JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 1, pp. 79-86, January 2020
https://doi.org/10.9708/jksci.2020.25.01.079

Implementation of AES and ARIA algorithm with Secure Structure for Power Analysis using LFSR Masking

Young-Jin Kang*, Ki-Hwan Kim*, Hoon Jae Lee**

*Graduate Student, Dept. of Ubiquitous IT, Dongseo University, Busan, Korea
*Graduate Student, Dept. of Ubiquitous IT, Dongseo University, Busan, Korea
**Professor, Div. of Information and Communication Engineering, Dongseo University, Busan, Korea

[Abstract]

In this paper, we analyzed the case vulnerable to the power analysis attack of the ARIA algorithm and AES algorithm. Through this, we propose an algorithm with a safe structure for power analysis and prove through experiment. The proposed technique is a masking method using LFSR with a cyclic structure. To verify this, 1000, 2000, and 4000 power traces were collected, and the corresponding results are shown and proved. We used ATmega328 Chip for Arduino Uno for the experiment and mounted each algorithm. In order to measure the power consumption, a resistor was inserted and then proceeded. The analysis results show that the proposed structure has a safe structure for power analysis. In the future, we will study ways to lead to performance enhancement.

▸ **Key words**: Power Analysis, LFSR, Masking, ARIA, AES

[요 약]

본 논문에서는 ARIA 알고리즘과 AES 알고리즘을 대상으로 전력분석공격을 시도한 사례를 찾아 취약점을 분석하고, 이를 통해 전력분석에 안전한 구조를 가지는 알고리즘을 제안하고 실험을 통해 증명하고자 한다. 제안하는 기법은 순환 구조를 가지는 LFSR을 이용하여 마스킹 하는 방식으로 이를 검증하기 위해 Power Trace를 각각 1000개, 2000개, 4000개를 수집한 뒤 전력분석공격을 시도하여 안전한 구조인지를 확인할 수 있는 결과를 보이고자 한다. 실험을 진행하기 위하여 Arduino Uno에 ATmega328 Chip을 사용하여 각 알고리즘을 탑재 하였으며, 소모 전력을 측정하기 위하여 저항을 삽입한 후 진행하였다. 분석결과 제안하는 구조는 전력분석에 안전한 구조를 가지는 것을 증명하였으며, 향후 성능고도화까지 이끌어 낼 수 있는 방법을 연구하고자 한다.

▸ **주제어**: 전력분석, LFSR, 마스킹, ARIA, AES

• First Author: Young-Jin kang, Corresponding Author: Hoon Jae Lee
*Young-Jin Kang (rkddudwls55@gmail.com), Dept. of Ubiquitous IT, Dongseo University
*Ki-Hwan Kim (ghksdl90@naver.com), Dept. of Ubiquitous IT, Dongseo University
**Hoon Jae Lee (hjlee@dongseo.ac.kr), Div. of Information and Communication Engineering, Dongseo University
• Received: 2019. 11. 13, Revised: 2019. 12. 01, Accepted: 2019. 12. 16.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

ARIA 알고리즘은 학계, 연구소, 정부 기관이 개발에 참여해서 만들어졌으며, 경량 환경 및 하드웨어 구현을 위해 최적화된 Involutional SPN 구조를 갖는 범용 블록 암호 알고리즘이다. 대부분의 연산은 XOR과 같은 단순한 바이트 단위 연산으로 구성되어 있으며, AES와 유사한 구조를 가지고 있기 때문에 대체하여 사용이 가능하다[1]. AES 알고리즘은 DES의 안전성에 대한 여러 가지 공격 방법들이 발표되면서 미국의 NIST에서는 1998년에 차세대 블록 암호 알고리즘인 AES를 공모하였다. 그 후 2년간의 심사 과정을 걸쳐 2000년 10월 Rijindael이 AES 알고리즘으로 선정되었으며, 11월 FIPS-197로 등록되었다[2].

