Proceedings of International Conference
on Cryptology and Information Security

How to use Exponent Permutations in Cryptography - Classifications and Applications -

Sangwoo Park, Seongtaek Chee, Sangjin Lee, Yongdae Kim, Kwangjo Kim

Section 0710, Electronics and Telecommunications Research Institute
161 Kajong-Dong, Yusong-Gu, Taejon; 305-350, KOREA
{psw,chee,sjlee,kyd,kkj}@dingo.etri.re.kr

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 Introduction

Usually, the total security of block ciphers could be strengthened by iteration of substitution and permutation functions in their internal structure. The main necessary conditions for strong permutations are high nonlinearity, high algebraic degree, and resistance against the differential analysis [4] and the linear cryptanalysis [11] in a cryptographic sense. A special type of exponent permutations with high nonlinearity, high algebraic degree, and good property against differential and linear cryptanalysis was proposed in [13].

In this paper, we define an equivalence relation on the group of all permutations over finite field $GF(2^n)$. And we prove that if we restrict the equivalence class on the group of all exponent permutations, the restricted set is equal to the residue set modulo cyclic group $<x^2>$ on the group of all exponent permutations, and show that each equivalence class has common cryptographic properties. Then, we classify all exponent permutations over $GF(2^7)$ and $GF(2^8)$ by computer search. As the application of our results, we propose the design method of $n \times 2n$ S-boxes by concatenation of two exponent permutations over $GF(2^n)$ and analyse their cryptographic properties. And through our classifications, we find a counterexample of the conjecture of Beth in Eurocrypt'93 [2] and we clarify the cryptographic strength of S-boxes used in LOKI encryption algorithm [5, 6].

2 Classification of exponent Permutations over $GF(2^n)$

Denote by $\mathcal{P}_n$ the set of all permutations over the finite field $GF(2^n)$. A polynomial x^e over $GF(2^n)$ is a permutation if and only if $\gcd(e, 2^n-1)=1$, and we call such a polynomial an exponent permutation over $GF(2^n)$. The set of all exponent permutations over $GF(2^n)$ is denoted by $\mathcal{EP}_n=\{x^e | \gcd(e, 2^n-1)=1, x \in GF(2^n)\}$, For permutations $f(x)$ and $g(x)$ over $GF(2^n)$, the composite permutation $h(x) = f(x) \circ g(x)$ is defined by $h(x) = f(g(x)) \bmod (x^{2^n}-x)$. Under this operation $\circ$, $\mathcal{P}_n$ is a group, and $\mathcal{EP}_n$ is an abelian subgroup of $\mathcal{P}_n$. For $x^{e_1}, x^{e_2} \in \mathcal{EP}_n$, $x^{e_1} = x^{e_2}$ if and only if $e_1 = e_2 \bmod (2^n-1)$. The following theorem is one of the basic in the finite field theory.

Theorem 1 *[10] The set of automorphisms over $GF(2^n)$ fixing any elements in $GF(2)$ is a subgroup of the automorphism group over $GF(2^n)$, and is equal to the cyclic group generated by Frobenius automorphism. That is,*

$$\mathcal{G}(GF(2^n)/GF(2)) = < x^2 > .$$

where $\mathcal{G}(GF(2^n)/GF(2))$ means the set of all automorphisms over $GF(2^n)$ fixing any elements in $GF(2)$.

Corollary 1 *The set of all linear permutations in $\mathcal{EP}_n$ is the cyclic subgroup $< x^2 > \subset \mathcal{EP}_n$.*

Now, we define a relation on the set of permutations over $GF(2^n)$.

