論文 95-5-5-15

데이터 보호를 위한 다변수 다항식 공개키 암호 방식

正會員 丘 冀 俊*, 沈 壽 輔**

Multivariable Polynomials Public Key Cryptosystem for Data Protection

Ki Jun Ku*, Soo Bo Sim** Regular Members

要 約

본 논문에서는 초증가 벡터의 각 요소를 다변수 다항식으로 표현하는 Knapsack 공개키 암호 방식을 제안한다. 제안된 Knapsack 공개키 암호 방식은 초증가 벡터의 각 요소를 변형하여 다변수 다항식으로 표현한 것을 암호 벡터로 구성하고, 이것과 평문 벡터와의 내적에 난수배한 공개키 다항식을 더하여 암호문으로 한다. 암호문의 복호는 공개키 다항식의 근과 비밀키의 초증가 벡터를 사용하면 평문이 구해진다. 따라서 Knapsack 공개키 암호 방식의 안전성은 공개키 다항식의 근을 다변수 다항식으로 나타내는 암호 벡터에 대입할 때 암호 벡터가 초증가 벡터로 되는 근을 구하는 것의 어려움에 근거하고 있다.

제안된 다변수 다항식을 이용한 Knapsack 공개키 암호 방식의 타당성이 컴퓨터 시뮬레이션을 통하여 입증되었다.

ABSTRACT

In this paper,the knapsack public key cryptosystem to represent each element of superincreasing vector with multivariable polynomial is proposed.Proposed knapsack public key cryptosystem composes what represented each element of superincreasing vector with multivariable polynomial after transforming it of ciphervector, and it makes the ciphertext by adding the public key polynomials multiplied by random number to the inner product of ciphervector and plaintext vector.For the deciphering of ciphertext,the plaintext is determined by using the root of public key polynomial and the superincreasing vector of secret key.Thus,the stability of knapsack public key cryptosystem is based on the difficulty of obtaining the root that ciphervector becomes the superincreasing vector, in substituting the root of public key polynomials for ciphervector to represent with the multi-

*翰林專門大學 電子通信科
**崇實大學校 情報通信工學科
論文番號：94351-1203
接受日字：1994年 12月 3日

variable polynomial.

The propriety of knapsack public key cryptosystem which used the proposed multivariable polynomials was proved through computer simulation.

1. 서 론

고도의 정보화 사회에서 컴퓨터 통신망(computer communication network)은 컴퓨터 기술과 통신 기술의 결합체로 발전하여 종합정보통신 시스템이 구축되고 있으며 사용자에게 요구되는 각종 서비스를 제공해 주고 있다. 그러나 실제 통신장치,통신 선로등으로 구성되는 통신망에서는 도청자가 통신중인 정보를 도청(eavesdropping)하여 해독함으로써 정보가 누출되거나 데이터를 변조(modification),삽입(injection) 및 삭제(deletion)등이 가능하기 때문에 이를 방지하기 위해서 컴퓨터 및 통신 시스템상에서 정보 보호를 위한 암호화 연구가 활발히 진행되고 있다.[1][2]

암호화 기법(cryptographic)은 데이터에 대한 변조 또는 정보의 누출을 방지하기 위해서 데이터를 암호화시켜 저장하거나 전송함으로써 비밀키를 알고 있는 인증(authentication)된 사람이 아니면 해독을 할 수 없도록 하는 기술로 평문(plaintext, message), 키(key), 알고리즘(algorithm),암호문(ciphertext)으로 구성되어 있다.여기서 평문은 암호화되지 않은 원래의 데이터이고,암호문은 암호화 알고리즘에 의해 변형된 데이터이며,키는 알고리즘에 사용되는 변수로서 암호화키 및 복호화키가 사용되는 암호 방식의 종류에 따라 동일할 수도 있고 그렇지 않을 수도 있다. 평문을 암호문으로 만드는 과정을 암호화 과정(encryption)이라 하고, 이와 반대로 암호문을 원래의 평문으로 만드는 과정을 복호화 과정(decryption)이라 한다.[1][2][3]

암호 방식은 암호키의 분배와 관리 방법에 따라 관용암호방식(conventional cryptosystem)과 공개키 암호방식(public key cryptosystem)으로 크게 나눌 수 있다. 전자는 암호화키와 복호화키가 동일한 방식으로 이 두 키는 송신자와 수신자가 공용하는 비밀키가 되며, 블럭암호(block cipher)에 속하는 DES(Data Encryption Standard), FEAL(Fast Data Encipherment Algorithm) 및 스트림 암호(stream cipher)등이 있다. 후자는 암호화키와 복호화키가 서로 다르며 암호화키는 공개하고 복호화키는 비밀로 보관하는 공개키(public key)와 비밀키(secret key)를 이용하여 키 전송이 필요치 않는 암호방식으로 1976년 Diffie-Hellman이 One-way함수를 이용한 공개키 개념을 도입함으로써 기존의 관용 암호 방식의 키 분배 문제를 해결하고 인증과 디지탈 서명(digital signature)이 가능한 새로운 공개키 암호 방식을 제안한 이후 연구가 현재 활발히 진행되고 있다.대표적인 공개키 암호 알고리즘에는 1978년 Rivest,Shamir와 Adieman에 의해 큰 합성수를 소인수분해하는 어려움에 근거한 RSA암호, 1978년에 Merkle와 Hellman,Chor와 Rivest등에 의해 수열의 초증가성인 knapsack문제의 어려움에 근거한 MH Knapsack 암호, 1985년에 Elgamal에 의해 유한체상의 이산적 대수(discrete logarithm)문제의 어려움에 근거한 암호 방식등이 있다.[3][4][5][6][7][8]

본 논문에서는 공개키 다항식의 근을 구하는 어려움에 근거한 다변수 다항식을 이용한 Knapsack 공개키 암호 방식을 제안한다.

