Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.2, Apr. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.2.155

블록암호 PRESENT에 대한 향상된 SITM 공격*

박 종 현,[1†] 김 한 기,[1] 김 종 성[2‡]
[1,2]국민대학교(대학원생, 교수)

Improved SITM Attack on the PRESENT Blockcipher*

Jonghyun Park,[1†] Hangi Kim,[1] Jongsung Kim[2‡]
[1,2]Kookmin University (Graduate student, Professor)

요 약

CHES 2020에서 제안된 SITM (See-In-The-Middle) 공격은 차분 분석과 부채널 분석이 조합된 분석 기법의 일종으로 SNR (Signal-to-Noise Ratio)이 낮은 열악한 환경에서도 적용할 수 있다. 이 공격은 부분 1차 또는 고차 마스킹으로 구현된 블록암호를 공격대상으로 하여, 마스킹 되지 않은 중간 라운드의 취약점을 이용한다. 블록암호 PRESENT는 CHES 2007에 제안된 경량 블록암호로, 저전력 환경에서 효율적으로 구현 가능하도록 설계되었다. 본 논문에서는 차분 패턴들을 이용하여 14-라운드 부분 마스킹으로 구현된 PRESENT에 대한 SITM 공격을 제안한다. 기존 공격은 4-라운드 부분 마스킹 구현된 PRESENT에 적용 가능했지만 본 공격은 더 많이 마스킹된 구현에도 유효하며, 이는 PRESENT가 본 공격에 내성을 가지기 위해서는 16-라운드 이상의 부분 마스킹이 필요함을 보인다.

ABSTRACT

The SITM (See-In-The-Middle) attack proposed in CHES 2020 is a type of analysis technique that combines differential cryptanalysis and side-channel analysis, and can be applied even in a harsh environment with a low SNR (Signal-to-Noise Ratio). This attack targets partial 1st or higher order masked block cipher, and uses unmasked middle round weakness. PRESENT is a lightweight blockcipher proposed in CHES 2007, designed to be implemented efficiently in a low-power environment. In this paper, we propose SITM attacks on 14-round masked implementation of PRESENT while the previous attacks were applicable to 4-round masked implementation of PRESENT. This indicates that PRESENT has to be implemented with more than 16-round masking to be resistant to our attacks.

Keywords: Differential Cryptanalysis, Side-Channel Anaylsis, See-In-The-Middle, Block Cipher, PRESENT

I. 서 론

차분 분석(Differential Cryptanalysis, DC)은 대표적인 암호분석 기법으로 블록암호의 안전성을 검사하거나 비밀키를 취득하기 위해 사용된다[1]. 이 공격은 평문의 특정 비트 자리에 반전 관계가 있는 평문 쌍을 암호화하여 얻은 암호문 쌍을 분석해 비밀키를 도출한다.

물리적인 분석 기법인 부채널 분석(Side-Channel Analysis, SCA)은 암호 시스템이 탑재된 전자장치에서 발생하는 연산 소요 시간, 전력 소모량, 전자파 방출 등의 부가적인 정보를 분석하여 비밀키를 도출한다[2]. 부채널 분석에 대응하는 방법에는 1차 마스킹 또는 고차 마스킹 기법이 있다[3].

Received(01. 12. 2022), Modified(02. 22. 2022), Accepted(02. 22. 2022)
* 본 연구는 고려대 암호기술 특화연구센터(UD210027XD)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.
† 주저자, mmo330@kookmin.ac.kr
‡ 교신저자, jskim@kookmin.ac.kr(Corresponding author)

DATE 2018에는 차분 분석과 부채널 분석을 조합한 분석 기법인 SCADPA (Side-Channel Assisted Differential Plaintext Attack)가 제안되었다[4]. SCADPA은 bit-permutation 기반의 블록암호로 대상이 제한되었지만 CHES 2020에는 이보다 확장된 SPN 구조의 블록암호를 공격대상으로 하는 SITM (See-In-The-Middle)이 제안되었다[5]. SITM 공격은 SNR (Signal-to-Noise Ratio)이 낮은 열악한 환경에서도 적용 가능한 분석 기법으로 소개되었다. 이 공격은 부분 마스킹으로 구현된 블록암호를 대상으로 마스킹이 되지 않은 중간 라운드의 취약점을 이용하기에 1차 또는 고차 마스킹으로 구현된 블록암호의 적절한 마스킹 라운드 수를 판단할 수 있고 이를 통해 마스킹 구현으로 발생하는 비용을 최소화할 수 있다.

