S-Box의 비선형 불변 도출 연구*

김성겸*, 이상협*, 조은지*, 홍득조**, 성재철***, 홍석희*

*고려대학교 정보보호학과, **전북대학교 IT정보공학과, ***서울시립대 수학과

A Study for Computing Nonlinear Invariants of S-Box

Seonggyeom Kim*, Sanghyeop Lee*, Eunji Jo*, Deukjo Hong**, Jaechul Sung***, Seokhie Hong*

*Graduate School of Information Security, Korea University.

**Department of Information Technology, Chonbuk National University.

***Department of Mathematics, University of Seoul.

요 약

본 논문은 S-Box의 비선형 불변을 도출하는 방법들을 비교하고, 다양한 블록암호에 적용하여 구한 결과를 제시한다. 비선형 불변 공격은 블록암호의 비선형 불변을 이용한 것으로, 비교적 간단한 키 스케줄을 갖춘 경량 블록암호에서 필수적으로 고려해야 한다. 일반적으로 S-Box의 자명하지 않은 비선형 불변을 확장하여 블록암호의 비선형 불변을 도출하기 때문에 S-Box의 비선형 불변의 존재성은 전체 블록암호의 보안 강도에 큰 영향을 미칠 수 있다. S-Box의 비선형 불변을 도출할 수 있는 방법은 세 가지가 있으며, 각각의 방법 중 모든 비선형 불변을 구하는데 가장 효율적인 방법을 다양한 S-Box에 적용한 결과를 제시한다. 뿐만 아니라, 작은 블록을 갖는 실험적인 블록암호를 통해 S-Box의 비선형 불변과 블록암호의 비선형 불변의 연관성을 파악한다.

I. 서론

경량 디바이스에서 암호화 서비스의 수요가 증가함에 따라 새로운 경량 블록암호가 지속적으로 제안되고 있다. 경량성과 보안 강도를 동시에 목표로 하는 경량 블록암호 설계는 주로 키 스케줄을 간소화하거나, 사용하지 않는 경향이 있다. 이는 경량 블록암호가 보통 연관키 공격에 대한 저항성을 주장하지 않고, 라운드 상수를 다르게만 사용하면 슬라이드 공격(Slide Attack)[17]을 방지할 수 있기 때문이다. 하지만 단순화된 키 스케줄을 가진 블록암호가 비선형 불변 공격(Nonlinear Invariant Attack)에 취약함이 최근 알려졌다.

비선형 불변 공격은 2016년에 제안되었다[1]. 이 공격법은 불변 부분공간 공격(Invariant Subspace Attack)[16]까지 설명할 수 있기 때문에 단순히 불변 공격으로 불리기도 한다[2]. 블록암호의 비선형 불변이 존재하기만 하면, 구별공격, 평문 복원 및 키 복구 공격이 가능하다. 따라서 블록암호의 비선형 불변을 도출하는 방법은 계속해서 연구되고 있다.

지금까지 알려진 블록암호의 비선형 불변 도출 방법은 S-Box나 선형 연산의 비선형 불변을 확장하는 방법이다. 이 방법은 블록암호의 모든 비선형 불변을 도출하지 못하지만 해당 비선형 불변을 도출할 수 있는 가장 현실적인 방법이다. 따라서 비선형 불변 공격에 대한 저항성은 세부 구성요소의 비선형 불변 존재성을 통해 파악된다. 이는 차분 공격이나 선형 공격을 위해 S-Box의 DDT(Differential Distribution Table)와 LAT(Linear Approximation Table)으로부터 해당 경로를 구성하는 것과 유사하다고 볼 수 있다.

본 논문은 S-Box의 비선형 불변을 도출하기 위한 방법들을 비교하고 다양한 S-Box의 비선형 불변을 도출한다. 구성은 Ⅱ장에서 비선형 불변에 대한 정의와 비선형 불변 공격을 소개로 시작한다. S-Box의 비선형 불변 도출 방법은 Ⅲ장에서 다루고 그 결과 및 해석을 Ⅳ장에서 보인다. 끝으로 Ⅴ장에서 결론을 제시한다.

II. 관련 연구

본 장에서는 전반적으로 사용하는 표기법 및 비선형 불변 공격을 소개한다.

2.1 표기법

* 본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.