제안된 Knapsack 공개키 암호 방식에서는 MH Knapsack 암호 방식의 초증가 벡터를 다변수 다항식으로 표현한 암호 벡터에 난수(random number)배한 공개키 다항식을 더하여 암호문으로 구성한다. 이 암호의 안전성은 공개키 다항식의 근을 다변수 다항식으로 나타내는 암호 벡터에 대입할 때 암호 벡터가 원래의 초증가 벡터로 되는 근을 구하는 데 어려움이 있다. 암호문의 복호는 공개키 다항식의 근과 비밀키 벡터의 초증가성을 이용하면 평문이 구해진다.

따라서 제안된 다변수 다항식을 이용한 Knapsack 공개키 암호 방식은 컴퓨터 시뮬레이션을 통하여 주어진 평문에 대해 암호화하고 복호화하여 알고리즘의 타당성을 보였다.

2. 암호 방식

2.1 관용 암호 방식[1][2]

관용 암호 방식(conventional cryptosystem)은 오래전부터 사용되어 온 일명 공통키 암호 방식 또는 비밀키 암호 방식(secret-key cryptosystem)이라 하며 그림 1과 같이 비밀 정보를 교환하고자 하는 상호 암호 통신망 가입자는 사전에 비밀 공통키 K를 제3자에게 노출되지 않게 나누어 가진 다음, 암호 통신을 필요로 할 때 평문 M을 암호 알고리즘 E와 공통키 K로 암호문 C를 생성시켜 통신 채널을 통해서 전달하고 암호문 C를 수신한 가입자는 복호화 알고리즘 D와 공통키 K로 평문 M을 얻는 방식이다.

한편 관용 암호 방식에서는 송신자와 수신자가 공통으로 비밀키를 가지고 통신을 수행하기 때문에 키를 전달해야 하며, 암호 통신망 가입자가 n명일 때 서로 교환해야 할 공통키의 수가 n(n-1)/2로 가입자의 증가에 따라 키의 수가 급격하게 증가하여 통신망을 이용한 암호 시스템 구축에 키 관리가 용이하지 않다. 따라서 제3자로 부터 비밀키를 보호하기 위한 적절한 키 분배 방식을 필요로 한다.

2.2 공개키 암호 방식[1][2][3][4][5][7]

키가 노출될 수도 있다는 관용 암호 방식의 단점은 1976년에 최초로 Diffie와 Hellman 에 의해 제안된 공개키 암호 방식의 개념으로서 해결될 수 있게 되었고, 그 이후 1976년 Rivest, Shamir와 Adlemand에 의해 지수승 암호인 RSA 암호 방식, 1978년 Merkle와 Hellman, Chor등에 의해 Knapsack 문제(knapsack problem)를 이용한 MH Knapsack 암호 방식 등이 제안되었다.

공개키 암호 방식은 암호화할 때 사용하는 키(공개키)와 복호화할 때 사용하는 키(비밀키)를 다르게 작성하여 공개키는 공개하고 비밀키만 안전하게 유지하는 방식으로서 그림 2와 같이 암호키 Ke와 해독키 Kd가 달라 암호키에서 해독키를 만들어 낼 수 없으며 송신자가 사용하는 암호키만을 공개하고 수신자는 암호키를 얻더라도 원래의 평문을 구하기가 어렵게 된다. 예를 들면 A에게 비밀 통신을 하고자 하는 사람은 누구라도 A가 공개한 A의 공개키를 가지고 송신할 내용을 암호화하여 A에게 전송하면 A는 자신만이 가지고 있는 비밀키를 이용하여 암호문을 복호화한다. 따라서 공개키 암호 방식에서는 관용 암호 방식에서 전제로 하였던 키의 안전한 분배는 필요없게 되고, 정보 통신을 하는 사람의 수가 n이라 하면 이용해야 하는 키의 갯수는 단방향 함수(one-way function)을 이용하여 n에 비례한다.

