S-boxes with Controllable Nonlinearity

Jung Hee Cheon, Seongtaek Chee, and Choonsik Park

Electronics and Telecommunications Research Institute,
161 Kajong-Dong,Yusong-Gu, Taejon, 305-350, ROK
{jhcheon, chee, csp}@etri.re.kr

Abstract. In this paper, we give some relationship between the nonlinearity of rational functions over $\mathbb{F}_{2^n}$ and the number of points of associated hyperelliptic curve. Using this, we get a lower bound on nonlinearity of rational-typed vector Boolean functions over $\mathbb{F}_{2^n}$. While the previous works give us a lower bound on nonlinearity only for special-typed monomials, our result gives us general bound applicable for all rational fuctions defined over $\mathbb{F}_{2^n}$. As an application of our results, we get a lower bound on nonlinearity of $n \times kn$ S-boxes.

1 Introduction

One of the powerful attack for block ciphers is linear cryptanalysis which was developed by Matsui[5] in 1993. The basic idea of linear cryptanalysis is to find a linear relation among the plain text, cipher text and key bits. Such a relation usually occurs by a low nonlinearity of substitutions in block ciphers.

Nonlinearity for Boolean functions was well-established [9]. However, it is very difficult to analyze nonlinearity for vector Boolean functions, in general. Some results on nonlinearity of vector Boolean functions were found in [2,6,7]. But the results are only concerned with the special types of monomials over $\mathbb{F}_{2^n}$.

In this paper, we derive a novel relationship between the nonlinearity of a rational function over $\mathbb{F}_{2^n}$ and the number of points of hyperelliptic curve over that field. And, using such a relationship we obtain a lower bound on nonlinearity of rational-typed vector Boolean functions over $\mathbb{F}_{2^n}$. Furthermore, we give a lower bound on nonlinearity of S-box constructed by concatenating two or more S-boxes over $\mathbb{F}_{2^n}$. Similar method has been used in the CAST algorithm [1], in which 8×32 S-boxes were constructed by selecting 32 bent Boolean functions over $\mathbb{F}_{2^8}$. In that case, their S-boxes has been believed to be highly nonlinear, but nobody gave lower bound on the nonlinearity. It has been known that it might be very difficult to prove the lower bound on the nonlinearity of such S-boxes [8].

2 Preliminaries

2.1 Nonlinearity

We consider a vector Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Let $b = (b_1, b_2, \cdots, b_n)$ be a nonzero element of $\mathbb{F}_{2^n}$. We denote by $b \cdot F$ the Boolean function which is the

J. Stern (Ed.): EUROCRYPT'99, LNCS 1592, pp. 286–294, 1999.
© Springer-Verlag Berlin Heidelberg 1999

linear combination $b_1f_1 + b_2f_2 + \cdots + b_nf_n$ of the coordinate Boolean functions $f_1, f_2, \cdots, f_n$ of F.

Definition 1. *The nonlinearity of F, $\mathcal{N}(F)$, is defined as*

$$\mathcal{N}(F) = \min_{b \neq 0} \min_{A \in \Gamma} \#\{x : A(x) \neq b \cdot F(x)\},$$

where Γ is the set of all affine functions over $\mathbb{F}_{2^n}$.

If we define $\mathcal{L}(F, a, b) = \#\{x : a \cdot x = b \cdot F(x)\}$, then we have

$$\mathcal{N}(F) = 2^{n-1} - \max_{b \neq 0} \max_{a} |2^{n-1} - \mathcal{L}(F, a, b)|. \tag{1}$$

Observe that nonlinearity of arbitrary vector Boolean functions is upper-bounded as

$$\mathcal{N}(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

and the equality holds for only bent functions.

The nonlinearity for special types of F, usually monomials, are investigated by Nyberg [7].

Theorem 2.

1. *Let $F(x) = x^{2^k+1}$.*
   (a) If n/s is odd for $s = \gcd(n, k)$, then

$$\mathcal{N}(F) = 2^{n-1} - 2^{(n+s)/2-1}. \tag{2}$$

   (b) If n is odd and $\gcd(n, k) = 1$, then

$$\mathcal{N}(F^{-1}) = 2^{n-1} - 2^{(n-1)/2}. \tag{3}$$

2. *For $F(x) = x^{-1}$,*

$$\mathcal{N}(F) \geq 2^{n-1} - 2^{n/2}. \tag{4}$$

2.2 Hyperelliptic Curves

In this section, we introduce a hyperelliptic curve and the Weil theorem which have important roles in proving our main theorem. A hyperelliptic curve C over $\mathbb{F}_{2^n}$ is an equation of the form

