論 文

컴퓨터 통신 NETWORK를 위한 공개키 암호 시스템에 관한 연구

正會員 丘 冀 俊* 正會員 李 榮 魯** 正會員 沈 壽 輔*

A Study on Public Key Cryptosystem for Computer Communication Networks

Gi Jun KU* Young No LEE** Soo Bo SIM* *Regular Members*

要 約

본 논문에서는 컴퓨터 통신 네트워크의 보안성을 위한 공개키 암호시스템을 제안하였다.

이러한 공개키 암호시스템은 인수분해의 어려움에 바탕을 두었다. 제안된 공개키 암호에서, 공개키 생성 앨고리듬은 두개의 다항식 f(x,y,z)와 h(x,y,z)를 선택한다. 암호화는 처음에 평문 다항식 M(x,y,z)을 선택하고, 공개키 다항식과 난수를 곱하므로써 암호문이 생성되도록 하였다. 제안된 공개키 암호시스템의 보안성이 디지탈 시뮬레이션을 통하여 입증되었다.

ABSTRACT

In this paper, a public key cryptosystem for security in computer communication networks is proposed.

This is based on the security to a difficulty of factorization. For the proposed public key cryptosystem, the public key generation algorithm selects two polynomials f(x,y,z) and h(x,y,z). The enciphering first selects plaintext polynomial M(x,y,z) and multiplies the public key polynomials and the random integers, then the ciphertext is computed. The security of proposed public key knapsack cryptosystem is verified with digital simulation.

I. 서 론

컴퓨터 네트워크는 컴퓨터 기술과 통신기술의 집합체로 오늘날 고도의 정보화 사회에서 요구되는 각종 서비스를 제공해 주고 있다.

통신 매체를 통한 정보 교환 및 자원 공유와 관련하여 정보의 양적 증가와 부대 가치의 증가라는 측면에서 정보를 생성 가공하여 사용자의 위치까지 전파하는 기술은 이제 괄목할 만한 발전을 이루었다.

데이타 통신 환경에서 두 통신 시스템간에 교환되는 정보를 보호하기 위하여 적절한 보안성 제어가 확립되어야 하는 경우가 급격히 증가하고 있다. 국내외적으로 정보 산업 사회의 발전과 정확성이 요구됨에 따라 다양한 정보 통신 네트워크와 이를 바탕으로 분산 처리 시스템이 양적으로 급성장하고 있다. 그러나 고도의 정보 통신 기술의 발전은 이와같은 긍정적인 측면외에 정보의 내용 변경, 정보의 불법적인 유출,

*崇實大學校 電子工學科
Dept. of Electronics Eng. Soong Sil Univ.
**서울産業大學 電子工學科
Dept. of Electronics Engineering Seoul National Polytechnic University
論文番號 : 92-22(接受1991. 10. 2)

순서 변경 그리고 미확인 발신자 및 수신자 등에 의하여 항상 위협을 받음으로써 정보의 보안성이 요구되고 있는 실정이다. 컴퓨터 통신 네트워크의 하부구조가 잘 정립이 되어 있더라도 여러 계층에서 각 사용자의 요구사항을 만족시킬 수 있는 통신 보안성이 보장되지 않으면 컴퓨터 통신 네트워크가 제공하는 서비스를 받는 데 큰 위험성이 뒤따르게 된다.

암호화 기법(cryptographic)은 메세지를 받도록된 사람에게만 그 메세지를 이해하도록 하고, 그외 다른 사람들이 그 메세지를 이해하지 못하도록 하기 위해 메세지를 변형시키는 기술이다.[1] 이러한 암호화 기법은 평문(plaintext), 키(key), 앨고리듬(algorithm), 암호문(ciphertext)으로 구성되어 있으며, 평문은 암호화 되지 않은 원래의 데이타이고, 암호문은 암호화 앨고리듬에 의해 변형된 데이타이며, 키는 앨고리듬에 사용되는 변수이다. 평문이 암호문이 되는 과정을 암호화 과정(enciphering)이라 하고, 이와 반대로 암호문을 원래의 평문으로 만드는 과정을 해독과정(deciphering)이라 한다.

