JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 7 : 1276~1284 Jul. 2017

경량 블록암호 LEA에 대한 상관관계 전력분석 공격 및 마스킹 대응 기법

안효식 · 신경욱*

Correlation Power Analysis Attack on Lightweight Block Cipher LEA and Countermeasures by Masking

Hyo-Sik An · Kyung-Wook Shin*

School of Electronic Engineering, Kumoh National Institute of Technology, Gumi, Kyungbuk 39177, Korea

요 약

우리나라 경량 블록암호 표준인 LEA 알고리듬을 8-비트 데이터 패스의 하드웨어로 구현하고, 구현된 LEA-128 암호 프로세서에 대해 상관관계 전력분석 공격의 취약성을 분석하였다. 본 논문에서 적용된 CPA는 공격을 위해 가정된 라운드키 값으로 계산된 데이터의 해밍 거리와 LEA 암호 프로세서의 전력 소모량 사이의 상관 계수를 분석함으로써 올바른 라운드키 값을 검출한다. CPA 공격 결과로, 최대 상관계수가 0.6937, 0.5507인 올바른 라운드키 값이 검출되었으며, 블록암호 LEA가 전력분석 공격에 취약함이 확인되었다. CPA 공격에 대한 대응 방안으로 TRNG (True Random Number Generator) 기반의 매스킹 방법을 제안하였다. TRNG에서 생성되는 난수를 암호화 연산 중간 값에 더하는 마스킹 기법을 적용한 결과, 최대 상관계수가 0.1293와 0.1190로 매우 작아 잘못된 라운드키 값이 분석되었으며, 따라서 제안된 마스킹 방법이 CPA 공격에 강인함을 확인하였다.

ABSTRACT

Lightweight Encryption Algorithm (LEA) that was standardized as a lightweight block cipher was implemented with 8-bit data path, and the vulnerability of LEA encryption processor to correlation power analysis (CPA) attack was analyzed. The CPA used in this paper detects correct round keys by analyzing correlation coefficient between the Hamming distance of the computed data by applying hypothesized keys and the power dissipated in LEA crypto-processor. As a result of CPA attack, correct round keys were detected, which have maximum correlation coefficients of 0.6937, 0.5507, and this experimental result shows that block cipher LEA is vulnerable to power analysis attacks. A masking method based on TRNG was proposed as a countermeasure to CPA attack. By applying masking method that adds random values obtained from TRNG to the intermediate data of encryption, incorrect round keys having maximum correlation coefficients of 0.1293, 0.1190 were analyzed. It means that the proposed masking method is an effective countermeasure to CPA attack.

키워드 : 부채널 공격, 상관관계 전력분석 공격, 블록암호 LEA, 참 난수 발생기, 마스킹 기법

Key word : Side channel attack, correlation power analysis attack, block cipher LEA, TRNG, masking technique

Received 20 February 2017, **Revised** 21 February 2017, **Accepted** 09 March 2017

* **Corresponding Author** Kyung-Wook Shin(E-mail:kwshin@kumoh.ac.kr, Tel:+82-54-478-7427)
School of Electronic Engineering, Kumoh National Institute of Technology, Gumi, Kyungbuk 39177, Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.7.1276 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

최근 사물인터넷(IoT) 기술이 빠른 속도로 확산되고 있으며, 스마트 홈, 스마트 카, 헬스케어, 산업시설 제어 등 다양한 분야에 걸쳐 적용되고 있다. 세계적으로 2020년까지 인터넷에 연결되는 사물의 수는 약 260억 개로 매년 40%씩 증가할 것으로 전망되고 있다. IoT는 주변의 모든 사물에 네트워크로 직접 연결되어 정보를 수집, 저장, 전송하므로, 악의적인 보안 공격에 의해 정보가 유출되거나 조작, 변조의 위험에 처할 수 있다. IoT 기술의 응용분야가 확대됨에 따른 다양한 형태의 보안 위협이 증가하고 있으며, IoT 기기의 확산속도에 비해 보안 기술의 적용이 미비해 IoT 관련 범죄가 증가할 것으로 전망되고 있다[1,2].

IoT 보안은 경량 암호・인증 및 이기종 네트워크 보안관리, 프라이버시 보호 등 다양한 보안기술이 요구되며, 디바이스 보안, 네트워크 보안 그리고 서비스 환경에 관련된 보안 등 크게 세 가지 영역으로 구분된다. IoT 디바이스 보안은 기존의 보안기술을 계승하여 경량화된 블록 암호 및 공개키 암호 알고리듬을 기반으로 하며, 최근에는 IoT 환경에 적합하도록 개발된 경량 블록 암호 알고리듬으로 LEA, PRESENT와 공개키 암호인 타원곡선 암호가 활발하게 구현되고 있다[3-6].

1996년 Paul C. Kocher에 의해 공개키 알고리듬에 대한 시차분석 공격[7]이 제시된 이래로 전력분석 공격[8], 전자기파분석 공격[9], 오류 주입 공격[10] 등 다양한 부채널 공격방법이 제시되었다. 특히, 전력분석 공격은 강력한 부채널 공격방법 가운데 하나이다. AES, LEA, PRESENT 등의 블록암호 알고리듬은 전력분석 공격에 취약성이 발견되고 있으며, 전력분석 공격에 대응하기 위한 다양한 기법들이 소개되고 있다[11-13].