본 논문에서는 CHES 2007에 제안된 경량 블록암호 PRESENT[6]의 차분 패턴을 제시한다. 이를 통해 기 제안된 공격[5]보다 마스킹 라운드 수가 증가한 14-라운드 부분 마스킹으로 구현된 PRESENT에 대한 SITM 공격을 제시한다. 이 공격 과정은 평문 쌍 수집 알고리즘과 키 복구 알고리즘으로 구성되며, 실험을 통해 적절한 평문 쌍 수집 개수와 공격 성공률을 계산한다. 논문의 실험 결과 제안하는 공격은 실현 가능한 공격 복잡도를 가진다.

본 논문은 다음과 같이 구성된다. 2장은 배경지식으로 PRESENT 알고리즘과 SITM 공격을 간단히 설명한다. 3장은 PRESENT 차분 패턴을 소개하고 4장은 앞서 소개한 차분 패턴을 사용하여 향상된 PRESENT에 대한 SITM 공격을 설명한다. 5장은 결론 및 향후 계획으로 마무리한다.

II. 배경지식

2.1 PRESENT 알고리즘

PRESENT는 경량 블록암호로, 저전력 환경에서 효율적인 구현이 가능하도록 설계되었다. 블록 크기는 64-비트이고 키 크기는 80, 128-비트로 나뉜다. 전체 라운드는 31-라운드이며, 라운드 함수는 다음과 같다.

- addRoundKey: 키스케줄 함수를 통해 생성된 라운드 키와 64-비트 입력값을 XOR 연산한 64-비트 값 출력
- sLayer: 64-비트 입력값을 니블 단위로 S-box 연산한 64-비트 값 출력, S-box: $\{0,1\}^4 \rightarrow \{0,1\}^4$
- pLayer: 64-비트 입력값을 비트 단위의 위치 이동한 64-비트 값 출력

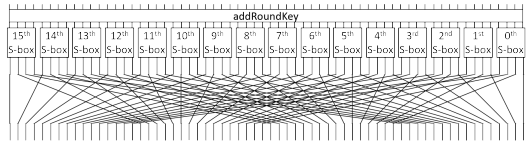

Fig. 1. Round function of PRESENT

Fig. 1은 PRESENT의 라운드 함수를 도식화한 그림이다. PRESENT의 알고리즘은 마지막 라운드 이후 whitening key를 XOR 연산한다. 본 논문에서는 PRESENT의 i번째 라운드를 iR로 표기하고 sLayer 함수에서 S-box의 순서를 Fig. 1과 같이 사용한다.

PRESENT-80의 키스케줄 함수는 다음과 같다. 80-비트 비밀키를 $k_{79}k_{78}k_{77}\cdots k_0$라고 표현하자.

1) $k_{79}k_{78}k_{77}\cdots k_0 \leftarrow k_{18}k_{17}k_{16}\cdots k_0k_{79}k_{78}\cdots k_{19}$.
2) $k_{79}k_{78}k_{77}k_{76} \leftarrow S(k_{79}k_{78}k_{77}k_{76})$.
3) $k_{19}k_{18}k_{17}k_{16}k_{15} \leftarrow k_{19}k_{18}k_{17}k_{16}k_{15} \oplus c$.
4) 라운드 키 $= k_{79}k_{78}k_{77}\cdots k_{16}$.

$S(\bullet)$는 S-box를 의미하고 c는 라운드 상수이다.

PRESENT-128의 키스케줄 함수는 위와 유사하다. 128-비트 비밀키를 $k_{127}k_{126}k_{125}\cdots k_0$라고 표현하자.

