코드 기반 양자 내성 암호 MEDS 알고리즘의 하드웨어 가속을 위한 부채널 공격 연구 동향 분석

이윤지[1], 이용석[1], 백윤흥[1]
[1]서울대학교 전기정보공학부, 서울대학교 반도체 공동연구소
yjlee@sor.snu.ac.kr, yslee@sor.snu.ac.kr, ypaek@snu.ac.kr

Side-Channel Attack Trends of Code-based PQC Algorithm for Hardware Acceleration of MEDS

Yunji Lee[1], Yongseok Lee[1], Yunheung Paek[1]
[1]Dept. of Electrical and Computer Engineering and Inter-University Semiconductor Research Center(ISRC), Seoul National University

요 약

양자컴퓨터 시대가 눈앞에 도래한 지금 차세대 암호로 주목받고 있는 양자 내성 암호는 다양한 수학적 알고리즘에 안전성을 기반하고 있으나 이 안전성을 위협하는 대표적인 공격 기법 중 하나인 부채널 분석 공격에 대응하기 위한 노력들이 계속되어 왔다. 이 논문에서는 코드 기반 양자 내성 암호를 중심으로 알고리즘에 위협적인 부채널 분석 공격에 대한 연구 동향을 분석하였다. 그리고 NIST 에서 PQC 표준화를 위해 Round 를 진행 중인 후보 중 하나인 코드 기반 알고리즘 MEDS 에 대해 소개하고, MEDS 알고리즘의 최적화를 위해 기존에 연구되었던 코드 기반 암호에 대한 부채널 분석 공격 대응 측면에서의 알고리즘의 안전성 확보라는 보안 비용과 하드웨어 가속 등을 통한 성능 향상이 적절한 조화를 이룰 수 있도록 설계하기 위한 방안에 대해 알아보았다.

1. 서론

양자컴퓨터의 개발이 현실화되면서 양자컴퓨터 시대를 대비하기 위한 양자 내성 암호에 대한 관심이 높아지고 있다. 지난 1994 년 Shor 알고리즘에 의해 양자컴퓨팅을 이용하면 인수분해, 이산대수 등 기존 공개키 암호의 내성이 깨진다는 것이 밝혀지면서 미국립표준기술연구소(NIST)에서는 이를 극복하기 위해 양자 내성 암호(Post-Quantum Cryptography, PQC)에 대한 연구를 본격적으로 시작하였다. 양자 내성 암호에 대한 연구는 공개키 암호화/키 캡슐화(PKE/KEM), 전자 서명 알고리즘(Digital Signature Algorithm, DSA)으로 각각 나누어 진행하고 있는데, 최근 Round 3 가 종료되면서 4 개의 표준화를 위한 알고리즘을 선정하였고, 선정되지 않은 나머지 후보 중에서 Round 4 를 진행할 4 가지 알고리즘을 추가로 선정하였다[1].

양자 내성 암호는 알고리즘에서 사용하는 난제 종류에 따라 5 가지 유형으로 구분되는데, 격자 기반(Lattice-based), 코드 기반(Code-based), 해시 기반(Hash-based), 다변수기반(Multivariate-based), 그리고 아이소제니 기반(Isogeny)이 그것이다. 현재 표준화 대상으로 선정된 4 개 알고리즘은 3 개가 격자 기반(CRYSTALS-KYBER, CRYSTALS-Dilithium, FALCON), 1 개가 해시 기반(SPHINCS+)이며 NIST 는 표준화 대상 알고리즘이 격자 등 특정 유형에 집중되어 취약성이 공유되는 것을 피하고자 Round 4 에서는 4 개의 KEM 알고리즘 중 3 개는 코드 기반(Classic McEliece, HQC, BIKE), 1 개는 아이소제니 기반(SIKE)으로 선정하여 다양한 위협에 대비하고자 하였다.

이에 더해 NIST 는 KEM 뿐만 아니라 DSA 알고리즘도 추가로 Round 1 을 진행하고 있으며 기존에 선정된 DSA 알고리즘이 격자 및 해시 기반인 데다 현재 진행중인 Round 4 KEM 대부분이 코드 기반인 점으로 미루어 볼 때 전자 서명 알고리즘에도 코드 기반 암호가 경쟁력이 있을 것으로 예상되고 있다.

따라서 본 연구에서는 코드 기반 양자 내성 암호의 특징에 대해 소개하고, 기존 코드 기반 알고리즘(Classic McEliece, HQC, BIKE)에 대해 연구되었던 부채널 분석 공격 동향을 분석하였다. 이를 통해 NIST 에서 진행하는 PQC DSA 알고리즘 Round 1 후보 중 하나인 MEDS (Matrix Equivalence Digital Signature) 알고리즘의 하드웨어 가속기를 설계하기 위해 적용 가능할 것으로 예상되는 부채널 분석 공격을 소개한다.