$\mathcal{B}_n$: n비트 입력의 불함수 집합

U_F : F의 비선형 불변 집합

LSU_F : 선형구조를 갖는 F의 비선형 불변 집합

$BLSU_F$: $=\{balanced\ \ g \in LSU_F\}$

K_g : 비선형 불변 g의 취약키 집합

$\mathcal{S}$: SPN의 S-Layer

$\mathcal{P}$: SPN의 P-Layer

$\mathcal{A}_{k_i \oplus rc_i}$: 라운드 키 및 상수 $k_i \oplus rc_i$ 덧셈 연산

$R_{k_i \oplus rc_i}$: SPN의 라운드 함수 ($=\mathcal{A}_{k_i \oplus rc_i} \circ \mathcal{P} \circ \mathcal{S}$)

$|s|$: S-Box s의 입력 비트 크기

k : 블록암호의 마스터 키

2.2 비선형 불변

비선형 불변 공격은 블록암호($E_k : F_2^n \rightarrow F_2^n$)의 비선형 불변을 특성으로 갖는다.

정의1. [비선형 불변]

주어진 블록암호 $E_k : F_2^n \rightarrow F_2^n$에 대해서, 불함수 $g : F_2^n \rightarrow F_2$가

$$g(x) \oplus g(E_k(x)) = c \quad \forall x \in F_2^n \ with\ a\ constant\ \ c \quad (1)$$

을 *다수의 키* k들에 대하여 만족할 때, g를 E_k의 비선형 불변이라 한다.

정의1에서 확인할 수 있듯이, 0 또는 1이 아닌 비선형 불변 g는 모든 키에 대해서 식 (1)을 만족하기 어렵다. 여기서 g가 비선형 불변이 될 수 있는 키의 집합 K_g을 g의 취약키 집합이라 정의하고, 최대한 큰 K_g를 갖는 g를 찾아 공격하는 것이 일반적이다.

2.3 비선형 불변을 활용한 공격

블록암호의 비선형 불변이 존재하는 경우, 구별 공격, 평문 복원 및 키 복원을 시행할 수 있다. 구별 공격 및 평문 복원은 2016년 [1]에서 보였다. 2018년에는 향상된 방법을 통해 비선형 불변을 도출하고, 포화 공격(integral attack)을 결합하여 키 복원을 시행하였다[2].

2.4 블록암호의 비선형 불변 도출 방법

비선형 불변의 도출 방법들은 SPN 구조를 갖는 블록암호에 적용되었다. [1]에서 사용된 방법은 S, P-Layer에 대한 비선형 불변 집합들의 교집합 $U_{\mathcal{S}} \cap U_{\mathcal{P}}$를 통해 블록암호 E_k의 비선형 불변을 도출한다. S-Layer($\mathcal{S}$)는 S-Box(s)를 워드 단위로 평행하게 연산하는 형식으로 $\mathcal{S} = s \times ... \times s$로 나타낼 수 있다. 따라서 s의 비선형 불변 집합 U_s을 통해 $\mathcal{S}$의 비선형 불변 집합 $U_{\mathcal{S}}$의 부분 집합을 도출할 수 있다.

정리2. $(U_s \times ... \times U_s) \subset U_{\mathcal{S}}$

정리3. $(U_s \times ... \times U_s) \cap U_{\mathcal{P}} \subset U_{\mathcal{S}} \cap U_{\mathcal{P}}$

정리2와 **정리3**을 통해 블록암호 라운드 함수의 비선형 불변을 얻을 수 있다. 각 라운드 함수는 각기 다른 값($k_i \oplus rc_i$)이 더해지기 때문에 **정리4**를 통해 최대한 다수의 k에서 식 (1)을 만족하는 블록암호 E_k의 비선형 불변을 도출할 수 있다.

정리4. r이 라운드 수이고, i-라운드의 라운드키 및 상수가 $k_i \oplus rc_i$일 때,

$$(U_s \times ... \times U_s) \cap U_{\mathcal{P}} \cap U_{k_1 \oplus rc_1} \cap ... \cap U_{k_r \oplus rc_r} \subset U_{E_k} \quad (2)$$

이다. (여기서 k_i들은 마스터키 k로부터 도출된다.)