암호 알고리즘의 안전성은 수학적 방식으로 증명되기에 일반적인 공격방식으로는 많은 시간을 필요로 한다. 이러한 안전성을 바탕으로 다양한 분야에 적용하고 있다. 하지만 1998년 P.Kocher 등이 제안한 전력분석 (Power Analysis)은 부채널 공격 (Side-Channel Attacks)의 한 종류로 암호화 과정에서 누설되는 소모 전력량을 이용하여 공격을 시도하기 때문에 수학적 방식으로 증명된 안전성과는 별개로 부가적인 정보 (소모전력, 동작 시간, 전자파 등)를 통해 알고리즘의 키를 유추할 수 있다[3]. 이렇게 공격이 소개 된 뒤 많은 연구자들이 암호 알고리즘에 다양한 공격시점을 선정한 다음 공격을 시도하여 키를 유추할 수 있다는 결론을 실험을 통해 증명하였다. 이처럼 전력분석공격은 알고리즘 자체의 안전성이 높아도 암호 알고리즘이 구현된 방법, 환경에 따라 적용이 가능하다. 이러한 특징 때문에 강력한 공격기법으로 인정을 받고 있지만 실험을 위한 환경은 단순히 스마트카드, 마이크로프로세서, 분석 보드 등으로 국한되며, 복잡한 시스템에서는 적용하기가 많이 힘들다. 이처럼 다양한 관점에서의 연구가 더욱 필요한 상황이며, 공격으로 인한 취약점을 보인만큼 다양한 대응기법도 연구가 필요하다.

기본적으로 전력분석을 대응하기 위해서는 마스킹(Masking)기법과 은닉(Hiding)기법으로 예로 설명할 수 있으며, Goubin은 암호장치에서 처리되는 데이터와 부채널 신호간의 상관관계를 제거하기 위한 방안으로 다음과 같은 방법을 소개 하였다[4]. 먼저 실행시간을 무작위로 옮기고, 기다리는 상태를 넣으며, 가짜 명령어를 삽입하고, 연산 실행을 무작위로 하는 등 암호 알고리즘의 실행에 따른 출력 추적 값의 상관관계를 제거하는 방법, 중요한 어셈블러 명령어를 분석하기 어렵도록 다른 명령어로 대치하고, 셀이나 메모리를 옮기는 중요한 회로를 재설계하는 방법, 자료나 키가 사용될 때 마다 다른 값을 갖도록 사용되는 암호 프리미티브의 알고리즘을 수정하여 공격이 어렵도록 만드는 방법을 소개하였다. 크게 구분을 지어보면 대응기법은 소프트웨어 기법과 하드웨어 기법으로 나눌 수 있지만 두 가지의 대응기법은 서로 다른 장단점이 존재 한다. 소프트웨어 기법의 경우 하드웨어에 알고리즘을 탑재하게 되는데 기존의 알고리즘을 탑재할 때 보다 대응 기법을 적용한 알고리즘을 탑재할 경우 퍼포먼스 측면에서 기존보다 느려지는 단점이 존재한다. 반대로 하드웨어의 경우 회를 재설계하거나 새로운 공정과정을 필요하기 때문에 비용이 발생하는 문제가 생긴다. 일단 소프트웨어 대응기법은 성능의 고도화만 이끌어낼 수 있으면 비용이 발생하지 않기 때문에 많은 연구자들이 다양한 방법을 제시하고 있다. 본 논문에서는 다른 연구자들의 ARIA 알고리즘과 AES 알고리즘을 공격한 사례를 분석하고 전력분석에 안전한 알고리즘의 구조를 제안한다. 다음으로 전력분석에 안전한 구조를 가지는지 실험을 통해 검증하고자 한다.

II. Related Works

전력분석은 암호 알고리즘이 동작할 때 원하는 곳의 공격 시점을 선정한 뒤 소모 전력을 수집해서 공격을 시도하기에 서로 다른 공격시점의 실험 데이터를 수집해서 분석을 하고자 한다.

1. Case Analysis

표1은 ARIA 알고리즘에 대한 전력분석 사례를 간단하게 공격 대상 소자, 대상 함수, 수집한 파형의 개수로 분리해서 정리하였다. 많은 사례가 있는 것은 아니지만 사례를 살펴보면 공격 대상 함수로 S-box 연산 시점으로 시도를 많이 하였으며, 전력분석에 취약함을 나타내었다. ARIA 알고리즘의 경우 다양한 공격 대상 함수를 공격 시점으로 삼은 논문을 찾고 싶었으나 더 이상의 다른 논문들을 찾을 수가 없어서 같은 공격 시점의 논문이라도 공격 대상 소자와 수집한 파형의 개수 또는 서로 다른 입력 값의 개수도 상이하기에 정리를 하였다. AES 알고리즘의 경우도 대체적으로 S-box 연산을 공격 시점으로 선정하여 공격을 시도한 논문이 많았으며, 이 또한 전력분석에 취약함을 나타내었다.

