A Class of Weightwise Almost Perfectly Balanced Boolean Functions with High Weightwise Nonlinearity

Deepak Kumar Dalai[1], **Krishna Mallick**[2]

[1]School of Mathematical Sciences,
[2]School of Computer Sciences,
National Institute of Science Education and Research,
An OCC of Homi Bhabha National Institute,
Bhubaneswar, Odisha 752050, India

The 8th International Workshop on Boolean Functions and their Applications (BFA) 2023
04.09.2023

Outline

- Introduction to Boolean function.
- Motivation: Impact of FLIP, a new stream cipher over the study of Boolean functions.
- Construction of Boolean functions with high nonlinearity and weightwise nonlinearity.

Introduction to Boolean Function

A n-variable Boolean function 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 is a 2^n-tuple vector,

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

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

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

$$\begin{aligned} f(x) &= \bigoplus_{I \subseteq \{1,2,\ldots,n\}} a_I (\prod_{i \in I} x_i) \\ &= a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1 \leq i < j \leq n} a_{i,j} x_i x_j + \cdots + a_{1,2,\ldots,n} x_1 x_2 \ldots x_n \end{aligned}$$

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 $wt(x) = |\{i \in [n] : x_i \neq 0\}|$.

Introduction to Boolean function (cont.).

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

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

Introduction to Boolean function (cont.).

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

- The Hamming weight of $x \in \mathbb{F}_2^n$ is $wt(x) = |\{i \in [n] : x_i \neq 0\}|$.
- The support of f, $sup(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. The Hamming weight of f is $wt(f) = |sup(f)|$.
- 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 $wt(x) = |\{i \in [n] : x_i \neq 0\}|$.
- The support of f, $sup(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. The Hamming weight of f is $wt(f) = |sup(f)|$.
- 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 $wt(x) = |\{i \in [n] : x_i \neq 0\}|$.
- The support of f, $sup(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. The Hamming weight of f is $wt(f) = |sup(f)|$.
- 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 $wt(f) = 2^{n-1}$.

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 $\mathbb{F}_2^n$.

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,

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

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.

Algebraic Immunity

- Given $f \in \mathcal{B}_n$, a nonzero $g \in \mathcal{B}_n$ is called an annihilator of f if $f.g = 0$, i.e., $f(x)g(x) = 0$ for all $x \in \mathbb{F}_2^n$.

Algebraic Immunity

- Given $f \in \mathcal{B}_n$, a nonzero $g \in \mathcal{B}_n$ is called an annihilator of f if $f.g = 0$, i.e., $f(x)g(x) = 0$ for all $x \in \mathbb{F}_2^n$.
- The set of all annihilators of $f \in \mathcal{B}_n$ is denoted by $An(f)$. The algebraic immunity of $f \in \mathcal{B}_n$ is defined as

$$\mathtt{AI}(f) = \min\{\deg(g) : g \in An(f) \cup An(1+f)\}.$$

Algebraic Immunity

- Given $f \in \mathcal{B}_n$, a nonzero $g \in \mathcal{B}_n$ is called an annihilator of f if $f.g = 0$, i.e., $f(x)g(x) = 0$ for all $x \in \mathbb{F}_2^n$.
- The set of all annihilators of $f \in \mathcal{B}_n$ is denoted by $An(f)$. The algebraic immunity of $f \in \mathcal{B}_n$ is defined as

$$\mathtt{AI}(f) = \min\{\deg(g) : g \in An(f) \cup An(1+f)\}.$$

- Majority function has highest AI.

Motivation

- A new stream cipher FLIP has been introduced by Méaux et al. [6] in 2016. The Boolean function used in FLIP, is restricted to $E_{n,\frac{n}{2}} = \{x \in \mathbb{F}_2^n : wt(x) = \frac{n}{2}\} \subset \mathbb{F}_2^n$.

Motivation

- A new stream cipher FLIP has been introduced by Méaux et al. [6] in 2016. The Boolean function used in FLIP, is restricted to $E_{n,\frac{n}{2}} = \{x \in \mathbb{F}_2^n : wt(x) = \frac{n}{2}\} \subset \mathbb{F}_2^n$.
- If the inputs of $f \in \mathcal{B}_n$ are restricted to some vectors with constant wt, then the security analysis does not depend on the criteria defined for f over $\mathbb{F}_2^n$.

  Symmetric bent function, majority function over $E_{n,k}$ behaves like a constant function.

Motivation

- A new stream cipher FLIP has been introduced by Méaux et al. [6] in 2016. The Boolean function used in FLIP, is restricted to $E_{n,\frac{n}{2}} = \{x \in \mathbb{F}_2^n : wt(x) = \frac{n}{2}\} \subset \mathbb{F}_2^n$.
- If the inputs of $f \in \mathcal{B}_n$ are restricted to some vectors with constant wt, then the security analysis does not depend on the criteria defined for f over $\mathbb{F}_2^n$.