데이타가 통신 선로를 경유하여 이동할 때 다른 이용자들이 도청하여 해독하기 어렵게 하는 데이타의 여러가지 암호화 기법은 크게 전통적인 암호시스템(conventional cryptosystem)과 공개키 암호시스템(public key cryptosystem)으로 나눌 수 있다.[2,3] 공개키 암호의 대표적인 것은 RSA[4] 암호는 큰 합성수의 소인수 분해의 어려움에 보안성의 근거를 가지고 있으며, Elgamal[5]은 이산적 대수 문제의 어려움에 대한 보안성을 가지고 있다.

본 논문에서는 3변수 다항식 $f(x,y,z)=0 \bmod n$의 인수 분해의 어려움에 바탕을 두어 보안성 있는 공개키 암호시스템을 제안한다. $(3,n-1)=1$을 만족하는 소수 n을 정하여 평문 다항식을 3승하고, 그것에 2개의 공개키 다항식에 각각 임의의 정수를 곱하여 더한 것을 암호문으로 한다. 법의 값을 $n=pq$로 하면 RSA암호의 보안성에 소인수 분해의 어려움을 더해서, 다항식의 인수 분해의 어려움이 첨가되어 더욱 효과적인 보안성을 가진 공개키 암호시스템 기법이 된다.

Ⅱ. 키 분배와 공개키 암호

Ⅱ.1. 전통적인 암호시스템

전통적인 암호시스템은 그림 1과 같이 단일키 암호화 방식으로 통신하고자 하는 사용자 사이에 연결된 회선상으로 정보를 전송하는 과정에서 정보의 보안성을 위하여, 송수신자가 공통적으로 갖고 있는 단일키로 암호화하고 해독하는 시스템이다. 여기서 K는 비밀키, M은 암호화 되지 않은 평문, C는 암호화된 암호문, $\bar{M}$은 감청자(eavesdropper)가 얻은 평문이다.

전통적인 암호화 기법은 평문의 글자를 다른 체계를 갖는 글자로 바꾸어 암호화 하는 대치법(substitution), 평문의 각 글자들의 위치를 바꾸어 놓는 방법으로서 평문에 사용된 글자를 모두 그대로 사용하고, 단지 그 위치만이 달라져 본래의 뜻을 알아 볼 수 없게 만드는 전환법(transposition), 컴퓨터와 관련하여 방정식을 이용하여 수학적 처리를 한 후 다시 글자로 바꾸거나, 평문의 글자를 2진화 10진수(BCD ; Binary Coded Decimal)로 표시한 후 논리 연산을 실행하여 암호화 하는 대수적인 방법, 또한 대치법과 전환법을 조화시켜 암호화 하는 합성법등이 있다.

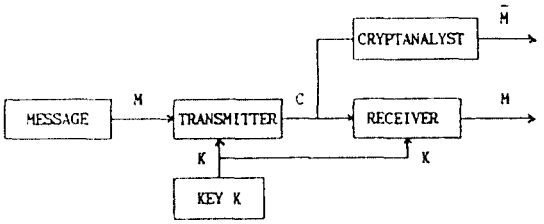


그림 1. 전통적인 암호시스템
Fig. 1. Conventional cryptosystem.

Ⅱ.2. 공개키 암호시스템

전통적인 암호시스템에서는 송신자와 수신자가 동시에 동일한 키를 가져야 하므로 어느 한쪽에서 반드시 상대방에게 약속된 키를 보내야 하는데 이 과정에서 키가 노출될 수도 있다는 것이 전통적인 암호시스템의 가장 큰 단점이다.[7] 이러한 단점은 1976년에 최초로 Diffie와 Hellman[8]에 의해 제안된 공개키 암호시스템의 개념으로서 해결될 수 있게 되었다. 이러한 공개키의 제안에 뒤이어 1978년 Rivest, Shamir, Adleman[4]에 의해 지수승 암호인 RSA법이 제안되었고, Merkle, Hellman[6], Chor[9]등에 의해 배낭 문제(Knapsack problem)를 사용한 MH법 등이 제안되었다.

