Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.2, Apr. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.2.151

SIKE에서의 최신 마스킹 대응기법에 대한 딥러닝 기반 부채널 전력 분석*

임 우 상,[1†] 장 재 영,[1] 김 현 일,[2] 서 창 호[2‡]
[1,2]공주대학교 (대학원생, 교수)

Deep Learning Based Side-Channel Analysis for Recent Masking Countermeasure on SIKE*

Woosang Im,[1†] Jaeyoung Jang,[1] Hyunil Kim,[2] Changho Seo[2‡]
[1,2]Kongju National University (Graduate student, Professor)

요 약

최근 양자 컴퓨터의 개발은 현재 사용 중인 이산대수 문제나 인수분해 문제 기반의 공개키 암호에 큰 위협이 되므로, 이에 NIST(National Institute of Standards and Technology)에서는 현재 컴퓨팅 환경 및 도래하는 양자 컴퓨팅 환경에서 모두 구현이 가능한 양자내성암호를 위해 공모전을 진행하고 있다. 이 중 NIST 양자내성암호 공모전 4라운드에 진출한 SIKE(Supersingular Isogeny Key Encapsulation)는 유일한 Isogeny 기반의 암호로써, 동일한 안전성을 갖는 다른 양자내성암호에 비해 짧은 공개키를 갖는 장점이 있다. 그러나, 기존의 암호 알고리즘과 마찬가지로, SIKE를 포함한 모든 양자내성암호는 현존하는 암호분석에 반드시 안전해야만 한다. 이에 본 논문에서는 SIKE에 대한 전력 분석 기반 암호분석 기술을 연구하였으며, 특히 웨이블릿 변환 및 딥러닝 기반 클러스터링 전력 분석을 통해 SIKE를 분석하였다. 그 결과, 현존하는 클러스터링 전력 분석 기법의 정확도를 50% 내외로 방어하는 마스킹 대응기법이 적용된 SIKE에 대해 100%에 가까운 분석 성공률을 보였으며, 이는 현존하는 SIKE 기법에 대한 가장 강력한 공격임을 확인하였다.

ABSTRACT

Recently, the development of quantum computers means a great threat to existing public key system based on discrete algebra problems or factorization problems. Accordingly, NIST is currently in the process of contesting and screening PQC(Post Quantum Cryptography) that can be implemented in both the computing environment and the upcoming quantum computing environment. Among them, SIKE is the only Isogeny-based cipher and has the advantage of a shorter public key compared to other PQC with the same safety. However, like conventional cryptographic algorithms, all quantum-resistant ciphers must be safe for existing cryptanlysis. In this paper, we studied power analysis-based cryptographic analysis techniques for SIKE, and notably we analyzed SIKE through wavelet transformation and deep learning-based clustering power analysis. As a result, the analysis success rate was close to 100% even in SIKE with applied masking response techniques that defend the accuracy of existing clustering power analysis techniques to around 50%, and it was confirmed that was the strongest attack on SIKE.

Keywords: Supersingular Isogeny Key Encapsulation, Clustering Power Analysis, Deep Learning, Wavelet Transform

Received(12. 12. 2022), Modified(02. 14. 2023), Accepted(02. 15. 2023)

* 이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2021-0-00400, 저사양 디바이스 대상 고효율 PQC 안전성 및 성능 검증 기술 개발).

† 주저자, tedy789@smail.kongju.ac.kr
‡ 교신저자, chseo@kongju.ac.kr(Corresponding author)

I. 서 론

현재의 공개키 암호는 이산대수 문제 및 인수분해 문제를 기반으로 그 안전성이 보장되어 있다. 하지만 양자 컴퓨터 시대의 도래는 양자 알고리즘인 Shor 알고리즘이 다항시간 내에 구동됨을 의미하며, 이는 인수분해 문제와 이산대수 문제가 해결되는 것을 의미한다[1]. 따라서 현재 사용되고 있는 공개키 암호 시스템은 더 이상 안전하지 않으므로 현재에도 사용이 가능하면서 동시에 양자 환경에서도 안전한 암호의 필요성이 대두되고 있다.

이에 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)에서는 양자 컴퓨터에 안전한 양자 내성 암호(Post Quantum Cryptography)에 대한 공모전을 진행하고 있으며, 2020년 7월 발표된 3 라운드 후보로는 격자 기반, 부호 기반, 다변수 기반, 해시 기반 그리고 Isogeny 기반 암호들이 공개 및 선정되었다. 그중 키 캡슐화 알고리즘(Key Encapsulation Mechanism)에서는 격자 기반 암호인 CRYSTALS-KYBER가, 전자서명 알고리즘에서는 격자 기반 암호 중 CRYSTALS-Dilithium, FALCON 및 해시 기반 전자서명인 SPHINCS+가 선정되었다.

한편 NIST에서는 공모전 추가로 4라운드를 진행하여 아직 표준화 대상이 되지 못한 BIKE, Classic McElice, HQC, SIKE에 대한 평가를 진행한다고 발표하였다. 이 중 SIKE(Supersingular Isogeny Key Encapsulation)는 3라운드 암호 후보 중 유일한 Isogeny 기반 암호로써, 동일한 안전성을 제공하는 양자 내성 암호에 비해 짧은 공개키를 갖는 큰 장점이 있어 주목받고 있다. 하지만, 상대적으로 느린 동작 시간이 큰 문제점이었으며, 해당 소요 시간을 줄이기 위한 연구가 지속적으로 수행되고 있다[2-5].

한편, 앞서 언급하였듯이 양자 내성 암호는 현재 컴퓨팅 환경에서도 구현 및 동작이 가능해야 하며, 이는 부채널 분석과 같은 기존의 암호분석 방법에 대한 안전성도 역시 반드시 고려되어야 함을 의미한다. 특히, SIKE는 부채널 분석 중 클러스터링 전력 분석(Clustering power analysis)[6]에 대하여 취약점이 발견되었으며, 이는 SIKE에 대한 추가적인 대응기법(Countermeasure)가 반드시 필요함을 보였다. 이에 Genet 등[6]은 현존하는 SIKE에 대한 클러스터링 전력 분석과 함께 해당 분석에 대한 대응기법을 함께 제시하였다.

본 논문에서는 SIKE에 대한 전력 분석 기반 암호분석 기술에 관한 연구를 수행한다. 특히, 현존하는 SIKE의 최신 대응기법[6]에 대한 웨이블릿 변환(Wavelet transform)[7] 기반 딥러닝 전력 분석 모델을 설계하고 제안한다, 이에 대한 실험 결과, 기존 클러스터링 전력 분석 기법의 정확도를 50% 내외로 방어하는 마스킹 대응기법이 적용된 SIKE에서도 100%에 가까운 분석 성공률을 보였으며, 이는 현존하는 SIKE 기법에 대한 가장 강력한 부채널 공격임을 확인하였다.

본 논문의 구성은 다음과 같다. 2장에서는 SIKE에 관한 전반적인 서술 및 공격 대상이 되는 Three-point Ladder와 내부의 swap 알고리즘에 관하여 언급하고 3장에서는 SIKE에 적용된 클러스터링 전력 분석 기법과 그에 관한 대응기법을 설명한다. 또한, 4장에서는 ECC에 관한 딥러닝 기반의 클러스터링 공격 기법에 관하여 전반적으로 소개한다. 그리고 5장에서는 SIKE에 관하여 딥러닝 기반의 클러스터링 전력 분석을 수행하고 결과를 분석하며 6장에서는 결론으로 마무리한다.

