정 보 보 호 학 회 지
제 31 권 제1호, 2021. 2

NIST PQC Round 3 격자 기반 암호의 부채널 대응 기법 동향 분석

송 진 교*, 김 영 범*, 곽 유 진**, 서 석 충***

요 약

NIST(National Institute of Standards and Technology) 양자 내성 암호 표준화 사업이 3차 라운드에 접어들면서, 3라운드 후보자에 대한 실제 구현 결과 및 관심이 꾸준히 증가하고 있다. 3라운드 후보자 중 대부분(5/7)은 격자 기반 암호이며, 격자 기반 암호는 다른 기반의 양자 내성 암호보다 효율적인 연산 처리로 인해 제약적인 리소스를 가진 임베디드 환경에서도 적용이 가능한 장점이 존재한다. 그러나 특히 임베디드 환경에서는 암호 알고리즘이 동작 시 발생하는 추가적인 정보(전력, 전자파, 시간차, 오류주입 등)를 이용한 부채널 공격에 취약하다. 실제 다수의 연구가 양자 내성 암호의 부채널 공격에 대한 가능성을 제시하고 있다. 여전히 부채널 공격은 양자 내성 암호를 표준화하기 위해 상당한 장애물이며, 이에 대응하기 위해서는 구현 시 부채널 대응 기법이 적용되어야 한다. 따라서 본 논문에서는 NIST PQC 3라운드 격자 기반 암호의 부채널 대응 방안에 대한 최신 동향을 분석한다, 또한 향후, NIST PQC 3라운드 격자 기반 암호의 연구 전망을 논의한다.

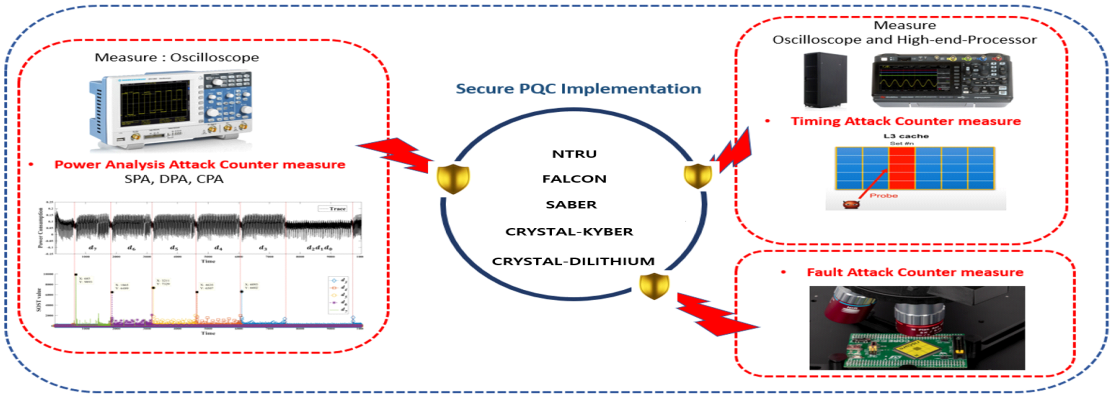
Ⅰ. 서 론

양자 컴퓨터의 발전으로, 기존 인수분해, 이산로그 등의 수학적인 안전성에 기반을 둔 공개키 암호 시스템에 Shor 알고리즘 [1]을 적용하게 되면 다항시간 내에 풀리게 된다. 이에 따라 NIST에서는 2016년부터 양자 컴퓨터 환경에서도 안전한 양자암호 표준화 사업을 진행하고 있으며, 현재 3라운드가 진행 중에 있다. 3라운드 후보자 대부분 (5/7)은 격자 기반 암호이며, 키 교환 메커니즘에서는 SABER, CRYSTAL-KYBER, NTRU, 전자서명에서는 CRYSTAL-DILITHIUM, FALCON이 해당된다. 격자 기반 암호는 행렬 곱셈 시, NTT(Number Theoretic Transform)와 같은 효율적인 알고리즘이 존재하며, 적절한 키 사이즈로 인해 임베디드 환경에서도 효율적으로 적용이 가능하다.

부채널 분석은 암호 알고리즘이 동작 시 발생하는 부가적인 정보를 가지고 비밀 키를 획득하는 공격으로써, 특히 임베디드 환경에서 매우 취약하다. 부채널 분석은 크게 침입공격, 준침입공격, 비침입공격으로 분류되며, 침입공격은 공격자가 물리적인 메모리에 접근하여 실제 비밀키의 정보를 획득하는 것이다. 준침입공격은 물리적인 장치에 오류를 주입하여 비밀키를 획득하는 공격이다. 대표적으로 DFA(Differential Fault Attack)이 존재한다. 비침입공격은 전력, 전자파, 시간차 등의 부가적인 정보를 통해 비밀키를 획득하는 공격이며, 대표적으로 SPA(Simple Power Analysis), DPA(Differential Power Analysis), TA(Timing Attack) 공격이 존재한다.