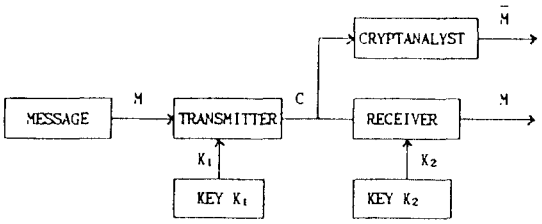


그림 2. 공개키 암호시스템
Fig. 2. Public key cryptosystem.

공개키 암호시스템은 그림 2와 같이 암호키 K_1과 해독키 K_2가 다르며, 암호키에서 해독키를 만들어 낼 수 없다는 것이다. 이 방식에서 송신자가 사용하는 암호키 만을 공개하고 수신자는 해독키만을 관리함으로써 감청자가 암호키를 얻더라도 원래의 평문을 구하기가 어렵다.

그리고 전통적인 암호시스템에서 정보 통신을 하는 사람의 n이라 하면 이용해야 하는 키의 갯수는 $n(n-1)/2$, 즉 키의 갯수는 n^2에 비례하나 공개키 암호시스템에서는 일방 통행 함수(one-way function)을 이용하여 키의 갯수는 n에 비례한다.[10]

다음절에서는 매우 큰 소수(prime number)를 인수 분해하여, 원래의 인수를 찾는데 어려움을 이용한 RSA 암호 알고리듬에 대하여 살펴본다.

RSA 암호 알고리듬은 MIT의 Rivest, Shamir, Adleman에 의해 제안된 것으로, 두개의 큰 소수인 곱을 구하는 것은 간단하지만 그 곱을 소인수 분해하여 소수를 구하는 것은 계산상으로 불가능하다는 사실을 이용하였다.

먼저, 사용자는 큰 소수 p와 q를 선택하고

$$n=pq \tag{1}$$

를 구한다. 다음에 공개키로 사용할 큰 수 E를 선정하는데 Euler 함수 V(n)가 E의 최대 공약수가 1이 되어야 한다. 그리고 E는 "man(p,q)+1"과 "(n-1)" 사이의 수이어야 한다. 즉

$$V(n)=(p-1)(q-1) \tag{2}$$

$$GCD(V(n), E)=1 \tag{3}$$

여기서 $(V(n), E)=1$을 구하고 나면 D는 다음 식을 만족하면 된다.

$$DE=1 \bmod V(n) \tag{4}$$

또한, 암호문을 해독하여 평문을 구하는데 사용되도록 암호키 (E,n)을 공개한다.

평문의 문자들을 0과 n-1사이의 정수(즉, A=01, B=02, C=03, ..., Z=26)로 대응시켜 나타낸다. 평문에 대치된 수들을 다음식에 의해 암호문의 수로 변형한다.

$$C=M^E \bmod n \tag{5}$$

그러므로 해독키 (D,n)를 사용하여 암호문의 수로부터 다음식에 의해 평문이 구해진다.

$$M=C^D \bmod n \tag{6}$$

Ⅲ. 데이타 보안성을 위한 공개키 암호

소인수 분해의 어려움에 기초를 둔 RSA 방법의 보안성에, 공개키 다항식에 2개의 3변수 다항식을 사용하여, 이 다항식을 동시에 만족하는 수을 구하는 어려움의 보안성을 더함으로써 RSA 방법보다 더 보안성 있는 공개키 암호 알고리듬을 제안한다.

