tQ_B$
$h_1 = H_1(M, U)$		
$h_2 = H_3(C)$		
$X = r_1^{-1}(h_1 + r_2h_2)Q_B$	-------- X ------>	$h_2 = H_3(C)$
$V = r_1Y$	<-------- Y --------	$Y = bX + th_2D_B$
서명 $sig = (C, U, V)$ 획득		

그림 2 제안하는 ID 기반 부분은닉서명 생성 과정

보 C가 서명에 포함된다는 것을 확신할 수 있다. 또한 $V=r_1(bX+th_2D_B)$는 서명자의 마스터키 b와 비밀 난수 t로 이루어진 값이기 때문에 서명의뢰자는 서명 $sig=(C, U, V)$에 삽입된 공통정보 C를 제거하거나 변형할 수 없다.

3) 익명성(Anonimity): 서명 $sig=(C, U, V)$에는 서명의뢰자의 신원을 연관시킬 정보가 아무것도 존재하지 않고 $U=r_1T+r_2Q_B$나 $V=r_1Y$로부터 은닉정보 r_1, r_2를 구하는 것은 DLP이므로 계산상 불가능하다. 그러므로 서명자는 부분은닉서명 방식을 통한 자신의 서명생성단계 수행과정에서 얻은 정보와 서명검증을 위해 수신한 메시지-서명 쌍을 서로 연결시키는 것은 불가능하다. 따라서 제안하는 서명 방식은 서명의뢰자의 익명성을 보호하며 서명의뢰자의 신원을 추정하거나 추적하는 것이 불가능하다.

제안하는 방식은 Cha의 ID 기반 서명 방식을 토대로 한 ID 기반 부분은닉서명 방식으로 적응 가능한 선택 메시지 공격(adaptively chosen message attacks)에 대하여 안전하며[20], 생성된 서명 $sig=(C, U, V)$는 서명자의 비밀정보 b가 사용되기 때문에 서명자이외의 어느 누구도 서명을 만들 수 없고 또한 서명 $sig=(C, U, V)$에는 서명의뢰자가 선택한 난수 $r_1, r_2 \in Z/\ell$이 삽입되었기 때문에 서명을 위조할 수는 없다. 그리고 제안하는 서명 방식은 bilinear pairing을 이용하여 누구든지 서명의 진위 여부를 쉽게 확인할 수 있으며, 만약 서명자가 후에 자신이 서명한 사실을 부인하더라도 서명 $sig=(C, U, V)$에는 서명자의 마스터키 b가 사용되었기 때문에 서명자는 자신이 서명한 사실을 부인할 수 없다.

6. 대리부분은닉서명 방식 제안

대리서명은 다른 특수서명과 결합하여 또 다른 형태의 특수서명 방식을 생성한다. 2001년 B. Lee, H. Kim과 K. Kim[11]은 대리서명을 부분은닉서명에 적용하면 대리부분은닉서명이라는 새로운 형태의 특수서명방식이 생성된다고 논하였다. 본 논문에서는 4장에서 제안한 대리서명 방식과 5장에서 제안한 ID 기반 부분은닉서명 방식을 결합하여 새롭게 제안된 특수서명 방식인 대리부분은닉서명 방식을 생성하였다.

6.1 제안하는 대리부분은닉서명 방식

제안하는 대리부분은닉서명 방식의 안전성은 GDHP를 기반으로 하고 있으며 서명 검증과정은 bilinear-pairing을 사용하여 이루어진다. 제안하는 방식은 5장에서 제안한 ID 기반 부분은닉서명 방식과 마찬가지로 단지 공통정보 C와 그와 관련된 해쉬값 $h_2=H_3(C)$를 제거함으로써 쉽게 대리은닉서명 방식으로 변환된다. 따라서 제안하는 대리은닉서명 방식은 기존 Zhang의 대리은닉서명 방식을 개선시킨 효율적인 서명방식이다. 제안하는 대리부분은닉서명 방식에서의 키 설정, 대리서명키 생성, 대리부분은닉서명 생성, 대리부분은닉서명 검증과정은 다음과 같다.

[키 설정]

- G_1 : 소수 ℓ을 위수로 가지는 GDH군
- P : G_1의 생성원
- e : $G_1 \times G_1 \rightarrow G_2$: bilinear pairing
- $H_1: \{0,1\}^* \times G_1 \rightarrow Z/\ell$, $H_2: \{0,1\}^* \rightarrow G_1$, $H_3: \{0,1\}^* \rightarrow Z/\ell$: 충돌 회피 해쉬함수
- a $(\in Z/\ell)$: 서명자 A의 비밀키
- b $(\in Z/\ell)$: 대리서명자 B의 비밀키
- $P_A=aP$: 서명자 A의 공개키
- $P_B=bP$: 대리서명자 B의 공개키
- W : 위임장
- $(G_1, G_2, e, \ell, P, H_1, H_2, H_3)$: 시스템 파라미터
- M : 서명될 메시지
- C : 부분은닉서명에 삽입할 공통정보로 사전에 서명의뢰자와 서명자간에 서로 합의된 내용이다.

