랜덤선형부호의 복호화 문제와 그의 암호학적 응용

김진수, 천정희
서울대학교

요 약

오류정정부호는 정보를 부호화하여 데이터 전송 과정에서 발생하는 에러를 감소시킴으로써 통신 신뢰성을 향상시킨다. 이에 따라 에러를 효율적으로 검출 및 정정할 수 있는 부호(code)가 필수적이다. 반면 암호에서는 중요한 정보를 은닉하기 위한 목적으로 비밀정보에 인위적으로 오류를 주입한다. 따라서 기밀성을 유지하기 위해서는 위와는 반대로 오류정정이 어려운 부호를 필요로 한다. 본고에서는 오류정정의 어려움으로 메시지의 비밀성은 유지되고, 덧문(trapdoor)을 가지고 있어 비밀정보가 있을 때는 메시지가 복구되는 암호학적 응용이 가능한 랜덤선형부호의 복호화 문제와 그의 응용에 대해 살펴보고자 한다. 이 문제는 암호학에서 LPN/LWE 문제로 불리며, 최근 LPN문제의 일반화된 문제인 LWE문제가 Regev에 의해 소개되면서 동형암호, 기능암호 등에 광범위하게 응용되고 있다.

Ⅰ. 서 론

스마트폰, 태블릿 PC등과 같은 스마트기기의 확산과 클라우드 서비스를 비롯한 관련 기술의 발달로 가정/업무환경을 비롯하여 사회 전 분야에 걸쳐 큰 혁신이 일어나고 있다. 원격으로 가사활동 뿐만 아니라 학습, 진료 등이 가능해지고, SNS를 통한 광범위한 정보공유와 새로운 사회적 관계가 형성되고 있다. 특히 최근에는 기존의 한계를 뛰어넘어 언제 어디서나 편리하면서도 효율적으로 업무에 종사할 수 있도록 스마트 워크 환경이 정착되가고 있다. 그러나 이러한 컴퓨팅환경은 그 특성상 기존의 서버환경과는 다르게 데이터를 클라우드 서버라 불리는 중앙 서버로 위탁하는 방식이기 때문에 서비스 제공자는 사용자의 데이터들을 위탁 받는다. 따라서 사용자들의 민감한 개인정보를 유출할 가능성이 더욱 높아지게 되었다. 이러한 문제점을 해결하기 위한 방법 중 하나로 암호화된 데이터를 복호화하지 않고 암호화된 상태에서 연산을 가능케 하는 동형암호가 매우 큰 관심을 받고 있으며, 이러한 배경에서 학계에서는 실용적이면서도 안전한 동형암호를 설계하고자 노력해오고 있다. 이러한 동형암호는 현재까지 효율적인 해결 알고리즘이 알려지지 않은 격자 문제(SVP, CVP)나 또는 이와 큰 관련성을 갖는 문제(LWE, AGCD)를 기반으로 설계되고 있다.

과거 안전한 암호학적인 스킴들은 주로 인수분해나, 이산로그와 같이 다항시간에 풀 수 없는 어려운 문제에 기반하여 설계되어 왔다. 그러나 1997년 Shor에 의해 인수분해와 이산로그는 양자컴퓨터를 이용하면 빠른 시간 내에 계산할 수 있다는 사실이 알려진 이후[47], 양자컴퓨터의 등장 이후의 미래 시대에도 안전할 수 있는 암호학적인 스킴들을 연구하는 분야가 형성되었으며, 이 분야를 Post Quantum Cryptography라 부르고 있다. 사용되는 도구들에 따라 해쉬(hash) 기반, 코드(code) 기반, 격자(lattice) 기반, 다변수 연립 2차 방정식(MQ) 기반 등 6가지 소분야로 나누어지며 이들의 공통된 목적은 현재 널리 사용되고 있는 RSA 암호와 같이 효율성, 범용성을 갖춤과 동시에 안전성을 보장할 수 있는 암호 프리미티브를 설계하는 것이다. 격자 기반 암호는 이와 같은 목적을 달성하기 위한 가장 유망한 분야 중 하나로써, 1996년 Ajtai에 의해 worst-case 격자 문제에서 average-case 격자 문제로의 환원에 대한 결과[5]와 2005년 Regev에 의한 LPN 문제의 일반화 문제인 LWE 문제 소개 및 worst-case 격자 문제로부터의 환원(reduction)을 바탕으로 현재 활발한 연구가 진행 중이다[44].

본고에서는 LPN 문제와 그의 확장인 LWE 문제에 대한 정의, 어려움의 정도 등을 알아보고, 이러한 문제에 기반하여 설계된 구체적인 암호 프리미티브들(인증프로토콜, 암호시스템 등)에 대해 살펴보고자 한다.

Ⅱ. LPN 문제와 응용

LPN 문제는 암호학계를 비롯하여 기계학습, 부호이론 분야에서도 지속적으로 연구되어 온 문제로, 간단히 이야기하

자면 에러가 있는 연립일차방정식의 해를 구하는 문제로, $\mathbb{Z}_2^n$의 균등분포로부터 랜덤하게 추출(smapling)한 $\boldsymbol{a}, \boldsymbol{s}$와 $\mathbb{Z}_2$의 베르누이 분포 Ber_τ로부터 추출한 에러 e로부터 만들어진 표본 $(\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s} \rangle \oplus e)$들이 다수 주어졌을 때 이진벡터 $\boldsymbol{s}$를 찾는 average-case 문제이다. LWE 문제는 LPN 문제에서의 법 2보다 더 큰 자연수 q로 법을 확장한 문제로서 에러의 분포는 보통 이산 가우스 분포를 따른다. LPN/LWE 문제에 에러가 없는 경우를 생각하면, 표본들로부터 n개의 선형 독립인 $\boldsymbol{a}$들을 찾고, 가우스 소거법을 이용해 $\boldsymbol{s}$를 다항시간 내에 쉽게 찾을 있지만, 작은 크기의 에러라도 있으면 가우스 소거법이 적용되는 과정에서 에러가 증폭되어 $\boldsymbol{s}$와는 전혀 다른 값을 얻게 되므로 문제가 어려워지게 된다.

두 문제 모두 랜덤선형부호의 복호화(decoding) 문제 또는 격자 문제의 관점에서 비교적 오랜 시간동안 연구되어 왔으나 아직까지, 인수분해나 이산로그와 같은 문제와 달리 현재까지 효율적인 양자컴퓨터 알고리즘이 알려지지 않고 있다.