Ⅲ.1. 키 생성

$(3, n-1)=1$을 만족하는 소수 n으로써 3개의 변수를 x, y, z로 나타낸다. 단, $0<x_i, y_i, z_i<n(i=1,2,3)$인 정수 x_i, y_i, z_i를 적당하게 정하고,

$$z_i z_i^{-1}=1 \bmod n \tag{7}$$

을 만족하는 승법 역원(multiplicative inverse element) z_i^{-1}을 구한다. 또한 $0<a_j, b_j<n(j=1,2,\ldots,6)$인 정수 a_j, b_j를 적당하게 선택하고,

$$r_i=-(a_i x_i+b_i y_i)z_i^{-1} \bmod n$$
$$r_{i+3}=-(a_{i+3}x_i+b_{i+3}y_i)z_i^{-1} \bmod n \ (i=1,2,3) \tag{8}$$

에서 r_i, r_{i+3}을 구한다. 다음에 2개의 독립된 다항식

$$f(x,y,z)=\prod_{i=1}^{3}(a_i x+b_i y+r_i z) \bmod n$$

$$=f_1x^3+f_2y^3+f_3z^3+f_4x^2y+f_5x^2z+f_6xy^2+f_7y^2z+f_8xz^2+f_9yz^2+f_{10}xyz \quad (9)$$

$$h(x,y,z)=\prod_{i=4}^{6}(a_ix+b_iy+r_iz) \bmod n$$
$$=n_1x^3+h_2y^3+h_3z^3+h_4x^2y+h_5x^2z+h_6xy^2+h_7y^2z+h_8xz^2+h_9yz^2+h_{10}xyz \quad (10)$$

을 계산하여 공개한다.

해독키는 x_i, y_i, z_i(i=1,2,3)과

$$3d=1 \bmod n-1 \quad (11)$$

을 만족하는 d와

$$(T_1T_2-T_3T_4)(T_1T_2-T_3T_4)^{-1}=1 \bmod p \quad (12)$$

여기서, $T_1=x_1z_2-x_2z_1$, $T_2=y_1z_3-y_3z_1$, $T_3=x_1z_3-x_3z_1$, $T_4=y_1z_2-y_2z_1$을 만족하는 승법 역원 $(T_1T_2-T_3T_4)^{-1}$와 또한

$$T_4T_4^{-1}=1 \bmod n \quad (13)$$

을 만족하는 승법 역원 T_4^{-1}이다.

Ⅲ.2. 암호화 과정

3개의 평문 M_i의 범위를 $0\le M_i<n$(i=1,2,3)로, 평문 다항식을

$$M(x,y,z)=M_1x+M_2y+M_3z \quad (14)$$

로 나타낸다. 암호화는 $0<a, b<n$인 2개의 임의의 수 a,b를 사용하여

$$C(x,y,z)=M(x,y,z)^3+af(x,y,z)+bh(x,y,z) \bmod n$$
$$=(M_1x+M_2y+M_3z)^3+a(f_1x^3+f_2y^3+f_3z^3+f_4x^2y+f_5x^2z+f_6xy^2+f_7y^2z+f_8xz^2+f_9yz^2+f_{10}xyz)+b(h_1x^3+h_2y^3+h_3z^3+h_4x^2y+h_5x^2z+h_6xy^2+h_7y^2z+h_8xz^2+h_9yz^2+h_{10}xyz)$$
$$=c_1x^3+c_2y^3+c_3z^3+c_4x^2y+c_5x^2z+c_6xy^2+c_7y^2z+c_8xz^2+c_9yz^2+c_{10}xyz \quad (15)$$

여기서,

$c_1=M_1^3+af_1+bh_1 \bmod n$
$c_2=M_1^3+af_2+bh_2 \bmod n$
$c_3=M_1^3+af_3+bh_3 \bmod n$
$c_4=3M_1^2M_2+af_4+bh_4 \bmod n$
$c_5=3M_1^2M_3+af_5+bh_5 \bmod n$
$c_6=3M_1M_2^2+af_6+bh_6 \bmod n$
$c_7=3M_2^2M_3+af_7+bh_7 \bmod n$
$c_8=3M_1M_3^2+af_8+bh_8 \bmod n$
$c_9=3M_2M_3^2+af_9+bh_9 \bmod n$
$c_{10}=6M_1M_2M_3+af_{10}+bh_{10} \bmod n$

이며, c_j(j=1,...,10)을 수신자에게 보내준다.

