정 보 보 호 학 회 지
제 32 권 제1호, 2022. 2

NIST PQC Round 3 격자 기반 암호 KEM에 대한 부채널 분석 기법 동향 분석

이 정 환*, 김 규 상**, 김 희 석*

요 약

NIST는 PQC Round 3 평가 기준으로 부채널 분석 및 오류 주입에 대한 안전성을 역설함에 따라 Round 3 양자내성암호에 대한 새로운 부채널 공격 시나리오 및 대응 기법이 빠르게 제시되고 있다. 따라서 각 방법론의 동향을 파악하고 재정의, 분류하는 작업이 필수적으로 요구된다. 본 논문에서는 NIST PQC Round 3 최종 후보 중 격자 기반 암호 KEM(SABER, CRYSTALS-KYBER, NTRU)에 대한 부채널 분석기법 및 대응기술 동향을 조사 및 분석하고 향후 Round 3 격자 기반 KEM 알고리즘의 부채널 연구 전망을 논의한다.

Ⅰ. 서 론

양자 컴퓨터의 발달로 Shor 알고리즘을 통해 소인수 분해 문제, 이산대수 문제를 다항시간 내에 해결할 수 있다. 이러한 기술이 알려짐에 따라 RSA, ECC 등 현존하는 공개키 암호 체계에 큰 위협이 되고 있다. 이에 따라 NIST는 PQCrypto 2016에서 양자내성암호에 대한 미국 연방 표준 사업 계획을 발효했으며 현재 3라운드가 진행 중에 있다. 3라운드에는 7개의 최종 후보(KEM 알고리즘 4개, 디지털 서명 3개)와 8개의 대안 후보가 존재한다.

1996년 P. Kocher에 의해 소개된 부채널 분석은 이론적으로 안전함이 증명된 암호가 장비 위에서 동작될 때 암호의 연산으로 인해 누출되는 전력, 전자파, 시간 등의 부가적인 정보를 이용하여 비밀정보를 추출하는 물리적 분석 기법으로 단순전력분석과 상관전력분석, 프로파일링 공격 기법 등이 존재한다. 이러한 부채널 공격으로부터 암호 알고리즘의 안전성을 보호하기 위해 부채널 대응기법이 개발되고 있으며 대표적으로 신호대잡음비(Signal-to-Noise, SNR)를 감소시켜 장비에서 나오는 부채널 정보와 암호화 연산의 중간값의 관계성을 제거하는 하이딩 기법과 난수값으로 암호 중간 연산값을 마스킹시켜 공격자가 부채널 정보를 통해 중간값을 추론하지 못하게 막는 마스킹 기법이 있다.

NIST가 PQC Round 3의 평가 기준에 부채널 분석 및 오류 주입에 대한 안전성을 역설하였고, 시간이 지날수록 양자내성암호에 대한 새로운 부채널 공격 시나리오 및 대응 기법이 계속해서 등장하고 있다. 이러한 방법론들이 지속적으로 다양하게 제시됨에 따라 그 동향을 파악하여 방법론을 재정의, 분류하고 이해하는 작업은 필수적이다.

본 논문에서는 NIST PQC Round 3 최종 후보 중격자 기반 암호 KEM(SABER, CRYSTALS-KYBER, NTRU)에 대한 부채널 분석 및 대응기술 동향을 조사한다. 본 논문의 구성은 다음과 같다. 2장에서는 격자 기반 암호 KEM과 부채널 분석 기술의 배경지식을 소개한다. 3장에서 LWE/LWR 기반 암호와 NTRU 암호 각각에 대한 최신 부채널 분석 기법을 소개하고 4장에서 SABER,CRYSTALS-KYBER, NTRU 각각에 대한 최신 부채널 대응 기법 동향을 알아본다. 마지막으로 결론 및 향후 연구 방향을 제시한다.

이 성과는 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구 재단의 지원을 받아 수행된 연구임(No.NRF-2019R1A2C2088960).
* 고려대학교 인공지능사이버보안학과 (학부생, hwani0814@korea.ac.kr, 부교수, 80khs@korea.ac.kr)
** 고려대학교 정보보호대학원 정보보호학과 (대학원생, ks9509@korea.ac.kr)

Ⅱ. 배경지식

2.1. 격자 기반 암호 KEM

격자 기반 암호는 수학적으로 정의된 격자 상의 어려운 문제를 기반으로 하는 암호이다. 대표적으로 잘 알려진 어려운 문제로 Shortest Vector Problem, Closest Vector Problem, Bounded Distance Decoding 등이 있다. Round 3 최종 후보에 있는 격자 암호 SABER, CRYSTALS-KYBER,NTRU는 앞서 언급한 어려운 문제의 변형을 기반으로 만들어졌다. 예를 들어 SABER는 LWR(Learning With Rounding), CRYSTALS-KYBER는 LWE(Learning With Errors), NTRU는 NTRU 격자 상의 SVP가 적용되어있다.

2.2. 부채널 분석 기법

부채널 분석 기법은 부채널 정보로부터 비밀 정보를 추출하는 방법에 따라 단순전력분석, 차분전력분석, 상관전력분석, 상호 정보량 분석, 프로파일링 공격 등으로 나뉜다. 단순전력분석은 단일 또는 소수의 파형을 가지고 공격 시점 중간값이 파형에 나타나는 특징을 파악한 후 비밀 정보를 추출하는 부채널 분석 기술이다. 차분전력분석, 상관전력분석, 상호정보량분석은 다수의 파형을 사용하여 통계적 분석으로 비밀 정보를 추출하는 부채널 분석 기술이다. 해밍무게, 해밍거리등의 전력모델을 가정한 후 키를 추측하여 중간값을 계산하고 이를 전력모델값으로 변환한다. 이 전력모델값과 실제 측정된 전력을 바탕으로 통계량을 계산한 뒤 가장 유의미한 통계량을 가진 키를 비밀정보로 채택한다. 이때 차분값을 통계량으로 사용할 경우 차분전력분석, 상관계수를 통계량으로 사용할 경우 상관전력분석, 상호정보량을 통계량으로 사용할 경우 상호정보량분석이라 부른다.

