부호 기반 McEliece 암호 체계와 안전성 분석

이향숙, 임수민, 임희진
이화여자대학교

요 약

오류 정정 부호(error-correcting code)를 사용하는 McEliece 암호 체계는 양자 컴퓨터에서도 안전한 공개키 암호 기법으로서 주목 받아왔다. 본고에서는 McEliece 암호 체계에 사용되는 오류 정정 부호와 그 조건, 암호 체계의 구조와 그 발전 과정 및 응용을 알아보고, 안전성 분석에 대해 소개한다.

Ⅰ. 서 론

통신문을 부호화(encoding)하여 통신로를 통하여 전달하면 송신된 통신문에 오류가 포함되어 수신자에게 도착한다. 이 경우 오류를 정정하여 원래의 통신문으로 복호(decoding)할 수 있는 체계를 적용하여 사용한다. 이를 이용하여 오류를 제대로 정정할 수 있는 능력을 기반으로 통신문을 안전하게 통신할 수 있는 암호 체계가 제안되었다.

1987년에 처음으로 제안된 McEliece 암호 체계는 효율적인 복호 알고리즘이 존재하는 오류 정정 부호를 비밀키로 사용하는 공개키 암호 체계이다[27]. McEliece는 체계에 선형 오류 정정 부호의 하나인 Goppa 부호(code)를 사용했다. 그러나 효율적인 복호 알고리즘이 알려져 있다고 해서 모든 오류 정정 부호를 암호 체계에 사용할 수 있는 것은 아니다. Goppa 부호 대신 GRS[37], Gabidulin, Reed-Muller, LDPC 등의 다른 오류 정정 부호들을 사용하기 위한 연구들이 있었지만 각 부호가 가지는 구조적 특성 때문에 비밀키를 숨길 수 없는 문제가 있었다[29].

McEliece 암호는 비밀키의 크기가 다른 공개키 암호 체계에 비해 크다는 단점을 가지고 있었지만 양자 컴퓨터에 대한 연구가 진행되면서 다시 주목을 받았다. 그 이유는 양자 컴퓨터 환경에서 소인수분해와 이산로그 문제의 답을 구할 수 있는 Shor의 알고리즘이 제안되어[36] RSA 암호가 안전성을 보장할 수 없음이 밝혀졌지만 McEliece 암호 체계는 격자 암호나 다변량 암호와 함께 양자 컴퓨터의 출현 이후에도 쓸 수 있는 암호로 생각되기 때문이다[29].

본고에서는 McEliece 암호 체계와 그 변형들 및 응용에 대해 서술하고, 공격 알고리즘을 통한 안전성 분석을 정리하였다.

Ⅱ. McEliece 암호 기법과 발전

본 장에서는 McEliece 암호 체계의 기법과 장점 및 한계점을 소개하고 한계점을 보완하기 위해 어떠한 방향으로 발전이 이루어지고 있는지에 대해 살펴본다. 또 McEliece 암호 기법을 이용한 응용에 대해 알아본다. McEliece 암호 체계는 부호이론을 기반으로 설계되었는데 본고에서는 부호이론에 대한 자세한 설명은 하지 않고 필요한 몇 가지 정의들에 대해 간략하게 소개한다.

다음을 만족하는 이진행렬 H가 존재할 때, x를 선형부호(linear code)라고 하고, 이 때 H를 홀짝검사 (parity-check) 행렬이라고 한다[33].

$$Hx^T = 0$$

통신상에서는 이진(binary) 선형부호를 사용하는데, 부호화(encoding) 된 통신문이 통신로를 지나갈 때 오류(error)를 동반하게 된다. 수신된 부호어가 오류를 포함하게 되면 이를 정정하여 복호(decoding)할 수 있는 능력이 필요한데, 이러한 복호 능력을 가진 부호(code)를 오류 정정 부호(error-correcting code)라고 한다.

주어진 두 부호에서 서로 다른 값을 가지는 자리의 개수를 Hamming 거리(Hamming distance)라고 하고, 주어진 부호에서 0이 아닌 자리의 개수를 Hamming 무게(Hamming weight)라고 하는데, 이러한 성질을 가지는 Hamming 부호 중 (7,3,4)-Hamming 부호가 좋은 오류 정정 부호로 알려져 있다. 하지만 (7,3,4)-Hamming 부호는 한 개의 오류만을 허용하기 때문에 실제로 통신 암호체계에서 사용하기에는 안전성의 측면에서 적절하지 않다.

