On concrete constructions of weightwise perfectly balanced functions with optimal algebraic immunity and high weightwise nonlinearity

Sihem Mesnager*, Sihong Su**, and Jingjing Li**

*Department of Mathematics, University of Paris VIII, F-93526 Saint-Denis, Laboratory Geometry, Analysis and Applications, LAGA, CNRS, University Sorbonne Paris Nord, CNRS, UMR 7539, F-93430, Villetaneuse, France, and Telecom Paris, Institute Polytechnic 91120 Palaiseau, France. Email: smesnager@univ-paris8.fr
**School of Mathematics and Statistics, Henan University, Kaifeng, 475004, China. Email: sush@henu.edu.cn(S. Su), 1663711127@qq.com(J. Li)

Abstract

Boolean functions satisfying good cryptographic criteria when restricted to the set of vectors with constant Hamming weight play an important role in the known FLIP stream cipher proposed by Méaux et al. at the conference Eurocrypt 2016. After providing a security analysis on the FLIP cipher, those functions were nicely-investigated firstly by Carlet et al. in 2017 before taking a high interest by the community. Handling such Boolean functions and designing those with optimal characteristic cryptographic properties is no easy assignment.

This paper attempts to broaden the range of choices for these functions by offering two new concrete constructions of weightwise perfectly balanced (WPB) functions on 2^m variables (where m is a positive integer) with optimal algebraic immunity. Simultaneously, the k-weight nonlinearities of these newly constructed WPB functions on 2^m variables are discussed for small values of m. Lastly, comparisons of the k-weight nonlinearities of all the known WPB functions are given, including the known results from computer investigations.

1 Introduction

In symmetric cryptographic framework, Boolean functions used as (important) primitives in stream ciphers and block ciphers are classically studied with input defined on the whole vector space $\mathbb{F}_2^n$ (where the integer n stands the number of variables of the Boolean function). A precious (very recent) book in this context is the one of Carlet [2] (without forget his chapter [1]).

At Eurocrypt 2016, Méaux et al. [8] proposed a new family of stream ciphers, called FLIP, which is intended to be combined with a homomorphic encryption scheme to create an acceptable system of fully homomorphic encryption. The FLIP cipher is based on a new stream cipher model, called the *filter permutator* and tries to minimize some parameters (including the multiplicative depth). It consists of updating at each clock cycle a key register by a permutation of the coordinates. A pseudorandom number generator (PRNG) pilots the choice of the permutation. The permuted key is then filtered, like in a classical stream cipher, by a Boolean function f whose output provides the keystream. A nice description of the FLIP cipher can be found in [8]).

The symmetric primitive FLIP requires the Hamming weight of the key register to be invariant. This produces a particular situation for the structure of the filter function: the input of the filter function consists of those vectors in $\mathbb{F}_2^n$ which have constant Hamming weight. Then, it leads to the problem of evaluating the security of a Boolean function f with restricted input, i.e., the input of f is a subset of $\mathbb{F}_2^n$. Besides, in particular stream ciphers, knowing the Hamming weight of a key register enables the attacker to distinguish the keystream from a random bit-stream [5]. Therefore, filter functions with a slight bias when restricted to vectors with constant Hamming weight are preferred.

Note that there exists a guess and determine attack on an early version of the FLIP cipher given by Duval, Lallemand, and Rotella ([4]) but such an attack is not efficient on the updated versions of FLIP. In 2017, Carlet, Méaux, and Rotella [3] provided a security analysis on FLIP cipher and gave the first study on cryptographic criteria of Boolean functions with restricted input. This produces a special situation for the structure of filter function: the input of the filter function consists of those vectors in $\mathbb{F}_2^n$ which have constant Hamming weight (in fact, by definition, in the filter permutator, the input to the Boolean function has constant Hamming weight equal to the weight of the secret key).

Boolean functions which are uniformly distributed over $\{0,1\}$ on any vector set of $\mathbb{F}_2^n$ with the same Hamming weight are called *weightwise perfectly balanced* functions.