양자 내성 암호는 수학적으로 양자 컴퓨팅 환경에서 안전하도록 설계되었지만, 여전히 부채널 분석에는 취약점이 존재한다. 2018년 S.J. An 등은 격자 기반의 행렬 곱셈에서 핵심적인 연산을 수행하는 NTT에서의 single-trace attack 공격을 소개하였다[2]. 이는 NTT를 사용하는 다양한 격자 기반 암호에 적용 가능하며, 실제 키를 복구할 수 있었음을 보여주었다. 2016년 L.G. Bruinderink 등은 Flush+Reload 캐시 타이밍 공격을 통해 CDT 또는 Bernoulli 샘플링을 사용하여 이산 가우시안 분포에서의 비밀키를 추출하는 방법을 제안하였다[3]. 이외에도 많은 NIST 3 Round 격자기반 암호에 대한 부채널 공격에 대한 연구결과가 존재한다. 따

이 논문은 2020년도 정부의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2019R1F1A1068494)
* 국민대학교 금융정보보안학과(대학원생, sjk9304@kookmin.ac.kr, darania@kookmin.ac.kr)
** 국민대학교 정보보안암호수학과(학부생, youjk@kookmin.ac.kr)
*** 국민대학교 정보보안암호수학과, 금융정보보안학과 (조교수, scseo@kookmin.ac.kr)



〔그림 1〕 부채널 분석 기법

라서 구현 시 부채널 공격에 대한 대응 방안이 고려되야한다.

본 논문에서는 NIST 3 Round 격자 기반 암호의 최근 부채널 대응기법에 대한 동향을 소개한다. 본 논문의 구성은 다음과 같다. 2장에서는 부채널 분석 기법(Timing Attack, Power Analysis, Fault Attack)을 설명한다. 3장에서는 NIST PQC 공모전 3라운드의 암호들에 대한 부채널 취약점을 분석하며, 4장에서는 NIST 3 Round 격자 기반 암호의 부채널 대응기법의 동향을 분석한다. 마지막으로 결론 및 향후 연구 전망을 제시하고 본 논문을 마무리한다.

Ⅱ. 격자기반 암호의 부채널 분석 기법

2.1. 타이밍 공격 (Timing Attack)

타이밍 공격은 암호 알고리즘이 동작 시 발생하는 시간차를 통해 비밀 값에 대한 정보를 분석하는 부채널 분석 기법이다. 즉, 타이밍 공격은 중간 연산과정에서 발생하는 시간 차이 정보를 이용하여 비밀 값을 분석하는 것이다. 중간 연산과정이 비밀 값에 의존하지 않는 Constant-time 구현이 아닐 경우 타이밍 공격에 취약하며, 대표적으로 타원곡선암호나 RSA 등에 대한 타이밍 공격 방법들이 제안되었다. 격자 기반 암호에서도 일부 Constant-time 구현이 아닌 부분이 존재하므로, 타이밍 공격에 취약하다. 이에 대응하기 위해서는 마찬가지로 비밀 값에 의존하지 않는 연산과정으로 구현된 Constant-time 구현이 요구된다. 또한, 2005년에 D.J.Bernsteint 등은 타이밍 공격을 캐시로 확장하여 AES에 대한 캐시 타이밍 공격을 제안하였다[4]. 캐시 타이밍 공격은 중간 값에 따라 캐시에 저장된 테이블에 접근확인을 통해 비밀키의 정보를 분석하는 기법이다. 최근 캐시 타이밍 공격은 실용적인 부채널 분석 기법이 되었으며, 특히 격자 기반 암호에서도 테이블 조회 기반 샘플링의 경우에는 캐시 타이밍 공격에 취약할 수 있다. 캐시 타이밍 공격을 대응하기 위해서는 메모리 접근에 대한 Shuffling 기법과 중간 값을 숨기는 마스킹 기법을 통해 대응할 수 있다.

2.2. 전력분석 (Power Analysis)

전력 분석은 암호 알고리즘이 동작 시 발생하는 전력을 통해 비밀 값에 대한 정보를 분석하는 부채널 분석 기법이다. 전력 분석 시에는 파워모델을 가지고 분석이 이루어지며, 헤밍 웨이트, 헤밍 디스턴스 모델 등이 존재한다. 분석하는 파형의 수에 따라 단순 전력 분석, 차분 전력 분석, 상관 전력 분석으로 분류된다. 단순 전력 분석은 소수의 전력 파형을 분석하여 비밀 값을 분석하는 공격 기법이다. 또한, 차분 전력 분석, 상관 전력 분석은 다수의 전력 파형을 분석하여 평균의 차와 상관계수를 통계적 분석을 통해 비밀 값을 분석하는 공격 기법이다. 이러한 전력 분석 공격들을 통해 공격자는 공개키암호 및 대칭키 암호에서 사용자의 비밀 키를 복구할 수 있다. 단순 전력 분석은 타원곡선암호와 RSA와 같은 공개키암호에 취약하다. 또한, 차분 전력 분석과 상관 전력 분석은 대칭키 암호 및 공개키 암호에 모두 취약하다. 모든 전력 분석에 취약한 원인은 비밀 키에 의존하여 연산이 수행되기 때문이다. 격

자 기반 암호에서도 역시 비밀 키에 의존하여 연산이 수행되는 부분이 있으므로, 전력 분석에 취약점이 존재한다. 이러한 전력 분석에 대응하기 위해서는 비밀키의 의존성을 제거하는 Constant-time 구현과 중간 값을 무작위화하는 마스킹 기법이 존재한다.

2.3 오류 공격 (Fault Attack)

오류 공격은 임베디드 환경에서 암호 알고리즘 동작 시 특정 시점에 오류를 주입하여, 비밀 값 정보를 분석하는 부채널 공격 기법이다. 일반적으로 차분 공격과 결합하여 차분 오류 공격(Differential Fault Attack)으로 응용된다. 오류주입 공격은 계산적인 오류주입과 명령어 오류주입으로 분류되며, 계산적인 오류주입은 암호 알고리즘이 동작 시 특정 위치의 레지스터 내에 워드 값을 랜덤하게 변경하는 것이다. 또한, 오류주입 시, 비트, 바이트, 워드 단위로 값에 오류를 주입할 수 있다. 명령어 오류주입은 오류를 주입하여 특정 명령어를 건너뛰는 방법이며, 대표적으로 명령어 스킵 방법이 있다. 격자 기반 암호에서의 오류주입 공격은 디지털 서명에서 서명을 위조하는데, 효율적으로 적용되고 있다. 이러한 오류주입 공격에 대응하기 위해서는 중복기법이 사용된다. 즉, 레지스터 내에 중복 값을 대입하여 암호화가 끝났을 시, 중복 값과 평문 값을 비교하여 암호화 중 공격자에 의한 오류주입 공격이 있었는지에 대한 여부를 확인하는 것이다.

