Applied Mathematics & Information Sciences
An International Journal

Constructions of Cryptographically Significant Boolean Permutations

Fengrong Zhang[1]*, Yupu Hu*[1]*, Min Xie*[1]*, Juntao Gao*[1,3] *and Qichun Wang*[2]

[1] Key laboratory of computer network and information security, Ministry of EducationXidian University, Xi'an 710071, PR China;
[2] Key laboratory of intelligent information Processing, School of Computer Science, Fudan University, Shanghai 200433, PR China
[3] State key laboratory of information security, Graduate University of Chinese Academy of Sciences, Beijing 100049, PR China

Received: Received December 22, 2010; Revised July 11, 2011; Accepted July 16, 2011
Published online: 1 January 2012

Abstract: In this paper, we focus on a class of Boolean permutations of an optimal algebraic degree. Firstly, we construct a class of Boolean permutations. We put forward a method to propose the inverse of a given Boolean permutation. It is shown that a Boolean permutation has an optimal algebraic degree if and only if its inverse has an optimal algebraic degree. Secondly, we present the inverse of the constructed Boolean permutation, and show the inverse permutation has the largest algebraic degree. Finally, we show that the constructed Boolean permutations can achieve optimum algebraic degree by selecting an appropriate initial vector and illustrate it with examples.

Keywords: Steam ciphers, Block ciphers, Boolean functions, Boolean permutations, Algebraic degree.

1. Introduction

Let n and m be two positive integers and F_2^n be the n-dimensional vector space over F_2. A Boolean function on n variables is an F_2-valued function on F_2^n. We call the functions, from F_2^n to F_2^m, (n, m)-functions. Such function F being given, the Boolean functions $f_1, \dots, f_m$ defined, at every $x \in F_2^n$, by $F(x) = (f_1, \dots, f_m)$, are called the coordinate functions of F. Obviously, these functions include the (single-output) Boolean functions which correspond to the case $m = 1$. For $n = m$, if $c \cdot F(x)$ is a balanced Boolean function for any $c \neq \mathbf{0} \in F_2^n$, then $F(x)$ is called a Boolean permutation on n variables.

Boolean permutations are used in various different areas and play an important role in the security of cryptosystems. Their most prominent cryptographic applications include the analysis and design of S-boxes in block ciphers [4]. For example, the S-box used in the design of the Advanced Encryption Standard (AES) is a Boolean permutation on 8 variables. The Boolean permutations used in a block cipher should possess a low differential uniformity, a high algebraic degree and a high nonlinearity to resist high order differential attacks [13] and linear attacks [16]. Recently, algebraic attacks on block ciphers, which are based on defining and solving systems of multivariate equations in variables corresponding to the bits of a secret key, have been introduced in [10].

All the criteria mentioned above cannot be satisfied simultaneously. For odd n, the most notable example is Almost Bent (AB) permutations [4]. Achieving the highest nonlinearity $2^{n-1} - 2^{(n-1)/2}$ (n odd) and the best differential uniformity, AB permutations permit to resist linear attacks and differential attacks in the best possible way. Therefore, AB functions have received much attention in cryptographic literature [4,14,12,5]. Unfortunately, the algebraic degrees of AB permutations on F_2^n are less than or equal to $(n+1)/2$ [7].

In order to obtain the Boolean permutations of the largest algebraic degree, a methodology was developed to construct Boolean permutation by Zhang et al. [20]. But there is only one nonlinear term (i.e., a monomial with degree $n-1$) in any one coordinate Boolean function and the number of the Boolean permutations is very limited. Recently, a class of Boolean permutations of an optimal algebraic degree were presented in [11,9]. But we can not easily propose the inverse of these permutations in [11,9].

In this paper, we present a class of Boolean permutations of optimal algebraic degree on F_2^n. Further, we pro-

[*] Corresponding author: e-mail: zhfl203@163.com

pose the inverse of the constructed Boolean permutations. We find that the ith ($1 \le i \le k$) coordinate function of the inverse of a constructed Boolean permutation is the function constructed in [19]. That is to say, the inverses are the permutation presented in [11,9]. Finally, it is shown that the Boolean permutations can achieve optimum algebraic degree by selecting an appropriate initial vector $b_1 \in F_2^k$.

2. Preliminaries

In the remainder of this article, we denote the additions and sums over the F_2 finite field by $\oplus$ and $\bigoplus$. Let F_2^n be the n-dimensional vector space over F_2. A Boolean function on n variables is an F_2-valued function on F_2^n. Let B_n be the set of all n-variable Boolean functions from F_2^n to F_2. Any Boolean function has a unique representation as a multivariate polynomial over F_2, called the *algebraic normal form*(ANF):

$$f(x_1,\ldots,x_n)=\bigoplus_{I\subseteq\{1,2,\ldots,n\}} a_I \prod_{l\in I} x_l$$

where $a_I \in F_2$, and the terms $\prod_{l\in I} x_l$ are called monomials. The *algebraic degree* $\deg(f)$ of a Boolean function f equals the maximum degree of those monomials whose coefficients are nonzero in its ANF. A Boolean function is affine if it has degree at most 1. The set of all n-variable affine functions is denoted by A_n. An n-variable affine function with constant term 0 is called a linear function, and is denoted by $\omega \cdot x = \omega_1 x_1 \oplus \ldots \oplus \omega_n x_n$ where $\omega = (\omega_1,\ldots,\omega_n) \in F_2^n, x = (x_1,\ldots,x_n) \in F_2^n$.

