Journal of the Korea Academia-Industrial cooperation Society
Vol. 23, No. 3 pp. 16-24, 2022

https://doi.org/10.5762/KAIS.2022.23.3.16
ISSN 1975-4701 / eISSN 2288-4688

양자 내성 암호 FALCON에 대한 차분 전력 분석 공격 성능 개선

장세창[1], 이재욱[2], 배대현[3], 하재철[1*]
[1]호서대학교 정보보호학과, [2]호서대학교 컴퓨터공학부, [3]고려대학교 정보보호대학원

Performance Improvement of Differential Power Analysis Attack on Post Quantum Cryptosystem FALCON

Sechang Jang[1], Jaewook Lee[2], Daehyeon Bae[3], Jaecheol Ha[1*]
[1]Dept. of Information Security, Hoseo University
[2]Division of Computer Engineering, Hoseo University
[3]Graduate School of Information Security, Korea University

요 약 양자 컴퓨터가 발전하면서 기존에 상용되던 암호 시스템은 양자 알고리즘으로 인해 안전성을 보장받을 수 없어졌으며 이에 대한 대안으로 NIST(National Institute of Standards and Technology)에서는 양자 내성 암호 표준화 사업이 진행되고 있다. NIST PQC Round 3에서 전자서명 분야 표준 후보 알고리즘인 FALCON은 격자 기반 전자서명 알고리즘으로 향후 표준화 진행이 유력하다. 하지만 서명 생성 시 실행되는 부동소수점 곱셈 연산에서 부채널 누설 정보가 존재하며 이를 통해 비밀 정보인 개인 키가 노출될 가능성이 있다. 본 논문에서는 부동 소수점 곱셈 연산 과정의 전력 파형을 분석하여 차분 전력 분석 공격을 시도하였다. 또한, 두 확률 분포의 차이를 계산하는 함수인 쿨백-라이블러 발산(Kullback-Leibler divergence)을 차분 전력 분석 공격에 적용하여 공격 성능을 향상시키는 방법을 제안한다.

Abstract With the development of quantum computers, the previous cryptographic system cannot be guaranteed safe due to the quantum algorithm. In NIST PQC Round 3, FALCON is likely to be standardized in the future as a standard candidate algorithm for lattice-based digital signatures. However, side-channel leakage information exists in the floating-point multiplication performed during signature generation. Moreover, there is a possibility that the private key, which is secret information, may be exposed. This research attempted a differential power analysis attack by analyzing the power traces of the floating-point multiplication process. In addition, we propose a method to improve the attack performance. This method applies the Kullback-Leibler divergence function to a differential power analysis attack to calculate the difference between two probability distributions.

Keywords : FALCON, Post-Quantum Cryptography, Side-Channel Attack, DPA, Kullback-Leibler Divergence

1. 서론

현재 상용화되고 있는 정보보호 시스템은 데이터에 대한 기밀성과 무결성을 제공하기 위해 RSA, AES, ECDSA 등과 같은 암호와 서명 알고리즘을 사용한다[1,2]. 그러나 이러한 암호용 알고리즘들이 양자 컴퓨팅 환경에서는 더 이상 안전성을 보장할 수 없다는 연구 결과가 보고되었다. 기존의 컴퓨터는 트랜지스터로 만들어진 게이트를 이용해 0과 1을 구분할 수 있는 비트(bit)로 연산을 수행하지만, 양자 컴퓨터는 양자를 연산 법칙으로 사용하여

본 논문은 2021년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다.
(No. 2021RIS-004)
*Corresponding Author : Jaecheol Ha(Hoseo Univ.)
email: jcha@hoseo.edu
Received December 30, 2021 Revised January 26, 2022
Accepted March 4, 2022 Published March 31, 2022

0과 1을 공존시키는 큐빗(qubit)으로 연산을 수행하여 초고속으로 데이터를 처리할 수 있다. 따라서 기존의 소인수 분해나 이산대수 문제 등에 기반한 공개 키 암호 시스템과 전치, 치환 등의 연산으로 이루어진 대칭 키 암호 시스템은 각각 양자 알고리즘인 Shor 알고리즘[3]과 Grover 알고리즘[4]을 구현한 양자 컴퓨터에 의해 안전성을 보장할 수 없게 되었다.

미국의 NIST(National Institute of Standards and Technology)에서는 2016년부터 이러한 양자 컴퓨터로부터 안전한 암호 알고리즘인 양자 내성 암호(Post Quantum Cryptography, PQC)의 표준화 작업을 진행하고 있다. 현재 진행 중인 NIST PQC Round 3의 PKE/KEM(Public-Key Encryption/Key Encapsulation Mechanism) 분야에는 SABER, CRYSTAL-KYBER, NTRU, Classic McEliece 그리고 전자서명 분야에는 CRYSTAL-DILITHIUM, FALCON, Rainbow가 표준안 후보로 선정되어 있다[5]. 최종적인 PKE/KEM 알고리즘과 전자서명 알고리즘은 2023년에 결정될 예정이다. 위와 같은 양자 내성 암호 알고리즘들은 수학적 난제에 기반하여 이론적인 안전성을 확보하고 있어야 하지만, 알고리즘을 구현하여 구동시키는 과정에서 발생하는 부채널 분석과 같은 물리적 공격에도 대응할 수 있어야 한다.

