Weightwise (almost) perfectly balanced functions based on total orders

Pierrick MÉAUX

Luxembourg University, Luxembourg

Montreal — Canada
Thursday August 29th

Summary

Boolean functions and balancedness

Boolean functions:

$$f : \mathbb{F}_2^n \to \mathbb{F}_2$$

- common object in symmetric cryptography,
- also called predicates in other areas.

Boolean functions and balancedness

Example:

$$f : \mathbb{F}_2^4 \rightarrow \mathbb{F}_2$$

0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

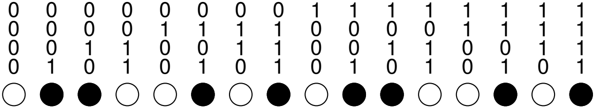
○ = 0

● = 1

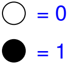
Boolean functions and balancedness

Example:

$$f : \mathbb{F}_2^4 \to \mathbb{F}_2$$

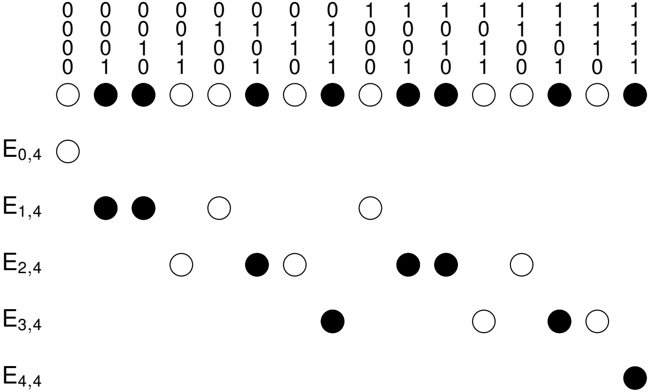


Balanced



Example:

$$f\colon \mathbb{F}_2^4 \to \mathbb{F}_2$$



$$\mathrm{E}_{k,n} = \{x \in \mathbb{F}_2^n \mid \mathrm{w_H}(x) = k\}$$

Weightwise perfectly balanced functions

Weightwise Perfectly Balanced function (WPB) [CMR17]

Let $n \in \mathbb{N}^*$, f is called WPB if:

- for all $k \in [1, n-1]$:
$$|\mathrm{supp}(f) \cap \mathrm{E}_{k,n}| = |\mathrm{E}_{k,n}|/2,$$
- $f(\mathbf{0}) = 0$, $f(\mathbf{1}) = 1$.

Weightwise perfectly balanced functions

Weightwise Perfectly Balanced function (WPB) [CMR17]

Let $n \in \mathbb{N}^*$, f is called WPB if:

- for all $k \in [1, n-1]$:
$$|\mathrm{supp}(f) \cap \mathsf{E}_{k,n}| = |\mathsf{E}_{k,n}|/2,$$
- $f(\mathbf{0}) = 0$, $f(\mathbf{1}) = 1$.

Weightwise Almost Perfectly Balanced:

$$\forall k \in [0, n], \quad \big|\,|\mathrm{supp}(f) \cap \mathsf{E}_{k,n}| - |\mathrm{supp}(f+1) \cap \mathsf{E}_{k,n}|\,\big| \leq 1$$

Weightwise perfectly balanced functions

Weightwise Perfectly Balanced function (WPB) [CMR17]

Let $n \in \mathbb{N}^*$, f is called WPB if:

- for all $k \in [1, n-1]$:
$$|\mathrm{supp}(f) \cap \mathsf{E}_{k,n}| = |\mathsf{E}_{k,n}|/2,$$
- $f(\mathbf{0}) = 0$, $f(\mathbf{1}) = 1$.

Weightwise Almost Perfectly Balanced:

$$\forall k \in [0, n], \quad \Big| |\mathrm{supp}(f) \cap \mathsf{E}_{k,n}| - |\mathrm{supp}(f+1) \cap \mathsf{E}_{k,n}| \Big| \leq 1$$

Motivations:

- cipher FLIP [MJSC16],
- properties on Boolean functions on restricted sets [CMR17],
- link with side channels: leakage of $\mathrm{w_H}(x)$ and $f(x)$.