Table 1. Case Analysis

Case	Target Board	Target Algorithm	Target Function	Number of Waveforms
1[5]	32bit CPU core (Smart-Card)	ARIA	Substitute bytes	5,000 power trace
2[6]	Telos module (MSP430 microcontroller)	ARIA	S-box	100,000 power trace
3[7]	FPGA (AlteraEP20K300EQC240-3)	ARIA	S-box output	100,000 power trace
4[8]	ATmega 328P-PU	AES	AddRoundKey	1,000 power trace
5[9]	AT89S52 microcontroller	AES	S-box output	5,000 power trace
6[10]	ATmega 328P	AES	AddRoundKey, SubBytes	-

먼저 사례 1)의 경우 ARM 계열의 32비트 CPU core를 사용했으며, 128비트 키를 사용한 12라운드 ARIA를 구현하였다. 공격을 위해 round key ad-dition, S-box에 의한 치환 및 확산과정을 확인하였으며, 8비트 모두를 해밍 웨이트 기반으로 분류하였다. 그리고 분명한 peak를 위해 5000개의 power trace를 이용하였지만, 2000개의 power trace를 사용해도 공격이 가능함을 실험으로 증명하였다. 사례 2)의 경우 공격 Telos RFID 디바이스에서 작동하는 Tiny OS에 ARIA 알고리즘을 탑재한 후 실험을 진행하였으며, DPA와 DPFA 공격을 통해 결과값을 분석하였다. 그 결과 전력소비 신호의 정렬이 잘못되어 실패하였으며, 이를 해결하기 DPFA로 구현하였지만 이 또한 실패하여 그 원인을 분석하고 다음 방안을 제시하였다. 사례 3)의 경우 multiplicative inverter과 table look-up으로 구현된 S-box 출력 시점을 DPA로 공격하였으며, 똑같은 공격 시점에 DEMA공격을 시도하여 공격이 성공함을 입증하였고, 동시에 상관계수 값을 비교분석하였다. 마지막으로 DEMA공격의 거리에 따른 필요한 trace를 정리하여 나타내었다. 사례 4)의 경우 ATmega328P-PU를 장착한 Arduino Uno를 사용하여 사용하였고, 모듈을 구성하였고, AddRoundKey 함수를 대상으로 공격하였다. 1000개 이상의 다른 평문을 이용하여 소모 전력파형을 수집한 뒤 상관전력분석을 시도하여 그 취약함을 입증하였다. 사례 5)의 경우 AT89S52 마이크로컨트롤러에 알고리즘을 탑재한 뒤 5000개의 전력 파형을 수집한 뒤 상관전력분석을 통해 정확한 키를 유추하였다. 또한 상관전력분석이 S-box와 Xor중에 어느 시점이 유리한지를 분석하였다.

사례 6)의 경우는 AES 알고리즘을 대상으로 차분전력분석과 상관전력분석 두 가지 공격을 시도하여 16바이트 키를 성공적으로 추론 할 수 있음을 보여준다. 그리고 두 가지 공격방법에 의해 생성된 결과를 비교하여 분석하기 쉬운 결과를 생성할 수 있음을 보여준다. 마지막으로 현재 기술의 한계점과 해결 방법을 제시하였다. 결과적으로 ARIA, AES 알고리즘은 전력분석에 취약함을 보였으며, 이를 토대로 전력 분석에 안전한 구조를 가지는 알고리즘을 제안하고 실험을 통해 검증하고자 한다.

III. The Proposed Scheme

전력분석을 대응하기 위한 기술에는 많은 기술들이 있으며, 대표적으로 마스킹기법이 있다. 기본적으로 마스킹 구조는 고정된 값을 사용하여 소모되는 전력을 측정하여 추측키에 해당하는 파형을 예측할 수 없도록 만드는 방법이며, 최근에는 다양한 방법들이 연구되면서 안티 마스킹 기법이 발표되고 있다. 이에 본 논문에서는 순환 구조를 가지는 LFSR을 통해 간단하게 마스킹하는 기법을 제안한다. ARIA는 33bit의 LFSR을 사용하고, AES는 31bit의 LFSR을 사용한다. LFSR이라는 공통점을 가지고 있으나 길이 값이 다르기 때문에 주기가 다르다. LFSR은 임의의 초기값을 통해 입력된 데이터 길이(n) 만큼 $2^n - 1$ 주기의 고유값을 생성하며, LFSR의 초기값은 비밀키의 값을 활용하므로 별도의 입력이 요구되지 않으며, 각각의 LFSR 메모리는 2개 이상의 비밀키 값을 조합하여 연산하기 때문에 마스킹 되는 값을 이용하여 비밀키를 유추하는 것이 어렵게 된다.

