IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received July 16, 2019, accepted July 28, 2019, date of publication August 1, 2019, date of current version August 16, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2932423

Constructing Boolean Functions Using Blended Representations

QICHUN WANG[1], CAIHONG NIE[2], AND YOULE XU[3]
[1]College of Science, Hunan University of Science and Engineering, Yongzhou 425199, China
[2]School of Mathematical Sciences, Nanjing Normal University, Nanjing 210046, China
[3]School of Computer Science and Technology, Nanjing Normal University, Nanjing 210046, China

Corresponding author: Qichun Wang (qcwang@fudan.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61572189.

ABSTRACT In this paper, we study blended representations of Boolean functions, and construct the following two classes of Boolean functions. Two bounds on the r-order nonlinearity were given by Carlet in the IEEE TRANSACTIONS ON INFORMATION THEORY, vol. 54. In general, the second bound is better than the first bound. But it was unknown whether it is always better. Recently, Mesnager *et al.* constructed a class of Boolean functions where the second bound is strictly worse than the first bound, for $r = 2$. However, it is still an open problem for $r \geq 3$. Using the blended representation, we construct a class of Boolean functions based on the trace function and show that the second bound can also be strictly worse than the first bound, for $r = 3$. The second class is based on the hidden weighted bit function, which seems to have the best cryptographic properties among all currently known functions.

INDEX TERMS Boolean functions, blended representations, nonlinearity, algebraic immunity, higher-order nonlinearity.

I. INTRODUCTION

Boolean functions have many applications in logic, electrical engineering, reliability theory, game theory, combinatorics, computational complexity, coding theory, cryptography, etc [14]. A Boolean function can be represented using many ways, e.g., the truth table, the algebraic normal form, the univariate polynomial representation, etc [2], [15]. In this paper, we combine the algebraic normal form and the univariate polynomial representation, and construct Boolean functions using blended representations.

The covering radius of the Reed–Muller code $RM(r, n)$ is the same as the maximum r-order nonlinearity of n-variable Boolean functions. In [36], Schatz proved that the maximum 2-order nonlinearity of 6-variable Boolean functions is 18. For $n \geq 7$, the covering radius of $RM(2, n)$ is still unknown [4], [9], [11]. In 2019, Wang and Stănică proved that the maximum 2-order nonlinearity of 7-variable Boolean functions is at most 42 [43]. For $n \geq 7$, the covering radius of $RM(3, n)$ is also unknown [9], [19]. In 2018, Wang *et al.* proved that the maximum 3-order nonlinearity of 7-variable Boolean functions with degree at most 4 is 20 [46].

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

For general n, two lower bounds on the r-order nonlinearity of n-variable Boolean functions were given by Carlet in [5]. In general, the second bound is better than the first bound. But it was unknown whether it is always better. In [31], Mesnager *et al.* constructed a class of Boolean functions where the first bound is tight and the second bound is strictly worse than the first bound, for $r = 2$. However, it is still an open problem for $r \geq 3$. Using the blended representation, we construct a class of Boolean functions based on the trace function and show that the second bound can be strictly worse than the first bound, for $r = 3$.

It is difficult to construct cryptographic Boolean functions resisting all the main attacks [7], [8], [10], [16]–[18], [23]–[27], [32]–[34], [37]–[39], [42], [44], [45], [48]–[50]. The hidden weighted bit function (HWBF) was introduced by Bryant in [1] and revisited by Knuth in [22]. In 2014, Wang *et al.* investigated the cryptographic properties of the HWBF and found that it seems to be a very good candidate for being used in real ciphers [40], [47]. Our second construction is based on the HWBF and seems to have the best cryptographic properties among all currently known functions.

The paper is organized as follows. In Section 2, the necessary background is established. We then introduce the blended representations in Section 3. In Section 4,

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

we construct two classes of Boolean functions using the blended representations. We end in Section 5 with conclusions.

II. PRELIMINARIES

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_2$. An n-variable Boolean function f is a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$, and it can be represented by the output column of its truth table, i.e., a binary string of length 2^n

$$f(0,\ldots,0), f(1,\ldots,0), f(0,1,\ldots,0),\\ f(1,1,\ldots,0),\ldots,f(1,\ldots,1).$$

We denote by B_n the set of all n-variable Boolean functions.

Any Boolean function $f \in B_n$ can be uniquely represented as a multivariate polynomial in $\mathbb{F}_2[x_1,\cdots,x_n]$,

$$f(x_1,\ldots,x_n) = \bigoplus_{K\subseteq\{1,2,\ldots,n\}} a_K \prod_{k\in K} x_k,$$

which is called its algebraic normal form (ANF). The algebraic degree of f, denoted by $\deg(f)$, is the number of variables in the highest order term with nonzero coefficient.

