검증 가능한 자체인증 개인식별 및 키분배 프로토콜

김 경 국† · 유 준 석†† · 원 동 호†††

요 약

본 논문에서는 인증서기반 방식의 장점과 Girault의 자체인증 공개키방식의 장점을 결합한 검증 가능한 자체인증 방식을 이용한 개인식별과 키분배 프로토콜을 제안한다. 제안한 방식의 안전성은 고차잉여류 문제와 이산대수 문제에 기반을 두고 있다.

Verifiable Self-Certified Identification and Key-Distribution Protocols

Kyung-Kug Kim† · Joon-Suk Yu†† · Dong-Ho Won†††

ABSTRACT

In this paper we propose verifiable self-certified identification and key distribution protocols which has advantages of certificate-based scheme and Girault's self-certified public key. The security of the proposed protocols is based on γ^{th}-residuosity problem and discrete logarithm problem.

1. 서 론

1976년 Diffie-Hellman 공개키 방식[1]을 발표한 이후 암호계는 놀랄만한 발전을 이루었으며, 이들은 수신자가 복호화 키만 비밀로 보관하고, 암호화 키는 공개해도 암호계를 위태롭게 하지 않는 새로운 종류의 암호방식을 제안하여 관용 암호방식의 키 전송 문제점을 해결하였다.

공개키 암호방식은 송수신자가 연관성이 있으나 서로 다른 두 개의 키를 이용하는 비대칭 암호 시스템(asymmetric cryptosystem)이며 한쪽 방향의 통신만 제공한다. 다른 방향으로 통신을 시작하려면 새로운 한 쌍의 키가 필요하다. 비대칭 암호방식에서 두 통신자를 구분하기 위해 각각 송신자(sender)와 수신자(receiver)라 부른다.

전형적인 공개키 방식에서 공개키 디렉토리를 제거하는 방식에는 2가지 방법이 있는 바, 그 중 하나는 certification-based 방식으로 변형하는 것이고, 또 하나는 identity-based 방식으로 변형하는 것이다. certification-based 방식은 신뢰센터(trusted center 또는 key authentication center)가 자신의 공개키를 공개하고, 가입자의 identity I와 공개키 P에 대한 서명(signature)을 가입자에게 분배하는 것이다. 이중 많은 공개키 방식이 제안되었는데, 대부분의 방식은 해당 가입자만이 아는 비밀키 s와 누구든지 아는 공개키 P를 가지고 구성되어진다.

s와 P는 수학적으로 강한 연관성을 가지나 P에서 s를

† 정 회 원 : 성균관대학교 전기전자 및 컴퓨터 공학부
†† 준 회 원 : 성균관대학교 대학원 전기전자 및 컴퓨터 공학부
††† 종신회원 : 성균관대학교 전기전자 및 컴퓨터 공학부 교수
논문접수 : 1999년 5월 4일, 심사완료 : 1999년 9월 9일

계산하는 것은 불가능하다. 공개키 P는 비밀성(Confidentiality)을 유지하기 위해 보호될 필요는 없다. 그러므로 공개키는 가능한 공개적으로 만들어져야 한다.

모든 사용자가 액세스할 수 있는 공개키 디렉토리에 의해 사용자 A의 공개키 P_A에 대한 제3자의능동적 공격(active attack)이 가능하게 되어 공개키 디렉토리내의 공개키에 대한 인증 문제가 야기된다. 이러한 안전성 문제를 해결하기 위해서는 인증서 W를 도입해 해결한다. 인증서의 형식은 사용자의 개인식별정보 I, 공개키 P에 대한 신뢰센터의 디지틀 서명꼴을 취한다.

Identity-based 방식에서는 각 사용자의 공개키 P가 바로 자신의 개인식별정보 I가 됨으로써 특별한 인증서 W를 요구하지 않는다. 즉, 이 방식에서 인증서 W는 바로 자신만이 소유한 비밀키 s가 된다.

