情報保護學會論文誌
第15券 第3號, 2005. 6

자체인증 공개키를 사용하는 threshold 대리서명 기법의 안전성 분석

박 제 홍,[1†‡] 강 보 경,[2] 한 상 근[2]
[1]국가보안기술연구소, [2]한국과학기술원

Security analysis of a threshold proxy signature scheme using a self-certified public key

Je Hong Park,[1†‡] Bo Gyeong Kang,[2] Sang Geun Hahn[2]
[1]NSRI, [2]KAIST

요 약

최근 다중 사용자 환경에서 안전한 대리서명을 설계하고자 하는 연구가 진행되면서, threshold 서명 방식을 대리서명에 적용한 threshold 대리서명 기법들이 제안되고 있다. 최근 Hsu와 Wu는 이산대수 문제 기반의 자체인증 공개키 (Self-certified public key)를 사용하는 threshold 대리서명 기법을 제안하였다. 본 논문에서는 이 대리서명 기법이 자체인증 공개키의 취약성에 의한 원서명자의 위조 공격 (Original signer's forgery attack)에 취약함을 보임으로써 부인 방지 (nonrepudiation) 성질을 가지지 못함을 확인한다.

ABSTRACT

On the research for constructing secure group-oriented proxy signature schemes, there are several proposals of threshold proxy signature schemes which combine the notions of proxy signature with threshold signature. Recently, Hsu and Wu proposed a threshold proxy signature scheme which uses a self-certified public key based on discrete logarithm problem. In this paper, we show that this scheme is vulnerable to original signer's forgery attack. So our attack provides the evidence that this scheme does not satisfy nonrepudiation property.

Keywords : *Proxy signature schemes, Proxy threshold signature scheme, Security analysis, Public key cryptosystem*

Ⅰ. 서 론

대리서명은 1996년 Mambo, Usuda 그리고 Okamoto에 의해 처음 제안된 개념으로, 원서명자로 불리는 한 사용자가 대리서명자로 불리는 다른 사용자에게 자신의 서명 권한을 위임하여 대리서명자가 원서명자 대신 서명을 생성할 수 있게 하는 방법이다.[1] 이러한 대리서명의 개념을 다중 사용자 환경 (multi-user setting)으로 확장하여, Zhang[2]과 Kim 등[3]은 각각 threshold 암호시스템과 비밀분산 기법 (secret sharing scheme)에 기반한 threshold 대리서명 기법을 제안하였다. 일반적으로 (t,n) threshold 대리서명 기법은 원서명자가 자신의 서명 권한을 n명의 대리서명자로 구성된 그룹에 위임하여 그룹에 속하는 t명 이상의 대리서명자가 서로 협력하여 대리서명을 생성한다. 안전한

접수일 : 2005년 3월 29일 ; 채택일 : 2005년 6월 7일
† 주저자, ‡ 교신저자 : jhpark@etri.re.kr

threshold 대리서명 기법은 다음의 안전성 조건을 만족해야 한다.[4]

- 비밀성 (Secrecy): 원서명자의 개인키는 대리서명키의 부분 정보나 대리서명 등의 어떠한 공개된 정보로부터도 얻을 수 없어야 한다. 특히, 모든 대리서명자가 공모할 경우에도 원서명자의 개인키가 노출되지 않아야 한다.
- 대리자 보호 (Proxy protected): 오직 위임받은 대리서명자만이 유효한 대리서명을 생성할 수 있으며, 원서명자라도 대리서명자의 역할을 수행할 수 없다.
- 위조 방지 (Unforgeability): 유효한 대리서명은 t명 이상의 대리서명자의 협력에 의해서만 생성될 수 있다. 이는 $t-1$명 이하의 대리서명자나 대리서명 권한을 위임받지 않은 제 삼자는 대리서명을 생성할 수 없음을 의미한다.
- 부인 방지 (Nonrepudiation): 실제 서명에 참여한 대리서명자는 자신이 메시지에 서명했다는 사실을 부인할 수 없다. 이와 함께, 원서명자는 대리서명자 그룹에 자신의 서명 권한을 위임했음을 부인할 수 없다.

