Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.2, Apr. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.2.179

참조 테이블 기반 스칼라 곱 알고리즘에 대한 충돌 특성을 이용한 향상된 수평상관분석*

박 동 준,[1†] 이 상 엽,[1] 조 성 민,[2] 김 희 석,[3‡] 홍 석 희[3]
[1,3]고려대학교 (대학원생, 교수), [2]크립트앤텍 (연구원)

An Improved Horizontal Correlation Analysis Using Collision Characteristics on Lookup Table Based Scalar Multiplication Algorithms*

Dongjun Park,[1†] Sangyub Lee,[1] Sungmin Cho,[2] HeeSeok Kim,[3‡] Seokhie Hong[3]
[1,3]Korea University (Graduate student, Professor), [2]Crypt and Tech (Researcher)

요 약

FBC(Fixed-Base Comb)는 사전계산된 참조 테이블을 활용하여 ECDSA(Elliptic Curve Digital Signature Algorithm) 서명 생성의 핵심 연산인 스칼라 곱을 효율적으로 연산하는 방법이다. FBC는 비밀정보에 의존하여 테이블을 참조하고 테이블의 값은 공개되어 있기 때문에 단일파형 부채널 공격 기법인 수평상관분석(HCA, Horizontal Correlation Analysis)에 의해 그 비밀정보가 드러날 수 있다. 그러나 HCA는 통계 분석의 일종으로 하나의 스칼라 곱 파형으로부터 충분한 수의 단위 연산 파형을 얻을 수 있어야만 공격에 성공할 수 있다. ECDSA 서명 생성에 쓰이는 스칼라 곱의 경우 RSA 거듭제곱에 비해 HCA에 이용 가능한 단위 연산 파형의 수가 현저히 적어 공격에 실패할 수 있다. 본 논문에서는 FBC와 같은 참조 테이블 기반 스칼라 곱에 대하여 향상된 HCA를 제안한다. 제안하는 기법은 충돌 분석으로 중간값이 같은 단위 연산 파형을 식별함으로써 공격에 이용되는 단위 연산 파형의 수를 증가시켜 HCA의 공격 성능을 향상시킨다. 제안하는 기법은 사용된 타원곡선 파라미터의 보안 강도가 높을수록 공격 성능이 향상하는 특징이 있다.

ABSTRACT

The FBC(Fixed-Base Comb) is a method to efficiently operate scalar multiplication, a core operation for signature generations of the ECDSA(Elliptic Curve Digital Signature Algorithm), utilizing precomputed lookup tables. Since the FBC refers to the table depending on the secret information and the values of the table are publicly known, an adversary can perform HCA(Horizontal Correlation Analysis), one of the single trace side channel attacks, to reveal the secret. However, HCA is a statistical analysis that requires a sufficient number of unit operation traces extracted from one scalar multiplication trace for a successful attack. In the case of the scalar multiplication for signature generations of ECDSA, the number of unit operation traces available for HCA is significantly fewer than the case of the RSA exponentiation, possibly resulting in an unsuccessful attack. In this paper, we propose an improved HCA on lookup table based scalar multiplication algorithms such as FBC. The proposed attack improves HCA by increasing the number of unit operation traces by determining such traces for the same intermediate value through collision analysis. The performance of the proposed attack increases as more secure elliptic curve parameters are used.

Keywords: Scalar Multiplication, Side Channel Attack, Single Trace Attack, Correlation Analysis, Collision Analysis

Received(03. 02. 2020), Accepted(03. 12. 2020)
* 이 성과는 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.NRF-2019R1A2C2088960)
† 주저자, djpark@korea.ac.kr
‡ 교신저자, 80khs@korea.ac.kr(Corresponding author)

I. 서 론

스칼라 곱은 ECDSA(Elliptic Curve Digital Signature Algorithm)[1]에서 서명 생성의 효율성과 안전성에 가장 큰 영향을 미치는 핵심 연산이다. ECDSA 서명 생성에서의 스칼라 곱은 고정된 점으로 계산을 수행하므로 사전계산된 참조 테이블을 활용하면 효율적으로 계산할 수 있다. 대표적인 방법으로는 FBC(Fixed-Base Comb)[2]가 있으며, 이 방법은 OpenSSL[3], GnuPG[4], Bitcoin Core[5] 등의 암호 라이브러리에서 실제로 사용되고 있다.

암호 연산을 구현할 때 연산 효율성만큼이나 중요한 요소는 안전성이다. 암호가 수학적으로 안전하다고 하여도 암호 연산을 수행 중인 기기의 전력 소비량[6]이나 전자기파[7] 등 부채널 정보를 통해 비밀정보가 노출될 수 있다. 이러한 공격을 부채널 공격이라 하며 교통카드[8], 키보드[9] 등이 공격당한 사례가 있다. 따라서 모든 암호 연산은 부채널 공격에 대해 안전해야 한다. 특히 ECDSA 서명 생성의 스칼라 곱은 일회성 비밀정보로 계산을 수행하므로 단일파형 부채널 공격에 대한 안전성이 요구된다.