Ⅲ. NIST PQC Round 3 격자기반 암호의 부채널 취약점

3.1. 타이밍 공격 (Timing Attack)

격자 기반 암호에서 시간차 공격의 취약점은 내부의 연산 중 Constant-time 구현이 아닌 연산이 존재할 경우이다. 격자 기반 암호에서는 가우시안 샘플러가 해당될 수 있다. 가우시안 샘플러에서 추출된 에러는 LWE 문제에서, 공격자가 양자 컴퓨팅으로 개인 키를 유추할 수 없도록 연산량을 높여 안전성을 보장한다. 에러값이 노출되면 비밀 값을 분석할 수 있으므로 에러 추출은 격자 기반 암호에서 가장 중요한 보안의 핵심이다. 가우시안 샘플링은 많은 연산량을 요구하므로, 실제 구현 시에는 Rejection 샘플링, CDT(Cumulative Distribution Function) 샘플링, Knuth-Yao 샘플링 등으로 구현이 된다. Rejection 샘플링은 CDT, Knuth-Yao 샘플링과 달리 사전 연산을 하지 않고, 부동소수점 연산을 수행한다. 또한, Rejection 샘플링은 거부되는 횟수의 시간 차이로 인해, 타이밍 공격에 취약하다.

CDT 샘플링은 주어진 정밀도를 통해 이산 가우시안 분포에 따라 CDF(Cumulative Distribution Function)의 테이블 T를 미리 사전 연산을 한다. CDT 샘플링은 기본적으로 CDF 테이블 T에 대한 검색 작업이며, 효율성을 높이기 위해서 이진 검색을 사용한다. 하지만 이진 검색 방법에서 불규칙한 사전 연산 테이블 접근 패턴으로 캐시 타이밍 공격에 취약하다. Knuth-Yao 샘플링은 DDG(Discrete Distribution generation) 트리로 불리는 루트 이진 트리를 사용한다. 루트 이진 트리에서 랜덤 워크가 터미널 노드에 도달하면 샘플링 프로세스가 완료된다. 하지만 데이터 의존적 분기로 인해 타이밍 공격에 취약한 단점이 존재한다.

2016년 L.G. Bruinderink 등은 Flush+Reload 캐시 타이밍 공격을 통해 BLISS의 가우시안 샘플링 과정에서 CDT 또는 Bernoulli 샘플링의 비밀키를 추출하는 방법을 제안하였다[3]. 제안하는 방법은 Flush+Reload 캐시 타이밍 공격을 적용하여 450개만의 서명만으로 공격자는 96%의 성공률로 2분 이내에 BLISS의 비밀키를 추출할 수 있음을 보여주었다.

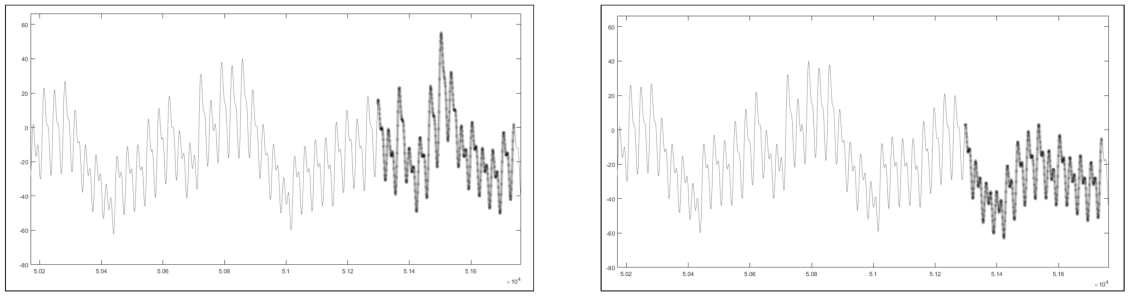
3.2. 전력분석 (Power Analysis)

KEM (Key Encapsulation Mechanism)분야 격자 기반 암호에서 캡슐화 단계에 대한 취약점이 존재한다. 2020년 B.Y. SIM 등은 메시지 인코딩 작업에 대한 단일 파형 공격을 제안했다[5]. CRYSTALS-KYBER, SABER에 대해 제안된 공격 방법은 최적화 수준과 관계없이 단일 파형만으로 100%의 성공률로 전체 비밀 메시지를 복구할 수 있음을 증명했으며, 복구된 비밀 메시지와 공개 값을 사용하여 공유 임시 세션 키를 생성하는 시나리오를 제시하였다. 핵심 아이디어는 메시지가 인코딩되면서 비밀 값이 인코딩될 때, 비트의 값이 유출되는 것을 이용하는 것이다. 따라서, 격자 기반 암호에서 메시지 인코딩 과정의 부채널 취약점에 대한 대응기법이 필요하다.

