通信情報保護論文誌
第9券 第4號 1999. 12

고차잉여류 문제에 기반한 검증 가능한 자체인증 방식

주미리*, 이보영*, 양형규**, 원동호*

Verifiable self-certified schemes based on γ^{th}-residuosity problem

Mi-ri Joo*, Bo-young Lee*, Hyung-kyu,Yang, Dong-ho Won*

요약

본 논문에서는 공개키가 사용될 때만 공개키 정당성을 검증할 수 있다는 Girault의 자체인증 공개키 방식의 단점을 개선한 검증 가능한 자체인증 공개키 방식의 개념을 이용하여, 고차잉여류에 기반한 검증 가능한 자체인증 방식(키분배 방식, 개인식별 방식, 디지털 서명 방식 등)을 제안한다. 제안한 방식의 안전성은 고차잉여류와 이산대수 문제에 기반을 두고 있다.

Abstract

In this paper we propose the verifiable self-certified schemes(key distribution scheme, identification scheme, digital signature scheme) based on γ^{th}-residuosity, which make up for defects of Girault's self-certified schemes allow the authenticity of public keys to be verified during the use of the keys.

The security of our schemes is based on the difficulty of γ^{th}-residuosity problem and discrete logarithm problem simultaneously.

* 성균관대학교 전기·전자 및 컴퓨터 공학부 정보통신보호연구실, ** 강남대학교 전자계산학과

I. 서론

대칭키 암호 시스템의 키 분배 문제 등을 해결하고자 제시된 공개키 암호 방식은 공개키 디렉토리 관리라는 새로운 문제를 발생시켰다. 공개키 디렉토리 관리 문제를 해결하기 위하여 제안된 방법으로는 개인식별정보에 기반(identity-based)을 둔 방식[1]과 인증서에 기반한 (certification-based) 방식[2]이 있다.

인증서에 기반한 방식이란 신뢰센터가 각 사용자의 공개키를 사용자의 개인식별정보와 함께 신뢰센터의 비밀키로 서명한 인증서(certificate)를 발행함으로서 각 사용자의 공개키를 인증하는 방식이다. 이 방식은 신뢰센터가 사용자의 비밀키를 알 수 없으나, 인증서 검증시 사용되는 추가적인 파라미터를 저장하기 위한 메모리와 전송 정보 및 계산량을 요구한다.

개인식별정보에 기반한 방식은 각 사용자들의 개인식별정보(identity) 자체가 공개키이며, 신뢰센터가 사용자들의 개인식별정보를 이용하여 그에 상응하는 비밀키를 생성하여 스마트 카드에 저장하여 발행한다.[1] 이 방식에서는 비밀키 자체가 공개키 인증서이므로 특별한 인증 절차를 요구하지 않으며, 인증서에 기반한 방식보다 공개키의 크기가 작다. 그러나 신뢰센터가 사용자의 비밀키를 생성하므로 신뢰센터는 임의의 가입자를 위장할 수 있다는 문제점을 내포하고 있다.

1991년 Girault는 인증서에 기반한 방식과 개인식별정보에 기반한 방식의 중간 개념인 자체인증 공개키 방식(self-certified public key)을 제안하였다.[2] 이 방식은 별도의 인증서를 요구하지 않고 공개키 자체가 인증서의 역할을 하는 방식이므로, 인증서에 기반한 방식이 아니며, 공개키가 사용자의 개인식별정보에 제한되지 않기 때문에 역시 개인식별정보에 기반을 둔 방식도 아니다.[3]

특히, Girault는 신뢰센터에 대한 다음의 3가지 신뢰 유형을 정의하였다.

- 신뢰 유형 1 : 신뢰센터가 모든 사용자의 비밀키를 아는 유형인 시스템으로 센터는 언제든지 각 사용자를 위장할 수 있다.
- 신뢰 유형 2 : 신뢰센터가 각 사용자의 비밀키를 알 수는 없으나, 사용자를 위장할 수 있다.
- 신뢰 유형 3 : 신뢰센터가 신뢰 유형 2와 마찬가지로 각 사용자의 비밀키를 알 수 없고, 또한 센터는 각 사용자를 위장할 수 없다. 여기서 위장할 수 없다 함은 실질적으로는 위장할 수 있으나 후에 센터의 거짓 행위를 알 수 있다는 것이다.

