通信情報保護學會論文誌
第6卷 第4號, 1996. 12

유한체 상의 지수 함수의 분류와 암호학에의 응용

박 상 우*, 김 광 조*

Classification of Exponent Permutations over finite fields $GF(2^n)$ and its applications

Sangwoo Park, Kwangjo Kim

요 약

유한체 $GF(2^n)$상의 모든 지수 함수들의 군에 동치 관계를 정의하고, 이들 동치 관계에 의해 분류된 각 동치류에 속하는 지수 함수들은 동일한 암호학적 성질을 가짐을 보인다. 그리고, $GF(2^7)$과 $GF(2^8)$ 상의 모든 지수 함수들을 분류한다. 다음으로 지수 함수 분류의 3 가지 응용을 제시한다. 우선 $GF(2^n)$ 상의 2개의 지수 함수의 연접에 의한 $n \times 2n$ S(ubstitution)-box의 설계 방법을 제안하고, 그들의 입·출력 변화 내성과 선형 내성을 분석한다. 그리고, Eurocrypt '93에서 Beth가 세운 가설이 그릇된 것임을 지적하고, LOKI 블록 알고리즘에 사용된 S-box의 안전성에 대하여 논한다.

Abstract

In this paper, we define an equivalence relation on the group of all permutations over the finite field $GF(2^n)$ and show each equivalence class has common cryptographic properties. And, we classify all exponent permutations over $GF(2^7)$ and $GF(2^8)$. Then, three applications of our results are described. We suggest a method for designing $n \times 2n$ S(ubstitution)-boxes by the concatenation of two exponent permutations over $GF(2^n)$ and study the differential and linear resistance of them. And we can easily indicate that the conjecture of Beth in Eurocrypt '93 is wrong, and discuss the security of S-box in LOKI encryption algorithm.

1. 서 론

일반적으로, 블록 알고리즘의 안전성은 대치(substitution)와 치환(permutation)의반복을 통하여 강화된다. 암호학적으로 안전한 치환의 주요 필수 조건으로는 높은 비선형치(nonlin-

* 한국전자통신연구소 부호기술연구부 부호1실

earity), 높은 대수적 차수(algebraic degree), 입·출력 변화 공격법(differential attack)[4]에 대한 안전성, 그리고, 선형 공격법(linear attack) [11]에 대한 안전성 등이 있으며, 특히 치환의 한 종류인 지수 함수(exponent permutation)의 특별한 형태들은 비선형치와 대수적 차수가 높고, 입·출력 변화 공격법과 선형 공격법에 대하여 우수한 안전성을 가지는 것으로 알려져 있다 [13].

본 논문에서는 유한체 $GF(2^n)$ 상의 모든 지수 함수들의 군(group) 상에 동치 관계(equivalence relation)를 정의하고, 정의된 동치 관계에 의해 분류된 동치류(equivalence class)가 유한체 상의 모든 지수 함수들의 군에 대한 법(modulo) 순환군(cyclic group) $\langle x^2 \rangle$의 잉여 집합(residue set)과 동일함을 증명한다. 그리고, 동일한 동치류에 속하는 지수 함수들은 동일한 암호학적 성질을 가짐을 보인다. 다음으로, 컴퓨터 조사를 통해, 유한체 $GF(2^7)$과 $GF(2^8)$상의 모든 지수 함수들을 분류한다. 또한, 이들 결과의 응용으로, $GF(2^n)$상의 두개의 지수 함수의 연접에 의한 $n \times 2n$ S-box 설계 방법을 제안하고, 그들의 암호학적 성질을 분석한다. 그리고, Eurocrypt '93에서 Beth가 제안한 가설[2]의 반례를 보이고, 블록 암호 알고리즘 LOKI[6, 5]에 사용된 S-box의 안전성에 대하여 논한다.

2. $GF(2^n)$상의 지수 함수의 분류

P_n을 유한체 $GF(2^n)$상의 모든 치환들의 집합이라 하자. 유한체 $GF(2^n)$상의 임의의 다항식(polynomial) x^e이 치환이면, $gcd(e, 2^n - 1) = 1$이고, 그 역 또한 성립한다. 그리고, 이러한 다항식을 유한체 $GF(2^n)$상의 지수 함수라 하며, $GF(2^n)$상의 모든 지수 함수들의 집합을 $\mathcal{E}P_n = \{x^e \mid gcd(e, 2^n - 1) = 1, x \in GF(2^n)\}$로 나타낸다. $GF(2^n)$상의 치환 $f(x)$ 와 $g(x)$에 대해서, 합성 치환 $h(x) = f(x) \circ g(x)$는 $h(x) = f(g(x)) \bmod (x2^n - x)$로 정의되며, 이 연산에 대해서, P_n은 군을 이루고, $\mathcal{E}P_n$는 P_n의 가환부분군(abelian subgroup)이다. 그리고, $x^{e_1}, x^{e_2} \in \mathcal{E}P_n$에 대해서, $x^{e_1} = x^{e_2}$이면 $e_1 = e_2 \bmod (2^n - 1)$이고, 역도 성립한다. 다음 정리는 유한체론의 기본 정리이다.

