Super Box의 고원 특성 분석* : 최적의 S-box 선형계층

김성겸*, 홍득조**, 성재철***, 홍석희****

*, ****고려대학교 (대학원생, 교수), **전북대학교 (교수), ***서울시립대학교 (교수)

On the Analysis of Plateau Characteristics of Super Box : Toward the Optimal Linear-layer for S-box

Seonggyeom Kim*, Deukjo Hong**, Jaechul Sung***, Seokhie Hong****

*, ****Korea University(Graduate student, Professor)

**Chonbuk National University(Professor) ***University of Seoul(Professor)

요 약

본 논문에서는 Super Box의 고원 특성 분석 방법을 제시하고 블록암호에 적용한 결과를 보인다. 고원 특성(plateau characteristic)은 확률 동등성 가설(hypothesis of stochastic equivalence)을 따르지 않는 차분 특성으로서, 사용하는 키에 따라서 확률이 다르다. 따라서, 고원 특성 기반의 공격 혹은 안전성 분석 결과는 사용하는 키에 따라 다를 수 있다. 이에 본 논문에서는 2-라운드 블록암호와 동등한 Super Box의 고원 특성을 분석하는 방법을 제시하고 6가지 블록암호에 적용한 결과를 보인다. 분석 결과로부터 우리는 LED, SmallAES, MIDORI의 Super Box가 기존의 최대 차분 확률보다 2배 이상 큰 확률을 갖는 고원 특성이 존재함을 파악할 수 있었다. 또한, S-box에 속한 선형계층과 고원 특성과의 관계를 통해 큰 확률을 갖는 고원 특성을 제거할 수 있는 최적의 S-box 선형계층을 도출하였다. 이러한 결과는 S-box 선형계층 설계에 도움이 될 수 있다.

I. 서론

블록암호의 차분공격에 대한 저항성은 마코브 암호(markov cipher) 가정과 차분 확률의 확률 동등성 가설을 기반으로 분석된다[1]. 대다수의 현대 블록암호는 키 교대암호(key alternative cipher)로서, 마코브 암호 가정을 만족함을 보일 수 있다. 이에 반면, 차분 특성 Q의 확률 $P_k(Q)$에 대한 키 k값이 영향이 없음† 을 가정하는 확률 동등성 가설에 대한 반례와 실험 결과는 다양한 방법을 통해 연구되고 있다[2,3,4,5].

확률동등성 가설의 반례 분석의 결과 중 하나로서, *고원 특성(plateau characteristic)*이 있다.

【정의 1([2]) 고원 특성(plateau characteristic)】 고원 특성 Q는 특정 키 집합 K_Q에서 특성을 따르는 입력쌍을 $2^{height(Q)}$개 갖고, 나머지 키 집합에서 0인 차분 특성을 지칭한다. n_b 블록암호의 비트 크기이고 특성의 확률이 $P(Q)=E_K[P_K(Q)]$ 일 때,

$$P_k(Q)=\begin{cases} 2^{height(Q)-n_b} & k \in K_Q \\ 0 & k \notin K_Q \end{cases} \quad \text{이고}$$

$|K_Q|/|K|=P(Q)/2^{height(Q)-n_b}$을 만족한다. 여기서 K는 서로 독립인 라운드 키 집합이다.

정의 1에 의하면, 고원 특성은 고정된 키 k에 따라서 다른 차분 확률값을 갖는다. 또한, $|K_Q|/|K|<1$인 경우 $P_k(Q)=2^{height(Q)-n_b}>P(Q) \quad k \in K_1$을 만족하기 때문에 특정 킷값에서 확률이 증폭 가능성을 파악할 수 있다. 이 특성은 [4, 6]에서 차분확률의 분포가 정규분포가 아닌 정규분포혼합(mixture of normal distributions)을 이론적으로 설명하는데 뒷받침이 될 수 있다.

결과적으로, 고원 특성의 성질은 확률 동등성 가설 기반으로 분석한 차분공격 저항성이 정확하지 않을 수 있음을 보여준다. 2-라운드 AES의 모든 고원 특성의 분석 결과는 [2]에 제시되어 있으며, 특정 키 집합에서 그 최대확률값(2^{-30})의 8배인 $P_k(Q)=2^{-27}$이 될 수 있음을 보였다‡ .