공개키 암호에 대한 단일파형 부채널 공격은 단순전력분석(SPA, Simple Power Analysis)[10], 수평상관분석(HCA, Horizontal Correlation Analysis)[11], 단일파형충돌분석(STCA, Single Trace Collision Analysis)[12] 등 다양한 기법이 있다. 이 중 HCA는 하나의 파형을 분해하여 여러 개의 단위 연산 파형을 얻은 뒤 상관전력분석(CPA, Correlation Power Analysis)[6]을 통해 비밀정보를 알아내는 기법이다. 이 기법은 이용가능한 단위 연산 파형의 수가 많을수록 높은 공격성공률을 보인다. 대표적 공개키 암호인 RSA의 거듭제곱은 비밀정보에 대한 단위 곱셈의 수가 충분하여 HCA의 공격 성공률이 높다. 반면에 ECDSA의 스칼라 곱은 비밀정보에 대한 단위 곱셈의 수가 현저히 적어 HCA의 공격 성공률이 낮다. 예를 들어 128비트 보안 강도[1]인 RSA-3072와 ECDSA P-256을 비교해 보자. RSA-3072의 거듭제곱은 하나의 정수 곱셈이 9,216개의 32-bit 단위 곱셈으로 이루어져 있다. 반면에 ECDSA P-256의 스칼라 곱은 하나의 타원곡선 덧셈이 11개의 체 곱셈으로 구성되고 각 체 곱셈은 64개의 32-bit 단위 곱셈으로 이루어져 있다. 이 중에서 비밀정보와 관련 있는 체 곱셈만 고려하면 HCA에 이용 가능한 32-bit 단위 곱셈 파형의 수는 총 128개뿐이다.

본 논문에서는 참조 테이블 기반 스칼라 곱에 대한 향상된 HCA를 제안한다. 제안하는 기법은 스칼라 곱의 타원곡선 덧셈이 비밀정보에 의존하여 테이블을 참조한다는 특성을 이용한다. 이 기법은 먼저 STCA를 통해 동일한 비밀정보에 의한 타원곡선 덧셈 파형을 분류한 뒤, HCA를 통해 분류된 덧셈 파형에 연관된 비밀정보를 알아낸다. 타원곡선 파라미터의 보안 강도가 높을수록 STCA에 의해 분류되는 파형의 수가 많다. 따라서 제안하는 기법은 안전한 파라미터를 사용할수록 공격 성능이 향상한다.

본 논문에서는 참조 테이블 기반의 스칼라 곱 중 다양한 암호 라이브러리에서 실제로 사용되고 있는 FBC의 부채널 공격에 대한 안전성을 분석한다. 또한, 제안하는 기법으로 FBC를 공격하는 과정을 설명한다. 제안하는 기법의 공격 성능 검증을 위해 MCU(Micro Controller Unit)에서 동작하는 FBC에 대한 실제 공격을 수행하였다.

본 논문의 2장에서는 ECDSA 및 FBC에 대한 부채널 공격을 설명한다. 3장에서는 제안하는 기법을 기술한다. 4장에서는 공격의 실험 결과를 보인다. 마지막으로 5장에서는 결론을 맺는다.

II. 배경 지식

본 장에서는 ECDSA 서명 생성과 FBC 스칼라 곱 알고리즘에 관하여 소개하고 이에 대한 부채널 공격을 설명한다. 기술의 편의를 위해 기기의 전력 소비 파형을 이용한 부채널 공격을 중심으로 설명한다.

2.1 ECDSA 서명 생성에 대한 부채널 공격

Fig. 1은 ECDSA의 서명 생성[1, 2] 과정을 나타낸다. 일반적으로 공격자의 최종 목표는 서명 생성의 입력인 개인키 d를 알아내는 것이다. ECDSA

Alg 1. ECDSA Signature Generation
Input: Domain parameters (E, p, n, G, H), private key d, and message m.
Output: Signature (γ, σ) of given message m.
1. Select $k \in [1, n)$ uniformly at random.
2. $(x, y) \leftarrow kG$ over $E/\mathbb{F}_p$. ◁ Scalar Multiplication
3. $\gamma \leftarrow x \bmod n$.
4. If $\gamma = 0$: go to step 1.
5. $\sigma \leftarrow k^{-1}(H(m) + d\gamma) \bmod n$.
6. If $\sigma = 0$: go to step 1.
7. Return (γ, σ).

Fig. 1. ECDSA signature generation algorithm.

서명 생성에서 부채널 공격자의 공격 대상이 되는 부분은 다음과 같이 크게 두 군데이다.

첫 번째는 step 5의 $d\gamma$ 곱셈이다. d는 고정된 비밀 값이고 γ는 공개 채널로 전송되는 서명 값이기 때문에 CPA[6]를 통해 d를 알아낼 수 있다. 하지만 이 공격은 다수의 서명 생성 파형이 필요할 뿐만 아니라 $k^{-1}H(m)+k^{-1}d\gamma$의 순서로 계산함으로써 쉽게 대응할 수 있다.

두 번째는 step 2의 kG 스칼라 곱이다. 만약 공격자가 k를 알아낼 수 있다면 step 5의 관계식 $d\equiv(k\sigma-H(m))\gamma^{-1}$으로부터 d를 계산할 수 있다. 이때 k는 서명을 생성할 때마다 새로운 난수로 선택되므로 공격자는 하나의 서명 생성 파형만을 이용할 수 있다. 따라서 스칼라 곱에 대한 부채널 공격은 단일파형으로 수행 가능한 기법이 요구되며, 이러한 공격은 다수 파형을 이용하는 공격보다 위협적이다.