$$C : y^2 + h(x)y = f(x), \tag{5}$$

where $f(x), h(x) \in \mathbb{F}_{2^n}[x]$ with $2 \deg h(x) + 1 \leq \deg f(x)$, and there are no solutions x, y in the algebraic closure of $\mathbb{F}_{2^n}$, which simultaneously satisfy the equation $y^2 + h(x)y = f(x)$ and the partial derivative equations $2y + h(x) = 0$ and $h'(x)y - f'(x) = 0$. When a curve C has no solutions which satisfies the three equations, we say that C is nonsingular. Otherwise, we say that C is sigular.

We define the set of $\mathbb{F}_{2^n}$-rational points on C, denoted $C(\mathbb{F}_{2^n})$, the set of all points $(x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ that satisfies the equation (5) of the curve C, together with a special point at infinity, denoted O.

For the number $\#C(\mathbb{F}_{2^n})$ of the $\mathbb{F}_{2^n}$-rational points on C, we have the following nontrivial bound [4].

Theorem 3 (Weil). *For any hyperelliptic curve C over $\mathbb{F}_{2^n}$, we have*

$$|\#C(\mathbb{F}_{2^n}) - 2^n - 1| \leq 2g\sqrt{2^n}, \tag{6}$$

where g is the genus of the hyperelliptic curve C.

By the Riemann-Hurwitz formula, we have $g = \lfloor \frac{d-1}{2} \rfloor$ for the degree d of f(See [4, p332]). When a curve given by the equation (5) is singular, the theorem does not hold. In this case, we have the following, using the theory of desigularization of algebraic curves(See [4, p.358]).

$$|\#C(\mathbb{F}_{2^n}) - 2^n - 1| \leq 2g\sqrt{2^n} - g + \frac{(d-1)(d-3)}{2}, \tag{7}$$

where g is the genus of the singular curve C and d is the degree of f. Since the genus g is less than $\lfloor \frac{d-1}{2} \rfloor$, we can get the same inequality for a singular curve under some condition.

Corollary 4. *Let C be a curve given by the irrducible equation $y^2 + h(x)y = f(x)$, which satisfies $\deg f \geq \max\{2\deg h + 1, 3\}$. Assume that C is nonsingular or $d = \deg f \leq 2^{n/4+1} + 2$. Then we have*

$$|\#C(\mathbb{F}_{2^n}) - 2^n - 1| \leq 2\lfloor \frac{d-1}{2} \rfloor \sqrt{2^n}. \tag{8}$$

Proof. If C is nonsingular, we have $g = \lfloor \frac{d-1}{2} \rfloor$. Hence the corollary is proved. If C is singular, we have $g \leq \lfloor \frac{d-1}{2} \rfloor - 1$ so that

$$|\#C(\mathbb{F}_{2^n}) - 2^n - 1| \leq (2\sqrt{2^n} - 1)(\lfloor \frac{d-1}{2} \rfloor - 1) + \frac{(d-1)(d-3)}{2}.$$

The right-hand side is less than or equal to $2\lfloor \frac{d-1}{2} \rfloor \sqrt{2^n}$ if $d^2 - 5d + 7 \leq 4\sqrt{2^n}$. Hence the corollary follows for $3 \leq d \leq 2^{n/4+1} + 2$.

3 Nonlinearity of Rational Functions over $\mathbb{F}_{2^n}$

In this section, we get a lower bound on nonlinearity of rational functions over a finite field, using the bound on the numbers of points of hyperelliptic curves over that field. We consider a rational function of the form $F(x) = P(x)/Q^2(x)$ for $P(x), Q(x) \in \mathbb{F}_{2^n}[x]$ where we may define $F(\alpha)$ to be any elements of $\mathbb{F}_{2^n}$ for a root α of $Q(x)$.

First, we introduce a lemma. We donote by $Tr(\cdot)$, an absolute trace mapping [3].

Lemma 5. *The following polynomial equation of one variable x*

$$x^2 + ax + b = 0, \quad a \neq 0, \quad b \in \mathbb{F}_{2^n} \tag{9}$$

is reducible over $\mathbb{F}_{2^n}$ if and only if $Tr(\frac{b}{a^2}) = 0$.