이진 Goppa 부호 중 기약(irreducible) 다항식을 사용하는 경우, 다음과 같은 특징을 가진다[13].

– 최소 거리의 하계를 계산하기 쉽다.

– Goppa 다항식 생성에 대한 정보를 알면 효율적인 오류 정정이 가능하다.

– Goppa 다항식 생성에 대한 정보가 없는 상태에서의 효율적인 오류 정정 알고리즘이 알려지지 않았다.

이와 같은 특징들에 의해 기약 이진 Goppa 부호는 암호 체계에서 사용하기에 좋은 조건을 갖추고 있다.

1. McEliece 암호의 기본 기법

1978년 McEliece에 의해[27] 이러한 Goppa 부호를 오류 정정 부호로 사용한 공개키 암호 체계가 다음과 같이 키 생성(Key Generation), 암호화(Encryption), 복호화(Decryption)의 구성으로 제안되었다[13].

McEliece 기본 암호 기법

▷시스템 파라미터: $t \ll n$인 자연수 n, t

▷키 생성: 주어진 n과 t에 대해 다음과 같은 행렬을 생성한다.

– G: 최소거리가 $d \geq 2t+1$인 (n,k)–이진 부호 g에 대한 $k \times n$–생성행렬

– S: 임의의 $k \times k$–이진 정칙행렬

– P: 임의의 $n \times n$–순열행렬

이 때 $G' = SGP$ 를 계산한다.

▷공개키: (G', t)

▷비밀키: (S, D_g, P). 이 때 D_g는 g에 대한 효율적인 복호 알고리즘이다.

▷암호화:

– $m \in \{0,1\}^k$: 암호화 할 평문

– $e \in \{0,1\}^n$: 무게 t의 임의 벡터

이 때 암호문 c 는 다음과 같이 계산한다.

$$c = mG' \oplus e.$$

▷복호화: 먼저 $cP^{-1} = (mS)G \oplus eP^{-1}$ 를 계산한 후, 복호 알고리즘 D_g를 Hamming 거리가 t인 cP^{-1} 에 적용하여 다음과 같이 계산한다.

$$mSG = D_g(cP^{-1}).$$

G_J 가 정칙인 $\{1,\ldots,n\}$ 의 부분집합을 J 라 하면, 다음과 같이 평문 m을 얻을 수 있다.

$$m = (mSG)_J (G_J)^{-1} S^{-1}.$$

처음 제안된 McEliece 암호 체계[27]에서 제시한 이진 부호 g는 (1024,524,50)–Goppa 부호이다.

이 구조에 생성행렬 대신 홀짝검사행렬을 사용한 Niederreiter 공개키 암호 체계가 있는데, 이 체계는 knapsack type에 속한다. McEliece 암호 체계와 Niederreiter 암호 체계의 안전성은 동치인 것으로 증명되었다[24].

2. 기존의 McEliece 기법의 장점과 한계

인수분해 문제나 이산로그 문제에 기반을 둔 기존의 공개키 암호 체계가 양자 컴퓨터에 의해 쉽게 풀릴 수 있다고 알려진 데에 반해, McEliece 설계는 최근까지도 양자 컴퓨터에서도 안전성이 보장된다는 장점을 가지고 있다[29].

하지만 McEliece 설계에서 공개키를 생성할 때 Goppa 부호를 사용한다는 점 때문에 McEliece 암호 체계의 공개키의 크기가 너무 크다는 단점을 가지고 있다[29]. 초기에 McEliece 암호 체계가 제안되었을 때에는 공개키의 크기가 큰 성질이 당시의 컴퓨터 기술에서 실제로 이 체계를 사용할 때 너무 많은 용량을 차지하기 때문에 실제 사용에 문제가 있었다. 약 30년이 지난 현재의 컴퓨터 기술에서는 소요되는 용량에 대한 부담이 훨씬 줄어들었다. 하지만 공개키의 크기를 줄이는 것이 McEliece 암호 체계의 효율성에 있어서 큰 차이를 가지기 때문에 여전히 공개키의 크기를 줄이려는 노력은 계속되고 있다[3].

