情報保護學會論文誌
第12券 第1號, 2002. 2

# 초타원 곡선위에서 생성된 대수기하 부호를 이용한 McEliece 유형의 공개키 암호시스템*

강 보 경**, 한 상 근**

# McEliece Type PKC Based on Algebraic Geometry Code over Hyperelliptic Curve

Bo Gyoung Kang**, Sang Geun Hahn**

요 약

1976년 McEliece는 충분한 키 공간을 가지면서 효율적인 복호(decoding) 알고리즘이 존재하는 이진 오류수정 부호 중 하나인 Goppa 부호를 사용한 공개키 암호시스템을 소개하였다. 이 시스템은 소인수 분해 문제, 이산로그 문제에 기반을 둔 기존의 공개키 암호시스템( RSA, ECC)보다 암호화, 복호화가 아주 빠르다는 장점이 있다. 하지만 최소 무게 부호어(codeword)를 찾는 확률적 알고리즘을 사용한 새로운 공격방법이 개발되면서 [1024,524,101] Goppa 부호를 사용한 McEliece 암호시스템이 충분한 안전성을 갖지 못한다는 사실이 밝혀졌고, 이를 보완하기 위한 새로운 Goppa 부호 파라메터 [2048,1608,81]가 제안되었다.[1] 그러나 McEliece 암호시스템의 키 사이즈가 다른 공개키 암호시스템에 비해 상대적으로 크다는 단점을 가지고 있으므로 이런 결과는 오류 수정부호에 기반한 공개키 암호시스템의 효용성을 저하시키는 요인이 된다. 따라서 본 논문에서는 이진 Goppa 부호가 아닌 초타원 곡선 위에서 생성된 적절한 파라메터를 가지는 $q(\neq 2)$진 대수기하 부호를 이용한 변형된 McEliece 암호시스템을 제안한다. 새로이 제안되는 암호시스템은 기존의 McEliece 암호시스템 보다 충분한 안전성을 가지고, 부호를 이용한 암호시스템의 최대 장점인 빠른 암호화, 복호화를 보장하는 동시에 키 사이즈는 3분의 1로 개선되었다.

ABSTRACT

McEliece introduced a public-key cryptosystem based on Algebraic codes, specially binary classical Goppa Codes which have a good decoding algorithm and vast number of inequivalent codes with given parameters. And the advantage of this system is low cost of their encryption and decryption procedures compared with other public-key systems specially RSA, ECC based on DLP(discrete logarithm problem). But in [1], they present new attack based on probabilistic algorithm to find minimum weight codeword, so for a sufficient security level, much larger parameter size [2048, 1608, 81] is required. Then the big size of public key make McEliece PKC more inefficient. So in this paper, we will propose New Type PKC using $q-ary$ Hyperelliptic code so that with smaller parameter(1 over 3) but still work factor as high as McEliece PKC and faster encryption, decryption can be maintained.

**keyword** : *McEliece PKC, Algebraic geometry code, Hyperellipic curve, Coding theory*

* 이 논문은 1999년도 한국학술진흥재단의 연구비에 의하여 지원되었음(KRF-99-041-D00020)
** 한국과학기술원 수학과 암호론 연구실({bogus,sghahn}@mathx.kaist.ac.kr)

## Ⅰ. 서 론

공개키 암호의 기반을 제시한 Diffie와 Hellman의 논문이 발표된 이후 최근까지 수많은 공개키 암호 알고리즘들이 제안되어 왔지만 아직까지 그 안전성을 보장받는 것은 거의 없다. 특히, 그 수학적 기반을 살펴보면 사실상 소인수분해 문제와 이산대수 문제로 대표되는 정수론에 의지하고 있다. 최근의 컴퓨터 환경의 획기적인 발전으로 인해 기존의 문제에 기반한 암호 알고리즘의 안전성을 보장하기 위해서는 키 길이의 증가가 필수적이다. 그러나 이로인해 효율적인 암호 알고리즘의 사용이 더욱 더 힘들어지게 되었을 뿐만 아니라 최근에 활발하게 연구되고 있는 퀀텀 컴퓨터가 실용화 될 경우 위의 두 문제가 모두 다항식 시간에 풀린다는 사실이 밝혀졌다.[2] 이런 상황에서 구조가 알려지지 않은 임의의 부호를 복호(decoding)하기 어렵다는 문제에 안전성의 기반을 둔 McEliece 암호시스템은 기존의 공개키 암호시스템의 좋은 대안이 될 수 있다. 또한 McEliece 암호시스템은 기존의 공개키 암호시스템에 비해 암호화(Encryption)와 복호화(Decryption) 과정이 빠르다는 장점이 있다.[1] 그러나 최근의 연구결과인 최소 무게(weight) 부호어(codeword)를 찾는 새로운 확률적 알고리즘을 이용하면, 지금까지 알려진 가장 강력한 공격방법인 Lee-Brickell 방법[7]보다 128배 개선된 $2^{64.2}$의 계산량으로 파라메터 [1024,524,101]를 가지는 이진 Goppa 부호를 이용하는 McEliece 암호시스템에서의 메시지를 복원할 수 있음이 밝혀졌다.[1] 그러므로, 기존의 McEliece 암호시스템의 충분한 안전성을 보장하기 위해서는 변형된 파라메터 [2048,1608,81]를 가지는 Goppa 부호가 필요한데 이를 사용할 경우, 키 사이즈가 기존에 비해 대략 6배 커지게 된다. McEliece 암호시스템이 다른 공개키 암호시스템들과 비교할 때 아주 빠른 암호화, 복호화가 가능한 장점에도 불구하고 상대적으로 큰 키 사이즈를 가진다는 단점이 있으므로 빠른 암호화 복호화를 보장하고, 충분한 안정성을 가지면서 동시에 키 사이즈를 개선하는 방법을 연구하는 것은 McEliece 암호시스템이 기존의 암호시스템의 실제적인 대안이 될 수 있는 가능성을 좀 더 구체적으로 제시하는 것이다.

지금까지 McEliece 공개키 암호시스템에 사용되는 Goppa 부호의 파라메터를 개선하기 위해서 아래와 같이 여러 가지 대안이 제시되었다.