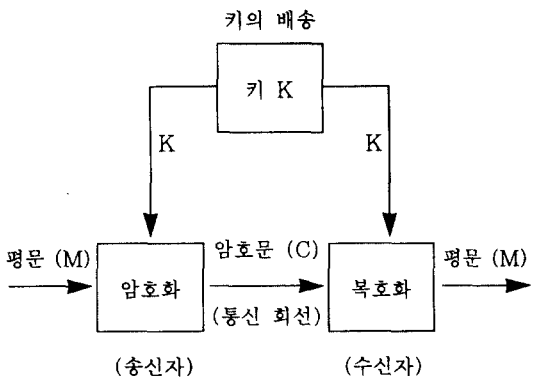

그림 1. 관용 암호 방식
Fig. 1. Conventional Cryptosystem

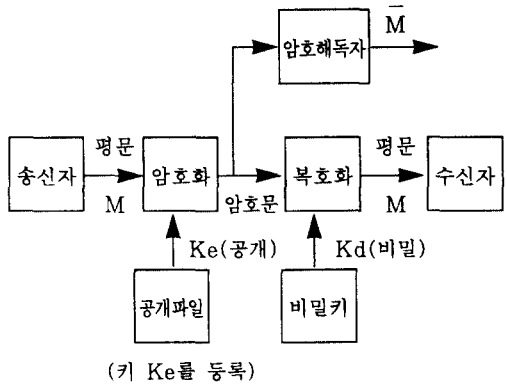

그림 2. 공개키 암호 방식
Fig. 2. Public Key Cryptosystem

2.3 Knapsack 암호 방식[1][2][5]

Knapsack 암호 방식(knapsack cryptosystem)은 1978년 Merkle 와 Hellman에 의하여 Knapsack 문제(knapsack problem)가 최초로 공개키 암호 기법에 적용되었다. Knapsack 문제는 주어진 정수의 집합 A = $(a_1, a_2, \cdots, a_n)$와 이것의 합 C가 주어졌을 때 C가 A의 부분합이 되는지 또는 A의 어떤 원소들의 합이 C가 되는지 알아내는 문제이다. 즉, $C = \Sigma a_i m_i (1 \le i \le n)$를 만족하는 2진 벡터 $M = (m_1, m_2, \cdots, m_n)$을 찾아내는 문제이다. 정수 벡터 A에서 그 부분집합의 합 C를 구하는 것은 쉽지만 그 역과정인 Knapsack 문제는 일반적으로 풀기 어려운 NP-complete 문제로 잘 알려져 있다.

이와 같이 Knapsack 문제는 일반적으로 풀기 어려운 문제이지만 모든 Knapsack 문제가 그러한 것은 아니며 특수한 구조를 갖는 많은 경우에 Knapsack 문제의 해를 구하기가 용이하다. Merkle과 Hellman은 초증가하는 정수 벡터 A를 구성하고 이것에 법(modula) 연산을 취함으로써 복잡한 Knapsack벡터로 변환하였다. 즉, Knapsack 일방향함수에 trapdoor를 부가하여 trapdoor Knapsack 공개키 암호 방식을 개발하였다.

이 MH Knapsack 암호 방식(Merkle-Hellman Knapsack Cryptosystem)의 기본 알고리즘은 다음과 같다.

2.3.1. 키 생성

Knapsack 벡터 $A = (a_1, a_2, \cdots, a_n)$에서 각 원소의 크기가 그 이전의 원소의 합보다 큰 경우에 A는 초증가(superincreasing)한다고 한다. 즉, 식(1)과 같다.

$$a_i > \sum_{j=1}^{i-1} a_j \quad (i = 2, 3, \cdots, n) \tag{1}$$

Knapsack 벡터가 초증가하는 성질을 지닐 때 Knapsack 문제의 해는 쉽게 구할 수 있다. 그러나 이것 자체만으로는 암호 체계가 될 수 없으므로 이를 trapdoor Knapsack 벡터로 변환시킨다. 무작위하게 초증가하는 Knapsack벡터 A를 선택하고 $\Sigma a_i (1 \le i \le n)$보다 큰 정수 p와 이에 서로 소인 정수 W를 임의로 선택한다. 즉,

$$p > \sum_{i=1}^{n} a_i \tag{2}$$

$$GCD(p, W) = 1, p > W,\ W \cdot W^{-1} = 1 \pmod p \tag{3}$$

그리고 공개키가 되는 trapdoor Knapsack 벡터 B = $(b_1, b_2, \cdots, b_n)$는 쉬운 Knapsack 벡터 A의 각 원소 a_i에 W를 곱한 다음 법 p를 연산하여 얻어진다. 즉, 식(4)와 같다.

$$b_i = a_i \cdot W \pmod p \tag{4}$$

이 trapdoor Knapsack 벡터 B는 공개 암호키가 되고, 법 p와 이에 서로소인 정수 W 및 초증가하는 Knapsack 벡터 A는 비밀키가 된다.

2.3.2. 암호화

원문을 2진수 평문 $M = (m_1, m_2, \cdots, m_n)$으로 변환시켜 공개키인 trapdoor 벡터 B를 사용하여 식(5)와 같이 암호화한다.

$$\begin{aligned} C &= B \cdot M \\ &= b_1 m_1 + b_2 m_2 + \cdots + b_n m_n \\ &= \sum_{i=1}^{n} b_i m_i \end{aligned} \tag{5}$$

2.3.3. 복호화

비밀 정보인 W^{-1}과 p를 알고 있는 수신자는 평문을 식(6)과 같이 복호화할 수 있다.

$$\begin{aligned} D &= W^{-1} \cdot C \pmod p \\ &= W^{-1} \sum_{i=1}^{n} b_i m_i \pmod p \\ &= W^{-1} \sum_{i=1}^{n} (a_i W) m_i \pmod p \end{aligned}$$

$$= \sum_{i=1}^{n} (W^{-1} Wa_i)m_i \pmod p$$

$$= \sum_{i=1}^{n} a_i m_i \pmod p$$

$$= A \cdot M \tag{6}$$

다음에 벡터 A의 초증가성을 이용하여 다음과 같은 복호 알고리즘으로 평문 벡터 $(m_1, m_2, \cdots, m_n)$을 구한다.

단계 1. i=n, D′= D
단계 2. IF a_i〉D′ THEN m_i = 0
ELSE m_i = 1, D′= D′-a_i
단계 3. i=i-1
단계 4. IF i=0 THEN STOP
단계 5. GOTO STEP 2

한편 Knapsack 암호 방식의 가장 큰 장점은 다른 공개키 암호 방식에 비하여 암호화 및 복호화의 계산이 매우 쉽다는 것이다. 그러나 Knapsack 암호 방식에서는 안전성을 위해서 암호화할 때 데이터의 확장이 불가피하다. 또한 공개키는 어려운 Knapsack 벡터로 구성되어 있으므로 공개키의 크기가 매우 커지게 된다. 그러므로 Merkle과 Hellman은 안전상의 관점에서 법 p가 100비트 이상의 수가 되어야 한다고 한다.