양자 내성 암호가 본격적으로 개발되기 전에는 블록 암호 알고리즘으로 AES가 많이 사용되었으며 공개 키 암호 알고리즘으로 RSA 및 ECDSA 등이 사용되었다. 그러나 이 역시 부채널 분석 공격으로 인해 구현상의 많은 취약점이 발견되었고 이에 대한 대응책을 마련하고 있다[6-8]. 블록 암호 알고리즘에서는 대부분 S-Layer에서 이루어지는 비선형 연산을 수행할 때 발생하는 부채널 누설 신호를 이용하여 바이트 단위로 비밀 키를 추출하였다. 공개 키 암호 알고리즘에서는 개인 키를 사용하는 모듈러 연산이나 타원곡선 연산에서 비트 단위로 비밀 정보를 복구하였다.

본 논문에서는 NIST PQC Round 3 전자서명 분야의 표준 후보인 FALCON(FAst Fourier Lattice-based COmpact signatures over NTRU)을 대상으로 전력 분석 공격을 수행하여 개인 키를 복구해 보고자 한다[9]. 또한, 두 확률 분포의 차이를 계산하는 함수인 쿨백-라이블러 발산(Kullback-Leibler divergence)[10]을 차분 전력 분석 공격에 적용하면 공격 성능이 향상됨을 실험적으로 확인하였다.

본 논문의 구성은 다음과 같다. 2장에서는 부채널 공격, FALCON 전자서명 알고리즘 및 쿨백-라이블러 발산을 설명한다. 3장에서는 FALCON의 서명 과정 중 진행되는 부동 소수점 곱셈 대상 차분 전력 분석 공격을 진행하여 그 공격 결과를 분석하며, 4장에서 결론을 맺는다.

2. 배경 지식

2.1 부채널 공격

부채널 공격은 암호 알고리즘이 실행될 때 발생하는 부가적인 정보를 통해서 비밀 정보를 획득하는 것을 말한다. 이러한 부채널 공격의 종류 중 하나인 비침투 공격은 전력, 전자파, 시간차 등의 부가적인 정보를 이용하여 비밀 정보를 찾는 것을 말한다. 이러한 전력 부채널 공격에는 단순 전력 분석 공격(Simple Power Analysis, SPA), 차분 전력 분석 공격(Differential Power Analysis, DPA) 그리고 상관 전력 분석 공격(Correlation Power Analysis, CPA) 등이 있다[11, 12]. 지금까지 제시된 많은 양자 내성 암호 또한 수학적 이론으로부터는 안전하지만 이러한 부채널 공격으로부터는 완전히 자유롭지 않다.

현재 NTST에서는 3 Round의 검증 과정을 거쳐 양자 내성 표준 후보 알고리즘 7개를 선정하였다. 그러나 PKE/KEM 분야에서 선정된 후보 암호 알고리즘도 다양한 형태의 부채널 공격으로 인해 암호 메시지가 복구되거나 비밀 키가 바로 노출되는 연구 결과가 있었다[13, 14]. 특히, 양자 내성 암호는 동일한 평문에 대해서도 다른 암호문을 출력하는 랜덤성이 부여된 경우가 많아 DPA나 CPA보다 단일 파형을 보고 비밀 키를 찾아내는 연구도 있었다[15].

본 논문에서는 NTST 3 Round에 진출한 격자 기반 전자서명 알고리즘인 FALCON에 대한 전력 기반 부채널 공격을 수행하였다. FALCON은 NTT(Number Theoretic Transform)를 통한 변환 대신 FFT(Fast Fourier Transform)[16] 기법을 활용한다. 서명 과정에서 FFT는 정수 값을 부동 소수점 값으로 변환시키게 된다. 서명 과정에서 수행되는 부동소수점 곱셈 연산의 전력 파형을 이용하면, 부동소수점으로 표현된 비밀 성분인 부호 비트, 지수 비트. 그리고 가수 비트를 각각 추출할 수 있음을 확인하고자 한다.

본 연구에서는 먼저 표준안에 제시된 FALCON 서명 알고리즘을 분석하여 비밀 정보가 사용되는 부분을 찾아 부채널 공격을 적용할 신호 측정 범위를 선정한다. 그 후 실제 실험용 마이크로프로세서에 구현 코드를 탑재한 후

암호 알고리즘을 구동하면서 소비 전력 신호를 측정하게 된다. 측정된 신호는 해밍 웨이트(Hamming weight) 전력 모델에 따라 DPA 공격을 통해 비밀 키가 복구 가능함을 검증하게 된다. 이 DPA 공격시에는 전력 신호의 정확한 분류가 공격 성공의 요인이 되므로 쿨백-라이블러 발산 기법을 이용하여 비밀 키 추출 성능이 향상됨을 증명하고자 한다.

2.2 FALCON 전자서명 알고리즘의 개요

다음 Fig. 1은 FALCON의 키 생성 알고리즘을 나타낸 것이다. 알고리즘에서 사용하는 중요한 파라미터는 ϕ와 q이다[17]. $\phi = x^n + 1$이고 q는 모듈러 연산에 사용되는 소수 값이다. 위의 두 인자를 이용하여 개인 키 생성에 필요한 다항식을 만들게 된다.

