Composition of Boolean Functions: An Application to the Secondary Constructions of Bent Functions[*][†]

Guangpu Gao [a,b], Dongdai Lin[b], Wenfen Liu[c], and Yongjuan Wang[a]

[a] State Key Laboratory of Mathematical Engineering and Advanced Computing, P.O. Box 1001-741, Zhengzhou 450002, Henan Province of P.R. China.
guangpu.gao@gmail.com

[b] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China.
ddlin@iie.ac.cn

[c] Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, Guangxi 541004, China.

Abstract

Bent functions are optimal combinatorial objects and have been attracted their research for four decades. Secondary constructions play a central role in constructing bent functions since a complete classification of this class of functions is elusive. This paper is devoted to establish a relationship between the secondary constructions and the composition of Boolean functions. We firstly prove that some well-known secondary constructions of bent functions, can be described by the composition of a plateaued Boolean function and some bent functions. Then their dual functions can be calculated by the Lagrange interpolation formula. By following this observation, two secondary constructions of bent functions are presented. We show that they are inequivalent to the known ones, and may generate bent functions outside the primary classes $\mathcal{M}$ and $\mathcal{PS}$. These results show that the method we present in this paper is genetic and unified and therefore can be applied to the constructions of Boolean functions with other cryptographical criteria.

Keywords : Secondary constructions, Composition of Boolean functions, Bent, Lagrange interpolation formula

1 Introduction

Nonlinearity is a primary requirement for Boolean functions used in cryptosystems (see e.g. [4,6]). The nonlinearity of a Boolean function f is the minimum Hamming distance between f and affine functions. A bent function is a Boolean function with an even number of variables which achieves the maximum possible nonlinearity. Such functions have been extensively studied for their wide applications in cryptography, spread spectrum, coding theory, and combinatorial design [6,8].

[*] During the revision process of this manuscript an independent work on the same topic has appeared on eprint archive https://arxiv.org/abs/1809.07390.

[†] The work of G. Gao and D. Lin are supported by National Nature Science Foundation of China under Grant 61872381 and 61872359.

Since the complete classification of bent functions seems elusive, many researchers turn to design constructions of bent functions and numerous bent functions have been obtained. Constructions of bent functions from scratch are called primary constructions [7, 16], and constructions of bent functions from known ones are called secondary constructions [6]. The two well known primary constructions are the Maiorana-McFarland class $\mathcal{M}$ of bent functions [16] and the $\mathcal{PS}$ class of bent functions [7]. The class $\mathcal{M}$ consists in concatenating affine functions while the $\mathcal{PS}$ class consists of functions whose support is the union of 2^{k-1} or $2^{k-1}+1$ summing (modulo 2)the indicators of pairwise disjoint k-dimensional subspaces of $GF(2)^{2k}$. However, there are only a few primary constructions in literature, and thus secondary constructions are necessary to obtain new bent functions. The two interesting secondary constructions of bent functions among others are from Rothaus [18] with extension of the number of variables and from Carlet [1–3] without extension of the number of variables. A series of constructions have been obtained by revisiting or generalizing these results [5, 11–13, 15, 19, 20]. But it seems hard to determine that if these constructed bent functions belong to the completed versions of primary classes up to affine equivalence. For more details, the readers can refer to the survey on four-decade research on bent functions [5] and the recent book [12].

This paper is devoted to design new secondary constructions of bent functions under the framework of "composition of Boolean functions". The paper is organized as follows. After introducing some formal definitions and necessary preliminaries in Section 2, we give the framework of composition of Boolean functions in Section 3. It shows that some well-known secondary constructions of bent functions can be described from the view point of the composition of bent functions. Consequently, their duals can be obtained by the famous Lagrange interpolation formula. By this observation, we present two secondary constructions of bent functions in Section 4. We show that these two constructions are inequivalent to the known ones, and may generate bent functions outside the primary classes $\mathcal{M}$ and $\mathcal{PS}$. We conclude this paper in Section 5.

2 Preliminaries

Let $\mathrm{GF}(2)^n$ be the n-dimensional vector space over the finite field $\mathrm{GF}(2) = \{0, 1\}$. We shall distinguish in the paper between the additions of integers in Z, denoted by $+$ and the additions in $\mathrm{GF}(2)$, denoted by $\oplus$. An n-variable Boolean function $f(x)$, where $x = (x_1, \ldots, x_n) \in \mathrm{GF}(2)^n$, is a mapping from $\mathrm{GF}(2)^n$ to $\mathrm{GF}(2)$, which can be represented in a unique way as an n-variable polynomial whose degree relative to each variable is at most 1, called its *algebraic normal form* (ANF):

$$f(x_1, \ldots, x_n) = \bigoplus_{u \in \mathrm{GF}(2)^n} a_u x^u, \qquad a_u \in \mathrm{GF}(2),$$

where $x^u = x_1^{u_1} \cdots x_n^{u_n}$. The binary sequence defined by $(f(v_0), f(v_1), ..., f(v_{2^n-1}))$ is called the *truth table* of an n-variable Boolean function f, where $v_0 = (0, ..., 0, 0), v_1 = (0, ..., 0, 1), ..., v_{2^n-1} = (1, ..., 1, 1)$ are ordered by lexicographical order. The *Lagrange interpolation formula* in terms of Boolean function is defined as:

$$f(x_1, \ldots, x_n) = \bigoplus_{i=0}^{2^n-1} f(v_i)(x_1 \oplus v_{i,1} \oplus 1)(x_2 \oplus v_{i,2} \oplus 1) \cdots (x_n \oplus v_{i,n} \oplus 1). \tag{1}$$

By applying the Lagrange interpolation method, it is a simple matter to obtain the ANF of every Boolean function from its truth table. The *Hamming weight* $w_H(x)$ of a binary vector $x \in \mathrm{GF}\,(2)^n$ is the number of its nonzero coordinates, and the Hamming weight $w_H(f)$ of a Boolean function f is the size of its support $\{x \in \mathrm{GF}(2)^n : f(x) = 1\}$. If $w_H(f) = 2^{n-1}$, we call $f(x)$ balanced.

We say that two n-variable Boolean functions $f(x)$ and $g(x)$ are affinely equivalent if $g(x) = f(xA \oplus b)$ where $b \in \mathrm{GF}(2)^n$, A is an $n \times n$ nonsingular binary matrix and xA is the product of the row-vector x and A. An important tool for studying Boolean functions is the Walsh transform. Given $x = (x_1, \dots, x_n)$ and $w = (w_1, w_2, \dots, w_n) \in \mathrm{GF}(2)^n$, let $w \cdot x$ be an inner product on $\mathrm{GF}(2)^n$, for instance the usual inner product $w_1x_1 \oplus \cdots \oplus w_nx_n$. The "sign" function of f is the integer-valued function, usually denoted by $\chi_f(x) = (-1)^{f(x)}$. The *Walsh transform* of f is the discrete Fourier transform of χ_f associated with this inner product, which is the following real-valued function over $\mathrm{GF}(2)^n$:

$$W_f(w) = \sum_{x \in \mathrm{GF}(2)^n} (-1)^{f(x) \oplus w \cdot x}.$$

The inverse Walsh transform is given by

$$(-1)^{f(x)} = \frac{1}{2^n} \sum_{w \in \mathrm{GF}(2)^n} W_f(w)(-1)^{w \cdot x}.$$

The *Walsh spectrum* of f is the multiset of values $W_f(w)$ where w ranges over $\mathrm{GF}(2)^n$. Throughout this paper, we denote by $S_f = \{w \in \mathrm{GF}(2)^n : W_f(w) \neq 0\}$ the *Walsh support* of f. We say two Walsh supports S_f and S_g are complementary if they have the same cardinality and $S_f \bigcap S_g = \emptyset$, $S_f \bigcup S_g = \mathrm{GF}(2)^n$. The *nonlinearity* of an n-variable Boolean function is given by

$$N_f = 2^{n-1} - \frac{1}{2} \max_{w \in \mathrm{GF}(2)^n} |W_f(w)|.$$

From the *Poisson summation formula,* we can derive the *Parseval's relation:*

$$\sum_{w \in \mathrm{GF}(2)^n} {W_f}^2(w) = 2^{2n}.$$

By this relation, we have the upper bound of the nonlinearity of a Boolean function $N_f \leq 2^{n-1} - 2^{n/2}$. Bent functions are those Boolean functions with maximal nonlinearity, in even numbers of variables.

