정 보 보 호 학 회 지
제27권 제6호, 2017. 12

격자 기반 차세대 양자 내성 암호에 대한 부채널 분석 기술 동향

김 수 리*, 김 한 빛*, 김 희 석**

요 약

양자 컴퓨터의 개발 가능성이 증가됨에 따라 인수분해나 이산대수 문제를 효율적으로 해결할 수 있는 Shor 알고리즘의 구현 가능성이 늘어나고 있다. 기존 RSA와 ECC 기반 암호시스템은 Shor 알고리즘이 구현될 경우 다항시간 안에 해독이 가능하기 때문에, 이를 대체할 후 양자 암호의 필요성이 대두되고 있으며, 이러한 후 양자 암호 중 격자 기반 암호는 빠른 속도와 비교적 작은 키 사이즈로 각광받고 있다. 후 양자 암호를 실생활에서 사용하려면 양자 컴퓨터 이외에 기존 공격에 대한 안전성도 고려해야 하며, 가장 강력한 암호 분석으로 알려진 부채널 분석에 대한 안전성 또한 필수적으로 구비되어야 한다. 본 논문에서는 격자 기반 암호에 대한 부채널 분석 및 대응기술 동향에 대해 알아본다.

Ⅰ. 서 론

양자역학에 기반을 둔 양자 컴퓨터는 기존에 수학적으로 안전하다고 알려진 암호 시스템에 중대한 위협요소가 되고 있다. 1994년에 제안된 Shor 알고리즘은 양자 컴퓨팅 환경에서 인수분해나 이산대수 문제를 효율적으로 해결할 수 있다. Shor 알고리즘이 구현될 경우 현재 사용하는 RSA나 ECC는 다항시간 안에 해결되기 때문에 많은 사람들은 Shor 알고리즘을 구현할 수 있는 양자 컴퓨팅 환경의 실현 가능성에 대해 관심을 가져왔다. 최근에는 양자 컴퓨터의 개발 가능성이 높아짐에 따라 RSA나 ECC를 대체하는 양자 컴퓨팅 환경에서도 안전한 후 양자 암호 혹은 양자 내성 암호(Post-quantum cryptography)에 대한 연구를 활발히 진행 중에 있으며, 이를 위한 NIST의 표준화 작업도 이루어지고 있다. 후 양자 암호는 크게 다변수 함수 기반 암호(Multivariate-based cryptography), 코드 기반 암호(Code-based cryptography), 격자 기반 암호(Lattice-based cryptography), 해시 기반 전자 서명(Hash-based digital signature), 아이소제니 기반 암호(Isogeny-based cryptography)의 5가지로 분류된다.

이 중 격자 기반 암호는 실제 사용 가능할 정도로 속도가 빠르게 구현이 가능하여, 이에 대한 구현기법과 안전성 분석 등과 같은 다양한 연구가 진행되고 있다. 2016년 Alkim 등이 발표한 격자 기반 키 교환 프로토콜 NewHope의 경우 구글 브라우저 중 하나인 크롬 카나리아(Chrome Canary)에 시험적으로 탑재되서 운영되고 있다. 하지만 후 양자 암호라는 새로운 암호 시스템이 양자 컴퓨터에 대해 수학적 안전성을 보장할 수 있다 하더라도, 현존하는 공격에 대해 안전성의 뒷받침 역시 필수요소이다.

1996년 P. Kocher에 의해 소개된 부채널 분석은 수학적으로 안전성이 증명된 암호라 할지라도 암호연산이 보안장비 위에서 동작하는 동안 누출되는 부가적인 정보를 이용하여 비밀정보을 분석하는 물리적 공격기법이다. 이러한 부채널 분석에 대한 안전성 보장은 정보보호 제품 공통 평가 기준과 CMVP, PIV, EMV 등 다양한 산업 표준 및 평가 기준에 포함되어 있으며, 암호 시스템의 신뢰도를 보장하는데 수학적 안전성과 더불어 매우 중요한 요소로 자리매김하고 있다.

격자 기반 암호 또한 개인키를 NTT(Number Theoretic Transform)로 바꾸는 과정, 복호화나 서명 생

이 성과는 2017년도 정부(과학기술정보통신부)의 재원으로 한국연구 재단의 지원을 받아 수행된 연구임(No. NRF-2017R1C1B2004583).
* 고려대학교 정보보호대학원 (luthien09@korea.ac.kr, luz-damoon@korea.ac.kr)
** 고려대학교 사이버보안전공 (80khs@korea.ac.kr)

성 과정, 가우시안 에러를 생성하는 가우시안 샘플링 과정에 대한 단순 전력 분석, 차분 전력 분석, 템플릿 공격, 충돌 공격, 캐시 공격 등의 다양한 부채널 분석이 연구되고 있으며, 이러한 다양한 부채널 분석에 대한 대응기술 또한 활발히 연구되고 있다.