2.2 FBC에 대한 단일파형 부채널 공격

Fig. 2는 참조 테이블을 활용한 FBC[2]의 계산 과정을 나타낸다. 이 알고리즘은 l비트 길이의 스칼라 k와 점 G가 입력되면 $t-1$번의 타원곡선 두 배(이하 두 배)와 타원곡선 덧셈(이하 덧셈)을 반복 수행하여 kG를 출력한다. 이때 $t=\lceil l/w \rceil$ 이며 w는 윈도 크기이다. 점 G는 고정된 점이므로 테이블의 생성 과정(step 2)은 생략될 수 있다. 또한 G는 공개된 점이므로 공격자는 테이블의 값을 알 수 있다.

다음 소절에서는 스칼라 곱에 대한 단일파형 부채널 공격 기법인 SPA[10], HCA[11], STCA[12]에 대하여 FBC의 부채널 안전성을 분석한다.

Alg 2. Fixed-Base Comb Scalar Multiplication
Input: Base point G, scalar $k=(k_{l-1}\cdots k_1k_0)_2$, and window width w.
Output: $P=kG$.
1. Divide k into w bit strings each of the same length $t=\lceil l/w \rceil$ so that $k=K^{w-1}\|\cdots\|K^1\|K^0$. Let K_i^j denote i-th bit of K^j and $K_i=(K_i^{w-1}\cdots K_i^1K_i^0)_2$.
2. { *Precomputation* }. For all bit strings $(b_{w-1}\cdots b_1b_0)_2$ of length w, compute $G[(b_{w-1}\cdots b_1b_0)_2]=b_{w-1}2^{(w-1)t}G+\cdots+b_12^tG+b_0G$.
3. $P\leftarrow G[K_{t-1}]$.
4. For i from $t-2$ down to 0:
4.1. $P\leftarrow 2P$. ◁ Point Doubling
4.2. $P\leftarrow P+G[K_i]$. ◁ Point Addition
5. Return P.

Fig. 2. FBC scalar multiplication algorithm.

2.2.1 SPA(Simple Power Analysis)

SPA[10]는 특정 연산이 입력된 비밀정보에 의존하여 선택적으로 수행된다는 사실을 이용해 비밀정보를 알아내는 기법이다. 예를 들면 이진 스칼라 곱에서는 두 배 후 스칼라의 비트가 1일 때만 덧셈이 수행되고 0이면 다음 두 배가 수행된다. Fig. 3은 이진 스칼라 곱의 전력 소비 파형에서 두 배(D)와 덧셈(A) 파형을 식별해 나타낸 그림이다. 만약 두 배 파형 뒤에 덧셈 파형이 존재한다면 해당 시점에서 스칼라의 비트는 1이고 존재하지 않는다면 0이다.

FBC에서는 $K_i=0$일 때를 제외하고 항상 덧셈(step 4.2)이 수행된다. 공격자는 SPA를 통해 덧셈의 발생 여부를 확인하더라도 참조 테이블의 어떤 점이 더해지는지 알 수 없다. 따라서 SPA만으로는 FBC의 스칼라를 완전하게 알아내기 어렵다.

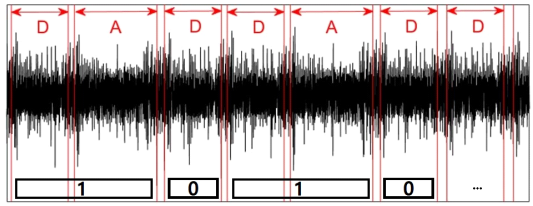


Fig. 3. SPA on the binary scalar multiplication.

2.2.2 HCA(Horizontal Correlation Analysis)

HCA[11]는 CPA에 기반하는 단일파형 부채널 공격 기법이다. 먼저, CPA[6]는 기기의 전력 소비량이 연산 입력값의 함수인 전력 소비 모델과 상관관계가 있다는 가정하에 입력값을 알아내는 기법이다. 공격자는 특정 전력 소비 모델을 가정하고, 수집된 다수의 전력 소비 파형과 각 파형의 입력을 추측해 얻은 전력 소비 모델 사이의 상관계수를 모든 가능한 입력에 대하여 계산한다. 특정 추측에서 구별될 정도로 큰 상관계수를 갖는 경우 해당 추측을 실제 연산의 입력값으로 판단함으로써 비밀정보를 알아낸다.

HCA는 스칼라 곱 파형을 다수의 단위 곱셈[1] 파형으로 분해한 후 CPA와 동일한 방법으로 비밀정보를 알아낸다. 스칼라 곱을 공격할 때 HCA가 유용한

1) 단위 곱셈은 소프트웨어가 긴 길이의 정수 곱셈(체 곱셈)을 여러 번에 나누어 처리할 때 행해지는 연산이다. 데이터 처리 단위를 W비트라 할 때 l비트 길이의 정수 곱셈은 일반적으로 $(l/W)^2$번의 단위 곱셈으로 처리된다.

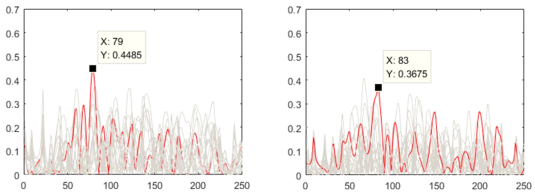


Fig. 4. Two results of HCA on the FBC.

