Title

Luca Bonnamino, Pierrick Méaux

Luxembourg university, Luxembourg
pierrick.meaux@uni.lu

Abstract. **Keywords:** Boolean functions, Weightwise perfectly balanced functions, Cryptographic criteria.

1 Introduction

[**PM:** recall here the main idea of finding AI and rank of Reed Muller code, maybe re-read the explanation in "Extreme algebraic attacks"]

[**LB:** example]

2 Preliminaries

For readability, we use the notation $+$ instead of $\oplus$ to denote the addition in $\mathbb{F}_2$, and $\sum$ instead of $\bigoplus$. In addition to classic notations, we denote by $[a, b]$ the subset of all integers between a and b: $\{a, a+1, \ldots, b\}$. For a vector $v \in \mathbb{F}_2^n$ we use $\mathsf{w_H}(v)$ to denote its Hamming weight $\mathsf{w_H}(v) = |\{i \in [1, n] \,|\, v_i = 1\}|$. For two vectors v and w in $\mathbb{F}_2^n$ we denote by $\mathsf{d_H}(v, w)$ the Hamming distance between v and w, that is, $\mathsf{d_H}(v, w) = \mathsf{w_H}(v + w)$. For two functions f and g we denote by $\mathsf{d_H}(f, g)$ the Hamming distance between their vectors of values.

2.1 Boolean functions, cryptographic criteria, and weightwise properties

In this section, we recall fundamental concepts concerning Boolean functions and their weightwise properties, which are utilized throughout this article. For a more comprehensive introduction to Boolean functions and their cryptographic parameters, we recommend consulting the book by Carlet [Car21], and for insights into weightwise properties—also known as properties on the slices—the article by [CMR17]. We denote by $\mathsf{E}_{k,n}$ the set $\{x \in \mathbb{F}_2^n \,|\, \mathsf{w_H}(x) = k\}$ for $k \in [0, n]$, referring to it as a slice of the Boolean hypercube (of dimension n). Consequently, the Boolean hypercube is divided into $n + 1$ slices, where the elements share the same Hamming weight.

Definition 1 (Boolean Function). *A Boolean function f in n variables is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The set of all Boolean functions in n variables is denoted by $\mathcal{B}_n$.*

When a property or a definition is restricted to a slice, we denote it by using the subscript k. For example, for an n-variable Boolean function f we denote its support $\mathsf{supp}(f) = \{x \in \mathbb{F}_2^n \,|\, f(x) = 1\}$. Furthermore, we denote by $\mathsf{supp}_k(f)$ the support of f restricted to a slice, which is defined as $\mathsf{supp}(f) \cap \mathsf{E}_{k,n}$.

Definition 2 (Balancedness). *A Boolean function $f \in \mathcal{B}_n$ is called balanced if $|\mathsf{supp}(f)| = 2^{n-1} = |\mathsf{supp}(f + 1)|$.*

For $k \in [0, n]$ the function is said balanced on the slice k if $||\mathsf{supp}_k(f)| - |\mathsf{supp}_k(f + 1)|| \leq 1$. In particular when $|\mathsf{E}_{k,n}|$ is even $|\mathsf{supp}_k(f)| = |\mathsf{supp}_k(f + 1)| = |\mathsf{E}_{k,n}|/2$.

Using the notion of restricted balancedness we can define the weightwise (almost) perfectly balanced functions, the focus of our work.

Definition 3 (Weightwise (Almost) Perfectly Balanced Function (WPB and WAPB)). *Let $m \in \mathbb{N}^*$ and f be a Boolean function in $n = 2^m$ variables. It will be called weightwise perfectly balanced (WPB) if, for every $k \in [1, n-1]$, f is balanced on the slice k, that is $\forall k \in [1, n-1], |\mathsf{supp}_k(f)| = \binom{n}{k}/2$, and:*

$$f(0, \cdots, 0) = 0, \quad \text{and } f(1, \cdots, 1) = 1.$$

The set of WPB functions in 2^m variables is denoted $\mathcal{WPB}_m$.

When n is not a power of 2, other weights than $k = 0$ and n can lead to slices of odd cardinality, we call $f \in \mathcal{B}_n$ weightwise almost perfectly balanced (WAPB) if:

$$|\mathsf{supp}_k(f)| = \begin{cases} |\mathsf{E}_{k,n}|/2 & \text{if } |\mathsf{E}_{k,n}| \text{ is even,} \\ (|\mathsf{E}_{k,n}| \pm 1)/2 & \text{if } |\mathsf{E}_{k,n}| \text{ is odd.} \end{cases}$$

The set of WAPB functions in n variables is denoted $\mathcal{WAPB}_n$.

We define additional crucial concepts for studying Boolean functions, namely the algebraic normal form and the Walsh transform. Subsequently, we introduce key cryptographic criteria for these functions, including algebraic immunity (both general and weightwise) and nonlinearity (both general and weightwise).