A Boolean function is affine if there exists no term of degree strictly greater than 1 in the ANF. The set of all affine functions is denoted by A_n.

Let

$$1_f = \{x \in \mathbb{F}_2^n | f(x) = 1\}, \quad 0_f = \{x \in \mathbb{F}_2^n | f(x) = 0\},$$

be the support of a Boolean function f, respectively, its complement. The cardinality of 1_f is called the Hamming weight of f, and will be denoted by $wt(f)$. The Hamming distance between two functions f and g is the Hamming weight of $f \oplus g$, and will be denoted by $d(f,g)$. We say that an n-variable Boolean function f is balanced if $wt(f) = 2^{n-1}$.

Let $f \in B_n$. The nonlinearity of f is its distance from the set of all n-variable affine functions, that is,

$$nl(f) = \min_{g\in A_n} d(f,g).$$

The nonlinearity of an n-variable Boolean function is bounded above by $2^{n-1} - 2^{n/2-1}$, and a function is said to be bent if it achieves this bound. Clearly, bent functions exist only for even n and it is known that the algebraic degree of a bent function is bounded above by $\frac{n}{2}$ [2], [35]. The r-order nonlinearity, denoted by $nl_r(f)$, is its distance from the set of all n-variable functions of algebraic degrees at most r.

For any $f \in B_n$, a nonzero function $g \in B_n$ is called an annihilator of f if fg (the function defined by $fg(x) = f(x)g(x)$) is null, and the algebraic immunity of f, denoted by $\mathcal{AI}(f)$, is the minimum value of d such that f or $f+1$ admits an annihilator of degree d [30]. It is known that the algebraic immunity of an n-variable Boolean function is bounded above by $\lceil \frac{n}{2} \rceil$ [13].

If we can find g of low degree and h of algebraic degree not much larger than $n/2$ such that $fg = h$, then f is considered to be weak against fast algebraic attacks [12], [20]. The higher order nonlinearities of a function with high (fast) algebraic immunity is also not very low [3], [29], [31], [41].

The Walsh transform of a given function $f \in B_n$ is the integer-valued function over the finite field $\mathbb{F}_{2^n}$ defined by

$$W_f(\omega) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+Tr(\omega x)},$$

where $\omega \in \mathbb{F}_{2^n}$ and $Tr(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. The nonlinearity of f can then be determined by

$$nl(f) = 2^{n-1} - \frac{1}{2}\max_{\omega\in\mathbb{F}_{2^n}} |W_f(\omega)|.$$

III. BLENDED REPRESENTATIONS OF BOOLEAN FUNCTIONS

Every function $g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ can be uniquely represented as a polynomial $\sum_{i=0}^{2^n-1} a_i x^i$ (called its univariate representation), where $a_i \in \mathbb{F}_{2^n}$. Clearly, g is a Boolean function if and only if $\sum_{i=0}^{2^n-1} a_i x^i \in \mathbb{F}_2$ for any $x \in \mathbb{F}_{2^n}$.

Let g be the univariate representation of an n-variable Boolean function and $\alpha \in \mathbb{F}_{2^n}$ be a primitive element. We define the function f_α from $\mathbb{F}_2^n$ into $\mathbb{F}_2$ as follows

$$f_\alpha(x) = \begin{cases} lg(0) & \text{if } x = 0,\\ g(\alpha^{|x|-1}) & \text{otherwise,}\end{cases} \tag{1}$$

where $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ and $|x| = x_1 + 2x_2 + 2^2x_3 + \ldots + 2^{n-1}x_n$.

Similarly, let f be the ANF of an n-variable Boolean function and $\alpha \in \mathbb{F}_{2^n}$ be a primitive element. We define the function g_α from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$ as follows

$$g_\alpha(x) = \begin{cases} f(0) & \text{if } x = 0,\\ f(i_1,\ldots,i_n) & \text{if } x = \alpha^i,\end{cases} \tag{2}$$

where $0 \le i \le 2^n-2$ and $i+1 = i_1+2i_2+2^2i_3+\ldots+2^{n-1}i_n$.

Example 1: Let $g(x) = Tr(x) \in B_3$ and $\alpha^3+\alpha+1 = 0$. Then the truth table of f_α defined by (1) is 01001011, and its ANF is $x_1x_2 \oplus x_1 \oplus x_3$. Let $f(x) = x_n \in B_n$. Then the support set of g_α defined by (2) is $1_{g_\alpha} = \{\alpha^{2^{n-1}-1}, \ldots, \alpha^{2^n-2}\}$, which can be viewed as a Carlet-Feng function [8].

Let g be the univariate representation of an n-variable Boolean function. A natural question is whether f_α and f_β defined by (1) are affine equivalent, for different primitive elements $\alpha, \beta \in \mathbb{F}_{2^n}$.

