情報保護學會論文誌
第17卷 第3號, 2007. 6

유한체 연산 기반의 치환상자 설계 및 변환 영역 특성 분석

진 석 용,[1†‡] 백 종 민[2], 송 홍 엽[1]
[1]연세대학교 전기전자공학과, [2]홈캐스트 부설연구소

Modification of Finite Field Based S-box and Its Transform Domain Analysis

Seok-Yong Jin,[1†‡] Jong-Min Baek[2], Hong-Yeop Song[1]
[1]YONSEI UNIVERSITY, [2]HOMECAST CO., LTD

요 약

본 논문에서는, 기존의 암호시스템에 사용되는 치환상자(S-box)를 변형시키는 방법을 제안한다. 제안된 기법은 부울(Boolean) 함수의 벡터공간 상에서의 표현을 유한체 상에서의 다항식으로 변환하는 방법을 이용한다. Rijndael 암호시스템의 치환상자에 제안된 기법을 적용하여, 치환상자를 구성하는 부울 함수의 선형복잡도가 증가한 새로운 치환상자를 생성한다. 변환 영역 해석 (Transform Domain Analysis)을 중심으로 이들의 암호학적 특성을 분석한다.

ABSTRACT

In this paper, we propose a simple scheme which produces a new S-box from a given S-box. We use well-known conversion technique between the polynomial functions over a finite field F_{2^n} and the boolean functions from F_2^n to F_2. We have applied this scheme to Rijndael S-box and obtained 29 new S-boxes, whose linear complexities are improved. We investigate their cryptographic properties via transform domain analysis.

Keywords : *S-box, Rijndael, Transform Domain Analysis*

I. 서 론

치환상자(S-box)의 성질이 암호시스템 전체의 성능에 매우 결정적인 역할을 한다는 것은 Shannon의 SP-네트워 이론[15] 이후에 잘 알려져 왔다. 치환상자는 주로 메모리에 저장된 표에서 위치를 찾는 방식으로 구현되므로 빠른 동작속도를 요구하는 암호화 시스템에 적합하다. 대부분의 널리 사용되는 블록 암호 및 일부 스트림 암호 시스템은 다양한 치환상자를 채택하고 있고, 더 좋은 치환상자를 설계하려는 시도가 많은 연구에서 이루어져 왔다[5].

암호학적으로 유용한 치환상자를 설계하는 여러 방법들이 제안되었는데, 이 중 유한체 상의 곱셈에 관한 역함수에(Finite Field Inversion Mapping: x^{-1}, $x \in GF(2^n)$) 기반을 둔 치환상자가 전통적인 블록암호 공격방법인 LC(Linear Cryptanalysis)[11]와 DC(Differential Cryptanalysis)[2]에 대하여 우수한 특성을 지닐[13] 뿐만 아니라, 비선형성 및 상관특성과 같은 측면에서도 우수하다는 것은 잘 알려져 있다. 실제로 SHARK, SQUARE, Rijndael[3, 4] 등 1996년 이후 표준으로 제안된 많은 암호 알고리듬에서 유한체 연산 기반의 치환

접수일: 2006년 8월 16일; 채택일: 2007년 4월 17일
† 주저자, ‡ 교신저자, sy.jin@yonsei.ac.kr

상자가 채택되었다.

Rijndael[3]은 2000년 10월 미국 NIST에 의하여 AES (Advanced Encryption Standard)로 채택되었고, 2001년 11월에 공표된[12] 블록암호 알고리듬으로서, Rijndael 치환상자 역시 함수 $f(x)=x^{-1}$, $x \in GF(2^8)$에 기반을 두고 있다. 그러나 이 함수는 보간 공격[8, 17]과(Interpolation Attack) 같은 대수적 공격에(Algebraic Attack) 취약할 수도 있으므로 Rijndael S-box는 역함수 이외에 출력 비트들 간의 일차 결합을(bitwise affine transformation) 추가하여 설계되었다[18].

Rijndael 알고리듬 및 치환상자 설계 및 분석에 관한 근래의 연구들은 주로 대수적 방법에 초점을 두고 있다. 한편으로는 Rijndael이 처음부터 DC와 LC같은 통계적 공격에 강인하도록 설계되었기 때문[4]이고, 다른 한편으로는 Rijndael S-box의 대수적 특성 때문이다. 즉, 우리가 bitwise affine transformation을 finite field inversion과 결합한다고 하더라도 Rijndael S-box를 구성하는 부울 함수들은 여전히 대수적으로 매우 간단한 형태로 표현될 수 있기 때문이다. Rijndael S-box의 각 출력 함수는 적당한 $\theta \in GF(2^8)$에 대해 $Tr(\theta x^{-1})$로 표현된다.

이 사실이 미치는 영향은 두 가지 측면에서 고려될 수 있다.

첫째, 모든 다변수 부울 함수는 유한체 상의 다항식 함수로 표현되며, 항상 trace 함수의 합으로 표현[7]되므로, Rijndael S-box의 출력함수는 대수적 표현(algebraic expression)에 있어 가장 간단한 형태이다. 즉, 가장 작은 선형복잡도를(linear complexity, linear span) 가진다. Gong과 Golomb은 1999년 그들의 논문[6]에서 여러 종류의 유사 DES[19] 암호시스템이 입력을 동반한 NLFSR(Nonlinear Feedback Shift Register with input)임을 입증함으로써, 치환상자가 일대일 단항식(bijective monomial)으로 근사화 되지 않아야 함을 제안한다[18]. 왜냐하면 임의의 c, $gcd(c, 2^n-1)=1$에 대하여 $Tr(\eta x^c)$과 $Tr(\lambda x)$ 모두 최저 선형복잡도를 갖는 최대길이수열(m-sequences)이기 때문이다[7]. 이 관점에서 Rijndael S-box를 개선하기 위한 시도, 즉 다른 암호학적 특성은 유지하면서, 복잡한 대수적 표현을 가지는 치환상자를 설계하려는 연구[9]가 제안되기도 했다.

둘째, Rijndael S-box를 구성하는 각각의 부울 함수 $a_i(x)$, $i=1,\cdots 8$는 affine 변환(affine transformation)에 관해 동치인(equivalent) 부울 함수들이다. 따라서 8개의 부울 함수 a_i 뿐만 아니라 a_i의 선형 결합으로 이루어진 255개의 모든 부울 함수가 서로 등가관계를 이루며 그 결과로, 255개 부울 함수의 Hadamard 변환 스펙트럼은 완벽하게 동일하다. Avalanche 변환의 경우도 마찬가지이다. 이는 대수적으로 매우 간단히 증명되는 아래 정리 때문이다

정리[5, Theorem 3.] The component output functions of finite field inversion are related by linear transform.