이러한 threshold 대리서명의 개념이 소개된 이후 여러 기법들[4-7]이 제안되었지만 모두 다양한 공격에 취약함이 증명되었다.[5,9,10]

최근 Hsu와 Wu는 자체인증 공개키 (Self-certified public key)를 사용하는 threshold 대리서명 기법을 제안하였다.[11] 이 HW 기법에서 각 사용자의 공개키는 시스템 관리자 (System Authority (SA))에 의해 생성되어 계산적으로 위조불가능한 성질 (computational unforgeable property)을 가지며, 이에 대응하는 개인키는 사용자에 의해 계산된다. 그러므로 사용자 인증을 위한 인증서가 필요하지 않고, 대신 사용자에 대한 인증은 자체인증 공개키를 사용하는 암호 기법자체의 검증 절차에 의해 암묵적으로 검증된다. 예를 들어, 서명 기법의 경우 주어진 서명에 대한 검증만으로 서명자에 대한 인증을 동시에 보장하는 것이다. 또한 HW 기법은 메시지 복원형 (message recovery type)으로 시간정보나 개인식별정보와 같은 작은 길이의 메시지를 서명해야 하는 다양한 응용 프로토콜에 적용이 가능하다.

본 논문에서는 HW 기법이 논문에서 주장하는 부인 방지 (nonrepudiation) 성질을 만족하지 않음을 보인다. 이 기법에서는 원서명자가 SA를 속여 대리서명자의 허가 없이 threshold 대리서명을 생성할 수 있다. 이는 원서명자가 스스로 자신이 위임한 대리서명자 그룹의 임의의 t명이 생성한 것으로 검증되는 대리서명을 위조할 수 있다는 것을 의미한다. 이러한 공격은 Hsu와 Wu가 제안한 자체인증 공개키를 사용하는 대리서명 기법[12]에 대한 Shao[13]의 공격방법을 적용한 것으로, Hsu와 Wu가 제안한 일반적인 공개키 기반구조 (conventional PKI)에서 정의되는 threshold 대리서명 기법[14]과 Hsu, Wu 그리고 He가 제안한 대리 다중서명 기법[15]에 대한 취약성을 보이는 데도 적용될 수 있다. 이러한 공격은 사용자가 자체인증 공개키를 발급받는 과정에서, 키를 발급해 주는 SA가 사용자로부터 전달받은 정보에 대한 적절한 검증을 하지 않기 때문에 발생하는 문제이다.

본 논문의 구성은 다음과 같다. 먼저 Ⅱ절에서 자체인증 공개키를 사용하는 threshold 대리서명 기법에 대해 소개한 다음, Ⅲ절에서는 그 안전성을 분석하며, Ⅳ절에서 결론을 맺는다.

Ⅱ. 자체인증 threshold 대리서명 기법

HW 기법은 이산대수 기반의 자체인증 공개키를 사용하며 메시지 복구 (message recovery) 성질을 가진다. 그러므로 이 기법은 자체인증 공개키 시스템에서 사용자 등록을 관리하는 시스템 관리자 (SA)가 필요하며 등록 (registration)과정을 통해 사용자가 SA로부터 자체인증 공개키를 받는다. 이어 대리서명 키를 생성하는 대리 비밀분산 생성 (proxy secret share generation), 그리고 이렇게 생성된 대리서명 키를 이용하여 대리서명을 생성하고 검증하는 대리서명 생성 (proxy signature generation)과 대리서명 검증 (proxy signature verification)의 네 단계로 구성된다.

먼저 p와 q를 두 큰 소수라 하자. 여기에서 $q \mid (p-1)$이고 g는 F_p상의 위수가 q인 부분군의 생성자 (generator)이다. 그리고 안전한 일방향 해쉬함수 $H_1 : \{0,1\}^* \rightarrow Z_q^*$와 $H_2 : \{0,1\}^* \rightarrow F_p^*$, 그리고 h를 가정하자. 논문 [11]에서는 H_1과 H_2의 구분 없이 하나의 일반적인 일방향 해쉬함수를 이용하여 표현하였지만, 본 논문에서는 그 역할을 구분하기 위하여 두 개의 해쉬함수로 표현하였다. 파라미터 (p,q,g)와 함수 H_1, H_2, h는 공개된다. ID_i는 사

용자 U_i에 대한 개인식별정보 (identity)로 정의된다. 논문 [11]에서는 ID_i가 Z_q^*의 원소로 사용되는데, 이는 실제 문자열로 표현되는 개인식별정보에 대한 해쉬값으로 보면 무방할 것이다. SA의 개인키와 공개키는 각각 γ와 β로 $\gamma \in Z_q^*$이고 $\beta = g^{\gamma} \bmod p$이다. 다음은 서명기법을 구성하는 네 단계에 대한 자세한 설명이다.