3. McEliece 암호 시스템의 개선 및 발전

McEliece 암호 체계를 개선하기 위한 연구는 2000년대에 이르러 활발해졌다. 이러한 연구 방향은 크게 두 가지로 나눌 수 있는데, 공개키의 크기를 줄이는 방향과 안전성에 있어서 의미론적으로 안전(semantically secure)하도록 설계를 고치는 방향이 있다.

공개키의 크기를 줄이는 방법에 대한 연구는 Goppa 부호의 자기동형군(automorphism group)을 이용[25]하거나 준순환(quasi–cyclic) 부호를 이용[19]하는 방법이 있다. 이 중 자기동형군을 이용한 방법은 깨졌지만[22] 대신 Goppa 부호의 부분류(subclass)를 사용하는 방법이 제안되었다. 하지만 Goppa 부호의 부분류를 사용할 때는 비밀키의 정보가 노출되는 것을 이용한 구조 공격(structural attack)에 취약해진다는 단점[14]을 가지게 된다. 이후 연구에서는 Generalized Srivastava 부호와 같이[32] Goppa 부호에서 특별한 매개변수를 선택(special parameter selection)하면서 가지는 상위 류(class)로서의 부호를 적용하여 공개키의 크기를 줄이면서도 구조 공격에 대한 안전성을 보장하고 있다.

준순환 부호를 사용하는 방법은 지금도 계속해서 연구가 많이 진행되고 있는 편이다[29]. 최근의 연구 중 MDPC(Moderate Density Parity–Check) 부호를 사용한 McEliece 암호 체계의 설계를 제안한 논문[28]에서는 MDPC 기법을 통해 안전성 수준을 높였을 뿐 아니라 준순환 구조를 적용함으로서 80 비트의 안전성 수준(security level)을 가지는 공개키의 크기를 4801 비트까지 줄일 수 있음을 보였다.

의미론적으로 안전한 방향으로 McEliece 설계를 개선하려

는 연구들은 주로 CCA2-security(security against adoptive Chosen Ciphertext Attack)를 보장하기 위하여 체계의 설계를 보완하고 있다. CCA2-secure한 전환을 사용하면 기존의 McEliece 기법이 재전송 공격(resend attack)[9]이나 부분노출 평문공격(partially known plaintext attack) 등에 취약하다는 단점을 피할 수 있다[41].

CCA2-security를 만족하는 포괄적 전환(generic conversion)은 대표적으로 Pointcheval[34], Fujisaki와 Okamoto[17], 그리고 Kobara와 Imai[21]에 의한 연구가 있다. Kobara와 Imai의 연구는 Pointcheval의 연구를 발전시킨 것과 Fujisaki와 Okamoto의 연구를 발전시킨 것이 있는데, 두 가지 전환들에 대하여 아직까지 효율적인 공격이 알려진 것이 없다. 하지만 공격자가 오류가 없는 통신문의 전문을 복호하지 않고, 이 통신문의 일부를 확인할 수 있으면 McEliece 암호 체계의 모든 전환에 일반적으로 적용할 수 있는 공격이 있다[41].

2010년의 Bernstein의 연구[6]는 이 연구들과는 달리 작은 F_q에 대한 부분체(subfield) 부호인 "wild Goppa 부호[40]"를 이용하여 오류 정정을 가능하게 하는 요소의 값을 $\frac{q}{q-1}$까지 높이는 McEliece 암호 체계를 설계 하고, 이 체계의 이름을 "Wild McEliece"라고 붙였다. 기존의 McEliece 체계에서 사용하는 Goppa 부호는 F_{2^m} 상에서 만들어지기 때문에 부호어(code word)들이 F_2의 원소들로만 이루어진다. 이 설계를 $q > 2$인 소수멱체(prime power field) F_q에 적용하면 information set 복호에서의 안전성 수준은 그대로 유지하면서 공개키의 크기가 줄어든다[31]. 하지만 소수 q의 값이 3이나 4인 경우에는 $q = 2$인 경우에 비해 공개키의 크기가 줄어드는 효과가 더 적은 편이고, q가 31정도로 큰 경우에만 이러한 효과가 충분히 나타난다[6]는 한계가 있다.

