Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.4, Aug. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.4.923

축소 마스킹이 적용된 경량 블록 암호 알고리즘 SIMON 패밀리에 대한 부채널 공격*

김 지 훈,[1†] 홍 기 원,[1] 김 소 람,[1] 조 재 형,[1] 김 종 성[1,2‡]
[1]국민대학교 금융정보보안학과, [2]국민대학교 정보보안암호수학과

Side Channel Attacks on SIMON Family with Reduced Masked Rounds*

Jihun Kim,[1†] Kiwon Hong,[1] Soram Kim,[1] Jaehyung Cho,[1] Jongsung Kim[1,2‡]
[1]Dept. of Financial Information Security, Kookmin University,
[2]Dept. of Information Security, Cryptology and Mathematics, Kookmin University

요 약

부채널 공격은 암호 장비의 물리적인 정보를 기반으로 내장된 암호 알고리즘을 공격하는 방법이다. 대표적인 부채널 공격 대응방법인 마스킹 기법은 암호 알고리즘의 라운드 중간 값에 임의의 마스킹 값을 연산하는 방법이다. 하지만 암호 알고리즘의 모든 라운드에 마스킹 연산이 적용되면 암호화 과정에 과부하가 발생 할 수 있다. 따라서 IoT(Internet of Things), 웨어러블 디바이스 등과 같은 경량 장비에는 마스킹 기법을 암호 알고리즘의 일부 라운드에만 적용하는 축소 마스킹 기법을 사용하는 것이 현실적이다. 본 논문에서는 축소 마스킹 기법이 적용된 SIMON 패밀리에 대한 해밍 웨이트 필터링을 이용한 공격 방법을 소개하고, 실제 프로그래밍을 통해 첫 라운드 키 복구가 가능함을 보인다.

ABSTRACT

A side-channel attack is a method of attacking a cipher based on physical information of a cryptographic device. The masking method, which is a typical method overcoming this attack, is a method of calculating an arbitrary masking value at the round intermediate value through rounds. Thus, it is difficult to guess the intermediate value by the side-channel attack, but if the masking operation is applied to all rounds of the encryption algorithm, the encryption process may become overloaded. Therefore, it is practical to use a reduced-round masking technique that applies a masking technique to only a part of the cipher for lightweight equipment such as Internet of Things(IoT) and wearable devices. In this paper, we describe a Hamming weight filtering for SIMON family with reduced-round masking technique and it is shown that first round key recovery is possible through actual programming.

Keywords: SIMON family, side-channel attack, reduced-round masking method

I. 서 론

최근 IT 관련 시장은 소형 모바일, 클라우드, IoT 등이 이슈화 되고 있다. 소프트웨어정책연구소에서 선정한 "2017년 SW 10대 이슈"를 보면 IoT, 클라우드, 모바일 결제 등 소형 장비에 대한 이슈들이 선정되어 있다[1]. 이와 같은 소형 장비는 기존 모듈들이 동작하기에는 제한적이기 때문에, 경량 환경에 적합한 기술 및 모듈 개발에 대한 연구가 활발히 진행되고 있다. 기존의 ARIA[2], AES[3] 등의

Received(05. 11. 2017), Modified(08. 01. 2017), Accepted(08. 13. 2017)
* 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.20170005200011001, SCR-Friendly 대칭키 암호 및 응용 모드 개발).
† 주저자, jhkim34@kookmin.ac.kr
‡ 교신저자, jskim@kookmin.ac.kr(Corresponding author)

Table 1. Summary of our attacks on SIMON family

Cipher	reduced masked rounds	data complexity	time complexity
SIMON32	10	$2^{22.587}$	$2^{19.587}$
SIMON48	11	$2^{24.838}$	$2^{18.347}$
SIMON64	12	$2^{22.838}$	$2^{19.379}$
SIMON96	15	$2^{23.253}$	$2^{19.499}$
SIMON128	18	$2^{24.324}$	$2^{20.154}$

암호 알고리즘 역시 경량 환경에서 사용하기에는 제한이 있어, 경량 암호 알고리즘 설계와 분석에 대한 연구가 활발하게 진행되고 있다.

본 논문에서는 축소 마스킹 기법이 적용된 대표적인 경량 암호 알고리즘인 SIMON에 대한 부채널 공격을 통해 첫 라운드 키를 복구하는 방법을 소개한다. 이 공격은 해밍 웨이트의 값으로 평문 쌍을 거르는 해밍 웨이트 필터링과 차분 공격으로 구성되어있다. 대략적인 공격 방법을 간략히 말하자면 우선 차분 공격을 가능하게 하는 차분 특성을 구한다. 그리고 해밍 웨이트 필터링을 이용하여, 차분 특성과 동일한 해밍 웨이트를 갖는 평문 쌍들을 수집한다. 그리고 SIMON 알고리즘의 비선형 연산의 특징을 이용하여 첫 라운드 키의 두 개 비트를 찾아내고, 다른 차분 특성을 이용해 이 과정을 반복하여 첫 라운드 키를 복구해 낸다. 공격 결과는 Table 1.과 같다.

해밍 웨이트 필터링을 이용한 공격에 대한 [4]와 같은 연구 결과가 있다. 주된 공격 및 공격 방법에는 큰 차이가 없지만 [4]의 경우 ARX 구조인 LEA에 대하여 공격을 적용했고, 본 논문에서는 AND 연산을 사용하는 SIMON에 대하여 공격을 적용했다.

본 논문의 구성은 다음과 같다. 2장에서 논문의 표기법과 SIMON 블록 암호 알고리즘을 소개하고, 3장에서 공격 이론 및 방법을 구체적으로 설명하고, 4장에서 공격 방법을 SIMON 알고리즘에 적용하는 방법 및 결과를 제시한다. 마지막으로 5장을 결론으로 논문을 맺는다.

II. 표기법 및 SIMON 알고리즘 소개

2.1 표기법

본 논문에서 사용된 표기법은 Table 2.와 같다.

Table 2. Notation

$\oplus$	Bitwise XOR
&	Bitwise AND
ROT_j	Left circular shift by j bits
d	Hamming Distance[1]
x_i	i bit of word x
$\overline{x_i}$	bit flip[2] of x_i

2.2 SIMON 알고리즘 소개

NSA에서 개발한 SIMON 블록 암호 알고리즘은 무선, IoT와 같은 경량 환경에서 동작하는 장비에 적합한 암호 알고리즘이다[5]. 하드웨어와 소프트웨어 두 환경에서 모두 좋은 성능을 보여주며 특히 하드웨어 환경에서 비교적 좋은 성능을 보인다. 알고리즘의 기본적인 블록 크기 및 인스턴스는 Table 3.와 같다.

SIMON 알고리즘은 Feistel 구조로, 비선형 함수에서 'AND(&)' 연산을 사용하는 것이 특징이다. 알고리즘의 연산은 AND, Rotate, XOR을 이용한다. 라운드 함수는 Fig.1.과 같으며 2개의 워드를 입력한 후 연산들을 사용하여 라운드를 진행한다. SIMON은 평문의 크기와 키 사이즈에 따라 여러 버전이 존재한다. 라운드 수는 SIMON 버전에 따라 달라지며 암호 분석 과정에서 키 스케줄은 사용하지 않기 때문에 키 스케줄의 세부 사항은 생략한다. 각 알고리즘에서 사용되는 $X^i[0]$는 i라운드의 왼쪽 워드를, $X^i[1]$는 i라운드의 오른쪽 워드를 의미한다.

1) 길이가 같은 두 비트열에서 같지 않은 비트의 수. 예를 들어, (00100, 10101)의 해밍 디스턴스는 2이다.

2) 비트의 숫자를 바꾸는 연산. x_i = 0일 경우, $\overline{x_i}$ = 1이고, x_i = 1일 경우, $\overline{x_i}$ = 0이다.