Input: A monic polynomial $\phi \in \mathbb{Z}[x]$, a modulus q
Output: A secret key sk and a public key h
1: $f, g, F, G \leftarrow$ NTRUGen(ϕ, q)
2: $B \leftarrow \begin{bmatrix} g & -f \\ G & F \end{bmatrix}$
3: $\hat{B} \leftarrow FFT(B)$
4: $G \leftarrow \hat{B} \times \hat{B}^*$ ▷ $\times$ represents matrix multiplication
5: $T \leftarrow$ ffLDL*(G)
6: **for each** leaf of T **do**
7: $\quad leaf.value \leftarrow \sigma / \sqrt{leaf.value}$
8: **end for**
9: $sk \leftarrow (\hat{B}, T)$
10: $h \leftarrow gf^{-1} mod(q)$
11: return sk, h

Fig. 1. FALCON key generation algorithm

먼저 NTRU에 기반한 다항식 생성 과정을 통해 정수 계수를 갖는 다항식 f와 g를 생성한다. f와 g는 이산 가우스 분포(discrete Gaussian distribution)를 통해 임의의 계수를 생성한다. 이때 f와 g는 $Z[x]$ 상에서 존재하는 값들이다. 암호 시스템 사용자는 f와 g를 생성하고 나서는 $Z[x]$상의 다항식 F와 G를 생성하게 된다. 이렇게 생성된 비밀 요소 f, g, F, G는 Eq. (1)과 같은 NTRU 방정식을 만족해야 한다.

$$fG - gF = q \bmod \phi \quad (1)$$

다음 단계에서는 위에서 생성된 비밀 요소를 이용하여 B를 생성하며 B는 FFT를 통해 $\hat{B}$으로 변환한다. $\hat{B}$을 이용하여 완전 계수 그람 행렬(full-rank Gram matrix) G를 만들며 G를 이용하여 트리 T를 생성한다. 최종적으로 $\hat{B}$와 트리 T를 이용하여 개인 키 sk를 생성한다. 공개 키 h는 비밀 요소 f와 g를 이용하여 생성한다. 개인 키와 공개 키는 모두 비밀 요소들로부터 생성되는데, 이러한 비밀 요소들은 공격자에게 노출되거나 복구될 수 없어야 한다.

Fig. 2는 FALCON의 서명 생성 알고리즘을 나타낸 것이다. 서명 생성에 필요한 320비트의 난수 r은 서명 과정을 거친 메시지와 함께 수신자에게 전달된다. 서명 시스템을 공격하는 입장에서 보면 서명 생성에 필요한 메시지 m 과 난수 r을 모두 알 수 있으므로 해시 함수 SHAKE-256을 사용하여 해시 메시지 c를 복원할 수 있다.

서명에서 c와 비밀 요소 f, F는 각각 FFT를 통해 64비트 부동소수점 형태로 변환되며 부동소수점 곱셈 연산을 수행한다. 이때 공격자는 Fig. 2의 3단계에서 보는 바와 같이 해시 메시지 c를 알고 있고 비밀 요소 f와 F 값을 복구하는 부채널 공격을 수행할 수 있다. 실제로 2021년 E. Karabulut 등은 전자기파 측정을 이용하여 서명 과정 중 진행되는 부동소수점 곱셈 연산에서 비밀 정보인 개인 키를 추출하는 방법을 소개한 바 있다[17].

Input: a message m, a secret key sk, a bound β^2
Output: a signature sig of m
1: $r \leftarrow \{0,1\}^{320}$ uniformly
2: $c \leftarrow$ HashToPoint $(r||m)$
3: $t \leftarrow (\frac{-1}{q} FFT(c) \odot FFT(F), \frac{1}{q} FFT(c) \odot FFT(f))$
4: **do** ▷ $\odot$ represents FFT multiplication
5: $\quad$ **do**
6: $\quad\quad z \leftarrow$ ffSampling (t, T)
7: $\quad\quad \mathbf{s} \leftarrow (t - z) \begin{bmatrix} FFT(g) & -FFT(f) \\ FFT(G) & -FFT(F) \end{bmatrix}$
8: $\quad$ **while** $s^2 > [\beta^2]$
9: $\quad (s_1, s_2) \leftarrow invFFT(s)$
10: $\quad s \leftarrow$ Compress$(s_2, 8 \cdot sbytelen - 328)$
11: **while** $s = \perp$
12: return $sig = (r, s)$

Fig. 2. FALCON signature generation algorithm

2.3 고속 푸리에 변환

공격자는 FALCON의 서명 과정에서 개인 키 f와 이미 알고 있는 c에 대해 고속 푸리에 변환(Fast Fourier Transform, FFT)을 사용하는 $FFT(c) \circ FFT(f)$ 연산에 전력 부채널 공격을 시도할 수 있다. 이 연산에서 c나 f를 부동 소수점으로 변환한 후 계수별 곱셈(coefficient-wise multiplication) 연산을 수행하게 된다. Fig. 3에서 보는 바와 같이 FFT 연산에서는 8비트 비밀 요소 (f, g, F, G)나 16비트 해시 메시지를 64비트 부동소수점 표현으로 변환된다. 변환된 64비트 다항식 계수 값의 최상위 1비트는 부호 비트이며, 이어지는 11비트는 지수부, 52비트는 가수부이다.

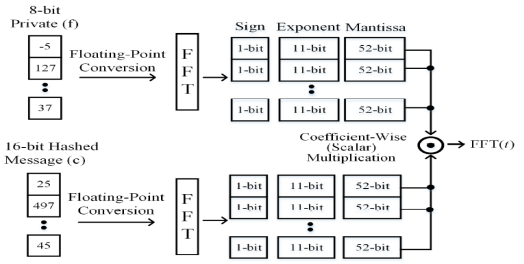

Fig. 3. Multiplication of the private element f and hashed message polynomial c

2.4 쿨백-라이블러 발산

본 논문에서는 서명 생성 시 발생하는 전력 소비량을 측정하고 DPA 공격을 적용함으로써 개인 키를 복구해 보고자 한다. DPA 공격의 핵심은 공격자가 추측한 비밀 정보를 바탕으로 공격 지점의 중간 값을 계산하고 그 중간 값들의 해밍 웨이트를 수집한다. 그리고 해밍 웨이트가 높은지 낮은지에 따라 측정한 전력 파형을 분류한다. 그 후 해밍 웨이트가 높은 그룹과 낮은 그룹으로 분류한 후 이를 차분(뺄셈)한 값들을 이용하여 개인 키를 복구하게 된다. 즉, 공격자가 추측한 키가 맞으면 두 그룹을 차분한 전력 파형은 해밍 웨이트가 높은 그룹과 낮은 그룹의 전력 소비량 차이가 나지만 키를 잘못 추측한 경우에는 차분 값이 잡음처럼 나타나 차분 값에 피크(peak)가 발생하지 않게 된다.