2. 코드 기반 암호

코드 기반 암호는 1978 년 Robert J. McEliece 가 코딩 이론을 바탕으로 Goppa 코드를 기반으로 한 최초의 코드 기반 공개키 암호화 시스템인 McEliece 알고리즘을 제안하며 처음 소개되었다[2]. 이후 1986 년 Harald Niederreiter 에 의해 초기 McEliece 는 단방향 방식이었던 것과 달리 듀얼(양방향) 방식 Niederreiter 공개키 암호화 시스템이 소개되었고, 현재는 양자 컴퓨터에 대해서도 내성을 가지는 높은 보안 수준인 IND-CCA2 를 갖춘 Classic McEliece 가 설계되어 NIST PQC 표준화 PKE/KEM 알고리즘 후보 중 하나로 Round 4 에 진출하였다.

코드 기반 암호 알고리즘의 동작 방식은 다음과 같다. 먼저 오류 수정이 가능한 생성 행렬을 공개키로 사용하며 이에 메시지를 조합하여 인코딩한 후 의도적으로 오류를 추가한 암호문을 수신자에게 전송한다. 이를 수신한 올바른 수신자는 오류 수정 코드인 생성 행렬에 대한 패리티 체크 행렬을 통해 의도적으로 추가된 오류를 제거하고 원본 메시지를 확인할 수 있다.

코드 기반 암호는 기본적으로 공개키의 크기가 크고 키 생성이 너무 오래 걸린다는 단점이 있었으나 현재 양자 컴퓨터의 개발로 효율성 문제가 개선되어 다시 주목받고 있다. 한편 NIST PQC 표준화 알고리즘으로 선정되기 위해서는 알고리즘 최적화 외에도 부채널 분석 공격 등 각종 공격으로부터 안전성을 보장받아야 한다.

3. 부채널 분석을 이용한 공격

코드 기반 암호에 대한 공격은 암호의 수학적 알고리즘 취약성에 기반한 공격 기법(Syndrome Decoding 문제에 기반한 Information Set Decoding 공격 등)과 부채널 분석 공격 기법으로 살펴볼 수 있다. 특히 암호가 수학적 완전성을 갖춘 알고리즘이라 하더라도 부채널 분석 공격에서 자유로울 수 없는데, 부채널 분석 공격 기법이란 암호 알고리즘이 작동하며 생기는 물리적 효과(시간, 전력, 전자기파 등의 부가 정보)를 바탕으로 암호화 동작과의 연관 정보를 분석하여 암호키나 부분적인 상태 정보, 전체 또는 부분적인 메시지 등과 같이 시스템 상에 암호화되어 있는 정보를 복구하는 기법을 말한다. 부채널 분석 기법에는 부채널 정보 종류 등에 따라 시간분석, 전력분석, 프로파일링 공격, 그리고 오류 주입 기법 등이 있다.

아래 표는 이 논문에서 살펴본 NIST PQC 표준화 PKE/KEM Round 4 알고리즘 후보 중 코드 기반 암호인 Classic McEliece, HQC, BIKE 에 대해 현재까지 연구되었던 대표적인 부채널 분석 기법을 암호 동작 공격과 연계하여 종류별로 구분한 것이다.

[표 1] 코드 기반 암호에서 나타나는 부채널 분석 공격 종류

	부채널공격	부가 정보 분석	암호 동작 관련 공격
[3]	시간분석 (Timming)	Decapsulation 동작 시간 차이	Syndrome inversion 공격
[4]			선택 암호문 공격
[5]	전력분석 (Power)	신드롬 행렬 연산 간 다수 전력파형 분석	메시지 복구 템플릿 공격, 신드롬 디코딩 문제
[6]		다수 전력파형 활용 딥러닝네트워크 학습	키 복구 딥러닝 기반 프로파일링 공격
[7]		단순 전력파형 매칭	키 복구 템플릿 공격
[8]		단순 전력파형 분석	Syndrome decoding 문제
[9]	기타	레이저 이용 오류(Fault) 주입	메시지 복구 공격, 신드롬 디코딩 문제 수정

먼저 대표적인 부채널 분석 기법인 시간분석을 이용한 선택 암호문 공격이 연구되었다[3][4]. 시간분석 공격에서는 하드웨어에서 암호화나 알고리즘을 수행하는 동안 CPU 나 메모리의 데이터가 이동하는 시간을 측정한다. 즉, 비밀 정보를 기반으로 하는 동작 시간 변동을 감지하거나 단순히 암호화 작업을 하는데 걸리는 시간을 측정하여 전체 비밀키가 무엇인지 알아낼 수 있다. 특히 [3]과 [4]에서는 decapsulation 과정 중 동작 시간 차이가 발생하는 점을 통해 암호문의 해밍 무게가 증가할 때 동작 시간 변화가 큰 암호문을 생성하여 비밀키 및 개인키를 복구할 수 있다.

