국산 경량 암호 PIPO에 대한 부채널 분석과 마스킹 기법 제안

심민주*, 김현준*, 권혁동*, 장경배*, 김현지*, 박재훈*, 엄시우*, 송경주*, 서화정*†
*한성대학교 IT융합공학부
*† 한성대학교 IT융합공학부
minjoos9797@gmail.com, khj930704@gmail.com, korlethean@gmail.com,
starj1023@gmail.com, khj1594012@gmail.com, p9595jh@gmail.com,
shuraatum@gmail.com, thdrudwn98@gmail.com, hwajeong84@gmail.com

Side-Channel analysis and masking scheme for domestic lightweight cipher PIPO

Min-Joo Sim*, Hyun-Jun Kim*, Hyeok-Dong Kwon*, Kyung-Bae Jang*,
Hyun-Ji Kim*, Jae-Hoon Park*, Si-Woo Eum*, Gyeong-Ju Song*,
Hwa-Jeong Seo*†
*Hansung University, Department of IT Convergence Engineering
*† Hansung University, Department of IT Convergence Engineering

요 약

최근 사물인터넷(IoT) 환경에서 다양한 장비의 인터넷 통신이 가능하여 이에 적절한 경량 블록 암호 알고리즘에 대한 연구가 활발히 진행되고 있다. ICISC 2020에서 새로 발표된 국산 경량 블록 암호 알고리즘인 PIPO는 새로운 경량 S-Box를 조합한 unbalanced-Bridge 구조로 효율적인 비트슬라이싱 구현을 제공한다. IoT 환경에 PIPO가 적용되기 위해서는 부채널 분석에 대한 안전성이 보장되어야 한다. 따라서 본 논문에서는 PIPO가 1차 CPA 공격에 취약함을 확인한다. 그리고 부채널 공격에 대응하기 위해 1차 마스킹 기법을 제안한다. 제안한 마스킹 기법은 1차 CPA 공격에 안전하였으며, 마스킹 적용 전보다 -375%의 성능을 보였다. 그리고 기존 기법보다 1287% 속도가 빨라진 것을 확인하였다.

1. 서론

최근 다양한 장비의 인터넷 통신이 가능한 사물인터넷(IoT) 환경에서 안전한 통신을 위해 적절한 경량 블록 암호 알고리즘에 대한 연구가 활발히 진행되고 있다. 이러한 환경 속에서 데이터를 안전하게 전달하기 위해서는 적절한 암호 알고리즘의 필요성이 요구된다. 이에 대한 여러 경량 블록 암호 알고리즘이 제안이 되고 있다. 대표적인 국산 블록 암호 알고리즘으로는 SEED, ARIA, HIGHT, LEA가 있다. 하지만 블록 암호에서 부채널 분석에 취약점이 존재한다[1,2]. 최근 ICISC 2020에서 국산 경량 블록 암호 알고리즘 PIPO가 처음 발표되었다[3]. SPN 구조인 PIPO는 효율적인 비트슬라이싱 구현을 제공하는 새로운 경량 S-Box를 조합한 unbalanced-Bridge 구조이다. IoT 환경에 암호모듈이 작동하기 위해서는 부채널 분석에 대한 안전성이 보장되어야 한다. 그렇기 때문에 PIPO 또한 IoT 환경에서 사용하기 위해서는 부채널 분석과 대응 기법이 필요하다. 실험을 통하여 PIPO-64/128가 1차 CPA 공격으로 마스터키값을 획득할 수 있음을 확인하였다. 본 논문에서는 IoT 상에서 안전하고 효율적인 PIPO 사용을 위해 1차 CPA 공격을 통해 취약점을 확인한다. 이에 대응하기 위해 PIPO의 1차 부채널 공격에 대한 취약점에 대한 대응 기법으로 1차 마스킹이 적용된 PIPO 알고리즘 설계 방법을 제안한다. 그리고 제안 기법에 대한 1차 CPA 공격을 시도하여 안전성을 확인하였고, 기존 기법과 비교하였

을 때, 더 나은 성능 향상을 보였다.

본 논문의 구성은 다음과 같다. 2장에서 PIPO에 대한 소개 등 배경지식에 대해 서술한다. 3장은 실험을 통해 PIPO-64/128에 대한 1차 부채널 분석을 진행하여 이에 대한 취약점을 분석한다. 4장에서는 PIPO에 대한 1차 마스킹 기법을 제안하고 이에 대한 안전성 검증과 성능 평가를 한다. 마지막으로 5장에서 본 논문에 대한 결론을 내린다.