LPN 문제와 LWE 문제는 유사해 보이지만, 응용의 관점에서 동형암호[16][12][26][17], 신원/속성기반암호[23][18][1], 불확정 전송 프로토콜[41] 등 LWE 문제를 기반으로 한 응용들이 더욱 다양하다. 또한 LWE 기반의 암호 프리미티브들은 worst-case 격자 문제의 안전성도 보장받는다. 한편 LPN 문제는 LWE 문제에 비해 상대적으로 간단하며 효율적이어서 전자태그(RFID)나 스마트카드, 센서 노드(sensor node)와 같은 연산 능력이 극도로 제한된 장치에 사용되고 있다.

1. LPN 문제의 정의

Ber_τ를 $\mathbb{Z}_2$에서 $\tau \in (0, 1/2)$를 파라미터로 하는 베르누이 분포라 하자.즉,

$$x \leftarrow Ber_\tau \text{ 이면, } Pr[x = 1] = \tau \text{ 이다.}$$

그리고 $m \geq 1$에 대해 Ber_τ^m는 Ber_τ확률로 m번 독립적으로 추출함으로써 형성되는 $\mathbb{Z}_2^n$의 확률 분포라 하자. 또한 비밀 이진 벡터 $\boldsymbol{s} \in \mathbb{Z}_2^n$와 $\tau \in (0, 1/2)$가 주어졌을 때, $\Lambda_{\tau,n}(s)$는 $(\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s} \rangle \oplus e) \in \mathbb{Z}_2^n \times \mathbb{Z}_2$의 확률 분포라 하자.(여기서

$$\boldsymbol{a} \leftarrow \mathbb{Z}_2^n, e \leftarrow Ber_\tau)$$

- Search $\mathbf{LPN_{\tau,n,m}}$:
  m개의 표본 $(\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s} \rangle \oplus e) \leftarrow \Lambda_{\tau,n}(\boldsymbol{s})$이 주어졌을 때, $\boldsymbol{s} \in \mathbb{Z}_2^n$를 찾는 문제.
- Decision $\mathbf{LPN_{\tau,n,m}}$:
  m개의 원소로 이루어진 두 표본 집합 $\{(\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s} \rangle \oplus e) \leftarrow \Lambda_{\tau,n}(\boldsymbol{s})\}$과 $\{\boldsymbol{r} \leftarrow U_{n+1}(\mathbb{Z}_2)\}$을 구별하는 문제.

이 문제들에 대한 어려움의 정도는 표본의 개수, 문제를 풀기 위해 걸리는 시간, 성공 확률의 개념을 이용하여 다음과 같이 보다 엄밀하게 정의된다.

정의 1. $\tau \in (0, 1/2)$에 대하여 시간 동안 작동하는 임의의 판단자(distinguisher) D가 m개의 표본으로부터, 최대 ε의 확률로 $\boldsymbol{s}$를 찾을 수 있다면, 즉

$$\left| Pr\left[\boldsymbol{s} \leftarrow \mathbb{Z}_2^n : \ D^{\Lambda_{\tau,n}(S)} = 1\right] - Pr[D^{U_{n+1}} = 1] \right| \leq \varepsilon$$

이면, Search $\mathbf{LPN_{\tau,n,m}}$문제는 (m, t, ε)-난해라 한다.

정의 2. $\tau \in (0, 1/2)$에 대하여 t시간 동안 작동하는 임의의 판단자(distinguisher) D가 다음의 m개의 원소를 갖는 표본 집합들에 대하여

$$\{(\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s} \rangle \oplus e) \leftarrow \Lambda_{\tau,n}(s)\}, \ \{\boldsymbol{r} \leftarrow U_{n+1}(\mathbb{Z}_2)\}$$

ε의 이득(advantage)으로 구별할 수 있다면, 즉

$$Pr\left[s \leftarrow \mathbb{Z}_2^n : \ D^{\Lambda_{\tau,n}(S)} = s\right] \leq \varepsilon$$

이면, Decision $\mathbf{LPN_{\tau,n,m}}$문제는 (m, t, ε)-난해라 한다.

[30]에서는 Search $\mathbf{LPN_{\tau,n,m}}$문제에서 Decision $\mathbf{LPN_{\tau,n,m}}$문제로의 다항시간 환원이 존재함을 보였으며, 반대 방향의 환원은 Search $\mathbf{LPN_{\tau,n,m}}$의 오라클의 결과를 관찰하여 쉽게 구성할 수 있으므로, 이 두 문제는 어려움의 정도가 동등한(equivalent) 문제임을 알 수 있다.

2. 부호이론에서의 LPN 문제

앞서 이야기하였듯이, LPN 문제는 랜덤선형부호의 복호화 문제로 볼 수 있다. m개의 $(\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s} \rangle \oplus e) \leftarrow \Lambda_{\tau,n}(\boldsymbol{s})$표본들을 모아서, $\boldsymbol{a}$를 열로 갖는 $m \times n$행렬을 A라 하면, 표본들은 $(A, A\boldsymbol{s} \oplus \boldsymbol{e})$의 형태가 되며, 행렬 A의 각 열을 랜덤선형부호라 하면 LPN 문제는 정확히 노이즈(또는 에러)가 있는 코드워드(codeword)로부터 메세지 $\boldsymbol{s}$를 찾는 문제가 된다. 한가지 유의할 점은 LPN 문제의 경우 $\boldsymbol{s}$가 균등한 분포로부터 랜덤하게 추출되는 average-case 문제이며, 랜던선형부호의 복호화 문제는 $\boldsymbol{s}$분포를 고려하지 않는 worst-case 문제이다. 이 문제는 1978년 Berlekamp et al.에 의하여 3차원 매칭문제로부터 다항시간 환원이 존재함을 보임으로써 NP-난해(NP-hard)문제임이 밝혀졌다[15]. NP-난해성으로부터 average-case 문제인 LPN 문제가 어렵다고 단정지을 수는 없으므로, 이 사실이 LPN 문제의 어려움을 내포하지는 않는다. 하지만 LPN 문제는 (weak)random self- reducibility 특성이 있어, 효율적인 해결알고리즘이 존재하지 않을 확률이 높다.[10] 또한 다른 관점에서 보면 LPN 문제에서 $\boldsymbol{s}$를 찾는 문제와 $A\boldsymbol{s}$를 찾는 문제가 동일함을 알 수 있는데, 주어진 표본들에서 $\langle \boldsymbol{a}, \boldsymbol{s} \rangle$를 $\boldsymbol{a}$에 관한 함수로 생각하면(즉, $\langle \boldsymbol{a}, \boldsymbol{s} \rangle = f(\boldsymbol{a})$), LPN 문제는 에러가 있는 labeled된 표본 $(\boldsymbol{a}, f(\boldsymbol{a}) \oplus e)$들로부터 불함수(Boolean function) f를 찾는 문제가 된다. 이런 면에서 LPN 문제는 기

계학습 분야 중에서도 계산학습 이론 분야에서 꾸준히 연구되어온 문제로, 특히 [21]에서는 LPN 문제를 효율적으로 풀 수 있으면 2-DNF formular, k-juntas와 같은 특정 불 함수들을 학습할 수 있다는 사실을 보였다.