특히, 키 스케줄이 함께 되면 차분공격 복잡도 분석 결과에 영향을 줄 수 있다. [5]에서는 키 스케줄로부터 얻은 라운드 키가 K_Q에 항상 속하지 않아 해당 특성을 따르는 입력쌍이 모든 마스터키에 대해 존재하지 않는 *환영 특성(phantom characteristic)*을 제시하여 충분한 확률($P(Q)$)을 갖는 차분 특성기반 공격이 불가능할 수 있음을 보였다. 이와는 반대로, 모

* 본 연구는 고려대 암호기술 특화연구센터를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.

† 즉, $E_K[P_K(Q)]=P_k(Q) \ \forall k$, $Var_K[P_K(Q)] \approx 0$

‡ 8배의 확률을 갖는 키의 비율($|K_Q|/|K|$)이 1/8이 되기 때문에, 키 스케줄을 고려하지 않으면 차분공격 관점의 복잡도에는 영향을 주기 어렵다.

든(혹은 대다수의) 라운드 키가 항상 K_Q에 속하게 되는 *팽창 특성(inflated characteristic)*은 차분공격 저항성을 낮출 수 있는 가능성을 제시할 수 있다.

본 논문에서는 AES-like암호의 Super Box에 존재하는 모든 고원 특성을 분석하는 방법을 제시하고* 다양한 블록암호에 적용한 결과를 보인다. 또한, LED, 64-bit SmallAES[7], MIDORI의 S-box 선형계층을 변경하여 얻은 고원 특성 분석 결과를 통해 최적의 S-box 선형계층을 각각 제시한다.

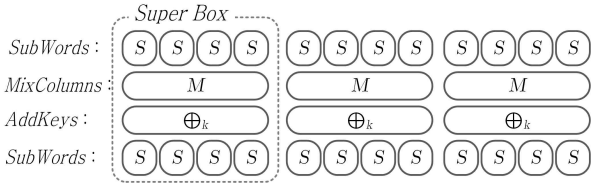
Ⅱ장에서는 Super Box와 고원 특성을 간단히 소개한다. 고원 특성 분석 방법과 각각의 블록암호 분석 결과는 Ⅲ장에서 서술하며, S-box의 최적 선형계층 탐색 결과는 Ⅳ장에서 다룬다. 마지막으로, Ⅴ장에서 본 논문의 결과로부터 추가 해결해야 하는 문제를 제시하고 결론을 맺는다.

II. 배경 지식

2.1 Super Box

*AES-like 암호*는 사용하는 $m\times n$ 라운드 함수가 AES[1]의 구성요소와 유사한 암호를 지칭하는 것으로, 라운드 함수가 *SubWords*($m\times n$개 S-box S), *MixColumns*(n개 열에 대한 선형연산 M), *ShufWords* ($m\times n$ 워드 순열)로 분해된다. AES-like 암호의 2-라운드 차분특성 분석은 첫 번째 라운드의 *ShufWords*와 두 번째 라운드의 *MixColumns, ShufWords*를 제외한 n개의 Super Box로 대신하여 분석할 수 있다.

【정의 2([8]) Super Box】
$m\times n$ 워드로 구성된 AES-like의 2-라운드 특성은 n개의 *Super Box*를 통해 분석할 수 있다. 아래 그림은 4×3 워드로 구성된 2-라운드 AES-like 암호를 3개의 Super Box로 도식화한 예시이다.



n개의 Super Box는 서로 독립이기 때문에, 결과적으로 1개의 Super Box를 통해 모든 2-라운드 차분특성 분석이 가능하다.

*MixColumns*을 행렬곱으로 구성된 AES-like 암호로 LED, MIDORI 등이 있으며, 비트순열(bit permutation)으로 구성된 암호로 PRESENT, GIFT가 대표적이다.

2.2 Super Box의 고원 특성

본 절에서는 Super Box의 고원 특성에 집중하여 소개한다. 고원 특성에 대한 추가적인 정보를 얻고자 하는 독자는 [2, 5]를 참조하기 바란다.

