Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.5, Oct. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.5.1079

부채널 분석에 안전한 하드웨어 이진 스칼라 곱셈 알고리즘에 대한 단일 파형 비밀 키 비트 종속 공격*

심 보 연,[1†] 강 준 기,[2] 한 동 국[1‡]
[1]국민대학교, [2]ETRI 부설 국가보안기술연구소

Key Bit-dependent Attack on Side-Channel Analysis-Resistant Hardware Binary Scalar Multiplication Algorithm using a Single-Trace*

Bo-Yeon Sim,[1†] Junki Kang,[2] Dong-Guk Han[1‡]
[1]Kookmin University, [2]The Affiliated Institute of ETRI

요 약

타원 곡선 암호 시스템의 주요 연산이 스칼라 곱셈 알고리즘[5]은 부채널 분석에 취약함이 보고되어 왔다. 특히 알고리즘이 수행되는 동안 소비되는 전력 패턴 및 방출되는 전자파 패턴을 활용하는 부채널 분석에 취약하다. 이에 다양한 대응 기법이 연구되어 왔으나 데이터 종속 분기 유형, 중간 값에 따른 통계 특성 또는 데이터 간의 상호 관계 기반 공격에 대한 대응 기법 등 주 연산에 대한 대응 기법만 연구되어 왔을 뿐 비밀 키 비트 확인 단계에 대한 대응 기법은 연구되지 않았다. 이에 본 논문에서는 하드웨어로 구현된 이진 스칼라 곱셈 알고리즘에 대한 단일 파형 비밀 키 비트 종속 공격을 수행하여 전력 및 전자 파형을 이용하여 100% 성공률로 비밀 스칼라 비트를 찾을 수 있음을 보인다. 실험은 차분 전력 분석 대응 기법이 적용된 Montgomery-López-Dahab ladder 스칼라 곱셈 알고리즘[13]을 대상으로 한다. 정교한 사전 전처리가 필요하지 않고 단일 파형만으로도 공격이 가능한 강력한 공격으로 기존 대응 기법을 무력화 시킬 수 있다. 따라서 이에 대한 대응 기법을 제시하고 이를 적용해야 함을 시사한다.

ABSTRACT

Binary scalar multiplication which is the main operation of elliptic curve cryptography is vulnerable to the side-channel analysis. Especially, it is vulnerable to the side-channel analysis which uses power consumption and electromagnetic emission patterns. Thus, various countermeasures have been studied. However, they have focused on eliminating patterns of data dependent branches, statistical characteristic according to intermediate values, or the interrelationships between data. No countermeasure have been taken into account for the secure design of the key bit check phase, although the secret scalar bits are directly loaded during that phase. Therefore, in this paper, we demonstrate that we can extract secret scalar bits with 100% success rate using a single power or a single electromagnetic trace by performing key bit-dependent attack on hardware implementation of binary scalar multiplication algorithm. Experiments are focused on the Montgomery-López-Dahab ladder algorithm protected by scalar randomization. Our attack does not require sophisticated pre-processing and can defeat existing countermeasures using a single-trace. As a result, we propose a countermeasure and suggest that it should be applied.

Keywords: Side-Channel Analysis, Elliptic Curve Cryptography, Single-Trace Attack, Key Bit-dependent Attack, Countermeasure

Received(08. 16. 2018), Modified(10. 04. 2018), Accepted(10. 05. 2018)

* 본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.

† 주저자, qjdusls@kookmin.ac.kr
‡ 교신저자, christa@kookmin.ac.kr(Corresponding author)

I. 서 론

4차 산업 혁명을 이끄는 새로운 기술로 각광받고 있는 블록체인 및 FIDO(Fast Identity Online)는 ECDSA 알고리즘을 활용하여 사용자를 인증한다. 그러나 ECDSA의 주요 연산인 스칼라 곱셈 알고리즘[5]은 부채널 분석(SCA, Side-Channel Attack)에 취약하다.

부채널 분석은 1996년 Paul Kocher에 의해 최초로 제안되었으며, 보안 디바이스가 동작하는 동안 소모되는 전력 패턴이나 방출되는 전자파 패턴과 같은 부가적인 정보의 누출을 기반으로 하는 공격이다[20]. 따라서 수학적으로 안전성이 증명된 암호 알고리즘이라도, 구현 단계에서 고려되지 못한 부가적인 정보의 누출을 이용한 부채널 분석에 취약하다.

이에 스칼라 곱셈 알고리즘에 대한 다양한 부채널 분석이 제안되어 왔으며, 그 중 알고리즘이 동작하는 동안 소모되는 전력 패턴을 활용한 전력 분석 공격은 가장 강력한 공격 기법으로 알려져 있다. 방출되는 전자파 패턴을 활용하는 전자기 분석 공격은 전력 분석 공격 방법과 유사하며, 사용하는 부채널 정보의 차이가 존재한다. 따라서 본 논문에서는 전력 분석 공격을 기준으로 설명한다.