■ **정리 1**[10] GF(2)의 임의의 원소를 고정시킨 $GF(2^n)$상의 자기동형사상(*automorphism*)들의 집합 $\mathcal{G}(GF(2^n)/GF(2))$은 $GF(2^n)$상의 자기동형사상군의 부분군이며, *Frobenius* 자기동형사상으로 생성되는 순환군과 동일하다. 즉,

$$\mathcal{G}(GF(2^n)/GF(2)) = \langle x^2 \rangle$$

이다.

■ **따름정리 1** $\mathcal{E}P_n$의 모든 선형 치환들의 집합은 순환부분군 $\langle x^2 \rangle \subset \mathcal{E}P_n$ 이다.

$GF(2^n)$상의 치환들의 집합에 관계(relation)를 정의한다.

■ **정의 1** $P = (p_1, \cdots, p_n)$, $Q = (q_1, \cdots, q_n) \in P_n$에 대해서, P_n상의 관계를 다음으로 정의한다.

$P = L_A \circ Q$를 만족하는 $n \times n$ 정칙 행렬(*nonsingular matrix*) A가 존재하면 $P \sim Q$이다.

여기서 L_A는 행렬 A의 선형 변환(*linear transformation*)이다. 성분 함수(*component function*)의 관점에서 보면, 위에 정의한 관계는 다음과 같다.

$P \sim Q \iff$ P와 Q의 성분 함수 p_i와 q_i에 대해서 $p_i = \sum_{j=1}^{n} a_{ij} q_j$, $1 \le i \le n$를 만족하는 정칙 행렬 $A = (a_{ij}) \in GL_n(GF(2))$가 존재한다.

■ **보조정리 1** 정의 1에 정의된 관계는 동치

관계이다.

정의 1에 정의된 관계가 동치 관계이므로, $P_n/\sim = \{\overline{P} \mid P \in P_n\}$에 대해, $\overline{P} = \{Q \in P_n \mid P \sim Q\}$ 이고, $P_n = \cup_{P \in P_n} \overline{P}$ 이다. 따라서, 집합 $\mathcal{E}P_n/\sim$을 $\mathcal{E}P_n/\sim = \{\overline{x^e} \cap \mathcal{E}P_n \mid x^e \in \mathcal{E}P_n\}$으로 정의할 수 있다. 다음으로 $\overline{x^{e_1}} \cap \mathcal{E}P_n$, $\overline{x^{e_2}} \cap \mathcal{E}P_n \in \mathcal{E}P_n/\sim$에 대해서, $\mathcal{E}P_n/\sim$상의 연산 $*$를 $(\overline{x^{e_1}} \cap \mathcal{E}P_n) * (\overline{x^{e_2}} \cap \mathcal{E}P_n) = \overline{x^{e_1} \circ x^{e_2}} \cap \mathcal{E}P_n$으로 정의하자. 그러면, $\mathcal{E}P_n$가 가환군이므로, 연산 $*$는 잘 정의되며(well-defined), 따라서, $\mathcal{E}P_n/\sim$은 군이다.

■ **정리 2** $x^e \in \mathcal{E}P_n$에 대해, $\overline{x^e} \cap \mathcal{E}P_n = \langle x^2 \rangle x^e$ 이다.

■ **증명.** 따름 정리 1에 의하여, $\langle x^2 \rangle x^e \subset \overline{x^e} \cap \mathcal{E}P_n$ 이다. 역으로, $y \in \overline{x^e} \cap \mathcal{E}P_n$에 대해서, $y = L_A \circ x^e$ 그리고, $y = x^i$를 만족하는 정칙 행렬 A와 정수 i가 존재한다. 따름 정리 1에 의해서, 어떤 k에 대해, $L_A = x^{i-e} = x^{2k}$ 이다.

정리 2에 의해서, ϕ가 오일러의 함수(Euler function)일 때, $\mathcal{E}P_n/\sim = \mathcal{E}P_n/\langle x^2 \rangle$ 이고 $\#(\mathcal{E}P_n/\sim) = \frac{\phi 2^n-1}{n}$ 이다.