〈표 1〉 암호 방식의 비교

	시스템 구성	공개키 (생성)	비밀키 (생성)	인증서 (생성)	신뢰 수준	검증성
Public key	(s,P)	P:사용자	s:사용자	-		
Certification -based	(I,s,P, W)	I, P:사용자 W:신뢰센터	s:사용자	(I, P)에 대한 신뢰센터의 서명	3	명시적
ID-based	(I, s) P=I, W=s	I	s:신뢰 센터	신뢰센터	1	묵시적
Self-certified public keys	(I, s, P) W=P	(I, P)	s:사용자	신뢰센터	2, 3	묵시적

또한 Girault의 자체인증 공개키 방식[2]에서는 공개키 P 자체가 인증서 W의 역할을 하게 된다. 즉, W = P가 된다. 바로 이 이유에서 자체인증 공개키라고 명명된다. 다음 <표 1>에서는 인증서 W의 형식에 의해 키 관리 방식들을 분류하였다. (여기서, I는 사용자의 개인식별정보(ID)이며, (s, P)는 (비밀키, 공개키) 쌍, 그리고 W는 인증서이다).

결론적으로 자체인증 공개키 방식은 가입자가 자신의 비밀키를 선택하므로 identity-based 방식이 갖는 문제점, 즉 센터가 모든 사용자의 비밀키를 안다 ==을 해결할 수 있고, 또한 메모리와 계산량을 감소시킨다는 장점이 있다. 그리고 Girault는 자체인증 공개키 방식과 더불어 키와 관련한 3가지 신뢰수준을 정의하였다.

(1) 신뢰수준 1 : 신뢰센터가 모든 사용자의 비밀키를 아는 유형의 시스템으로 신뢰센터는 언제든지 각 사용자를 흉내 낼 수 있다.
(2) 신뢰수준 2 : 신뢰센터가 각 사용자의 비밀키를 알 수는 없으나, 비합법적인 공개키 인증서를 만들어서 합법적인 사용자를 흉내 낼 수 있다.
(3) 신뢰수준 3 : 신뢰센터가 신뢰수준 2와 마찬가지로 각 사용자의 비밀키를 알 수 없고 또한 신뢰센터는 각 사용자를 흉내 낼 수 없다. 여기서 흉내낼 수 없다는 것은 신뢰센터가 비합법적인 공개키 인증서를 생성하여 합법적인 사용자를 흉내낼 수 있으나, 후에 신뢰센터의 위법 행위를 알 수 있다.

그러나, 자체인증 공개키 방식은 암호화나 서명 검증 또는 키 교환 등에 키가 사용될 때에만 키가 검증된다는 단점이 있다. 즉, 디지틀 서명의 검증 과정에서 문제가 발생했다면, 자체인증 공개키에 기반한 방식에서는 이것이 디지틀 서명의 문제인지, 공개키 자체의 문제인지 구별해 낼 수 없다. 이러한 문제점을 해결하기 위해서 김승주 등은 검증 가능한 자체인증 공개키 방식을 제안하였다[5].

본 논문에서는 자체인증 공개키 방식을 이용한 개인식별 및 키분배 프로토콜을 제안한다. 제안하는 방식의 안전성은 고차잉여류와 이산대수의 어려움에 기반을 두었으며, 특히 이 방식은 Schnorr 방식만큼 효율적임을 밝혀둔다.

2. Girault의 자체인증 공개키 방식

신뢰센터는 시스템 설정을 위하여 RSA의 키 (e, d)를 생성하고, 승산군 Z/nZ^*내에서 최대 위수를 갖는 g를 생성한다 (단, $n = p \cdot q$). 센터는 (n, e, g)를 공개하고 (p, q, d)를 비밀로 한다. 가입자 등록과정에서 가입자는 자신의 비밀키 s(150비트 이상)를 선택하고 $v = g^{-s} \pmod n$를 계산하여 v를 센터에 제시하고, 영지식 대화형 증명프로토콜을 이용하여 s를 알고 있다는 것을 센터에게 증명한다 [13, 14, 15]. 가입자의 신원을 확인한 후, 센터는 자체인증 공개키

$$w = (v - I)^d \pmod n$$

를 계산하여 사용자에게 전달한다.