스칼라 곱셈 알고리즘이 전력 분석 공격에 대응할 수 있도록 다양한 부채널 대응 기법이 연구되어 왔으나, 주로 데이터 종속 분기 유형, 중간 값에 따른 통계 특성 또는 데이터 간의 상호 관계 기반 공격에 대한 대응 기법만 연구되어 왔을 뿐 비밀 키 비트 확인 단계에 대한 대응 기법의 연구는 이루어지지 않았다[6, 13-17, 22]. 비밀 키 비트 확인 단계에서는 비밀 키 비트 값이 추출되어 변수에 저장되기 때문에 취약점이 존재한다는 것이 밝혀지면 비밀 키가 노출될 수 있다.

이에 본 논문에서는 하드웨어로 구현된 이진 스칼라 곱셈 알고리즘에 대한 비밀 키 비트 종속 특성을 정의하고, 실제 이를 기반으로 공격을 수행하여 비밀 키를 찾을 수 있음을 보인다. 제안하는 비밀 키 비트 종속 공격은 단일 파형으로 공격이 가능하며, 중간 값에 대한 사전 정보가 필요하지 않다. 따라서 기존 대응기법을 무력화 시킬 수 있는 강력한 공격이다. 또한 높은 신호 대 잡음비(SNR, Signal-to-Noise Ratio)를 갖는 파형을 얻기 위한 정교한 사전 전처리가 필요하지 않다.

실험은 차분 전력 분석 대응 기법이 적용된 Montgomery-López-Dahab ladder 스칼라 곱셈 알고리즘[13]을 하드웨어로 구현한 것을 대상으로 한다. 비밀 키는 단순 전력 분석 및 K-평균 군집화 알고리즘을 이용하여 추출한다. 실험 결과 전력 및 전자파형을 이용하여 100%의 성공률로 비밀 키 비트를 찾을 수 있음을 보인다. 그리고 비밀 키 비트 종속 공격 대응 기법을 제시하고 이를 적용해야 함을 시사한다.

본 논문의 구성은 다음과 같다. 2장에서는 스칼라 곱셈 알고리즘에 대한 부채널 분석을 설명하고, 비밀 키 비트 확인 단계를 정의한다. 3장에서는 비밀 키 비트 종속 특성을 정의하고, 단일 파형 비밀 키 비트 종속 공격 방법을 설명한다. 그리고 4장에서는 본 논문에서 제시하는 단일 파형 비밀 키 비트 종속 공격 실험 결과를 보이고, 5장에서 대응기법을 제시한다. 마지막으로 6장에서 결론으로 본 논문을 마무리한다.

II. 사전 연구

2.1 스칼라 곱셈 알고리즘에 대한 부채널 분석

스칼라 곱셈 알고리즘에 대한 전력 분석 공격은 단순 전력 분석(SPA, Simple Power Analysis), 차분 전력 분석(DPA, Differential Power Analysis), 템플릿 공격(TA, Template Attack), 충돌 공격(CA, Collision Attack)으로 분류된다.

2.1.1 단순 전력 분석

단순 전력 분석[21]은 보안 디바이스내의 암호 알고리즘이 동작할 때 소비되는 전력의 패턴을 관찰하여 암호 알고리즘에 사용되는 비밀 키의 정보를 직접 분석하는 방법이다. 암호 알고리즘이 동작할 때 프로세서의 명령에 따라 서로 다른 전력 소비 패턴을 가지기 때문에, 이를 외부에서 관측하여 비밀 키 또는 순간 작동중인 명령어에 대한 정보를 추론하는 분석 방법이 주를 이룬다. 즉, 주로 데이터 종속 분기 패턴을 기반으로 하며, 하나 또는 소수의 파형으로 공격이 가능하다. 예를 들어 타원 곡선 위의 서로 같은 점을 더하는 두 배 연산은 항상 수행되고, 비밀 키 비트 값이 1일 때만 서로 다른 두 점을 더하는 덧셈 연산을 수행하는 이진 스칼라 곱셈 알고리즘의 경우, 두 배 연산과 덧셈 연산 패턴의 차이를 이용하여 비밀 키를 찾을 수 있다. 즉, 비밀 키 비트 값에 따라서 비규칙적인 연산을 수행하는 알고리즘은 단순 전력

Left to Right

Input : $P=(x,y)$ a point on $\boldsymbol{EC}$, an n-bit key $k=(k_{n-1},\cdots,k_0)_2$
Output : $Q=kP$

1: $R_0 \leftarrow \infty$, $R_1 \leftarrow P$
2: **for** $i=n-1$ down to 0 **do**
3: $\quad R_{1-k_i} \leftarrow R_{k_i}+R_{1-k_i}$
4: $\quad R_{k_i} \leftarrow 2R_{k_i}$
5: **end for**
6: **Return** R_0

Right to Left

Input : $P=(x,y)$ a point on $\boldsymbol{EC}$, an n-bit key $k=(k_{n-1},\cdots,k_0)_2$
Output : $Q=kP$

