$\mathcal{S}_0$-equivalent classes, a new direction to find better weightwise perfectly balanced functions, and more

Agnese Gini and Pierrick Méaux

University of Luxembourg

BFA - September 3rd, 2023

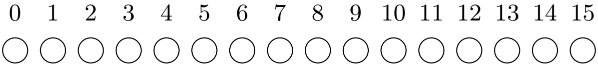
securityandtrust.lu

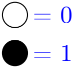
UNIVERSITÉ DU LUXEMBOURG

$\mathcal{S}_0$-equivalent classes, a new direction to find better weightwise perfectly balanced (WPB) functions , and more

A sketch is better!

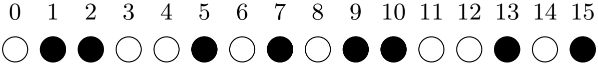
$$f\colon \mathbb{F}_2^4 \to \mathbb{F}_2$$



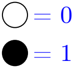


A sketch is better!

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

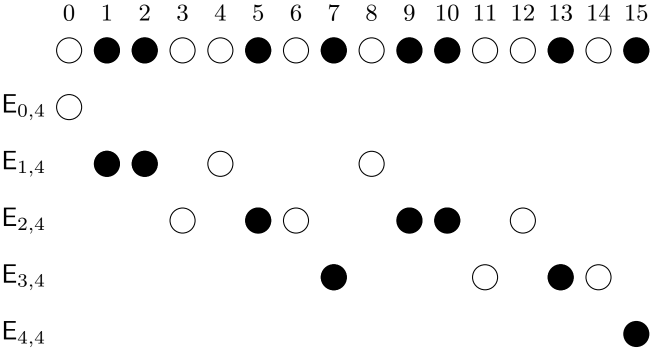


Balanced



A sketch is better!

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



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

WPB functions

Weightwise Perfectly Balanced Function (WPB)[CMR17]

Let $n \in \mathbb{N}^+$ and f be a n-variables Boolean functions. We require for every $k \in [1, n-1]$ f being balanced on the slice k, i.e. for $k = 1, \ldots, n-1$

$$|\mathsf{supp}(f_{|\mathsf{E}_{k,n}})| = |\mathsf{E}_{k,n}|/2$$

and $f(\mathbf{0}) = 0$ and $f(\mathbf{1}) = 1$.

- Why? FLIP stream cipher [MJSC16] filter function has Hamming weight invariant input.

WPB functions

Weightwise Perfectly Balanced Function (WPB)[CMR17]

Let $n \in \mathbb{N}^+$ and f be a n-variables Boolean functions. We require for every $k \in [1, n-1]$ f being balanced on the slice k, i.e. for $k = 1, \ldots, n-1$

$$|\mathsf{supp}(f_{|\mathsf{E}_{k,n}})| = |\mathsf{E}_{k,n}|/2$$

and $f(\mathbf{0}) = 0$ and $f(\mathbf{1}) = 1$.

- Why? FLIP stream cipher [MJSC16] filter function has Hamming weight invariant input.
- WPB functions exist only if $n = 2^m$. Other cases, we consider WAPB function.

Cryptographic criteria

Study the properties of Boolean functions applied only on a subset, *e.g.* $\mathsf{E}_{k,n}$.

Global cryptographic criteria:

- balancedness,
- nonlinearity (NL),
- degree (deg),
- algebraic immunity (AI).

Restricted cryptographic criteria:

- restricted balancedness,
- restricted nonlinearity (*e.g.*, NL_k),
- restricted degree,
- restricted algebraic immunity (*e.g.*, AI_k).

Cryptographic criteria

Study the properties of Boolean functions applied only on a subset, *e.g.* $\mathsf{E}_{k,n}$.

Global cryptographic criteria:

- balancedness,
- nonlinearity (NL),
- degree (deg),
- algebraic immunity (AI).