Proof. If we replace by ax, x of the equation (5) and divide the equation by a^2, we get $x^2+x+b/a^2=0$. Hence $x^2+ax+b=0$ is reducible over $\mathbb{F}_{2^n}$ if and only if $x^2-x=b/a^2$ has a root in $\mathbb{F}_{2^n}$. By Hilbert theorem 90 [3], it is equivalent to $Tr(b/a^2)=0$.

By using the above lemma, we can derive the following theorem.

Theorem 6. *Let $P(x), Q(x), G(x) \in \mathbb{F}_{2^n}[x]$, $F(x)=P(x)/Q^2(x)$ where $G(x)$ is a permutation. Suppose that $C_{a,b}: y^2+Q(x)y = aQ^2(x)G(x)+bP(x)$ is nonsingular for each $a,b \neq 0$ in $\mathbb{F}_{2^n}$, or $d=\max\{2\deg Q+\deg G, \deg P\} \leq (2^{n/2+2}-2)^{1/2}+2$. If $Q(x)$ has r distinct roots in $\mathbb{F}_{2^n}$ and $\gcd(P(x),Q(x))$ has s distinct roots in $\mathbb{F}_{2^n}$, then the nonlinearity of $F\circ G^{-1}$ is lower-bounded as follows :*

$$\mathcal{N}(F\circ G^{-1}) \geq 2^{n-1} - \lfloor\frac{d-1}{2}\rfloor 2^{n/2} - r + \frac{s}{2}.$$

Proof. Choose a basis B of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and take its dual basis $\hat{B}$. Represent binary vectors in $\mathbb{F}_{2^n}$, a and b by the basis B, and $G(x)$ and $F(x)$ by its dual basis $\hat{B}$. Then we have

$$a\cdot G(x) = Tr(aG(x)), \quad b\cdot F(x) = Tr(bF(x)).$$

Hence

$$\begin{aligned}\mathcal{L}(F\circ G^{-1}, a, b) &= \#\{x | a\cdot x = b\cdot F(G^{-1}(x))\}\\ &= \#\{x | Tr(aG(x)) = Tr(bF(x))\}\\ &= \#\{x | Tr(aG(x)+bF(x)) = 0\}\end{aligned}$$

Let $\alpha_1, \alpha_2, \cdots, \alpha_r$ be r distinct roots of $Q(x)$. If $\alpha \neq \alpha_i$ for all i, $C_{a,b}$ has two distinct points whose x-coordinate is α, whenever the equation of y, $y^2+Q(\alpha)y-(aQ^2(\alpha)G(\alpha)+bP(\alpha))$, is reducible. Also, $C_{a,b}$ has one point whose x-coordinate is α_i, whenever the equation of y, $y^2-bP(\alpha_i)$, is reducible. Considering the infinity point O, we have

$$\begin{aligned}&\#C_{a,b}(\mathbb{F}_{2^n}) - 1\\ &= 2\cdot\#\{x | Tr(\frac{aQ^2(x)G(x)+bP(x)}{Q(x)^2}) = 0, Q(x)\neq 0\} + \sum_i \#\{y | y^2 = bP(\alpha_i)\}\\ &= 2\cdot\#\{x | Tr(aG(x)) = Tr(bF(x)), Q(x)\neq 0\} + \sum_i \#\{y | y^2 = bP(\alpha_i)\} \qquad (10)\\ &= 2\mathcal{L}(F\circ G^{-1}, a, b) - 2\#\{i | Tr(aG(\alpha_i)) = Tr(bF(\alpha_i))\} + \sum_i \#\{y | y^2 = bP(\alpha_i)\}.\end{aligned}$$

The first equality follows from lemma 5. Observe that all curves $C_{a,b}$ for $a,b\neq 0$ satisfy the assumption of Corollary 4 and the degree of the equation $C_{a,b}$ at x is less than or equal to d. Hence we have

$$|\#C_{a,b}(\mathbb{F}_{2^n}) - 2^n - 1| \leq 2\lfloor\frac{d-1}{2}\rfloor\sqrt{2^n}. \qquad (11)$$

Combining it with the identity (10), we have

$$|2^{n-1} - \mathcal{L}(F \circ G^{-1}, a, b)|$$
$$\leq \lfloor \frac{d-1}{2} \rfloor \sqrt{2^n} + |\#\{i | Tr(aG(\alpha_i)) = Tr(bF(\alpha_i))\} - \frac{1}{2} \sum_i \#\{y | y^2 = bP(\alpha_i)\}|.$$

If we take the maximum through all $a, b \neq 0 \in \mathbb{F}_{2^n}$, we have

$$\max_{a,b \neq 0} |2^{n-1} - \mathcal{L}(F \circ G^{-1}, a, b)| \leq \lfloor \frac{d-1}{2} \rfloor \sqrt{2^n} + r - \frac{s}{2}.$$