Fuller와 Millan은[5] $n \geq 6$에 대해 n-비트 입·출력 치환상자를 구성하는 출력함수의 모든 선형결합이 상호 동치(equivalent)인 것이 확률적으로 극히 드물게 발생하는 현상임을 컴퓨터 조사를 통해 관찰한다. 이를 근거로 2003년에 발표된 그들의 논문[5]에서 치환상자에 관한 새로운 randomness criterion, 즉 6비트 이상의 입·출력으로 구성된 치환상자의 출력함수 및 그 선형결합으로 이루어진 함수가 얼마나 다양한 equivalence class에 속하게 되는지 고려해야 한다는 테스트(equivalence class variety test)를 제안한다. (Rijndael S-box와 같이 완벽한 "linear redundancy"를 갖는 S-box의 안정성에 위협이 될 수 있는 공격방법에 대한 논의, 그리고 linear redundancy를 갖는 S-box로부터 자신들이 제안한 randomness criterion을 만족하는 S-box를 구성하는 알고리듬에 대해서는 같은 논문을 참조)

본 논문에서는 Rijndael S-box와 같이 유한체 연산에 기반을 둔 치환상자를 변형하여 새로운 치환상자를 설계하는 방법을 제안한다. 우선, Ⅱ장에서는 부울 함수의 표현과 관련된 내용을 소개하고, 암호시스템의 성능 분석에 자주 이용되는 몇몇 정의를 소개한다. Ⅲ장에서는 기존의 치환상자로부터 새로운 치환상자를 디자인하는 방법을 제안하고 예제를 통해 설명한다. Ⅳ장에서는 제안된 방법을 Rijndael S-box에 적용하여 29개의 새로운 치환상자를 생성하고, 그 특성들을 조사한다. 제안된 방법에 의해 생성된 치환상자는 선형복잡도 관점에서 크게 개선되었다. 그 중 일부는 변환 영역 특성이 Rijndael S-box와 동일하면서 선형복잡도는 증가되었고, 또 다른 일부는 equivalence class variety test를 만족하지만 변환 영역 특성에서는 단점을 내포한다. 마지막으로 Ⅴ장에서는 해결되지 않은 문제들에 관해 토의한다.

Ⅱ. 배경지식

2.1 부울 함수의 유한체 상 표현법

지금부터 2^n개의 원소를 가지는 유한체를 기호로 F_{2^n}로 표시하기로 한다.

n-변수 부울 함수 $g(x_{n-1},\cdots,x_0)$에 대하여, 아래와 같이 정의되는 Lagrange 복원법(Lagrange Interpolation)을 적용하면 $g(x_{n-1},\cdots,x_0)$의 유한체 상 다항식 표현 $f(x)$를 얻을 수 있다.

$$f(x)=\begin{cases} g(0,\cdots,0) & x=0 \\ \sum_{j=1}^{2^n-1} d_j x^j & x\in F_{2^n}^* \end{cases} \quad (1)$$

여기서, $j=1,\cdots,2^n-1$에 대하여 변수 d_j는 다음과 같이 계산된다.

$$d_j=\sum_{\lambda\in F_{2^n}^*} g(x_{n-1},\cdots,x_0)\lambda^{-j} \quad (2)$$

$\lambda=\sum_{i=0}^{n-1} x_i\alpha_i$는 유한체 F_{2^n}의 원소이며, $\{\alpha_0,\cdots,\alpha_{n-1}\}$는 F_{2^n}의 기저(basis)이다. 앞으로는 $\{\alpha_0,\cdots,\alpha_{n-1}\}$이 F_{2^n}의 기저라는 사실을 기호로 $F_{2^n}=\langle\{\alpha_0,\cdots,\alpha_{n-1}\}\rangle$과 같이 표현한다.

반대로, 유한체에서 정의된 다항식 함수로부터 벡터 공간에서 정의된 다변수 부울 함수 표현을 얻는 방법은 다음과 같다.

$$g(x_{n-1},\cdots,x_0)=f(x_0\alpha_0+\cdots+x_{n-1}\alpha_{n-1}) \quad (3)$$

여기서도 마찬가지로 기저는 $\{\alpha_0,\cdots,\alpha_{n-1}\}$이다. 즉, $F_{2^n}=\langle\{\alpha_0,\cdots,\alpha_{n-1}\}\rangle$. 본 논문에서 $f(\mathbf{x})=f(x_{n-1},\cdots,x_0)$, $\mathbf{x}\in F_2^n$과 $f(x)$, $x\in F_{2^n}$ 두 가지 모두를 n-변수 부울 함수로 지칭한다.

2.2 변환 영역 해석 도구(Transform Domain Analysis Tools)

암호학적 함수를 변환 영역 해석 도구를 이용하여 분석한 대표적인 예로는, DES[19] 암호시스템의 치환상자를 분석[6]한 경우를 들 수 있다. 본 절에서는 부울 함수의 암호학적 특성을 파악하는 도구로 자주 사용되는 몇 가지 정의를 소개한다[7].

$f(x)$, $x\in F_{2^n}$(혹은 $f(\mathbf{x})=f(x_{n-1},\cdots,x_0)$, $\mathbf{x}\in F_2^n$)를 n-변수 부울 함수라 하자. $f(x)$의 Hadamard 변환(Transform)은 다음과 같이 정의된다:

$$\hat{f}(\lambda)=\sum_{x\in F_{2^n}} (-1)^{Tr(\lambda x)+f(x)},\ \lambda\in F_{2^n}.$$

n-변수 부울 함수 f의 비선형도 (Nonlinearity) N_f는 다음과 같이 정의된다.

$$N_f=\min_{\mathbf{w}\in F_2^n,\, c\in F_2} d(f(\mathbf{x}),\mathbf{w}\cdot\mathbf{x}+c).$$

여기서 $d(\mathbf{x},\mathbf{y})$는 두 벡터 $\mathbf{x}$와 $\mathbf{y}$사이의 해밍 거리(Hamming Distance)이다. 부울 함수의 비선형도는 Hadamard 변환을 이용한 아래 식에 의해서 쉽게 계산된다.

$$N_f=2^{n-1}-\frac{1}{2}\max_{\lambda\in F_{2^n}} |\hat{f}(\lambda)| \quad (4)$$

$f(x)$의 Avalanche 변환은 다음과 같이 정의된다. $\mathbf{w}\in F_2^n$에 대하여,

$$(f*f)(\mathbf{w})=F(\mathbf{w})=\sum_{\mathbf{x}\in F_2^n}(-1)^{f(\mathbf{x}+\mathbf{w})+f(\mathbf{x})}.$$

부울 함수 f가 해밍 무게(Hamming Weight) $wt(\mathbf{w})=1$인 모든 $\mathbf{w}\in F_2^n$에 대하여 $F(\mathbf{w})=0$일 때, f는 SAC (Strict Avalanche Criterion)를 충족시킨다고 한다.

2.3 부울 함수의 등가성(equivalence)

f와 g를 두 개의 n-변수 부울 함수라 하자. 만약 역행렬이 존재하는 n차 이진 정방행렬 D, 길이가 n인 이진 행벡터 $\mathbf{a}$와 $\mathbf{b}$, 그리고 이진 상수 c가 존재해서 모든 $\mathbf{x}\in F_2^n$에 대하여 다음 식을 만족할 때, 두 개의 부울 함수 f와 g는 등가(equivalent) 관계에 있다고 말한다[5].

$$g(\mathbf{x})=f(D\mathbf{x}^T\oplus\mathbf{a}^T)\oplus\mathbf{b}\cdot\mathbf{x}^T\oplus c$$

2.4 Rijndael S-box

n-비트 입출력 모드에서 동작하는 치환상자의 입력 $\mathbf{x}\in F_2^n$에 대한 출력을 $s(\mathbf{x})=(s_{n-1}(\mathbf{x}),\cdots,s_1(\mathbf{x}),s_0(\mathbf{x}))$로 표현했을 때, $i=0,\cdots,n-1$에 대한 각각의 $s_i(\mathbf{x})$를 치환상자의 구성함수(coordinate function) 또는 출력함수

(output function)라고 한다. 식 (3)에 의하여, $s_i(\mathbf{x})$, $\mathbf{x}\in F_2^m$를 앞으로는 유한체 상의 표기법을 이용하여 $s_i(x)$, $x=x_0b_0+\cdots x_{n-1}b_{n-1}\in F_{2^n}$와 같이 나타내기로 하자. 단 $F_{2^n}=\langle\{b_0,\cdots,b_{n-1}\}\rangle$.