위 프로토콜의 특징은 검증할 인증서가 없으며 공개키 자신이 인증서 역할을 한다. 즉 자체인증(self-certified)이다. 어떠한 제3자도 가입자의 공개키 w에서 가입자의 비밀키를 추론 할 수 없으며, n의 소인수를 알고 있는 센터라도 그 소인수들이 충분히 크면, 이산

대수 s를 계산할 수 없다[2]. 물론 센터는 아직도 s를 s′로 변경하여 거짓 공개키 w′를 계산할 수 있다. 그러나, 센터만이

$$w^e + I = g^s \pmod n$$

를 만족하는 공개키를 생성할 수 있으므로 동일가입자에 대하여 2개 이상의 다른 합당한 공개키가 존재한다는 것은 센터가 부정했다는 것을 증명하는 것이다. (신뢰수준 3 만족)

[프로토콜 2.1] 자체인증 키 분배 프로토콜

순서 1-1. 가입자 A는 I_A, w_A를 B에게 전송한다.
1-2. 가입자 B는 $v_A = w_A^e + I_A \pmod n$을 계산한다.
1-3. 가입자 B는 $K_{AB} = v_A^{sA} = g^{sAsB} \pmod n$를 계산한다.

순서 2-1. 가입자 B는 I_B, w_B를 가입자 A에게 전송한다.
2-2. 가입자 A는 $v_B = w_B^e + I_B \pmod n$을 계산한다.
2-3. 가입자 A는 $K_{AB} = v_B^{sA} = g^{sAsB} \pmod n$를 계산한다

위 프로토콜은 Diffie-Hellman 방식과 밀접한 관계를 갖고 있으며, 가입자 A는 B와 키 K_{AB}를 공유했다는 것을 확신할 수 있다. 그러나 키분배에 문제가 발생했다면, 자체인증 공개키에 기반한 키분배 방식에서는 이것이 키분배 방식의 문제인지, 공개키 자체의 문제인지 구별해 낼 수 없다.

3. 제안하는 자체인증 개인식별 프로토콜

신뢰수준이 3인 새로운 자체인증 개인식별 프로토콜을 제안한다. 신뢰센터는 다음과 같이 시스템을 설정한다.

[신뢰센터의 시스템 구성]

공개정보(N, M, ζ), 비밀정보(p, q, p′, q′)

① 소수 p, q를 선택하고 N=pq 계산(단, $2^{256} \le pq$)
② 소수 p′, q′를 선택하고 M=p′q′ 계산(p′/(p-1), q′/(q-1), $2^{256} \le p'q'$)
③ ord(g)=M인 $g \in Z_N$을 선택
④ security parameter ζ ($1 \le \zeta \le M$)

[가입자의 등록]

① 사용자는 자신의 ID를 센터에 제출한다.
② 사용자는 $s \in_R Z_N$를 선택하고, $v = g^s \pmod N$을 계산한다.
③ 사용자는 v를 센터에 제출하고, 그가 s를 안다는 것을 증명한다.
④ 센터는 $ID^{-1} = g^s P^2 \pmod N$을 만족하는 P를 계산한다.
⑤ 센터는 사용자에게 (ID, s, P)를 전송한다.

센터는 N=pq를 알기 때문에 $ID^{-1} = g^s P^2 \pmod N$, $P = (ID^{-1} g^{-s})^{1/2}$인 P를 쉽게 계산할 수 있다.