Definition 4 (Algebraic Normal Form (ANF) and degree). *We call Algebraic Normal Form of a Boolean function f its n-variable polynomial representation over $\mathbb{F}_2$ (i.e. belonging to $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n)$):*

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq [1,n]} a_I \left(\prod_{i \in I} x_i \right)$$

where $a_I \in \mathbb{F}_2$. The (algebraic) degree of f, denoted $\mathsf{deg}(f)$ is:

$$\mathsf{deg}(f) = \max_{I \subseteq [1,n]} \{|I| \,|\, a_I = 1\} \text{ if } f \text{ is not null}, 0 \text{ otherwise}.$$

Definition 5 (Algebraic immunity and restricted algebraic immunity). *The algebraic immunity of a Boolean function $f \in \mathcal{B}_n$, denoted as $\mathsf{AI}(f)$, is defined as:*

$$\mathsf{AI}(f) = \min_{g \neq 0} \{\mathsf{deg}(g) \mid fg = 0 \text{ or } (f+1)g = 0\},$$

where $\mathsf{deg}(g)$ is the algebraic degree of g. The function g is called an annihilator of f (or $f + 1$).

The restricted algebraic immunity of a Boolean function $f \in \mathcal{B}_n$ on the set $S \subset \mathbb{F}_2^n$, denoted as $\mathsf{AI}_S(f)$, is defined as:

$$\mathsf{AI}_S(f) = \min_{g \neq 0 \text{ over } S} \{\mathsf{deg}(g) \mid fg = 0 \text{ or } (f+1)g = 0\}.$$

For $S = \mathsf{E}_{k,n}$ we denote $\mathsf{AI}_{\mathsf{E}_{k,n}}(f)$ by $\mathsf{AI}_k(f)$ and call it weightwise algebraic immunity.

Definition 6 (Walsh transform and restricted Walsh transform). *Let $f \in \mathcal{B}_n$ be a Boolean function, its Walsh transform W_f at $a \in \mathbb{F}_2^n$ is defined as:*

$$W_f(a) := \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + a \cdot x}.$$

Let $f \in \mathcal{B}_n$, $S \subset \mathbb{F}_2^n$, its Walsh transform restricted to S at $a \in \mathbb{F}_2^n$ is defined as:

$$W_{f,S}(a) := \sum_{x \in S} (-1)^{f(x)+ax}.$$

For $S = \mathsf{E}_{k,n}$ we denote $W_{f,\mathsf{E}_{k,n}}(a)$ by $\mathcal{W}_{f,k}(a)$.

Property 1 (WAPB functions and restricted Walsh transform)**.** *Let $n \in \mathbb{N}^*$, $f \in \mathcal{B}_n$ is WAPB if and only if:*

$$\forall k \in [0,n],\ \mathcal{W}_{f,k}(0_n) = \begin{cases} 0 & \text{if } |\mathsf{E}_{k,n}| \text{ is even,} \\ \pm 1 & \text{if } |\mathsf{E}_{k,n}| \text{ is odd.} \end{cases}$$

If $n = 2^m$ with $m \in \mathbb{N}^*$, $f \in \mathcal{B}_n$ is WPB if and only if:

$$\mathcal{W}_{f,0}(0_n) = 1, \quad \mathcal{W}_{f,n}(0_n) = -1, \text{ and } \quad \forall k \in [1, n-1]\, \mathcal{W}_{f,k}(0_n) = 0.$$

Definition 7 (Nonlinearity and weightwise nonlinearity). *The nonlinearity $\mathsf{NL}(f)$ of a Boolean function $f \in \mathcal{B}_n$, where n is a positive integer, is the minimum Hamming distance between f and all the affine functions in $\mathcal{B}_n$:*

$$\mathsf{NL}(f) = \min_{g,\, \mathsf{deg}(g) \leq 1} \{\mathsf{d_H}(f,g)\},$$

where $g(x) = a \cdot x + \varepsilon$, $a \in \mathbb{F}_2^n, \varepsilon \in \mathbb{F}_2$.

The nonlinearity can also be defined from the Walsh transform:

$$\mathsf{NL}(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |W_f(a)|.$$

For $k \in [0,n]$ we denote NL_k the nonlinearity on the slice k, the minimum Hamming distance between f restricted to $\mathsf{E}_{k,n}$ and the restrictions to $\mathsf{E}_{k,n}$ of affine functions over $\mathbb{F}_2^n$. Accordingly:

$$\mathsf{NL}_k(f) = \min_{g,\, \mathsf{deg}(g) \leq 1} |\mathsf{supp}_k(f+g)|.$$

Property 2 (Nonlinearity on the slice, adapted from [CMR17], Proposition 6)**.** *Let $n \in \mathbb{N}^*, k \in [0,n]$, for every n-variable Boolean function f over $\mathsf{E}_{k,n}$:*

$$\mathsf{NL}_k(f) = \frac{|\mathsf{E}_{k,n}|}{2} - \frac{\max_{a \in \mathbb{F}_2^n} |\mathcal{W}_{f,k}(a)|}{2}.$$

2.2 Krawtchouk polynomials

We use Krawtchouk polynomials and some of their properties to prove one of our results, we give the necessary preliminaries here and refer to *e.g.* [MS78] for more details.