격자 기반 암호 중 NTRU 기반의 양자 내성 암호 알고리즘은 이론적 보안이 잘 연구되었지만, 전력 분석 공격기반의 부채널 공격에는 취약할 수 있다, 먼저 NTRU의 복호화 연산 중에서 내부 정보의 유출이 발생할 수 있다. 2010년 M.K. Lee 등은 NTRU의 복호화 연산 $e*f \bmod q$에 대해 단순 전력 분석 공격을 제안했다[6]. 개인 키 f의 경우 실제 소프트웨어에서 구현의 효율성을 위해 $f=1+pF$ 에서 F 을 저장하여 복호화 연산을 수행하는데, 이때 $e*F$ 컨볼루션 연산이 수행되는 시점을 부채널 공격 대상으로 잡을 수 있다. NTRU의 컨볼루션 과정은 반복적인 덧셈 연산으로 구성되며, 공격 시 단순 전력 분석의 경우 메인 변수에 0이 더해지는 경우와 0이 아닌 값이 더해지는 경우에 서로 다른 전력 소모를 보인다는 점을 이용한다. 공격자는 NTRU 복호화 시 수행되는 컨볼루션 연산의 입력인 다항식을 다양한 값으로 설정한다. 그 후에, 컨볼루션 연산을 수행한 후 비교하여 비밀 값을 공격한다. 또한, 최근 S.J. An 등은 복호화 연산에 대한 단일 파형 분석 공격이 발표하였다[2]. NTRU기반 암호의 복호화 연산에 부채널 대응기법이 필수적 이게 되었다.

격자기반 암호 (LWE\LWR)의 경우 핵심 연산 및 세부 연산에서 전력 분석 공격이 시행될 수 있다. 핵심연산의 경우 CRYSTALS-KYBER와 CRYSTALS-DILITHIUM에 사용되는 NTT 알고리즘에서 전력 분석 기반 공격을 통해 보안이 유지되어야 하는 비밀 값이 노출될 수 있다. 2017년 Primas R 등은 NTT 알고리즘에 대한 효과적인 전력 분석 공격 방법이 제안되었다[7]. 공격 방법은 크게 3단계로 구성된다. 첫 번째는, KEM 분야 암호들의 복호화 과정에서 역 NTT 컨볼루션이 수행되는 각 모듈식 연산에 템플릿 매칭을 수행한다. 그 후 전체 NTT 연산의 그래프 구조와 신뢰전파 (Belief Propagation, BP)를 이용해 연산과정의 정보들을 수집한다. 마지막으로 복원된 비밀 값과 공개키를 이용하여 개인 키를 복원한다, 구체적으로 먼저 공개키의 크기를 줄인 다음 격자 디코딩을 수행하여 전체 암호 해독키를 복구한다. NIST PQC 공모사업 3라운드에서 CRYSTAL 알고리즘과 NTRU 알고리즘이 NTT를 사용 중이다.

세부 연산의 경우 CDT 샘플러는 STA에 안전하지 않을 수 있다. Constant-time CDT 샘플러를 사용하는 격자 기반 암호 (LWE) 시스템을 공격자가 STA를 통해 복구된 오류 벡터를 사용하여 개인 키를 탈취할 수 있기 때문이다[13]. 샘플링에 대한 STA는 다음과 같이 수행된다. 공격자가 약 2000개의 값을 샘플링 하는 전력 소비 추적을 얻는다고 가정한다. 그 뒤 공격자는 전력 소비 트레이스를 나누어 2000개의 하위 트레이스를 생성하고, 각 트레이스에 대하여 공격자는 알고리즘의 루프를 식별한다. 그 뒤 공격자는 임계 값을 설정한 후 각 루프에 대해 전력 소비량을 평균화하고 이를 임계값과 비교한다. 평균이 임계 값 보다 큰 경우 샘플링된 값에 1을 증가시킨다. 추가된 1의 합계가 샘플링된 값과 같으므로 공격자는 샘플링된 값을 복구할 수 있다. 또한, 샘플링된 값의 부호 비트도 상기 과정과 비슷하게 진행하여 공격할 수 있다. [그림 2]는 부호 비트에 따른 전력 소비 파형을 나타낸다. (a)는 부호 비트가 1 이래의 전력 소비 파형이며, (b)는 부호 비트가 0일 때 전력 소비 파형이다. 공격자는 단일 전력 소비 파형을 통해 정확하게 샘플링된 값인지 확인할 수 있다. 따라서, CDT 샘플러의 경우 비밀 값의 유출이 발생할 수 있다.



(a) (b)

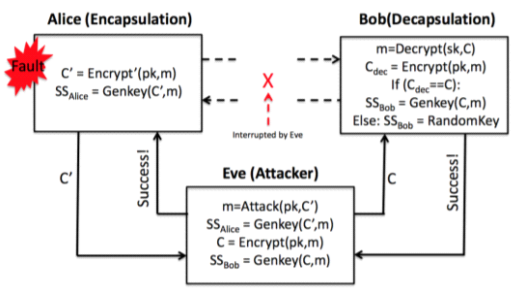
〔그림 2〕 부호비트에 따른 전력 소비 파형 (a : 부호 비트 = 1, b : 부호 비트 = 0)〔8〕

3.3. 오류 공격 (Fault Attack)

격자 기반 암호에서의 오류주입 공격의 대부분은 난스 재사용 시나리오를 만드는 것이다. LWE 구조에서 비밀 s와 오류 e 구성요소는 난스 값만 다른 시드를 사용하여 생성된다. 이러한 시드들은 XOF 함수에 추가 입력으로 입력되어, 다항식을 생성한다. 난스 재사용 시나리오는 s와 e를 같게 만드는 것이며, 이때 오류주입를 주입한다. 비밀 s와 오류 e가 같으면 변형된 LWE 구조를 형성하고, 가우시안 제거를 통해 비밀 s 값을 알 수 있다.