1994년 박성준 등은 자체인증 공개키 방식을 개인식별정보에 기반을 둔 방식에 적용한 자체인증 개인식별정보 방식을 제안하였다. 이 방식은 자체인증 공개키 방식에서 인증서의 역할을 하는 공개키가 바로 개인식별정보이다.[4][5]

Girault가 제시한 자체인증 공개키 방식에서 공개키는 메시지 암호화나 서명 검증 또는 키 분배 등에서 공개키가 사용될 때 검증되므로, 자체인증 공개키를 사용하는 프로토콜이 실패하는 경우, 프로토콜에 오류가 발생하였는지 아니면 공개키에 오류가 발생하였는지 정확히 알 수 없다는 단점을 가지고 있다. 1999년 김승주 등은 이를 개선한 자체인증(self certification)과 검증 가능성(verifiability)을 가진 검증 가능한 자체인증 공개키 방식을 제안하였다.[6]

본 논문에서는 검증 가능한 자체인증 공개키 방식을 이용하여 고차 잉여류에 기반한 검증 가능한 자체인증 방식을 제시하고자 한다. 2장에서는 검증 가능한 자체인증 방식에 대하여 소개하고 3장에서는 본 논문의 기반이 되는 고차잉여류에 대한 수학적인 배경에 대하여 설명한다. 또한 4장에서는 제안하는 고차잉여류에 기반한 검증 가능한 자체인증 방식을 제시하고 5장에서 결론으로 끝을 맺는다.

II. 검증 가능한 자체인증 방식

1999년 김승주 등은 암호화나 서명 검증 또는 키 교환 등에 키가 사용될 때 검증되므로, 자체 인증 공개키를 이용하는 디지털 서명이 실패할 경우, 서명이 잘못 되었는지 아니면 공개키가 잘못 되었는지를 확실히 알 수 없다는 자체인증 공개키 방식의 단

점을 해결하기 위해서 검증 가능한 자체인증 방식을 제안하였다.[6]

2.1 검증 가능한 자체인증 방식의 정의[6]

검증 가능한 자체인증 공개키(Verifiable self-certified public keys) 방식은 다음 2가지 조건을 만족한다.

(1) 자체인증(self certification)
: 인증 정보는 공개키와 같다. 사용자의 개인식별정보(ID)나 비밀키/공개키 등은 어떠한 암호 프로토콜에서도 사용 중에 암시적으로 검증되는, 계산적으로 위조 불가능한 관계를 만족한다.

(2) 검증 가능(verifiability)
: 필요할 경우에는 인증 정보를 알고 난 후 공개키를 검증할 수 있는 효율적인 방법이 존재한다.