II. 배경 지식

2.1 SIKE(Supersingular Isogeny Key Encapsulation)

SIKE는 양자내성암호 중 하나로 NIST PQC 공모전 3라운드 대체 후보(Alternative) 중 하나였으며, 현재 부호 기반 암호인 Classic McElice, BIKE, HQC와 함께 4라운드 후보로 선정되었다. SIKE는 2011년에 처음 제안된 Isogeny 기반 암호인 SIDH(Supersingular Isogeny Diffie Hellman)[9]에 기반하고 있으며, 공개키 암호 알고리즘과 선택 평문 공격(Chosen Ciphertext Attack, CCA)을 방어할 수 있는 KEM(Key Encapsulation Mechanism)을 제공하는 알고리즘이다. Isogeny 기반 암호는 초특이 타원곡선 상에서 정의되는 Isogeny 그래프를 활용하여 키를 교환하는 기술이며, 이는 모든 유한체 위에서 정의되는 두 초특이 타원곡선 사이에는 Isogeny 그래프가 존재하나 Isogeny 경로를 알아내기 어려운 성질에 기반하고 있다. 또한, SIKE는 양자 내성 암호 중 동일한 안전성을 제공하는 암호에 비해 짧은 공개키를 갖

는다는 큰 장점이 있다. 또한, 상대적으로 느린 동작 시간을 줄이기 위한 연구가 지속적으로 수행되고 있어[2-5] SIKE에 대한 장점이 부각되며 NIST PQC 4라운드에서 유망한 KEM 알고리즘으로 주목받았으나 최근 특정 조건에서 공격이 수행되어 더 이상 SIKE에 관한 관심이 줄었다.

2.1.1 SIKE 프로토콜[10]

SIKE의 기반이 되는 SIDH protocol은 서로소인 두 수 l_A, l_B에 대하여 $p = l_A^{e_2} \cdot l_B^{e_3} - 1$인 소수를 활용하며 해당 소수에 기반한 복소수체 F_{p^2}위에서 정의되는 타원곡선 $E_0 := y^2 = x^3 + ax^2 + x$, $(x,y) \in F_{p^2}$을 선택한다. 이때, 소수 p는 $l_A^{e_2} \approx l_B^{e_3}$을 만족해야 하고 E_0는 복소수체 F_{p^2} 위에서 위수가 $(l_A^{e_2} \cdot l_B^{e_3})^2$인 초특이 타원곡선을 만족해야 한다. 이와 유사하게 SIKE는 소수 p를 $2^{e_2} \approx 3^{e_3}$인 $p = 2^{e_2} \cdot 3^{e_3} - 1$를 사용하며, 시작 타원곡선을 $E_0 := y^2 = x^3 + 6x^2 + x$로 고정하여 사용한다.

이러한 SIKE의 키 공유 과정은 그림 1과 같으며, Alice의 공개키 생성 과정은 파란색 화살표로 표시된 $E \rightarrow E_A$ 부분이며 Bob의 공개키 생성 과정은 빨간색으로 표시된 $E \rightarrow E_B$에 해당한다. 우선 키를 공유하려는 두 사람을 Alice와 Bob이라고 가정했을 때, 두 사람은 각각 E_0 위의 기저(basis)인 두 점 $\{P_A, Q_A\}$와 $\{P_B, Q_B\}$를 선택하고 사전에 공유한다. 이후, 두 사람은 각자 두 점을 통해 생성자 $R_A = P_A + [sk_A]Q_A$, $R_B = P_B + [sk_B]Q_B$를 만들고 계산된 생성자에 기반하여 생성군 $\langle R_A \rangle$와 $\langle R_B \rangle$를 생성한다. 그 다음 생성군 $\langle R_A \rangle$와 $\langle R_B \rangle$를 통해서 각자의 Isogeny인 $\varnothing_A := E_0 \rightarrow E_0 / \langle R_A \rangle$와 $\varnothing_B := E_0 \rightarrow E_0 / \langle R_B \rangle$를 생성하게 된다. 이때

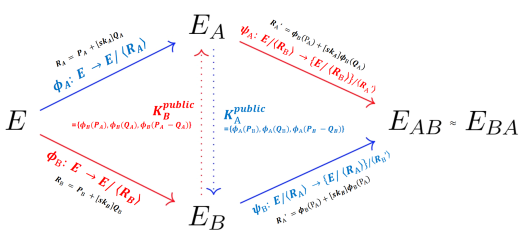

Fig. 1. Secret Key sharing of SIKE

Alice는 생성된 Isogeny를 통해 상대방의 기저 $\{P_B, Q_B\}$와 기저를 통해 연산된 $P_B - Q_B$를 $E_A = E_0 / \langle R_A \rangle$ 위의 세 점 $\{\varnothing_A(P_B), \varnothing_A(Q_B), \varnothing_A(P_B - Q_B)\}$로 옮긴다. 마찬가지로 Bob 역시 Alice의 기저 $\{P_A, Q_A\}$와 기저로부터 파생된 점 $P_A - Q_A$을 $E_B = E_0 / \langle R_B \rangle$위의 세 점 $\{\varnothing_B(P_A), \varnothing_B(Q_A), \varnothing_B(P_A - Q_A)\}$을 생성한다. 이렇게 생성된 세 점은 각자의 공개키가 된다.

서로의 공개키를 공유받은 후 두 사람은 서로의 공개키로부터 식 1과 2와 같이 R'_A와 R'_B와 각자의 생성군 $\langle R'_A \rangle$와 $\langle R'_B \rangle$을 만들어낸다.

$$R'_A = \varnothing_B(P'_A) + [sk_A]\varnothing_B(Q'_A) \quad (1)$$

$$R'_B = \varnothing_A(P'_B) + [sk_B]\varnothing_A(Q'_B) \quad (2)$$

따라서 Alice는 생성군 $\langle R'_A \rangle$를 통하여 Isogeny $\psi_A := E_A \rightarrow E_A / \langle R'_A \rangle$를, Bob은 생성군 $\langle R'_B \rangle$를 통하여 $\psi_B := E_B \rightarrow E_B / \langle R'_B \rangle$을 생성한다. 이때, Isogeny의 치역 $E_{BA} = E_A / \langle R'_A \rangle$와 $E_{AB} = E_B / \langle R'_B \rangle$는 Isogeny의 성질에 의하여 동형이 된다. 따라서 Alice가 Bob의 공개키로부터 E_{BA}를 생성하는 과정은 그림 1에서 빨간색 화살표로 표시된 $E_A \rightarrow E_{BA}$에서 확인할 수 있으며, Bob이 Alice의 공개키로부터 E_{AB}를 생성하는 과정은 파란색 화살표로 표시된 $E_B \rightarrow E_{AB}$이 된다. 최종적으로 동형인 두 타원곡선 E_{BA}와 E_{AB}는 동일한 j-불변량을 갖는다. 이때, 처음 선택된 E_0는 몽고메리 타원곡선이기 때문에 E_{AB}, E_{BA} 또한, 몽고메리 타원곡선이 된다. 따라서 몽고메리 타원곡선 식 $y^2 = x^3 + Ax^2 + x$에 따라 두 사람은 몽고메리 타원곡선의 j-불변량인 식 3과 같이 계산된 값을 공유한다.

$$j = \frac{256(A^2-3)^3}{A^2-4} \quad (3)$$

이러한 j-불변량은 Alice와 Bob이 공유하는 키가 된다. SIKE는 해당 프로토콜을 기반으로 공개키 암호화와 KEM을 제공한다.