  Symmetric bent function, majority function over $E_{n,k}$ behaves like a constant function.
- 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 $E_{n,k} = \{x \in \mathbb{F}_2^n : wt(x) = k\}$. So, it is required to construct functions that are balanced over $E_{n,k}, \forall k \in [n]$ with high nonlinearity and algebraic immunity over $E_{n,k}$.

Weightwise almost perfectly balanced (WAPB) Boolean function.

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

Weightwise almost perfectly balanced (WAPB) Boolean function.

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

Weightwise almost perfectly balanced (WAPB) Boolean function.

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

Definition ([1])

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

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

Weightwise almost perfectly balanced (WAPB) Boolean function.

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

Definition ([1])

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

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

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 $k \in \{1, 2, \dots, n-1\}$ i.e., $wt_k(f) = \frac{\binom{n}{k}}{2}$.

Nonlinearity over $E_{n,k}$

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

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

Nonlinearity over $E_{n,k}$

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 $E_{n,k}$

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

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

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

Algebraic immunity over $E_{n,k}$

For $E_{n,k} \subseteq \mathbb{F}_2^n$, a function $g \in \mathcal{B}_n$ is called an annihilator of f over $E_{n,k}$ if $g(x) \neq 0$ for some $x \in E_{n,k}$ and $f(x)g(x) = 0$ for all $x \in E_{n,k}$.

Algebraic immunity over $E_{n,k}$

For $E_{n,k} \subseteq \mathbb{F}_2^n$, a function $g \in \mathcal{B}_n$ is called an annihilator of f over $E_{n,k}$ if $g(x) \neq 0$ for some $x \in E_{n,k}$ and $f(x)g(x) = 0$ for all $x \in E_{n,k}$.

The set of all annihilators of f over $E_{n,k}$ is denoted by $An_{E_{n,k}}(f)$. The algebraic immunity of f over $E_{n,k}$ is defined by

$$\mathtt{AI}_{E_{n,k}}(f) = \min\{\deg(g) : g \in An_{E_{n,k}}(f) \cup An_{E_{n,k}}(1+f)\}.$$

Algebraic immunity over $E_{n,k}$

For $E_{n,k} \subseteq \mathbb{F}_2^n$, a function $g \in \mathcal{B}_n$ is called an annihilator of f over $E_{n,k}$ if $g(x) \neq 0$ for some $x \in E_{n,k}$ and $f(x)g(x) = 0$ for all $x \in E_{n,k}$.

The set of all annihilators of f over $E_{n,k}$ is denoted by $An_{E_{n,k}}(f)$. The algebraic immunity of f over $E_{n,k}$ is defined by

$$\mathtt{AI}_{E_{n,k}}(f) = \min\{\deg(g) : g \in An_{E_{n,k}}(f) \cup An_{E_{n,k}}(1+f)\}.$$

For $f \in \mathcal{B}_n$ and $E_{n,k} \subseteq \mathbb{F}_2^n$, if $g \in An_{E_{n,k}}(f)$ then $g \neq 0$ over $E_{n,k}$. This implies that an annihilator of f is not necessarily an annihilator of f on $E_{n,k}$. That is,

- $An(f) \not\subseteq An_{E_{n,k}}(f)$. Hence $\mathtt{AI}_{E_{n,k}}(f) \not\leq \mathtt{AI}(f)$ for any $f \in \mathcal{B}_n$ and $E_{n,k} \subseteq \mathbb{F}_2^n$

Recursive Constructions of WPB and WAPB functions in Literature.

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

- [Carlet, Méaux, Rotella 2017[1]] Let $f_n \in \mathcal{B}_n$ for $n \geq 3$, be defined by

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

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

Cont.

- [Mesnager, Su 2021 [7]] Given a positive integer m, a $sup(f_m)$ for $f \in \mathcal{B}_{2^m}$ is defined as:

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

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

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

The function f_m with this defined $supp(f_m)$ is WPB.

Our Construction.

Theorem (Presented at ALCOCRYPT-2023)

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.

The ANF of f_n, defined in the above Theorem is

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

The ANF of f_n, defined in the above Theorem is

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

- For $n > p$ and even, the $f_n(X_n)$ over $E_{n,k}$ for k odd $f_n(X)$ is a linear function. Hence nonlinearity is 0 over $E_{n,k}$.
- $AI_{E_{n,k}}(f_n) = 1$ for k odd and $AI_{E_{n,k}}(f_n) = 2$ for k even .

Modification of Support for high nonlinearity.