본 논문에서는 우리나라 국가 표준으로 채택된 128-비트 블록암호 알고리듬 LEA에 대해 IoT 환경에 적합하도록 저면적의 8-비트 데이터 패스를 갖는 LEA 프로세서를 설계하고, 부채널 공격 방법 중 하나인 상관관계 전력분석 공격으로 비밀키 정보의 획득이 가능함을 실험으로 보였다. 또한, 부채널 공격에 대한 대응 방안으로 링 오실레이터 기반의 TRNG(True Random Number Generator)와 마스킹 기법을 제안하고, LEA 프로세서에 적용하여 상관관계 전력분석 공격에 강한 내성을 가짐을 실험적으로 확인하였다.

Ⅱ. 전력분석 공격

암호 알고리듬이 구현된 장치에서 암호화 연산이 수행될 때 누출되는 전력소모량은 내부 데이터 변화를 간접적으로 알려주는 부채널 정보이며, 전력분석에 의해 비밀 정보가 노출될 수 있다. CYPTO'99에서 Paul C. Kocher에 의해 단순 전력분석(simple power analysis; SPA)과 차분 전력분석 (differential power analysis; DPA) 공격 방법이 제시되었다[8].

차분 전력분석 공격은 전력소모 파형을 분석하는 것뿐만 아니라, 전력 소모량과 비밀키의 상관관계를 통계적인 방법으로 분석한다. 분석을 위해 암호장치가 임의의 평문 P와 비밀키 K를 이용하여 암호화 연산을 수행할 때의 전력소모 파형을 수집하여 표본화하고, 추측한 비밀키를 이용하여 연산을 수행하고, 분류 함수에 따라 전력소모 파형을 분류하여 평균의 차분 신호를 구한다. 상관관계 전력분석 공격(correlation power analysis; CPA)은 차분 전력분석 공격과 달리, 비밀키를 추정하여 얻은 암호화 연산 중간값을 해밍무게(hamming weight) 모델 또는 해밍거리(hamming distance) 모델로 변환한다[14].

해밍무게 모델은 소프트웨어로 구현된 암호장치에 적용되는 전력소모 모델로서 '1'의 값을 갖는 비트 수와 소비전력이 동일한 패턴을 갖는다는 모델이다. 해밍거리 모델은 하드웨어로 구현된 암호장치에 적용되는 전력소모 모델이며, 스위칭된 비트의 개수와 소비전력이 동일한 패턴을 갖는다는 모델이다. 두 비트열 $R0, R1$에 대한 해밍거리 모델은 식 (1)과 같이 $HD(R0, R1)$으로 나타내며, HW은 해밍무게 모델을 나타낸다.

$$HD(R0, R1) = HW(R0 \oplus R1) \quad (1)$$

CMOS 회로로 구현된 하드웨어 장치는 출력이 0→1로 스위칭 될 때 전원으로부터 전류가 흐르며, 1→0로 스위칭 될 때는 출력 커패시터에 저장되어있던 전류가 흘러 전력소모가 일어난다. 따라서 특정 비트의 스위칭 전력소모는 식 (2)와 같이 모델링할 수 있다.

$$W = a \cdot HD(R0, R1) + b \quad (2)$$

W는 총 전력 소모량이며, a는 전력 소모량과 해밍거리

모델 간의 스칼라 이득 값이며, b는 암호화 연산과 상관없이 발생하는 오프셋과 잡음 성분으로 구성된 전력 소모량이다.

상관관계 전력분석 공격은 추측된 비밀키를 사용하여 계산된 암호화 연산 중간값을 해밍거리 모델로 변환한 값과 실제 측정된 소모전력과의 상관관계를 계산하여 올바른 비밀키를 분석한다. 상관관계 계산방법은 식 (3)과 같이 정의된다.

$$corr(x,y) = \frac{E(xy)-E(x)E(y)}{\sqrt{VAR(x)\,VAR(y)}} = \frac{\sum_{n=1}^{N}(x_n-E(x))(y_n-E(y))}{\sqrt{\sum_{n=1}^{N}(x_n-E(x))^2 \cdot \sum_{n=1}^{N}(y_n-E(y))^2}} \quad (3)$$

식 (3)을 통해 계산된 상관계수는 -1과 1 사이의 값을 갖는다. -1과 1에 가까울수록 각각 음, 양의 상관관계를 가지며, 두 분포 사이에 연관성이 없다면 상관계수는 0에 가까워진다. 실제 소모전력과 변환된 해밍거리 모델은 모두 비트의 스위칭에 관계되므로, 양의 상관관계를 가진다. 추측된 비밀키를 사용해서 계산된 상관계수가 가장 높을 때, 추측된 비밀키를 옳은 비밀키로 판단한다.

Ⅲ. LEA-128 암호화 프로세서 설계

블록암호 알고리듬 LEA는 국가보안기술연구소에서 개발한 128-비트 블록암호 알고리듬이다[4]. LEA의 라운드 함수는 32-비트 ARX(Addition, Rotation, XOR) 연산으로 구성되며, 비선형 치환함수인 S-box를 사용하지 않아 경량 구현이 가능하다.