1. Propose of ARIA algorithm Structure

제안하는 LFSR의 구조는 아래 그림 1과 같으며, ARIA의 각 라운드별로 스크램블러는 키 길이에 맞게 동작하게 된다. 이 때, 라운드별 동작 횟수를 결정하는 값은 그림 1과 같이 33bit 구조의 LFSR 결과를 기존 데이터 집합에 밀어 넣는 구조로 진행된다.

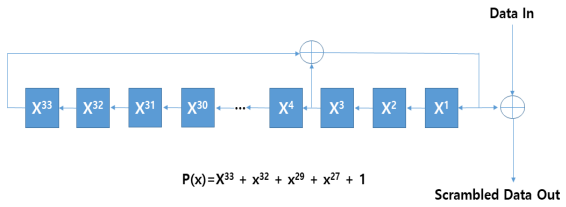

Fig. 1. ARIA scrambler LFSR structure

최종적으로 ARIA 암호 알고리즘에 스크램블러를 적용하게 되면 아래 그림 2와 같이 동작하게 된다.

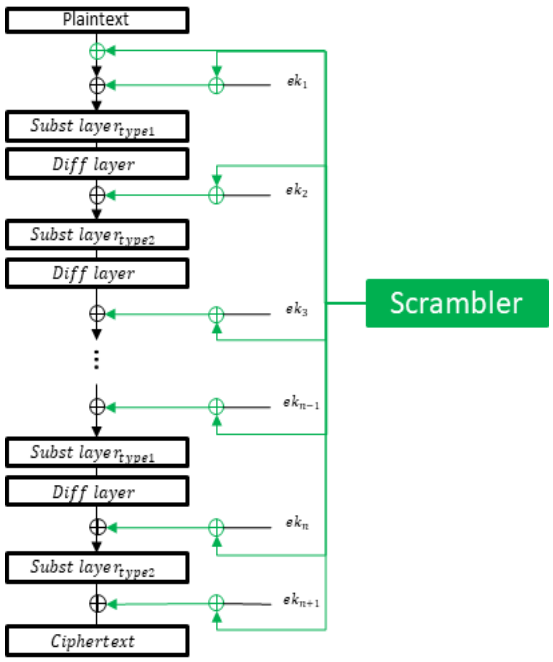

Fig. 2. Proposed of ARIA structure

본 제안의 스크램블러는 33bit의 길이를 가진 LFSR이므로 최대 주기는 $2^{33}-1$ = 8,589,934,591이며, 암호화는 각 라운드별로 32비트를 모두 사용하므로 최대주기에서 각 라운드별 사용되는 비트를 제외하여 고려할 수 있다. 만약 공격자가 사전계산을 통해 비교하는 방법을 사용하는 경우 1라운드에 대하여 사용될 수 있는 모든 경우의 수는 16,777,216가지로 각 경우의 수는 4byte를 할당하기 때문에 512MB의 크기를 가질 수 있다. 전력분석은 8bit ARM 코어를 대상으로 공격할 수도 있고, 32bit FPGA보드를 대상으로 공격을 시도할 수 있으며, 보드에 탑재된 알고리즘을 공격하기 위한 소요시간을 살펴보면 공격시점의 전력을 수집하고 키를 분석하기 위해선 최소 3시간 이상(실험환경의 방법에 따라 다양한 경우가 있다.) 걸린다. 그 이유는 공격시점의 전력을 많이 수집할수록 키를 분석하는데 용이하고, 적게 수집할수록 분석하는데 많은 어려움이 따르기 때문에 제안하는 방법은 각 라운드 별 소비전력에 따른 파형을 비교하여 유사한 패턴을 찾아야 하므로 올바른 비밀 키를 찾기 위해서는 더 많은 시간을 필요로 한다.

2. Propose of AES algorithm Structure

AES는 각 라운드별 AddRoundKey 연산에 128비트의 평문과 비밀키를 사용하며, 스크램블러의 메모리 크기가 8 이상이 될 경우 128비트 이상의 주기를 생성할 수 있으며, AddRoundKey가 호출되기 이전에 임의의 시점부터 미리 동작하였을 경우 주기의 시작과 끝을 구분할 수 없다. 아래 그림 3은 31bit 구조의 LFSR을 사용한다.