3. 제안된 Knapsack 공개키 암호 방식

본 논문에서는 MH Knapsack 암호 방식의 안전성에 공개키 다항식의 근을 구하는 어려움에 근거하여 보다 안전성이 있는 다변수 다항식을 이용한 Knapsack 공개키 암호 방식을 제안한다.

제안된 Knapsack 공개키 암호 방식의 키 생성, 암호화 및 복호화 알고리즘은 다음과 같다.

3.1. 키 생성

제안된 다변수 다항식을 이용한 Knapsack 공개키 암호 방식의 키 생성 순서는 다음과 같다.

먼저,

$$a_i \rangle t \sum_{j=1}^{i-1} a_j \quad (i=2,3,\cdots,n) \tag{7}$$

을 만족하는 t배(t=1, 2, 3, …)초증가한 벡터

$$A = (a_1, a_2, \cdots, a_n) \tag{8}$$

을 정한다. 그리고

$$p \rangle t \sum_{i=1}^{n} a_i \tag{9}$$

을 만족시키는 법 p의 값을 정한 후 $0 \langle x_{01}, x_{02}, \cdots, x_{0L} \langle p$를 만족하는 임의의 정수 $x_{01}, x_{02}, \cdots, x_{0L}$을 선택한다.

다음에 식(8)의 초증가 벡터 A의 요소(element) a_i를 식(10)과 같이 만족하도록 적당하게 $a_{i1}, a_{i2}, \cdots, a_{iL}$로 L분할하여 표현한다.

$$a_i = (a_{i1} + a_{i2} + \cdots + a_{iL}) \pmod p \tag{10}$$

식 (10)에서 우변의 각 항을 변수 $x_1, x_2, \cdots, x_L$을 사용하여 식(11)과 같이 변형한다.

$$\begin{aligned} a_{i1} &= (b_{i1}x_1 + r_{i1}) \pmod p \\ a_{i2} &= (b_{i2}x_2 + r_{i2}) \pmod p \\ &\text{--------} \\ a_{iL} &= (b_{iL}x_L + r_{iL}) \pmod p \end{aligned} \tag{11}$$

여기서, $b_{i1}, b_{i2}, \cdots, b_{iL}$과 $r_{i1}, r_{i2}, \cdots, r_{iL}$은 각각 $a_{i1}, a_{i2}, \cdots, a_{iL}$을 $x_1, x_2, \cdots, x_L$로 나눈 몫과 잉여이고, 이 L개의 잉여 합을 식(12)와 같이 $b_{i(L+1)}$로 표현한다.

$$\begin{aligned} b_{i(L+1)} &= (r_{i1} + r_{i2} + \cdots + r_{iL}) \pmod p \\ &= (-b_{i1}x_1 + a_{i1}) + (-b_{i2}x_2 + a_{i2}) + \cdots + (-b_{iL}x_L + a_{iL}) \\ &= -(b_{i1}x_1 + b_{i2}x_2 + \cdots + b_{iL}x_L) + a_{i1} + a_{i2} + \cdots + a_{iL} \\ &= -(b_{i1}x_1 + b_{i2}x_2 + \cdots + b_{iL}x_L) + a_i \pmod p \end{aligned} \tag{12}$$

단, $0 \langle b_{i(L+1)} \langle p, (1 \le i \le n)$

한편 식(10)에서 식(11)을 대입하면

$$\begin{aligned} a_i &= (a_{i1} + a_{i2} + \cdots + a_{iL}) \pmod p \\ &= (b_{i1}x_1 + r_{i1}) + (b_{i2}x_2 + r_{i2}) + \cdots + (b_{iL}x_L + r_{iL}) \\ &= (b_{i1}x_1 + b_{i2}x_2 + \cdots + b_{iL}x_L) + (r_{i1} + r_{i2} + \cdots + r_{iL}) \\ &= (b_{i1}x_1 + b_{i2}x_2 + \cdots + b_{iL}x_L) + b_{i(L+1)} \pmod p \end{aligned}$$

와 같이 되므로 식(12)가 성립함을 알 수 있다.

이와 같이 초증가 벡터 A의 요소 a_i가 식(11),(12)와 같이 다변수 다항식으로 표현된다. 이러한 다변수 다항식을 이용하여 식(13)과 같이 다변수 다항식 벡터 B $(x_1, x_2, \cdots, x_L)$를 표현한 후 암호 벡터로 공개한다.

$$B(x_1, x_2, \cdots, x_L) = (b_{11}x_1+b_{12}x_2+\cdots+b_{1L}x_L+b_{1(L+1)},\ b_{21}x_1+b_{22}x_2+\cdots+b_{2L}x_L+b_{2(L+1)},\ \text{---------},\ b_{n1}x_1+b_{n2}x_2+\cdots+b_{nL}x_L+b_{n(L+1)}) \quad (13)$$

그러므로 초증가 벡터 A의 요소가 n개인데 비해서 다변수 다항식 벡터 $B(x_1, x_2, \cdots, x_L)$의 계수는 n(L+1)개로 된다. 그리고 키 다항식 $f(x_1, x_2, \cdots, x_L)$의 계수 f_j는 $0<f_j<p$ $(j = 1, 2, \cdots, L)$을 만족시키는 정수를 적당히 선택한 후 잉여 계수 f_{L+1}를 식 (14)에서 구하여 식(15)와 같은 키 다항식 $f(x_1, x_2, \cdots, x_L)$를 공개한다.