Table 3. Parameters according to SIMON algorithm version

Block size($2n$)	Key size	Word size(n)	Round
32	64	16	32
48	72	24	36
	96		36
64	96	32	42
	128		44
96	96	48	52
	144		54
128	128	64	68
	192		69
	256		72

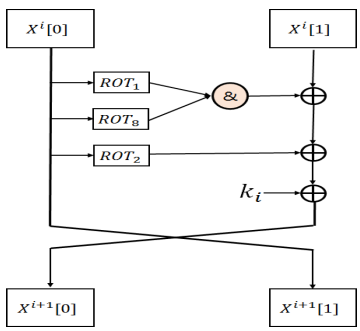

Fig. 1. SIMON algorithm round function

III. 블록 암호 공격 방법과 해밍 웨이트 필터링

3.1 부채널 공격과 마스킹 기법

부채널 공격은 암호 모듈이 동작하는 과정에서 발생하는 물리적인 정보를 바탕으로 알고리즘을 분석하는 공격 방법이다[6]. 즉, 암호 시스템의 실행 시간, 소비 전력, 전자기파, 소리 등의 정보를 통해 키에 대한 정보를 찾아내는 방법을 말한다. 그 중 전력 분석은 대표적인 부채널 공격 방법으로 암호 알고리즘이 수행되는 동안 소비되는 전력 패턴을 분석하여 알고리즘에서 사용되는 키 정보를 획득한다.

전력 분석에 대응하는 방법으로 마스킹 기법이 있다[7]. 추측되는 중간 값에 마스킹 값을 연산해 암호 알고리즘의 라운드에서 중간 값을 추측하기 어렵게 만드는 방법이다. 연산에 따라 가산 마스킹, 곱셈 마스킹, 고차 마스킹 등이 있다. 하지만 마스킹 기법은 암호화 속도, 메모리 등에서 오버로드를 발생시키기 때문에, 암호 모듈에서 실제로 적용될 경우 제품 성능이나 서비스 등에 문제가 될 수 있다. 그래서 경량 환경의 암호모듈에서는 전체 라운드에 마스킹 기법을 적용하는 대신 일부 라운드에만 마스킹 기법을 적용하는 것이 현실적이다. 이를 축소 마스킹 기법이라 하며 보통 처음 특정 라운드와 마지막 특정 라운드에 적용한다. 하지만 축소 마스킹 기법이 적용된 암호 알고리즘은 알고리즘 특성 혹은 적용 범위에 따라 차분 분석 등 암호 알고리즘 분석법에 취약할 수 있다[4,8,9,10].

3.2 차분 공격

차분 공격은 1990년 Biham과 Shamir가 소개했으며 차분을 이용한 대칭키 암호 분석 방법이다[11]. 여기서 차분은 일반적으로 두 값을 XOR한 값을 의미한다. 일반적으로 '선택된 평문 공격' 또는 '선택된 암호문 공격'을 가정으로 한다. n 비트 암호 알고리즘의 평문 쌍(X, X') 차분이 $\triangle X$일 때 i라운드 암호화한 결과를 (C_i, C_i'), 그 차분을 $\triangle C_i$라 하자. 이상적인 암호 알고리즘의 경우, $\triangle X$이 암호화 과정을 거쳐 $\triangle C$가 될 확률은 $\Pr_i(\triangle X \mapsto \triangle C) = 2^{-n}$이다. 그러나 암호 알고리즘에 취약점이 있을 경우 그 확률은 2^{-n}보다 커질 수 있다. 따라서, 차분 공격은 $\Pr_i(\triangle X \mapsto \triangle C)$이 2^{-n}보다 크도록 하는 $\triangle X \rightarrow \triangle C$을 만족하는 평문 쌍을 모아서 공격하는 방법이다. 또한 이를 바탕으로 다양한 차분 공격에 응용되어 사용되기도 한다.

3.3 해밍 웨이트 필터링

해밍 웨이트($hwt(x)$)란 입력된 워드(x)의 비트열에 대해 '1'인 비트의 수를 뜻한다. 해밍 웨이트 필터링이란 임의의 평문 쌍으로부터 차분의 해밍 웨이트를 이용하여 차분 공격에 필요한 평문 쌍을 선별하는 과정을 말한다. 논문에서 제안하는 공격은 해밍 웨이트 필터링을 사용하기 위해 [8]의 특성 1, 2, 3을 이용한다.

특성 1. k 비트 두 블록 워드 $X^i[0]$, $X^i[1]$에 대한 해밍 웨이트를 $hwt(X^i[0])$, $hwt(X^i[1])$로 가정한다. 두 블록 워드를 임의의 값으로 선택하면 다음의 주어진 확률로 $hwt(X^i[0]) = hwt(X^i[1]) \pm d$가 된다. 이때 d를 만족하는 확률 계산식은 다음과 같

다.

$d=0$이면,

$$\Pr(hwt(X)=hwt(X'))=\sum_{l=0}^{k}\left(\frac{\binom{k}{l}}{2^k}\right)^2$$

$d\neq 0$이면,

$$\Pr(hwt(X)=hwt(X')\pm d)=2\times\sum_{l=d}^{k-d}\left(\frac{\binom{k}{l}}{2^k}\times\frac{\binom{k}{l+d}}{2^k}\right)$$

'특성 1'에 대하여 $k=16,24,32,48,64$일 때 계산한 결과는 appendix A에 서술한다.

특성 2. 두 워드의 차분$(X\oplus X')$을 $\triangle X$라 할 때, $\triangle X$의 해밍 웨이트는 다음의 조건을 만족한다.

$hwt(\triangle X)$가 홀수이면,
$hwt(X)=hwt(X')\pm h,\ (h=1,3,\cdots,hwt(\triangle X))$
$hwt(\triangle X)$가 짝수이면,
$hwt(X)=hwt(X')\pm h,\ (h=0,2,\cdots,hwt(\triangle X))$

특성 3. 임의의 두 평문 P,P'에 대해 i라운드 출력 결과를 T_i, T_i'라고 한다면, $T_i\oplus T_i'=\triangle T$을 만족할 확률$(P_{hwt_i})$은 다음과 같다.

$$P_{hwt_i}=\prod_{j=0}^{1}\left(\sum_{d=0}^{t}\Pr(hwt(T_i[j])=hwt(T_i[j]')\pm d^*)\right),$$

이 때, $T=T[0]\|T[1]$,

$$d^*=\begin{cases}2d, & hwt(T_i[j]:\text{짝수})\\ 2d+1, & hwt(T_i[j]:\text{홀수})\end{cases},$$

$$t=\left\lfloor\frac{hwt(\triangle T_i[j])}{2}\right\rfloor$$

IV. SIMON 알고리즘에 공격 적용

본 장에서는 3장의 공격 방법을 SIMON 알고리즘에 적용하고 그에 대한 결과를 제시한다. 먼저 정해진 평문 차분을 이용해, 각 라운드 별로 차분 특성과 해밍 웨이트 필터링 확률을 계산한다. 누적 차분 특성 확률 P_{diff_i}은 차분 특성이 i라운드까지 만족될 확률이다. k비트가 한 워드인 SIMON 알고리즘의 P_{diff_i}은 $\mathrm{xdp}^{\&}$[12]을 이용해 다음과 같이 계산한다.

$$\mathrm{xdp}^{\&}(\alpha,\beta\mapsto\gamma)=2^{-k}\cdot\prod_{i=0}^{k-1}(((2\cdot(\overline{\alpha_i}\wedge\overline{\beta_i}\wedge\overline{\gamma_i}))\vee\overline{(\overline{\alpha_i}\wedge\overline{\beta_i})})\wedge\overline{(\overline{\alpha_i}\wedge\overline{\beta_i}\wedge\gamma_i)})$$

각 연산에 사용하는 $\vee$와 $\wedge$연산은 각각 bitwise OR과 AND를 뜻하며, α와 β는 입력 워드의 차분, γ는 α,β에 대한 알고리즘 결과 차분을 의미한다. x_{k-1}는 최상위 비트를 의미한다.

