Joint Conference of 1996 International Computer Symposium
December 19~21, Kaohsiung, Taiwan, R.O.C.

Some Cryptographic Properties of Exponential Functions *

Dawu Gu and Guozhen Xiao

Research Institute of Information Security and Privacy
Xidian University
Xi'an 710071, P.R.China
gzxiao@xidian.edu.cn

Abstract

Further analysis of cryptographic properties of exponential functions given in [1] is made. Emphasis is put on its enumeration, fixed points and cyclic structure. The results obtained provide some cryptographic principles for the design of secure S boxes based on such functions.

Key words: *Exponential function, Exponential permutation, Fixed point, Cyclic period, S box*

1 Introduction

It is well known that the security of modern block cipher system largely depends on the cryptographic properties of its substitution boxes (or, S boxes). Therefore the study of it appears to be more important. As shown in present research[3–6], a good S boxes should satisfy all (or most) of the following known security criteria, such as balance, non-linearity, correlation-immunity, strict avalanche criteria (SAC), propagation characteristics and I/O XOR distribution properties, etc. To fully evaluate the S box, further research on new designing principles is necessary.

In the general case, an S box can be denoted by the permutation over $GF(2)^n$. There are various ways to construct such permutations. As a result. the S boxes obtained have different secure characteristics. To measure its security precisely (or approximately), the S box must have an algebric or topological structure which is convenient to analyse. With the adoption of exponential funstions over a finite field to construct the S boxes in [1], some valuable results have been available. Meanwhile, such exponential function is well proved with SAC and non-linearity. With the study of the exponential function from a new viewpoint, this paper begins with the discussion on the enumerating problem of permutations generated by such functions, which we call exponential permutations, under different coordinate bases, followed by two new safety indexes, or, the number of fixed points and cyclic periods. Certain relevent parameters of exponential functions are given. Moreover, the elements in $GF(2^n)$ are classified in accordance with its cyclic structure. All of the results we expect to provide some evidence in cryptology for the design of secure S boxes based on exponential functions. Finally, some experimental results and a conjecture are given.

*This work was sponsored by National Natural Science Fund, People's Republic of China.

2 Enumeration of Exponential Permutations

Given that $b \in GF(2^n), c \in \{s : (s, 2^n-1) = 1, 0 \leq s \leq 2^n-1\}$. Let $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a basis of $GF(2^n)$ over $GF(2)$ and $\beta_0, \beta_1, \ldots, \beta_{n-1} \in GF(2^n)$. A mapping f is defined as follows:

$$\begin{array}{rcl} \mathrm{f} : GF(2)^n & \rightarrow & GF(2)^n \\ \mathrm{x} = (x_0, \ldots, x_{n-1}) & \mapsto & \mathrm{f}(\mathrm{x}) = (f_0(\mathrm{x}), \ldots, f_{n-1}(\mathrm{x})) \end{array} \quad (1)$$

where $f_j(\mathrm{x}) = Tr(\beta_j(\sum_{i=0}^{n-1} x_i\alpha_i + b)^c)$. Then we have the following lemma about the transformation given in equation (1).

Lemma 1[1] f is a permutation over $GF(2)^n$ if and only if $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ is a basis of $GF(2^n)$ over $GF(2)$. We call f an exponential permutation. □

It is not difficult to prove the valid of the inverse permutation f^{-1}: $\mathrm{f}^{-1}(\mathrm{y}) = (f_0^{-1}(\mathrm{y}), f_1^{-1}(\mathrm{y}), \ldots, f_{n-1}^{-1}(\mathrm{y}))$, where $f_j^{-1}(\mathrm{y}) = Tr(\alpha'_j((\sum_{i=0}^{n-1} y_i\beta'_i)^{c'} - b))$, and c' satisfies $cc' \equiv 1 \ mod \ 2^n - 1, 0 \leq c' \leq 2^n - 1$. Here $\{\alpha_j\}$ is the dual basis of $\{\alpha'_j\}$, and $\{\beta_j\}$ is the one of $\{\beta'_j\}$.

