Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.4, Aug. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.4.961

소비 전력 테이블 생성을 통한 부채널 분석의 성능 향상*

고 가 영,† 진 성 현, 김 한 빛, 김 희 석,‡ 홍 석 희
고려대학교

Improved Side Channel Analysis Using Power Consumption Table*

Gayeong Ko,† Sunghyun Jin, Hanbit Kim, HeeSeok Kim,‡ Seokhie Hong
Korea University

요 약

차분전력분석공격은 추측하는 비밀 정보 값에 따라 계산한 중간 값을 전력 소비 모델에 대입하여 전력 소비량을 구한 후 실제 발생한 전력 소비량과 함께 분석하여 암호화에 쓰인 비밀 정보 값을 복원한다. 이 때 흔히 쓰이는 전력 소비 모델로는 해밍 웨이트 모델이나 해밍 디스턴스 모델이 있으며 좀 더 정확한 전력 소비 모델을 구하기 위해서 전력 모델링 기법을 이용한다. 하지만 공격 타켓이 되는 장비가 가정한 전력 소비 모델과 상이한 경우 중간 값에 해당하는 전력 소비량을 옳게 반영하지 못하는 문제가 발생한다. 본 논문에서는 실제 공격 장비에서 측정한 소비 전력을 테이블 형태로 저장하여 전력 소비 모델로써 이용하는 방법을 제안한다. 제안하는 방법은 암호화 과정에서 활용 가능한 정보(평문, 암호문 등)가 쓰이는 시점에서의 소비 전력을 이용한다. 이 방법은 사전에 탬플릿 구성을 할 필요가 없으며 실제 공격 장비에서 측정한 소비 전력을 이용하기 때문에 해당 장비의 소비 전력 모델을 정확하게 반영한다. 제안하는 방법의 성능을 확인하기 위해 시뮬레이션과 실험을 진행하였으며 제안하는 방법의 성능이 기존의 전력 모델링 기법보다 부채널 공격 성능이 향상됨을 확인하였다.

ABSTRACT

The differential power analysis calculates the intermediate value related to sensitive information and substitute into the power model to obtain (hypothesized) power consumption. After analyzing the calculated power consumption and measuring power consumption, the secret information value can be obtained. Hamming weight and hamming distance models are most commonly used power consumption model, and the power consumption model is obtained through the modeling technique. If the power consumption model assumed by the actual equipment differs from the power consumption of the actual equipment, the side channel analysis performance is declined. In this paper, we propose a method that records measured power consumption and exploits as power consumption model. The proposed method uses the power consumption at the time when the information (plain text, cipher text, etc.) available in the encryption process. The proposed method does not need template in advance and uses the power consumption measured by the actual equipment, so it accurately reflects the power consumption model of the equipment.. Simulation and experiments show that by using our proposed method, side channel analysis is improved on the existing power modeling method.

Keywords: Side Channel Analysis, Power Analysis, Power Model, AES

Received(06. 21. 2017), Modified(07. 27. 2017), Accepted(7. 31. 2017)

* 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2017-2015-0-00385)

† 주저자, koga12321@gmail.com
‡ 교신저자, 80khs@korea.ac.kr(Corresponding author)

I. 서 론

암호학적으로 안전한 암호 알고리즘이라도 물리적인 동작 과정에서 비밀 정보값에 의존해 동작시간, 전력소모량, 전자기파 등의 부가적인 정보가 발생한다. 1996년 Kocher는 이런 부가적인 정보를 이용하여 비밀정보를 복원하는 부채널 공격(Side Channel Attack)을 제안하였다[1]. 부채널 공격은 공격에 이용하는 정보에 따라서 소요시간공격[1], 전력분석공격[2], 전자기파공격[5,6]등으로 나누어진다. 이 중 전력 분석공격은 하나 또는 적은 수의 파형을 이용하는 단순 전력분석공격(Simple Power Analysis)과 많은 수의 파형을 이용하여 통계적 방법으로 분석하는 차분 전력분석공격(Differential Power Analysis, DPA)[3,4]으로 분류할 수 있다. 차분 전력분석공격은 알려진 데이터와 추측하는 비밀 정보 값에 따라 목표로 잡은 지점의 중간 값을 연산한 후에 선택한 전력 소비 모델에 중간 값을 대입한 전력 소비량과 실제 수집된 파형을 특정 구별자를 통해 분석하여 비밀 정보 값을 복원해 내는 방법이다.

DPA 공격을 할 때 전력 소비 모델과 구별자의 선택이 공격 성공률을 좌우하게 되는 데 구별자는 주로 피어슨 상관계수를 이용한 CPA[17]를 선택한다. 주로 쓰이는 전력 소비 모델에는 모든 비트의 가중치가 동일하다고 가정하여 전력 소모량은 1의 개수에 비례하다고 보는 해밍 웨이트 모델, 전력소모량은 비트 변화가 일어날 때 발생한다고 보는 해밍 디스턴스 모델이 있다. 해밍 웨이트 모델이나 해밍 디스턴스 모델을 쓰는 것외에 전력 소비 모델을 추정을 통해 구한다. 기존에 연구되어 오던 전력 모델링 기법들은 사전에 전력 소비 모델을 가정을 한 후 그 가정에 따라 미지수인 계수를 찾는 형태가 일반적이며[9,10,11] 전력 모델링 기법의 한 예로는 선형 회귀법[9]이 존재한다. 하지만 전력 소비 모델로 해밍 웨이트 모델, 해밍 디스턴스 모델을 쓰는 경우나 모델링 기법을 통해 전력 소비 모델을 구하는 경우에는 공격 타켓이 되는 장비가 가정한 소비 모델과 상이한 경우 중간 값에 해당하는 전력 소비를 옳게 반영하지 못하는 문제가 발생한다.