Significant attention has been made to the constructions of weightwise perfectly balanced functions, but the literature is still thin on this topic since studying Boolean functions in restricted input and deriving those which are weightwise perfectly balanced is not an easy task. In the following, we briefly present the state-of-the-art (given chronology) on the known construction of weightwise perfectly balanced functions.

- in 2017, Carlet, Méaux, and Rotella provided in paper [3] a construction of a weightwise perfectly balanced function. Such construction is designed through a method involving secondary constructions.
- in 2019, Liu and Mesnager ([7]) proposed a large class of weightwise perfectly balanced functions, which is 2-rotation symmetric.
- in 2019, Tang and Liu gave in [11] a family of weightwise (almost) perfectly balanced Boolean functions with optimal algebraic immunity.
- in 2020, Mesnager and Su have exhibited in [9] several concrete constructions of weightwise (almost) perfectly balanced Boolean functions by modifying linear or quadratic functions.
- in 2020, Li and Su have also derived in [6] constructions of weightwise perfectly balanced Boolean functions after modifications of Boolean functions with a low algebraic degree.

An important parameter adapted to the restricted Boolean functions is the k-weight nonlinearity, inherited from the classic concept of nonlinearity. We emphasize that upper bounds on the k-weight nonlinearity of Boolean functions have been discovered in the literature. More specifically, a first upper bound on the nonlinearity of a Boolean function restricted to a subset of $\mathbb{F}_2^n$ was given by Carlet, Méaux, and Rotella ([3]). In the same paper, Carlet et al. have also derived bounds on the weightwise nonlinearity of Boolean functions. Two years after, Mesnager, Zhou, and Ding have improved in [10] the best know upper bound on nonlinearity of a Boolean function restricted to a subset of $\mathbb{F}_2^n$ and discussed also bounds on the weightwise nonlinearity of Boolean functions.

In this paper, we continue our way in investigating constructions of WPB functions initiated by Carlet et al. Our main strategy is to push further the method presented by Tang and Liu in their paper [11]. Consequently, two concrete constructions of weightwise perfectly balanced (WPB) functions on 2^m variables (where m is a positive integer) with optimal algebraic immunity are derived.

The remainder of this paper is organized as follows. Formal definitions and necessary preliminaries are introduced in Section 2. A first concrete construction of a family of WPB functions with optimal algebraic immunity is presented in Section 3. Next, another concrete construction of WPB functions with optimal algebraic immunity is presented in Section 4. Simultaneously, the comparison of the k-weight nonlinearities of all the known WPB functions is given.

2 Some preliminaries

An n-variable Boolean function is a mapping from (the $\mathbb{F}_2$-vector space of dimension n) $\mathbb{F}_2^n$ into $\mathbb{F}_2$. We denote by $\mathcal{B}_n$ the set of all the n-variable Boolean functions. A function $f \in \mathcal{B}_n$ is said to be balanced if its truth table contains an equal number of 1's and 0's, i.e., if its Hamming weight $\mathrm{wt}(f) = 2^{n-1}$. We denote $\mathbf{0}_n = (0, 0, \cdots, 0) \in \mathbb{F}_2^n$ and $\mathbf{1}_n = (1, 1, \cdots, 1) \in \mathbb{F}_2^n$.

Definition 2.1 *Given an n-variable Boolean function f, denote*

$$\mathrm{AI}(f) = \min\{\deg(g) \mid 0 \neq g \in \mathcal{B}_n \text{ such that } fg = 0 \text{ or } (f \oplus 1)g = 0\},$$

which is called the algebraic immunity of the function f.

An n-variable Boolean function f is said to have optimal algebraic immunity if $\mathrm{AI}(f) = \lceil \frac{n}{2} \rceil$.