[표 1] McEliece PKC에 제안된 오류 수정 부호

| | | |
|---|---|---|
| 1 | McEliece | 이진 Goppa 부호 |
| 2 | Niederreiter | GRS(Generalized Reed-Solomon) 부호 |
| 3 | Gabidulin | 빠른 복호 알고리즘을 가진 Gabidulin 부호 |
| 4 | Sidelnikov | Reed-Muller 부호 |
| 5 | Janwa | $q=p^n$, $F_q$에서 정의된 대수기하 부호, 부분체에서 정의된 부분 $q$진 부호, $q^m$진 대수기하 부호와 $q$진 부호를 연결한 부호 |

그러나 위에서 제시된 부호를 사용한 McEliece 암호시스템들은 대다수가 그 부호가 가진 특별한 성질에 의해 공격당했다. 예를 들어 Sidelnikov와 Shestakov는 Niederreiter가 제안한 GRS 부호를 사용한 McEliece 유형 암호시스템은 GRS 부호의 MDS(Maximum Distance Separable) 성질과 생성행렬이 가진 Vandemonde 구조에 의해 안전하지 않음을 보였다.[15] GRS 부호가 rational 대수기하 부호(genus $g=0$인 rational 함수체에서 생성된 부호)의 쌍대부호(dual code)라는 사실에 비추어 보면 결국 rational 대수기하 부호를 사용한 McEliece 유형 암호시스템이 안전하지 못하다는 사실을 알 수 있다. 그러나, Krouk은 더 많이 생성행렬을 뒤섞음으로써 GRS의 구조를 대칭적이지 않게 하여 McEliece 암호시스템의 안전성을 보장하는 방법을 제시하였다.[13] 본 논문에서는 그 구조가 취약한 rational 함수체가 아닌 함수체에서 생성된 대수기하 부호를 사용하는 새로운 McEliece 유형의 암호시스템을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 이진 부호를 사용하는 McEliece 암호시스템에 대해 살펴보고 지금까지 제안된 공격방법과 암호화, 복호화의 계산복잡도(complexity)에 대해 정리한다. 그리고 3장에서는 초타원 함수체위에서 대수기하 부호를 생성하는 방법과 복호(decoding) 알고리즘에 대해 정리하며 마지막 4장에서는 본 논문에서 제안하는 개선된 McEliece 유형의 공개키 암호 알고리즘을 소개하고, 가능한 공격방법과 그에 대한 저항성, 그리고 구현을 통해 부호를 이용한 암호시스템의 최대 장점인 빠른 암호화, 복호화가 가능하다는 것을 검증할 것이다.

## Ⅱ. McEliece 공개키 시스템

### 2.1 McEliece 공개키 시스템

이 장에서는 간단하게 McEliece 암호시스템의 알고리즘을 소개하도록 하겠다. 사용자는 $[n,k,2t+1]$ 이진 Goppa 부호의 생성행렬 $G$를 선택한다. 여기에서 $n$은 $G$의 길이(암호문의 길이), $k$는 $G$의 차원(평문의 길이) 그리고 $t$ 는 오류수정이 가능한 최대 비트수를 의미한다. $S$는 $k\times k$ 정칙행렬, $P$는 $n\times n$ 전치행렬이다.

비밀키 : $S, P, G$ 이진 Goppa 부호
공개키 : $G' = SGP$, $t$
암호화 : $m \in F_2^k$
$c \in mG' + e$, $e \in F_2^n$
$w(e) = t$ : $e$가 가진 1의 개수
복호화 : $c \in mG' + e = m(SGP) + e$,
$P$는 정칙행렬
$cP^{-1} = (mS)G + eP^{-1}$
$G$의 빠른 복호 알고리즘을 이용하여 오류 $eP^{-1}$를 고치고, $mS$ 값을 얻는다. 평문 $m$은 $(mS)S^{-1}$로 복원된다.

McEliece의 [1024,524,101] 이진 Goppa 부호를 사용한 암호 시스템이 취약하다는 것이 밝혀졌으므로[1] 본 논문에서 제안하는 암호시스템의 안전성은 [2048,1608,81] 이진 Goppa 부호를 사용한 McEliece 암호시스템과 비교한다.

## 2. 공격 방법

### 2.1 유형 1 : 공개키 분해

① $G' = SGP$로 분해한다. $k$ 차원을 가진 이진 $k\times n$ 행렬의 집합에 동치관계 $R(A,B)$는 어떤 $n\times n$행렬 $P$가 존재해서, $A = BP$가 되는 경우로 정의하자. 이 동치관계에 의해 서로 동치가 아닌 [1024,524,101] 이진 Goppa 부호는 $2^{466}$개로 충분하다.[4]

② 구조적 공격방법[5]
지금까지 부호의 구조를 이용한 효율적인 공격방법은 제시되지 않았다. Sendrier는 SSA(Support Splitting Algorithm)를 이용하여 두 개의 치환동치관계인 부호사이의 치환을 계산함으로써 비밀키를 알아내는 새로운 공격방법을 제안하였다.[6] 그러나 위 알고리즘은 특별한 파라메터를 가지는 부호를 사용한 McEliece 암호시스템에만 적용될 수 있고, 일반적인 경우에 대해서는 효과적이지 못하다. 또한, 이런 유형의 구조적 공격방법은 약한 키를 사용하지 않으면 간단히 피해갈 수 있다. 또한 P.Loidreau는 이런 약한 키를 사용하는 대신 $t$-복호가능한(decodable) 집합을 정의한 후, 그 집합 안의 50보다 더 많은 오류를 가진 오류 벡터를 사용하여 McEliece 암호시스템이 상대적으로 취약한 복호(decoding) 공격방법에 강하도록 하는 방법을 소개하였다.[14]

### 2.2 유형 2 : 공개키 분해없이 암호문 복호

① $G'$로 부터 직접 평문을 얻어내는 방법
㉠ $G'$에서 오류가 없는 $k$개의 위치를 이용한 공격방법
만약 $e$에서 오류가 없는 위치에 해당하는 $G'$의 $k\times k$ 부분행렬 $G'_k$을 선택했다면, 평문 $m = c_k G'^{-1}_k$로 복원될 수 있다. 그러나 이런 위치를 선택할 확률은

$$ {}_{974}C_{524} / {}_{1024}C_{524} = 0.72 \times 10^{-16} $$

로 아주 낮다. 따라서, $k\times k$행렬의 역행렬을 얻는데 $k^3$의 계산량이 필요하다고 하면, 이 공격방법에 필요한 총 계산량은 $1.98\times 10^{24} \sim 2^{80.71}$이다.
㉡ 작은 오류를 가진 $k$개의 위치를 이용한 공격방법[7]
선택된 $k$개의 위치에 있는 오류의 개수를 $j$라 할 때 작은 $j$ 만큼의 오류가 있을 때라도 평문을 복원할 수 있는 방법으로 그 계산량은 약 $2^{73.4}$이다.