State of the art

Various constructions:

CMR17, LM19, TL19, LS20, MS21, MSL21, Su21, ZS21, GM22b, GS22, MCL22, MPJDL22, MSLZ22, DM23, YCLXHJZ23, ZS23, ZJZQ23, ZLCQZ23, DM24, GM24,...

Study of main cryptographic parameters:

- Nonlinearity [GM23a],
  -> minimum distance between f and an affine function.
- Weightwise nonlinearity [GM22a],
  -> minimum distance between f and an affine function considered only on the slice.
- Algebraic immunity [GM23b],
  -> minimum degree of g such that $fg = 0$ (or $(f + 1)g = 0$).

State of the art

Main issues:

- mostly WPBs,
- difficult to implement,
- some low parameters.

Contributions:

- new families of WPB and WAPB functions,
- easier to implement,
- good nonlinearities, high algebraic immunities.

Summary

Orders on binary strings

Order

Let X be a set, the binary relation $\preceq$ is called partial order if it is:

- reflexive, $\forall a \in X, \quad a \preceq a$
- transitive, $\forall a, b, c \in X, \quad a \preceq b$ and $b \preceq c \Rightarrow a \preceq c$
- antisymmetric, $\forall a, b \in X \quad a \preceq b$ and $b \preceq a \Rightarrow a = b$.

It is a total order if $\forall a, b \in X$ it holds $a \preceq b$ or $b \preceq a$.

Orders on binary strings

Order

Let X be a set, the binary relation $\preceq$ is called partial order if it is:

- reflexive,
- transitive,
- antisymmetric,

It is a total order if $\forall a, b \in X$ it holds $a \preceq b$ or $b \preceq a$.

Examples:

- Lexicographic: $a, b \in \mathbb{F}_2^n$, $a = (a_1, \cdots, a_n)$, $b = (b_1, \cdots, b_n)$

$$a \preceq b \Leftrightarrow a_i < b_i \text{ on the first index such that } a_i \neq b_i, \text{ or } a = b.$$

$$000 \preceq 001 \preceq 010 \preceq 011 \preceq 100 \preceq 101 \preceq 110 \preceq 111$$

- Cool: choose a first element, apply successive rule:
  - i minimum value such that $(a_i, a_{i+1}) = (1, 0)$ and $i > 1$.
  - If i exists, rotate i bits, otherwise flip a_1 and rotate $n - 1$ bits.

$$000 \preceq 001 \preceq 011 \preceq 111 \preceq 110 \preceq 101 \preceq 010 \preceq 100$$

Construction 1

Description:

- $n = 2^m$
- m orders: order $\preceq_i$ on $\mathbb{F}_2^{2^i}$, for $i \in [0, m-1]$
- Recursive definition:

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

$z = \mathbf{0}$ $\rightarrow f_m(z) = 0$

Construction 1

Description:

- $n = 2^m$
- m orders: order $\preceq_i$ on $\mathbb{F}_2^{2^i}$, for $i \in [0, m-1]$
- Recursive definition:

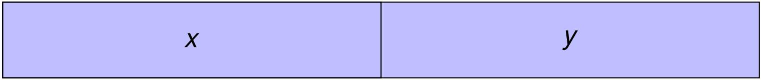
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

$z = \mathbf{1}$ $\rightarrow f_m(z) = 1$

Construction 1

Description:

- $n = 2^m$
- m orders: order $\preceq_i$ on $\mathbb{F}_2^{2^i}$, for $i \in [0, m-1]$
- Recursive definition:

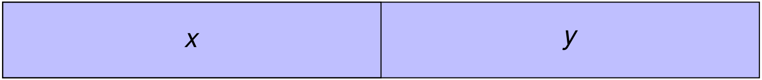


$x \prec_{m-1} y$ $\rightarrow f_m(x, y) = 0$

Construction 1

Description:

- $n = 2^m$
- m orders: order $\preceq_i$ on $\mathbb{F}_2^{2^i}$, for $i \in [0, m-1]$
- Recursive definition:

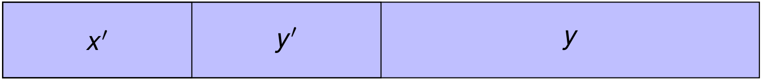


$y \prec_{m-1} x \quad \rightarrow f_m(x, y) = 1$

Construction 1

Description:

- $n = 2^m$
- m orders: order $\preceq_i$ on $\mathbb{F}_2^{2^i}$, for $i \in [0, m-1]$
- Recursive definition:

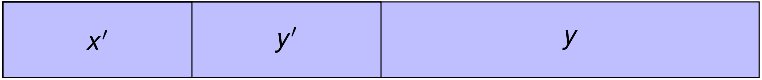


$x = y = (x', y') \quad \rightarrow f_m(x, y) = f_{m-1}(x', y')$

Construction 1

Description:

- $n = 2^m$
- m orders: order $\preceq_i$ on $\mathbb{F}_2^{2^i}$, for $i \in [0, m-1]$
- Recursive definition:



$x = y = (x', y')$ $\rightarrow f_m(x, y) = f_{m-1}(x', y')$

Intuition WPB property:
In a slice $\mathrm{E}_{k,n}$:
$(x, y) \in \mathrm{E}_{k,n} \Rightarrow (y, x) \in \mathrm{E}_{k,n}$

- If $x \neq y$, one is in $\mathrm{supp}(f_m)$ one is not,
- if $x = y$, $f_m(x, x)$ from $f_{m-1}(x)$ which is WPB.

Construction 2

Description:

- $n = 2^m$
- 2 orders: $\preceq$ and $\preceq'$ on $\mathbb{F}_2^{2^{m-1}}$,
  $\preceq'$ such that u is the 2^{m-2}-th element in this order, and half elements of each slice are smaller than u.
- Definition:
  - $g_m(\mathbf{0}) = 0$, $g_m(\mathbf{1}) = 1$,
  -
$$g_m(x, y) = \begin{cases} 0 & \text{if } x \prec y, \\ 1 & \text{if } y \prec x, \\ 0 \text{ if } x \preceq' u, 1 \text{ otherwise} & \text{if } x = y. \end{cases}$$

Construction 2

Description:

- $n = 2^m$
- 2 orders: $\preceq$ and $\preceq'$ on $\mathbb{F}_2^{2^{m-1}}$,
  $\preceq'$ such that u is the 2^{m-2}-th element in this order, and half elements of each slice are smaller than u.
- Definition:
  - $g_m(\mathbf{0}) = 0$, $g_m(\mathbf{1}) = 1$,
  - $$g_m(x, y) = \begin{cases} 0 & \text{if } x \prec y, \\ 1 & \text{if } y \prec x, \\ 0 \text{ if } x \preceq' u, 1 \text{ otherwise} & \text{if } x = y. \end{cases}$$

Intuition WPB property:
In a slice $\mathsf{E}_{k,n}$:
$(x, y) \in \mathsf{E}_{k,n} \Rightarrow (y, x) \in \mathsf{E}_{k,n}$

- If $x \neq y$, one is in $\mathrm{supp}(f_m)$ one is not,
- if $x = y$, by definition of $\preceq'$ half of (x, x) sent to 0.

Nonlinearity bounds

Nonlinearity

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

Nonlinearity bounds

Nonlinearity

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

Theorem:
$m \in \mathbb{N}^*$, $n = 2^m$ and f be any function from Constructions 1 and 2:

$$\mathrm{NL}(f) \ge 2^{n-2} - 2^{n/2-1}.$$

Nonlinearity bounds

Nonlinearity

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

Theorem:
$m \in \mathbb{N}^*$, $n = 2^m$ and f be any function from Constructions 1 and 2:

$$\mathrm{NL}(f) \geq 2^{n-2} - 2^{n/2-1}.$$

Weightwise nonlinearity:

$$\mathrm{NL}_k(f) = \min_{g,\, \deg(g) \leq 1} \{\mathrm{d}_{\mathrm{H},\mathrm{E}_{k,n}}(f, g)\} = \frac{|\mathrm{E}_{k,n}|}{2} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \Big| \sum_{x \in \mathrm{E}_{k,n}} (-1)^{f(x)+a\cdot x} \Big|.$$

$\rightarrow$ lower bound on the NL_k using Krawtchouk polynomials.