본 논문에서는 실제 장비에서 발생하는 전력 소비량을 이용해 테이블 형태로 만들어 전력 소비 모델로 이용할 것을 제안한다. 제안하는 방법은 암호화를 하는 모든 장비에는 평문이 로딩되거나 암호문이 쓰이는 과정이 반드시 필요하다는 사실을 활용하여 평문이 로딩되거나 암호문이 쓰이는 시점에서의 소비전력을 이용하여 테이블을 생성한 후 테이블을 전력 소비 모델로 이용한다. 이 방법은 실제 공격 대상 장비에서 측정한 소비 전력을 테이블 형태로 만들어 전력 소비 모델로써 이용하기 때문에 실제 장비 전력 소비 모델을 잘 반영하며 전력 소비 모델들의 미지수인 계수를 구하기 위한 과정이 필요 없다. 제안하는 방법은 실험 장비의 전력 소비 모델을 보다 정확하게 반영하기 때문에 전력 소비 모델을 잘못 설정했을 때보다 부채널 공격 성능이 향상된다.

기존의 방법들과의 비교를 위해 잘 알려진 블록암호인 AES(Advanced Encryption Standard)에 대해 CPA를 시행하였다. CPA를 시행할 때 전력 소비 모델은 해밍 웨이트 모델과 본 논문에서 제안한 소비 전력 테이블을 전력 소비 모델로 설정하였으며 시뮬레이션 결과 제안한 방법의 CPA성능이 향상되었음을 확인하였다. 전력 모델링 기법중 하나인 선형 회귀법과의 연산량 비교와 성능 비교는 추후 연구사항으로 남겨 놓는다. 또한 제안한 방법의 응용 사례로 1차 마스킹 테이블이 적용된 AES에 대해서도 마스킹 복원 시뮬레이션을 진행하고 실제 실험 보드인 SCARF-MSP430보드[15]에 대해 실험을 진행하였다. 그 결과 시뮬레이션과 실험에서 모두 제안한 방법의 마스킹 복원률이 향상됨을 확인하였다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구에 대해 살펴본다. 3장에서 제안하는 방법을 소개하며 제안하는 방법을 이용한 공격 시나리오에 대해 설명한다. 4장에서는 기존의 방법과의 성능 비교를 하며 마지막 5장에서 결론을 맺는다.

II. 관련 연구

2.1 절에서는 데이터에 대한 전력 소비 모델을 기술한다.

2.1 데이터에 따른 전력 모델

본 논문에서 사용된 표기법은 다음과 같다.

$E_k(p)$: 평문 p 를 비밀 정보 값 k 로 암호화한 값

x : $[x_{n-1}, x_{n-2}, \ldots, x_0]$

x_i : x의 i번째 비트
p_i : 암호화에 사용된 i 번째 평문
$p_{i,j}$: i번째 평문의 j번째 바이트
k_j : 비밀 정보 k의 j번째 바이트
$v_{k,i}$: $E_k(p_i)$ 를 계산하는 동안 발생하는 민감한 정보
$l_{k,i}$: $v_{k,i}$ 에 의존하여 발생하는 전력파형 등의 부채널 정보
V_k, L: 샘플 $v_{k,i}, l_{k,i}$들의 확률 변수
δ: 결정론적 함수
K: 상수
B: 독립적인 노이즈
$N(,)$: 가우시안 분포
σ: 노이즈의 표준 편차
α_i : 비트별 가중치
σ_α : 비트별 가중치의 표준 편차
$s^1()$: AES의 1라운드 sbox 8비트 출력값

마이크로 컨트롤러에서 암호 알고리즘이 동작될 때 중간값 $v_{k,i}$들이 계산되며 $v_{k,i}$에 의존하여 전력 소비량 $l_{k,i}$ 이 발생하게 된다. 이때 V_k 와 L 은 다음과 같이 표현 가능하다[10].

$$L = \delta(\mathrm{V_k}) + \mathrm{B}.$$

결정론적 함수는 전력 소비 모델에 따라 다음과 같이 정의할 수 있다[11].