다음으로, 유한체 $GF(2^n)$상의 지수 함수의 암호학적 성질을 알아보자. 정의 1에 정의된 동치 관계와 암호학적 성질에 의하여 $GF(2^n)$상의 지수 함수들을 분류할 수 있다. 먼저, 임의의 동치류에 속하는 지수 함수들은 동일한 비선형치와 대수적 차수를 가짐을 증명한다.

■ **보조정리 2** $P(x) = x^e$를 $GF(2^n)$상의 지수 함수라 하자. 그러면 다음이 성립한다.

1. $P(x)$의 성분 함수의 모든 선형 결합(*linear combination*)들의 대수적 차수는 $wt(e)$이다.
2. $P(x)$의 성분 함수의 모든 선형 결합들의 비선형치는 동일하다.

■ **증명.** 1의 증명은 참고 문헌 [7]에 되어 있다. $P(x) = x^e$이 치환이고, $gcd(e, 2^{n-1}) = 1$ 이므로, $t_1e + t_2(2^{n-1}) = 1$인 t_1, $t_2 \in Z$가 존재한다. 그러므로, 임의의 $x = GF(2^n)$ 에 대해서,

$$x = x^1 = (x^{2^{n-1}})^{t_2}(x^e)^{t_1} = (x^e)^{t_1} = P(x)^{t_1}$$

이다. $p_i(x)$를 $P(x)$의 성분 함수들의 임의의 선형 결합이라 하자. 그러면, 어떤 $\alpha_i \in GF(2^n)$ 에 대해서, 다음이 성립한다 [10].

$$\begin{aligned} p_i(x) &= Tr(\alpha_i P(x)) \\ &= Tr(P(\alpha_i)^{t_1} P(x)) \\ &= Tr(P(\alpha_i^{t_1} x)). \end{aligned}$$

그러므로, $A_i : GF(2^n) \rightarrow GF(2^n)$를 $A_i(x) = \alpha_i^{t_1} x$로 정의하면, $p_i = Tr \circ P \circ A_i$에 대해서, 비선형치는 변화하지 않는다. 그리고, A_i는 선형 함수이다. 따라서,

$$N_{P_k} = N_{Tr \circ P}$$

이다.

$P(x)$의 성분 함수 $p_i(x)$들의 임의의 선형 결합의 대수적 차수 및 비선형치가 동일하므로, $deg(P(x)) = deg(p_i(x))$과 $N_P = N_{p_i}$로 나타낼 수 있다. 정리 2와 보조정리 2에 의해서, 다음을 얻는다.

■ **정리 3** $P \sim Q$인 $P, Q \in \mathcal{E}P_n$에 대해서 다음이 성립한다.

1. $N_P = N_Q$.
2. $deg(P) = deg(Q)$.

P를 n개의 입력변수를 가지는 치환이라 할 때, P의 입·출력 변화 공격법에 대한 안전성을 분석하기 위하여, 집합

$D_P(a,b) = \{x \in GF(2)^n \mid P(x \oplus a) \oplus P(x) = b\}, a \neq 0$

에 대해,

$\delta_P(a,b) = \#D_P(a,b)$

이 필요하며, 다음을 치환 P의 입·출력 변화 공격법에 대한 안전성의 척도(differential resistance)로 삼는다.

$\Delta_P = \max_{a \neq 0, b} \delta_P(a,b)$.

유사하게, 선형 공격법에 대한 안전성을 분석하기 위하여, 집합

$L_P(a,b) = \{x \in GF(2^n)\} \mid (a \cdot x) \oplus (b \cdot P(x)) = 0\}, b \neq 0$

에 대해,

$\lambda_P(a,b) = \#L_P(a,b) - 2^{n-1}$

이 필요하며,

다음을 선형 공격법에 대한 안전성의 척도(linear resistance)로 삼는다.

$\lambda_P(a,b) = \max_{a \neq 0, b} |\lambda_P(a,b)|$.

치환 P는 Δ_P와 λ_P가 작을 수록, 입·출력 변화 공격법과 선형 공격법에 대하여 안전하다. $\Delta_P = \delta$일 경우, P를 입·출력 변화 관점에서 δ 균등하다고 한다(differentially δ-uniform). Δ_P가 최소 값을 가지면, P는 입·출력 변화 공격법에 대하여 내성을 가진다(differential resistant). 또한, λ_P가 최소 값을 가지면, P는 선형 공격법에 대하여 내성을 가진다(linear resistant)[8]. 참고 문헌 [13], [17]과 정리 3에 의해, 다음 결과를 얻는다.

■ **정리 4** $P \sim Q$인 $P, Q \in \mathcal{E}P_n$에 대해 다음이 성립한다.

