On constructions of weightwise perfectly balanced functions

Sihem Mesnager* and Sihong Su**

*University of Paris VIII (Department of Mathematics), 93526 Saint-Denis, France, University of Paris XIII, Sorbonne Paris Cité 93430 Villetaneuse, LAGA, UMR 7539, CNRS, France Telecom Paris, 91120 Palaiseau, France. Email: smesnager@univ-paris8.fr

**School of Mathematics and Statistics, Henan University, Kaifeng, 475004, China, and the Department of Mathematics, University of Paris VIII, 93526 Saint-Denis, France. Email: sush@henu.edu.cn

Abstract

The recent FLIP cipher is an encryption scheme described by Méaux et al. at the conference EUROCRYPT 2016. It is based on a new stream cipher model, called the filter permutator and tries to minimize some parameters (including the multiplicative depth). In the filter permutator, the input to the Boolean function has constant Hamming weight equal to the weight of the secret key. As a consequence, Boolean functions satisfying good cryptographic criteria when restricted to the set of vectors with constant Hamming weight play an important role in the FLIP stream cipher. Carlet et al. have shown that for Boolean functions with restricted input, balancedness and nonlinearity parameters continue to play an important role with respect to the corresponding attacks on the framework of FLIP ciphers. In particular, Boolean functions which are uniformly distributed over $\mathbb{F}_2$ on $E_{n,k} = \{x \in \mathbb{F}_2^n \mid \mathrm{w_H}(x) = k\}$ for every $0 < k < n$ are called weightwise perfectly balanced (WPB) functions, where $\mathrm{w_H}(x)$ denotes the Hamming weight of x. In this extended abstract, we firstly propose two methods of constructing weightwise perfectly balanced Boolean functions in 2^k variables (where k is a positive integer) by modifying the support of linear and quadratic functions. Furthermore, we derive a construction of n-variable weightwise almost perfectly balanced Boolean functions for any positive integer n.

1 Introduction

In a cryptographic framework, Boolean functions are classically studied with an input ranging over the vector space $\mathbb{F}_2^n$ of binary vectors of length n [2]. This is the case when the Boolean functions are used as the (main) nonlinear components of a stream cipher, in the so-called combiner and filter models of pseudo-random generators. However, the input of a Boolean function can be restricted to a subset of the vector space $\mathbb{F}_2^n$. A recent example of such a situation is given by the FLIP cipher [10]. The FLIP cipher is a new family of stream ciphers proposed by Méaux et al. at Eurocrypt 2016, which is intended to be combined with a homomorphic encryption scheme to create an acceptable system of fully homomorphic encryption [4, 8]. Essentially, the FLIP cipher is one of the encryption schemes specifically designed to be combined with a homomorphic encryption scheme to improve the efficiency of somewhat homomorphic encryption frameworks [1]. 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). The reader notices that Méaux et al [9] have proposed in 2019, an improved filter permutators for efficient FHE (in particular better Instances and implementations). A nice description of FLIP can be found in [10]. An early version of FLIP faces an attack given by Duval et al. [5], which leads the design of the filter function to become more complicated to reach better criteria on the subsets of $\mathbb{F}_2^n$. 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). Carlet et al. [3] have shown that for Boolean functions with restricted input, balancedness and nonlinearity parameters continue to play an important role with respect to the corresponding attacks on the framework of FLIP ciphers. In particular, Boolean functions which are uniformly distributed over $\mathbb{F}_2$ on $E_{n,k} = \{x \in \mathbb{F}_2^n \mid \mathrm{w_H}(x) = k\}$ for every $0 < k < n$ are called *weightwise perfectly balanced* (WPB) functions, where $\mathrm{w_H}(x)$ denotes the Hamming weight of x. To our best knowledge, the first known construction of WPB functions is due to [3] in 2017, which is designed through a recursive method. In 2008, Liu and Mesnager [6] proposed a large class of WPB functions, which is 2-rotation symmetric.In 2019, Tang and Liu [11] also gave a construction of WPB functions. Some upper bounds on the k-weight nonlinearity of Boolean functions are discussed in [3] and [7], respectively.

In this extended abstract, we firstly give a full study of the Hamming weight distributions of the linear function $f(x_1, x_2, \cdots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_m$ and the quadratic function $g(x_1, x_2, \cdots, x_n) = x_1(x_{m+1} \oplus 1) \oplus x_2(x_{m+2} \oplus 1) \oplus \cdots \oplus x_m(x_n \oplus 1)$, where $n = 2m$. And then, two concrete constructions of 2^k-variable (where k is a positive integer) WPB functions by modifying the support of the linear function and the quadratic function are respectively proposed. Lastly, a construction of n-variable almost-WPB functions for any positive integer n is given.