4.1 평문 쌍 획득

축소 마스킹 기법이 적용된 경우, 중간 값을 알아내기 어렵기 때문에 원하는 차분의 평문 쌍을 얻기 쉽지 않지만 마스킹이 적용되지 않은 중간 값의 해밍 웨이트는 알아낼 수 있다. 따라서 해밍 웨이트 필터링을 이용해 공격에 필요한 평문 쌍의 해밍 웨이트와 동일한 해밍 웨이트를 갖는 평문 쌍을 획득할 수 있다.[3] i라운드까지 마스킹을 적용했을 경우, 부채널 공격을 통해 i라운드 출력에 대한 해밍 웨이트를 획득할 수 있다. 임의의 평문 쌍을 넣고 i라운드 이후에 출력된 해밍 웨이트가 차분 경로의 해밍 웨이트를 만족시키면 그 평문 쌍은 해밍 웨이트 필터링을 통과한 평문 쌍이다.

해밍 웨이트 필터링을 통과한 평문 쌍은 차분경로를 만족시키는 평문 쌍과 그렇지 않은 평문 쌍으로 나뉜다. 따라서 실제 해밍 웨이트 필터링 통과 확률 $\widehat{P_{hwt_i}}$은 차분 경로에 대한 확률을 고려하여 계산해야 한다. $\widehat{P_{hwt_i}}$은 다음과 같이 계산한다.

$$\widehat{P_{hwt_i}}=P_{diff_i}+(1-P_{diff_i})\times P_{hwt_i}$$

SIMON 암호 알고리즘의 특성상 $X^0[0]\rightarrow X^1[1]$의 경로는 차분이 항상 유지된다. 따라서 $X^1[1]$에

3) 실제로 수집된 전력 파형을 통해 템플릿을 구성하면 중간 값의 해밍 웨이트를 구할 수 있다[13]. 또한 본 논문에서는 평문 쌍을 얻는 과정에서 생기는 noise는 고려하지 않는다.

Table 4. Differential characteristics of SIMON32 and cumulative probability to pass hamming weight filtering

round	differential characteristic	P_{diff_i}	P_{hwt_i}	$\widehat{P_{hwt_i}}$
0	$0x1000$ $0x4400$	-	-	-
1	$0x0400$ $0x1000$	2^{-2}	$2^{-1.924}$	$2^{-1.158}$
2	$0x0000$ $0x0400$	2^{-4}	$2^{-4.761}$	$2^{-3.365}$
3	$0x0400$ $0x0000$	2^{-4}	$2^{-4.761}$	$2^{-3.365}$
4	$0x1000$ $0x0400$	2^{-6}	$2^{-3.849}$	$2^{-3.575}$
5	$0x4400$ $0x1000$	2^{-8}	$2^{-3.401}$	$2^{-3.348}$
6	$0x0001$ $0x4400$	2^{-12}	$2^{-3.401}$	$2^{-3.397}$
7	$0x4404$ $0x0001$	2^{-14}	$2^{-3.159}$	$2^{-3.158}$
8	$0x1010$ $0x4404$	2^{-20}	$2^{-2.711}$	$2^{-2.711}$
9	$0x0444$ $0x1010$	2^{-24}	$2^{-2.711}$	$2^{-2.711}$
10	$0x0100$ $0x0444$	2^{-30}	$2^{-3.159}$	$2^{-3.159}$

대한 확률은 항상 1이므로 해밍 웨이트 필터링 확률에 영향을 받지 않는다. P_{hwt_i}를 계산할 때 $X^0[0] \rightarrow X^1[1]$의 경로에 대한 계산은 제외하고 $X^1[0]$에 대한 해밍 웨이트 필터링 확률만 계산하면 된다. SIMON32 버전에 대한 계산한 P_{diff_i}와 $\widehat{P_{hwt_i}}$ 값은 Table 4.와 같다.

4.2 1라운드 키 두 개 비트 복구 과정

4.1절에서 얻은 평문 쌍을 이용하여 1라운드 키 두 개 비트를 복구하는 방법은 다음과 같다.

step 1. 공격에 필요한 필터링 평문 쌍 N개를 획득한다.

공격에 필요한 필터링 평문 쌍은 임의의 평문 쌍으로부터 해밍 웨이트 필터링을 적용해서 얻는다. 이 때 공격에 필요한 해밍 웨이트 필터링 통과 평문 쌍의 수가 N이면, 필요한 임의의 평문의 수는 $2 \times N \times (\widehat{P_{hwt_i}})^{-1}$이다. 평문 쌍의 수는 키 후보들 중에 옳은 키를 걸러 내는데 큰 영향을 미친다. 해밍 웨이트 필터링을 통과한 평문 쌍의 경우 차분경로를 따르지 않는 노이즈 평문 쌍이 존재하기 때문에 이를 고려해야 한다. 따라서 공격에 필요한 평문 쌍의 수는 일반적인 암호 알고리즘 분석에서 필요한 평문 쌍의 수보다 많다.

step 2. 입력한 차분이 영향을 미치는 비트 위치를 찾는다.

Fig. 2.의 2라운드 차분 경로를 비트 단위로 계산하기 위해 $X^1[0] = X$, $X^1[1] = Y$로, 차분이 포함된 워드는 $X' = X \oplus 0x0400$, $Y' = Y \oplus 0x1000$라 한다. 그러면 2라운드 차분 경로에서 다음과 같은 식을 얻는다.

$$\begin{aligned}&(ROT_1(X) \& ROT_8(X)) \oplus Y \oplus ROT_2(X) \\ &\oplus (ROT_1(X') \& ROT_8(X')) \oplus Y' \oplus ROT_2(X') \\ &= 0x0000\end{aligned}$$

이 때, $Y \oplus ROT_2(X) = Y' \oplus ROT_2(X')$이므로 식 (4.1)을 만족한다.

$$\begin{aligned}&(ROT_1(X) \& ROT_8(X)) \\ &= (ROT_1(X') \& ROT_8(X'))\end{aligned} \tag{4.1}$$

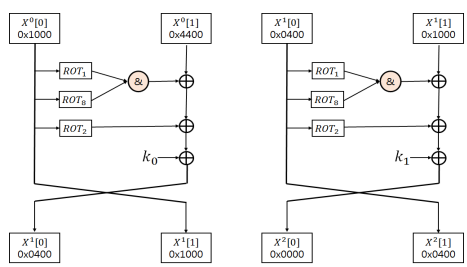

Fig. 2. The first and second round (left and right) differential paths to SIMON32

위 식 (4.1)을 비트 단위로 표현하면 다음과 같다.

$$x_{14}x_{13}x_{12}x_{11}\ x_{10}x_9x_8x_7\ x_6x_5x_4x_3$$
$$x_2x_1x_0x_{15}$$
$$\&\ x_7x_6x_5x_4\ x_3x_2x_1x_0\ x_{15}x_{14}x_{13}x_{12}$$
$$x_{11}x_{10}x_9x_8$$

$$= x_{14}x_{13}x_{12}x_{11}\ \overline{x_{10}}x_9x_8x_7\ x_6\ x_5\ x_4\ x_3$$
$$x_2\ x_1\ x_0x_{15}$$
$$\&\ x_7x_6x_5x_4\ x_3x_2x_1x_0\ x_{15}x_{14}x_{13}x_{12}$$
$$x_{11}\overline{x_{10}}x_9x_8$$

이 결과, $(x_{10}\&x_3)=(\overline{x_{10}}\&x_3)$와 $(x_1\&x_{10})=(x_1\&\overline{x_{10}})$이 되어 x_1과 x_3이 '0'이 된다. 즉, 1라운드 함수 출력 워드인 $X^1[0]$의 하위 두 번째, 네 번째 비트는 0으로 고정된다. 따라서 입력 차분이 영향을 미치는 비트 위치는 $X^1[0]$의 하위 두 번째, 네 번째 비트이다.

step 3. 후보 키의 비트를 카운트 한다.

step 1에서 수집한 평문 쌍들을 이용해 차분 특성을 만족 하는 1라운드 키의 두 번째, 네 번째 비트 값(step 2에서 찾은 비트 위치)에 대하여 카운트를 한다. 수집한 모든 평문 쌍에 대하여 카운트를 진행한 후, 가장 많이 카운트된 두 번째, 네 번째 비트 값을 옳은 키의 비트로 한다. 이와 같은 방식으로 수집한 평문 쌍에 대하여 키 후보들 중에 가장 카운트가 많이 된 키 후보를 가져오되, 그 키 후보 중 차분이 영향을 미치는 비트만을 옳은 키의 비트로 한다.