· 등록: 각 사용자 U_i는 임의로 $t_i \in Z_q^*$를 선택하여 $v_i = g^{H_1(t_i \| ID_i)} \bmod p$를 계산하고 (v_i, ID_i)를 SA에게 보낸다. SA는 임의로 $k_i \in Z_q^*$를 선택하고

$$y_i = v_i H_2(ID_i)^{-1} g^{k_i} \bmod p \quad (1)$$
$$e_i = k_i + H_1(y_i \| ID_i)\gamma \bmod q,$$

를 계산하여 (y_i, e_i)를 U_i에게 보낸다. 그러면 U_i는 $x_i = e_i + H_1(t_i \| ID_i) \bmod q$를 계산하고 그 유효성을 다음 식을 통해 확인한다.

$$\beta^{H_1(y_i \| ID_i)} H_2(ID_i) y_i = g^{x_i} \bmod p \quad (2)$$

이 식이 성립하면 U_i는 (x_i, y_i)를 자신의 개인키와 공개키 쌍으로 받는다. 그리고 SA는 등록 과정 완료 후, U_i의 공개키 y_i를 공시한다.

· 대리 비밀분산 생성: U_o를 원서명자, $G = \{U_1, \cdots, U_n\}$를 n명의 대리서명자 U_i로 구성된 그룹, 그리고 GID를 G에 속한 서명자들의 개인식별정보를 포함하는 집합이라 하자. 그리고 m_w는 원서명자와 대리서명자들의 개인식별정보와 위임 기간 (delegation duration), threshold 값 t 등의 정보를 담고있는 위임장 (warrant)이라 하자. U_o는 자신의 서명 권한을 위임하기 위해 다음의 절차를 수행한다.

① 먼저 임의로 $k \in Z_q^*$를 선택하고, 다음 값을 계산한다.

$$K = g^k \left(\beta^{\sum_{i=1}^{n} H_1(y_i \| ID_i)} \prod_{i=1}^{n} H_2(ID_i) y_i \right)^{-1},$$

$$\sigma = H_1(m_w \| K \| GID) x_o + k \bmod q.$$

② 계수가 Z_q^*의 원소인 $(t-1)$차 다항식 $f(x) = f(x) = \sigma + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \bmod q$를 결정하고 계수로부터 각 i $(1 \le i \le t-1)$에 대해 $A_i = g^{a_i} \bmod p$를 계산한다.

③ 대리 비밀분산 $\sigma_i = f(ID_i)$를 각 대리서명자 $U_i \in G$에게 안전한 경로 (secure channel)로 전송한다. 원서명자 U_o로부터 σ_i를 받은 각 사용자 $U_i \in G$는 다음 식으로부터 이 값의 유효성을 확인하며, 만일 유효할 경우 대리 비밀분산 σ_i가 검증된다.

$$g^{\sigma_i} = (\beta^{H_1(y_i \| ID_i)} H_2(ID_o) y_o)^{H_1(m_w \| K \| GID)} K \beta^{\sum_{j=1}^{n} H_1(y_j \| ID_j)} \left(\prod_{j=1}^{n} H_2(ID_j) y_j\right) \left(\prod_{j=1}^{t-1} A_j^{ID_i^j}\right) \bmod p.$$

· 대리서명의 생성: 주어진 메시지 m에 대해, G에 속하는 t명 이상의 대리서명자는 U_o를 대신해서 유효한 대리서명을 생성할 수 있다. 일반성을 잃지 않고 $D = \{U_1, \cdots, U_t\}$를 실제 서명에 참여하는 대리서명자라 하고 $ASID$를 D에 속하는 모든 사용자의 개인식별정보의 집합이라 하자. D에 속하는 모든 사용자는 협력하여 U_o를 대신해 m에 대한 서명을 다음과 같은 절차에 따라 생성한다.

① 각 사용자 $U_i \in D$는 임의로 $z_i \in Z_q^*$를 선택하고 $r_i = g^{z_i} \bmod p$를 계산하여 공개한다.

② 다른 사용자들의 r_i를 얻은 다음, 각 사용자 $U_i \in D$는 다음을 계산한다.

$$R = (m \| h(m)) \prod_{i=1}^{t} r_i^{r_i} \bmod p,$$
$$s_i = z_i r_i + L_i \sigma_i H_1(GID \| R \| K) + x_i H_1(ASID \| R \| K) \bmod q.$$

여기에서 $L_i = \prod_{\substack{j=1 \\ i \neq j}}^{t} -ID_j (ID_i - ID_j)^{-1} \bmod q$ 이다.