Goppa 부호를 키 생성에 이용하면 비밀키 G를 생성할 때 사용되는 Goppa 다항식을 뽑을 수 있는 선택의 폭이 크기 때문에 안전성이 보장된다. 기존의 wild McEliece에서 공개키의 크기를 줄인 정도를 같게 하면서 선택의 폭의 크기에 의존하여 안전성이 보장되는 정도가 줄어들지 않게 유지하는 방법에 대한 Bernstein의 연구[7]에서는 이전의 연구[6]과 크게 다르지 않은 정도의 체 크기(field size) 범위 내에서 연구되었는데, q의 크기가 $2, 3, \ldots 32$인 경우에 대하여 다루었다.

4. McEliece 암호 기법의 응용

McEliece와 같은 부호 기반 암호 체계로는 서명 기법을 만들 수 없다고 알려져 있었다. 하지만 2001년에 Courtois, Finiasz, Sendrier이 이 사실이 틀렸음을 증명하며 McEliece 암호 기법의 응용으로 McEliece 서명 기법을 제안했다[12]. 이 서명 기법은 McEliece라는 이름을 가지고는 있지만 실제로는 기존의 McEliece 암호 기법보다는 Niederreiter의 암호 기법을 기반으로 설계되었다. 하지만 신드롬 복호 문제(Syndrome decoding Problem)로 환원(reduce)되는 실용적인 부호 기반 전자 서명 기법을 처음으로 제안했다는 것에 의미가 있다[16].

기존의 McEliece 암호 체계를 양자 컴퓨터 환경에서도 사용할 수 있는 방법이 요구되면서 quantum McEliece 공개키 암호 체계가 제안되었다[18]. 이 체계는 키 생성, 암호화, 복호화 과정을 가지는 기존의 McEliece 암호 체계와 흡사한 구조를 이루고 있고, 기본적으로 stabilizer 부호 이론에 기반을 두고 있다. 하지만 Goppa 부호를 사용한 기존의 McEliece 기법과는 달리 quantum McEliece 기법에서는 GRS 부호에 기반한 CSS(Calderbank - Shor-Steane)부호를 사용하였다.

Ⅲ. 안전성 검증(Cryptanalysis)

본 장에서는 McEliece 암호 체계의 안전성에 대해서 살펴본다. McEliece 암호 체계의 안전성은 다음의 두 가지 가정에 기반을 둔다[29].

- 체계에 사용된 오류 정정 부호가 임의의 선형 부호와 구분 불가능함
- 일반적인 선형 부호의 복호가 어려움

이 두 가정은 엄밀히 증명된 것은 아니지만 여러 시도를 통해 사실이라 믿어지는 명제들이다. 따라서 McEliece 암호 체계의 안전성을 검증하고자 할 때는 사용된 오류 정정 부호가 임의의 선형 부호와 구분이 불가능함을 보이거나 일반적인 선형 부호를 복호하는 가능한 알고리즘이 충분히 효율적이지 않음을 보인다. 현재까지는 McEliece 암호 체계는 디지털 컴퓨터와 달리 Grover 알고리즘이나 Shor 알고리즘도 사용할 수 있는 양자 컴퓨터에서도 안전한 것으로 알려져 있다[5]. 이 외에도 체계를 실제로 사용하는 데 있어서 물리적으로 정보를 얻어내는 부채널 공격(side-channel attack)도 시도되곤 한다. 신드롬의 역에 Timing 공격을 하거나[39] 다항식 값매김 공격(polynomial evaluation attack) 등 다양한 시도가 있었다[2].

1. 오류 정정 부호와 임의의 선형 부호간의 구분불가능성

오류 정정 부호를 아무 조건 없이 McEliece 암호 체계에 사용할 수 있는 것은 아니다. 이를 McEliece 암호 체계에 적용하기 위해서는 다음의 두 조건을 만족해야한다.