그래서 해밍 웨이트가 높은 그룹과 낮은 그룹을 서로 차분하여 두 그룹의 차이를 표현하는 것보다 두 그룹의 특징을 극대화할 수 있는 방안이 필요하다. 따라서 본 논문에서는 쿨백-라이블러 발산 기법을 이용하여 전력 소비 파형을 가진 두 그룹의 특징을 더 명확히 구분하고자 한다.

원래 쿨백-라이블러 발산이란 주어진 두 확률 분포 P, Q의 차이를 계산하는 함수이다. 상대 엔트로피(relative entropy)라고도 불리는 쿨백-라이블러 발산은 P 분포에 대해 이를 근사하는 Q 분포를 사용해 샘플링 했을 때 발생하는 정보 엔트로피의 차이를 의미한다. 이산 확률 분포 P의 정보 엔트로피는 Eq. (2)와 같이 계산될 수 있다.

$$-\sum_i P(i) \cdot \log_2 P(i) \tag{2}$$

확률 분포 P를 근사하는 Q 분포로 샘플링 했을 때의 정보 엔트로피는 Eq. (3)과 같이 표현될 수 있다.

$$-\sum_i P(i) \cdot \log_2 Q(i) \tag{3}$$

따라서 두 확률 분포 P, Q의 정보 엔트로피 차이는 Eq. (4)와 같이 계산될 수 있다.

$$-\sum_i P(i) \cdot \log_2 Q(i) - (-\sum_i P(i) \cdot \log_2 P(i)) \tag{4}$$

또한, 두 이산 확률 분포 P, Q에 대한 쿨백-라이블러 발산을 Eq. (5)와 같이 표현할 수도 있다.

$$KLD = \sum_i P(i) \cdot \log_2 \frac{P(i)}{Q(i)} \tag{5}$$

결국, 쿨백-라이블러 발산의 값이 0이라면 두 확률 분포는 같다는 것을 의미하며, 0보다 큰 경우에는 두 확률 분포의 차이에 비례하는 값을 갖는다. 따라서 본 논문에서 수행하는 부동소수점 연산에 대한 DPA 공격에서 두 파형의 차분을 이용하는 것이 아니라 쿨백-라이블러 발산을 사용하여 정확한 개인 키를 추측했을 때 두 그룹의 차이를 표현할 수 있도록 KLD 값을 활용한다.

3. 부동소수점 곱셈 연산 시 차분 전력 분석

3.1 DPA 공격 실험 환경

Fig. 4는 FALCON의 서명 생성 과정 중 진행되는 부동소수점 곱셈을 대상으로 한 DPA 공격의 핵심 연산을 도시한 것이다. 64비트 부호 없는 정수로 정의된 부동소수점은 52비트의 가수부, 11비트의 지수부, 1비트의 부호 비트로 구성되어 있다. 이때 부동소수점 곱셈 연산은 가수의 곱셈, 지수의 덧셈, 부호의 XOR 연산 순서로 진행된다.

본 논문에서는 가수부, 지수부에 대해 각각 DPA 공격을 수행한다. 공격이 성공하였을 경우 FFT(f) 값을 얻을 수 있고, 역 FFT 연산을 통해 비밀 요소인 f 값을 복구할 수 있다. 비밀 요소 f를 복구하게 되면 공개 키를 이용해 비밀 요소 g를 알아낼 수 있게 된다. 이 때 f와 g를 모두 알면 다항식 F 및 G를 계산할 수 있어 공격자는 전체 개인 키를 도출할 수 있고 임의의 메시지에 서명할 수 있다.

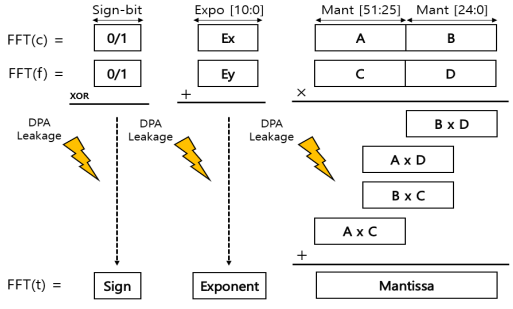

Fig. 4. DPA attack on floating-point multiplication

DPA 공격 실험에 사용한 FALCON은 NIST PQC Round 3에 공개된 참조용 소스 코드(reference source code)를 사용하였다. 이 코드를 arm-none-eabi-gcc 컴파일러와 -O0 플래그를 사용하여 컴파일한 후 ARM-Cortex-M4 코어가 탑재된 32비트 프로세서인 STM32F MCU에 구현하여 실험하였다. 전력 파형은 ChipWhisperer Lite를 사용하여 29.5MS/s 속도로 측정하였다[18]. 다음 Fig. 5는 FALCON에 대한 부채널 공격 실험 환경을 나타낸 것이다.