2018년 L.G. Bruinderink 등은 CRYSTALS-DILITHIUM, qTESLA에서 단일 랜덤 오류들을 통해 난스 재 사용 시나리오를 제안하였다 [9]. CRYSTALS-DILITHIUM, qTESLA에서는 서명 생성 시 다음과 같은 식이 요구된다. z=y+cs, 여기서 c는 챌랜지 값이며, s는 비밀, y (nonce)는 결정론적으로 계산된 값이다. 제안하는 방법에서는 챌랜지 c의 계산에 오류를 주입하여 값을 그대로 유지함으로써, 임시 값을 재사용하는 시나리오를 제안하였다. 다른 챌랜지 c가 있는 동일한 메시지의 두 서명은 행렬 계산을 통해 개인 키 s 값을 추출할 수 있다. 제안하는 방법을 ARM Cortex-M4 마이크로 컨트롤러에서 글리칭을 수행하여 공격에 대한 실험적 검증을 제공하며, 서명 절차 중 임의의 오류가 삽입되어 성공적으로 키가 복구되는 것을 보여주었다.

2019년 P. Ravi 등은 명령어 스킵 오류 모델을 사용하여, 난스 재사용 시나리오를 만들었다 [10]. 이를 통해 NewHope, CRYSTALS-KYBER, Frodo, CRYSTALS-DILITHIUM에서의 성공적인 키 및 메시지 복구를 보여주었다. 하지만 CCA 보안 KEM에서는 오류를 감지할 수 있어, 메시지 복구가 어렵다. 본 논문에서는 CCA 보안 KEM 에서도 메시지 복구를 수행하기 위해 (Man-In-Middle) 공격을 제안하였다. Man-In-Middle 공격 방법은 [그림 3]와 같으며, 본 공격 방법을 통해 CCA 보안 KEM에서도 오류가 발생하였음에도 메시지 복구 공격을 수행 가능함을 보여주었다.또한, PQM4 라이브러리에서의 가져온 참조 구현을 ARM Cortex-M4F 마이크로 컨트롤러에서 실행하여 제안하는 공격들에 대해 검증을 하였다.



〔그림 3〕 Man-In-Middle 공격〔10〕

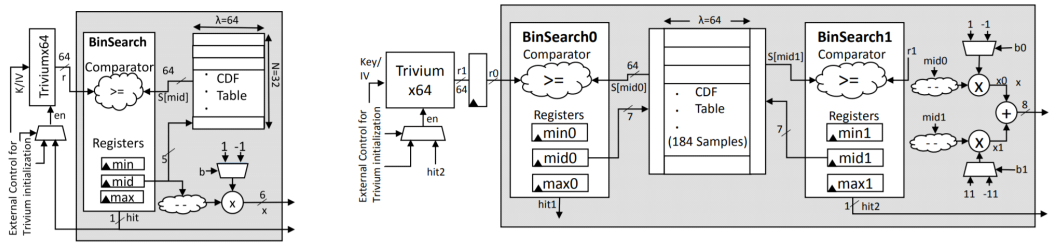
Ⅳ. NIST PQC Round 3 격자기반 암호의 부채널 대응기법

4.1. 시간차 공격에 대한 대응기법

시간 차 정보를 이용한 타이밍 공격에 대한 대응책은 비밀 값에 의존하지 않고 연산을 수행하는 Constant-time 구현과 중간 값을 랜덤하게 하여 시간 차 정보를 랜덤하게 만드는 마스킹 기법이 있다. 격자 기반 암호 내에서도 타이밍 공격에 취약한 부분이 존재하며, 격자 기반 암호 내에서 시간적인 정보를 누출하는 부분에 대한 부채널 대응기법의 연구들이 활발히 진행되고 있다.

2016년 A. Khalid 등은 CDT 기반 이산 가우시안 샘플러의 FPGA 기반 설계를 통한 Constant-time 구현을 제안하였다[11]. 저전력 및 메모리 사용량 최소화에 초점을 맞추었으며, [그림 4]는 제안하는 암호화 및 서명에서의 Constant-time CDT 샘플링 과정이다. [그림 4]의 a는 암호화를 위한 CDT 샘플링이며, 단일 포트 ROM과 5 비트 주소 포트 및 64 데이터 포트가 사용된다. Triviumx64는 균일하게 샘플을 생성할 때 사용되며, 이후 이진 검색 시스템인 BinSearch에 의해 제어된다. [그림 4]의 b는 서명을 위한 CDT 샘플링이며, BinSearch0, BinSearch1 두 개의 독립적인 병렬 이진 검색 방법을 제안하였다. 각 상태 머신에는 8 비트 주소와 64 비트 데이터 포트가 있다. 제안하는 CDT 샘플러는 암호화의 경우, 이전의 가장 빠른 CDT 샘플러 설계보다 9배 더 빠르며, 서명의 경우에서는 하드웨어에서의 최초의 Constant-time 구현의 CDT 샘플러를 제안하였다.

2018년 A. Karmakar 등은 Knuth-Yao기반 가우시안 샘플러의 Constant-time 구현을 제안하였다[12]. 기



(a) CDT sampler for encryption parameters. (b) CDT sampler for digital signature scheme parameters.

〔그림 4〕 FPGA 기반 암호화 및 서명에서의 Constant-time CDT 샘플링[11]

본 가우시안 샘플러는 데이터에 종속된 분기 처리가 발생하여 실행시간은 데이터에 따라 다르다. 본 논문에서는 Knuth-Yao기반 이산 가우시안 샘플링에서의 데이터 종속 분기가 되지 않도록 하였다. Constant-time 구현을 달성하기 위해 Knuth-Yao 알고리즘에서 출력 샘플 값과 입력 비트 간의 고유한 맵핑을 부울 함수로 표현하였다. 샘플링동안 이러한 각 부울 함수는 Constant-time이므로, Knuth-Yao기반 가우시안 샘플링 절차를 Constant-time 구현으로 만들 수 있다. 또한, 샘플러의 비트슬라이싱 기법을 제안하여 효율적으로 처리량을 향상시켰다. 성능 측정에서는 제안하는 기법을 Intel R i7-Broadwell 프로세서에서 측정하였으며, Constant-time 구현으로 만든 CDT 샘플러보다 약 2.4배 빠른 결과를 제시하였다.