Definition 1. *Let $\phi(y) = (\phi_1(y), \phi_2(y), \ldots, \phi_m(y))$ be an (n,m)-function. Then the algebraic degree of $\phi(y)$ is defined as*

$$\deg(\phi(y)) = \min\{\deg(v\cdot\phi(y)) | v \in F_2^m, v \neq \mathbf{0}\}.$$

In this paper, we say an n-variable Boolean permutation has optimal algebraic degree if its algebraic degree equals $n-1$.

The basic representation of a Boolean function $f(x_1,\ldots,x_n)$ is by the output column of its truth table, i.e., a binary string of length 2^n,

$$[f(0,\ldots,0,0,0), f(0,\ldots,0,0,1),\ldots,f(1,\ldots,1,1,1)].$$

The *Hamming weight* wt(f) of a Boolean function $f \in B_n$ is the weight of the above binary string. We say $f \in B_n$ is *balanced* if its Hamming weight equals 2^{n-1}. The *Hamming distance* d(f,g) between two Boolean functions f and g is the Hamming weight of their difference $f \oplus g$.

The *nonlinearity* of $f \in B_n$ is its distance from the set of all n-variable affine functions, i.e.,

$$N_f = \min_{g\in A_n}(d(f,g)).$$

Boolean functions used in cryptographic systems must have high nonlinearity to withstand linear and correlation attacks [1].

Definition 2.[18] *A Boolean function $f \in B_n$ is called Bent function on n variables if its nonlinearity equals $2^{n-1} - 2^{n/2-1}$, where n is even.*

There is a class of Bent functions which is called original Maiorana-McFarland's (M-M) class of Bent functions [18]. The original M-M class of Bent functions is the set of all the (Bent) Boolean functions on $F_2^{2k} = \{(x,y), x,y \in F_2^k\}$ of the form:

$$f(y,x) = \phi(y)\cdot x \oplus g(y)$$

where $\phi(y) = (\phi_1(y),\ldots,\phi_k(y))$ is any permutation on F_2^k and $g(y)$ is any Boolean function on F_2^k. In 2004, Carlet [2] indicated that there existed a one-to-one correspondence between Boolean permutations and the original M-M class of Bent functions.

Lemma 1.[2]
Let $x \in F_2^k, y \in F_2^k$, $\phi_i(y)$ with $1 \le i \le k$ be a k-variable Boolean function, and $g(y)$ be any k-variable Boolean function. A $2k$-variable Boolean function $f(y,x) = \phi(y)\cdot x \oplus g(y)$ is a Bent function if and only if

$$\phi(y) = (\phi_1(y), \phi_2(y), \ldots, \phi_k(y))$$

is a Boolean permutation.

Moreover, by the representation of polynomial basis [17], we present a corollary.

Corollary 1.
Let $x,y \in F_2^k, \tau \in F_2^k$. A $2k$-variable Boolean function

$$f(y,x) = \bigoplus_{\tau\in F_2^k} \delta_\tau(y) a_\tau(x) \tag{1}$$

is a Bent function defined as Lemma 1 if and only if $a_\tau(x) = \phi(\tau)\cdot x \oplus g(\tau)$, where both $\phi(y)$ and $g(y)$ are defined as Lemma 1.

Let F_{2^n} denote a finite field with 2^n elements. It can be viewed as an n-dimensional vector space over its subfield F_2. Every function $f : F_{2^n} \to F_{2^n}$ can be uniquely represented as a polynomial $\bigoplus_{i=0}^{2^n-1} a_i x^i$ (called its univariate representation), where $a_i \in F_{2^n}$, and f is a Boolean function if and only if $\bigoplus_{i=0}^{2^n-1} a_i x^i \in F_2$ for $x \in F_{2^n}$. Given a basis $(\beta_1, \beta_2, \ldots, \beta_n)$, we can identify any element $x = \bigoplus_{i=1}^{n} x_1\beta_i \in F_{2^n}$ with the n-tuple of its coordinate $(x_1, x_2, \ldots, x_n) \in F_2^n$.

For $f \in B_n$, we define $AN(f) = \{g \in B_n | fg = 0\}$. Any function $g \in AN(f)$ is called an annihilator of f. The *algebraic immunity* (AI) of f is the minimum degree of all the nonzero annihilators of f and of all those of $f \oplus 1$. We denote it by AI(f).

Two Boolean functions f and g are said to be affine equivalent if there exist an invertible $n \times n$ binary matrix D and a vector $b \in F_2^n$ such that $g(x) = f(Dx \oplus b)$. Clearly, algebraic degree, algebraic immunity and nonlinearity are all affine invariant [3].