[개인식별 프로토콜]

아래 프로토콜의 특징은 검증할 certification이 없으며 공개키 자신이 certificate 역할을 하므로 self-certificated이다. 또한, 어떠한 가입자도 가입자 A의 공개키에서 가입자 A의 비밀키를 추론할 수 없으며 N의 소인수를 알고 있는 센터라도 그 소인수들이 충분히 크면 $g^x \pmod N$에서 x를 계산할 수 없다.

물론 센터는 아직도 x를 x′로 변경하여 거짓 공개키 P′를 계산할 수 있으나, 센터만이 $P^2 \cdot ID = g^s \pmod N$을 만족하는 공개키를 생성할 수 있으므로 동일 가입자에 대하여 2개 이상의 다른 합당한 공개키가 존재한다는 것은 그것 자체가 센터의 부정을 증명하는 것이다. 그러므로 위 프로토콜은 신뢰수준 3이다.

사용자 A		사용자 B
	ID_A, P_A ------>	
		$v = P_A^2 \cdot ID_A \pmod N$
<t번 반복> $r \in_R Z_M$ $t = g^r \pmod N$		
	t ------>	
		$e \in_R (0, \cdots, \zeta - 1)$
	e <-------	
$y = r + s_A \cdot e \pmod M$		
	y ------>	
		$t \doteq g^y \cdot v^e$

(그림 1) 제안하는 자체인증 개인식별 프로토콜

4. 제안하는 검증 가능한 자체인증 키분배 프로토콜

인증서에 기반한 방식에서는, 인증서 w를 알게 된후에 곧바로 공개키 P를 검증(explicit verifia-bility)할 수 있는 반면, 자체인증 공개키 방식에서는 암호화나 서명

검증 또는 키교환 등에 키가 사용될 때에 검증된다 (implicit verifiability). 따라서 자체인증 공개키를 이용하는 디지틀 서명이 실패할 경우, 서명의 잘못 여부를 알 수 없을 뿐만 아니라 공개키가 잘못 되었는지의 여부에 대해서도 알지 못하게 된다. 검증 가능한 자체인증 공개키 방식은 다음의 두 가지 조건을 만족한다[5].

(1) **자체인증성 (self-certification)** : 인증서는 공개키와 같다. 사용자의 ID나 비밀키/공개키 등은 어떠한 암호 프로토콜에서도 사용 중에 묵시적으로 검증되는, 계산적으로 위조 불가능한 관계를 만족한다.

(2) **검증가능성 (verifiability)** : 필요할 경우, 인증서를 알고난 후 공개키를 곧바로 검증할 수 있는 효율적인 방법이 존재한다.

4.1 수학적 배경

이차 잉여류 문제의 확장으로 gcd(z, n)=1인 정수 z에 대하여, 법 n에 관한 고차 합동식 $w^{\gamma}=z \pmod n$ ($\gamma>2$)가 해를 가질 때 z를 법 n에 관한 γ^{th}-잉여류 (γ^{th}-residue)라 하고 이 합동식이 해를 가지지 않을 때 z를 법 n에 관한 γ^{th}-비잉여류 (γ^{th}-nonresidue)라고 한다.

[정의 4.1] 양의 정수 γ, n이 주어질 때 정수 z가 다음의 조건을 만족하면, z를 법 n에 관하여 γ^{th}-잉여류라 한다. (조건) gcd(z, n)=1이고 $z= x^{\gamma} \pmod n$를 만족하는 x가 존재한다. 위의 조건을 만족하지 않는 z는 법n에 관하여 γ^{th} -비잉여류라 한다.

고차 잉여류 문제 (γ^{th}-Residuosity Problem : 약어로 γ^{th}-RP)란 주어진 gcd(z, n)=1인 양의 정수 $z \in Z_n^*$가 γ^{th}-잉여류인지 γ^{th}-비잉여류인지를 결정하는 문제이다. 고차 잉여류 문제의 계산복잡도는 γ가 다항식 크기(polynomial size)일 때는 n의 소인수분해 문제와 동치이고 γ가 지수적 크기(exponential size)일 때는 n의 소인수분해 문제보다 어렵다고 간주하고 있다.