본 논문에서는 격자 기반 암호의 부채널 분석 및 대응기술 개발 현황을 조사한다. 먼저 격자 기반 암호의 구조를 소개한 뒤, 최신 부채널 분석 기법 및 대응기술을 소개하고 향후 격자 기반 암호 적용에 있어서 고려해야할 사항을 정리한다.

Ⅱ. 격자 기반 양자 내성 암호

과거에서는 암호 알고리즘을 공격하는데 사용되었던 격자(lattice)는 1996년 Ajtai의 제안 이후 많은 연구가 진행되어왔다[1]. 이후 2005년 Regev가 증명 가능한 격자 기반 암호 시스템이 제안되고, 양자 컴퓨터에 안전함과 동시에 빠른 연산으로 활발히 연구가 진행되어왔다[2]. 본 장에서는 격자 기반 암호의 기반 문제 및 기본 이론에 대해서 설명하고, 현재 대표적인 격자 기반 암호 알고리즘을 소개한다.

2.1. 격자 기반 암호

격자 $L \subset R^n$ 은 기저 $b_1, ..., b_n \in R^n$에 대한 정수 결합의 집합을 나타내며, 이를 기호로 다음과 같이 표현할 수 있다.

$$L = \{\sum a_i b_i | a_i \in Z\}$$

초기 격자 암호의 안전성 기반 문제는 Shortest Vector Problem (SVP)로 다음과 같이 정의할 수 있다.

Definition) Shortest Vector Problem : 임의의 집합 B를 기저로 갖는 격자 L에 대해서 격자 L안의 0이 아닌 가장 작은 벡터 v를 찾는 문제

SVP를 기반으로 하는 알고리즘으로는 NTRU 등이 있다. 최근에는 2005년 Regev가 제안한 Learning With Error(LWE) 문제를 기반으로 한 알고리즘이 제안되고 있으며, LWE는 다음과 같이 정의할 수 있다.

Definition) LWE distribution : 주어진 비밀 벡터 $s \in Z_q^n$에 대해 랜덤한 $a \in Z_q^n$과 분포 χ에서 선택한 에러 e를 이용해 출력한 (a,b), $b = \langle s,a \rangle + e \bmod q$를 샘플한 집합 $A_{s,\chi}$를 LWE distribution이라 한다.

Definition) Search-LWE : LWE distribution으로부터 독립적으로 샘플된 m개의 (a_i, b_i) 쌍이 주어졌을 때, s를 구하는 문제

LWE를 기반으로 한 암호 시스템의 경우 안전성을 수학적으로 증명할 수 있으며, 환 구조를 이용하면 Number Theoretic Transform을 이용한 빠른 연산이 가능하기 때문에, 많이 연구되고 있다. 대표적인 암호 시스템으로는 키 교환 프로토콜인 NewHope 와 서명 알고리즘인 BLISS 가 있다.

2.2. 격자 기반 암호의 구조

격자 기반 암호는 가우시안 샘플링과 Number Theoretic Transform 으로 나눌 수 있다.

2.2.1. Gaussian Sampling

격자 암호의 에러들은 격자 위에서 가우시안 분포를 이루고 있다. 따라서 가우시안 분포를 구현하는 것이 격자 암호에서 중요하며, 선택된 에러값은 노출되지 않아야 한다. 가우시안 샘플링 방법은 rejection sampling, inversion sampling 혹은 cumulative distribution sampling (CDT sampling), Knuth-Yao sampling 등이 있으며, 본 논문에서는 테이블 참조로 빠른 샘플링이 가능해서 많이 쓰이는 CDT 샘플링에 대해 소개를 하도록 한다[3].

CDT 샘플러는 가우시안 샘플링을 하는 가장 빠르고 직접적인 방법이다. Cumulative distribution function (누적 분포 함수) $\Phi(k)$는 다음과 같이 정의된다.

$$\Phi(k) = \sum_{e=-\infty}^{k} \Pr(E=e)$$

샘플링을 수행하기 위해 CDT 샘플러는 $[0,1)$사이에서 랜덤한 값을 선택 한 뒤,

$$\Phi(k-1) < U \leq (k)$$

를 만족하는 k를 출력한다. CDT 샘플링 시 사용되는 누적 분포 테이블은 공개 값이고, CDT 샘플링에 대한 알고리즘은 [Alg. 1]과 같다.