This extended abstract is organized as follows. Some definitions are presented in Section 2 but we assume the reader familiar with background on Boolean functions as well as standard notation. In Section 3, a construction of WPB functions on 2^k variables (where k is a positive integer) obtained by modifying the support of a linear function is given. Next, a construction of WPB functions on 2^k variables obtained by modifying the support of a quadratic function is proposed in Section 4. The construction of n-variable almost-WPB functions for any positive integer n is given in Section 5.

2 Some preliminaries

For $0 \leq k \leq n$, we always denote $E_{n,k} = \{x \in \mathbb{F}_2^n \,|\, \mathrm{wt}(x) = k\}$. Obviously, $\bigcup_{k=0}^{n} E_{n,k} = \mathbb{F}_2^n$. 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 $\mathrm{wt}(f) = 2^{n-1}$. The k-weight of the function $f \in \mathcal{B}_n$, denoted by $\mathrm{wt}_k(f)$, is the cardinality of the subset $\{x \in E_{n,k} \,|\, f(x) = 1\}$, i.e. $\mathrm{wt}_k(f) = |\{x \in E_{n,k} \,|\, f(x) = 1\}|$. It is known that the cardinality of the subset $E_{n,k}$ is $|E_{n,k}| = \binom{n}{k}$ for $0 \leq k \leq n$. Since $\binom{n}{0} = \binom{n}{n} = 1$, we have the following Definition.

Definition 2.1 *If a function $f \in \mathcal{B}_n$ satisfies $\mathrm{wt}_k(f) = \frac{1}{2}\binom{n}{k}$*

for all integers $1 \leq k \leq n-1$, the function $f(x)$ is called a weightwise perfectly balanced (WPB) function.

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

Definition 2.3 *If a function $f \in \mathcal{B}_n$ satisfies $\mathrm{wt}_k(f) = \left\lfloor \frac{1}{2}\binom{n}{k} \right\rfloor$ for all integers $0 \leq k \leq n$, then the function $f(x)$ is called a weightwise almost perfectly balanced (almost-WPB) function.*

3 Construction of WPB functions by modifying a linear function

.

Define an n-variable Boolean function as

$$f(x_1, x_2, \cdots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_m, \tag{1}$$

where $n = 2m$ with m being a positive integer. Then, the support of the n-variable Boolean function $f(x)$ in (1) is

$$\mathrm{supp}(f) = \{(x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n \,|\, \mathrm{wt}(x_1, x_2, \cdots, x_m) \text{ is odd}\}. \tag{2}$$

.

Theorem 3.1 *For any odd integer $k \in \{1, 3, \cdots, n-1\}$ and $n = 2m$, the n-variable Boolean function $f(x)$ in (1) satisfies $\mathrm{wt}_k(f) = \frac{1}{2}\binom{n}{k}$. Hence, the function $f(x)$ in (1) is odd-WPB.*

Theorem 3.2 *For any even integer $k \in \{2, 4, 6, \cdots, n-2\}$ and $n = 2m$, the n-variable Boolean function $f(x)$ in (1) satisfies $\mathrm{wt}_k(f) = \frac{1}{2}\binom{n}{k} - \frac{(-1)^{\frac{k}{2}}}{2}\binom{m}{\frac{k}{2}}$.*

Corollary 3.3 *For any even integer $k \in \{2, 4, 6, \cdots, n-2\}$ and $n = 2m$, we have $\sum\limits_{\substack{0 \le i \le k \\ i \text{ is odd}}} \binom{m}{i}\binom{m}{k-i} = \frac{1}{2}\binom{n}{k} - \frac{(-1)^{\frac{k}{2}}}{2}\binom{m}{\frac{k}{2}}$.*

Given a positive integer m, define a 2^m-variable Boolean function as

$$\mathrm{supp}(f_m) = \bigsqcup_{i=1}^{m} \big\{(x, y, x, y, \cdots, x, y) \in \mathbb{F}_2^{2^m} \,|\, x, y \in \mathbb{F}_2^{2^{m-i}}, \mathrm{wt}(x) \text{ is odd}\big\}. \tag{3}$$