프로파일링 공격은 공격자가 공격 대상과 같은 장비를 가지고 있거나 암호화 오라클 등에 접근할 수 있어 공격자의 선택 평문 또는 암호문에 대해 공격 대상 시점의 중간값을 알 수 있고 그에 해당하는 파형을 수집할 수 있는 환경을 가정한다. 이때 공격자는 중간값과 수집한 파형을 통해 부채널 정보를 특징화할 수 있고 이를 이용해 비밀정보를 추출할 수 있다. 대표적으로 템플릿 공격과 딥러닝 기반 프로파일링 공격이 존재한다. 두 공격 모두 선택 평문 또는 암호문으로부터 계산한 중간값이 파형에서 연산되는 유의미한 시점을 추출한다. 템플릿 공격은 이 시점들에 대한 분포가 정규 분포를 이룬다고 가정하고 다변수 정규 분포의 통계량인 평균과 공분산 행렬을 템플릿으로 형성한다. 공격 시, 공격 대상에서 추출한 파형과 앞서 만든 템플릿을 통해 최대우도측정법으로 계산하여 중간값을 추론할 수 있다. 그 후 중간값을 통해 비밀 정보를 추출한다. 딥러닝 기반 프로파일링 공격은 유의미한 시점 또는 파형 전체를 MLP, CNN 등 딥러닝 네트워크의 입력층에 넣고 중간값(또는 중간값에 대한 전력모델값)을 라벨로 네트워크를 학습시킨다. 공격 시, 공격 대상 파형을 학습시킨 네트워크에 넣고 스코어 벡터를 얻는다. 가장 유의미한 스코어 벡터를 출력한 네트워크에 해당하는 라벨값을 중간값으로 채택한다.

Ⅲ. NIST PQC Round 3 격자기반 KEM에 대한 부채널 분석 기법

격자 기반 암호에 대한 부채널 분석 기법은 암호 구조로 인한 차이 때문에 크게 두 부류로 나뉜다. LPR PKE 구조를 기반으로 FO 변환을 통해 만들어진 LWR 기반 KEM 알고리즘에 대한 부채널 분석과 기존 NTRU PPKE에서 Targhi-Unruh 변환을 통해 만들어진 NTRU 기반 KEM 알고리즘에 대한 부채널 분석을 다룰 것이다.

3.1. LWE/LWR 기반 KEM에 대한 부채널 공격

LWE/LWR 기반 KEM에 대한 부채널 공격은 크게 오라클 기반 공격과 기반 연산 소프트웨어 구현에 대한 공격이 존재한다. 오라클 기반 공격은 공격자가 만든 선택 암호문에 대해 부채널 파형에서 추출된 정보를 바탕으로 오라클을 만들고 이를 통해 비밀키를 복구하는 공격 방법이다. 추출된 부채널 정보에 따라 Plaintext-Checking 오라클 기반, Full-Decryption 오라클 기반, Decryption-Failure 오라클 기반 부채널 공격으로 나눌 수 있다. PC 오라클은 공격자의 선택 암호문에 대한 복호화 메시지 추측값의 진위 여부를 제공하고 FD 오라클은 더 나아가 공격자의 선택 암호문에 대한 복호화 메시지를 제공한다. DF 오라클은 디캡슐화 과

〔표 1〕 오라클의 종류와 응답

오라클 종류	응답
plaintext-checking(PC)	$m_0(No), m_1(Yes)$
Full-Decryption(FD)	$valid, invalid$
Decryption-Failure(DF)	m

정에서 선택 암호문의 유효성 여부, 곧 복호화 성패 여부를 제공한다. 기반 연산 소프트웨어 구현에 대한 공격은 다항식 연산에 쓰이는 NTT 알고리즘 소프트웨어 구현물에 대한 부채널 공격을 의미한다.

3.1.1. Plaintext-Checking(PC) 오라클 기반 부채널 공격

[16]에서 소개한 부채널 PC 오라클 기반 공격은 NIST round 2 격자기반 PKE/KEM에 대한 범용적 공격이다. pqm4 라이브러리를 사용하였으며 ARM Cortex-M4 위에서 보호기법이 적용안된 상수시간 암호 구현물을 동작시켜 EM 파형을 수집하였다. 복호화 과정에서 공격 시나리오의 메시지 비트에 대한 템플릿을 만들어 공격자의 선택 암호문에 대한 PC 오라클을 만들었다. 특히, CRYSTALS-KYBER에서 공격자는 $u_0[0]=k_u$, $v[0]=k_v$이고 나머지 계수가 모두 0인 선택 암호문 $u\in R^{k_q}$, $v\in R_q$를 만들고 이 값을 디캡슐화 과정의 입력으로 넣는다. 적당한 (k_u,k_v)값을 통해 아래와 같은 식을 만족시킬 수 있다.

$$m'_j=\begin{cases}\mathsf{Poly\_to\_Msg}(k_{\mathbf{v}}-k_{\mathbf{u}}\cdot\mathbf{s}_0[0]), & \text{if } j=0\\ \mathsf{Poly\_to\_Msg}(-1\cdot k_{\mathbf{u}}\cdot\mathbf{s}_0[j]), & \text{for } 1\le j\le n-1\end{cases}$$

$$m'_i=\begin{cases}\mathcal{D}(\mathbf{s}_0[0]), & \text{if } i=0\\ 0, & \text{for } 1\le i\le n-1\end{cases}$$

〔그림 1〕 선택 암호문과 메시지의 관계

여러 (k_u,k_v) 값을 통하여 $s_0[0]$의 값을 추론할 수 있다. CRYSTALS-KYBER 512 파라미터 기준으로 비밀키 계수 한 개를 구하는데 총 5개의 파형이 필요하였다. 따라서 모든 키를 복구할시 최소 $5\cdot256\cdot2=2560$개의 파형을 필요로 한다.