② 최소 무게 부호어 찾기 : 복호(decoding) 공격방법
평문을 얻기 위해서는 임의의 오류 벡터 $e$를 제거해야한다. $G'$를 복호하는 문제는 다음과 같이 $G''$에서 최소 무게 부호어를 찾는 문제로 변환될 수 있다.

$$ G'' = \begin{pmatrix} G' \\ c = mG' + e \end{pmatrix} = \begin{pmatrix} G' \\ e \end{pmatrix} $$

후에 J.S.Leon과 J.Stern은 이 문제를 해결하기

위한 확률적 알고리즘을 소개하였고, F.Chabaud는 더욱 최적화 된 알고리즘으로 구현하였다. 또한, [1024,524,101] 부호가 최소 무게 부호어를 찾는 알고리즘에 취약하므로, 이 공격방법에 안전하기 위해서는 [2048,1608,81] 이진 Goppa 부호를 사용하는 것이 필요함을 밝혔다.[11] 이와 같이 더욱 커진 공개키의 크기는 오류 수정 부호를 사용하는 공개키 암호시스템의 효율성을 크게 저하시킬 수 있다. 그러나 P.Loidreau는 McEliece 암호시스템이 가진 구조적 공격방법에 강한 장점과 복호(decoding) 공격방법에 취약한 단점을 교환하여 공개키의 크기를 늘리지 않고 충분한 안전성을 보장하는 암호시스템을 제안하였다.[4]

### 2.3 유형 3 : 공개키 사이즈와 구조에 관계없는 공격방법

유형 3의 공격방법은 키의 크기를 증가시켜도 피할 수 없는 심각한(critical) 공격방법이다. 이 공격에 안전하기 위해서 H-M. Sung은 McEliece 암호시스템의 변형 방법을 제시하였다.[12] 또한 K.Kobara와 H.Imai는 일반적인 방법의 OAEP중 McEliece 암호시스템에 적용 가능한 것들을 살펴보고 나아가서 잉여 데이터(redundant data)의 양를 줄이는 새로운 변형 방법을 제안하였다.[7] 능동 선택 암호문 공격(Adaptive Chosen-Ciphertext Attack)에 안전한 이 방법은 본 논문에서 제시할 $q$진 대수기하 부호를 이용한 McEliece 유형의 암호시스템에도 그대로 적용할 수 있을 것이다. 현재까지 제시된 공격방법들을 좀 더 자세하게 살펴보자.

① 같은 평문의 반복 암호화, 서로 연관된 평문의 암호화[8]

하나의 평문 $m$을 $c_1 = mSGP + e_1$, $c_2 = mSGP + e_2$로 두 번 암호화 하면 $c_1 + c_2 = e_1 + e_2 \pmod 2$이다. 먼저, 공격자는 $s = c_1 + c_2$의 해밍중(Hamming Weight)을 계산하여 그 무게가 100 미만이라는 사실로부터 동일한 평문이 두 번 암호화된 것을 알아낸 후에 $c_1 + c_2$ 으로부터 아래와 같은 두 집합을 계산한다.

$$L_0 = \{l \in [1,1024] : c_1(l) + c_2(l) = e_1(l) + e_2(l) = 0\}$$
$$L_1 = \{l \in [1,1024] : c_1(l) + c_2(l) = e_1(l) + e_2(l) = 1\}$$

암호를 해독하기 위해서 공격자는 만약 $l \in L_0$이면, $c_1(l)$과 $c_2(l)$ 모두 오류 벡터에 영향을 받지 않았을 가능성이 높고 $l \in L_1$이면 확실하게 둘 중 하나는 오류 벡터에 의해 영향을 받았다는 사실을 이용한다.

공격자가 두 평문들 사이의 관계식 $\sigma = m_1 + m_2$을 알고, 각 평문이 $c_1 = m_1 SGP + e_1$와 $c_2 = m_2 SGP + e_2$로 암호화 되었다고 하자. 공격자는 우선 두 암호문을 이용하여 $c_1 + c_2 + (m_1 + m_2)SGP = e_1 + e_2$를 계산한다. 그 후에 앞의 방법을 이용하여 평문을 복원한다.

② 능동 선택 암호문 공격[9]

McEliece 암호시스템은 암호학적으로 매우 강한 공격인 능동 선택 암호문 공격에 취약하다. 해독하고 싶은 암호문 $c$의 2개 비트를 바꾼 후 오라클에게 해독을 요청한다. 만약, 바꾼 2개 비트가 오류 벡터의 2개 비트를 '0'을 '1'로 '1'은 '0'으로 바꾼 것이라면, 오라클은 평문 $m$을 준다. 이 확률은

$$_{50}C_1 \times {}_{974}C_1 / {}_{1024}C_2 \sim 0.092978$$

이다. 따라서 공격자는 약 13번의 시행으로 평문을 복원 할 수 있다. 그러나 공격 후 $e = c + mG'$의 무게가 50인지 아닌지 여부에 따라 복원된 평문이 올바르게 해독되었는지 판단하는 것이 필요하다.

③ 비유연성(non-malleability)을 만족하지 않는다.[9]

주어진 암호문 $c$가 있을 때 공격자는 이 암호문에 대응하는 평문 $m$과 관계 있는 또 다른 평문 $m'$에 대한 암호문을 만들어 낼 수 있다. 그 예로 평문 $m' = m + \langle 1,1,\ldots,1 \rangle$ 의 암호문 $c'$는 다음과 같이 생성될 수 있다.

$$c' = c + \langle 1,\ldots,1 \rangle G'$$
$$= (m + \langle 1,\ldots,1 \rangle)G' + e = m'G' + e$$

④ Reaction 공격 방법 : 약한 선택 암호문 공격 (Chosen Ciphertext Attack)

공격자는 해독하고자 하는 암호문 $c$의 몇 비트들을 바꾼 후, 그것을 수신자에게 보내고 그 반응을 살펴본다. 만약 수신자가 메시지를 다시 보내 달라고 요청한다면 바꾼 비트들이 오류 벡터의 무게를 증가시켰다는 사실을 얻어낼 수 있다. 그렇지 않다면, 오류 벡터의 무게가 비트 변환 후에도 50을 초과하지 않는다는 사실을 알 수 있다. 따라서, 공격자는 오류

벡터에서 오류가 있는 위치를 추측해 낼 수 있고, 그 후에 오류가 없는 $k$개의 행을 선택하여 유형 2의 ① 번 공격방법으로 평문 $m$을 복원할 수 있다.