1: $R_0 \leftarrow \infty$, $R_1 \leftarrow P$, $R_2 \leftarrow P$
2: **for** $i=0$ up to $n-1$ **do**
3: $\quad R_{1-k_i} \leftarrow R_{1-k_i}+R_2$
4: $\quad R_2 \leftarrow R_0+R_1$
5: **end for**
6: **Return** R_0

Fig. 1. Examples of regular algorithms for binary scalar multiplication

분석에 취약하다. 따라서 이에 대응하기 위해 Fig.1.과 같이 비밀 키 비트 값에 상관없이 규칙적인(regular) 연산을 수행하는 이진 스칼라 곱셈 알고리즘이 제시되었다[16, 17, 22].

2.1.2 차분 전력 분석

차분 전력 분석[21]은 다수의 전력 신호를 통계적으로 분석해 비밀 키를 찾는 방법이다. 대표적으로 암호 알고리즘이 수행되는 동안 소비되는 전력 패턴이 연산되는 데이터 값에 의존한다는 사실에 근거한 데이터 비트 차분 전력 분석이 있다. 그리고 이와 유사하게 암호 알고리즘이 수행되는 동안 소비되는 전력 패턴이 연산 수행 시 데이터를 불러오거나 저장하는 레지스터의 주소 값에 의존한다는 사실에 근거한 주소 비트 차분 전력 분석이 있다. 단순 전력 분석 대응기법이 적용되어 있어도 차분 전력 분석에 취약하다. 따라서 이에 대응하기 위해 전력 소비 패턴과 비밀 키에 따라 나타나는 중간 값 사이의 연관성을 제거하거나 숨김으로써 차분 전력 분석에 대응하는 대응 기법이 제시되었다. 임의의 난수를 사용하여 암호 알고리즘이 수행되는 동안 발생 가능한 모든 중간 값을 감추는 랜덤화 기법이 대표적이다[6, 14, 15].

2.1.3 템플릿 공격 및 충돌 공격

템플릿 공격[8, 11]과 충돌 공격[2-3, 7, 9-10, 12, 18-19, 23-25]은 단순 전력 분석 및 차분 전력 분석에 안전하도록 설계된 암호 알고리즘일지라도 단일 파형을 이용하여 비밀 키 값을 찾을 수 있는 매우 강력한 공격 기법이다. 템플릿 공격은 프로파일링 공격으로 통계 모델링과 전력 분석을 결합한 공격 유형이다. 충돌 공격은 고차 차분 전력 분석의 일종으로 데이터 간의 상호 관계를 기반으로 하는 공격이다. 현재까지 이론적으로 완벽하게 템플릿 공격과 충돌 공격에 대응할 수 있는 대응 기법이 제시되지 않았다. 하지만 높은 신호 대 잡음비를 갖는 파형을 얻기 위한 디캡슐레이션(decapsulation), 지역화(localization), 다중 프로브(multi-probe), 주성분 분석(PCA, Principal Component Analysis) 등 정교한 사전 전처리가 필요하다는 단점이 있다.

2.2 비밀 키 비트 확인 단계

이진 스칼라 곱셈 알고리즘은 Fig.1.과 같이 비밀 스칼라 비트 k_i값에 따라 동작이 결정되는 반복 연산으로 구성되어 있다. 따라서 각 반복 연산 시작 시에는 k_i값이 무엇인지 확인하는 단계가 있다. 즉, n비트열 스칼라 $k=(k_{n-1},\cdots k_0)_2$ 로부터 i번째 비트인 k_i를 추출하여 해당 변수에 저장한다. 본 논문에서는 이 단계를 키 비트 확인 단계라고 정의한다.

III. 비밀 키 비트 종속 공격

3.1 비밀 키 비트 종속 특성

이진 스칼라 곱셈 알고리즘의 키 비트 확인 단계에서는 n비트열 스칼라 $k=(k_{n-1},\cdots k_0)_2$에서 i번째 비트인 k_i를 추출하여 해당 변수에 저장한다. 따라서 비밀 키 비트 확인 단계에서 소모되는 전력과 방출되는 전자파는 k_i값과 연관되어 있다. 특히 하드웨어로 구현된 암호 알고리즘의 경우, 전력 소비 모델(또는 전자파 방출 모델)이 주로 헤밍 디스턴스(HD, Ham

ming Distance) 정보에 의존한다. 따라서 비밀 키 비트 확인 단계에서 비밀 키 비트 종속 특성을 정리하면 다음과 같다[1].