Obviously, the number of exponential permutations defined by equation (1) is $\prod_{i=0}^{n-1}(2^n - 2^i)$, when b, c and $\{\alpha_j\}$ are given.

For the convenience of operating in Galois field and lowering the memory capacity, sometimes we need to select some special types of bases, for instance, the

polynomial basis and normal one. The number of exponential permutation under this situation should be considered in designing S boxes. For this reason, a few definitions and lemmas are given as follows.

An ordered set $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ of any n elements in $GF(2^n)$ considered as an n dimension space over $GF(2)$ is called a basis if it is linear independent. If the set appears in the form of $\{1, \alpha, \ldots, \alpha^{n-1}\}$ and $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$, we call a polynomial basis and a normal one respectively (generated by the element α).

Lemma 2[2] The number of polynomial bases of $GF(2^n)$ over $GF(2)$ is

$$P(n) = \sum_{d|n} \mu(d) 2^{\frac{n}{d}}$$

where μ is the Möebius function. Similarly, given that $n = 2^m n_1, (n_1, 2) = 1$, then the number of normal bases is

$$Q(n) = 2^{(2^m-1)n_1} \prod_{d|n_1} (2^{r(d)} - 1)^{\frac{\varphi(d)}{r(d)}}$$

where φ is the Euler function, $r(d)$ the multiply order of 2 modulo d, and $r(1) = 1$. □

From Lemma 1,2 we have the following results.

Theorem 1 Let $\alpha_j = \alpha^j, \beta_j = \beta^j, (j = 0, 1, \ldots, n-1)$, and α can generate a polynomial basis, then f is an exponential permutation if and only if β can generate a polynomial basis. And if b, c and $\{\alpha^i\}$ are given, the number of such permutations is $P(n)$. Similarly, let $\alpha_j = \alpha^{2^j}, \beta_j = \beta^{2^j}, (j = 0, 1, \ldots, n-1)$, and α can generate a normal basis, then f is an exponential permutation if and only if β can generate a normal basis. Under the same condition mentioned before , the number of such permutation is $Q(n)$. □

3 Fixed Points of Exponential Function

Let $f(x) = (x + b)^c$ be an exponential function over $GF(2^n)$, where $b \in GF(2^n), (c, 2^n - 1) = 1$, and $c = 2^{l_1} + 2^{l_2} + \cdots + 2^{l_s} (1 \le l_1 < l_2 < \ldots < l_s < n)$. We define the set of fixed points of f as

$$Fix_f^{(b,c)} = \{x_0 \in GF(2^n) : f(x_0) = x_0\}$$

It is easily seen that

$$Fix_f^{(b,c)} = \{x_0 + b \in GF(2^n) : x_0^c + x_0 + b = 0\}$$

In view of the design of an S box, f should have any fixed points as less as possible so that f can provide the necessary confusion at all the points, concerning all the parameters (b, c).

When $b = 0$, the following results can be found.

Theorem 2 (1) If $c = 2^l$, then $Fix_f^{(0,c)} = GF(2^d)$ and $|Fix_f^{(0,c)}| = 2^d$, where $d = (l, n)$. Especially when n is prime, $Fix_f^{(0,c)} = \{0, 1\}$. (2) If $s \ge 2$, then $Fix_f^{(0,c)} = \{0, x \in GF(2^n) : o(x) | (c - 1, 2^n - 1)\}$ and $|Fix_f^{(0,c)}| = 1 + \sum_{d|(c-1,2^n-1)} \varphi(d)$. In the special case that $2^n - 1$ is prime, we have $Fix_f^{(0,c)} = \{0, 1\}$. □

Generally, we have the following theorem.