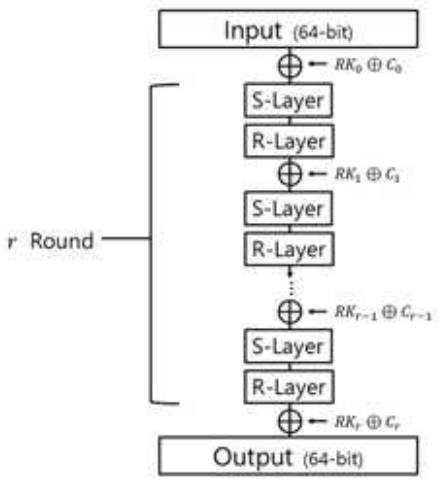
2. 관련 연구

2.1 국산 경량 블록 암호 PIPO 알고리즘

Cipher	n	k	r
PIPO-128	64	128	13
PIPO-256	64	256	17

<Table. 1> Specification of PIPO

ICISC 2020에서 발표된 국산 경량 블록 암호 알고리즘인 PIPO는 SPN 구조로 2가지 암호화 모드를 제공한다[3]. <Table. 1> 은 키 사이즈에 따른 PIPO의 설명이다. 각 암호는 블록 크기가 n 비트, 키 크기가 k 비트, 라운드 수는 r이다.



<Fig. 1> PIPO overall structure

PIPO는 <Fig. 1>과 같이 동작한다. PIPO의 각 라운드는 비선형 레이어로 표현된 S-Layer, 선형 레이어로 표현된 R-Layer, 라운드 키와 상수의 XOR 연산으로 구성된다.

이때, RK_0은 whitening 키를 나타내고, $RK_1, RK_2, \ldots, RK_r$은 라운드 키를 나타낸다. S-Layer는 8개의 동일한 8bit S-Box(S8)를 병렬로 실행한다. R-Layer는 각 행의 비트를 주어진 offset으로 회전시키는 특징을 갖고 있다.

2.2 상관관계 전력분석

전력분석 공격은 일반적으로 데이터 수집 단계와 데이터 분석 단계를 거쳐 공격이 진행된다. 우선 데이터 수집 단계에서는 랜덤하게 선택된 평문을 이용하여 암호화 연산을 수행한 후, 해당 연산에 대한 소비전력 파형을 수집한다. 그리고 데이터 분석 단계에서 비밀키 일부분에 대한 해당 값을 예측한 후, 예측 값과 입력된 평문을 이용하여 내부 연산 값을 계산한다. 이렇게 얻은 계산 값의 유효성을 수집된 전력소비 파형을 이용하여 검증하는 과정을 반복하면 서 비밀키 전체 값을 복구한다[4].

전력 분석 공격 중 일반적으로 사용되는 방법으로 상관관계 전력분석 공격(Correlation Power Analysis, CPA) 등이 있다. CPA은 암호 알고리즘이 적용된 모듈을 계속 동작시켜 고정된 비밀키에 다른 평문을 입력으로 넣는다. 그 결과, 암호문을 획득할 수 있는 동시에 파형 수집 장치를 통해 파형을 수집한다. 수집된 파형, 평문, 암호문을 통해 설계된 분류 함수를 기준으로 파형 통계 처리하여 분석하는 방식이다[5].

상관 전력 분석에 대한 대응 기법으로는 마스킹 기법이 있다. 중요한 데이터에 임의의 변수를 연산 방법으로 불 마스킹이 주로 사용된다.

3. PIPO에 대한 CPA 공격

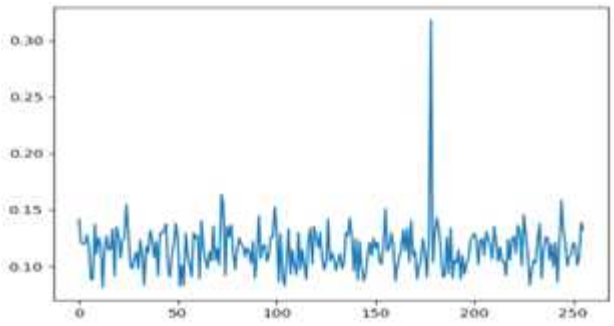
3.1 실험환경

실험은 비트슬라이싱으로 구현된 PIPO-64/128를 대상으로 8bit 프로세스 XMEGA 보드에 Chipwhisperer를 사용하여 13라운드까지의 파형을 10,000개 수집하였다.