[대리서명 키 생성]

4장에서와 같이 원서명자 A는 Bonech의 서명 방식을 이용하여 대리서명에 사용될 비밀키 $D_P=S_W+bH_2(W)=(a+b)H_2(W)$와 공개키 $P_P=P_A+P_B=(a+b)P$를 생성한다.

[대리부분은닉서명 생성]

서명의뢰자 C에게 서명요청을 받은 대리서명자 B는 난수 $t \in Z/\ell$를 선택하여 $T=tH_2(W)$를 계산하고 서명의뢰자 C에게 위임장 W와 T를 전달한다. T를 전달받은 서명의뢰자 C는 메시지 M을 은닉하기 위해 난수 $r_1, r_2 \in Z/\ell$를 선택하고 $U=r_1T+r_2H_2(W)$, $h_1=H_1(M, U)$, $h_2=H_3(C)$와 $X=r_1^{-1}(h_1+r_2h_2)$를 계산하여 서명자 B에게 X를 전송한다. X를 전송 받은 서명자 B는 $h_2=H_3(C)$와 $Y=(X+th_2)D_P$를 계산하여 서명의뢰자 A에게 Y를 전송한다. 서명의뢰자 C는 전달받은 Y를 자신이 처음 선택한 난수 r_1로 곱하여 $V=r_1Y$를 계산하고 서명 $sig=(W, C, U, V)$를 획득한다

[대리부분은닉서명 검증]

서명요청자 C는 수신된 메시지 M의 대리부분은닉서명 $sig=(W, C, U, V)$를 검증하기 위해 원서명자의 공개키 P_A와 대리서명자의 공개키 P_B를 이용하여 대리서명에 사용된 공개키 P_P를 생성하고 위임장 W에 대한 해쉬

의뢰자(A)		대리서명자(B)
난수 $r_1, r_2 \in Z/\ell$ 선택 $U = r_1 T + r_2 H_2(W)$ $h_1 = H_1(M, U)$ $h_2 = H_3(C)$ $X = r_1^{-1}(h_1 + r_2 h_2)$ $V = r_1 Y$ 서명 $sig = (W, C, U, V)$ 획득	<---- W, T --- ------ X ----->\n<----- Y -----	난수 $t \in Z/\ell$ 선택 $T = tH_2(W)$ $h_2 = H_3(C)$ $Y = (X + th_2)D_P$

그림 3 제안하는 대리부분은닉서명 생성 과정

값 $H_2(W)$를 생성한다. 생성한 P_P, $H_2(W)$와 bilinear-pairing e를 사용하여 $(P, P_P, h_1H_2(W)+h_2U, V)$가 DDH쌍인지 확인한다. 즉, $e(P_P, h_1H_2(W)+h_2U) = e(P, V)$ 인지 확인하여 서명의 정당성을 검증한다.

$$
\begin{aligned}
& e(P_P, h_1H_2(W)+h_2U) \\
&= e((a+b)P, h_1H_2(W)+h_2(r_1T+r_2H_2(W))) \\
&= e(P, h_1H_2(W)+h_2r_1tH_2(W)+h_2r_2H_2(W))^{(a+b)} \\
&= e(P, (a+b)(h_1+h_2r_1t+h_2r_2)H_2(W)) \\
&= e(P, (h_1+h_2r_1t+h_2r_2)D_P) \\
&= e(P, r_1(r_1^{-1}(h_1+r_2h_2)+th_2)D_P) \\
&= e(P, r_1(X+th_2)D_P) \\
&= e(P, r_1Y) \\
&= e(P, V)
\end{aligned}
$$

6.2 제안하는 대리부분은닉서명 방식 분석

대리부분은닉서명 방식은 대리서명과 부분은닉서명을 결합한 서명 방식이다. 따라서 대리부분은닉서명이 가져야할 조건은 대리서명이 가져야할 조건에 부분은닉서명이 가져야할 요구조건이 추가된다. 제안하는 대리부분은닉서명 방식은 구별가능성, 검증가능성, 강한 위조 방지, 강한 신원확인, 강한 부인 방지, 오남용 방지, 랜덤화 특성, 부분은닉성과 익명성을 모두 만족하는 서명 방식이다. 제안하는 대리부분은닉서명 방식의 안전성은 4장과 5장에서 제안하는 서명 방식들에 대한 안전성과 같다.

7. 결 론

대리서명은 대리서명자가 원서명자를 대신해서 서명하는 암호방식이고, 부분은닉서명은 서명자가 삽입하고자 하는 정보를 은닉서명에 삽입할 수 있도록 하는 암호방식으로 행위자의 행동이 노출되어서는 안 되는 보안서비스에 중요하게 활용되며 데이타베이스의 무제한적인 증가문제를 해결한다. 대리서명과 부분은닉서명은 안전한 전자상거래에 중요하게 활용되는 서명 방식으로, 실제로 전자상거래에서는 다양한 형태의 변형된 특수서명 방식들이 사용되고 있다. 본 논문에서는 보증부분위임방식에 의한 대리서명 방식과 ID 기반 부분은닉서명 방식을 제안한다. 그리고 이 두 방식을 결합한 대리부분은닉방식을 제안한다. 또한 본 논문에서 제안한 ID 기반 부분은닉서명 방식과 대리부분은닉서명 방식에서 공통정보를 제거하면 각각 ID 기반 은닉서명 방식과 대리은닉서명 방식이 된다. 제안하는 방식 모두 bilinear-pairing을 사용하며 안전하고 효율적인 서명 방식들이다.