For $0 \leq k \leq n$, we always denote

$$E_{n,k} = \{x \in \mathbb{F}_2^n \mid \mathrm{wt}(x) = k\}. \tag{1}$$

Obviously, $E_{n,0} = \{\mathbf{0}_n\}$, $E_{n,n} = \{\mathbf{1}_n\}$, and $\bigcup_{k=0}^{n} E_{n,k} = \mathbb{F}_2^n$. Denote by $\mathrm{supp}_k(f)$ the support of a Boolean function f on all the input with fixed Hamming weight k, i.e., $\mathrm{supp}_k(f) = \{x \in E_{n,k} \mid f(x) = 1\}$. The k-Hamming weight of the function $f \in \mathcal{B}_n$, denoted by $\mathrm{wt}_k(f)$, is the cardinality of the subset $\mathrm{supp}_k(f)$, i.e., $\mathrm{wt}_k(f) = \big|\{x \in E_{n,k} \mid f(x) = 1\}\big|$.

Definition 2.2 *If a function $f \in \mathcal{B}_n$ satisfies $\mathrm{wt}_k(f) = \frac{1}{2}\binom{n}{k}$ for all $1 \leq k \leq n-1$ and $f(\mathbf{0}_n) \neq f(\mathbf{1}_n)$, then $f(x)$ is called a weightwise perfectly balanced (WPB) function.*

The nonlinearity of f with input restricted on the subset $E_{n,k}$ defined in (1) is called k-weight nonlinearity, which is denoted by $\mathrm{NL}_k(f)$, where $1 \leq k \leq n-1$. The set of all the k-weight nonlinearity for all $1 \leq k \leq n-1$ is called the weightwise nonlinearity profile of the function f.

Proposition 2.3 ([3]) *Given an n-variable Boolean function f, its k-weight nonlinearity is equal to*

$$\mathrm{NL}_k(f) = \frac{1}{2}\binom{n}{k} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\Big|\sum_{x\in E_{n,k}}(-1)^{f(x)\oplus a\cdot x}\Big|,$$

where the subset $E_{n,k}$ is defined in (1) and $1 \leq k \leq n-1$.

3 Construction of WPB functions with optimal algebraic immunity

Lemma 3.1 ([11]) *Let n be equal to a power of 2. For every integer $1 \leq k \leq n-1$, we define U_k to be an arbitrary subset of $E^{=}_{n,k} = \{(x', x'') \,|\, x' \in E_{\frac{n}{2},\frac{k}{2}}, x'' \in E_{\frac{n}{2},\frac{k}{2}}\}$ such that $|U_k| = \frac{1}{2}|E^{=}_{n,k}|$. Obviously, U_k is an empty set when k is odd. Define a Boolean function $f \in \mathcal{B}_n$ as follows*

$$f(x) = \begin{cases} 1, & x \in W^{>} \cup U, \\ 0, & \text{otherwise}, \end{cases}$$

where $x \in \mathbb{F}_2^n$, $E_{\frac{n}{2},\frac{k}{2}}$ is defined in (1), $W^{>} = \{(x', x'') \,|\, x' \in \mathbb{F}_2^{\frac{n}{2}}, x'' \in \mathbb{F}_2^{\frac{n}{2}}, \mathrm{wt}(x') > \mathrm{wt}(x'')\}$, and $U = \bigcup_{k=1}^{n-1} U_k \cup \{\mathbf{0}_n\}$ or $\bigcup_{k=1}^{n-1} U_k \cup \{\mathbf{1}_n\}$. Then, f is a WPB function with optimal algebraic immunity.

For $m \geq 2$, define a 2^m-variable Boolean function as

$$f_m(x) = \begin{cases} 1, & \mathrm{wt}(x') > \mathrm{wt}(x''), \\ 0, & \mathrm{wt}(x') < \mathrm{wt}(x''), \\ f_{m-1}(x'), & \mathrm{wt}(x') = \mathrm{wt}(x''), \end{cases} \tag{2}$$

where $x = (x_1, x_2, \cdots, x_{2^m}) \in \mathbb{F}_2^{2^m}$, $x' = (x_1, x_2, \cdots, x_{2^{m-1}})$, $x'' = (x_{2^{m-1}+1}, x_{2^{m-1}+2}, \cdots, x_{2^m})$, and $f_1(x_1, x_2) = x_1$.