Ⅲ.3. 해독 과정

$f(x,y,z)=h(x,y,z)=0 \bmod n$의 근 x_i, y_i, z_i(i=1,2,3)을 사용하여

$$D_i(C)=C(x,y,z)\{x=x_i,\ y=y_i,\ z=z_i \bmod n \quad (i=1,2,3) \quad (16)$$

을 구하기 위해 다음에 해독키 d를 사용하고,

$$\{D_i(C)\}^d \bmod n=M_1x_i+M_2y_i+M_3z_i \ (i=1,2,3) \quad (17)$$

을 계산하여, 승법 역원 $(T_1T_2-T_3T_4)^{-1}$와 T_4^{-1}을 사용하면 3개의 평문이

$$M_1=[\{D_1(C)^dz_2-D_2(C)^dz_1\}T_2-\{D_1(C)^dz_3-D_3(C)^dz_1\}T_1(T_1T_2-T_3T_4)^{-1} \bmod n \quad (18)$$

$$M_2=[D_1(C)^dz_2-D_2(C)^dz_1-T_4M_1]T_1^{-1} \bmod n \quad (19)$$

$$M_3=[D_1(C)^d-M_1x_1-M_2y_1]z_1^{-1} \bmod n \quad (20)$$

로 구해진다. 제안된 공개키 암호 앨고리듬은 그림 3과 같다.

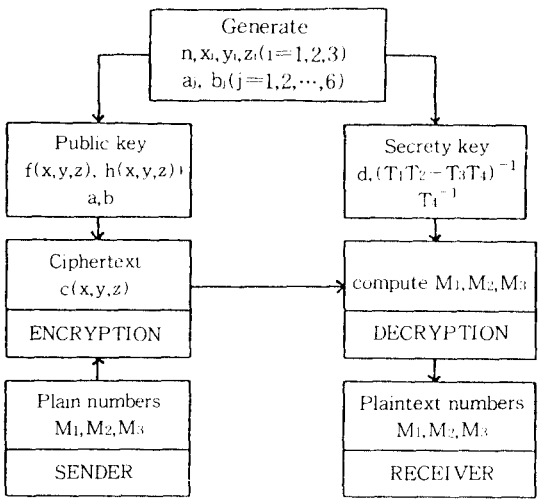


그림 3. 제안된 공개키 암호 알고리듬
Fig. 3. Proposed public key cryptosystem algorithm.

Ⅳ. 시뮬레이션

제안된 공개키 암호 알고리듬의 타당성을 입증하기 위해 주어진 평문에 대해 시뮬레이션 한다.

$n=29$와 $x_1=10$, $y_1=17$, $z_1=22$, $x_2=18$, $y_2=8$, $z_2=23$, $x_3=25$, $y_3=5$, $z_3=14$로 정하면, 승법 역원 $z_1^{-1}=4$, $z_2^{-1}=24$, $z_3^{-1}=27$로 구해진다. 또한 임의의 정수 $a_i=i$, $b_i=i+1$ $(i=1,2,\ldots,6)$으로 하면, $r_1=27$, $r_2=10$, $r_3=16$, $r_4=22$, $r_5=23$, $r_6=22$로 구해지고, 이에 따라 공개키 다항식은

$$f(x,y,z)=6x^3+24y^3+28z^3+0x^2y+21x^2z+17xy^2+7y^2z+7xz^2+28yz^2+4xyz$$

$$h(x,y,z)=4x^3+7y^3+25z^3+28x^2y+28x^2z+xy^2+11y^2z+27xz^2+15yz^2+xyz$$

로 얻어진다. 또 해독키는 $d=19$, $(T_1T_2-T_3T_4)^{-1}=28$, $T_4^{-1}=17$로 구해진다.