In the sequel, we recall some notation from [19]. Let $p(z) = z^n + c_{n-1}z^{n-1} + \ldots + c_1 z + 1$ be a primitive polynomial over the field F_2. The companion matrix D of it is

$$D = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & c_1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix}.$$

Given any initial value b_1, we can define an iterative sequence $B = \{b_i | 1 \le i \le 2^n - 1\}$ as follows:

$$\begin{cases} b_1 \in F_2^n; \\ b_{i+1} = Db_i, \ 1 \le i < 2^n - 1. \end{cases}$$

Clearly, $B = \{\mathbf{0}\}$ if and only if $b_1 = \mathbf{0}$.

In [19], Wang et al. showed that $B = F_2^n - \{\mathbf{0}\}$ if $b_1 \neq \mathbf{0}$. Given any $b_1 \neq \mathbf{0}$, we define a multiplication ”$*$” on the set B as follows:

$$D^i b_1 * D^j b_1 = D^{i+j} b_1.$$

Then B will be a cyclic group of order $2^n - 1$ and Db_1 is its generator. Moreover, we know that $D^{2^l} b_1$ is also its generator since $\gcd(2^n - 1, 2^l) = 1$ where $l = 1, 2, \ldots, n-1$. Thus, $B \cup \{\mathbf{0}\}$ is a finite field of order 2^n and B is its multiplicative group. Clearly, its additive identity is $\mathbf{0}$ and its multiplicative identity is b_1.

3. Main Results

From now on, we always assume that $\delta_\tau(y) = \prod_{i=1}^{k} (y_i \oplus \tau_i \oplus 1)$, where $y, \tau \in F_2^k$.

Definition 3. *An (k,k)-function $\phi(y) = (\phi_1(y), \phi_2(y), \ldots, \phi_k(y))$ is called a* Boolean permutation *if the number of solutions $y \in F_2^k$ of $\phi(y) = \boldsymbol{a}$ is exactly 1 for any $\boldsymbol{a} \in F_2^k$.*

Lemma 2.*[19] Let $x \in F_2^n$. Let $1_f = \{x | f(x) = 1\} = \{(b_{i1}, \ldots, b_{in}) \in F_2^n | 1 \le i \le wt(f)\}$. Then f can be represented as follows:*

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{i=1}^{wt(f)} \prod_{j=1}^{n} (x_j \oplus 1 \oplus b_{ij}).$$

Obviously, $\deg(f) < n$ *if and only if* $wt(f)$ *is even. Moreover,* $\deg(f) = n - 1$ *if and only if* $wt(f)$ *is even and*

$$\bigoplus_{i=1}^{wt(f)} (b_{i1}, \ldots, b_{in}) \neq 0.$$

The above fact will play an important role in proving Boolean functions of an optimum algebraic degree.

Since a Boolean permutation is a bijective mapping, the inverse of a Boolean permutation is a Boolean permutation as well. In what follows, we put forward a method to present the inverse of a given Boolean permutation.

Theorem 1. *Let $x, y \in F_2^k$ and $\phi(y) = (\phi_1(y), \phi_2(y), \cdots, \phi_k(y))$ be a Boolean permutation. Then*

$$f'(y, x) = \bigoplus_{\tau \in F_2^k} \delta_{\phi(\tau)}(y)\,(\tau \cdot x) \qquad (2)$$

is a M-M Bent function. Furthermore,

$$\psi'(y) = \left(f'(y, \mathbf{e}^{(1)}), f'(y, \mathbf{e}^{(2)}), \ldots, f'(y, \mathbf{e}^{(k)})\right) \qquad (3)$$

is the inverse of the Boolean permutation $\phi(y)$, where $\mathbf{e}^{(l)}$ denotes the vector with the lth entry 1 and the others 0.

Proof Clearly, $f'(y, x)$ is a Bent function in that $\phi(y)$ is a Boolean permutation. According to definition of $\psi'(y)$, we have $f'(y, x) = \psi'(y) \cdot x$. Hence, $f'(y, x) = \bigoplus_{\tau \in F_2^k} \delta_{\psi'(y)}(\tau)(\tau \cdot x)$. On the other hand, $\delta_{\phi(\tau)}(y) = \delta_{\phi^{-1}(y)}(\tau)$, then we have $\psi' = \phi^{-1}$ by the uniqueness of the ANF.

Theorem 2. *Let $y \in F_2^k$ and $\phi(y)$ be a Boolean permutation. Let $\phi^{-1}(y)$ be the inverse of $\phi(y)$. Then* $\deg(\phi(y)) = k - 1$ *if and only if* $\deg(\phi^{-1}(y)) = k - 1$.

Proof Since $(\phi^{-1})^{-1}(y) = \phi(y)$, it suffices to show that $\deg(\phi^{-1}(y)) = k - 1$ if $\deg(\phi(y)) = k - 1$.

Let E be a set with 2^{k-1} elements. If $\oplus_{x \in E} x = 0$, then E is a hyperplane and vice versa. According Definition 1 and Lemma 2, we know that the set $1_{v \cdot \phi} = \{y | v \cdot \phi(y) = 1, y \in F_2^n\}$ must not be a hyperplane for any $v \in F_2^n$, where 1_f denote the support set of a function f. However, $H^{(v)} = \{\phi(y) | \phi(y) \cdot v = 1, y \in F_2^n\}$ is a hyperplane for any nonzero vector $v \in F_2^n$. That is to say, $\phi^{-1}(H^{(v)}) = 1_{v \cdot \phi}$ must not be a hyperplane for any $v \in F_2^n$. Again by Lemma 2, the algebraic degree of $\phi^{-1}(y)$ is equal to $k - 1$.

