# Constructing WAPB Boolean Functions from the Direct Sum of WAPB Boolean Functions

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

Indocrypt 2024
Chennai, India

# Relevance:

- In Eurocrypt 2016, Méaux et. al. proposed a stream cipher FLIP.

# Relevance:

- In Eurocrypt 2016, Méaux et. al. proposed a stream cipher FLIP.
- Boolean function $f$ used in FLIP restricted to the set $E = \{v \in \mathbb{F}_2^n : \mathrm{w_H}(v) = \frac{n}{2}\} \subseteq \mathbb{F}_2^n$.

# Relevance:

- In Eurocrypt 2016, Méaux et. al. proposed a stream cipher FLIP.
- Boolean function $f$ used in FLIP restricted to the set $E = \{v \in \mathbb{F}_2^n : w_H(v) = \frac{n}{2}\} \subseteq \mathbb{F}_2^n$.
- **Q:** Does it impact the security analysis of such functions ?
  **Yes.**

# Relevance:

- In Eurocrypt 2016, Méaux et. al. proposed a stream cipher FLIP.
- Boolean function $f$ used in FLIP restricted to the set $E = \{v \in \mathbb{F}_2^n : \mathrm{w_H}(v) = \frac{n}{2}\} \subseteq \mathbb{F}_2^n$.
- **Q:** Does it impact the security analysis of such functions ?
  **Yes.**
- "Symmetric bent Boolean functions" over this set behave like a constant function.

# Relevance:

- In Eurocrypt 2016, Méaux et. al. proposed a stream cipher FLIP.
- Boolean function $f$ used in FLIP restricted to the set $E = \{v \in \mathbb{F}_2^n : \mathrm{w_H}(v) = \frac{n}{2}\} \subseteq \mathbb{F}_2^n$.
- **Q:** Does it impact the security analysis of such functions ?
  **Yes.**
- "Symmetric bent Boolean functions" over this set behave like a constant function.

Therefore, studying functions with more robust cryptographic properties over such subsets is important.

# Outline

- Introduction to Boolean function.
- Existing results on direct sum, Motivation and the problem.
- Direct sum of WPB and WAPB.
- Cryptographic properties: Direct Sum.
- Examples of WPB/WAPB using direct sum method.

# Boolean Function

A $n$-variable Boolean function $f : \mathbb{F}_2^n$ to $\mathbb{F}_2$.
$\mathcal{B}_n$ : set of all $n$-variable Boolean functions. Hence, Cardinality of $\mathcal{B}_n = 2^{2^n}$.

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

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

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

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

# Boolean Function (cont.).

$\{1, 2, \ldots, n\} := [n]$, and $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$.

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

  Let $\mathcal{E}$ be a family of subsets of $\mathbb{F}_2^n$ i.e. $\mathcal{E} = \{\mathrm{E}_{0,n}, \mathrm{E}_{1,n}, \ldots, \mathrm{E}_{n,n}\}$, where $\mathrm{E}_{k,n} = \{x \in \mathbb{F}_2^n : \mathrm{w_H}(x) = k\}$.

# Boolean Function (cont.).

$\{1, 2, \ldots, n\} := [n]$, and $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$.

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

  Let $\mathcal{E}$ be a family of subsets of $\mathbb{F}_2^n$ i.e. $\mathcal{E} = \{\mathrm{E}_{0,n}, \mathrm{E}_{1,n}, \ldots, \mathrm{E}_{n,n}\}$, where $\mathrm{E}_{k,n} = \{x \in \mathbb{F}_2^n : \mathrm{w_H}(x) = k\}$.
- The support of $f$, $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. The Hamming weight of $f$ is $\mathrm{w_H}(f) = |\mathrm{supp}(f)|$.

  support of $f$ restricted to $\mathrm{E}_{k,n}$, $\mathrm{supp}_k(f) = \{x \in \mathrm{E}_{k,n} : f(x) = 1\}$.

  Hamming weight of $f$ restricted to $\mathrm{E}_{k,n}$ is $\mathrm{w}_k(f) = |\mathrm{supp}_k(f)|$.

# Boolean Function (cont.).

$\{1, 2, \ldots, n\} := [n]$, and $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$.

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

  Let $\mathcal{E}$ be a family of subsets of $\mathbb{F}_2^n$ i.e. $\mathcal{E} = \{\mathrm{E}_{0,n}, \mathrm{E}_{1,n}, \ldots, \mathrm{E}_{n,n}\}$, where $\mathrm{E}_{k,n} = \{x \in \mathbb{F}_2^n : \mathrm{w_H}(x) = k\}$.

- The support of $f$, $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. The Hamming weight of $f$ is $\mathrm{w_H}(f) = |\mathrm{supp}(f)|$.

  support of $f$ restricted to $\mathrm{E}_{k,n}$, $\mathrm{supp}_k(f) = \{x \in \mathrm{E}_{k,n} : f(x) = 1\}$.

  Hamming weight of $f$ restricted to $\mathrm{E}_{k,n}$ is $\mathrm{w}_k(f) = |\mathrm{supp}_k(f)|$.

- Let $f, g \in \mathcal{B}_n$. The Hamming distance between $f$ and $g$ is $\mathrm{d_H}(f, g) = |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}|$.
  Hamming distance between $f$ and $g$ over $\mathrm{E}_{k,n}$,
  $\mathrm{d_k}(f, g) = |\{x \in \mathrm{E}_{k,n} : f(x) \neq g(x)\}|$.