위와 같이 PC 오라클을 통해 비밀키 전체 복원하는 것이 가능하지만 해당 오라클에 사용된 부채널 정보는 한번에 한 비트 정보만을 제공하므로 선택 평문 공격을 통한 키 복구에 많은 파형이 필요하다는 단점이 존재한다.

3.1.2. Full-Decryption(FD) 오라클 기반 부채널 공격

앞선 PC 오라클 기반 부채널 공격은 선택 암호문 구성의 특성 상 한 개의 파형 당 메시지 비트 한 개에 대한 정보만 추출 가능했다. [24]에서 소개한 FD 오라클 기반 부채널 공격은 공격자가 선택 암호문을 더 효율적인 구조로 선정하여 한 개의 파형에서 전체 메시지를 복구 및 사용할 수 있게 만들었다. 구체적으로, $u_0[0]=k_u$, $v=\Sigma_{n=0}^{255}(k_v\bullet x^n)$이고 나머지 계수가 모두 0인 선택 암호문 $u\in R^{k_q}$, $v\in R_q$를 구성한 뒤 디캡슐화의 입력한다. 이러한 공격자는 적당한 k_v, k_u을 선택하여 비밀키 계수 한 개가 메시지 비트 하나에 관여하도록 만든다. 재암호화의 메시지 디코딩 과정에서 그림 3과 같이 단순전력분석을 통해 해당 메시지 비트를 확인할 수 있고 이를 One-versus-the-Rest(OvR) classifier로 이용할 수 있다. 결과적으로 pqm4 ARM 기반 구현 CRYSTALS-KYBER 512파라미터에 대해 8개의 파형만으로 비밀키 전체를 복구할 수 있게 하였다.

Algorithm 7 Decoding: `poly_frommsg()`

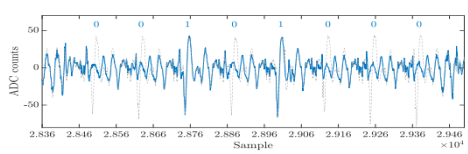
Input: Input message in msg [32]

```
for i = 0 ... 31 do
    for j = 0 ... 7 do
        mask = -((msg[i] >> j) & 1);
        coeffs[8·i + j] = mask & ((q + 1)/2);
    end for
end for
return coeffs[]
```

〔그림 2〕 〔24〕 공격 지점

m-distributions for different intervals of $u_0[0]$ with $v=\sum_{n=0}^{255}416\cdot x^n$

t / coeff. of s	-2	-1	0	1	2
u_0					
[0, 208]	0	0	0	0	0
[211, 416]	1	0	0	0	0
[419, 624]	1	1	0	0	0
...	...	...	...	...	...
[2705, 2910]	0	0	0	1	1
[2913, 3118]	0	0	0	0	1
...	...	...	...	...	...



〔그림 3〕 〔24〕 메시지 디코딩 단순전력분석

[15]에서 소개한 FD 오라클 기반 공격은 앞선 [24]와 같은 원리로 선택 암호문을 만들고 FD 오라클을 구성한 뒤 비밀키를 복구하였다. 그러나 부채널 정보를 통해 메시지를 복구하는 과정에서 단순전력분석이 아닌 템플릿 공격을 사용하였는데, 먼저 1비트씩 값이 누적으로 입력되는 변수 공간을 증분 공간이라 정의하고 LWE/LWR 기반 암호의 증분 공간 부채널 정보를 이용하여 메시지 비트를 복구하였다. 증분 공간의 부채널 공격 과정은 전처리 단계와 공격 단계로 나뉜다. 전처리 과정에서는 NICV를 통해 해밍무게 템플릿의 POI를 선택한다. 그 뒤 POI에 해당하는 파형들의 평균을 내어 해밍무게 템플릿을 구성한다. 공격 단계에서는 공격 대상 파형에 대해 복구하고 싶은 메시지 POI에 해당하는 부분의 파형과 POI에 해당하는 템플릿과의 거리를 계산한다. 가장 가까운 거리에 있는 템플릿의 해밍무게를 POI 메시지의 해밍무게라 판단한다. 증분 공간의 크기가 8비트라면 8번의 누적을 반복하게 되는데 누적이 시행될 시점마다 나올 수 있는 해밍무게에 대한 템플릿을 구성하고 위 공격을 적용하면 모든 메시지에 대한 복구가 가능하다.

[8]에서 소개한 FD 오라클 기반 공격은 1차 마스킹된 SABER에 대한 부채널 공격이다. [24]와 같은 원리로 선택 암호문을 만든 뒤 FD 오라클을 구성하고 $[8,4,4]_2$ 해밍코드를 이용한 결정 테이블을 만들어 오라클의 응답에 따라 비밀키를 복구하였다. 오라클을 구성하기 위해 앞서 [15]에서 정의한 증분 공간을