Theorem 3.2 *The 2^m-variable Boolean function f_m defined in (2) is WPB.*

Sketch of proof: We proceed a mathematical induction on m. Assume that the function f_{m-1} is WPB.

(1) When k is odd, then we show that

$$\begin{aligned} \mathrm{wt}_k(f_m) &= \big|\{x \in E_{2^m,k} \,|\, \mathrm{wt}(x') > \mathrm{wt}(x'')\}\big| \\ &= \sum_{i=0}^{\frac{k-1}{2}} \binom{2^{m-1}}{k-i}\binom{2^{m-1}}{i} \\ &= \frac{1}{2}\binom{2^m}{k}. \end{aligned}$$

(2) When k is even, then we show that

$$\begin{aligned} \mathrm{wt}_k(f_m) &= \big|\{x \in E_{2^m,k} \,|\, \mathrm{wt}(x') > \mathrm{wt}(x'')\}\big| + \\ &\quad \big|\{x \in E_{2^m,k} \,|\, \mathrm{wt}(x') = \mathrm{wt}(x''), f_{m-1}(x') = 1\}\big| \\ &= \sum_{i=0}^{\frac{k}{2}-1} \binom{2^{m-1}}{k-i}\binom{2^{m-1}}{i} + \big|\{x' \in E_{2^{m-1},\frac{k}{2}} \,|\, f_{m-1}(x') = 1\}\big|\big|E_{2^{m-1},\frac{k}{2}}\big| \\ &= \sum_{i=0}^{\frac{k}{2}-1} \binom{2^{m-1}}{k-i}\binom{2^{m-1}}{i} + \frac{1}{2}\binom{2^{m-1}}{\frac{k}{2}}^2 \\ &= \frac{1}{2}\binom{2^m}{k}. \end{aligned}$$

□

Next, the algebraic immunity of our newly constructed WPB functions is examined by highlighting that our functions form a subclass of the one given by Tang and Liu in[11]. From this fact, we deduce the 2^m-variable WPB function f_m in (2) has an optimal algebraic immunity as well.

4 Construction of WPB functions with optimal algebraic immunity and higher k-weight nonlinearity

In this section, another concrete construction of WPB functions with optimal algebraic immunity is presented. The k-weight nonlinearities of these newly constructed WPB functions are high enough when k is even.

For $m \geq 2$, define a 2^m-variable Boolean function as

$$g_m(x) = \begin{cases} 1, & \mathrm{wt}(x') > \mathrm{wt}(x'') \text{ or } x = \mathbf{1}_{2^m}, \\ 0, & \mathrm{wt}(x') < \mathrm{wt}(x''), \\ g_{m-1}(x') \oplus g_{m-1}(x''), & \mathrm{wt}(x') = \mathrm{wt}(x'') \text{ and } x \neq \mathbf{1}_{2^m}, \end{cases} \tag{3}$$

where $x = (x_1, x_2, \cdots, x_{2^m}) \in \mathbb{F}_2^{2^m}$, $x' = (x_1, x_2, \cdots, x_{2^{m-1}})$, $x'' = (x_{2^{m-1}+1}, x_{2^{m-1}+2}, \cdots, x_{2^m})$, and $g_1(x_1, x_2) = x_1$.

Theorem 4.1 *The 2^m-variable Boolean function g_m defined in* (3) *is WPB.*

Sketch of proof: The proof consists of mathematical induction on m. Assume that the function g_{m-1} is WPB for $m \geq 4$. Then, by Definition 2.2, the k-Hamming weight of the function g_{m-1} is

$$\begin{aligned} \mathrm{wt}_k(g_{m-1}) &= \left|\{x \in E_{2^{m-1},k} \,|\, g_{m-1}(x) = 1\}\right| \\ &= \frac{1}{2}\binom{2^{m-1}}{k}, \end{aligned}$$

where $1 \leq k \leq 2^{m-1}-1$ and $E_{2^{m-1},k}$ is defined in (1). Furthermore, $g_{m-1}(\mathbf{0}_{2^{m-1}}) = 0$ and $g_{m-1}(\mathbf{1}_{2^{m-1}}) = 1$. Then, the weightwise perfectly balancedness of the Boolean function $g_m(x)$ is determined according to k, $1 \leq k \leq 2^m - 1$, being odd or even as follows.