1) $k_{127}k_{126}\cdots k_0 \leftarrow k_{66}k_{65}\cdots k_0k_{127}k_{126}\cdots k_{67}$.
2) $k_{127}k_{126}k_{125}k_{124} \leftarrow S(k_{127}k_{126}k_{125}k_{124})$.
3) $k_{123}k_{122}k_{121}k_{120} \leftarrow S(k_{123}k_{122}k_{121}k_{120})$.
4) $k_{66}k_{65}k_{64}k_{63}k_{62} \leftarrow k_{66}k_{65}k_{64}k_{63}k_{62} \oplus c$.
5) 라운드 키 $= k_{127}k_{126}k_{125}\cdots k_{64}$.

2.2 SITM 개요

SITM 공격은 차분 분석과 부채널 분석이 조합된 분석 기법의 일종으로, 부분 마스킹으로 구현된 SPN 구조의 블록암호를 대상으로 한다. 차분 분석은 두 값을 XOR 연산한 값인 차분이 라운드 함수 과정을 거치면서 전파되는 특성을 이용하는 암호분석 기법이다. SITM 공격 설명에서는 다음과 같은 용어

들이 사용된다.

- 전력 파형: 블록암호가 탑재된 전자장치에서 발생하는 전력의 파형
- 차분 파형: 두 전력 파형 T_1, T_2의 차이, $T_1 - T_2$
- 차분 경로: 암호화 과정을 거치면서 입력 차분이 전파되는 예상 경로
- Active S-box: 차분 경로에서 입력 차분이 0이 아닌 S-box
- Inactive S-box: 차분 경로에서 입력 차분이 0인 S-box
- Depth: 전력 파형 관찰을 하는 블록암호의 라운드 위치, 만약 depth를 3으로 설정한다면 암/복호화 방향을 모두 고려하여 4-라운드 마스킹으로 구현된 블록암호를 SITM의 공격대상으로 함

이 공격은 S-box 동작 과정에서 발생한 전력 파형의 차이를 이용한다. 서로 다른 2개의 평문을 암호화하는 과정에서 발생한 전력 파형을 수집하였다고 가정하였을 때, 같은 입력값으로 S-box가 동작하였다면, 이 과정에서 발생한 2개의 전력 파형은 비슷할 것이고 서로 다른 입력값으로 동작하였다면 2개의 전력 파형은 상이할 것으로 예상할 수 있다. 이와 같은 원리를 이용해 공격자가 설정한 차분 경로를 실제 평문 쌍이 만족하였는지를 판단할 수 있다. 만약 만족하는 평문 쌍을 수집하였다면, 유효한 차분 특성을 이용하여 키의 후보를 줄일 수 있다. 자세한 키 복구 과정은 4장에서 다룬다.

III. PRESENT 차분 패턴

PRESENT에는 4-라운드 반복 차분 특성이 존재함이 밝혀져 있다[7]. 이 특성을 이용하면 확률적으로 active S-box가 전파되는 것을 최소화할 수 있다. 3장에서는 이 특성을 이용한 4가지 PRESENT 차분 패턴 A, B, C, D를 제안한다. 각 차분 패턴의 1R 4개 active S-box 위치는 서로 다르며, 패턴 A는 15, 14, 13, 12번째, 패턴 B는 11, 10, 9, 8번째, 패턴 C는 7, 6, 5, 4번째, 그리고 패턴 D는 3, 2, 1, 0번째 S-box만이 active S-box이다. 이때, 1R의 모든 active S-box의 입력 차분은 4이다. Fig. 2는 PRESENT 차분 패턴 A, B, C, D를 도식화한 그림이다.

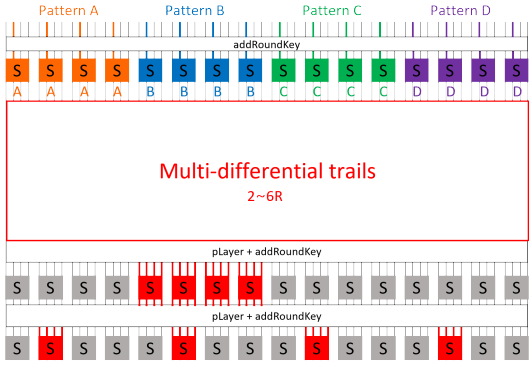

Fig. 2. Four differential patterns of PRESENT. The orange, blue, green, and purple trails are different differential patterns. A, B, C, and D represent the difference. The red trail is the truncated differential trail and grey trail is inactive s-box.