정리1. 하드웨어로 구현된 이진 스칼라 곱셈 알고리즘의 키 비트 확인 단계에서 소비되는 전력과 방출되는 전자파는 k_{i+1}과 k_i의 헤밍 디스턴스 정보에 의존한다. 즉, 만약 $k_{i+1}=k_i$이면 $k_{i+1}\oplus k_i=0$과 연관된 전력 소비와 전자파 방출이 발생한다. 그리고 만약 $k_{i+1}\neq k_i$이면 $k_{i+1}\oplus k_i=1$과 연관된 전력 소비와 전자파 방출이 발생한다. $(0\le i\le n-2)$

3.2 규칙적인 이진 스칼라 곱셈 알고리즘 비밀 키 비트 종속 특성

이진 스칼라 곱셈 알고리즘에 대한 단순 전력 분석(또는 단순 전자파 분석)은 가장 기본적인 부채널 공격으로 대응 기법의 적용이 필수적이다. 따라서 Fig. 1.과 같이 k_i값에 상관없이 항상 동일한 연산을 수행하여 단순 전력 분석에 안전하게 설계된 규칙적인 스칼라 곱셈 알고리즘이 주로 사용된다. 하지만, 단계 3, 4연산 수행 시 참조되는 레지스터의 주솟값이 k_i 값에 따라 결정되며, 이 때 소모되는 전력과 방출되는 전자파는 참조되는 레지스터 주솟값과 연관되어 있다. 즉, k_i값에 종속된 전력이 소모되고 전자파가 방출된다.

특히 하드웨어로 구현된 암호 알고리즘의 경우, 연산이 병렬적으로 수행되기 때문에 비밀 키 비트 확인 단계에서 k_i값이 결정됨과 동시에 참조되는 레지스터의 주소가 결정된다. 따라서 비밀 키 비트 확인 단계에서 소모되는 전력과 방출되는 전자파는 k_i값뿐만 아니라 k_i값에 따라 참조되는 레지스터 주솟값과 연관된다. 그러므로 규칙적인 이진 스칼라 곱셈 알고리즘의 비밀 키 비트 확인 단계에서 비밀 키 비트 종속 특성을 정리하면 다음과 같다.

정리 2. 하드웨어로 구현된 스칼라 곱셈 알고리즘의 키 비트 확인 단계에서 소비되는 전력과 방출되는 전자파는 k_{i+1}과 k_i의 헤밍 디스턴스 정보뿐만 아니라 k_{i+1}과 k_i의 값에 따라 결정되는 레지스터 주솟값 $RegAddr_{k_{i+1}}$과 $RegAddr_{k_i}$의 헤밍 디스턴스 정보에도 의존한다. 즉, 만약 $k_{i+1}=k_i$이면 소비되는 전력과 방출되는 전자파는 $k_{i+1}\oplus k_i=0$, $RegAddr_{k_{i+1}}\oplus RegAddr_{k_i}=0$과 연관된다. 만약 $k_{i+1}\neq k_i$이면 $k_{i+1}\oplus k_i=1$, $RegAddr_{k_{i+1}}\oplus RegAddr_{k_i}\neq 0$과 연관된 전력 소비와 전자파가 방출된다. $(0\le i\le n-2)$

3.3 단일 파형 비밀 키 비트 종속 공격

본 논문에서는 차분 전력 분석 대응기법으로 중간값 랜덤화 기법이 적용된 규칙적인 이진 스칼라 곱셈 알고리즘을 대상으로 한다. 따라서 공격자는 단일 파형을 이용한 비밀 키 비트 종속 공격을 수행해야 한다고 가정한다. 더불어 공격자는 수집된 파형에서 각 반복 연산을 식별할 수 있다고 가정한다. 공격 단계는 다음 4단계로 구성되어 있다.

- **전처리**

첫째, 스칼라 곱셈 알고리즘이 1회 수행되는 동안 수집한 파형을 T라고 했을 때, 이를 각 반복 연산에 해당하는 하위 파형 O_i로 나눈다. $(0\le i\le n-1)$ 즉, T를 Fig. 2와 같이 n개의 하위 파형 $T=\{O_{n-1}\|O_{n-2}\|\cdots\|O_0\}$으로 나눈다. 그리고 n개 하위 파형의 정렬을 맞춘다.

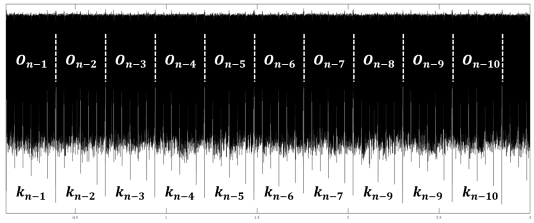


Fig. 2. Power consumption trace of 10 iterations

- **공격 지점(PoI, Points of Interest) 선택**

만약 공격 대상 장비와 동일한 장비를 사용할 수 있다면, 알려진 입력 값에 대한 파형을 수집한 후 n개의 하위 파형 O_i를 두 개의 그룹 G_1, G_2로 나눌 수 있다. 그리고 SOST(Sum Of Squared pairwise T-differences) 값을 계산하여 Fig. 3. (bottom)과 같이 SOST 값이 가장 높은 위치를 공격 지점 p_i로 쉽게 선택할 수 있다. 두 개의 그룹 G_1, G_2에 대한 SOST 값 계산 수식은 아래와 같다. $(0\le i\le n-1)$

$$SOST = \left(\frac{E[G_1] - E[G_2]}{\sqrt{\frac{\sigma_{G_1}^2}{n_{G_1}} + \frac{\sigma_{G_2}^2}{n_{G_2}}}} \right)^2 \quad (1)$$