2.1.2 Three-point Ladder

Three-point Ladder는 타원곡선암호에서 부채널 분석에 대한 안전성을 높이기 위하여 사용된 기법 중 Montgomery Ladder에 기반한 기법[11]이다. SIKE에서는 세 개의 변수를 활용하여 Isogeny에 필요한 생성자 $P+[sk]Q$를 계산하기 위해 Three-point Ladder를 사용된다. 타원곡선 위 세 점 $Q, P, Q-P$는 세 변수 R, R_0, R_1로 할당되며, 이후 비밀키 sk의 i번째 비트 sk_i가 0일 때에는 $R_1 = R + R_1$가 수행되고 sk_i가 1일 때에는 $R_0 = R + R_0$가 수행된다. 이러한 Point Addition 연산을 수행한 후 R은 Point Doubling 연산 $R = 2 \cdot R$을 수행한다. 해당 절차가 끝난 후, R_0 변수에 할당되어있는 값은 $P+[sk]Q$가 된다.

예를 들어, 비밀키 sk가 간단하게 13이라고 가정한다면, $P+13Q$를 계산할 시 Three-point Ladder를 사용하게 되는데, 이때 비밀키 sk는 $sk = (1101)_2 = (sk_3, sk_2, sk_1, sk_0)_2$로 표현된다. 따라서 $sk_0 = 1$에 대해 $R_0 = R + R_0 (= Q + P)$ 및 $R = 2R$을 수행한다. 다음 비트인 sk_1은 0이므로 $R_1 = R_1 (Q - P) + R (= 2Q)$와 $R = 2R = 4Q$가 계산된다. 이와 같은 과정을 반복하면 $sk_3 = 1$에 대해 $R_0 = R_0 (= P + 5R) + R (= 8R)$과 $R = 2R = 16R$이 수행되면서 $R_0 = P + 13Q$가 생성되며, 최종적으로 $sk = 13$이므로 구하고자 하는 $P + 13Q$가 계산되는 것을 알 수 있다.

특히, SIKE에서는 Three-point Ladder 알고리즘이 R_0와 R_1을 번갈아 가며 수행하는 성질을 반영하기 위해 Algorithm 1의 swap 알고리즘을 수행하게 된다. 이때 추가적인 부채널 정보 누출을 방지하기 위해 타원곡선암호(Elliptic Curve Cryptography)에서 사용된 기법인 Double and Add[12] 기법 및 점을 정사영(Projection)시키는 기법[13]을 사용한다. 이를 xDBLADD 알고리즘이라고 하며, SIKE는 해당 xDBLADD 알고리즘을 통해 Point Doubling과 Point Addition을 함께 수행하게 된다.

Algorithm 1. Swap algorithm

Require : 32bit scalar a, b

1: Let $mask = \begin{cases} 0x00000000 & \text{if } sk_{i-1} \oplus sk_i = 0 \\ 0xFFFFFFFF & \text{if } sk_{i-1} \oplus sk_i = 1 \end{cases}$

2: Compute $tmp = mask \,\&\, (a \oplus b)$

3: Compute $a = tmp \oplus a$

4: Compute $b = tmp \oplus b$

Fig. 2. Swap Algorithms in Three-point Ladder

2.2 부채널 분석

2.2.1 부채널 분석 개요

부채널 분석이란 암호가 동작하면서 발생하는 전력 소비량, 전자파, 소요 시간 등과 같은 다양한 부채널 정보를 수집하고 분석하여 암호에 사용된 비밀키를 복구하는 공격 기법이다.

이러한 부채널 분석 기법 중 가장 활발히 연구되고 있는 분야는 1999년에 처음 제안된 전력 분석 기법이다[14]. 이는 암호가 동작하면서 누출되는 전력 소비량을 측정하여 비밀키와의 관계를 파악하여 공격하는 기법으로써, 크게 단순 전력 분석(Simple Power Analysis, SPA)과 차분 전력 분석(Differential Power Analysis, DPA)로 구분된다. SPA는 단일 파형을 분석하여 비밀키를 복구하는 공격으로 암호가 동작하면서 암호 내부 알고리즘에 따라 다르게 소비되는 전력 소비량의 패턴을 분석하여 비밀키를 알아내는 공격 기법이다[14]. 이와 다르게 DPA는 다수의 파형을 수집하여 암호의 내부 알고리즘과 파형들과의 통계적 분석을 수행하여 비밀키를 복구하는 공격 기법이다[14]. 특히, DPA 중 통계적 분석을 기반으로 파형 간의 상관관계 분석을 수행하는 공격을 상관관계 전력 분석(Correlation Power Analysis, CPA)이라고 한다[15]. 이러한 DPA는 SPA보다 고도화된 기법에 해당하며 상대적으로 더욱 방어하기 어려운 강력한 공격 기법이지만 비밀키를 복구하기 위해 동일한 단일 비밀키 값에 대응하는 다수의 파형을 수집해야 하는 단점이 있다. 이러한 단점을 극복하기 위해 더욱 고도화된 단일 전력 파형을 기반으로 통계적 분석을 수행하는 수평적인 차분 전력 분석(Horizontal Differential Power Analysis, Horizontal DPA)이 제안되었다[16]. Horizontal DPA는 단일 파형을 기준으로 비밀키의 비트에 해당하는 전력 파형을 특정 기준(전력 파형의 평균, 전력 파형의 중간값 등)을 통해 두 집단으로 분류하는 기법이며, 이는 군집화(Clustering)를 활용하는 공격으로써 클러스터링 전력 분석(Clustering Power Analysis)이라고도 불

린다[17]. 또한, 단일 파형을 분리하여 CPA 공격을 수행하는 수평적인 상관관계 분석(Horizontal Correlation Analysis, Horizontal CPA) 공격이 존재한다[18].

한편, 전력 분석에 대하여 기계학습 방법을 적용하는 다양한 연구[8, 19, 20]가 수행되고 있으며 RSA와 ECC등의 기존 암호뿐만 아니라 Saber 등의 양자내성암호에 대한 딥러닝 기반의 부채널 분석이 활발히 수행되고 있다[20]. 이들은 기존에 수작업으로 이루어지던 전력 파형 분석을 자동으로 수행하게 되며, 전력 파형 분석을 위하여 암호 알고리즘 내부의 작동 원리를 이해해야 하는 기존의 전력 분석 방법과 다르게 파형만으로 공격을 수행하는 블랙박스 공격으로서의 장점이 존재한다. 또한, 딥러닝을 활용하면 더욱 정밀한 분석이 가능하여 높은 성능을 보이고 있다.

2.2.2 SIKE에 적용된 부채널 분석

이전까지 SIKE에 적용된 부채널 분석은 DPA, Horizontal CPA, 그리고 클러스터링 전력 분석이 수행되었다[21, 22, 6]. 이 중 Zhang등[21]은 DPA 기반 분석 기법을 제시하였으며 이는 SIKE에 대한 부채널 분석 연구에 대한 바탕이 되었다. 또한, Genet 등[22]은 Horizontal CPA를 적용하였으며, 이는 Three-point Ladder 내부에서 수행되는 덧셈 연산을 대상으로 수행하였다. 그 결과, 해당 공격은 비밀키를 100% 복구하였으며 이후 다수의 대응방법(countermeasure)이 적용될 수 있음을 언급하였다.

또한, Genet 등[6]에 의해 제시된 SIKE에 대한 클러스터링 전력 분석은 군집화 중 하나인 k-means를 사용하였으며, 해당 공격은 전력 파형을 두 그룹으로 분류하여 분석한다. 해당 공격의 대상은 2.1.2장에서 소개된 Three-point Ladder 내부에서 수행되는 swap 알고리즘이며, 이는 전수조사에 필요한 비밀키 후보군을 줄일 수 있다는 장점이 존재한다. 특히, 해당 연구에서는 대응기법도 함께 제시하였으며 그 결과 기존 100%가량의 공격 성공률을 50% 근방으로 떨어짐이 확인되었다. 따라서, 해당 대응기법을 파훼하기 위한 더욱 고도화된 공격 기법이 필요하다.