(1) When k is odd, we prove that k-Hamming weight of the function g_m equals $\mathrm{wt}_k(g_m) = \mathrm{wt}_k(f_m) = \frac{1}{2}\binom{2^m}{k}$ (since f_m is WPB by Theorem 3.2).

(2) When k is even, the k-Hamming weight of the function g_m is given by

$$\begin{aligned} \mathrm{wt}_k(g_m) &= \left|\{x \in E_{2^m,k} \,|\, \mathrm{wt}(x') > \mathrm{wt}(x'')\}\right| + \\ &\quad \left|\{x \in E_{2^m,k} \,|\, \mathrm{wt}(x') = \mathrm{wt}(x''), g_{m-1}(x') = 1, g_{m-1}(x'') = 0\}\right| + \\ &\quad \left|\{x \in E_{2^m,k} \,|\, \mathrm{wt}(x') = \mathrm{wt}(x''), g_{m-1}(x') = 0, g_{m-1}(x'') = 1\}\right| \\ &= \sum_{i=0}^{\frac{k}{2}-1} \binom{2^{m-1}}{k-i}\binom{2^{m-1}}{i} + \\ &\quad 2\left|\{x \in E_{2^m,k} \,|\, \mathrm{wt}(x') = \mathrm{wt}(x''), g_{m-1}(x') = 1, g_{m-1}(x'') = 0\}\right| \\ &= \sum_{i=0}^{\frac{k}{2}-1} \binom{2^{m-1}}{k-i}\binom{2^{m-1}}{i} + 2\left[\frac{1}{2}\binom{2^{m-1}}{\frac{k}{2}}\right]\left[\frac{1}{2}\binom{2^{m-1}}{\frac{k}{2}}\right] \\ &= \sum_{i=0}^{\frac{k}{2}-1} \binom{2^{m-1}}{k-i}\binom{2^{m-1}}{i} + \frac{1}{2}\binom{2^{m-1}}{\frac{k}{2}}^2 \\ &= \frac{1}{2}\binom{2^m}{k}, \end{aligned}$$

where $x = (x', x'')$ with $x', x'' \in \mathbb{F}_2^{2^{m-1}}$, $E_{2^m,k}$ is defined in (1), the third identity holds by the assumption that the function g_{m-1} is WPB and the fact that $1 \leq \frac{k}{2} \leq 2^{m-1}-1$ since $1 \leq k \leq 2^m - 1$ and k is even, and the last identity holds by a technical lemma that we establish.

□

We also study the algebraic immunity and prove that

Theorem 4.2 *The 2^m-variable WPB function g_m in* (3) *has an optimal algebraic immunity.*

Example 4.3 *For $m = 2$ and 3, the k-weight nonlinearities of the WPB functions in papers [6, 7, 9], the WPB function f_m defined in* (2)*, and the WPB function g_m defined in* (3) *are given in Table 1 and Table 2.*

Table 1: Weightwise nonlinearity profiles of the known 4-variable WPB functions

functions	f in [7]	g in [6]	h in [9]	k in [9]	f_m in (2)	g_m in (3)	$\lfloor \binom{n}{k}/2 - \sqrt{\binom{n}{k}/2} \rfloor$
$\mathrm{NL}_2(\cdot)$	0,1	1	1	1	0	1	1