Hence we have

$$\mathcal{N}(F \circ G^{-1}) \geq 2^{n-1} - \lfloor \frac{d-1}{2} \rfloor 2^{n/2} - r + \frac{s}{2}.$$

Observe that $C(F, a, b)$ is singular if and only if $Q(x) = 0$, $Q'(x)y = bP'(x)$ and $y^2 = bP(x)$ has a common solution. Hence $C(F, a, b)$ is non-singluar for any nonzero $b \in \mathbb{F}_{2^n}$ if $F(x)$ satisfies the following condition:

For any root of $Q(x) = 0$ in the algebraic closure of $\mathbb{F}_{2^n}$,

$$(\frac{Q'(\alpha)}{P'(\alpha)})^2 P(\alpha) \notin \mathbb{F}_{2^n}^*. \tag{12}$$

If we use Theorem 6, we can obtain the following useful results.

Corollary 7.

1. *For any polynomial $F(x) \in \mathbb{F}_{2^n}[x]$ of degree $d \geq 3$,*

$$\mathcal{N}(F) \geq 2^{n-1} - \lfloor \frac{d-1}{2} \rfloor 2^{n/2}.$$

2. *For any polynomial $H(x) \in \mathbb{F}_{2^n}[x]$ of degree m and a positive integer k, $F(x) = \frac{H(x)}{x^{2k-1}}$ has a lower bound on its nonlinearity as follows:*

$$\mathcal{N}(F) \geq 2^{n-1} - \lfloor \frac{d-1}{2} \rfloor 2^{n/2} - \frac{1}{2},$$

where $d = \max\{2k+1, m+1\}$.

Proof. 1. We take $G(x) = x$, $Q(x) = 1$ and $P(x) = F(x)$ in Theorem 6. Then a curve $C_{a,b} : y^2 + y = ax + bF(x)$ is irreducible and nonsingular for each $a, b \neq 0$. Since the degree of each curve $C_{a,b}$ at x is d, we have the above assertion.

2. We take $G(x) = x$, $Q(x) = x^k$ and $P(x) = xH(x)$ in Theorem 6. Then a curve $C_{a,b} : y^2 + x^k y = ax^{2k+1} + bxH(x)$ is irreducible and nonsingular for each $a, b \neq 0$. If we take $d = \max\{2k+1, m+1\}$, the degree of each curve $C_{a,b}$ is less than or equal to d, which completes the proof.

We can extend the above corollary to the composite function cases.

Corollary 8. *Assume that e, f be integers satisfying $ef \equiv 1 \bmod (2^n - 1)$.*

1. *For any polynomial $F(x) \in \mathbb{F}_{2^n}[x]$ of degree $m \geq 3$,*
$$\mathcal{N}(F(x^f)) \geq 2^{n-1} - \lfloor \frac{d-1}{2} \rfloor 2^{n/2},$$
where $d = \max\{e, m\}$.
2. *For any polynomial $H(x) \in \mathbb{F}_{2^n}[x]$ of degree m and a positive integer k, let $F(x) = \frac{H(x)}{x^{2k-1}}$.*
$$\mathcal{N}(F(x^f)) \geq 2^{n-1} - \lfloor \frac{d-1}{2} \rfloor 2^{n/2} - \frac{1}{2},$$
where $d = \max\{2k + e, m + 1\}$.

Proof. 1. Take $G(x) = x^e$, $Q(x) = 1$ and $P(x) = F(x)$ in Theorem 6. Then for a curve $C_{a,b} : y^2 + y = ax^e + bF(x)$ the similar assertions as the proof of Corollary 7 hold.

2. Take $G(x) = x^e$, $Q(x) = x^k$ and $P(x) = xH(x)$ in Theorem 6. Then for a curve $C_{a,b} : y^2 + x^k y = ax^{2k+e} + bxH(x)$ the similar assertions as the proof of Corollary 7 hold.

By applying Corollary 7, we get some useful results. See the example.

Example 9. 1. For $F(x) = x^3 + x^5 + x^6 \in \mathbb{F}_{2^n}[x]$,
$$\mathcal{N}(F) \geq 2^{n-1} - 2^{n/2+1}.$$

2. For $F(x) = x^{-1} + x^3 \in \mathbb{F}_{2^n}[x]$,
$$\mathcal{N}(F) \geq 2^{n-1} - 2^{n/2+1} - \frac{1}{2}.$$
Furthermore we can get rid of the last term '1/2' if n is odd.