III. SIKE에 대한 클러스터링 전력 분석[6]

3.1 공격 기법

DPA의 파생 기법에 해당[17]하는 클러스터링 전력 분석은 비밀키를 복구하기 위해 다수의 전력 파형이 필요한 기존의 차분 전력 분석과 달리 단일 전력 파형을 통해 공격을 수행하는 수평적 전력 분석 기법의 하나이며, 이는 단일 파형을 통해 공격하기 때문에 더욱 실용적인 분석 기법이다. SIKE에서의 클러스터링 전력 분석 대상은 2.2장에서 설명한 swap 알고리즘(Algorithm 1)이다. 이러한 swap 알고리즘에서의 마스킹(masking) 값은 $(sk_{i-1} \oplus sk_i)$이 0인 경우와 1인 경우에 따라 hamming weight(1인 비트의 개수)의 차이가 발생하며, 이러한 차이는 곧 전력 소비량에 차이를 발생시키게 된다. 클러스터링 전력 분석은 이러한 특징을 활용하여 군집화 기법의 하나인 k-means를 활용하여 구별할 수 있음을 실험적으로 입증하였다[6].

클러스터링 전력 분석에 대한 구체적인 공격 기법은 다음과 같다. 우선 비밀키의 비트 길이를 n이라고 할 때, 수집된 전력 파형을 n개의 파형으로 분리한다. 이때 분리된 전력 파형의 길이가 T, i번째 비트에 대한 각 지점의 전력 소비량을 $s_{i,j}(0<j\leq T)$라고 하면, j번째 지점의 모든 전력 소비량 $\{s_{i,j}|0<i<n\}$에 대해 k-means를 수행하여 두 그룹으로 분류하게 된다. 이때 각 군집의 평균 변화가 없도록 군집화를 진행하게 되면 평균이 다른 두 군집이 생성된다. 이때, 평균이 작은 군집의 index를 0, 평균이 큰 군집의 index를 1로 지정하고, 해당 index를 활용하여 키 후보군을 생성하게 된다. 구체적으로 j번째 지점의 전력 소비량인 $\{s_{i,j}|\text{for all } i\}$에서 $s_{i,j}$가 속한 군집의 index을 $swap'$으로 지정할 때, 키 후보군의 i번째 비트 sk_i에 대해 $sk_i = sk_{(i-1)} \oplus swap'_i$이며 이를 통해 모든 비트를 유추하여 키 후보군을 생성할 수 있다. 이는 각 j에 대해 하나의 키 후보군을 생성할 수 있게 되며 총 파형의 길이가 T이기 때문에 최종적으로 하나의 비밀키당 T개의 키 후보군을 생성할 수 있다.

[6]에서는 총 1000개의 서로 다른 비밀키를 통하여 실험을 수행하였으며, 이는 1000번의 실험이 진행되었음을 의미한다. 각 비밀키에 대하여 파형의 길이가 25,000일 때, 평균적으로 약 251개의 키 후보

가 올바른 비밀키와 일치하였다. 즉, 25,000개 중 100개를 선택할 시 평균적으로 100개 중 하나는 올바른 비밀키가 존재함을 의미한다.

3.2 전력 파형에 대한 웨이블릿 변환 기법

본 논문에서는 공격의 성공률 및 공격의 속도를 위하여 웨이블릿 변환을 적용하였다. 웨이블릿 변환[7]은 전력 파형에 대한 일종의 차원 축소(dimensionality reduction)를 수행하는 것이며, 이는 파형을 주파수와 시간에 관하여 분석하고 저주파수와 고주파수 영역으로 파형을 분해하게 된다.

$$Y(t) = \sum_{n \in N} 2^{-j/2} h_j(n) \varnothing (2^{-j}t - k) + \sum_{i=1}^{j} 2^{-j/2} l_j(n) \Psi(2^{-j}t - k) \quad (3)$$

이때, 식 3의 과정을 통하여 파형이 변환되며, 여기서 j,k는 켤레 복소수, $Y(t)$는 분해된 신호, j는 분해 단계를 의미한다. 또한, $\varnothing(t)$는 크기를 나타내는 함수이며 $\Psi(t)$는 웨이블릿 함수에 해당하며 $h_j(n)$와 $l_j(n)$은 각각 높은 주파수 필터(high frequency filter)와 낮은 주파수 필터(low frequency filter)를 의미하며 웨이블릿 변환을 활용하면 파형의 높은 주파수 필터를 통하여 변환된 파형을 반환하게 된다. 즉, 낮은 주파수 영역을 걸러 주어 파형의 잡음을 줄일 수 있다. 한편, 각 low frequency filter를 거친 파형의 주파수들은 다음 단계의 웨이블릿 변환에 입력값으로 활용된다.

결론적으로, 이러한 웨이블릿 변환을 활용하면 해당 전력 파형에 대한 특징점이 유지된 채로 기존의 전력 파형에 비해 절반의 길이를 갖게 된다. 이러한 장점으로 인해 웨이블릿 변환을 이용하게 되면 공격의 속도를 올리면서 동시에 공격의 성공률을 유지할 수 있게 된다.

해당 공격에서는 웨이블릿 변환 중 'sym4'를 사용하였으며 웨이블릿 변환은 최대 7번 적용하였다. 7번의 웨이블릿 변환과 1번의 푸리에 변환을 함께 적용했을 때 파형의 길이는 101이고 101개의 키 후보군을 특정할 수 있었으며 해당 키 후보군 중 평균적으로 4개의 키 후보가 올바른 비밀키와 동일하였다.

3.3 대응 기법

앞서 언급하였듯이, 해당 클러스터링 전력 분석[6]은 swap 알고리즘에서 누출되는 미세한 전력 파형의 차이를 통해 키를 복구하는 기법에 해당한다. 이러한 전력 파형 차이는 algorithm 1의 swap 알고리즘에서 사용되는 $mask$ 값에서 발생하며, 해당 전력 파형의 차이를 줄이기 위해 마스킹 값을 임의의 값 $m1$과 그에 따라 파생되는 값 $m2$로 분리하여 계산하는 방어 기법을 제시하였다. 이때 $m1$, $m2$ 값은 $m1 \oplus m2 = mask$를 만족해야 한다.

해당 기법에서 사용되는 $m1$은 랜덤한 값으로 선택되며 $m2$는 $(1-2 \cdot swap)(m1 + swap)$으로 계산되고 이때 $swap = sk_{i-1} \oplus sk_i$이다. 즉, swap이 0이라면 $m1$과 동일한 값이 되며 swap이 1이 되면 $m2$는 $m1$의 비트별 보수가 된다. 따라서 대응기법을 적용한 swap 알고리즘은 Algorithm 2[6]와 같다.

[6]에서 해당 대응기법을 적용한 SIKE에서 서로 다른 비밀키 500개에 대하여 클러스터링 전력 분석을 수행한 결과, 500번의 실험 모두 올바른 비밀키와 일치하는 키 후보군을 찾지 못하였다. 또한, 각 실험당 모든 키 후보군에 대하여 올바른 비밀키와의 비트별 일치율을 확인한 결과 평균 50%의 일치율이 발생하였음이 입증되었다.

