On the Diffusion Property of Iterated Functions

Jian Liu[1] ⋆, Sihem Mesnager[2], and Lusheng Chen[3]

[1] School of Computer Software, Tianjin University, Tianjin 300072, P. R. China and CNRS, UMR 7539 LAGA, Paris, France
jianliu.nk@gmail.com
[2] Department of Mathematics, University of Paris VIII, University of Paris XIII, CNRS, UMR 7539 LAGA and Telecom ParisTech, Paris, France
smesnager@univ-paris8.fr
[3] School of Mathematical Sciences, Nankai University, Tianjin 300071, P. R. China
lschen@nankai.edu.cn

Abstract. For vectorial Boolean functions, the behavior of iteration has consequence in the diffusion property of the system. We present a study on the diffusion property of iterated vectorial Boolean functions. The measure that will be of main interest here is the notion of the degree of completeness, which has been suggested by the NESSIE project. We provide the first (to the best of our knowledge) two constructions of (n, n)-functions having perfect diffusion property and optimal algebraic degree. We also obtain the complete enumeration results for the constructed functions.

Keywords: Boolean functions; degree of completeness; perfect diffusion property; algebraic degree; balancedness.

1 Introduction

Vectorial Boolean functions have been extensively studied for their applications in cryptography, coding theory, combinatorial design etc., see [4] for a survey. Let $\mathbb{F}_2^n$ denote the n-dimensional vector space over the finite field $\mathbb{F}_2$ with two elements. Vectorial Boolean functions are functions from the vector space $\mathbb{F}_2^n$ to the vector space $\mathbb{F}_2^m$, for given positive integers n and m. These functions are called (n, m)-functions and include the single-output Boolean functions (which correspond to the case $m = 1$).

In 1949, Shannon [16] used the term diffusion to denote the quantitative spreading of information. For an (n, m)-function, the diffusion property describes the influence of input bits on the output bits. The exact meaning of diffusion relates strongly to the methods of cryptanalysis. An intuitive measure related to diffusion is of considerable importance for vectorial Boolean functions: the *degree of completeness*, denoted by D_c, which is given by the comments from the NESSIE project [15]. In [10], Kam and Davida introduced the concept of

⋆ This work is supported by the National Key Basic Research Program of China under Grant 2013CB834204.

complete functions, which means that every output bit depends on every input bit (also see [7,9]). For a vectorial Boolean function, the degree of completeness quantifies the rate of input bits that the output bits depend on. A complete function possesses optimal degree of completeness, i.e., $\mathrm{D}_c = 1$. In this paper, we use the notion of the degree of completeness to indicate the diffusion property of a vectorial Boolean function. In this sense, by perfect diffusion property we mean iterated vectorial Boolean functions which possess optimal degree of completeness. There are other indicators of diffusion property which shall not be discussed here. For instance, the *branch number of diffusion layers* (see [6]) relates closely to differential cryptanalysis [2] and linear cryptanalysis [12] on block ciphers. The *diffusion factor* (see [6]) quantifies the average number of changed output bits when a single input bit is changed. The degree of completeness can be seen as some kind of weakened version of diffusion factor.

The investigation on the degree of completeness of iterated (n, n)-functions helps in general the understanding of the evolution of diffusion property of cryptographic systems. Some methods of cryptanalysis on cryptosystems are based on the idea of identifying the relation between a particular output bit with the input bits. If every output bit depends on only a few of the input bits, there may exist some potential attacks, such as algebraic attacks [1,5], since one may convert the cipher-text into a system of polynomial equations and solve it directly. For example, in a product cryptosystem [16] such as block cipher and hash function, the degrees of completeness of iterated round functions (seen as vectorial Boolean functions) have consequence in the diffusion property of the whole system. A round function is preferable to have perfect diffusion property for providing complete diffusion, see the general model in Section 3.2. In the context of stream ciphers, the model of augmented functions should be considered (see [8]), where an update function L is iterated to generate keystreams by composing an output function. If the degrees of completeness of the iterated update functions $L^{(i)}$, $i = 1, 2, \ldots$, are very low, then the algebraic attack is expected to be efficient. Other potential applications of functions with perfect diffusion property could be found.

Though the degree of completeness has been observed from a cryptographic point of view, it seems that as a mathematical object, vectorial Boolean function with good diffusion property has rarely been studied in the literature. In this paper, we mainly study the diffusion property of vectorial Boolean functions. A function is called to have *perfect diffusion property* (see Definition 2) if the degree of completeness always attains 1 (under the affine permutations) after the function has been iterated some number of times. We provide two constructions of vectorial Boolean functions which have perfect diffusion property, and prove that the iterated functions always have optimal algebraic degree. To the best of our knowledge, this is the first time when such constructions are proposed. We first construct a class of rotation symmetric (n, n)-functions (see Definition 3) with perfect diffusion property. These functions are generalizations of rotation symmetric Boolean functions, which have practical advantages that the evaluations are efficient and the representations are short. In our second construction,

a class of almost balanced (n, n)-functions with perfect diffusion property is given. Moreover, complete enumeration results for the constructed functions are obtained, which show that there are many (n, n)-functions with perfect diffusion property.

This paper is organized as follows. Formal definitions and necessary preliminaries are introduced in Section 2. In Section 3, two constructions of vectorial Boolean functions with perfect diffusion property are proposed for the first time, and the complete enumeration results for these functions are presented. To avoid being too theoretical, we give an explicit example to show that it is possible to construct recursive round functions to provide complete diffusion. We summarize this paper in the last section.

2 Background and Preliminaries

In this paper, additions and multiple sums calculated modulo 2 will be denoted by $\oplus$ and $\bigoplus_i$ respectively, additions and multiple sums calculated in characteristic 0 or in the additions of elements of the finite field $\mathbb{F}_{2^n}$ will be denoted by $+$ and $\sum_i$ respectively. The functions from the vector space $\mathbb{F}_2^n$ to $\mathbb{F}_2$ are called *n-variable Boolean functions*, and the set of all the n-variable Boolean functions is denoted by $\mathcal{B}_n$. For $f \in \mathcal{B}_n$, the *Hamming weight* (in brief, *weight*) of f is $\mathrm{wt}(f) = \big|\{x \in \mathbb{F}_2^n \mid f(x) = 1\}\big|$, and the $(0,1)$-sequence defined by $(f(\mathbf{v}_0), f(\mathbf{v}_1), \ldots, f(\mathbf{v}_{2^n-1}))$ is called the *truth table* of f, where $\mathbf{v}_0 = (0, \ldots, 0, 0), \mathbf{v}_1 = (0, \ldots, 0, 1), \ldots, \mathbf{v}_{2^n-1} = (1, \ldots, 1, 1)$ are ordered by lexicographical order. An n-variable Boolean function f can be uniquely represented in the *algebraic normal form* (in brief, *ANF*) that

$$f(x) = \bigoplus_{v \in \mathbb{F}_2^n} c_v x_1^{v_1} x_2^{v_2} \cdots x_n^{v_n},$$

where $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, $v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$, $c_v \in \mathbb{F}_2$. Let $\mathrm{wt}(v)$ denote the Hamming weight (or weight) of a vector v, that is the number of its nonzero coordinates, then $\deg(f) = \max_{v \in \mathbb{F}_2^n}\{\mathrm{wt}(v) \mid c_v \neq 0\}$ is called the *algebraic degree* of f.