1. $\Delta_P = \Delta_Q$
2. $\Lambda_P = \Lambda_Q$

정리 4에 의하여, 임의의 동치류에 속하는 지수 함수들은 동일한 Δ_P와 Λ_P를 가진다. 참고 문헌 [13]에는 유한체 $GF(2^n)$상의 지수 함수 중 특별한 형태의 지수 함수 P에 대하여, P의 대수적 차수, Δ_P, 그리고 Λ_P가 증명되어 있는데, 이를 정리하면 표 1과 같다.

표1 특수한 형태를 가지는 유한체 $GF(2^n)$상의 지수 함수 $P = x^e$의 대수적 차수, Δ_P, Λ_P

P	$deg(P)$	Δ_P	Λ_P	조 건
x^{2k+1}	2	2^s	$2^{\frac{n+s}{2}} - 1$	$s = gcd(n, k)$ $\frac{n}{s}$은 홀수
$(x^{2k+1})^{-1}$	$\frac{n+1}{2}$	2	$2^{\frac{n-1}{2}}$	$gcd(n, k) = 1$ n은 홀수
x^{-1}	$n-1$	2	$\geq 2^{\frac{n}{2}}$	n은 홀수
x^{-1}	$n-1$	4	$\geq 2^{\frac{n}{2}}$	n은 짝수

다음으로, 정의 1의 동치 관계에 의해 $GF(2^7)$과 $GF(2^8)$상의 지수 함수들을 분류한다. 표 2는 $GF(2^7)$상의 지수 함수들을 분류한 것이다. 표 2에서, 동치류 (P1, P13), (P2, P11), (P3, P9), (P4, P16), (P5, P6), (P7, P15), (P8, P14), (P10, P12)은 각각 역함수 관계이다. 그리고,

표2 : $GF(2^7)$ 상의 지수 함수의 분류

동치류	대수적 차수	비선형치	Δ	Λ	지 수						
P1	2	56	2	8	3	6	12	24	48	65	96
P2	2	56	2	8	5	10	20	33	40	66	80
P3	2	56	2	8	9	17	18	34	36	68	72
P4	3	44	6	20	7	14	28	56	67	97	112
P5	3	56	2	8	11	22	44	49	69	88	98
P6	3	56	2	8	13	26	35	52	70	81	104
P7	3	44	4	20	19	25	38	50	73	76	100
P8	3	44	6	20	21	37	41	42	74	82	84
P9	4	56	2	8	15	30	71	99	113	120	160
P10	4	56	2	8	23	46	57	75	91	101	114
P11	4	56	2	8	27	51	54	77	89	102	108
Pi2	4	56	2	8	29	39	58	78	83	105	116
P13	4	56	2	8	43	45	53	85	86	90	106
P14	5	44	6	20	31	62	79	103	115	121	124
P15	5	44	4	20	47	61	87	94	107	117	122
P16	5	44	6	20	55	59	91	93	109	110	118
P17	6	54	2	10	63	95	111	119	123	125	126
P18	1	0	128	64	1	2	4	8	16	32	64

동치류 P17에 속하는 지수 함수들은 x^{-1}와 동치 관계이다. 동치류 P18에 속하는 지수 함수들은 선형이다. $GF(2^7)$상의 지수 함수들 중, 동치류 P9, P10, P11, P12, P13들이 가장 우수한 암호학적 성질을 가지며, 입·출력 변화 공격법과 선형 공격법에 대하여 내성을 가진다. 표 3은 $GF(2^8)$상의 지수 함수들을 분류한 것이다. 표 3에서, 동치류 (P1, P5), (P2, P7), (P3, P12), (P4, P11), (P6, P13), (P10, P14)은 서로 역함수 관계이다. 그리고, 동치류 P8과 P9의 지수 함수들은 각 동치류 내에 역함수를 가진다. 또한, 동치류 P15의 지수 함수들은 x^{-1}와 동치 관계이며, 동치류 P16에 속하는 지수 함수들은 선형 함수이다. $GF(2^8)$상의 지수 함수들 중에 동치류 P15에 속하는 지수 함수들의 암호학적 성질이 가장 우수하다.

3. 응 용

본 장에서는 2장 결과의 3가지 응용 방법을 서술한다.

3.1 $n \times 2n$ S-box 설계

첫 번째 응용으로 $GF(2^n)$상의 지수 함수의 연접에 의한 $n \times 2n$ S-box의 설계 방법을 제안하고, 설계된 $n \times 2n$ S-box의 입·출력 변화 공격법과 선형 공격법에 대한 안전성을 분석

한다. 그리고, $GF(2^8)$상의 2개의 지수 함수의 연접에 의해 설계된 8 × 16 S-box S의 Δ_S와 Λ_S를 조사한다.