# WAPB and WPB Boolean Functions

1. A function $f$ is said to be balanced, if

$$|\{x \in \mathbb{F}_2^n : f(x) = 0\}| = |\{x \in \mathbb{F}_2^n : f(x) = 1\}|.$$

# WAPB and WPB Boolean Functions

1. A function $f$ is said to be balanced, if

$$|\{x \in \mathbb{F}_2^n : f(x) = 0\}| = |\{x \in \mathbb{F}_2^n : f(x) = 1\}|.$$

2. A functions $f \in \mathcal{B}_n$ is said to be **weightwise almost perfectly balanced (WAPB)** if $\forall k \in [0, n]$,

$$\mathrm{w}_k(f) = \begin{cases} \frac{\binom{n}{k}}{2} & \textit{if } \binom{n}{k} \textit{ is even}, \\ \frac{\binom{n}{k} \pm 1}{2} & \textit{if } \binom{n}{k} \textit{ is odd.} \end{cases}$$

# WAPB and WPB Boolean Functions

1. A function $f$ is said to be balanced, if

$$|\{x \in \mathbb{F}_2^n : f(x) = 0\}| = |\{x \in \mathbb{F}_2^n : f(x) = 1\}|.$$

2. A functions $f \in \mathcal{B}_n$ is said to be **weightwise almost perfectly balanced (WAPB)** if $\forall k \in [0, n]$,

$$\mathrm{w}_k(f) = \begin{cases} \frac{\binom{n}{k}}{2} & \textit{if } \binom{n}{k} \textit{ is even,} \\ \frac{\binom{n}{k} \pm 1}{2} & \textit{if } \binom{n}{k} \textit{ is odd.} \end{cases}$$

3. A balanced Boolean function $f \in \mathcal{B}_n$ is said to be **weightwise perfectly balanced (WPB)** if $f$ restricted to $\mathrm{E}_{k,n}$, is balanced for all $k \in [1, n-1]$, i.e.,

$$\mathrm{w}_k(f) = \frac{\binom{n}{k}}{2}$$

for all $k \in [1, n-1]$ and, $f(0, 0, \ldots, 0) \neq f(1, 1, \ldots, 1)$.

# WAPB and WPB Boolean Functions

1. A function $f$ is said to be balanced, if

$$|\{x \in \mathbb{F}_2^n : f(x) = 0\}| = |\{x \in \mathbb{F}_2^n : f(x) = 1\}|.$$

2. A functions $f \in \mathcal{B}_n$ is said to be **weightwise almost perfectly balanced (WAPB)** if $\forall k \in [0, n]$,

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

3. A balanced Boolean function $f \in \mathcal{B}_n$ is said to be **weightwise perfectly balanced (WPB)** if $f$ restricted to $\mathrm{E}_{k,n}$, is balanced for all $k \in [1, n-1]$, i.e.,

$$\mathrm{w}_k(f) = \frac{\binom{n}{k}}{2}$$

for all $k \in [1, n-1]$ and, $f(0, 0, \ldots, 0) \neq f(1, 1, \ldots, 1)$.
Exist: if $n$ is power of 2 .

# Direct sum

Let $f \in \mathcal{B}_m$ and $g \in \mathcal{B}_n$ be two Boolean functions, then the **direct sum** $h \in \mathcal{B}_{n+m}$ of $f$ and $g$ is defined by:

$$h(x, y) = f(x) + g(y)$$

for $x \in \mathbb{F}_2^m$ and $y \in \mathbb{F}_2^n$.

# Direct sum

Let $f \in \mathcal{B}_m$ and $g \in \mathcal{B}_n$ be two Boolean functions, then the **direct sum** $h \in \mathcal{B}_{n+m}$ of $f$ and $g$ is defined by:

$$h(x, y) = f(x) + g(y)$$

for $x \in \mathbb{F}_2^m$ and $y \in \mathbb{F}_2^n$.

- $\mathrm{w}_k(h) = \sum_{i=0}^{k} \mathrm{w}_i(f)\left(\binom{n}{k-i} - \mathrm{w}_{k-i}(g)\right) + \mathrm{w}_{k-i}(g)\left(\binom{m}{i} - \mathrm{w}_i(f)\right)$

# Direct sum

Let $f \in \mathcal{B}_m$ and $g \in \mathcal{B}_n$ be two Boolean functions, then the **direct sum** $h \in \mathcal{B}_{n+m}$ of $f$ and $g$ is defined by:

$$h(x, y) = f(x) + g(y)$$

for $x \in \mathbb{F}_2^m$ and $y \in \mathbb{F}_2^n$.