2.2 검증 가능한 자체인증 공개키 방식 프로토콜

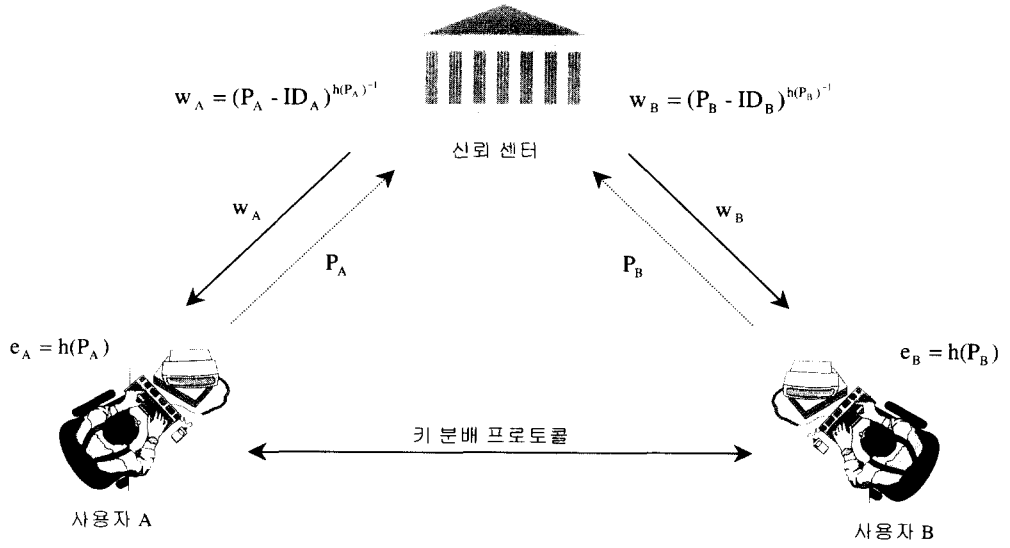
검증 가능한 자체인증 공개키 방식은 신분이 확인된 사용자가 자신의 공개키 P를 신뢰센터에게 전달하면, 신뢰센터는 사용자의 개인식별정보와 공개키를 이용한 인증 정보 w를 생성하여 사용자에게 전달한다. 다음 프로토콜은 RSA 디지털 서명 방식을 이용한 검증 가능한 자체인증 공개키 방식으로, 사용자 A에 대한 인증 정보 w_A는 다음과 같은 과정을 통 생성되며, 다른 사용자들도 같은 과정을 통해 인증 정보를 신뢰센터로부터 발급 받는다. [그림 1]은 검증 가능한 자체인증 공개키 방식을 나타낸다.

[단계 1]
사용자 A는 임의 정수 S_A를 자신의 비밀키로 선택하고 공개키 P_A를 다음과 같이 계산한 후, 신뢰센터에 P_A를 전송한다.

$$P_A \equiv g^{-S_A} \pmod{n}$$

[단계 2]
신뢰 센터는 사용자 A의 신분을 확인 한 후, A의 공개키와 개인식별정보를 이용하여 인증 정보 w_A를 다음과 같이 계산한 후 사용자 A에게 전송한다.

$$w_A \equiv (P_A - ID_A)^{h(P_A)^{-1}} \pmod{n}$$



[그림 1] 검증 가능한 자체 인증 공개키 방식
[Fig 1] Verifiable self-certified public key scheme

[단계 3]

사용자 A의 검증 가능한 자체인증 공개키는 w_A와 e_A이다.

$$e_A = h(P_A) = h(b^{S_A}) \pmod n$$

III. 수학적 배경

이 절에서는 본 논문에서 사용하는 고차잉여류 문제에 대한 수학적인 기본 개념들을 정리한다.[7][8][9][10]

3.1 고차잉여류 문제 (γ^{th}-residuosity problem)

양의 정수 γ, n이 주어질 때 정수 z가 다음의 조건을 만족하면, z를 법 n에 관하여 고차잉여류(γ^{th}-residue)라 한다.

[조건] $\gcd(z, n) = 1$이고 $z = x^{\gamma} \pmod n$을 만족하는 x가 존재한다.

위의 조건을 만족하지 않는 z는 고차비잉여류(γ^{th}-nonresidue)라 한다.

고차잉여류 문제(γ^{th}- Residuosity Problem : 약어로 γ^{th}-RP)란 주어진 $\gcd(z, n) = 1$인 양의 정수 $z \in Z_n^*$가 고차잉여류인지 고차비잉여류인지를 결정하는 것이다.

고차잉여류 문제의 계산 복잡도는 γ가 다항식 크기(polynomial size)일 때는 n의 소인수 분해 문제와 동치이고 γ가 지수적 크기(exponential size)일 대는 n의 소인수 분해 문제보다 어렵다고 간주되고 있다.[7]

n이 소수인 경우 위의 문제는 쉽게 해결되지만, n의 소인수를 알 수 없는 합성수인 경우 위의 문제는 매우 어렵다고 알려져 있다.

3.2 Acceptable triple (n, γ, y)

(n, γ, y)가 아래의 세 가지 조건을 만족할 때 acceptable triple이라 한다.

[조건 1] $n = n_1 n_2 \ldots n_t$. 여기서 각 n_i는 홀수의 소수이다.

[조건 2] γ는 $1 \le k \le t$인 하나의 k에 대해 $\gcd(\gamma, \phi(n_k)) = \gamma$ 이고, 나머지 $i\ (\neq k)$에 대해 $\gcd(\gamma, \phi(n_i)) = 1$인 2 보다 큰 홀수이다.