Proposition 1. *[3] Let $f \in \mathcal{B}_n$ and $f(x) = \bigoplus_{v \in \mathbb{F}_2^n} c_v x_1^{v_1} x_2^{v_2} \cdots x_n^{v_n}$. Then, $c_v = \bigoplus_{x \in \mathbb{F}_2^n, x \preceq v} f(x)$, where $x \preceq v$ means that $x = (x_1, \ldots, x_n)$ is covered by $v = (v_1, \ldots, v_n)$, i.e., for any $i = 1, \ldots, n$, $x_i = 1$ implies $v_i = 1$. In particular, $\deg(f) = n$ if and only if $\mathrm{wt}(f)$ is odd.*

An affine permutation L on $\mathbb{F}_2^n$ is defined as $L(x) = xM \oplus a$, where M is a nonsingular $n \times n$ matrix over $\mathbb{F}_2$ and $a \in \mathbb{F}_2^n$. Moreover, if $a = \mathbf{0}$, then L is called a linear permutation.

Proposition 2. *[3] The algebraic degree of an n-variable Boolean function f is affine invariant, i.e., for every affine permutation L, we have $\deg(f \circ L) = \deg(f)$.*

For $i = 1, \ldots, n$, denote by e_i the vector in $\mathbb{F}_2^n$ whose i-th component equals 1, and 0 elsewhere. The *degree of completeness* of an n-variable Boolean function f is defined as

$$\mathrm{D}_c(f) = 1 - \frac{|\{i \mid a_i = 0, 1 \leqslant i \leqslant n\}|}{n}, \tag{1}$$

where $a_i = |\{x \in \mathbb{F}_2^n \mid f(x) \oplus f(x \oplus e_i) = 1\}|$, $i = 1, \ldots, n$. Equivalently, let

$$\mathcal{V}(f) = \left\{ i \;\middle|\; \exists x \in \mathbb{F}_2^n \text{ such that } f(x) \oplus f(x \oplus e_i) = 1, 1 \leqslant i \leqslant n \right\}, \tag{2}$$

be the set of indices of the variables appearing in the ANF of f, then $\mathrm{D}_c(f) = |\mathcal{V}(f)|/n$.

Let n and m be two positive integers. The functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called (n, m)-*functions* (or *vectorial Boolean functions*). Such a function F is given by $F = (f_1, \ldots, f_m)$, where the Boolean functions $f_1, \ldots, f_m$ are called the *coordinate functions* of F. An (n, m)-function is called *balanced* if for any $b \in \mathbb{F}_2^m$, the size of the pre-image set $|F^{-1}(b)| = 2^{n-m}$. The *derivative* of F at direction a is defined as

$$\triangle_a F(x) = F(x) \oplus F(x \oplus a), \quad a \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}.$$

The *algebraic degree* of F, denoted by $\mathrm{Deg}(F)$, is defined as

$$\mathrm{Deg}(F) = \max_{1 \leqslant i \leqslant m} \deg(f_i).$$

The *degree of completeness* of F is defined as

$$\mathrm{D}_c(F) = \frac{1}{m}(\mathrm{D}_c(f_1) + \cdots + \mathrm{D}_c(f_m)). \tag{3}$$

Since the degree of completeness of an n-variable Boolean function can also be described as $\mathrm{D}_c(f) = |\mathcal{V}(f)|/n$, where $\mathcal{V}(f)$ is defined as in (2), then for an (n, m)-function $F = (f_1, \ldots, f_m)$, we have $\mathrm{D}_c(F) = \left(|\mathcal{V}(f_1)| + \cdots + |\mathcal{V}(f_m)|\right)/nm$. Also, the following equivalent definition is easy to obtain, which is originally given by the NESSIE project [15].

Definition 1. *[15] For an (n, m)-function $F = (f_1, \ldots, f_m)$, the* degree of completeness *is defined as*

$$\mathrm{D}_c(F) = 1 - \frac{|\{(i, j) \mid a_{ij} = 0, 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}|}{mn},$$

where $a_{ij} = |\{x \in \mathbb{F}_2^n \mid f_j(x) \oplus f_j(x \oplus e_i) = 1\}|$, $i = 1, \ldots, n$, $j = 1, \ldots, m$.

For an (n, m)-function F, it is obvious that $0 \leqslant \mathrm{D}_c(F) \leqslant 1$, and F is called *complete* if $\mathrm{D}_c(F) = 1$ (see [10]), which provides the highest possible level of diffusion. Note that $\mathrm{D}_c(F)$ defined in (3) takes the mean value of all the $\mathrm{D}_c(f_i)$'s with $i = 1, \ldots, m$, while the following two meaningful measures are also intuitive,

$$\mathrm{D}_c^{max}(F) = \max_{1 \leqslant i \leqslant m} \{\mathrm{D}_c(f_i)\}, \quad \mathrm{D}_c^{min}(F) = \min_{1 \leqslant i \leqslant m} \{\mathrm{D}_c(f_i)\}.$$

Clearly, $\mathrm{D}_c^{min}(F) \leqslant \mathrm{D}_c(F) \leqslant \mathrm{D}_c^{max}(F)$, and $\mathrm{D}_c^{min}(F) = 1$ if and only if $\mathrm{D}_c(F) = 1$. Hence, D_c^{min} is the strongest measure of completeness for vectorial Boolean functions. In this paper, we mainly discuss the measure D_c suggested by the NESSIE project [15].