실제 구현으로 키 복구를 시도한 결과, Intel Core i7-4790K CPU와 8GB 메모리를 가진 PC 환경에서 수 초 이내에 1라운드 키 두 개 비트를 복구했고, 임의 평문의 수를 증가시키면 키 복구 성공률이 더 높아지는 것을 확인했다. step 2의 방법은 두 개의 라운드를 이용해 키를 복구하는 방법이기 때문에 1라운드 축소 마스킹 기법은 공격대상에서 제외한다.

4.3 1라운드 키 두 개 비트 복구 결과

본 절에서는 4.2절의 방법으로 1라운드 키 두 개 비트를 복구한 결과를 제시한다. Table 5.는 Table 4.의 데이터와 2절의 방법을 기반으로 키 복구를 100번 진행했을 때, 1라운드 키 중 두 개 비트를 찾아낼 확률이 70%를 넘어가는 임의 평문 쌍 개수를 나타낸 결과이다.

시간 복잡도 계산은 다음과 같이 계산하며, 키 추측 복잡도는 2^2이다.

Table 5. Plaintext pairs and complexity required for SIMON32 analysis(two bits of round key)

filtering round	genereted random plaintext pairs	filtering pass plaintext pairs	plaintext pairs satisfied differential characteristic	data complexity	time complexity	Two round key bits success rate(%)
1	-	-	-	-	-	-
2	30	2	2	$2^{4.907}$	$2^{1.907}$	72
3	25	2	1	$2^{4.644}$	$2^{1.644}$	75
4	180	19	8	$2^{7.492}$	$2^{4.492}$	75
5	1700	201	46	$2^{10.731}$	$2^{7.731}$	72
6	4500	482	123	$2^{12.136}$	$2^{9.136}$	71
7	15000	1630	441	$2^{13.873}$	$2^{10.873}$	73
8	190000	29114	7419	$2^{17.536}$	$2^{14.536}$	71
9	600000	92302	23279	$2^{19.195}$	$2^{16.195}$	77
10	6300000	707068	177562	$2^{22.587}$	$2^{19.587}$	71

Table 6. Hamming weight filtering probability of SIMON32 and plaintext pairs for attack (two bits of round key)

filtering round	hamming weight filtering probability $\widehat{P_{hwt_i}}$(theoretical)	hamming weight filtering probability $\widehat{P_{hwt_i}}$(practical)	plaintext pairs for attack(N)
1	-	-	-
2	$2^{-3.365}$	$2^{-3.907}$	4
3	$2^{-3.365}$	$2^{-3.644}$	4
4	$2^{-3.575}$	$2^{-3.244}$	16
5	$2^{-3.348}$	$2^{-3.080}$	166
6	$2^{-3.397}$	$2^{-3.223}$	428
7	$2^{-3.158}$	$2^{-3.202}$	1680
8	$2^{-2.711}$	$2^{-2.706}$	29024
9	$2^{-2.711}$	$2^{-2.701}$	91654
10	$2^{-3.159}$	$2^{-3.155}$	705241

$$(\text{시간복잡도}) = (\text{데이터 복잡도}) \times (\text{키 추측 복잡도}) \times \frac{1}{(\text{라운드수})}$$

11라운드 이후부터는 키 복구 성공률 70% 이상을 만족하기 위해서는 공격에 사용되는 평문 쌍이 많이 필요하기 때문에 실제 공격에 적용하기 어렵다. 따라서 10라운드 이내의 마스킹 라운드는 취약함을 보인다.

주어진 실험치를 이용해 실제 공격에 필요한 필터링 평문 개수를 계산한다. 임의 평문 쌍의 개수를 증가시키면서 실험을 진행하였기 때문에 Table 5.에 나와 필터링 통과 평문 쌍의 수가 실제 공격에 필요한 평문 쌍의 개수와 다를 수 있다. 필요한 임의의 평문 쌍의 수는 $N \times (\widehat{P_{hwt_i}})^{-1}$이기 때문에 실험한 임의 평문 쌍의 개수와 이론상의 $\widehat{P_{hwt_i}}$을 이용해 이론적으로 공격에 필요한 평문 쌍의 개수 N을 역으로 계산한다. 계산 결과 실험 수치와 이론적인 N의 값이 유사함을 비교할 수 있다. 1라운드 키 두 개 비트를 찾는 경우의 이론적인 N은 Table 6.과 같다.

SIMON32 이외의 나머지 버전도 위와 같은 방법으로 공격이 가능하다. 앞서 소개한 축소 마스킹이 적용된 SIMON32에 대한 공격 외에 다른 버전의 SIMON 알고리즘 또한 프로그래밍을 통해 공격하였다. 각 버전 별 공격 가능 라운드 수를 Table 7.에 정리하였다. 나머지 버전에 대하여 달라지는 내용 및 결과 값은 appendix에 서술한다.

Table 7. Attacked masking rounds on SIMON family

family	attacked masking round
SIMON32	≤ 10 round
SIMON48	≤ 11 round
SIMON64	≤ 12 round
SIMON96	≤ 15 round
SIMON128	≤ 18 round

4.4 키 전체 비트 복구 방법

본 절에서는 4.3절의 방법을 바탕으로 1라운드 키를 찾아내는 방법을 설명한다. step 2에서 입력 차분을 다르게 하면, 복구할 수 있는 키의 비트 위치가 달라진다. 즉, 입력 차분에 따라 각각 키의 두 개 비트를 복구할 수 있다. 따라서 입력 차분을 다르게 하여 2절의 방법을 8번 반복하면, 각 차분에 대하여 독립적으로 얻은 각각의 키 비트를 이용해 1라운드 모든 키 비트를 복구할 수 있다. SIMON32의 경우 키 비트 추측을 위해 필요한 실제 입력 차분의 값과 그에 따른 키 비트 복구 위치는 Table 8.과 같다.

이 때, 모든 키 비트 복구 성공률을 70%대로 높이기 위해서는 두 개 비트 복구 성공률이 약 96%가 되어야 한다.[4] 이를 위해서 평문 쌍의 개수는 기존 평문 쌍의 개수의 약 5배가 필요함을 프로그래밍을

4) $(0.96)^8 \approx 0.72$

Table 8. SIMON32 input differential characteristics and key bit recovery location

input differential characteristic	key bit recovery location
$0x1000$ $0x4400$	1, 3
$0x2000$ $0x8800$	2, 4
$0x0001$ $0x4004$	5, 7
$0x0002$ $0x8008$	6, 8
$0x0010$ $0x0044$	9, 11
$0x0020$ $0x0088$	10, 12
$0x0100$ $0x0440$	13, 15
$0x0200$ $0x0880$	0, 14

통해 확인하였다.