(E는 평균, σ는 표준편차, n은 원소 개수)

만약 공격 대상 장비와 동일한 장비를 사용할 수 없다면, 대상 알고리즘이 어떻게 구현되어 있는지를 알아야 한다. 그리고 비밀 키 비트 연산이 수행되는 클록 위치를 공격 지점 p_i로 선택한다. 일반적으로 비밀 키 비트 확인 연산은 각 하위 파형 O_i의 시작 클록 인근에 위치한다. $(0 \le i \le n-1)$

- **두 집합으로 분류 및 비밀 키 추출**

단순 전력 분석 또는 K-평균 군집화(K-means Clustering), 퍼지 K-평균 군집화(fuzzy K-means Clustering), EM(Expectation Maximization) 등과 같은 군집 알고리즘[4]을 이용하여 n개의 하위 파형 O_i의 공격 지점 p_i를 두 개의 그룹 G_1, G_2로 나눈다. $(0 \le i \le n-1)$ G_1에 속한 p_i는 $k_{i+1} = k_i$일 때, 즉, 0과 연관된 누출이 발생하는 파형이고, G_2에 속한 p_i는 $k_{i+1} \neq k_i$일 때, 즉, 0이 아닌 값과 관련된 누출이 발생하는 파형이라고 가정한다. 그리고 비밀 키 k의 최상위 비트 값 k_{n-1}는 항상 1인 사실과 p_i가 속해있는 집합을 기준으로 k_i값을 찾을 수 있다. $(0 \le i \le n-2)$ 만약 G_1에 속한 p_i를 $k_{i+1} \neq k_i$, G_2에 속한 p_i를 $k_{i+1} = k_i$에 대한 파형이라고 가정할 때 앞서 찾은 비밀 키 비트열과 반전된 결과의 비트열을 얻을 수 있다. 즉, 후보 키는 총 2개로 입출력 값 확인을 통해 비밀 키를 찾을 수 있다.

정리 1과 2를 기반으로 본 논문에서 제시하는 하드웨어로 구현된 이진 스칼라 곱셈 알고리즘에 대한 비밀 키 종속 공격을 다음과 같이 정의한다.

정의1. 하나의 공격 지점(Points of Interest)을 이용하여 비밀 키 비트 종속 정보를 획득하는 것을 1차 비밀 키 비트 종속 공격이라 한다.

IV. 단일 파형을 이용한 비밀 키 비트 종속 공격 실험 결과

4.1 실험 환경

본 논문에서는 차분 전력 분석 대응기법으로 스칼라 랜덤화 기법이 적용된 Montgomery-López-Dahab ladder 스칼라 곱셈 알고리즘을 대상으로 한다. 따라서 공격자는 단일 파형을 이용한 공격을 수행해야 한다고 가정한다. 비밀 키 비트는 224비트이

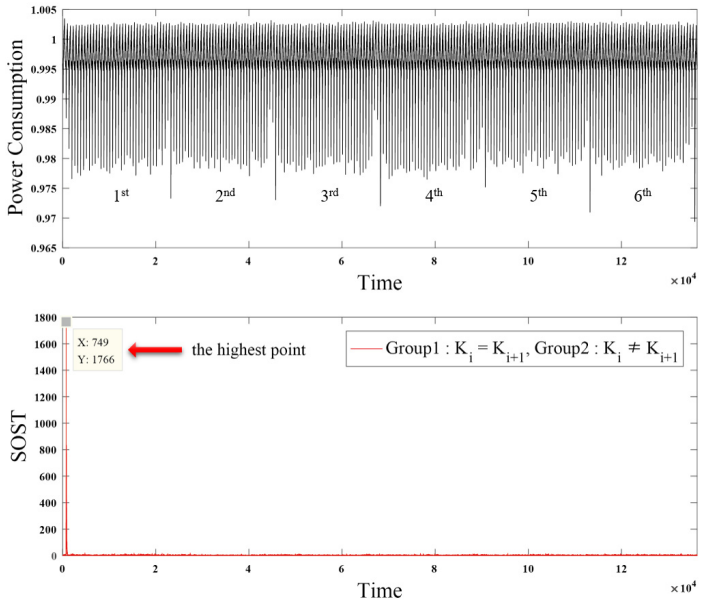


Fig. 3. One of the sub-traces(top) and SOST value between two sub-trace groups(bottom)

며, 부채널 분석 검증 보드로는 SASEBO-GII FPGA 보드를 이용하여 2.5 GS/s으로 전력 및 전자파형을 수집하였다. 전자파형 수집 시 사용한 프로브는 100 kHz~50 MHz 대역의 신호를 수집할 수 있는 Langer LF-R 400이다.