⑤ 평문의 일부분을 알 때의 공격방법(Known partial plaintext attack)

평문의 일부분을 알고 있을 때 완전한 평문을 얻어내는 것은 그렇지 않을 때 보다 적은 계산량을 필요로 한다. 평문 $m$중에서 알고 있는 $k_l$비트를 $m_l$이라 놓고 모르는 부분의 $k_r$비트를 $m_r$이라 놓으면 $m=(m_l \| m_r)$이다. 이 때 $m_r$을 복원하는 데 필요한 계산량은 $k_r^3 {}_nC_{k_r} / {}_{n-t}C_{k_r}$가 된다. 또한 평문의 일부분의 정보와 Canteaut가 제안한 확률적 복호(decoding) 알고리즘[1]을 같이 이용하면 계산량을 감소시킬 수 있다.

## Ⅲ. 초타원 함수체, 대수기하 부호

### 3.1 초타원 함수체

지금부터 소개할 대수기하 부호에 관한 내용은 부호 자체가 가진 오류수정기능이 아니라 McEliece 암호시스템에 적용되었을 때 고려할 수 있는 공격방법들에 대한 안전성 여부에 중점을 둔다. 또한 공개키의 크기를 줄이는 동시에 안전성을 보장하기 위한 최적의 오류 벡터 크기를 제안한다.

$q=p^m$ : $p\neq 2,3$ 인 소수
$K=F_q$ : $q$개의 원소를 가진 유한체
$\overline{K}=\cup F_q^m$ : $K$의 대수적 폐체
$F/K$ : $K$상에서 대수적 함수체
$P_F$ : $F$의 Place 들의 집합
$P_F^{(k)}$ : $F$안에 있는 $k$차의 Place 들의 집합

◇ 정의 및 기호

* Place $P\in P_F^{(1)}$와 $ord_p(u)\geq 1$인 $u\in F$에 대하여 $u(P):=u+P\in K$ 값이다.

[Proposition 1] $p\neq 2,3$ 인 경우

1) $F/K$는 genus가 $g$인 초타원 함수체이다. 이때 다음을 만족하는 $x, y\in F$ 가 존재한다.
$F=K(x,y)$이고 $d$는 $2g+1$ 또는 $2g+2$인 제곱이 아닌 수이다. 다항식인 차수가 $d$인 함수 $f(x)\in K[x]$가 존재하여 다음을 만족한다.

$$E(x,y)=y^2-f(x)=0 \qquad (3.1)$$

2) 반대로 만약 $F=K(x,y)$이고 제곱 다항식이 아닌 차수가 3 이상인 $f(x)\in K[x]$에 대하여 $y^2=f(x)\in K[x]$라면 $F/K$는 genus $g$가 아래와 같은 초타원 곡선이다.

$$g=\begin{cases}(d-1)/2 & \text{if } d\equiv 1 \mod 2\\ (d-2)/2 & \text{if } d\equiv 0 \mod 2\end{cases}$$

3) $y^2=f(x)$, $F=K(x,y)$라면 place $P\,INP_{K(x)}$ 중
- $\deg(f(x))\equiv 0 \pmod 2$이면 $f(x)$의 모든 근 또는
- $\deg(f(x))\equiv 1 \pmod 2$이면 $f(x)$의 모든 근과 poles인 경우 $F/K(x)$에서 ramify 한다.

증명) 참고문헌 [10]의 pp.188과 pp.194를 참조.

여기서 $d$는 홀수인 경우로 제한한다. 위의 명제에 의해 초타원 함수체 $F$는 초타원 곡선식 $E(x,y)=y^2-f(x)=0$과 대응되어 함수체 $F=K(x,y)$의 원소는 $g(x)+h(x)y$ ($g(x)$, $h(x)$는 $K$계수 다항식)함수의 분수꼴로 표현가능하다. 또한 $x, y\in F$ 원소의 1차 plac $P\in P_F^{(1)}$에서 값은 $x_P:=x(P)$, $y_P:=y(P)$로 $K=F_q$ 상의 원소가 된다. 따라서, 차수가 1인 place $P$는 $x_P$와 $y_P$의 값에 의해 유일하게 결정되어 자연스럽게 $E(x,y)$의 $K$-유리점(rational point)들로 이해할 수 있다.

$F/K$에서 정의된 divisor $D$는 유한개의 place를 제외하고 모든 place $P$에 대해서 $n_P=0$ 인 형식합(formal sum) $D=\sum_{P\in supp(D)} n_P(P)$, $n_P\in Z$이다. divisor $D$의 support는 $supp\,D=\{P\in P_F^k \mid n_p!=0\}$로 정의한다. 이렇게 정의한 divisor들의 집합은 place들에 의해 생성되는 free 교환군(free commutative group)이며 divisor $D$의 차수는 $\sum n_P \deg(P)$로 정의한다. 여기서 $F=K(x,y)=K(E)$로 놓고 $F$의 원소를 유리함수라 하자. 그러면 각각의 place $P\in P_F^{(1)}$에 대해 $v_p(u)=1$인유리함수 $u$(uniformizer of $P$)가 존재하여 모든 $f\in F^*$에 대해 $f=u^d s(s(P)\neq 0, s\in F)$가 성립한다. 이때 $v_p(f)=ord_p(f)=d$이다. Place $P=(x_P,y_P)$, $P=(x_P,0)$와 $P_\infty$ 각각에 대한 uniformizer는 $u=x-x_P$, $u$ $y$ 그리고 $u=x/y$ 이다. 그리고

함수체 위의 원 $f\in F$의 divisor는 $(f):=\sum_P v_P(f)P$로 정의된다.

[Definition 1] $D$가 $F/K$ 위의 divisor일 때 $\overline{K}$ 위의 벡터공간

$$L(D):=\{f\in \overline{K}(E)^* \mid (f)+D\geq 0\}\cup\{O\}$$

이고, 이때 $l(D):=\dim_{\overline{K}} L(D)$이라 하자.