임의의 $n \times 2n$ S-box S에 대해서, $\Delta_S \geq \max(2, 2^{n-m})$이다. $n > m$일 때, 최소 입·출력 변화 균등치(differential uniformity)가 2^{n-m}이기 위해서는, $n \geq 2m$이고 n이 짝수이며, 그 역 또한 성립하고, 이러한 S-box를 완전 비선형(perfect nonlinear)이라 한다 [12]. $n > m$인 임의의 S-box는 출력의 경우의 수보다 입력의 경우의 수가 많다. 이것은 두 개 또는 그 이상의 입력이 동일한 출력을 결정하는 경우가 적어도 한 개 이상 존재함을 의미한다. 즉, 한 개 또는 그 이상의 입력 XOR(exclusive-or)가 출력 XOR값을 0으로 가진다. 따라서, $n > m$인 S-box에 대해 지금 언급한 경우가 높은 확률을 가지면, 입·출력 변화 공격시 사용될 수 있다. 이러한 사실은 DES(Data Encryption Standard)[15] 형 알고리즘에 적용된다. 실제로, 참고문헌 [3]에서 벤트 함수(bent function) 기반 S-box가 $n > m$인 경우에 약점을 가짐을 보이고, 특히, 벤트 함수 기반 6 × 4 S-box가 DES에 사용되면, DES는 약 2^{30}개의 선택 평문에 의해 해독됨을 보였다. 그러나, $n > m$이면, 이러한 공격 방법은 각 입력이 유일한 출력에 대응되므로 불가능하다. 실제로, 출력 비트 길이가 입력 비트 길이보다 충분히 큰 단사(injective) S-box를 사용하는 것은 $\delta_S(a, b)$를 감소시킨다. 최근 제안된 블록 알고리즘인 CAST[1] 와 Blowfish [16]에서 $n \leq m$인 S-box를 사용하였다. 그리고, 참고문헌 [18]에는 랜덤하게 선택된 단사 S-box의 Λ_S 값을 이론적으로 추정하였으며, 컴퓨터 조사를 통하여 $m > 8$인 $8 \times m$ 단사 S-box의 Λ_S를 구하고, 이론적 추정치 와 비교하였다. $GF(2^n)$상의 2개 지수 함수 P_i와 P_j의 연접에 의해 $n \times 2n$ S-box를 얻을 수 있다. 즉, $S(x) = (P_i(x), P_j(x))$ 이다. 이 방법으로 설계된 S-box는 단사 함수이다. 다음 정리는 이 방법으로 설계된 S-box의 입·출력 변화 내성과 선형 내성을 분석하기 위하여 필요하다.

■ **정리 5**[14] 임의의 함수 $F : Z_2^n \rightarrow Z_2^m$의 성분 함수가 $f_1, \cdots, f_m$이고, $g : Z_2^n \rightarrow Z_2$라 하자. 그리고 $\tilde{F} = (f_1, \cdots, f_m, g)$라 하자. 그러면 다음이 성립한다.

1. $\Delta_F \geq \Delta_{\tilde{F}} \geq \frac{1}{2}\Delta_F$,
2. $\Delta_{\tilde{F}} \geq \max(\Delta_F, \Lambda g) \geq \Delta_F$.

정리 5에 의하면, 임의의 2개의 지수 함수 P_i와 P_j의 연접에 의해 설계된 $n \times 2n$ S-box $S = (P_i, P_j)$의 Δ_S 는 Δ_{P_i}보다 같거나 작고, Λ_S는 Λ_{P_i}와 Λ_{P_j}의 최대값보다 같거나 크다. 이제 컴퓨터 조사를 통해 $GF(2^8)$상의 2개의 지수 함수의 연접에 의해 설계된 모든 8 × 16 S-box의 Δ_S와 Λ_S를 알아보자. 먼저 다음을 증명한다.

■ **정리 6** $P1, P2, Q1, Q2 \in \mathfrak{E}P_n$를 $P1 \sim P2$이고 $Q1 \sim Q2$ 라하고, $S1 = (P1, Q1)$, $S2 = (P2, Q2)$ 라 하면, 다음이 성립한다.

1. $\Delta_{S1} = \Delta_{S2}$,
2. $\Lambda_{S1} = \Lambda_{S2}$.