2.2.2 Number Theoretic Transform

격자 암호의 또 다른 중요한 구성 요소로는 NTT가 있다. 기존 LWE의 기본 연산은 행렬-벡터 연산 혹은 행렬-행렬 연산으로, 차원이 n인 행렬의 연산은 $O(n^2)$의 연산량이 든다. 이를 줄이기 위해 링 위의 LWE를 이용하는 방법에 대해서 생각하게 되었다. 링 위에서의 연산은 여러 가지 장점을 가져다준다. 먼저 격자 암호에서 사용되는 링은 $R=Z_q[x]/\langle x^n+1\rangle$ 인데, 모든 원소가 $(n-1)$차 다항식으로 표현되어 키 길이를 효율적으로 줄일 수 있다. 또한 기존 $(n-1)$차 다항식 두 개를 곱하는데 $O(n^2)$의 연산이 들었다면, 고속 푸리에 변환(Fast Fourier Transform, FFT)을 이용한 곱셈을 수행한다면 $O(n\log n)$정도로 줄어들게 된다. FFT를 이용한 연산은 복소수를 사용하므로 $n=2^k$인 n을 사용하고 $q\equiv 1 \bmod 2n$을 만족하는 소수 q를 사용하여 $\psi^{2n}\equiv 1 \bmod q$를 만족하는 $2n$-th root of unity와 $\omega^n\equiv 1 \bmod q$인 n-th root of unity 모두 Z_q안에 있도록 한다. 이 경우 FFT 모든 연산은 정수 위에서 이루어지게 되는데 이를 Number Theoretic Transform 이라 한다.

Algorithm 1. CDT Sampling

Input : 격자 차원 n, tail bound z_t, 확률 정확도 범위 ϵ, CDT 테이블 Φ
Output : 가우시안 분포를 따르는 n개의 랜덤 값

1. for $i=0$ up to $n-1$ by 1 do
2. generate ϵ bit random number U
3. $k=0$
4. While $U>\Phi[k]$ do
5. $k=k+1$
6. end while
7. generate a 1 bit random s
8. gauss[i] = $-1^s\times k$
9. end for
10. return gauss

NTT를 사용하여 다항식 곱을 할 수 있는 이유는 다음 두 가지 때문이다.

1) 차수가 n인 임의의 다항식 $A(x)$는 n개의 서로 다른 점 (x_i,y_i)로 나타낼 수 있고, 이 점들이 나타내는 다항식은 $A(x)$로 유일하다. 이 때, $1\le i\neq j\le n$ 이면 $x_i\neq x_j$ 이며, $y_i=A(x_i)$ 이다.

2) $C(x)=A(x)B(x)$라 할 때, $C(x_i)=A(x_i)B(x_i)$가 되어, $A(x)$, $B(x)$를 표현한 n개의 점을 이용하여 $C(x)$를 n개의 점으로 표현할 수 있다.

일반적으로 $(n-1)$차 다항식을 서로 곱하면 $(2n-2)$차 다항식이 생성되어, 결과값을 표시하기 위해서는 $(2n-1)$개의 점이 필요하다. 하지만 RLWE의 경우에서는 곱하는 중간에 다항식은 $(2n-1)$이 될 수 있지만, (x^n+1)로 감산되기 때문에 결과는 $(n-1)$차 다항식이며, n개의 점으로도 충분하다. 이를 위해 'negative wrap convolution'을 사용하며, 해당 NTT 알

Algorithm 2. NTT based on Cooley-Tukey

Input : A vector $a=(a[0],a[1],...,a[n-1])\in Z_q^n$ in standard ordering, prime q such that $q\equiv 1 \bmod 2n$, $n=2^k$, pre-computed $\Psi_{rev}\in Z_q^n$ storing powers of ψ in bit-reversed order
Output : $a\leftarrow NTT(a)$ in bit-reversed ordering

1. $t=n$
2. for $(m=1;m<n;m=2m)$ do
3. $t=t/2$
4. for $(i=0;i<m;i++)$ do
5. $j_1=2\cdot i\cdot t$
6. $j_2=j_1+t-1$
7. $S=\Psi_{rev}[m+i]$
8. for$(j=j_1;j\le j_2;j++)$ do
9. $U=a[j]$
10. $V=a[j+t]\cdot S$
11. $a[j]=U+V \bmod q$
12. $a[j+t]=U-V \bmod q$
13. end for
14. end for
15. end for
16. return a

고리즘은 [Alg. 2]와 같다[4].

