A Class of Weightwise Almost Perfectly Balanced Boolean Functions

Deepak Kumar Dalai, **Krishna Mallick**

School of Computer Sciences
National Institute of Science Education and Research
Bhubaneswar

Outline

- Introduction to Boolean function.
- Motivation: Impact of FLIP, a new stream cipher over the study of Boolean functions.
- Constructions of Boolean functions in the framework of FLIP.

Introduction to Boolean Function

A Boolean function of n-variable is a map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.

- $\mathcal{B}_n$: set of all n-variable Boolean functions.
  Cardinality of $\mathcal{B}_n = 2^{2^n}$
- A basic representation is Truth Table.

$x \in \mathbb{F}_2^n$	$f(x)$
$00\ldots0$	$f(00\ldots0)$
$00\ldots1$	$f(00\ldots1)$
$\vdots$	$\vdots$
$11\ldots1$	$f(11\ldots1)$

The output of the truth table of length 2^n,

$$f = [f(00\ldots0), f(00\ldots1), \ldots, f(11\ldots1)]$$

Representation of a Boolean Function: Algebraic normal form (ANF)

Let $f \in \mathcal{B}_n$. Then f can be expressed as:

$$f(x) = \bigoplus_{I \subseteq \{1,2,\ldots,n\}} a_I \left(\prod_{i \in I} x_i\right)$$

$$= a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1 \leq i < j \leq n} a_{i,j} x_i x_j + \cdots + a_{1,2,\ldots,n} x_1 x_2 \ldots x_n$$

where $a_0, a_i, a_{i,j}, \ldots, a_{1,2,\ldots,n} \in \mathbb{F}_2$.
This implies, $f(x) \in \mathbb{F}_2[x_1, x_2, \ldots, x_n] / < x_1^2 + x_1, \ldots, x_n^2 + x_n >$.

Introduction to Boolean function (cont.).

$\{1, 2, \ldots, n\} := [n]$.

- The Hamming weight of $x \in \mathbb{F}_2^n$ is $w_H(x) = |\{i \in [n] : x_i \neq 0\}|$.

Introduction to Boolean function (cont.).

$\{1, 2, \ldots, n\} := [n]$.

- The Hamming weight of $x \in \mathbb{F}_2^n$ is $w_H(x) = |\{i \in [n] : x_i \neq 0\}|$.
- The support of f, $sup(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$.

Introduction to Boolean function (cont.).

$\{1, 2, \ldots, n\} := [n]$.

- The Hamming weight of $x \in \mathbb{F}_2^n$ is $w_H(x) = |\{i \in [n] : x_i \neq 0\}|$.
- The support of f, $sup(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$.
- The algebraic degree of f, denoted by $deg(f)$ is the number of variables in the highest order monomial with non-zero coefficient .

Introduction to Boolean function (cont.).

$\{1, 2, \ldots, n\} := [n]$.

- The Hamming weight of $x \in \mathbb{F}_2^n$ is $w_H(x) = |\{i \in [n] : x_i \neq 0\}|$.
- The support of f, $sup(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$.
- The algebraic degree of f, denoted by $deg(f)$ is the number of variables in the highest order monomial with non-zero coefficient .
- Let $f, g \in \mathcal{B}_n$. The Hamming distance between f and g is $d_H(f, g) = |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}|$.

Introduction to Boolean function (cont.).

$\{1, 2, \ldots, n\} := [n]$.

- The Hamming weight of $x \in \mathbb{F}_2^n$ is $w_H(x) = |\{i \in [n] : x_i \neq 0\}|$.
- The support of f, $sup(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$.
- The algebraic degree of f, denoted by $deg(f)$ is the number of variables in the highest order monomial with non-zero coefficient .
- Let $f, g \in \mathcal{B}_n$. The Hamming distance between f and g is $d_H(f, g) = |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}|$.
- A function $f \in \mathcal{B}_n$ is balanced if $w_H(f) = 2^{n-1}$.

Nonlinearity.