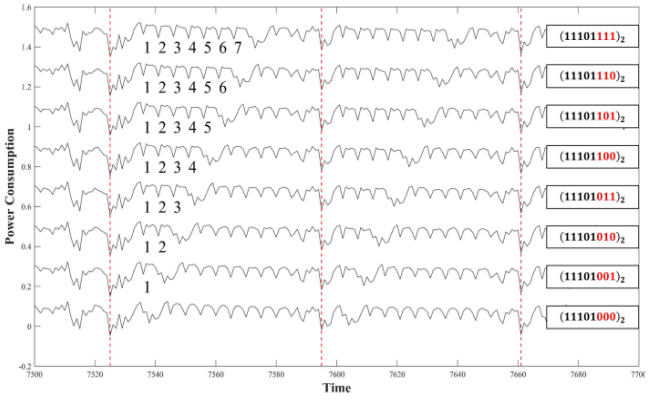
Algorithm 1 : Pseudo code of attack: BikeAttack(h, w^*, M, I)

```
                                                          // Preamble
m ← Plaintext such that H(m) is easily distinguishable by timing attack
while True do
    Generate random e, of hamming weight w*
    if DecodingFailureDistinguisher(e, I) = True then
        break                  // Found the first e which causes a decoding failure
    end
end
                                                          // Main body
F, G, A, B ← empty vectors
for i ← 1, M do
    e* ← Move random non-zero bit in e
    ΔD_d ← Distance spectrum differences between e and e*
    if DecodingFailureDistinguisher(e*, I) = True then
        e ← e*
        Update lists F, G with ΔD_d according to [NJW18]
    else
        Update lists A, B with ΔD_d according to [NJW18]
    end
end
                                                          // Postamble
A' ← max(A) − A + min(A)
D ← F + G + A' + B
Recover secret key with distance spectrum D as per [GJS16]
```

[알고리즘 1] BIKE 동작 시간 차이 발생 알고리즘 예시[4]

또한 대표적인 전력분석 즉 전력파형 분석을 이용한 템플릿 공격, 신드롬 디코딩 공격 등이 연구되었다[5][6][7][8]. 전력 분석 공격은 CPU 또는 암호화 회로와 같은 하드웨어의 전력 소비 변화를 관찰하면

서 정보를 얻는 방식이다. 이 공격은 단순 전력 분석과 차등 전력 분석으로 나뉘며 단순 전력 분석은 단일 또는 일부 전력파형 수집을 통해, 차등 전력 분석은 다수의 전력파형을 통해 중간값 연산하여 상관분석을 함으로써 메시지, 개인키 등을 복구할 수 있다.



[그림 1] B.-Y. Sim et al 의 알고리즘에 대한 단순 전력 파형 분석 예시[8]

마지막으로 또한 Classic McEliece 를 대상으로 플래시 메모리 뒷면에 레이저 오류를 주입하여 메시지를 복구하는 부채널 분석 공격 기법도 연구되었다[9]. [그림 3]에서 보는 바와 같이 레이저 오류를 주입할 경우 XOR 연산이 add-with-carry 연산으로 변경되는 것을 볼 수 있으며 이 오류를 바탕으로 신드롬 연산을 수정하여 메시지를 복구할 수 있음을 보여주었다.

[표 2] 레이저 오류 주입에 의한 연산 변경 예시[9]

Fault	Assembly code	Binary machine code	Readout

No	mov r3, #90
	mov r4, #90
	eors r3, r4
		0010 0011 0101 1010
		0010 0100 0101 1010
		0010 0000 0110 0011
			r3 = 0x00

Yes	mov r3, #90
	mov r4, #90
	adcs r3, r4
		0010 0011 0101 1010
		0010 0100 0101 1010
		0010 0001 0110 0011
			r3 = 0xB4

4. MEDS 알고리즘과 하드웨어 가속

MEDS(Matrix Equivalence Digital Signature)[10]는 매트릭스 코드 동등성 문제에 기반한 코드 기반의 전자서명 알고리즘이다. MEDS 는 코드 기반 암호임에도 매개 변수를 최적화함으로써 공개키와 서명의 크기를 효율적으로 줄이는 성능 향상을 이끌어냈을 뿐 아니라, 키 생성 및 서명 간 시간분석 공격에 대한 안전성을 구현한 것으로 평가되고 있다[11].