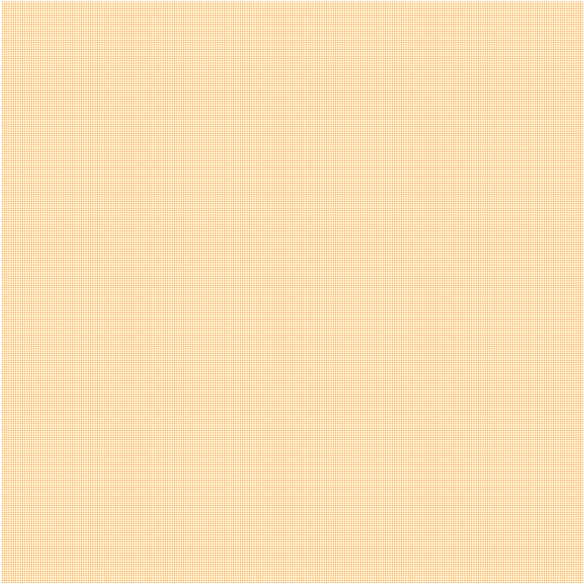
Restricted cryptographic criteria:

- restricted balancedness,
- restricted nonlinearity (*e.g.*, NL_k),
- restricted degree,
- restricted algebraic immunity (*e.g.*, AI_k).

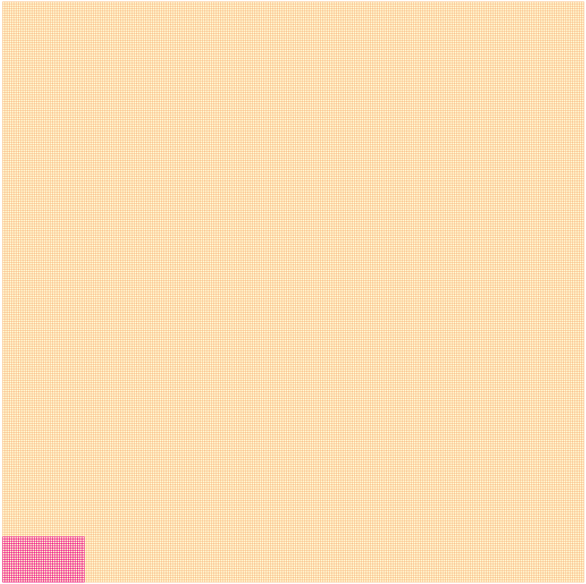
Many constructions and related works since [CMR17]: *e.g.*, [LM19, TL19, LS20, MS21, ZS21, MSL21, GS22, ZS22, MPJ$^+$22, GM22a, GM22b, MKCL22, MSLZ22, GM23a, ZJZQ23, ZLC$^+$23, GM23b, YCL$^+$23]

$\mathcal{S}_0$-equivalent classes, a new direction to find better weightwise perfectly balanced (WPB) functions, and more

Boolean functions in n variables $\mathcal{B}_n$

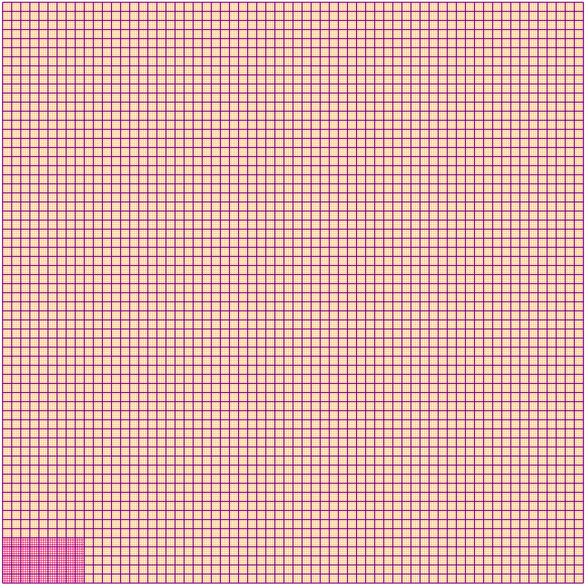


Boolean functions in n variables $\mathcal{B}_n$



$\mathcal{WPB}_m$

Boolean functions in n variables $\mathcal{B}_n$



$\mathcal{WPB}_m$

Strategy: successive refinement

1. Define a suitable partition
2. Search for a desirable class □
3. Search for a function □ inside the class

We want:

- every function in the same class $\square$ to satisfy some given properties $P_1, \ldots, P_r$. For example:
  - $P_i =$ "being WPB",
  - $P_i =$ "having the same NL",
  - $P_i =$ "having the same NL_3 ".
- the partition to be computationally convenient. For example:
  - compact representation,
  - efficient computations inside classes,
  - application friendly,
  - …

$\mathcal{S}_0$-equivalent classes, a new direction to find better weightwise perfectly balanced (WPB) functions, and more

Symmetric function

A Boolean function is called *symmetric* if every output is invariant under permutation of its input bits.