- The nonlinearity of f denoted by $nl(f)$ is

$$nl(f) = \min_{l_{\boldsymbol{a},\boldsymbol{b}}(x) \in \mathcal{A}_{\boldsymbol{n}}} d_H(f(x), l_{a,b}(x))$$

where, $\mathcal{A}_n = \{l_{a,b} \in \mathcal{B}_n : l_{a,b}(x) = a.x + b; a \in \mathbb{F}_2^n, b \in \mathbb{F}_2\}$ is the set of all affine functions on $\mathbb{F}_2^n$.

Nonlinearity.

- The nonlinearity of f denoted by $nl(f)$ is

$$nl(f) = \min_{l_{\boldsymbol{a},\boldsymbol{b}}(x) \in \mathcal{A}_{\boldsymbol{n}}} d_H(f(x), l_{a,b}(x))$$

  where, $\mathcal{A}_n = \{l_{a,b} \in \mathcal{B}_n : l_{a,b}(x) = a.x + b; a \in \mathbb{F}_2^n, b \in \mathbb{F}_2\}$ is the set of all affine functions on $\mathbb{F}_2^n$.

- The upper bound of nonlinearity is,

$$nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Nonlinearity.

- The nonlinearity of f denoted by $nl(f)$ is

$$nl(f) = \min_{l_{a,b}(x) \in \mathcal{A}_n} d_H(f(x), l_{a,b}(x))$$

where, $\mathcal{A}_n = \{l_{a,b} \in \mathcal{B}_n : l_{a,b}(x) = a.x + b; a \in \mathbb{F}_2^n, b \in \mathbb{F}_2\}$ is the set of all affine functions on $\mathbb{F}_2^n$.

- The upper bound of nonlinearity is,

$$nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

- $f \in \mathcal{B}_n$ (n is even). If the $nl(f)$ reaches the upper bound i.e.

$$nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1},$$

then f is called a bent function.

Motivation

- A new stream cipher FLIP has been introduced by Méaux et al. [2] in 2016. The Boolean function used in FLIP, is restricted to $E_{n,\frac{n}{2}} = \{x \in \mathbb{F}_2^n : w_H(x) = \frac{n}{2}\} \subset \mathbb{F}_2^n$.

Motivation

- A new stream cipher FLIP has been introduced by Méaux et al. [2] in 2016. The Boolean function used in FLIP, is restricted to $E_{n,\frac{n}{2}} = \{x \in \mathbb{F}_2^n : w_H(x) = \frac{n}{2}\} \subset \mathbb{F}_2^n$.
- In classical stream cipher, the inputs to f reaches all the elements in $\mathbb{F}_2^n$. So, all the security analysis has been studied for f is over $\mathbb{F}_2^n$.

Motivation

- A new stream cipher FLIP has been introduced by Méaux et al. [2] in 2016. The Boolean function used in FLIP, is restricted to $E_{n,\frac{n}{2}} = \{x \in \mathbb{F}_2^n : w_H(x) = \frac{n}{2}\} \subset \mathbb{F}_2^n$.
- In classical stream cipher, the inputs to f reaches all the elements in $\mathbb{F}_2^n$. So, all the security analysis has been studied for f is over $\mathbb{F}_2^n$.
- If the inputs of $f \in \mathcal{B}_n$ are restricted to some vectors with constant w_H, then the security analysis does not depend on the criteria defined for f over $\mathbb{F}_2^n$.

Motivation

- A new stream cipher FLIP has been introduced by Méaux et al. [2] in 2016. The Boolean function used in FLIP, is restricted to $E_{n,\frac{n}{2}} = \{x \in \mathbb{F}_2^n : w_H(x) = \frac{n}{2}\} \subset \mathbb{F}_2^n$.
- In classical stream cipher, the inputs to f reaches all the elements in $\mathbb{F}_2^n$. So, all the security analysis has been studied for f is over $\mathbb{F}_2^n$.
- If the inputs of $f \in \mathcal{B}_n$ are restricted to some vectors with constant w_H, then the security analysis does not depend on the criteria defined for f over $\mathbb{F}_2^n$.
- Let $\mathcal{E}$ be a family of subsets of $\mathbb{F}_2^n$ i.e. $\mathcal{E} = \{E_{n,0}, E_{n,1}, \ldots, E_{n,n}\}$, where $E_{n,k} = \{x \in \mathbb{F}_2^n : w_H(x) = k\}$. So, it is required to construct functions that are balanced over $E_{n,k}, \forall k \in [n]$.