오류 정정 부호 g의 생성행렬 G를 알 때 효율적인 복호 알고리즘 D_g가 존재함

G를 알지 못하면 G'과 암호문 c만을 통해 g에 대한 복호가 어려움

즉, 암호화와 복호화 계산이 효율적으로 가능해야하는 동시에 McEliece 체계에서 공개키 G'과 암호문 c만으로 평문 m을 얻을 수 없어야한다. 두 번째 조건에서 G'과 g를 통해서 G를 복원할 수 있다면 임의의 선형 부호 g'과 g는 구분 가능하다. G를 직접 구하지 않고 복호하는 방법은 2절에서 소개하기로 한다.

1978년 제안된 McEliece 암호 체계는 Goppa code를 사용하고 있다. 일반적인 Goppa 부호가 임의의 선형 부호와 구분이 불가능하다는 것을 증명하는 것은 여전히 어려운 문제이다[35]. 그러나 종수가 낮은 초타원곡선을 사용해 만들어진 Goppa 부호에 대해서는 다항식 시간(polynomial-time)의 복잡도를 가지는 효율적인 복호 알고리즘이 제안되었다[15].

그 후로 다른 오류 정정 부호들에 대해서도 McEliece 암호 체계에 사용하기 위한 꾸준한 시도가 있었지만 GRS[37], Gabidulin, Reed-Muller, LDPC 등의 부호들은 구조적으로 임의의 선형 부호와 구분이 가능해 G'으로부터 대체 비밀키 G''을 알아낼 수 있어 안전성에 문제가 있는 것으로 판명되었다[29].

2. 일반적인 선형 부호의 복호 알고리즘 (Information set 복호)

이 절에서는 일반적인 선형 부호를 복호하기 위한 공격인 information set 복호를 소개한다. 이 방법이 발표된 이후 여러 변형을 통해 발전해 왔지만 여전히 알려진 방법들은 모두 지수 시간(exponential-time)의 복잡도를 가지기 때문에 McEliece 암호 체계를 효율적으로 공격할 수 없다. Information set 복호 방법은 다음과 같은 공격법이다[13].

Information Set 복호

▷입력: G', c
▷출력: m

행렬 G'의 n개의 열 중 임의의 k개를 선택한 집합을 $\mathcal{J}$라 하고 G'의 i열들($i \in \mathcal{J}$)을 모은 행렬을 $G_{\mathcal{J}}$, c의 i열들($i \in \mathcal{J}$)을 모은 벡터를 $c_{\mathcal{J}}$라 한다.
$c \oplus c_{\mathcal{J}} G_{\mathcal{J}}^{-1} G'$을 계산한 값을 이용해 m을 구한다.

이 방법은 복잡도를 개선하기 위해 신드롬 복호와 낮은 무게 벡터(low weight vector)를 찾는 알고리즘과 접목된다. 신드롬(syndrome)이란 부호의 $k \times n$-생성행렬 G마다 G로 생성된 $n \times n$-홀짝검사 행렬 H를 이용해 임의의 벡터 x에 따라 Hx^T를 계산한 값을 의미한다. 신드롬 복호(syndrome decoding)란 암호문의 신드롬 값을 구하고 오류가 없을 때 부호의 신드롬이 0임을 이용한 복호 방법이다. McEliece 체계의 암호문 $x(=mG' \oplus e)$의 신드롬을 계산하면,

$$Hx^T = H(mG' \oplus e)^T = H(mG')^T \oplus He^T = He^T$$

를 만족하는데, e는 무게가 t 이하인 오류 벡터이므로, $x - mG'$를 낮은 무게 벡터로 만드는 메시지 m을 빠르게 찾는 것이 곧 McEliece 암호 체계를 복호화 하는 것과 같다.

여기서 오류 벡터를 찾은 후 오류 벡터를 포함하지 않는 벡터들로 information set을 구성하면 더 빠르게 information set 복호를 수행할 수 있다.

현재 알려진 복호 알고리즘들은 모두 비효율적이지만 변형되고 개선되면서 처음 McEliece가 제시한 공격 알고리즘과 비교하면 복잡도가 줄어들었다. 공격 알고리즘들의 주요한 보완 및 개선 알고리즘은 다음과 같다.