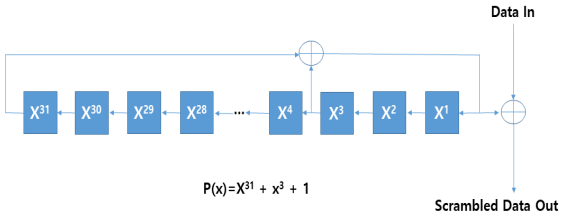

Fig. 3. AES scrambler LFSR structure

스크램블러를 사용하는 것으로 기존의 AES연산 결과에 영향을 미치는 일이 없도록 그림 4와 같이 변경하였다.

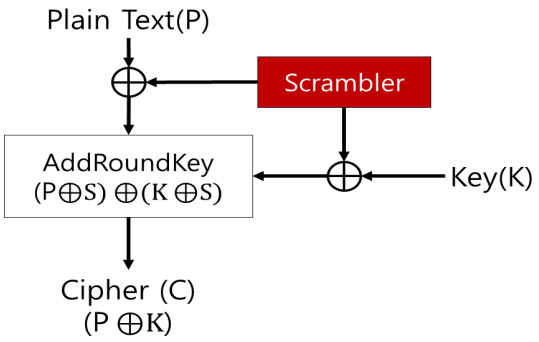

Fig. 4. Change AES scrambler AddRoundKey function

스크램블러는 AddRoundKey 연산에서 자연스럽게 소멸되고 연산결과가 기존 AES와 동일한 것을 볼 수 있으며, 이를 수식으로 나타내면 다음과 같다.

$$(P_i \oplus S_i) \oplus (K_i \oplus S_i) = (P_i \oplus K_i) \oplus (S_i \oplus S_i) = (P_i \oplus K_i) \oplus 0 = P_i \oplus K_i = C_i \quad (1)$$

최종적으로 AES 암호 알고리즘에 스크램블러를 적용하게 되면 아래 그림 5와 같이 동작하게 된다[11].

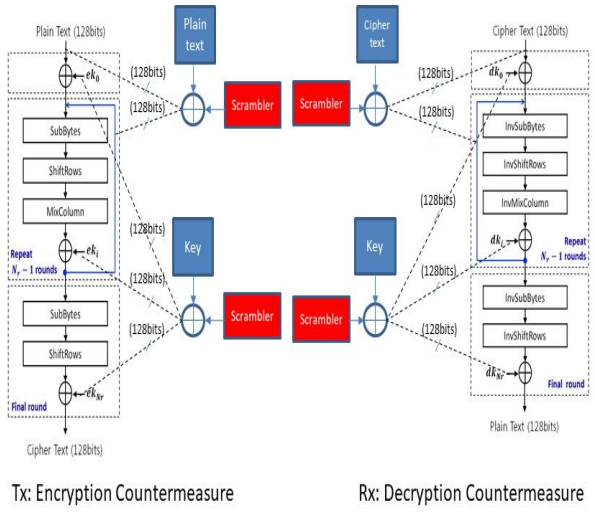

Fig. 5. Proposed of AES structure

스크램블러는 스트림 암호의 특성을 가지고 있으며, 스트림 암호(S)는 절대로 '0'을 반환하지 않는 특성을 가지고 있어 추측 가능한 모든 비밀키 조합(G)과 스크램블러에 의하여 무작위로 변조된 비밀키 조합(R)의 관계를 다음과 같이 정의할 수 있다.

$$G \oplus S = R,\ (S \neq 0) \\ \therefore G \neq R \tag{2}$$

전력분석은 평문과 암호문이 만들어 지는 순간의 소모전력 신호(T_t)를 암호문 결과(C_t)와 치환하는 것으로 비밀키(K_t)를 알 수 있다는 근거에 기반하고 있다.

$$P_t \oplus K_t = C_t = T_t = T_t \oplus P_t = K_t \tag{3}$$

즉, 추측 가능한 모든 비밀키 조합은 중복이 허용되지 않는 순차적인 신뢰할 수 있는 데이터의 집합에 해당했으나 스크램블러로 인하여 중복이 존재할 수 있고 비순차적인 신뢰할 수 없는 데이터로 변질된다.

$$P_t \oplus (G_t \oplus S_t) = P_t \oplus R_t = \\ T_t^{'} \neq T_t,\ (T_t = P_t \oplus K_t) \tag{4}$$