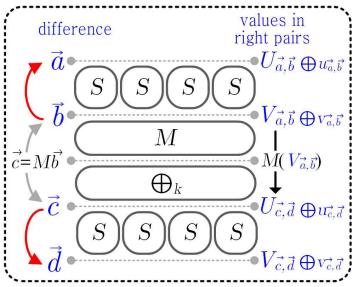
【정의 3([2]) Input/Output-Planar】
차분특성 Q를 따르는 입력쌍(출력쌍)에 속하는 입력(출력)값 들의 집합이 공집합이거나 아핀부분공간을 이루면 Q는 *input(output)-planar*라고 한다.

【따름정리 1([2])】 차분 균일성이 4인 S-box의 모든 차분특성은 input(output)-planar이다.

따름정리 1은 원소가 2 또는 4로 이루어진 모든 집합이 아핀부분공간임을 통해 증명이 가능하다. 또한, *SubWords*는 서로 독립된 $m\times n$개의 S-box로 구성되어 있으므로, 따름정리 2를 도출할 수 있다.

【따름정리 2】 차분 균일성이 4인 S-box들로 구성된 *SubWords*의 모든 차분특성은 input(output)-planar이다.

따라서, 차분 균일성이 4인 S-box로 구성된 AES-like 암호의 2-라운드 차분특성 $Q:(\vec{a},\vec{b},\vec{c},\vec{d})$을 따르는 입(출)력 쌍의 집합은 각 부분특성을 만족하는 입력(출력) 아핀부분공간을 구성하는 부분공간 $U_{i,o}^{\rightarrow}(V_{i,o}^{\rightarrow})^{\dagger}$들의 관계로, 정리 3이 유도된다.



【정리 3([2] Theorem 5)】
차분 균일성이 4인 S-box들로 구성된 Super Box의 차분특성 Q는 고원 특성이며 다음을 만족한다.

$$K_Q = M\left(U_{a,b}^{\rightarrow}\oplus u_{a,b}^{\rightarrow}\right)\oplus V_{c,d}^{\rightarrow}\oplus v_{c,d}^{\rightarrow} \quad \cdots\cdots\cdots\cdots\cdots\cdots (1)$$

$$height(Q) = \dim\left(M\left(U_{a,b}^{\rightarrow}\right)\cap V_{c,d}^{\rightarrow}\right) \quad \cdots\cdots\cdots\cdots\cdots\cdots (2)$$

III. Super Box의 고원 특성 분석

본 장에서는 Super Box의 $P(Q)\neq 0$인 모든 차분특성의 $height(Q)$를 분석하는 방법을 제시한다. 제시하는 방법은 AES의 Super Box를 분석한 [2]의 결과를 일반화한 것으로, $GF(2^n)$의 곱셈 역원(x^{-1})기반 S-box뿐만 아니라, 차분 균일성이 4이하인 모든 S-box에 대해 분석이 가능하다.

비트 크기가 n_{SS}인 Super Box의 $P(Q)\neq 0$인 모든 차분 특성의 개수는 $[\vec{x}, M\vec{x}^{T}]$의 모든 값을 계산하여 얻을 수 있으며 결과는 표 1과 같다.

블록암호	n_{SS}	$\underline{act}$	$\overline{act}$	d_2	d_4	θ_4	|Super Box 특성|
SmallAES	16	5	8	90	15	1	$243,111,658,335(2^{37.82})$
LED		5	8	72	24	1.6	$119,559,765,450(2^{36.79})$
MIDORI		4	8	72	24	1.6	$121,083,893,744(2^{36.82})$
SKINNY		2	8	72	24	1.6	$124,578,218,296(2^{36.86})$
CRAFT		2	8	72	24	1.6	$137,334,742,256(2^{36.99})$
PRESENT		2	8	72	24	1.6	$121,529,261,822(2^{36.82})$
AES	32	5	8	2^{15}	255	1	$2^{87.8647}$

$\underline{act}(\overline{act})$: 특성의 활성 S-box 최소(최대)개수
d_i : S-box DDT i값 엔트리 개수
θ_4 : 차분분포표 행/열에 속한 4 엔트리 평균 개수

표 1 Super Box의 확률이 0이 아닌 모든 차분 특성

* https://github.com/jeffgyeom/CISC_Plateau_Characteristic

† LED S-box $\Delta 1\rightarrow\Delta 3$를 만족하는 입력 아핀부분공간은 $U_{1,3}=\{0,1,2,3\}$으로 구성되고, 출력은 $V_{1,3}=\{0,3,5,6\}$이다.