전역 모델 : $\delta(x) = K$
선형 모델 : $\delta(x) = \sum_{i=0}^{n-1} x_i \alpha_i$
플립 모델 : $\delta(x) = F(x, x_{last})$
이차 모델 :

$$\delta(x) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} X_{00_{ij}}\alpha_{00_{ij}} + X_{01_{ij}}\alpha_{01_{ij}} + X_{10_{ij}}\alpha_{10_{ij}} + X_{11_{ij}}\alpha_{11_{ij}}$$

$where\ X_{ab_{ij}} = 1 \quad \text{iff } x_i = a\,, x_j = b.$

전역 모델의 경우 모든 값에 대하여 같은 전력 소비량을 발생시킨다고 가정하며 그 값을 상수 값으로 쓴다. 선형 모델의 경우 모든 비트가 독립적이고 특정한 가중치를 갖는다고 가정하고 있다. 만약 모든 $0 \le i \le n-1$에 대하여 $\alpha_i = 1$로 고정하는 경우 해밍 웨이트 모델을 따르게 된다. 플립 모델은 연산을 수행하는 데이터의 마지막 값이 전력 소비량에 영향을 미친 경우를 나타낸다. $F = HW(data \oplus data_{last})$인 경우 이는 상태가 바뀐 비트의 갯수를 나타내게 되며 전력 소비 모델은 해밍 디스턴스 모델을 따르게 된다. 이차 모델은 한 번에 두 비트씩 전력 소모량에 영향을 미친 경우를 나타낸다. 실제 회로에선 여러 비트 값이 동시에 전력 소모량에 영향을 미칠 수 있기 때문에 위의 모델들 중 데이터의 전력 소비 모델을 가장 근접하게 표현한 모델이 된다. 위의 전력 소비 모델말고 전력 소비 모델을 최대 n차수를 갖는 선형식으로 표현한 후 미지수를 구하는 선형 회귀법이 존재한다[10]. 기존의 모델링 기법들은 위의 전력 소비 모델들 중 한 전력 소비 모델을 가정한 후에 미지수인 계수를 구하는 방법으로 전력 소비 모델을 예측한다. 여러 연구 결과에서는 대부분의 장비의 전력 소비 모델이 해밍 웨이트 모델이나 해밍 디스턴스 모델과 유사하다는 결론을 내고 있다[2,12,13].

III. 제안하는 방법

본 논문에서 제안하는 방법은 실제 장비에서 암호화가 진행되는 동안 활용 가능한 정보의 소비 전력을 이용한다. 예를 들면 실제 장비에서의 암호화 과정에는 평문이 로딩되거나 암호문이 저장되는 과정이 반드시 존재하기 때문에 이 시점에서의 소비 전력을 이용하여 테이블을 구성한다. 또한 평문과 암호문이 아니더라도 공격에 활용 가능한 정보라면 해당 정보의 소비 전력을 이용한 전력 테이블 구성이 가능하다. 마스킹이 적용된 SPN 구조 블록 암호의 경우 사전에 마스킹 S-box을 생성하는 과정이 필요하다. 이 과정에는 $S(0) \sim S(255)$까지를 로딩하는 부분이 존재한다. 공격자는 이 시점의 전력 정보를 이용하여 테이블 구성이 가능하다.

제안한 방법은 사전에 탬플릿을 구성하지 않은 채 암호화 과정에서 측정한 전력 소비량으로 전력 테이블을 구성한다. 또한 실제 공격 대상 장비에서 측정한 전력 소비량을 테이블 형태로 만들어 전력 소비 모델로 이용하기 때문에 실제 장비 회로의 전력 소비

특성을 잘 반영한다. 제안하는 방법은 소비 전력 테이블을 생성하는 단계와 전력 테이블을 이용하는 단계로 나눌 수 있다. 전력 테이블을 생성하는 단계는 다음과 같은 과정으로 이루어진다.

3.1 소비 전력 테이블 생성

① 공격자는 전력 테이블 구성이 가능한 정보(평문, 암호문 등) 중 사용할 정보를 선택한다.
② N개의 파형을 ①에서 선택한 정보에 대해 CPA를 수행한 후 전력 파형에서 해당 정보가 쓰인 위치(POI)를 찾는다.
③ 선택한 정보의 값이 0x00 ~ 0xff인 경우에 따라 ②에서 구한 POI의 전력 파형들을 분류한다.
④ 모아놓은 파형들의 평균값을 각각 구한다.

공격자는 자신이 알 수 있는 정보(평문, 암호문 등)들을 활용하여 데이터 0x00 ~ 0xff 값에 대응하는 전력 소비량을 구할 수 있다. 예를 들어 암호 알고리즘 동작 과정에서 평문이 불리어 오는 과정의 정보를 활용하는 경우 첫 번째로 공격자가 관찰한 N개의 전력 파형을 이용하여 평문 값에 대한 CPA를 통해 파형에서 평문이 불리어지는 위치를 찾는다. 전력 파형에서 얻은 위치의 전력 소비량을 평문의 데이터 값 0x00 ~ 0xff에 따라 분류한다. 128비트의 평문 N개를 이용한 경우라면 총 16*N개의 전력 소비량을 얻을 수 있기 때문에 수많은 랜덤한 평문들을 이용한다면 데이터 0x00 ~ 0xff에 해당하는 전력 소비량을 모으는 것이 가능하다. 공격자는 모아놓은 전력 소비량들을 각각 평균을 냄으로써 노이즈를 줄인 후 소비 전력 테이블을 구성한다. 이와 마찬가지로 공격자는 암호문이 저장되어지는 지점의 전력 소비량을 이용하여 암호문을 활용한 소비 전력 테이블 구성이 가능하다. 평문과 암호문이 아니더라도 공격에 활용 가능한 정보라면 그 정보를 이용하여 소비 전력 테이블 구성이 가능하다. 예를 들어 마스킹이 적용된 AES같은 경우 사전연산단계에서 마스킹 S-box를 계산하는 연산단계가 존재하기 때문에 $s(u), 0 \le u \le 255$가 로드되는 부분의 소비 전력을 이용하여 소비 전력 테이블을 구성할 수 있다.