SIMON32 이외의 나머지 버전도 위와 같은 방법으로 공격이 가능하다. 나머지 버전에 대해서도 모든 키 비트 추측 성공률을 70%대로 높이기 위해서 기존 평문 쌍의 개수의 약 5배의 평문 쌍의 개수가 필요하다. 나머지 버전에 대한 입력 차분과 키 복구 위치는 appendix에 서술한다.

V. 결 론

사물 인터넷 등이 이슈화 되고, 소형 장비에 대한 관심이 높아지면서, 소형 장비에 사용되는 경량 암호 알고리즘의 중요성이 높아지고 있다. 소형 장비에 경량 암호를 사용할 경우 부채널 공격을 막기 위해 축소 마스킹 기법 적용이 현실적이다. 하지만 적은 라운드의 축소 마스킹을 적용할 경우, 본 논문에서 제시한 공격에 취약할 수 있다. 따라서 축소 마스킹을 적용할 때에는 충분한 라운드의 마스킹을 해야 한다.

본 논문에서는 축소 마스킹 기법이 적용된 SIMON에 대한 부채널 공격을 제안하였고, 그 결과 1라운드 키 두 개 비트 복구에 성공하였다. 그리고 입력하는 차분을 변경하며 같은 과정을 반복했을 때 1라운드 키의 모든 비트를 복구할 수 있음을 설명하였다. 두 개 비트의 성공률이 70% 이상인 마스킹 라운드를 제안하였고 실제 프로그래밍을 통해 확인하였다. 키 복구에 걸리는 시간은 짧으며 각 SIMON 버전별로 취약한 축소 마스킹의 수를 계산하였다.

향후에는 SPECK 알고리즘을 비롯한 다른 경량 암호에 대해서도 취약한 축소 마스킹 라운드에 대한 연구가 필요하다. SPECK의 경우 SIMON과 구조가 비슷하기 때문에 위와 같은 공격에 취약함을 보일 수 있다. 그래서 SPECK도 취약한 마스킹 라운드의 수를 정리하여 부채널 공격에 대비해야 한다.

References

[1] Donghyun Lee, Jungmin Kim, "The 2017 Top 10 SW Issues," 2016-015, SPRi, Jan. 2017.

[2] Daesung Kwon, Jaesung Kim, Sangwoo Park, Soo Hak Sung, Yaekwon Sohn, Jung Hwan Song, Yongjin Yeom, E-Joong Yoon, Sangjin Lee, Jaewon Lee, Seongsaek Chee, Daewan Han, and Jin Hong, "New block cipher: ARIA," Proceedings of the Information Security and Cryptology-ICISC'03, LNCS vol. 2971, pp. 432 - 445, Nov. 2003.

[3] Joan Daemen and Vincent Rijmen. "The Design of Rijndael: AES - The Advanced Encryption Standard," Springer, 2002.

[4] Myungseo Park, Jongsung Kim, "Side-Channel Attacks on LEA with reduced masked rounds," KIISC, Journal of KIISC vol. 25, pp.253-260, Dec. 2014.

[5] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers, "The SIMON and SPECK Families of Lightweight Block Ciphers," Cryptology ePrint Archive, Report 2013/404, Jun. 2013.

[6] Paul Kocher, Joshuna Jaffe, and Benjamin Jun, "Differential Power Analysis," CRYPTO, LNCS vol. 1666, pp.388-397, Aug. 1999.

[7] Thomas S. Messerges, "Securing the AES finalists against power analysis attacks," Fast Software Encryption, FSE 2000, LNCS 1978, pp. 150-164, Apr. 2000.

[8] Jongsung Kim, Seokhie Hong, Dong-Guk Han, and Sangjin Lee, "Improved Side-Channel Attack on DES with the First Four Rounds Masked," ETRI Journal, 31(5), pp. 625-627, Oct. 2009

[9] Jongsung Kim, Seokhie Hong, "Side

Channel Attack using Meet in the Middle Technique," The Computer Journal, vol. 53, no. 7, pp. 934-938, Jun. 2009
[10] Jongsung Kim, Yuseop Lee, Sangjin Lee, "DES with any reduced masked rounds is not secure against side-channel attacks," Computers & Mathematics with Application, vol. 60, no. 2, pp. 347-354, Jul. 2010
[11] Eli Biham, Adi Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," CRYPTO, LNCS vol. 537, pp.2-21, Aug. 1990.
[12] Alex Biryukov, Arnab Roy, Vesselin Velichkov, "Differential Analysis of Block Ciphers SIMON and SPECK," FSE, LNCS vol. 4727, pp.450-466, Mar. 2007.
[13] Stefan Mangard, Elisabeth Oswald, and Thomas Popp, "Power Analysis Attack(Revealing the Secrets of Smart Cards)," pp. 105-107, 2007.

Appendix

A. 해밍 디스턴스와 k에 따른 확률 계산 결과

Table 9. Probability calculation results for hamming distance

d	Probability				
	$k=16$	$k=24$	$k=32$	$k=48$	$k=64$
0	$2^{-2.838}$	$2^{-3.125}$	$2^{-3.331}$	$2^{-3.622}$	$2^{-3.829}$
1	$2^{-1.925}$	$2^{-2.184}$	$2^{-2.276}$	$2^{-2.652}$	$2^{-2.851}$
2	$2^{-2.188}$	$2^{-2.361}$	$2^{-2.509}$	$2^{-2.741}$	$2^{-2.918}$
3	$2^{-2.630}$	$2^{-2.657}$	$2^{-2.731}$	$2^{-2.890}$	$2^{-3.030}$
4	$2^{-3.298}$	$2^{-3.072}$	$2^{-3.043}$	$2^{-3.098}$	$2^{-3.187}$
5	$2^{-4.433}$	$2^{-3.610}$	$2^{-3.446}$	$2^{-3.367}$	$2^{-3.388}$
6	$2^{-6.560}$	$2^{-4.293}$	$2^{-3.939}$	$2^{-3.696}$	$2^{-3.635}$
7	$2^{-10.480}$	$2^{-5.227}$	$2^{-4.525}$	$2^{-4.085}$	$2^{-3.927}$
⋮	⋮	⋮	⋮	⋮	⋮

B. SIMON48 공격 결과

Table 10. Differential characteristics of SIMON48 and cumulative probability to pass hamming weight filtering

round	differential characteristic	P_{diff_i}	P_{hwt_i}	$\widehat{P_{hwt_i}}$
0	$0x100000$ $0x440000$	-	-	-
1	$0x040000$ $0x100000$	2^{-2}	$2^{-2.185}$	$2^{-1.269}$
2	$0x000000$ $0x040000$	2^{-4}	$2^{-5.310}$	$2^{-3.537}$
3	$0x040000$ $0x000000$	2^{-4}	$2^{-5.310}$	$2^{-3.537}$
4	$0x100000$ $0x040000$	2^{-6}	$2^{-4.369}$	$2^{-3.983}$
5	$0x440000$ $0x100000$	2^{-8}	$2^{-3.878}$	$2^{-3.803}$
6	$0x000001$ $0x440000$	2^{-12}	$2^{-3.878}$	$2^{-3.873}$
7	$0x440004$ $0x000001$	2^{-14}	$2^{-3.586}$	$2^{-3.585}$
8	$0x100010$ $0x440004$	2^{-20}	$2^{-3.095}$	$2^{-3.095}$
9	$0x040044$ $0x100010$	2^{-24}	$2^{-3.095}$	$2^{-3.095}$
10	$0x000100$ $0x040044$	2^{-30}	$2^{-3.586}$	$2^{-3.586}$
11	$0x040444$ $0x000100$	2^{-32}	$2^{-3.409}$	$2^{-3.409}$