Theorem 3 (1)

$$Fix_f^{(b,2)} = \begin{cases} \emptyset & Tr(b) \neq 0 \\ x_0 + b + GF(2) & Tr(b) = 0 \end{cases}$$

where $x_0^2 + x_0 + b = 0$, and

$$|Fix_f^{(b,2)}| = \begin{cases} 0 & Tr(b) \neq 0 \\ 2 & Tr(b) = 0 \end{cases}$$

When $l \ge 2$ and if $x^{2^l} + x + b$ has no factor in $GF(2^n)[x]$ of even degree, then

$$Fix_f^{(b,2^l)} = \begin{cases} \emptyset & Tr(b) \neq 0 \\ x_0 + b + GF(2^l) & Tr(b) = 0 \end{cases}$$

where $x_0^{2^l} + x_0 + b = 0$, and

$$|Fix_f^{(b,2^l)}| = \begin{cases} 0 & Tr(b) \neq 0 \\ 2^l & Tr(b) = 0 \end{cases}$$

(2) Let $B^{(c)} = \{b \in GF(2^n) : x^c + x + b$ is irreducible over $GF(2^n)\}$, then for each element $b \in B^{(c)}$, $Fix_f^{(b,c)} = \emptyset$. □

It is our regret that we could not yet get the expression of $|Fix_f^{((b,c)}|$ when $s > 1$, for the question concerned is equivalent to factoring the general polynomial $x^m + x + b$ over $GF(2^l)$. However, it is shown from some experiments that there exists many (b, c) satisfying the condition of theorem 3, each of which makes f have some fixed points. For this reason, the security of such functions deserves to be questioned.

4 Cyclic Structures of Exponential Functions

Definition 1 For the given $b \in GF(2^n)$ and $c \in S = \{s : (s, 2^n - 1) = 1, 0 \le s \le 2^n - 1\}$, a recurrencing sequence $\{x_i\}_{i=0}^{\infty}$ is defined by the exponential function $f(x) = (x + b)^c$ over Galois field, as well as initial state $x_0 \in GF(2^n)$ with a relation of $x_{i+1} = f(x_i) = f^2(x_{i-1}) = \cdots = f^{i+1}(x_0)$. The sequence $\{x_i\}_{i=0}^{\infty}$ we call one derived from $f(x_0)$. If

there exists a minimum positive integer T satisfying $x_{i+T} = x_i (i \geq 0)$, T is called the period of $\{x_i\}_{i=0}^{\infty}$ and the cyclical one of $f(x_0)$ as well, which is written by $T_{(b,c,x_0)}$. For x_j, if there exists a minimum positive integer t_j satisfying that $x_{j+t_j} = x_j$, then t_j is called the period of x_j, with its written form of $t_{(b,c,x_j)}$. $T_{(b,c)} = min\{T : f^T(x) = x, \forall x \in GF(2^n)\}$ is said to be the period of $f(x) = (x+b)^c$. □

From this definition, the following results are easily found.

Lemma 4 Suppose $x_0 \in GF(2^n)$, then the sequence $\{x_i\}_{i=0}^{\infty}$ derived from $f(x_0)$ satisfies

$$T_{(b,c,x_0)} = t_{(b,c,x_j)} | T_{(b,c)} (j = 0, 1, 2, \ldots)$$

□

Lemma 5 For any element x in $GF(2^n)$, the inequality $T_{(b,c,x)} \leq 2^n$ is held. □

The above lemmas make it clear that the period of each element in sequence $\{x_i\}_{i=0}^{\infty}$ derived from $f(x_0)$ is the same. In addition, as shown in figure 1, $f(x)$ started at any point x_0 must pass $T_{(b,c,x_0)}$ times iteration before it return to the point x_0.