- $\mathrm{w}_k(h) = \sum_{i=0}^{k} \mathrm{w}_i(f) \left( \binom{n}{k-i} - \mathrm{w}_{k-i}(g) \right) + \mathrm{w}_{k-i}(g) \left( \binom{m}{i} - \mathrm{w}_i(f) \right)$
- $h$ is balanced over $\mathbb{F}_2^{n+m}$, if $f$ or $g$ is balanced.

$$\begin{aligned} W_{f+g}(0) &= \sum_{z=(x,y)\in\mathbb{F}_2^{n+m}} (-1)^{f(x)+g(y)} \\ &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)} \cdot \sum_{y\in\mathbb{F}_2^m} (-1)^{g(x)} \\ &= W_f(0) \cdot W_g(0) = 0 \end{aligned}$$

# Direct sum of WPB functions

**Proposition (Carlet, Méaux, Rotella (2017))**

*Let $n = 2^l$ for $l \in \mathbb{Z}$. Let $h \in \mathcal{B}_n$ such that*

$$h(x_1, x_2, \ldots, x_n) = g_1(x_1, x_2, \ldots, x_{\frac{n}{2}}) + g_2(x_{\frac{n}{2}+1}, x_{\frac{n}{2}+2}, \ldots, x_n).$$

*If $g_1$ and $g_2$ are two WPB Boolean functions, then $h$ is not WPB.*

# Direct sum of WPB functions

**Proposition (Carlet, Méaux, Rotella (2017))**

*Let $n = 2^l$ for $l \in \mathbb{Z}$. Let $h \in \mathcal{B}_n$ such that*

$$h(x_1, x_2, \ldots, x_n) = g_1(x_1, x_2, \ldots, x_{\frac{n}{2}}) + g_2(x_{\frac{n}{2}+1}, x_{\frac{n}{2}+2}, \ldots, x_n).$$

*If $g_1$ and $g_2$ are two WPB Boolean functions, then $h$ is not WPB.*

**Proposition (Carlet, Méaux, Rotella (2017))**

*Let $f, g \in \mathcal{B}_n$ be WPB Boolean functions. Then $h \in \mathcal{B}_{2n}$ defined by*

$$h(x, y) = f(x) + g(y) + \prod_{i=1}^{n} x_i,$$

*where $x, y \in \mathbb{F}_2^n$, is a WPB Boolean function.*

# Direct sum of WPB functions

**Proposition (Zhu, Linya and Su, Sihong (2022))**

*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*

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

*is WAPB.*

# Motivation and Problem :

**Q: Is the direct sum of two WAPB Boolean functions WAPB or WPB?**

# Example

Let $f \in \mathcal{B}_3$ and $g \in \mathcal{B}_5$ be two WAPB Boolean functions. Assume that,

| | |
|---|---|
| $\mathrm{w}_0(f) = \frac{\binom{3}{0}+1}{2} = 1$ | $\mathrm{w}_0(g) = \frac{\binom{5}{0}+1}{2} = 1$ |
| $\mathrm{w}_1(f) = \frac{\binom{3}{1}+1}{2} = 2$ | $\mathrm{w}_1(g) = \frac{\binom{5}{1}+1}{2} = 2$ |
| $\mathrm{w}_2(f) = \frac{\binom{3}{2}-1}{2} = 1$ | $\mathrm{w}_2(g) = \frac{\binom{5}{2}}{2} = 5$ |
| $\mathrm{w}_3(f) = \frac{\binom{3}{3}-1}{2} = 0$ | $\mathrm{w}_3(g) = 5$ |
| | $\mathrm{w}_4(g) = 3$ |
| | $\mathrm{w}_5(g) = 0$ |

## Example

Let $f \in \mathcal{B}_3$ and $g \in \mathcal{B}_5$ be two WAPB Boolean functions. Assume that,

$$\begin{aligned} w_0(f) &= \frac{\binom{3}{0}+1}{2} = 1 \\ w_1(f) &= \frac{\binom{3}{1}+1}{2} = 2 \\ w_2(f) &= \frac{\binom{3}{2}-1}{2} = 1 \\ w_3(f) &= \frac{\binom{3}{3}-1}{2} = 0 \end{aligned}$$

$$\begin{aligned} w_0(g) &= \frac{\binom{5}{0}+1}{2} = 1 \\ w_1(g) &= \frac{\binom{5}{1}+1}{2} = 2 \\ w_2(g) &= \frac{\binom{5}{2}}{2} = 5 \\ w_3(g) &= 5 \\ w_4(g) &= 3 \\ w_5(g) &= 0 \end{aligned}$$

The direct sum $h \in \mathcal{B}_8$ is defined by $h(x, y) = f(x) + g(y)$. Hence,

$$w_0(h) = 0$$

$$\begin{aligned} w_1(h) &= w_0(f)\left(\binom{5}{1} - w_1(g)\right) + w_1(g)\left(\binom{3}{0} - w_0(f)\right) \\ &+ w_1(f)\left(\binom{5}{0} - w_0(g)\right) + w_0(g)\left(\binom{3}{1} - w_1(f)\right) \\ &= 1(3) + 2(0) + 2(0) + 1(1) = 4 = \frac{\binom{8}{1}}{2} \ \text{(balanced over } E_{1,8}\text{)} \end{aligned}$$

# Cont.

## Example (Cont.)

$$\begin{aligned} w_2(h) &= w_0(f)\left(\binom{5}{2} - w_2(g)\right) + w_2(g)\left(\binom{3}{0} - w_0(f)\right) \\ &+ w_1(f)\left(\binom{5}{1} - w_1(g)\right) + w_1(g)\left(\binom{3}{1} - w_1(f)\right) \\ &+ w_2(f)\left(\binom{5}{0} - w_0(g)\right) + w_0(g)\left(\binom{3}{0} - w_0(f)\right) \\ &= 1(5) + 5(0) + 2(3) + 2(1) + 1(0) + 1(0) = 13 \end{aligned}$$

For $h$ to be balanced over $E_{2,8}$, $w_2(h) = \frac{\binom{8}{2}}{2} = 14$.