참 고 문 헌

[1] 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, pp. 1338-1353, Sep., 1996.

[2] S. Kim, S. Park and D. Won, "Proxy signature, revisited," Proc. of ICICS'97, LNCS 1334, Springer-Verlag, pp. 223-232, 1997.

[3] Z. Tan, Z. Liu and C. Tang, "Digital Proxy Blind Signature Schemes Based on DLP and ECDLP," MM Research Preprints, No. 21, MMRC, AMSS, Academia, Sinica, Beijing, pp. 212-217. Dec., 2002.

[4] K. Zhang, "Threshold proxy signature schemes," 1997 Information Security Workshop, Japan, pp. 191-197. Sep., 1997.

[5] A. Boldyreva, A. Palacio and B. Warinschi, "Secure Proxy Signature Schemes for Delegation of Signing Rights," Cryptology ePrint Archive, Report 2003/096, available at http://eprint.iacr.org/2003/096/.

[6] H. M. Sun and B. T. Hsieh, "On the Security of

Some Proxy Signature Schemes," Cryptology ePrint Archive, Report 2003/068, available at http://eprint.iacr.org/2003/068/.

[7] B. Lee, H. Kim and K. Kim, "Secure mobile agent using strong non-designated proxy signature," Proc. of ACISP'01, LNCS 2119, Springer Verlag, pp. 474-486, 2001.

[8] S. Lai and A. K. Awasthi, "Proxy blind signature scheme," Cryptology ePrint Archive, Report 2003/072, available at http://eprint.iacr.org/2003/072/.

[9] F. Zhang, R. Safavi-Naini and C. Y. Lin, "New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Schemes from Bilinear Pairings," Cryptology ePrint Archive, Report 2003/104, available at http://eprint.iacr.org/2003/104/.

[10] S. Lal and A. K. Awasthi, "A New Multi-Proxy Signature Scheme for Partial Delegation with Warrant," eCryp ePrint Archive, Report No. 2003/001 http://www.gfcr.org/ecryp/multi.pdf.

[11] B. Lee, H. Kim and K. Kim, "Strong Proxy Signature and its Applications," Proc. of SCIS 2001, available at http://caislab.icu.ac.kr/~sultan/.

[12] F. Hess, "Efficient identity based signature schemes based on pairings," SAC 2002, LNCS 2595, pp. 310-324, Springer-Verlag, 2002.

[13] F. Zhang and K. Kim, "Efficient ID-based blind singature and Proxy Signature form Pairings," to appear at ACISP 2003, Springer-Verag, 2003.

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

[15] M. Abe and E. Fujisaki. "How to date blind signatures," In K. Kim and T. Matsumoto, editors, Advances in Cryptology - Asiacrypt'96, LNCS 1163, Springer-Verag, pp. 244-251, 1996.

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

[17] 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.

[18] 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.

[19] H. Y. Chien, J. K. Jan, Y. M. Tseng, "RSA-Based Partially Blind Signature with Low Computation," Proc. of ICPADS'01, KyunJu, Korea. pp. 385-389. 2001.

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

[21] T. Okamoto and D. Pointcheval, "The Gap-Problems: A new class of problems for the security of cryptographic schemes," Advances in Cryptology, Proc. of PKC'01, Springer-Verlag, preprint, pp. 104-118., 2001.

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

[23] D. Bonech, B. Lynn, H. Shacham, "Short signatures from the Weil pairing," Advanvances in Cryptology, Proc. of Asiacrypt'01, Springer-Verlag, preprint, 2001.

[24] K. G. Paterson, "ID-based signatures from pairings on elliptic curves," Electron. Lett., Vol. 38, No. 18, pp. 1025-1026, 2002.

[25] F. Hess, "Exponent group signature schemes and efficient identity based signature schemes based on pairings," Cryptology ePrint Archive, Report 2002/012, available at http://eprint.iacr.org/2002/012/.

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

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

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

[29] 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

1995년 세명대학교 수학과 졸업(학사) 1997년 서강대학교 수학과 졸업(석사) 1999년~현재 성균관대학교 전기전자 및 컴퓨터공학부 박사과정. 관심분야는 암호이론, 전자상거래보안

여 상 희

1994년 순천향대학교 전산통계학과(학사) 2001년 충북대학교 경영학과(석사). 2002년~현재 성균관대학교 정보통신공학부 박사과정. 관심분야는 암호이론, 전자상거래보안

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. 2003년~2004년 성균관대학교 연구처장. 1982년~현재 성균관대학교 정보통신공학부 교수. 2000년~현재 정보통신부 지정 정보보호인증기술연구센터장. 관심분야는 암호이론, 정보시스템보안 등