Proposition

A function is symmetric $\Leftrightarrow$ it's constant on each slice $\mathsf{E}_{k,n}$ for $k \in [0, n]$.

Let $n = 2^m$ for $m \in \mathbb{N}^+$ and consider the subset of symmetric functions

$$\mathcal{S}_0 = \{\sigma \in \mathcal{SYM}_n : \sigma(\mathbf{0}) = \sigma(\mathbf{1}) = 0\}$$

Let $n = 2^m$ for $m \in \mathbb{N}^+$ and consider the subset of symmetric functions

$$\mathcal{S}_0 = \{\sigma \in \mathcal{SYM}_n : \sigma(\mathbf{0}) = \sigma(\mathbf{1}) = 0\}$$

$\mathcal{S}_0$-equivalence relation

Let f, g be Boolean functions in n variables.

- f, g are called $\mathcal{S}_0$-*equivalent* $\Leftrightarrow \exists \sigma \in \mathcal{S}_0$ such that $f = g + \sigma$.
- $\mathcal{S}_0(f)$ is the $\mathcal{S}_0$-*class* of f, *i.e.* the set of functions $\mathcal{S}_0$-equivalent to f.

- Being $\mathcal{S}_0$-equivalent is an equivalence relation.

- $\{\mathcal{S}_0(f) : f \in \mathcal{B}_n\}$ is partition such that
  $P_1 :$ If $f \in \mathcal{WPB}_m,\ \mathcal{S}_0(f) \subseteq \mathcal{WPB}_m$.
  $P_2 :$ If $f \in \mathcal{WAPB}_n,\ \mathcal{S}_0(f) \subseteq \mathcal{WAPB}_n$.

- Being $\mathcal{S}_0$-equivalent is an equivalence relation.

- $\{\mathcal{S}_0(f) : f \in \mathcal{B}_n\}$ is partition such that

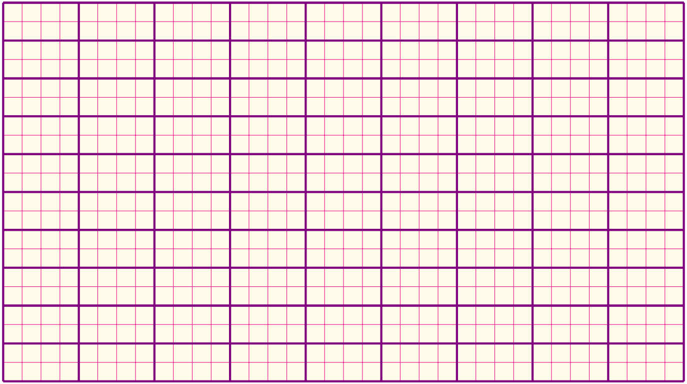
  P_1 : If $f \in \mathcal{WPB}_m$, $\mathcal{S}_0(f) \subseteq \mathcal{WPB}_m$.

  P_2 : If $f \in \mathcal{WAPB}_n$, $\mathcal{S}_0(f) \subseteq \mathcal{WAPB}_n$.

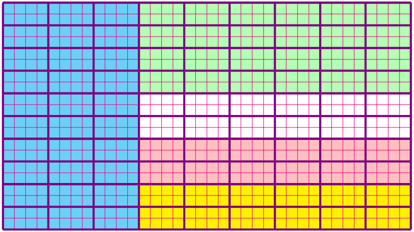
  P_3 : For every $k \in [0, n]$ it holds $\mathsf{AI}_k(f) = \mathsf{AI}_k(g)$ for every f, g $\mathcal{S}_0$-equivalent.

  P_4 : For every $k \in [0, n]$ it holds $\mathsf{NL}_k(f) = \mathsf{NL}_k(g)$ for every f, g $\mathcal{S}_0$-equivalent.