# Cont.

## Example (Cont.)

$$
\begin{aligned}
w_2(h) &= w_0(f)\left(\binom{5}{2} - w_2(g)\right) + w_2(g)\left(\binom{3}{0} - w_0(f)\right) \\
&\quad + w_1(f)\left(\binom{5}{1} - w_1(g)\right) + w_1(g)\left(\binom{3}{1} - w_1(f)\right) \\
&\quad + w_2(f)\left(\binom{5}{0} - w_0(g)\right) + w_0(g)\left(\binom{3}{0} - w_0(f)\right) \\
&= 1(5) + 5(0) + 2(3) + 2(1) + 1(0) + 1(0) = 13
\end{aligned}
$$

For $h$ to be balanced over $E_{2,8}$, $w_2(h) = \frac{\binom{8}{2}}{2} = 14$.

Not necessarily a WPB/WAPB.

**Q: Can we construct a WAPB(or, WPB) Boolean function from the direct sum of two WAPB Boolean functions?**

# Notations:

- $\delta_k^f$ : For $k \in [0, n]$, $\delta_k^f \in \{-1, 0, 1\}$ is defined as $\delta_k^f = 2\mathrm{w}_k(f) - \binom{n}{k}$ (in case of WPB and WAPB functions).

- $x \preceq y$ : For $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_2^n$, $y$ covers $x$ (i.e., $x \preceq y$), if $x_i \leq y_i, \forall i \in [1, n]$.

- Given $n \in \mathbb{Z}^+$, denote $e(n) = \{a_1, a_2, \ldots, a_w\} \subseteq \mathbb{N} \cup \{0\}$ if $n = 2^{a_1} + 2^{a_2} + \cdots + 2^{a_w}$.
  Hence, $x \preceq y$ iff $e(x) \subseteq e(y)$.

# $\mathrm{w}_k(h)$ : $\delta_k^h$ in terms of $\delta_i^f$ and $\delta_{k-i}^g$.

**Theorem (Dalai,-, Indocrypt2024)**

*Let* $f \in \mathcal{B}_m, g \in \mathcal{B}_n$ *be two WAPB Bfs with*

| $\mathrm{w}_i(f) = \frac{\binom{m}{i}+\delta_i^f}{2}$ | $\mathrm{w}_{k-i}(g) = \frac{\binom{n}{k-i}+\delta_{k-i}^g}{2}$ |
|---|---|
| *for* $i \in [0, m]$ | *for* $k-i \in [0, n]$, |

*where* $\delta_i^f, \delta_{k-i}^g \in \{-1, 0, 1\}$.
*Let* $h \in \mathcal{B}_{m+n}$ *defined as* $h(x, y) = f(x) + g(y)$ *for* $x \in \mathbb{F}_2^m$ *and* $y \in \mathbb{F}_2^n$.
*Then*

$$\mathrm{w}_k(h) = \frac{\binom{m+n}{k} - \sum_{i=0}^{k} \delta_i^f \delta_{k-i}^g}{2} \text{ for } k \in [0, m+n].$$

# $\mathrm{w}_k(h)$ : $\delta_k^h$ in terms of $\delta_i^f$ and $\delta_{k-i}^g$.

**Theorem (Dalai,-, Indocrypt2024)**

*Let $f \in \mathcal{B}_m, g \in \mathcal{B}_n$ be two WAPB Bfs with*

| | |
|---|---|
| $\mathrm{w}_i(f) = \frac{\binom{m}{i}+\delta_i^f}{2}$ | $\mathrm{w}_{k-i}(g) = \frac{\binom{n}{k-i}+\delta_{k-i}^g}{2}$ |
| *for* $i \in [0, m]$ | *for* $k - i \in [0, n]$, |

*where $\delta_i^f, \delta_{k-i}^g \in \{-1, 0, 1\}$.*
*Let $h \in \mathcal{B}_{m+n}$ defined as $h(x, y) = f(x) + g(y)$ for $x \in \mathbb{F}_2^m$ and $y \in \mathbb{F}_2^n$.*
*Then*

$$\mathrm{w}_k(h) = \frac{\binom{m+n}{k} - \sum_{i=0}^{k} \delta_i^f \delta_{k-i}^g}{2} \text{ for } k \in [0, m+n].$$

• If $f, g$ satisfies $\sum_{i=0}^{k} \delta_i^f \delta_{k-i}^g \in \{-1, 0, 1\}$ then $h$ is an WAPB Boolean function.

# Case-I: Direct sum is WAPB.

**Theorem (Dalai,-,Indocrypt2024)**

*Let $m, n \in \mathbb{Z}^+$ such that $e(m) \cap e(n) = \emptyset$. Let $f \in \mathcal{B}_m$ and $g \in \mathcal{B}_n$ be two WAPB Boolean functions.*
*Then the direct sum $h \in \mathcal{B}_{m+n}$ is a WAPB Boolean function with*

$$\delta_k^h = \begin{cases} 0 & \text{if } e(k) \not\subseteq e(m) \cup e(n) = e(m+n) \\ & k \not\preceq m+n \\ -\delta_s^f \delta_{k-s}^g \text{ where } e(s) = e(k) \cap e(m) & \text{if } e(k) \subseteq e(m) \cup e(n) = e(m+n) \\ & \text{i.e., } k \preceq m+n. \end{cases}$$