For an n-variable Boolean function f, since for any $b \in \mathbb{F}_2^n$,

$$a_i = |\{x \in \mathbb{F}_2^n \mid f(x) \oplus f(x \oplus e_i) = 1\}| = |\{x \in \mathbb{F}_2^n \mid f(x \oplus b) \oplus f(x \oplus b \oplus e_i) = 1\}|,$$

where $i = 1, \ldots, n$, then from (1), we have $\mathrm{D}_c(f(x)) = \mathrm{D}_c(f(x \oplus b))$. In general, the degree of completeness is not invariant under composition on the right by linear permutations. For example, let $f(x_1, \ldots, x_n) = x_1 \oplus \cdots \oplus x_n \in \mathcal{B}_n$, and $L(x_1, \ldots, x_n) = (x_1 \oplus \cdots \oplus x_n, x_2, \ldots, x_n)$ which is a linear permutation on $\mathbb{F}_2^n$, then $f \circ L(x_1, \ldots, x_n) = x_1$, and thus $\mathrm{D}_c(f) = 1 > \mathrm{D}_c(f \circ L) = 1/n$. For a positive integer r, let $F^{(r)} = \overbrace{F \circ \cdots \circ F}^{r}$ denote the r-th iterated function of F.

Definition 2. *An (n, m)-function F is called* non-degenerate *if for every linear permutation L on $\mathbb{F}_2^n$, $\mathrm{D}_c(F \circ L) = 1$. Moreover, F is said to have* perfect diffusion property *if $m = n$ and for any positive integer k, $F^{(k)}$ is non-degenerate.*

Theorem 1. *For an (n, m)-function $F = (f_1, \ldots, f_m)$, if for all $i = 1, \ldots, m$, $\deg(f_i) = n$, then F is non-degenerate.*

Proof. According to Proposition 2, one gets that for every linear permutation L on $\mathbb{F}_2^n$ and every $1 \leqslant i \leqslant m$, $\deg(f_i \circ L) = \deg(f_i) = n$, thus $\mathrm{D}_c(f_i \circ L) = 1$. From (3), we have that $\mathrm{D}_c(F \circ L) = (\mathrm{D}_c(f_1 \circ L) + \cdots + \mathrm{D}_c(f_m \circ L))/m = 1$. Hence, F is non-degenerate. □

Remark 1. When we choose a basis $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, then the vector space $\mathbb{F}_2^n$ can be endowed with the structure of finite field $\mathbb{F}_{2^n}$ by an isomorphism $\pi : x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n \to x_1\alpha_1 + \cdots + x_n\alpha_n \in \mathbb{F}_{2^n}$. For a Boolean function f on $\mathbb{F}_{2^n}$, we identify $\mathrm{D}_c(f)$ with $\mathrm{D}_c(f \circ \pi)$. Since for any $i = 1, \ldots, n$,

$$\begin{aligned} a_i &= |\{x \in \mathbb{F}_2^n \mid f \circ \pi(x) + f \circ \pi(x \oplus e_i) = 1\}| \\ &= |\{x \in \mathbb{F}_2^n \mid f(\pi(x)) + f\left(\pi(x) + \pi(e_i)\right) = 1\}| \\ &= |\{x \in \mathbb{F}_{2^n} \mid f(x) + f\left(x + \alpha_i\right) = 1\}|, \end{aligned}$$

then from (1), one gets that $\mathrm{D}_c(f) = \mathrm{D}_c(f \circ \pi) = 1$ if and only if for any $i = 1, \ldots, n$, the derivative $\Delta_{\alpha_i} f(x)$ is not a zero function (i.e., there exists $x \in \mathbb{F}_{2^n}$ such that $\Delta_{\alpha_i} f(x) = 1$). Note that L is a linear permutation on $\mathbb{F}_2^n$ if and only if $\pi \circ L \circ \pi^{-1}$ is an additive automorphism on $\mathbb{F}_{2^n}$. Hence, from Definition 2, a Boolean function f is non-degenerate if for any $i = 1, \ldots, n$ and any additive automorphism L of $\mathbb{F}_{2^n}$, $\Delta_{\alpha_i} f \circ L(x)$ is not a zero function.

Remark 2. The trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is defined as

$$\mathrm{Tr}_1^n(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}},$$

where $x \in \mathbb{F}_{2^n}$. Given a basis $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, a function F from $\mathbb{F}_{2^n}$ to itself can be written as $F(x) = f_1(x)\alpha_1 + \cdots + f_n(x)\alpha_n$, where $f_i(x) = \mathrm{Tr}_1^n(\beta_i F(x))$, $i = 1, \ldots, n$, are the n-variable coordinate Boolean functions of F, and $\{\beta_1, \ldots, \beta_n\}$ is the *dual basis* of $\{\alpha_1, \ldots, \alpha_n\}$ satisfying

$$\mathrm{Tr}_1^n(\alpha_i\beta_j) = \begin{cases} 0 \text{ for } & i \neq j, \\ 1 \text{ for } & i = j. \end{cases}$$

It is known that for any basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, there exists a dual basis (see [11, Chapter 2]). From Definition 2, we know that an (n, n)-function F has perfect diffusion property if and only if for every k, every coordinate function of $F^{(k)}$ is non-degenerate, which is equivalent to saying that, for any $j \in \{1, \ldots, n\}$, $f_j^{(k)}(x) = \mathrm{Tr}_1^n\left(\beta_j F^{(k)}(x)\right)$ is non-degenerate. From Remark 1, we have that $f_j^{(k)}(x)$ is non-degenerate if and only if for any $i \in \{1, \ldots, n\}$ and any additive automorphism L of $\mathbb{F}_{2^n}$,

$$\begin{aligned} \Delta_{\alpha_i} f_j^{(k)} \circ L(x) &= f_j^{(k)} \circ L(x) + f_j^{(k)} \circ L(x + \alpha_i) \\ &= \mathrm{Tr}_1^n\left(\beta_j F^{(k)} \circ L(x)\right) + \mathrm{Tr}_1^n\left(\beta_j F^{(k)} \circ L(x + \alpha_i)\right) \\ &= \mathrm{Tr}_1^n\left(\beta_j \triangle_{\alpha_i} F^{(k)} \circ L(x)\right) \end{aligned}$$

is not a zero function. As a consequence, from Definition 2, an (n, n)-function F is said to have perfect diffusion property if for any positive integer k, any $i, j \in \{1, \ldots, n\}$, and any additive automorphism L of $\mathbb{F}_{2^n}$, $\mathrm{Tr}_1^n\left(\beta_j \triangle_{\alpha_i} F^{(k)} \circ L(x)\right)$ is not a zero function.

3 Constructions of Vectorial Boolean Functions with Perfect Diffusion Property

In this section, we construct two classes of (n, n)-functions which have perfect diffusion property. Moreover, the enumeration results for the constructed functions are obtained.

3.1 Rotation Symmetric (n, n)-Functions with Perfect Diffusion Property

Let $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$. For $1 \leqslant k \leqslant n-1$, define

$$\rho_n^k(x_1, x_2, \ldots, x_n) = (x_{k+1}, \ldots, x_n, x_1, \ldots, x_k),$$

and $\rho_n^0(x_1, x_2, \ldots, x_n) = (x_1, x_2, \ldots, x_n)$. Inspired by the concept of rotation symmetric Boolean functions used in fast hashing algorithms [14], we present the following definition of rotation symmetric (n, n)-functions.