[Alg. 2]에서 사용된 Ψ_{rev}테이블은 $\psi^0, \psi^1, ..., \psi^{n-1}$값을 역비트 순으로 저장한 테이블로, 공개된 값이다. 역비트 순이란 다음과 같다. 예를 들어 $n=1024$를 사용할 경우, 0부터 $n-1$값들은 9비트로 표현할 수 있다. ψ^0에서 지수는 $0=000000000_2$으로 배열의 첫 번째에 저장된다. ψ^1에서 지수는 $1=000000001_2$이므로 100000000_2로 비트열을 바꾸어 배열의 512번째에 저장한다. 비트가 뒤바뀌는 이유는 NTT 알고리즘 수행 중 n-th root of unity ω에 대해 $\omega^{\frac{n}{2}+k}=-\omega^k$ 성지를 이용하고 분할 정복법이 사용되기 때문이다.

Ⅲ. 격자 기반 양자암호에 대한 부채널 분석 기술 동향

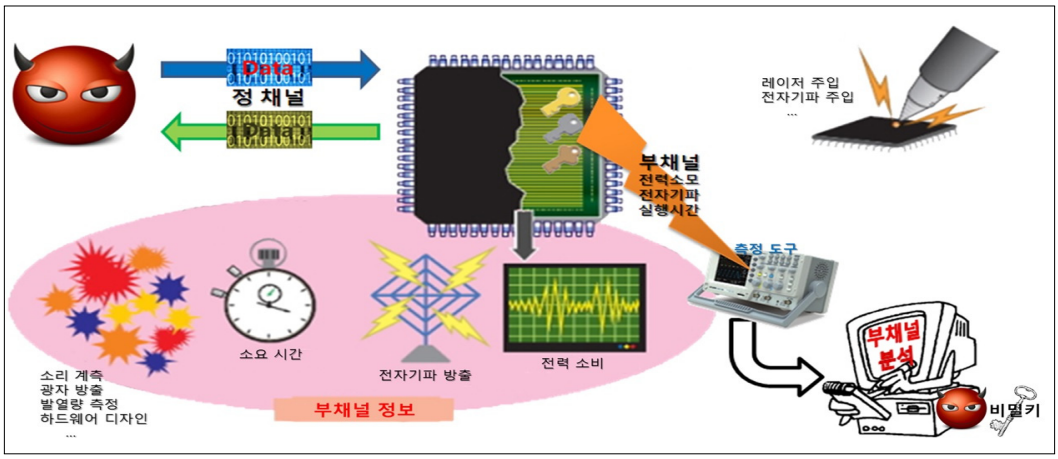
본 장에서는 격자 기반 암호의 부채널 분석 기술 동향에 대해서 알아본다. 부채널 분석을 통해서 비밀값을 알아내는 것이 목적이므로, 보통 개인키를 NTT로 바꾸는 과정에서의 연산이나, 복호화나 서명 생성 과정에서 부채널 분석이 이루어진다. 또한 가우시안 에러를 이용하여 격자 구조를 가리는 것이 격자 기반 암호의 핵심인 만큼, 가우시안 샘플링 단계에서 부채널 분석을 통해 에러값을 알아내는 공격 등이 존재한다. 먼저 부채널 분석에 대해 간략하게 소개한 다음, 격자 기반 암호의 부채널 분석에 대해 소개한다.

3.1. 부채널 분석 기술

최근 정보통신 이용자의 폭발적인 증가와 다양한 네트워크, 통신 인프라의 발전으로 통신 서비스에 대한 이용자의 요구가 고도화/다양화되고 있다. 이에 대응하기 위해 정보보호 기술, 정보통신 기술의 향상을 위한 연구개발이 세계적으로 활발하게 이루어지고 있으며, 기술의 고도화를 지지하기 위한 소프트웨어 및 하드웨어 기술의 연구 개발이 활발하게 진행되고 있다. 특히 IC 카드 및 보안 토큰, ATM기, 보안 라우터 등과 같은 하드웨어 기반의 보안 시스템에 대한 양질의 보안 서비스를 제공하기 위한 연구 및 표준화 작업이 활발하게 진행되고 있다.