각각의 PRESENT 차분 패턴은 다음과 같은 조건을 가지고 있다.

- 1R: 4개의 active S-box 출력 차분이 같음
- 2~6R: 다중 차분 경로
- 7~8R: 부정차분 경로
- 8R: 1, 5, 9, 13번째 S-box를 제외하고 모두 inactive S-box

차분 패턴의 1R 조건은 다음과 같이 사용된다. 차분 패턴의 active S-box 입력 차분은 정해진 값으로 DDT (Differential Distribution Table)를 통해 가능한 출력 차분 후보들을 추측할 수 있다. 입력 차분이 4이면 출력 차분은 5, 6, 7, 9, 10, 12, 14가 가능하다. 만약 출력 차분이 5일 경우, 가능한 S-box 입력값이 4개임은 Table 1을 통해 알 수 있고 1R active S-box 4개의 입력값 후보 $4^4 = 2^8$개를 얻을 수 있다. 나머지 출력 차분 후보까지 고려한다면 $4^4 + 6 \times 2^4 = 352 \approx 2^{8.46}$개의 입력값 후보들을 얻을 수 있다. 유사한 방법으로 입력 차분을 4가 아닌 2 로 설정하여도 1R active S-box 입력값 후보들을 계산할 수 있다. 4장의 키 복구 알고리즘 과정에서는 위와 같은 입력값 후보들을 사용한다.

7R에는 11, 10, 9, 8번째 S-box를 제외하고 모두

Table 1. A part of DDT with a input difference of 4

	0	⋯	5	6	7	8	9	10	11	12	13	14	15
4	0	⋯	4	2	2	0	2	2	0	2	0	2	0

inactive S-box를 만족하는 조건이 있다. 이 조건을 만족하다면 8R 조건은 자동 성립된다. Fig. 3, 4, 5, 6은 각각의 PRESENT 차분 패턴을 만족하는 최적의 확률을 가진 차분 경로 중 하나를 도식화한 그림이다.

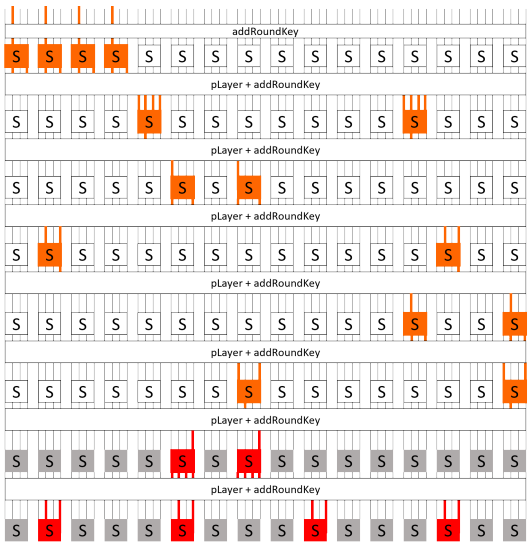

Fig. 3. One of the best differential trails about PRESENT differential pattern A.

PRESENT 차분 패턴 A를 만족하는 최적의 차분 경로 확률은 2^{-32}이다.

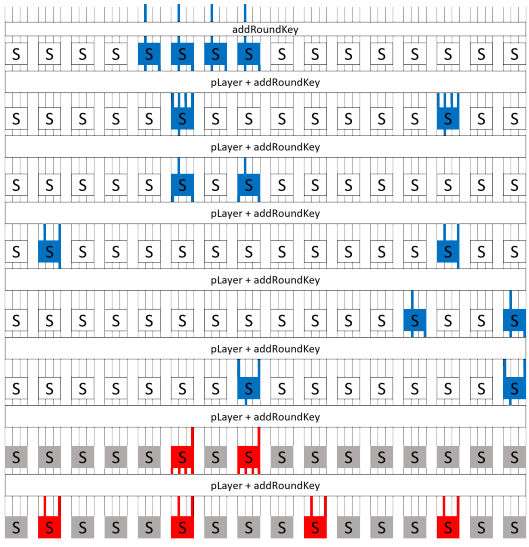

Fig. 4. One of the best differential trails about PRESENT differential pattern B.