3. LPN 문제의 어려움(hardeness)

위에서 살펴보았듯이 LPN 문제를 다항시간 이내로 풀 수 있는 알고리즘이 존재하지 않을 가능성이 높으며, LPN 문제를 해결하기 위한 기본적인 방법으로는 전수조사 방법과 에러분포의 확률을 근사하는 방법이 있다.

가. 직관적(naive) 알고리즘

• 전수조사

LPN 문제의 사례 $(A, \boldsymbol{y} = A\boldsymbol{s} \oplus \boldsymbol{e})$가 주어졌을 때, 모든 가능한 $\acute{\boldsymbol{s}}$에 대하여 $\boldsymbol{y} \oplus A\acute{\boldsymbol{s}}$의 해밍 웨이트(Hamming weight)가 대략 τm개인 $\acute{\boldsymbol{s}}$를 찾는 방법으로 $2^{\Omega(n)}$개의 표본과 $2^{O(n)}$의 복잡도를 갖는다.

• 확률분포 근사

Search $\mathbf{LPN}_{\tau,n,m}$문제의 표본을 계속 쿼리(query)하면서 표본 중에서 $\boldsymbol{a} = \boldsymbol{e_1}$인 표본을 충분히 많이 모으면 $\langle \boldsymbol{a}, \boldsymbol{s} \rangle \oplus e = s_1 \oplus e$이고, $e \longleftarrow Ber_\tau$이었으므로 $\langle \boldsymbol{a}, \boldsymbol{s} \rangle \oplus e = 1$인 표본들의 개수가 $\langle \boldsymbol{a}, \boldsymbol{s} \rangle \oplus e = 0$인 표본들의 개수보다 많으면 $s_1 = 1$, 반대로 $\langle \boldsymbol{a}, \boldsymbol{s} \rangle \oplus e = 0$인 표본들의 개수가 훨씬 많으면 $s_1 = 0$임을 Chernoff bound에 의해 매우 높은 확률로 보장받는다. 따라서 이와 같은 방법으로 각각의 s_i를 알 수 있어 결국 $\boldsymbol{s}$전체를 알아낼 수 있다. 하지만 이 방법은 매우 낮은 확률로 나오는 $\boldsymbol{a} = \boldsymbol{e_i}$인 표본을 확률근사를 위해 충분히 얻어야 하므로 매우 비효율적인 방법이다.

나. BKW 알고리즘

LPN 문제를 푸는 가장 빠른 알고리즘은 [9][31]에 제시된 알고리즘으로 자세한 내용은 〈정리 1〉과 같다.

정리 1.(BKW알고리즘의 복잡도): Security 파라미터 λ에 대해 $n = poly(\lambda)$, $\varepsilon(\lambda) \in (0,1)$, $ab \geq n$, $m = poly((2\varepsilon)^{2^a}, 2^b)$이라 하자. 그러면 $\mathrm{LPN}_{1/2-\varepsilon,n}$을 $O(poly(m))$의 복잡도로 푸는 알고리즘이 존재한다.

$a = 1/2 \log n$, $b = 2n/\log n$이라 하면, $(2\varepsilon)^{2^a} = (2\varepsilon)^{\sqrt{n}}$, 를 얻고, 상수 ε으로부터 $m = 2^{O(n/\log n)}$을 얻는다. 따라서 위 알고리즘은 $2^{\Theta(n/\log n)}$의 표본으로부터 $2^{\Theta(n/\log n)}$복잡도로 해결할 수 있음을 알 수 있다. BKW 알고리즘의 아이디어는 위에서 제시한 확률분포 근사 방법을 개선한 것이다. 표본집합에서 적절한 표본을 골라 XOR연산을 하여 단위벡터 $\boldsymbol{e_i}$를 $\boldsymbol{a}$로 가지는 표본을 다수 만든 후 위의 확률분포 근사 방법을 이용하여 $\boldsymbol{s}$를 찾아낸다. [31]의 LF1/LF2 알고리즘은 BKW 알고리즘을 개선한 것으로서 $\tau = 1/2 - \varepsilon$에 대여 $n^{1+\varepsilon}$개의 표본과 $2^{O(n/loglogn)}$ 복잡도를 가지며, 다음과 같은 구체적인 안전성을 갖는다[49].

표 1. LPN 문제의 안전성

키 길이	BKW	LF2
64	2^{35}	2^{28}
96	2^{46}	2^{33}
128	2^{56}	2^{38}
160	2^{64}	2^{43}
192	2^{72}	2^{47}
224	2^{80}	2^{52}
256	2^{88}	2^{56}

한편 기존의 LPN 문제의 분포와 달리 m개의 표본으로부터 만들어지는 에러 벡터 $\boldsymbol{e} \in \mathbb{Z}^m$의 각 성분이 Ber_τ분포로부터 독립적으로 추출되지 않고, 길이가 h인 블록별로 최대 $h\tau$개의 1을 갖도록 랜덤하게 추출하면 $n^{n\tau}$의 복잡도로 $\boldsymbol{s}$를 찾아낼 수 있으며[4], 비밀정보 $\boldsymbol{s} \in \mathbb{Z}_2^n$를 균일분포가 아닌 임의의 분포로부터 추출하는 경우는 균일분포로부터 랜덤하게 추출한 원래의 LPN 문제에서 $\boldsymbol{s}$를 찾는 알고리즘과 동일한 확률로 $\boldsymbol{s}$를 찾아낼 수 있다. 왜냐하면 $\mathbb{Z}_2^n$의 임의의 분포로부터 추출한 $\hat{\boldsymbol{s}}$로부터 $(A, A\hat{\boldsymbol{s}} \oplus e)$형태의 표본들이 주어지면, $\acute{\boldsymbol{s}} \in \mathbb{Z}_2^n$을 균일분포로부터 랜덤하게 추출하여, 주어진 표본들을 $(A, A\hat{\boldsymbol{s}} \oplus \boldsymbol{e} \oplus A\acute{\boldsymbol{s}}) = (A, A(\hat{\boldsymbol{s}} \oplus \acute{\boldsymbol{s}}) \oplus \boldsymbol{e})$로 변환한 후 LPN 문제의 오라클에 입력하면 $\hat{\boldsymbol{s}} \oplus \acute{\boldsymbol{s}}$를 얻고, 이로부터 $\hat{\boldsymbol{s}} = (\hat{\boldsymbol{s}} \oplus \acute{\boldsymbol{s}}) \oplus \acute{\boldsymbol{s}}$를 얻을 수 있기 때문이다. 이 사실은 환원의 관점에서 LPN 문제는 비밀정보 $\boldsymbol{s}$의 분포가 균일분포일 때 가장 어렵다는 것을 보여준다.