The support of f_n over $E_{n,k}$ is defined as follows;

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

- For k odd,

$$\begin{aligned} \mathtt{sup}_k(f_n) &= \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = k\} \\ &= \sum_{i=1}^{\frac{n}{2}} x_i \end{aligned}$$

Lemma

Let $a \in \mathcal{B}_{\frac{n}{2}}$. A function $f \in \mathcal{B}_n$ such that for $k \in [0, n]$ and odd,

$$
\begin{aligned}
\mathtt{sup}_k(f^a) &= \{(x, y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ } odd, y \in \mathtt{sup}(a), \mathtt{wt}(x, y) = k\} \\
&\cup \{(y, x) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ } odd, y \notin \mathtt{sup}(a), \mathtt{wt}(y, x) = k\}
\end{aligned}
$$

Then $\mathtt{wt}_k(f^a) = \frac{1}{2}\binom{n}{k}$.

- For k even,

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

$$
\triangle \{(z, z) \in \mathbb{F}_2^n : z \in \mathtt{sup}_{\frac{k}{2}}(f_{\frac{n}{2}})\}
$$

Lemma

Let $f_n \in \mathcal{B}_n$ be the function defined in above ANF. For $k \in [0, n]$ and even, let

$$W_k = \{(x, y) \in \mathtt{sup}_k(f_n) : \mathtt{wt}(x) \text{ odd, and there is an } i \in [1, \frac{n}{2}] \text{ s.t. } x_j = y_j \text{ for } 1 \le j \le i-1 \text{ and } y_i = 1, x_i = 0\}$$

and

$$W'_k = \{(x^i, y^i) | (x, y) \in W_k \text{ and } i \in [1, \frac{n}{2}] \text{ s.t. } x_j = y_j \text{ for } 1 \le j \le i-1 \text{ and } y_i = 1, x_i = 0\}.$$

where $(x^i, y^i) = (x_1, \ldots, x_{i-1}, y_i, x_{i+1}, \ldots, x_{\frac{n}{2}}, y_1, \ldots, y_{i-1}, x_i, y_{i+1}, \ldots, y_{\frac{n}{2}})$. A function $g_n \in \mathcal{B}_n$ such that for $k \in [0, n]$ and even, such that

$$\mathtt{sup}_k(g_n) = (\mathtt{sup}_k(f_n) \setminus W_k) \cup W'_k.$$

Then $\mathtt{wt}_k(g_n) = \mathtt{wt}_k(f_n)$ if k is even.

Lemma

Let $b \in \mathcal{B}_{\frac{n}{2}}$. *Let* $g_n \in \mathcal{B}_n$ *as defined in above Lemma with* W_k *and* W'_k. *A function* $h_n^b \in \mathcal{B}_n$ *such that for* $k \in [0, n]$ *and even,*

$$\begin{aligned}\mathtt{sup}_k(h_n^b) = &\{(x,y) \in \mathtt{sup}_k(g_n) : (x,y) \notin W'_k\} \\ &\cup \{(x,y) : (x,y) \in W'_k \cap \mathtt{sup}(b)\} \\ &\cup \{(y,x) : (x,y) \in W'_k \text{ and } (x,y) \notin \mathtt{sup}(b)\}\end{aligned}$$

Then $\mathtt{wt}_k(h_n^b) = \mathtt{wt}_k(g_n)$.

Construction

For $n \geq 2$, the support of $F_n \in \mathcal{B}_n$ is defined by

$$\mathrm{sup}(F_n) = \begin{cases} \{(x,1) \in \mathbb{F}_2^2 : x \in \mathbb{F}_2\} = \{(0,1),(1,1)\} & \text{if } n = 2, \\ \{(x,0) \in \mathbb{F}_2^n : x \in \mathrm{sup}(F_{n-1})\} & \\ \cup\{(x,1) \in \mathbb{F}_2^n : x \notin \mathrm{sup}(f_{n-1})\} & \text{if } n > 2 \text{ and odd,} \\ S_n \triangle \{(z,z) \in \mathbb{F}_2^n : z \in \mathrm{sup}(f_{\frac{n}{2}})\} & \text{if } n > 2 \text{ and even.} \end{cases}$$

Here $S_n = \cup_{k=0}^{n} \mathrm{sup}_k(F_n)$ *and*

$$\mathrm{sup}_k(F_n) = \begin{cases} \mathrm{sup}_k(h_n^b) & \text{if } n > 2 \text{ and even and } k \text{ is even} \\ \mathrm{sup}_k(h_n^a) & \text{if } n > 2 \text{ and even and } k \text{ is odd.} \end{cases}$$