4.2. 전력분석에 대한 대응기법

비밀 값에 대한 덧셈 연산 혹은 비트 연산 등에서 발생하는 전력 차이를 이용한 전력 분석 공격에 대한 대응책은 비밀 값의 연산 자체를 수정하는 방법과 마스킹과 셔플링을 이용해 값을 숨기는 방법이 존재한다. 현재 격자 기반 암호 내에서 비밀 값에 대한 연산에 대해 전력 분석 대응 기법들에 대한 연구가 활발히 진행되고 있다.

NTRU 암호의 복호화에서 컨볼루션 과정의 반복적인 덧셈 연산에서 부채널 취약점이 존재하는것에 대하여, 연산 자체를 수정하여, 덧셈과정을 생략하는 방법이 존재한다. 그러나, 이 방법은 공격자가 입력다항식을 특정하게 설정하고 공격하는 경우 오버플로우를 강제로 발생시켜 덧셈 연산을 만들 수 있기 때문에, 특정한 상황에서만 가용할 수 있다. 따라서, 일반적인 경우에서 전력 분석 공격을 막기 위하여, 컨볼루션 연산을 진행할 때 입력 배열에 대한 셔플링 연산을 수행한다[6]. 입력 배열의 순서를 무작위화 함으로써, 공격자가 수집한 전력분석 파형을 예측하기 어렵게 할 수 있다. 이때 발생하는 오버헤드의 경우, 셔플링할 배열의 인덱스를 랜덤으로 추출하는 과정과 SWAP 연산에 대한 오버헤드가 발생한다. NTRU에서 셔플링 기법을 제외한 전력분석 기반 공격에 대한 대응 방안으로 피연산자의 값을 무작위화 하는 방법이 존재한다. NTRU에서 컨볼루션의 피연산자의 배열을 초기에 제로화가 아닌 무작위화를 통하여, 공격자가 전력소모 패턴을 예측하기 어렵게 만들 수 있다. 이 방안의 경우 무작위 수를 추출하는 연산 및 배열에 할당하는 오버헤드가 발생한다. 이 두 기법을 통해 NTRU의 전력분석기반 공격에 대응할 수 있다.

음의 값과 양의 값의 해밍 가중치의 차이로 인해 Constant-time CDT 샘플러는 단일 파형 공격에 취약하다는 것이 밝혀졌고, 이에 따라 대응기법에 관한 연구가 진행되고 있다[13]. 샘플링 시 음수 값은 해밍 가중치가 더 크기 때문에 전력 소비량이 바뀌게 되고, 이를 통해 공격자가 비밀 값에 0 혹은 1이 추가되었음을 알 수 있다. 이에 대응하기 위해 주어질 샘플러의 출력 데이터를 미리 계산함으로써 공격자의 공격 대상을 제거한다. 여기서, 부호 비트의 노출을 제거하기 위해 추가로 CDT에서 1비트를 더 샘플링하고, 테이블의 길이를 두 배로 늘린다. 예를 들어, 8비트 데이터를 샘플링할 시에 처음 7 비트는 정수 데이터를 의미하고, 마지막 비트는 샘플링된 값의 부호를 결정하는데 사용한다.

[표 1]은 샘플러의 출력 데이터를 미리 계산하는 표이고, [표 2]은 부호를 포함한 샘플링의 값이다. 이 방안은 추가적인 연산량이 존재하지 않고 유일한 단점은 조회 테이블의 저장량이다. 표 2의 경우 128바이트의 메모리를 요구하고, 표 3의 경우 256바이트의 메모리

〔표 1〕 부호를 포함한 입력값이 제공된 샘플링 값〔13〕

x	0	1	...	63	...	154	...	255
output	0	0	...	1	...	-1	...	-4

〔표 2〕 입력값이 주어진 샘플링된 값〔13〕

x	0	1	...	63	64	...	127
output	0	0	...	1	2	...	4

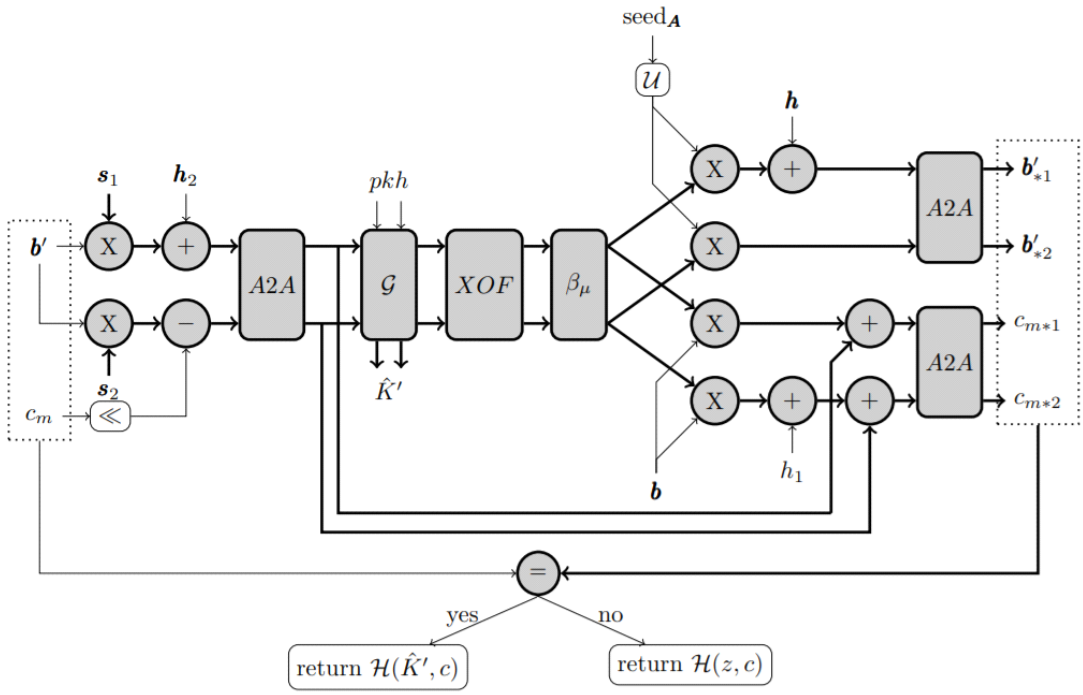
를 요구하는데, 크지 않은 양이므로 임베디드 기기에도 적용이 가능한 장점이 있다.