3. For $F(x) = x^{-3} + x^{-1} \in \mathbb{F}_{2^n}[x]$,
$$\mathcal{N}(F) \geq 2^{n-1} - 2^{n/2+1} - \frac{1}{2}.$$
Furthermore we can get rid of the last term '1/2' if n is even.

If we apply Corollary 8, we can obtain lower bounds on nonlinearity of some monomials whose nonlinearity has not analyzed theoretically yet.

Example 10. Consider $\mathbb{F}_{2^7}$. Let $F(x) = x^3$ and $G(x) = (x^5)^{-1} = x^{51}$. Then we have $F \circ G^{-1}(x) = x^{28}$. By the above statement, we have
$$\mathcal{N}(x^{28}) \geq 2^{n-1} - 2^{n/2+1}.$$
Since nonlinearity preserves under composition with linear functions like x^2, x^7 has the same nonlinearity with $(x^7)^4$. Hence we have
$$\mathcal{N}(x^7) \geq 2^{n-1} - 2^{n/2+1}.$$

We can apply Theorem 6 directly to get a lower bound on nonlinearity of some rational functions,

Example 11. 1. For any irreducible polynomial $H(x)$ of degree d, we have

$$\mathcal{N}(1/H) \geq 2^{n-1} - d \cdot 2^{n/2}.$$

2. For $F(x) = x^{-3}(x-1)^{-1}$(we assume $F(0) = F(1) = 0$),

$$\mathcal{N}(F) \geq 2^{n-1} - 3 \cdot 2^{n/2} - 1.$$

Table 1 shows the tightness of our lower bound on nonlinearity. The third columnn shows the lower bound obtained by Theorem 6 and the fourth column shows the exact value of nonlinearity calculated by computational experiment. Note that S-boxes in Table 1 may not be a permutation. In order to apply them for block cipher, the other properties such as differential probability should be investigated.

Table 1. Lower bound on Nonlinearity and its Exact Value

Function	n	Our Lower Bound	Exact Value
$x^3 + x^5 + x^6$	7	48	48
	8	96	96
$x^{-1} + x^3$	7	41	46
	8	96	100
$x^{-3} + x^{-1}$	7	41	46
	8	96	97

4 Nonlinearity of $n \times kn$ S-boxes

In this section. we derive nonlinearity of $n \times kn$ S-box constructed by concatenating k $n \times n$ S-boxes over $\mathbb{F}_{2^n}$. At first, we present a proposition to relate nonlinearity of $n \times kn$ S-box to that of $n \times n$ S-box.

Proposition 12. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^{kn}}$ be a vector Boolean fuctions with $F = (F_1, F_2, \cdots, F_k)$ for $F_i : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Then we have*

$$\mathcal{N}(F) = \min_{(c_1,c_2,\cdots,c_k) \in \mathbb{F}^*_{2^{kn}}} \mathcal{N}(c_1F_1 + c_2F_2 + \cdots + c_kF_k),$$

where the sum and product are the field operations in $\mathbb{F}_{2^{kn}}$.

Proof. Choose a basis B of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and take its dual basis $\hat{B}$. Let us represent by the basis B the left sides of all inner products and by its dual basis $\hat{B}$ their right sides. For any nonzero $b = (c_1, c_2, \cdots, c_k)$ with $c_i \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned}\mathcal{L}(F, a, b) &= \#\{x | a \cdot x = b \cdot F(x)\} \\ &= \#\{x | Tr(ax + bF(x)) = 0\} \\ &= \#\{x | Tr(ax + c_1F_1(x) + \cdots + c_kF_k(x)) = 0\} \\ &= \mathcal{L}(c_1F_1 + \cdots + c_kF_k, a, 1).\end{aligned}$$

where 1 is a binary vector representing an identity element by the basis B.

Conversely, for any nonzero $(c_1, c_2, \cdots, c_k) \in \mathbb{F}_{2^{kn}}, c_i \in \mathbb{F}_{2^n}$ and a nonzero $b_0 \in \mathbb{F}_{2^n}$, there exists a nonzero $b \in \mathbb{F}_{2^{kn}}$ such that $\mathcal{L}(c_1F_1 + \cdots + c_kF_k, a, b_0) = \mathcal{L}(F, a, b)$, which completes the proof.