2.5 비선형 불변 공격에 대한 저항성

비선형 불변 공격의 저항성은 다수의 k에 대한 비선형 불변 $g \in U_{E_k}$의 존재 여부에 따라 결정된다. 따라서 어떠한 k에 대해서도 $U_{E_k} = \{0,1\}$임을 보일 수 있다면, 해당 블록암호는 비선형 불변 공격에 안전하다고 볼 수 있다. 그러나 일반적으로 블록암호의 블록 크기가 64비트 보다 크기 때문에 U_{E_k}에 속하는 모든 비선형 불변을 구하기 어렵다. 따라서 **정리4**의 식 (2)에 포함된 부분집합 중 하나가 $\{0,1\}$임을 보여 저항성을 주장하는 것이 일반적이다. [3]에서는 $U_{\mathcal{P}} \cap U_{k_1 \oplus rc_1} \cap ... \cap U_{k_r \oplus rc_r}$에 속할 수 있는 비선형 불변이 0 또는 1이거나 선형임을 보여 다양한 암호가 비선형 불변 공격에 충분한 저항성이 있음을 보였다.

III. S-Box의 비선형 불변 도출 방법

정리2에서 언급한 바와 같이 S-Layer($\mathcal{S}$)에 대한 비선형 불변 집합 $U_{\mathcal{S}}$의 부분집합은 S-Box(s)의 비선형 불변 집합 U_s를 통해 도출될 수 있다. 본 장에서는 s의 비선형 불변 집합 U_s를 구하는 세 가지 알고리즘을 비교한다.

3.1 도출 방법-1

[1]에서 제안한 방법은 $|s|$가 s의 비트 크기일 때, $\mathcal{B}_{|s|}$의 단항식들(β_{mono})을 기저(basis)로 갖는 행렬 $M_s \in F_2^{2^{|s|}} \times F_2^{2^{|s|}}$을 통해 U_s를 구할 수 있다. M_s의 각 행은 각기 다른 단항식 $m_i \in \beta_{mono}$과 s의 연산식을 통해 구한 벡터값 $[m_i(\mathbb{X}) \oplus m_i(s(\mathbb{X}))]_{\beta_{mono}}$으로 구성된다. β_{mono}의 첫 번째 기저가 $m_0 = 1$일 때, $\mathbb{S}_0^T \times M_s = \mathbf{0}$을 만족하는 $\mathbb{S}_0^T$와 $\mathbb{S}_1^T \times M_s = \{1,0,...,0\}$ 만족하는 $\mathbb{S}_1^T$가 $g \in U_s$의 벡터값 $[g]_{\beta_{mono}}$가 된다. 따라서 $[U_s]_{\beta_{mono}} = \mathbb{S}_0^T \cup \mathbb{S}_1^T$임을 알 수 있고, **정리 5**를 도출할 수 있다.

정리5. $f : F_2^n \rightarrow F_2^n$의 비선형 불변 집합($U_f \subset \mathcal{B}_n$)는 $\{0,1\} \subset U_f$인 부분 공간(subspace)이다.

표 1 S-Box의 비선형 불변 도출 방법 비교

	방법-1	방법-2	방법-3
관련 S-Box 정보	Algebraic Normal Form	Cycle Decomposition	Correlation Matrix
하나의 비선형 불변 도출 복잡도	$O(2^{3\|s\|})$	$O(2^{2\|s\|})$	$O(2^{2^{\|s\|}})$
모든 비선형 불변 도출 복잡도	$O(2^{3\|s\|})$	홀수 Cycle 존재 : $O(2^{2\|s\|})$ 짝수 Cycle만 존재 : $O(2^{2^{\|s\|}})$	$O(2^{2^{\|s\|}})$
특정 Degree를 갖는 비선형 불변만 도출	가능	불가능	불가능
여러 라운드 확장 가능성	불가능	불가능	가능

3.2 도출 방법-2

3.1절에서 소개된 방법은 복잡도가 $O(2^{3|s|})$이기 때문에 $|s|$가 큰 경우에는 실용적이지 못하다. [1]에서는 더 큰 S-Box의 비선형 불변을 도출하기 위해 s를 구성하는 cycle을 이용한 방법을 제시했다. 해당 방법은 s를 구성하는 cycle들의 주기 중에 적어도 하나가 홀수일 때, $O(2^{2|s|})$복잡도에 U_s의 기저를 구할 수 있다.