이는 적용된 방어 기법이 클러스터링 공격을 충분히 방어하고 있다고 볼 수 있다. 그림 4는 $\{s_{i,2499}\}$에 대한 클러스터링 결과를 정규분포로 그려낸 그래프에 해당한다. 파란색 실선은 k-means 알고리즘에 의하여 0번째 군집으로 대응된 $\{s_{j,2499} \mid j \in 0,1,2,...,n-2,n-1\}$들의 정규분포며, 주황색 점선은 1번째 군집으로 대응된 $\{s_{k,2499} \mid k \in 0,1,2,...,n-2,n-1\}$들의 정규분포다. 이때, 두 정규분포가 비슷한 양상을 보이고 있으며,

Algorithm 2. Swap algorithm with Countermeasure

Require : 32bit scalar a, b
1: Pick random $m1$
2: Compute $m2 = (1-2 \cdot swap)(m1 + swap)$
  where $swap = sk_{i-1} \oplus sk_i$
3: Compute $tmp1 = m1 \,\&\, (a \oplus b)$
4: Compute $tmp1 = m1 \,\&\, (a \oplus b)$
5: Compute $a = (tmp \oplus a) \oplus tmp2$
6: Compute $b = (tmp \oplus b) \oplus tmp2$

Fig. 3. Swap Algorithms with Countermeasure

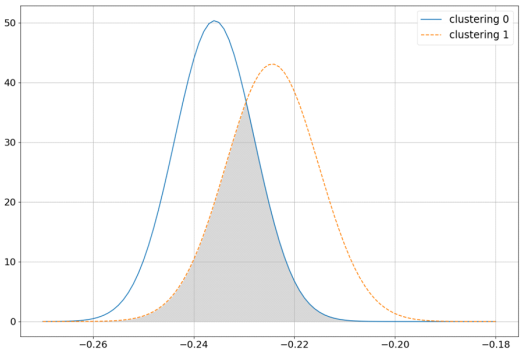

Fig. 4. Normal distribution graphs of clustering results at $j = 2499$

두 그룹의 중첩된 부분이 많이 발생하는 것을 알 수 있고 중첩된 부분에 속한 $s_{i,2499}$가 어느 한쪽에 속하기 힘들다는 것을 의미한다. 즉, 올바른 군집화가 이루어지지 못하였음을 간접적으로 보여주고 있다. 따라서 적용된 대응기법은 군집화를 방해하여 매우 효과적으로 클러스터링 전력 분석을 방어하는 기법이라고 할 수 있다.

IV. ECC에 대한 딥러닝 기반 클러스터링 공격[8]

최근에는 부채널 분석에 딥러닝을 활용하는 연구가 수행되고 있다[8, 19, 20]. 딥러닝 기반 부채널 분석 기법은 기존에 모든 파형에 대한 분류를 위해 사전 작업을 수행해야 하는 부채널 분석과는 다르게 생성한 파형 데이터 자체를 입력값으로 두어 자동 분석이 가능하므로 여러 이점을 지니고 있다. 또한, 최근 들어 딥러닝 기반 부채널 분석 기법이 기존 기법에 비해 월등한 성능을 보임이 입증되었다. 이번 장에서는 21년에 제안된 최신 연구[8]를 기반으로 딥러닝 기반 부채널 공격에 관해 설명한다.

특히, 21년에 제안된 연구[8]에서는 부채널 공격에 관한 대응기법(Cswap)[23]이 적용된 타원곡선암호(Elliptic Curve Cryptography, ECC)에 대해 딥러닝 기반 부채널 분석을 수행하였으며, 해당 공격으로 최대 정확도 99%와 평균 90% 후반대의 높은 정확도를 제시하였다. 따라서, 이러한 딥러닝 기반 부채널 분석은 NIST PQC 구성 암호에 대해 모두 분석되고 연구되어야만 한다.

4.1 공격 구성

Perin[8] 등에 의해 제안된 기법은 Cswap[23]이 적용된 타원곡선암호를 목표로 딥러닝 기반 부채널 분석을 수행하였다. 해당 공격에서는 k-means를 기반으로 클러스터링 공격을 일차적으로 수행한 후 해당 결과를 기반으로 1D convolution 연산을 수행하였다. 상세하게, 이는 일차적으로 군집화 알고리즘인 k-means를 통해 전력 파형에 대한 군집화를 수행한 후 분류된 값들에 대해 레이블(label)을 설정하였고, 이처럼 레이블이 설정된 전력 파형 데이터를 딥러닝 계층에 삽입하였다. 이때 사용된 딥러닝 계층 마지막에는 2진 분류를 수행하는 계층인 완전 연결 계층(Fully Connected Layer, FCL)을 삽입하여 이진 분류를 수행하게 된다. 또한, 과적합(overfitting)을 방지하기 위해 데이터 증강(data augmentation) 및 드롭아웃(dropout)을 활용하였다. 해당 연구에서 활용한 데이터 증강 기법은 파형 하나당 랜덤하게 오른쪽이나 왼쪽으로 파형을 최대 5번 시프트(shift) 하여 데이터의 다양성을 높이고, 이를 통한 결과를 상호 간에 비교하였다. 그 결과, 95% 이상의 분류 정확성을 보였으며, 이는 딥러닝 기반 기법이 부채널 분석에 유효하게 사용될 수 있음을 입증하였다.

4.2 학습 방법

해당 기법[8]에서는 일반적인 학습 방법인 training, validation, test 순서의 학습 방법이 아닌 새로운 학습 방법을 활용하였다. 먼저, 데이터 셋으로부터 Training set와 validation set을 5:1로 구성하였으며 Training set을 다시 1:1로 구분하여 데이터셋 D1, D2를 생성하였다. 또한, 해당 연구에서는 두 번의 배치 학습을 묶어 한 번의 Iteration으로 정의하였으며, 데이터 셋 D1으로 배치 학습이 완료되면 D2로 test를 진행한다. 이때, test의 예측된 값들은 다음 배치 학습에서 D2의 label로써 활용되며 이를 재레이블화(relabeling)이라고 명칭하고 있다. D1의 배치 학습이 완료된 후 D2의 배치 학습이 진행되며 마찬가지로 D1에 대하여 다시 relabeling을 진행한 후 두 데이터 셋 D1과 D2를 다시 통합하여 순서를 섞어준다. 위의 과정을 통하여 한 번의 Iteration이 완료되며, 이때 모든 배치 학습에서 validation 과정을 진행한다.

이때 처음에 진행되는 학습의 레이블로 주어지는 값은 학습 데이터로 클러스터링 공격을 수행하였을 때, 해당 파형이 속한 군집의 index가 주어진다. 또한, 학습이 진행되면서 relableing를 통하여 계속 변화된다. 이때 정확도를 측정하는 방법은 실제 비밀키의 비트를 비교 대상으로 하여 신경망의 예측값과의 정확도를 측정한다. 해당 방법을 활용하면 k-means 같은 군집화와 유사하게 비지도 학습을 유지할 수 있다.

이러한 비지도 학습은 두 그룹에 대하여 명확한 차이가 보일 때 좋은 학습을 진행할 수 있다. 하지만 SIKE에 적용된 3.3장의 대응기법은 군집화되는 두 그룹 차이를 모호하게 해서 학습에 어려움이 존재할 수 있고 이를 해결하기 위하여 학습에 대한 확실한 지표가 필요하다. 따라서 3.3의 대응기법에 대하여 지도 학습을 진행할 필요가 있다.

V. 제안하는 SIKE에 대한 딥러닝 기반 클러스터링 공격

이번 장에서는 본 논문이 제안하는 SIKE에 대한 딥러닝 기반 클러스터링 공격에 대해 정의하고 설명한다. 특히, 제안하는 기법은 ECC에 대한 딥러닝 기반 부채널 분석 기법[8]과 웨이블릿 변환[7]을 이용하여 SIKE에 대한 부채널 분석 중 클러스터링 전력 분석 공격에 대한 대응기법[6]에 대하여 공격을 수행하였다. 또한, 제안하는 기법에 대한 실험 과정 및 결과에 대해 분석한다.