Definition 1 *Let $n = 2m$ be even. A Boolean function f is bent if its Walsh coefficients satisfy:*

$$W_f(w) = \pm 2^m, \quad \text{for all } w \in \mathrm{GF}(2)^n.$$

If f is bent, then the *dual function* $\tilde{f}$ of f, defined on $\mathrm{GF}(2)^n$ by: $W_f(w) = 2^{n/2}(-1)^{\tilde{f}}$ is also bent and its own dual is f itself.

An n-variable Boolean function is said to be *plateaued* if its Walsh transform takes at most the three values 0 and $\pm 2^k$, where k is a positive integer with $n/2 \leq k \leq n$ [21]. We call 2^k the *amplitude* of the function. Thanks to the Parseval's relation, the cardinality of Walsh support S_f is $2^{2(n-k)}$.

Let n, m be two positive integers. Given any (n, m)-function $F(x)$, there exist Boolean functions $f_1(x), f_2(x), \dots, f_m(x)$ such that $F(x) = (f_1(x), f_2(x), \dots, f_m(x))$. When the numbers m, n are not specified, (n, m)-functions are also called multi-output Boolean functions, vectorial Boolean functions or S-boxes [4]. When $m = 1$, we call the $(n, 1)$-functions Boolean functions for simplicity. For any positive integer n, m, let $F(x)$ be any (n, m)-function with m coordinate functions $f_1(x), f_2(x), \dots, f_m(x)$ of n variables. Let $G(z_1, z_2, \dots, z_m)$ be any Boolean function of m variables. The composition of F and G, denoted by $G \circ F$ is an n-variable Boolean function, defined by $G(F(x)) = G(f_1(x), f_2(x), \dots, f_m(x))$.

3 Composition of Boolean Functions

Composition of Boolean functions was firstly studied in [10] to construct resilient Boolean functions and bent functions in the form of $f(x) \oplus g(y) \oplus \varphi(h_1(x), h_2(y))$, where φ is a 2-variable Boolean function. Nyberg in [17] considered the cases of its applications to cryptanalysis of block ciphers and stream ciphers. Gupta and Sarkar [9] continued to generalize Nyberg's work and obtained the Walsh spectrum of the composition of Boolean functions by computing the corresponding inverse Walsh transform as:

Theorem 1 *Let $G(z), z = (z_1, z_2, \dots, z_k)$ be any k-variable Boolean function, and $f_1(x), f_2(x), \dots, f_k(x)$ be Boolean functions of n variables. Denote by $F = (f_1(x), f_2(x), \dots, f_k(x))$, which is an $(n, k)-$function. Then the Walsh coefficient of the composition function $G(f_1(x), f_2(x), \dots, f_k(x))$ is*

$$W_{G(f_1,f_2,\dots,f_k)}(w) = \frac{1}{2^k} \sum_{v \in \mathrm{GF}(2)^k} W_{G(z)}(v) \cdot W_{v \cdot F}(w),\ w \in \mathrm{GF}(2)^n. \tag{2}$$

It is interesting to note that secondary construction builds new Boolean functions from known ones, this can be viewed as a composition of Boolean functions. Therefore, we may derive new secondary constructions of bent functions by researching the well-known methods in terms of compositions of bent functions.

3.1 Secondary Constructions of Bent Functions

1. The first secondary construction is given by J. Dillon [7] and O. Rothaus [18] as: let f be a bent function on $\mathrm{GF}(2)^m$ (m even) and g be a bent function on $\mathrm{GF}(2)^n$ (n even), then the function h defined on $\mathrm{GF}(2)^{m+n}$ by $h(x, y) = f(x) \oplus g(y)$ is bent. It is obvious that if we let $G(z_1, z_2) = z_1 \oplus z_2$, then $h(x, y) = G(f(x), g(y))$.

2. *Rothaus's construction* A more interesting result from Rothaus is the following theorem, and we reprove it from the view point of the composition of Boolean functions.

   Theorem 2 *If g, h, k and $g \oplus h \oplus k$ are bent functions on $\mathrm{GF}(2)^m$ (m even), then the function, defined on any element (x_{n+1}, x_{n+2}, x) of $\mathrm{GF}(2)^{n+2}$ $((x_{n+1}, x_{n+2}, x) \in \mathrm{GF}(2)^{n+2})$ by:*

   $$f(x_{n+1}, x_{n+2}, x) = g(x)h(x) \oplus g(x)k(x) \oplus h(x)k(x) \oplus (g(x) \oplus h(x))x_{n+1} \oplus (g(x) \oplus k(x))x_{n+2} \oplus x_{n+1}x_{n+2}$$

   is bent.

   Proof Now we take $G(z_1, z_2, z_3, z_4, z_5) = z_1z_2 \oplus z_1z_3 \oplus z_2z_3 \oplus z_4(z_1 \oplus z_2) \oplus z_5(z_1 \oplus z_3) \oplus z_4z_5$. With a computation, the nonzero Walsh coefficients of $G(z)$ are

   $$W_{G(z)}(0,0,1,1,0) = 16, W_{G(z)}(0,1,0,0,1) = 16,$$
   $$W_{G(z)}(1,0,0,0,0) = 16, W_{G(z)}(1,1,1,1,1) = -16.$$

   with its support $\mathrm{supp}(W_{G(z)}) = \{(0,0,1,1,0), (0,1,0,0,1), (1,0,0,0,0), (1,1,1,1,1)\}$. Let $z_1 = g(x), z_2 = h(x), z_3 = k(x),\ z_4 = x_{n+1}, z_5 = x_{n+2}$, then for any $w \in \mathrm{GF}(2)^n$ and $(w_{n+1}, w_{n+2}) \in$

$\mathrm{GF}(2)^2$, we obtain the following relations from Relation (2)

$$\begin{aligned} W_{G(g,h,k,x_{n+1},x_{n+2})}(w, w_{n+1}, w_{n+2}) &= \frac{1}{2}\big(W_g(w, w_{n+1}, w_{n+2}) + W_{k\oplus x_{n+1}}(w, w_{n+1}, w_{n+2}) \\ &\quad + W_{h\oplus x_{n+2}}(w, w_{n+1}, w_{n+2}) - W_{g\oplus h\oplus k\oplus x_{n+1}\oplus x_{n+2}}(w, w_{n+1}, w_{n+2})\big) \\ &= \begin{cases} 2W_g(w), w_{n+1}, = 0, w_{n+2} = 0 \\ 2W_k(w), w_{n+1}, = 1, w_{n+2} = 0 \\ 2W_h(w), w_{n+1}, = 0, w_{n+2} = 1 \\ -2W_{g\oplus h\oplus k}(w), w_{n+1}, = 1, w_{n+2} = 1 \end{cases} . \end{aligned} \tag{3}$$

It is clearly an $(n+2)$-variable bent function if h, g, k and $h \oplus g \oplus k$ are bent functions □