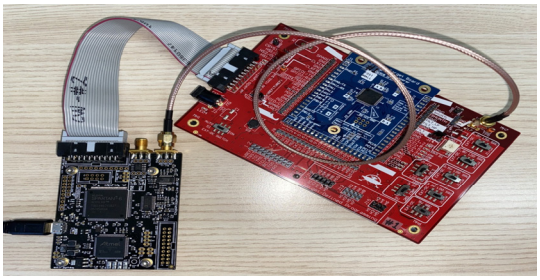

Fig. 5. Experimental setup using STM32F MCU and ChipWhisperer platform.

먼저, ChipWhisperer를 사용하여 측정한 부동소수점 곱셈 부분의 전력 소비 파형은 Fig. 6과 같다. 실험에서는 복구해야 할 비밀 부동 소수 값을 0xC33828BB90A8AABC로 가정하였다. 이 경우 올바른 부호 비트는 0x01, 지수 비트는 0x433, 가수 비트는 0x828BB90A8AABC(상위 비트 : 0x4145DC8, 하위 비트 : 0xA8AABC)이다.

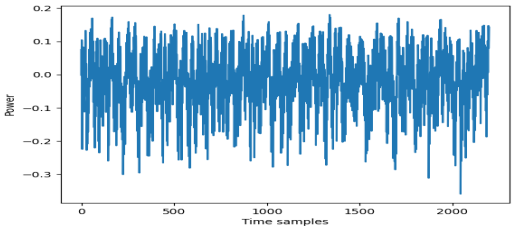

Fig. 6. Power trace of floating-point multiplication

3.2 가수부 DPA 공격

부동 소수점 곱셈 연산 진행 시 가수부는 곱셈 연산을 시행한다. 먼저 FFT(c)와 FFT(f) 계수의 가수부분인 하위 52비트를 구한다. 이때 가수부 곱셈은 1.xx 형식 간의 곱셈이므로 각각의 값 앞에 1을 붙여 53비트의 부호 없는 정수로 만든다. 이어서 FFT(c)의 가수와 FFT(f)의 가수를 하위 25비트, 상위 28비트로 나누어 곱셈을 진행한다. 곱셈 결과 2^{105} 이상의 값은 지수의 덧셈 부분으로 반올림하며 나머지 값 중 상위 52비트를 새로운 가수로 반환한다.

FTT(f) 가수부의 하위 25비트 (Fig. 4의 D)를 공격하기 위해 먼저 25비트인 D에 대해 추측한 비밀 정보를 생성한다. $B \times D$ 연산을 누출 지점으로 선택하여 해밍 웨이트를 계산하고 중간 값에 따라 두 그룹으로 분류한 후 DPA 공격을 진행한다. 논문에서는 공격의 성공 여부를 확인하기 위해 D에 대한 추측 값을 key_map으로 생성하여 256개로 설정하였다. 이때 올바른 값(계수 0xC33828BB90A8AABC)은 key_map의 0x04에 위치한다. 그리고 공격에 사용한 파형의 개수는 10,000개이다. Fig. 7은 가수부 하위 25비트에 대한 DPA 결과이다. 올바른 추측 값의 위치인 0x04에서 높은 차분 값이 관찰되어 DPA 공격으로 비밀 정보가 복구됨을 확인하였다.

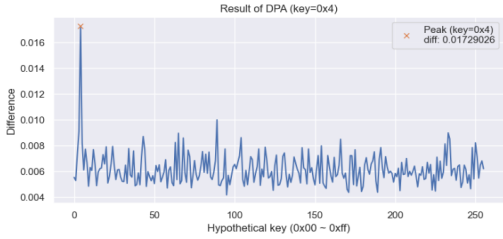

Fig. 7. DPA results on lower-order 25-bits of mantissa

다음으로 FTT(f) 가수부의 하위 25비트를 대상으로 본 논문에서 제안하는 쿨백-라이블러 발산을 적용한 DPA 공격을 수행하였다. 기존의 DPA 공격에서는 중간 값에 따라 파형을 두 그룹으로 나누고, 각 그룹의 평균을 차분하는 연산을 진행하지만, DPA 공격에 확률 분포의 차이를 계산하는 함수인 쿨백-라이블러 발산을 적용하면 파형의 평균을 단순히 차분한 결과보다 더 좋은 공격 결과를 기대할 수 있다. 즉, 쿨백-라이블러 발산 값이 클수록 두 그룹의 차이가 크다는 것을 의미한다.

다음 Fig. 8은 하위 25비트에 대한 쿨백-라이블러 발산이 적용된 DPA 결과이다. 공격 결과 올바른 키를 찾아내는 데 성공하였으며 기존의 일반 DPA 공격을 진행한 Fig. 7과 비교하여 추측이 올바른 값일 때와 다른 추측일 때의 차이가 크게 나타나는 것을 확인할 수 있다. 따라서 쿨백-라이블러 발산 기법을 DPA 공격에 활용하면 두 그룹의 차이를 명료하게 구분할 수 있기 때문에 공격이 더 용이함을 확인할 수 있었다.

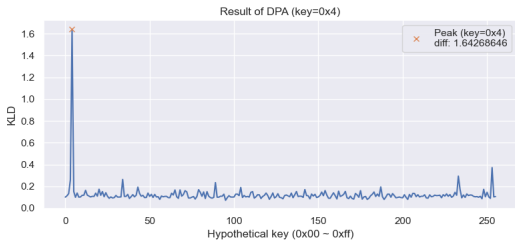

Fig. 8. KLD-DPA results on lower-order 25-bits of mantissa

논문에서는 가수부 하위 25비트에 대하여 파형의 개수에 따른 공격 성능을 알아보기 위해 전력 파형을 100개씩 늘려가며 총 100번의 DPA를 진행하였다. 그림에서 적색 라인이 올바르게 추측한 값에 대한 차분 이며 회색 라인은 틀리게 추측한 값에 대한 차분을 의미한다. 분석 결과 Fig. 9와 같이 약 1,200개 이상의 파형을 이용하여 공격을 진행할 경우 올바른 가수 값을 복구할 수 있다는 것을 확인하였다.