Definition 1 *For $P = (p_1, \cdots, p_n)$, $Q = (q_1, \cdots, q_n) \in \mathcal{P}_n$, we define a relation on $\mathcal{P}_n$ as follows :*

$P \sim Q$ *if there exists an $n \times n$ non-singular matrix A satisfying $P = L_A \circ Q$,*

where L_A is a linear transformation of a matrix A. In a view of component functions, the above relation can be written as follows :

$P \sim Q$ *if there exists a non-singular matrix $A=(a_{ij})$*

$\in GL_n(GF(2))$ *such that* $p_i = \sum_{j=1}^{n} a_{ij} q_j$, $1 \leq i \leq n$, *where* p_i *and* q_j *are component functions of* P *and* Q, *respectively.*

Lemma 1 *The relation defined in definition 1 is an equivalence relation.*

Since the relation defined on definition 1 is an equivalence relation, $\mathcal{P}_n = \bigcup_{P \in \mathcal{P}_n} \overline{P}$, where $\overline{P} = \{Q \in \mathcal{P}_n \mid P \sim Q\}$, and $\mathcal{P}_n/\sim = \{\overline{P} \mid P \in \mathcal{P}_n\}$. Naturally, we can define a set $\mathcal{EP}_n/\sim$ by $\mathcal{EP}_n/\sim = \{\overline{x^e} \cap \mathcal{EP}_n \mid x^e \in \mathcal{EP}_n\}$. For $\overline{x^{e_1}} \cap \mathcal{EP}_n, \overline{x^{e_2}} \cap \mathcal{EP}_n \in \mathcal{EP}_n/\sim$, define an operation $*$ on $\mathcal{EP}_n/\sim$ as $(\overline{x^{e_1}} \cap \mathcal{EP}_n) * (\overline{x^{e_2}} \cap \mathcal{EP}_n) = \overline{x^{e_1} \circ x^{e_2}} \cap \mathcal{EP}_n$. Then, $*$ is a well-defined operation, for $\mathcal{EP}_n$ is an abelian group. Hence, $\mathcal{EP}_n/\sim$ is a group.

Theorem 2 *Let* $x^e \in \mathcal{EP}_n$. *Then* $\overline{x^e} \cap \mathcal{EP}_n = < x^2 > x^e$.

Proof. By Corollary 1, $< x^2 > x^e \subset \overline{x^e} \cap \mathcal{EP}_n$. *Conversely, for* $y \in \overline{x^e} \cap \mathcal{EP}_n$, *there exist a non-singular matrix* A *and an integer* i *such that* $y = L_A \circ x^e$, *and* $y = x^i$. *By Corollary 1, for some* k, $L_A = x^{i-e} = x^{2k}$. *Hence, the converse is also true.*

□

By theorem 2, it is clear that $\mathcal{EP}_n/\sim = \mathcal{EP}_n/ < x^2 >$ and $|\mathcal{EP}_n/\sim| = \frac{\phi(2^n-1)}{n}$, where ϕ is an Euler function.

Now, we consider the cryptographic properties of exponent permutations over the finite field $GF(2^n)$. Using the cryptographic properties and the equivalence relation defined in definition 1, we can classify exponent permutations over $GF(2^n)$. First, we prove that exponent permutations in an equivalence class have same non-linearity and same algebraic degree.

Lemma 2 *Let* $P(x) = x^e$ *be an exponent permutation over* $GF(2^n)$. *Then*

1. *the algebraic degree of any linear combinations of component functions of* $P(x)$ *is* $wt(e)$.
2. *the non-linearity of any linear combinations of component functions of* $P(x)$ *has the same value.*

Proof. The proof of 1 is well-known [7]. Since $P(x) = x^e$ *is a permutation and* $\gcd(e, 2^n - 1) = 1$, *there exist* $t_1, t_2 \in \mathcal{Z}$ *such that* $t_1 e + t_2(2^n - 1) = 1$. *Therefore, for any* $x \in GF(2^n)$,

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

Let $p_i(x)$ *be any linear combination of component functions of* $P(x)$. *Then, for some* $\alpha_i \in GF(2^n)$, *the following equations hold [10] :*

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

Therefore, if we define $A_i : GF(2^n) \longrightarrow GF(2^n)$ *as* $A_i(x) = \alpha_i^{t_1} x$, *the non-linearity does not change, for* $p_i = Tr \circ P \circ A_i$, *and* A_i *is a linear function. Hence,*

$$\mathcal{N}_{P_k} = \mathcal{N}_{Tr \circ P}.$$

□

Since the algebraic degrees and non-linearities of any linear combination $p_i(x)$ of component functions of $P(x)$ are equivalent, we denote $deg(P(x)) = deg(p_i(x))$ and $\mathcal{N}_P = \mathcal{N}_{p_i}$. By Theorem 2 and Lemma 2, the following is easily obtained.