$f,g\in\overline{K}(E)$에 대해 미분형식(Differential Forms)의 공간 $\Omega_E$는 $\overline{K}(E)$의 1차 벡터공간으로 $df$[1]들의 집합이다. $P$를 $m$차의 place라 하면 임의의 $\omega\in\Omega_E$에 대해 $f\in\overline{K}(E)$가 존재하여

$$\omega=fdt \quad (t\text{는 } P\text{에서의 uniformizer})$$

가 된다. $\omega$의 divisor는 $(\omega):=\sum v_P(\omega)P$로 정의되고 $v_P=v_P(f)=\rho$이며, canonical divisor라 부른다. 이때, $\deg((\omega))=2g-2$이다. 또한 위의 함수 $f$가 *Laurent* 시리즈 $\sum_{i=\rho}^{\infty} a_i u^i$를 가질 때

$$res_P(\rho)=Tr(a_{-1}) \quad (Tr\text{는 } trace\ map)$$

으로 정의된다.

[Definition 2] $D$가 $F/K$ 위의 divisor일 때

$$\Omega(D):=\{\omega\in\Omega_E \mid (\omega)-D\geq 0\}\cup\{O\}$$

이다. 이때 $\dim_{\overline{K}} L(D)=l(D)$, $\delta(D)=l(W-D)$라 하면 Riemann-Roch 정리[10]에 의해

$$l(D)=\deg(D)+1-g+\delta(D)$$

을 만족한다.

### 3.2 대수기하 부호

$\overline{F}=\overline{K}(x,y)=\overline{K}(E)$는 genus가 $g$인 대수적 함수체위에서 두 가지 종류의 대수기하 부호를 정의할 수 있다.[10] Divisor $D$는 1차 place들 $P_1,P_2,\ldots,P_n$의 형식합 $D=P_1+P_2+\cdots+P_n$이고, $G$는 $D$와 support가 다른 divisor로 $2g-2<\deg G<n$를 만족한다.

① 일반적인 Reed-Solomon 부 $C(D,G)$ : $F_q$-선형함수 $\alpha: L(G)\rightarrow F_q^n$ 의 상(image)

$$\alpha(f):=(f(P_1),f(P_2),\ldots,f(P_n))$$

으로 다음의 조건을 만족한다.

- $C(D,G)$의 차원 $k=\deg(G)-g+1$
- $C(D,G)$의 최소 거리 $d\geq n-\deg(G)$

② 대수적 Goopa 부호 $C^*(D,G)$ : $F_q$-선형함수 $\alpha^*:\Omega(G-D)\rightarrow F_q^n$ 의 상

$$\alpha^*(\eta):=(resP_1(\eta),resP_2(\eta),\ldots resP_n(\eta))$$

으로 다음의 조건을 만족한다.

- $C^*(D,G)$의 차원 $k^*=n-\deg(G)+g-1$
- $C^*(D,G)$의 최소거리 $d\geq\deg(G)-2g+2$.

이때, ① 과 ② 부호는 쌍대부호이다.[10]

## Ⅳ. 새로운 McEliece 유형의 공개키 알고리즘

### 4.1 개선된 McEliece 유형의 공개키 알고리즘

이 절에서는 충분한 안전성을 보장하기 위해 $q=491$인 유한체 $F_q$와 파라메터 [400,312]를 가지는 초타원 곡선에서 정의된 대수기하 부호를 이용한 새로운 McEliece 유형의 암호시스템을 제안하고 키 생성, 암호화, 복호화 방법을 설명한다. 소프트웨어 구현을 통해 기존의 McEliece 암호시스템과 암,복호화 속도를 비교한다. 본 논문에서 제시하는 McEliece 유형 암호시스템의 기본적인 형태는 다음과 같다.

비밀키 : $C^*(D,G)$ 의 생성행렬 $G^*$
$F_{491}$ 원소를 갖는 $312\times 312$ 정칙행 $S$
$\phi\in S_{400}$ : $SC^*$의 행을 치환시키는 함수
$400\times 400$ 치환행렬 $P$로 볼수있다.
$e\in F_{491}^n$ 무게(weight)38인 오류벡터

1) $f\in\overline{K}(E)$, $d$는 derivation map $K$-선형함수로써 Leibniz 조건을 만족한다.

공개키 : $\phi(SG^*) = SG^*P$

#### 4.1.1 키 생성( Key Generation)

을은 genus $g \leq 6$인 400개 이상의 1차 place 갖는 $F_{491}$ 위에서 정의된 초타원 곡선 $E_A : y^2 = f(x)$를 선택한다. $P_\infty$을 제외한 400개의 place들을 이용하여 divisor $D = P_1 + ,.. + P_{400}$와 support가 다른 degree가 $87+g$인 divisor $G = n_\infty P_\infty + \sum n_Q Q$ ($n_Q \geq 1$ , $n_\infty \geq 2g+2$)를 선택한다. 그리고 앞 장에서 소개한 대수기하 부호 생성방법으로 오류 수정 능 $t$가 38인 $C^*(D, G) = [400, 312]$ 부호를 생성한다. 이때 선형함수 $\alpha^*$를 구하는 것이 어려우므로 먼저 $L(G)$의 기저[11]를 이용하여 $C(D, G) = [400, 88]$ 부호를 생성한 후 비밀키 $C^*(D, G)$는 $C(D, G)$의 nullspace로 계산한다. 또한 비밀키를 숨기기 위한 크기가 $312 \times 312$인 $F_q$ 계수의 정칙 행렬 $S$와 순환 함수(permutation) $\phi$(One line expression 사용)를 선택하고 자신의 공개키로 오류 수정 능력이 $t = 38$인 행 $\phi(SC^*(D, G))$을 공개한다.

#### 4.1.2 암호화 방법(Encryption)

갑은 을의 공개키 행렬을 선택하여 평 $m$을 곱한 $(m)\phi(SG^*))$에 오류벡터를 더한 값을 암호문으로 을에게 전송한다. 즉, 암호문 $c = m\ \phi(SG^*) + e$

#### 4.1.3 복호화 방법(Decryption)

전송된 암호문을 해독하는 과정은 McEliece 암호 시스템과 동일하다. $\phi$ 함수는 entry가 1인 $400 \times 400$ 치환행렬 $P$ 이다. 따라서, $eP^{-1} = \phi^{-1}(e)$의 무게(weight) 또한 38로 변함없다. 복호화 과정은 아래와 같다.