제안하는 방법은 장비에서 얻은 실제 장비에서 모은 파형으로 테이블을 구성하기 때문에 기존의 해밍 웨이트 모델이 장비의 회로마다의 특성을 반영하지 못한다는 단점을 극복할 수 있다. 또한 기존의 모델링 기법과 달리 전력 소비 모델을 가정한 후 미지수인 계수를 구하는 과정을 필요로 하지 않은 채 직관적인 방법을 통해 전력 소비 모델을 구할 수 있다는 장점이 있다.

3.2 소비 전력 테이블을 활용한 공격방법론

공격자는 다음과 같은 방법으로 소비 전력 테이블을 이용하여 부채널 공격을 수행할 수 있다.

① N 개의 평문 p_i 에 대하여 전력 소비량 $l_{k,i}$를 측정한다.
② 부채널 정보의 전력 소비 모델을 모델링하기 위해 3.1에서 제안된 방법으로 소비 전력 테이블 pwt를 생성한다.
③ 추측하는 비밀 정보값 $\hat{k}$에 따라서 $pwt_{\hat{k},i} = pwt(v_{\hat{k},i})$ 을 계산한다.
④ 구별자 $\triangle$을 선택한다.
⑤ 모든 $\hat{k}$ 에 대하여 $\triangle_{\hat{k}} = \triangle(l_{k,i}, pwt_{\hat{k},i})$ 을 계산한다.
⑥ 구별자에 따라 $\triangle_{\hat{k}}$ 값을 최대화(또는 최소화) 시키는 $\hat{k}$ 값을 산출한다.

제안된 공격 방법을 이용한 AES에 대한 공격 시나리오는 다음과 같다.

3.2.1 AES 공격 시나리오

본 절에서는 제안한 소비 전력 테이블을 이용하여 AES를 공격하는 시나리오를 설계한다.

공격자는 랜덤한 평문에 대하여 전력 소비량을 측정할 수 있으며 AES 1라운드의 출력값을 공격 타겟으로 한다. 공격 시나리오는 다음과 같다.

① N 개의 평문 p_i 에 대하여 전력 소비량 $l_{k,i}$를 측정한다.
② 공격자는 평문에 대한 전력 소비량을 공격에 사용할 수 있다. 공격자는 관측한 전력 소비량들을 이용하여 평문값 0x00 ~ 0xff에 해당하는 테이블 pwt을 구성한다.

③ 추측하는 비밀 정보값 $\hat{k}$에 따라서 $pwt_{\hat{k},i} = pwt(s(p \oplus \hat{k}))$을 계산한다.

④ 모든 $\hat{k}$ 에 대하여 $l_{k,i}$ 와 $pwt_{\hat{k},i}$의 피어슨 상관계수 $corr_{\hat{k}}$을 계산한다.

⑤ $corr_{\hat{k}}$을 최댓값으로 갖는 $\hat{k}$ 값을 산출한다.

3.2.2 1차 마스킹 테이블이 적용된 AES 공격 시나리오

본 절에서는 소비 전력 테이블 공격의 응용으로 1차 마스킹 적용된 AES[16]에서 대한 마스킹 복원 시나리오를 설계한다.

논문[14]에서는 마스킹 S-box가 생성되는 사전연산에 대해 1차 CPA를 시행함으로써 마스킹 값을 복원하는 공격을 제안하였다. 논문[14]에서 제안한 방법을 이용한다.

마스킹이 적용된 경우 모든 암호화 과정에는 마스킹 S-box을 생성하는 사전연산 단계가 필요하게 된다. 마스킹 S-box 생성은 Alg.1. 을 통해 이루어진다.

Algorithm.1 Generation of MS table [16]
Input : random number m, m′
Output: MS
1. For u=0 to 255 do
$MS(u \oplus m) = s(u) \oplus m'$
2. Return MS

마스킹 S-box를 생성할 때 전력 파형엔 $s(u)$가 로드되는 부분의 전력 소비량이 존재한다는 것을 알 수 있다. 또한 이 부분은 마스킹 값이 다르더라도 모든 파형에서 공통된 부분이다. 이런 사실을 이용하여 공격자는 관측 가능한 모든 파형에서 $s(u)$에 해당하는 전력 소비량을 수집한 후 평균을 내어 전력 테이블을 구성할 수 있다. 공격자가 i번째 암호화 과정에서의 마스킹 m'의 복원을 원하는 경우 다음과 같은 시나리오로 공격이 가능하다. 공격자는 i번째 암호화 과정의 사전 연산 단계에서 $0 \le u \le 255$에 대한 전력 소비량을 관측할 수 있으며 공격 타겟은 $s(u) \oplus m'$으로 한다. 공격 시나리오는 다음과 같다.