본 논문에서는 LEA에 대한 전력분석 공격 모의실험을 위해 평문을 128-비트 비밀키로 암호화하여 암호문을 생성하는 LEA-128 암호화 프로세서를 8-비트 데이터 패스로 설계하였다. 설계된 LEA-128 암호화 코어는 그림 1의 구조를 가지며, 라운드 블록, 키 스케줄 블록, 제어 블록으로 구성된다. 라운드 블록과 키 스케줄 블록을 8-비트 데이터 패스 구조로 설계하였으며, 평문과 비밀키가 입력되는 핀이 공유되도록 하였다.

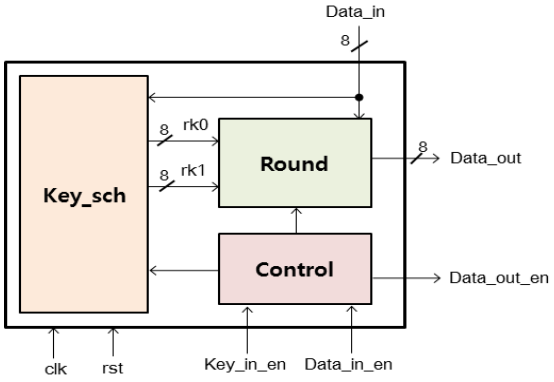

Fig. 1 LEA-128 encryption processor

LEA-128의 라운드 함수는 32-비트 단위의 ARX 연산으로 구성되므로, 8-비트 단위의 ARX 연산을 구현하기 위해서는 구조적인 변경이 필요하다. 8-비트 데이터 패스로 구현된 라운드 블록은 그림 2와 같으며, 8-비트 상태 레지스터 16개($X[00] \sim X[33]$)와 XOR, 모듈로 덧셈 및 1-비트 캐리보존 레지스터로 구성된다.

32-비트 데이터패스 구조에서는 라운드키 가산과 비트 순환이동 후, 상태 레지스터에 업데이트된다. 32-비트 순환이동이 8-비트 데이터 패스에서 처리되기 위해 4-클록이 필요하다. 본 논문의 8-비트 데이터패스 구조에서는 라운드키 가산과 상태 레지스터에 업데이트되고 4-클록에 걸쳐 쉬프트 되는 동안에 비트 순환이동이 이루어지도록 구현하였으며, 이를 통해 추가적인 레지스터 없이 비트 순환이동이 수행되도록 최적화 하였다.

암/복호화 라운드 연산에 사용되는 라운드키는 키 스케줄에 의해 생성된다. 생성된 라운드키는 내부 상태 레지스터에 저장되어 선택적으로 8-비트 크기로 출력된다. 그림 3은 구현된 LEA-128 암호화 프로세서의 기능검증 결과이다. 문헌[4]의 표준에 제시된 128-비트의

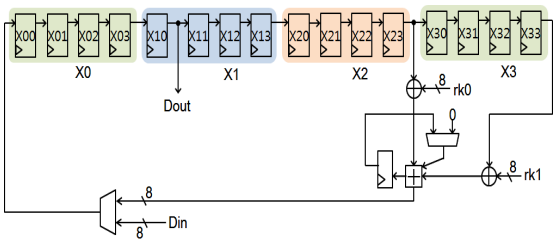

Fig. 2 LEA-128 round block implemented with 8-bit data-path

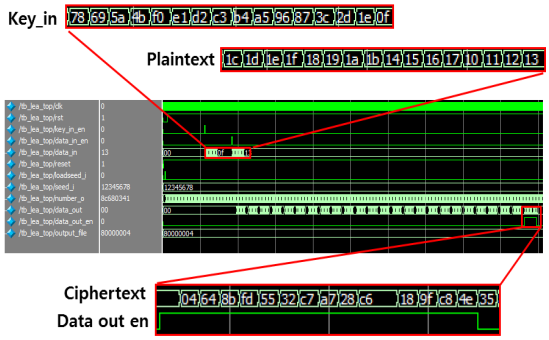

Fig. 3 Simulation result of LEA encryption processor

평문 “0x10111213_14151617_18191a1b_1c1d1e1f”와 비밀키 “0x0f1e2d3c_4b5a6978_8796a5b4_c3d2e1f0”를 검증용 테스트 벡터로 사용하였다. 기능 검증결과로 암호문 “0x9fc84e35_28c6c618_5532c7a7_04648bfc”가 출력되어 구현된 LEA-128 프로세서의 기능이 정상 동작함을 확인하였다.

설계된 LEA-128 암호 코어에 대한 전력분석 공격 모의실험을 위해 0.18-㎛ CMOS 표준셀을 사용하여 레이아웃을 설계하였다. 그림 4는 Astro 툴을 사용하여 Auto P&R 방식으로 설계된 레이아웃 도면이다. 레이아웃으로부터 기생(parasitic) RC가 포함된 네트리스트를 추출하고, 시뮬레이션을 통해 전력소모 파형 측정하였다.