상황으로는 특수한 타원곡선을 사용해 두 배와 덧셈의 연산식이 같거나[13], 두 배와 덧셈의 연산식이 같아지도록 내부에 더미 연산이 삽입된 경우[14] 등이 있다. 두 경우 모두 두 배와 덧셈을 시각적으로 구분할 수 없는 상황이지만 HCA를 통해 이를 구분함으로써 스칼라를 알아낼 수 있다. 이진 스칼라 곱에 더미 덧셈이 삽입된 경우[15]에도 더미 여부를 판단함으로써 스칼라를 비트 단위로 알아낼 수 있다.

FBC는 이론적으로 HCA에 대해 취약하지만, 현실적으로 이용 가능한 단위 곱셈 파형의 수가 적어 공격 성공률이 낮다. 수집된 전력 소비 파형은 잡음이 포함되어있고 공격자가 가정한 모델을 정확히 따르지 않기 때문이다. Fig. 4의 좌측은 두 개의 덧셈을 128개의 단위 곱셈 파형으로 분해해 수행한 HCA 결과이다. 올바른 추측으로 계산한 상관계수 값(적색)은 틀린 추측으로 계산한 상관계수 값(회색)과 근소한 차이만을 보인다. Fig. 4의 우측은 같은 환경에서 수집된 다른 두 개의 덧셈으로 수행한 HCA 결과이며 공격 실패를 보여주는 사례이다. 이 그림에서는 올바른 추측으로 계산한 상관계수 값이 오히려 틀린 추측으로 계산한 상관계수 값보다 낮다.

2.2.3 STCA(Single Trace Collision Analysis)

STCA[12]는 단일파형 내에서 같은 값으로 같은 명령어를 처리하는, 이른바 충돌하는 두 구간의 전력 소비량이 서로 상관관계가 있다는 가정하에 두 연산의 입력값 일치 여부를 판단하는 기법이다. 반복되는 특정 연산에 관한 두 개의 전력 소비 파형이 큰 상관계수를 갖는 경우 두 연산의 입력값이 같다고 판단한다. 공격 대상 알고리즘에 충돌 여부로부터 비밀정보를 확정할 수 있는 특성이 존재한다면 STCA로 비밀정보를 알아낼 수 있다[12]. 더미 덧셈이 삽입된 이진 스칼라 곱[15], 몽고메리 스칼라 곱[16] 등은 이러한 특성이 존재해 STCA에 대해 취약하다.

FBC는 충돌 여부로부터 비밀정보를 확정할 수 있는 특성이 존재하는지 아직 밝혀지지 않았다. 단지 STCA를 통해 입력값이 같은 덧셈끼리 분류할 수 있을 뿐이다. 모든 덧셈을 입력값에 따라 분류하더라도 그 값을 추측하는 경우의 수는 $2^w!$이다. 이는 w가 증가함에 따라 매우 빠르게 증가하여 $w=4$일 때 2^{44} 정도의 값을 갖는다. 따라서 STCA만으로는 FBC의 스칼라를 완전하게 알아내기 어렵다.

III. 제안하는 공격 기법

제안하는 공격 기법의 목표는 ECDSA 서명에 쓰인 개인키 d를 계산하기 위해 스칼라 곱으로부터 k를 알아내는 것이다. 공격자는 서명 생성 시 사용된 스칼라 곱이 FBC로 구현되어있다는 최소한의 지식만으로 공격을 수행할 수 있다. 공격에 필요한 데이터는 k와 G로 스칼라 곱을 계산하는 시점의 전력 소비 파형이다. 필요한 파형의 수는 하나이며 테이블을 생성하는 시점의 파형은 공격에 필요하지 않다.

제안하는 기법은 세 단계로 구성된다. 먼저 파형 분해 단계에서는 하나의 스칼라 곱 파형을 여러 개의 단위 곱셈 파형으로 분해한다. 충돌 분석 단계에서는 분해된 곱셈 파형들을 충돌 여부에 따라 분류한다. 마지막으로 상관 분석 단계에서는 HCA와 동일한 방법으로 스칼라 k를 알아낸다. 공격자는 스칼라를 알아낸 뒤 2.1절에서 설명한 바와 같이 서명에 쓰인 개인키를 계산함으로써 공격 목표를 달성할 수 있다.

3.1 파형 분해 단계(Decomposition Stage)

파형 분해 단계는 하나의 스칼라 곱 파형을 여러 개의 단위 곱셈 파형으로 분해하는 전처리 단계이다.

FBC의 파형은 Fig. 2와 같이 $t-1$개의 두 배와 덧셈으로 구성된다. i번째 덧셈은 Fig. 5와 같이 11개의 체 곱셈으로 구성된다[2]. 이 중 $Q=G[K_i]$와 관련 있는 두 개의 체 곱셈(step 3, step 4) 파형만이 공격에 이용된다. 이 두 개의 체 곱셈 파형을 분해하여 총 $2(l/W)^2$개의 단위 곱셈 파형 $T_i[0]$, …, $T_i[2(l/W)^2-1]$을 얻을 수 있다. Fig. 6은 각 단위 곱셈 파형의 샘플 수를 m이라 할 때, 두 개의 체 곱셈 파형을 분해해 단위 곱셈 파형 집단 $T_i \in \mathbb{R}^{2(l/W)^2 \times m}$을 얻는 과정을 묘사한 그림이다.

Alg 3. Point Addition in Affine-Jacobian Coordinates

Input: Points $P=(X_1:Y_1:Z_1)$ in Jacobian coordinates and $Q=(x_2,y_2)$ in affine coordinates on $E/K_{p_i}: y^2=x^3-3x+b$.