Rijndael S-box[3]의 대수적 표현은 다음과 같이 구해진다[9, 18].

$$
\begin{aligned}
s_0(x) &= Tr(\beta^{166}x^{-1})+1 = Tr(\beta^{83}x^{127})+1\\
s_1(x) &= Tr(\beta^{53}x^{-1})+1 = Tr(\beta^{154}x^{127})+1\\
s_2(x) &= Tr(\beta^{36}x^{-1}) = Tr(\beta^{18}x^{127})\\
s_3(x) &= Tr(\beta^{11}x^{-1}) = Tr(\beta^{133}x^{127})\\
s_4(x) &= Tr(\beta^{72}x^{-1}) = Tr(\beta^{36}x^{127})\\
s_5(x) &= Tr(\beta^{76}x^{-1})+1 = Tr(\beta^{38}x^{127})+1\\
s_6(x) &= Tr(\beta^{51}x^{-1})+1 = Tr(\beta^{153}x^{127})+1\\
s_7(x) &= Tr(\beta^{26}x^{-1}) = Tr(\beta^{13}x^{127})
\end{aligned}
\tag{5}
$$

여기서 β는 기약다항식(irreducible polynomial) $g(z)=z^8+z^4+z^3+z^1+1$에 의해 정의된 유한체 F_{2^8}의 원시원소(primitive element)이며, $g(z)$의 근 α에 대하여 다항식 기저(polynomial basis) $\{\alpha^0,\alpha^1,\cdots,\alpha^7\}$를 이용했을 때, $x=x_0\alpha^0+x_1\alpha^1+\cdots x_7\alpha^7\in F_{2^8}$이다.

Ⅲ. 기존의 치환상자를 이용한 새로운 치환상자의 설계법

본 장에서는 기존의 치환상자로부터 새로운 치환상자를 디자인하는 알고리듬을 제안한다. 편의상 작은 크기, 즉 4-비트 입출력 모드에서 동작하는 치환상자의 예를 통해 설명하도록 한다.

〔표 1〕 F_{2^4}에서 정의된 치환상자 SB-0와 변형된 치환상자 SB-1, SB-2

	00	01	10	11
00	0	1	f	a
01	8	6	5	9
10	4	7	3	e
11	d	c	b	2

SB-0

	00	01	10	11
00	0	1	a	f
01	6	8	5	9
10	2	b	d	c
11	3	e	7	4

SB-1

	00	01	10	11
00	0	c	7	0
01	6	7	4	7
10	e	2	e	6
11	8	a	5	a

SB-2

〔표 1〕에 표시된 세 개의 치환상자를 살펴보기로 하자. 치환상자 SB-0는, 4차 이진 기약다항식 $g_0(z)=z^4+z^3+z^2+z^1+1$를 이용하여 정의된 유한체 F_O에서의 곱셈에 관한 역원 ($s(x)=x^{-1}$)으로 정의된 치환상자로서, 16진법으로 표시되었다. 아래에서 설명하는 알고리듬을 이용하여 두 개의 새로운 치환상자 SB-1과 SB-2를 설계하고자 한다.

SB-0를 구성하는 네 개의 부울 함수 각각의 F_O 위에서의 다항식 표현은, Ⅱ장에서 설명한 Lagrange 복원법에 의하여 다음과 같이 구할 수 있다.

$$
\begin{aligned}
&s(x)=(s_3(x),s_2(x),s_1(x),s_0(x)),\\
&s_3(x)=Tr_1^4(\beta^{14}x^7)\\
&s_2(x)=Tr_1^4(\beta^{7}x^7)\\
&s_1(x)=Tr_1^4(\beta^{10}x^7)\\
&s_0(x)=Tr_1^4(\beta^{8}x^7)
\end{aligned}
\tag{6}
$$

여기서 F_O를 정의하는 기약다항식 $g_0(z)$의 근 α에 대하여 $\beta\triangleq 1+\alpha$는 F_0의 원시원소이며, $x=x_0b_0+x_1b_1+x_2b_2+x_3b_3\in F_O$, $F_O\cong\langle\{b_i|b_i=\alpha^i,i=0,1,2,3\}\rangle$이다. 이 때, (x_3,x_2,x_1,x_0)는 SB-0의 입력 비트열이다.

이제, F_O와 마찬가지로 2^4개의 원소를 갖지만, 곱셈이 $(\mathrm{mod}\ \ g_1(z)=z^4+z^3+1)$에 의해 수행되는 유한체를 F_C라 하자. 이 때, SB-0를 구성하는 부울 함수의 F_C 위에서의 다항식 표현은 다음과 같다.

$$
\begin{aligned}
&r(x)=(r_3(x),r_2(x),r_1(x),r_0(x)),\\
&r_3(x)=Tr_1^4(\gamma^{10}x^1+\gamma^{12}x^3+\gamma^{14}x^7)+Tr_1^2(\gamma^{10}x^5)\\
&r_2(x)=Tr_1^4(\gamma^{3}x^1+\gamma^{4}x^3+\gamma^{5}x^7)+Tr_1^2(x^5)\\
&r_1(x)=Tr_1^4(\gamma^{9}x^1+\gamma^{10}x^3+\gamma^{13}x^7)+Tr_1^2(\gamma^{5}x^5)\\
&r_0(x)=Tr_1^4(\gamma^{2}x^1+\gamma^{13}x^3+\gamma^{16}x^7)+Tr_1^2(\gamma^{5}x^5)
\end{aligned}
\tag{7}
$$

여기서 $x=x_0c_0+x_1c_1+x_2c_2+x_3c_3\in F_C$, $F_C\cong\langle\{c_i|c_i=\gamma^i,\ i=0,1,2,3\}\rangle$이고, γ는 $g_1(z)$의 근으로서 F_C의 원시원소이다.

〔표 1〕에서 SB-1이라고 지칭한 새로운 치환상자를 구성하는 부울 함수의 다항식 표현을 찾기 위하여, 식

(7)의 계수들을 (γ의 거듭제곱이 아닌) β의 거듭제곱으로 치환한다. 계수 치환에 의해 다음의 네 개의 부울 함수 h_3, h_2, h_1, h_0를 얻을 수 있고, 이들은 새로운 치환상자의 구성함수(coordinate function)가 된다.

$$h_3(x) = Tr_1^4(\beta^{10}x + \beta^{12}x^3 + \beta^{14}x^7) + Tr_1^2(\beta^{10}x^5)$$
$$h_2(x) = Tr_1^4(\beta^{3}x + \beta^{4}x^3 + \beta^{5}x^7) + Tr_1^2(x^5)$$
$$h_1(x) = Tr_1^4(\beta^{9}x + \beta^{10}x^3 + \beta^{13}x^7) + Tr_1^2(\beta^{5}x^5)$$
$$h_0(x) = Tr_1^4(\beta^{2}x + \beta^{13}x^3 + \beta^{6}x^7) + Tr_1^2(\beta^{5}x^5)$$

마지막으로, SB-1을 구성하기 위하여 네 개의 부울 함수를 F_O 위에서 계산하여, 즉 곱셈을 $(\mathrm{mod}\, g_0(z))$로 수행하여, 모든 입력에 대한 출력을 진리표(Truth Table) 형태로 작성한다.