Table 2: Weightwise nonlinearity profiles of the known 8-variable WPB functions

functions	f in [7]	g in [6]	h in [9]	k in [9]	f_m in (2)	g_m in (3)	$\lfloor \binom{n}{k}/2 - \sqrt{\binom{n}{k}/2} \rfloor$
$\mathrm{NL}_2(\cdot)$	≤ 9	2	2	2	2	6	11
$\mathrm{NL}_3(\cdot)$	≤ 22	12	0	14	8	8	24
$\mathrm{NL}_4(\cdot)$	≤ 27	19	3	19	8	26	30

Remark 4.4 *In order to make sure the newly constructed WPB functions g_m in* (3) *have optimal algebraic immunity, we only modified the support of the function $f_m(x)$ in* (2) *on the vectors $x \in \mathbb{F}_2^{2^m}$ satisfying* $\mathrm{wt}(x') = \mathrm{wt}(x'')$*, where $x = (x', x'')$ with $x', x'' \in \mathbb{F}_2^{2^{m-1}}$. It is known that if* $\mathrm{wt}(x') = \mathrm{wt}(x'')$ *then* $\mathrm{wt}(x)$ *is even. Hence, when k is odd, the k-weight nonlinearity of g_m is the same as f_m's, since $g_m(x) = f_m(x)$ if* $\mathrm{wt}(x) = k$*. However, when k is even, the k-weight nonlinearity of g_m is much higher than the k-weight nonlinearity of f_m, and it is very close to the optimal result of computer simulation. This is the first concrete construction of WPB functions in the literature, which have such a high even-weight nonlinearity. We leave the construction of WPB functions with very high odd-weight nonlinearity and optimal algebraic immunity as an open problem.*

References

[1] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes.* Y. Crama and P. Hammer eds, Cambridge University Press, 2010.

[2] C. Carlet, *Boolean Functions for Cryptography and Coding Theory.* Cambridge University Press, Cambridge 2021.

[3] C. Carlet, P. Méaux, and Y. Rotella, *Boolean functions with restricted input and their robustness: application to the FLIP cipher.* IACR Transactions on Symmetric Cryptology, vol. 2017, no. 3, pp. 192-227, 2017.

[4] S. Duval, V. Lallemand, and Y. Rotella, *Cryptanalysis of the FLIP family of stream ciphers.* In: Advances in Cryptology-CRYPTO 2016, Lecture Notes in Computer Science, vol. 9814, Berlin: Springer-Verlag, pp. 457-475, 2016.

[5] A. Joux and P. Delaunay, *Galois LFSR, embedded devices and side channel weaknesses.* In: Progress in Cryptology-INDOCRYPT 2006, Lecture Notes in Computer Science, vol. 4329, pp. 436-451, Berlin: Springer-Verlag, 2006.

[6] J. Li and S. Su, *Construction of weightwise perfectly balanced Boolean functions with high weightwise nonlinearity.* Discrete Applied Mathematics, vol. 279, pp. 218-227, 2020.

[7] J. Liu and S. Mesnager, *Weightwise perfectly balanced functions with high weightwise nonlinearity profile.* Designs, Codes and Cryptography, vol. 87, no. 8, pp. 1797-1813, 2019.

[8] P. Méaux, A. Journault, F. X. Standaert, and C. Carlet, *Towards stream ciphers for efficient FHE with low-noise ciphertexts.* In: Advances in Cryptology-EUROCRYPT 2016, Lecture Notes in Computer Science, vol. 9665, pp. 311-343, Berlin: Springer-Verlag, 2016.

[9] S. Mesnager and S. Su, *On constructions of weightwise perfectly balanced functions.* In: The 5th International Workshop on Boolean Functions and their Applications (BFA 2020), Online, Loen, Norway (2020).

[10] S. Mesnager, Z. Zhou, and C. Ding, *On the nonlinearity of Boolean functions with restricted input.* Cryptography and Communications, vol. 11, no. 1, pp. 63-76, 2019.

[11] D. Tang and J. Liu, *A family of weightwise (almost) perfectly balanced boolean functions with optimal algebraic immunity.* Cryptography and Communications, vol. 11, no. 6, pp. 1185-1197, 2019.