# Case-I: Direct sum is WAPB.

### Theorem (Dalai,-,Indocrypt2024)

*Let $m, n \in \mathbb{Z}^+$ such that $e(m) \cap e(n) = \emptyset$. Let $f \in \mathcal{B}_m$ and $g \in \mathcal{B}_n$ be two WAPB Boolean functions.*
*Then the direct sum $h \in \mathcal{B}_{m+n}$ is a WAPB Boolean function with*

$$\delta_k^h = \begin{cases} 0 & \text{if } e(k) \not\subseteq e(m) \cup e(n) = e(m+n) \\ & k \not\preceq m+n \\ -\delta_s^f \delta_{k-s}^g \text{ where } e(s) = e(k) \cap e(m) & \text{if } e(k) \subseteq e(m) \cup e(n) = e(m+n) \\ & \text{ i.e., } k \preceq m+n. \end{cases}$$

- Thus this theorem, implies the [Theorem 3] in [Zhu and Su,2022].

# Theorem $\implies$ Zhu and Su (2022) WAPB constructions.

- $n = \sum_{i=1}^{p} n_i$ for $n_i = 2^{a_i}$ for $i \in [1, p]$,
- $\cap_{i=1}^{p} e(n_i) = \phi$,
- $e(n) = \{a_1, a_2, \ldots, a_p\}$ with $0 \leq a_1 < a_2 < \cdots < a_p$.

## Theorem (Dalai,-,Indocrypt2024)

*Let $f_{n_i} \in \mathcal{B}_{n_i}$ 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,*

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

*is a WAPB, with $\mathrm{w}_k(h_n) = \frac{\binom{n}{k} + \delta_k^{h_n}}{2}$ where*

$$\delta_k^{h_n} = \begin{cases} -(-1)^{|e(k)|} = -(-1)^{\mathrm{w_H}(k)} & \text{if } e(k) \subseteq e(n) \\ 0 & \text{if } e(k) \not\subseteq e(n), \end{cases}$$

*for $k \in [0, n]$.*

# Case-II: Direct sum is WPB.

## Theorem (Dalai,-, Indocrypt2024)

*Let* $m, n \in \mathbb{Z}^+$ *such that* $m + n = 2^l$ *for* $l \in \mathbb{Z}^+$ *(i.e.* $e(m) \cap e(n) = \{a_1\}$ *and* $e(m) \cup e(n) = \{a_1, a_1 + 1, \ldots, l - 1\}$*).*
*Let* $f \in \mathcal{B}_m$ *and* $g \in \mathcal{B}_n$*, two WAPB. Then* $h \in \mathcal{B}_{m+n}$*, WPB if there is a* $c \in \{-1, 1\}$ *such that*

$$\begin{aligned}
\frac{\delta^f_0}{\delta^f_m} &= -\frac{\delta^g_0}{\delta^g_n}; \\
\frac{\delta^f_{2^{T_1}\setminus\{a_1\}}}{\delta^f_{2^{T_1}}} &= c \text{ for every } T_1 \subseteq e(m) \text{ with } a_1 \in T_1; \\
\frac{\delta^g_{2^{T_2}\setminus\{a_1\}}}{\delta^g_{2^{T_2}}} &= -c \text{ for every } T_2 \subseteq e(n) \text{ with } a_1 \in T_2; \\
\frac{\delta^f_{2^{U_1}}}{\delta^f_{2^{V_1}}} &= -\frac{\delta^g_{2^{V_2}}}{\delta^g_{2^{U_2}}} \text{ for every } k > 0 \text{ satisfying } e(k) \subseteq (e(m) \cup e(n)) \setminus \{a_1\}
\end{aligned}$$

*where* $U_1 = e(k) \cap e(m), U_2 = e(k) \cap e(n)$,
$V_1 = (U_1 \setminus \{s\}) \cup (e(m) \cap \{a_1, a_1 + 1, \ldots, s - 1\})$ *and*
$V_2 = (U_2 \setminus \{s\}) \cup (e(n) \cap \{a_1, a_1 + 1, \ldots, s - 1\})$ *with s be the smallest integer in* $e(k)$*.*

## Example

Consider $m = 3$ and $n = 5$. Then $e(3) = \{1, 0\}, e(5) = \{2, 0\}$. So from the Theorem-9, find a $c \in \{-1, 1\}$ such that the following conditions to be satisfied by $f$ and $g$.

i. $\frac{\delta_0^f}{\delta_3^f} = -\frac{\delta_0^g}{\delta_5^g}$

ii. $\frac{\delta_0^f}{\delta_1^f} = \frac{\delta_2^f}{\delta_3^f} = c$ and $\frac{\delta_0^g}{\delta_1^g} = \frac{\delta_4^g}{\delta_5^g} = -c$

iii. $\frac{\delta_0^f}{\delta_3^f} = -\frac{\delta_1^g}{\delta_4^g}$ ; $\frac{\delta_2^f}{\delta_1^f} = -\frac{\delta_1^g}{\delta_0^g}$ ; $\frac{\delta_2^f}{\delta_1^f} = -\frac{\delta_5^g}{\delta_4^g}$.

Considering, $c = 1$, for

$$\begin{array}{l|l} \delta_0^f = -1, \delta_3^f = -1 & \delta_0^g = 1, \delta_5^g = -1 \\ \delta_1^f = -1, \delta_2^f = -1 & \delta_1^g = -1, \delta_4^g = 1. \end{array}$$

Conditions *i.*, *ii.* and *iii.* are satisfied.