U_i는 s_i를 지정된 대표자 (designated clerk)에게 전송한다.

③ s_i를 받은 대표자는 다음을 확인하여 유효성을 검증한다.

$$g^{s_i}=r_i^{r_i}((\beta^{H_1(y_i\|ID_i)}H_2(ID_o)y_o)^{H_1(m_w\|K\|GID)}K$$
$$(\beta^{\sum_{i=1}^{n}H_1(y_i\|ID_i)}\prod_{j=1}^{n}H_2(ID_j)y_j\prod_{j=1}^{t-1}A_j^{ID_j^i})^{LH_1(GID\|R\|K)}$$
$$\times(\beta^{H_1(y_i\|ID_i)}H_2(ID_i)y_i)^{H_1(ASID\|R\|K)}\bmod p.$$

만일 유효하다면, (r_i,s_i)는 m에 대한 U_i의 유효한 개별 대리서명 (individual proxy signature)이다. 만일 모든 i $(1\le i\le t)$에 대해 (r_i,s_i)가 검증되면, 대표자는 $S=\sum_{i=1}^{t}s_i \bmod q$를 계산하고 m에 대한 대리서명으로 $(K,R,S,m_w,GID,ASID)$을 제시한다.

· 대리서명의 검증: 메시지 m에 대한 대리서명 $(K,R,S,m_w,GID,ASID)$을 받은 검증자는 위임장 m_w로부터 원서명자의 개인식별정보와 대리서명자 그룹을 확인하고 $ASID$로부터 실제 서명자들의 개인식별정보를 확인한다. 이어서 SA나 대리서명자 그룹으로부터 필요한 공개키를 확보하여 메시지 m과 해쉬값 $h(m)$의 연접을 다음의 식을 통해 구한다.

$$m\|h(m)=Rg^{-S}((\beta^{H_1(y_i\|ID_i)}H_2(ID_o)y_o)^{H_1(m_w\|K\|GID)} \quad (3)$$
$$K(\beta^{\sum_{i=1}^{n}H_1(y_i\|ID_i)}\prod_{i=1}^{n}H_2(ID_i)y_i)^{H_1(GID\|R\|K)}$$
$$\times(\beta^{\sum_{i=1}^{t}H_1(y_i\|ID_i)}\prod_{i=1}^{t}H_2(ID_i)y_i)^{H_1(ASID\|R\|K)}\bmod p.$$

대리서명 $(K,R,S,m_w,GID,ASID)$은 m에 대한 해쉬값과 $h(m)$이 일치할 경우 유효하다.

III. 안전성 분석

개인식별정보 ID_o를 가진 사용자 U_o가 대리서명자 그룹 $G=\{U_1,\cdots,U_n\}$의 동의없이 threshold 대리서명을 생성하려고 한다고 가정하자. GID를 G에 속하는 서명자들의 모든 개인식별정보들의 집합이라 하고 $ASID$를 U_o가 위조할 서명의 실제 서명자로 정한 G의 구성원 $\{U_1,\cdots,U_t\}$의 모든 개인식별정보들의 집합이라 하자. 그리고 G의 각 구성원 U_i $(i=1,\cdots,n)$는 등록 과정을 거쳐, 식 (2)의 관계를 만족하는 개인키/공개키 쌍 (x_i,y_i)을 갖는다.

메시지 m에 대해, U_o는 임의로 $k\in Z_q^*$를 선택하고 각 i $(1\le i\le t)$에 대해 $z_i\in Z_q^*$를 선택한 후,

$$r_i=g^{z_i}(i=1,2,\cdots,t),\quad R=m\|h(m)\prod_{i=1}^{t}r_i^{r_i},$$
$$K=g^k(\beta^{\sum_{i=1}^{n}H_1(y_i\|ID_i)}\prod_{i=1}^{n}H_2(ID_i)y_i)^{-1}\bmod p$$

를 계산하고 다음 값을 정한다.

$$\alpha=\frac{H_1(ASID\|R\|K)}{H_1(m_w\|K\|GID)H_1(GID\|R\|K)}.$$

여기에서 m_w는 원서명자의 개인식별정보와 GID, 그리고 위임 기간 등의 정보를 포함하는 위조된 위임장이다.