3.3 도출 방법-3

S-Box의 Correlation Matrix[4]를 이용한 방법으로도 U_s를 도출할 수 있다. [2]에서 제안된 이 방법은 모든 $g \in U_s$의 Walsh Coefficient가 s의 Correlation Matrix $C_s \in Q^{2^{|s|}} \times Q^{2^{|s|}}$의 Eigenvalue λ를 1 또는 -1로 갖는 Eigenspace $E_{\lambda=1}$, $E_{\lambda=-1}$에 속함을 이용했다. 따라서 C_s의 Eigenspace를 계산하는 복잡도 이외에 $E_{\lambda=1}$, $E_{\lambda=-1}$에 속하는 원소 중 불함수의 Walsh Coefficient를 찾는 부가적인 연산이 요구된다. 그러나 C_s를 이용한 방법은 여러 라운드 함수의 비선형 불변을 얻어내는 이론적 기반이 된다.

3.4 도출 방법 비교

$|s|$ 크기를 갖는 S-Box s의 0 또는 1이 아닌 비선형 불변의 존재성을 보이기 위한 복잡도는 cycle을 이용한 두 번째 방법이 가장 효율적이다. 하지만 S-Box가 짝수 cycle만 존재하는 경우에 방법-2의 복잡도가 방법-1에 비해 커짐을 확인할 수 있다. 표 1은 세 가지 방법의 비교를 보여 준다.

IV. 적용 결과

본 장에서는 Ⅲ장에서 언급한 방법들을 PRINTcipher[5], GIFT[6], MIDORI[7], PRINCE[9], SKINNY[10], PRESENT[8], AES[12], ARIA[13], RECTANGLE[11], SCREAM[14]의 S-Box에 적용한 결과를 보인다.

4.1 저항성 판단을 위한 기준

정리 4에서 언급한 바와 같이 U_s에 포함된 비선형 불변은 다수의 라운드 키 연산에 대해서도 비선형 불변이어야 공격에 사용될 수 있다. 따라서 U_s에 포함된 비선형 불변 중 선형구조(linear structure)을 가진 것만 공격에 이용될 가능성이 있다. [1]에서 제안된 구별 공격은 사용한 비선형 불변의 balanced 여부가 공격의 성공 확률에 영향을 미친다. 따라서 본 논문에서는 S-Box의 모든 비선형 불변을 Ⅲ장에서 언급한 방법들로부터 구하고, 해당 비선형 불변의 선형구조 및 balanced 여부를 확인하였다.

4.2 결과 및 해석

SageMath Version 8.7[15]을 이용하여 Ⅲ장에서 언급한 세 가지 방법을 구현하였다*. S-Box를 구성하는 cycle 중 적어도 하나는 홀수 주기를 갖는 경우가 대부분이고, 구성 cycle의 개수가 적기 때문에 방법-2가 방법-1에 비해 효율적으로 U_s의 기저를 도출하였다.

표 2는 방법-2를 통해 얻은 결과이다. $|U_s|$가 큰 경우, 해당하는 모든 비선형 불변의 선형구조, balanced 여부를 확인하기 어렵기 때문에 해당 결과를 얻을 수 없었다.

$g \in LSU_s - \{0,1\}$가 존재할 경우 S-Box는 비선형 불변 공격에 취약할 가능성이 있다. GIFT의 S-Box와 SKINNY의 8비트 S-Box를 제외한 모든 S-Box에서는 이런 g를 가지고 있었다. 특히 MIDORI의 S-Box($s = s^{-1}$)는 주기가 1 또는 2만 갖는 cycle로 구성되어 있어 상대적으로 큰 LSU_s를 가짐을 알 수 있었다.

U_s와 $U_{\mathcal{P}\circ s}$의 연관성을 확인하기 위해 PRESENT와 GIFT의 16비트 버전인 SMALLPRESENT16 및 SMALLGIFT16의 비선형 불변을 도출해 보았다. GIFT의 $|U_s|$는 PRESENT에 비해 작은 값을 가짐에도 불구하고 GIFT의 부분적인 $\mathcal{P}$연산을 포함한 SMALLGIFT16의 U_s는 SMALLPRESENT16보다 상당히 큼을 알 수 있었다. 이는 SMALLGIFT16의 $\mathcal{P}$연산을 사용하고 S-Box를 SMALLPRESENT16의 S-Box를 사용한 VARSMALLGIFT16에서도 유사한 결과를 보였다. 이를 통해 $U_{\mathcal{P}\circ s}$의 성질을 단순히 U_s만으로 파악하기에는 어려움이 있음을 알 수 있다.