Definition 3. *Let f be an n-variable Boolean function. An (n,n)-function F is called* rotation symmetric *(in brief,* RS*) if it has the form*

$$F(x) = \left(f(x), f\circ\rho_n^1(x), f\circ\rho_n^2(x), \ldots, f\circ\rho_n^{n-1}(x)\right). \tag{4}$$

Let $f \in \mathcal{B}_n$ and $F = (f, f\circ\rho_n^1, \ldots, f\circ\rho_n^{n-1})$. For any $x \in \mathbb{F}_2^n$ and any integer $l \geqslant 1$,

$$\begin{aligned} F\circ\rho_n^l(x) &= \left(f\circ\rho_n^l(x), f\circ\rho_n^{l+1}(x), \ldots, f\circ\rho_n^{l-1}(x)\right) \\ &= \rho_n^l\left(f(x), f\circ\rho_n^1(x), \ldots, f\circ\rho_n^{n-1}(x)\right) = \rho_n^l\circ F(x). \end{aligned} \tag{5}$$

An (n,n)-function F satisfying Eq.(5) is called *shift-invariant* in [6]. Recall that an n-variable rotation symmetric Boolean function f is defined as $f\circ\rho_n^1(x) = f(x)$ for any $x \in \mathbb{F}_2^n$ (see [14]). By Eq.(5), the following equivalent definition of RS (n,n)-functions is easy to obtain.

Proposition 3. *An (n,n)-function F is RS if and only if for any $x \in \mathbb{F}_2^n$,*

$$F\circ\rho_n^1(x) = \rho_n^1\circ F(x).$$

Proposition 4. *If F is an RS (n,n)-function, then for any integer $k \geqslant 1$, $F^{(k)}$ is an RS (n,n)-function.*

Proof. We prove it by induction on k. The result is already true for $k = 1$. Suppose that $F^{(k)}$ is RS for $k = s$, where $s \geqslant 1$, then $F^{(s)}$ has the form

$$F^{(s)}(x) = \left(f(x), f\circ\rho_n^1(x), \ldots, f\circ\rho_n^{n-1}(x)\right),$$

which implies that

$$\begin{aligned} F^{(s+1)}(x) = F^{(s)}(F(x)) &= \left(f\left(F(x)\right), f\circ\rho_n^1\left(F(x)\right), \ldots, f\circ\rho_n^{n-1}\left(F(x)\right)\right) \\ &= \left(f\circ F(x), f\circ F\circ\rho_n^1(x), \ldots, f\circ F\circ\rho_n^{n-1}(x)\right), \end{aligned} \tag{6}$$

where Eq.(6) follows from Eq.(5) since F is RS. Hence, for $k = s+1$, $F^{(k)}$ is an RS (n,n)-function. By the mathematical induction, we get that for $k \geqslant 1$, $F^{(k)}$ is RS. □

Remark 3. From Proposition 3 and Proposition 4, one can see that rotation symmetric (n,n)-functions possess many desirable properties like (i) the algebraic representations are short; (ii) the evaluation of the functions is efficient (since a circular shift of the input bits leads to the corresponding shift of the output bits); (iii) the iterated functions are still rotation symmetric.

Under the action of ρ_n^k, $0 \leqslant k \leqslant n-1$, the *orbit* generated by the vector $x = (x_1, x_2, \ldots, x_n)$ is defined as

$$\mathcal{O}_n(x) = \left\{\rho_n^k(x_1, x_2, \ldots, x_n) \;\middle|\; 0 \leqslant k \leqslant n-1\right\}. \tag{7}$$

It is easy to check that the cardinality of an orbit generated by $x = (x_1, \ldots, x_n)$ is a factor of n. In fact, let $|\mathcal{O}_n(x)| = t$, and suppose that $n = p\cdot t + r$ for $p, r \in \mathbb{Z}$ and

$0 < r < t$. Then $\rho_n^t(x) = x$, which implies that $\rho_n^{p \cdot t}(x) = x$, thus $\rho_n^{n-p \cdot t}(x) = x$, i.e., $\rho_n^r(x) = x$, a contradiction to the fact that $|\mathcal{O}_n(x)| = t > r$. Clearly, all the orbits generate a partition of $\mathbb{F}_2^n$. Every orbit can be represented by its lexicographically first element, called the *representative element*. It is proved that (see e.g. [6, Appendix A.1]) the number of distinct orbits is $\Psi_n = \frac{1}{n} \sum_{k|n} \phi(k) 2^{n/k}$, where $\phi(k)$ is the Euler's *phi*-function. Let $\left\{\Lambda_1^{(n)}, \Lambda_2^{(n)}, \ldots, \Lambda_{\Psi_n}^{(n)}\right\}$ denote the set of all the representative elements in lexicographical order, where $\Lambda_1^{(n)} = \mathbf{0}$ and $\Lambda_{\Psi_n}^{(n)} = \mathbf{1}$, and we use $\{\Lambda_1, \Lambda_2, \ldots, \Lambda_{\Psi_n}\}$ for short if there is no risk of confusion.

For $f \in \mathcal{B}_n$ and $1 \leqslant i \leqslant \Psi_n$, let $f|_{\mathcal{O}_n(\Lambda_i)}$ denote the restriction of f to $\mathcal{O}_n(\Lambda_i)$, i.e., for $x \in \mathcal{O}_n(\Lambda_i)$, $f|_{\mathcal{O}_n(\Lambda_i)}(x) = f(x)$. Then, we have the following theorem.

Theorem 2. *For any n-variable Boolean function f satisfying the following conditions:*
(i) For $i = 1, 2, \ldots, \Psi_n - 1$, $\mathrm{wt}\left(f|_{\mathcal{O}_n(\Lambda_i)}\right) = t_i \cdot \mathrm{wt}(\Lambda_i)/n$, where $t_i = |\mathcal{O}_n(\Lambda_i)|$;
(ii) $f(\mathbf{1}) = 0$,
the RS (n, n)-function $F(x) = \left(f(x), f \circ \rho_n^1(x), \ldots, f \circ \rho_n^{n-1}(x)\right)$ has perfect diffusion property, and for every $k \geqslant 1$, $\mathrm{Deg}\left(F^{(k)}\right) = n$.