PRESENT 차분 패턴 B를 만족하는 최적의 차분 경로 확률은 2^{-32}이다.

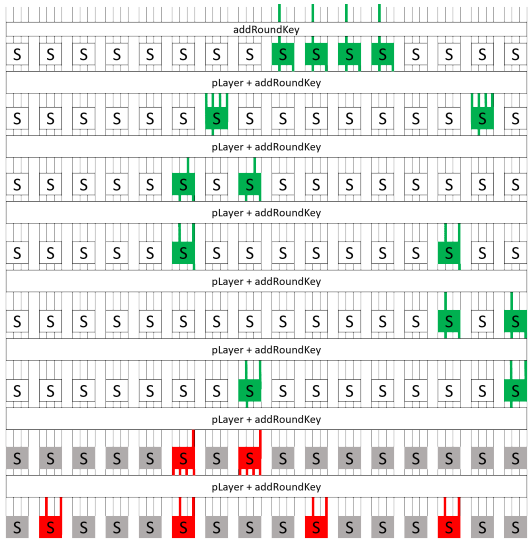

Fig. 5. One of the best differential trails about PRESENT differential pattern C.

PRESENT 차분 패턴 C를 만족하는 최적의 차분 경로 확률은 2^{-32}이다.

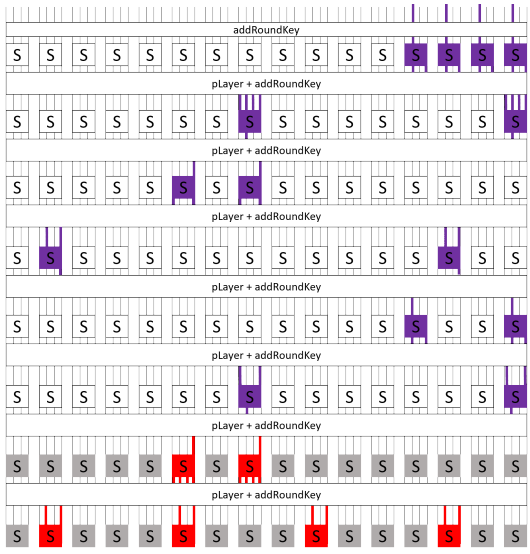

Fig. 6. One of the best differential trails about PRESENT differential pattern D.

PRESENT 차분 패턴 D를 만족하는 최적의 차분 경로 확률은 다른 패턴의 최적 확률보다 높은 2^{-30}이다. 이 경로들은 4장의 평문 쌍 수집 알고리즘 실험을 통해 얻은 경로들이다.

IV. 차분 패턴을 사용한 PRESENT SITM 공격

4.1 PRESENT SITM 공격 과정

3장에서 소개한 PRESENT 차분 패턴의 8R inactive S-box 조건의 만족 여부를 판단하기 위해 depth를 8로 설정하면서 14-라운드 부분 마스킹으로 구현된 PRESENT를 공격대상으로 한다. 차분 패턴을 이용한 SITM 공격 과정은 크게 **차분 패턴을 만족하는 평문 쌍 수집 알고리즘**과 **키 복구 알고리즘**으로 나뉜다. 공격 과정은 차분 패턴 A, B, C, D가 독립적으로 사용되며 각 과정에서 2-바이트 키 후보를 약 1.89개로 줄일 것으로 기대한다. 4장에서는 차분 패턴 A를 사용하는 공격 과정을 설명하며, 나머지 패턴들 또한 유사한 방법으로 적용할 수 있다.

차분 패턴을 만족하는 평문 쌍 수집 알고리즘은 다음과 같다.

1) 차분 패턴 A의 입력 차분을 만족하는 평문 쌍 하나를 랜덤하게 생성한다.

2) 각각의 평문을 암호화하여 8R의 sLayer 함수에서 발생하는 전력 파형을 수집한다.

3) 수집된 전력 파형 쌍을 통해 차분 파형을 계산한다.