[조건 3] $y = h_1^{b_1\gamma + e} \prod_{j=2}^{t} h_j^{b_j} \pmod n$. 여기서 모든 $i \neq k$, $1 \le j \le t$ 에 대해 $0 < e < \gamma$, $\gcd(e, \gamma) = 1$, $k \le b_j \le \phi(n_j)$ 이고, $\langle h_1, h_2, \ldots, h_t \rangle$는 Z_n^*의 생성 벡터(generator-vector)이다.

3.3 잉여류 지수(class-index)

Acceptable triple (n, γ, y)과 $z \in Z_n^*$가 주어졌을 때 $z = y^i u^{\gamma} \bmod n$을 만족하는 i를 z의 잉여류 지수(class-index)라 한다.

γ^{th}-RP와 관련된 문제로 잉여류-지수-비교(class-index-comparing) 문제와 잉여류-지수-계산(class-index-finding) 문제가 있다.

① 고차잉여류 문제

Acceptable triple (n, γ, y)과 $\gcd(z, n) = 1$인 양의 정수 $z \in Z_n^*$가 주어졌을 때 $z \in Z_n^*$가 고차잉여류인지 고차비잉여류인지를 결정하는 문제이다.

②잉여류-지수-비교(Class-index-comparing) 문제

Acceptable triple (n, γ, y)과 $z_1, z_2 \in Z_n^*$이 주어졌을 때 $z_1 = y^i u^{\gamma} \pmod n$과 $z_2 = y^j u^{\gamma} \pmod n$의 잉여류 지수 i, j를 비교하는 문제이다.

③ 잉여류-지수-계산(Class-index-finding) 문제

Acceptable triple (n, γ, y)과 양의 정수 $z \in Z_n^*$가 주어졌을 때 $z = y^i u^\gamma \bmod n$의 잉여류 지수 i를 찾는 문제이다.

IV. 제안하는 검증 가능한 자체 인증 방식

본 절에서 이산대수 문제와 결합한 고차잉여류에 기반을 두고 있는 검증 가능한 자체인증 방식을 제안한다.

4.1 시스템 초기화

신뢰센터는 acceptable triple (n, γ^d, y)을 선택한다. 단, n은 소수 p와 q의 곱 $(n = p \cdot q)$이고, d는 γ가 지수적 크기를 갖도록 하는 임의의 정수이며 형태는 다음과 같다.

$$n = p \cdot q = (2\gamma^d fp' + 1) \cdot (2fq' + 1)$$

여기서, f, p', q'는 서로 다른 소수이고, $\gcd(\gamma, q') = 1$, $\gcd(\gamma, f) = 1$이다. y는 modulus n 상에서 (γ^{d}-th)-비잉여류이고, b는 modulus p와 modulus q 상에서 위수(order)가 f인 Z_n의 원소로, 법 n 상에서의 위수(order)도 f이다. 신뢰센터의 공개키는 (n, γ^d, y, b, f)이고 비밀키는 (p', q')이다.

4.2 검증 가능한 자체인증 공개키 생성

사용자 A는 신뢰센터 CA에 의해서 정당한 신분임을 확인 받은 후에, 신뢰 센터로부터 인증 정보(witness) w_A를 받는다. 인증 정보 w_A는 다음과 같이 생성된다.

[단계 1]

사용자 A는 자신의 비밀키로 f보다 적은 임의의 수 S_A를 자신의 비밀키로 선택하고 자신의 개인식별정보 ID_A와 공개키 P_A를 다음과 같이 계산하여, 신뢰센터를 방문하여 공개키 P_A를 전달한다.

$$P_A \equiv b^{S_A} \pmod n$$

[단계 2]

신뢰 센터는 사용자 A의 신분을 확인 한 후, 사용자 A의 식별정보 ID_A와 공개키 P_A를 이용하여 $(h(ID_A) \oplus h(b^{S_A}) b^{S_A})^{-1} \pmod n$의 잉여류 지수 i_A와 $(h(ID_A) \oplus h(b^{S_A}) b^{S_A} y^{i_A})^{-1} \pmod n$