4. LPN 문제의 암호학적 응용

LPN 문제의 암호학적 응용은 1994년 Blum et al.에 의해 시작되었다. 이들은 LPN 문제를 소개한 후 일방향함수, 의사난수 생성기, 대칭키암호와 같은 프리미티브들을 설계할 수 있음을 보였다[10].

가. 의사난수 생성기

LPN 문제를 기반으로 만든 의사난수 생성기로는 [10],[2]가 있다. [10]에서는 Decision LPN 문제표본의 의사난수성에 기초해 만들어졌으며, LPN 문제로부터 일방향 함수를 만들고, 이를 이용하여 의사난수 생성기를 만드는 일반적인 방법에 비해 효율적으로 설계되었다. [2]에서는 의사난수 생성기의 효율성을 시드(seed) 길이에 대한 준선형함수(quasilinear) 복잡도로

다소 향상시켰다.

나. 대칭키암호

Gilbert et al.은 LPN기반의 간단한 구조를 갖는 아래와 같은 대칭키 암호를 제안하였다[25].

• Encryption : 메시지 $\boldsymbol{x} \in \mathbb{Z}_2^n$, 비밀키 $\boldsymbol{s} \leftarrow \mathbb{Z}_2^n$, tm개 이하의 에러를 정정할 수 있는 오류정정부호 생성 행렬 $G \in \mathbb{Z}_2^{m \times n}$에 대하여 암호문 $C = (A, A\boldsymbol{s} \oplus \boldsymbol{e} \oplus G\boldsymbol{x})$를 계산한다. 여기서 $\boldsymbol{e}$에 발생하는 에러의 개수는 매우 높은 확률로 tm개 이하가 되도록 설정한다.

• Decryption : 암호문 C와 비밀키 $\boldsymbol{s}$로부터 $\boldsymbol{e} \oplus G\boldsymbol{x}$를 얻고 오류를 정정하여 메시지 $\boldsymbol{x}$를 얻는다.

Decisional LPN 문제의 어려움을 가정하면 암호문 $C = (A, A\boldsymbol{s} \oplus e \oplus G\boldsymbol{x})$ 역시 의사난수이며, 따라서 메시지 $\boldsymbol{x}$가 감추어지게 된다. 이 스킴은 IND-CPA 안전성과 동시에 subspace LPN 문제와 LPN 문제와의 동치관계로부터 키연관 공격(Key Dependent Attack)에도 안전함이 증명되었다.

다. 신분확인(identification) 프로토콜

LPN을 기반으로한 인증 프로토콜은 HB 프로토콜이라 불리우며[27][29], 특히 이 프로토콜들은 RFID 시스템과 같이 RFID 태그의 연산 능력이 제한되어 경량화된 인증을 필요로 하는 곳에 사용되어 왔다.

HB 프로토콜은 prover(태그)와 verifier(리더) 간에 먼저 비밀값인 이진벡터 $\boldsymbol{s} \in \mathbb{Z}_2^n$를 공유한 뒤, 이 값을 통해 인증을 진행한다. 먼저 verifier는 prover에게 난수 $\boldsymbol{a} \in \mathbb{Z}_2^n$를 전송하면 prover는 자신의 비밀값 $\boldsymbol{s} \in \mathbb{Z}_2^n$와 전송 받은 $\boldsymbol{a} \in \mathbb{Z}_2^n$값에 bit-wise AND 연산을 한 뒤 해당 결과의 패리티($\langle \boldsymbol{a}, \boldsymbol{s} \rangle \oplus e$)를 다시 verifier에게 전송해 준다. 이 때, prover는 τ만큼의 확률로 잘못된 값을 verifier에게 전송해주게 되는데, verifier는 m라운드만큼의 프로토콜을 수행했을 때, 실패 횟수가 tm보다 작으면 적법한 대상임을 매우 높은 확률로 인증한다. 프로토콜을 수행하면서 공개되는 정보는 $\mathrm{LPN}_{\tau,n,m}$문제의 사례이므로 문제의 어려움으로부터 수동공격에 안전함을 알 수 있다.

2005년 Juels와 Weis는 HB 프로토콜이 수동공격에는 안전하지만 인증의 과정에서 고정된 비밀값 $\boldsymbol{s}$를 쓰는 경우, $\langle \boldsymbol{a}, \boldsymbol{s} \rangle \oplus e$는 난수비트벡터 $\boldsymbol{a}$에 의해 완전히 결정된다는 사실에 기초하여 재사용공격(replay attack)과 같은 능동공격에 취약함을 밝혔다. 이러한 취약성을 개선하기 위해, prover가 verifier에게 보내는 은닉 요소(blinding factor) $\boldsymbol{a_1} \in \mathbb{Z}_2^n$을 추가한 프로토콜을 제안하였다. 이 프로토콜은 HB+라 불리며, 결과 값 $\langle \boldsymbol{a_1}, \boldsymbol{s} \rangle \oplus \langle \boldsymbol{a}, \boldsymbol{s} \rangle \oplus \boldsymbol{e}$는 verifier의 난수비트벡터 $\boldsymbol{a}$뿐만 아니라, prover의

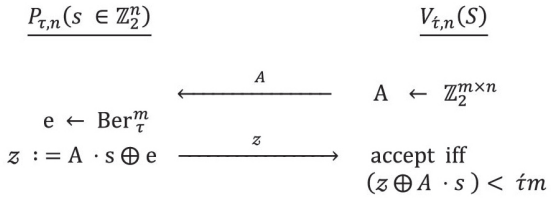

그림 1. HB 프로토콜

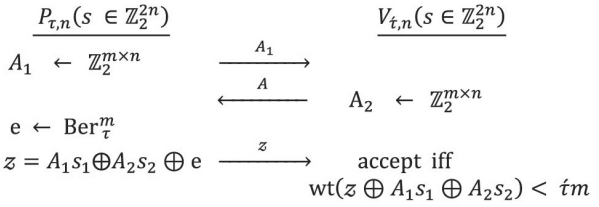

그림 2. HB+ 프로토콜

난수비트벡터 $\boldsymbol{a_1}$에도 의존하기 때문에, 더 이상 재사용공격은 할 수 없다.