In 4 variables



$\mathcal{WPB}_2$



$\mathcal{WPB}_2$

$\mathsf{NL}_2, \mathsf{NL}, \mathsf{deg}$	$\#\mathcal{S}_0$-classes	
$1, \{4\}, \{3\}$	30	
$1, \{2,4\}, \{3\}$	12	
$1, \{4\}, \{2,3\}$	12	
$0, \{2,4\}, \{2,3\}$	12	
$0, \{2,4\}, \{3\}$	24	

Behaviour inside $\mathcal{S}_0$-classes

What is the best guaranteed value achievable by modifying a WPB function, while staying within its $\mathcal{S}_0$-class?

$$\mathsf{mAI}\mathcal{S}_0(m) = \min_{f \in \mathcal{WPB}_m} \max_{g \in \mathcal{S}_0(f)} \mathsf{AI}(g),$$

$$\mathsf{mNL}\mathcal{S}_0(m) = \min_{f \in \mathcal{WPB}_m} \max_{g \in \mathcal{S}_0(f)} \mathsf{NL}(g),$$

$$\mathsf{mdeg}\mathcal{S}_0(m) = \min_{f \in \mathcal{WPB}_m} \max_{g \in \mathcal{S}_0(f)} \mathsf{deg}(g).$$

Mem: $n = 2^m$ variables.

Behaviour inside $\mathcal{S}_0$-classes

We can prove:

Algebraic immunity

Let $t \in \mathbb{N}$, $t \geq 2$, if $m > \log(2t+1) + t + 1 + (t \mod 2)$ then

$$\mathsf{mAI}\mathcal{S}_0(m) \geq t + 1.$$

Nonlinearity

$$\mathsf{mNL}\mathcal{S}_0(m) \geq 2^{n-2} - 2^{\frac{n}{2}-2}.$$

Degree

$$\mathsf{mdeg}\mathcal{S}_0(m) = n - 1$$

$\mathcal{S}_0$-equivalent classes, a new direction to find better weightwise perfectly balanced (WPB) functions, and more

Degree

- We can exactly describe the behaviour of the degree inside $\mathcal{S}_0(f)$ by looking at the ANF of f.
- We construct for any value between $n/2$ and $n-1$ (included) a WPB functions reaching this degree.
- We show that more than half of WPB functions have degree $n-1$.

More than just a summary

- We described the *successive refinement* strategy to find functions with good properties.
- We introduced the notion of $\mathcal{S}_0$-equivalent classes.
- Explain how to use it to find better WPB functions.
- We gave lower bounds for nonlinearity and algebraic immunity inside $\mathcal{S}_0$-classes.
  (*The proofs of these bounds hold for functions that are not WPB*)
- We observed that the distribution of degree inside a class of a WPB can be fully described.
- We presented experimental results: a taxonomy of 4-variable classes; *for 8 variables we analysed $\mathcal{S}_0$-classes of some functions from known families, such as [CMR17, LM19, TL19, GM23a, GM23b].*

More than just a summary: open questions

- In the full version of this work outline a possible extension to other equivalence relations defined up to the addition of functions from a family $\mathcal{T}$. For cryptographic application a family $\mathcal{T}$ easy to compute!
- Improve our bounds on $\mathsf{mAI}\mathcal{S}_0(m)$ and $\mathsf{mNL}\mathcal{S}_0(m)$. For instance, $\mathsf{mAI}\mathcal{S}_0(m) = 2^{m-1}$?
- Improve computational aspects: *e.g.*
  - speed up the search inside equivalence classes;
  - improve algorithms for cryptographic criteria.

Thank you for your attention!

Full paper: `https://ia.cr/2023/1101`

`https://github.com/agnesegini/WAPB_pub`

References I

[CMR17] 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.

[GM22a] Agnese Gini and Pierrick Méaux. On the weightwise nonlinearity of weightwise perfectly balanced functions. *Discret. Appl. Math.*, 322:320–341, 2022.

[GM22b] Agnese Gini and Pierrick Méaux. Weightwise almost perfectly balanced functions: Secondary constructions for all n and better weightwise nonlinearities. In Takanori Isobe and Santanu Sarkar, editors, *Progress in Cryptology - INDOCRYPT*, volume 13774 of *Lecture Notes in Computer Science*, pages 492–514. Springer, 2022.