4.2 실험 결과

- **전처리**

Montgomery-López-Dahab ladder 스칼라 곱셈 알고리즘은 최상위 비트를 제외하고 반복 연산을 수행한다. 따라서 알고리즘이 1회 수행되는 동안 수집한 파형 T를 $n-1=223$개의 하위 파형 O_i로 분할한 후 정렬을 맞춘다. $(0 \le i \le 222)$ Fig. 3. (top)은 하나의 하위 파형을 나타낸다. 각 하위 파형은 6개의 유한체위에서의 곱셈 연산으로 구성되어 있다.

- **공격 지점(PoI, Points of Interest) 선택**

공격 대상 알고리즘은 각 하위 파형의 두 번째 클록에서 비밀 키 비트 확연 연산을 수행한다. 따라서 각 하위 파형의 두 번째 클록 파형을 공격 지점 p_i로 선택한다. 특징 2를 기반으로 하위 파형을 두 집합으로 나눠 SOST 값을 계산하면 Fig. 3. (bottom)과 같이 두 번째 클록에서 가장 높은 것을 확인할 수 있다. $(0 \le i \le 222)$

- **두 집합으로 분류 및 비밀 키 추출**

단순 전력 분석 또는 K-평균 군집화 알고리즘을 이용하여 223개 공격 지점 p_i를 두 개의 그룹 G_1, G_2로 나눈다. 전력파형의 경우 Fig. 4와 같이 육안으로 쉽게 구분이 가능한 정보량이 존재하였다. 따라서 단순 전력 분석을 통해 100%의 성공률로 비밀 스칼라 비트를 추출할 수 있었다.

전자파형의 경우 전력파형과 달리 노이즈의 영향으로 Fig.5와 같이 두 집합의 분포가 겹친다. 그러므로 단순 전력 분석을 통해 두 집합으로 완벽히 분류하는 것이 어렵다. 따라서 본 논문에서는 K-평균 군집화 알고리즘을 적용하여 두 집합으로 분류하였다. 노이즈를 제거하기 위한 전처리를 수행하지 않았음에도 하나의 전자파형을 이용하여 99.50%의 성공률로 비밀 스칼라 비트를 추출할 수 있었다.

전자파형의 신호 왜곡을 최소화하면서 노이즈를 제거하기 위해 75Ω 임피던스를 가지는 Mini-Circuit

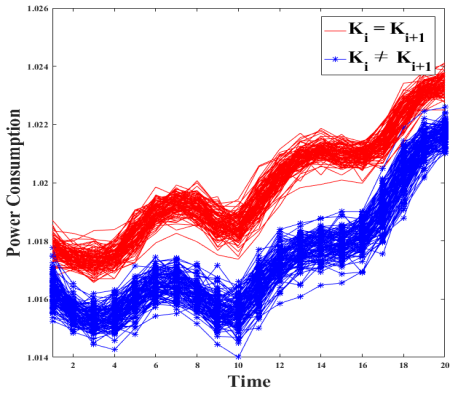


Fig. 4. Classification according to hamming distance between k_i and k_{i+1} (Power consumption trace)

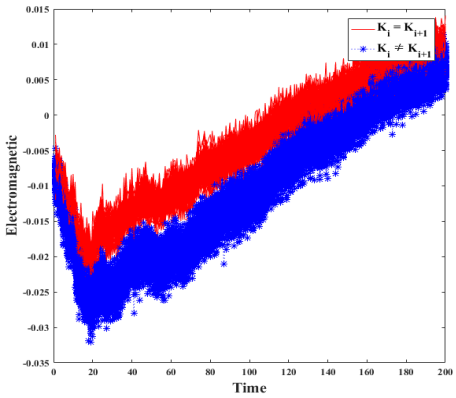


Fig. 5. Classification according to hamming distance between k_i and k_{i+1} (Electromagnetic trace, LF-R 400)

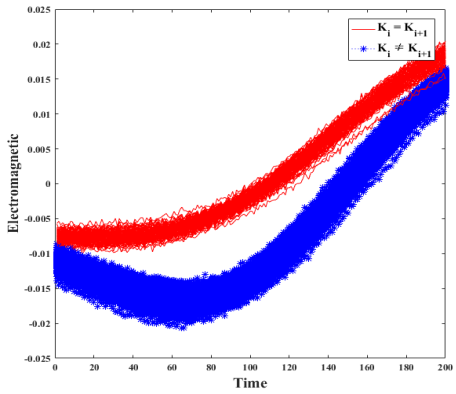


Fig. 6. Classification according to hamming distance between k_i and k_{i+1} (Electromagnetic trace, LF-R 400 with BLP-10.7-75+)

s 저역 통과 여파기(Low Pass Filter) BLP-10.7-75+를 사용하여 DC ~ 11 MHz 대역의 전자파형을 수집한 경우 Fig. 6과 같이 육안으로 쉽게 구분 가능한 정보량이 존재하였다. 따라서 단순 전력 분석을 통해 100%의 성공률로 비밀 스칼라 비트를 추출할 수 있었다.