Weightwise almost perfectly balanced (WAPB) Boolean function.

- Support of f restricted to $E_{n,k}$ is $sup(f)_k = \{x \in \mathbb{F}_2^n : w_H(x) = k, f(x) = 1\}$.

Weightwise almost perfectly balanced (WAPB) Boolean function.

- Support of f restricted to $E_{n,k}$ is $sup(f)_k = \{x \in \mathbb{F}_2^n : w_H(x) = k, f(x) = 1\}$.
- Hamming weight of f restricted to $E_{n,k}$ is $w_H(f)_k = |sup(f)_k|$.

Weightwise almost perfectly balanced (WAPB) Boolean function.

- Support of f restricted to $E_{n,k}$ is $sup(f)_k = \{x \in \mathbb{F}_2^n : w_H(x) = k, f(x) = 1\}$.
- Hamming weight of f restricted to $E_{n,k}$ is $w_H(f)_k = |sup(f)_k|$.

Definition ([1])

$f \in \mathcal{B}_n$ is said to be weightwise almost perfectly balanced function (WAPB), if $\forall k \in \{1, 2, \ldots, n-1\}$,

$$w_H(f)_k = \begin{cases} \frac{\binom{n}{k}}{2}; & \binom{n}{k} \text{ even }, \\ \frac{\binom{n}{k} \pm 1}{2}; & \binom{n}{k} \text{ odd }. \end{cases}$$

Weightwise almost perfectly balanced (WAPB) Boolean function.

- Support of f restricted to $E_{n,k}$ is $sup(f)_k = \{x \in \mathbb{F}_2^n : w_H(x) = k, f(x) = 1\}$.
- Hamming weight of f restricted to $E_{n,k}$ is $w_H(f)_k = |sup(f)_k|$.

Definition ([1])

$f \in \mathcal{B}_n$ is said to be weightwise almost perfectly balanced function (WAPB), if $\forall k \in \{1, 2, \ldots, n-1\}$,

$$w_H(f)_k = \begin{cases} \frac{\binom{n}{k}}{2}; & \binom{n}{k} \text{ even }, \\ \frac{\binom{n}{k} \pm 1}{2}; & \binom{n}{k} \text{ odd }. \end{cases}$$

Definition ([1])

$f \in \mathcal{B}_n$ is said to be weightwise perfectly balanced (WPB) if f is balanced over $E_{n,k}$, for all $k \in \{1, 2, \ldots, n-1\}$ i.e., $w_H(f)_k = \frac{\binom{n}{k}}{2}$.

Nonlinearity over $E_{n,k}$ (defined in [1]).

The non-linearity of $f \in \mathcal{B}_n$ over $E_{n,k}$ is,

$$nl_{E_{\boldsymbol{n},\boldsymbol{k}}}(f) = min_{l_{\boldsymbol{a},\boldsymbol{b}}(x) \in \mathcal{A}_{\boldsymbol{n}}} d_H(f(x), l_{a,b}(x)).$$

Nonlinearity over $E_{n,k}$ (defined in [1]).

The non-linearity of $f \in \mathcal{B}_n$ over $E_{n,k}$ is,

$$nl_{E_{n,k}}(f) = min_{l_{a,b}(x) \in \mathcal{A}_n} d_H(f(x), l_{a,b}(x)).$$

By computing, we have

$$nl_{E_{n,k}}(f) = \frac{|E_{n,k}|}{2} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |\sum_{x \in E_{n,k}} (-1)^{f(x)+a.x}|; \quad a \in \mathbb{F}_2^n.$$

Nonlinearity over $E_{n,k}$ (defined in [1]).

The non-linearity of $f \in \mathcal{B}_n$ over $E_{n,k}$ is,

$$nl_{E_{n,k}}(f) = min_{l_{a,b}(x) \in \mathcal{A}_n} d_H(f(x), l_{a,b}(x)).$$

By computing, we have

$$nl_{E_{n,k}}(f) = \frac{|E_{n,k}|}{2} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |\sum_{x \in E_{n,k}} (-1)^{f(x)+a.x}|; \quad a \in \mathbb{F}_2^n.$$

The upper bound of nonlinearity over $E_{n,k}$ is

$$nl_{E_{n,k}}(f) \leq \frac{1}{2}\left[|E_{n,k}| - \sqrt{|E_{n,k}|}\right]$$

where $|E_{n,k}| = \binom{n}{k}$.