Extending to WAPB, Construction 3

Description:

- $n \in \mathbb{N}$, $n \geq 2$
- $\lfloor \log_2(n) \rfloor$ orders: order $\preceq_{\lfloor n/(2^i) \rfloor}$ on $\mathbb{F}_2^{2^{\lfloor n/(2^i) \rfloor}}$, for $i \in [1, \lfloor \log_2(n) \rfloor]$
- Recursive definition:
  Let f_n be the n-variable function defined as:
  - if $n = 1$, $f_1(0) = 0$ and $f_1(1) = 1$,
  - if n is odd, $f_n(x_1, \ldots, x_n) = f_{n-1}(x_1, \ldots, x_{n-1})$,
  - write $z \in \mathbb{F}_2^n$ as (x, y) where $x, y \in \mathbb{F}_2^{n/2}$,

$$f_n(x, y) = \begin{cases} f_{n/2}(x) & \text{if } x = y, \\ 0 & \text{if } x \prec_{n/2} y, \\ 1 & \text{if } y \prec_{n/2} x. \end{cases}$$

Extending to WAPB, Construction 3

Description:

- $n \in \mathbb{N}$, $n \geq 2$
- $\lfloor \log_2(n) \rfloor$ orders: order $\preceq_{\lfloor n/(2^i) \rfloor}$ on $\mathbb{F}_2^{2^{\lfloor n/(2^i) \rfloor}}$, for $i \in [1, \lfloor \log_2(n) \rfloor]$
- Recursive definition:
  Let f_n be the n-variable function defined as:
  - if $n = 1$, $f_1(0) = 0$ and $f_1(1) = 1$,
  - if n is odd, $f_n(x_1, \ldots, x_n) = f_{n-1}(x_1, \ldots, x_{n-1})$,
  - write $z \in \mathbb{F}_2^n$ as (x, y) where $x, y \in \mathbb{F}_2^{n/2}$,

$$f_n(x, y) = \begin{cases} f_{n/2}(x) & \text{if } x = y, \\ 0 & \text{if } x \prec_{n/2} y, \\ 1 & \text{if } y \prec_{n/2} x. \end{cases}$$

Intuition WAPB property:

- n even: split in 2 sets as for Construction 1,
- n odd: using Siegenthaler's decomposition.

Summary

Common orders

Tries with Lexicographic and Cool order, n up to 16.

$\rightarrow$ low parameters.

Common orders

Tries with Lexicographic and Cool order, n up to 16.

$\rightarrow$ low parameters.

Proposition:
$n = 2^m$, $m \geq 2$ and f be any BF from Construction 1 or 2 with Lexicographic order on $\mathbb{F}_2^{2^{m-1}}$:

$$\mathrm{AI}(f) = 2, \quad \text{and} \quad \forall k \in [1, 2^m - 1]\ \mathrm{AI}_k(f) \leq 2.$$

$\rightarrow$ worst possible AI.

Weightwise orders

Weightwise order

Order $\preceq$ such that for all $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^n$:

$$\mathrm{w_H}(x) < \mathrm{w_H}(y) \Rightarrow x \prec y.$$

Weightwise orders

Weightwise order

Order $\preceq$ such that for all $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^n$:

$$\mathrm{w_H}(x) < \mathrm{w_H}(y) \Rightarrow x \prec y.$$

$\rightarrow$ better algebraic immunity

Proposition:
$n = 2^m$, $m \geq 2$ and f be any BF from Construction 1 or 2 with a weightwise order on $\mathbb{F}_2^{2^{m-1}}$:

$$\mathrm{AI}(f) = 2^{m-1}.$$

$\rightarrow$ optimal AI.

