갈로아체 멱승 순환 함수의 입출력 변환의 균등성

김희진 김종덕 손중제 임종인
고려대학교 수학과

A differential Uniformity of Permutations u^x in $GF(2^n)$

Kim, Hee-Jean Kim, Jong-Deok Son, Jung-Je Lim, Jong-In
Dept. of Mathematics, Korea University

November 7, 1997

Abstract

S-box의 암호학적 성질이 블록 암호 알고리즘의 안정성을 좌우한다. 여기서 말하는 암호학적 성질이란 선형 공격법에 안전한 높은 비선형성과 입출력 변화공격법에 안전한 입출력 변환의 낮은 균등성을 말한다. 본 논문에서는 갈로아 체의 원시원을 밑으로 하는 멱승 순환 함수를 이용한 S-box의 입출력 변환의 균등성에 관하여 서술한다.

1 Introduction

Most block ciphers have S-boxes(substitution box) or vector Boolean functions for encryption and decryption. The desirable properity which S-boxes and Boolean functions have to have is nonlinearity. We want to find out S-boxes and vector Boolean functions with high nonlinearity for designing block cipher and stream ciphers. Security of block cipher depends mainly on S-boxes and that of stream cipher also depends on Boolean functions. How to construct or how to find out cryptographically good S-boxes are very important problems in designing a block cipher. A vector Boolean function $f : \mathbf{Z}_2^n \longrightarrow \mathbf{Z}_2^m$ is considered as a S-box.

For even small n, m, to search exaustively vector Boolean functions is infeasible. Thus we need a systematic method to construct S-boxes. Many

results on the area to construct S-boxes have been published[1], [5], [6]. Now we are concerned with the case of $n = m$, that the domain and the co-domain of a vector Boolean function f are same, which says f is a permutation of $GF(2^n)$.

K. Nyberg [5], [6], researched cryptographic properties on some types of the permutation functions, for example, x^{-1} and x^{2^k+1} over $GF(2^n)$. She presented a permutation function u^x over a prime field $GF(p)$, where p is prime, u is a primitive element of $GF(p)$ and x is an integer, and studied cryptographic properties on permutation functions.

Now we want to present a permutation over $GF(2^n)$ with cryptographically good properties. Assume $u \in GF(2^n)$ is a primitive element. Define $f : \mathbf{Z}_{2^n} \longrightarrow GF(2^n)$ by

$$f(x) = \begin{cases} u^x & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}.$$

It will be said to be a exponent permutation, informally. But K. Nyberg, [6], T. Beth [1] and others have called a permutation like x^k to be a exponent permutation, but we had better call it by a monomial permutation.

Exponential permutations have very useful properties. First, it can have a precomputation table since the base u is fixed. Thus, secondly, we can design the block cipher with a large-size S-box. Generally speaking, the more S-box size, the better S-box security. In fact, it is impossible for block ciphers to have large-size S-box, because S-box data are in the memory and to encrypt a message without sufficient memories takes too much long time. Large size S-boxes need huge memory exponentially. Finally, we can construct variable size S-boxes using the exponent permutation.

2 Definitions and Notations

For a Boolean function $f : GF(2^n) \longrightarrow GF(2^m)$, $a \in GF(2^n)$ and $b \in GF(2^m)$ Then we make the following notation.

$$\delta_f(a, b) = \#\{x \in GF(2^n) | f(x + a) + f(x) = b\}$$

Definition 2.1 *Let $f : GF(2^n) \longrightarrow GF(2^m)$ be a function. Then f is called differentially δ-uniform if*

$$\max_{a \neq 0, b} \delta_f(a, b) \leq \delta \text{ for all } a \in GF(2^n)(a \neq 0), b \in GF(2^m),$$

$\Delta(f) = \max_{a \neq 0, b} \delta_f(a, b)$ is said to be the differential uniformity of f.

Clearly $\Delta(f) \geq \max\{2, 2^{n-m}\}$ and f is differentially $\Delta(f)$-uniform. In order that a S-box f is resisitant against the differential cryptanalysis, $\Delta(f)$ have to be small.

Since $GF(2^n) \cong GF(2)[t]/g(t)$, where $g(t)$ is an irreducible polynomial in $GF(2)[t]$ and t is an indeterminate. Then $x \in GF(2^n)$ can be represented by a polynomial basis $\{t^{n-1}, \cdots, t, 1\}$, say $x = x_{n-1} \cdot t^{n-1} + \cdots + x_1 \cdot t + x_0$.

Assume that u is a primitive element in a Galois field $GF(2^n)$. Consider the function $f(x) : \mathbf{Z}_{2^n} \longrightarrow GF(2^n)$ defined by $f(x) = u^x$. But f is not a injective map, since $u^0 = u^{2^n-1} = 1$. and there is not $x \in \mathbf{Z}_{2^n}$ with $f(x) = 0$. Thus we have to replace $f(0)$ by 0 or $f(2^n - 1)$ by 0. Then f is injective.