① N개의 평문 p_i 에 대하여 전력 소모량 $l_{m,i}$를 측정한다.

② i번째 암호화 과정에서 사전연산 단계에서의 파형을 256개의 파형으로 나눈다.

③ 공격자는 $0 \le u \le 255$을 평문으로 생각하며 ②에서 나눈 256개의 파형을 이용하여 $s(u)$에 대한 소비 전력 테이블 pwt을 구성한다.

④ 추측하는 마스킹 값 $\hat{m}$에 따라서 $pwt_{\hat{m},i} = pwt(s(u) \oplus \hat{m})$ 을 계산한다.

⑤ 모든 $\hat{m}$ 에 대하여 $l_{m,i}$ 와 $pwt_{\hat{m},i}$의 피어슨 상관계수 $corr_{\hat{m}}$을 계산한다.

⑥ $corr_{\hat{m}}$을 최댓값으로 갖는 $\hat{m}$ 값을 산출한다.

IV. 성능 비교

본 장에서는 기존의 전력 소비 모델과 소비 전력 테이블을 이용한 경우의 CPA성능 비교를 보인다. 기존의 전력 소비 모델은 CPA를 시행할 때 일반적으로 사용되는 해밍 웨이트 모델을 선택한다.

4.1 AES

본 절에서는 3.2.1절에서 설계한 시나리오를 통해 AES를 공격한다. 4.1.1절은 해밍 웨이트 모델과 소비전력 테이블을 사용한 경우의 CPA 성능 비교를 시뮬레이션을 통해 보인다.

시뮬레이션은 실험장비의 전력 소비 모델이 비트별 가중치와 노이즈가 $\alpha_i \sim N(1,\sigma_\alpha)$, $B \sim N(0,\sigma)$을 따르는 선형 모델인 상황에 대해 진행하였다. 시뮬레이션에서의 장비의 전력 소비 모델은 (1)과 같다.

$$L(x) = \sum_{i=0}^{n} x_i \alpha_i + B \tag{1}$$

4.1.1 시뮬레이션

본 절에서는 장비의 전력 소모량이 선형 모델인 상황에 대하여 공격을 진행한다. 100번에 걸쳐서 독립적으로 비트 가중치 $\alpha_i, (0 \le i \le 7)$ 를 생성하였다. 각각 독립적인 100개의 비트 가중치

$\alpha_i, (0 \le i \le 7)$에 대하여 5,000개의 평문을 매번 랜덤하게 생성하였으며 랜덤하게 생성된 평문에 따라 식 (1)를 따르는 전력 소모량을 구하였다. 이 때 전체 노이즈 B 는 매번 랜덤한 값을 생성하였다.

시뮬레이션 결과는 100개의 비트 가중치들에 대한 CPA 결과의 평균치이다. CPA를 시행할 땐 각각 5,000개의 파형을 이용하였다. Fig.1. 은 $\sigma_\alpha = 0.5$ 인 경우 $\sigma = 1$인 상황에서 해밍 웨이트 모델로 전력 소비 모델을 설정한 경우와 전력 테이블을 전력 소비 모델로 이용한 경우에 대한 CPA 결과이다. 검정 실선은 해밍 웨이트 모델의 경우를 나타내며 빨간 점선은 제안된 기법을 이용한 경우에 해당한다. 가로축은 비밀 정보값 0x00~ 0xff 이며 세로축은 CPA 결과를 의미한다. 소비 전력 테이블을 전력 소비 모델로 이용한 경우의 CPA 성능이 좋다는 것을 확인할 수 있다.

Table 1. 은 $\sigma_\alpha = 0.5$ 인 상황에서 σ값의 변화에 따른 CPA 성능 비교를 나타낸 것이다. 실험을 진행한 모든 σ의 경우에서 제안한 방법의 성능이 좋다.

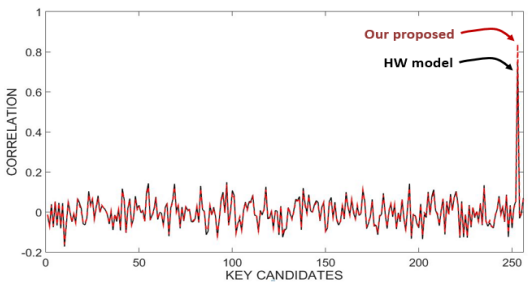

Fig. 1. $\sigma = 0.5, \sigma_\alpha = 1$

Table 1. CPA result

σ	HW model	Proposed model
1	0.7575	0.8366
2	0.5539	0.6108
4	0.3283	0.3624
8	0.1736	0.1914
16	0.0866	0.0949

4.2 1차 마스킹 테이블이 적용된 AES

4.2.1절은 시뮬레이션을 통해 해밍 웨이트 모델과 제안하는 방법의 마스킹 복원률 성능 비교를 진행하며 4.2.2절에서는 실제 실험 보드인 SCARF MSP430[15]를 통해 성능 비교를 진행하였다.