3.2 CPA 공격 결과

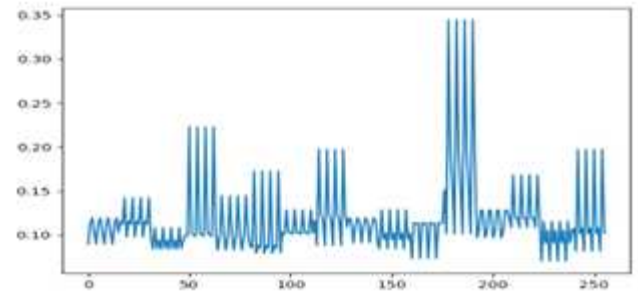
CPA 공격 진행은 S-Box 연산 후의 값을 중간 값으로 사용하여 공격을 진행하였다. 비트 단위로 연산되는 특성을 고려하여 1bit씩 공격을 수행하였다. 그 결과 각각의 비트마다 특징적인 공격 결과가 나온 것을 확인하였다. <Fig. 2>처럼 최상위 비트, 네 번째, 다섯 번째, 여섯 번째 비트에서는 가장 높은 상관계수 값이 1개로 얻고자 하는 라운드 키값을

얻을 수 있었다. <Fig. 2>에서 가장 큰 상관계수 값(0.33)이 나타났다. 이는 네 번째 비트가 공격이 가장 잘 되는 비트임을 확인하였다.



<Fig. 2> The 4th high-order bit is the best attack. The highest correlation coefficient value is represented at (0xb2).

반면, <Fig. 3>과 같이 동일한 상관계수 값이 한꺼번에 여러 개의 키값이 나온 공격 결과도 나타났다. 두 번째 비트, 세 번째, 일곱 번째, 최하위 비트가 이에 해당했다. 2개 이상의 동일한 상관계수 값을 갖는 것을 확인하였다.



<Fig. 3> The second high-order bit has 4 correlation coefficients. The highest correlation coefficient value is represented at (0xb2, 0xb6, 0xba, 0xbe).

<Fig. 3>에 나타난 두 번째 비트 값의 결과값으로 분석한 결과, 각각 0xb2, 0xb6, 0xba, 0xbe의 8비트 중 6개의 모두 같은 비트 값을 지니고 있다는 것을 확인하였다. 이와 같은 결과는 얻고자 하는 키값은 총 8비트에 해당하여 정확한 키값을 얻을 수는 없지만, 해당 공격으로 총 6개의 비트를 얻을 수 있었다. 다른 2개 이상의 동일한 상관계수 값을 갖는 경우도 특정 비트의 값 만 얻을 수 있었다. 결과적으로 최상위 비트, 네 번째, 다섯 번째, 일곱 번째 비트를 공격을 하였을 때, 모든 비트를 알 수 있었으며, PIPO가 CPA 공격에 취약함을 확인할 수 있었다.

4. 1차 부채널 공격에 안전한 PIPO 마스킹 대응 기법

본 장에서는 PIPO에 대한 1차 마스킹 기법을 제안한다. 그리고 구현 전과 구현 후의 연산속도를 차이를 비교한다.

AND 연산과 OR 연산에 사용되는 마스킹은 [3]과 동일하게 ISW 마스킹을 사용하였다. 새로운 마스크 값을 생성할 때, 연산 시간을 고려하여 암호화 전에 마스크 값을 미리 생성한다. 미리 생성하는 마스크 값은 평문에 적용하는 8bit 8개, 라운드 키에 적용하는 8bit 8개 그리고 ISW 마스킹에서 사용할 8bit 마스크 2개를 사용한다.

암호가 구동될 때, 평문과 라운드 키에 마스크를 적용한다. 그리고 로테이션 연산과 XOR 연산을 수행할 때, 마스크 값에도 같은 연산을 수행하여 마스크 상태를 유지한다. ISW-AND, ISW-OR에서는 초기에 생성했던 2개의 마스크 중 하나를 사용하고 예외적으로 연산 과정 $X[4] \oplus (X[5] \wedge X[6])$ 중에서는 마스크 상태가 중복되기 때문에 다른 마스크를 사용한다.