3. *Carlet's construction* Rothaus' construction depends on the bentness of $g \oplus h \oplus k$, it was shown by Carlet in [3]:

Let f_1, f_2 and f_3 be three Boolean functions on $\mathrm{GF}(2)^n$. Denote by σ_1 the Boolean function equal to $f_1 \oplus f_2 \oplus f_3$ and by σ_2 the Boolean function equal to $f_1f_2 \oplus f_1f_3 \oplus f_2f_3$. It holds that $f_1 + f_2 + f_3 = \sigma_1 + 2\sigma_2$. This implies

$$W_{f_1} + W_{f_2} + W_{f_3} = W_{\sigma_1} + 2W_{\sigma_2}.$$

From this formula, it derives that:

Theorem 3 *[3] Let n be any positive even integer. Let f_1, f_2 and f_3 be three bent functions on $\mathrm{GF}(2)^n$. Denote by σ_1 the Boolean function $f_1 \oplus f_2 \oplus f_3$ and by σ_2 the function $f_1f_2 \oplus f_1f_3 \oplus f_2f_3$. Then:*
if σ_1 is bent and if $\widetilde{\sigma_1} = \widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3}$, then σ_2 is bent and $\widetilde{\sigma_2} = \widetilde{f_1}\widetilde{f_2} \oplus \widetilde{f_1}\widetilde{f_3} \oplus \widetilde{f_2}\widetilde{f_3}$.

Proof Let $G(z_1, z_2, z_3) = z_1z_2 \oplus z_1z_3 \oplus z_2z_3$ be a 3-variable Boolean function. By a direct computation, the Walsh spectrum of $G(z)$ is $W_G = \{0, 4, 4, 0, 4, 0, 0, -4\}$ and its support is $\mathrm{supp}(W_G) = \{(001), (010), (100), (111)\}$. Since $\sigma_2 = G(f_1, f_2, f_3)$, then from Relation (2), we have

$$\begin{aligned} W_{G(f_1,f_2,f_3)}(w) &= \frac{1}{8}\sum_{v\in \mathrm{GF}(2)^3} W_{G(z)}(v) W_{\nu_1 f_1 \oplus v_2 f_2 \oplus v_3 f_3}(w) \\ &= \frac{1}{2}\big(W_{f_1}(w) + W_{f_2}(w) + W_{f_3}(w) - W_{f_1\oplus f_2\oplus f_3}(w)\big) \\ &= 2^{\frac{n}{2}-1}\Big(\chi(\widetilde{f_1}(w)) + \chi(\widetilde{f_2}(w)) + \chi(\widetilde{f_3}(w)) - \chi(\widetilde{\sigma_1}(w))\Big). \end{aligned} \tag{4}$$

If $\widetilde{\sigma_1} = \widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3}$, we have the following table:

Table 1: truth table of Boolean function $\widetilde{\sigma_2}$

$\widetilde{f_1}(w)$	$\widetilde{f_2}(w)$	$\widetilde{f_3}(w)$	$W_{\sigma_2}(w)$	$\widetilde{\sigma_2}(w)$
0	0	0	$2^{\frac{n}{2}}$	0
0	0	1	$2^{\frac{n}{2}}$	0
0	1	0	$2^{\frac{n}{2}}$	0
0	1	1	$-2^{\frac{n}{2}}$	1
1	0	0	$2^{\frac{n}{2}}$	0
1	0	1	$-2^{\frac{n}{2}}$	1
1	1	0	$-2^{\frac{n}{2}}$	1
1	1	1	$-2^{\frac{n}{2}}$	1

Note that Table 1 only describes a symbolical correspondence from $(\widetilde{f_1}(w), \widetilde{f_2}(w), \widetilde{f_3}(w))$ to $\widetilde{\sigma_2}(w)$. Then by applying Lagrange interpolation formula to Table 1, the function $\widetilde{\sigma_2}$ can be represented by $\widetilde{f_1}, \widetilde{f_2}, \widetilde{f_3}$ as:

$$\begin{aligned}\widetilde{\sigma_2} &= (\widetilde{f_1}\oplus 1)\widetilde{f_2}\widetilde{f_3} \oplus \widetilde{f_1}(\widetilde{f_2}\oplus 1)\widetilde{f_3} \oplus \widetilde{f_1}\widetilde{f_2}(\widetilde{f_3}\oplus 1) \oplus \widetilde{f_1}\widetilde{f_2}\widetilde{f_3}\\ &= \widetilde{f_1}\widetilde{f_2} \oplus \widetilde{f_1}\widetilde{f_3} \oplus \widetilde{f_2}\widetilde{f_3}.\end{aligned} \tag{5}$$

This completes the proof. □

4. Mesnager and Zhang [13, Th.4] proposed a generalization of Rothaus' construction of bent functions in 2017 as follows:

Theorem 4 *[13, Th.4] Let n and m be two even positive integers. Let f_1, f_2 and f_3 be n-variable bent functions. Let g_1, g_2 and g_3 be m-variable bent functions. Denote by ν_1 the function $f_1\oplus f_2\oplus f_3$ and by ν_2 the function $g_1\oplus g_2\oplus g_3$. If both ν_1 and ν_2 are bent functions and if $\widetilde{\nu_1} = \widetilde{f_1}\oplus\widetilde{f_2}\oplus\widetilde{f_3}\oplus 1$, then*

$$\begin{aligned}f(x,y) \quad &= \quad (f_1\oplus f_2)(x)(g_1\oplus g_2)(y)\oplus(f_2\oplus f_3)(x)(g_2\oplus g_3)(y)\oplus f_1(x)\\ &\quad\oplus g_1(y)g_2(y)\oplus g_1(y)g_3(y)\oplus g_2(y)g_3(y)\end{aligned}$$

is an $(n+m)$-variable bent function. Further, if $\widetilde{\nu_2} = \widetilde{g_1}\oplus\widetilde{g_2}\oplus\widetilde{g_3}\oplus\pi$, where π is an m-variable Boolean function, then

$$\begin{aligned}\widetilde{f}(x,y) \quad &= \quad (\widetilde{f_1}\oplus\widetilde{f_2})(x)(\widetilde{g_1}\oplus\widetilde{g_2})(y)\oplus(\widetilde{f_2}\oplus\widetilde{f_3})(x)(\widetilde{g_2}\oplus\widetilde{g_3})(y)\oplus\widetilde{f_1}(x)\\ &\quad\oplus\widetilde{g_3}(y)\oplus\pi(y)\Big((\widetilde{f_1}\oplus\widetilde{f_2})(\widetilde{f_2}\oplus\widetilde{f_3})(x)\Big).\end{aligned} \tag{6}$$

Relation (6) holds under the hypothesis $\widetilde{\nu_2} = \widetilde{g_1}\oplus\widetilde{g_2}\oplus\widetilde{g_3}\oplus\pi$. We shall show that the hypothesis is not necessary when one compute the dual of the bent function $f(x,y)$. We have