복호화 : $c \in m\phi(SG^*) + e = m(SG^*P) + e$,
$P$는 치환행렬
$cP^{-1} = (mS)G^* + eP^{-1}$
$G^* = C^*(D, G)$의 빠른 복호 알고리즘을 이용하여 오류 $eP^{-1}$를 고치고, $mS$ 값을 얻는다. 평문 $m$은 $(mS)\ S^{-1}$로 복원된다.

위에서 오류를 수정하는 과정(부호의 복호 과정)에서 $O(n^3)$의 계산량을 갖는 알고리즘을 사용한다.[10] 본 논문에서 제안된 암호시스템의 파라메터는 이 알고리즘이 수정할 수 있는 오류 수정 능력 $t = 38\left(\leq \frac{d^* - 1 - g}{2}\right)$를 만족한다. 다음은 잘 알려진 대수기하 부호의 복호 알고리즘을 새로운 시스템의 파라메터에 적용한 것이다.

**[초타원 부호의 복호화 알고리즘]**

$c \in F_q^n$와 $f \in L(G)$의 오증(syndrome)을

$$[c, f] := \sum_{i=1}^{n} c_i \cdot f(P_i)$$

으로 정의한다. 그리고 $t = \lfloor \frac{d^* - 1 - g}{2} \rfloor$ 일 때, 아래 세 가지 조건을 만족하는 divisor $G_1$은 존재한다.

1. $supp G_1 \cap supp D = \emptyset$
2. $\deg(G_1) < \deg(G) - (2g-2) - t$
3. $l(G_1) > t$

① Precomputation
파라메터 $g = 6, l = 39, k = 44, m = 88$ 일 때 다음 세 개 벡터공간 기저들을 구해 놓는다.

$L(G_1)$의 기저 $\{f_1, f_2, ..., f_l\}$,
$L(G - G_1)$의 기저 $\{g_1, g_2, ..., g_k\}$,
$L(G)$의 기저 $\{h_1, h_2, ..., h_m\}$,

② 알고리즘(오류 위치 찾기)
INPUT : $a = c + e$ (전달된 message)
PROC : 선형방정식

$$\sum_{j=1}^{l} [a, f_j g_i] \cdot x_j = 0 \quad i = 1, 2, ...k$$

을 푼다.
OUTPUT : $f = \sum_{j=1}^{l} a_j f_j \in L(G_1)$, $(a_1, a_2, ..., a_l)$ 은 0이 아닌 해

이렇게 구해진 함수 $f$는 오류의 위치를 알려주는 함수이다. 즉, 오류 위치 집합 $I = \{v \mid 1 \leq v \leq n \text{ and } e_v \neq 0\}$의 원소 $\nu \in I$ 에 대하여 $f(P_\nu) = 0$이 된다.

$N(f) = \{\nu \mid 1 \leq \nu \leq n \text{ and } f(P_\nu) = 0\}$라 하자. 오류 위치를 구한 후에 실제 오류의 값을 찾기 위한 알고리즘은 다음과 같다.

③ 알고리즘(오류 값 찾기)
INPUT : $L(G)$와 앞의 알고리즘의 결과인 집합 $N(f)$
PROC : 선형 방정식

$$\sum_{\nu \in N(f)} h_j(P_\nu) \cdot y_\nu = [a, h_j], \quad j = 1, 2, \ldots m$$

의 해 $(e_\nu)_\nu \in N(f)$를 구한다.
OUTPUT : 오류 값은

$$e_\nu = \begin{cases} e_\nu & \nu \in N(f) \\ 0 & \nu \notin N(f) \end{cases}$$

이며 $w(e) = 38$일 때, 원래 message는 오류 값을 제거한 $c = a - e$로 복원된다.

#### 4.1.4 암호화, 복호화 속도 비교(구현)

이 소절에서는 이진 [2048,1608,101] Goppa 부호를 이용하는 McEliece 암호시스템과 새로 제안된 시스템 그리고, RSA ( $e = 17$)의 구현을 통해 각각의 암호화, 복호화 속도를 비교한다. 각 암호 알고리즘의 구현은 Linux(mandake)를 운영체제로 가지는 Intel Pentium III-800MHz, 128 RAM을 장착한 컴퓨터에서 gcc 버전 2.95.3을 이용하여 컴파일하였다. RSA 속도 측정을 위해 암호화는 open_ssl (버전 0.9.5a)에 들어있는 bignum library를 사용하였고, Pentium Ⅲ에서 최적화된 컴파일 옵션을 사용하였다. 빠른 암호화 속도를 측정하기 위해서, 암호화는 $10^9$번, 복호화는 $10^3$번 시행한 시간을 초(second)로 표현하였다. [표 2]는 각 알고리즘의 구현 결과를 기록한 것이다.

이 표에서 알 수 있듯이, 새로 제안된 암호시스템이 오히려 이진 부호를 이용하는 McEliece 암호보다 더욱 빠른 암·복호화가 가능하다. 우선 새로운 시스템의 암호문은 $F_q$ ($q = 491$)의 원소로 이루어진 $1 \times 312$ 행렬과 $312 \times 400$ 행렬의 곱은 312번의 정수 곱셈과 한번의 mod 491 연산을 총 400번하여 얻어지게 된다. 그러나, McEliece 암호시스템의 암호문은 비트 표현으로 이루어진 $1 \times 1608$ 행렬과 $1608 \times 2048$ 행렬의 곱이다. 32비트를 정수(integer) 1개로 표현하면, 암호문이 정수의 논리곱연산(and 연산) 51번을 2048번 반복하여 얻어지게된다. 즉, 비트 연산이 많아지면 오히려 정수연산보다 느리기 때문에 암호화가 느려진다는 것을 알 수 있다. 적절한 $q$(=491)진 부호를 사용하면 이진 부호를 사용할 때보다 유형 2의 첫 번째 공격 계산량을 증가시키고 암호화 속도도 향상됨을 확인 할 수 있다.

McEliece 암호시스템의 복호화는 [16, 144p]에 소개된 복호(decoding) 알고리즘을 사용하여 구현하였고, 새로 제안된 암호시스템은 앞에서 소개한 (IV.1.3) 복호(decoding) 알고리즘으로 구현하였다. 아래 구현결과는 아직 최적화 된 값은 아니지만, 오히려 제안된 시스템이 복호(decoding)할 때 풀어야 하는 두 개의 선형방정식을 더욱 빠른 알고리즘을 이용하여 구현할 수 있기 때문에 McEliece 암호시스템의 구현보다 더욱 최적화가 가능하다.