■ **증명** 정의 1에 의해, $P1 = A \circ P2$ 이고 $Q1 = B \circ Q2$인 정칙 행렬 $A, B \in GL_n(GF(2))$가 존재한다. $\alpha \in Z_2^n$, $\beta = (\beta_1, \beta_2) \in Z_2^n$라 하면, 다음이 성립한다.

$$\begin{aligned}\delta_{S1}(\alpha, \beta) &= \#\{x \mid (P1, Q1)(x) \oplus (P1, Q1)(x \oplus \alpha) = (\beta_1, \beta_2)\} \\ &= \#\{x \mid (P1(x) \oplus P1(x \oplus \alpha)), (Q1(x) \oplus Q1(x \oplus \alpha)) = (\beta_1, \beta_2)\} \\ &= \#\{x \mid (P2(x) \oplus P2(x \oplus \alpha)), (Q2(x) \oplus Q2(x \oplus \alpha)) = (A(\beta_1), B(\beta_2))\}\end{aligned}$$

$= \delta_{S2}(A(\beta_1), B(\beta_2))$

즉, $\Delta_{S1} = \Delta_{S2}$이다. 그리고, 정의 1에 의해 $\Lambda_{S1} = \Lambda_{S2}$ 이다.

정리 6에 의해 $GF(2^n)$상의 2개의 지수 함수의 연접에 의해 설계되는 모든 $n \times 2n$ S-box S의 Δ_S와 Λ_S를 조사하려면, 서로 다른 동치류에 속하는 P_i와 P_j에 의해 설계되는 $n \times 2n$ S-box의 Δ_S와 Λ_S만을 조사하면 된다. 이를 바탕으로, 컴퓨터 조사를 통해 $GF(2^8)$상의 모든 지수 함수에 의해 설계되는 모든 8 × 16 S-box의 Δ_S와 Λ_S를 얻었으며, 그 결과를 표 4와 표 5에 수록하였다. 표 4와 표 5에서 각 원소는 $S = (P_i, P_j)$의 Δ_S와 Λ_S를 의미하며, i 는 행을, j는 열을 의미한다. 정리 5와 표 4에 의하면, $GF(2^n)$상의 2개의 지수 함수의 연접에 의해서 생성되는 대부분의 $n \times 2n$ S-box는 입·출력 변화 공격 관점에서 매우 우수하다. 그러나, 선형 공격 관점에서는 일반적으로 그 안전성을 충분히 제공하지 못한다. 특히, 동일한 동치류에 속하는 지수 함수들의 연접으로 생성된 S-box들은 $\Lambda_S = 2^{n-1}$}으로, 선형 공격 관점에서 가장 좋지 않은 특성을 가진다. 이는 동일한 동치류에 속하는 지수 함수의 성분 함수들이 역시 동일한 동치류에 속하는 지수 함수의 성분 함수의 선형 결합으로 표시되기 때문이다. 그러나, 서로 다른 동치류에 속하는 두 지수 함수를 연접하여 설계된 S-box들은 표 5에서와 같이, 선형 공격 관점에서 비교적 우수한 성질을 가진다. 따라서, 제안하는 설계 방법을 통하여, 입·출력 공격법과 선형 공격법 관점에서 우수한 $n \times 2n$ S-box를 충분히 생성할 수 있다.

표 4 : $GF(2^8)$상의 2개 지수 함수의 연접으로 설계된 모든 8 × 16 S-box 들의 Δ_S

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}
P_1	6	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
P_2	4	10	4	4	4	4	4	4	4	4	4	4	4	4	4	10
P_3	4	4	12	4	4	4	4	4	12	4	4	12	4	4	4	12
P_4	4	4	4	16	4	16	4	4	16	16	16	4	16	16	4	16
P_5	4	4	4	4	6	4	4	4	4	4	4	4	4	4	4	6
P_6	4	4	4	16	4	16	4	4	16	16	16	4	16	16	4	16
P_7	4	4	4	4	4	4	10	4	4	4	4	4	4	4	4	10
P_8	4	4	4	4	4	4	4	30	4	4	4	4	4	4	4	30
P_9	4	4	12	16	4	16	4	4	16	16	16	12	16	16	4	16
P_{10}	4	4	4	16	4	16	4	4	16	16	16	4	16	16	4	16
P_{11}	4	4	4	16	4	16	4	4	16	16	16	4	16	16	4	16
P_{12}	4	4	12	4	4	4	4	4	12	4	4	12	4	4	4	12
P_{13}	4	4	4	16	4	16	4	4	16	16	16	4	16	16	4	16
P_{14}	4	4	4	16	4	16	4	4	16	16	16	4	16	16	4	16
P_{15}	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
P_{16}	6	10	12	16	6	16	10	30	16	16	16	12	16	16	4	256

3.2 Beth의 가설의 오류

Eurocrypt '93[2]에서 Beth는 다음 가설을 제안하였다.