다만 파라미터의 크기가 커질 때 공개키와 서명의 크기는 여전히 다른 알고리즘에 비해 최적화했음에도 불구하고 큰 편이라는 제한사항을 가지고 있다. 또한 최근 진행된 표준화 컨퍼런스(5th PQC Standardization Conference 2024)에 따르면[12] 서명과 검증에 소요되는 시간이 오래 걸리는 특징이 있다. 다만 MEDS 알고리즘 특성상 효율적인 병렬화가 가능한 구조를 가지고 있기 때문에 하드웨어 가속 분야도 계속 연구되고 있다. 따라서 효과적인 최적화 방안을 적용하여 NIST PQC 의 DSA 표준화 후보로 선정될 수 있을지 기대되고 있다.

5. 결론

본 논문에서는 차세대 양자 내성 암호의 주요 후보로 떠오른 코드 기반 암호 알고리즘에 대한 부채널 분석 공격 연구 동향을 살펴보고 하나의 후보인 MEDS 알고리즘에 대해 앞서 살펴본 코드 기반 암호에 대한 부채널 분석 연구가 어떻게 적용될 수 있을지 살펴보았다. 특히 시간 및 전력분석을 중심으로 많은 부채널 분석에 대한 연구들이 이루어지고 있음을 알 수 있었는데, 양자 내성 암호는 부채널 분석 공격에 대한 안전성을 확보하기 위한 보안 비용과 알고리즘 성능 향상 사이 최적화된 trade-off 를 달성하기 위해서는 하드웨어 가속을 비롯한 많은 연구들을 통해 양자컴퓨팅 시대에 대비해야 할 것으로 기대된다.

ACKNOWLEDGEMENT

이 논문은 2023 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구이며 (IITP-2023-RS-2023-00256081), 2024 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구이며 (RS-2023-00277326), 2024 년도 BK21 FOUR 정보기술 미래인재 교육연구단에 의하여 지원되었음. 본 연구는 IDEC 에서 EDA Tool 을 지원받아 수행하였음.

참고문헌

[1] Alagic, Gorjan, et al. “Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process.” NIST, 2022. Available: https://doi.org/10.6028/NIST.IR.8413
[2] McEliece, Robert J. “A public-key cryptosystem based on algebraic coding theory.” Technical Report, NASA, 1978.
[3] Strenzke, Falko J. “Timing Attacks against the Syndrome Inversion in Code-Based Cryptosystems.” PQCrypto 2013, LNCS 7932, pp.217-230, 2013.
[4] Qian, Guo, et al. “Don’t Reject This: Key-Recovery Timing Attacks Due to Rejection-Sampling in HQC and BIKE.” TCHES, vol. 2022, no. 3, pp. 223-263, 2022.
[5] B. Colombier, et al. “Profiled Side-Channel Attack on Cryptosystems Based on the Binary Syndrome Decoding Problem.” IEEE Transactions on Information Forensics and Security, vol. 17, pp. 3407-3420, 2022.
[6] Q. Guo, A. Johansson, and T. Johansson, “A Key-Recovery Side-Channel Attack on Classic McEliece Implementations”, TCHES, vol. 2022, no. 4, pp. 800–827, 2022.
[7] T. Schamberger, et al. “A Power Side-Channel Attack on the CCA2-Secure HQC KEM.” Smart Card Research and Advanced Applications, vol. 12609, 2021.
[8] B.-Y. Sim, et al. “Novel Side-Channel Attacks on Quasi-Cyclic Code-Based Cryptography.” TCHES, vol. 2019, no. 4, pp. 180-212, 2019.

[9] P.-L. Cayrel, et al. “Message-Recovery Laser Fault Injection Attack on the Classic McEliece Cryptosystem.” Advances in Cryptology-EUROCRYPT, pp. 438-467, 2021.
[10] Chou, Tung, et al. “MEDS Metrix Equivalence Digital Signature.” NIST, 2023. Available: https://www.meds-pqc.org/
[11] Chou, Tung, et al. “Take your MEDS: Digital Signatures from Matrix Code Equivalence.” AfricaCrypt 2023, Lecture Notes in Computer Science, Springer, 2023.
[12] Kannwischer, Matthias, et al. “pqm4: Benchmarking NIST Additional Po<t-Quantum Signature Schemes on Microcontrollers.’ ɔth PQC Standardization Conference, 2024. Available: https://eprint.iacr.org/2024/112