평문의 문자들을 " "=00, A=01, B=02, C=03, ..., Z=26으로 대응시키고, 3개의 평문이 $M_1=11$, $M_2=16$, $M_3=23$일때 임의의 정수를 $a=6$, $b=25$로 선택하면, 암호문은 (15)식에 의해 구하면 표 1과 같다. 이 $c_j(j=1,\ldots,10)$의 값을 수신자에게 보낸다.

또한 수신된 $c_j(j=1,\ldots,10)$의 값을 이용하여, (16)

표 1. 암호시스템의 데이타
Table 1. Datas of cryptosystem

※PUBLIC KEY※	
f(x,y,z) :	6 24 28 0 21 17 7 7 28 4
h(x,y,z) :	4 7 25 28 28 1 11 27 15 1
PLAINTEXT :	PUBLIC KEY FOR COMPUTER NETWORK SECURITY
BLOCK 1	: PUB
PLAINTEXT	: 16 21 2
CIPHERTEXT	: 27 10 18 8 13 9 5 10 12 21
BLOCK 2	: LIC
PLAINTEXT	: 12 9 3
CIPHERTEXT	: 8 4 8 6 5 27 2 26 3 21
BLOCK 3	: KE
PLAINTEXT	: 0 11 5
CIPHERTEXT	: 20 26 19 4 14 11 15 21 5 20
BLOCK 4	: Y F
PLAINTEXT	: 25 0 6
CIPHERTEXT	: 14 0 23 4 12 11 27 24 21 20
BLOCK 5	: OR
PLAINTEXT	: 15 18 0
CIPHERTEXT	: 2 3 10 3 14 4 27 21 21 20
BLOCK 6	: COM
PLAINTEXT	: 3 15 13
CIPHERTEXT	: 18 11 3 3 17 6 15 5 28 21
BLOCK 7	: PUT
PLAINTEXT	: 16 21 20
CIPHERTEXT	: 27 10 6 8 4 9 10 23 20 1
BLOCK 8	: ER
PLAINTEXT	: 5 18 0
CIPHERTEXT	: 0 3 10 20 14 28 27 21 21 20
BLOCK 9	: NET
PLAINTEXT	: 14 5 20
CIPHERTEXT	: 9 9 6 15 0 17 19 1 18 10
BLOCK 10	: WOR
PLAINTEXT	: 23 15 18
CIPHERTEXT	: 7 11 13 0 15 21 26 18 14 15
BLOCK 11	: K S
PLAINTEXT	: 11 0 19
CIPHERTEXT	: 17 0 25 4 9 11 27 15 21 20
BLOCK 12	: ECU
PLAINTEXT	: 5 3 21
CIPHERTEXT	: 0 27 20 26 23 1 14 24 17 25
BLOCK 13	: RIT
PLAINTEXT	: 18 9 20
CIPHERTEXT	: 23 4 6 23 24 6 15 16 4 1
BLOCK 14	: Y
PLAINTEXT	: 25 0 0
CIPHERTEXT	: 14 0 10 4 14 11 27 21 21 20
PLAINTEXT :	PUBLIC KEY FOR COMPUTER NETWORK SECURITY

식-(20)식으로 부터 해독된 평문은 표 1과 같다.

공개키 다항식에 2개의 3변수 다항식을 사용하여, $f(x,y,z)=h(x,y,z)=0 \bmod n$를 동시에 만족하는 근을 구하는 것의 어려움에 보안성의 근거를 갖고 있고, 암호문의 길이는 평문 길이의 약 10/3배가 되었다. 또 법의 값을 2개의 소수의 곱으로 정하면 이 암호는 소인수 분해의 어려움과 다항식 인수분해의 어려움의 양자에 보안성을 둔 암호가 된다.