Proof. For $i = 1, 2, \ldots, \Psi_n - 1$, let $F|_{\mathcal{O}_n(\Lambda_i)}$ denote the $t_i \times n$ matrix over $\mathbb{F}_2$ that

$$F|_{\mathcal{O}_n(\Lambda_i)} = \begin{pmatrix} F(\Lambda_i) \\ F\left(\rho_n^1(\Lambda_i)\right) \\ \vdots \\ F\left(\rho_n^{t_i-1}(\Lambda_i)\right) \end{pmatrix}_{t_i \times n} = \begin{pmatrix} F(\Lambda_i) \\ \rho_n^1\left(F(\Lambda_i)\right) \\ \vdots \\ \rho_n^{t_i-1}\left(F(\Lambda_i)\right) \end{pmatrix}_{t_i \times n},$$

where $t_i = |\mathcal{O}_n(\Lambda_i)|$ and the last equality is from Eq.(5). It is obvious that the number of 1's in every column (as well as every row) of $F|_{\mathcal{O}_n(\Lambda_i)}$ is the same. Since $\mathrm{wt}\left(f|_{\mathcal{O}_n(\Lambda_i)}\right) = t_i \cdot \mathrm{wt}(\Lambda_i)/n$, then every row of $F|_{\mathcal{O}_n(\Lambda_i)}$ has the same weight that

$$\frac{\mathrm{wt}\left(f|_{\mathcal{O}_n(\Lambda_i)}\right) \cdot n}{t_i} = \frac{t_i \cdot \mathrm{wt}(\Lambda_i) \cdot n}{n \cdot t_i} = \mathrm{wt}(\Lambda_i).$$

Hence, for $x = \rho_n^l(\Lambda_i)$, where $i = 1, 2, \ldots, \Psi_n - 1$ and $l = 0, \ldots, |\mathcal{O}_n(\Lambda_i)| - 1$,

$$\mathrm{wt}(F(x)) = \mathrm{wt}\left(F\left(\rho_n^l(\Lambda_i)\right)\right) = \mathrm{wt}\left(\Lambda_i\right) = \mathrm{wt}\left(\rho_n^l(\Lambda_i)\right) = \mathrm{wt}(x),$$

i.e., for every $x \in \mathbb{F}_2^n \setminus \{\mathbf{1}\}$, $\mathrm{wt}(F(x)) = \mathrm{wt}(x)$. Therefore, for every $k \geqslant 1$ and every $x \in \mathbb{F}_2^n \setminus \{\mathbf{1}\}$, we have

$$\mathrm{wt}\left(F^{(k)}(x)\right) = \mathrm{wt}(x). \tag{8}$$

Thanks to Proposition 4, we know that $F^{(k)}$ is still an RS (n, n)-function, thus we can write $F^{(k)}$ as $\left(f^{(k)}, f^{(k)} \circ \rho_n^1, \ldots, f^{(k)} \circ \rho_n^{n-1}\right)$, where $f^{(k)} \in \mathcal{B}_n$. From

Eq.(8), we have that for $i = 1, 2, \ldots, \Psi_n - 1$, every column of the matrix

$$F^{(k)}\big|_{\mathcal{O}_n(\Lambda_i)} = \begin{pmatrix} F^{(k)}(\Lambda_i) \\ F^{(k)}\left(\rho_n^1(\Lambda_i)\right) \\ \vdots \\ F^{(k)}\left(\rho_n^{t_i-1}(\Lambda_i)\right) \end{pmatrix}_{t_i \times n} = \begin{pmatrix} F^{(k)}(\Lambda_i) \\ \rho_n^1\left(F^{(k)}(\Lambda_i)\right) \\ \vdots \\ \rho_n^{t_i-1}\left(F^{(k)}(\Lambda_i)\right) \end{pmatrix}_{t_i \times n}$$

has weight $t_i \cdot \mathrm{wt}(\Lambda_i)/n$. Since $\bigcup_{i=1}^{\Psi_n} \mathcal{O}_n(\Lambda_i) = \mathbb{F}_2^n$, then it is easy to prove that

$$\sum_{i=1}^{\Psi_n} \frac{t_i \cdot \mathrm{wt}(\Lambda_i)}{n} = 2^{n-1}.$$

Condition (ii) implies $\mathrm{wt}\left(F^{(k)}(\mathbf{1})\right) = 0$, then we have

$$\mathrm{wt}\left(f^{(k)}\right) = \sum_{i=1}^{\Psi_n - 1} \frac{t_i \cdot \mathrm{wt}(\Lambda_i)}{n} = 2^{n-1} - 1.$$

Hence, according to Proposition 1, $\deg\left(f^{(k)}\right) = n$, which leads to $\mathrm{Deg}\left(F^{(k)}\right) = n$. Note that for $l = 0, \ldots, n-1$, ρ_n^l is an affine permutation on $\mathbb{F}_2^n$, then from Proposition 2, we have $\deg\left(f^{(k)} \circ \rho_n^l\right) = \deg(f^{(k)}) = n$. Thus, Theorem 1 implies that $F^{(k)}$ is non-degenerate. Therefore, $F(x)$ has perfect diffusion property. □

In Theorem 3, we will calculate the number of all the functions constructed in Theorem 2. Before that, we introduce the following lemma which is given by Maximov [13, Lemma 1].

Lemma 1. *[13] For $\mathbb{F}_2^n$, the number of orbits with t elements of weight w is*

$$\eta_{n,t,w} = \begin{cases} \frac{1}{t}\sum_{k|t,q_k|w} \mu(t/k) \cdot \binom{n/q_k}{w/q_k}, & \text{for } t, w = 1, \ldots, n, \text{ where } q_k = \frac{n}{\gcd(n,k)}, \\ 1, & \text{for } t = 1, w = 0, \\ 0, & \text{otherwise}, \end{cases} \tag{9}$$

where $\mu(\cdot)$ is the Möbius function, i.e., for integer $t \geqslant 1$, $\mu(t) = 1$, if $t = 1$; $\mu(t) = (-1)^m$, if $t = p_1 p_2 \cdots p_m$, where $p_1, \ldots, p_m$ are distinct primes; $\mu(t) = 0$, for all other cases.

Theorem 3. *The number of distinct RS (n, n)-functions constructed in Theorem 2 is*

$$\mathcal{N}_n = \prod_{w=1}^{n-1} \prod_{t=1}^{n} \binom{t}{\frac{t \cdot w}{n}}^{\eta_{n,t,w}}, \tag{10}$$

where $\eta_{n,t,w} = \frac{1}{t}\sum_{k|t,q_k|w} \mu(t/k) \cdot \binom{n/q_k}{w/q_k}$, $q_k = \frac{n}{\gcd(n,k)}$, and $\mu(\cdot)$ is the Möbius function.