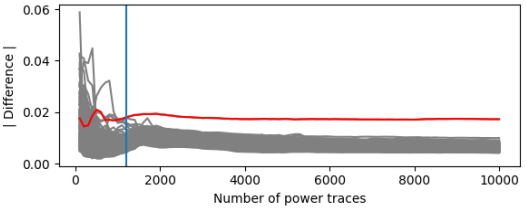

Fig. 9. Comparison of differences according to the number of traces on multiplication of lower-order 25-bits mantisss

Fig. 10은 위와 같은 방법으로 쿨백-라이블러 발산이 적용된 DPA를 진행하였을 때 전력 파형 개수에 따른 KLD 결과를 나타낸 것이다. 분석 결과 파형이 약 300개 이상일 때부터 올바른 가수 값을 복구할 수 있는 것을 확인하였으며 Fig. 9의 DPA 분석 결과와 비교하여 더 좋은 성능을 보이는 것을 확인하였다.

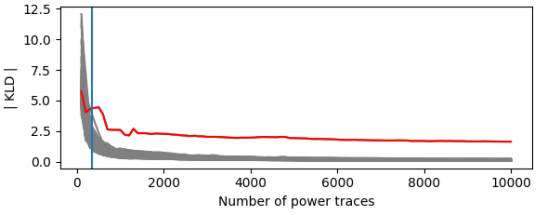

Fig. 10. Comparison of KLD parameters according to the number of traces on multiplication of lower-order 25-bits mantissas

FTT(f) 가수부의 상위 27비트 (Fig. 4의 C)를 공격하기 위해 27비트인 C에 대한 추측을 생성한 후 $B \times C$ 연산을 누출 지점으로 선택하여 해밍 웨이트를 계산하고 DPA 공격을 진행하였다. 가수부 상위 27비트에 대한 DPA 결과도 올바른 추측 값의 위치에서 높은 차분 값이 관찰되어 공격이 성공함을 확인하였다. 동일한 방법으로 FTT(f) 가수부의 상위 27비트를 대상으로 쿨백-라이블러 발산을 적용한 DPA 공격을 수행하였는데 하위 비트 공격과 같이 명확히 비밀 정보를 구분할 수 있었다.

상위 27비트에 대한 쿨백-라이블러 발산이 적용된 경우 효과를 알아보기 위해 전력 파형을 100개씩 늘려가며 총 100번의 DPA를 진행하였다. DPA 분석 결과는 Fig. 11과 같으며 약 700개 이상의 파형을 이용하여 공격을 진행할 경우 올바른 상위 27비트 가수 값을 복구할 수 있다.

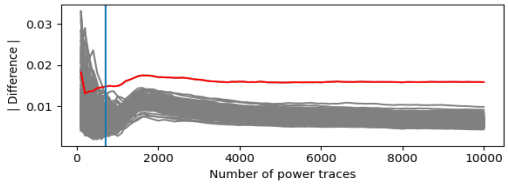

Fig. 11. Comparison of differences according to the number of traces on multiplication of higher-order 27-bits mantissas

다음 Fig. 12는 위와 같은 방법으로 쿨백-라이블러 발산이 적용된 DPA를 진행하였을 때 전력 파형 개수에 따른 KLD 분포를 나타낸 것이다. 분석 결과 파형이 약 200개 이상일 때부터 올바른 상위 27비트 가수 값을 복구할 수 있는 것을 확인하였으며 Fig. 13의 DPA 분석 결과와 비교하여 더 좋은 성능을 보이는 것을 확인하였다.

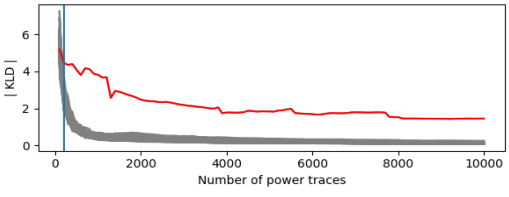

Fig. 12. Comparison of KLD parameters according to the number of traces on multiplication of higher-order 27-bits mantissas

3.3 지수부 DPA 공격

부동 소수점 곱셈 연산을 구동할 경우 지수부는 곱셈이 아닌 덧셈 연산을 수행하게 된다. 즉, 공격자 입장에서는 지수부 연산에 대한 전력 소비량이 미미하기 때문에 전력 분석 공격은 더욱 어렵다고 볼 수 있다.

지수부 연산에서는 먼저 FFT(c)와 FFT(f) 계수의 지수 부분인 11비트를 구한다. 이후 두 지수 값에 대한 덧셈 연산을 하고 가수부에서 반올림된 값을 더하여 새로운 지수 값으로 반환하게 된다.

FFT(f)의 지수부(Fig. 4의 Ey)를 공격하기 위해 먼저 11비트인 Ey에 대한 추측 값을 생성한다. 두 지수 값이 더해지는 연산을 누출 지점으로 선택하여 해밍 웨이트를 계산하고 중간 값에 따라 두 그룹으로 분류한 후 DPA 공격을 진행한다. 실험에 사용한 D에 대한 추측 값은 key_map을 생성하여 256개로 설정하였으며 계수 0xC33828BB90A8AABC에 대한 올바른 지수 값인 0x433으로 가정하였다. 공격에 사용한 파형의 개수는 100,000개이며 Fig. 13은 지수부 덧셈 연산에 대한 DPA 결과이다. 올바른 추측 값인 0x433을 찾는 데 성공하였지만, 가수부 DPA 결과와 달리 올바른 추측 값과 그렇지 않은 추측 값의 차분 결과 값 차이가 크게 나지 않는 것을 확인할 수 있다.