Ⅳ. LEA-128에 대한 전력분석 공격

4.1. LEA에 대한 상관관계 전력분석 공격

설계된 LEA-128 암호 프로세서에 대해 상관관계 전력분석 공격은 그림 5의 과정으로 진행하였다. 임의의

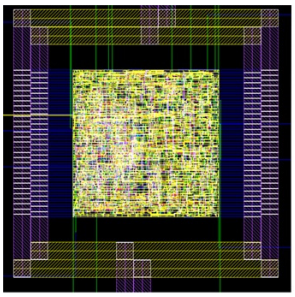

Fig. 4 Layout of LEA-128 encryption processor

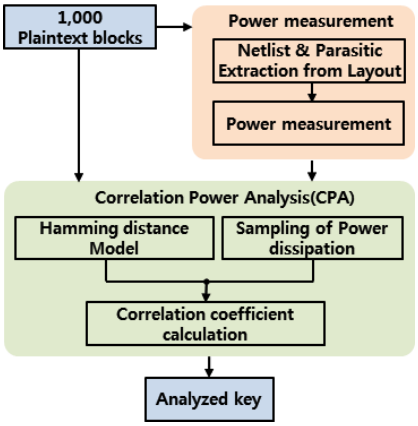

Fig. 5 Flow of correlation power analysis attack

평문 1,000개에 대하여 암호화 연산 중 발생하는 소비전력 측정을 위해 레이아웃에서 추출된 게이트 레벨 네트리스트를 이용하여 PrimeTime- PX로 전력소모 파형을 측정한다.

상관계수 계산을 위해 소비전력 측정에 사용된 임의의 평문 1,000개와 추측된 비밀키를 사용하여 계산된 암호 연산 중간값에 따른 소모전력 모델을 생성하기 위해 해밍거리 모델로 변환한다. 다음으로, 측정된 전력소모 파형을 표본화한다. 암호화 과정에서 특정 시점에 사용된 라운드키를 분석하기 위해서는 그 시점의 전력소모 파형과 해밍거리 모델 간의 상관관계를 분석해야 하므로, 라운드키가 사용된 시점의 전력소모 파형만을 표본화한다.

본 논문에서는 그림 6의 실선과 점선의 경로를 따라 연산되어 출력 레지스터 Dout에 저장된 값의 변화에 따른 실제 전력소모량과 해밍거리 모델 간의 상관계수 계산을 통해 라운드키를 분석하였다. 출력 레지스터는 다른 레지스터에 비해 부하 커패시턴스 용량이 비교적 크기 때문에 LEA-128 코어의 전체 전력소모량에서 차지하는 비중이 높아 분석 위치로 적합하다.

입력된 128-비트 평문은 암호화 연산이 수행되기 전 내부 레지스터에 저장되어 있으며, $X[23], X[33]$에 저장된 평문은 실선의 경로를 따라 라운드키 가산이 이루어지고 모듈로 덧셈 이후에 $X[00]$ 레지스터에 저장된다. 이후 실선 경로를 따라 비트 순환이동이 이루어지고 출력 레지스터로 쉬프트 된다.

해밍거리 모델에 사용되는 라운드키 $rk0, rk1$는 키

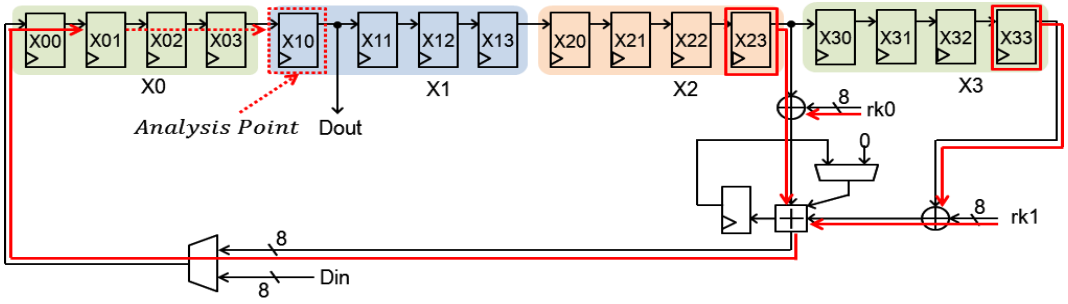

Fig. 6 Signal path for correlation power analysis

스케줄 블록에서 생성된 라운드키 가운데 선택적으로 입력되는 8-비트 값이다. 추측 가능한 라운드키 조합 $2^8 \times 2^8$개에 대해 해밍거리 모델값을 계산한다.

4.2. 상관계수 계산

상관계수는 다음의 3단계 과정으로 계산되며, 상관계수 계산 결과가 1에 가장 근접 할 때, 상관계수 계산에 사용된 라운드키를 옳은 라운드키로 판단한다.

(1) 임의의 평문 1,000개에 대한 암호화 연산의 전력소모량 W를 측정 및 표본화

(2) $2^8 \times 2^8$개의 라운드키 조합에 대해 그림 6에 표시된 경로의 해밍거리 값 HD를 계산

(3) 계산된 HD와 W를 식 (4)에 대입하여 상관계수 r을 계산(단, $\overline{HD}$ 와 $\overline{W}$는 평균값을 나타냄)

$$r = \frac{\sum (HD - \overline{HD})(W - \overline{W})}{\sqrt{\sum (HD - \overline{HD})^2}\sqrt{\sum (W - \overline{W})^2}} \quad (4)$$

4.3. CPA 공격 결과

본 실험에 사용된 비밀키는 “0x0f1e2d3c_4b5a6978_8796a5b4_c3d2e1f0”이며, 키 스케줄링을 통해 생성된 최초 192-비트 라운드키는 “0x003a0fd4_02497010_194f7db1_02497010_090d0883_02497010” 이다.

