경량 블록 암호 PIPO에 대한 상관관계 전력분석 공격

심민주*, 김현준**, 서화정*†

*한성대학교 IT융합공학부 (대학원생)

**한성대학교 정보컴퓨터공학과 (대학원생)

*† 한성대학교 IT융합공학부 (교수)

Correlation Power Analysis Attack on Lightweight Block Cipher PIPO

Min-Joo Sim*, Hyun-Jun Kim**, Hwa-Jeong Seo*†

*Hansung University, Department of IT Convergence Engineering (Graduate student)

**Hansung University, Department of Information Computer Engineering (Graduate student)

*† Hansung University, Department of IT Convergence Engineering (Professor)

요 약

다양한 통신환경에서 보안 요소와 성능을 충족시키기 위해서 경량 블록 암호 알고리즘이 필요하다. 이론적인 안전성이 증명된 국산 블록 암호 알고리즘으로는 SEED, ARIA, HIGHT, LEA가 있다. 최근 ICISC 2020에서 처음 국산 경량 블록 암호 PIPO가 발표되었다. 본 논문에서는 PIPO에 대한 상관관계 전력분석 공격을 시도하여 PIPO가 부채널 공격에 대한 취약성을 갖고 있음을 증명한다.

I. 서론

사물인터넷(IoT) 환경에서 다양한 장비에서 인터넷 통신이 가능하다. 다양한 통신환경에서 보안 요소와 성능을 충족시키기 위한 경량 블록 암호 알고리즘이 필요하다. 다양한 환경에서의 적절한 알고리즘의 필요성이 요구되어 여러 경량 블록 알고리즘이 제안이 되고 있다. 이론적인 안전성이 증명된 국산 블록 암호 알고리즘으로는 SEED, ARIA, HIGHT, LEA가 있다. 하지만 블록 암호에서 부채널 분석에 취약점이 존재한다[1,2]. 최근 ICISC 2020에서 처음 발표된 국산 경량 블록 암호 PIPO가 발표되었다[3]. 본 논문에서는 새로 발표된 PIPO-64/128에 대한 전력분석 공격 실험을 통하여 마스터키 값을 획득할 수 있음을 확인하였다. 해당 실험은 XMEGA 보드에서 동작하는 PIPO 알고리즘을 대상으로 전력분석을 수행하였다.

본 논문의 구성은 다음과 같다. 2장에서 PIPO에 대한 소개 및 전력분석 공격 방법에 대해 간략하게 서술한다. 3장은 PIPO-64/128이 갖는 보안 취약점을 이용한 공격 방법을 최초로 제시한다. 마지막으로 4장에서 본 논문에 대한 결론을 내린다.

II. 관련 연구

2.1 경량 블록 암호 PIPO 알고리즘

ICISC 2020에서 발표된 PIPO는 Plug-In과

Plug-Out의 약자로, 각각 부채널 보호 환경과 비보호 환경에서 사용된다. Table 1.은 키 사이즈에 따른 PIPO의 설명이다.

Cipher	Size of blocks	Key length	Number of rounds
PIPO-128	64	128	13
PIPO-256	64	256	17

Table 1. Specification of PIPO

단순한 형태로 더 작은 S-box를 조합한 Unbalanced-Bridge 구조의 S-Layer로 Fig. 1.과 같이 구성된다.

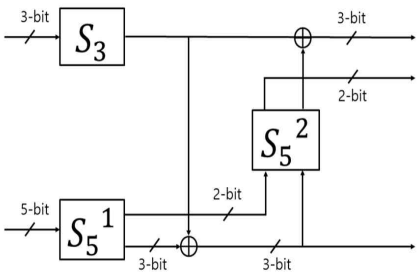

Fig. 1. Unblanced-Bridge

PIPO의 전체적인 구조는 Fig. 2.에서 확인할 수 있다. PIPO의 각 라운드는 S-Layer로 표현된 비선형 레이어, R-Layer로 표현된 선형 레이어, 라운드 키와 상수의 XOR 연산으로 구성된다. 라운드 키도 단순하게 키를 평문의 길이처럼 64bit로 나눠 반복된 키를 사용한다.