- We have chosen $a, b \in \mathcal{B}_{\frac{n}{2}}$, a very high nonlinear function

$$a(y) = b(y) = \begin{cases} y_1y_2 + \cdots + y_{\frac{n}{2}-1}y_{\frac{n}{2}} & \text{if } \frac{n}{2} \text{ is even} \\ y_1y_2 + \cdots + y_{\frac{n}{2}-2}y_{\frac{n}{2}-1} + y_{\frac{n}{2}} & \text{if } \frac{n}{2} \text{ is even.} \end{cases}$$

WPB/ WAPB functions	$\mathtt{nl}_2$	$\mathtt{nl}_3$	$\mathtt{nl}_4$	$\mathtt{nl}_5$	$\mathtt{nl}_6$
Upper Bound [1]	11	24	30	24	11
[1]	2	12	19	12	6
[5]	6,9	0,8,14, 16,18,20, 21, 22	19,22,23, 24,25 26, 27	19,20, 21,22	6,9
[4, $g_{2^{q+2}}$ Equation(9)]	2	12	19	12	2
[7, f_m Equation(13)]	2	0	3	0	2
[7, g_m Equation(22)]	2	14	19	14	2
[8, f_m Equation(2)]	2	8	8	8	2
[8, f_m Equation(3)]	6	8	26	8	6
[2, Table 1]	5,3, 2, 2	10,7, 12, 12	16,15, 18, 19	12,11, 12, 12	5,3, 2,6
[2, Table 3]	5	16	20	17	5
[9, g_m Equation(11)]	2	12	19	12	6
[3]	6,6,7	19,14,15	21,20,18	11,11,14	3,6,6
F_n	4	16	20	16	4

Table: Comparison of $\mathtt{nl}_k$ of 8-variable WPB constructions.

n	function	nl	nl_2	nl_3	nl_4	nl_5	nl_6	nl_7	nl_8	nl_9	nl_{10}	nl_{11}	$\sum_{k=0}^{n} nl_k$
8	UB	120	11	24	30	24	11	-	-	-	-	-	100
	F_8	96	4	16	20	16	4	-	-	-	-	-	60
9	UB	244	15	37	57	57	37	15	-	-	-	-	218
	F_9	192	6	22	45	45	22	6	-	-	-	-	146
10	UB	496	19	54	97	118	97	54	19	-	-	-	498
	F_{10}	416	9	36	69	94	73	12	9	-	-	-	302
11	UB	1000	23	76	155	220	220	155	76	23	-	-	948
	F_{11}	832	11	50	113	163	173	117	34	11	-	-	672
12	UB	2016	28	102	236	381	446	381	236	102	28	-	1940
	F_{12}	1596	12	36	146	264	286	264	148	36	14	-	1206
13	UB	4050	34	134	344	625	837	837	625	344	134	34	3948
	F_{13}	3192	15	69	219	507	660	660	495	240	69	17	2951

Table: Comparison $nl_k(F_n)$ with the upper bound(UB) presented in [1]

References. I

[1] Claude Carlet, Pierrick Méaux, and Yann Rotella. Boolean functions with restricted input and their robustness; application to the FLIP cipher. *IACR Trans. Symmetric Cryptol.*, 2017(3):192–227, 2017.

[2] Agnese Gini and Pierrick Méaux. Weightwise almost perfectly balanced functions: Secondary constructions for all n and better weightwise nonlinearities. In *Progress in Cryptology - INDOCRYPT 2022*, volume 13774 of *Lecture Notes in Computer Science*, pages 492–514. Springer, 2022.

[3] Agnese Gini and Pierrick Méaux. On the algebraic immunity of weightwise perfectly balanced functions. *IACR Cryptol. ePrint Arch.*, page 495, 2023.

[4] Jingjing Li and Sihong Su. Construction of weightwise perfectly balanced Boolean functions with high weightwise nonlinearity. *Discrete Applied Mathematics*, 279:218–227, 2020.

[5] Jian Liu and Sihem Mesnager. Weightwise perfectly balanced functions with high weightwise nonlinearity profile. *Designs, Codes and Cryptography*, 87(8):1797–1813, 2019.

References. II

[6] Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet. Towards stream ciphers for efficient FHE with low-noise ciphertexts. In *Advances in Cryptology - EUROCRYPT 2016*, volume 9665 of *Lecture Notes in Computer Science*, pages 311–343. Springer, 2016.

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

[8] Sihem Mesnager, Sihong Su, and Jingjing Li. On concrete constructions of weightwise perfectly balanced functions with optimal algebraic immunity and high weightwise nonlinearity. In *The 6th International Workshop on Boolean Functions and Applications*, 2021.

[9] Rui Zhang and Sihong Su. A new construction of weightwise perfectly balanced Boolean functions. *Advances in Mathematics of Communications*, 17(4):757–770, 2023.

Thank You.