On the diffusion property of iterated functions

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

[1]Tianjin University, China
[2]University of Paris VIII and University of Paris XIII
Department of mathematics,
LAGA (Laboratory Analysis, Geometry and Application), CNRS,
Telecom Paristech, France
[3]School of Mathematical Sciences, Nankai University, China

Fifteenth International Conference on Cryptography and Coding,
IMACC 2015
Oxford, United Kingdom
16th December 2015

Outline

1. **Background**
   - Boolean functions
   - Vectorial Boolean functions
2. **A perfect diffusion property**
   - Study of the degree of completeness
   - Some characterizations
3. **Constructions of vectorial Boolean functions with perfect diffusion property**
   - Rotation symmetric (n, n)-functions with perfect diffusion property
   - Almost balanced (n, n)-functions which have perfect diffusion property

Notation and preliminaries

$f : \mathbb{F}_2^n \to \mathbb{F}_2$ an n-variable Boolean function.
$\mathcal{B}_n := \{\mathbb{F}_2^n \to \mathbb{F}_2\}$.

- For $f \in \mathcal{B}_n$, the *support* of f is the set $\{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ and the *Hamming weight* of f is $\mathrm{wt}(f) = \left|\{x \in \mathbb{F}_2^n \mid f(x) = 1\}\right|$.
- 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.

Notation and preliminaries

Definition (Algebraic Normal Form (A.N.F))

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ *be a Boolean function. Then* f *can be expressed as :*

$$f(x_1, \ldots, x_n) = \bigoplus_{I \subset \{1,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u, a_I \in \mathbb{F}_2$$

where $I = \mathrm{supp}(u) = \{i = 1, \ldots, n \mid u_i = 1\}$ *and* $x^u = \prod_{i=1}^{n} x_i^{u_i}$.

The A.N.F exists and is unique.

Definition (The algebraic degree)

The algebraic degree $\deg(f)$ *is the degree of the A.N.F.*

Affine functions f $(\deg(f) \leq 1)$:

$$f(x) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n, \; a_i \in \mathbb{F}_2$$

- 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

$$\mathrm{D}_c(f) = |\mathcal{V}(f)|/n.$$

The degree of completeness

Vectorial Boolean functions or (n, m)*-functions* : functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. 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 $b \in \mathbb{F}_2^m$, $|F^{-1}(b)| = 2^{n-m}$.
- 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

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

  We have

$$\mathrm{D}_c(F) = (|\mathcal{V}(f_1)| + \cdots + |\mathcal{V}(f_m)|) \, / nm.$$

The degree of completeness

In this talk, we mainly discuss the measure D_c suggested by the NESSIE project [Prennel-Bosselaers-Rijmen 1999].

Definition

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 $\mathrm{D}_c(F)=1$, which provides the highest possible level of diffusion.

☞ Note that $\mathrm{D}_c(F)$ defined above 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, $\mathrm{D}_c^{min}(F)=1$ if and only if $\mathrm{D}_c(F)=1$. Hence, D_c^{min} is the strongest measure of completeness for vectorial Boolean functions.

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, 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 $\mathrm{D}_c(f) = 1 > \mathrm{D}_c(f \circ L) = 1/n$.

Perfect diffusion property

For a positive integer r, let $F^{(r)} = \overbrace{F \circ \cdots \circ F}^{r}$ denote the r-th iterated function of F.

Definition

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

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.

Remark

Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, Hence, 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 (1/2)

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*

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

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.*

Remark (2/2)

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.
The (n,n)*-function* F *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.*

Constructions of vectorial Boolean functions with perfect diffusion property

Our aim : construct classes of (n,n)-functions having perfect diffusion property.

- ☞ We provide two classes of (n,n)-functions which have perfect diffusion property. We shall enumerate the constructed functions are obtained.

1. First class : rotation symmetric (n,n)-functions which have perfect diffusion property ;
2. Second class : almost balanced (n,n)-functions which have perfect diffusion property.

Constructions of vectorial Boolean functions with perfect diffusion property

DEFINITION

A Boolean function f is rotation symmetric (RS) if it is invariant under the cyclic shift :

$$f(x_{n-1}, x_0, x_1, \ldots, x_{n-2}) = f(x_0, x_1, \ldots, x_{n-1}).$$

- RS structure allowed obtaining Boolean functions, with $n = 9, 11, 13$, improving the best known nonlinearities [Kavut-Maitra-Yücel, 2007].
- RS functions also have the interest of :
  1. needing less space to be stored
  2. allowing faster computation of the Walsh transform.

A first construction :

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 $\rho_n^0(x_1, x_2, \ldots, x_n) = (x_1, x_2, \ldots, x_n)$. We extend the notion of concept of rotation symmetric Boolean functions to (n, n)-functions :

Definition

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

$$F(x) = \left(f(x), f \circ \rho_n^1(x), f \circ \rho_n^2(x), \ldots, f \circ \rho_n^{n-1}(x)\right)\,. \tag{3}$$

Constructions of vectorial Boolean functions with perfect diffusion property

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 $l \geqslant 1$,

$$\begin{aligned} F \circ \rho_n^l(x) &= \left(f \circ \rho_n^l(x), f \circ \rho_n^{l+1}(x), \ldots, f \circ \rho_n^{l-1}(x)\right) \\ &= \rho_n^l \left(f(x), f \circ \rho_n^1(x), \ldots, f \circ \rho_n^{n-1}(x)\right) = \rho_n^l \circ F(x). \end{aligned} \tag{4}$$

An (n,n)-function F satisfying Eq.(4) is called *shift-invariant* [Daemen 1995]. An n-variable RS Boolean function f is defined as : $f \circ \rho_n^1(x) = f(x)$ for any $x \in \mathbb{F}_2^n$ [Pieprzyk-Qu 1999].