5.1 구성 및 방법

본 연구에서는 3.3장의 대응기법에 대해 5장의 딥러닝 기반 클러스터링 공격을 활용하여 공격을 수행한다. 학습 방법은 4장의 딥러닝 기반 클러스터링 공격과 유사하게 파형을 데이터 셋을 2.5: 2.5: 1 비율의 D1, D2, validation set으로 구성한다. 또한, Iteration 한번당 D1, D2의 학습을 진행한다. 각 데이터 셋에 대한 학습이 끝난 후 validation과 test를 진행한다. 하지만 4장의 딥러닝 학습과 다르게 relabeling을 진행하지 않는다. 이는 앞서 4.2에서 설명했듯이 해당 3.3의 대응기법이 적용된 파형은 군집화되는 두 그룹의 차이를 모호하게 하므로 정확한 지표가 필요하기 때문이다.

Table 1. CNN Construction

Layer	composition
Input	input_size = 2500
Conv1D_1	8 filters, ks=20, stride=4
Conv1D_2	16 filters, ks=20, stride=4
Conv1D_3	32 filters, ks=20, stride=4
Dense_1	100 neurons
Dense_2	100 neurons
softmax	2 neurons

5.2 제안하는 기법의 모델 구성

제안하는 기법에 대한 딥러닝 모델 구성은 표 1과 같다. 실험에 활용된 1D convolution 구조는 [8]와 유사하게 3계층 convolution과 2계층 FCL 구조를 활용하였다. Convolution 연산의 kernel 크기는 20으로 사용하였으며, 각 레이어의 필터 개수는 8개, 16개 32개로 구성하였다. 또한, stride의 크기는 모두 4로 고정하였다. 모델에게 입력값으로 주어지는 파형의 길이는 2500이며, 최종 출력값은 이진 분류를 위해 2개로 구성되어 있다. 또한, [8]에서도 적용한 과적합 방지를 위해 데이터 증강과 드롭아웃을 활용하였다. 데이터 증강에 대해서는 [8]에서 활용한 각 파형 당 임의로 오른쪽 또는 왼쪽으로 최대 5번 시프트(shift)를 통해 데이터의 다양성을 높이는 기법을 적용하였다.

학습에 사용된 손실함수(loss fuction)은 교차엔트로피(cross entropy)를 사용하였으며, 최적화 기법(optimizer)은 RMSprop 및 Adam을 사용하였다. 또한, 활성화 함수(activation function)에 대해서는 ReLU(Rectified Linear Unit) 및 LeakyReLU를 사용하였으며, 모델의 학습률(Learning rate)은 0.0001로 고정하였다.

5.3 실험 환경

전력 파형 수집을 위해 ChipWhisperer-Lite Level 2 Starter Kit을 사용했으며, 대상 기기는 ChipWhisperer의 32bit Cortex-M4 칩인 STM32F3을 탑재한 UFO 보드를 사용하였다. 또한, 딥러닝 학습 환경에는 Intel(R) Core(TM) i9-10980XE CPU @ 3.00GHz, NVIDIA Geforce RTX 3090를 활용하였으며, Ubuntu 20.04.4 LTS에서 실험을 진행하였다.

데이터 셋은 총 600개의 서로 다른 비밀키에 대하여 파형을 수집하였다. 이때 비밀키는 n bit라고 할 때, 모든 비트에 대하여 swap 알고리즘이 수행된다. 따라서 수집된 파형의 개수는 총 $600 \bullet n$개이며, 파형 하나당 길이는 2500이다. 또한, 파형에 해당하는 $swap = sk_{i-1} \oplus sk_i$ 값을 label로 사용하였으며 2개의 class 즉, 0은 [0,1], 1은 [1,0]으로 변형하여 label로 입력하였다. 본 연구에서는 4장에서 진행한 비지도 학습과 마찬가지로 relabeling을 통한 실험을 진행한 결과 최대 73% 정확도가 측정되었으며 해당 실험을 통하여 일정 수치 이상 정확도가 올라가지 않음을 확인하였다. 따라서 비지도 학습이 아닌 실제 $swap$을 label로 활용한 지도 학습을 진행하였다. 이는 3.3장의 대응기법으로 인해 비지도 학습으로는 파형들이 명확히 구별되지 않기 때문이며, 이를 해결하기 위해 정확한 지표를 제시하기 위함이다.

5.4 최적 공격 모델 수립 및 결과

공격 수행에 앞서, 4장에서 설명한 딥러닝 공격을 3.3장의 대응기법에 적용하기 위하여 최적의 모델을 찾는 과정을 수행하였다. 기본적인 모델 구성은 동일하게 3계층 CNN 계층과 2계층 FCL 계층을 사용하였다.

상기 언급하였듯이 해당 모델에 대하여 먼저 최적화 함수를 RMSprop와 Adam으로 비교하였고, 활성화 함수는 ReLU, LeakyReLU를 적용하여 비교하였다. 최적화 함수에 대해, RMSprop는 학습 시 최적화 과정에서 최종 적용되는 학습률을 학습 상황에 알맞게 조정함으로써 보다 효율적이고 안전하게 수렴하는 최적화 기법에 해당한다. 이러한 특징으로 인해 [8]에서는 RMSprop를 사용하였다. 추가적으로, Adam 최적화 기법은 RMSprop와 Momentum을 합친 최적화 함수로써 현재 가장 많이 활용되는 최적화 함수에 해당하며, RMSprop와 마찬가지로 학습 속도가 조절되면서 학습의 방향성까지 고려할 수 있는 장점이 있다. 따라서 본 실험에서는 최적화 함수의 범용성을 고려하여 RMSprop와 Adam을 비교 진행하였다. 또한, 활성화 함수 측면에서, [8]에서는 ReLU[24]만을 사용했지만 ReLU의 경우 입력값이 음수일 경우 모두 0으로 반환하는 특성이 존재하기 때문에 가중합이 음수인 노드를 비활성화 시키는 단점이 존재한다. 이를 해결하기 위하여 음수의 입력값(x)에도 $0.01x$을 반환하는 LeakyReLU[25]를 사용하여 비교 분석을 수행하였다. 추가적으로, 가중치 초깃값 설정에서도 [8]의 경우에는 Xavier 초기화를 사용하였는데, 이는 초기화의 경우 비선형함수에 대하여 효과적인 성능을 나타내지만[26], ReLU 함수와 함께 사용하였을 때 비효

Table 2. Result of optimal model search

Method	Optimizer	Activation	Initializer	Accuracy
Without Wavelet transform	RMSprop	ReLU	He	95%
			Xavier	96%
		Leaky ReLU	He	97%
			Xavier	97%
	Adam	ReLU	He	95%
			Xavier	96%
		Leaky ReLU	He	96%
			Xavier	97%
With Wavelet transform	RMSprop	ReLU	He	99%
			Xavier	99%
		Leaky ReLU	He	99%
			Xavier	99%
	Adam	ReLU	He	99%
			Xavier	99%
		Leaky ReLU	He	99%
			Xavier	99%

율적인 문제가 존재한다. 따라서 He 초기화가 Xavier 초기화에 비해 ReLU와 함께 사용하기 좋은 초기화 함수[27]이기 때문에 두 가지의 초기화 함수를 적용하고 최적의 모델을 탐색하였다.

또한, 본 논문에서는 딥러닝 기반 분석이 수행되기 이전에 전력 파형에 대한 웨이블릿 변환[7]을 추가적으로 수행하였다. 이는 전력 파형이 가지고 있는 잡음을 제거하고 특징점을 두드러지게 하기 위함으로써 일종의 차원 축소를 적용하여 Convolution 계층이 특징점을 효율적으로 학습시킬 것으로 예상하였다.