Definition 8 (Krawtchouk Polynomials). *The Krawtchouk polynomial of degree k, with $0 \leq k \leq n$ is given by:* $\mathsf{K}_k(\ell, n) = \sum_{j=0}^{k} (-1)^j \binom{\ell}{j} \binom{n-\ell}{k-j}$.

Property 3 (Krawtchouk polynomials relation)**.** *Let $n \in \mathbb{N}^*$ and $k \in [0,n]$, the following hold: $\mathsf{K}_k(\ell, n)$ is the value of the restricted Walsh transform on $\mathsf{E}_{k,n}$ of any n variable linear function $a \cdot \ell$ such that $\mathsf{w_H}(a) = \ell$.*

Property 4 (Vandermonde Convolution)**.** *Let $a, b, c \in \mathbb{N}$, then:*

$$\binom{a+c}{b} = \sum_{j=0}^{b} \binom{c}{b-j} \binom{a}{j}.$$

2.3 Tang-Liu WPB functions

We recall the construction of WPB functions from Tang and Liu [TL19] and one on its properties. We use these results to prove the algebraic immunity of special cases of our main constructions.

Definition 9 (TL WPB construction (adapted from [TL19], Construction 1)). *Let $m \in \mathbb{N}^*$ and $n = 2^m \geq 4$ be an integer. A TL WPB Boolean function h on n-variable is such that*

- $h(0_n) = 0$ *and* $h(1_n) = 1$
- $h(x, y) = 0$ *if* $\mathsf{w_H}(x) < \mathsf{w_H}(y)$.
- $h(x, y) = 1$ *if* $\mathsf{w_H}(x) > \mathsf{w_H}(y)$.
- *the cardinality of* $U_i = \mathsf{supp}(h) \cap \left\{(x, y) \in \mathbb{F}_2^{2^{m-1}} \times \mathbb{F}_2^{2^{m-1}} : \mathsf{w_H}(x) = \mathsf{w_H}(y) = j\right\}$ *is exactly* $\binom{2^{m-1}}{j}^2/2$ *for all* $0 < j < 2^{m-1}$.

Remark 1. Despite Definition 9 may appear quite different respect the original paper, it is equivalent when considering the restriction on n to be a power of two, and the values in 0_n and 1_n imposed by Definition 3.

Property 5 (TL WPB functions properties [TL19])**.** *Let $m \in \mathbb{N}^*$ and $n = 2^m$, a n-variable TL function h_n has optimal algebraic immunity* $\mathsf{AI}(h_n) = \frac{n}{2}$.

3 Computing the restricted AI from generator matrices of Reed-Muller punctured codes

[**PM:** mostly one algorithm, or in 2 parts but 1 page max, then proposition that justify it gives the lowest degree annihilator.]

Algorithm 1 Algorithm to find the algebraic immunity of a function f on the restricted set $S \subseteq \mathbb{F}_2^n$

Input: $x \in \mathbb{F}_2^{2^n}$ truth table of $f \in B_n$
Output: $AI_S(f)$

Function *construct_S_f_and_g_generators*(x, n, S)
  function body
  return $matrix_1, matrix_2, matrix_3$
End Function

$m_{max}, D^{\leq n_{max,res}} \leftarrow$ *read_values_from_file*()
$G^{f_{res},S}_{rows,n}, G^{(f\oplus 1)_{res},S}_{rows,n}, G^{S}_{n,n} \leftarrow construct\_S\_f\_and\_g\_generators\,(x, n, S)$
$immunity_f, immunity_{f+1} \leftarrow ($
$find\_deg\_smallest\_S\_annihilator(G^{f_{res},S}_{rows,n}, G^{S}_{n,n}, D^{\leq n_{max,res}})$
$\mid find\_deg\_smallest\_S\_annihilator(G^{(f\oplus 1)_{res},S}_{rows,n}, G^{S}_{n,n}, D^{\leq n_{max,res}})$
$)$
▷ // min takes care of $null$ values $\min(immunity_f, null) = immunity_f$ and $\min(null, immunity_{f+1}) = immunity_{f+1}$
return $\min(immunity_f, immunity_{f+1})$

example Construction 2

Construction 2 Construction of 2-RotS WAPB Boolean function

Input: $\pi \in Sn$

Output: A 2-RotS WAPB Boolean function $f_\pi \in \mathcal{B}_n$

```
Initiate supp(f_π) = φ
t = 0
for k ← 0 to n do
    for i ← 1 to g_{k,n} do
        u = ν_{k,n,i}; l = |O_π(u)|
        if l is even then
            for j ← 1 to l/2 do
                supp(f_π).append(u)
                u ← π ∘ π(u)
            end for
        else
            u = π^t(u)
            for j ← 1 to ⌈(l−t)/2⌉ do
                supp(f_π).append(u)
                u ← π ∘ π(u)
            end for
            Update t ← 1 − t
        end if
    end for
end for
return f_π
```

4 Computing the restricted AI iteratively

5 Applications to WAPB functions

6 Conclusion and open questions

References

Car21. Claude Carlet. *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2021.

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), 2017.

MS78. F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-holland Publishing Company, 2nd edition, 1978.

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.