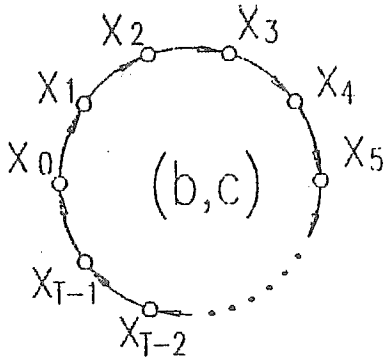

Figure 1. The state diagram of the sequence derived from $f(x_0)$.

With lemma 4, we can see that there is no smaller cycle in figure 1. Lemma 5 shows that $T_{(b,c,x)} \leq 2^n$. Hence, the elements in $GF(2^n)$ can be categoried with the help of the state diagram of sequence derived from $f(x)$ as shown in figure 2.

Let

$$A_i = \{x_0^{(i)}, x_1^{(i)}, \ldots, x_{T_{(b,c,x_0^{(i)})}-1}^{(i)}\} (i = 1, 2, \ldots, s)$$

then

$$GF(2^n) = \bigcup_{i=1}^{s} A_i$$

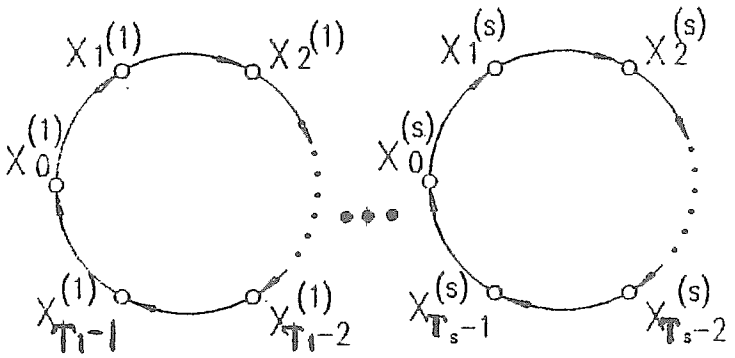

Figure 2. The cyclic structure of elements in $GF(2^n)$.

and for any $i \neq j$, the two equations $A_i \bigcap A_j = \emptyset$, $\sum_{i=1}^{s} T_{(b,c,x_0^{(i)})} = 2^n$ hold.

In view of cryptographic design, we hope that all (or almost) of the points in $GF(2^n)$ are in the same circle. In this case, the period is the largest.

In general case, the cyclic structure of the elements in $GF(2^n)$, as shown in figure 2, can lead to the following theorem.

Theorem 4 (1) If $T_{(b,c,x_0^{(i)})} \neq T_{(b,c,x_0^{(j)})}$, then $A_i \neq A_j$.

(2) If $T_{(b,c,x_0^{(i)})} = T_{(b,c,x_0^{(j)})} > 2^{n-1}$, then $A_i = A_j$.

(3) If $T_{(b,c,x_0^{(1)})} = T_{(b,c,x_0^{(2)})} = \cdots = T_{(b,c,x_0^{(r)})} > 2^n/r$, then there must be $A_i = A_j$ for some $1 \leq i < j \leq r$.

(4) $T_{(b,c)} = lcm(T_{(b,c,x_0^{(1)})}, T_{(b,c,x_0^{(2)})}, \cdots, T_{(b,c,x_0^{(s)})})$. □

The discussion on the distribution of $T_{(b,c,x)}$ is as follows. Suppose $b = 0$ firstly.

Theorem 5 For any x in $GF(2^n)$, there is $T_{(o,c,x)} | o(c) = T_{(o,c)} | \varphi(2^n - 1)$, where $o(c)$ is the order of c modulo $2^n - 1$, φ the Euler function. And for the cyclic classification $\bigcup_{i=1}^{s} A_i$ of $GF(2^n)$, there is $s \geq 2^n/o(c) > 1$. □

It is shown by theorem 5 that when $b = 0$, each A_i in $\bigcup_{i=1}^{s} A_i$ consists of $o(c)$ elements at most. At the same time, there exist at least A_i and A_j whose intersection is empty. Therefore, considering the design

of S box, $o(c)$ should be as large as possible.