Definition 2.2 *Let ψ be a bijective mapping defined by*

$$\begin{aligned} \psi : \ GF(2^n) &\longrightarrow \mathbf{Z}_{2^n} \\ x &\longmapsto x_{n-1} \cdot 2^{n-1} + \cdots + x_1 \cdot 2 + x_0, \end{aligned}$$

where x is represented by a polynomial basis and let u be a primitive element of $GF(2^n)$. Define $f : GF(2^n) \longrightarrow GF(2^n)$ by

$$f(x) = \begin{cases} u^{\psi(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}.$$

Then f is said to be a exponent permutation.

In general, two different exponent permutation f and g are not equivalent in the sense that $f = A \circ g \circ B$ for some linear transformations A and B.

Theorem 2.1 *The number of exponent permutations of $GF(2^n)$ is less than or equal to*

$$\frac{\phi(2^n-1)}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) 2^d = \frac{\phi(2^n-1)}{n} \sum_{d|n} \mu(d) 2^{n/d},$$

where ϕ is the Euler function and μ is the Möbius function.

3 Differential uniformity of exponent permutations

Our purpose is to find cryptographically good vector Boolean functions or S-boxes, say $f : GF(2^n) \longrightarrow GF(2^m)$, which means it has high non-linearity and small differential uniformity. But it is not easy to find a good vector

Boolean function exaustively for even small n, m. Thus we want to use a algebraic tool to construct good vector Boolean function. First of all, we will restrict the concerned vector Boolean functions to the permutation on Galois fields $GF(2^n)$, that is, $f : GF(2^n) \longrightarrow GF(2^n)$. Some algebraically special type of permutations on Galois fields were researched. K. Nyberg studied on the permutation functions on Galois field like x^{-1} and x^{2^k+1} and on the exponent permutation functions on finite prime fields $\mathbf{Z}_p$ like u^x, where u is a primitive element [6]. But the study on the exponent functions on $GF(2^n)$ was not researched cryptographically in a sense. In this paper, we want to study on them.

Let $\psi : GF(2^N) \longrightarrow \mathbf{Z}_{2^n}$ be the function defined in Definition 2.2. In general, $\psi(x+a) \neq \psi(x)+\psi(a)$, since the algebraic structues of $GF(2^n)$ and $\mathbf{Z}_{2^n}$ are different from each other. But, its equality may hold in some cases. The following lemma says their cases. To find an upper bound of $\Delta(f)$, we need the following lemma. If x is an element of $GF(2^n)$, we can represent x as $x = (x_{n-1}, \cdots, x_1, x_0)$, since $GF(2^n)$ is a vector space over $GF(2)$.

Lemma 3.1 *Let x and a be elements in $GF(2^n)$, then we can represent x and a as $x = (x_{n-1}, \cdots, x_1, x_0)$ and $a = (a_{n-1}, \cdots, a_1, a_0)$, respectively. Assume that if $a_i = 1$, then $x_i = 0$, which says that the case of $x_i = a_i = 1$ does not occur for all $i \in \{0, 1, \cdots, n-1\}$. Then $\psi(x \oplus a) = \psi(x) + \psi(a)$, where ψ is the function defined in Definition 2.2.*

Proof. Let $\oplus$ denote the addition over $\mathbf{Z}_2$ i.e. the bitwise exclusive or operation in the computer instruction. Under the given condition, $x_i + a_i$ has no carry in the usual addition, since the case of $x_i = a_i = 1$ does not occur for all $i \in \{0, 1, \cdots, n-1\}$. Thus

$$\begin{aligned}
\psi(x) + \psi(y) &= \psi\left((x_{n-1}, \cdots, x_1, x_0) \oplus (a_{n-1}, \cdots, a_1, a_0)\right) \\
&= x_{n-1} \cdot 2^{n-1} + \cdots + x_1 \cdot 2 + x_0 \\
&\quad + a_{n-1} \cdot 2^{n-1} + \cdots + a_1 \cdot 2 + a_0 \\
&= (x_{n-1} + a_{n-1}) \cdot 2^{n-1} + \cdots + (x_1 + a_1) \cdot 2 + (x_0 + a_0) \\
&= (x_{n-1} \oplus a_{n-1}) \cdot 2^{n-1} + \cdots + (x_1 \oplus a_1) \cdot 2 + (x_0 \oplus a_0) \\
&= \psi(x_{n-1} \oplus a_{n-1}, \cdots, x_1 \oplus a_1, , x_0 \oplus a_0) \\
&= \psi\left((x_{n-1}, \cdots, x_1, x_0) \oplus (a_{n-1}, \cdots, a_1, a_0)\right) \\
&= \psi(x + a)
\end{aligned}$$

The lemma is proved. □

Some tedious manipulation yields the following theorem using Lemma 3.1.