따라서 모든 경우를 고려하여 연산을 수행하더라도 스크램블러의 간섭을 배제하지 않는 이상 소비전력 결과를 올바르게 해석할 수 없기 때문에 의미 없는 데이터가 된다. 만약 알고리즘을 공격하기에 앞서 스크램블러를 공격할 경우 스크램블러의 구조와 초기값에 대하여 공격해야 한다. 그러나 전력분석은 초기값을 직접 알아내는 것이 아닌 모든 가능한 방법을 조합하여 가장 높은 매칭율을 보이는 추정값을 선택하는 것이므로 앞서 스크램블러에 사용되는 초기값이 이상이라고 가정했다면, 주기는 $2^{31}-1=2,147,483,647$이다. 만약 AES128 암호를 방어할 경우 128비트를 생성하며, 약 $\cong 2^{31-7}=2^{24}$회로 스크램블러가 반복된다. 실험에서 1회 측정이 약 5초임을 감안했을 때 스크램블러 자체를 공격하는 것은 많은 비용이 발생하는 것을 알 수 있다.

IV. Experiment Result

본 장에서는 제안한 구조를 통해 전력분석에 안전한 구조를 가지는가를 검증하고자 한다. 먼저 실험 환경으로 데이터를 분석하고 프로그램을 러닝 시킬 PC의 사양은 AMD Ryzen 7 1700X 8코어 프로세서, 메모리는 16G, 윈도우 10 환경을 기반으로 하였다. 오실로스코프의 경우 ARIA알고리즘과 AES 알고리즘은 서로 다른 오실로스코프를 사용했으며, ARIA의 경우 DPO4032모델에 1채널에는 2.0mV, 2채널에는 500mV로 트리거 신호를 주었다. Sampling Rate의 경우 2.5GS/s, Record Length는 100k로 설정하였다. AES의 경우 MSO2012B모델에 1채널에는 20.0mV, 2채널에는 2.0V로 트리거 신호를 주었다. Sampling Rate의 경우 1.00GS/s, Record Length는 100k로 설정하였다. 대상 보드는 Arduino-Uno 보드에 ATmega328 Chip을 올려서 알고리즘을 탑재한 후 사용하였으며, 소모전력을 측정하기 위해 GND에 저항을 삽입하였다. 저항의 값은 ARIA의 경우 33옴을 사용하였고, AES의 경우 10옴을 사용하여 측정하였다. 저항의 경우 대상보드가 동작하는데 문제가 없는 정도의 값을 사용하면 되기에 위와 같은 값을 설정하여 실험하였다.

본 실험에서는 각 알고리즘에 스크램블러를 적용한 후 Power Trace를 각각 1000개, 2000개, 4000개를 수집한 후 결과 값을 도출 하였다. 먼저 ARIA에 대한 결과 값을 확인(그림의 순서는 순차적으로 1000개, 2000개, 4000개이다.)하면 그림 6과 같다. 보통 암호 알고리즘에 전력분석을 시도하여 그 결과를 확인하면 최대 peak를 가지는 상관계수를 확인할 수 있으며, 특정 주기마다 파형이 크게 튀는 것을 확인할 수 있다. 하지만 본 실험에서의 결과는 전력분석을 성공적으로 차단할 수 있는가를 가늠하는 실험이기에 그림을 보면 특정하게 최대 peak를 가지는 부분

도 없이 전체적으로 비슷한 모양의 파형이 반복되는 것을 확인할 수 있으며, 이를 통해 공격이 성공적으로 방어된 것을 증명하였다.