1988년에 McEliece의 공격[27]을 일반화, 체계화한 Lee-Brackell 알고리즘[23]이 발표되었고, Stern이 meet-in-the-middle 공격 방식을 적용한 collision 알고리즘을 제시해 공격 알고리즘의 계산량을 줄였다[38]. 1998년에는 Stern의 알고리즘이 가우스 소거법 때문에 계산량이 큰 것을 개선한 Canteaut-Chabaud 알고리즘이 발표되었다[11]. 그 후 2008년에 발표된 Bernstein, Lange, Peters의 새로운 알고리즘은 Stern의 알고리즘을 일반화한 것으로 복잡도는 여전히 지수시간이었지만 McEliece의 초기 파라미터 (1024, 524, 50)-부호의 복호를 적당한 시간 안에 복호 가능한 정도까지 계산량을 줄였다[4]. 2011년에는 Bernstein, Lange, Peters가 Stern의 알고리즘을 일반화하여 Ball-collision 복호법을 발표했다[8]. 2011년에 May, Meurer, Thomae가 이전의 연구[20]에 소개된 부분합 표현 기술(subset sum representation technique)을 사용하는 기법으로 복호를 가속화시켰다[26].

다음 표는 위에서 언급한 복호 알고리즘들의 (1024,524,50)-부호 복호에 필요한 비트 계산량을 정리한 표이다.

년도	알고리즘	계산량
1986	McEliece [27]	$2^{80.7}$
1988	Lee-Brickell [23]	$2^{70.89}$
1989	Stern [38]	$2^{66.21}$
1998	Canteaut-Chabaud [11]	$2^{64.1}$
2008	Bernstein-Lange-Peters [4]	$2^{60.4}$
2011	Ball-collision [8]	$2^{49.69}$
2011	May, Meurer, Thomae [26]	$2^{38.74}$

Bernstein, Lange, Peters의 연구와 실험 결과에 따르면 컴퓨터 성능을 생각할 때 비트 계산량이 2^{60}정도로는 안전한 파라미터라고 생각할 수 없다[4].

따라서 (1024,524,50)보다 큰 파라미터를 선택해야 한다. 그러나 전체적인 복호 알고리즘 복잡도는 여전히 지수시간이기 때문에 파라미터를 교체함으로써 안전성을 확보할 수 있다.

이 밖에 낮은 무게 벡터를 찾는 효율적인 알고리즘을 설계하는 데에는 이미 알려진 다양한 방법이 활용되기도 했다. 2010년 Bernstein이 양자 컴퓨터에서 사용가능한 Grover 알고리즘을 이용해 양자컴퓨터에서 information set 복호를 가속화하는 방법을 제안했고[5], 오류 벡터를 직접 찾는 통계적 알고리즘[1]이나 낮은 무게 벡터를 찾는 것을 격자에서 SVP (Shortest vector problem) 문제로 환원해서 해결하는 방법이 제안되기도 했다[10].

Ⅳ. 결 론

McEliece 암호 체계는 오류 정정 부호의 생성행렬을 비밀키로 사용하는 공개키 암호 체계로서, 암호화와 복호화의 계산이 효율적이고 디지털 컴퓨터 뿐만 아니라 양자 컴퓨터에서도 효율적인 공격 알고리즘이 제안된 바 없어 안전한 것으로 알려져 있다. 최근에는 McEliece 암호 체계의 공개키 크기를 줄여 공간 효율성을 개선하고 의미론적인 안전성을 강화하는 방향의 연구들이 진행되고 있다.

본고에서는 이러한 McEliece 암호 기법과 그 특성을 살펴보며 그 발전 방향을 소개하였다. 더불어 McEliece 암호 체계의 안전성에 대해 정리하였다.

Acknowledgement

이 논문은 한국연구재단의 이공계중점연구소사업 지원을 받아 작성되었음(과제번호: 2009-0093827)

참 고 문 헌

[1] Al Jabri A. Kh. "A statistical Decoding Algorithm for General Linear Blockl Codes," IMA Int. Conf., volume 2260 of Lecture Notes in Computer Science, Springer (2001), pp. 1-8.

[2] Avanzi R., Hoerder S., Page D., and Tunstall M. "Side-Channel Attacks on the McEliece and Niederreiter Public-Key Cryptosystems," Journal of Cryptographic Engineering 1(4) (2011), pp. 271-281.