### 4.2 기반이 되는 안전성 및 공격방법

새로운 시스템은 임의의 $q$진 부호를 복호(decoding)하는 것이 NP-complete 문제임에 기반하고 있으며 동시에 충분한 크기의 키 공간을 가지고 있기 때문에 전수조사에 안전하다. 앞에서 제시한 McEliece 암호시스템의 공격방법을 그대로 적용해도 안전할 뿐만 아니라 일반적인 공격방법인 유형 2의 ㉠과 ㉡의 경우에 대해서는 더욱 안전한 것을 [표 3]에서 확인 할 수 있다.

#### 4.2.1 키 공간[11]

① [400,312] 초타원 부호집합에 동치관계 $R(A, B)$를 $\phi \in S_{400}$가 존재하여 $A = \phi(B)$인 경우로 정의하자. $F_q$ 상의 $400 \times 400$ 치환 행렬 $P$를 이용하여 비밀키 $G$를 숨기는 것( $PG$ 계산)이 안전해 보이나 실제 $S_{400}$의 크기가 $400! = 2^{2886}$으로 충분하므로, 치환함수 $\phi(SG)$를 이용하여 $G$를 숨

[표 2] 암호화 복호화 속도 비교(단위 : 초(s))

| | 초타원 부호 $q = 491$[400,312] $t = 38$를 이용한 새로운시스템 | 이진 Goppa 부호 [2048,1606,81] 이용한 McEliece 시스템 | RSA-1024 (e=17) |
|---|---|---|---|
| 암호화 $10^9$번 시행 | 116.00 | 573.44 | 36599.99 |
| 복호화 $10^3$번시행 | 3.61 | 4.19 | 24.82 |

〔표 3〕 오류 수정 부호에 기반을 둔 PKC의 공격 계산량

| | 초타원 부호 $q=251$ 〔200, 108〕 $t=42$를 이용한 새로운 시스템 | 이진 Goppa 부호 〔1024, 524, 101〕를 이용한 McEliece 시스템 | 초타원 부호 $q=491$〔400,312〕 $t=38$를 이용한 새로운 시스템 | 이진 Goppa 부호 〔2048, 1608,81〕를 이용한 McEliece 시스템 |
|---|---|---|---|---|
| 공개키 | 21,600 Bytes | 67,072 Bytes | 140,400 Bytes | 411,648 Bytes |
| 비밀키 | 11,864 Bytes | 34,450 Bytes | 109,962 Bytes | 323,454 Bytes |
| Transmission rate | 54% | 51.17% | 78% | 78% |
| $W_1$(유형 2, ㉠) | $2^{85.79}$ | $2^{80.71}$ | $2^{128.39}$ | $2^{122.78}$ |
| $W_2$(유형 2, ㉡) | $2^{65.04}$ | $2^{64.2}$ | $2^{101.92}$ | $2^{100}$ |

기는 방법도 충분한 안전성을 보장할 수 있다.

② 본 논문에서 선택한 $C^*(D, G)$부호(〔400,312〕, $t=38$)는 부호 동형군 $\{\pi\in S_n \mid \pi(C^*)=C^*\}$과 함수체의 동형군 $Aut_{D,G}(F/K)=\{\sigma\in Aut(F/K) \mid \sigma(D)=D, \sigma(G)=G\}$이 서로 동일하다.[11] 따라서, $\phi$를 취한 후에도 $SG$의 구조가 그대로 드러날 가능성은 $0.2766\times10^{-864}$이므로 충분히 무시할만하다.

③ 키 공간의 크기

갑이 divisor $D, G$를 초타원 곡선 $E_A$: $y^2=x^{13}+x^2+1$에서 선택하였다고 하자. $\#E_A(K)=518$ 이므로 $C^*(D, G)$를 선택하는 방법의 수는 약 $2^{580}$ 이고,

$$C^*(D, G)=C^*(\sigma(D), \sigma(G)),\ \sigma\in Aut(F/K)$$

이므로 최대 $26\times\#E_A(K)\sim2^{14}$개의 $C^*(D, G)$가 부호로서 동일하다. 따라서, 갑이 선택한 임의의 초타원 곡선 $E_A$ 위에서 생성할 수 있는 동치가 아닌 $C^*(D, G)$ 부호는 약 $2^{566}$개이고, $F_{491}$에서 genus $g$가 6인 초타원 함수체가 약 $2^{116}$ 이므로 전체 키 공간은 전수조사 공격을 방어할 정도로 충분히 크다.

#### 4.2.2 공격방법

① 공개키 $G^*$를 분해하는 유형 1의 공격방법은 본 논문에서 제시한 시스템의 키 공간이 충분히 크기 때문에 적용 불가능하다. 그러나 유형 3의 공격방법은 기존의 McEliece 암호시스템의 경우와 마찬가지로 키 크기를 증가시켜도 피할 수 없는 구조적인 문제다. K. Kobara와 H. Imai가 제시한 McEliece 암호시스템에 사용 가능한 변형 방법[7]을 본 논문에서 제시한 새로운 McEliece 유형 암호시스템에 그대로 적용할 수 있고 이를 통해 적응 선택 암호문 공격에 대한 안전성을 보장할 수 있다.

② 가장 일반적인 유형 2의 공격방법의 계산량을 살펴보자. 첫 번째 $G'$로 부터 직접 평문을 얻어내는 방법(유형 2의 ㉠)의 경우에는 McEliece 암호시스템과 같이 $F_q$ 위의 $k\times k$ 행렬의 역행렬 계산을 위해 $(klog(q))^3$의 연산이 필요하므로 ${}_{400}C_{312}/{}_{400-38}C_{312}\times(312\times\log(q))^3=2^{128.79}$의 계산량이 필요하다.

다음으로 최소 무게 부호어를 찾아내는 확률적 알고리즘을 이용한 복호 (decoding) 공격방법[1] (유형 2의 ㉡)을 그대로 제안된 새로운 시스템에 적용했을 때의 계산량을 살펴본다. $\Omega_{p,\sigma}$는 한번 시행에 필요한 계산량, $W_{p,\sigma}$는 알고리즘이 성공하기 위한 총 계산량, $E(N)$는 알고리즘이 성공하기 위해 기대되는 반복회수 그리고, $A_\omega$는 무게가 $\omega$ 인 부호어의 수라 하면 이 공격방법의 계산량은 다음과 같다.

$$\Omega_{p,\sigma} = 2p\sigma_{k/2}C_p(q-1)^p(81+9) + 2p(n-k-\sigma)(81+9)_{k/2}C_p^2/q^\sigma K(p_{k/2}C_p(q-1)^p + q^\sigma) + k(n-k)(81+9)$$

$$W_{p,\sigma}=\frac{\Omega_{p,\sigma}E(N)}{A_\omega}$$

계산량( $W_{p,\sigma}$)이 최소가 되는 파라메터는 $p=1$, $\rho=2$ 이고, 그 계산량은 $2^{101.92}$이다(그림 1).