4차 이진 기약다항식은 총 3개 이므로, $g_0(z)$와 $g_1(z)$ 이외에 새로운 기약다항식 $g_2(z) = z^4 + z^1 + 1$를 이용해도 새로운 치환상자를 구성할 수 있다. $g_2(z)$에 의해 곱셈 구조가 정의된 유한체를 F_D라 했을 때, 비슷한 방법으로 SB-0를 구성하는 부울 함수의 다항식 표현을 F_D 상에서 구하면 다음과 같다.

$$\begin{aligned} t(x) &= (t_3(x), t_2(x), t_1(x), t_0(x)), \\ t_3(x) &= Tr_1^4(\delta^{2}x^1 + \delta^{9}x^3 + \delta^{10}x^7) + Tr_1^2(\delta^{5}x^5) \\ t_2(x) &= Tr_1^4(\delta^{4}x^1 + \delta^{12}x^3 + \delta^{12}x^7) + Tr_1^2(x^5) \\ t_1(x) &= Tr_1^4(\delta^{6}x^1 + \delta^{2}x^3 + \delta^{14}x^7) + Tr_1^2(x^5) \\ t_0(x) &= Tr_1^4(\delta^{11}x^1 + \delta^{11}x^3 + \delta^{2}x^7) + Tr_1^2(\delta^{10}x^5) \end{aligned} \quad (8)$$

여기서 $x = x_0 d_0 + x_1 d_1 + x_2 d_2 + x_3 d_3 \in F_D$, $F_D \cong \langle \{d_i \mid d_i = \delta^i,\ i = 0,1,2,3\} \rangle$이고, δ는 $g_2(z)$의 근으로서 F_D의 원시원소이다. 식 (8)에서 계수인 δ의 거듭제곱을 β의 거듭제곱으로 치환함으로서, 또 다른 네 개의 부울 함수 u_3, u_2, u_1, u_0를 얻을 수 있다.

$$u_3(x) = Tr_1^4(\beta^{2}x + \beta^{9}x^3 + \beta^{10}x^7) + Tr_1^2(\beta^{5}x^5)$$
$$u_2(x) = Tr_1^4(\beta^{4}x + \beta^{12}x^3 + \beta^{12}x^7) + Tr_1^2(x^5)$$
$$u_1(x) = Tr_1^4(\beta^{6}x + \beta^{2}x^3 + \beta^{14}x^7) + Tr_1^2(x^5)$$
$$u_0(x) = Tr_1^4(\beta^{11}x + \beta^{11}x^3 + \beta^{2}x^7) + Tr_1^2(\beta^{10}x^5)$$

이 부울 함수들을 모든 입력 x에 대하여 F_O 위에서 계산함으로써, 즉 곱셈을 $(\mathrm{mod}\, g_2(z))$가 아닌 $(\mathrm{mod}\, g_o(z))$로 수행함으로써 〔표 1〕의 또 다른 치환상자 SB-2를 생성할 수 있다.

SB-1과 SB-2 모두 SB-0로부터 같은 방법으로 설계된 치환상자임에도 불구하고, SB-1은 일대일 대응이고 SB-2는 그렇지 않다. SB-1과 SB-2이 서로 다른 특성을 가지는 현상은 V장에서 다시 언급될 것이다.

Ⅳ. 제안된 알고리듬을 Rijndael 치환상자에 적용시킨 경우: 설계 및 분석

지금부터는 Ⅲ장에서 제안하고 설명한 디자인 방법을 Rijndael 알고리듬의 치환상자(BOX-0라고 부르기로 한다)에 적용하고자 한다. Ⅲ장과 유사한 기호를 사용하며, 다만 $g_0(z)$, $g_1(z)$, 그리고 $g_2(z)$는 차수가 8인 이진 기약다항식으로서 아래와 같다:

$$g_0(z) = z^8 + z^4 + z^3 + z^1 + 1,$$
$$g_1(z) = z^8 + z^4 + z^3 + z^2 + 1,$$
$$g_2(z) = z^8 + z^5 + z^3 + z^1 + 1$$

여기서 $g_0(z)$는 Rijndael 알고리듬에서 정의된 유한체 F_{2^8}의 곱셈을 정의하는 기약다항식이고, $g_1(z)$과 $g_2(z)$ 각각은 임으로 선택된 차수가 8인 이진 기약다항식으로서 원시다항식(primitive polynomial)이다.

4.1 $g_1(z)$를 이용한 경우

F_O를 $g_0(z)$에 의해 곱셈 규칙이 정의된, 2^8개의 원소를 가지는 유한체라고 할 때, BOX-0를 구성하는 여덟 개의 부울 함수의 F_O 위에서의 다항식 표현 $s_i(x)$, $i = 0,1,\cdots,7$, $x \in F_O$는 식 (5)와 같다.

반면에 F_C를 $g_1(z)$에 의해 정의된 유한체, 즉 F_C상에서의 곱셈은 $(\mathrm{mod}\ \ g_1(z))$로 계산되는 유한체라 했을 때, 동일한 부울 함수의 F_C 위에서의 다항식 표현 $r_i(x)$, $i = 0,1,\cdots,7$, $x \in F_C$은 $s_i(x)$보다 훨씬 더 복잡한 형태를 가지고 있다. 예를 들어, $r_7(x)$는 아래와 같다.

$$\begin{aligned} r_7(x) = {} & Tr_1^2(\gamma^{85}x^{85}) \\ & + Tr_1^4(\gamma^{238}x^{17} + \gamma^{34}x^{51} + \gamma^{136}x^{119}) \\ & + Tr_1^8(\gamma^{4}x^1 + \gamma^{43}x^3 + \cdots + \gamma^{13}x^{127}) \end{aligned} \quad (9)$$

여기서 γ는 $g_1(z)$의 근으로서, F_C의 원시원소이다.