Output: $P+Q=(X_3:Y_3:Z_3)$ in Jacobian coordinates.

1. $T_1 \leftarrow Z_1^2$.
2. $T_2 \leftarrow T_1 Z_1$.
3. $T_1 \leftarrow T_1 x_2$. ◁ Field Multiplication Related to Q
4. $T_2 \leftarrow T_2 y_2$. ◁ Field Multiplication Related to Q
5. $T_1 \leftarrow T_1 - X_1$.
6. $T_2 \leftarrow T_2 - Y_1$.
7. $Z_3 \leftarrow Z_1 T_1$.
8. $T_3 \leftarrow T_1^2$.
9. $T_4 \leftarrow T_3 T_1$.
10. $T_3 \leftarrow T_3 X_1$.
11. $T_1 \leftarrow 2T_3$.
12. $X_3 \leftarrow T_2^2$.
13. $X_3 \leftarrow X_3 - T_1$.
14. $X_3 \leftarrow X_3 - T_4$.
15. $T_3 \leftarrow T_3 - X_3$.
16. $T_3 \leftarrow T_3 T_2$.
17. $T_4 \leftarrow T_4 Y_1$.
18. $Y_3 \leftarrow T_3 - T_4$.
19. Return $(X_3:Y_3:Z_3)$.

Fig. 5. Elliptic curve point addition algorithm in affine-Jacobian mixed coordinates.

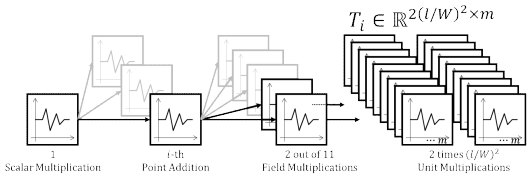


Fig. 6. A bunch of unit multiplication traces decomposed from a scalar multiplication trace.

3.2 충돌 분석 단계(Collision Analysis Stage)

충돌 분석 단계는 제안하는 기법의 핵심으로 충돌 분석을 통해 기존 HCA의 공격 성능을 향상시킨다.

먼저, FBC의 파형에서 충돌하는 덧셈들을 찾는다. 2^w개의 점이 저장된 참조 테이블을 $t-1$번 호출할 경우 한 점당 평균 호출 횟수는 $(t-1)/2^w$이다. Table 1은 NIST 타원곡선 $E/\mathbb{F}_{p_i}$[1]에 대하여 한 점당 평균 호출 횟수를 계산한 표이다. 최악의 경우인 p_{192}와 $w=6$일 때의 한 점당 평균 호출 횟수는 0.48이지만, 충돌이 적어도 한 번 발생할 확률은 $1-\left(\frac{64}{64}\frac{63}{64}\cdots\frac{34}{64}\right)=0.99985$이므로 높은 확률로 충돌 분석 단계를 통한 성능 향상 효과를 볼 수 있다.

다음으로, 충돌하는 덧셈들을 이용해 HCA의 공격 성능을 향상시킨다. 만약 전력 소비 파형의 잡음이 특정 확률 분포를 따른다면 평균 파형의 잡음은

Table 1. The average number of calls per one point. The probability that collision occurs is approximately 1 even in the worst case.

	$w=2$	$w=3$	$w=4$	$w=5$	$w=6$
p_{192}	23.75	7.88	2.94	1.17	0.48
p_{224}	27.75	9.21	3.44	1.37	0.57
p_{256}	31.75	10.54	3.94	1.57	0.65
p_{384}	47.75	15.88	5.94	2.37	0.98
p_{521}	64.88	21.58	8.08	3.23	1.34

분산이 줄고 기댓값에 수렴하게 된다. 따라서 충돌하는 파형들의 평균 파형을 이용하면 원본 파형을 이용했을 때보다 HCA의 공격 성능이 향상한다.

알고리즘 2의 i번째와 j번째 덧셈(step 4.2)이 충돌하는지 판단하는 지표로는 ST(Squared Pairwise t-differences)[17]를 사용한다. ST는 두 파형 집단의 분산과 개수를 고려한 평균적 차이를 시점별로 계산한 수치이다. 두 단위 곱셈 파형 집단 T_i와 T_j에 대하여, 특정 시점에서 T_i의 평균을 μ_i, 분산을 σ_i, 개수를 n_i라 할 때 ST는 다음과 같다.

$$ST_{i,j}=\left(\frac{\mu_i-\mu_j}{\sqrt{\frac{\sigma_i}{n_i}+\frac{\sigma_j}{n_j}}}\right)^2 \quad (1)$$

두 파형 집단의 모든 시점에서 계산한 ST를 전부 더한 값을 SOST(Sum of Squared Pairwise t-distribution)라 한다. SOST가 설정된 문턱 값(threshold) 이하일 때 두 단위 곱셈 파형 집단은 충분히 유사하여 해당 덧셈이 서로 충돌한 것으로 판단한다. 이때 문턱 값은 충돌 확률을 고려해 SOST의 가중평균으로 설정한다. 충돌이 발생했을 때와 하지 않았을 때의 SOST를 각각 a, b라 하면 이상적인 문턱 값은 $((2^w-1)a+b)/2^w$이다. 하지만 공격자는 충돌 여부를 알지 못하므로 SOST의 최솟값과 최댓값을 각각 a, b로 하여 문턱 값을 설정한다.