## Example (Cont.)

Hence,

| | |
|---|---|
| $w_0(f) = 0$ | $w_0(g) = 1$ |
| $w_1(f) = 1$ | $w_1(g) = 2$ |
| $w_2(f) = 1$ | $w_2(g) = 5$ |
| $w_3(f) = 0$ | $w_3(g) = 5$ |
| | $w_4(g) = 3$ |
| | $w_5(g) = 0$ |

The direct sum $h(x, y) = f(x) + g(y)$ for $x \in \mathbb{F}_2^3$ and $y \in \mathbb{F}_2^5$ is a WPB Boolean function.

# Cryptographic properties of direct sum

- Nonlinearity of $f$ over $\mathbb{F}_2^n$,

$$\mathrm{NL}(f) = \min_{g \in \mathcal{A}_n} \mathrm{d_H}(f, g) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \Big| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a\cdot x} \Big|$$

and,
weightwise nonlinearity of $f$ over $\mathsf{E}_{k,n}$,

$$\mathrm{NL}_k(f) = \min_{g \in \mathcal{A}_n} \mathrm{d_k}(f, g) = \frac{|\mathsf{E}_{k,n}|}{2} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \Big| \sum_{x \in \mathsf{E}_{k,n}} (-1)^{f(x)+a\cdot x} \Big|$$

# Cryptographic properties of direct sum

- Nonlinearity of $f$ over $\mathbb{F}_2^n$,

$$\mathrm{NL}(f) = \min_{g \in \mathcal{A}_n} \mathrm{d_H}(f,g) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \Big| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a\cdot x} \Big|$$

  and,
  weightwise nonlinearity of $f$ over $\mathrm{E}_{k,n}$,

$$\mathrm{NL}_k(f) = \min_{g \in \mathcal{A}_n} \mathrm{d_k}(f,g) = \frac{|\mathrm{E}_{k,n}|}{2} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \Big| \sum_{x \in \mathrm{E}_{k,n}} (-1)^{f(x)+a\cdot x} \Big|$$

- Algebraic immunity(AI) of $f$ over $\mathbb{F}_2^n$, $\mathrm{AI}(f) = \min\{\deg(g) : f(x)g(x) = 0 \text{ or } (1+f(x))g(x) = 0 \forall x \in \mathbb{F}_2^n \text{ for } g(x) \neq 0 \text{ for some } x \in \mathbb{F}_2^n\}$
  and,
  Algebraic immunity(AI) of $f$ over $\mathrm{E}_{k,n}$,
  $\mathrm{AI}_k(f) = \min\{\deg(g) : f(x)g(x) = 0 \text{ or } (1+f(x))g(x) = 0 \forall x \in \mathrm{E}_{k,n} \text{ for } g(x) \neq 0 \text{ for some } x \in \mathrm{E}_{k,n}\}$.

# Cryptographic properties of direct sum

## Proposition (Carlet, Méaux, Rotella (2017))

*$f \in \mathcal{B}_m$, $g \in \mathcal{B}_n$ and $h \in \mathcal{B}_{m+n}$ be defined as $h(x, y) = f(x) + g(y)$. Then*

1. *the nonlinearity over* $\mathsf{E}_{k,m+n}$

$$\mathsf{NL}_k(h) \geq \sum_{i=0}^{k} \left( \binom{m}{i} \mathsf{NL}_{k-i}(g) + \binom{n}{k-i} \mathsf{NL}_i(f) - 2\mathsf{NL}_i(f)\mathsf{NL}_{k-i}(g) \right).$$

# Cryptographic properties of direct sum

Let $f \in \mathcal{B}_m$, $g \in \mathcal{B}_n$ and $h \in \mathcal{B}_{m+n}$ be defined as $h(x, y) = f(x) + g(y)$ for $x \in \mathbb{F}_2^m$ and $y \in \mathbb{F}_2^n$. Then

- [1][An Braeken and Bart Preneel, 2005]
  $\max(\mathrm{AI}(f), \mathrm{AI}(g)) \leq \mathrm{AI}(h) \leq \min\{\max\{\deg(f), \deg(g)\}, \mathrm{AI}(f) + \mathrm{AI}(g)\}$.

# Cryptographic properties of direct sum

Let $f \in \mathcal{B}_m$, $g \in \mathcal{B}_n$ and $h \in \mathcal{B}_{m+n}$ be defined as $h(x, y) = f(x) + g(y)$ for $x \in \mathbb{F}_2^m$ and $y \in \mathbb{F}_2^n$. Then

- [1][An Braeken and Bart Preneel, 2005]
  $\max(\mathrm{AI}(f), \mathrm{AI}(g)) \leq \mathrm{AI}(h) \leq \min\{\max\{\deg(f), \deg(g)\}, \mathrm{AI}(f) + \mathrm{AI}(g)\}$.
- [2][Carlet, Méaux, Rotella (2017)] for all $k \leq \min\{m, n\}$,

$$\mathrm{AI}_k(h) \geq \min_{0 \leq j \leq k} \{\max\{\mathrm{AI}_j(f), \mathrm{AI}_{k-j}(g)\}\}$$

.

# Cryptographic properties of direct sum

Let $f \in \mathcal{B}_m$, $g \in \mathcal{B}_n$ and $h \in \mathcal{B}_{m+n}$ be defined as $h(x, y) = f(x) + g(y)$ for $x \in \mathbb{F}_2^m$ and $y \in \mathbb{F}_2^n$. Then

- [1][An Braeken and Bart Preneel, 2005]
  $\max(\mathrm{AI}(f), \mathrm{AI}(g)) \leq \mathrm{AI}(h) \leq \min\{\max\{\deg(f), \deg(g)\}, \mathrm{AI}(f) + \mathrm{AI}(g)\}$.