When $b \neq 0$, it is so diffucult to calculate $T_{(b,c,x)}$ accurately that we can only have the following result (simply written as $m = T_{(b,c,x)}$).

Theorem 6 When $c = 2^l$, there is

$$min_{x \in GF(2^n)} T_{(b,2^l,x)} = min\{m : x^{2^{ml}} + x + \sum_{i=1}^{m} b^{2^{il}} \in GF(2^n)[x] \text{ is reducible over } GF(2^n)\}$$

When $s > 1$, we could not provide the algebric expression of $minT_{(b,c,x)}$ except the following experimental results.

Choose $n = 13$, with the adoption of irreducible polynomial $h(x) = x^{13}+x^{12}+x^{10}+x^9+1$ over $GF(2)$, the finite field $GF(2^{13})$ can be constructed. It can be proved[2] that the set $\{\alpha, \alpha^2, \cdots, \alpha^{2^{12}}\}$ of all the roots of $h(x)$ in $GF(2^{13})$ is a normal basis of $GF(2^{13})$. Let $b = \sum_{i=0}^{5} \alpha^{2^i}, c = 241 = 2^7 + 2^6 + 2^5 + 2^4 + 1$, then we have

$$T_{(\sum_{i=0}^{5} \alpha^{2^i}, 241, x_0)} = \begin{cases} 6527 & x_0 = \alpha \\ 1420 & x_0 = \alpha^{2^4} \end{cases}$$

about the cyclic periods of the function $f(x) = (x + b)^{241}$.

We see from above discussion that there may exist some small cycles in the diagram of cyclic structures, which is unfavorable to cipher designers. So, to prevent such disadvantage from appearing, we must choose (b, c) cautiously. However, considering the number of keys in cryptology, it narrows the range of (b, c) available in a further step. As a result, it must be tradeoff while considering this point.

Finally, as to cyclic structure diagram, we have the following conjecture.

Conjecture If $T_{(b,c,x_i)} = T_{(b,c,x_j)}$ and $x_i \in A_i (i \neq j)$, then $x_j \in A_i$. □

5 Conclusion

For the S box constructed by an exponential function, two new security indexes are proposed. Moreover, the enumeration of exponential permutations, the distribution of fixed points of exponential functions and its cyclic structure diagram are discussed theoretically, which to some degree provide some cryptographic characteristics of such type of S box and point out the problems deserving more attention concerning to the design of S box. However, the work on the paper need to be gone a step further which makes us deal with some of the problems unsolved in finite field.

References

[1] X.G.Chang, Z.D.Dai and G.Gong, "Some cryptographic properties of exponential functions", LNCS 917, Advances in Cryptology, Proceedings of ASIACRYPT'94, pp.415-418, 1994

[2] R.Lidl and H.Niederreiter, Finite Fields, Encyclopedia Mathematics and its Applications, Vol.20, Addison-Wesley, Reading, 1983.

[3] A.F.Webster and S.E.Tavares, "On the design of S-boxes", Advances in Cryptology, Proc. Crypto'85, Lecture Notes in Computer Science, Vol.218, pp523-534, Springer-Verlag, 1986.

[4] R.Forré, "The strict avalanche criterion: spectral properties of Boolean functions and an extended definition", Advances in Cryptology, Proc. Crypto'88, Springer-Verlag, pp450-468, 1990.

[5] B.Preneel, et al., "Propagation characteristics of Boolean functions", Advances in Cryptology, Proc. Eurocrypto'90, Lecture Notes in Computer Science, Springer-Verlag, Vol.437, pp161-173, 1991.

[6] Y.Desmedt, J.-J.Quisquater and M.Davio, "Dependence of output on input in DES: small avalanche characteristics", Advances in Cryptology, Proc. Crypto'84, Springer-Verlag, pp359-376, 1985.