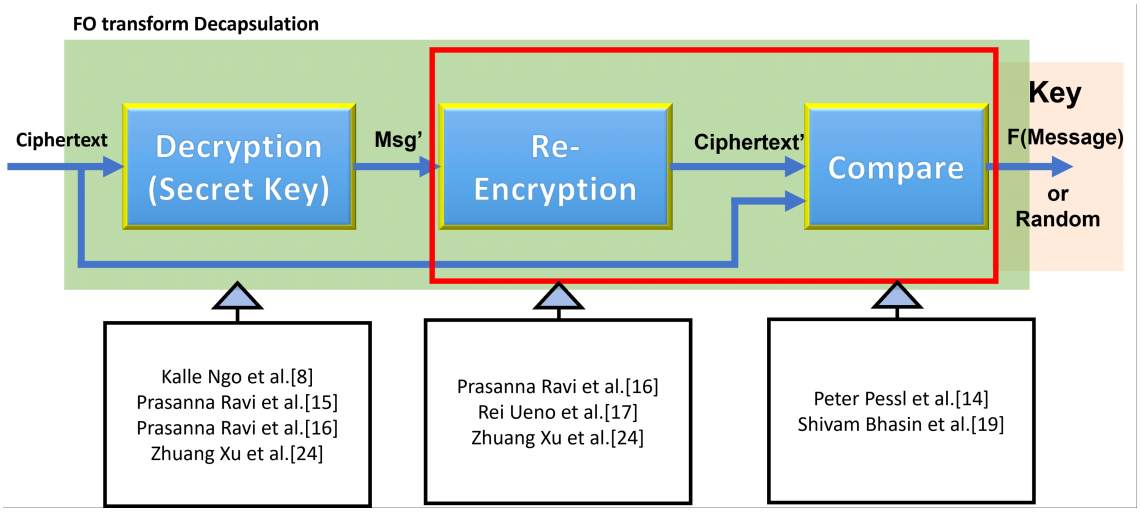
```
void Decode(unsigned char *m, poly *x)
{
  uint16_t t;
  int i, j;
  poly_csubq(x);
  for (i = 0; i < 32; i++)
  {
    /* init byte m[i] to zero */
    m[i] = 0;
    for (j = 0; j < 8; j++)
    {
      k = 8*i+j;
      t = (x->coeffs[k] ≪ 1) + Q/2;
      /* Calculate Message Bit */
      t = (t/Q) & 1;
      /* Bit Update in Memory */
      m[i] |= t ≪ j;
    }
  }
}
```

〔그림 4〕〔15〕 공격 지점

SABER 알고리즘에서 찾고 마스킹된 증분 공간의 구간에 대한 파형을 딥러닝 네트워크의 입력층에 넣고 해밍무게로 라벨링하여 학습시켰다.

3.1.3. Decryption-Failure(DF) 오라클 기반 부채널 공격

[19]에서 소개한 DF 기반 오라클 공격은 [6],[21]의 마스킹된 비교연산에 대한 부채널 취약점을 이용하여 DF 오라클을 만들어 키를 복구한다. 공격자는 암호문을 임의로 초기화한 e만큼 수정하여 DF를 유도한 뒤 부채널 파형에서 t-test를 통해 DF 여부를 확인한다. DF가 일어나지 않았을 경우 DF가 일어날 때까지 e 값을 수정, 파형 수집, DF 여부 확인을 반복한다. 이를 통해 정확한 노이즈 값 e를 복구할 수 있고 메시지 인코



〔그림 5〕 LWE/LWR 기반 KEM에 대한 오라클 기반 부채널 공격 논문의 파형 수집 시점

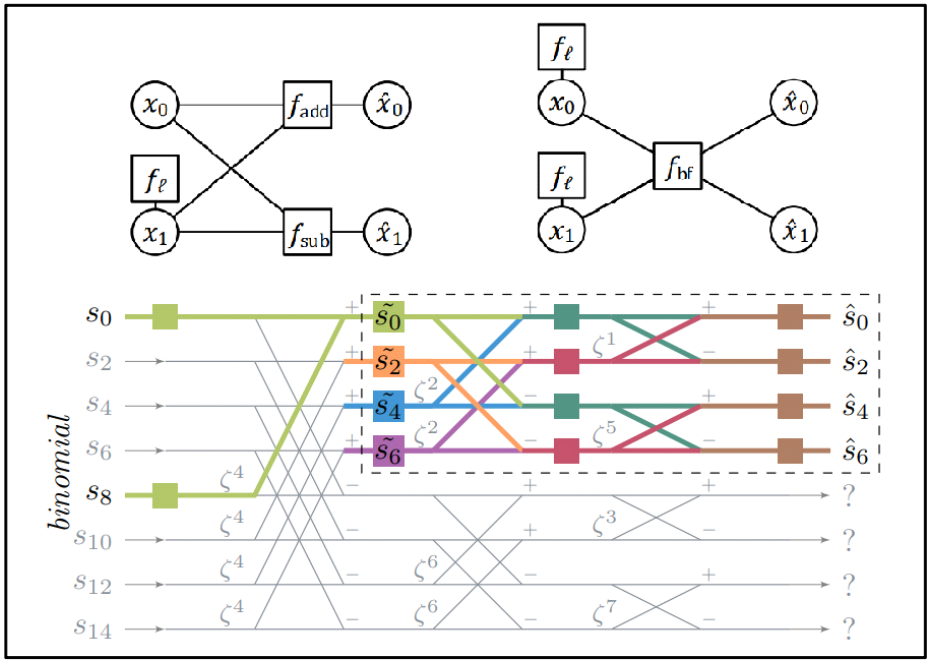
딩 방정식을 만들어 비밀키 값을 알아낼 수 있다.

[14]에서 소개한 DF 기반 오라클 공격은 CRYSTALS-KYBER에 대한 오류 주입 공격이다. 선택 암호문 공격이며 캡슐화 과정의 모든 중간값을 인지한다고 가정한다. CRYSTALS-KYBER의 메시지 인코딩 과정 중 (+q/2) 과정을 오류 주입으로 생략한다. 이때 오류 주입으로 인한 메시지 복호화 성패 여부를 부채널 정보로 추출하여 DF 오라클을 구성한다. 이 DF 오라클을 통해 노이즈와 비밀키에 대한 2n개의 선형 부등식을 형성하고 LP solver나 신뢰전파 알고리즘을 통하여 이 부등식을 풀어 비밀키를 추출한다.