Theorem 5 *Let n and m be two even positive integers. Let f_1, f_2, f_3 be n-variable bent functions, and g_1, g_2, g_3 be m-variable bent functions. Denote by ν_1 the function $f_1\oplus f_2\oplus f_3$ and by ν_2 the function $g_1\oplus g_2\oplus g_3$. If both ν_1 and ν_2 are bent functions and if $\widetilde{\nu_1} = \widetilde{f_1}\oplus\widetilde{f_2}\oplus\widetilde{f_3}\oplus 1$, then*

$$\begin{aligned}f(x,y) \quad &= \quad (f_1\oplus f_2)(x)(g_1\oplus g_2)(y)\oplus(f_2\oplus f_3)(x)(g_2\oplus g_3)(y)\oplus f_1(x)\\ &\quad\oplus g_1(y)g_2(y)\oplus g_1(y)g_3(y)\oplus g_2(y)g_3(y)\end{aligned}$$

is an $(n+m)$-variable bent function, and its dual is

$$\begin{aligned}\widetilde{f}(x,y) =&(\widetilde{f_1}\oplus\widetilde{f_2})(\widetilde{f_2}\oplus\widetilde{f_3})(x)\left(\widetilde{g_1}\oplus\widetilde{g_2}\oplus\widetilde{g_3}\oplus\widetilde{\nu_2}\right)(y)\oplus(\widetilde{f_1}\oplus\widetilde{f_2})(x)(\widetilde{g_1}\oplus\widetilde{g_2})(y)\\ &\oplus(\widetilde{f_2}\oplus\widetilde{f_3})(x)(\widetilde{g_2}\oplus\widetilde{g_3})(y)\oplus\widetilde{f_1}(x)\oplus\widetilde{g_3}(y).\end{aligned}\tag{7}$$

Proof Taking $G(z)=(z_1\oplus z_2)(z_4\oplus z_5)\oplus(z_2\oplus z_3)(z_5\oplus z_6)\oplus z_1\oplus z_4z_5\oplus z_4z_6\oplus z_5z_6$, then we have $f(x,y)=G(g_1,g_2,g_3,f_1,f_2,f_3)$. By a straight computation, the nonzero Walsh coefficients of $G(z)$ are as follows:

$$\begin{array}{llll}
W_G(0,0,1,0,0,1)=16, & W_G(0,0,1,0,1,0)=-16, W_G(0,0,1,1,0,0)=16, & & W_G(0,0,1,1,1,1)=16,\\
W_G(0,1,0,0,0,1)=16, & W_G(0,1,0,0,1,0)=16, W_G(0,1,0,1,0,0)=-16, & & W_G(0,1,0,1,1,1)=16,\\
W_G(1,0,0,0,0,1)=16, & W_G(1,0,0,0,1,0)=16, W_G(1,0,0,1,0,0)=16, & & W_G(1,0,0,1,1,1)=-16\\
W_G(1,1,1,0,0,1)=16, & W_G(1,1,1,0,1,0)=-16, W_G(1,1,1,1,0,0)=-16, & & W_G(1,1,1,1,1,1)=-16.
\end{array}$$

According to Relation (2) and together with the bentness of f_1,f_2,f_3,g_1,g_2,g_3, and ν_1, ν_2, we have

$$\begin{aligned}
W_f(w,u) &= \frac{1}{4}W_{g_1}(w)\left(W_{f_1}(u)-W_{f_2}(u)+W_{f_3}(u)+W_{f_1\oplus f_2\oplus f_3}(u)\right)\\
&\quad+\frac{1}{4}W_{g_2}(w)\left(W_{f_1}(u)+W_{f_2}(u)-W_{f_3}(u)+W_{f_1\oplus f_2\oplus f_3}(u)\right)\\
&\quad+\frac{1}{4}W_{g_3}(w)\left(W_{f_1}(u)+W_{f_2}(u)+W_{f_3}(u)-W_{f_1\oplus f_2\oplus f_3}(u)\right)\\
&\quad-\frac{1}{4}W_{g_1\oplus g_2\oplus g_3}(w)\left(-W_{f_1}(u)+W_{f_2}(u)+W_{f_3}(u)+W_{f_1\oplus f_2\oplus f_3}(u)\right)\\
&= 2^{\frac{n+m}{2}-2}\chi_{\widetilde{g_1}}(w)\left(\chi_{\widetilde{f}_1}(u)-\chi_{\widetilde{f_2}}(u)+\chi_{\widetilde{f_3}}(u)+\chi_{\widetilde{\nu_1}}(u)\right)\\
&\quad+2^{\frac{n+m}{2}-2}\chi_{\widetilde{g_2}}(w)\left(\chi_{\widetilde{f}_1}(u)+\chi_{\widetilde{f_2}}(u)-\chi_{\widetilde{f_3}}(u)+\chi_{\widetilde{\nu_1}}(u)\right)\\
&\quad+2^{\frac{n+m}{2}-2}\chi_{\widetilde{g_3}}(w)\left(\chi_{\widetilde{f}_1}(u)+\chi_{\widetilde{f_2}}(u)+\chi_{\widetilde{f_3}}(u)-\chi_{\widetilde{\nu_1}}(u)\right)\\
&\quad-2^{\frac{n+m}{2}-2}\chi_{\widetilde{\nu 2}}(w)\left(-\chi_{\widetilde{f_1}}(u)+\chi_{\widetilde{f_2}}(u)+\chi_{\widetilde{f}_3}(u)-\chi_{\widetilde{\nu_1}}(u)\right).
\end{aligned}$$

We will show that $W_f(w,u)=\pm2^{\frac{n+m}{2}}$ for any $(\widetilde{f}_1(u),\ \widetilde{f}_2(u),\widetilde{f}_3(u))\in GF(2)^3$ with the condition $\widetilde{\nu_1}=\widetilde{f_1}\oplus\widetilde{f_2}\oplus\widetilde{f_3}\oplus1$. In fact, we have the following table:

Table 2: truth table of Boolean function $\widetilde{f}(x,y)$

$\widetilde{f}_1(u)$	$\widetilde{f}_2(u)$	$\widetilde{f}_3(u)$	$W_f(w,u)$	$\widetilde{f}(w,u)$
0	0	0	$2^{\frac{n+m}{2}}\chi_{\widetilde{g_3}}(w)$	$\widetilde{g_3}(w)$
0	0	1	$2^{\frac{n+m}{2}}\chi_{\widetilde{g_2}}(w)$	$\widetilde{g_2}(w)$
0	1	0	$2^{\frac{n+m}{2}}\chi_{\widetilde{g_1}}(w)$	$\widetilde{g_1}(w)$
0	1	1	$2^{\frac{n+m}{2}}\chi_{\widetilde{\upsilon_2}}(w)$	$\widetilde{\upsilon_2}(w)$
1	0	0	$-2^{\frac{n+m}{2}}\chi_{\widetilde{\upsilon_2}}(w)$	$\widetilde{\upsilon_2}(w)\oplus1$
1	0	1	$-2^{\frac{n+m}{2}}\chi_{\widetilde{g_1}}(w)$	$\widetilde{g_1}(w)\oplus1$
1	1	0	$-2^{\frac{n+m}{2}}\chi_{\widetilde{g_2}}(w)$	$\widetilde{g_2}(w)\oplus1$
1	1	1	$-2^{\frac{n+m}{2}}\chi_{\widetilde{g_3}}(w)$	$\widetilde{g_3}(w)\oplus1$

From Table 2, we conclude that the Boolean function $f(x,y)$ is bent.