그림 7은 CPA 공격 실험결과를 보인 것이다. 그림 7-(a)는 최대 상관계수 0.6937로 계산된 라운드키 $RK_{i,4}^{enc}$의 최하위 8-비트($RK_{i,4}^{enc}[7:0]$)인 0x83과 $RK_{i,5}^{enc}$의 최하위 8-비트($RK_{i,5}^{enc}[7:0]$)인 0x10이 분석되었음을 보이고 있다. 그림 7-(b)는 최대 상관계수 0.5507로 계산된 라운드키 $RK_{i,4}^{enc}$의 나머지 하위 8-비트($RK_{i,4}^{enc}[15:8]$)인 0x08과 $RK_{i,5}^{enc}$의 나머지 하위 8-비트($RK_{i,5}^{enc}[15:8]$)인 0x70이 분석되었음을 보이고 있다. 두 번의 분석으로 $RK_{i,4}^{enc}$의 하위 16-비트($RK_{i,4}^{enc}[15:0]$)인 0x0883과 $RK_{i,5}^{enc}$의 하위 16-비트 ($RK_{i,5}^{enc}[15:0]$)인 0x7010이 정확하게 분석되어 LEA- 128 암호 코어에 대한 CPA 공격이 성공하였음을 확인할 수 있다.

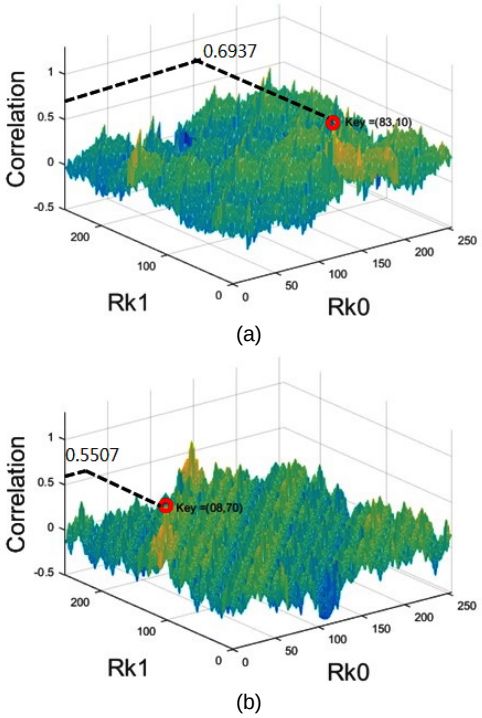

Fig. 7 Recovering correct round keys by CPA attack for LEA-128 encryption processor (a) $RK_{i,4}^{enc}[7:0]$, $RK_{i,5}^{enc}[7:0]$ (b) $RK_{i,4}^{enc}[15:8]$, $RK_{i,5}^{enc}[15:8]$

Ⅴ. CPA 대응을 위한 마스킹 기법

CPA 공격은 실제 측정된 소모전력 파형과 공격자가 모델링한 암호화 중간값의 해밍거리 모델 간의 관련성을 분석하는 방법이다. 따라서 소모전력과 해밍거리 모델 간의 상관관계를 제거하는 것이 효과적인 대응 방안이다. 주로 사용되는 대응 방법으로는 암호화 연산 중간값에 난수를 더하는 마스킹(masking) 기법과 비트 스위칭에 따른 전력 소모량을 일정하게 하는 하이딩 기법 등이 있다. 특히 마스킹 기법은 구현과 적용이 쉬워 암호 시스템에서 많이 사용된다[11].

5.1.난수 발생기 설계

마스킹 기법을 적용하기 위해서는 난수 발생기가 필요하다. 난수 발생기는 구현 방법에 따라 참 난수 발생기(true random number generator; TRNG)와 유사 난수 발생기(pseudo random number generator; PRNG)로 분류된다. PRNG는 시드(seed)를 입력받아 난수 생성 알고리듬을 기반으로 유사 난수를 생성하며, TRNG는 방사성 물질이나 링 오실레이터(ring oscillator; RO)의 지터(jitter) 같은 예측이 불가능한 비결정적인 잡음원을 사용하여 난수를 생성한다.

본 논문에서는 하드웨어 환경에서 구현이 쉬운 RO 샘플링 방법 기반 TRNG을 구현한다[15]. 난수 발생기는 잡음원와 후처리 단계로 구성된다. 엔트로피 소스는 난수성의 원천이며, 후처리 단계는 엔트로피 소스로부터 추출된 비트열에 대해 편차 성분과 비난수성(non-random) 요소를 제거하는 기능을 한다. 후처리 단계는 PRNG와 유사하게 알고리듬 기반으로 난수성을 높이며, 해시(hash) 함수나 선형귀환 시프트 레지스터(linear feedback shift register; LFSR) 등을 이용한다.