3라운드 표준화 작업이 진행되면서 SABER 개발팀에서 SABER의 전력 분석 공격에 대한 대응방안에 대하여 제안하였다[14]. [그림 5]에서 회색 표시는 SABER의 디 캡슐레이션 과정 중에 전력분석 시 노출될 수 있는 부분이고 마스킹이 반드시 되어야 하는 부분이다. SABER의 경우 Module-LWR 구조 기반이고 라운딩의 효율성을 위해 링의 차수를 2의 지수 승으로 설정했기 때문에, 전력 분석에 대응하기 위한 Saber의 마스킹 설계는 다른 격자 기반 암호 알고리즘보다 효율적이다. 제안된 논문에서 산술과 부울 마스킹 간에 변환에 대한 A2B의 응용인 A2A 방법과, 이항 샘플러의 마스킹 방법을 제안하였다. A2A 변환은 산술 공유에서 수행되는 논리적 시프트 연산의 대체 역할을 수행한다. 마스킹 작업시 Saber는 ARM-Cortex-M4 환경에서 2.5배 정도의 오버헤드를 발생한다. 제안된 방안은 기존의 Saber에 대한 마스킹 기법 (5.7배)보다 성능 향상이 존재한다.

4.3. 오류 공격에 대한 대응기법

오류를 주입하여 난스 재사용 시나리오를 대응하기 위해서는 두 번의 암호화를 수행하거나, 오류 주입이 발견되면 오류 복구 메커니즘이 오류를 감지하고 새 계산을 수행하는 것이다. 하지만 이러한 대응 기법들은 추가적인 연산 소모로 인해 성능 부하가 많이 발생하며, 이를 줄이거나 더욱 효율적인 부채널 대응기법의 연구들이 다양히 진행되고 있다.

2018년 L.G. Bruinderink 등은 CRYSTALS-DILITHIUM, qTESLA에서의 오류공격 및 대응책을 제안하였다[9]. 위의 연구결과는 서명 절



〔그림 5〕 SABER 부채널 대응 기법〔14〕

차 중 임의의 오류를 삽입하여 난스 재사용 시나리오를 통해 성공적으로 키가 복구되는 것을 보여주었다. 대응방안으로는 Double computation, Verification-after-sign, Additional randomness 방법을 제안하였다. Double computation은 서명 알고리즘을 두 번 실행하여, 동일한지 비교를 통해 오류를 감지하는 방법이다. 하지만 실행시간이 두 배로 늘어나며, 동일한 결함을 두 번 주입 시 오류 감지에 실패할 수도 있다. Verification-after-sign은 제안한 공격들은 모두 서명을 유효하지 않게 만들기 때문에, 서명 후 서명을 확인하는 방법이다. 이는 실행시간이 서명의 1/3 미만으로 두 번 서명 생성하는 것보다 효율적이지만, 단점은 유효한 서명을 생성하기 위해 y의 샘플링에 삽입된 결함을 감지할 수 없다는 것이다. 마지막으로 Additional randomness는 가장 간단한 방법으로 잡음 y에 솔트를 추가하여 값을 무작위 하는 것이다. 하지만 이를 위해 엔트로피 소스가 필요하며, 제한된 환경에서는 사용하지 못할 수도 있고, 이는 CRYSTALS-DILITHIUM의 보안을 위반한다. 제안하는 대응책들에 대한 안전성 결과는 [표 3]과 같으며 fA_p, fA_E, fY, fW, fH는 각 시나리오이다. 이 외에도 성능, 안전성의 효율성을 보장하는 오류공격 대응책에 대한 연구가 수행되고 있다.

〔표 3〕 제안하는 대응책의 안전성 분석[9]

	fA_p	fA_E	fY	fW	fH
Double computation	X	√	√	√	√
Verification after sign	√	√	X	√	√
Additional randomness	√	√	√	√	√

Ⅴ. 결 론

양자 컴퓨터의 발전으로 기존 공개키암호 기반의 수학적인 난제들이 다항 시간 내에 해결됨에 따라, 양자내성 암호의 중요성이 강조되고 있다. NIST에서는 2016년 양자 내성 암호의 표준화 사업을 공모하였으며, 현재 3라운드가 진행 중이다. 그중 대부분 (5/7)은 격자 기반 암호로서, 연산처리 및 적절한 키 사이즈를 제공하여 임베디드 환경에서도 적용할 수 있다. 그러나, 임베디드 환경의 경우 일반 컴퓨팅 환경보다 부채널 공격에 취약하므로 대응 방안이 필수적이다.