Proof. In Theorem 2, for any $i = 1, 2, \ldots, \Psi_n - 1$, $\mathrm{wt}\left(f|_{\mathcal{O}_n(\Lambda_i)}\right) = t_i \cdot \mathrm{wt}(\Lambda_i)/n$, which implies that one can construct $\binom{t_i}{t_i \cdot \mathrm{wt}(\Lambda_i)/n}$ distinct $f|_{\mathcal{O}_n(\Lambda_i)}$'s. Moreover, Lemma 1 claims that the number of orbits with $t = t_i$ elements of weight $w = \mathrm{wt}(\Lambda_i)$ is $\eta_{n,t,w}$. Then, one can get that the number of distinct RS (n, n)-functions constructed in Theorem 2 is $\mathcal{N}_n$ in Eq.(10). □

Example 1. For $\mathbb{F}_2^6$, all the orbits and the values of $\eta_{6,t,w}$ in Eq.(9) are listed in Table 1, where t and w are respectively the number and the weight of elements in an orbit.

Table 1. All the orbits of $\mathbb{F}_2^6$ and the values of $\eta_{6,t,w}$

	t	w		t	w
$\mathcal{O}_6(000000)$	1	0	$\mathcal{O}_6(010011)$	6	3
$\mathcal{O}_6(000001)$	6	1	$\mathcal{O}_6(010101)$	2	3
$\mathcal{O}_6(000011)$	6	2	$\mathcal{O}_6(001111)$	6	4
$\mathcal{O}_6(000101)$	6	2	$\mathcal{O}_6(010111)$	6	4
$\mathcal{O}_6(001001)$	3	2	$\mathcal{O}_6(011011)$	3	4
$\mathcal{O}_6(000111)$	6	3	$\mathcal{O}_6(011111)$	6	5
$\mathcal{O}_6(001011)$	6	3	$\mathcal{O}_6(111111)$	1	6

$\eta_{6,t,w}$	t 1 2 3 4 5 6
w	
0	1 0 0 0 0 0
1	0 0 0 0 0 1
2	0 0 1 0 0 2
3	0 1 0 0 0 3
4	0 0 1 0 0 2
5	0 0 0 0 0 1
6	1 0 0 0 0 0

Then, from Theorem 3, we have

$$\mathcal{N}_6 = \prod_{w=1}^{5} \prod_{t=1}^{6} \binom{t}{\frac{t \cdot w}{6}}^{\eta_{6,t,w}} = 2.6244 \times 10^{11} \approx 2^{37.9},$$

while the number of all the $(6, 6)$-functions is $2^{2^6 \cdot 6} = 2^{384}$.

Example 2. In Example 1, we have shown all the orbits $\{\mathcal{O}_6(\Lambda_i), i = 1, \ldots, 14\}$ of $\mathbb{F}_2^6$. Let f be a 6-variable Boolean function defined as

$$\begin{aligned}
&f|_{\mathcal{O}_6(000000)} = (0), && f|_{\mathcal{O}_6(010011)} = (1, 0, 0, 1, 0, 1),\\
&f|_{\mathcal{O}_6(000001)} = (0, 0, 0, 1, 0, 0), && f|_{\mathcal{O}_6(010101)} = (0, 1),\\
&f|_{\mathcal{O}_6(000011)} = (0, 0, 1, 1, 0, 0), && f|_{\mathcal{O}_6(001111)} = (1, 1, 0, 1, 1, 0),\\
&f|_{\mathcal{O}_6(000101)} = (0, 1, 0, 1, 0, 0), && f|_{\mathcal{O}_6(010111)} = (0, 1, 1, 1, 0, 1),
\end{aligned}$$

$$
\begin{aligned}
&f|_{\mathcal{O}_6(001001)} = (1,0,0), && f|_{\mathcal{O}_6(011011)} = (1,0,1),\\
&f|_{\mathcal{O}_6(000111)} = (0,1,0,0,1,1), && f|_{\mathcal{O}_6(011111)} = (1,1,1,1,0,1),\\
&f|_{\mathcal{O}_6(001011)} = (1,0,0,1,0,1), && f|_{\mathcal{O}_6(111111)} = (0),
\end{aligned}
$$

where the binary vectors on the right-hand side denote the truth tables of the restriction functions $f|_{\mathcal{O}_6(\Lambda_i)}$, $i = 1, \ldots, 14$, i.e.,

$$f|_{\mathcal{O}_6(\Lambda_i)} = \left(f(\Lambda_i), f \circ \rho_6^1(\Lambda_i), \ldots, f \circ \rho_6^{t_i-1}(\Lambda_i)\right),$$

where $t_i = |\mathcal{O}_6(\Lambda_i)|$. Since the function f satisfies the conditions in Theorem 2, then the RS $(6,6)$-function

$$F = \left(f, f \circ \rho_6^1, \ldots, f \circ \rho_6^5\right)$$

has perfect diffusion property. Due to Proposition 4, the iterated function $F^{(k)}$ is RS for $k \geqslant 2$. Let $f^{(k)} = f\left(F^{(k-1)}\right)$, then $F^{(k)} = \left(f^{(k)}, f^{(k)} \circ \rho_6^1, \ldots, f^{(k)} \circ \rho_6^5\right)$. By Proposition 1, the ANFs of the following Boolean functions can be obtained from the truth tables of f, $f^{(2)}$, $f^{(3)}$, $f^{(4)}$ respectively.

$$
\begin{aligned}
&f(x_1, \ldots, x_6)\\
=&x_1x_2x_3x_4x_5x_6 \oplus x_1x_2x_3x_4x_5 \oplus x_2x_3x_4x_5x_6 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5\\
&\oplus x_1x_2x_4x_5 \oplus x_1x_2x_4x_6 \oplus x_1x_2x_5x_6 \oplus x_1x_3x_4x_6 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4x_6\\
&\oplus x_2x_4x_5x_6 \oplus x_3x_4x_5x_6 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_3x_4 \oplus x_1x_3x_6 \oplus x_1x_5x_6\\
&\oplus x_3x_4x_5 \oplus x_3x_4x_6 \oplus x_4x_5x_6 \oplus x_4,\\
&f^{(2)}(x_1, \ldots, x_6)\\
=&x_1x_2x_3x_4x_5x_6 \oplus x_1x_2x_3x_5x_6 \oplus x_1x_2x_4x_5x_6 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3x_6\\
&\oplus x_1x_2x_4x_5 \oplus x_1x_3x_4x_6 \oplus x_2x_4x_5x_6 \oplus x_3x_4x_5x_6 \oplus x_1x_2x_3\\
&\oplus x_1x_3x_4 \oplus x_2x_4x_5 \oplus x_3x_4x_5 \oplus x_1,\\
&f^{(3)}(x_1, \ldots, x_6)\\
=&x_1x_2x_3x_4x_5x_6 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4x_6 \oplus x_1x_3x_4x_5x_6 \oplus x_2x_3x_4x_5x_6\\
&\oplus x_1x_2x_3x_5 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4x_6 \oplus x_1x_2x_5x_6 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_4x_6\\
&\oplus x_2x_3x_4x_5 \oplus x_2x_4x_5x_6 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_3x_4 \oplus x_1x_3x_6 \oplus x_1x_5x_6\\
&\oplus x_2x_3x_4 \oplus x_3x_4x_6 \oplus x_4x_5x_6 \oplus x_4,\\
&f^{(4)}(x_1, \ldots, x_6) = f^{(2)}(x_1, \ldots, x_6).
\end{aligned}
$$