3.1 효율적인 Super Box의 고원 특성 분석

표 1을 통해 0이 아닌 모든 차분특성의 개수가 약 $O(2^{2n_{ss}})$임을 유추할 수 있다. 따라서 정리 3의 부분공간 교집합 $M(U_{a,b}^{\rightarrow}) \cap V_{c,d}^{\rightarrow}$의 분석 복잡도가 $O(\eta)$일 때, 모든 고원 특성의 $height(Q)$를 분석하기 위해 $O(2^{2n_{ss}} \times \eta)$의 복잡도가 요구됨을 알 수 있다. $Min_{act}=2$이고 4-bit S-box 4개로 구성된 Super Box의 모든 고원 특성 분석은 복잡도 $O(2^{32+10.61})$*가 요구된다.

고원 특성 분석은 두 가지 방법을 통해서 고속화 시킬 수 있다. Algorithm 1은 제안하는 고원 특성 분석에 대한 의사 코드를 보여준다.

첫 번째 방법은 분석 특성의 개수 $O(2^{2n_{ss}})$를 정리 4를 통해 감소시키는 방법이다.

【정리 4】 각 S-box에 해당하는 부분아핀공간의 크기가 2이면 $V_{a_i,b_i}=\{0,a_i\}\ \forall a_i$, $U_{c_i,d_i}=\{0,c_i\}\ \forall d_i$ 이다.

따라서 차분특성 $Q:(\vec{a},\vec{b},\vec{c},\vec{d})$에서 부분아핀공간의 크기가 2인 위치의 차분값$(\vec{a},\vec{b})$을 변경한 차분특성은 탐색하지 않아도 동일한 $height(Q)$를 갖음을 알 수 있다. 이러한 차분특성의 개수는 각 S-box에서 크기 2를 갖는 차분 특성의 개수를 통해 도출할 수 있다(Line 21).

반면, 부분아핀 공간의 크기가 4일 때(즉, 차분분포표의 엔트리가 4인 차분 특성들), 추가되는 기저벡터 V_{a_i,b_i}^{auxi}, U_{c_i,d_i}^{auxi}는 a_i,d_i에 따라 다르기 때문에 다른 $height(Q)$를 갖는다. 이러한 점을 고려하기 위해 Algorithm 1의 Line 15는 각기 다른 기저벡터를 추가한다.

두 번째는 $\dim(A\cap B)=\dim(A)+\dim(B)-\dim(A+B)$를 활용한 방법으로 $O(\eta)$ 복잡도를 감소시킬 수 있다. 고원 특성 분석에 있어서 $M(U_{a,b}^{\rightarrow}), V_{c,d}^{\rightarrow}$의 각각의 기저벡터들은 사전연산을 통해 알 수 있기 때문에 각각의 부분공간을 구하지 않고, 하나의 부분공간 $M(U_{a,b}^{\rightarrow})+V_{c,d}^{\rightarrow}$를 구하여 $height(Q)$를 도출할 수 있다(즉, $O(\eta/2)$로 개선). Line 20은 이 방법이 적용된 부분이다.

분석 복잡도는 Line 2, 8, 9, 14의 **For** 문의 크기로 분석할 수 있으며 각각은 다음과 같다.

Line 2	Line 8	Line 9	Line 14	Total
$O(2^{n_{ss}})$	$O(2^{2m})$		$O(\theta_4^{2m})$	$O(\theta_4^{2m}\times 2^{n_{ss}+2m}\times\eta/2)$

여기서 θ_4는 S-box의 차분분포표 행과 열에 4인 엔트리의 평균 개수로서 AES/SmallAES S-box의 경우 1이고, 분석 나머지 분석 암호는 1.6이다(표 1 참조).

3.2 Super Box 고원 특성 분석 결과

SageMath를 통해 제안 방법을 구현하였으며, 2개의 Intel Xeon Gold 6230 @2.1GHz로 구성된 시스템에서 76개의 프로세스를 생성하여 병렬화(Line 1)하여 약 40분이 소요되었다. 구현 프로그램은 256개 이하의 프로세스를 병렬화할 수 있도록 구현되어 있다. 지면상 LED 분석 결과만 상세히 표 2에 기재하였다.