Table 11. Plaintext pairs and complexity required for SIMON48 analysis(two bits of round key)

filtering round	genereted random plaintext pairs	filtering pass plaintext pairs	plaintext pairs satisfied differential characteristic	data complexity	time complexity	Two round key bits success rate(%)
1	-	-	-	-	-	-
2	30	6	3	$2^{4.907}$	$2^{1.737}$	72
3	20	3	2	$2^{4.322}$	$2^{1.152}$	74
4	120	16	7	$2^{6.907}$	$2^{3.737}$	74
5	1000	87	31	$2^{9.966}$	$2^{3.474}$	74
6	2100	162	49	$2^{11.036}$	$2^{7.866}$	75
7	5100	465	152	$2^{12.316}$	$2^{9.146}$	75
8	40000	4803	1273	$2^{15.288}$	$2^{12.118}$	75
9	100000	11763	2986	$2^{16.610}$	$2^{13.440}$	74
10	750000	62888	15828	$2^{19.517}$	$2^{16.347}$	70
11	3000000	281869	70509	$2^{24.838}$	$2^{18.347}$	71

Table 12. Hamming weight filtering probability of SIMON48 and plaintext pairs for attack (two bits of round key)

filtering round	hamming weight filtering probability $\widehat{P_{hwt_i}}$(theoretical)	hamming weight filtering probability $\widehat{P_{hwt_i}}$(practical)	plaintext pairs for attack(N)
1	-	-	-
2	$2^{-3.537}$	$2^{-2.322}$	4
3	$2^{-3.537}$	$2^{-2.737}$	2
4	$2^{-3.983}$	$2^{-2.907}$	8
5	$2^{-3.803}$	$2^{-3.523}$	72
6	$2^{-3.873}$	$2^{-3.696}$	144
7	$2^{-3.585}$	$2^{-3.455}$	426
8	$2^{-3.095}$	$2^{-3.058}$	4682
9	$2^{-3.095}$	$2^{-3.088}$	11704
10	$2^{-3.586}$	$2^{-3.576}$	62448
11	$2^{-3.409}$	$2^{-3.412}$	282480

Table 13. SIMON48 input differential characteristics and key bit recovery location

input differential characteristic	key bit recovery location
$0x100000$ $0x440000$	1, 11
$0x200000$ $0x880000$	2, 12
$0x000001$ $0x400004$	5, 15
$0x000002$ $0x800008$	6, 16
$0x000010$ $0x000044$	9, 19
$0x000020$ $0x000088$	10, 20
$0x000100$ $0x000440$	13, 23
$0x000200$ $0x000880$	0, 14
$0x001000$ $0x004400$	3, 17
$0x002000$ $0x008800$	4, 18
$0x010000$ $0x044000$	7, 21
$0x020000$ $0x088000$	8, 22

C. SIMON64 공격 결과

Table 14. Differential characteristics of SIMON64 and cumulative probability to pass hamming weight filtering

round	differential characteristic	P_{diff_i}	P_{hwt_i}	$\widehat{P_{hwt_i}}$
0	$0x10000000$ $0x44000000$	-	-	-
1	$0x04000000$ $0x10000000$	2^{-2}	$2^{-2.376}$	$2^{-1.342}$
2	$0x00000000$ $0x04000000$	2^{-4}	$2^{-5.707}$	$2^{-3.636}$
3	$0x04000000$ $0x00000000$	2^{-4}	$2^{-5.707}$	$2^{-3.636}$
4	$0x10000000$ $0x04000000$	2^{-6}	$2^{-4.752}$	$2^{-4.261}$
5	$0x44000000$ $0x10000000$	2^{-8}	$2^{-4.238}$	$2^{-4.141}$
6	$0x00000001$ $0x44000000$	2^{-12}	$2^{-4.238}$	$2^{-4.232}$
7	$0x44000004$ $0x00000001$	2^{-14}	$2^{-3.918}$	$2^{-3.917}$
8	$0x10000010$ $0x44000004$	2^{-20}	$2^{-3.405}$	$2^{-3.405}$
9	$0x04000044$ $0x10000010$	2^{-24}	$2^{-3.405}$	$2^{-3.405}$
10	$0x00000100$ $0x04000044$	2^{-30}	$2^{-3.918}$	$2^{-3.918}$
11	$0x04000444$ $0x00000100$	2^{-32}	$2^{-3.711}$	$2^{-3.711}$
12	$0x10001010$ $0x04000444$	2^{-40}	$2^{-2.878}$	$2^{-2.878}$

Table 15. Plaintext pairs and complexity required for SIMON64 analysis(two bits of round key)

filtering round	genereted random plaintext pairs	filtering pass plaintext pairs	plaintext pairs satisfied differential characteristic	data complexity	time complexity	Two round key bits success rate(%)
1	-	-	-	-	-	-
2	30	7	4	$2^{4.907}$	$2^{1.447}$	74
3	20	4	2	$2^{4.322}$	$2^{0.862}$	71
4	120	10	3	$2^{6.907}$	$2^{3.447}$	71
5	900	79	27	$2^{9.814}$	$2^{6.354}$	74
6	1500	112	39	$2^{10.551}$	$2^{7.091}$	73
7	3100	248	95	$2^{11.598}$	$2^{8.139}$	74
8	12000	1109	324	$2^{13.551}$	$2^{10.091}$	74
9	30000	2837	741	$2^{14.873}$	$2^{11.413}$	76
10	170000	11306	2889	$2^{17.375}$	$2^{13.916}$	71
11	400000	30923	7855	$2^{18.610}$	$2^{15.150}$	73
12	7500000	1021718	255583	$2^{22.838}$	$2^{19.379}$	73

Table 16. Hamming weight filtering probability of SIMON64 and plaintext pairs for attack (two bits of round key)

filtering round	hamming weight filtering probability $\widehat{P_{hwt_i}}$(theoretical)	hamming weight filtering probability $\widehat{P_{hwt_i}}$(practical)	plaintext pairs for attack(N)
1	-	-	-
2	$2^{-3.636}$	$2^{-2.100}$	4
3	$2^{-3.636}$	$2^{-2.322}$	2
4	$2^{-4.261}$	$2^{-3.585}$	8
5	$2^{-4.141}$	$2^{-3.510}$	52
6	$2^{-4.232}$	$2^{-3.743}$	80
7	$2^{-3.917}$	$2^{-3.644}$	204
8	$2^{-3.405}$	$2^{-3.436}$	1134
9	$2^{-3.405}$	$2^{-3.403}$	2832
10	$2^{-3.918}$	$2^{-3.910}$	11244
11	$2^{-3.711}$	$2^{-3.693}$	30544
12	$2^{-2.878}$	$2^{-2.876}$	1020263

Table 17. SIMON64 input differential characteristics and key bit recovery location

input differential characteristic	key bit recovery location
$0x10000000$ $0x44000000$	1, 19
$0x20000000$ $0x88000000$	2, 20
$0x00000001$ $0x40000004$	5, 23
$0x00000002$ $0x80000008$	6, 24
$0x00000010$ $0x00000044$	9, 27
$0x00000020$ $0x00000088$	10, 28
$0x00000100$ $0x00000440$	13, 31
$0x00000200$ $0x00000880$	0, 14
$0x00001000$ $0x00004400$	3, 17
$0x00002000$ $0x00008800$	4, 18
$0x00010000$ $0x00044000$	7, 21
$0x00020000$ $0x00088000$	8, 22
$0x00100000$ $0x00440000$	11, 25
$0x00200000$ $0x00880000$	12, 26
$0x01000000$ $0x04400000$	15, 29
$0x02000000$ $0x08800000$	16, 30