- [2][Carlet, Méaux, Rotella (2017)] for all $k \leq \min\{m, n\}$,

  $$\mathrm{AI}_k(h) \geq \min_{0 \leq j \leq k} \{\max\{\mathrm{AI}_j(f), \mathrm{AI}_{k-j}(g)\}\}$$

  .

- For $0 \leq k \leq m + n$ and $m \leq n$, then

  $$\min_{\max\{0,k-m\} \leq j \leq \min\{m,k\}} \{\max\{\mathrm{AI}_j(f), \mathrm{AI}_{k-j}(g)\}\} \leq \mathrm{AI}_k(h) \leq \deg(h).$$

# Construction: WPB/WAPB Boolean function.

**Theorem (Dalai,-, Indocrypt2024)**

*For $n = 2^l, l \geq 1$, let $f_n \in \mathcal{B}_n$ be defined recursively as*

$$f_n(x_1, \ldots, x_n) = f_{\frac{n}{2}}(x_1, \ldots, x_{\frac{n}{2}}) + f_{\frac{n}{2}}(x_{\frac{n}{2}+1}, \ldots, x_n) + \prod_{i=\frac{n}{2}+1}^{n} x_i, \text{ for } l \geq 2 \text{ and}$$

*$f_2(x_1, x_2) = x_2$. Then*

1. *$f_n$ is WPB.*
2. $f_n(x_1, \ldots, x_n) = \sum_{2^1|i} x_i + \sum_{2^2|i} x_{i-1}x_i + \sum_{2^3|i} x_{i-3}x_{i-2}x_{i-1}x_i + \cdots + x_{\frac{n}{2}+1} \cdots x_n$.
3. $\mathrm{NL}(f_n) = 2^{n-1} - \frac{1}{2}(3^{\frac{n}{2}} - 1)$.
4. $\mathrm{AI}(f_n) \leq 1 + \frac{n}{4}$.

# Construction: WPB/WAPB

**Definition**

$f \in \mathcal{B}_n$ be WAPB with $\delta_i^f = -\delta_{i-1}^f$ for $i \in [1, n]$ (i.e., $\delta_i^f = (-1)^i \delta_0^f$, for $i \in [0, n]$) is defined as an **alternating WAPB (AWAPB)** Bf.

# Construction: WPB/WAPB

### Definition

$f \in \mathcal{B}_n$ be WAPB with $\delta_i^f = -\delta_{i-1}^f$ for $i \in [1, n]$ (i.e., $\delta_i^f = (-1)^i \delta_0^f$, for $i \in [0, n]$) is defined as an **alternating WAPB (AWAPB)** Bf.

### Lemma (Dalai,-, Indocrypt2024)

*Let $n = 2^l$ and $f, g \in \mathcal{B}_{n-1}$, AWAPB Bfs (i.e. $\delta_i^f = -\delta_{i-1}^f$) with $\delta_i^f = \delta_i^g$ for $i \in [1, n]$. Then $h \in \mathcal{B}_n$ defined as*

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

*is WPB.*

# Construction: WPB/WAPB

Let $n = 2^l \in \mathbb{Z}^+$.

## Lemma (Dalai,-, Indocrypt2024)

*$f \in \mathcal{B}_{n-1}$, AWAPB and $g \in \mathcal{B}_n$ unbalanced WAPB i.e. $\delta_0^g = \delta_n^g$.*
*Then direct sum $h \in \mathcal{B}_{2n-1}$ is AWAPB for $x \in \mathbb{F}_2^{n-1}, y \in \mathbb{F}_2^n$.*

# Construction: WPB/WAPB

Let $n = 2^l \in \mathbb{Z}^+$.

## Lemma (Dalai,-, Indocrypt2024)

*$f \in \mathcal{B}_{n-1}$, AWAPB and $g \in \mathcal{B}_n$ unbalanced WAPB i.e. $\delta_0^g = \delta_n^g$.*
*Then direct sum $h \in \mathcal{B}_{2n-1}$ is AWAPB for $x \in \mathbb{F}_2^{n-1}, y \in \mathbb{F}_2^n$.*

## Corollary (Dalai,-, Indocrypt2024)

*Let $f \in \mathcal{B}_{n-1}$, AWAPB Bf and $g \in \mathcal{B}_n$, WPB Bf.*
*Then $h \in \mathcal{B}_{2n-1}$ defined as*

$$h(x, y) = f(x) + g(y) + \prod_{i=1}^{n} y_i$$

*for $x \in \mathbb{F}_2^{n-1}, y \in \mathbb{F}_2^n$ is a AWAPB Bf.*

# Example

## Example

- $f_1 \in \mathcal{B}_1$ s.t. $f_1(x_1) = x_1$, **AWAPB** with $\delta_0^f = -1$ and $\delta_1^f = 1$.

# Example

## Example

- $f_1 \in \mathcal{B}_1$ s.t. $f_1(x_1) = x_1$, **AWAPB** with $\delta_0^f = -1$ and $\delta_1^f = 1$.
- $f = g = f_1$ in, $f_2(x_1, x_2) = x_2 x_1 + (1 + x_2) x_1 = x_1$, **WPB** in $\mathcal{B}_2$.