이 후 Gilbert et al.은 HB+ 프로토콜이 중간자 공격(man in the middle attack)에 취약함을 밝히고 중간자 공격을 막기 위해, 비밀값과 순열함수를 프로토콜에 추가하여 HB++이라 불리는 프로토콜을 제안하였다[24]. 이 프로토콜은 다시 Wagner의 중간자 공격을 통해 비밀값 노출이 확인되었고, 이후 중간자 공격에 안전한 프로토콜과 HB프로토콜의 효율성을 개선한 프로토콜이 계속 연구되어 왔다.

이외에도 commitment 스킴[28], 영지식 증명 등의 응용이 있으며 비교적 최근에는 LWE기반 공개키 암호에서의 아이디어를 적용한 LPN기반의 공개키 암호시스템이 제안된 바 있다[7][19].

Ⅲ. LWE 문제와 응용

LWE 문제가 구체적으로 드러나지는 않았지만, LWE문제와 관련된 암호학적 응용의 시작은 1997년 Ajtai와 Dwork에 의해서이다[3]. 그들은 γ-uSVP라는 격자 문제의 어려움에 기반한 암호 스킴을 제안하였으며,(여기서 γ-uSVP는 격자내의 선형독립인 격자점(벡터)의 길이가 가장 작은 격자점의 길이에 비해 배 이상 클 때, 최소길이 격자점을 찾는 문제이다.) 특정 조건을 만족하는 제한된 격자들 위에서만 정의되는 γ-uSVP문제는 임

의의 격자위에서 정의된 문제들과 averagecase 격자 문제들과 관련있음이 밝혀졌다[34][6][43][36][40][32]. 이러한 진전가운데 Regev는 LPN 문제의 일반화한 LWE를 문제를 도입, 소개하였으며, LPN 문제와 마찬가지로 random self-reducibility와 search, decision문제의 동치 특성을 갖고 있음을 보였다[44][45]. 또한 중요한 특성 중 하나로 에러의 분포가 가우스 분포를 따를 때 (양자컴퓨터로도 어려운)worst-case 격자 문제로부터 LWE 문제로 (classical, quantumn)환원이 있음을 보였다. 최근 이러한 환원은 이후 [35][14]를 통하여, LWE 문제는 GapSVP라는 worst-case 격자 문제와 어려움의 정도가 동등함이 밝혀졌다.

1. LWE 문제

Security 파라미터 λ, 법 $q \geq 2$, 차원 $n = poly(\lambda)$에 대해 χ는 $\mathbb{Z}_q$의 에러분포라 하자. $\boldsymbol{a},\ \boldsymbol{s} \leftarrow \mathbb{Z}_q^n,\ e \longleftarrow \chi$에 대해 LWE 문제는 다음과 같이 정의한다.

- Search $\mathbf{LWE_{n,m,q,\chi}}$:
  m개의 표본 $\{(\boldsymbol{a},\ \langle \boldsymbol{a}, \boldsymbol{s}\rangle \oplus e)\}$이 주어졌을 때,
  $s \in \mathbb{Z}_q^n$를 찾는 문제.
- Decision $\mathbf{LWE_{n,m,q,\chi}}$:
  m개의 원소로 이루어진 두 표본 집합
  $\{(\boldsymbol{a},\ \langle \boldsymbol{a}, \boldsymbol{s}\rangle \oplus e)\}$, $\{\boldsymbol{r} = (\boldsymbol{a}, u) \longleftarrow U_{n+1}(\mathbb{Z}_q)\}$을 구별하는 문제.

물론 여기서 $q = 2$이고 χ가 Ber_τ이면 LWE 문제는 LPN 문제와 동일하다. 참고로 주어지는 표본의 개수에 제한이 없는 LWE 문제에 대해서는 $\mathrm{LWE}_{n,q,\chi}$으로 m을 생략하여 표기하겠다. LWE 문제는 LPN 문제와 마찬가지로 다음 〈보조정리 1〉과 같이 random self- rucibility 특성을 갖는다.

보조정리 1. (worst-case to average-case): 만일 $\mathbf{LWE_{n,m,q,\chi}}$ 문제를 non-negligible 확률로 풀 수 있는 확률적 다항시간 알고리즘(Probabilistic polynomial time)이 존재하면, 임의의 $\boldsymbol{s} \in \mathbb{Z}_q^n$에 대한 LWE 문제를 non-negligible 확률로 풀 수 있는 알고리즘이 존재한다.

증명의 아이디어만 살펴보면, 균일분포로부터 랜덤한 $\acute{\boldsymbol{s}} \leftarrow \mathbb{Z}_q^n$를 추출하여, 주어진 표본 $(\boldsymbol{a},\ \langle \boldsymbol{a}, \boldsymbol{s}\rangle + e)$을 $(\boldsymbol{a},\ \langle \boldsymbol{a}, \boldsymbol{s}\rangle + \langle \boldsymbol{a}, \acute{\boldsymbol{s}}\rangle + e) = (\boldsymbol{a},\ \langle \boldsymbol{a}, \boldsymbol{s} + \acute{\boldsymbol{s}}\rangle + e)$로 변환한 후 $\mathrm{LWE}_{n,m,q,\chi}$를 문제를 푸는 오라클에 입력하면, 그 결과로 $\boldsymbol{s} + \acute{\boldsymbol{s}}$를 얻고, 따라서 $\boldsymbol{s} = (\boldsymbol{s} + \acute{\boldsymbol{s}}) - \acute{\boldsymbol{s}}$를 얻는다.

또한 LPN 문제에서와 같이 Search $\mathbf{LWE_{n,m,q,\chi}}$와 Decision $\mathbf{LWE_{n,m,q,\chi}}$는 동등한 문제이다. Decision $\mathbf{LWE_{n,m,q,\chi}}$에서 Search $\mathbf{LWE_{n,m,q,\chi}}$로의 환원은 LWE 문제의 표본 $(\{(\boldsymbol{a},\ \langle \boldsymbol{a}, \boldsymbol{s}\rangle \oplus e)\})$을 Search $\mathbf{LWE_{n,m,q,\chi}}$를 푸는 오라클에 입력으로 넣어 $\boldsymbol{s}$를 얻고, 이로부터 두 표본집합에서 $\boldsymbol{e} \in \mathbb{Z}_q^m$와 $\boldsymbol{u} - \boldsymbol{As} \in \mathbb{Z}_q^m$를 얻는다. 이중에서 벡터의 길이가 작은 쪽이 LWE 문제의 표본임을 알 수 있다. 반대방향의 환원은 Regev와 Micciancio, Mol에 의해 소개되었으며[44][35], 증명의 아이디어는 LPN 문제와 동일하다.