D. SIMON96 공격 결과

Table 18. Differential characteristics of SIMON96 and cumulative probability to pass hamming weight filtering

round	differential characteristic	P_{diff_i}	P_{hwt_i}	$\widehat{P_{hwt_i}}$
0	$0x100000000000$ $0x440000000000$	-	-	-
1	$0x040000000000$ $0x100000000000$	2^{-2}	$2^{-2.652}$	$2^{-1.437}$
2	$0x000000000000$ $0x040000000000$	2^{-4}	$2^{-6.274}$	$2^{-3.744}$
3	$0x040000000000$ $0x000000000000$	2^{-4}	$2^{-6.274}$	$2^{-3.744}$
4	$0x100000000000$ $0x040000000000$	2^{-6}	$2^{-5.303}$	$2^{-4.624}$
5	$0x440000000000$ $0x100000000000$	2^{-8}	$2^{-4.767}$	$2^{-4.626}$
6	$0x000000000001$ $0x440000000000$	2^{-12}	$2^{-4.767}$	$2^{-4.758}$
7	$0x440000000004$ $0x000000000001$	2^{-14}	$2^{-4.418}$	$2^{-4.416}$
8	$0x100000000010$ $0x440000000004$	2^{-20}	$2^{-3.881}$	$2^{-3.881}$
9	$0x040000000044$ $0x100000000010$	2^{-24}	$2^{-3.881}$	$2^{-3.881}$
10	$0x000000000100$ $0x040000000044$	2^{-30}	$2^{-4.418}$	$2^{-4.418}$
11	$0x040000000444$ $0x000000000100$	2^{-32}	$2^{-4.176}$	$2^{-4.176}$
12	$0x100000001010$ $0x040000000444$	2^{-40}	$2^{-3.290}$	$2^{-3.290}$
13	$0x440000004404$ $0x100000001010$	2^{-46}	$2^{-3.121}$	$2^{-3.121}$
14	$0x000000010001$ $0x440000004404$	2^{-56}	$2^{-3.470}$	$2^{-3.470}$
15	$0x440000044400$ $0x000000010001$	2^{-60}	$2^{-3.470}$	$2^{-3.470}$

Table 19. Plaintext pairs and complexity required for SIMON96 analysis(two bits of round key)

filtering round	genereted random plaintext pairs	filtering pass plaintext pairs	plaintext pairs satisfied differential characteristic	data complexity	time complexity	Two round key bits success rate(%)
1	-	-	-	-	-	-
2	70	5	3	$2^{6.129}$	$2^{2.374}$	74
3	40	5	2	$2^{5.322}$	$2^{1.567}$	73
4	160	19	7	$2^{7.322}$	$2^{3.567}$	73
5	900	88	34	$2^{9.814}$	$2^{6.059}$	74
6	1600	108	40	$2^{10.644}$	$2^{6.889}$	72
7	2900	225	63	$2^{11.502}$	$2^{7.747}$	73
8	7000	578	159	$2^{12.773}$	$2^{9.018}$	74
9	11000	876	236	$2^{13.425}$	$2^{9.670}$	73
10	25000	1301	363	$2^{14.610}$	$2^{10.855}$	73
11	48000	2824	723	$2^{15.551}$	$2^{11.796}$	74
12	130000	13536	3444	$2^{16.988}$	$2^{13.233}$	73
13	380000	44172	10987	$2^{18.536}$	$2^{14.781}$	73
14	3000000	271704	68273	$2^{21.517}$	$2^{17.762}$	72
15	10000000	902576	226509	$2^{23.253}$	$2^{19.499}$	73

Table 20. Hamming weight filtering probability of SIMON96 and plaintext pairs for attack (two bits of round key)

filtering round	hamming weight filtering probability $\widehat{P_{hwt_i}}$(theoretical)	hamming weight filtering probability $\widehat{P_{hwt_i}}$(practical)	plaintext pairs for attack(N)
1	-	-	-
2	$2^{-3.744}$	$2^{-3.807}$	6
3	$2^{-3.744}$	2^{-3}	4
4	$2^{-4.624}$	$2^{-3.074}$	8
5	$2^{-4.626}$	$2^{-3.354}$	38
6	$2^{-4.758}$	$2^{-3.889}$	60
7	$2^{-4.416}$	$2^{-3.688}$	136
8	$2^{-3.881}$	$2^{-3.598}$	476
9	$2^{-3.881}$	$2^{-3.650}$	748
10	$2^{-4.418}$	$2^{-4.264}$	1170
11	$2^{-4.176}$	$2^{-4.087}$	2656
12	$2^{-3.290}$	$2^{-3.264}$	13286
13	$2^{-3.121}$	$2^{-3.105}$	43688
14	$2^{-3.470}$	$2^{-3.465}$	270714
15	$2^{-3.470}$	$2^{-3.470}$	902576

Table 21. SIMON96 input differential characteristics and key bit recovery location

input differential characteristic	key bit recovery location
$0x100000000000$ $0x440000000000$	1, 35
$0x200000000000$ $0x880000000000$	2, 36
$0x000000000001$ $0x400000000004$	5, 39
$0x000000000002$ $0x800000000008$	6, 40
$0x000000000010$ $0x000000000044$	9, 43
$0x000000000020$ $0x000000000088$	10, 44
$0x000000000100$ $0x000000000440$	13, 47
$0x000000000200$ $0x400000000880$	0, 14
$0x000000001000$ $0x000000004400$	3, 17
$0x000000002000$ $0x000000008800$	4, 18
$0x000000010000$ $0x000000044000$	7, 21
$0x000000020000$ $0x000000088000$	8, 22
$0x000000100000$ $0x000000440000$	11, 25
$0x000000200000$ $0x000000880000$	12, 26
$0x000001000000$ $0x000004400000$	15, 29
$0x000002000000$ $0x000008800000$	16, 30
$0x000010000000$ $0x000044000000$	19, 33
$0x000020000000$ $0x000088000000$	20, 34
$0x000100000000$ $0x000440000000$	23, 37
$0x000200000000$ $0x000880000000$	24, 38
$0x001000000000$ $0x004400000000$	27, 41
$0x002000000000$ $0x008800000000$	28, 42
$0x010000000000$ $0x044000000000$	31, 45
$0x020000000000$ $0x088000000000$	32, 46

E. SIMON128 공격 결과

Table 22. Differential characteristics of SIMON128 and cumulative probability to pass hamming weight filtering

round	differential characteristic	P_{diff_i}	P_{hwt_i}	$\widehat{P_{hwt_i}}$
0	$0x1000000000000000$ $0x4400000000000000$	–	–	–
1	$0x0400000000000000$ $0x1000000000000000$	2^{-2}	$2^{-2.851}$	$2^{-1.498}$
2	$0x0000000000000000$ $0x0400000000000000$	2^{-4}	$2^{-6.679}$	$2^{-3.803}$
3	$0x0400000000000000$ $0x0000000000000000$	2^{-4}	$2^{-6.679}$	$2^{-3.803}$
4	$0x1000000000000000$ $0x0400000000000000$	2^{-6}	$2^{-5.702}$	$2^{-4.856}$
5	$0x4400000000000000$ $0x1000000000000000$	2^{-8}	$2^{-5.153}$	$2^{-4.970}$
6	$0x0000000000000001$ $0x4400000000000000$	2^{-12}	$2^{-5.153}$	$2^{-5.141}$
7	$0x4400000000000004$ $0x0000000000000001$	2^{-14}	$2^{-4.789}$	$2^{-4.786}$
8	$0x1000000000000010$ $0x4400000000000004$	2^{-20}	$2^{-4.240}$	$2^{-4.240}$
9	$0x0400000000000044$ $0x1000000000000010$	2^{-24}	$2^{-4.240}$	$2^{-4.240}$
10	$0x0000000000000100$ $0x0400000000000044$	2^{-30}	$2^{-4.789}$	$2^{-4.789}$
11	$0x0400000000000444$ $0x0000000000000100$	2^{-32}	$2^{-4.529}$	$2^{-4.529}$
12	$0x1000000000001010$ $0x0400000000000444$	2^{-40}	$2^{-3.616}$	$2^{-3.616}$
13	$0x4400000000044404$ $0x1000000000001010$	2^{-46}	$2^{-3.426}$	$2^{-3.426}$
14	$0x0000000000010001$ $0x4400000000044404$	2^{-56}	$2^{-3.790}$	$2^{-3.790}$
15	$0x4400000000044400$ $0x0000000000010001$	2^{-60}	$2^{-3.790}$	$2^{-3.790}$
16	$0x1000000000101000$ $0x4400000000044400$	2^{-70}	$2^{-3.426}$	$2^{-3.426}$
17	$0x0400000000440400$ $0x1000000000101000$	2^{-76}	$2^{-3.616}$	$2^{-3.616}$
18	$0x0000000001000000$ $0x0400000000440400$	2^{-84}	$2^{-4.529}$	$2^{-4.529}$