Here, we present a class of Boolean permutations.

Theorem 3. *Let $y \in F_2^k$. Let $\phi(y) = D^{[y]} b_1$ for $y \neq \mathbf{1}$, $\phi(y) = \mathbf{0}$ for $y = \mathbf{1}$ where $b_1 \neq \mathbf{0}$, $[y]$ denotes the decimal expansion of y (i.e., $[(0, \ldots, 0, 1, 1)] = 3$). Then $\phi(y)$ is a Boolean permutation on F_2^k.*

Proof For $b_1 \neq \mathbf{0}$, $B = \{D^i b_1 | i = 0, 1, \ldots, 2^k - 1\} = F_2^k \setminus \{\mathbf{0}\}$. Then, $\phi(y)$ is a Boolean permutation on F_2^k.

By using Theorem 1, we can present the inverse permutation of $\phi(y)$.

Theorem 4.*Let $n = 2k$, $x, y \in F_2^k$, $b_1 \neq \mathbf{0} \in F_2^k$. Then*

$$f'(y, x) = \bigoplus_{\tau \in F_2^k \setminus \{\mathbf{1}\}} \delta_{D^{[\tau]} b_1}(y)(\tau \cdot x) \oplus \delta_{\mathbf{0}}(y)(\mathbf{1} \cdot \mathbf{x}) \quad (4)$$

is a Bent function. Moreover,

$$\psi'(y) = \left(f'(y, \mathbf{e}^{(1)}), f'(y, \mathbf{e}^{(2)}), \ldots, f'(y, \mathbf{e}^{(k)})\right)$$

is a Boolean permutation.

Proof Let $\phi(y)$ be defined as Theorem 3. Then $\phi(y)$ is a Boolean permutation on k variables. Further, according to Theorem 1, we have that $f'(y,x)$ is a bent function on $2k$ variables and $\psi'(y)$ is a permutation on k variables.

Remark. According to Corollary 1, we know that

$$f^{(1)}(y,x) = \bigoplus_{\tau\in F_2^k\setminus\{\mathbf{1}\}} \delta_{D^{[\tau]}b_1}(y)c_\tau(x) \oplus \delta_{\mathbf{0}}(y)c_{\mathbf{1}}(x) \quad (5)$$

is a Bent function, where $c_\tau(x) = (\tau\oplus\mathbf{1})\cdot\mathbf{x}$. Moreover,

$$\psi(y) = \left(f^{(1)}(y,\mathbf{e}^{(1)}), f^{(1)}(y,\mathbf{e}^{(2)}), \ldots, f^{(1)}(y,\mathbf{e}^{(k)})\right)$$

is a Boolean permutation.

Clearly, $\psi(y) = \psi'(y)\oplus\mathbf{1}$, that is, both $\psi(y)$ and $\psi'(y)$ have same algebraic degree and nonlinearity. In addition, we find that $f^{(1)}(y,\mathbf{e}^{(1)})$, which is the function constructed in [19] by Wang and Peng, has a high nonlinearity, an optimal algebraic degree and an optimal immunity. Recently, Carlet [6] showed that the first of the two constructions in [19] is the same as the construction presented in [8]. In [9], Carlet and Feng studied the cryptographic properties of an infinite class of balanced vectorial Boolean functions over finite fields which were introduced by Feng, Liao and Yang [11]. Thus, by the arguments proposed in [6], the Boolean permutation $\psi(y)$ presented in Remark 3 is the same as the vectorial functions in [11,9]. In the following, we show that the Boolean permutation $\psi(y)$ on F_2^k has an optimal algebraic degree from its truth tables.

Lemma 3.*[19] Let $y\in F_2^k$, $h(y)\in B_k$ and $1_h = \{D^ib_1|0\le i<2^{k-1}\}$, where $\mathbf{0}\ne b_1\in F_2^k$. Then $h(y)$ has optimum algebraic immunity $\lceil k/2\rceil$ and algebraic degree $k-1$.*

From Theorem 4 and Lemma 3, we find that $f(y,\mathbf{e}^{(1)})$ may be exactly the function $h(y)$. We consider the properties of $f(y,\mathbf{e}^{(l)})$ where $l=2,3,\ldots,k$.

Definition 4. *Let F_{p^n} be a finite field and a prime characteristic p. Let $\alpha\in F_{p^n}$. The map σ defined by: $\sigma:\alpha\longrightarrow\alpha^p$ is bijective and a homomorphism, and is therefore an automorphism on the field F_{p^n} which fixes the subfield with p elements. It is called the* Frobenius automorphism.