4) 차분 파형 관찰을 통해 8R에서 14, 10, 6, 2번째 S-box를 제외하고 모두 inactive S-box를 만족하는지를 판단한다. 만약 이를 만족한다면, 이때 사용된 평문 쌍을 수집한다.

5) N개의 평문 쌍이 수집될 때까지 1~4) 과정을 반복한다.

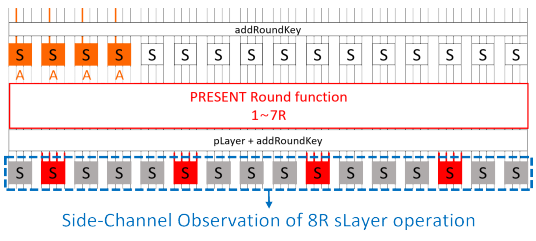

Fig. 7. Step 4 of the algorithm to collect plaintext pairs.

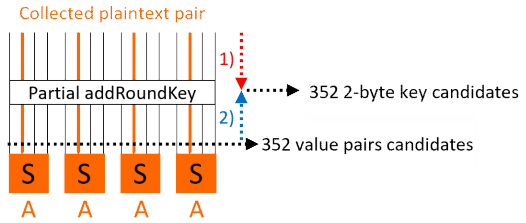

Fig. 8. Steps 1-2 of the algorithm to key recovery algorithm

평문 쌍 수집이 완료되면 키 복구 과정을 진행한다. **키 복구 알고리즘**은 다음과 같다.

1) 수집된 평문 쌍 1개를 준비한다.

2) 3장에서 소개한 1R active S-box의 입력값 후보 352개를 준비된 평문 쌍 값으로 XOR 연산하여 352개 2-바이트 키 후보 집합을 생성한다.

3) 수집된 모든 평문 쌍에 대해 1, 2) 과정을 반복하여 N개의 키 후보 집합 $SET_1, SET_2, \cdots, SET_N$을 구한다.

4) 모든 키 후보 집합 중 중복되는 집합들을 카운트한다. 그리고 가장 많이 카운트된 집합을 right key가 포함된 집합으로 판단하고 키 복구 알고리즘을 마무리한다.

4.2 PRESENT SITM 공격 실험

차분 패턴을 만족하는 평문 쌍 수집 과정에서 다수의 평문 쌍을 수집하는 이유는 다음과 같다. 차분 패턴 8R 조건을 만족하는 평문 쌍 3,000개를 수집했을 때, 약 20%의 평문 쌍이 1R 조건을 만족하지 못했다. 이는 비교적 높은 비율인 80%의 평문 쌍이 1R 조건을 만족하였지만, 1R 조건을 만족하지 않아도 8R 조건을 만족하는 차분 경로가 존재하는 것을 의미한다. 1R 조건을 만족하지 못하는 평문 쌍을 키 복구 알고리즘에 사용하면 right key가 포함된 키 집합을 구하기 어렵다. 이를 방지하기 위해 N개의 평문 쌍을 수집하여 키 복구 알고리즘 과정에서 가장 많이 중복되는 키 후보 집합을 선택한다.

수집하는 평문 쌍의 적절한 개수를 구하기 위해 다음과 같은 실험을 진행하였다. 차분 패턴 A, B, C, D를 사용하여 200번의 평문 쌍 수집 알고리즘과 키 복구 알고리즘을 테스트하였고 평균 평문 쌍의 개수와 키 복구 알고리즘을 통해 얻은 키 후보 집합이 right key를 포함하는 확률을 Table 2에 제시한다.

Table 2. For each difference patterns, the experimental results of the algorithm for finding plaintext pairs and the key recovery algorithm.

N		Pattern A	Pattern B	Pattern C	Pattern D
4	Data	$2^{30.76}$	$2^{29.33}$	$2^{29.72}$	$2^{27.6}$
	Prob.	0.915	0.93	0.92	0.93
8	Data	$2^{31.89}$	$2^{30.4}$	$2^{30.91}$	$2^{28.68}$
	Prob.	0.935	0.985	0.99	0.96
16	Data	$2^{32.66}$	$2^{31.4}$	$2^{31.84}$	$2^{29.7}$
	Prob.	0.93	1.0	0.98	0.99

Table 2는 $N=4$로 설정했을 때 0.9 이상의 높은 공격 성공 확률을 가짐을 알 수 있었으며, 이에 본 공격의 공격 복잡도는 $N=4$일 때를 기준으로 하였다.