* $\vec{b}$가 i개의 활성 S-box이면, $U_{a,b}^{\rightarrow}$, $V_{c,d}^{\rightarrow}$는 각각 최대 $4(4-i)+2i$, $4(4-(Min_{act}-i))+2(Min_{act}-i)$의 기저벡터로 구성될 수 있다.

Algorithm 1 - Super Box의 모든 고원 특성 분석

Input : S-box S, Matrix $M \in GL(m, F_{|S|})$
Output : Analysis Result Table Tab

1. **For All** $\vec{b} \in F_{|S|}^{m}$:
2. compute $\vec{c}=M\vec{b}$
3. $A_{M\vec{b}} \leftarrow M(b_0^*)\cup M(b_1^*)\cup M(b_2^*)\cup M(b_3^*)$
4. $A_{\vec{c}} \leftarrow c_0^*\cup c_1^*\cup c_2^*\cup c_3^*$
5. obtain the indices I_{d_4}, whose S-box can have d_4
6. obtain the indices $\check{I}_{d_4}$, whose S-box ONLY have d_4
7. $I_{vari} \leftarrow I_{d_4}-\check{I}_{d_4}$
8. **For** $0 \le n_4 \le |I_{vari}|$:
9. **For All** $I_{chan} \in Combinations(I_{vari}, n_4)$:
10. $B_{M\vec{b}} \leftarrow \varnothing$, $B_{\vec{c}} \leftarrow \varnothing$
11. **call** $Construct\_Basis(I_{chan}\cup\check{I}_{d_4}, B_{M\vec{b}}, B_{\vec{c}}, 0)$
12. **Procedure** $Construct\_Basis(I_{chan}\cup\check{I}_{d_4}, B_{M\vec{b}}, B_{\vec{c}}, idx)$:
13. **If** $idx \in I_{chan}\cup\check{I}_{d_4}$: //Add the auxiliary vector
14. **For All Possible** $a_{idx}\,(d_{idx-m})$:
15. $B'_{M\vec{b}} \leftarrow B_{M\vec{b}}\cup\{V_{a_{idx},b_{idx}}^{auxi}\}$ or $B'_{\vec{c}} \leftarrow B_{\vec{c}}\cup\{U_{c_{idx-m},d_{idx-m}}^{auxi}\}$
16. **call** $Construct\_Basis(I_{chan}\cup\check{I}_{d_4}, B'_{M\vec{b}}, B'_{\vec{c}}, idx+1)$
17. **Else**:
18. **call** $Construct\_Basis(I_{chan}\cup\check{I}_{d_4}, B_{M\vec{b}}, B_{\vec{c}}, idx+1)$
19. **If** $idx=2m$: //We travered all the S-boxes
20. compute $\dim(span(A_{M\vec{b}}\cup A_{\vec{c}}\cup B_{M\vec{b}}\cup B_{\vec{c}}))$, $height(Q)$
21. obtain # of the equivalent characteristics N_Q
22. $Tab[height(Q)]$ += N_Q

if $b_i \neq 0$, $b_i^*=\{\langle 0,..,b_i,...,0\rangle\}$,
else $b_i^*=\{\langle 0,..,v_{std},...,0\rangle | v_{std}\}$, where $v_{std} \in F_{|S|}$ are the corresponding elements to standard basis vectors over $F_2^{\log|S|}$.

#act	weight	$n_{ss}-height$						
		15	14	13	12	11	10	9
5	10	-	-	-	-	-	12.97	5.46
	11	-	-	-	-	16.92	10.53	-
	12	-	-	-	19.56	14.57	-	-
	13	-	-	21.10	17.53	-	-	-
	14	-	21.44	19.47	-	-	-	-
	15	19.98	19.90	-	-	-	-	-
6	12	-	-	-	16.18	12.60	2.00	-
	13	-	-	20.21	17.75	11.62	-	-
	14	-	22.76	21.65	17.05	7.75	-	-
	15	23.86	24.48	21.44	14.89	-	-	-
	16	25.94	24.75	19.94	10.17	-	-	-
	17	26.56	23.76	16.52	-	-	-	-
	18	25.75	21.13	-	-	-	-	-
7	14	-	18.45	17.56	13.55	7.21	-	-
	15	21.91	22.68	20.04	14.62	-	-	-
	16~21	33.05	28.32	22.12	14.00	-	-	-
8	16~24	36.67	28.58	20.12	10.29	-	-	-