[3] Berger T. P., Cayrel P., Gaborit P., and Otmani A. "Reducing Key Length of the McEliece Cryptosystem," AFRICACRYPT, volume 5580 of Lecture Notes in Computer Science, Springer (2009), pp. 77-97.

[4] Bernstein D. J., Lange T., and Peters C. "Attacking and defending the McEliece cryptosystem," PQCrypto, volume 5299 of Lecture Notes in Computer Science, Springer (2008), pp. 31-46.

[5] Bernstein D. J. "Grover vs McEliece," PQCrypto, volume 6061 of Lecture Notes in Computer Science, Springer (2010), pp. 73-80.

[6] Bernstein D. J., Lange T., and Peters C. "Wild McEliece," Selected Areas in Cryptography, volume 6544 of Lecture Notes in Computer Science, Springer (2010), pp. 143-158.

[7] Bernstein D. J., Lange T., and Peters C. "Wild McEliece Incognito," PQCrypto, volume 7071 of Lecture Notes in Computer Science, Springer (2011), pp. 244-254.

[8] Bernstein D. J., Lange T., and Peters C. "Smaller decoding exponents: ball-collision decoding," CRYPTO, LNCS vol 6841 (2011), pp.743-760.

[9] Berson T. A. "Failure of the McEliece Public-Key Cryptosystem Under Message-Resend and Related-Message Attack," CRYPTO, volume 1294 of Lecture Notes in Computer Science, Springer (1997), pp. 213-220.

[10] Brickell E. F., and Odlyzko A. M. "Cryptanalysis: A survey of recent results," Proc. of IEEE '88, vol. 75, pp578-593.

[11] Canteaut A., and Chabaud F. "A new algorithm for Finding Minimum-Weight Words in a Linear Code: Application to McEliece's Cryptosystem and to narrow-sense BCH codes of length 511," IEEE Transactions on Information Theory, 44(1) (1998), pp. 367-378.

[12] Courtois N., Finiasz M., and Sendrier N. "How to achieve a McEliece-based Digital Signature Scheme", ASIACRYPT, volume 2248 of Lecture Notes in Computer Science, Springer (2001), pp. 157-174.

[13] Engelbert D., Overbeck R., and Schmidt A. "A Summary of McEliece-Type Cryptosystems and their Security," Journal of Mathematical Cryptology 1(2) (2007), pp. 151-199.

[14] Faugere J., Otmani A., Perret L., Portzamparc F., and Tillich J. "Structural Cryptanalysis of McEliece Schemes with Compact Keys," Cryptology ePrint Archive, (2014), Report 2014/210.(http://eprint.iacr.org/).

[15] Faure C., and Minder L. "Cryptanalysis of the McEliece cryptosystem over hyperelliptic curves," Proceedings of the eleventh International Workshop on Algebraic and Combinatorial Coding Theory (2008), pp. 99-107.

[16] Finiasz M., and Sendrier N. "Digital Signature Scheme Based on McEliece," Encyclopedia of Cryptography and Security (2011), pp. 342-343.

[17] Fujisaki E., and Okamoto T. "Secure Integration of Asymmetric and Symmetric Encryption Schemes," CRYPTO, volume 1666 of Lecture Notes in Computer Science, Springer (1999), pp. 537-554.

[18] Fujita H. "Quantum McEliece public-key cryptosystem," Quantum Information & Computation 12(3-4) (2012), pp. 181-202.

[19] Goborit P. "Shorter keys for code based cryptography," Proceedings of WCC 2005 (2005), pp. 81-91.

[20] Howgrave-Graham N., and Joux A. "New Generic Algorithms for Hard Knapsacks," EUROCRYPT, volume 6110 of Lecture Notes in Computer Science, Springer (2010), pp. 235-256.

[21] Kobara K., and Imai H. "Semantically Secure McEliece Public-Key Cryptosystems-Conversions for McEliece PKC," Public Key Cryptography, volume 1992 of Lecture Notes in Computer Science, Springer (2001), pp. 19-35.

[22] Kobara K., and Imai H. "On the one-wayness against chosen-plaintext attacks of the Loidreau's modified McEliece PKC," IEEE Transactions on Information Theory 49(12) (2003), pp. 3160-3168.

[23] Lee P. J., and Brickell E. F. "An Observation on the security of McEliece's Public-Key Cryptosystem," EUROCRYPT, Lec Notes in CS (1988), pp. 275-280.