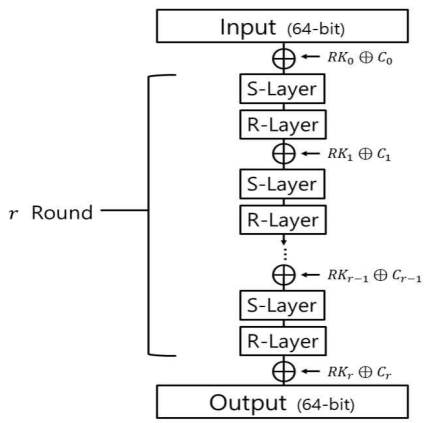

Fig. 2. PIPO overall structure

여기서 RK_0은 whitening 키이며, $RK_1, RK_2, \cdots, RK_r$은 라운드 키이다. S-Layer는 8개의 동일한 8bit s-box(S8)를 병렬로 실행한다. R-Layer는 각 행의 비트를 주어진 오프셋으로 회전시킨다[3].

2.2 상관관계 전력분석 공격

전력분석 공격은 보통 데이터 수집 단계와 데이터 분석 단계 총 2단계를 거쳐 공격이 진행된다. 먼저 데이터 수집 단계에서는 랜덤하게 선택된 평문을 이용하여 암호화 연산을 수행한 후, 해당 연산에 대한 소비전력 파형을 수집한다. 이후 데이터 분석 단계에서 비밀키 일부분에 대한 그 값을 예측한 후, 예측값과 입력된 평문을 이용하여 내부 연산 값을 계산한다. 이렇게 얻은 계산 값의 유효성을 수집된 전력 소비 파형을 이용하여 검증하는 과정을 반복하면서 비밀키 전체 값을 복구한다[4].

상관관계 전력분석 공격(correlation power analysis, CPA)은 암호 모듈을 계속 동작시키고 고정된 비밀키에 다른 평문을 입력으로 넣어 암호문을 얻는 동시에 파형 수집 장치를 통해 파형들을 수집한다. 수집된 파형, 평문, 암호문을 통해 설계된 분류 함수를 기준으로 파형 통계 처리하여 분석하는 방식이다[5].

III. 실험 결과

실험은 PIPO-64/128를 대상으로 8bit 프로세스 XMEGA 보드에 Chipwhisperer를 사용하여 13라운드의 S-box의 파형을 10,000개 수집하였다. 실험 결과의 효율성을 위해 마스터키값을 고정 값으로 놓고 진행하였다. CPA 공격을 진행하기 위해서 비트 단위 병렬로 S-Layer가 구성된 특성으로 인해 S-box 연산 후의 값을 중간값으로 사용하여 공격을 진행하였다.

중간값 8bit에서 1bit씩 공격을 수행하였을 때, 각각의 비트마다 공격 결과가 다르게 나온 것을 확인하였다. 가장 높은 상관계수 값이 1개였기 때문에 얻고자 하는 키값을 얻을 수 있었다. Fig. 3.처럼 최상위 비트, 네 번째, 다섯 번째, 여섯 번째 비트에서는 획득하고자 하는 1라운드의 라운드 키값을 얻었다.

Fig. 3. 에서 가장 큰 상관계수 값

(0.33129548988263025)이 나타났다. 이는 상위 네 번째 비트가 공격이 가장 잘 되는 비트였음을 확인할 수 있었다.