The ANFs of the functions directly show that the RS $(6,6)$-function F has perfect diffusion property, and for every $k \geqslant 1$, $\mathrm{Deg}\left(F^{(k)}\right) = 6$.

3.2 Almost Balanced (n,n)-Functions with Perfect Diffusion Property

We have presented a construction of RS (n,n)-functions with perfect diffusion property. These functions are of interest from a practical point of view as their

representations are short and the evaluations are efficient. In this part, we propose a large set of almost balanced (n,n)-functions with perfect diffusion property. Here we call an (n,m)-function F *almost balanced*, if for every $b \in \mathbb{F}_{2^m}$, $|F^{-1}(b) - 2^{n-m}|$ takes a small value. For a finite set E with cardinality $|E| = N$, the set of all the permutations on E forms a symmetric group $\mathcal{S}_N$ whose group operation is the function composition.

Note that for $n \geqslant 2$, there is no balanced (n,n)-function (i.e., permutation on $\mathbb{F}_2^n$) with perfect diffusion property. In fact, let F be a permutation on $\mathbb{F}_2^n$, then since all the permutations on $\mathbb{F}_2^n$ form a finite symmetric group, there must exist some $i \geqslant 1$ such that $F^{(i)} = \mathrm{id}$, where id denotes the identity permutation. Hence, we have $F^{(i)}(x) = x$ for every $x \in \mathbb{F}_2^n$, which implies $\mathrm{D}_c\left(F^{(i)}\right) = 1/n < 1$. Thus, F cannot have perfect diffusion property. Therefore, finding almost balanced (n,n)-functions with perfect diffusion property is attractive.

Theorem 4. *For any σ that belongs to the symmetric group on the set $\mathbb{F}_2^n \setminus \{\mathbf{0},\mathbf{1}\}$, the almost balanced (n,n)-function*

$$F(x) = \begin{cases} \mathbf{0}, & x = \mathbf{0} \text{ or } \mathbf{1}, \\ \sigma(x), & \text{otherwise}, \end{cases} \tag{11}$$

has perfect diffusion property, and for every $k \geqslant 1$, $\mathrm{Deg}\left(F^{(k)}\right) = n$.

Proof. From Eq.(11), one gets that for any $k \geqslant 1$,

$$F^{(k)}(x) = \begin{cases} \mathbf{0}, & x = \mathbf{0} \text{ or } \mathbf{1}, \\ \sigma^{(k)}(x), & \text{otherwise}. \end{cases}$$

Since $\sigma^{(k)}$ is a permutation on $\mathbb{F}_2^n \setminus \{\mathbf{0},\mathbf{1}\}$, then it is easy to see that every coordinate function of $F^{(k)}$ has weight $2^{n-1}-1$, which implies from Proposition 1 and Theorem 1 that $\mathrm{Deg}\left(F^{(k)}\right) = n$ and $F^{(k)}$ is non-degenerate. Therefore, F has perfect diffusion property. □

The following enumeration result is obvious.

Theorem 5. *The number of distinct almost balanced (n,n)-functions constructed in Theorem 4 is $\mathcal{P}_n = (2^n-2)!$.*

Example 3. The number of almost balanced $(6,6)$-functions with perfect diffusion property constructed in Theorem 4 is $\mathcal{P}_6 = (2^6-2)! \approx 2^{284}$, compared with the enumeration result in Example 1 that the number of RS $(6,6)$-functions with perfect diffusion property constructed in Theorem 2 is $\mathcal{N}_6 \approx 2^{37.9}$.

Remark 4. Denote by $\mathscr{F}_n$, $\mathscr{G}_n$ the sets of all the (n,n)-functions constructed in Theorem 2 and Theorem 4 respectively. Then, it is easy to check that $\mathscr{F}_2 = \mathscr{G}_2$, $\mathscr{F}_3 \subseteq \mathscr{G}_3$, and for $n \geqslant 4$, $\mathscr{F}_n \bigcap \mathscr{G}_n \neq \emptyset$ but neither $\mathscr{F}_n \subseteq \mathscr{G}_n$ nor $\mathscr{G}_n \subseteq \mathscr{F}_n$.

As an application in product cryptosystems, we consider the following model.

Model. *Let G be an (n,n)-function, K_i, $i=0,1,\ldots$, be vectors in $\mathbb{F}_2^n$. Then, in a product cryptosystem, the i-th round function F_i is*

$$F_i(x)=\begin{cases} G(x\oplus K_0), & \text{if } i=1,\\ G(F_{i-1}(x)\oplus K_{i-1}), & \text{if } i\geqslant 2.\end{cases} \tag{12}$$

Suppose that $K_0=K_1=\cdots=K$, and we define $F(x)=G(x\oplus K)$. Then, by (12), we have for $i\geqslant 1$, $F_i(x)=F^{(i)}(x)$. The function F is preferable to have perfect diffusion property, which leads to $\mathrm{D}_c(F_i)=1$ for each $i\geqslant 1$. If the K_i's are not identical, then the case is more complicated. In the following, we use a simple example to illustrate that by using (n,n)-functions in (11), one can get $\mathrm{D}_c(F_i)=1$ for i odd. The example given here is suggestive if not very practical.