Field-based orders

Field-based order

$r \in \mathbb{N}^*$, $s \in \mathbb{N}$ such that $s \leq 2^r - 2$ and α a primitive element of $\mathbb{F}_{2^r}$,
we call field order defined by α and s the total order over $\mathbb{F}_2^r$ given by:

$$\alpha^s \prec \alpha^{s+1} \prec \ldots \prec \alpha^{2^r-2} \prec 0 \prec 1 \prec \ldots \prec \alpha^{s-2} \prec \alpha^{s-1}.$$

Field-based orders

Field-based order

$r \in \mathbb{N}^*$, $s \in \mathbb{N}$ such that $s \leq 2^r - 2$ and α a primitive element of $\mathbb{F}_{2^r}$,
we call field order defined by α and s the total order over $\mathbb{F}_2^r$ given by:

$$\alpha^s \prec \alpha^{s+1} \prec \ldots \prec \alpha^{2^r-2} \prec 0 \prec 1 \prec \ldots \prec \alpha^{s-2} \prec \alpha^{s-1}.$$

$\rightarrow$ Good parameters for both nonlinearities and algebraic immunities

Parameter comparisons

Comparisons for $n = 8, 10, 12, 14, 16$ between the different order based.

Parameter comparisons

Comparisons for $n = 8, 10, 12, 14, 16$ between the different order based.

Comparisons with SOTA for field based order:

$n = 8$

	res	deg	NL	AI	NL_2	NL_3	NL_4	AI_2	AI_3	AI_4
Field based	0	7	92	4	6	15	24	2	2	3
SOTA	0	7	116	4	9	22	28	2	2	3

Parameter comparisons

Comparisons for $n = 8, 10, 12, 14, 16$ between the different order based.

Comparisons with SOTA for field based order:

$n = 8$

	res	deg	NL	AI	NL_2	NL_3	NL_4	AI_2	AI_3	AI_4
Field based	0	7	92	4	6	15	24	2	2	3
SOTA	0	7	116	4	9	22	28	2	2	3

$n = 16$

	res	NL	NL_2	NL_3	NL_4	NL_5	NL_6	NL_7	NL_8
FB	0	30196	40	219	765	1887	3518	5138	5875
SOTA	0	32598	40	219	765	1887	3629	5138	5875

	deg	AI	AI_2	AI_3	AI_4	AI_5	AI_6	AI_7	AI_8
FB	15	8	2	3	4	4	5	6	6
SOTA	15	8	2	3	4	4	5	6	6

Parameter comparisons

Comparisons for $n = 8, 10, 12, 14, 16$ between the different order based.

Comparisons with SOTA for field based order:

$n = 8$

	res	deg	NL	AI	NL_2	NL_3	NL_4	AI_2	AI_3	AI_4
Field based	0	7	92	4	6	15	24	2	2	3
SOTA	0	7	116	4	9	22	28	2	2	3

$n = 16$

	res	NL	NL_2	NL_3	NL_4	NL_5	NL_6	NL_7	NL_8
FB	0	30196	40	219	765	1887	3518	5138	5875
SOTA	0	32598	40	219	765	1887	3629	5138	5875

	deg	AI	AI_2	AI_3	AI_4	AI_5	AI_6	AI_7	AI_8
FB	15	8	2	3	4	4	5	6	6
SOTA	15	8	2	3	4	4	5	6	6

best known parameter, optimal value

Summary

Conclusion and open questions

Conclusion:

- 3 W(A)PB constructions based on the notion of total orders,
- proven bounds on relevant cryptographic parameters,
- experimental studies and improvements on the SOTA.

Conclusion and open questions

Conclusion:

- 3 W(A)PB constructions based on the notion of total orders,
- proven bounds on relevant cryptographic parameters,
- experimental studies and improvements on the SOTA.

Open questions:

- NL bound on the entire family; better bound on a subfamily?
- Determine the maximum achievable AI_k.

Conclusion and open questions

Conclusion:

- 3 W(A)PB constructions based on the notion of total orders,
- proven bounds on relevant cryptographic parameters,
- experimental studies and improvements on the SOTA.

Open questions:

- NL bound on the entire family; better bound on a subfamily?
- Determine the maximum achievable AI_k.

Thank you!