\# act : 특성의 활성 S-box 개수
$weight$: $\log_2 P(Q)$
- # act = 7~8의 경우에는 지면상 $weight$를 범위로 기재
- 각 개수의 값은 $\log_2$ 스케일 값
- $weight$에 비해 증폭된 확률을 갖는 경우 음영표시

표 2 LED Super Box 고원 특성 분석 결과

표 2의 결과에서 주목할 만한 것은 $height(Q)=7$인 결과가 존재한다는 것이다. LED의 2-라운드는 최대 차분확률이 2^{-10}임이 알려져 있으나, 해당 확률을 갖는 차분특성 중 $44(2^{5.46})$개가 특정 키 집합에서 확률이 2^{-9}가 됨을 파악할 수 있다. 이는 2^{-10}확률 기반으로 도출한 LED의 차분공격 저항성이 특정키에서 틀릴 수 있음을 보여준다. 이외의 블록암호 분석결과는 다음과 같다.

블록암호	$n_{ss}-height$											
	15	14	13	12	11	10	9	8	7	6	5	4
SmallAES	37.8	29.1	22.8	19.1	15.4	10.9	4.3	-	-	-	-	-
MIDORI	36.7	33.3	29.9	27.5	24.0	21.7	19.8	16.5	13.8	10.6	-	-
SKINNY	36.6	34.1	32.0	28.8	25.9	23.5	20.7	17.4	14.4	11.7	8.5	6.7
CRAFT	36.1	35.5	33.3	31.0	27.9	25.4	22.4	19.1	16.2	13.6	11.0	8.2
PRESENT	36.3	34.9	31.9	28.0	23.2	19.6	16.7	13.6	11.0	9.2	8.0	5.6

- Super Box의 최대 차분 확률보다 큰 $2^{height-n_{ss}}$ 값을 가진 특성의 경우 음영표시

IV. 최적의 S-box 선형계층

본 장에서 S-box의 선형계층을 변경($S' = L_1 \circ S \circ L_2$)하여, 최대 차분확률을 벗어나는 고원 특성을 제거하거나 그 숫자를 감소시킨다.

4.1 S-box의 선형계층과 고원 특성

AES의 설계 원리인 WTS(wide trail strategy)와 같이 활성 S-box의 최소개수를 통해 차분공격의 저항성을 분석하는 경우에 S-box의 선형계층은 저항성에 영향을 미치지 않는다. 이에 반해 Algorithm 1의 Line 14~16에서 추가되는 기저벡터 $V^{auxi}_{a_i b_i}$, $U^{auxi}_{c_i d_i}$는 S-box의 선형계층에 따라 다르기 때문에 선형계층의 변경은 $height(Q)$값에 영향을 준다.

4-bit 선형함수 L_i는 총 20,160개 존재하기 때문에 24개의 4-bit 순열 P_i만 고려하였다. 최대 차분확률을 벗어나는 고원 특성을 갖는 암호는 LED, SmallAES, MIDORI이다. $height(Q)$ 결과는 동일한 차분분포표를 갖는 S-box에서 동일하기 때문에, 순열 함수 조합 중 $\{(P_1, P_2) \mid S \neq \oplus_{c_1} \circ P_1 \circ S \circ P_2 \circ \oplus_{c_2} \ \forall\, c_1, c_2\}$인 순열만 고려하였다. 각각의 암호는 288, 576, 24*개가 고려 대상이었다.

4.2 최적의 선형계층

- LED : $mac_Q[height(Q)]=7$에서 향상 가능한 조합이 없었으나, 고원 특성의 개수를 44개에서 12개로 감소시킬 수 있는 (P_1,P_2)조합이 8개 존재하였다.
- SmallAES : $mac_Q[height(Q)]=7 \rightarrow 6$으로 향상 가능한 (P_1,P_2)조합을 81개 얻을 수 있었다.
- MIDORI : $mac_Q[height(Q)]=10 \rightarrow 9$으로 향상 가능한 (P_1,P_2)조합을 8개 얻을 수 있었다.