In fact, the σ satisfies

$$\sigma(\alpha+\beta) = (\alpha+\beta)^p = (\alpha)^p+(\beta)^p = \sigma(\alpha)+\sigma(\beta),$$
$$\sigma(\alpha\cdot\beta) = (\alpha\cdot\beta)^p = \sigma(\alpha)\cdot\sigma(\beta).$$

Moreover, $\sigma(1)=1, 1\notin ker(\sigma)$, so $ker(\sigma)=0$, i.e., σ is an injective. Thus, this shows that σ is an *automorphism* on F_{p^n}.

From Definition 4, it is clear that σ^r is also an *automorphism* on F_{p^n} for any $r\in\{1,2,\ldots n-1\}$, where $\sigma^r(\alpha)=\alpha^{p^r}$.

Theorem 5. *Let $f^{(1)}(y,x)\in B_{2k}$ be as in Remark 3. Then $f^{(1)}(y,\mathbf{e}^{(l)})$ has an optimal algebraic immunity $\lceil k/2\rceil$ and algebraic degree $k-1$, where $l=1,2,\ldots,k$.*

Proof From Remark 3, we know

$$1_{f^{(1)}(y,\mathbf{e}^{(l)})} = \{D^ib_1|i\in \bigcup_{t=0,2,4,\ldots,2^l-2}[t2^{k-l},(t+1)2^{k-l}-1]\}$$

where $i\in[t2^{k-l},(t+1)2^{k-l}-1]$ denotes $t2^{k-l}\le i\le(t+1)2^{k-l}-1$, $l=1,2,3,\ldots,k$. For $l=1$, we have that $1_{f^{(1)}(y,\mathbf{e}^{(1)})} = \{D^ib_1|0\le i\le 2^{k-1}-1\}$. Thus, by Lemma 3, the function $f^{(1)}(y,\mathbf{e}^{(1)})$ has an optimal algebraic immunity $\lceil k/2\rceil$ and algebraic degree $k-1$.

Let σ be the Frobenius automorphism on finite field $B\cup 0$. That is to say, $\sigma(D^ib_1)=(D^ib_1)^2$. Since Db_1 is a generator of B and $\gcd(2^r,2^k-1)=1$, $\sigma^r(Db_1)$, denoted by D_rb_1, is also a generator for any $r\in\{1,2,\ldots k-1\}$. Clearly, the support of $f^{(1)}(y,\mathbf{e}^{(l)})$ can be represented as $D_{l-1}b_1$, i.e.,

$$1_{f^{(1)}(y,\mathbf{e}^{(l)})} = \{D_{l-1}^ib_1|0\le i\le 2^{k-1}-1\},$$

where $l=2,3,\ldots,k$.

By the proving process of Lemma 3, the function $f(y,\mathbf{e}^{(l)})$ has an optimal algebraic immunity $\lceil k/2\rceil$ and algebraic degree $k-1$ for any $l\in\{2,\ldots,k\}$. The theorem is proved.

In the following, we show that the Boolean permutation $\phi(y)$ has an optimal algebraic degree $k-1$ by selecting an appropriate b_1.

Lemma 4.*[15] For any finite field F_{p^n} there exists a normal basis of F_{p^n} over its prime subfield that consists of primitive elements of F_{p^n}.*

Theorem 6. *Let $f^{(1)}(y,x)\in B_{2k}$ and the Boolean permutation $\psi(y)$ be as in Remark 3. Then* $\deg(\psi(y)) = k-1$ *if and only if $\{D^{\nu(2^{k-1}-1)mod\ (2^k-1)}b_1, D_{2-1}^{\nu(2^{k-1}-1)mod\ (2^k-1)}b_1, \ldots, D_{k-1}^{\nu(2^{k-1}-1)mod\ (2^k-1)}b_1\}$ is a* normal basis *of $B\cup\{0\}$ over $\{0,b_1\}$, where ν is an integer and $b_1\oplus Db_1 = D^\nu b_1$. Furthermore, there exists at least a vector $b_1\in F_2^k$ such that $\{D^{\nu(2^{k-1}-1)mod\ (2^k-1)}b_1, D_{2-1}^{\nu(2^{k-1}-1)mod\ (2^k-1)}b_1, \ldots, D_{k-1}^{\nu(2^{k-1}-1)mod\ (2^k-1)}b_1\}$ is a* normal basis *of $B\cup\{0\}$ over $\{0,b_1\}$.*

Proof From Theorem 5, we know that $f^{(1)}(y,\mathbf{e}^{(1)})$ has algebraic degree $k-1$. Thus, we have

$$\bigoplus_{i=0}^{2^{k-1}-1} D^ib_1 = (b_1\oplus Db_1)^{2^{k-1}-1}$$
$$= D^{\nu(2^{k-1}-1)mod\ (2^k-1)}b_1 \ne 0,$$

where $0\le\nu\le 2^k-1$ is an integer.

Let σ be also the Frobenius automorphism on finite field $B\cup 0$. By the proving process of Theorem 5, we have $1_{f^{(1)}(y,\mathbf{e}^{(2)})} = \{D_{2-1}^ib_1|0\le i\le 2^{k-1}-1\}$.