4.3 공격 복잡도

위 PRESENT SITM 공격 과정을 거치면 각 차분 패턴마다 352개의 2-바이트 키 후보를 가진 집합 M을 생성할 수 있다. 차분 패턴의 active S-box 입력 차분을 4가 아닌 2로 변경하여 유사한 공격 과정을 거치면 마찬가지로 352개의 2-바이트 키 후보 집합 N을 생성할 수 있다. 2-바이트 키 후보 집합 M와 N은 2^{16}개의 원소를 가진 전체 집합에서 독립적으로 $352(\approx 2^{8.46})$개 원소들이 선택된 것이기에 중복되는 원소의 개수는 $2^{16-7.54-7.54}=2^{0.92}\approx 1.89$로 기대할 수 있다. 각 차분 패턴에 대해서 위 공격 과정을 마친다면 첫 번째 라운드 키의 후보를 $1.89^4\approx 2^{3.67}$개로 줄일 수 있다.

PRESENT-80에 대한 공격 복잡도는 다음과 같다. $N=4$일 때 집합 M을 구하기 위한 데이터 복잡도는 $2\times(2^{30.76}+2^{29.33}+2^{29.72}+2^{27.6})\approx 2^{32.74}$이기에 집합 N 또한 고려하면 첫 번째 라운드 키 후보를 구하는 시간/데이터 복잡도는 $2^{33.74}$이다. 공간 복잡도는 352개의 2-바이트 키 후보 집합 2개를 저장하기 위해 약 $2^{10.46}$ 바이트가 필요하다. 최종적으로 첫 번째 라운드 키 후보 $2^{3.67}$개와 나머지 16-비트의 마스터 키를 조합하면 $2^{19.67}$번의 전수조사를 통해 전체 마스터 키를 복구할 수 있다.

Table 3. Comparison of the SITM attack complexity on PRESENT

	Target Depth	Time	Data	Memory	Ref.
PRESENT-80	3, 4	$O(2^9)$	$2^{12.32}$	2^9	[5]
	8	$2^{33.74}$	$2^{33.74}$	$2^{10.57}$	Ours
PRESENT-128	3, 4	$O(2^9)$	2^{13}	$2^{9.02}$	[5]
	8, 9	$2^{34.74}$	$2^{34.74}$	$2^{14.4}$	Ours

PRESENT-128에 대한 공격 복잡도는 다음과 같다. $N=4$일 때 첫 번째 라운드 키 후보를 구하는 복잡도는 PRESENT-80과 같다. 첫 번째 라운드 키 후보 $2^{3.67}$개를 이용하여 사전에 첫 번째 라운드에 대한 부분 암호화를 할 수 있기에 depth를 한 라운드 증가시킨 SITM 공격을 할 수 있다. 이를 통해, $2^{3.67+3.67}=2^{7.34}$개의 첫 번째와 두 번째 라운드 키 후보를 구할 수 있다. 최종적으로 두 라운드 키를 이용하여 마스터 키의 125-비트를 구할 수 있고 나머지 3-비트는 $2^{7.34+3}=2^{10.34}$번의 전수조사를 통해 전체 마스터 키를 복구할 수 있다.

Table 3는 기 제안된 PRESENT에 대한 SITM 공격과 본 논문의 결과를 비교한 표이다. 본 논문의 공격은 PRESENT-80와 PRESENT-128 모두에 대해서 기 제안된 SITM 공격보다 높은 target depth에 효과적임을 알 수 있다. 이는 PRESENT가 본 공격에 내성을 가지기 위해서는 총 16-라운드 이상의 부분 마스킹을 적용해 구현되어야만 함을 의미한다.