■ 가설 : n과 2^n-1을 소수라 하면, $2 \le i \le n$-1에 대해서, 방정식 $Y^{2^i}-1+1=r(Y+1)$, $r \neq 0, 1$는 $GF(2^n)$에서 1 이외에 많아야 두 개의 근을 가진다. 또한, $2 \le m \le n$-1인 x^{2^m-1}의 형태를 가지는 임의의 치환은 Beth의 가설이 사실이라면 입·출력 변화 공격법에 대하여 내성을 가진다.

n = 7이면 n 과 2^n - 1은 소수이다. 그러나, m = 3인 경우에 지수 함수 $x^{2^m-1}=x^7$은 표 2에서 보면 입·출력 변화 공격법에 대한 내성을 가지지 않는다. 그러므로, Beth의 가설은 사실이 아니다. 이 사실은 본 논문의 결과와는 별도로 참고 문헌 [9]에서 저자들은 $GF(2^n)$에서 1이 아닌 3개의 근을 발견하여, Beth의 가설이 틀렸음을 밝힌 바 있다.

표 5 : $GF(2^8)$상의 2개 지수 함수의 연접으로 설계된 모든 8 × 16 S-box 들의 Λ_S

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}
P_1	128	40	32	32	32	48	32	48	32	48	32	32	36	40	32	128
P_2	40	128	32	32	32	32	32	48	32	32	32	48	48	48	32	128
P_3	32	32	128	48	40	36	32	48	56	48	40	56	32	32	48	128
P_4	32	32	48	128	40	48	32	48	48	64	48	48	40	48	40	128
P_5	32	32	40	40	128	32	32	48	32	32	32	36	48	32	48	128
P_6	48	32	36	48	32	128	32	48	40	32	48	32	48	40	48	128
P_7	32	32	32	32	32	32	128	48	32	48	40	32	32	48	48	128
P_8	48	48	48	48	48	48	48	128	48	48	48	48	48	48	48	128
P_9	32	32	56	48	32	40	32	48	128	40	48	56	32	32	48	128
P_{10}	48	32	48	64	32	32	48	48	40	128	40	40	48	64	32	128
P_{11}	32	32	40	48	32	48	40	48	48	40	128	48	48	64	48	128
P_{12}	32	48	56	48	36	32	32	48	56	40	48	128	32	32	40	128
P_{13}	36	48	32	40	48	48	32	48	32	48	48	32	128	40	32	128
P_{14}	40	48	32	48	32	40	48	48	32	64	64	32	40	128	48	128
P_{15}	32	32	48	40	48	48	48	48	48	32	48	40	32	48	128	128
P_{16}	128	128	128	128	128	128	128	128	128	128	128	128	128	128	128	128

3.3 LOKI S-box의 암호학적 성질

블록 알고리즘 LOKI[6, 5]의 안전성은 $GF(2^8)$상의 지수 함수 x^{31}에 의존한다. 그러나, 표 3에 의하면, 동치류 $P15$에 속하는 지수 함수들이 x^{31} 보다 대수적 차수와 입·출력 변화 특성 면에서 우수한 성질을 가진다. 물론 이 사실이 LOKI의 S-box를 표 3의 동치류 $P15$에 속하는 지수 함수로 대치하였을 때, LOKI의 안전성이 좋아진다는 것을 의미하는 것은 아니기 때문에, S-box를 대치한 LOKI의 전체 알고리즘에 대한 충분한 분석이 이루어져야 한다.

4. 결 론

지금까지 본 논문에서는 $GF(2^n)$상의 지수 함수들의 군에 동치 관계를 정의하고, 동일한 동치류에 속하는 지수 함수들은 동일한 암호학적 성질을 가짐을 증명하였다. 다음으로, 컴퓨터 조사를 통하여, 실제로 $GF(2^7)$과 $GF(2^8)$상의 지수 함수들을 분류하였다. 지수 함수 분류의 응용으로 2개 지수 함수의 연접에 의한 $n \times 2n$ S-box의 설계 방법을 제안하고, 그들의 입·출력 변화 공격법과 선형 공격법에 대한 안전성을 분석하였다. 그리고, Beth의 가설이 그릇된 것임을 반례를 들어 증명하였고, LOKI에 사용된 S-Box보다 암호학적 성질이 우수한 치환이 존재함을 예를 통하여 보였다.

참 고 문 헌

[1] Carlisle M. Adams and Stafford E. Tavares. Designing S-boxes for ciphers resistant to differential crypanalysis. In *the 3rd symposium of state and progress of research in crytography, Rome, Italy*, pages 386-397, 1994.