시뮬레이션은 실험장비의 전력 소비 모델에 따른 전력 소모량과 노이즈가 각각 $\delta_i \sim N(1, \sigma_\alpha)$, $B \sim N(0, \sigma)$을 따르는 선형 모델인 상황에 대해 진행하였다. 시뮬레이션에서의 장비의 전력 소비 모델은 (1)와 같다.

실제 장비인 SCARF-MSP430보드의 경우 소프트웨어를 통해 구현하였다. 파형을 수집할 때 100MS/s의 샘플링 레이트로 10,000개의 파형을 수집하였다. SCARF-MSP430의 동적 주파수는 8MHz이다[15].

4.2.1 시뮬레이션

본 절에서는 3.2.2절에서 소개한 시나리오에 대한 시뮬레이션 결과를 소개한다. 10번에 걸쳐서 독립적으로 비트 가중치 $\alpha_i, (0 \le i \le 7)$ 를 생성하였다. 각각 독립적인 10개의 비트 가중치 $\alpha_i, (0 \le i \le 7)$ 에 대하여 1,000번의 암호화 과정마다 평문과 마스킹 값을 매번 랜덤하게 생성하였다. 시뮬레이션 파형은 랜덤하게 생성된 마스킹 값에 따라 식 (1)을 만족한다. 이 때 전체 노이즈 B 는 매번 랜덤한 값을 생성하였다.

Fig.2. 은 3.2.2절의 시나리오에 따라 공격하였을 때 $\sigma_\alpha = 0.5$ 인 상황에서 σ에 따른 마스킹 값 복원 성공률을 나타낸다. 마스킹 복원 성공률은 각각 10개의 비트 가중치 $\alpha_i, (0 \le i \le 7)$에 대하여 1,000번의 공격 중 실제 마스킹이 CPA를 통해 첫 번째 후보군으로 나타나는 확률의 평균 값이다. 빨간 점선은 제안한 기법의 성공률을 나타내며 검정 실선

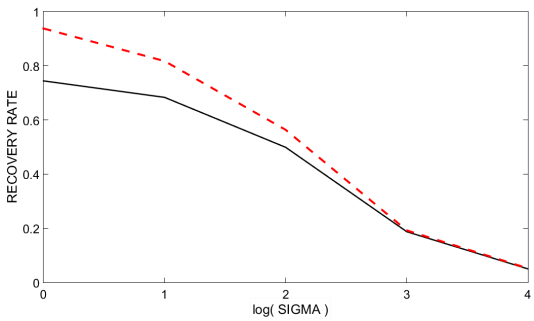

Fig. 2. $\sigma_\alpha = 0.5$, masking recovery rate

은 해밍 웨이트 모델의 성공률을 나타낸다. 모든 경우에 대해서 해밍 웨이트 모델을 사용한 경우보다 제안한 방법의 성공률이 높게 나타난다.

4.2.2 실험 결과

수집한 파형은 Fig.3. 과 같다. 그림은 사전 연산 단계를 포함한 10개 라운드 연산의 모든 부분을 포함하고 있다. Fig.4. 는 사전 연산 단계만을 나타낸다. 사전 연산 단계에서의 파형을 확대하여 살펴보면 Fig.5. 와 같이 동일한 패턴이 반복되는 것을 확인할 수 있다. SPA를 통해 패턴의 시작점과 윈도 우 사이즈(참조 파형)를 예측한다. 예측한 참조 파형을 한 포인트씩 밀어가면서 상관성을 계산하는 상호 상관을 통해 사전 연산 단계에서의 파형을 256개의 파형으로나눈다. Fig.6.은 사전연산단계를 256개로 나눈 후 중첩시킨 파형을 나타낸다. 전력 테이블을 구성하기 위해 256개의 파형을 이용하여 $s(u)$에 대한 전력모델링을 HW모델로 한 후 CPA를 수행한다. CPA 결과로 해당 정보가 불리어오는 위치를 찾는다. Fig.7. 상단은 CPA의 결과를 나타내며 하 단은 256개로 자른 파형 중 한 파형을 나타낸 것이다. Fig.7. 에서 상관계수가 가장 높게 나타나는 지점이