해당 실험을 수행한 결과는 표 2와 같다. 해당 정확성은 평균값을 나타낸다. 웨이블릿 파형이 적용된 딥러닝 기반 분석 모델이 적용되지 않았을 경우에 비해 모두 높은 정확도를 보이는 것을 알 수 있다. 또한, 모델 최적화 측면에서는, 활성화 함수를 LeakyReLU로 진행했을 때보다 높은 정확성을 보이는 것을 알 수 있다. 또한, Adam에 비해 RMSprop가 안정적으로 학습이 진행되는 것을 확인하였으며, 가중치 초기화 함수 역시 He 초기화보다는 Xavier 초기화가 더 좋은 성능을 보임을 알 수 있다.

또한, 탐색된 최적 모델을 활용하여 과적합을 방지하기 위해서는 데이터 증강 및 드롭아웃과 같은 과정이 추가로 필요하다. 본 논문에서도 역시 이들을 적용하여 비교하였으며, 실험 진행 결과 모두 평균 90% 후반의 높은 정확도가 측정되는 것을 확인하였다. 그림 5은 데이터 증강(data augmentation)과 드롭아웃(dropout)을 적용한 결과를 나타낸다.

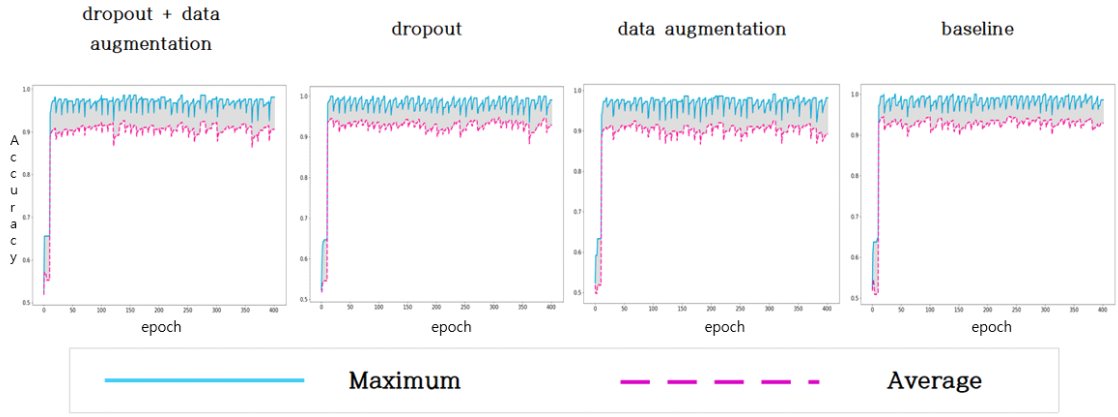

Fig. 5. Maximum, and average single trace accuracy with deep learning framework on the countermeasure of clustering

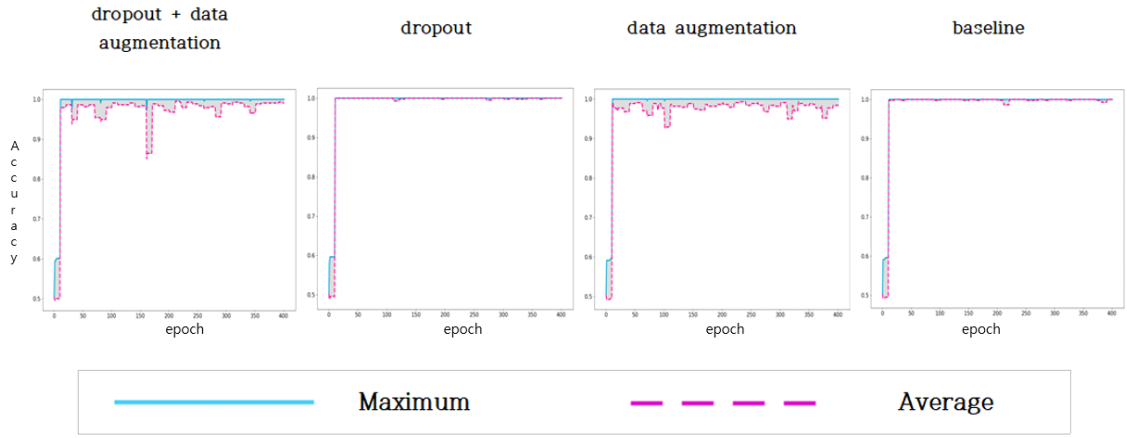

Fig. 6. Maximum, and average single trace accuracy with deep learning framework on the countermeasure of clustering when applied wavelet transform('sym4')

Baseline은 드롭아웃과 데이터 증강이 모두 적용되지 않은 상태를 의미한다. 이는 하나의 비밀키 n비트에 대하여 예측한 swap값에 대한 정확도를 나타낸 것이다. 또한, 그림 6는 웨이블릿 변환이 적용된 상태에서 그림 5와 마찬가지의 과적합 방지 기법을 적용한 결과이다. 이들은 모두 전체 100개의 비밀키에 대하여 정확도를 측정하였으며, 파란색 실선은 비밀키의 최대 정확도를, 붉은색 파선은 평균 정확도를 나타낸 것이다. 이때 그림 3 및 그림 4에서 확인할 수 있듯이, 데이터 증강 활용 시 오히려 평균 정확도가 소폭 하강한다는 것을 확인할 수 있으며, 이는 SIKE 및 적용되어있는 대응기법의 경우 데이터의 다양성을 증가시키기 위하여 사용한 기법이 오히려 학습 데이터에 잡음을 추가한 것으로 볼 수 있다. 또한, 드롭아웃 적용 결과, baseline과 유사한 정확도를 보임을 알 수 있었으나, 마찬가지로 데이터 증강과 함께 사용하게 되면 학습 데이터에 대한 잡음 추가로 인해 정확도가 소폭 하강하였다.

VI. 결 론

본 논문에서는 SIKE에 대한 전력 분석 기반 암호 분석 기술에 관한 연구를 수행하였다. 특히, 웨이블릿 변환 및 딥러닝 부채널 공격 모델을 설계하여 최신 대응기법이 적용된 SIKE에 대한 전력 분석을 수행하였으며, 그 결과 기존 클러스터링 전력 분석 기법의 정확도가 50% 내외인 반면, 본 연구에서는 100% 가까운 분석 성공률을 보였다. 이는 현존하는 SIKE 기법에 대한 가장 강력한 공격임을 실험적으로 입증하였다.

하지만 최근 SIKE의 알고리즘 내부 구조를 활용하여 공격을 수행하는 기법이 제안[28]되었으며, 이는 NIST PQC Standard 4라운드 후보군으로 속해있는 SIKE에 대한 최종 선정 가능성을 떨어트렸다. 그러나, Isogeny 기반 암호는 여러 특장점으로 인해 아직 경쟁력이 유효한 분야이며, 이는 CSIDH[29]와 같은 또 다른 Isogeny 기반 암호에 대한 가능성은 아직 열려있음을 의미한다. 실제로 NIST 측에서도 Isogeny 기반 암호에 대한 추가 공모 등의 스케줄을 고려하고 있는 것으로 발표하기도 하였으며[30], 이와 동시에 현재 SIKE 외 Isogeny 기반 암호는 수학적으로 안전한 것으로 확인되고 있다[31].