We now compute the dual of $f(x,y)$ by using Lagrange interpolation formula. Assuming that $z_1 = \widetilde{f}_1, z_2 = \widetilde{f}_2, z_3 = \widetilde{f}_3$ and $y_1 = \widetilde{g}_1, y_2 = \widetilde{g}_2, y_3 = \widetilde{g}_3, y_4 = \widetilde{\nu}_2$. Applying the Lagrange interpolation formula to Table 2, we have

$$\begin{aligned} H(z_1,z_2,z_3,y_1,y_2,y_3,y_4) =& y_3(z_1\oplus 1)(z_2\oplus 1)(z_3\oplus 1)\oplus(y_3\oplus 1)z_1z_2z_3\\ &\oplus y_2(z_1\oplus 1)(z_2\oplus 1)z_3\oplus(y_2\oplus 1)z_1z_2(z_3\oplus 1)\\ &\oplus y_1(z_1\oplus 1)z_2(z_3\oplus 1)\oplus(y_1\oplus 1)z_1(z_2\oplus 1)z_3\\ &\oplus y_4(z_1\oplus 1)z_2z_3\oplus(y_4\oplus 1)z_1(z_2\oplus 1)(z_3\oplus 1)\\ =& (y_3\oplus y_4)\, z_1\oplus((y_1\oplus y_2\oplus y_3\oplus y_4)\, z_1\oplus y_1\oplus y_3)\, z_2\\ &\oplus((y_1\oplus y_2\oplus y_3\oplus y_4)\, z_1\oplus(y_1\oplus y_2\oplus y_3\oplus y_4)\, z_2\oplus y_2\oplus y_3)\, z_3\oplus z_1\oplus y_3\\ =&(z_1\oplus z_2)(z_1\oplus z_3)\,(y_1\oplus y_2\oplus y_3\oplus y_4)\oplus(z_1\oplus z_2)(y_1\oplus y_2)\\ &\oplus(z_2\oplus z_3)(y_2\oplus y_3)\oplus z_1\oplus y_3. \end{aligned} \tag{8}$$

Hence

$$\begin{aligned} \widetilde{f}(x,y) =& H(\widetilde{f}_1,\widetilde{f}_2,\widetilde{f}_3,\widetilde{g}_1,\widetilde{g}_2,\widetilde{g}_3,\widetilde{\nu}_2)\\ =&(\widetilde{f}_1\oplus\widetilde{f}_2)(\widetilde{f}_1\oplus\widetilde{f}_3)\,(\widetilde{g}_1\oplus\widetilde{g}_2\oplus\widetilde{g}_3\oplus\widetilde{\nu}_2)\oplus(\widetilde{f}_1\oplus\widetilde{f}_2)(\widetilde{g}_1\oplus\widetilde{g}_2)\\ &\oplus(\widetilde{f}_2\oplus\widetilde{f}_3)(\widetilde{g}_2\oplus\widetilde{g}_3)\oplus\widetilde{f}_1\oplus\widetilde{g}_3. \end{aligned} \tag{9}$$

This completes the proof. □

Remark 1 *The proof of Theorem 5 shows that one can obtain an explicit form of the dual of $f(x,y)$. In particular, when the dual of ν_2 is $\widetilde{\nu}_2 = \widetilde{g}_1\oplus\widetilde{g}_2\oplus\widetilde{g}_3$, then $\widetilde{f}(x,y) = (\widetilde{f}_1\oplus\widetilde{f}_2)(\widetilde{g}_1\oplus\widetilde{g}_2)\oplus(\widetilde{f}_2\oplus\widetilde{f}_3)(\widetilde{g}_2\oplus\widetilde{g}_3)\oplus\widetilde{f}_1\oplus\widetilde{g}_3$. This implies that the composition of Boolean functions has advantage in analyzing secondary constructions of Boolean functions as a cryptographical tool. Note that the above Boolean functions used to be composed are plateaued functions. This will simplify the design process of building bent functions in terms of the initial functions. Therefore, we should investigate the plateaued Boolean functions which could be used in the secondary constructions of bent functions.*

4 New Secondary Constructions of Bent functions

Throughout this paper, we denote by D the subset of $GF(2)^n$ satisfying that $w\cdot x$ is either balanced or constant on D, for all $w\in GF(2)^n$. We define the *partial Walsh transform* of an n-variable Boolean function f on D(denoted by W_{f_D}) as follows:

$$W_{f_D}(w) = \sum_{x\in D}(-1)^{f(x)\oplus w\cdot x} \text{ for } w\in GF(2)^n. \tag{10}$$

When the cardinality of D is equal to 2^r with even r, we call f *locally bent* restricted to D if and only if $|W_{f_D}(w)| = 2^{r/2}$ for all $w\in \mathrm{GF}(2)^n$. If there is no ambiguity, we say f locally bent function for simplicity. The following observation on plateaued Boolean functions is intrinsic, but we do not find it appear in the literature.

Proposition 1 *Let $S = \{W_g(w) : w\in GF(2)^n\}$ be the Walsh spectrum of a Boolean function g. Then g is plateaued, if and only if there exists an n-variable Boolean function such that it is locally bent restricted to the support of S.*

Proof Let $D = \mathrm{supp}(S)$ the support of S. Assume that g is an n-variable plateaued Boolean function with amplitude 2^k. Then the Parseval's relation implies that $|D|2^{2k} = 2^{2n}$. We have $|D| = 2^{2(n-k)}$. By the inverse Walsh transform we have

$$\begin{aligned}(-1)^{g(x)} &= \frac{1}{2^n}\sum_{w\in GF(2)^n} W_g(w)(-1)^{w\cdot x}\\ &= \frac{1}{2^n}\sum_{w\in D} W_g(w)(-1)^{w\cdot x} \qquad (11)\\ &= \frac{1}{2^{n-k}}\sum_{w\in D}(-1)^{f(w)\oplus w\cdot x}, \text{ for any } x\in GF(2)^n,\end{aligned}$$

where

$$f(w) = \begin{cases} 0, & W_g(w) = 2^k;\\ 1, & W_g(w) = -2^k;\\ 0 \text{ or } 1, & \text{others.}\end{cases}$$

From Relation (11), we deduce that the function $g(x)$ is Boolean if and only if the summation $\sum_{w\in D}(-1)^{f(w)\oplus w\cdot x}$ is constant and equal to $\pm 2^{n-k}$. Note that function $g(x)$ is plateaued, and the cardinality of D is $2^{2(n-k)}$. This implies that $f(x)$ is a locally bent function restricted to D. The sufficiency of Proposition 1 clearly holds from the above discussion. □

Remark 2 *If the subset D of $GF(2)^n$ is a flat, then each $w\cdot x$ is obviously either balanced or constant on D. But the converse is not true. For instance, let $\alpha,\beta\in GF(2)^n, n\geq 4$ and $D = \{\alpha,\beta,\alpha\oplus 1_n,\beta\oplus 1_n\}$, where 1_n is the all-one vector in $GF(2)^n$. Then each $w\cdot x$ is either balanced or constant on D. But the set D is not a flat for $\alpha\neq\beta,\beta\oplus 1_n$.*

The proof of Proposition 1 implies that the corresponding locally bent function with n variables can not be uniquely determined when a plateaued Boolean function is given, since its true values at the points in $\mathrm{GF}(2)^n\backslash D$ is uncertain. To simplify the design process, we hereafter assume that the subset D of $\mathrm{GF}(2)^n$ is a flat and the locally bent function $f(a) = 0$ for any $a\in\mathrm{GF}(2)^n\backslash D$. We illustrate the method of constructing plateaued functions from locally bent functions in the following example.