# Example

## Example

- $f_1 \in \mathcal{B}_1$ s.t. $f_1(x_1) = x_1$, **AWAPB** with $\delta_0^f = -1$ and $\delta_1^f = 1$.
- $f = g = f_1$ in, $f_2(x_1, x_2) = x_2 x_1 + (1 + x_2) x_1 = x_1$, **WPB** in $\mathcal{B}_2$.
- $f = f_1, g = f_2$, $f_3(x_1, x_2, x_3) = x_1 + x_2 + x_2 x_3$, **AWAPB** in $\mathcal{B}_3$.

# Example

## Example

- $f_1 \in \mathcal{B}_1$ s.t. $f_1(x_1) = x_1$, **AWAPB** with $\delta_0^f = -1$ and $\delta_1^f = 1$.
- $f = g = f_1$ in, $f_2(x_1, x_2) = x_2 x_1 + (1 + x_2)x_1 = x_1$, **WPB** in $\mathcal{B}_2$.
- $f = f_1, g = f_2$, $f_3(x_1, x_2, x_3) = x_1 + x_2 + x_2 x_3$, **AWAPB** in $\mathcal{B}_3$.
- $f(x) = f_3(x)$ and $g(x) = f_3(Ax)$ where $A$ : permutation matrix. $g$ is also **AWAPB** with $\delta_i^f = \delta_i^g$ for $i \in [0, n]$. Take, $g(x_1, x_2, x_3) = x_1 + x_3 + x_2 x_3$.

# Example

## Example

- $f_1 \in \mathcal{B}_1$ s.t. $f_1(x_1) = x_1$, **AWAPB** with $\delta_0^f = -1$ and $\delta_1^f = 1$.
- $f = g = f_1$ in, $f_2(x_1, x_2) = x_2 x_1 + (1 + x_2)x_1 = x_1$, **WPB** in $\mathcal{B}_2$.
- $f = f_1, g = f_2$, $f_3(x_1, x_2, x_3) = x_1 + x_2 + x_2 x_3$, **AWAPB** in $\mathcal{B}_3$.
- $f(x) = f_3(x)$ and $g(x) = f_3(Ax)$ where $A$ : permutation matrix. $g$ is also **AWAPB** with $\delta_i^f = \delta_i^g$ for $i \in [0, n]$. Take, $g(x_1, x_2, x_3) = x_1 + x_3 + x_2 x_3$.
- $f_4(x_1, x_2, x_3, x_4) = x_4 f(x_1, x_2, x_3) + (1 + x_4)g(x_1, x_2, x_3) = x_1 + x_2 + x_2 x_3 + x_2 x_4 + x_3 x_4$, **WPB**.

# Example

## Example

- $f_1 \in \mathcal{B}_1$ s.t. $f_1(x_1) = x_1$, **AWAPB** with $\delta_0^f = -1$ and $\delta_1^f = 1$.
- $f = g = f_1$ in, $f_2(x_1, x_2) = x_2 x_1 + (1 + x_2) x_1 = x_1$, **WPB** in $\mathcal{B}_2$.
- $f = f_1, g = f_2$, $f_3(x_1, x_2, x_3) = x_1 + x_2 + x_2 x_3$, **AWAPB** in $\mathcal{B}_3$.
- $f(x) = f_3(x)$ and $g(x) = f_3(Ax)$ where $A$ : permutation matrix. $g$ is also **AWAPB** with $\delta_i^f = \delta_i^g$ for $i \in [0, n]$. Take, $g(x_1, x_2, x_3) = x_1 + x_3 + x_2 x_3$.
- $f_4(x_1, x_2, x_3, x_4) = x_4 f(x_1, x_2, x_3) + (1 + x_4) g(x_1, x_2, x_3) = x_1 + x_2 + x_2 x_3 + x_2 x_4 + x_3 x_4$, **WPB**.
- $f = f_3, g = f_4$ , $f_7(x_1, \ldots, x_7) = f_3(x_1, x_2, x_3) + f_4(x_4, x_5, x_6, x_7) + x_4 x_5 x_6 x_7 \in \mathcal{B}_7$, **AWAPB**.

# Future work:

- To study the direct sum $h(x, y) = f(x) + g(y)$, when $e(m) \cap e(n) \neq \phi$.

# Future work:

- To study the direct sum $h(x, y) = f(x) + g(y)$, when $e(m) \cap e(n) \neq \phi$.
- Improve bound for $\mathrm{NL}_k(h)$ and $\mathrm{AI}_k(h)$ for the direct sum construction.

**Questions ?**

# References. I


An Braeken and Bart Preneel
On the Algebraic Immunity of Symmetric Boolean Functions.
*Progress in Cryptology-INDOCRYPT 2005, Lecture Notes in Computer Science, 35-48, 2005.*

Claude Carlet and Pierrick Méaux and Yann Rotella
Boolean functions with restricted input and their robustness; application to the FLIP cipher
*IACR Trans. Symmetric Cryptol., 2017, 3.*

Jian Liu and Sihem Mesnager
Weightwise perfectly balanced functions with high weightwise nonlinearity profile
*Des. Codes Cryptogr., 2019, 1797–1813*

MacWilliams, F.J. and Sloane, N.J.A.,
The Theory of Error-Correcting Codes,
*North-holland Publishing Company,1978*

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, 2022, 181-190*