Theorem 3 *For* $P, Q \in \mathcal{EP}_n$ *and* $P \sim Q$, *we have*

1. $\mathcal{N}_P = \mathcal{N}_Q$,
2. $deg(P) = deg(Q)$. ·

Let P be a permutation with n input variables which we want to cryptanalysis. If we use the differential cryptanalysis method [4], we will need non-empty sets

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

where $a \neq 0$. The efficiency of differential cryptanalysis based upon a set $D_P(a, b)$ is measured by its cardinality

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

Similarly, if we use the linear cryptanalysis method [11], we will take advantage of sets

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

where $b \neq 0$. The efficiency of linear cryptanalysis that uses the set $L_P(a, b)$ is measured by the discrepancy between the cardinality of $L_P(a, b)$ and the average cardinality

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

Hence the resistance of permutation P can be measured by :

$\Delta_P = \max_{a \neq 0, b} \delta_P(a, b)$ for differential cryptanalysis,
$\Lambda_P = \max_{a, b \neq 0} |\lambda_P(a, b)|$ for linear cryptanalysis.

The lower these values are, the more resistant the permutation P will be against the corresponding cryptanalysis method. If $\Delta_P = \delta$, then P is said to be differentially δ-uniform. If Δ_P is minimal, P is differential resistant. By the same way, if Λ_P is minimal, P is linear resistant [8]. By [13], [17] and Theorem 3, we can obtain the following major results.

Theorem 4 *For* $P, Q \in \mathcal{EP}_n$ *with* $P \sim Q$, *the followings are hold*

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

Table 1: The known results of algebraic degree of P, Δ_P and Λ_P, where $P{=}x^e$ in $GF(2^n)$

P	$deg(P)$	Δ_P	Λ_P	conditions
x^{2^k+1}	2	2^s	$2^{\frac{n+s}{2}-1}$	$s{=}\gcd(n,k)$ $\frac{n}{s}$ is odd
$(x^{2^k+1})^{-1}$	$\frac{n+1}{2}$	2	$2^{\frac{n-1}{2}}$	$\gcd(n,k){=}1$ n is odd
x^{-1}	$n-1$	2	$\geq 2^{\frac{n}{2}}$	n is odd
x^{-1}	$n-1$	4	$\geq 2^{\frac{n}{2}}$	n is even

Table 2: Exponent permutations over $GF(2^7)$

class	algebraic degree	non-linearity	Δ	Λ	Exponent						
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
P12	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

So, we have the result that exponent permutations in an equivalence class have same Δ_P and Λ_P.

In [13], for a special type of exponent permutation $P = x^e$ in $GF(2^n)$, the algebraic degree of P, Δ_P and Λ_P are well-verified. We summarize the results in table 1.

Now, we classify the exponent permutations over $GF(2^7)$ and $GF(2^8)$ by the equivalence relation defined in definition 1. The table 2, we describe the results of classification of the exponent permutations over $GF(2^7)$. In table 2, the classes (P1, P13), (P2, P11), (P3, P9), (P4, P16), (P5, P6), (P7, P15), (P8, P14), and (P10, P12) have inverse function of each others, and exponent permutations in the class P17 are equivalent to x^{-1}, and the permutations in the class P18 are linear. Among exponent permutations over $GF(2^7)$, exponent permutations in the classes P9, P10, P11, P12, P13 are the best, and linear and differential resistant.