Table 23. Plaintext pairs and complexity required for SIMON128 analysis(two bits of round key)

filtering round	genereted random plaintext pairs	filtering pass plaintext pairs	plaintext pairs satisfied differential characteristic	data complexity	time complexity	Two round key bits success rate(%)
1	–	–	–	–	–	–
2	30	8	5	$2^{4.907}$	$2^{0.737}$	73
3	20	3	3	$2^{4.322}$	$2^{0.152}$	71
4	120	16	9	$2^{6.907}$	$2^{2.737}$	71
5	800	74	22	$2^{9.644}$	$2^{5.474}$	74
6	1400	81	26	$2^{10.451}$	$2^{6.281}$	73
7	2700	219	59	$2^{11.399}$	$2^{7.229}$	75
8	6000	496	133	$2^{12.551}$	$2^{8.381}$	74
9	10000	831	236	$2^{13.288}$	$2^{9.118}$	74
10	20000	911	265	$2^{14.288}$	$2^{10.118}$	73
11	25000	1352	338	$2^{14.610}$	$2^{10.440}$	75
12	40000	3610	954	$2^{15.288}$	$2^{11.118}$	76
13	65000	6413	1626	$2^{15.988}$	$2^{11.818}$	75
14	130000	9633	2435	$2^{16.988}$	$2^{12.818}$	73
15	250000	18231	4682	$2^{17.932}$	$2^{13.762}$	75
16	900000	84269	21430	$2^{19.780}$	$2^{15.610}$	71
17	2400000	196272	49171	$2^{21.195}$	$2^{17.025}$	72
18	21000000	912264	229123	$2^{24.324}$	$2^{20.154}$	75

Table 24. Hamming weight filtering probability of SIMON128 and plaintext pairs for attack (two bits of round key)

filtering round	hamming weight filtering probability $\widehat{P_{hwt_i}}$(theoretical)	hamming weight filtering probability $\widehat{P_{hwt_i}}$(practical)	plaintext pairs for attack(N)
1	-	-	-
2	$2^{-3.803}$	$2^{-1.907}$	4
3	$2^{-3.803}$	$2^{-2.737}$	2
4	$2^{-4.856}$	$2^{-2.907}$	6
5	$2^{-4.970}$	$2^{-3.434}$	26
6	$2^{-5.141}$	$2^{-4.111}$	40
7	$2^{-4.786}$	$2^{-3.624}$	98
8	$2^{-4.240}$	$2^{-3.597}$	318
9	$2^{-4.240}$	$2^{-3.589}$	530
10	$2^{-4.789}$	$2^{-4.456}$	724
11	$2^{-4.529}$	$2^{-4.209}$	1084
12	$2^{-3.616}$	$2^{-3.470}$	3264
13	$2^{-3.426}$	$2^{-3.341}$	6050
14	$2^{-3.790}$	$2^{-3.754}$	9396
15	$2^{-3.790}$	$2^{-3.777}$	18068
16	$2^{-3.426}$	$2^{-3.427}$	83765
17	$2^{-3.616}$	$2^{-3.612}$	195792
18	$2^{-4.529}$	$2^{-4.525}$	909657

Table 25. SIMON128 input differential characteristics and key bit recovery location

input differential characteristic		key bit recovery location
$0x1000000000000000$	$0x4400000000000000$	1, 51
$0x2000000000000000$	$0x8800000000000000$	2, 52
$0x0000000000000001$	$0x4000000000000004$	5, 55
$0x0000000000000002$	$0x8000000000000008$	6, 56
$0x0000000000000010$	$0x0000000000000044$	9, 59
$0x0000000000000020$	$0x0000000000000088$	10, 60
$0x0000000000000100$	$0x0000000000000440$	13, 63
$0x0000000000000200$	$0x0000000000000880$	0, 14
$0x0000000000001000$	$0x0000000000004400$	3, 17
$0x0000000000002000$	$0x0000000000008800$	4, 21
$0x0000000000010000$	$0x0000000000044000$	7, 21
$0x0000000000020000$	$0x0000000000088000$	8, 22
$0x0000000000100000$	$0x0000000000440000$	11, 25
$0x0000000000200000$	$0x0000000000880000$	12, 26
$0x0000000001000000$	$0x0000000044000000$	15, 29
$0x0000000002000000$	$0x0000000008800000$	16, 30
$0x0000000010000000$	$0x0000000044000000$	19, 33
$0x0000000020000000$	$0x0000000088000000$	20, 34
$0x0000000100000000$	$0x0000000440000000$	23, 37
$0x0000000200000000$	$0x0000000880000000$	24, 38
$0x0000001000000000$	$0x0000004400000000$	27, 41
$0x0000002000000000$	$0x0000008800000000$	28, 42
$0x0000010000000000$	$0x0000044000000000$	31, 45
$0x0000020000000000$	$0x0000088000000000$	32, 46
$0x0000100000000000$	$0x0000440000000000$	35, 49
$0x0000200000000000$	$0x0000880000000000$	36, 50
$0x0001000000000000$	$0x0004400000000000$	39, 53
$0x0002000000000000$	$0x0008800000000000$	40, 54
$0x0010000000000000$	$0x0044000000000000$	43, 57
$0x0020000000000000$	$0x0088000000000000$	44, 58
$0x0100000000000000$	$0x0440000000000000$	47, 61
$0x0200000000000000$	$0x0880000000000000$	48, 62

〈저자소개〉

김 지 훈 (Jihun Kim) 학생회원
2017년 2월: 국민대학교 수학과 졸업
2017년 3월~현재: 국민대학교 금융정보보안학과 석사과정
〈관심분야〉 정보보호, 암호 알고리즘

홍 기 원 (Kiwon Hong) 학생회원
2016년 2월: 국민대학교 수학과 졸업
2016년 3월~현재: 국민대학교 금융정보보안학과 석사과정
〈관심분야〉 디지털 포렌식, 정보보호

김 소 람 (Soram Kim) 학생회원
2016년 2월: 국민대학교 수학과 졸업
2016년 3월~현재: 국민대학교 금융정보보안학과 석사과정
〈관심분야〉 디지털 포렌식, 정보보호

조 재 형 (Jaehyung Cho) 학생회원
2015년 8월: 국민대학교 수학과 졸업
2015년 9월~현재: 국민대학교 금융정보보안학과 석사과정
〈관심분야〉 정보보호, 암호 알고리즘, 디지털 포렌식

김 종 성 (Jongsung Kim) 종신회원
2000년 8월/2002년 8월: 고려대학교 수학 전공 학사/이학석사
2006년 11월: K.U.Leuven, ESAT/SCD-COSIC 정보보호 전공 공학박사
2007년 2월: 고려대학교 정보보호대학원 공학박사
2007년 3월~2009년 8월: 고려대학교 정보보호기술연구센터 연구교수
2009년 9월~2013년 2월: 경남대학교 e-비즈니스학과 조교수
2013년 3월~2017년 2월: 국민대학교 수학과 부교수
2014년 3월~현재: 국민대학교 일반대학원 금융정보보안학과 부교수
2017년 3월~현재: 국민대학교 정보보안암호수학과 부교수
〈관심분야〉 정보보호, 암호 알고리즘, 디지털 포렌식