정리 2. (Search LWE Decision LWE): λ는 security 파라미터, $n, m = poly(\lambda)$, 법 q는 소수이며 $q = poly(\lambda)$, χ는 $\mathbb{Z}_q^m$의 에러분포라 하자. 만일 Decision $\mathbf{LWE_{n,m,q,\chi}}$ 문제를 non-negligible 확률로 풀 수 있는 확률적 다항시간 알고리즘이 존재하면, Search $\mathbf{LWE_{n,m,q,\chi}}$ 문제를 non-negligible 확률로 찾는 알고리즘이 존재한다.

2. LWE 문제의 어려움(hardness)

가. 격자 문제와의 관계

worst-case 격자 문제 SIVP(Shortest Independent Vectors Problem), GapSVP로부터 LWE 문제로의 다항시간 환원 알고리즘은 2005년 Regev에 의해 제안되었다[44]. 이후 2009년 Peikert는 양자컴퓨터 환원알고리즘이 아닌 일반적인 (classical) 환원알고리즘이 존재함을 보였다.

정리 3.(GapSVP LWE): λ는 security 파라미터, $n = poly(\lambda)$, $\alpha = \alpha(\lambda) \in (0,1)$, $q = q(\lambda) \geq 2^{n/2}$하자. 만일 $\mathrm{LWE}_{n,q,D_{\alpha q}}$ 문제를 non-negligible 확률로 풀 수 있는 확률적 다항시간 알고리즘이 존재하면, 임의의 $\mathrm{GapSVP}_{\tilde{O}(n/\alpha)}$를 효율적으로 풀 수 있는 (classical)알고리즘이 존재한다.

나. LWE 공격 알고리즘

LPN 문제에서의 전수조사 방법, 확률근사 방법, BKW 알고리즘은 LWE 문제에도 거의 비슷한 형태로 적용이 가능하며, 그 외에 격자축소 알고리즘을 이용한 복호화 공격(Decoding attack)[33], 구별 공격(Distinguishing attack)[37][46], 재선형화 공격[4] 등 준지수시간 알고리즘이 알려져 있다.

3. LWE 문제의 암호학적 응용

[44]에서 Regev는 LWE 문제의 어려움에 기반하여 간단한 형태의 공개키 암호를 제안하였으며, 그 이후 다양한 형태의 LWE 문제가 연구되었다[23] [41][42]. 그 결과 인수분해나, 이산로그 같은 정수론 분야의 어려운 문제에 기반하여 설계되었던 속성/신원기반암호와 같은 공개키 암호가 LWE 문제를 기반으로 하여 설계되었고, 특히 많은 중요성을 갖고 있는 동형암호가 LWE 문제를 기반으로 설계되었다. 여기서는 LWE 문제를 기반으로 한 응용 중 동형암호에 대해 살펴보고자 한다.

가. 동형암호

동형암호는 암호화된 자료를 복호화 하는 과정을 거치지 않고 암호화된 상태에서 원하는 자료를 연산 할 수 있는 암호 스킴으로, 복호화 및 재암호화에 소요되는 시간의 낭비를 줄여줌과 동시에 자료 처리를 위해 복호화 된 자료나 키정보의 유출을 막을 수 있어, 클라우드 컴퓨팅 환경에서 보안 문제의 해결책 중 하나로 기대를 모으고 있다. 동형 암호를 찾는 문제는 이미 1970년대 후반부터 암호학계에서 큰 관심을 받아 왔으며, 이에 따라 다양한 연구들이 진행되어 왔다.

Rivest, Adleman, Dertouzo는 1978년 처음으로 동형 암호의 개념 및 필요성을 설명하고, 효율적인 대칭키방식의 준동형 암호 스킴들을 제시하였다 [48]. 그 이후 1982년 Goldwasser와 Micali는 Quadratic Residuosity를 이용하여 최초로 의미론적으로 안전한(IND-CPA) 공개키 방식의 준동형 암호를 발표하였고[22], 덧셈에 대한 준동형 성질을 가지면서 동시에 의미론적으로 안전한 공개키 방식의 준동형 암호들이 개발되었다. 한편, 곱셈에 대한 준동형 성질을 갖는 스킴으로는 1985년 ElGamal에 의하여 개발되었다[20]. 그러나 이러한 암호 스킴들은 덧셈과 곱셈 중 한 가지 연산만을 보존하는 준동형 성질을 갖는다는 점에서 한계가 있었다. 두 가지 연산, 즉 환(ring) 구조를 보존하는 준동형 암호에 대한 연구도 이루어져 왔는데, 덧셈과 곱셈에 대한 준동형 성질을 모두 만족하면서 의미론적으로 안전한 스킴으로는 2005년 Boneh 등에 의해 제시된 페어링(pairing) 기반 준동형 암호가 있다 [11]. 다만 이 암호 스킴은 덧셈에 대해선 제한이 없지만, 곱셈은 단지 1번만 지원하는 한계가 있다.

2009년에는 Gentry에 의해서 처음으로 덧셈과 곱셈 두 가지 연산 모두 횟수 제한이 없는 동형암호스킴(fully homomorphic encryption)이 제안되었다. 평문 공간이 환 $\mathbb{Z}_2$로써 곱셈이 비트의 AND 연산, 덧셈이 비트의 XOR 연산 역할을 하므로, 이 두 연산을 조합하여 임의의 연산을 구성할 수 있다. 좀 더 자세히 살펴보면, 우선 제한된 횟수의 덧셈, 곱셉 연산을 지원하는 준동형 암호 SHE(Somewhat Homomorphic Encryption)를 설계한다. 이 스킴에는 안전성을 위해 각 암호문에 특정한 크기의 노이즈 또는 에러가 존재하는데, 암호문 간의 연산을 수행하고 난 암호문은 최초의 암호문(fresh ciphertext)에 비해 더 큰 크기의 노이즈를 갖게 된다. 따라서 수회 암호문간의 연산 이후 노이즈가 크게 확대되어 복호화 과정이 정확하게 이루어지지 않게 된다. 이 문제를 해결하기 위해 암호문의 노이즈를 줄이는 과정이 필요하며, Gentry는 squashing과 bootstrapping이라는 기법을 이용해 암호문의 노이즈 줄이는 방법을 제안하였다. squashing 기법은 복호화 과정을 가능한 간단한 형태로 바꾸어 복호화의 복잡도를 개선하는 것을 말하며, squashing 과정이 끝난 후에는, 암호문과 비밀키의 암호문을 이용하여 복잡도가 개선된 복호화 연산을 수행함으로써 에러의 크기가 작으면서도 동일한 평문에 대한 암호문(refresh ciphertext)을 얻는다. 이를 bootstrapping이라 부르며, SHE에 이러한 기법들을 적용하면 암호문간의 무한번 연산이 가능한 동형암호를 만들 수 있다.