표 3은 각 블록암호의 최적 S-box 선형계층 예시를 보여준다.

V. 결론 및 열린 문제

본 논문에서는 Super Box의 고원 특성을 분석 하는 방법을 제시하였다. 제시한 방법은 차분균일성이

* MIDORI는 $\overrightarrow{P_1} \circ M \circ \overrightarrow{P_2} = M \circ \overrightarrow{P_1} \circ \overrightarrow{P_2}$을 만족하기 때문

LED	P_2 : (0, 4, 2, 6, 1, 5, 3, 7, 8, 12, 10, 14, 9, 13, 11, 15) P_1 : (0, 2, 8, 10, 1, 3, 9, 11, 4, 6, 12, 14, 5, 7, 13, 15) S' : (9, 3, 6, 15, 5, 14, 11, 8, 12, 10, 1, 4, 0, 13, 7, 2)
SmallAES	P_2 : (0, 4, 2, 6, 1, 5, 3, 7, 8, 12, 10, 14, 9, 13, 11, 15) P_1 : (0, 2, 8, 10, 1, 3, 9, 11, 4, 6, 12, 14, 5, 7, 13, 15) S' : (9, 3, 6, 15, 5, 14, 11, 8, 12, 10, 1, 4, 0, 13, 7, 2)
MIDORI	P_2 : (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15) P_1 : (0, 8, 4, 12, 1, 9, 5, 13, 2, 10, 6, 14, 3, 11, 7, 15) S' : (3, 6, 11, 12, 7, 14, 15, 13, 2, 10, 8, 9, 0, 4, 1, 5)

표 3 블록암호별 최적의 S-box 선형계층 예시

4 이하인 모든 S-box기반 블록암호에 적용 가능하다. 이에, 우리는 다양한 블록암호의 Super Box에 적용하여 최대 차분확률보다 큰 확률을 갖는 고원 특성 존재 여부를 파악할 수 있었다.

또한, 기존 S-box의 선형계층을 변경하여 고원 특성이 안전성 증명 측면에서 개선될 수 있음을 보이고 최적의 선형계층을 도출하였다. 다만, 고려하는 선형계층을 분석 복잡도의 이유로 비트 순열로 제한했기 때문에 전체 선형계층을 고려할 수 있도록 개선해야 할 것으로 보인다.

차분균일성이 4이하가 아닌 S-box를 사용하는 경우 input(output)-planar를 만족하지 못하게 되어 본 논문의 분석 방법을 사용할 수 없다. 따라서 GIFT와 같이 차분균일성이 4이하가 아닌 S-box를 사용하는 블록암호의 고원 특성분석은 새로운 방법을 고안해야 할 것으로 보인다.

마지막으로, 본 논문에서는 고원 특성을 설계 측면에서만 고려하였으나, 공격 측면에서 이러한 특성을 활용하기 위한 추가 연구가 요구된다.

[참고문헌]

[1] Lai, Xuejia, James L. Massey, and Sean Murphy. "Markov ciphers and differential cryptanalysis." Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1991.

[2] Daemen, Joan, and Vincent Rijmen. "Plateau characteristics." IET information security 1.1 (2007): 11-17.

[3] Canteaut, Anne, et al. "Refined probability of differential characteristics including dependency between multiple rounds." IACR Transactions on Symmetric Cryptology (2017): 203-227.

[4] Sun, Ling, Wei Wang, and Meiqin Wang. "More accurate differential properties of led64 and midori64." IACR Transactions on Symmetric Cryptology (2018): 93-123.

[5] Liu, Yunwen, et al. "The phantom of differential characteristics." Designs, Codes and Cryptography 88.11 (2020): 2289-2311.

[6] 조은지, 김성겸, 홍득조, 성재철, 홍석희 (2019). GPGPU 기술을 활용한 차분 확률의 통계적 분석. 정보보호학회논문지, 29(3), 477-489

[7] Cid, Carlos, Sean Murphy, and Matthew JB Robshaw. "Small scale variants of the AES." International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 2005.

[8] Daemen, Joan, and Vincent Rijmen. "Understanding two-round differentials in AES." International Conference on Security and Cryptography for Networks. Springer, Berlin, Heidelberg, 2006.