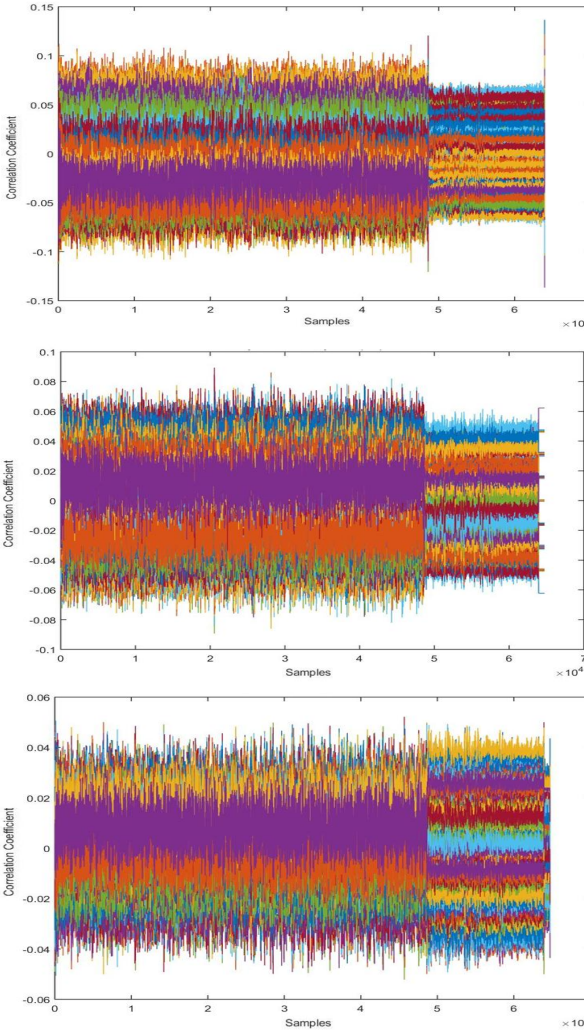

Fig. 6. ARIA Experimental results for 1000, 2000 and 4000

AES 알고리즘도 마찬가지로 스크램블러를 적용한 후 Power Trace를 각각 1000개, 2000개, 4000개를 수집한 후 결과를 도출하였으며, 아래 그림7을 보면 순서는 마찬가지로 1000개, 2000개, 4000개 순으로 나열하였다. 결과값을 살펴보면 특정한 최대 peak를 가지는 부분이 없으며 , 전체적으로 비슷한 모양의 파형이 반복되는 것을 확인할 수 있다. 이를 통해 공격이 성공적으로 차단된 것을 증명하였으며, 2000개의 결과를 잠시 보면 윗부분의 파형이 잘린 것을 확인할 수 있는데 이는 오실로스코프의 해상도 차이로 인한 부분이기에 크게 문제 되지 않을 것으로 생각된다.

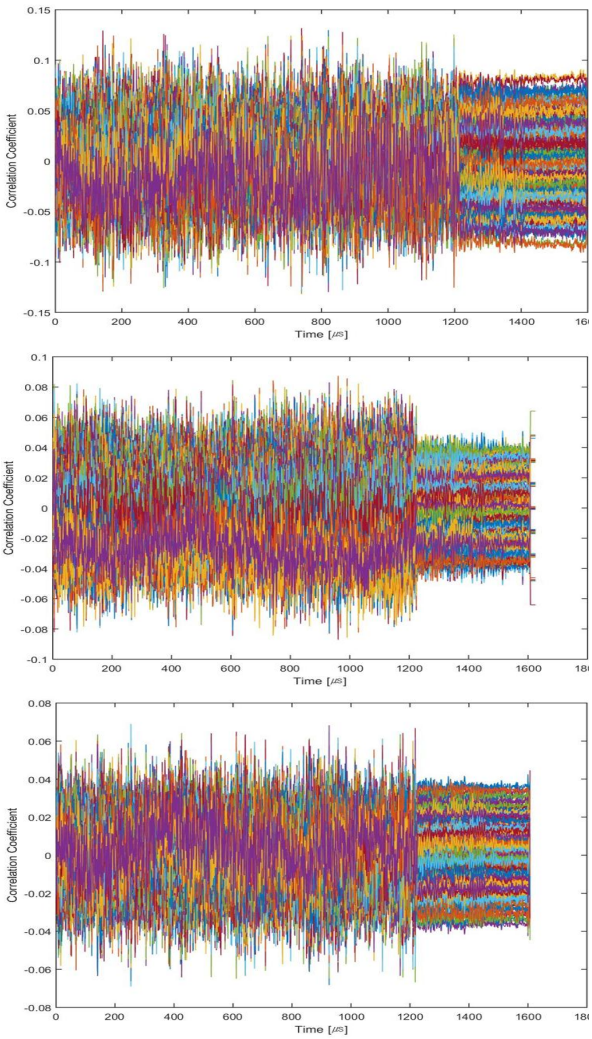

Fig. 7. AES Experimental results for 1000, 2000 and 4000

V. Conclusions

본 논문에서는 전력분석에 ARIA, AES 암호 알고리즘이 가지는 취약점을 먼저 분석하였다. 그 결과 어떠한 함수를 공격시점으로 선정하더라도 전력분석에 취약하다는 결론을 나타낼 수 있었다. 따라서 전력분석에 안전한 구조를 가질 수 있게 만드는 대응 기법이 필요함에 따라 순환구조를 가지는 LFSR을 사용한 마스킹 기법을 제안하였다. 본 제안이 전력분석에 안전한 구조인지를 검증하기 위하여 실험을 진행하였고, 그 결과 최대 peak를 가지는 부분도 없이 전체적으로 비슷한 모양의 파형이 반복되는 것을 확인하였기에 두 알고리즘 모두 전력분석에 안전한 구조를 가진다는 것을 증명하였다.