위조된 서명이 $ASID$에 의해 서명된 것처럼 보이게 하기 위해, U_o는 등록단계에서 SA를 다음과 같이 속인다. 먼저, U_o는 임의로 $t_o\in Z_q^*$를 선택하고,

$$v=g^{H_1(t_o\|ID_o)}(\beta^{\sum_{i=1}^{t}H_1(y_i\|ID_i)}\prod_{i=1}^{t}H_2(ID_i)y_i)^{-\alpha}\bmod p$$

를 계산한 후, (v,ID_o)를 SA에게 보낸다. 그러면 SA는 등록 과정의 절차 (식 (1))에 따라 $z\in Z_q^*$를 임의로 선택한 후, $y_o=vH_2(ID_o)^{-1}g^z \bmod p$와 $e=z+H_1(t_o\|ID_o)\gamma \bmod q$를 계산하고, (y_o,e)를 U_o에게 반환한다. U_o는 $x_o=e+H_1(t_o\|ID_o)\bmod q$를 계산하고

$$\beta^{H_1(y_o\|ID_o)}H_2(ID_o)y_o$$
$$\times(\beta^{\sum_{i=1}^{t}H_1(y_i\|ID_i)}\prod_{i=1}^{t_o}H_2(ID_i)y_i)^{\alpha}=g^{x_o}\bmod p$$

이 성립하면, (x_o,y_o)를 자신의 개인키/공개키 쌍으로 받아들인다. 이 과정은 SA가 식 (1)의 계산을 정확하게 수행한 것인지 U_o가 확인하는 것이다. 이

러한 과정이 끝나면 SA는 U_o의 공개키 y_o를 공시한다. 이제 U_o는

$$S' = \sum_{i=1}^{t_o} z_i r_i + x_o H_1(m_w \| K \| GID) H_1(GID \| R \| K) + k H_1(GID \| R \| K) \bmod q$$

를 계산하고 메시지 m에 대한 대리서명으로 $(K, R, S', m_w, GID, ASID)$를 제시한다. 검증자는

$g^k = K(\beta^{\sum_{i=1}^{n} H_1(y_i \| ID_i)} \prod_{i=1}^{n} H_2(ID_i) y_i) \bmod p$, 그리고

$$g^{x_o} = \beta^{H_1(y_o \| ID_o)} H_2(ID_o) y_o \times (\beta^{\sum_{i=1}^{t_o} H_1(y_i \| ID_i)} \prod_{i=1}^{t_o} H_2(ID_i) y_i)^{\alpha} \bmod p$$

으로부터 아래와 같은 관계를 확인할 수 있다.

$$\begin{aligned} & Rg^{-S'} ((\beta^{H_1(y_o \| ID_o)} H_2(ID_o) y_o)^{H_1(m_w \| K \| GID)} \\ & K(\beta^{\sum_{i=1}^{n} H_1(y_i \| ID_i)} \prod_{i=1}^{n} H_2(ID_i) y_i))^{H_1(GID \| R \| K)} \\ & \times (\beta^{\sum_{i=1}^{t_o} H_1(y_i \| ID_i)} \prod_{i=1}^{t_o} H_2(ID_i) y_i)^{H_1(ASID \| R \| K)} \\ & = m \| h(m). \end{aligned}$$

그러므로, 검증자는 식 (3)을 계산하여 $m \| h(m)$을 얻게 되므로, S'의 유효성을 검증하게 된다. 즉, S'는 메시지 m에 대해 원서명자 U_o가 $ASID$의 구성원들에 서명권한을 위임하여 생성한 것으로 위조된 threshold 대리서명이다.

이러한 공격은 근본적으로 HW 기법에서 사용하는 자체인증 공개키의 생성과정의 문제에 기인한다. 등록 과정에서 SA는 키를 발급받으려는 사용자로부터 정보를 받아 이에 대한 아무런 검증 없이 키 생성에 필요한 값만 계산하여 사용자에게 전송한다. 그러므로 위의 공격과 같이 원하는 형태의 키를 얻기 위해 공격자는 등록 과정에서 처음 전송 정보를 조작하는 것이 가능하다.

V. 결 론

본 논문에서는 Hsu와 Wu가 제안한 자체인증 공개키를 사용하는 threshold 대리서명 기법이 원서명자 위조공격에 취약함을 보였다. 이러한 공격은 서명 기법이 사용하는 자체인증 공개키 생성 방식의 취약성에서 비롯한 것으로 원사용자는 시스템 관리자를 속임으로써 주어진 메시지에 대한 서명을 위조할 수 있음을 보였다. 이를 통해 HW 기법이 부인방지 성질을 만족하지 않음을 알 수 있다.