알고리즘 2의 덧셈(step 4.2)에서 충돌이 발생한 i끼리 묶은 집합을 $\mathbb{I}_0$, …, $\mathbb{I}_{2^w-1}$라 하자. 이때 아래 첨자는 순서대로 매긴 일련번호일 뿐 실제로 참조한 테이블의 인덱스와는 관련이 없다. 각 집합은 Table 1과 같이 평균적으로 $(t-1)/2^w$개의 반복자(iterator)를 원소로 갖는다. 같은 집합에 속하는 덧셈들의 평균 파형은 원본 파형보다 잡음이 적으므

로 상관 분석 단계의 성공률을 증가시킨다.

3.3 상관 분석 단계(Correlation Analysis Stage)

상관 분석 단계에서는 특정 집합 $\mathbb{I}_*$의 평균 파형을 이용하여 해당 연산이 호출한 참조 테이블의 인덱스이자 스칼라의 일부인 K_*를 알아낸다.

첫 번째 집합 $\mathbb{I}_0$에 속하는 모든 덧셈의 입력값은 테이블에 저장된 2^w개의 점 $G[0]$, …, $G[2^w-1]$ 중 하나이다. 이때 G는 파라미터로서 공개된 점이므로 공격자는 테이블에 저장된 모든 값을 알 수 있다.

집합 $\mathbb{I}_0$의 입력이 $G[guess]$라고 추측했을 때, 전력 소비 모델 L을 가정하여 얻는 이론적 전력 소비량은 $X=L(G[guess])$이다. $\mathbb{I}_0$의 평균 덧셈 파형을 구성하는 단위 곱셈 파형을 $Y=\overline{T_{i\in\mathbb{I}_0}}$라 할 때, X와 Y의 피어슨 상관계수 $\rho_{guess,0}$는 다음과 같다.

$$\rho_{guess,0}=\frac{Cov(X,Y)}{\sqrt{Var(X)}\sqrt{Var(Y)}} \quad (2)$$

모든 $0\leqq guess<2^w$에 대하여 $\rho_{guess,0}$가 가장 클 때의 $guess$를 $\mathbb{I}_0$의 덧셈들이 호출한 참조 테이블의 인덱스이자 스칼라의 일부인 K_*라고 판단한다.

위와 같이 K를 w비트 단위로 알아내는 과정을 $\mathbb{I}_{2^w-1}$까지 2^w번 반복한다. K를 완전하게 알아낸 후에는 Fig. 2의 step 1로부터 k를 계산할 수 있다.

IV. 실험 결과

본 논문에서는 NIST가 권고하는 secp256r1[1] 파라미터로 실험을 진행하였다. 공격 대상 알고리즘은 Fig. 2의 FBC이며 윈도 크기는 $w=4$이다. 참조 테이블을 구성하는 $2^w=16$개의 점을 사전계산해 두어 테이블 생성 과정(step 2)은 생략하였다. 공격 대상 기기는 ARM Cortex-M4 프로세서를 탑재한 MCU이다. 프로세서의 동작 주파수는 7.37MHz이고 데이터 처리 단위는 $W=32$비트이다. 전력 측정에 사용된 오실로스코프는 LeCroy HDO6104A로서 12비트의 해상도와 2GHz의 대역폭을 갖는다.

4.1 파형 분해 단계(Decomposition Stage)

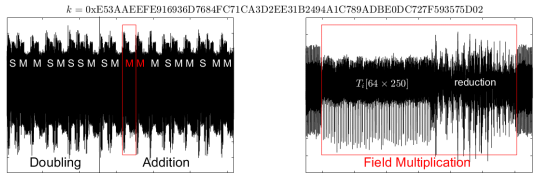


Fig. 7. Decomposed traces. The letter S and M stand for field squaring and field multiplication.

Fig. 7은 스칼라 $k=0\text{x}E53A\cdots$가 입력되었을 때 프로세서의 전력 소비량을 50MS/s의 샘플링레이트로 측정한 파형의 일부이다. 이 스칼라는 여러 번의 난수 생성기 결과 중 0을 더하는 일이 없도록 특수하게 선택된 값이다. 그림의 좌측은 스칼라 곱 파형에서 나타나는 $t-1=63$개의 두 배와 덧셈 파형 중 한 쌍을 확대한 모습이다. 그림의 우측은 좌측의 덧셈 파형에서 상자 안에 있는 하나의 체 곱셈을 확대한 모습으로 64개의 단위 곱셈 파형이 각각 250개의 샘플로 이루어진 것을 보여준다.

4.2 충돌 분석 단계(Collision Analysis Stage)

Fig. 8은 좌측부터 차례로 $i=62$번째 파형과, $j=61$, 43, 42번째 파형으로 계산한 ST를 나타낸 그래프이다. $ST_{62,61}$과 $ST_{62,43}$은 전체적으로 작은 값을 갖지만 $ST_{62,42}$는 큰 정점이 나타난 것을 확인할 수 있다. 시각적으로도 62번째와 61, 43번째 덧셈은 서로 같은 참조 테이블을 호출한 것으로 판단할 수 있지만, 객관적이고 정확한 판단을 위해서는 SOST가 문턱 값 이하인지를 확인해야 한다.

충돌 여부에 따라 모든 i를 집합 $\mathbb{I}_0$, …, $\mathbb{I}_{15}$ 중 하나로 분류한다. 분류를 마친 후에는 같은 집합에 속하는 덧셈들의 평균 파형을 얻을 수 있다.