따라서, SIKE뿐만 아니라 CSIDH 기반 암호 등에 대한 클러스터링 공격 등의 부채널 분석 연구는 지속되어야하며, 이는 본 논문에서 제안하는 기법 등이 향후 부채널 분석 연구에의 주요한 기술이 될 것으로 기대된다. 그러나 SIDH와 다르게, CSIDH는 Three-point Ladder 기법을 사용하지 않으므로 본 논문에서 제시한 클러스터링 공격 활용을 위해서는 CSIDH에 대한 추가적인 분석이 필요하다. 따라서 향후 부채널 공격을 적용하기 위한 CSIDH의 취약점을 찾는 연구를 진행할 예정이며, CSIDH 및 CSIDH를 기반으로 하는 SeaSign[32] 등에 대한 부채널 공격 기술 및 대응 기법에 대한 연구를 계획할 예정이다.

References

[1] W. Shor, Peter, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review, pp.303-332, Jun. 1999.

[2] R. Elkhatib et al, "Faster Isogenies for Quantum-Safe SIKE," Cryptology ePrint Archive, 2021.

[3] R. Elkhatib et al, "Faster Isogenies for Post-quantum Cryptography: SIKE," In Cryptographers' Track at the RSA Conference, pp. 49-72, Jan. 2022.

[4] B. Koziel et al, "SIKE'd up: Fast hardware architectures for super-singular Isogeny key encapsulation," IEEE Transactions on Circuits and System I: Regular Papers 67.12, pp. 4842-4854, Dec. 2020.

[5] M Anastasova et al, "Compressed SIKE Round 3 on ARM Cortex-M4," In International Conference on Security and Privacy in Communication Systems, pp.441-457, Sep. 2021.

[6] A. Genêt and N. Kaluderović, "Single-trace clustering power analysis of the point-swapping procedure in the three point ladder of Cortex-M4 SIKE." In International Workshop on Constructive Side-Channel Analysis and

Secure Design, pp. 164-192, Apr. 2022.
〔7〕 D. Zhang and D. Zhang, "Wavelet transform," In Fundamentals of image data mining: Analysis, Features, Classification and Retrieval, pp. 35-44, May. 2019.
〔8〕 G. Perin et al "Keep it unsupervised: Horizontal attacks meet deep learning," IACR Transactions on Cryptographic Hardware and Embeded Systems, pp. 343-372, Jan. 2021.
〔9〕 L. De Feo, D. Jao, J. Plût "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," Journal of Mathematical Cryptology, 8(3), pp. 209-247, May. 2014.
〔10〕 M. Campagna et al, "Supersingular isogeny key encapsulation," 2019.
〔11〕 D. J. Bernstein and T. Lange, "Montgomery curves and the montgomery ladder," Cryptology ePrint Archive, 2017.
〔12〕 K. Elsentrager, " An efficient Procedure to double and add points on an elliptic cuve," Cryptology ePrint Archive, 2002.
〔13〕 P. Y. Liardet and N.P. Smart, "Preventing SPA/DPA in ECC Systems using the Jacobi form", In International Workshop on Cryptographic Hardware and Embedded Systems, pp. 391-401, May. 2001.
〔14〕 P. Kocher et al. "Differential power analysis," In Annual International cryptology conference, pp. 388-397, Aug. 1999.
〔15〕 E. Brier et al. "Correlation power analysis with a leakage model," In International workshop on cryptographic hardware and embedded systems, pp. 16-29, Aug. 2004.
〔16〕 I. kabin et al, "Horizontal address-bit DPA against montgomery kP implementation," In 2017 International Conference on ReConFigurable Computation and FPGAs, pp. 1-8, Dec. 2017.
〔17〕 F. Shi et al, "A systematic approach to horizontal clustering analysis on embeded RSA implementation," In 2019 IEEE 25th International Conference on Parallel and Distributed Systems, pp. 901-906, Dec. 2019.
〔18〕 C. Clavier et al. "Horizontal correlation analysis on exponentiation," In International Conference on Information and Communications Security, pp. 46-61, Dec. 2010.
〔19〕 H. Machrebi, "Deep learning based side channel attacks in pratice," Cryptology ePrint Archive, 2019.
〔20〕 K. Ngo et al, "A side-channel attack on a masked IND-CCA secure saber KEM implementation," IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 676-707, Sep. 2021.
〔21〕 F. Zhang et al, "Side-channel analysis and countermeasure design on ARM-based quantum-restitant SIKE," IEEE Transactions on Computers, vol. 69, no. 11, pp. 1681-1693, Aug. 2020.
〔22〕 A. Genet et al. "Full key recovery side-channel attack against ephemeral SIKE on the Cortex-M4," In International Workshop on Constructive Side-Channel Analysis and Secure Design, pp. 228-254, 2021.
〔23〕 G. Hinterwalder et al, "Full-size high-security ECC implementation on MSP430 microcontrollers," In International conference on cryptology and information security in Latin America, pp. 31-47, Sep. 2014.
〔24〕 A. F. Agarap, "Deep learning using rectified linear units(relu)," arXiv preprint arXiv: 1803.08375, 2018
〔25〕 B. Xu et al, "Empirical evaluation of rectified activation in convolution

network," arXiv preprint arXiv: 1505.00853, 2015.
〔26〕 X. Clorot and Y. Bengio, "Understading the difficulty of training deep feedforward neural networks," Proceeding of the thirteenth international conference on artificial intelligence and statistics, pp. 249-256, Mar. 2010.
〔27〕 K. He et al, " Delving deep into rectifiers: Surpassing human-level performance on Imagenet classification," In Proceedings of the IEEE international conference on computer vision, pp. 1026-1034, 2015.
〔28〕 W. Castryck. and T. Decru. "An efficient key recovery attack on SIDH (preliminary version)," Cryptology ePrint Archive. 2022.
〔29〕 W. Castryck et al, "CSIDH: an efficient post-quantum commutative group action," In International Conference on the Theory and Application of Cryptology and Information Security, pp. 395-427, Dec. 2018.
〔30〕 D. Moody, "The Future of PQC", In Inside Quantum Technology, Oct. 2022.
〔31〕 D. Jao, "SIKE Update", In Forth PQC Standardization Conference. Nov. 2022.
〔32〕 L. De Feo, and S. D. Galbraith, "SeaSign: compact isogeny signatures from class group actions", In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 759-789. Springer, Cham. May. 2019.

〈저자소개〉

임 우 상 (Woosang Im) 학생회원
2021년 2월: 공주대학교 응용수학과 학사
2023년 2월: 공주대학교 융합과학과 공학석사
2023년 3월~현재: 공주대학교 융합과학과 박사과정
〈관심분야〉 양자내성암호, 부채널 분석, 인공지능 등

장 재 영 (Jaeyoung Jang) 학생회원
2023년 2월: 공주대학교 응용수학과 학사
2023년 3월~현재: 공주대학교 응용수학과 석사과정
〈관심분야〉 데이터보안, 블록체인, PQC, DID 인증 기술

김 현 일 (Hyunil Kim) 정회원
2014 2월: 공주대학교 응용수학과 학사
2016 2월: 공주대학교 융합과학과 공학석사
2019년 8월: 공주대학교 융합과학과 공학박사
2020년 3월~2022년 6월: 대구경북과학기술원 박사후연구원
2022년 7월~현재: 공주대학교 연구교수
〈관심분야〉 암호기술, 프라이버시 보존형 연합학습 기술, DID 인증 기술

서 창 호 (Changho Seo) 종신회원
1990년: 고려대학교 수학과 학사
1992년: 고려대학교 수학과 이학석사
1996년: 고려대학교 수학과 이학박사
1996년~1996년: 국방과학연구소 선임연구원
1996년~2000년: 한국전자통신연구원 선임연구원, 팀장
2000년~현재: 공주대학교 응용수학과 교수
〈관심분야〉 암호알고리즘, PKI, 무선인터넷 보안 등