〔표 1〕 고차잉여류에 기반한 검증 가능한 자체인증 공개키 생성

[Table 1] Verifiable self-certified public key generation based on γ^{th}-residuosity

사용자 A		신뢰 센터
$S_A \in_R [0, f-1]$ $P_A \equiv b^{S_A} \bmod n$	P_A, ID_A →	$h(ID_A) \oplus h(b^{S_A})$ $\equiv b^{-S_A} \cdot y^{-i_A} \cdot x_A^{-\gamma^d} \pmod n$
	← i_A, x_A	i_A, x_A 계산
$w_A = (i_A, x_A)$ $e_A = h(P_A) = h(b^{S_A})$		

〔표 2〕 키분배 프로토콜

[Table 2] Key distribution protocol

사용자 A		사용자 B
K_{AB} $\equiv [(h(ID_B) \oplus h(b^{S_B})) \cdot y^{i_B} \cdot x_B^{\gamma^d}]^{S_A}$ $\equiv b^{S_B S_A} \pmod n$	i_A, x_A, e_A → i_B, x_B, e_B ←	K_{AB} $\equiv [(h(ID_A) \oplus h(b^{S_A})) \cdot y^{i_A} \cdot x_A^{\gamma^d}]^{S_B}$ $\equiv b^{S_A S_B} \pmod n$

의 γ^d의 근 x_A를 계산한다. 즉, 신뢰 센터는 다음 수식을 만족하는 인증 정보 $w_A (= (i_A, x_A))$를 계산하여 사용자 A에게 전송한다. 특히 i_A와 x_A는 비밀일 필요가 없다. 즉, 사용자 A의 비밀키는 S_A뿐이다.

$$h(ID_A) \oplus h(b^{S_A}) \equiv b^{-S_A} \cdot y^{-i_A} \cdot x_A^{-\gamma^d} \pmod n$$

〔단계 3〕

사용자 A의 검증 가능한 자체인증 공개키는 (i_A, x_A)와 e_A이다.

$$e_A = h(P_A) = h(b^{S_A})$$

4.3 키 분배 프로토콜

신뢰센터에 의해서 신분이 확인된 사용자 A와 B는 각각 검증 가능한 자체인증 공개키 (i_A, x_A, e_A)와 (i_B, x_B, e_B)를 갖는다. 사용자 A와 B가 공통키를 분배하고자 할 때의 프로토콜은 다음과 같다.

〔단계 1〕

사용자 A는 자신의 검증 가능한 자체인증 공개키 (i_A, x_A, e_A)를 B에게 전송한다.

〔단계 2〕

사용자 B도 자신의 검증 가능한 자체인증 공개키 (i_B, x_B, e_B)를 A에게 전송한다.

〔단계 3〕

사용자 A와 사용자 B의 공통키 K_{AB}를 다음 식에 의해서 얻는다.(modulus n 상에서)

$$\begin{aligned} K_{AB} &\equiv [(h(ID_A) \oplus h(b^{S_A})) \cdot y^{i_A} \cdot x_A^{\gamma^d}]^{S_B} \\ &\equiv [(h(ID_B) \oplus h(b^{S_B})) \cdot y^{i_B} \cdot x_B^{\gamma^d}]^{S_A} \\ &\equiv b^{-S_A S_B} \pmod n \end{aligned}$$

4.4 개인식별 프로토콜

증명자 A가 검증자 B에게 자신이 A임을 증명하고자 할 때의 프로토콜은 다음과 같다.

〔단계 1〕

증명자 A는 $[0, f-1]$ 상에서 난수 r을 선택하여, R을 다음과 같이 계산하여 검증자 B에게 전송한다.

$$R \equiv b^r \pmod n$$

〔단계 2〕

검증자 B는 $[0, 2^t-1]$상에서 난수 e를 선택하여 증명자 A에게 전송한다.

〔단계 3〕

증명자 A는 $z \equiv r + S_A e \pmod f$를 계산하여, (i_A, x_A), e_A, z를 검증자 B에게 전송한다.