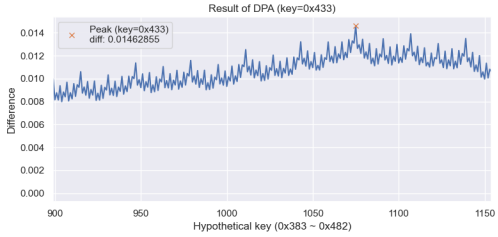

Fig. 13. DPA results on 11-bits of exponent

FFT(f) 가수부 공격과 동일한 방법으로 지수부를 대상으로 쿨백-라이블러 발산을 적용한 DPA 공격을 진행하였다. 그 결과 Fig. 14와 같이 올바른 키를 찾아내는 데 성공하였다. 또한, 기존의 일반 DPA 공격을 진행한 Fig. 13과 비교하여 추측이 올바른 값일 때의 차분 값과 다른 추측에 대한 KLD 결과의 차이가 크게 나타나는 것을 확인할 수 있었다.

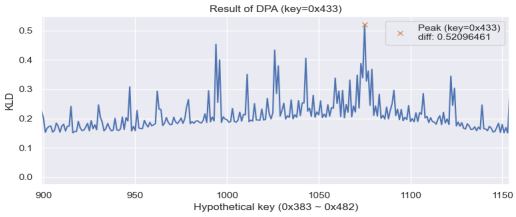

Fig. 14. KLD-DPA results on 11-bit of exponent

지수부 11비트에 대하여 파형의 개수에 따른 공격 성능을 알아보기 위해 전력 파형을 1,000개씩 늘려가며 총 100번의 DPA를 진행하였다. 분석 결과 전체적으로 올바른 추측 값과 다른 추측과의 차분 값 차이가 아주 미세하여 성능이 좋지 않음을 Fig. 15를 통해 확인할 수 있다.

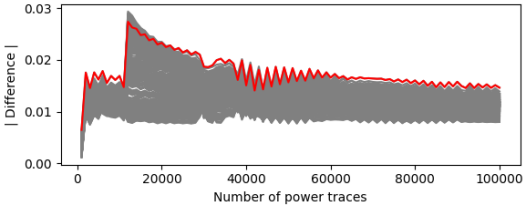

Fig. 15. Comparison of differences according to the number of traces on addition of two exponents

반면, Fig. 16은 지수부 11비트에 대하여 쿨백-라이블러 발산이 적용된 DPA를 진행하였을 때 전력 파형 개수에 따른 KLD 결과를 나타낸 것이다. 분석 결과 1,000개 이상의 파형을 이용하여 공격을 진행할 경우 올바른 지수 값을 복구할 수 있다는 것을 확인하였으며 기존의 DPA 분석 결과와 비교하여 더 좋은 성능을 보이는 것을 확인하였다.

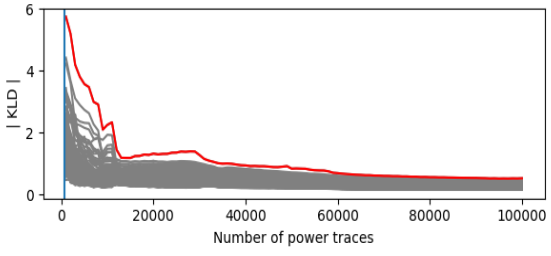

Fig. 16. Comparison of KLD parameters according to the number of traces on addition of two exponents

5. 결론

양자 컴퓨터가 개발되고 발전됨에 따라 기존 암호 알고리즘의 안전성이 위협받고 있다. 따라서 NIST를 중심으로 양자 컴퓨터로부터 안전한 양자 내성 암호 표준화 작업이 이루어지고 있다. 본 논문에서는 양자 내성 암호 중 전자서명 분야의 FALCON을 대상으로 한 차분 전력 분석 공격에 대한 가능성을 실험하였다. 실험 결과, FALCON은 두 부동 소수점 표현 값을 곱셈하는 과정에서 차분 전력 공격에 의해 개인 키가 노출될 수 있음을 고찰하였다. 또한, 두 확률 분포의 차이를 계산하는 함수인 쿨백-라이블러 발산 기법을 차분 전력 분석 공격에 적용하였다.

FALCON를 대상으로 차분 전력 분석 공격을 실험한 결과, 서명 과정 중 구동되는 부동 소수점 곱셈에서 비밀 요소의 가수부 및 지수부를 모두 복구할 수 있었다. 또한, DPA에 쿨백 라이블러 발산을 적용하여 공격을 수행한 결과 분석 성능이 향상되는 결과를 얻었다. 본 논문을 통해 FALCON의 서명 과정 중 부채널 정보 누출이 존재하며 비밀 요소를 복구할 수 있기 때문에 향후 FALCON을 구현할 경우에는 이에 대한 대응책을 마련하여야 할 것이다.