[17]에서 소개한 DF 기반 오라클 공격은 KEM알고리즘에 대한 범용적인 전력, 전자기파 공격이다. [14],[19]가 디캡슐화 과정 중 비교연산의 부채널 정보를 통해 DF 오라클을 구성하여 노이즈와 비밀키값에 관한 식을 만들었던것에 반해 [17]은 재암호화의 의사난수함수의 부채널 정보를 통해 DF 오라클을 구성한다. KEM의 디캡슐화 과정 중 재암호화는 같은 입력으로부터 기존 암호문과 같은 출력을 만들기 위해 시드값을 파라미터로 받는다. 이때 복호화 오라클의 출력값(메시지 인코딩 값)과 공개키를 연접해 해쉬함수를 거친 값을 시드값으로 사용한다. 따라서 만약 DF가 일어났을 경우 복호화 오라클은 잘못된 평문을 출력할 것이고 이로 인해 해쉬값이 바뀌어 결과적으로 의사난수함수의 입력으로 들어갈 시드값이 완전히 바뀌게 된다. [17]은 이 의사난수함수에서 얻은 부채널 정보에서 딥러닝 기반 프로파일링을 통해 메시지 복호화 성패 여부를 알아내고 이를 통해 DF 오라클을 구성한다.

3.1.4. 기반 연산 소프트웨어 구현에 대한 부채널 공격

[11], [13], [18]에서 소개한 부채널 공격은 기반연산 소프트웨어 구현에 대한 공격이다. CRYSTALS-KYBER의 INTT, NTT를 대상으로 Soft Analytical Side Channel Attack(SASCA)을 적용하여 얻은 부분 비밀정보를 바탕으로 BKZ 알고리즘 등의 격자 디코딩을 통하여 비밀키를 추출한다. [18]은 INTT 연산의 입력값과 회전인자의 곱셈 결과값에 대해 템플릿을 형성하였고 이를 바탕으로 신뢰 전파 알고리즘을 실행하여 비밀 부분정보를 추론하였다. 그러나 이러한 방법은 백만이 넘은 템플릿을 필요로 하고 그래프에 국소적인 루프가 생겨 신뢰전파 성능을 저하하였다. 이를 해결하기 위해 [13]는 입력값이 load/store 될 시점의 해밍무게 템플릿을 만들어 좁은 영역에서의 그래프 루프를 피하고 신뢰



〔그림 6〕〔18〕 인자 그래프(왼쪽 위), 〔13〕 인자 그래프(오른쪽 위), 〔11〕 인자 그래프(아래)

전파 알고리즘 성능을 향상하였다. 그러나 load/store 해밍무게 템플릿과 신뢰전파 알고리즘 만으로 실용적으로 키를 복구하는데 한계가 있었다. [11]에서는 선택 암호문 공격을 가정하고 NTT 도메인에서 sparse vector를 형성하는 선택 암호문을 만든다. 해당 선택 암호문을 CRYSTALS-KYBER 디캡슐화에 입력하고 그림 6과 같이 작은 범위의 비밀키가 관여한 인자 그래프를 형성한다. 그 다음 신뢰 전파 알고리즘을 이용하여 NTT 도메인 상 비밀키의 부분값을 복원한다.

3.2. NTRU에 대한 부채널 공격

NTRU[5]는 역사가 가장 오래된 격자 암호로 2017년 NIST에서 주관하는 표준화 작업이 진행되기 전부터 부채널 분석 기법이 많이 등장하였다. NTRU의 경우 기반 연산 소프트웨어 구현에 대한 부채널 공격만이 제안되어 따로 소단원을 나누지 않고 진행할 예정이다.

2008년, [3]에서 소개한 NTRU를 대상으로 한 첫 부채널 공격은 RFID에서 구현된 NTRU의 복호화 과정 중에 일어나는 암호문과 비밀키의 곱셈 과정에서 일어나는 전력을 대상으로 CPA 공격이다. RFID에서 구현된 NTRU 복호화 과정에서는 암호문과 비밀키의 곱셈 과정에서 일어나는 계수간의 곱셈이 발생하는데 NTRU 구조 특성상 비밀키의 계수가 -1, 0, 1만 가능하므로 암호문과 비밀키의 곱셈 과정에서 일어나는 계수간의 곱셈의 결과는 암호문의 값이 e인 경우, 비밀키의 계수 값에 따라 각각 $-e$, 0, e로 나타나게된다. 이때 7비트 연산을 수행하는 구조 특성상 $-e = (e \oplus 127) + 1$로 표현 가능하며 암호문의 값을 공격자가 알고 있다면, $-e$, 0, e의 해밍무게를 이용하여 비밀키를 복구할 수 있다.