Example 4. In the above model, let

$$G(x)=\begin{cases}\mathbf{0}, & x=\mathbf{0} \text{ or } \mathbf{1},\\ \sigma(x), & otherwise,\end{cases}$$

be an almost balanced function in (11), where σ is a permutation on $E=\mathbb{F}_2^n\setminus\{\mathbf{0},\mathbf{1}\}$ satisfying $\{\mathbf{0},\mathbf{1}\}\bigcup U(\sigma)$ is a $\mathbb{F}_2$-subspace of $\mathbb{F}_2^n$, where $U(\sigma)=\{x\in E\mid \sigma(x)=x\}$ is the set of fixed points of σ. Let K_{i-1}, F_i, $i\geqslant 1$, be defined in (12). We now prove that if $U(\sigma)\neq\emptyset$ and for $i\geqslant 1$, $K_i\in U(\sigma)\setminus A_i$, where $A_1=\emptyset$ and

$$A_i=\left\{\bigoplus_{j=1}^{k}K_{i-j},\bigoplus_{j=1}^{k}K_{i-j}\oplus\mathbf{1}\;\middle|\;k=1,\ldots,i-1\right\},\quad i\geqslant 2,$$

then $\mathrm{Deg}(F_i)=n$ and $\mathrm{D}_c(F_i)=1$ for all odd i. One can easily check that for $i\geqslant 2$, A_i is a set, i.e., all the elements in A_i are distinct.

For $i\geqslant 1$, let $f_l^{(i)}$ be the l-th coordinate function of F_i, where $1\leqslant l\leqslant n$. It is clear that $\mathrm{wt}\left(f_l^{(1)}\right)=2^{n-1}-1$ which is odd, then from the proof of Theorem 4, we have $\mathrm{Deg}(F_1)=n$ and $\mathrm{D}_c(F_1)=1$. Moreover, there exist exactly two $x\in\mathbb{F}_2^n$ such that $F_1(x)=\mathbf{0}$, and for each $y\in E\setminus A_1$, there exists exactly one $x\in\mathbb{F}_2^n$ such that $F_1(x)=y$. By calculating iteratively, one can get that for every $i\geqslant 2$ and every $k=1,\ldots,i-1$, there exist exactly two $x\in\mathbb{F}_2^n$ such that $F_i(x)=\bigoplus_{j=1}^{k}K_{i-j}$ or $\mathbf{0}$, and for each $y\in E\setminus A_i$, there exists exactly one $x\in\mathbb{F}_2^n$ such that $F_i(x)=y$. Since for $i\geqslant 1$, $K_i\notin A_i$, then $K_i\oplus\mathbf{1}\in E\setminus A_i$, thus there exists exactly one $x\in\mathbb{F}_2^n$, denoted by $x_{i,0}$, such that $F_i(x_{i,0})=K_i\oplus\mathbf{1}$, which implies $G(F_i(x_{i,0})\oplus K_i)=\mathbf{0}$. Recall that $\{\mathbf{0},\mathbf{1}\}\bigcup U(\sigma)$ is a $\mathbb{F}_2$-subspace of $\mathbb{F}_2^n$, then for $i\geqslant 1$, since $K_i\in U(\sigma)$, we have $A_i\subseteq U(\sigma)$. From the above discussion, we obtain that for $i\geqslant 1$, the multiset $\{*\ G(F_i(x)\oplus K_i)\mid x\in\mathbb{F}_2^n\setminus\{x_{i,0}\}\ *\}$ is equal to the multiset $\{*\ F_i(x)\oplus K_i\mid x\in\mathbb{F}_2^n\setminus\{x_{i,0}\}\ *\}$. Hence, for $i\geqslant 1$, denote by $g_l^{(i)}$ the l-th coordinate function of $F_i(x)\oplus K_i$, where $1\leqslant l\leqslant n$, then we have

$$\mathrm{wt}\left(f_l^{(i+1)}\right)=\mathrm{wt}\left(g_l^{(i)}\right)-1.$$

It is obvious that wt $\left(f_l^{(i)}\right)$ and wt $\left(g_l^{(i)}\right)$ have the same parity, which leads to that wt $\left(f_l^{(i)}\right)$ and wt $\left(f_l^{(i+1)}\right)$ have different parities. Therefore, if $i \geqslant 1$ is odd, then wt $\left(f_l^{(i)}\right)$ is odd, thus we have $\mathrm{Deg}(F_i) = n$ and $\mathrm{D}_c(F_i) = 1$.

4 Concluding Remarks

In this paper, we construct two classes of (n, n)-functions with perfect diffusion property and optimal algebraic degree. These functions provide complete diffusion after iterations. The enumeration results for the constructed functions show that there are many (n, n)-functions which have perfect diffusion property.

The functions constructed in Theorem 2 and Theorem 4 represent a theoretical interest, which may have weak resistance to different cryptanalysis. Further improvements in the design of (n, n)-functions with perfect diffusion property are of interest. In addition, the RS (n, n)-functions defined in this paper may be worth discussing in the future for their efficient evaluations and short representations.

Acknowledgments. The authors would like to thank the anonymous referees for their helpful comments.

References

1. Bard, G.V.: Algebraic Cryptanalysis. Springer, New York (2009)
2. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. 4(1), 3–72 (1991)
3. Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Crama, Y., Hammer, P. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering. pp. 257–397. Cambridge University Press, London (2010)
4. Carlet, C.: Vectorial Boolean functions for cryptography. In: Crama, Y., Hammer, P. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering. pp. 398–469. Cambridge University Press, London (2010)
5. Courtois, N.T., Pieprzyk, J.: Cryptanalysis of block ciphers with overdefined systems of equations. In: Zheng, Y. (eds.) Advances in Cryptology—ASIACRYPT 2002. LNCS, vol. 2501, pp. 267–287. Springer, Heidelberg (2002)
6. Daemen, J.: Cipher and hash function design strategies based on linear and differential cryptanalysis. PhD thesis, Catholic University of Louvain (1995)
7. Feistel, H.: Cryptography and computer privacy. Sci. Am. 228(5), 15–23 (1973)
8. Fischer, S., Meier, W.: Algebraic immunity of S-boxes and augmented functions. In: Biryukov, A. (eds.) Fast Software Encryption, FSE 2007. LNCS, vol. 4593, pp. 366–381. Springer, Heidelberg (2007)
9. Forré, R.: Methods and instruments for designing S-boxes. J. Cryptol. 2(3), 115–130 (1990)
10. Kam, J.B., Davida, G.I.: Structured design of substitution-permutation encryption networks. IEEE Trans. Comput. C-28(10), 747–753 (1979)

11. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press, New York (1997)
12. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (eds.) Advances in Cryptology—EUROCRYPT'93. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
13. Maximov, A.: Classes of plateaued rotation symmetric Boolean functions under transformation of Walsh spectra. Cryptology ePrint Archive, Report 2004/354 (2004), https://eprint.iacr.org/2004/354
14. Pieprzyk, J., Qu, C.X.: Fast hashing and rotation-symmetric functions. J. Universal Comput. Sci. 5(1), 20–31 (1999)
15. Preneel, B., Bosselaers, A., Rijmen, V., et al.: Comments by the NESSIE project on the AES finalists (2000) http://www.nist.gov/aes
16. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. 28(4), 656–715 (1949)