〔표 2〕 BOX-0의 F_C 위에서의 다항식 표현

k	n_k	r_7	r_6	r_5	r_4	r_3	r_2	r_1	r_0
	const	-	1	1	-	-	-	1	1
85	2	85	0	170	0	170	170	0	85
17	4	238	0	102	136	136	68	17	119
51	4	34	102	238	17	85	17	17	85
119	4	136	0	187	85	0	∞	187	51
1	8	4	129	65	213	52	83	14	127
3	8	43	251	43	12	233	23	174	30
5	8	60	163	162	197	79	57	166	24
7	8	3	19	50	233	134	193	246	119
9	8	54	221	120	97	33	139	159	33
11	8	155	31	242	163	92	∞	2	226
13	8	86	80	199	91	17	151	208	153
15	8	157	143	74	56	242	41	86	214
19	8	157	∞	231	16	99	148	65	251
21	8	48	28	69	3	190	33	106	136
23	8	163	48	100	173	16	198	248	120
25	8	98	78	37	9	197	242	225	72
27	8	50	29	25	115	16	157	189	167
29	8	92	74	21	220	162	25	71	174
31	8	67	49	69	157	233	130	107	35
37	8	69	253	52	155	32	6	219	230
39	8	181	145	68	145	114	121	12	91
43	8	1	125	168	228	244	242	217	58
45	8	2	253	127	200	25	64	133	164
47	8	194	246	233	173	43	102	108	119
53	8	110	23	129	77	16	133	245	136
55	8	145	173	74	35	6	143	159	64
59	8	105	65	121	186	228	90	182	108
61	8	246	176	111	176	17	161	213	100
63	8	192	252	141	80	142	81	213	178
87	8	45	7	157	61	230	6	98	78
91	8	20	239	73	76	251	20	123	94
95	8	160	236	186	66	236	222	156	248
111	8	144	41	149	35	167	32	154	210
127	8	13	141	14	91	90	220	166	71
	LS	254	247	255	254	254	242	255	255

식 (9)에서 축약된 부분 및 나머지 $r_i(x)$에 관해서는 〔표 2〕에 나타내었다.

〔표 3〕 BOX-1 (16진법 표기)

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	7b	77	6b	f2	6f	c5	76	ab	fe	d7	67	2b	01	30
1	82	ca	c9	7d	fa	59	f0	47	72	c0	a4	9c	af	a2	ad	d4
2	c3	23	04	c7	05	9a	96	18	eb	27	75	b2	12	07	80	e2
3	93	26	fd	b7	cc	f7	36	3f	d8	71	31	15	34	a5	f1	e5
4	fc	20	b1	5b	53	d1	ed	00	be	39	cb	6a	cf	58	4a	4c
5	1b	6e	a0	5a	83	09	2c	1a	b3	d6	52	3b	2f	84	e3	29
6	33	85	4d	43	fb	aa	d0	ef	f9	45	02	7f	50	3c	a8	9f
7	f5	38	92	9d	40	8f	a3	51	bc	b6	21	da	ff	10	f3	d2
8	16	bb	b0	54	2d	0f	99	41	8c	a1	0d	89	e6	bf	42	68
9	28	df	55	ce	e9	87	9b	1e	f8	e1	98	11	69	d9	94	8e
a	4b	bd	8a	8b	dd	e8	74	1f	2e	25	ba	78	b4	c6	a6	1c
b	c1	86	1d	9e	61	35	b9	57	b5	66	3e	70	0e	f6	48	03
c	ac	62	d3	c2	79	e4	91	95	06	49	24	5c	e0	32	0a	3a
d	ea	f4	6c	56	ae	08	7a	65	8d	d5	a9	4e	c8	e7	37	6d
e	ee	46	b8	14	de	5e	db	0b	90	88	2a	22	dc	4f	60	81
f	c4	a7	3d	7e	5d	64	19	73	17	44	5f	97	13	ec	0c	cd

〔표 2〕의 첫 번째 열은 Trace 함수로 표현된 다항식 함수에서 x의 지수를 나타내고, 두 번째 열은 Trace 함수의 종류를 가리킨다. 세 번째 열은 $r_7(x)$에서 계수들의 지수를 나타낸다. 그리고 $\gamma^{\infty}=0$이다. 〔표 2〕의 제일 마지막 행은 각각의 다항식 $r_i(x)$를 구성하는 항(monomial)의 수를 나타낸다. Ⅲ장의 식 (5)와 비교했을 때, 항의 수가 크게 늘어난 것을 쉽게 확인할 수 있다.

이제 Ⅲ장에서와 마찬가지 방법으로, $r_i(x)$에서 γ의 거듭제곱으로 이루어진 계수들을 F_O의 원시원소인 β의 거듭제곱으로 치환함으로써 새로운 여덟 개의 부울 함수 $h_i(x)$, $i=0,\cdots,7$를 생성할 수 있다. 예를 들어, $h_7(x)$는 식 (9)의 $r_7(x)$로부터 얻을 수 있다.

$$\begin{aligned} h_7(x) = {} & Tr_1^2(\beta^{85}x^{85}) \\ & + Tr_1^4(\beta^{238}x^{17}+\beta^{34}x^{51}+\beta^{136}x^{119}) \\ & + Tr_1^8(\beta^{4}x^{1}+\beta^{43}x^{3}+\cdots+\beta^{13}x^{127}) \end{aligned} \tag{10}$$

마지막으로 $h_i(x)$를 모든 입력 x에 대하여 유한체 F_O 위에서 계산함으로써, 즉 곱셈을 $(\mathrm{mod}\, g_0(z))$로 수행함으로써 BOX-0와 같은 크기의 새로운 치환상자 BOX-1(〔표 3〕 참조)을 생성할 수 있다.

지금부터 새로이 설계된 BOX-1의 성질을, 현재

AES 표준으로 채택된 Rijndael 알고리듬의 치환상자 BOX-0와 비교하며 살펴보도록 하자. $h_i(x)$는 BOX-1을 구성하는 부울 함수를, $s_i(x)$는 BOX-0를 구성하는 부울 함수를 지칭한다.

1. BOX-1은 일대일 대응이다. (BOX-0와 동일)
2. BOX-1을 구성하는 개개의 부울 함수에서 '0'과 '1'의 개수가 같다(Balanced). (BOX-0와 동일)
3. ANF (Algebraic Normal Form) 비교: 진리표로부터 부울 함수의 ANF을 계산하는 방법은 잘 알려져 있다[14]. 선형계획법을 이용하여 Rijndael S-box를 구성하는 부울함수의 ANF를 구할 수도 있다[1]. 아래 표는 h_i와 s_i 각각의 ANF에서 일차항의 수와 최고차 항인 7차 항의 수를 나타낸다. h_i모두 7차 항을 가지고 있으므로 ANF 측면에서 BOX-1은 BOX-0와 유사한 성능을 갖고 있다.

	h_0	h_1	h_2	h_3	h_4	h_5	h_6	h_7
1차 항의 개수	4	3	4	4	6	3	3	3
7차 항의 개수	4	4	5	1	5	4	3	3
	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7
1차 항의 개수	6	4	6	4	6	2	4	4
7차 항의 개수	5	4	2	4	2	3	4	4

4. 선형 복잡도 비교: s_i에 비하여 h_i의 선형 복잡도는 크게 증가하였다.(최대값: 255)

	h_0	h_1	h_2	h_3	h_4	h_5	h_6	h_7
선형복잡도	255	255	242	254	254	255	247	254
	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7
선형복잡도	9	9	8	8	8	9	9	8

5. Hadamard 변환의 스펙트럼 분석 및 비선형도: Hadamard 변환의 절대값 최대치는 부울 함수의 비선형도 및 1차 상관 면역도와 관련되어 있다[7]. BOX-1의 Hadamard 변환 스펙트럼은 BOX-0의 스펙트럼과 정확히 동일하며, 따라서 식 (4)에 의한 비선형도 역시 112로 일치한다.