〔단계 4〕

검증자 B는 modulus n상에서 사용자 A로부터 수신한 R이 $[(h(ID_A) \oplus h(b^{S_A}))y^{i_A}x_A^{\gamma^d}]^e b^z$ 인지를 검증한다.

〔표 3〕 개인 식별 프로토콜
[Table 3] Identification protocol

증명자 A		검증자 B
$S_A \in_R [0, f-1]$ $P_A \equiv b^{S_A} \pmod n$ $r \in_R [0, f-1]$ $R \equiv b^r \pmod n$	R →	
	← e	$e \in_R [0, 2^t-1]$
$z \equiv r + S_A e \pmod f$	$(i_A, x_A), e_A, z$ →	$R \stackrel{?}{=} [(h(ID_A) \oplus h(b^{S_A})) \cdot y^{i_A} \cdot x_A^{\gamma_A^d}]^e b^z \pmod n$

4.5 디지털 서명 프로토콜

사용자 A가 평문 m에 서명을 하여 사용자 B에게 전달하고자 할 때의 프로토콜은 다음과 같다.

〔단계 1〕

사용자 A는 $[0, f-1]$상에서 난수 r을 선택하여 R을 계산한다.

$$R \equiv b^r \pmod n$$

〔단계 2〕

또한 e를 다음과 같이 계산한다.

$$e = h(R \| m)$$

여기서 h는 공통의 해쉬 함수이다.

〔단계 3〕

사용자 A는 $z \equiv r + S_A e \pmod f$를 계산한 후, (i_A, x_A), e_A, e, z를 사용자 B에게 전송한다.

〔단계 4〕

사용자 B는 $[(h(ID_A) \oplus h(b^{S_A}))y^{i_A}x_A^{\gamma_A^d}]^e b^z$과 수신한 R이 같은지를 modulus n 상에서 검증한다.

〔단계 5〕

사용자 B는 $e \stackrel{?}{=} h(R \| m)$인지를 검증한다.

4.6 공개키 검증

만일 위에서 제안한 키분배, 개인식별, 디지털 서명 프로토콜들이 실패할 경우, 각 사용자들은 다음과 같이 공개키를 검증함으로써 프로토콜에서 사용되었던 공개키의 정당성을 확인할 수 있다.

$$\widetilde{P_{A(B)}} \equiv [(h(ID_{A(B)}) \oplus h(b^{S_{A(B)}})) \cdot y^{i_{A(B)}} \cdot x_{A(B)}^{\gamma_{A(B)}^d}]^{-1} \pmod n$$

$$\equiv \widetilde{b^{S_{A(B)}}} \pmod n$$

$$e_{A(B)} \stackrel{?}{=} h(\widetilde{b^{S_{A(B)}}})$$

위의 식이 정당하다고 검증되면 프로토콜에 오류가 발생한 것이고, 만일 식이 정당하지 않으면 사용자의 공개키가 정당하지 않은 것이다.

〔표 4〕 디지털 서명 프로토콜
[Table 4] Digital signature protocol

사용자 A		사용자 B
$S_A \in_R [0, f-1]$ $P_A \equiv b^{S_A} \pmod n$ $r \in_R [0, f-1]$ $R \equiv b^r \pmod n$ $e = h(R \| m)$ $z \equiv r + S_A e \pmod f$	$(i_A, x_A), e_A\ e, z,$ →	$R \equiv [(h(ID_A) \oplus h(b^{S_A})) \cdot y^{i_A} \cdot x_A^{\gamma^d}]^e \cdot b^z \pmod n$ 계산 $e \stackrel{?}{=} h(R \| m)$검증

V. 결론

Girault가 제시한 자체인증 공개키 방식에서 공개키는 메시지 암호화나 서명 검증 또는 키 분배 등에서 공개키가 사용될 때 검증된다. 그러므로, 자체인증 공개키를 사용하는 프로토콜이 실패하는 경우, 프로토콜에 오류가 발생하였는지 아니면 공개키에 오류가 발생하였는지를 정확히 알 수 없다는 단점을 가지고 있다. 본 논문에서는 위에서 언급한 방식의 단점을 개선하고자 김승주 등이 제시한 검증 가능한 자체인증 공개키 방식을 고차 잉여류에 기반을 둔 방식에 적용한 키분배 및 개인 식별, 디지털 서명 등을 제안하였다. 제안한 방식의 안전성은 고차잉여류 문제와 이산 대수 문제에 기반을 두고 있으며, 사용자의 개인식별정보와 공개키를 해쉬 함수에 적용하여 인증 정보와 검증 가능한 공개키를 생성하므로 효율적이다.