Example 1 *We shall construct a 3-variable plateaued Boolean function with Walsh support*

$$D = \{(0,0,1),(0,1,0),(1,0,0),(1,1,1)\}.$$

Denote by $a = (0,0,1)$ and $E = \{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}$. Then E is a linear subspace of $\mathrm{GF}(2)^3$, and thus $D = a\oplus E$ is a flat of $\mathrm{GF}(2)^3$. We choose a basis of E, such as $\{(0,1,1),(1,0,1)\}$, and construct a matrix as:

$$H = \begin{pmatrix} 0 & 1 & 1\\ 1 & 0 & 1\end{pmatrix},$$

where the row vectors of H is the basis of E. Then we obtain a one-to-one mapping from the vector space $GF(2)^2$ to the flat D defined by

$$\begin{aligned}\mathrm{GF}(2)^2 &\rightarrow D\\ v &\mapsto a\oplus vH.\end{aligned}$$

Given any bent function $h(x) = x_1x_2$ on $\mathrm{GF}(2)^2$, let

$$f(a\oplus vH) := \begin{cases} h(v), & v\in\mathrm{GF}(2)^2;\\ 0, & \textit{others}.\end{cases}$$

Then $f(0,0,1)=0, f(0,1,0)=0, f(1,0,0)=0, f(1,1,1)=1$. It shows that the Walsh coefficients of g is $W_g(w)=4(-1)^{f(w)}$ if $w\in D$, that is $W_g(0,0,1)=4, W_g(0,1,0)=4, W_g(1,0,0)=4, f(1,1,1)=-4$, and $W_g(w)=0$ if $w\in \mathrm{GF}(2)^n\backslash D$. By the inverse Walsh transform, we have that the truth table of g is $(0,0,0,1,0,1,1,1)$. Thus the ANF of g is $z_1z_2\oplus z_1z_3\oplus z_2z_3$ which is the function being composed in Theorem 3.

By refining previous constructions, we can develop two general secondary constructions of bent functions according to Proposition 1. Since the proof of following Theorem 6 and Theorem 7 is the same as previous, we omit them.

Theorem 6 *Let $D=\{(0,0,1),(0,1,0),(1,0,0),(1,1,1)\}$ and $D^2=D\times D$ be the Cartesian product. Denote by Ω the concatenation of $GF(2)^4$ and D^2, i.e. $\Omega=GF(2)^4\parallel D^2=\{z||(\alpha,\beta), z\in GF(2)^4, \alpha,\beta\in D\}=\{9,74,140,207,273,338,404,471,545,610,676,743,825,890,956,1023\}$ where the positive integer $i\in\Omega$ is denoted by the binary expansion of the vector $(i_9,i_8,\ldots,i_0)\,\mathrm{GF}(2)^{10}$ with $i=\sum\limits_{j=0}^{9} i_j2^j$ for simplicity. It is easy to check that $w\cdot x$ is either balanced or constant on Ω for all $w\in\mathrm{GF}(2)^{10}$.*
Let G be a 10-variable plateaued Boolean function with amplitude 2^8 and Walsh support set Ω. Let f_1, f_2 and f_3 be n-variable bent functions, g_1, g_2 and g_3 be m-variable bent functions. Denote by ν_1 the function $f_1\oplus f_2\oplus f_3$ and by ν_2 the function $g_1\oplus g_2\oplus g_3$. If both ν_1 and ν_2 are bent functions then the composition of Boolean functions $G(z_1,z_2,z_3,z_4,f_1(x),f_2(x),f_3(x),g_1(y),g_2(y),g_3(y))$ is bent.

Proof With the notations in Theorem 6, we assume that $f_1(x), f_2(x), f_3(x)$, and $g_1(y), g_2(y), g_3(y)$ are all bent functions with n and m variables, respectively. By Proposition 1, we can construct a 10-variable plateaued Boolean function with amplitude 2^8 and denote it by G. We construct the composition of Boolean functions

$$f(z_1,z_2,z_3,z_4,x,y)=G(z_1,z_2,z_3,z_4,f_1(x),f_2(x),f_3(x),g_1(y),g_2(y),g_3(y)).$$

Let $F=(z_1,z_2,z_3,z_4,f_1(x),f_2(x),f_3(x),g_1(y),g_2(y),g_3(y))$, $z^*=(z_1,z_2,z_3,z_4)$, $\phi=(f_1(x),f_2(x),f_3(x))$, $\psi=(g_1(y),g_2(y),g_3(y))$. For any $w\in GF(2)^4, u\in GF(2)^n, v\in GF(2)^m$,

$$\begin{aligned} W_f(w,u,v) &= \frac{1}{2^{10}}\sum_{\gamma\in\Omega} W_{G(z)}(\gamma)W_{\gamma\cdot F}(w,u,v) \\ &= \frac{1}{2^{10}}\sum_{\lambda||\alpha||\beta\in\Omega} W_{G(z)}(\lambda,\alpha,\beta)W_{\lambda\cdot z^*}(w)W_{\alpha\cdot\phi}(u)W_{\beta\cdot\psi}(v), \end{aligned} \tag{12}$$

where $\gamma=\lambda||\alpha||\beta$. Because of the equation $W_{\lambda\cdot z^*}(w)=2^4$ if $\lambda=w,$ and 0 others, we have $W_f(w,u,v)=\pm 2^{(n+m+4)/2}$. It shows that f is bent. □

Construction 1 *According to Proposition 1 and Example 1, we obtain a 10-variable plateaued Boolean function with amplitude 2^8 whose ANF is as follows:*

$$\begin{aligned} G(z) =&(z_2\oplus z_4)z_1\oplus(z_1\oplus z_2)z_3\oplus(z_2\oplus z_3\oplus z_4)z_5\oplus(z_1z_3\oplus z_5)z_6 \\ &\oplus(z_1\oplus z_2\oplus z_4\oplus z_5\oplus z_6)z_7\oplus(z_1\oplus z_2\oplus z_5\oplus z_6)z_8\oplus(z_1\oplus z_5\oplus z_7)z_9 \\ &\oplus(z_2\oplus z_6\oplus z_7\oplus 1)z_{10} \end{aligned} \tag{13}$$

By a direct confirmation, we obtain its Walsh support

$$\mathrm{supp}(W_G)=\{9,74,140,207,273,338,404,471,545,610,676,743,825,890,956,1023\},$$

which is equal to Ω. Then the composition of Boolean functions

$$f(z_1,z_2,z_3,z_4,x,y)=G(z_1,z_2,z_3,z_4,f_1(x),f_2(x),f_3(x),g_1(y),g_2(y),g_3(y)) \tag{14}$$

is a bent function.

Because of the extensiveness of the bent functions in the class $\mathcal{M}$, we need to show that the above construction may generate bent functions outside the class $\mathcal{M}$. Recall that the first derivative of an n-variable Boolean function f in the direction of $a \in GF(2)^n$ is defined as $D_a f(x) = f(x) \oplus f(x \oplus a)$. As stated in [7], a bent function f is in the class $\mathcal{M}$ if and only if, $f(x, y) : GF(2)^m \times GF(2)^m \to GF(2)$, the second order derivative of $f(x, y)$ defined as:

$$D_{(a,0_m)} D_{(b,0_m)} f(x, y) = f(x \oplus a \oplus b, y) \oplus f(x \oplus a, y) \oplus f(x \oplus b, y) \oplus f(x, y) = 0,$$

for all $a, b \in GF(2)^m \backslash \{0_m\}$. We consider the special case of $m = 8$ in the following example.