Absolute HT value	0	4	8	12	16	20	24	28	32
$h_i,\ 0 \le i < 8$	17	48	36	40	34	24	36	16	5
$s_i,\ 0 \le i < 8$	17	48	36	40	34	24	36	16	5

6. Avalanche 변환의 스펙트럼 분석 및 그 결과: BOX-1과 BOX-0의 Avalanche 변환 스펙트럼 역시 정확히 일치한다. 따라서 BOX-1을 구성하는 부울 함수 h_i와 BOX-0의 구성 함수 s_i가 모두 등가관계에 있을 가능성이 있다. 아래의 정리는 이 사실을 입증한다.

Absolute AT value	0	8	16	24	32	Total
$h_i,\ 0 \le i < 8$	32	84	74	52	13	255
$s_i,\ 0 \le i < 8$	32	84	74	52	13	255

정리 1. $\Gamma = \{s_0, s_1, \cdots, s_7, h_0, h_1, \cdots, h_7\}$를 BOX-0와 BOX-1을 구성하는 모든 부울 함수들의 모임이라고 하자. Γ의 어떤 두 부울 함수도 서로 등가관계에 있다.

(증명) 모든 $i=0,1,\cdots,7$에 대하여 적당한 $\theta_i \in F_{2^8}$와 $e_i \in F_2$가 존재해서 $s_i(x) = Tr(\theta_i x^{-1}) + e_i$이므로 (식 (5) 참조) $0 \le i,j \le 7$에 대하여 s_i와 s_j는 서로 등가 관계에 있음은 분명하다[5]. 나아가 s_i와 h_i의 등가관계를 입증하기 위해서는 모든 $\mathbf{x} \in F_2^8$에 대하여 $h_i(\mathbf{x}) = s_i(D_i\mathbf{x}^{\mathbf{T}}) + c_i$를 만족하는 이진 정방행렬 D_i와 상수 c_i가 존재해야 한다. 모든 $i=0,\cdots,7$에 대하여 아래의 D_i와 c_i가 존재하여 요구되는 조건을 만족한다. 단 D_i 행렬은 10진법으로 표시하였다. 즉, D_o의 첫 번째 열 11_d는 $[00001011]^T$의 십진법 표기이다.

$$D_0 = [11_d\ 148_d\ 182_d\ 82_d\ 224_d\ 8_d\ 105_d\ 31_d]$$

$$D_1 = [51_d\ 150_d\ 235_d\ 156_d\ 223_d\ 77_d\ 28_d\ 1_d]$$

$$D_2 = [47_d\ 78_d\ 142_d\ 86_d\ 149_d\ 164_d\ 62_d\ 240_d]$$

$$D_3 = [35_d\ 112_d\ 68_d\ 4_d\ 213_d\ 186_d\ 121_d\ 129_d]$$

$$D_4 = [26_d\ 94_d\ 156_d\ 1_d\ 172_d\ 55_d\ 85_d\ 124_d]$$

$$D_5 = [42_d\ 101_d\ 4_d\ 220_d\ 237_d\ 35_d\ 247_d\ 191_d]$$

$$D_6 = [47_d\ 90_d\ 18_d\ 241_d\ 151_d\ 137_d\ 143_d\ 122_d]$$

$$D_7 = [67_d\ 146_d\ 81_d\ 29_d\ 161_d\ 199_d\ 246_d\ 61_d]$$

상수 c_i는 다음과 같다.

$$c_0 = c_1 = c_5 = c_6 = 0,$$
$$c_2 = c_3 = c_4 = c_7 = 1.$$

〔표 4〕 BOX-1(h_i)과 BOX-0(s_i)의 SAC 테이블 (Avalanche 변환)

	00000001	00000010	00000100	00001000	00010000	00100000	01000000	10000000
h_7	0	-16	-8	-24	-32	-8	16	8
h_6	24	-16	8	-8	8	-24	16	-32
h_5	8	16	24	24	24	-8	-16	-8
h_4	24	-8	-16	-8	32	0	24	16
h_3	-32	16	24	-16	8	-8	16	-16
h_2	24	-16	32	24	-16	0	0	-8
h_1	-8	0	24	-16	8	-8	8	-24
h_0	-8	16	24	-8	-8	0	16	0
s_7	-8	16	-8	-16	24	24	-16	-8
s_6	-8	8	-8	-16	0	-8	-16	-32
s_5	24	-32	0	16	24	-8	16	-8
s_4	-32	0	16	24	-8	16	-8	-16
s_3	24	8	-32	0	0	16	16	8
s_2	8	24	0	-16	0	-24	-16	-16
s_1	24	0	-16	0	-24	-16	-16	8
s_0	0	-16	0	-24	-16	-16	8	-8

7. SAC (Strict Avalanche Criterion) 조사: 〔표 4〕는 BOX-1과 BOX-0의 SAC 값을 나타낸다. SAC는 부울 함수의 안정성을 평가하는 전통적인 방법 중 하나로서 부울 함수의 입력 변화에 따른 출력 변화의 관계를 나타낸다[16, 10]. 부울 함수 $f: F_2^n \rightarrow F_2$에 대해 다음은 필요충분조건이다. 즉, 임의의 $\boldsymbol{c} \in F_2^n$,(해밍 무게 $wt(\boldsymbol{c})=1$)에 대하여

$$(f*f)(\boldsymbol{c})=0 \Leftrightarrow \left|\{x \in F_2^n \mid f(\boldsymbol{x}+\boldsymbol{c})=f(\boldsymbol{x})\}\right| = \left|\{x \in F_2^n \mid f(\boldsymbol{x}+\boldsymbol{c}) \neq f(\boldsymbol{x})\}\right|.$$

부울 함수의 일차 변환(affine transformation)에 의해 Avalanche 변환의 값들이 나타나는 위치가 바뀔 수 있으므로, 똑같은 $\mathbf{w} \in F_2^n$에 대한 $(h_i * h_i)(\mathbf{w})$와 $(s_i * s_i)(\mathbf{w})$은 일치하지 않을 수 있다. 그러나 두 경우 공히 절대값의 최대치가 32로 같고 각각의 값들의 발생 빈도가 유사하므로 BOX-1과 BOX-0는 상관성(correlation) 측면에서는 비슷한 성능을 가지고 있음을 확인할 수 있다.

4.2 나머지 8차 기약다항식을 이용한 경우

이번에는, 제안된 설계 방법의 변환 과정에서 $g_2(z)=z^8+z^5+z^3+z^1+1$을 이용하여 생성된 새로운 치환상자 BOX-2(〔표 5〕 참조)의 성질을 살펴보도록 하자.