Theorem 3.1 *Let $f : GF(2^n) \longrightarrow GF(2^n)$ be a exponent permutation and let $a(\neq 0), b$ be in $GF(2^n)$. Then*

$$\delta_f(a,b) \leq \min\{2^{wt(a)}+2, 2^{n-wt(a)+1}+2\},$$

where $wt(a)$ is the Hamming weight of a.

Theorem 3.1 says that a small difference of input data yields good differential uniformities. Now we may get a differential uniformity of exponent permutation using the above theorem.

Theorem 3.2 *Let f be a exponent permutation of $GF(2^n)$. Then $\Delta(f) \leq 2^{\lceil \frac{n}{2} \rceil}+2$.*

In addition, we have a result on a differential uniformity.

Theorem 3.3 *Let f and g be exponent permutations of $GF(2^n)$. Then $\Delta(g) \leq \Delta(f)+4$.*

This theorem says that when we get a differental uniformity of an exponent permutation of $GF(2^n)$, we may know an upper bound of differential uniformity of all exponent permutations of $GF(2^n)$.

The following tables are some computational experiment results.

irreducible polynomials	primitive elements u	
$g(t)$	t	$t+1$
t^2+t+1	4	4

Table 1: $\Delta(f)$ in $GF(2^2)$

irreducible polynomials $g(t)$	primitive elements u					
	t	$t+1$	t^2	t^2+1	t^2+t	t^2+t+1
t^3+t+1	2	4	2	4	2	4
t^2+t^2+1	4	2	4	2	2	4

Table 2: $\Delta(f)$ in $GF(2^3)$

primitive element u	irreducible polynomial $g(t)$		
	t^4+t+1	t^4+t^3+1	$t^4+t^3+t^2+t+1$
t	4	6	·
$t+1$	4	·	6
t^2	4	6	·
t^2+1	4	·	6
t^2+t	·	4	4
t^2+t+1	·	4	4
t^3+1	6	6	6
t^3+t	·	·	4
t^3+t+1	6	·	4
t^3+t^2	·	4	·
t^3+t^2+1	6	4	·
t^3+t^2+t	6	6	6

Table 3: $\Delta(f)$ in $GF(2^4)$

4 Conclusion

In the cases of $n = 2$ and $n = 4$, the upper bound of $\Delta(f)$ in Theorem 3.2 is tight. But in the cases of $n \geq 5$, $\Delta(f)$ is less than the above upper bound, which says it is more resilent to the differential cryptanalysis. The thoerem says that the largest probability for the differential cryptanalysis is less than or equal to $2^{-\frac{n}{2}} + 2^{-n+1}$ when n is even and $2^{-\frac{n-1}{2}} + 2^{-n+1}$ when n is odd. In the application to Feistel network in designing a block cipher, it has the probability less than or equal to the value approximate to 2^{-n+1} in s-round

differential, $s \geq 4$ [8].

To prove that the exponent permutation is resistant against the different cryptanalysis, we have to find an upper bound less than that of Theorem 3.2. In addition, we did not state the nonlinearity of exponent permutations for resistance against the linear cryptanalysis. Thus we need more research on the exponent permutation to construcr S-box.

References

[1] T. Beth and C. Ding, *On Almost Perfect Nonlinear Permutations* Advances in Cryptology - Eurocrypt '93. Lecture Notes in Computer Science 765, Springer-Verlag(1993).

[2] E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, J. Cryptology 4 (1991).

[3] X. Lai, J. L. Massey and S. Murphy, *Markov Ciphers and Differential Cryptanalysis*, Advances in Cryptology - Eurocrypt '91, Lecture Notes in Computer Science 547, Springer-Verlag (1992).

[4] R. Lidl and H. Niederreiter, *Finite Fields* Addition-Wesley Publishing Company Inc.(1983).

[5] K. Nyberg, *On the construction of highly nonlinear permutations*, Advances in Cryptology - Eurocrypt '92, Lecture Notes in Computers Science 547, Springer-Verlag (1993).

[6] K. Nyberg, *Differential uniform mappings for cryptography* Advances in Cryptology - Eurocrypt '93, Lecture Notes in Computer Science 765, Springer-Verlag(1993).

[7] K. Nyberg and L. R. Knudsen, *Provable Security Against Differential Cryptanalysis*, Advaces in Cryptology - Crypto '92 Lecture Notes in Computers Science 740, Springer-Verlag(1992).

[8] K. Nyberg and L. R. Knudsen, *Provable Security Against a Differential Attack*, J. Cryptology 8 (1995)