$$f_{L+1} = -(f_1x_{01}+f_2x_{02}+\cdots+f_Lx_{0L}) \pmod p \quad (14)$$

$$f(x_{01}, x_{02}, \cdots, x_{0L}) = f_1x_{01}+f_2x_{02}+\cdots+f_Lx_{0L}+f_{L+1} \quad (15)$$

제안된 다변수 다항식을 이용한 Knapsack 공개키 암호 방식은 법 p를 공개하고, 초증가 벡터 A를 변형하여 다변수 다항식으로 표현한 암호 벡터 $B(x_1, x_2, \cdots, x_L)$의 계수 $b_{i(L+1)}$과 적당히 선택한 키 다항식 $f(x_1, x_2, \cdots, x_L)$의 계수 f_{j+1}을 공개한다. 또한 비밀키는 초증가 벡터 A와 키 다항식 f의 근$(x_{01}, x_{02}, \cdots, x_{0L})$이다.

따라서 다변수 다항식을 이용한 Knapsack 공개키 암호 방식의 안전성은 MH Knapsack 암호 방식의 안전성과 함께 암호 벡터의 요소를 만족시키는 키 다항식 $f(x_1, x_2, \cdots, x_L) \equiv 0 \pmod p$를 인수분해하여 근$(x_{01}, x_{02}, \cdots, x_{0L})$을 찾는 어려움에 근거를 둔다.

3.2. 암호화

송신하고자 하는 n비트의 평문 벡터 M을

$$M = (m_1, m_2, \cdots, m_n),\ m_i \in \{0, 1\} (1 \le i \le n) \quad (16)$$

와 같이 표시하고 난수 $\alpha(0<\alpha<p)$를 사용하여 식(17)과 같이 암호화한다.

$$C(x_1, x_2, \cdots, x_L) = B(x_1, x_2, \cdots, x_L) \cdot M + \alpha \cdot f(x_1, x_2, \cdots, x_L)$$

$$= \sum_{i=1}^{n} \{(b_{i1}x_1+b_{i2}x_2+\cdots+b_{iL}x_L+b_{i(L+1)})m_i\} + \alpha(f_1x_1+f_2x_2+\cdots+f_LX_L+f_{L+1}) \pmod p$$

$$= \sum_{i=1}^{n} (b_{i1}m_i+\alpha f_1)x_1 + \sum_{i=1}^{n} (b_{i2}m_i+\alpha f_2)x_2+\cdots + \sum_{i=1}^{n} (b_{iL}m_i+\alpha f_L)x_L + \sum_{i=1}^{n} (b_{iL+1}+\alpha f_{L+1})$$

$$= C_1x_1+C_2x_2+\cdots+C_Lx_L+C_{L+1} \pmod p \quad (17)$$

단, $C_j = \sum_{i=1}^{n} (b_{ij}m_i+\alpha f_j),\ (1 \le j \le L+1) \pmod p$

식(17)에서 구한 암호문의 다항식 계수 C_j를 수신자에게 보낸다. 따라서 송신하고자 하는 n비트의 평문 벡터 M을 암호화하면 (L+1)개의 십진수로 된 데이터로 변형되어 수신자에게 보내진다.

3.3. 복호화

복호화는 수신자가 수신된 암호문을 복호하기 위한 과정으로 암호문 $C(x_1, x_2, \cdots, x_L)$에 키 다항식 $f(x_1, x_2, \cdots, x_L) \equiv 0 \pmod p$의 근 $x_{01}, x_{02}, \cdots, x_{0L}$을 대입하여 식 (18)과 같이 D를 구한다.

$$D(C) = C(x_1, x_2, \cdots, x_L) \mid_{x_1=x_{01}, \cdots, x_L=x_{0L}} \pmod p$$

$$= C_1x_1+C_2x_2+\cdots+C_Lx_L+C_{L+1} \mid_{x_1=x_{01}, \cdots, x_L=x_{0L}}$$

$$= \sum_{i=1}^{n} (b_{i1}x_1+b_{i2}x_2+\cdots+b_{iL}x_L+b_{i(L+1)})m_i \mid_{x_1=x_{01}, \cdots, x_L=x_{0L}}$$

$$= \sum_{i=1}^{n} \{(b_{i1}x_1+b_{i2}x_2+\cdots+b_{iL}x_L)+(r_{i1}+r_{i2}+\cdots+r_{iL})\}m_i$$

$$= \sum_{i=1}^{n} \{(b_{i1}x_1+r_{i1})+(b_{i2}x_2+r_{i2})+\cdots+(b_{iL}x_L+r_{iL})\}m_i$$

$$= \sum_{i=1}^{n} (a_{i1}+a_{i2}+\cdots-a_{iL})m_i$$

$$= \sum_{i=1}^{n} a_i m_i \pmod p \quad (18)$$

따라서 식(18)에서 구한 D와 비밀키 벡터 A의 초증가성을 사용하여 2.3.3절에서 나타낸 복호 알고리즘으로 평문 벡터 $M = (m_1, m_2, \cdots, m_n)$이 얻어진다. 이 과정에서 암호화에 사용된 난수 α는 복호와는 무관하게 처리됨을 알 수 있다.