다음은 γ가 임의의 작은 홀수(다항식 크기로 소수의 여부에 상관없음)일 경우에 Zheng, Matsumoto, Imai 등이 γ^{th}-잉여류 문제에 안전성 기반을 둔 확률론적 암호알고리즘(probabilistic encryption)을 제안하기 위하여 사용한 기본적인 정의 및 정리들이다.

[정의 4.2] (n, γ, y)가 아래의 세 가지 조건을 만족할 때 acceptable triple이라 한다.

(1) n이 서로 다른 홀수인 소수들의 곱으로 되어 있다. $n=n_1 \cdot n_2 \cdot \ldots \cdot n_t$.

(2) γ는 2보다 큰 홀수인 정수이며, $1 \le l \le t$ 인 하나의 l에 대해 $\gcd(\varphi(n_l), \gamma)=\gamma$ 이고, 나머지 $i(\neq l)$에 대해 $\gcd(\varphi(n_i), \gamma)=1$ 이다.

(3) $y = h_1^{b_1\gamma+e}\prod h_j^{b_j} \pmod n$, 여기서 모든 $i \neq l$, $1 \le j \le t$에 대해 $0 < e < \gamma$, $\gcd(e, \gamma)=1$, $1 \le b_j \le \varphi(n_j)$ 이고, $<h_1, h_2, \ldots, h_t>$는 Z_n^*의 생성 벡터(generator-vector)이다.

γ^{th} -잉여류 문제와 관련하여 completeness를 위해 다음 정리가 성립해야 한다.

[정리 4.3] Acceptable triple (n, γ, y)과 임의의 $z \in Z_n^*$가 주어졌을 때, $z=y^i u^r \pmod n$를 만족하는 유일한 i가 존재한다.

[정리 4.3]의 i를 z의 잉여류 지수 (class-index : acceptable triple (n, γ, y)에 관한)로 정의한다.

4.2 검증 가능한 자체인증 키분배 프로토콜

[Set-up 단계]

n을 다음의 형태를 갖는 두 소수 p와 q의 곱이라 하자. 즉, $n=p \cdot q$, $p= 2\gamma^d fp' +1$ 이고 $q=2fq' +1$, 여기서 f, p', q'는 서로 다른 소수이고 $\gcd(\gamma, q')=1$, $\gcd(\gamma, f)=1$ 이다. y는 법 n상에서 $(\gamma^d)^{th}$-비잉여류이고 (n, γ^d, y)는 acceptable triple이다. 또한 법 p상에서 b의 지수(order)와 법 q상에서 b의 지수는 f이다. 그러므로 법 n상에서 b의 지수는 f이다.

신뢰센터의 공개키는 (n, γ^d, y, b, f)이고 비밀키는 (p', q')이다.

[키 생성 단계]

사용자 A의 신분이 신뢰센터 TA에 의해서 확인되

면, 사용자 A는 신뢰센터로부터 인증서 w_A를 받는다. 인증서 w_A는 다음과 같이 생성된다.

① 사용자 A는 임의의 정수 $s_A(0 < s_A < f)$를 그의 비밀키로 선택하고 공개키를 다음과 같이 계산한 후, 신뢰센터를 방문하여 v_A를 준다.

$$v_A = b^{s_A} \pmod n$$

② 사용자 A의 신분을 확인한 후, 신뢰센터는 다음을 계산한 후, (i_A, x_A)를 사용자 A에게 전송 한다.

$$h(ID_A \| h(b^{sA})) = b^{-s_A} y^{-i_A} x_A^{-r^d} \pmod n$$

③ 사용자 A의 검증 가능한 자체인증 공개키는 (i_A, s_A)와 $e_A = h(b^{sA})$ 이다.