2010년, [9]에서 소개한 부채널 공격은 Convolution Product 계산에서의 SPA, CPA 공격을 다루고 있다. 실제 NTRU에서는 계수가 -1, 0, 1을 가지는 ternary polynomial을 비밀키로 사용하지만, 해당 연구에서의 공격은 ternary polynomial과 계수가 0, 1을 가지는 binary polynomial과 동일한 공격 구조를 가지기 때문에 후에 설명은 binary polynomial에 대한 공격으로 대체한다. NTRU를 대상으로 하는 SPA 공격은 0이 아닌 두 수의 덧셈과 0을 포함하는 두 수의 덧셈과 파형의 패턴이 다름을 이용한다. 덧셈의 한 피연산자의 값이 0이라면 덧셈 연산 대신 메모리 복사 연산이 발생하므로 실제 덧셈 연산의 파형과는 다른 모양의 파형이 발생한다. Convolution Product 특성상 새로운 인덱스가 등장하는 부분만큼 메모리 복사 연산이 일어나므로 메모리 복사 연산이 일어나는 부분의 수로 비밀키 내부 1의 위치를 파악할 수 있다. NTRU를 대상으로 하는 CPA 공격은 암호문의 어떤 부분이 암호문의 처음 부분과 더해지는지를 이용한다. 예를 들어 비밀키의 계수가 1인 위치가 1과 4에 있었다면, 암호문의 네 번째 수가 처음에 존재하고 암호문의 첫 번째 수가 그 후에 더해지게 될 것이다. 그렇다면 각 암호문의 각 위치에 암호문의 첫 번째 수를 더한 후 그때의 해밍거리를 이용하여 CPA 공격을 수행하여 암호문의 네 번째 수가 더해짐을 알게 된다면, 공격자는 비밀키의 계수가 1인 위치의 거리가 3임을 알 수 있다.

2013년, [23]에서 소개한 부채널 공격은 [9]에서 제시한 부채널 대응 기술을 충돌 공격을 통해 무력화시킨다. 무작위 초깃값을 사용하는 Convolution Product에 대해서 각 레지스터에 무작위 초깃값을 로드하는 부분에서의 MOV 연산과 암호문의 첫 부분과 덧셈이 일어나기 직전에서의 MOV 연산과의 충돌 공격을 이용한다. 해당 공격을 통해 어떠한 레지스터에서 암호문의 첫 부분과 덧셈이 일어나는지 알 수 있으며 이는 비밀키의 계수 값이 1인 위치를 알 수 있게 해 준다.

2017년 NIST에서 주관하는 PQC 표준화 1 Round에서는 NTRUEncrypt가 등장했다. 그 후 2018년에 [1]은 이전의 NTRU 버전과 NTRUEncrypt 모두에 대한 단일 파형 공격을 제안한다. 이전의 NTRU 버전에 대한 단일 파형 공격은 다항식의 곱셈이 일어나는 부분에서 발생하는 다수의 덧셈 연산들에 대해 반복문이 끝나

Algorithm 1 Convolution Product Computation

Input: b (array of d locations for '1' representing the binary polynomial $a(X)$); $c(X)$ (general polynomial).
Output: $t(X)$.

```
for 0 ≤ j < 2N do
    t_j ← 0        // t_N through t_{2N−1}: temporary buffer
end for
for 0 ≤ j < d do
    for 0 ≤ k < N do
        t_{k+b[j]} ← t_{k+b[j]} + c_k
    end for
end for
for 0 ≤ j < N do
    t_j ← (t_j + t_{j+N}) mod q
end for
```

〔그림 7〕 Convolution Product 계산

〔그림 8〕 충돌공격 예시

는 부분에서는 파형이 살짝 변함을 이용한다. 알고리즘 특성상 파형이 변하는 부분이 두 부분 발생하게 되는데 이 사이에서 몇 번의 덧셈 연산이 진행되었는지 조사한 후 그 값이 비밀키와 관련된 정보가 나오게 된다. 이때 파형이 살짝 변하는 부분을 눈으로 확인하기보단 덧셈 파형 하나를 이용해서 밀면서 상관계수를 계산한다면, 상관계수가 유난히 낮은 두 구간의 거리를 확인하는 방법으로 계산하면 쉽다. NTRUEncrypt에 대한 단일 파형 공격은 비밀키의 계수 값에 따라 해밍무게의 차이가 큰 중간값을 이용해 비밀키의 계수를 복원하는 방식이다.

2020년 NIST에서 주관하는 PQC 표준화 3 Round에서는 1 Round에서 등장한 NTRUEncrypt와 NTRU-HRSS-KEM을 합쳐 최종 NTRU 알고리즘으로 등장한다. 그 후 2021년에 [2]에서 소개한 부채널 공격은 복호화 부분에서 디코딩 알고리즘을 대상으로 한 단일 파형 공격이다. 디코딩 알고리즘에서는 mod3 알고리즘과 poly_Z3_to_Zq 알고리즘이 동작하며 각 알고리즘은 중간값에 따라 두 개의 그룹을 생성하며 두 그룹 사이의 해밍무게의 차이가 크기 때문에 전력 파형을 분석하면 어떠한 그룹에 속하는지 알 수 있다. 그 후 대수적 공격을 통해 비밀키의 일정 부분 복구가 가능하다.

Ⅳ. NIST PQC Round 3 격자기반 KEM에 대한 부채널 대응기법

4.1. SABER에 대한 부채널 대응 기법

[10]에서 제시한 부채널 대응기법은 SABER 디캡슐화에 대한 1차 산술 마스킹 기법이다. A2A 알고리즘을 제시하여 산술 마스킹을 유지한채 SABER의 shift 연산을 빠른 속도로 수행할 수 있게 하였다. 기존 Shift 연산을 사용하기 위해서 A2B, B2A 변환을 사용하였지만. A2A 알고리즘은 최하위부터 상위 n-1번째 비트까지 기존 A2B와 같이 캐리값을 계산한 뒤 하위 n 비트를 버려 산술 마스킹을 유지한채 shift 연산을 수행한다. ARM Cortex-M4 환경에서 구현한 1차 마스킹 SABER는 2.5배 정도의 오버헤드가 발생하였고 A2A 알고리즘을 사용한 마스킹 기법이 A2B 알고리즘을 사용한 마스킹 기법보다 5배 성능 향상을 보였다.