BOX-2를 구성하는 여덟 개의 부울 함수는 u_i, $i=0,\cdots,7$로 표시하도록 한다. u_i의 Hadamard 변환 스펙트럼과 SAC 조사를 위한 Avalanche 변환 값을 〔표

〔표 5〕 BOX-2 (16진법 표기)

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	12	31	1d	f9	50	e6	22	4f	2f	2e	e8	18	f1	03	08
1	4a	eb	84	c2	b9	90	34	d4	02	b6	61	6c	ea	29	46	2b
2	cd	d3	c7	f2	2f	34	9e	d4	c3	14	b3	56	7b	9d	d0	58
3	ff	d4	7e	82	85	55	90	88	21	ba	af	23	b2	aa	ba	49
4	1e	ac	27	2f	94	cb	0c	eb	7f	c3	9f	b1	53	2b	19	d2
5	78	2e	dd	ca	c3	18	a3	51	12	31	22	6e	2d	59	87	da
6	4a	ec	f2	a7	a8	1e	1b	33	5e	60	94	f5	07	f4	6d	ac
7	9b	01	64	55	93	d9	80	1c	2b	de	98	78	42	eb	65	c5
8	3f	56	f3	dc	e1	18	f0	db	59	e7	ab	cc	fa	3d	89	18
9	a8	3c	62	8b	70	55	7c	7a	0d	aa	c7	4c	9e	d4	bf	00
a	e7	48	50	7c	48	9b	89	72	cb	c4	a5	40	05	b1	00	fc
b	4a	b4	ac	85	bb	62	98	22	6d	b4	e4	b7	ac	30	d0	70
c	ce	09	bb	e8	ef	11	e6	f8	3a	14	ac	7c	75	29	c1	79
d	1b	ff	9c	31	49	7b	5a	57	cb	b6	d0	3e	b9	48	47	c8
e	1d	02	eb	7d	d7	df	31	3f	72	9c	a3	91	b5	75	c9	08
f	38	06	a4	b9	2d	f6	20	99	3a	9b	5e	6e	7e	36	58	14

〔표 6〕 BOX-2의 Hadamard 변환 스펙트럼의 프로파일 (발생빈도)

HT	0	4	8	12	16	20	24	28	32	36	40	44	48	52	Total
u_7	27	59	45	28	21	30	25	7	5	4	2	0	3	0	256
u_6	26	45	46	42	31	22	17	13	6	4	1	2	1	0	256
u_5	22	55	42	38	32	23	18	8	10	3	4	1	0	0	256
u_4	25	45	38	33	42	31	15	17	5	2	3	0	0	0	256
u_3	23	46	44	46	34	25	16	7	5	3	4	1	2	0	256
u_2	33	53	38	32	33	22	15	15	5	6	3	0	1	0	256
u_1	22	55	40	39	35	21	21	10	6	1	3	1	1	1	256
u_0	30	44	47	41	29	20	15	16	4	6	2	1	1	0	256

〔표 7〕 BOX-2의 SAC

	10000000	01000000	00100000	00010000	00001000	00000100	00000010	00000001
u_7	-8	8	-8	-24	0	-8	8	-24
u_6	16	24	-24	-24	0	-24	0	8
u_5	40	24	8	-8	-8	0	-8	-24
u_4	24	-32	16	0	8	0	56	8
u_3	24	16	-24	8	-8	8	24	-32
u_2	-8	8	-8	-8	-24	-8	24	0
u_1	0	8	8	32	16	-8	16	16
u_0	40	16	24	-16	0	16	-8	0

6〕과 〔표 7〕에 나타내었다. BOX-2의 성질은 다음과 같다.

1. BOX-2는 일대일 대응 치환상자가 아니다(not bijective). 더욱이, BOX-2를 구성하는 개개의 부울 함수의 진리표에서 0과 1의 개수가 일치하지 않는다(not balanced). 따라서 BOX-2는 BOX-1에 비해 선형 공격[11]에 취약하다. LC(Linear Cryptanalysis) 특성을 나타내는 Linear Approximation Table의 요약 결과를 〔부록〕에 첨부하였다.
2. BOX-2를 구성하는 개개의 부울 함수 u_i들의 Hadamard 변환 스펙트럼은 상호간 일치하지 않는다. 따라서 u_i, $i=0,\cdots,7$은 서로 등가적이지 않다(inequivalent). Fuller와 Millan은 그들의 논문[5]에서 이러한 성질을 갖는 치환상자를 찾는 컴퓨터 알고리듬을 다루고 있다.
3. BOX-2는 Hadamard 변환이나 Avalahche 변환의 스펙트럼 상의 최대값이 BOX-1에 비해 더 크다. 따라서 BOX-2는 비선형성 및 SAC 측면에서 BOX-1보다 열악한 성능을 보인다. 실례로 〔표 6〕과 식 (4)에 의하면 BOX-2의 비선형도는 부울 함수 u_1의 비선형도인 100(=128-56/2) 이하임을 알 수 있다. (BOX-1의 비선형도는 112이다.)
4. 유한체 위의 다항식 표현 관점: BOX-2를 구성하는 부울 함수는 어떠한 8차 이진 기약다항식으로 정의된 유한체 위에서도 항상 복잡한 (많은 항을 가진) 형태의 다항식으로 표현된다. (BOX-1을 구성하는 부울 함수는 $g_0(z)$로 정의된 유한체 F_O 위에서는 복잡한 다항식 표현을 갖지만, $g_1(z)$로 정의된 유한체 F_C 상에서는 간단한 다항식으로 표현된다.)

V. 결 론

본 논문에서는, 유한체 연산에 근거한 치환상자를 변

형하여 새로운 치환상자를 설계하는 간단한 방법을 제안하였다. 설계 방법의 단계별 절차는 아래와 같다.

단계 1. 주어진 치환상자를 구성하는 부울 함수의 다항식 표현 계산

단계 2. 단계 1에서 계산한 다항식 표현의 계수 변경

단계 3. 단계 2의 다항식 함수를 모든 입력에 대해 계산: 진리표 작성 및 새로운 치환상자 완성

〔단계 1〕에서 다항식 표현을 찾을 때는, (기존의 치환상자가 정의된 유한체 F_O위에서가 아닌) 새로운 곱셈 규칙을 갖는 유한체 F_C 위에서 Lagrange 복원법을 적용한다. 〔단계 2〕에서는 〔단계 1〕에서 구한 다항식 함수의 계수(유한체 F_C의 원시원소의 거듭제곱으로 표현되어 있음)를 F_O의 원시원소의 거듭 제곱으로 치환한다. 다시 〔단계 3〕에서는 F_O의 곱셈 규칙에 의해 부울 함수의 진리표를 계산한다.

우리는 제안된 설계 방법을 Rijndael 알고리듬의 치환상자 BOX-0에 적용하여 BOX-1, BOX-2, ···, BOX-29로 지칭한 29개의 새로운 치환상자를 생성하였다. 새로이 생성된 29개의 치환상자 모두 각각을 구성하는 개별 부울 함수의 선형복잡도가 크게 증가되어 유한체 위에서 다항식 표현이 매우 복잡해 졌다는 장점을 가진다. 한편, Ⅳ장의 분석결과 29개의 치환상자는 변환 영역 특성에 따라 2가지로 분류될 수 있다. BOX-1은 BOX-0와 정확히 동일한 변환 영역 특성을 가지고 있다. 나머지 28개의 치환상자(BOX-2, BOX-3, ...)의 경우 equivalence class variety test 관점에서 우수하지만 상대적으로 열악한 변환 영역 특성을 보이기도 한다. 29개의 새로운 치환상자 중, 오로지 BOX-1만이 BOX-0와 동일한 변환 영역 스펙트럼을 가지는 것은, BOX-1을 구성하는 부울 함수들만이 BOX-0의 부울 함수와 등가관계에 있기 때문이다. 나머지 28개의 치환상자들은 대체로 유사한 성질을 갖고 있고, BOX-0 (혹은 BOX-1)과는 구별되는 특성을 보인다.

지금까지의 고찰을 바탕으로 다음의 연구 주제들을 제안한다.