Moreover,

$$\begin{aligned}\bigoplus_{i=0}^{2^{k-1}-1} D_{2-1}^{i} b_1 &= \sigma^{2-1}(\bigoplus_{i=0}^{2^{k-1}-1} D^{i} b_1)\\ &= D_{2-1}^{\nu(2^{k-1}-1) mod\ (2^{k}-1)} b_1 \neq 0.\end{aligned}$$

By using the same argument as above, one may show that

$$\begin{aligned}\bigoplus_{i=0}^{2^{k-1}-1} D_{l-1}^{i} b_1 &= \sigma^{l-1}(\bigoplus_{i=0}^{2^{k-1}-1} D^{i} b_1)\\ &= D_{l-1}^{\nu(2^{k-1}-1) mod\ (2^{k}-1)} b_1 \neq 0,\end{aligned}$$

where $l \in \{3, \ldots, k\}$.

According to Definition 3, we know $\deg(\psi(y)) = k-1$ if and only if

$$(D^{\nu(2^{k-1}-1) mod\ (2^{k}-1)} b_1, D_{2-1}^{\nu(2^{k-1}-1) mod\ (2^{k}-1)} b_1, \ldots,\\ D_{k-1}^{\nu(2^{k-1}-1) mod\ (2^{k}-1)} b_1) \cdot v \neq 0,$$

where $v \in F_2^k \setminus \{\mathbf{0}\}$.

Therefore, according to the above equation, we know that the following three conditions are equivalent.

1.$\deg(\psi(y)) = k-1$;
2.$D^{\nu(2^{k-1}-1) mod\ (2^{k}-1)} b_1, D_{2-1}^{\nu(2^{k-1}-1) mod\ (2^{k}-1)} b_1, \ldots, D_{k-1}^{\nu(2^{k-1}-1) mod\ (2^{k}-1)} b_1$ are linearly independent;
3.$\{D^{\nu(2^{k-1}-1) mod\ (2^{k}-1)} b_1, D_{2-1}^{\nu(2^{k-1}-1) mod\ (2^{k}-1)} b_1, \ldots, D_{k-1}^{\nu(2^{k-1}-1) mod\ (2^{k}-1)} b_1\}$ is a *normal basis* of $B \cup \{0\}$ over $\{0, b_1\}$.

Next, we show that there exists a b_1 such that $\{D^{\nu(2^{k-1}-1) mod\ (2^{k}-1)} b_1, D_{2-1}^{\nu(2^{k-1}-1) mod\ (2^{k}-1)} b_1, \ldots, D_{k-1}^{\nu(2^{k-1}-1) mod\ (2^{k}-1)} b_1\}$ is a *normal basis* of $B \cup \{0\}$ over $\{0, b_1\}$.

Let $\mathbf{0} \neq a_0 \in F_2^k, a_{i+1} = Da_i$. Then there exists a positive integer $\nu < 2^k - 1$ such that $a_0 \oplus Da_0 = D^{\nu} a_0 (= a_{\nu})$. Moreover, we have

$$\begin{aligned}&(Da_0 \oplus D^2 a_0)^{2^{k-1}-1}\\ &= (D^{(\nu+1) mod\ (2^{k}-1)} a_0)^{2^{k-1}-1}\\ &= a_{(1+\nu)(2^{k-1}-1) mod\ (2^{k}-1)};\\ &(D^2 a_0 \oplus D^3 a_0)^{2^{k-1}-1}\\ &= (D^{(\nu+2) mod\ (2^{k}-1)} a_0)^{2^{k-1}-1}\\ &= a_{(2+\nu)(2^{k-1}-1) mod\ (2^{k}-1)};\\ &\qquad\vdots\\ &(D^{2^k-3} a_0 \oplus D^{2^k-2} a_0)^{2^{k-1}-1}\\ &= (D^{(\nu+2^k-3) mod\ (2^{k}-1)} a_0)^{2^{k-1}-1}\\ &= a_{(2^k-3+\nu)(2^{k-1}-1) mod\ (2^{k}-1)};\\ &(D^{2^k-2} a_0 \oplus a_0)^{2^{k-1}-1}\\ &= (D^{(\nu+2^k-2) mod\ (2^{k}-1)} a_0)^{2^{k-1}-1}\\ &= a_{(2^k-2+\nu)(2^{k-1}-1) mod\ (2^{k}-1)}.\end{aligned}$$

We have

$$\{a_{(i+\nu) mod\ (2^k-1)} | i = 0, 1, \ldots, 2^k - 2\} = B = F_2^k \setminus \{\mathbf{0}\}.$$

On the other hand, $\gcd(2^{k-1} - 1,\ 2^k - 1) = 1$ in that $\gcd(2^k - 2,\ 2^k - 1) = 1$. Consequently,

$$\begin{aligned}\{a_{(i+\nu)(2^{k-1}-1) mod\ (2^k-1)} | i = 0, \ldots, 2^k - 2\} &= B\\ &= F_2^k \setminus \{\mathbf{0}\}.\end{aligned}$$