4.2. CRYSTALS-KYBER에 대한 부채널 대응 기법

[7]에서 제시한 부채널 대응 기법은 CRYSTALS-KYBER 디캡슐화에 대한 고차 산술 마스킹 기법이다. NTT 등 대부분의 연산은 산술 연산에 대해 선형이므로 따로 고려할 필요가 없으나 Compress, Comparison 연산은 비선형 연산이므로 산술 마스킹을 유지하려면 특별한 알고리즘을 필요로 한다. [7]에서 이를 해결하기 위해 High-Order n Bit Compression과 Decompressed Comparison 알고리즘을 제시하였다. High-Order n Bit Compression은 CRYSTALS-KYBER 다항식 계수에 q/4를 더한 뒤 이진 탐색을 이용하여 상위비트의 연산만으로 마스킹을 유지한 채 Compress 값을 계산하는 알고리즘이다.

Decompresseed Comparison 알고리즘은 CRYSTALS-KYBER의 기존 비교연산을 마스킹할 때 나타나는 두가지 문제점을 해결하기 위해 제시되었다. 첫번째 문제는 [6],[21]가 제시한 비교연산 마스킹이 부채널 공격에 취약하다는 것이 [19]에서 밝혀졌다는 것이고 두번째 문제는 비교연산을 수행하기 전 Compression 연산을 마스킹하려면 큰 연산시간이 소모된다는 것이다. 이를 해결하기 위해 Decompressed Comparison 알고리즘은 Compression 연산을 하지 않고 마스킹된 상태에서 값의 범위를 체크하여 비교연산을 수행하였다. ARM Cortext-M0와 ‐M4 위에서 1차 마스킹 CRYSTALS-KYBER는 마스킹하지 않을 때보다 2.7~3.5의 오버헤드를 발생시켰다.

4.3. NTRU에 대한 부채널 대응 기법

2010년, [9]에서 제시한 부채널 대응 기술은 Convolution Product 계산에서의 CPA에 대한 대응 기

술을 다루고 있다. 3장에서 다룬 CPA 공격에서 값이 변화하는 부분의 해밍거리를 예측하여 공격했었는데, 이를 막기 위한 세 가지 방법을 소개한다. 첫 번째 방법은 기존 초깃값을 0이 아닌 무작위 값으로 바꾼 후 계산이 전부 끝난 후 그 값을 빼주는 방식을 통해 원래 계산 결괏값으로 돌려주는 방식이다. 기존 초깃값에 따라 해밍거리가 달라지기 때문에 공격자는 값을 쉽게 예측할 수 없게 된다. 두 번째 방법은 계산되기 전 암호문에 일정 값을 더한 후, 모든 Convolution Product 계산이 끝난 후 원래 계산값으로 돌리는 방식이다. 첫 번째 방법과 유사하게 더한 값에 따라 해밍거리가 달라지기 때문에 공격자가 값을 쉽게 예측할 수 없게 된다. 마지막 방법은 하이딩 기법으로 더하는 순서를 무작위로 섞는 방법이다. 어떠한 계산이 먼저 되었는지 공격자는 알 수 없으므로 공격에 필요한 파형의 위치를 찾기 힘들게 된다.

2017년, [22]에서 제시한 부채널 대응 기술은 2013년에 등장한 충돌 공격[23]에 대한 부채널 대응 기술이다. NTRU에서 $x^N = 1$임을 이용하여 무작위로 i를 선정 후, 비밀키에는 x^i를 곱하고 암호문에는 x^{N-i}를 곱해 기존 비밀키와 암호문을 곱하는 것과 같은 결과를 일으키는 방법을 사용한다. 하지만 이런 간단한 방법으로도 공격자는 암호문의 첫 번째 값이 무엇인지 알 수 없으므로 공격 복잡도가 커지게 된다.

2019년, [20]에서 제시한 부채널 대응 기술은 ARM Cortex-M4에서 동작하는 NTRUEncrypt에서의 마스킹 알고리즘을 다룬다. 일반적인 마스킹 알고리즘과 동일한 방법을 취하며 암호문에 마스크값을 더한 상태로 곱셈 연산을 진행한 후 비밀키와 마스크값의 곱한 값과의 차이는 암호문과 비밀키를 곱한 값과 같게 된다. 하지만 공격자로서는 마스크값을 알 수 없으므로 중간값에 대한 예측이 불가능해 CPA 공격을 수행할 수 없게 된다.

Ⅴ. 결 론

본 논문은 NIST가 PQC Round 3 평가 기준에 부채널 분석과 오류 주입에 대한 안전성을 제시한 뒤 빠르게 제시되고 있는 부채널 공격 시나리오 및 대응 기법 동향에 대해 소개하였다. LWE/LWR 기반 KEM과 달리 NTRU는 오라클 기반 공격 시나리오가 없어 범용적인 적용이 불가능하며 추후 NTRU 오라클 기반 공격 시나리오가 새롭게 나올 것으로 생각된다. 또한 pqm4 라이브러리의 기반 연산 구현에 대한 범용적 공격 시나리오도 활발히 연구될 것으로 예상된다.

참 고 문 헌

[1] AnSoojung, KimSuhri, JinSunghyun, KimHanbit, KimHeeseok. "Single Trace Side Channel Analysis on NTRU Implementation.", Applied Sciences 8. 2018.

[2] Askeland, Amund , and Sondre Ronjom. "A Side-Channel Assisted Attack on NTRU." IACR CryptoI. ePrint Arch.. 2021. 790.

[3] Atici, Ali Can, Lejla Batina, Benedikt Gierlichs, and Ingrid Verbauwhede. "Power analysis on NTRU implementations for RFIDs: First results." 2008.

[4] Bo-Yeon Sim, Jihoon Kwon, Joohoo Lee, Il-Ju Kim, Tae-Ho Lee, Hyojin Yoon, Jihoon Cho, Dong-Gak Han. “Single-trace attacks on message encoding in lattice-based KEMs”, IEEE Access, 8:183175-183191, 2020

[5] Chen, Cong , Oussama Danba, Jeffrey Hoffstein, Andreas Hulsing, Joost Rijneveld, John M Schanck, Tsunekazu Saito, Peter Schwabe, William Whyte, Keita Xagawa, Takashi Yamakawa, and Zhenfei Zhang. " NTRU Algorithm specifications and supporting documentation." Accessed. 2019.