- 변형된 치환상자가 일대일 대응이 되는 이유와 조건은 무엇인가?
- 변형된 치환상자가 변환 영역에서 기존의 치환상자와 같은 혹은 다른 스펙트럼을 갖는 이유와 조건은 무엇인가?
- 논의의 틀을 Rijndael 알고리듬의 치환상자로 한정했을 때, 29개의 기약다항식 중 임의로 선택된 것 기약다항식 $g_1(z)$을 변환 과정에서 사용해 생성된 BOX-1만이 원래의 치환상자와 유사한 특성을 보이는 이유는 무엇인가?
- $g_0(z)$를 제외한 8차 이진 기약다항식 29개 중, ($g_0(z)$와 연관되어 고려했을 때) $g_1(z)$가 나머지 28개의 기약다항식과 확연히 구별되는 특성을 지니는가?

참고문헌

〔1〕 송정환, 구본욱, "수리계획법을 이용한 S-box의 부울함수 합성" 정보보호학회논문지 14권 4호, pp. 49-59, 2004.

〔2〕 E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," Journal of Cryptology, vol. 4, pp. 3-72, 1993.

〔3〕 J. Daemen and V. Rijmen, Submission to NIST AES Process, 1997. http://csrc.nist.gov/CryptoToolkit/aes

〔4〕 J. Daemen and V. Rijmen, The Design of Rijndael, Springer, 2002.

〔5〕 J. Fuller, W. Millan, "Linear redundancy in S-boxes," T. Johansson (Ed.) Fast Software Encryption 2003, LNCS vol. 2887, Springer-Verlag, pp. 74-86, 2003.

〔6〕 G. Gong, S.W. Golomb, "Transform domain analysis of DES," IEEE Transactions on Information Theory, vol. 45, no. 6, pp. 2065-2073, Sep., 1999.

〔7〕 S.W. Golomb, G. Gong, Signal Design for Good Correlation: for wireless communication, cryptography, and radar, Cambridge University Press, 2005.

〔8〕 T. Jakobsen and L. Knudsen, "The interpolation attack on block ciphers," in E. Biham (Ed.) Fast Software Encryption 1997, LNCS vol. 1267, Springer, pp.28-40, 1997.

〔9〕 L. Jing-mei, W. Bao-dian, C. Xiang-guo, W. Xin-mei, "Cryptanalysis of Rijndael S-box and improvement," Applied Mathematics and Computation, vol. 170, pp. 958-975, 2005.

〔10〕 Yuan Li and T. W. Cusick, "Strict Avalanche

criterion over finite fields," http://eprint.iacr.org/2005/361.pdf

[11] M. Matsui, "Linear cryptanalysis method for DES cipher," T. Helleseth (Ed.), Advances in Cryptology: Eurocrypt '93, LNCS vol. 765, Springer, pp. 386-397, 1993.

[12] National Institute of Standards and Technology. The Advanced Encryption Standard, Federal Information Processing Standards Publication (FIPS) 197, 2001. http://csrc.nist.gov/publications/fips

[13] K. Nyberg, "Differentially uniform mappings for cryptography," T. Helleseth (Ed.) Advances in Cryptology - EUROCRYPT '93, LNCS vol. 765, Springer, pp. 55-64, 1994.

[14] R. A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, 1986.

[15] C. E. Shannon, "Communication theory of secrecy systems," Bell Systems Technical Journal, vol. 28, pp. 656-715, 1949.

[16] A.F. Webster and S.E. Tavares, "On the design of S-box," In: H.C. Williams (Ed.), Advances in Cryptology: Crypto '85, LNCS vol. 218, Springer-Verlag, 1986, pp. 523-534.

[17] A. M. Youssef and G. Gong, "On the interpolation attacks on block ciphers," in B. Schneier (Ed.) Fast Software Encryption 2000, LNCS vol. 1978, Springer, pp.109-120, 2001.

[18] A. M. Youssef, S. E. Tavares, "Affine equivalence in the AES round function," Discrete Applied Mathematics, vol. 148, pp. 161-170, 2005.

[19] National Bureau of Standards, The Data Encryption Standard, Federal Information Processing Standards Publication (FIPS) 46, 1977.

[20] Howard M. Heys, "A tutorial on linear and differential cryptanalysis," Technical Report, CORR 2001-17, University of Waterloo, Waterloo, Canada, 2001.

Ⅵ. 부록: Linear Approximation Table

치환 상자의 입력을 $(X_0, X_1, \cdots, X_7)$, 출력을 $(Y_0, Y_1, \cdots, Y_7)$라고 하자. 아래 표는 bias가 없도록 만드는 입출력 선형 결합의 경우의 수[20]를 나타낸다. 즉 모든 8비트 입력에 대해 입력 선형 결합(input linear combination)과 출력 선형 결합(output linear combination)이 정확히 절반은 일치하고 절반은 불일치하게 되는 입출력 선형 결합의 경우의 수는 BOX-0와 BOX-1의 경우 4590, BOX-2의 경우 6790, BOX-29의 경우는 6875임을 나타낸다. BOX-2, ..., BOX-29의 경우 BOX-0와 BOX-1에 비해 maximum bias가 크기 때문에 선형 공격(Linear Cryptanalysis)에 취약하다.

〈표 8〉 Linear Approximation Table

Probability bias magnitude (multiplied by 256)	The number of linear combinations of input and output bits				
	BOX-0	BOX-1	BOX-2	.....	BOX-29
0	4590	4590	6790		6875
2	12240	12240	12617		12568
4	9080	9080	11472		11509
6	10200	10200	9859		9800
8	8670	8670	7945		7880
10	6120	6120	6024		5963
12	9180	9180	4199		4222
14	4080	4080	2700		2778
16	1275	1275	1673		1744
18	0	0	1062		1003
20	0	0	631		619
22	0	0	292		320
24	0	0	153		150
26	0	0	69		69
28	0	0	24		18
30	0	0	15		9
32	0	0	6		6
34	0	0	2		2
36	0	0	2		0
Total	$2^{16}-1$	$2^{16}-1$	$2^{16}-1$	.....	$2^{16}-1$

〈著者紹介〉

진 석 용 (Seok-Yong Jin) 정회원

2001년 8월: 연세대학교 전기전자공학과 졸업
2003년 8월: 연세대학교 전기전자공학과 석사
2003년 9월~현재: 연세대학교 전기전자공학과 박사과정
<관심분야> PN Sequences, Block/Stream Cipher Systems, Error Correcting Codes, Spread Spectrum Communication Systems

백 종 민 (Jong-Min Baek) 정회원

2005년 2월: 연세대학교 전기전자공학과 졸업
2007년 2월: 연세대학교 전기전자공학과 석사
2007년 1월~현재: (주)홈캐스트 부설연구소 연구원
<관심분야> PN Sequences, Block/Stream Cipher Systems, Error Correcting Codes

송 홍 엽 (Hong-Yeop Song) 종신회원

1984년 2월: 연세대학교 전자공학과 졸업 (공학사)
1986년 5월: USC 대학원 전자공학과 졸업 (공학석사)
1991년 12월: USC 대학원 전자공학과 졸업 (공학박사)
1992년 ~ 1993년: Post Doc., USC 전자공학과
1994년 ~ 1995년: Qualcomm Inc., 선임연구원
1995년 9월 ~ 현재: 연세대학교 전기전자공학과 교수
<관심분야> PN Sequences, Error Correcting Codes, Block/Stream Cipher Systems, Spread Spectrum Communication Systems