And, the table 3, we describe the results of classification of the exponent permutations over $GF(2^8)$. In table 3, the classes (P1, P5), (P2, P7), (P3, P12), (P4, P11), (P6, P13), and (P10, P14) have inverse function of each others, and the permutations in the classes P8 and P9 have inverse function in each class, and the exponent permutations in the class P15 are equivalent to x^{-1}, and the permutations in the class P16 are linear. Among exponent permutations over $GF(2^8)$, exponent permutations in the class P15 are the best.

3 Applications

In this section, three applications of the results in the previous section are described.

3.1 Design of $n{\times}2n$ S-boxes

As the first application, we propose a design method for $n{\times}2n$ S-boxes by the concatenation of two exponent permutations over $GF(2^n)$, and analyse the differential resistance and linear resistance of them. And, we simulate both Δ_S and Λ_S, where S is an $8{\times}16$ S-box which has a concatenated form of two exponent permutations over $GF(2^8)$.

For an $n{\times}m$ S-box S, $\Delta_S \geq \max(2, 2^{n-m})$. It was shown in [12] that for $n > m$ the minimum differential uniformity 2^{n-m} is reached if and only if $n \geq 2m$ and n is even. Such S-boxes are called perfect nonlinear and they are the same as the bent functions

Table 3: Exponent permutations over $GF(2^8)$

class	algebraic degree	non-linearity	Δ	Λ	Exponent							
P1	3	96	6	32	7	14	28	56	112	131	193	224
P2	3	96	10	32	11	22	44	88	97	133	176	194
P3	3	96	16	32	13	26	52	67	104	134	161	208
P4	3	104	16	24	19	38	49	76	98	137	152	196
P5	3	96	6	32	37	41	73	74	82	146	148	164
P6	4	96	16	32	23	46	92	184	113	139	197	226
P7	4	96	10	32	29	58	71	116	142	163	209	232
P8	4	80	30	48	43	86	89	101	149	172	178	202
P9	4	96	16	32	53	77	83	106	154	166	169	212
P10	5	112	16	16	31	62	124	143	199	227	241	248
P11	5	104	16	24	47	94	121	151	188	203	229	242
P12	5	96	12	32	59	103	118	157	179	206	217	236
P13	5	96	16	32	61	79	122	158	167	211	233	244
P14	5	112	16	16	91	107	109	173	181	182	214	218
P15	7	112	4	16	127	191	223	239	247	251	253	254
P16	1	0	256	128	1	2	4	8	16	32	64	128

[14]. Any S-box with $n > m$ has more input vectors than output vectors. This necessarily means that there will be at least one case where two or more inputs are mapped to the same output i.e., where one or more input XORs have an output XOR of zero. The weakness with having such an S-box is that such cases have a fixed, non-negligible probability of occurrence which may be exploited in a characteristic and used in differential cryptanalysis. This would be true for any DES-like cryptosystem. In fact, in [3], it could be generalized to show that bent function-based S-boxes would have a weakness for any $n > m$. In particular, in [3], it has observed that if 6×4 bent function-based S-boxes were to be used in DES [15], then DES could be broken using approximately 2^{30} chosen plaintext pairs. This is because such S-boxes would have equiprobable $\delta_S(a,b)$, meaning that "the input XORs which modify only private input bits of the S-boxes may cause zero output XOR with non-negligible probability" [1]. If $n \leq m$, this avenue of attack is typically not available because each input can be mapped to a unique output. In fact, the way to use injective S-boxes such that the number of output bits of the S-box is sufficiently larger than the number of input bits reduces $\delta_S(a,b)$ of the S-box. Some proposed block ciphers, such as CAST [1] and Blowfish [16], take advantage of this property.

And, in [18], the size of Λ_S was theoretically estimated, where S is a randomly selected injective S-boxes. And, by a simulation, it was compared theoretical estimate with simulation results for $8\times m$ injective S-boxes, when $m > 8$.

By the concatenation of two exponent permutations Pi and Pj over $GF(2^n)$, we can obtain an $n\times2n$ S-box, i.e., $S(x) = (Pi(x), Pj(x))$. Clearly, such an S-box is injective. The following theorem is the useful tool to analyse differential resistance and linear resistance of such S-boxes.