RO 기반 엔트로피 소스는 홀수개의 인버터로 구성된 RO들의 출력을 XOR 트리로 묶고, 시스템의 정규 클록 신호를 사용하여 샘플링 한다. 샘플링된 값은 RO의 지터에 의해 불확실한 값을 갖는 천이 구간과 그렇지 않은 구간이 포함되어있으며, 불확실한 값을 갖는 구간의 비율을 fill rate f라고 한다. 일반적으로 f는 RO의 주기 대비 지터 비율이 높거나, RO의 개수가 많을수록 높아지며 난수 생성에 좋은 특성을 갖는다. 하지만 f=1에 가깝게 구현하기 위해서는 높은 구현 비용이 필요하므로, 성능과 면적간의 교환조건 관계를 고려하여 구현

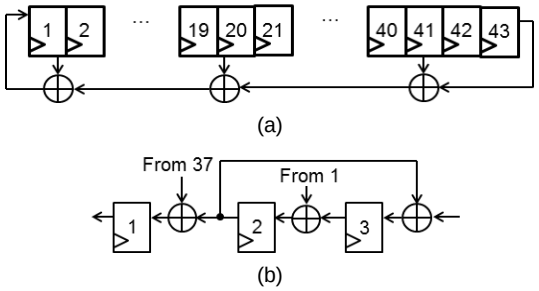

Fig. 8 Post-processing of TRNG (a) 43-b LFSR, (b) 37-b CASR

하는 것이 바람직하다. 본 논문에서는 인버터의 개수가 3, 5, 7, 11, 13, 17, 19개인 RO를 각각 20개 사용하여 엔트로피 소스을 구현하였다.

후처리 단계에서는 임의의 길이의 데이터를 고정된 길이로 매핑하는 해쉬 함수, 큰 주기를 갖는 비트열을 생성하는 LFSR 등이 주로 사용된다. 본 논문에서는 그림 8(a),(b)의 43-비트 LFSR과 37-비트 CASR를 사용하였다. 43-비트 LFSR은 $x^{43}+x^{41}+x^{20}+x+1$의 특성 다항식을 가지며, 최대 사이클 길이 $2^{43}-1$와 편차 2^{-43}을 갖는다. 37-비트 CASR의 동작은 식 (5)와 같으며, 최대 사이클 길이 $2^{37}-1$와 편차 2^{-37}을 갖는다.

$$a_i(t+1) = a_{i-1}(t) \oplus a_{i+1}(t) \tag{5}$$

본 논문에서는 그림 9와 같이 TRNG를 설계하였으며, 후처리 단계는 최대 사이클 길이 $2^{80}-2^{43}-2^{37}+1$와 편차 2^{-80}을 갖는다. 43-비트 LFSR의 하위 8-비트와 37-비트 CASR의 하위 8-비트를 XOR하여 마스크 값으로 사용하며, 1회의 암호연산이 완료되면 새로운 마스크 값이 사용된다.

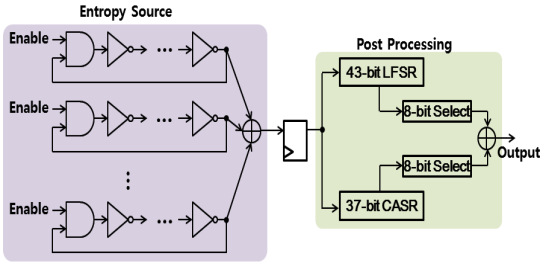

Fig. 9 TRNG using ring oscillator

Table. 1 Verification results of randomness of TRNG

	FIPS 140-2	This paper
Monobit test	9725 < x < 10275	9852
Runs test	length of run 1 2343-2657 2 1135-1365 3 542-708 4 251-373 5 111-201 6+ 111-201	length of run 1 2424 2 1209 3 609 4 341 5 160 6+ 156
Long run test	< 26	13

생성된 난수는 표 1과 같이 FIPS 140-2의 기준[16]을 적용하여 Monobit 테스트, Runs 테스트, Long run 테스트를 진행하였다. Monobit 테스트는 비트열에서 '1'의 개수이며, Runs 테스트는 '0' 또는 '1'로만 구성된 연속적인 비트들의 개수이다. Long run 테스트는 동일한 비트로 구성된 연속적인 비트의 최대 길이이다. 출력된 난수를 20,000 비트로 구성된 비트열로 변환한 후, 각각의 테스트 방법을 적용하여 기준 만족 여부를 판단한 결과, 구현된 TRNG는 FIPS 140-2 기준을 만족하는 것으로 평가되었다.

5.2. 마스킹 기법을 적용한 라운드 회로 설계

LEA 암호 프로세서의 라운드 블록에서 소모되는 전력과 암호화 연산 중간값의 해밍거리 모델과의 상관관계를 제거하기 위해 그림 10과 같이 라운드 블록에 마스킹 기법을 적용하였다. 마스크 값은 TRNG로부터 8-비트 난수값을 16-클록에 걸쳐 입력받아 32-비트 레지스터 mask_1, mask_2, mask_3, mask_4에 저장되며, 그림 10에 적용되는 8-비트 마스크 값 m1, m2, m3, m4를 출력한다. 해당 8-비트 값은 매 클록마다 순차적으로 바뀌며, 32-비트 레지스터의 [7:0], [15:8], [23:16], [31:24]