[GM23a] Agnese Gini and Pierrick Méaux. Weightwise perfectly balanced functions and nonlinearity. In Said El Hajji, Sihem Mesnager, and El Mamoun Souidi, editors, *Codes, Cryptology and Information Security*, pages 338–359, Cham, 2023. Springer Nature Switzerland.

References II

[GM23b] Agnese Gini and Pierrick Méaux. On the algebraic immunity of weightwise perfectly balanced functions. Cryptology ePrint Archive, Paper 2023/495, 2023. `https://eprint.iacr.org/2023/495`.

[GS22] Xiaoqi Guo and Sihong Su. Construction of weightwise almost perfectly balanced boolean functions on an arbitrary number of variables. *Discrete Applied Mathematics*, 307:102–114, 2022.

[LM19] Jian Liu and Sihem Mesnager. Weightwise perfectly balanced functions with high weightwise nonlinearity profile. *Des. Codes Cryptogr.*, 87(8):1797–1813, 2019.

[LS20] Jingjing Li and Sihong Su. Construction of weightwise perfectly balanced boolean functions with high weightwise nonlinearity. *Discret. Appl. Math.*, 279:218–227, 2020.

[MJSC16] Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet. Towards stream ciphers for efficient FHE with low-noise ciphertexts. pages 311–343, 2016.

References III

[MKCL22] Sara Mandujano, Juan Carlos Ku Cauich, and Adriana Lara. Studying special operators for the application of evolutionary algorithms in the seek of optimal boolean functions for cryptography. In Obdulia Pichardo Lagunas, Juan Martínez-Miranda, and Bella Martínez Seis, editors, *Advances in Computational Intelligence*, pages 383–396, Cham, 2022. Springer Nature Switzerland.

[MPJ+22] Luca Mariot, Stjepan Picek, Domagoj Jakobovic, Marko Djurasevic, and Alberto Leporati. Evolutionary construction of perfectly balanced boolean functions. In *2022 IEEE Congress on Evolutionary Computation (CEC)*, page 1–8. IEEE Press, 2022.

[MS21] Sihem Mesnager and Sihong Su. On constructions of weightwise perfectly balanced boolean functions. *Cryptography and Communications*, 2021.

[MSL21] Sihem Mesnager, Sihong Su, and Jingjing Li. On concrete constructions of weightwise perfectly balanced functions with optimal algebraic immunity and high weightwise nonlinearity. *Boolean Functions and Applications*, 2021.

References IV

[MSLZ22] Sihem Mesnager, Sihong Su, Jingjing Li, and Linya Zhu. Concrete constructions of weightwise perfectly balanced (2-rotation symmetric) functions with optimal algebraic immunity and high weightwise nonlinearity. *Cryptogr. Commun.*, 14(6):1371–1389, 2022.

[SZZ93] Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. Nonlinearly balanced boolean functions and their propagation characteristics (extended abstract). In Douglas R. Stinson, editor, *Advances in Cryptology - CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, pages 49–60. Springer, 1993.

[TL19] Deng Tang and Jian Liu. A family of weightwise (almost) perfectly balanced boolean functions with optimal algebraic immunity. *Cryptogr. Commun.*, 11(6):1185–1197, 2019.

[YCL+23] Lili Yan, Jingyi Cui, Jian Liu, Guangquan Xu, Lidong Han, Alireza Jolfaei, and Xi Zheng. Iga: An improved genetic algorithm to construct weightwise (almost) perfectly balanced boolean functions with high weightwise nonlinearity. In *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security*, ASIA CCS '23, page 638–648, New York, NY, USA, 2023. Association for Computing Machinery.

[ZJZQ23] Qinglan Zhao, Yu Jia, Dong Zheng, and Baodong Qin. A new construction of weightwise perfectly balanced functions with high weightwise nonlinearity. *Mathematics*, 11(5), 2023.

[ZLC+23] Qinglan Zhao, Mengran Li, Zhixiong Chen, Baodong Qin, and Dong Zheng. A unified construction of weightwise perfectly balanced boolean functions. Cryptology ePrint Archive, Paper 2023/460, 2023. `https://eprint.iacr.org/2023/460`.

[ZS21] Rui Zhang and Sihong Su. A new construction of weightwise perfectly balanced boolean functions. *Advances in Mathematics of Communications*, 0:–, 2021.

[ZS22] 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.