암호 시스템에 대한 기존의 안전성 평가는 증명 가능한 안전성이나 계산적 안정성과 같은 이론에 기반을 두고 있다. 그러나 최근 암호시스템이 구현된 하드웨어에 대한 또 다른 형태의 공격이 제기되고 있어 암호 시스템의 실질적인 안전성 평가가 중요한 쟁점으로 떠오르고 있다. 스마트 카드, 모바일 폰, PDA 등과 같은 하드웨어 장치에서 암호 알고리즘이 구현 될 때, 전력 소모량, 알고리즘의 수행시간, 및 전자파 방출량 등과 같은 비밀키에 관련된 부가정보가 공격자에게 악의적으로 이용될 수 있다. 암호시스템에 대한 이러한 형태의 공격을 부채널 분석(Side Channel Analysis)이라고 한다.

1996년 P. Kocher가 암호 프리미티브에 대한 최초의 부채널 분석인 시차 공격(Timing Attack)을 도입하고[5], 1999년에 차분 전력 분석(Differential Power Analysis, DPA)을 소개한 이후 다양한 관점에서 부채



〔그림 1〕 부채널 분석 개요도

널 분석은 진화하고 있다[6]. 부채널 분석은 사용되는 부채널 신호에 의해 시차 공격(Timing Attack)[5], 전력 분석 공격(Power Analysis Attack)[6], 전자기파 분석 공격(Electromagnetic Analysis Attack)[7], 오류 주입 공격(Fault Injection Attack)[8] 등으로 분류되며, 분석 기법에 따라 단순 전력 분석(Simple Power Analysis, SPA)[5], 차분 전력 분석(Differential Power Analysis, DPA)[6], 충돌 공격(Collision Attack)[9], 템플릿 공격(Template Attack)[10], 캐시 공격(Cache Attack)[11] 등으로 분류된다. 최근 전력 분석 공격 기법이 고도화됨에 따라 USB, 스마트카드, IC chip과 같은 소형 디바이스 뿐 아니라 노트북, 데스크탑과 같은 고사양 CPU가 탑재된 제품

에도 공격의 시도가 있으며, 공격에 성공하였다는 연구들이 발표되고 있다.

부채널 공격에 대한 대응방법은 알고리즘적인 수준과 물리적인 수준에서 강구될 수 있다. 부채널 공격은 비밀키와 암호 알고리즘 수행의 연관성을 이용한다. 제안된 부채널 공격이 가능하기 위해서는 여러가지 공격의 모델링 및 실험 가정이 필요하다. 만약 스마트 카드와 같은 하드웨어에 암호 알고리즘이 장착되었을 때, 모델링 및 가정을 어렵도록 스마트 카드를 설계하면 부채널 공격을 원천적으로 봉쇄하는 방법이 될 수 있다. 암호 알고리즘이 장착된 하드웨어를 통해 신뢰할 수 있는 보안 서비스를 제공하기 위해서는 부채널 공격기술에 대한 이해와 이에 대비한 암호 알고리즘의 개발이 필수적이다.

3.2. Gaussian sampling SPA

CDT sampling은 선택한 랜덤값이 주어진 CDT 테이블의 어느 범위에 위치하는지 찾는 알고리즘이다. [Alg. 1]을 참고하면 4-6 번 과정에서 선택된 랜덤값에 따라 루프의 횟수가 결정되며, 이 루프의 횟수는 곧 가우시안 에러값과 일치한다. 격자 기반 암호에서 주어진 격자의 구조를 가우시안 에러로 가리는 만큼, 이 에러값을 안다는 것은 단순한 연산으로 비밀값을 알 수 있다는 것이다. 따라서 최근에는 [Alg. 1]과 같은 초기 버전의 CDT 샘플링을 사용하지 않고 어느 랜덤값이여도 동일한 시간에 종료하는(constant time) 알고리즘을 사용한다.

3.3. Flush+Reload cache attack

캐시 메모리는 CPU와 같은 처리 속도가 빠른 프로세서와 RAM과 같은 상대적으로 속도가 느린 메모리 사이에 위치하여, 자주 사용되는 데이터를 저장하여 프로세서와 메모리 사이의 접근 시간을 아낄 수 있도록 고안된 크기는 작지만 빠른 메모리이다.