3.4 안전성의 검사

다변수 다항식을 이용한 변형 Knapsack 공개키 암호의 안전성은 다음의 조건식

$$b_{i1}x_1+b_{i2}x_2+\cdots+b_{iL}x_L+b_{i(L+1)} \pmod p$$
$$\rangle \sum_{j=1}^{i-1} (b_{j1}x_1+b_{j2}x_2+\cdots+b_{jL}x_L+b_{j(L+1)}) \mid_{x_1=x_{01},\cdots,x_L=x_{0L}}$$
$$(i=2,3,\cdots,n) \pmod p$$

을 만족하는 $f(x_1, x_2, \cdots, x_L) \equiv 0 \pmod p$의 근 $x_{01}, x_{02}, \cdots, x_{0L}$을 구하는 것의 어려움에 기인하고 있다. 또한 식(15)의 L변수 키 다항식 $f(x_1, x_2, \cdots, x_L) \equiv 0 \pmod p$의 근 $(x_{01}, x_{02}, \cdots, x_{0L})$은 법 p가 소수이므로 모두 p^{L-1} 개 존재한다. 이때 연립 1차 방정식의 총수도 최대 p^{L-1}개가 된다. 그리고 식(15)의 키 다항식 $f(x_1, x_2, \cdots, x_L) \equiv 0 \pmod p$의 근 $(x_{01}, x_{02}, \cdots, x_{0L})$인 비밀키$(x_{01}, x_{02}, \cdots, x_{0L})$을 구하는데 필요한 최대 계산량은 $O(p^{L-1})$이 되며, 비밀키가 초증가성을 만족하고 암호 해독을 위한 전수검사에 요하는 시간을 많이하여 안전성을 높이기 위해 t배 초증가한다고 하는 조건을 붙이는 경우도 최대 계산량은 $O(\prod_{i=0}^{L-2} p-(t+1)^i)$이므로 본 암호를 깨기 위해서는 $f(x_1, x_2, \cdots, x_L) \equiv 0 \pmod p$를 만족하는 근$(x_{01}, x_{02}, \cdots, x_{0L})$과 $B(x_1, x_2, \cdots, x_L)$에 의해 변형된 비밀키인 t배의 초증가 벡터 $A = (a_1, a_2, \cdots, a_n)$을 찾는 것은 계산량적으로 어렵다고 판단된다. 그리고 법의 값 p에 대응하는 초증가 벡터가 얻어지는 비율은 작은 것으로 생각되지만 안전성을 높이는 의미에서는 차수가 3차 이상의 다변수 다항식 2개를 이용하여 연립시키는 것이 좋다고 생각되어진다. 그러나 다변수 연립방정식의 근을 구하는 알고리즘이 얻어지는 경우에는 암호화, 복호화가 다소 복잡하지만 (2i+1)변수 (2i+1)차의 다항식을 2i개 연립시킴으로써 (i=1, 2, 3, ···)해독이 어려운 다변수 다항식 변형 Knapsack 암호가 된다. 한편 a_i의 분할과 x_i, f_i의 선택에 많은 융통성이 있으므로 키 선택의 가능성의 조합이 많아져 해독의 어려움과 함께 다양한 키 선택이 가능하다는 장점을 갖고 있다.

4. 시뮬레이션 과정 및 결과 고찰

제안된 다변수 다항식를 이용한 Knapsack 공개키 암호 방식의 타당성을 입증하기 위하여 주어진 평문에 대해 컴퓨터 시뮬레이션을 한다.

먼저, 식(8)를 만족하는 t(=1)배 초증가한 벡터 A = (2, 3, 6, 13, 25, 50, 100, 200)을 정하고 식(9)를 만족하는 법 p=403으로 정한 후 임의의 정수 x_{01}= 11, x_{02}=6, x_{03}=44로 선택한 후 초증가 벡터 A의 요소 a_i를 다음과 같이 변형한다.

$$\begin{aligned} A &= (a_{11}+a_{12}+a_{13},\ a_{21}+a_{22}+a_{23},\ a_{31}+a_{32}+a_{33},\\ &\quad a_{41}+a_{42}+a_{43},\ a_{51}+a_{52}+a_{53},\ a_{61}+a_{62}+a_{63},\\ &\quad a_{71}+a_{72}+a_{73},\ a_{81}+a_{82}+a_{83}) \pmod p \\ &= (332 + 33 + 40, 343 + 23 + 40, 628 + 94 + 90,\\ &\quad 333 + 38 + 45, 146 + 63 + 55, 373 + 47 + 33,\\ &\quad 200 + 250 + 53, 200 + 148 + 255) \pmod{403} \end{aligned}$$

그리고 변수 x_1, x_2, x_3를 이용한 다항식 벡터 $B(x_1, x_2, x_3)$를 식(19)와 같이 표현한 후 암호 벡터로 공개한다.

$$\begin{aligned} B(x_1, x_2, x_3) = (&30x_1+5x_2+0x_3+45, 31x_1+3x_2+0x_3+47,\\ &57x_1+15x_2+2x_3+7, 30x_1+6x_2+1x_3+6,\\ &13x_1+105x_2+1x_3+14, 33x_1+7x_2+0x_3+48,\\ &18x_1+41x_2+1x_3+15, 18x_1+24x_2+5x_3+41) \end{aligned} \quad (19)$$

또한 식(14)를 만족하는 키 다항식 $f(x_1, x_2, x_3)$의 계수를 f_1=12, f_2=33, f_3=68로 선택하면 f_4=305가 되므로 공개키 다항식은 식(20)과 같이 된다.