Literature in WAPB Boolean function construction.

$(x_1, x_2, \ldots, x_n) := X_n$.

Proposition (Carlet et al.,2017 [1])

Let $f_n \in \mathcal{B}_n$ for $n \geq 3$, be defined by

$$f_n(X_n) = \begin{cases} f_{n-1}(X_{n-1}) & \text{if } n \text{ is odd}, \\ f_{n-1}(X_{n-1}) + x_{n-2} + \prod_{i=1}^{2^{d-1}} x_{n-i} & \text{if } n = 2^d; d > 1, \\ f_{n-1}(X_{n-1}) + x_{n-2} + \prod_{i=1}^{2^d} x_{n-i} & \text{if } n = p.2^d; p > 1 \text{ odd}; d \geq 1. \end{cases}$$

where $f_2(x_1, x_2) = x_1$, is a WAPB Boolean function.

Literature in WAPB Boolean function construction.

Proposition (Linya Zhu, Sihong Su, 2022[4])

Let $n = n_1 + n_2 + \cdots + n_p$ *for* n_i *being the power of 2 for* $1 \leq i \leq p$ *and* $0 < n_1 < n_2 < \cdots < n_p$. *Let* $f_{n_i} \in \mathcal{B}_{n_i}$ *be WPB with* $f_{n_i}(0, 0, \ldots, 0) = 0$, $f_{n_i}(1, 1, \ldots, 1) = 1$ *for* $1 \leq i \leq p$. *Then* $h \in \mathcal{B}_n$ *defined as*

$$h_n(x_1, x_2, \ldots, x_n) = f_{n_1}(x_1, x_2, \ldots, x_{n_1}) + f_{n_2}(x_{n_1+1}, x_{n_1+2}, \ldots, x_{n_1+n_2}) + \cdots + f_{n_p}(x_{n-n_p+1}, x_{n-n_p+2}, \ldots, x_n)$$

is WAPB.

A WPB construction by Mesnager and Su [3].

Given a positive integer m, a $sup(f_m)$ for $f \in \mathcal{B}_{2^m}$ is defined as:

$$sup(f_m) = \triangle_{i=1}^{m}\{(x, y, x, y, \ldots, x, y) \in \mathbb{F}_2^{2^m} : x, y \in \mathbb{F}_2^{2^{m-i}}, \\ w_H(x) \text{ is odd}\}$$

Lemma (Mesnager, Su 2021 [3])

The $sup(f_m)$ can also be written as

$$sup(f_m) = \begin{cases} \{(x, y) : x = 1, y \in \mathbb{F}_2\}; & m = 1 \\ \{(x, y) : x, y \in \mathbb{F}_2^{2^{m-1}}, w_H(x) \text{ is odd}\} & \\ \qquad \triangle\{(x, x) : x \in sup(f_{m-1})\}; & m \geq 2 \end{cases}$$

The function f_m with this defined $supp(f_m)$ is weightwise perfectly balanced.

Constructions of WAPB Boolean functions.

Lemma

Let $n > 1$ be an odd integer and $g, h \in \mathcal{B}_{n-1}$ be two WAPB Boolean functions. Then $f \in \mathcal{B}_n$ defined as

$$f(x_1, x_2, \ldots, x_n) = (1 + x_n)g(x_1, x_2, \ldots, x_{n-1}) + x_n h(x_1, x_2, \ldots, x_{n-1})$$

i.e., $\mathtt{sup}(f) = \{(x, 0) \in \mathbb{F}_2^n : x \in \mathtt{sup}(g)\} \cup \{(y, 1) \in \mathbb{F}_2^n : y \in \mathtt{sup}(h)\}$

is a WAPB Boolean function.

Constructions of WAPB Boolean functions.