V. 단일 파형을 이용한 비밀 키 비트 종속 공격 대응 기법

본 논문에서 제시하는 단일 파형을 이용한 비밀 키 비트 종속 공격 대응 기법으로 Fig. 7.과 같이 각 반복 연산에서 비밀 키 비트 확인 연산을 수행하기 전에 k_i 변수를 랜덤 값으로 초기화 하는 방법을 제안한다. 하나의 공격 지점에서 공격자가 획득할 수 있는 정보는 $k_i \oplus random\,bit$ 값으로 k_{i+1}와 k_i 사이의 연관성을 제거 가능하며, 실험에 따르면 Fig. 8.과 같이 $k_{i+1} \oplus k_i$ 값에 따른 두 집합으로 분류되지 않는다. 이는 하나의 파형 집합을 $k_{i+1} \oplus k_i = 0$, 다른 파형 집합을 $k_{i+1} \oplus k_i = 1$로 구분하여 비밀 키 비트를 추정할 경우 성공확률이 50%이며, 이는 비밀 스칼라 비트를 1/2의 확률로 랜덤하게 추정한 것과 동일하다. 따라서, 단일 파형을 이용한 1차 비밀 키 비트 종속 공격에 대응할 수 있다.

VI. 결 론

본 논문에서 제시하는 비밀 키 비트 종속 공격은

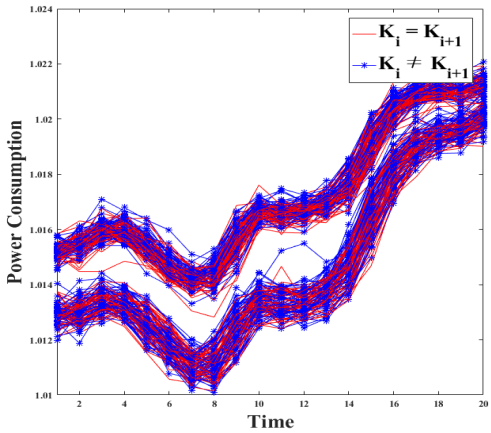


Fig. 8. Classification according to hamming distance between k_i and k_{i+1} (Power consumption trace, countermeasure)

단일 파형을 이용하여 공격이 가능하며, 사전 전처리 없이 전력파형의 경우 100%, 전자파형의 경우 99.50%의 성공률로 비밀 스칼라 비트를 추출할 수 있었다. 상용 저역 통과 여파기를 이용하여 수집한 전자파형의 경우에는 100%의 성공률로 비밀 스칼라 비트를 추출할 수 있었다. 즉, 하나의 전력 또는 전자파형을 이용하여 비밀 키 비트 종속 공격으로 100%의 성공률로 비밀 키 획득이 가능하다. 이는 기존의 부채널 대응기법을 무력화 시킬 수 있는 강력한 공격으로, 본 논문에서는 ECC 스칼라 곱셈 알고리즘에 초점을 맞추었지만 RSA 모듈러 지수승 알고리즘에도 적용이 가능하다. 따라서 대응 기법의 적용이 필수적임을 시사하며, 본 논문에서는 매 반복 연산 수행 전

ECC Scalar Multiplication (Initilized by random bit)

Input : $P = (x, y)$ a point on $E(\mathbb{F}_q)$, a n-bit scalar $k = (k_{n-1}, k_{n-2}, \cdots, k_0)_2$
Output : $Q = kP$

1: $regK[n-1:0] \leftarrow \{k_{n-1}, k_{n-2}, \cdots, k_0\}$
2: $R_0 \leftarrow \infty$, $R_1 \leftarrow P$
3: $k_i \leftarrow random\ bit$
4: **for** $i = n-1$ down to 0 **do**
5: $\quad k_i \leftarrow regK[i]$
6: $\quad R_{1-k_i} \leftarrow R_{k_i} + R_{1-k_i}$
7: $\quad R_{k_i} \leftarrow 2R_{k_i}$
8: $\quad k_i \leftarrow random\ bit$
9: **end for**

Fig. 7. Initialized by random bit

에 랜덤 값으로 초기화 하는 대응 기법을 제시하였다.

References

[1] B.-Y. Sim and D.-G. Han, "Key Bit-Dependent Attack on Protected PKC Using a Single Trace", ISPEC 2017, pp. 168-185, 2017.

[2] C. Clavier, B. Feix, G. Gagnerot, M. Roussellet, and V. Verneuil, "Horezontal correlation analysis on exponentiation", ICISC 2010, pp. 46-61, 2010.

[3] C.D. Walter, "Sliding windows succumbs to Big Mac attack", CHES 2001, pp. 286-299, 2001.

[4] C.M. Bischop, Pattern recognition and Machine Learning, Information Science and Statistics, Springer, New York, 2007.

[5] D. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography, Springer, ISBN 0-387-95273-X, 2003.