By the above proposition, we can apply Theorem 6 to get a lower bound on nonlinearity of $n \times kn$ S-box. For example, consider an $n \times 2n$ S-box $F = (F_1, F_2)$ where $F_1(x) = x^{-1}$ and $F_2(x) = x^3$ are S-boxes over $\mathbb{F}_{2^n}$. Then

$$\begin{aligned}\mathcal{N}(F) &= \min_{(c_1,c_2)\neq 0} \mathcal{N}(c_1x^{-1} + c_2x^3) \\ &= \min\{\min_{c_i \neq 0} \mathcal{N}(c_1x^{-1} + c_2x^3), \mathcal{N}(x^{-1}), \mathcal{N}(x^3)\} \\ &\geq 2^{n-1} - 2^{n/2+1} + \frac{1}{2}.\end{aligned}$$

The first equality follows from Proposition 12 and the last inequality follows from Corollary 7.

Similarly, we can get lower bounds on nonlinearity of various n-by-kn boxes. We present some of them in Table 2. The second column shows a lower bound of nonlinearity of the S-boxes in the first column for even or odd n. The third and fourth column shows the exact value of nonlinearity calculated by computational experiment.

In Table 2, every rational function such as x^{-1} and x^3 is a vector Boolean function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Note that all functions are permutations for odd n, but only x^{-1} and x^7 are permutations for $n = 8$. If we combine our result with Theorem 17 in [8], we can also construct highly nonlinear $kn \times kn$ S-boxes.

Acknowledgement
We would like to thank Sang Geun Hahn for his helpful comments. We are especially grateful to Sangjoon Park who pointed us to the problem of relating hyperelliptic curves to nonlinearity of Boolean functions.

References

1. C. Adams and S. E. Tavares, "Designing S-boxes for Ciphers Resistant to Differential Cryptanalysis," Proc. of SPRC'93, 1993.

Table 2. Lower Bounds of Nonlinearity of n-by-kn S-boxes

S-box	Lower Bound of Nonlinearity	$n = 7$	$n = 8$
(x^{-1}, x^3)	$2^{n-1} - 2^{n/2+1} - \frac{1}{2}$	41	96
(x^{-1}, x^{-3})	$2^{n-1} - 2^{n/2+1} - \frac{1}{2}$	41	96
(x^3, x^5)	$2^{n-1} - 2^{n/2+1}$	42	96
(x^{-3}, x^{-5})	$2^{n-1} - 3 \cdot 2^{n/2} - \frac{1}{2}$	30	80
(x^{-3}, x^{-1}, x^3)	$2^{n-1} - 3 \cdot 2^{n/2} - \frac{1}{2}$	30	80
(x^{-1}, x^3, x^5)	$2^{n-1} - 3 \cdot 2^{n/2} - \frac{1}{2}$	30	80
(x^3, x^5, x^7)	$2^{n-1} - 3 \cdot 2^{n/2}$	31	80
$(x^{-3}, x^{-1}, x^3, x^5)$	$2^{n-1} - 4 \cdot 2^{n/2} - \frac{1}{2}$	19	64
(x^{-1}, x^3, x^5, x^7)	$2^{n-1} - 4 \cdot 2^{n/2} - \frac{1}{2}$	19	64
(x^3, x^5, x^7, x^9)	$2^{n-1} - 4 \cdot 2^{n/2}$	19	64

2. T. Beth and D. Ding, "On Almost Perfect Nonlinear Permutations," Proc. of Eurocrypt'93, pp. 65 – 76, Springer-Verlag, 1994.
3. R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1986.
4. D. Lorenzini, *An Invitation to Arithmetic Geometry*, American Mathematical Society, 1996.
5. M. Matsui, "Linear Cryptanalysis Method for DES cipher," Proc. of Eurocrypt'93, pp.386 – 397, Springer-Verlag, 1993.
6. K. Nyberg, "On the Construction of Highly Nonlinear Permutation," Proc. of Eurocrypt'92, pp. 92 – 98, Springer-Verlag, 1993.
7. K. Nyberg, "Differentially Uniform Mappings for Cryptography," Proc. of Eurocrypt'93, pp. 55 – 64, Springer-Verlag, 1994.
8. K. Nyberg, "S-Boxes and Round Functions with Controllable Linearity and Differential Uniformity," Proc. of the Second Fast Software Encryption, pp. 111 – 130, Springer-Verlag, 1994.
9. J. Seberry, X. -M. Zhang and Y. Zheng, "Nonlinearly Balanced Functions and Their Propagation Characteristics," Proc. of Crypto'93, pp. 49 – 60, Springer-Verlag, 1993.
10. J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1992.