Theorem 3.4 *The function f_m in 2^m variables defined in (3) is weightwise perfectly balanced.*

Theorem 3.5 *The ANF of the 2^m-variable Boolean function $f_m(x)$ in (3) is $f_m(x_1, x_2, \ldots, x_{2^m}) = \bigoplus\limits_{i=1}^{2^{m-1}} x_i \oplus f_{m-1}(x_1, x_2, \ldots, x_{2^{m-1}}) \prod\limits_{i=1}^{2^{m-1}} (x_i \oplus x_{2^{m-1}+i} \oplus 1)$, where $f_1(x_1, x_2) = x_1$. Moreover, the algebraic degree of the 2^m-variable Boolean function $f_m(x)$ in (3) is $\deg(f_m) = 2^m - 1$.*

In order to get a flexible construction of WPB functions, define

$$\begin{cases} I_1^{(1)} \subseteq \{1, 2, \cdots, n\}, I_2^{(1)} = \{1, 2, \cdots, n\} \setminus I_1, \\ I_1^{(2)} \subseteq I_1^{(1)}, I_2^{(2)} = I_1^{(1)} \setminus I_1^{(2)}, I_3^{(2)} \subseteq I_2^{(1)}, I_4^{(2)} = I_2^{(1)} \setminus I_3^{(2)}, \\ \cdots\cdots \\ I_1^{(m)} \subseteq I_1^{(m-1)}, I_2^{(m)} = I_1^{(m-1)} \setminus I_1^{(m)}, \cdots\cdots, I_{2^m-1}^{(m)} \subseteq I_{2^{m-1}}^{(m-1)}, I_{2^m}^{(m)} = I_{2^{m-1}}^{(m-1)} \setminus I_{2^m-1}^{(m)}, \end{cases}$$

where $|I_j^{(i)}| = 2^{m-i}$, for $1 \le i \le m$ and $1 \le j \le 2^i$. For convenience, denote $x_I = (x_{i_1}, x_{i_2}, \cdots, x_{i_t})$ for $x = (x_1, x_2, \cdots, x_n)$ and $I = \{i_1, i_2, \cdots, i_t\} \subseteq \{1, 2, \cdots, 2^m\}$. Then, a flexible construction of 2^m-vriable WPB function is given as

$$\mathrm{supp}(f_m) = \bigsqcup_{i=1}^{m} \big\{x \in \mathbb{F}_2^{2^m} \,|\, \mathrm{wt}(x_{I_1^{(i)}}) \text{ is odd}, x_{I_1^{(i)}} = x_{I_3^{(i)}} = \cdots = x_{I_{2^i-1}^{(i)}}, x_{I_2^{(i)}} = x_{I_4^{(i)}} = \cdots = x_{I_{2^i}^{(i)}}\big\},$$

where m is a positive integer. In fact, if the order of the entries in the vector $x_{I_j^{(i)}}$ is considered, a more flexible constructions of WPB functions can be obtained.

4 Construction of WPB functions by modifying the support of a quadratic function

Define an n-variable Boolean function as

$$g(x_1, x_2, \cdots, x_n) = x_1(x_{m+1} \oplus 1) \oplus x_2(x_{m+2} \oplus 1) \oplus \cdots \oplus x_m(x_n \oplus 1), \tag{4}$$

where $n = 2m$ with m being a positive integer.

Theorem 4.1 *For any integer $k \in \{1, 2, \cdots, n-1\}$ and $n = 2m$, the n-variable Boolean function $g(x)$ in* (4) *satisfies* $\mathrm{wt}_k(g) = \frac{1}{2}\binom{n}{k} - \frac{\delta_k}{2}\binom{m}{\frac{k}{2}}$, *where* $\delta_k = \begin{cases} 1, & k \text{ is even}, \\ 0, & k \text{ is odd}. \end{cases}$

According to the values of the k-weights of the n-variable Boolean function $g(x)$ defined in (4), $1 \leq k \leq n-1$, we can construct another WPB function as follows.

Define a 2^m-variable Boolean function $g_m(x)$ as

$$g_m(x_1, x_2, \ldots, x_{2^m}) = g(x_1, x_2, \ldots, x_{2^m}) \oplus g_{m-1}(x_1, x_2, \ldots, x_{2^{m-1}}) \prod_{i=1}^{2^{m-1}} (x_i \oplus x_{2^{m-1}+i} \oplus 1), \quad (5)$$

where $m \geq 1$, $g(x)$ is defined in (4), and $g_0(x_1) = 0$.