V. 결 론

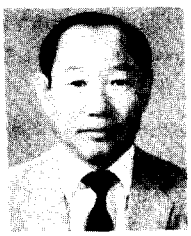
본 논문에서는 컴퓨터 네트워크의 데이타 보안성을 위한 공개키 암호 알고리듬을 제안하였다.

제안된 공개키 암호 알고리듬은 공개키 다항식에 2개의 3변수 다항식을 사용하여, $f(x,y,z)=h(x,y,z)=0 \bmod n$를 동시에 만족하는 근을 구하는 어려움에 대한 보안성의 근거를 두었다. 암호문은 평문 다항식을 3승하여, 그것에 2개의 공개키 다항식을 각각 임의의 정수를 곱하여 더한 것을 암호문으로 하였으며, 법의 값을 2개의 소수의 곱으로 정하면, 비록 암호문의 길이는 평문 길이의 약 10/3배가 되나, 이 암호는 RSA 암호의 보안성, 즉 소인수 분해의 어려움에 부가하여 다항식의 인수 분해의 어려움에도 보안성을 가진 암호로 되었다. 제안된 공개키 암호시스템의 보안성을 컴퓨터 시뮬레이션을 통하여 입증하였다.

참 고 문 헌

1. W.Diffie, M.Hellman, "Privacy and Authentication : An Introduction to Cryptography ' Proc. IEEE, Vol.67, pp.397-527, 1979.
2. M.E.Hellman, "An Overvlew of Public Key Cryptography," IEEE Communication Society Magazine, pp.24-32, 1978.
3. C.S.Kline, G.J.Popek, "Public key vs. conventional key encryption," National Computer Conference, pp.831-837, 1979.
4. R.L.Rivest, A.Shamir, L.Adleman, "A method for obtaining digital signatures and public key cryptosystem," Comm. ACM, Vol. 21, No.2, pp.120-126, 1978.
5. T.Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory, Vol. IT-31, No.4, pp.469-472, 1985.
6. R.C.Merkle, M.E.Hellman, "Hiding information and signatures in trapdoor Knapsacks," IEEE Trans. Info. Theory, Vol. IT-24, 1978.
7. C.H.Meyer, S.M.Matyas, Cryptography : A New Dimension in Computer Data security, John Wiley & Sons, 1982.
8. W.Diffie, M.E.Hellman, "New Direction in Cryptography," IEEE Trans. Inform. Theory, Vol. IT-22, Nov. 1976.
9. B.Chor, R.L.Rivest, "A Knapsack-Type Public Key Cryptosystem Based on Arithmetic in Finite Fields." IEEE Trans. Inf. Theory, Vol.34, No.5, pp.901-909, 1988.
10. D.B.Newman, Jr., et al., Public Key Management for network Security, IEEE Network Magazine, April 1987.

丘 貴 俊(Gi Jun KU) 正會員
1959年 4 月28日生
1983年 2 月：檀國大學校 工科大學 電子工學科 卒業(工學士)
1988年 8 月：漢陽大學校 大學院 電子工學科 卒業(工學碩士)
1989年 8 月～現在：崇實大學校 大學院 電子工學科 博士課程
※ 主關心分野：암호및 부호이론



沈 壽 輔(Soo Bo SIM) 正會員
1931年 5 月30日生
• 現在：崇實大學校 工科大學 電子工學科 教授
※ 主關心分野：무선통신시스템

李 榮 魯(Young No LEE) 正會員
1936年 4 月 9 日生
• 檀國大學校 電子工學科卒業(工學士)
• 建國大學校 電氣및 電子工學科 卒業(工學碩士)
• 檀國大學校 電子工學科 工學博士
• 現在：國立 서울産業大學 電子工學科 副教授
• 主關心分野：信號處理및 Computer Network