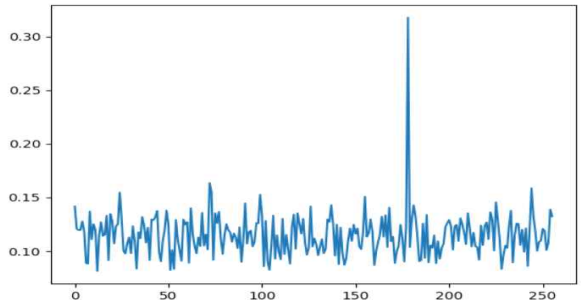

Fig. 3. The 4th high-order bit is the best attack. The highest correlation coefficient value is represented at (0xb2).

반면, Fig. 4.처럼 상관계수 값이 같은 한꺼번에 여러 개의 키값이 나온 비트 공격 결과도 확인하였다. 이와 같은 결과는 두 번째 상위 비트, 세 번째, 일곱 번째, 최하위 비트가 해당되는 것을 확인하였다. 각각 같은 상관계수 값은 4개, 2개, 2개, 2개를 갖는다. 이와 같은 결과를 얻게 되면 해당 비트에서는 완벽한 라운드 키 값을 얻을 수는 없다.

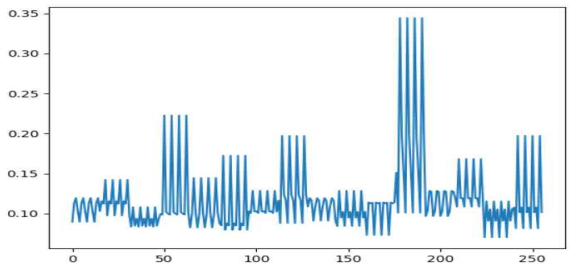

Fig. 4. The second high-order bit has 4 correlation coefficients. The highest correlation coefficient value is represented at (0xb2, 0xb6, 0xba, 0xbe).

하지만, Fig. 4.에 나타난 두 번째 상위 비트 값의 결과값으로 분석한 결과, 각각 0xb2, 0xb6, 0xba, 0xbe의 8비트 중 6개의 모두 같은 비트 값을 지니고 있다는 것을 확인하였다. 이는 얻고자 하는 키값은 총 8비트에 해당하여 정확한 키값을 얻을 수는 없지만, 해당 공격으로 총 6개의 비트를 얻을 수 있음을 의미한다.

결과적으로, 각각 공격 결과가 달랐음에도 불구하고, 0~7 사이의 비트마다 모든 공격한 결과값에서 획득하려는 값인 0xb2가 모두 포함된 것을 확인하였다.

IV. 결론

본 논문에서는 경량 블록 암호 알고리즘 PIPO-64/128을 대상으로 저사양 8bit AVR 프로세서상에서의 상관관계 전력분석 공격에 대한 취약성을 확인하였다.

V. Acknowledgment

이 성과는 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2020R1F1A1048478).

[참고문헌]

[1] T. Kim, Y. Won, J. Park, H. An, D. Han, “Side Channel Attacks on HIGHT and Its Countermeasures” Journal of the Korea Institute of Information Security & Cryptology 25(2), 2015.4, 457-465(9 pages), 2015.

[2] D. Hong, J. Sung, S. Hong, J. Lim, “HIGHT : a new block cipher suitable for low-resource device”, CHES 2006, LNCS 4249:46~59, Oct. 2006.

[3] https://eprint.iacr.org/2020/1582.pdf

[4] 백유진. (2020). 전력분석공격에 대한 하드웨어 마스킹 대응기법 동향. 정보보호학회지, 30(1), 23-33.

[5] J. Kim, K. Oh, Y. Choi, T. Kim, D. Choi, “Side channel analysis system technology trend”, Electronic Communication Trend Analysis, 28(3), 2013.

[5] D. Kwon, S. Jin, H. Kim, S. Hong, “Improving Non-Profiled Side-Channel Analysis Using Auto-Encoder Based Noise Reduction Preprocessing”, Journal of The Korea Institute of Information Security & Cryptology, Vol.29(3), pp. 491-501 , Jun. 2019.