Lemma

Let $n > 1$ be an odd integer and $g, h \in \mathcal{B}_{n-1}$ be two WAPB Boolean functions. Then $f \in \mathcal{B}_n$ defined as

$$f(x_1, x_2, \ldots, x_n) = (1 + x_n)g(x_1, x_2, \ldots, x_{n-1}) + x_n h(x_1, x_2, \ldots, x_{n-1})$$

i.e., $\mathtt{sup}(f) = \{(x, 0) \in \mathbb{F}_2^n : x \in \mathtt{sup}(g)\} \cup \{(y, 1) \in \mathbb{F}_2^n : y \in \mathtt{sup}(h)\}$

is a WAPB Boolean function.

Corollary

Let $n = 2^m \geq 2$ and $g, h \in \mathcal{B}_n$ be two WPB Boolean functions. Then $f \in \mathcal{B}_{n+1}$ such that

$$f(x_1, x_2, \ldots, x_{n+1}) = (1 + x_{n+1})g(x_1, x_2, \ldots, x_n) + x_{n+1} h(x_1, x_2, \ldots, x_n)$$

is a WAPB Boolean function.

Constructions of WAPB Boolean functions: Cont.

Lemma

Let $n = n_0 2^m$ where n_0 be an odd positive integer and $m \geq 0$ be an integer. Let $f_{n_0} \in \mathcal{B}_{n_0}$ be a WAPB Boolean function. Then $f_n \in \mathcal{B}_n$, recursively defined as

$$\mathtt{sup}(f_n) = \begin{cases} \mathtt{sup}(f_{n_0}) & \text{if } n = n_0 \text{ is odd }, \\ \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}\} \triangle & \\ \qquad \{(z,z) \in \mathbb{F}_2^n : z \in \mathtt{sup}(f_{\frac{n}{2}})\}, & \text{if } n \text{ is even}, \end{cases}$$

is a WAPB Boolean function.

Constructions of WAPB Boolean functions: Cont.

Theorem

For $n \geq 2$, the support of an n variable Boolean function is defined as

$$\mathtt{sup}(f_n) = \begin{cases} \{(x,1) \in \mathbb{F}_2^2 : x \in \mathbb{F}_2\} = \{(0,1),(1,1)\} & \text{if } n = 2, \\ \{(x,0) \in \mathbb{F}_2^n : x \in \mathtt{sup}(f_{n-1})\} \cup & \\ \quad \{(x,1) \in \mathbb{F}_2^n : x \notin \mathtt{sup}(f_{n-1})\} & \text{if } n > 2 \text{ and odd}, \\ \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}\} \triangle & \\ \quad \{(z,z) \in \mathbb{F}_2^n : z \in \mathtt{sup}(f_{\frac{n}{2}})\}, & \text{if } n > 2 \text{ and even}, \end{cases}$$

is a WAPB Boolean function.

Theorem

For $p \geq 2$, let f_p be a WAPB Boolean function. Let n be a positive integer such that, for a $m \geq 0$,

- $p = \lfloor \frac{n}{2^m} \rfloor$ *i.e,* $n = a_0 2^0 + a_1 2^1 + \cdots + a_{m-1} 2^{m-1} + p 2^m$

  or,

- $p + 1 = \lfloor \frac{n}{2^m} \rfloor$

  i.e, $n = a_0 2^0 + a_1 2^1 + \cdots + a_{m-1} 2^{m-1} + (p+1) 2^m$ *, if p is even.*

Then $f_n \in \mathcal{B}_n$ whose support is defined as

$$\mathrm{sup}(f_n) = \begin{cases} \mathrm{sup}(f_p) & \text{if } n = p, \\ \{(x,0) \in \mathbb{F}_2^n : x \in \mathrm{sup}(f_{n-1})\} & \\ \quad \cup \{(x,1) \in \mathbb{F}_2^n : x \notin \mathrm{sup}(f_{n-1})\} & \text{if } n > p \text{ and odd}, \\ \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathrm{wt}(x) \text{ is odd}\} & \\ \quad \triangle \{(z,z) \in \mathbb{F}_2^n : z \in \mathrm{sup}(f_{\frac{n}{2}})\} & \text{if } n > p \text{ and even} \end{cases}$$

is a WAPB Boolean function.