Example 2 *Let $f(x) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$ be a bent function in $\mathcal{M}$ with 6 variables. Assume that $f_1(x) = f(x) \oplus x_1, f_2(x) = f(x) \oplus x_2, f_3(x) = f(x) \oplus x_3, g_1(y) = f(y) \oplus y_1, g_2(y) = f(y) \oplus y_2, g_3(y) = f(y) \oplus y_3$. By Construction 1, we have*

$$\begin{aligned} G(z_1,&z_2, z_3, z_4, f_1(x), f_2(x), f_3(x), g_1(y), g_2(y), g_3(y)) \\ =&z_1z_2 \oplus z_1z_3 \oplus z_1z_4 \oplus z_1x_2 \oplus z_1x_3 \\ &\oplus z_1y_1 \oplus z_1y_2 \oplus z_2z_3 \oplus z_2x_1 \oplus z_2x_3 \oplus z_2y_1 \oplus z_2y_3 \\ &\oplus z_3x_1 \oplus z_3x_2 \oplus z_4x_1 \oplus z_4x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \\ &\oplus x_1x_4 \oplus x_1y_1 \oplus x_1y_2 \oplus x_2x_3 \oplus x_2x_5 \oplus x_2y_1 \oplus x_2y_3 \\ &\oplus x_3x_6 \oplus x_3y_2 \oplus x_3y_3 \oplus y_1y_2y_3 \oplus y_1y_4 \oplus y_2y_5 \oplus y_3y_6 \oplus y_3 \end{aligned} \tag{15}$$

It can be written as

$$\begin{aligned} h : \mathrm{GF}(2)^8 \times \mathrm{GF}(2)^8 &\to \mathrm{GF}(2) \\ (z_1, z_2, x, z_3, z_4, y) &\mapsto \mathrm{GF}(2). \end{aligned} \tag{16}$$

Using the programming SageMath, we confirm that the second order derivatives $D_{(a,0_8)} D_{(b,0_8)} h(z_1, z_2, x, z_3, z_4, y)$ do not vanish for many $a, b \in \mathrm{GF}(2)^8 \backslash \{0_8\}$. This implies that this function is outside the class $\mathcal{M}$. Furthermore, the function is of degree 3, and therefore it does not belong to the class $\mathcal{PS}$. The source codes of SageMath involved in these results are presented in the Section Appendix.

Remark 3 *The Construction 1 is clearly inequivalent to the constructions in Theorem 2,3,4, because it does not depend on the products of input bent functions. But it is uncertain what kind of input functions might be used to possibly generate bent functions outside the known primary classes. We leave it as an open question.*

We can also obtain another generalization of Rothaus' construction when we choose a new set D.

Theorem 7 *Let $D = \{(1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}$, then $\Omega = D \parallel \mathrm{GF}(2)^2$. Choose a plateaued Boolean function G of 5 variables with amplitude 2^4, whose Walsh support is Ω. Let f_1, f_2 and f_3 be n-variable Boolean functions. If the functions $f_1, f_1 \oplus f_2, f_1 \oplus f_3$, and $f_1 \oplus f_2 \oplus f_3$ are all bent, then the composition function $G(f_1, f_2, f_3, z_3, z_4)$ is bent.*

Construction 2 *Let $G(z_1, z_2, z_3, z_4, z_5)$=$(z_1 \oplus z_4)$ $(z_2 \oplus z_5) \oplus z_3$ be a plateaued function with amplitude 2^4, then the Walsh support of G is $\Omega = \{4, 13, 22, 31\}$. Choose any n-variable bent function $f(x)$ and two affine Boolean functions $l_2(x), l_3(x)$, let $f_1 = f$, f_2 =$l_2(x)$, f_3 =$l_3(x)$, then $f_1 \oplus f_2$, $f_1 \oplus f_3$, and $f_1 \oplus f_2 \oplus f_3$ are all bent. We construct the composition of $G(z)$ and f_1, f_2, f_3, as*

$$G(f_1, f_2, f_3, z_4, z_5) = (z_4 \oplus l_2(x))(z_5 \oplus l_3(x)) \oplus f(x).$$

Then $G(f_1, f_2, f_3, z_4, z_5)$ is bent by Theorem 7.

Remark 4 *We note that $G(f_1, f_2, f_3, z_4, z_5)$ can be viewed as a concatenation of functions $f(x) \oplus l_2(x)l_3(x)$, $f(x) \oplus l_2(x)l_3(x) \oplus l_2(x)$, $f(x) \oplus l_2(x)l_3(x) \oplus l_3(x)$, and $f(x) \oplus l_2(x)l_3(x) \oplus l_2(x) \oplus l_3(x)$ by fixing $(z_4, z_5) \in GF(2)^2$. These four Boolean functions are not necessarily bent functions when f is bent. From this observation, we deduce that Construction 2 is not equivalent to the previous ones. However, the function $G(f_1, f_2, f_3, z_4, z_5)$ is of class $\mathcal{M}$ only if $f(x)$ is a bent function in $\mathcal{M}$, since $(z_4 \oplus l_2(x))(z_5 \oplus l_3(x))$ is quadratic.*

5 Conclusion

In this paper, we have shown that some well-known secondary constructions of bent functions can be described by the composition of a plateaued Boolean function and the bent functions. Their duals can be calculated by Lagrange interpolation formula. By following this observation, we proposed two new secondary constructions of bent functions. Since the theory of the constructions we present in this paper is genetic and unified, it is interesting to apply our method to construct Boolean functions with other cryptographical properties. That the problem of choosing the initial functions to produce bent functions outside the known primary classes remains open.

6 Acknowledgement

This research was supported by National Nature Science Foundation of China under Grant No. 61872381, 61872359, 61402522 and 61862011. The work of Wenfen Liu is also supported by Guangxi Key Laboratory of Cryptography and Information Security under No. GCIS201704.