사용자 A		신 뢰 센 터
$s_A \in_R [0, f-1]$ $v_A = b^{s_A} \pmod n$		
	v_A --------->	
		$(i_A, x_A) : h(ID_A \| h(b^{sA}))$ $= b^{-s_A} y^{-i_A} x_A^{-r^d} \pmod n$
$e_A = h(b^{sA})$	(i_A, x_A) <---------	

(그림 2) 검증 가능한 자체인증 공개키 생성 단계

[키 분배 단계]

사용자 A		사용자 B
	(i_A, x_A, e_A) --------->	
	(i_B, x_B, e_B) <---------	
<t번 반복> $r \in_R Z_f$ $t = g^r \pmod N$		
	t --------->	
		$c \in_R (0, \cdots, g-1)$
	c <---------	
$y = r + s_A \cdot c \pmod f$		
	y --------->	
		$v = h(ID_A \| h(b^{sA})) \cdot y^{iA} \cdot x_A^{rd}$ $t \doteq b^y v^c \pmod N$
$K_{AB} = [h(ID_B \| e_B) \cdot y^{ie} \cdot x_B^{r^d}]^{sA}$		$K_{AB} = [h(ID_A \| e_A) \cdot y^{iA} \cdot x_A^{r^d}]^{sB}$

(그림 3) 키분배 프로토콜

사용자 A는 (i_A, x_A, e_A)를 갖고, 사용자 B는 (i_B, x_B, e_B)를 갖는다. 양측은 검증 가능한 자체인증 키를 상호 교환함에 의해 세션키 K_{AB}를 생성할 수 있다.

$$K_{AB} = b^{-s_A s_B} = [h(ID_{A(B)} \| e_{A(B)}) \cdot y^{i_{A(B)}} \cdot x_{A(B)}^{r^d}]^{sB(A)} \pmod n$$

만약 위의 키 분배 프로토콜이 실패할 경우, 각 사용자는 다음을 계산함으로써 공개키의 정당성을 확인할 수 있다.

$$\widetilde{b^{s_{A(B)}}} = [h(ID_{A(B)} \| e_{A(B)}) \cdot y^{i_{A(B)}} \cdot x_{A(B)}^{r^d}]^{-1} \pmod n,$$

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

5. 결 론

Girault의 자체인증 공개키 방식은 개인식별정보에 기반한 방식이 갖는 문제점을 해결할 수 있고, 또한 메모리와 계산량을 감소시킨다는 장점이 있으나, 암호화나 서명 검증 또는 키 교환 등에 키가 사용될 때에만 키가 검증된다는 단점이 있다. 본 논문에서는 Girault의 자체인증 공개키방식의 장점을 가지면서도, 필요한 경우에 공개키를 곧바로 검증할 수 있게 함으로써 인증서 방식의 장점까지도 결합한 검증 가능한 자체인증 키분배 프로토콜을 제안한다. 제안한 방식의 안전성은 고차잉여류 문제와 이산대수 문제에 기반을 두고 있다.

참 고 문 헌

[1] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, Vol.22, pp.644-654, 1976.

[2] M. Girault, "Self-certified public keys," Advances in Cryptology (Proc. of EuroCrypt'91), Lecture Notes in Computer Science, Vol.547, Springer, pp.490- 497, 1991.

[3] S. Saeednia, "Identity-Based and Self-Certified Key-Exchange Protocols," Information Security and Privacy (Proc. of ACISP), Lecture Notes in Computer Science, Vol.435, Springer, pp.239-252.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes," Advances in Cryptology (Proc.

of Crypto'84), Lecture Notes in Computer Science, Vol.196, Springer, pp.47-53, 1985.

[5] Seungjoo Kim, Soo-Hyun Oh, Sangjoon Park and Dongho Won, "Verifiable Self-Certified Public Keys," Proc. of WCC '99, INRIA Workshp on Coding and Cryptograpy, pp.139-148 ; Proceedings published by INRIA, France ISBN 2-7261-1136-X, 1999.