V. 결 론

SITM 공격은 SPN 구조의 블록암호를 공격대상으로 S-box 동작 과정에서 발생하는 전력 파형의 차이를 이용하는 분석 기법이다. 본 논문은 SITM을 이용한 PRESENT 공격을 제시하였다. 기 제안된 공격은 4-라운드 부분 마스킹으로 구현된 PRESENT SITM 공격 방법을 제시하였으나, 본 논문에서는 depth를 8로 설정할 수 있는 새로운 차분 패턴을 사용하여 14-라운드 부분 마스킹으로 구현된 PRESENT 공격을 제안하였다. 결과적으로 실현 가능한 복잡도를 가진 본 공격은 SITM 공격 관점에서 PRESENT의 적절한 마스킹 라운드 수를 확장하였다.

향후 계획으로는 블록암호 ARIA[8]와 GIFT[9]에 대한 SITM 공격 연구와 단순 S-box 동작 과정에서 발생하는 전력 파형의 차이가 아닌 동작 범위를 확장하여 NIST 표준 경량 암호 최종 후보들[10]에 적용하는 방안을 연구할 계획이다.

References

[1] E. Biham, and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," Journal of CRYPTOLOGY, vol. 4, no. 1, pp. 3-72, Jan. 1991.

[2] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," In: Annual international cryptology conference, LNCS, vol 1666, pp. 388-397, Dec. 1999.

[3] S. Nikova, C. Rechberger and V. Rijmen, "Threshold Implementations Against Side-Channel Attacks and Glitches," International conference on information and communications security, LNCS, vol 4307, pp. 529 - 545, Dec. 2006.

[4] J. Breier, D. Jap, and S. Bhasin, "SCADPA: Side-channel assisted differential-plaintext attack on bit permutation based ciphers," 2018 Design, Automation & Test in Europe Conference & Exhibition, IEEE, Mar. 2018.

[5] S. Bhasin, J. Breier, X. Hou, D. Jap, R. Poussier and S. M. Sim, "Sitm: See-in-the-middle side-channel assisted middle round differential cryptanalysis on spn block ciphers," IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2020, no. 1, pp. 95-122, Nov. 2019.

[6] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, et al., "Present: An ultra-lightweight block cipher," International Workshop on Cryptographic Hardware and Embedded Systems, LNCS, vol 4727, pp. 450-466, Sep. 2007

[7] M. Wang, "Differential cryptanalysis of reduced-round PRESENT," International Conference on Cryptology in Africa, LNCS, vol 5023, pp. 40 - 49, Jun. 2008.

[8] D. Kwon, J. Kim, S. Park et al. "New block cipher: ARIA," International Conference on Information Security and Cryptology, LNCS, vol 2971, pp. 432 - 445, Nov. 2003

[9] S. Banik, S. K. Pandey, T. Peyrin, Y. Sasaki, S. M. Sim and Y. Todo, "GIFT: a small present," International Conference on Cryptographic Hardware and Embedded Systems, LNCS, vol 10529, pp. 321-345, Sep. 2017.

[10] NIST Lightweight Cryptography Standardization: Finalists Announced, https://csrc.nist.gov/News/2021/lightweight-crypto-finalists-announced

〈저자소개〉

박 종 현 (Jonghyun Park) 학생회원
2021년 2월: 국민대학교 정보보안암호수학과 졸업
2021년 3월~현재: 국민대학교 금융정보보안학과 석사과정
〈관심분야〉 정보보호, 암호 알고리즘

김 한 기(Hangi Kim) 학생회원
2016년 2월: 국민대학교 수학과 졸업
2018년 2월: 국민대학교 금융정보보안학과 석사
2018년 3월~현재: 국민대학교 금융정보보안학과 박사과정
〈관심분야〉 정보보호, 암호 알고리즘

김 종 성(Jongsung Kim) 종신회원
2006년 11월: K.U.Leuven, ESAT/COSIC 정보보호 전공 공학박사
2007년 2월: 고려대학교 정보보호대학원 공학박사
2009년 9월~2013년 2월: 경남대학교 e-비즈니스학과 교수
2013년 3월~2017년 2월: 국민대학교 수학과 교수
2017년 3월~현재: 국민대학교 정보보안암호수학과/금융정보보안학과 교수
〈관심분야〉 정보보호, 암호 알고리즘, 디지털 포렌식