7 Appendix

```
#Source Codes of SageMath about Example 2
#We first validate the bentness of the composition function in Example 2.
sage: B.<z0,z1,z2,z3,z4,z5,z6,z7,z8,z9,x0,x1,x2,x3,x4,x5,
y0,y1,y2,y3,y4,y5> = BooleanPolynomialRing(22)
#pla_subs is the plateaued Boolean function in Example 2
sage: pla_subs = z0*z1 + z0*z2 + z0*z3 + z0*z5 + z0*z6 + z0*z7 + z0*z8
sage:+ z1*z2 + z1*z4 + z1*z6 + z1*z7 + z1*z9 + z2*z4 + z2*z5
sage:+ z3*z4 + z3*z6 + z4*z5 + z4*z6 + z4*z7 + z4*z8 + z5*z6 +
sage:   z5*z7 + z5*z9 + z6*z8 + z6*z9 + z9
sage:show(plateau_subs.expand_trig().trig_simplify())
(x1+x3)x0+(x0+x1)x2+(x1+x2+x3)x4+(x0+x2+x4)x5+(x0+x1+x3+x4+x5)x6
+(x0+x1+x4+x5)x7+(x0+x4+x6)x8+(x1+x5+x6+1)x9
sage: pla_bent_composition = pla_subs.substitute({z4:x0*x1*x2+x0*x3+x1*x4+x2*x5+x0,
sage:z5:x0*x1*x2+x0*x3+x1*x4 +x2*x5+x1,
sage:z6:x0*x1*x2+x0*x3+x1*x4 +x2*x5+x2,
sage:z7:y0*y1*y2+y0*y3+y1*y4 +y2*y5+y0,
sage:z8:y0*y1*y2+y0*y3+y1*y4 +y2*y5+y1,
sage:z9:y0*y1*y2+y0*y3+y1*y4 +y2*y5+y2});
sage: pla_bent_composition
sage: print("*****************************************")
sage: print("The composition of bent functions with plateaued function pla_subs")
sage: print pla_bent_composition;
```

```
sage: print("*****************************************")

*****************************************
The composition of bent functions with plateaued function pla_subs
z0*z1 + z0*z2 + z0*z3 + z0*x1 + z0*x2 + z0*y0 + z0*y1
+ z1*z2 + z1*x0 + z1*x2 + z1*y0 + z1*y2 + z2*x0 + z2*x1
+ z3*x0 + z3*x2 + x0*x1*x2 + x0*x1 + x0*x2 + x0*x3
+ x0*y0 + x0*y1 + x1*x2 + x1*x4 + x1*y0 + x1*y2
+ x2*x5 + x2*y1 + x2*y2 + y0*y1*y2 + y0*y3 + y1*y4
+ y2*y5 + y2
******************************************
sage: from sage.crypto.boolean_function import BooleanFunction
sage: P.<z0,z1,z2,z3,x0,x1,x2,x3,x4,x5,y0,y1,y2,y3,y4,y5> = BooleanPolynomialRing(16)
sage: pla_bent_composition =z0*z1 + z0*z2 + z0*z3 + z0*x1 + z0*x2 + z0*y0 + z0*y1
sage: + z1*z2 + z1*x0 + z1*x2 + z1*y0 + z1*y2 + z2*x0 + z2*x1 + z3*x0 + z3*x2
sage: + x0*x1*x2 + x0*x1 + x0*x2 + x0*x3 + x0*y0 + x0*y1
sage: + x1*x2 + x1*x4 + x1*y0 + x1*y2 + x2*x5 + x2*y1 + x2*y2
sage: + y0*y1*y2 + y0*y3 + y1*y4 + y2*y5 + y2
sage: pla_bent_composition=BooleanFunction(pla_bent_composition)
sage: pla_bent_composition.is_bent( )
True

#Validate the function constructed in Theorem 6 is not in the class M
#D_\alpha D_\beta : \alpha=(e0,e1,a0,a1,a2,a3,a4,a5,0_9)\belta=(f0,f1,c0,c1,c2,c3,c4,c5,0_9)

sage: B.<z0,z1,z2,z3,x0,x1,x2,x3,x4,x5,y0,y1,y2,y3,y4,y5,e0,e1,f0,f1,
a0,a1,a2,a3,a4,a5,c0,c1,c2,c3,c4,c5,d0,d1,d2,d3,d4,d5> = BooleanPolynomialRing(44)
sage: B.<z0,z1,z2,z3,x0,x1,x2,x3,x4,x5,y0,y1,y2,y3,y4,y5,
sage: e0,e1,f0,f1,a0,a1,a2,a3,a4,a5,c0,c1,c2,c3,c4,c5> = BooleanPolynomialRing(32)
sage: pla_bent_composition =z0*z1 + z0*z2 + z0*z3 + z0*x1 + z0*x2 + z0*y0 + z0*y1
+ z1*z2 + z1*x0 + z1*x2 + z1*y0 + z1*y2 + z2*x0 + z2*x1 + z3*x0 + z3*x2
+ x0*x1*x2 + x0*x1 + x0*x2 + x0*x3 + x0*y0 + x0*y1 + x1*x2 + x1*x4 + x1*y0 + x1*y2
+ x2*x5 + x2*y1 + x2*y2 + y0*y1*y2 + y0*y3 + y1*y4 + y2*y5 + y2


sage: print("The 2-derivation of composition of bent functions")
sage: g1 = pla_bent_composition.substitute({z0:z0+e0+f0,z1:z1+e1+f1,
x0:x0+a0+c0,
sage: x1:x1+a1+c1,x2:x2+a2+c2, x3:x3+a3+c3, x4:x4+a4+c4, x5:x5+a5+c5})
sage: g2 = pla_bent_composition.substitute({z0:z0+e0,z1:z1+e1,x0:x0+a0,
x1:x1+a1,x2:x2+a2,x3:x3+a3, x4:x4+a4,x5:x5+a5})
sage: g3 = pla_bent_composition.substitute({z0:z0+f0,z1:z1+f1,x0:x0+c0,
x1:x1+c1,x2:x2+c2,x3:x3+c3, x4:x4+c4,x5:x5+c5})
sage: D_aD_bg = g1+g2+g3 +pla_bent_composition
sage: print D_\alpha D_{\beta}g
sage: show(g1+g2+g3 +pla_bent_composition)
sage: The 2-derivative of composition of bent functions
sage: x0*a1*c2 + x0*a2*c1 + x1*a0*c2 + x1*a2*c0 + x2*a0*c1 + x2*a1*c0
+ e0*f1 + e0*c1 + e0*c2 + e1*f0 + e1*c0 + e1*c2
+ f0*a1 + f0*a2 + f1*a0 + f1*a2 + a0*a1*c2 + a0*a2*c1 + a0*c1*c2 + a0*c1 + a0*c2 + a0*c3
+ a1*a2*c0 + a1*c0*c2 + a1*c0 + a1*c2 + a1*c4 + a2*c0*c1 + a2*c0 + a2*c1 + a2*c5 + a3*c0
+ a4*c1 + a5*c2
#This  shows that  the function we constructed is bent function outside the class M.
```

References

[1] C. Carlet, A construction of bent functions, in S. Cohen & H. Niederreiter (Eds.), Fields and Applications, London Math. Soc., LNCS 233, 1996, 47–58.

[2] C. Carlet, On the secondary constructions of resilient and bent functions, in Proc. Workshop Coding Crypt. Combin. 2003, Birkhäuser Verlag, 2004, 3–28.

[3] C. Carlet, On bent and highly nonlinear balanced/resilient functions and their algebraic immunities, in Proc. AAECC 16, 2006, 1–28.

[4] C. Carlet, "Boolean Functions for Cryptography and Error Correcting Codes", Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering," Cambridge University Press (Peter Hammer and Yves Crama editors), pages 257-397, 2010.

[5] C. Carlet and S. Mesnager, Four decades of research on bent functions, Des. Codes Crypt., 78 (2016), 5–50.

[6] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications. Academic Press, San Diego, 2009.

[7] J. Dillon. Elementary Hadamard Difference Sets, PhD dissertation, Universtiy of Maryland, 1974.

[8] G. Gao, X. Zhang, W. Liu and C. Carlet. Constructions of quadratic and cubic rotation symmetric bent functions. IEEE Transactions on Information Theory, 2012, 58(7), pp. 4908–4913.

[9] K. Gupta, P. Sarkar. A general correlation theorem, in Cryptology ePrint Archive, report 2003/124, see http://ePrint. iacr. org/2003/124.

[10] S. Li, B. Zeng, Y. Lian, A decomposition formula of joint distribution of Boolean random vectors and its applications (in Chinese), Journal on Communications, 1998, 19(11), pp. 61–64.

[11] S. Mesnager, Several new infinite families of bent functions and their duals, IEEE Trans. Inf. Theory, 2014, 60(7), pp. 4397–4407.

[12] S. Mesnager, Bent Functions: Fundamentals and Results, Springer-Verlag, 2016.

[13] S. Mesnager, and F. Zhang. On constructions of bent, semi-bent and five valued spectrum functions from old bent functions. Advances in Mathematics of Communications, 2017, 11(2), pp. 339–345..

[14] Mesnager, P. Ongan, F. Özbudak. New bent functions from permutations and linear translators. Codes, Cryptology and Information Security, LNCS vol. 10194, pp. 282–297, 2017.

[15] S. Mesnager, F. Zhang, and Y. Zhou. On construction of bent functions involving symmetric functions and their duals. Advances in Mathematics of Communications, 2017, 11(2), pp. 347–352.

[16] R. L. McFarland. A family of noncyclic difference sets, Journal of Comb. Theory, Series A, no. 15, 1973, pp. 1–10.

[17] K. Nyberg, Correlation theorems in cryptanalysis. Discrete Applied Mathematics2001, 111, pp. 177–188.

[18] O. S. Rothaus. On “bent” functions. J. Comb. Theory, 20A, 1976, pp. 300-305.

[19] F. Zhang, C. Carlet, Y. Hu and W. Zhang, New secondary constructions of bent functions, Appl. Algebra Eng. Commun. Comput., 2016, 27, pp. 413–434.

[20] F. Zhang, E. Pasalic, Y. Wei, N. Cepak, Constructing bent functions outside the Maiorana-McFarland class using a general form of Rothaus, IEEE Transactions on Information Theory, 2017, 63(8), pp. 5336 –5349.

[21] Y. Zheng, X. M. Zhang, On plateaued functions, IEEE Transactions on Information Theory, 47(3), 2001, pp. 1215–1223.