참 고 문 헌

[1] M. Mambo, K. Usuda, E. Okamoto, "Proxy signatures for delegating signing operation," *Proc. 3rd ACM CCS*, pp. 48-57, 1996.

[2] K. Zhang, "Threshold proxy signature schemes," *Information Security - ISW '97*, Lecture Notes in Comput. Sci. Vol. 1396, pp. 282-290, 1997.

[3] S. Kim, S. Park, D. Won, "Proxy signatures, revisited," Information and *Communications Security - ICICS '97*, Lecture Notes in Comput. Sci. Vol. 1334, pp. 223-232, 1997.

[4] M.-S. Hwang, E.J.-L. Lu, I.-C. Lin, "A practical (t,n) threshold proxy signature scheme based on the RSA cryptosystem. *IEEE T. Knowl. Data En.*, Vol.15(6), pp. 1552-1560, 2003.

[5] H.M. Sun. "An efficient nonrepudiable threshold proxy signatures with known signers." *Comput. Commun.* Vol. 22(8), pp. 717-722, 1999.

[6] C.-L. Hsu, T.-S. Wu, T.-C. Wu, "New nonrepudiable threshold proxy signature scheme with known signers. *J. Syst. Software*, vol. 58, pp. 119-124, 2001.

[7] C.-Y. Yang, S.-F. Tzeng, M.-S. Hwang, "On the efficiency of nonrepudiable threshold proxy signatures with known signers. *J. Syst. Software*, Vol.22(9), pp. 1-8, 2003.

[8] S.-F. Tzeng, M.-S. Hwang, C.-Y. Yang,

"An improvement of nonrepudiable threshold proxy signature scheme with known signers," *Comput. Secur.*, Vol.23, pp. 174-178, 2004.

[9] G. Wang, F. Bao, J. Zhou, R.H. Deng, "Comments on "A practical (t,n) threshold proxy signature scheme based on the RSA cryptosystem"," *IEEE T. Knowl. Data En.*, Vol. 16(10), pp. 1309-1311, 2004.

[10] Z. Tan, Z. Liu, "On the security of some nonrepudiable threshold proxy signature schemes with known signers, *Cryptology ePrint Archive*, Report 2004/234.

[11] C.-L. Hsu, T.-S. Wu "Self-certified threshold proxy signature schemes with message recovery, nonrepudiation, and traceability," *Appl. Math. Comput.*, Vol.164(1), pp. 201-225, 2005.

[12] C.-L. Hsu, T.-S. Wu, "Efficient proxy signature schemes using self-certified public keys," *Appl. Math. Comput.*, Vol.152(3), pp. 807-820, 2004.

[13] Z. Shao, "Improvement of efficient proxy signature schemes using self-certified public keys," *Appl. Math. Comput.*, in press, 2005.

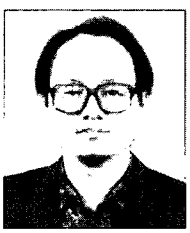
[14] C.-L. Hsu, T.-S. Wu, "Efficient nonrepudiable threshold proxy signature scheme with known signers against the collusion attack," *Appl. Math. Comput.*, in press.

[15] C.-L. Hsu, T.-S. Wu, W.-H. He, "New proxy multi-signature scheme," *Appl. Math. Comput.*, Vol. 162(3), pp. 1201-1206, 2005.

〈著者紹介〉

박 제 홍 (Je Hong Park)
1998년 2월: 경북대학교 수학과 졸업
2000년 2월: 한국과학기술원 수학과 석사
2004년 2월: 한국과학기술원 수학과 박사
2004년 3월~현재: 국가보안기술연구소 연구원
〈관심분야〉 암호론, 정수론

강 보 경 (Bo Gyeong Kang)
1999년 8월: 서울대학교 수학교육학과 졸업
2001년 8월: 한국과학기술원 수학과 석사
2001년 9월~현재: 한국과학기술원 수학과 박사과정
2004년 9월~현재: Visiting Researcher, Univ. of Maryland at College Park
〈관심분야〉 암호론, 타원곡선, Complexity theory



한 상 근 (Sang Geun Hahn)
1979년: 서울대학교 수학과 졸업
1982년: 뉴멕시코 주립대 수학과 석사
1987년: 오하이오 주립대 수학과 박사
1987년~현재: 한국과학기술원 수학과 교수
〈관심분야〉 암호학, 타원곡선, 정수론