나. LWE 기반 동형암호

Brakerski et al.은 LWE 문제를 기반으로 한 다음과 같은 동형암호를 제안하였다[16].

나.1. 암호화/복호화 스킴

λ는 security 파라미터, $n, k = poly(\lambda), q = 2^{O(n)}$,

χ는 $\mathbb{Z}_q$의 에러 분포라 하자. $A \leftarrow \mathbb{Z}_q^{k\times n}$, $\boldsymbol{e} \leftarrow \chi^k$에 대하여 $(A, \boldsymbol{v} = A\boldsymbol{s} + 2\boldsymbol{e})$를 공개키, $\boldsymbol{s} = (s_1,\cdots, s_n)$를 비밀키라고 할 때, 평문 $m \in \{0,1\}$은 다음과 같이 암호화 및 복호화 된다.

- Encryption :
  $\boldsymbol{r} \leftarrow \{0,1\}^k$, $\boldsymbol{a} = A^T\boldsymbol{r}$, $b = \boldsymbol{v}^T\boldsymbol{r} + m$를 계산하여, 암호문 $C = (\boldsymbol{a}, b) \in \mathbb{Z}_q^{n+1}$를 얻는다.
- Decryption : $C = (\boldsymbol{a}, b)$로부터 $b' = b - \langle \boldsymbol{a}, \boldsymbol{s}\rangle = 2\boldsymbol{e}^T\boldsymbol{r} + m \in \mathbb{Z}_q$를 계산한 후, $m = b' \bmod 2$를 얻는다.

나.2. 키 변환(재선형화)

이 스킴은 재선형화 또는 키 변환(key switching) 이라는 기법을 통하여 환에 대한 준동형 성질을 갖는다. 임의의 암호문 $(\boldsymbol{a}, b)$에 대하여

$$\boldsymbol{a} = (a_1,\cdots, a_n),$$
$$f_{a,b}(x) = b - <\boldsymbol{a}, \boldsymbol{x}> = b - \sum_{i=1}^n a_i x_i \pmod q$$

라 하자. 여기서 $\boldsymbol{x} = (x_1,\cdots, x_n)$이다.

그러면 $m = f_{a,b}(s)$이고, f는 덧셈에 대하여 준동형이고, 다음과 같이 곱셈에 대해서도 준동형이다.

$$\begin{aligned} & f_{(a,b)}(x) \cdot f_{(a',b')}(x) \\ &= (b - \sum_{i=1}^n a_i x_i) \cdot (b' - \sum_{i=1}^n a'_i x_i) \\ &= h_0 + \sum_{i=1}^n h_i x_i + \sum_{1\le i\le j\le n} h_{i,j} x_i x_j, \end{aligned}$$

여기서 $h_0 = bb'$, $h_i = -(ba'_i + b'a_i)$이고,

$h_{i,j} = a_i a'_j + a_j a'_i$이다.

따라서 위 다항식의 계수의 개수는 $\frac{(n+1)(n+2)}{2}$으로 $\boldsymbol{s}$의 크기에 제곱 정도이며, 비밀키의 크기가 커지는 문제를 해결하기 위해서는 비밀키 $\boldsymbol{s}$로부터 새로운 비밀키,

$$\boldsymbol{t} = (s_1, \ldots, s_n, s_1 s_1, s_1 s_2, \ldots, s_n s_n)$$

를 만든다. 따라서 $h_{a,b}(x) = f_{(a,b)}(x) \cdot f_{(a',b')}(x)$는 새로운 비밀키 t에 대해 선형이며

$$h_{a,b}(t) \bmod 2 = m\, m'$$

이므로, 곱셈에 대해서 준동형임을 알 수 있다. 새로운 비밀키를 만듬으로써 키의 길이가 다소 길어지지만, 새로운 비밀키는 오직 복호화 과정에서만 사용되기 때문에 homomorphic evaluation 과정의 복잡도는 증가시키지 않는다.

SHE 스킴을 무한번 연산 가능한 동형암호 스킴으로 만들기 위해서는 에러를 감소시키는 과정이 필요한데, 이를 위해서는 법 변환(modulus switching)이라는 기법을 이용한다. 이 기법은 암호문 $C \in \mathbb{Z}_q^{n+1}$로부터 동일한 평문에 대한 에러가 작은 암호문 $C' \in \mathbb{Z}_p^{n+1}$를 얻는 기법으로, Gentry의 스킴과 달리 squashing 기법을 필요로 하지 않는 특징이 있다.

IV. 결 론

랜덤선형부호의 복호화 문제는 암호학계에서 LPN/LWE 문제로 구체화되어 여러 암호스킴을 설계하는데 이용되고 있다. LPN 문제의 경우 주로 의사난수 생성기, 인증 프로토콜을 비롯한 대칭키 기반의 암호 프리미티브를 설계하는데 이용되어왔고, LWE문제의 경우 공개키 암호 그 중에서도 신원기반암호, 속성기반암호, 동형암호와 같은 부가적인 기능이 추가된 공개키 암호를 설계하는데 응용되어왔다. 안전성을 위해 노이즈를 인위적으로 삽입하는 방식은 암호문의 길이가 길어지는 문제가 있으나 단순하고 효율적인 특성으로 추후 더 다양한 암호 프리미티브 설계에 응용될 수 있을 것으로 보인다.

LPN/LWE 문제는 근사적으로(asymptotic) NP-complete 문제의 worst-case에서 환원된다는 사실로부터 이에 기반한 암호시스템이 다항식 시간에 공격되지 않음을 알 수 있다. 하지만 이것이 실제 파라미터가 언제 안전한지에 대해서는 답을 주지 않는다. 아직까지 이 문제들을 해결하는 알고리즘 연구들은 많지 않다. 향후 격자 이론이나 정수론의 접근방식을 이용하여 이들 문제를 푸는 알고리즘을 연구하는 것은 매우 흥미로운 문제이다. 이를 통해 안전하면서도 보다 더 효율적인 암호 프리미티브들을 설계하는 일이 가능해질 것이다.

참 고 문 헌

[1] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (h)ibe in the standard model," EUROCRYPT, pp. 553-572, 2010.

[2] B. Applebaum, D. Cash, C. Peikert, and A. Sahai, "Fast cryptographic primitives and circular-secure encryption based on hard learning problems," CRYPTO 2009, vol. 5677, pages 595-618, 2009.

[3] M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/average-case equivalence," STOC, pp. 284-293, 1997.

[4] S. Arora and R. Ge, "New algorithms for learning in presence of errors," ICALP(1), pp. 403-415, 2011.