[24] Li Y., Deng R. H., and Wang X. "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems," IEEE Transactions on Information Theory 40(1) (1994) pp. 271-273.

[25] Loidreau P. "Strengthening McEliece cryptosystem," ASIACRYPT, volume 1976 of Lecture Notes in Computer Science, Springer (2000), pp. 585-598.

[26] May A., Meurer A., and Thomae E. "Decoding Random Linear Codes in $\tilde{O}(2^{0.054n})$," ASIACRYPT, volume 7073 of Lecture Notes in Computer Science, Springer (2011), pp. 107-124.

[27] McEliece R. J. "A Public Key Cryptosystem based on Algebraic Coding Theory," DSN progress report 42-44 (1978), pp. 114-116.

[28] Misoczki R., Tillich J., Sendrier N., and Barreto P. S. L. M. "MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes," Proceedings of the 2013 IEEE International Symposium on Information Theory, IEEE (2013), pp. 2069-2073.

[29] Overbeck R., and Sendrier N. "Code-based cryptography," Post-Quantum Cryptography, Springer (2009), pp. 95-145.

[30] 박승안, "선형 부호," 부호이론, 京文社 (2005), pp. 207-306.

[31] Peters C. "Information-Set Decoding for Linear Codes over Fq," PQCrypto, volume 6061 of Lecture Notes in Computer Science, Springer (2010), pp. 81-94.

[32] Persichetti E. "Compact McEliece keys based on Quasi-Dyadic Srivastava codes," Journal of Mathematical Cryptology 6(2) (2012), pp. 149-169.

[33] Pless V. "Introduction to the Theory of Error-Correcting Codes," John Wiley & Sons (1998), pp.1-38.

[34] Pointcheval D. "Chosen-Ciphertext Security for Any One-Way Cryptosystem," Public Key Cryptography, volume 1751 of Lecture Notes in Computer Science,

Springer (2000), pp. 129–146.

[35] Sendrier N. "On the security of the McEliece pk cryptosystem," M. Blaum, P. Farrel, and H. van Tilborg, editors, Proceedings of Workshop honoring Prof. Bob McEliece on his 60th birthday (2002), pp. 141–163.

[36] Shor P. W. "Polynomial–Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing 26(5) (1997), pp. 1484–1509.

[37] Sidelnikov V.M., and Shestakov S.O. "On insecurity of cryptosystems based on generalized Reed–Solomon codes," Discrete Mathematics and Applications, 1(4) (1992), pp. 439 – 444.

[38] Stern J. "A method for finding codewords of small weight," Proceedings of Coding Theory and Applications (1989), pp. 106–113.

[39] Strenzke F. "Timing Attacks against the Syndrome Inversion in Code–Based Cryptosystems," Post–Quantum Cryptography, LNCS vol 7932 (2013), pp. 217–230.

[40] Sugiyama Y., Kasahara M., Hirasawa S., and Namekawa T. "aFurther results on Goppa codes and their applications to constructing efficient binary codes," IEEE Transactions on Information Theory 22(5) (1976), pp. 518–526.

[41] Zajac P. "A note on CCA2–protected McEliece cryptosystem with a systematic public key," Cryptology ePrint Archive, (2014), Report 2014/651. (http://eprint.iacr.org/).

약 력

이 향 숙

1986년 이화여자대학교 수학과 학사
1988년 이화여자대학교 수학과 석사
1993년 Northwestern 대학교 수학과 박사
1994년~1994년 Northwestern 대학교 수학과 연구원
1995년~현재 이화여자대학교 수학과 재직
관심분야: 암호학, 계산적 정수론, pairing 기반 암호, homomorphic encryption, Lattice 기반 암호 등

임 수 민

2012년 이화여자대학교 수학과 이학사
2014년 이화여자대학교 수학과 이학석사
2014년~현재 이화여자대학교 박사과정
관심분야: 암호학, 양자 정보 이론, Biometric 인증 등

임 희 진

2012년 이화여자대학교 수학과 이학사
2012년~현재 이화여자대학교 수학과 석박사 통합과정
관심분야: 암호학, 속성 기반 암호, Biometric 인증 등