[6] D. May, H.L. Muller, and N.P. Smart, "Random register renaming to foil DPA", CHES 2001, pp. 28-38, 2001.

[7] G. Perin, L. Imbert, L. Torres, and P. Maurine, "Attacking randomized exponentiations using unsupervised learning", COSADE 2014, pp. 144-160, 2014.

[8] G. Perin and L. Chmielewski, "A Semi-parametric approach for side-channel attacks on protected RSA implemtations", CARDIS 2015, pp. 34-53, 2016.

[9] I. Diop, P.Y. Liardet, and P. Maurine, "Collision based attacks in practice", DSD 2015, pp. 367-374, 2015.

[10] I. Diop, M. Carbone, S. Ordas, Y. Linge, P.Y. Liardet, and P. Maurine, "Collision for estimating SCA measurement quality and related applications", CARDIS 2015, pp. 143-157, 2015.

[11] J. Heyszl, S. Mangard, B. Heinz, F. Stumpf, and G. Sigl, "Localized electromagnetic analysis of cryptographic implementations", CT-RSA 2012. pp. 231-244, 2012.

[12] J. Heyszl, A. Ibing, S. Mangard, F. De Santis, G. Sigl, "Clustering algorithms for non-profiled single-execution attacks on exponentiations", CARDIS 2013, pp. 79-93, 2014.

[13] J. López, and R. Dahab, "Fast multiplication on elliptic curves over $GF(2^m)$ without precomputation", CHES 1999, pp. 316-327, 1999.

[14] J.-S. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems", CHES 1999, pp. 292-302, 1999.

[15] M. Ciet, M. Joye, "(Virtually) free randomization techniques for elliptic curve cryptography", ICISC 2003, pp. 348-359, 2003.

[16] M. Joye, and S.-M. Yen, "The montgomery powering ladder", CHES 2002, pp. 291 - 302, 2003.

[17] M. Joye, "Highly regular right-to-left algorithms for scalar multiplication", CHES 2007, pp. 135-147, 2007.

[18] N. Hanley, H.S. Kim, and M. Tunstall, "Exploiting collisions in addition chain-based exponentiation algorithms using a single trace", CT-RSA 2015, pp. 431-448, 2015.

[19] N. Homma, A. Miyamoto, T. Aoki, A. Satoh, "Comparative power analysis of modular exponentiation algorithms", IEEE Trans, pp. 759-807, 2010.

[20] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems", CRYPTO 1996, pp. 104-113, 1996.

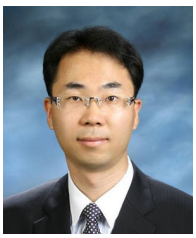
[21] P. Kocher, J. Jaffe, and B. Jun,

"Differential Power Analysis", CRYPTO 1999, pp. 388-397, 1999.
〔22〕 P. Montgomery, "Speeding the pollard and elliptic curve methods of factorization", Mathematics of Computation, pp. 243-264, 1987.
〔23〕 R. Specht, J. Heyszl, M. Kleinsteuber, and G. Sigl, "Improving non-profiled attacks on exponentiations based on clustering and extracting leakage from multi-channel high-resolution EM measurements", COSADE 2014, pp. 3-19, 2015.
〔24〕 T. Sugawara, D. Suzuki, and M. Saeki, "Internal collision attack on RSA under closed EM measurement", SCIS 2014.
〔25〕 T. Sugawar, D. Suzuki, and M. Saeki, "Tow operands of multipliers in side-channel attack", COSADE 2014, pp. 64-78, 2015.

〈저자소개〉

심 보 연 (Bo-Yeon Sim) 학생회원
2013년 2월: 국민대학교 수학과 졸업
2015년 2월: 국민대학교 금융정보보안학과 석사
2015년 3월~현재: 국민대학교 수학과 박사과정
〈관심분야〉 공개키 암호 시스템, 부채널 분석 및 대응기법 설계, 정보보호 기술

강 준 기 (Junki Kang) 정회원
2007년 2월: 충남대학교 전자전파정보통신전공 졸업
2012년 2월: 과학기술연합대학원대학교 박사
2012년 3월~현재: ETRI부설국가보안기술연구소
〈관심분야〉 정보보호



한 동 국 (Dong-Guk Han) 종신회원
1992년 2월: 고려대학교 수학과 졸업 (학사)
2002년 2월: 고려대학교 수학과 석사 (이학석사)
2005년 2월: 고려대학교 정보보호대학원 박사 (공학박사)
2004년 4월~2005년 4월: 일본 Kyushu Univ. 방문연구원
2006년 6월~2009년 2월: 한국전자통신연구원 정보보호연구단 선임연구원
2009년 3월~현재: 국민대학교 정보보안암호수학과 및 금융정보보안학과 교수
〈관심분야〉 공개키 암호시스템 안전성 분석 및 고속 구현, 부채널 분석 및 대응법 설계, IoT 정보보호 기술