본 논문의 중점은 대상 암호 알고리즘이 전력분석에 안전한 구조를 가질 수 있는지를 우선순위로 두고 연구를 진

행하였으며, 성능의 고도화는 크게 신경 쓰지 않았기에 기존의 알고리즘보다 방어기법이 적용된 알고리즘과의 성능 차이는 어느 정도 있다고 생각된다. 차후에는 전력분석을 차단하면서도 성능고도화를 이끌어 낼 수 있는 부분을 집중적으로 연구하고자 한다.

ACKNOWLEDGEMENT

This work was supported by Institute for Information and Communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00285) and also supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (grant number: NRF-2016R1D1A1B01011908).

REFERENCES

[1] Kwon, Daesung, et al. "New block cipher: ARIA", International Conference on Information Security and Cryptology, LNCS, volume 2971, pp. 432-445, Berlin, Heidelberg, 2003.

[2] AES cryptographic algorithm, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[3] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun, “Differential Power Analysis”, In Michael Wiener, editor, Advances in Cryptology - CRYPTO ’99, volume 1666 of Lecture Notes in Computer Science, pages 388–397. Springer, December, 1999.

[4] L. Goubin, J. Paratin, "DES and differential power analysis The “Duplication” Method", CHES'99, LNCS 1717, pp.158-172, February, 1999.

[5] JungKab Seo, ChangKyun Kim, JaeCheol Ha, SangJae Moon, IlHwan Park, “Differential Power Analysis Attack of Block Cipher ARIA”, Journal of The Korea Institute of Information Security & Cryptology, Vol.15 No.l, pp. 99-106, 2005.

[6] Park, Jae Hoon, HoonJae Lee, and ManKi Ahn. "Side-channel attacks against aria on active rfid device." 2007 International Conference on Convergence Information Technology (ICCIT 2007). IEEE, pp. 2163-2168, November, 2007.

[7] Kim, ChangKyun, Martin Schläffer, and SangJae Moon. "Differential side channel analysis attacks on FPGA implementations of ARIA." ETRI journal vol. 30, no.2, pp. 315-325, April, 2008.

[8] Young Jin Kang et al., "An Experimental CPA Attack for Arduino Cryptographic Module and Analysis in Software-based CPA Countermeasures", International Journal of Security and Its Applications, Vol. 8, No.2, pp. 261-270, Apr. 2014.

[9] Zhang, Xiaoyu, et al. "Correlation power analysis for AES encryption device." 2015 4th National Conference on Electrical, Electronics and Computer Engineering, Atlantis Press, pp. 1003-1009, December, 2015.

[10] Lo, Owen, William J. Buchanan, and Douglas Carson. "Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA).", Journal of Cyber Security Technology, 1(2):88-107, 2017.

[11] Young-Jin Kang, Ki-Hwan Kim, and HoonJae Lee. "Scrambler Based AES for Countermeasure Against Power Analysis Attacks." Advanced Multimedia and Ubiquitous Engineering. Springer, Singapore, pp. 152-157, April, 2019.

Authors

Young-Jin Kang received the B.S., M.S. degree in Computer Networking from Dongseo University, Republic of Korea in 2015. Mr. Kang is now a Phd student in the ubiquitous IT department at Dongseo Graduate School in 2015. He research interests are Wireless Sensor Networks, Cryptography, Network Security, Side Channel Analysis.

Ki-Hwan Kim received the B.S., M.S. degree in Computer Networking from Dongseo University, Republic of Korea in 2015. Mr. Kim is now a Phd student in the ubiquitous IT department at Dongseo Graduate School in 2017. He research interests are cryptography, network security and Artificial Intelligent.

Hoon Jae Lee received the B.S., M.S. and Ph.D. degree in Electrical Engineering from Kyungpook national university in 1985, 1987 and 1998, respectively. Prof. Lee had been engaged in the research on cryptography and network security at Agency for Defense Development from 1987 to 1998. Since 2002 he has been working for Department of Computer Engineering of Dongseo University as an associate professor, and now he is a full professor. His current research interests are in security communication system, side-channel attack, USN & RFID security. He is a member of the Korea institute of Information security and cryptology, IEEE Computer Society, IEEE Information Theory Society and etc