Theorem 5 [14] *Given a functions $F : Z_2^n \longrightarrow Z_2^m$ with cordinate functions $f_1, \ldots, f_m$ and a functions $g : Z_2^n \longrightarrow Z_2$, we set $\tilde{F} = (f_1, \ldots, f_m, g)$. Then*

1. $\Delta_F \geq \Delta_{\tilde{F}} \geq \frac{1}{2}\Delta_F$
2. $\Lambda_{\tilde{F}} \geq \max(\Lambda_F, \Lambda_g) \geq \Lambda_F$

By theorem 5, the $n\times2n$ S-boxes $S = (Pi, Pj)$ obtained by the concatenation of two exponent permutations Pi and Pj have Δ_S less than or equal to Δ_{Pi}, and Λ_S greater than or equal to the maximum value of Δ_{Pi} and Δ_{Pj}.

Now, we compute Δ_S and Λ_S for all 8×16 S-boxes which constructed by the concatenation of two exponent permutations over $GF(2^8)$. First of all, we prove following theorem.

Theorem 6 *Let $P1, P2, Q1, Q2 \in \mathcal{EP}_n$, with $P1 \sim P2$, $Q1 \sim Q2$ and $S1 = (P1, Q1)$, $S2 = (P2, Q2)$. Then the followings are hold*

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

Proof. Since, by definition 1, there exist non-singular matrices $A, B \in GL_n(GF(2))$ such that $P1 = A \circ P2$ and $Q1 = B \circ Q2$. Let $\alpha \in Z_2^n$, $\beta = (\beta_1, \beta2) \in Z_2^{2n}$ Then

$$\begin{aligned}
& \delta_{S1}(\alpha, \beta) \\
= \; & \#\{x | (P1, Q1)(x) \oplus (P1, Q1)(x \oplus \alpha) = (\beta_1, \beta_2)\} \\
= \; & \#\{x | (P1(x) \oplus P1(x \oplus \alpha)), (Q1(x) \oplus Q1(x \oplus \alpha)) = \\
& \quad (\beta_1, \beta_2)\} \\
= \; & \#\{x | (P2(x) \oplus P2(x \oplus \alpha)), (Q2(x) \oplus Q2(x \oplus \alpha)) = \\
& \quad (A(\beta_1), B(\beta_2))\} \\
= \; & \delta_{S2}(A(\beta_1), B(\beta_2))
\end{aligned}$$

So, $\Delta_{S1} = \Delta_{S2}$. And by the definition 1, $\Lambda_{S1} = \Lambda_{S2}$. □

Table 4: Δ_S of all 8×16 S-boxes constructed by concatenation of two exponent permutations over $GF(2^8)$

	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}
$P1$	6	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
$P2$	4	10	4	4	4	4	4	4	4	4	4	4	4	4	4	10
$P3$	4	4	12	4	4	4	4	4	12	4	4	12	4	4	4	12
$P4$	4	4	4	16	4	16	4	4	16	16	16	4	16	16	4	16
$P5$	4	4	4	4	6	4	4	4	4	4	4	4	4	4	4	6
$P6$	4	4	4	16	4	16	4	4	16	16	16	4	16	16	4	16
$P7$	4	4	4	4	4	4	10	4	4	4	4	4	4	4	4	10
$P8$	4	4	4	4	4	4	4	30	4	4	4	4	4	4	4	30
$P9$	4	4	12	16	4	16	4	4	16	16	16	12	16	16	4	16
$P10$	4	4	4	16	4	16	4	4	16	16	16	4	16	16	4	16
$P11$	4	4	4	16	4	16	4	4	16	16	16	4	16	16	4	16
$P12$	4	4	12	4	4	4	4	4	12	4	4	12	4	4	4	12
$P13$	4	4	4	16	4	16	4	4	16	16	16	4	16	16	4	16
$P14$	4	4	4	16	4	16	4	4	16	16	16	4	16	16	4	16
$P15$	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
$P16$	6	10	12	16	6	16	10	30	16	16	16	12	16	16	4	256