PROPOSITION

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

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

By induction on k, we obtain :

PROPOSITION

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

Note that from the previous propositions, one can see that rotation symmetric (n,n)-functions possess many desirable properties :

- the iterated functions are still rotation symmetric ;
- the evaluation of the functions is efficient (since a circular shift of the input bits leads to the corresponding shift of the output bits) ;
- the algebraic representations are short.

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

$$\mathcal{O}_n(x)=\left\{\rho_n^k(x_1,x_2,\ldots,x_n)\;\middle|\;0\leqslant k\leqslant n-1\right\}. \tag{5}$$

- The cardinality of an orbit generated by $x=(x_1,\ldots,x_n)$ is a factor of n.
- All the orbits generate a partition of $\mathbb{F}_2^n$.
- 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.
- Every orbit can be represented by its lexicographically first element, called the *representative element*.

Constructions of vectorial Boolean functions with perfect diffusion property

Let $\{\Lambda_1^{(n)}, \Lambda_2^{(n)}, \ldots, \Lambda_{\Psi_n}^{(n)}\}$ 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 (for short) we use the notation : $\{\Lambda_1, \Lambda_2, \ldots, \Lambda_{\Psi_n}\}$.
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 $x \in \mathcal{O}_n(\Lambda_i)$, $f|_{\mathcal{O}_n(\Lambda_i)}(x) = f(x)$.

THEOREM (MAIN RESULT 1)

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 $k \geqslant 1$, $\mathrm{Deg}\left(F^{(k)}\right) = n$.

Using the following result :

LEMMA (MAXIMOV 2004)

The number of orbits with t elements in $\mathbb{F}_2^n$ of weight w is

$$\eta_{n,t,w} = \begin{cases} \frac{1}{t}\sum_{k|t,q_k|w} \mu(t/k)\cdot\binom{n/q_k}{w/q_k}, & \text{for } t,w=1,\ldots,n, \text{ where } q_k = \frac{n}{\gcd(n,k)}, \\ 1, & \text{for } t=1, w=0, \\ 0, & \text{otherwise}, \end{cases} \tag{6}$$

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 $t=p_1p_2\cdots p_m$, where $p_1,\ldots,p_m$ are distinct primes ; $\mu(t)=0$, for all other cases.

We prove

Theorem

The number of distinct RS (n, n)-functions constructed in the first construction is

$$\mathcal{N}_n = \prod_{w=1}^{n-1} \prod_{t=1}^{n} \binom{t}{\frac{t \cdot w}{n}}^{\eta_{n,t,w}}, \tag{7}$$

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.*

Example (1/3) :
For $\mathbb{F}_2^6$, all the orbits are listed in the table below, where t and w are respectively the number and the weight of elements in an orbit.

TABLE: All the orbits of $\mathbb{F}_2^6$

	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

Example (2/3) : The values of $\eta_{6,t,w}$ are listed in the table below, where t and w are respectively the number and the weight of elements in an orbit.

TABLE: All the values of $\eta_{6,t,w}$

$\eta_{6,t,w}$	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

Example (3/3) : Then, from the previous theorem 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 $2^{2^6 \cdot 6} = 2^{384}$.

Construction 2 :

Definition

An (n,m)-function F is 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, if F is a permutation on $\mathbb{F}_2^n$, then F cannot have perfect diffusion property. Therefore, finding almost balanced (n,n)-functions with perfect diffusion property is attractive.

Constructions of vectorial Boolean functions with perfect diffusion property

THEOREM (MAIN RESULT 2)

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

$$F(x) = \begin{cases} \mathbf{0}, & x = \mathbf{0} \text{ or } \mathbf{1}, \\ \sigma(x), & otherwise, \end{cases} \tag{8}$$

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

Moreover, we have the following enumeration result :

THEOREM

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

EXAMPLE

The number of almost balanced $(6, 6)$-functions with perfect diffusion property constructed in the second construction is $\mathcal{P}_6 = (2^6 - 2)! \approx 2^{284}$.

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*

$$F_i(x) = \begin{cases} G(x \oplus K_0), & \text{if } i = 1, \\ G(F_{i-1}(x) \oplus K_{i-1}), & \text{if } i \geqslant 2. \end{cases} \tag{9}$$

Suppose that $K_0 = K_1 = \cdots = K$, and we define $F(x) = G(x \oplus K)$. Then, by (9), 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.

An application

Here we use a simple example to illustrate that by using (n,n)-functions, one can get $\mathrm{D}_c(F_i)=1$ for i odd.

Example

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 (8), 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 (9). We can 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

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

then $\mathrm{Deg}(F_i)=n$ and $\mathrm{D}_c(F_i)=1$ for all odd i.

Conclusion

For vectorial Boolean functions, the behavior of iteration has consequence in the diffusion property of the system.

- We have presented a study on the diffusion property of iterated vectorial Boolean functions. The measure of the diffusion property here is related to the notion of the degree of completeness.
- We have provided the first two constructions of (n, n)-functions having perfect diffusion property and optimal algebraic degree.
- We also obtained the complete enumeration results for the constructed functions.

The functions constructed represent a theoretical interest, which may have weak resistance to different cryptanalysis.