- Hence, if we have a WAPB function of 5 variables, then we can construct a WAPB Boolean function of variable 10, 11, 20, 21, 22, 23 , 40, 41,..so on.

- Hence, if we have a WAPB function of 5 variables, then we can construct a WAPB Boolean function of variable 10, 11, 20, 21, 22, 23 , 40, 41,..so on.

- The ANF of f_n, defined in the above Theorem is

$$f_n(X_n) = \begin{cases} f_p & \text{if } n = p, \\ x_n + f_{n-1}(X_{n-1}) & \text{if } n > p \text{ and odd}, \\ \sum_{i=1}^{\frac{n}{2}} x_i + f_{\frac{n}{2}}(X_{\frac{n}{2}}) \prod_{i=1}^{\frac{n}{2}} (x_i + x_{\frac{n}{2}+i} + 1) & \text{if } n > p \text{ and even} \end{cases}$$

  is a WAPB Boolean function.

Nonlinearity of this construction.

Lemma

Let $n > 0$ be an even integer and $f_n \in \mathcal{B}_n$ such that

$$\mathtt{sup}(f_n) = \{(x, y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}\} \triangle \{(z, z) \in \mathbb{F}_2^n : z \in \mathtt{sup}(f_{\frac{n}{2}})\}$$

where $f_{\frac{n}{2}} \in \mathcal{B}_{\frac{n}{2}}$. Then $\mathtt{nl}(f_n) \leq \mathtt{wt}(f_{\frac{n}{2}})$.

Nonlinearity of this construction.

Lemma

Let $n > 0$ be an even integer and $f_n \in \mathcal{B}_n$ such that

$$\mathtt{sup}(f_n) = \{(x, y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}\} \triangle \{(z, z) \in \mathbb{F}_2^n : z \in \mathtt{sup}(f_{\frac{n}{2}})\}$$

where $f_{\frac{n}{2}} \in \mathcal{B}_{\frac{n}{2}}$. Then $\mathtt{nl}(f_n) \leq \mathtt{wt}(f_{\frac{n}{2}})$.

The following table presents the nonlinearity and weight nonlinearity of the functions for $n = 10, 11, 12, 13, 14$.

n	$\mathtt{nl}$	$\mathtt{nl}_2$	$\mathtt{nl}_3$	$\mathtt{nl}_4$	$\mathtt{nl}_5$	$\mathtt{nl}_6$	$\mathtt{nl}_7$	$\mathtt{nl}_8$	$\mathtt{nl}_9$	$\mathtt{nl}_{10}$	$\mathtt{nl}_{11}$	$\mathtt{nl}_{12}$	$\mathtt{nl}_{13}$
10	16	3	0	5	0	5	0	3	0	0	–	–	–
11	32	3	3	5	5	5	5	3	3	0	0	–	–
12	32	3	0	7	0	10	0	8	0	3	0	0	–
13	64	3	3	7	7	10	10	8	8	3	3	0	0
14	64	4	0	10	0	18	0	18	0	10	0	4	0

Weightwise Nonlinearity

For $n = 6$,

Construction	nl	nl_1	nl_2	nl_3	nl_4	nl_5
$\frac{1}{2}\left[\lvert E_{6,k}\rvert - \sqrt{\lvert E_{6,k}\rvert}\right]$	-	1	5	7	5	1
Carlet et al.,2017		0	2	4	2	0
Zhu and Su, 2022		0	1	4	1	0
Our		0	2	0	2	0

References.

[1] Claude Carlet, Pierrick Méaux, and Yann Rotella. Boolean functions with restricted input and their robustness; application to the flip cipher. *Cryptology ePrint Archive*, 2017.

[2] Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet. Towards stream ciphers for efficient fhe with low-noise ciphertexts. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 311–343. Springer, 2016.

[3] Sihem Mesnager and Sihong Su. On constructions of weightwise perfectly balanced boolean functions. *Cryptography and Communications*, 13(6):951–979, 2021.

[4] Linya Zhu and Sihong Su. A systematic method of constructing weightwise almost perfectly balanced boolean functions on an arbitrary number of variables. *Discrete Applied Mathematics*, 314:181–190, 2022.

Thank You