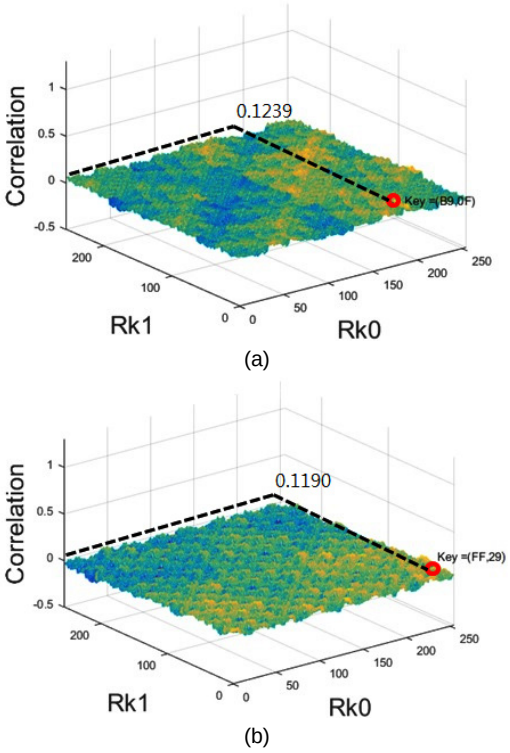

Fig. 11 Recovering incorrect round keys by CPA attack for LEA-128 encryption processor with masking circuit (a) $RK_{i,4}^{enc}[7:0]$, $RK_{i,5}^{enc}[7:0]$ (b) $RK_{i,4}^{enc}[15:8]$, $RK_{i,5}^{enc}[15:8]$

의 값이다. m5, m6, m7은 적용된 마스크 값을 해제하는데 사용되는 값이며, m5=m7⊕m2⊕m3, m6=m7⊕m2⊕m3⊕m4의 관계를 갖는다.

5.3. 마스킹 적용 회로에 대한 CPA 공격 결과

실험에 사용된 비밀키는 4.3절에서와 동일한 값 "0x0f1e2d3c_4b5a6978_8796a5b4_c3d2e1f0"이며, 키

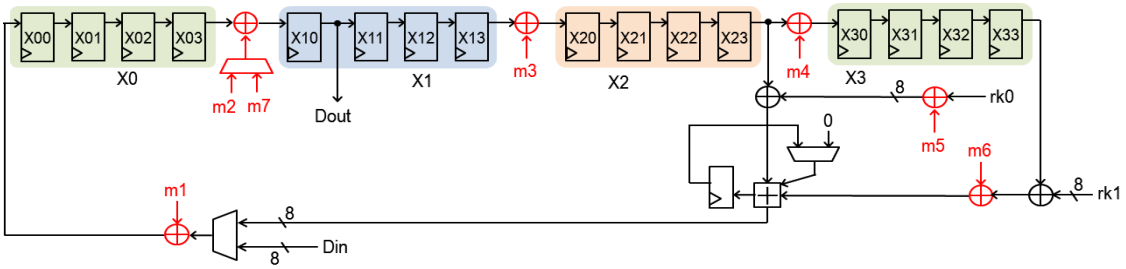

Fig. 10 CPA-path with masking

스케줄링을 통해 생성된 최초 192-비트 라운드키는 “0x003a0fd4_02497010_194f7db1_02497010_090d0883_ 02497010” 이다.

그림 11은 마스킹 적용 회로에 대한 CPA 공격 결과이다. 매스킹에 의해 매우 낮은 상관계수 값이 얻어졌으며, CPA 공격을 통한 비밀키 획득이 불가능함을 확인할 수 있다. 그림 11-(a)는 최대 상관계수 0.1239로 계산된 라운드키 $RK_{i,4}^{enc}$의 최하위 8-비트($RK_{i,4}^{enc}[7:0]$)는 0xb9, $RK_{i,5}^{enc}$의 최하위 8-비트($RK_{i,5}^{enc}[7:0]$)는 0x0f로 분석되었음을 보이고 있다. 그림 11-(b)는 최대 상관계수 0.1190으로 계산된 라운드키 $RK_{i,4}^{enc}$의 나머지 하위 8-비트($RK_{i,4}^{enc}[15:8]$)는 0xff, $RK_{i,5}^{enc}$의 나머지 하위 8-비트($RK_{i,5}^{enc}[15:8]$)는 0x29로 분석되었음을 보이고 있다. 분석된 라운드키 값들은 모두 잘못된 값이며, 본 실험 결과를 통해 마스킹 기법이 적용된 LEA-128 코어는 CPA 공격에 안전하다는 것이 확인되었다.

Ⅵ. 결 론

본 논문에서는 IoT 환경에 적합한 8-비트 데이터 패스를 갖는 LEA-128 암호 프로세서를 설계하고, 설계된 LEA-128 암호 프로세서에 대해 CPA 공격 실험을 했다. 두 개의 라운드 변환에 대한 전력분석 공격의 결과로, 최대 상관계수 0.6937과 0.5507을 갖는 하위 16비트의 라운드키 값이 얻어졌으며, 올바른 킷값으로 확인되었다. 전력분석 공격에 대한 대응 방안으로 마스킹 기법을 적용하였다. 링 발진기 기반의 참 난수발생기를 구현하고, 생성된 난수를 라운드 블록에 마스크 값으로 적용하였다. 마스킹 기법을 적용한 LEA 암호 프로세서에 CPA 공격 실험을 진행한 결과, 최대 상관계수 0.1293, 0.1190를 갖는 잘못된 라운드키 값이 얻어졌다.