2014년 Y. Yarom이 제안한 Flush+Reload 캐시 공격은 공격자가 임의로 캐시 메모리를 지우고(Flush), 비밀정보와 관련된 연산이 수행된 이후 메모리를 다시 불러오는(Reload)과정을 통해 해당 메모리 값이 캐시에서 불러오는지 RAM과 같은 외부 메모리에서 불러오는지의 시간차이를 측정하여 비밀정보를 분석하는 공격기법이다[12]. 좀 더 구체적으로, 공격자는 분석 대상이 비밀 정보와 관련된 연산을 수행하기 직전에 캐시 메모리를 임의로 지우는(Flush) 과정을 수행한다. 이 후, 분석 대상이 비밀 정보와 관련된 연산을 수행하면 비밀 정보에 해당하는 데이터가 캐시 메모리에 올라가게 된다. 비밀 정보가 캐시 메모리에 올라간 이 후, 공격자는 비밀 정보로 추정되는 데이터를 다시 불러오는 과정(Reload)을 수행한다. 이 때 공격자는 비밀 정보와 관련된 중요한 정보를 얻을 수 있다. 만약 비밀 정보로 추정한 데이터를 불러오는 속도가 빠르다면, 이는 캐시에 해당 비밀 정보가가 있다는 의미이며 이는 추정한 데이터가 비밀 정보라는 강력한 증거가 된다. 만약 비밀 정보로 추정한 데이터를 불러오는 속도가 느리다면 이는 추정한 데이터가 이전 연산에 사용되지 않았음을 의미한다.

CHES2016에서 L.G. Bruinderink는 BLISS의 가우시안 샘플러를 대상으로 Flush+Reload 캐시 공격을 수행하였다[13]. BLISS 격자 암호는 비밀 정보를 가리기 위해 사용되는 노이즈를 생성하는 가우시안 샘플링 과정이 필요하다[17]. 이 때 생성되는 노이즈에 가우시안 분포는 BLISS 격자 암호의 안전성을 보장하는 매우 중요한 비밀요소로 작용한다. 논문에서는 가우시안 샘플링 과정에서 참조 테이블을 메모리에서 불러오는 과정을 대상으로 Flush+Reload 캐시 공격을 수행하고, 이를 통해 노이즈의 가우시안 분포와 관련된 비밀정보를 분석하여 BLISS 서명 알고리즘의 비밀키를 복원하였다. 해당 논문에서는 96%의 성공 확률로 단 450개의 서명만을 이용하여 2분 내에 비밀키를 찾아냈다.

3.4. Belief Propagation

2017년 CHES에서 발표된 Primas 등은 단일 파형을 이용하여 격자 기반 암호를 공격하는 방법을 적용하였다[14]. 제안한 공격 기법은 단일 파형을 사용하기 때문에 기존에 제안되었던 마스킹 기법에서도 적용이 가능하다.

앞서서 격자 기반의 암호는 가우시안 샘플링 외에도 NTT 변환을 이용한 다항식 곱셈이 중요하다고 하였다. Primas 등은 개인키가 Inverse NTT(INTT) 변환을 이용해 다시 원래 링 위의 원소로 변환될 때를 공격하여 개인키를 복원하였다. 공격은 크게 3 단계로 나눌 수 있다. 먼저 템플릿을 이용해서 INTT 연산시 일어나는 모듈러 연산값을 알아낸다. 그 후 모든 INTT 연산 부분에서 일어나는 정보들을 모은다. 이 과정은 INTT 연산의 그래프 구조와 신뢰전파(Belief Propagation, BP) 알고리즘을 사용한다. 마지막 복원된 비밀값과 공개키를 이용해서 개인키를 복원한다.

BP 알고리즘은 Pearl 등에 의해 처음으로 제안되었으며, 함수의 인수분해 결과가 주어졌을 때 효율적인 주변화를 수행한다. N개의 변수 x=$\{x_n\}_{n=1}^{N}$으로 이루어진 함수 P^*가 다음과 같이 M개의 인자로 나타낼 수 있다고 하자.

$$P^*(\mathrm{x}) = \prod_{m=1}^{M} f_m(x_m)$$

여기에서 각 인자 $f_m(x_m)$은 x 의 부분집합 x_m에 대한 함수이며, 각각의 x_n들은 어느 정의역 D에 정의되어 있다. 이 때 어느 변수 x_n에 대한 주변화 함수 Z_n을 연산한다는 것은 다음을 연산한다는 것과 동일하다.

$$Z_n(x_n) = \sum_{\{x_{n'}\}n' \neq n} P^*(\mathrm{x})$$

이 주변화 함수의 연산의 복잡도는 변수의 숫자 N에 대해 지수적으로 증가한다. BP 알고리즘은 주어진 함수의 인수분해 결과를 이용해서 Z_n 연산을 감소시키는 것을 목표로 한다. BP 알고리즘은 메시지 전달 법칙을 기반으로 하며, 주어진 함수를 이분그래프로 나타내야 사용할 수 있다. 변수는 x의 한 변수 x_i를 의미하며 인자노드는 함수의 한 인자 f_m을 의미한다. BP 알고리즘은 변수로부터 인자노드로, 인자노드로부터 변수로를 반복적으로 수행하여 주변화 함수를 연산한다.