$$f(x_1, x_2, x_3) = 12x_1+33x_2+68x_3+305 \quad (20)$$

만일 송신하고자 하는 문자 p인 경우 8비트 2진수로 표현하면 평문의 데이터는 M = (00110000)와 같고, 난수 α=284로 선택하면 암호문은 식(17)에서 식(21)과 같이 구해진다.

$$C(x_1,x_2,x_3) = (57x_1+15x_2+2x_3+7)+(30x_1+6x_2+1x_3+6) +284(12x_1+33x_2+68x_3+305) \pmod{403}$$
$$= (271x_1+124x_2+374x_3+391) \pmod{403} \quad (21)$$

복호는 먼저 식(18)에서 D를 구하면 식(22)와 같다.

$$D(C)=C(x_1, x_2, x_3)\,|_{x_1=11,\ x_2=6,\ x_3=44} \pmod{403}$$
$$=(271x_1+124x_2+374x_3+391)\,|_{x_1=11,\ x_2=6,\ x_3=44}$$
$$=19 \pmod{403} \quad (22)$$

이것을 이용하여 복호하면 2.3.3에 나타낸 복호화 알고리즘으로 부터 평문 M=(00110000)이 얻어진다.

따라서 공개키(p,B,f)와 비밀키(A,x_i)의 값을 가지고 송신자가 송신하고자 할 원문 〔Public Key Knapsack Cryptosystem〕을 시뮬레이션한 결과 송신 2진수 평문(M)은 표1, 난수(α)는 표2,암호문(C)는 표3,수신 2진수 평문(M)은 표4와 같다.여기에서 송신 2진수 평문은 원문의 각 문자에 대응하는 8비트 2진수로 나타내었고, 난수는 $0<\alpha<p$의 범위에서 임의로 뽑아 사용하였다. 이와 같이 송신 2진수 평문에 대해 난수와 암호 알고리즘을 적용하면 암호문이 얻어진다.이 암호문를 수신자에게 전송하면 수신자는 공개키와 비밀키를 사용하여 암호문을 복호함으로써 수신 2진수 평문을 얻는다. 그리고 수신 2진수 평문을 8비트 2진수에 대응시키면 원문 〔Public Key Knapsack Cryptosystem〕을 얻는다.

즉 송신 원문 〔Public Key Knapsack Cryptosystem〕의 첫번째 문자 〔P〕를 8비트 2진수로 바꾸면 〔00110000〕와 같은 송신 2진수 평문이 되고,난수 α=284와 암호 알고리즘을 적용하면 암호문 〔271,124,374,391〕이 얻어진다. 이 암호문을 수신자가 복호하면 수신 2진수 평문 〔00110000〕을 얻고 원문으로 바꾸면 송신한 문자 〔P〕을 얻는다.

또한 송신 원문 〔Public Key Knapsack Cryptosystem〕에서 〔Key〕에 있는 문자 〔K〕와 〔Knapsack〕에 있는 문자 〔K〕에 대하여 암호화하는 데 사용되는 난수 α가 각각 306,166과 같이 서로 다르므로 암호문도 〔151,208,264,314〕,〔57,9,11,372〕와 같이 각각 다르게 되어 해독이 어렵게 됨을 알 수 있다.

제안된 다변수 다항식을 이용한 변형 Knapsack 공개키 암호 방식은 t배 초증가한 벡터의 요소를 변형하여 다항식으로 표현한 암호 벡터에 난수배한 공개키 다항식을 더한 것을 암호문으로 하였다. 이 암호의 안전성은 다변수 다항식 암호 벡터 $B(x_1,x_2,x_3)$의 각 변수에 공개키 다항식$f(x_1,x_2,x_3)\equiv 0 \pmod{403}$의 근을 대입할 때 공개키 다항식을 인수분해하여 초증가 벡터가 얻어지는 $f(x_1,x_2,x_3)\equiv 0$의 근의 집합을 구하는데 어려움이 있다.또한 안전성을 높이기 위해서는 암호 해독을 위한 전수검사에 요하는 시간을 많이 하기 위해서 t배 초증가한 벡터의 밀도를 높이고 법의 값을 가능한 작게 정하며, 암호 벡터의 계수와 키다항식의 계수 벡터를 1차 독립으로 정한다. 식(20)의 3변수 키다항식 $f(x_1,x_2,x_3)\equiv 0 \pmod{p}$의 근 (x_{01},x_{02},x_{03})은 법 p가 소수이므로 모두 p^2개 존재한다. 이때 전수검사에 요하는 계산량은 $O(p^2)$이다.

표 1. 송신 2진수 평문(M)
Table 1. Sender Binary Digit Plaintext(M)

00110000	01010101	01000010	01001100
01001001	01000011	00000000	00101011
01000101	01011001	00000000	01001011
01001110	01000001	01010000	01010011
01000001	01000011	01001011	00000000
00100011	01010010	01011001	01010000
01010100	01001111	01010011	01011001
01010011	01010100	01000101	01001101

표 2. 난수(α)
Table 2. Random Numbers(α)

284	214	233	116
121	312	5	306
328	285	18	166
347	318	150	387
351	22	382	146
211	309	21	238
188	120	250	261
106	112	334	332

표 3. 암호문(C)
Table 3. Ciphertext(C)