[6] Florian Bache, Clara Paglialong, Tobias Oder, Tobias Schneider, Tim Güneysu, “High-speed masking for polynomial comparison in lattice-based KEMs”.IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020:483-507, 2020.

[7] Joppe W. Bos, Marc Gourjon, Joost Renes, Tobias Schneider, Christine van Vredendaal, “Masking Kyber: First- and Higher-Order Implementations”, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021:173-214, 2021.

[8] Kalle Ngo, Elena Dubrova, Qian Guo, Thomas Johansson. “A Side-Channel Attack on a Masked IND-CCA Secure Saber KEM Implementation”, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021:676-707, 2021.

[9] Lee, MunKyu , JeongEun Song, Dooho Choi, and DongGuk Han. "Countermeasures against Power Analysis Attacks for the NTRU Public Key Cryptosystem." IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences. 2010. 153-163.

[10] Michiel van Beirendonck, Jan-Peter D’anvers, Angshuman Karmakar, Josep Balasch, and Ingrid Verbauwhede. “A side-channel-resistant implementation of SABER”, ACM Journal on Emerging Technologies on Computing Systems, 17(2), 2021.

[11] Mike Hamburg, Julius Hermelink, Robert Primas, Simona Samadjiska, Thomas Schamberger, Silvan Streit, Emanuele Strieder, Christine van Vredendaal. “Chosen Ciphertext k-Trace Attacks on Masked CCA2 Secure Kyber”, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021:88-113, 2021.

[12] Matthias J. Kannwischer, Peter Pessl, Robert Primas. “Single-Trace Attack on Keccak”, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020:243-268, 2020.

[13] Peter Pessl, Robert Primas. “More practical single-trace attacks on the number theoretic transform”, LATINCRYPT, volume 11774 of Lecture Notes in Computer Science, pp 130-149. Springer, 2019.

[14] Peter Pessl, Lukas Prokop. “Fault attacks on CCA-secure lattice KEMs”, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021:37-60, 2021

[15] Prasanna Ravi, Shivam Bhasin, Sujoy Sinha Roy, Anupam Chattopadyay. “On exploiting message leakage in (few) NIST PQC candidates for practical message recovery and key recovery attacks”, IACR ePrint archive: Report 2020/1159, 2020. https://eprint.iacr.org/2020/1559.

[16] Prasanna Ravi, Sujoy Sinha Roy, Anupam Chattopadhyay, Shivam Bhasin. “Generic Side-Channel attacks on CCA-secure lattice-based PKE and KEMs”, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020:307-335, 2020.

[17] Rei Ueno, Keita Xagawa, Yutaro Tanaka, Akira Ito, Junko Takahashi, Naofumi Homma. “Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs”, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022:296-322, 2022.

[18] Robert Primas, Peter Pessl, Stefan Mangard. “Single-trace side-channel attacks on masked lattice-based encryption”, In International Conference on Cryptographic Hardware and Embedded Systems, volume 10529 of Lecture Notes in Computer Science, pp. 513-553. Springer, 2017

[19] Shivam Bhasin, Jan-Pieter D’Anvers, Daniel Heinz et al. “Attacking and Defending Masked Polynomial Comparison for Lattice-Based Cryptography”, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021:334-359, 2021.

[20] ThomasSchamberger, OliverMischke, JohannaSepulveda. "Practical Evaluation of Masking for NTRUEncrypt on ARM Cortex-M4." "Constructive Side-Channel Analysis and Secure Design." Springer: 2019. 253-269.

[21] Tobias Oder, Tobias Schneider, Thomas Pöppelmann, Tim Güneysu. “Practical CCA2-secure masked Ring-LWE implementations”, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018:142-174, 2018.

[22] WangAn, WangCe, ZhengXuexin, TianWeina, XuRixin, ZhangGuoshuang. "Random key rotation: Side-channel countermeasure of NTRU." "Computers & Electrical Engineering." ELSEVIER: 2017. 220-231.

[23] Zheng, Xuexin , An Wang, and Wei Wei. First-order collision attack on protected NTRU cryptosystem. 6-7. Vol. 37. Microprocessors and Microsystems: 2013.

[24] Zhuang Xu, Owen Pemberton, Sujoy Sinha Roy, David Oswald. “Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of Kyber”, IACR ePrint archive: Report 2020/912, 2020. https://eprint.iacr.org/2020/912.

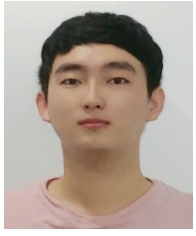
〈저 자 소 개〉

이 정 환 (JeongHwan Lee)

학생회원

2017년~현재 : 고려대학교 과학기술대학 인공지능사이버보안학과 학사과정

<관심분야> 부채널 공격, 부채널 대응, 공개키 암호



김 규 상 (GyuSang Kim)

학생회원

2020년 2월 : 연세대학교 수학과 학사

2020년 9월~현재 : 고려대학교 정보보호학과 석박사 통합 과정

<관심분야> 공개키 암호, 부채널 공격

김 희 석 (HeeSeok Kim)

정회원

2006년 : 연세대학교 수학과 학사

2008년 : 고려대학교 정보보호대학원 석사

2011년 : 고려대학교 정보보호 대학원 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 인공지능사이버보안학과 부교수

<관심분야> 부채널 공격, 암호시스템 안전성 분석 및 고속구현, 암호칩 설계 기술, 보안관제, 네트워크 보안