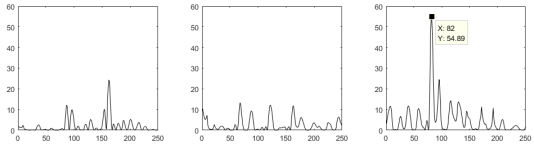


Fig. 8. ST values $ST_{62,61}$, $ST_{62,43}$, and $ST_{62,42}$ in order from the left.

4.3 상관 분석 단계(Correlation Analysis Stage)

$\mathbb{I}_0$를 제외한 $\mathbb{I}_1$, …, $\mathbb{I}_{15}$의 평균 파형을 이루는 단

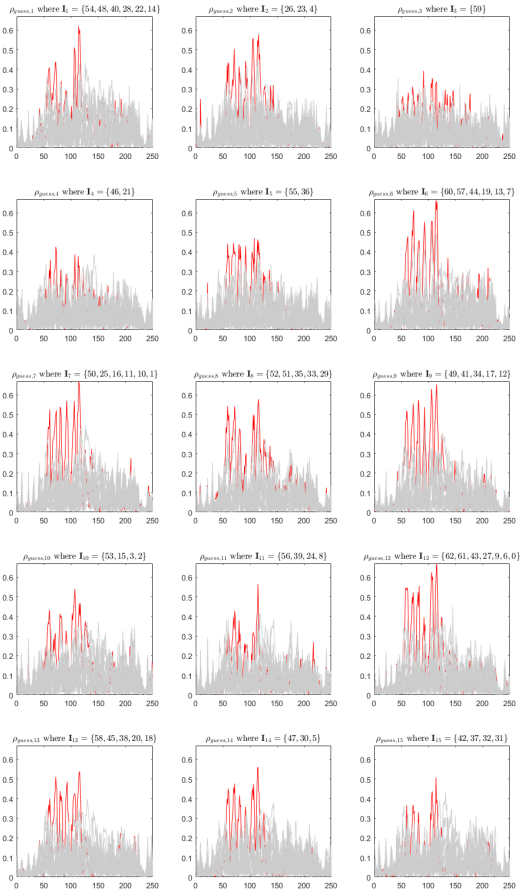


Fig. 9. The result of the proposed attack.

위 곱셈 파형으로 $\rho_{guess,1}$, …, $\rho_{guess,15}(0 \leq guess < 2^w)$를 계산하여 해당 집합의 덧셈들이 호출한 참조 테이블의 값을 추측한다. Fig. 9는 각 집합 $\mathbb{I}_*$의 아래 첨자를 $\rho_{guess,*}$가 가장 클 때의 $guess$로 변경하여 나타낸 상관계수 그래프이다. 그림에서 적색 그래프는 올바른 추측으로 계산한 상관계수를, 회색 그래프는 틀린 추측으로 계산한 상관계수를 의미한다. 충돌하는 덧셈이 많이 발견된 집합일수록 평균 파형으로 얻는 이점이 크므로 올바른 추측으로 계산한 상관계수가 도드라지게 나타난다.

HCA 단독으로는 덧셈이 호출하는 테이블의 값을 잘못 추측하는 경우가 존재했지만(Fig. 4의 우측), 제안하는 기법으로는 옳게 추측하였다. 제안하는 기법으로는 $i(<63)$번째 덧셈이 호출하는 테이블의 값을 전부 올바르게 추측하였다. 즉, 제안하는 기법은 대입으로 처리되는 최상위 워드 K_{63}을 제외하면 K를 완전하게 복원하는 데 성공하였다.

V. 결 론

FBC는 ECDSA 서명 생성의 핵심 연산인 스칼라 곱을 효율적으로 계산하기 위해 사전계산된 참조 테이블을 활용한다. FBC는 단일파형 부채널 공격 기법인 SPA, STCA에 대해 안전하나 HCA에 의해 비밀정보가 드러날 수 있다. 하지만 HCA는 하나의 스칼라 곱에서 이용 가능한 단위 곱셈 파형의 수가 적기 때문에 공격 성공률이 낮다는 한계가 있다.

본 논문에서는 중간값 충돌 분석을 통해 HCA의 공격 성능을 향상시키는 방법을 제안하였다. FBC와 같이 참조 테이블을 활용하는 스칼라 곱은 테이블의 동일한 값을 중복하여 호출한다는 특성이 있다. 제안하는 기법은 하나의 스칼라 곱 파형 내에 존재하는 덧셈들을 입력값에 따라 분류함으로써 공격에 이용 가능한 파형의 수를 증가시킨다. 충돌 분석으로 찾아낸 파형들의 평균 파형은 원본보다 잡음 수준이 낮으므로 공격 성능을 향상시킬 수 있다.

의미있는 후속 연구 주제는 고사양의 상용 장비를 대상으로 성공적인 공격 결과를 도출하는 것이다. 고사양 기기는 충분한 자원을 바탕으로 작동하므로 프로세서의 동작 주파수가 높으며 백그라운드 프로세스가 많다. 이는 수집된 파형의 잡음 수준이 높아지는 결과를 초래한다. 이러한 이유로 고사양 기기를 대상으로 하는 부채널 공격은 어려운 것으로 알려져 있다. 본 논문의 연구 결과는 하나의 파형만을 이용한다는 실용적인 공격자 가정에서도 파형의 잡음 수준을 낮출 수 있으므로 고사양 기기 대상 부채널 공격 연구의 밑바탕이 될 수 있다.