BP를 이용한 INTT 공격 방법은 다음과 같다. 먼저 모든 모듈로 덧셈, 뺄셈, 곱셈에 대한 전력소모 등과 같은 부채널 누출(leakage)을 측정한다. 그 뒤 템플릿을 이용해 정확한 연산값을 확인 한 뒤, INTT의 버터플라이 연산의 각 부분에 대한 부채널 정보를 획득한다. 여기서 버터플라이 연산이란 [Alg. 2]의 11-12를 의미한다. 그 후 BP를 이용해 전체 INTT 연산의 정보를 합친 뒤, 수렴할 때 까지 BP를 수행한다. 수행 결과 BP 알고리즘을 20번 반복하는 것으로도 개인키에 대한 엔트로피가 많이 감소하였다.

Ⅳ. 격자 기반 양자암호에 대한 대응기술 동향

격자 기반 암호의 부채널 대응기술로는 기존 대칭키 암호나 RSA 혹은 ECC에 적용했던 대응기술과 유사하게 제안되었다. 본 장에서는 격자 기반 암호의 마스킹 관련 기법에 대해 알아보도록 한다.

4.1. Blinding, shuffling, random constant multiplication

부채널 분석 지점은 주로 개인키와 연관된 부분을 수행하기 때문에, 개인키와 관련된 연산을 공격자가 알아내지 못하도록 하는 것이 중요하다. 이를 바탕으로 NTT 도메인에서 개인키와 암호문이 연산될 때 마스킹 기법이 제안되었다[15].

NTT 함수는 다음과 같은 성질을 가지고 있다. 임의의 다항식 f, g와 상수 a, b에 대해서

$$NTT(a \cdot f^* b \cdot g) = ab \cdot NTT(f^* g)$$

를 만족한다. 따라서 랜덤한 값 a, b를 선택한 뒤 $a \cdot f$와 $b \cdot g$를 이용해 연산을 수행하고, 결과값에 ab^{-1}를 취해주면 원래 값이 나오게 된다. 다른 의미로는 셔플링(shuffling)이 있을 수 있는데, NTT에서 일어나는 곱셈은 coefficient-wise 하기 때문에 순서를 섞어도 상관이 없다. 따라서 랜덤하게 곱셈 연산을 수행하는 것도 한 방법이다.

4.2. Additive homomrphic masking

2016년 Reparaz 등이 PQCrypto에서 발표한 대응기술로, LPR 알고리즘의 복호화 과정을 랜덤화 하여 DPA 공격에 대응하였다[16]. LPR 알고리즘의 마지막 단계는 덧셈에 대해 동형이며 이에 대한 증명은 다음과 같다. 주어진 두 암호문 (c_1, c_2), (c_1', c_2')에 대해

$$\begin{aligned} &DEC(c_1,c_2) \oplus DEC(c_1',c_2') \\ &= (c_1 \cdot s + c_2) \oplus (c_1' \cdot s + c_2') \\ &= (c_1 + c_1') \cdot s + (c_2 + c_2') \\ &= DEC(c_1 + c_1', c_2 + c_2') \end{aligned}$$

를 만족한다. 제안한 랜덤 복호화 방법은 다음과 같다. 먼저 랜덤한 메시지 m'을 생성한 뒤, m'에 대한 암호문 (c_1', c_2')를 연산한다. $(c_1 + c_1', c_2 + c_2')$ 에 대한 복호화를 실행한 뒤 $m \oplus m'$연산을 수행해 원래 값을 복원한다.

Ⅴ. 결 론

최근 2017년 11월 30일을 마지막으로 NIST에서 후양자 암호 표준화를 위한 알고리즘 공모를 마쳤다. 총 82개가 제출되었고 그 중 격자 기반 암호는 28개로 가장 많이 제출되었다. NIST 에서도 부채널에 안전한 후양자 암호 알고리즘을 권장한 만큼, 향후에도 격자 기반 암호에 대한 부채널 분석 연구가 활발히 진행될 것으로 보인다.