## V. 결론 및 앞으로의 연구

본 논문에서는 참고문헌 〔11〕에서 계산된 $L(G)$의

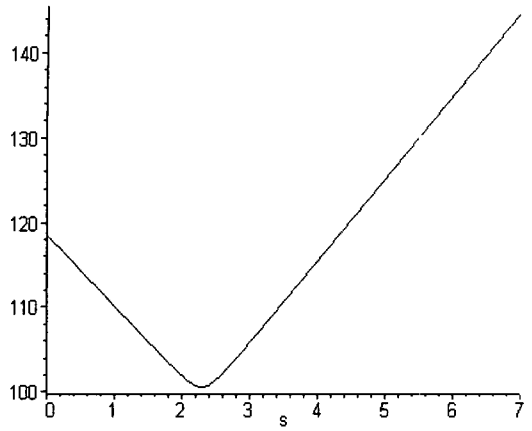

그림 1: 가로 축( $\rho$ 값 ), 세로 축( $\log_2$계산량 )

기저를 이용하면 초타원 부호를 쉽게 생성할 수 있을 뿐만 아니라 이 부호의 동형군(Automorphism Group)이 잘 알려져 있어 키 공간이 충분히 크다는 사실을 이용하여 부호어의 가장 작은 무게 $d$ 가 $n-k-g \leq d \leq n-k+1$ ($g \leq 6$)인 유한체 $F_{491}$위에서 생성된 초타원 부호를 사용한 새로운 공개키 암호시스템을 제안하였다. 이 암호시스템은 기존의 이진 Goppa 부호를 사용하는 McEliece 암호시스템보다 키 크기가 3분의 1로 줄었고, 부호를 이용한 공개키 암호시스템의 최대 장점인 빠른 암호화를 보장하면서 ([표 2]) 복호 공격에 대해 동일한 안전성을 보장할 수 있다 ([표 3]). 또한, 평문을 직접적으로 복원하는 공격방법의 경우는 기존의 경우보다 32배 더 많은 계산량을 필요로 한다.

앞으로는 비단 본 논문에서 제시된 파라메터를 가지는 초타원 부호 뿐만 아니라 위의 안전성 조건에 부합되는 적절한 유한체 $F_q$와 함께 MDS 그리고, Vandemonde 구조를 가지지 않은 대수기하 부호 혹은 다른 유형의 부호를 이용하여 새로운 유형의 암호시스템을 설계하는 방법에 대한 연구도 가능할 것이다. 그리고, Niederreiter 암호시스템과 McEliece 암호시스템은 서로 동치이면서 전자의 경우 암호화의 속도와 키 크기에서 상대적인 이점이 있기 때문에[14] 본 논문에서 제시된 암호시스템에 사용된 부호를 Niederreiter 암호시스템에 적용하는 방법을 생각해 볼 수도 있다.

## 참 고 문 헌

[1] Canteaut, N.Sendrier, "Cryptoanalysis of the Original McEliece Cryptosystem", *In Advances Cryptology ASIACRYPT'98*, pp. 187~199, 1998.

[2] P.W. Shor, "Polynomial-Time Algorithms for Pime Factorization and Discrete Logarithm on a Quantum Computer", *In em Proc. of Coding Theory and Application LNCS 388*, pp. 106~113, 1989.

[3] G.A. Kabatianskii, "On security of McEliece and Niederreiter type cryptosystems", *Lecture delivered at the University of Pureto Rico*, September 1993.

[4] P.Loidreau, "Strengthening McEliece Cryptosystem", *In Advances Cryptology ASIACRYPT'2000. LNCS* 1976.

[5] P.Loidreau, N.Sendrier, "Some weak keys in McEliece public-key cryptosystem", *In Proc. of IEEE International Symposium on Information Theory, ISIT'98*, pp. 382, 1998.

[6] N.Sendrier, "Finding the permutation Between Equivalent Linear codes:The Support Splitting Algorithm", *In IEEE Transactions on Information Theory*, Vol. 46, pp. 1193~1203, 2000.

[7] K.Kobara, H.Imai, "Semantically Secure McEliece public-key cryptosystems - Conversions for McEliece PKC-", 2000.

[8] Berson, T.A, "Failure of the McEliece public-key cryptosystem under Message-resend and related-message Attack", *Advanced in Cryptology - Crypto'97*, pp. 213~220, 1997.

[9] Hung-Min Sun, "Further Cryptanalysis of the McEliece Public-Key Cryptosystem", *In IEEE Transactions on Information Theory*, Vol. 4, 2000.

[10] Henning Stichtenoth, *Algebraic Function Fields and Codes*, 1991.

[11] S.Wesemeyer, " On the Automorphism Group of Various Goppa Codes", *IEEE Transactions on Information Theory*, Vol. 44, No. 2, 1998.

[12] Hun-Min Sun, "Improving the Security of the McEliece Public-Key Cryptosystem",

*In Advances Cryptology ASIACRYPT'98*, pp. 200~213, 1998.
[13] E. Krouk, "A new public key cryptosystem", *Proceedings of the Sixth Swedish-Russian International WorkShop on Information Theroy*, pp. 285~286, 1993.
[14] H. Niederrieter, "Knapsack-Type cryptosystems and algebraic coding theory", *Problems of Control and Information Theory*, Vol. 15, No. 2, 1986, pp. 159~166.
[15] V.M. Sidelnikov, S.O.Shestakov, " On insecurity of cryptosystems based on generalized Reed-Solomon codes", *Diskretnaya Matematika*, Vol. 4, No. 3, 1992.
[16] J. H. van Lint, *Introduction to Coding Theory*, 1991.

## 〈著者紹介〉

**강 보 경 (Bo Gyoung Kang)** 비회원
1999년 8월 : 서울대학교 수학교육학과 졸업
2001년 8월 : 한국과학기술원 수학과 석사 졸업
2001년 9월~현재 : 한국과학기술원 수학과 박사과정
〈관심분야〉 암호학, Coding Theory, 타원곡선

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