[2] T. Beth and C. Ding. On almost perfect nonlinear permutations. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT'93, volume 765 of Lecture Notes in Computer Science, pages* 65-76. Springer-Verlag, Berlin, 1994.

[3] Eli Biham. *Differential cryptanalysis of DES-like crytosystems*. PhD thesis, Wiezman Institute of Science, Rehovot, Israel, 1992.

[4] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3-72, 1991

[5] Lawewnce Brown, Matthew Kwan, Josef Pieprzyk, and Jennifer Seberry. Improving resistance to differential crytanalysis and the redesign of LOKI. In Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors, *Advances in Cryptology - ASIACRYPT'91, vilume 739 of Lecture Notes in computer Sience*, pages 36-50. Springer-Verlag, Berlin, 1993.

[6] Lawewnce Brown, Josef Pieprzyk, and Jennifer Seberry. LOKI - a cryptographic primitive for authentication and secrecy applications. In Jennifer Seberry and Josef Pieprzyk, editor, *Advances in Cryptology - AUSCRYPT'90, volume 453 of Lecture notes in Computer Science*, pages 229-236. Springer-Verlag, Berlin, 1990.

[7] C. Carlet. *Codes de Reed-Muller*. PhD thesis, Institute Blasie Pascal, Université Paris, 1990.

[8] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptoanalysis. In Alfredo De Santis editor, *Advances in Crytology: EUROCRYPT'94, volume 950 of Lecture Notes in Computer Science*, pages 356-365. Spinger-Verlag, Berlin, 1995.

[9] D. Feng and B. Liu. Almost perfect nonlinear permutations. *Electronics Letters*, 30(3):208-209, Feb 1994.

[10] R. Lidl and H. Niederreiter. Finite fields. In *Encyclopedia of Mathematics and its Applications*, volume 20. Addison-Wesley, 1983.

[11] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *Advances in Cryptology: EUROCRYPY'93, volume 765 of Lecture Notes in Computer Science*, pages 386-397. Springer-Verlag, Berlin, 1994.

[12] Kaisa Nyberg. Perfect nonlinear S-boxs. In D. W. Davices, editor, *Advances in Crytology: EUROCRYPT'91, volume 547 of Lecture Notes in Computer Science*, pages 378-386. Springer-verlag, Berlin, 1991.

[13] Kasia Nyberg. Differentially uniform mappings for cryptography. In Tor Helleseth, editor, *Advances in Cryptology: EUROCRYPT'93, volume 765 of Lecture Notes in Computer Science*, pages 55-64. springer-Verlag, Berlin, 1994.

[14] Kaisa Nyberg. S-boxs and round functions with controllable linearity and differential uniformity. In Bart Preneel, editor, *Fast Software Encryption: Second Internatonal Workshop, volume 1008 of Lecture Notes in Computer Science*, pages 111-130. Springer-Verlag, Berlin, 1995.

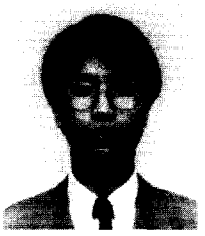
[15] National Bureau of Standards. FIPS PUB 46 : Data Encryption Standard, January 1997.

[16] Bruce Schneier. Description of a new variable-length key, 64-bit block cipher(blowfish). In Ross Anderson, editor, *Fast software encryption, Cambridge Security Workshop, volume 809 of Lecture Notes in Computer Science*, pages 191-204. Springer-Verlag, Berlin, 1994.

[17] Hennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. Systematic generation of cryptographically robust S-boxes. In *Proceedings of the first ACM Conference on Computer and Communication Security*, pages 172-182, 1993.

[18] A. Youssef, Stafford E. Tavares, S. Mister, and Carlisle M. Adams. Linear approximation of injective s-boxes. *Electronics Letters*, 31(25):2165-2166, Dec 1995.

□ 著者紹介



박 상 우

1985년 ~ 1989년 고려대학교 사범대학 수학교육과(이학사)
1989년 ~ 1991년 고려대학교 대학원 수학과(이학석사 : 응용수학 및 확률론)
1991년 ~ 현재 한국전자통신연구소 연구원

김 광 조(정회원)

1973년 ~ 1980년 연세대학교 전자공학과(학사)
1981년 ~ 1983년 연세대학교 대학원 전자공학과(석사)
1988년 ~ 1991년 요꼬하마 국립대학 대학원 전자정보공학과(박사)
현 한국전자통신연구소 실장,
본 학회 암호이론연구회 및 ISO/IEC JTC1 JSC-27 의장,
KIISC, IEICE, IEEE, IACR 각 회원

※ 주관심 분야 : 암호학 및 응용 분야, M/W 통신