본 논문에서는 격자 기반 암호의 부채널 취약점과 현재 NIST PQC 공모사업의 3 Round 격자 기반 암호에 대한 최신 부채널 대응기법에 대한 동향을 분석하였다. 격자 기반 암호의 부채널 취약점에서는 실제 타이밍 공격, 전력분석, 오류공격을 통해 비밀 값을 복구하는 연구 동향을 분석하였다. 또한, 이에 대응하기 위해 NIST 3 Round 격자 기반 암호에 대한 Constant-time 구현, 마스킹, 오류 검출 기반의 대응기법들을 소개하였다.

현재 PQC 공모사업 3라운드가 진행 중이며, 응용관점에서 활발히 논의가 이루어지고 있다. 지금까지 수학적, 이론적 안전성 분석이 다양하게 진행되었지만, 부채널 관점에서의 PQC에 대한 논의는 상대적으로 미미한 편이다. 따라서, 앞으로 PQC가 표준화 및 상용화가 되기 위해서 부채널 공격에 대한 안전성을 가질 수 있도록 대응 기법에 관한 연구가 활발히 진행될 것으로 예상한다.

참 고 문 헌

[1] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quatum-computer”, SIAM review, 1999, pp 303-332.

[2] S.J. An, S.R. Kim, S.H. Jin, H.B. Kim, H.S. Kim, “Single Trace Side Channel Analysis on NTRU Implementation”, MDPI Applied Sciences, 2018, 8(11)

[3] L.G. Bruinderink, A.T. Hülsing, T. Lange, Y. Yarom, “Flush, Gauss, and Reload - A Cache Attack on the BLISS Lattice-Based Signature Scheme”, CHES, 2016, pp 323-345.

[4] D.J. Bernstein, “Cache-timing attacks on AES”, Citeseer, 2005.

[5] B.Y. SIM, J.H. Kwon, J.H. LEE, I.J. Kim, T.H. Lee, J.S. Han, H.J. Yoon, J.H. Cho, D.G. Han, “Single-Trace Attacks on Message Encoding in Lattice-Based KEMs”, IEEE ACCESS, 2020, pp 183175-183191.

[6] M.K. Lee, J. Song, D.H. Choi, D.G. Han.

Countermeasures against Power Analysis Attacks for the NTRU Public Key Cryptosystem. IEICE Transactions. (2010)

[7] Primas R., Pessl P., Mangard S. (2017) Single-Trace Side-Channel Attacks on Masked Lattice-Based Encryption. In: Fischer W., Homma N. (eds) Cryptographic Hardware and Embedded Systems – CHES 2017. CHES 2017. Lecture Notes in Computer Science, vol 10529. Springer, Cham.

[8] P. Ravi, D.B. Roy, S. Bhasin, A. Chattopadhyay, D. Mukhopadhyay3, “Number ”Not Used“ Once – Practical fault attack on pqm4 implementation of NIST candidates”, Constructive Side-Channel Analysis and Secure Design (COSADE), 2019, pp 232-250

[9] L.G. Bruinderink, P. Pessl, “Differential Fault Attacks on Deterministic Lattice Signatures”, CHES, 2018, 21-43.

[10] P. Ravi, D.B. Roy, S. Bhasin, A. Chattopadhyay, D. Mukhopadhyay3, “Number ”Not Used“ Once – Practical fault attack on pqm4 implementation of NIST candidates”, Constructive Side-Channel Analysis and Secure Design (COSADE), 2019, pp 232-250

[11] A. Khalid, J. Howe, C. Rafferty, M. O’Neill, “Time-independent discrete Gaussian sampling for post-quantum cryptography”, IEEE International Conference on Field-Programmable Technology (FPT), 2016.

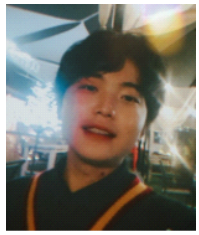
[12] A. Karmakar, S.S. Roy, O. Reparaz , F. Vercauteren, I. Verbauwhede, “Constant-Time Discrete Gaussian Sampling”, IEEE TRANSATION ON COMPUTERS, VOL 67, 2018.

[13] S.R.Kim, S.H. Hong, “Single Trace Analysis on Constant Time CDT Sampler and Its Counter-measure”, MDPI Appl. Sci. 2018, 8, 1809.

[14] Beirendonck, M.V., D'Anvers, J., Karmakar, A., Balasch, J., & Verbauwhede, I. (2020). A Side-Channel Resistant Implementation of SABER. IACR Cryptol. ePrint Arch., 2020, 733.

〈저자소개〉

송 진 교 (JinGyo Song)
정회원
2020년 : 국민대학교 정보보안암호수학과 졸업
2020년~현재 : 국민대학교 금융정보보안학과 석사과정
<관심분야> 암호구현, 임베디드 보안, 부채널 분석



김 영 범 (YoungBeom Kim)
정회원
2021년 : 국민대학교 정보보안암호수학과 졸업
2021년~현재 : 국민대학교 금융정보보안학과 석사과정
<관심분야> 암호최적화, 양자내성암호

곽 유 진 (Yujin Kwak)
정회원
2017년~현재 : 국민대학교 정보보안암호수학과 학사과정
<관심분야> 암호최적화, 임베디드 보안

서 석 충 (Seog Chung Seo)
정회원
2011년 8월 : 고려대학교 정보보호대학원 박사
2013년 11월 : 삼성전자 종합기술원 전문연구원
2014년 4월 : 삼성전자 DMC 연구소 책임연구원
2019년 2월 : 국가보안기술연구소 선임연구원
2019년 3월~현재 : 국민대학교 정보보안암호수학과 조교수
<관심분야> 암호최적화, 공개키 암호, 암호모듈검증,네트워크보안