According to Lemma 4, there exists a number ρ' such that

$$\{D^{2^0(\nu+\rho')(2^{k-1}-1) mod (2^k-1)} a_0,\\ D^{2^1(\nu+\rho')(2^{k-1}-1) mod (2^k-1)} a_0, \ldots,\\ D^{2^{k-1}(\nu+\rho')(2^{k-1}-1) mod (2^k-1)} a_0\}$$

is a normal basis of $B \cup \{\mathbf{0}\}$ over $\{0, a_0\}$. We set $b_1 = D^{\rho'(2^{k-1}-1) mod (2^k-1)} a_0$. Thus, the above normal basis can be represented as follows:

$$\{D^{2^0\nu(2^{k-1}-1) mod (2^k-1)} b_1, D^{2^1\nu(2^{k-1}-1) mod (2^k-1)} b_1, \ldots,\\ D^{2^{k-1}\nu(2^{k-1}-1) mod (2^k-1)} b_1\}.$$

That is to say, the vectors $D^{2^0\nu(2^{k-1}-1) mod (2^k-1)} b_1$, $D^{2^1\nu(2^{k-1}-1) mod (2^k-1)} b_1, \ldots, D^{2^{k-1}\nu(2^{k-1}-1) mod (2^k-1)} b_1$ are linearly independent. The theorem is proved.

Example 1. Let $n = 2k = 16, x, y \in F_2^8, \mathbf{0} \neq b_1 \in F_2^8$. Denote $(i)_2$ the binary expansion of the integer $i \in [0, 2^k - 1]$. Let $f(y, x) \in B_{16}$ and $\phi(y)$ be as in Remark 3. Clearly, $f(y, \mathbf{e}^{(l)})$ is balanced, has optimum algebraic immunity and optimum algebraic degree where $l = 1, 2, \ldots, 8$. Here, we take $P(z) = z^8 \oplus z^6 \oplus z^5 \oplus z \oplus 1$. From Theorem 6, we know that there exists at least a vector $b_1 \in F_2^8$ such that $\deg(\phi(y)) = 7$. By calculation, we find that $\deg(\phi(y)) = 7$ when arbitrary $b_1 \in \{(1)_2, (2)_2, (3)_2, (6)_2, (9)_2, (14)_2, (26)_2, (28)_2, (29)_2, (36)_2, (38)_2, (41)_2, (42)_2, (43)_2, (44)_2, (47)_2, (48)_2, (50)_2, (57)_2, (61)_2, (67)_2, (69)_2, (73)_2, (74)_2, (82)_2, (83)_2, (84)_2, (90)_2, (92)_2, (93)_2, (96)_2, (105)_2, (107)_2, (109)_2, (111)_2, (115)_2, (117)_2, (118)_2, (119)_2, (125)_2, (130)_2, (131)_2, (135)_2, (138)_2, (139)_2, (141)_2, (143)_2, (148)_2, (149)_2, (150)_2, (153)_2, (156)_2, (158)_2, (161)_2, (165)_2, (166)_2, (168)_2, (169)_2, (177)_2, (180)_2, (181)_2, (182)_2, (183)_2, (189)_2, (201)_2, (209)_2, (218)_2, (219)_2, (220)_2, (227)_2, (233)_2, (237)_2, (240)_2, (246)_2, (248)_2, (250)_2, (255)_2\}$. There are 77 elements in the set.

Theorem 7. *Let $y \in F_2^k$ and $\phi(y)$ be defined as in Theorem 3. Then there exists at least one vector $b_1 \in F_2^k$ such that $\deg(\phi(y)) = k - 1$.*

Proof From Theorem 2, we know that $\deg(\phi(y)) = k - 1$ if and only if $\deg(\phi^{-1}(y)) = k - 1$. By Theorem 4, we have $\phi^{-1}(y) = \psi'(y)$. Further, according to Remark 3, we know $\psi'(y) \oplus \mathbf{1} = \psi(y)$. Clearly, the algebraic degree of $\psi'(y)$ is same as that of $\psi(y)$. Combining to Theorem 5 and 6, there exists at least one vector b_1 such that $\psi(y)$ has an optimal algebraic degree $k - 1$. Thus, both $\psi'(y)$ and $\phi(y)$ have an optimal algebraic degree.

For $k = 8$, we can obtain 77 Boolean permutations of an optimal algebraic degree on 8 variables by using Theorem 7 and Example 1.

4. Conclusion

In the design and analysis of cryptographic transformations such as block ciphers and stream ciphers, Boolean permutations play an important role. In this paper, we put forward a method to propose the inverse of a given Boolean permutation. It was shown that a Boolean permutation had an optimal algebraic degree if and only if its inverse had an optimal algebraic degree. We presented a class of Boolean permutations and showed that the constructed Boolean permutations have an optimal algebraic degree if we selected an appropriate initial vector b_1. In addition, we found that the sum of the inverse of the constructed Boolean permutations and vector $\mathbf{1}$ was the Boolean permutations presented in [11,9]. In terms of constructions of Boolean permutations with good criteria (which mainly include high algebraic degree, high nonlinearity and low differential uniformity), the research results are relatively few. The problem of how to construct Boolean permutations with good criteria is an interesting topic that we would like to address in the future.

Acknowledgments: This work was supported in part by National Science Foundation of China (60833008), 973 Project (2007CB311201), and in part Science and Technology on Communication Security Laboratory (Grant No. 9140C110201110C1102), in part Fundamental Research Funds for the Central Universities (K50510010015).