참고 문헌

〔1〕Shamir, "Identity-Based Cryptosystems and Signature Schemes", Crypto'84, pp.47- 53, 1984.

〔2〕 M. Girault, "Self-certified public keys" ,Advances in Cryptology EUROCRYPT'91, pp.490-497, 1991.

〔3〕 C.Y.Kwon, D.H.Won, "A study on self-certified public key scheme", The Review of Korea Institute of Information Security & Cryptology, Vol.3/No 3, 1993.9

〔4〕 S. J. Park and D. H. Won, "A paradoxical identity-based scheme based on γ^{th}-residuosity problem and discrete logarithm problem", KIISC vol. 4, No. 2, pp. 113-118, 1994

〔5〕 S. J. Park, H. K. Yang, D. H. Won, "Self-certified identity", Proc. of

CISC'94(Conference on Information Security & Cryptology), Vol.4/No 1, 1994.11

[6] Seung-joo Kim, Soo-hyun Oh, Sang-joon Park and Dong-ho Won, "Verifiable self-certified public keys", Daniel AUGOT and Claude CARLET (Eds.): Proc. of WCC'99, INRIA Workshop on Coding and Cryptography, pp.139-148, 1999

[7] Y. Zneng, T. Matsumoto and H. Imai, "Residuosity Problem and its Application to Cryptography", Trans, IEICE, vol.E71, No.8, pp.759-767, 1988.

[8] S.J.Park, H.K.Yang, D.H.Won, "A class of public key residue cryptosystems", Proc. of CISC'95, Conference on Information Security & Cryptology, Vol.5/No 1, 1995

[9] S.J. Kim, C.Y. Kwon, S.G. Kang, D.H. Won, "A study on public key authentication schemes", The Riview of Korea Institute of Information Security & Cryptology, Vol. 6/No 4, 1996

[10] B.Y. Lee, Y.Y. Choi, M.R. Joo, D.H. Won, "An efficient ID-based authentication scheme based on the γ^{th}-residuosity problem in wireless environment", Journal of the Korea Institute of Information Security and Cryptology, Vol.9/No 2, 1999.6

著者紹介

주 미 리(Mi-ri Joo) 정회원

1996년 2월 :성균관대학교 정보공학과 졸업
1998년 2월 :성균관대학교 정보공학과 석사
1999년 3월 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학부 박사과정
〈관심분야〉 암호이론, 이동통신보안

이 보 영(Bo-young Lee) 정회원

1989년 2월 :성균관대학교 정보공학과 졸업
1995년 8월 :성균관대학교 정보공학과 석사
1996년 3월 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학부 박사과정
〈관심분야〉 암호이론, 이동통신보안

양 형 규(Hyung-kyu,Yang) 정회원

1983년 2월 :성균관대학교 전자공학과 졸업
1985년 8월 :성균관대학교 전자공학과 석사
1994년 8월 :성균관대학교 정보공학과 박사
1984년 12월 ~ 1990년 2월 : 삼성전자 컴퓨터부문 선임연구원
1995년 3월 ~ 현재 :강남대학교 이공대학 전자계산학과전공 조교수
〈관심분야〉 네트워크 보안, 암호화 프로토콜

원 동 호(Dong-ho Won) 정회원

1976년 2월 :성균관대학교 전자공학과 졸업
1978년 2월 :성균관대학교 전자공학과 석사
1988년 2월 :성균관대학교 전자공학과 박사
1978년 4월 ~ 1980년 3월 한국전자통신연구원 연구원
1985년 9월 ~ 1986년 8월 일본 동경공대 객원연구원
1982년 ~ 현재 성균관대학교 공과대학 전기전자 및 컴퓨터공학부 정교수
1996년 4월 ~ 1998년 4월 정보화 추진위원회 자문위원
〈관심분야〉 암호이론, 정보이론