본 논문의 매스킹 기법을 적용한 LEA 암호 프로세서는 상관관계 전력분석 공격에 라운드키 값이 노출되지 않는 안전성이 확인되었으며, 경량화된 암호 장치를 필요로 하는 IoT 시스템의 디바이스 보안 SoC 개발에 효과적으로 사용될 수 있을 것으로 평가된다.

REFERENCES

[1] J. Ambareen, P. G. Shah and M. Prabhakar, “A Survey of Security in Internet of Things – Importance and Solutions,” *Indian Journal of Science and Technology*, vol. 9, no. 45, pp. 1-7, Dec. 2016.

[2] IoT Information Security Roadmap, Ministry of Science, ICT and Future Planning, Oct. 2014.

[3] M. J. Sung and· K. W. Shin, “An Efficient Hardware Implementation of Lightweight Block Cipher LEA-128/ 192/ 256 for IoT Security Applications,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 19, no. 7, pp. 1608-1616, Jul. 2015.

[4] TTAK.KO-12.0223, *128-bit Block Cipher LEA*, Telecommunications Technology Association (TTA), 2013.

[5] W. L. Cho, K. B. Kim and K. W. Shin, “A Hardware Design of Ultra-Lightweight Block Cipher Algorithm PRESENT for IoT Applications,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 20, no. 7, pp. 1296-1302 Jul. 2016.

[6] H. A. Selma and H. M’hamed, “Elliptic curve cryptographic processor design using FPGAs,” *Proceedings of the IEEE 2015 International Conference on Control, Engineering & Information Technology (CEIT)*, Univ. of Tlemcen Tlemcen, Algeria, pp. 1-6, 2015.

[7] P. Kocher, “Timing attacks on implementations of Diffie-Hellmann,” *Proceedings of the 16th Annual International Cryptology Conference (CRYTO’96)*, Santa Barbara, California, USA, pp. 104-113, 1996.

[8] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” *Proceedings of the 19th Annual International Cryptology Conference (CRYPTO’99)*, Santa Barbara, California, USA, pp. 388-397, 1999.

[9] K. Gandolfi, C. Mourtel, and F. Olivier, “Electromagnetic analysis: Concrete results,” *Proceedings of the Cryptographic Hardware and Embedded Systems (CHES 2001)*, Paris, France, pp. 251- 261, 2001.

[10] E. Biham, A. Shamir, “Differential fault analysis of secret key cryptosystems,” *Proceedings of the 17th Annual International Cryptology Conference (CRYPTO'97)*, Santa Barbara, California, pp. 513-525, 1997.

[11] M. Masoumi, P. Habibi and M. Jadidi, “Efficient Implementation of Masked AES on Side-Channel Attack Standard Evaluation Board,” *Proceedings of the International Conference on Information Society (i-Society 2015)*,

London, England, pp. 151-156, 2015.

[12] J. Choi and Y. Kim, “An improved LEA block encryption algorithm to prevent side-channel attack in the IoT system,” *Proceedings of the 2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*, Jeju, Korea, pp. 1-4, 2016.

[13] X. Duan, Q. Cui, S. Wang, H. Fang and G. She, “Differential Power Analysis Attack and Efficient Countermeasures on PRESENT,” *Proceedings of the 2016 8th IEEE International Conference on Communication Software and Networks*, Beijing, China, pp. 8-12, 2016.

[14] E. Brier, C. Clavier, and F. Oliver, “Correlation Power Analysis with a Leakage Model”, *Proceedings of the Cryptographic Hardware and Embedded Systems (CHES 2004)*, MA, USA, pp. 16-29, 2004.

[15] B. Sunar, W. J. Martin and D. R. Stinson, “A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks,” *IEEE Transactions on Computers*, vol. 56, no. 1, pp. 109-119, Jan. 2007.

[16] FIPS PUB 140-2, *security requirements for cryptographic modules*, National Institute of Standard and Technology (NIST), 2001.

안효식(Hyo-Sik An)

2014년 8월 금오공과대학교 전자공학부(공학사)
2017년 2월 금오공과대학교 전자과(공학석사)
2017년 2월 ~ 아이쓰리시스템(연구원)
※관심분야 : 통신 및 신호처리용 반도체 IP 설계, 정보보호용 반도체 IP 설계

신경욱(Kyung-Wook Shin)

1984년 2월 한국항공대학교 전자공학과(공학사)
1986년 2월 연세대학교대학원 전자공학과(공학석사)
1990년 8월 연세대학교대학원(공학박사)
1990년 9월~1991년 6월 한국전자통신연구소 반도체연구단(선임연구원)
1991년 7월~현재 금오공과대학교 전자공학부(교수)
1995년 8월~1996년 7월 University of Illinois at Urbana-Champaign(방문교수)
2003년 1월~2004년 1월 University of California at San Diego(방문교수)
2013년 2월~2014년 2월 Georgia Institute of Technology(방문교수)
※관심분야 : 통신 및 신호처리용 SoC 설계, 정보보호 SoC 설계, 반도체 IP 설계