References

[1] A.Canteaut, M. Trabbia, Improved fast correlation attacks using parity-check equations of weight 4 and 5, in: Proceedings of Cryptology-EUROCRYPT 2000, LNCS, vol.1807, Springer, Herdelberg, 2000, 573–588.

[2] C.Carlet, On the confusion and diffusion properties of Maiorana-McFarland's and extended Maiorana-McFarland's functions, *J. Complexity*, **20**(2004), 182–204.

[3] C.Carlet, Boolean functions for cryptography and error correcting codes, in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, 2010, 257–397. Available: http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html

[4] C.Carlet, Vectorial boolean functions for cryptography, Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, 2010, 398–469, Preliminary version available at http://www-roc.inria.fr/secret/Claude.Carlet/chap-vectorial-fcts-corr.pdf

[5] C. Carlet, Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions, *Des. Codes Cryptogr.*, **59**(2011), 89-109.

[6] C.Carlet, Comments on "Constructions of Cryptographically Significant Boolean Functions Using Primitive Polynomials", *IEEE Tans. Inf. Theory*, **57**(7)(2011), 4852–4853.

[7] C.Carlet, P.Charpin, V.Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Designs, Codes Cryptogr.*, **15**(1998), 125–156.

[8] C.Carlet and K.Feng, An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity, in: Proceedings of Cryptology-ASIACRYPT 2008, LNCS, vol.5350, Springer, 2008, 425–440.

[9] C.Carlet and K.Feng, An Infinite Class of Vectorial Boolean functions with Optimal Algebraic Immunity and Good Nonlinearity, in: Proceedings of IWCC2009, LNCS, vol.5557, Springer, 2009, 1–11.

[10] N. Courtois, J. Pieprzyk, Cryptanalysis of block ciphers with overdefined systems of equations, in: Proceedings of ASIACRYPT 2002, LNCS, vol.2501, Springer, Herdelberg, 2003, 267–287.

[11] K.Feng, Q.Liao and J.Yang, Maximal values of generalized algebraic immunity, *Des. Codes Cryptogr.*, **50**(2009), 243–252.

[12] K. Khoo, C. W. Lim, G. Gong, Highly nonlinear balanced S-boxes with improved bound on unrestricted and generalized nonlinearity, *Appl. Algebra Engrg. Comm. Comput.*, **19**(2008), 323–338.

[13] X.Lai, Higher order derivatives and differential cryptanalysis, Communications and Cryptography: Two sides of Tapestry, Kluwer Academic Publishers, 1994, 227–233.

[14] P.Langevin, P.V*é*ron, On the nonlinearity of power functions, *Des. Codes Cryptogr.*, **37**(2005), 31–43.

[15] R.Lidl and H.Niederreiter, *Finite felds*, in: Encyclopedia of Mathematics and Its Applications. Reading, 20, MA: Addison-Wesley, 1983, 186–204.

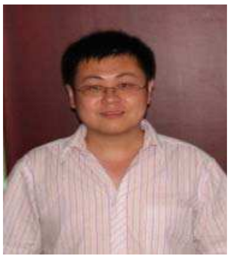
[16] M.Matsui, Linear cryptanalysis method for DES cipher, in: Proceedings of Cryptology-EUROCRYPT'93, LNCS, vol.765, Springer, 1994, 386–397.

[17] W.Meier, E.Pasalic and C.Carlet, Algebraic attacks and decomposition of Boolean functions. in: Proceedings of Cryptology-EUROCRYPT 2004, LNCS, vol.3027, Springer, 2004, 474–491.

[18] O.S.Rothaus. On "Bent" functions, *J. Combin. Theory Ser. A*, **20** (1976), 300–305.

[19] Q.Wang, J.Peng, H.Kan and X.Xue, Constructions of cryptographically signicant Boolean functions using primitive polynomials, *IEEE Trans. Inform. Theory*, **56** (2010), 3048–3053.

[20] W.Zhang, C.Wu, S.Li, Construction of cryptographically important Boolean permutations, *Appl. Algebra Engrg. Comm. Comput.*, **15**(2004), 173–177.



Fengrong Zhang born in 1982, received the M.S. degree in Mathematics from Xidian University, Xi'an, China in 2006. He is currently a Ph.D. candidate in Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University, China. His current research interests include stream ciphers and cryptographic functions.

Yupu Hu was born in 1955, is Professor and Ph.D. supervisor in Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University, China. His current research interests include stream ciphers, block ciphers, digital signature and network security.

Min Xie was born in 1976, is Associate Professor in Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University, China. Her current research interests include stream ciphers, block ciphers, information theory.

Juntao Gao is a Doctor in Xidian University, and is Associate Professor in Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University, China. His research interests include stream ciphers, information security, pseudo-random sequences and cryptographic functions.

Qichun Wang received the M.S. degree in mathematics in 2006 from Fudan University, Shanghai, China, where he is currently pursuing the Ph.D. degree in the School of Computer Science. From November 2009 to October 2010, he was with Lund University, Lund, Sweden, as a joint Ph.D. student between Fudan University and Lund University.