Table 5: Λ_S of all 8×16 S-boxes constructed by concatenation of two exponent permutations over $GF(2^8)$

	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

By theorem 6, we can simply compute Δ_S and Λ_S for 8×16 S-boxes $S = (Pi, Pj)$, where Pi and Pj are in other equivalence classes. By computer search, we obtain all Δ_S and Λ_S for all 8×16 S-boxes which constructed by all exponent permutations over $GF(2^8)$. We describe the simulation results in table 4 and 5. In table 4 and 5, each entry means Δ_S and Λ_S, respectively, where $S = (Pi, Pj)$, i is a row entry and j is a column entry. Among these, the best 8×16 S-box is $S = (P15, P15)$.

3.2 Falsity of Beth's Conjecture

In Eurocrypt'93 [2], Beth conjectured as follows :
Conjecture: Assume that n and $2^n - 1$ are two primes, then for each $2 \leq i \leq n-1$, an equation

$$Y^{2^m-1} + 1 = r(Y+1), r \neq 0, 1$$

has at most two solutions other than 1 in $GF(2^n)$.

Furthermore, he insisted that, any permutation of the form x^{2^m-1} with $2 \leq m \leq n-1$ is differential resistant, if his conjecture is true.

If n is equal to 7, then n and $2^n - 1$ are prime. But, for $m = 3$, a permutation $x^{2^m-1} = x^7$ does not have minimum differential resistance(P4 in table 2). Hence, the conjecture of Beth is not true. Already, in [9], Feng and Liu have indicated that the conjecture of Beth is wrong by finding three solutions other than 1 in $GF(2^n)$.

3.3 S-Box of LOKI Encryption Algorithm

The security of LOKI [6, 5] mostly depends on exponent permutation x^{31} over $GF(2^8)$. But, in table 3, exponent permutation in the class P15 is better than x^{31} in the aspect of algebraic degree and differential

cryptanalysis, though x^{31} has same linear resistivity as permutations in the class P15. Even if our result is good for alternative S-box of LOKI, total security of LOKI replaced its S-Box with permutations in the class P15 must be carefully considered, and it needs to study its strength against linear cryptanalysis and differential cryptanalysis.

4 Conclusions

In this paper, we defined an equivalence relation on the group of exponent permutations over $GF(2^n)$, and proved the exponent permutations in the same equivalence class have the same cryptographic properties. We classified exponent permutations over $GF(2^7)$ and $GF(2^8)$ with cryptographic properties according to the equivalence relation. For applications of classification of exponent permutations, we designed $n \times 2n$ S-boxes by concatenating two exponent permutations and analysed their differential and linear characteristics. Also, we found counter example to indicate that the conjecture of Beth is wrong and found better permutations compared with S-Boxes used in LOKI encryption algorithm.

References

[1] Carlisle M. Adams and Stafford E. Tavares. Designing S-boxes for ciphers resistant to differential crypsanalysis. In *the 3rd symposium of state and progress of research in cryptography, 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 cryptosystems.* Ph.D thesis, Wiezman Institute of Science, Rehovot, Israel, 1992.

[4] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, volume 4, number 1, pages 3–72, 1991.

[5] Lawewnce Brown, Matthew Kwan, Josef Pieprzyk, and Jennifer Seberry. Improving resistance to differential cryptanalysis and the redesign of LOKI. In Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors, *Advances in Cryptology - ASIACRYPT'91*, volume 739 of *Lecture Notes in Computer Science*, 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, editors, *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.* Ph.D thesis, Institute Blasie Pascal, Université Paris, 1990.

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

[9] D. Feng and B. Liu. Almost perfect nonlinear permutations. *Electronics Letters*, volume 30, number 3, pages 208–209, Feb 1994.

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

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

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

[13] Kaisa 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-boxes and round functions with controllable linearity and differential uniformity. In Bart Preneel, editor, *Fast Software Encryption : Second International 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 1977.

[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] Jennifer 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*, volume 31, number 25, pages 2165–2166, Dec 1995.