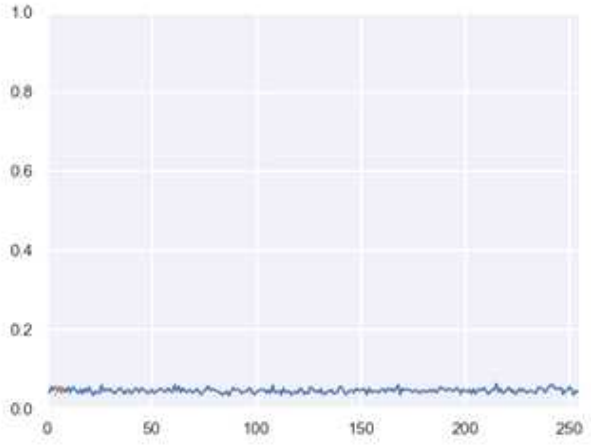
4.1 실험 환경

실험은 본 논문에서 제안하는 마스킹 기법을 적용한 비트슬라이싱으로 구현된 PIPO-64/128를 대상으로 8bit 프로세스 XMEGA 보드에 Chipwhisperer를 사용하여 13라운드까지의 파형을 10,000개 수집하였다. 기존 PIPO와 본 논문에서 제안하는 마스킹 기법이 적용된 PIPO의 연산속도 비교하기 위해 Atmelstudio 시뮬레이터를 사용하였으며, C언어를 사용하여 구현하였다. 장치는 ATmega328P를 사용하였고, 최적화 옵션은 O2를 사용하였다.

4.2 마스킹이 적용된 PIPO에 대한 CPA 공격 결과

해당 공격은 3장에서 사용한 공격 기법과 동일하게 진행하였다. <Fig. 4>는 최상위 비트를 대상으로 CPA 공격을 수행하였을 때의 결과이다. <Fig. 2>와는 다르게 모든 추측키에서 0.1 이하의 상관계수가 나타난 것을 확인할 수 있다. 그리고 가장 높은 상관계수를 나타내고 있는 추측 키는 실제 키와 무

관하다는 것을 확인하였다. 그리고 다른 비트를 대상으로 공격을 진행하였을 때, 실제 키와 무관한 키 값을 나타내는 것을 확인하여 본 논문에서 제안한 마스킹 기법은 적용된 PIPO는 1차 CPA에 대해 안전하다.



<Fig. 4> Results of the most significant bit attack on PIPO with masking applied

4.3 성능 비교

성능 결과는 <Table. 2>와 같다. 본 논문에서 제안한 기법이 적용된 PIPO와 기존 PIPO를 비교하였을 때 마스킹 적용 전의 결과인 3425 clock cycle를 성능을 갖는 기존 PIPO보다 -375%의 성능 차이를 확인하였다. 그리고 [3]에 적혀있는 마스크 적용된 것보다는 1287% 빠르다는 것을 확인하였다. 따라서 제안 기법은 기존 기법보다 효율적으로 사용할 수 있다.

	Clock Cycle	Response to side-channel attacks
Reference	3,452	x
[3]	225,792	o
this paper	16,273	o

<Table. 2> Performance comparison of the existing PIPO and the proposed masking applied PIPO

5. 결론

본 논문에서는 국산 경량 블록 암호 알고리즘 PIPO-64/128을 대상으로 1차 부채널 공격에 취약성을 실험을 통해 검증하였다. 그리고 이에 대한 대응 기법으로 PIPO에 대한 1차 마스킹 기법을 제안하였다. 제안한 마스킹 기법은 1차 CPA를 시도하였을 때, 모든 추측키에서 상관계수가 0.1 보다 작았으며, 실제 키와는 무관하였다. 따라서, 제안 마스킹 기법이 1차 CPA에 대해 안전하다. 그리고 기존 마스킹 기법과 비교하였을 때, 1287%의 성능 향상을 보여 효율적이고 안전한 마스킹을 제안하였다.

6. Acknowledgment

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구) 그리고 이 성과는 2021년도 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), 457-465(9 pages), 2015.4.

[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] H. Kim, Y. Jeon, G. Kim, J. Kim, B. Sim, D. Han, H. Seo, S.Kim, S. Hong, J. Sung and D. Hong, "PIPO : A Lightweight Block Cipher with Efficient Higher-Order Masking Software Implementations", ICISC’ 2020, Seoul, 2020, 105~132.

[4] Y. Baek, “Trends in hardware masking response to power analysis attacks”, Journal of the Korea Institute of Information Security & Cryptology, 30(1), 23-33, 2020.

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