참 고 문 헌

[1] M.Ajtai et al. “A public-key cryptosystem with worst-case/average-case equivalence,” *STOC*, pp. 284-293, 1997.

[2] O. Regev. “On lattices, learning with errors, random linear codes, and cryptography,” *STOC*, 2005.

[3] C. Du et al. “Towards efficient discrete gaussian sampling for lattice-based cryptography,” *FPL*, pp.1-6, 2015.

[4] P. Longa et al. “Speeding up the number theoretic transform for faster ideal lattice-based cryptography,” *CANS*, pp. 124-139, 2016.

[5] Kocher, Paul C. “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems.” *Annual International Cryptology Conference,* Springer, Berlin, Heidelberg, 1996.

[6] Kocher, Paul, Joshua Jaffe, and Benjamin Jun. “Differential power analysis.” *Advances in cryptology—CRYPTO’99,* Springer Berlin/Heidelberg, 1999.

[7] Quisquater, Jean-Jacques, and David Samyde. “Electromagnetic analysis (ema): Measures and counter-measures for smart cards.” *Smart Card Programming and Security,* pp. 200-210, 2001.

[8] Biham, Eli, and Adi Shamir. “Differential fault analysis of secret key cryptosystems.” *Advances in Cryptology—CRYPTO'97,* pp. 513-525, 1997.

[9] Schramm, Kai, Thomas Wollinger, and Christof Paar. “A new class of collision attacks and its application to DES.” *FSE,* Vol. 2887, 2003.

[10] Chari, Suresh, Josyula R. Rao, and Pankaj Rohatgi. “Template attacks.” *International Workshop on Cryptographic Hardware and Embedded Systems,* Springer, Berlin, Heidelberg, 2002.

[11] Gullasch, David, Endre Bangerter, and Stephan Krenn. “Cache games--bringing access-based cache attacks on AES to practice.” *Security and Privacy (SP),* IEEE Symposium on. IEEE, 2011.

[12] Yarom, Yuval, and Katrina Falkner. “FLUSH+ RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack.” *USENIX Security Symposium,* 2014.

[13] Bruinderink, Leon Groot, et al. “Flush, Gauss, and Reload‐a cache attack on the BLISS lattice-based signature scheme.” *International Conference on Cryptographic Hardware and Embedded Systems,* Springer Berlin Heidelberg, 2016.

[14] R. Primas et al. “Single-trace side-channel

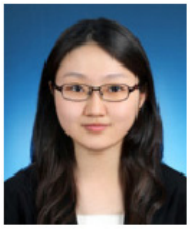
attacks on masked lattice based-encryption," *CHES*, pp. 513-533, 2017.

[15] M. Saarinen, "Arithmetic coding and blinding countermeasures for lattice signatures," *Cryptology eprint archive*, 2016.

[16] O. Reparaz et al. "Additively homomorphic ring-lwe masking," *PQCrypto*, pp. 233-244, 2016.

[17] L. Ducas et al. "Lattice signatures and bimodal gaussians," *CRYPTO* 2013, pp.40-56, 2013.

〈저 자 소 개〉



김 수 리 (Suhri Kim)
학생회원

2014년 2월 : 고려대학교 수학과 학사
2016년 2월 : 고려대학교 정보보호대학원 석사
2016년 2월~현재 : 고려대학교 정보보호대학원 박사과정
관심분야 : 부채널 공격, 공개키 암호시스템

김 한 빛 (HanBit Kim)
학생회원

2014년 2월 : 고려대학교 신소재공학 학사
2016년 2월 : 고려대학교 정보보호대학원 석사
2016년 2월~현재 : 고려대학교 정보보호대학원 박사과정
관심분야 : 부채널 공격 및 대응기법, 암호시스템 안전성 분석 및 고속구현

김 희 석 (HeeSeok Kim)
정회원

2006년 : 연세대학교 수학과 학사
2008년 : 고려대학교 정보보호대학원 석사
2011년 : 고려대학교 정보보호대학원 박사
2011년 9월~2012년 12월 : Bristol University 박사후 연구원
2013년~2016년 8월 : 한국과학기술정보연구원(KISTI) 선임연구원
2015년~2016년 8월 : 과학기술연합대학원대학교(UST) 조교수
2016년 9월~현재 : 고려대학교 과학기술대학 사이버보안 전공 조교수
관심분야 : 부채널 공격, 암호시스템 안전성 분석 및 고속구현, 암호칩 설계 기술, 보안관제, 네트워크 보안