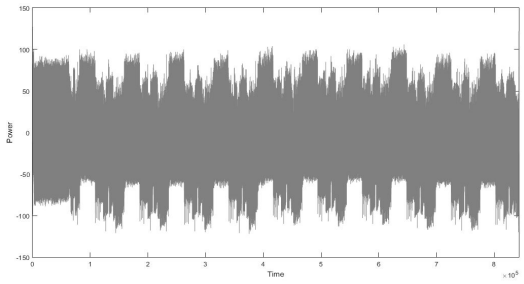

Fig. 3. Full round of 1st order AES

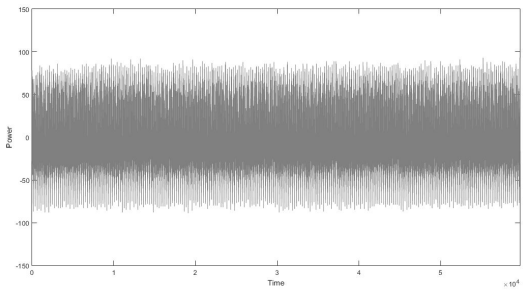

Fig. 4. Precomputation

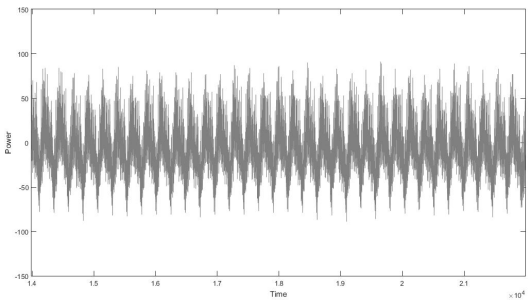

Fig. 5. Precomputation 2

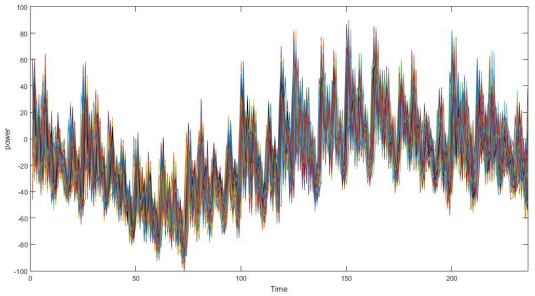

Fig. 6. Subtraces of precomputation step

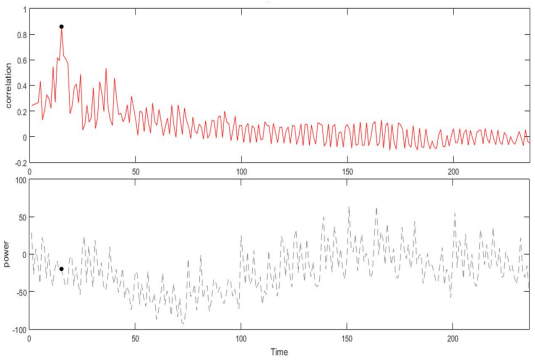

Fig. 7. Point of Interest

$s(u)$가 불리어 오는 지점으로 이 지점의 소비 전력을 이용하여 소비 전력 테이블을 구성할 수 있다. 공격자는 전력 테이블을 전력 소비 모델로 이용한다. Fig.3.~Fig.6. 의 가로축은 파형의 시점을 나타내며 세로축은 전력 소비량을 나타낸다.

구성한 소비 전력 테이블을 전력 소비 모델로 이용한 경우와 기존의 해밍 웨이트 모델을 전력 소비모델을 이용한 경우의 마스킹 복원 성공률은Table. 2 와 같다.

Table 2. SCARF-MSP430 result

HW model	Proposed model
64.18%	65.07%

마스킹 복원 성공률은 10,000개의 파형 중 실제 마스킹 값이 CPA 결과 첫번 째 후보군으로 나타난 경우의 확률을 구한 것이다. 해밍 웨이트 모델을 잘 따른다고 알려진 SCARF-MSP430보드에 대해서 해밍 웨이트 모델로 전력 소비 모델을 설정하였을 때보다 제안된 방법의 마스킹 값 복원 성공률이 증가하였다. 실험 장비가 해밍 웨이트 모델을 잘 따르지 않는 경우 전력 소비 모델을 해밍 웨이트 모델로 설정하는 것보다 제안된 방법의 성능이 크게 향상될 것이다.

V. 결 론

본 논문에서는 실제 공격 장비에서 이용 가능한 정보(평문과 암호문 등)와 관련된 전력 소비량을 테이블로 만들어 전력 소비 모델로 사용하는 방법을 제안하였다. 이 방법은 기존의 모델링 기법과 달리 실제 파형을 테이블로 만들어 전력 소비 모델로 이용하기 때문에 실제 장비의 전력 소비 특성을 잘 반영한다. AES에 대해 해밍 웨이트 모델과 제안한 방법의 성능 비교를 시뮬레이션을 통해 보였으며 제안하는 방법의 응용으로 1차 마스킹이 적용된 AES에 대해서도 시뮬레이션과 실험을 통해 성능을 비교하였다. 시뮬레이션 결과 실험 장비가 해밍 웨이트 모델을 따르지 않는 경우 제안하는 기법을 이용하면 성능이 향상됐다. 또한 전력 소비 모델이 해밍 웨이트 모델을 잘 따른다고 알려져 있는 SCARF-MSP430보드 같은 경우에서도 성능이 소폭 향상됨을 확인하였다. 전력 소비 모델이 해밍 웨이트 모델을 따르지 않는 실험 장비에 대해선 제안하는 공격 방법의 큰 효과를 보일 것으로 기대된다. 본 논문에서는 CPA를 수행할 때 전력 소비모델로 주로 사용되는 해밍 웨이트 모델과의 비교만을 수행하였으며 전력 모델링 기법 중 한 연구 분야인 선형 회귀법을 통해 전력모델을 계산한 경우와의 성능비교는 추후 연구 사항으로 남겨 놓는다.