References

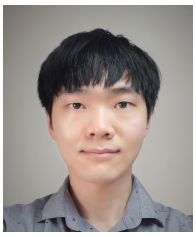
[1] National Institute of Standards and Technology, "Digital Signature Standard (DSS)," FIPS 186-4, July 2013.

[2] D. Hankerson, A. Menezes and S. Vanstone, Guide to elliptic curve cryptography, Springer, New York, pp. 75-186, 2004.

[3] OpenSSL, "openssl software library" https://www.openssl.org/

[4] GnuPG, "gnupg software library" https://gnupg.org/
[5] Bitcoin Core, "bitcoin core software library" https://bitcoin.org/
[6] E. Brier, C. Clavier, F. Olivier, "Correlation power analysis with a leakage model," Cryptographic Hardware and Embedded Systems - CHES 2004, LNCS 3156, pp. 16-29, Aug. 2004.
[7] K. Gandolfi, C. Mourtel, F. Olivier, "Electromagnetic analysis: concrete results," Cryptographic Hardware and Embedded Systems - CHES 2001, LNCS 2162, pp. 251-261, May. 2001.
[8] T. Kim, T. Kim, S. Hong, "Breaking Korea transit card with side-channel attack - Unauthorized recharging," Blackhat Asia, Mar. 2017
[9] K. Kim, T. Kim, T. Kim, S. Ryu, "AES wireless keyboard - template attack for Eavesdropping," Blackhat Asia, Mar. 2018.
[10] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis," Advances in Cryptology - CRYPTO' 99, LNCS 1666, pp. 388-397, Aug. 1999.
[11] C. Clavier, B. Feix, G. Gagnerot, M. Roussellet, V. Verneuil, "Horizontal correlation analysis on exponentiation," Information and Communications Security, LNCS 6476, pp. 46-61, Dec. 2010.
[12] N. Hanley, H. Kim, M. Tunstall, "Exploiting collisions in addition chain-based exponentiation algorithms using a single trace," Topics in Cryptology - CT-RSA 2015, LNCS 9048, pp. 431-448, Apr. 2015.
[13] H.M. Edwards, "A normal form for elliptic curves," Bulletin of the American Mathematical Society, vol. 44, no. 3, pp. 393-422, Apr. 2007.
[14] A. Bauer, E. Jaulmes, E. Prouff, J.R. Reinhard, J. Wild, "Horizontal collision correlation attack on elliptic curves," Cryptography and Communications, vol. 7, no. 1, pp. 91-119, Mar. 2015.
[15] J.S. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," Cryptographic Hardware and Embedded Systems - CHES 1999, LNCS 1717, pp. 292-302, Aug. 1999.
[16] M. Joye, S.M. Yen, "The Montgomery powering ladder," Cryptographic Hardware and Embedded Systems - CHES 2002, LNCS 2523, pp. 291-302, Aug. 2002.
[17] B. Gierlichs, K. Lemker-Rust, C. Paar, "Templates vs. stochastic methods," Cryptographic Hardware and Embedded Systems - CHES 2006, LNCS 4249, pp. 15-29, Oct. 2006.

〈저 자 소 개〉



박 동 준 (Dongjun Park) 학생회원
2018년 8월: 세종대학교 정보보호학과 학사
2018년 9월~현재: 고려대학교 정보보호학과 석사과정
〈관심분야〉 부채널 공격

이 상 엽 (Sangyub Lee) 학생회원
2010년 8월: 고려대학교 전파통신공학과 학사
2015년 8월: 고려대학교 정보보호대학원 석사
2015년 9월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 부채널 공격

조 성 민 (Sungmin Cho) 정회원
2008년 2월: 광운대학교 수학과 학사
2011년 8월: 고려대학교 정보보호대학원 석사
2019년 2월: 고려대학교 정보보호대학원 박사
2016년 8월~현재: ㈜크립트앤텍 연구원
〈관심분야〉 부채널 공격, 공개키 암호 알고리즘, 암호구현

김 희 석 (HeeSeok Kim) 종신회원
2006년 2월: 연세대학교 수학과 학사
2008년 2월: 고려대학교 정보보호대학원 석사
2011년 8월: 고려대학교 정보보호대학원 박사
2011년 9월~2012년 12월: Bristol University 박사후연구원
2013년 2월~2016년 8월: 한국과학기술정보연구원(KISTI) 선임연구원
2015년 3월~2016년 8월: 과학기술연합대학원대학교(UST) 조교수
2016년 9월~현재: 고려대학교 과학기술대학 사이버보안전공 부교수
〈관심분야〉 부채널 공격, 암호시스템 안전성 분석 및 고속구현, 암호칩 설계 기술, 보안관제, 네트워크 보안

홍 석 희 (Seokhie Hong) 종신회원
1995년 2월: 고려대학교 수학과 학사
1997년 2월: 고려대학교 수학과 석사
2001년 8월: 고려대학교 수학과 박사
1999년 8월~2004년 2월: ㈜시큐리티 테크놀로지 선임연구원
2003년 3월~2004년 2월: 고려대학교 정보보호기술연구센터 선임연구원
2004년 4월~2005년 2월: K.U. Leuven ESAT/SCD-COSIC 박사후연구원
2005년 3월~2013년 8월: 고려대학교 정보보호대학원 부교수
2013년 9월~현재: 고려대학교 정보보호대학원 정교수
〈관심분야〉 대칭키 및 공개키 암호 알고리즘, 부채널 공격 및 대응기법, 디지털 포렌식