[5] M. Ajtai, "Generating hard instances of lattice problems(ex-tended abstract)," STOC, pp. 99-108, 1996.

[6] M. Ajtai, "Generating hard instances of the short basis problem," ICALP, pp. 1-9, 1999.

[7] M. Alekhnovich, "More on average case vs approximation complexity," computational complexity, vol. 20, pp. 755-786, 2011.

[8] L. Babai, "lattice reduction and the nearest lattice point problem," STACS'85, pp. 13-20, 1985.

[9] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," J.ACM, vol. 50, pp. 506-519, Jul. 2003.

[10] A. Blum, M. L. Furst, M. J. Kearns, and R. J. Lipton, "Cryptographic primitives based on hard learning problems," CRYPTO, pp. 278-291, 1993.

[11] D. Boneh, E. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," Crypto, vol. 3378, pp.325-341, Aug. 2005.

[12] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(leveled)fully homomorphic encryption without bootstrapping," ITCS, pp. 309-325, 2012.

[13] D. J. Bernstein and T. Lange, "Never trust a bunny," Cryptology ePrint Archive: 2012/355, 2012.

[14] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé, "Classical hardness of learning with errors," STOC, pp. 575-584, 2013.

[15] E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems," IEEE Trans. on Inf Theory, vol. 24, pp. 384-386, may 1978.

[16] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE,"

FOCS, pp. 97-106, 2011.

[17] Z. Brakerski and V. Vaikuntanathan, "Lattice-based FHE as secure as PKE," ITCS, pp. 1-12, 2014.

[18] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsaitrees, or how to delegate a lattice basis," Cryptology ePrint Archive: 2010/591, 2010.

[19] N. Dttling, J. Mller-Quade, and A. C.A. Nascimento, "IND-CCA secure cryptography based on a variant of the LPN problem, ASIACRYPT, vol. 7658, pp. 485-503, 2012.

[20] T. ElGamal, "A Public-Key Cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. on Inf. Theory, vol. 31, pp. 469-472, 1985.

[21] V. Feldman, P. Gopalan, S. Khot, and A. K. Ponnuswami, "New results for learning noisy parities and half-spaces," Found. of Comp. Science, pp. 563-574, oct. 2006.

[22] S. Goldwasser, S. Micali, "Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Patial Information," Proc. of the 14th Annual ACM Symp. on Theory of Comp., pp. 365-377, 1982.

[23] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," STOC, pp. 197-206, 2008.

[24] H. Gilbert, M. Robshaw and H. Sibert, "An Active Attack against HB+ - A Provably Secure Lightweight Protocol," Cryptology ePint Archive: 2005/237, 2005.

[25] H. Gilbert, M. J.B. Robshaw, and Y. Seurin, "How to encrypt with the LPN problem," Automata, Languages and Programming, vol. 5126, pp. 679-690, 2008.

[26] C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based," CRYPTO, pp. 75-92, 2013.

[27] N. J. Hopper and M. Blum, "Secure human identification protocols," ASIACRYPT, vol. 2248, pp. 52-66, 2001.

[28] A. Jain, S. Krenn, K. Pietrzak, and A. Tentes, "Commitments and efficient zero-knowledge proofs from learning parity with noise," Cryptology ePrint Archive: 2012/513, 2012.

[29] A. Juels and S. A. Weis, "Authenticating pervasive devices with human protocols," CRYPTO, vol. 3621, pp 293-308, 2005.

[30] J. Katz, J. Shin, and A. Smith, "Parallel and concurrent security of the hb and hb+ protocols," Journal of Crypto., vol.23, pp. 402-421, 2010.

[31] E. Levieil and P. Fouque, "An improved LPN algorithm," Security and Cryptography for Networks, vol. 4116, pp. 348-359, 2006.

[32] V. Lyubashevsky and D. Micciancio, "On bounded distance decoding, unique shortest vectors, and the minimum distance problem," CRYPTO, pp. 577-594, 2009.

[33] R. Lindner and C. Peikert, "Better key sizes (and attacks) for LWE-based encryption," CT-RSA, pp. 319-339, 2011.

[34] D. Micciancio, "The shortest vector in a lattice is hard to approximate to within some constant," FOCS, pp. 92-98, 1998.

[35] D. Micciancio and P. Mol, "Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions," CRYPTO, pp. 465-484, 2011.

[36] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on gaussian measures," FOCS, pp. 372-381, 2004.

[37] D. Micciancio and O. Regev, "Lattice-based cryptography," 2008.

[38] C. Peikert, "Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem," Proc. of the 41st annual ACM symp. on Theory of computing, pp. 333-342, 2009.

[39] K. Pietrzak, "Subspace LWE," The theory of Cryptography, vol. 7194, 2012.

[40] C. Peikert and A. Rosen, "Lattices that admit logarithmic worst-case to average-case connection factors," STOC, pp. 478-487, 2007.

[41] C. Peikert, V. Vaikuntanathan, and B. Waters, "A framework for efficient and composable oblivious transfer," CRYPTO, pp. 554-571, 2008.

[42] C. Peikert and B. Waters, "Lossy trapdoor functions

and their applications," STOC, pp. 187-196, 2008.
[43] O. Regev, "New lattice-based cryptographic constructions," J. ACM, vol. 51, pp. 899-942, 2004.
[44] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," Proc. of the 37th annual ACM symp. on Theory of Comp.,pp. 84-93, 2005.
[45] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," J. ACM, vol. 56, 2009.
[46] A. Rosen and G. Segev, "Chosen-ciphertext security via correlated products," SIAM J. Comput., vol. 39, pp. 3058-3088, 2010.
[47] P. W. Shor, "Polynomial-time algorithms for prime factorizationand discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, pp. 1484-1509, 1997.
[48] R. Rivest, L. Adleman, M. Dertouzo, "On Data Banks and Privacy Homomorphisms," Found. of Secure Comput., pp. 169-177, 1978.
[49] S. A. Weis, "New Foundations for Efficient Authentication, Commutative Cryptography and Private Disjointness Testing," MIT Computer Science Ph.D.Thesis. 2006.

약 력

김 진 수

2004년 해군사관학교 공학사
2012년 서울대학교 이학석사
2014년~현재 서울대학교 수리과학부 박사과정
관심분야: 암호론, 계산수론

천 정 희

1991년 한국과학기술원 이학사
1993년 한국과학기술원 이학석사
1997년 한국과학기술원 이학박사
1997년~2000년 한국전자통신연구원 선임연구원
2000년 Brown University Postdoc
2000년~2003년 한국정보통신대학교 조교수
2003년~현재 서울대학교 수리과학부 조교수/부교수/교수
관심분야: 정수론, 계산수론, 암호론