[6] H. Petersen and P. orster, "Self-certified keys-concepts and applications," Proc.3. Conf. on Communications and Multimedia Security, Chapman & Hall, September, 22~23, 1997.

[7] S. Goldwasser, S. Micali, and C. Rackoff. "The Knowledge Complexity of Interactive Proof Systems," SIAM J. Comput., 18, pp.186-208, 1989.

[8] T. Beth, "Efficient Zero-knowlledge Identification Scheme for Smart Cards," EuroCrypt'88, Lecture Notes in Computer Science, Vol.330(198), Springe, Berlin, pp.77-86.

[9] L. C. Guillou, J. J. Quisquater "A Practical Zero-Knowledge Protocol Fitted to security Microprocessor Minimizing both transmission and memory," Proc. of EuroCrypt'88, pp.123-128.

[10] C. P. Schnorr. "Efficient Identification and Signatures for Smart Cards," EuroCrypt'89. pp.686-689.

[11] C. P. Schnorr. "Efficient Identification and Signatures for Smart Cards," J. of Cryptology. Vol.4. No.3. pp.161-174, 1991.

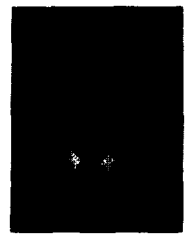
[12] Y. Zheng, "Residuosity Problem and its Applications to Cryptography," Trans. IEICE, Vol.E71, No.8. pp.759-767, 1988.

[13] 권창영, 양형규, 원동호, "영지식 대화형 증명방식 및 응용에 관한 연구", 한국통신정보보호학회 학회지, 제2권, 제2호, pp.31-39, 1992.

[14] 권창영, 이인숙, 원동호, "영지식 대화형 증명방식 및 응용 프로토콜", 대한전자공학회 학회지, 제20권, 제2호, pp.101-114, 1993.

[15] 이윤호, 양형규, 권창영, 원동호, "ID 기반의 영지식 대화형 프로토콜을 이용한 개인식별 및 키분배 프로토콜에 관한 연구", 한국통신정보보호학회 논문지, 제2권, pp.3-15, 1992.

[16] P. Horster, H. Knobloch, "Discrete Logarithm Based Protocols," EuroCrypt'91, pp.399-408, 1991.



김 경 국

e-mail : kkkim@dosan.skku.ac.kr

1983년 성균관대학교 수학과(학사)

1990년 연세대학교 교육대학원 수학과(이학석사)

1997~현재 성균관대학교 전기 전자 및 컴퓨터 공학부(박사과정)

관심분야 : 암호이론, 부호이론

유 준 석

e-mail : jsyu@dosan.skku.ac.kr

1999년 성균관대학교 정보공학과(학사)

1999년~현재 성균관대학교 대학원 전기 전자 및 컴퓨터 공학부(석사과정)

관심분야 : 암호이론

원 동 호

e-mail : dhwon@dosan.skku.ac.kr

1976년 성균관대학교 전자공학과(학사)

1978년 성균관대학교 대학원 전자공학과(석사)

1988년 성균관대학교 대학원 전자공학과(박사)

1978년~1980년 한국전자통신연구소 전임 연구원

1985년~1986년 일본 동경공대 객원 연구원

1992년~1994년 성균관대학교 전산소장

1995년~1997년 성균관대학교 교학처장

1996년~1998년 국가정보화 추진위원회 자문위원

1990년~1999년 한국통신정보보호학회 이사

1998년~1999년 성균관대학교 정보통신기술연구소장

1982년~현재 성균관대학교 전기 전자 및 컴퓨터 공학부 교수

1999년~현재 성균관대학교 전기 전자 및 컴퓨터 공학부장 (겸)정보통신대학원장

한국통신정보보호학회 부회장

관심분야 : 암호이론, 부호이론