References

[1] P. Kocher, J. Jaffe, and B. Jun, “Timing Attacks onImplementations of Diffie-Hellman, RSA, DSS, and Others Systems,” Annual International Cryptology Conference, Springer, Berlin, Heidelberg pp. 104-113, 1996

[2] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” CRYPTO'9, Springer Berlin/Heidelberg, pp. 789-789, 1999.

[3] P. Kocher, J. Jaffe, and B. Jun, “Introduction to differential power analysis,” Journal of Cryptographic Engineering vol. 1, no. 1, pp. 5-27, 2011.

[4] Ors,S.B, Gurkaynak, F. Oswald, E, and Preneel. B, “Power-Analysis Attack on an ASIC AES implementation,” Information Technology: Coding and Computing, Proceedings. ITCC 2004. International Conference on. IEEE, vol. 2. pp. 546-552, April. 2004.

[5] Agrawal, D, Rao, J.R., nd Rohatgi, P, “Multi-channel attacks,” CHES, vol. 2779, pp. 2-16, September, 2003.

[6] Gandolfi, Karine, Christophe Mourtel, and Francis Olivier. “Electromagnetic analysis: Concrete results,” Cryptographic Hardware and Embedded Systems-CHES 2001, Springer Berlin, Heidelberg, pp. 251-261, Sep, 2001.

[7] Brier, Eric, Christophe Clavier, and Francis Olivier. “Correlation power analysis with a leakage model,” International Workshop on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, pp. 16-29, 2004

[8] Messerges, Thomas S., Ezzy A. Dabbish, and Robert H. Sloan. “Investigations of Power Analysis Attacks on Smartcards,” Smartcard 99, pp. 151-161, 2011

[9] Schindler, Werner, Kerstin Lemke, and Christof Paar. “A stochastic model for dif-

ferential side channel cryptanalysis," International Workshop on Cryptographic Hardware and Embedded Systems, Springer Berlin Heidelberg, pp. 30-46, 2005.

〔10〕 Doget, J., Prouff, E., Rivain, M., and Standaert, F.X., "Univariate side channel attacks and leakage modeling," Journal of Cryptographic Engineering, vol. 1, no. 2, pp 123-144, 2011

〔11〕 Akkar, M.L., Bevan, R., Dischamp, P., and Moyart. D, "Power analysis, what is now possible," Advances in Cryptology-ASIACRYPT 2000, pp. 489-502, 2000.

〔12〕 Biham, Eli, and Adi Shamir, "Power analysis of the key scheduling of the AES candidates," Proceedings of the second AES Candidate Conference,, pp. 115-121, 1999.

〔13〕 Chari, S., Jutla, C., Rao, J.R., and Rohatgi, P, "A cautionary note regarding evaluation of AES candidates on smart-cards," Second Advanced Encryption Standard Candidate Conference, pp. 133-147, 1999.

〔14〕 Tunstall, Michael, Carolyn Whitnall, and Elisabeth Oswald. "Masking tables-an underestimated security risk," International Workshop on Fast Software Encryption, Springer Berlin Heidelberg, pp. 425-444, 2013.

〔15〕 YongJe Choi, DooHo Cho, and JaeCheol Ryou, "Implementing Side Channel Analysis Evaluation Boards of KLA-SCARF system," Journal of The Korea Institude of Information Security & Cryptology, vol. 24, no. 1, pp. 229-240, Feb, 2014.

〔16〕 Herbst, Christoph, Elisabeth Oswald, and Stefan Mangard. "An AES smart card implementation resistant to power analysis attacks," International Conference on Applied Cryptography and Network Security, Springer Berlin Heidelberg, vol. 3989, pp. 239-252, Jun, 2006.

〔17〕 Brier, Eric, Christophe Clavier, and Francis Olivier, "Correlation power analysis with a leakage model," International Workshop on Cryptographic Hardware and Embedded Systems, Springer Berlin Heidelberg, pp. 16-29, 2004.

〈저자소개〉

고 가 영 (Gayeong Ko) 학생회원
2016년 2월: 광운대학교 수학과 학사
2016년 3월 ~ 현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 부채널 공격, 공개키 암호 알고리즘

진 성 현 (Sunghyun Jin) 학생회원
2015년 2월: 서울시립대학교 수학과 학사
2015년 3월~2017년 2월: 고려대학교 정보보호대학원 석사
2017년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 부채널 공격

김 한 빛 (Hanbit Kim) 학생회원
2014년 2월: 고려대학교 신소재공학과 석사
2014년 3월~2016년 2월: 고려대학교 정보보호대학원 석사
2016년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 부채널 공격, 부채널 대응기법, 암호시스템 안전성 분석 및 고속구현

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

홍 석 희 (Seokhie Hong) 종신회원
1995년: 고려대학교 수학과 학사
1997년: 고려대학교 수학과 석사
2001년: 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-CCOSIC 박사후 연구원
2005년 3월~2013년 8월: 고려대학교 정보보호대학원 부교수
2013년 9월~현재: 고려대학교 정보보호대학원 정교수
〈관심분야〉 대칭키 및 공개키 암호알고리즘, 부채널 공격 및 대응기법, 디지털 포렌식