References

[1] Federal Information Processing Standards Publication (FIPS 197), "Advanced Encryption Standard(AES)," National Institute of Standards and Technology (NIST), 2001.
DOI: https://doi.org/10.6028%2FNIST.FIPS.197

[2] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM Vol. 21, Issue 2, pp. 120–126, 1978.
DOI: https://doi.org/10.1145/359340.359342

[3] P. Shor, "Polynomial time algorithms for discrete logarithms and factoring on a quantum computer," SIAM Journal on Computing, Vol. 26, Issue 5, pp. 1484–15091997.
DOI: https://doi.org/10.1137/S0097539795293172

[4] L. Grover, "A fast quantum mechanical algorithm for database search," ACM symposium on Theory of Computing(STOC'96), pp. 212-219, 1996.
DOI: https://doi.org/10.1145/237814.237866

[5] G. Alagic et al., "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process," US Department of Commerce, National Institute of Standards and Technology, 2021.
DOI: https://doi.org/10.6028/NIST.IR.8309

[6] T. Messerges, "Securing the AES finalists against power analysis attacks", FSE'00, LNCS 1978, pp. 150-164, 2001.
DOI: https://doi.org/10.1007/3-540-44706-7_11

[7] T. Messerges, E. Dabbis, and R. Sloan, "Power analysis attacks of modular exponentiation in smartcard," CHES'99, LNCS 1717, pp. 144-157, 1999.
DOI: https://doi.org/10.1007/3-540-48059-5_14

[8] J. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," CHES'99, LNCS 1717, pp. 292-302, 1999.
DOI: https://doi.org/10.1007/3-540-48059-5_25

[9] T. Oder, J. Speith, K. Höltgen, and T. Güneysu, "Towards Practical Microcontroller Implementation of the Signature Scheme Falcon", PQCrypto'19, LNCS 11505, pp. 65-80, 2019.
DOI: https://doi.org/10.1007/978-3-030-25510-7_4

[10] S. Kullback and R. Leibler, "On information and sufficiency.", The annals of mathematical statistics, Vol. 22, No. 1, pp. 79-86, 1951
DOI: http://dx.doi.org/10.1214/aoms/1177729694

[11] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", CRYPTO'99, LNCS 1666, pp. 388-397, 1999.
DOI: https://doi.org/10.1007/3-540-48405-1_25

[12] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model", CHES'04, LNCS 3156, pp. 16-29, 2004.
DOI: https://doi.org/10.1007/978-3-540-28632-5_2

[13] P. Ravim, S. Roy, A. Chattopadhyay, and S. Bhasin, "Generic side-channel attacks on CCA-secure lattice-based PKE and KEMs", TCHES'20, Vol. 2020, No. 3, pp. 307–335, 2020.
DOI: https://doi.org/10.13154/tches.v2020.i3.307-335

[14] K. Ngo1, E. Dubrova1, Q. Guo, T. Johansson, "A Side-Channel Attack on a Masked IND-CCA Secure Saber KEM Implementation", TCHES'21, Vol. 2021, No. 4, pp. 676–707, 2021.
DOI: https://10.46586/tches.v2021.i4.676-707

[15] B. Sim, J. Kwon, J. Lee, I. Kim, T. Lee, J. Han, H. Yoon, J. Cho, and D. Han, "Single-trace attacks on the message encoding of lattice-based KEMs", IEEE Access Vol. 8, pp. 183175-183191, 2020
DOI: https://doi.org/10.1109/ACCESS.2020.3029521

[16] M. Fürer, "Faster integer multiplication", SIAM Journal on Computing, Vol. 39, No. 3, pp. 979-1005, 2009
DOI: https://doi.org/10.1137/070711761

[17] E. Karabulut and A. Aysu, "Falcon Down: Breaking Falcon Post-Quantum Signature Scheme through Side-Channel Attacks", ACM/IEEE Desion Automation Conference(DAC'21), pp. 691-696, 2021
DOI: http://dx.doi.org/10.1109/DAC18074.2021.9586131

[18] C. O'Flynn and Z. Chen, "ChipWhisperer: An Open-Source Platform for Hardware Embedded

Security Research, COSADE'14, LNCS 8622, pp. 243-260, 2014.
DOI: https://doi.org/10.1007/978-3-319-10175-0_17

장 세 창(Sechang Jang) [준회원]

- 2022년 2월 : 호서대학교 정보보호학과 (학사)
- 2022년 3월 ~ 현재 : 호서대학교 정보보호학과 석사과정

〈관심분야〉
양자 암호, 네트워크 보안, 부채널 분석

이 재 욱(Jaewook Lee) [준회원]

- 2017년 3월 ~ 현재 : 호서대학교 컴퓨터공학부 학부과정

〈관심분야〉
인공지능 보안, 자연어처리, 부채널 공격

배 대 현(Daehyeon Bae) [준회원]

- 2021년 2월 : 호서대학교 컴퓨터정보공학부 (학사)
- 2022년 2월 : 호서대학교 정보보호학과 (석사)
- 2022년 3월 ~ 현재 : 고려대학교 정보보호대학원 박사과정

〈관심분야〉
부채널 공격, 암호학, 정보보호

하 재 철(Jaecheol Ha) [종신회원]

- 1989년 2월 : 경북대학교 전자공학과 (학사)
- 1993년 8월 : 경북대학교 전자공학과 (석사)
- 1998년 2월 : 경북대학교 전자공학과 (박사)
- 1998년 3월 ~ 2007년 2월 : 나사렛대학교 정보통신학과 부교수
- 2007년 3월 ~ 현재 : 호서대학교 컴퓨터공학부 교수
- 2013년 1월 ~ 현재 : 한국정보보호학회 상임부회장
- 2009년 1월 ~ 현재 : 한국산학기술학회 이사

〈관심분야〉
암호학, 네트워크 보안, 부채널 공격, 머신러닝