271	124	374	391	262	251	50	126	24	76	128	199	260	316	232	25
305	95	174	334	184	289	266	155	60	165	340	316	151	208	264	314
391	380	144	232	288	274	43	388	216	191	15	251	57	9	11	372
229	323	224	373	238	743	270	358	249	123	126	264	308	352	128	65
231	326	96	348	331	391	293	365	231	286	191	160	140	385	256	200
207	192	251	341	160	172	58	11	344	25	226	65	96	206	65	103
335	175	292	215	344	110	107	92	276	264	81	192	0	288	23	322
160	348	364	199	229	85	363	6	60	175	149	47	49	214	14	257

표 4. 수신 2진수 평문(M)
Table 4. Received Binary Digit Plaintext(M)

00110000	01010101	01000010	01001100
01001001	01000011	00000000	00101011
01000101	01011001	00000000	01001011
01001110	01000001	01010000	01010011
01000001	01000011	01001011	00000000
00100011	01010010	01011001	01010000
01010100	01001111	01010011	01011001
01010011	01010100	01000101	01001101

5. 결 론

본 논문에서는 MH Knapsack 암호 방식을 분석하고 이 암호 알고리즘에 다변수 다항식의 근을 구하는 어려움에 근거한 데이터 통신의 안전성을 갖는 다변수 다항식을 이용한 Knapsack 공개키 암호 방식을 제안하였다.

제안된 Knapsack 공개키 암호 방식에서는 MH Knapsack 암호 방식의 초증가 벡터의 각 요소를 변형하여 다변수 다항식으로 표현한 것을 암호 벡터로 구성하고, 이것과 평문 벡터와의 내적에 난수를 곱한 공개키 다항식을 더하여 암호문으로 한다. 송신하고자 하는 평문 벡터을 암호화하면 L+1개의 십진수로 된 데이터로 변형되어 수신자에게 전송된다. 이때 난수의 사용으로 동일한 평문에 대하여 각각 다른 암호문이 구성되는 장점이 있다. 그리고 다변수 다항식 $f(x_1, x_2, \cdots, x_L) \equiv 0 \pmod p$의 근을 구하기 위한 전수검사에 요하는 계산량은 $O(p^{L-1})$이다.

따라서 본 논문에서 제안된 Knapsack 공개키 암호 방식은 법, 암호 벡터 및 키 다항식을 공개키로 구성하고, 암호의 안전성은 초증가 벡터의 요소를 변형하여 표현한 다변수 다항식인 암호 벡터의 각 변수에 공개키 다항식의 근을 대입할 때 공개키 다항식을 인수분해하여 근을 찾는데 어려움이 있다.

참고문헌

1. S.Tsujii, M.O.Kasahara, Cryptography and Information Security, 昭晃堂, 1990.
2. 池野信一, 小山謙二, 現代暗號理論, 日本電子情報通信學會, 1989.
3. W.Diffie and M.E. Hellman, "New Direction in Cryptography," IEEE Trans.Inform. Theory, Vol. IT-22, No. 1976.
4. R.L.Rivest, A.Shamir and L.Adleman, "A Method for obtaining Digital Signatures and Public Key Cryptosystem," Comm. Vol. 21, No.2, pp.120-126, 1978.
5. R.C.Merkle and M.E.Hellman, "Hiding Information and Signatures in Trapdoor Knapsacks," IEEE Trans. Info. Theory, Vol. IT-24, 1978.
6. W. Diffie and M.Hellman, "Privacy and Authentication : An Introduction to

Cryptography," Proc. IEEE, Vol. 67, pp.397-527, 1979.
7. B.Chor and R.L.Rivest, "A Knapsack - Type Public Key Cryptosystem Based on in Arithmetic in Finite Fields," IEEE Trans. Inf. Theory, Vol. 34, No. 5, pp.901-909, 1988.
8. T.Egamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discret Logarithms," IEEE Trans. Inf. Theory, Vol. IT-31, No.4, pp.469-472, 1985.
9. 小林邦勝, 田村桓一, 根元義章, "多變數多項式を用いたナップザック暗號," 電子通信學會論文誌(A), Vol. J73-A, No. 3, pp.570-575, 1990.
10. M.E. Hellman, "An Overview of Public Key Cryptography," IEEE Communication Society Magazine, pp.24-32, 1978.
11. C.S. Kline and G.J.Popek, "Public Key vs. Conventional Key Encryption," National Computer Conference, pp.831-837, 1979.
12. C.H.Meyer, S.M. Matyas, Cryptography : A New Dimension in Computer Data Security, John Wiley and Sons, 1982.
13. D.B.Newman, Jr., et al., Public Key Management for Network Security,IEEE Network Magazine, Vol. 1, No. 2, pp.11-16, April. 1987.
14. R.M.Needham and M.D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers," Comm. ACM, Vol. 21, No. 12, pp.993-999, December. 1978.
15. Shamir,A., "Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem," IEEE Trans.on Informat. Theory 30, pp.699-704, 1984.

丘 冀 俊(Ki Jun KU) 정회원

1959년 4월 28일생
1983년 2월 : 단국대학교 전자공학과 졸업(공학사)
1988년 8월 : 한양대학교 대학원 전자공학과 졸업(공학석사)
1992년 8월 : 숭실대학교 대학원 전자공학과 박사과정 수료
1984년 3월~1994년 2월 : 유성전자공고 교사
1994년 3월~현재 : 한림전문대학 전자통신과 전임강사
※주관심 분야 : 정보통신, 암호 및 부호이론, 무선통신

沈 壽 輔(Soo Bo SIM) 정회원

1931년 5월 30일생
현재 : 숭실대학교 정보통신공학과 교수
※주관심 분야 : 정보 및 무선통신 시스템