Theorem 4.2 *The Boolean defined in* (5) *is weightwise perfectly balanced. Its algebraic degree equals* $\deg(g_m) = 2^m$ *(hence it has a maximal algebraic degree).*

5 Construction of almost-WPB functions

In this section, a construction of almost-WPB functions by modifying the support of a quadratic Boolean function in any variables is proposed.

Define an n-variable Boolean function as

$$h(x_1, x_2, \cdots, x_n) = x_1(x_{m+1} \oplus 1) \oplus x_2(x_{m+2} \oplus 1) \oplus \cdots \oplus x_m(x_{2m} \oplus 1), \quad (6)$$

where n is a positive integer and $m = \lfloor \frac{n}{2} \rfloor$.

Theorem 5.1

- *For any integer $k \in \{1, 2, \cdots, n-1\}$ and $n = 2m+1$ with $m \geq 1$, the n-variable Boolean function $h(x)$ in* (6) *satisfies* $\mathrm{wt}_k(h) = \frac{1}{2}\binom{n}{k} - \frac{1}{2}\binom{m}{\lfloor \frac{k}{2} \rfloor}$.
- *For any integer $k \in \{1, 2, \cdots, n-1\}$ with $n \geq 2$, the n-variable Boolean function $h(x)$ in* (6) *satisfies* $\mathrm{wt}_k(h) = \begin{cases} \frac{1}{2}\binom{n}{k}, & n \text{ is even and } k \text{ is odd}, \\ \frac{1}{2}\binom{n}{k} - \frac{1}{2}\binom{\lfloor \frac{n}{2} \rfloor}{\lfloor \frac{k}{2} \rfloor}, & \text{otherwise}. \end{cases}$

Define an n-variable Boolean function $h_n(x)$ as

$$h_n(x_1, x_2, \ldots, x_n) = h(x_1, x_2, \ldots, x_n) \oplus h_{\lfloor \frac{n}{2} \rfloor}(x_1, x_2, \ldots, x_n) \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} (x_i \oplus x_{\lfloor \frac{n}{2} \rfloor + i} \oplus 1), \quad (7)$$

where $n \geq 2$, $h(x_1, x_2, \ldots, x_n)$ is defined in (6), and $h_1(x_1) = 0$.

Theorem 5.2

- *The Boolean function h_n defined in* (7) *is almost weightwise perfectly balanced.*
- *Its Hamming weight equals* $\mathrm{wt}(h_n) = 2^{n-1} - 2^{\mathrm{wt}(n)-1}$, *where* $\mathrm{wt}(n) = \mathrm{wt}(n_1, n_2, \cdots, n_t)$ *satisfying* $n = n_1 2^0 + n_2 2^1 + \cdots + n_t 2^{t-1}$.
- *Its algebraic degree equals* $\deg(h_n) = n - \mathrm{wt}(n) + 1$, *where* $\mathrm{wt}(n) = \mathrm{wt}(n_1, n_2, \cdots, n_t)$ *satisfying* $n = n_1 2^0 + n_2 2^1 + \cdots + n_t 2^{t-1}$.

References

[1] A. Canteaut, S. Carpov, C. Fontaine, T. Lepoint, M. Naya-Plasencia, P. Paillier, and R. Sirdey, Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression, In Thomas Peyrin, editor, FSE 2016, Lecture Notes in Computer Science, vol. 9783, pp. 313-333, Springer, 2016.

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

[3] C. Carlet, P. Méaux, and Y. Rotella, Boolean functions with restricted input and their robustness: application to the FLIP cipher. IACR Trans. Symmetric Cryptol. (3), pp. 192-227, 2017.

[4] J. Coron, T. Lepoint, M. Tibouchi, Scale-Invariant Fully Homomorphic Encryption over the Integers. in Krawczyk, H. (ed.) Public-Key Cryptography-PKC 2014. Lecture Notes in Computer Science, vol. 8383, pp. 311-328, Springer, 2014.

[5] 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.

[6] 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.

[7] 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.

[8] P. Méaux, Symmetric Encryption Scheme adapted to Fully Homomorphic Encryption Scheme, in Journées Codage et Cryptographie-JC2, France 2015.

[9] P. Méaux, C. Carlet, A. Journault and F. X. Standaert, Improved Filter Permutators for Efficient FHE: Better Instances and Implementations. INDOCRYPT , pp. 68-91, 2019.

[10] 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.

[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.