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

비선형 불변과 $\mathcal{P} \circ \mathcal{S}$의 연산 반복 횟수(라운드 수)와의 연관성을 확인해 보기 위해 SMALLPRESENT16의 두 라운드 함수 사이에 임의의 16-bit 키 500개를 연산시켜 얻은 $|U_s|$의 평균값을 측정해 보았다. SMALLPRESENT16의 라운드 함수의 비선형 불변의 개수(=16)가 상대적으로 적음에도 불구하고, 두 라운드 함수 연산을 시행하여 얻은 비선형 불변의 평균 개수(=$2^{16.61}$)개로 상당한 차이가 있음을 알 수 있었다. 이는 $\mathcal{P} \circ \mathcal{S}$의 비선형 불변 존재성만으로 여러 라운드 함수($R_{k_i \oplus rc_i} \circ \ldots \circ R_{k_1 \oplus rc_1}$)로 구성된 블록암호의 비선형 불변 존재성을 전적으로 표현하기에 어려움이 있음을 보여주는 결과이다.

표 2 비선형 불변 도출 결과 : ARIA는 두 개의 S-Box 중 AES와 다른 S-Box의 결과값이다.

블록암호	$\|s\|$	$\|U_s\|$	$\|LSU_s\|$	$\|BLSU_s\|$
PRINT	3	8	4	0
PRESENT	4	16	4	0
MIDORI	4	1024	72	26
PRINCE	4	32	12	6
RECTANGLE	4	32	8	4
GIFT	4	4	2	0
SKINNY	4	16	4	0
	8	4096	2	0
AES	8	32	4	0
ARIA	8	128	4	0
SCREAM	8	8192	2056	1094
SMALLPRESENT16	16	16	2	0
SMALLGIFT16	16	2^{36}	-	-
VARSMALLGIFT16	16	2^{32}	-	-
SMALLPRESENT16 -2 rounds	16	$2^{16.61}$	-	-

V. 결론

본 논문에서는 S-Box의 비선형 불변을 도출하기 위한 알고리즘을 비교하고, 실제 블록암호의 S-Box에 적용하였다. 도출한 결과를 통해 각 블록암호의 비선형 불변 공격에 대한 저항성을 확인해 볼 수 있었다. 향후에 도출된 S-Box의 비선형 불변을 통해 블록암호의 비선형 불변으로 확장 가능 여부를 검토해 볼 예정이다.

[참고문헌]

[1] Todo, Yosuke, Gregor Leander, and Yu Sasaki. "Nonlinear invariant attack." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2016.

[2] Beyne, Tim. "Block cipher invariants as eigenvectors of correlation matrices." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2018.

[3] Beierle, Christof, et al. "Proving resistance against invariant attacks: How to choose the round constants." Annual International Cryptology Conference. Springer, Cham, 2017.

[4] Daemen, Joan, et al. "Correlation matrices." International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 1995.

[5] Knudsen, Lars, et al. "PRINTcipher: a block cipher for IC-printing." International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2010.

[6] Banik, Subhadeep, et al. "GIFT: a small present." International Conference on Cryptographic Hardware and Embedded Systems. Springer, Cham, 2017.

[7] Banik, Subhadeep, et al. "Midori: a block cipher for low energy." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2015.

[8] Bogdanov, Andrey, et al. "PRESENT: An ultra-lightweight block cipher." International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2007.

[9] Borghoff, Julia, et al. "Prince – a low-latency block cipher for pervasive computing applications." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2012.

[10] Beierle, Christof, et al. "The SKINNY family of block ciphers and its low-latency variant MANTIS." Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 2016.

[11] Zhang, Wentao, et al. "RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms." Science China Information Sciences 58.12 (2015): 1-15.

[12] NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," November 2001.

[13] Kwon, Daesung, et al. "New block cipher: ARIA." International Conference on Information Security and Cryptology. Springer, Berlin, Heidelberg, 2003.

[14] Grosso, Vincent, et al. "SCREAM & iSCREAM side-channel resistant authenticated encryption with masking." Submission to CAESAR (2014).

[15] Stein, W.A.: The Sage Development Team: Sage Mathematics Software (2016). http://sagemath.org

[16] Leander, Gregor, et al. "A cryptanalysis of PRINTcipher: the invariant subspace attack." Annual Cryptology Conference. Springer, Berlin, Heidelberg, 2011.

[17] Biryukov, Alex, and David Wagner. "Slide attacks." International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 1999.