If α and β are roots of the same primitive polynomial, then f_α and f_β are affine equivalent, which can be seen from the following proposition.

Proposition 1: Let $\alpha, \beta \in \mathbb{F}_{2^n}$ be primitive elements and $\beta = \alpha^{2^i}$, where $1 \le i \le n-1$. Then f_α and f_β defined by (1) are affine equivalent.

Proof: For $0 \neq x \in \mathbb{F}_2^n$, we have

$$f_\beta(x) = g(\beta^{|x|}) = g(\alpha^{2^i|x|}) = g(\alpha^{x_{n-i+1}+\ldots+2^{i-1}x_n+2^i x_1+\ldots+2^{n-1}x_{n-i}}) = f_\alpha(y),$$

where $y = (x_{n-i+1}, \ldots, x_n, x_1, \ldots, x_{n-i})$. Let A be the $n \times n$ matrix with entries from $\mathbb{F}_2$ such that $(x_1, x_2, \ldots, x_n)A = y$. Then A is nonsingular and $f_\beta(x) = f_\alpha(xA)$. Hence, f_α and f_β are affine equivalent. □

If α and β are roots of different primitive polynomials, then there exists an infinite class of $g \in B_n$ such that f_α and f_β defined by (1) are not affine equivalent, which can be seen from the following proposition.

Proposition 2: Let $\alpha, \beta \in \mathbb{F}_{2^n}$ be primitive elements and $\beta \neq \alpha^{2^i}$, where $0 \leq i \leq n-1$. Let $1_g = \{\alpha^{2j-1} \mid 1 \leq j \leq 2^{n-1}\}$. Then f_α and f_β defined by (1) are not affine equivalent.

Proof: Since f_β and $f_{\beta^{2^i}}$ are affine equivalent, we only need to prove the proposition for $\beta = \alpha^d$, where $3 \leq d < 2^{n-1}$ is odd and $(d, 2^n-1) = 1$. Clearly, the truth table of f_α is

$$c_0c_1c_2c_3\cdots c_{2^n-2}c_{2^n-1} = 0101\cdots01$$

and $f_\alpha(x_1, \ldots, x_n) = x_1$. The truth table of f_β is

$$c'_0c'_1c'_2c'_3\cdots c'_{2^n-2}c'_{2^n-1} = c_0c_dc_{2\circ d}c_{3\circ d}\cdots c_{(2^n-2)\circ d}c_{2^n-1},$$

where $k \circ d = kd \ (mod\ 2^n-1)$, for $k = 2, 3, \ldots, 2^n-2$. Clearly, we have

$$c'_i = \begin{cases} c_i, & \text{if } \lfloor \frac{2k(2^n-1)}{d} \rfloor + 1 \leq i \leq \lfloor \frac{(2k+1)(2^n-1)}{d} \rfloor, \\ \overline{c_i}, & \text{if } \lfloor \frac{(2k+1)(2^n-1)}{d} \rfloor + 1 \leq i \leq \lfloor \frac{(2k+2)(2^n-1)}{d} \rfloor, \end{cases}$$

where $k \in \mathbb{Z}$ and $\overline{c_i} = c_i \oplus 1$.

Suppose f_α and f_β are affine equivalent. Then f_β is an affine function and for $1 \leq m \leq n-2$, it can be written as $f_0||f_1||\cdots||f_{2^m-1}$, where $\deg(f_i) \leq 1$ for $0 \leq i \leq 2^m-1$.

Claim 1: There exists an integer $2 \leq t \leq n-2$ such that $\lfloor \frac{2^n-1}{d} \rfloor = 2^t - 1$.

Proof: Suppose $2^{t-1} < \lfloor \frac{2^n-1}{d} \rfloor + 1 < 2^t$, where $2 \leq t \leq n-1$. We write f_β as $f_0||f_1||\cdots||f_{2^{n-t}-1}$, where $f_i \in B_t$. Then

$$0 < wt(f_0 \oplus x_1) = 2^t - \lfloor \frac{2^n-1}{d} \rfloor - 1 < 2^{t-1}.$$

Therefore, $\deg(f_0) \geq 2$ which is a contradiction.

Claim 2: $\lfloor \frac{k(2^n-1)}{d} \rfloor = k2^t - 1$, for $2 \leq k \leq d-1$.

Proof: Let $f_\beta = f_0||f_1||\cdots||f_{2^{n-t}-1}$. Suppose $2 \leq k_0 \leq d-1$ is the smallest number such that $\lfloor \frac{k_0(2^n-1)}{d} \rfloor \neq k_02^t - 1$. Then $\lfloor \frac{k_0(2^n-1)}{d} \rfloor = k_02^t$ or $k_02^t - 2$. If $\lfloor \frac{k_0(2^n-1)}{d} \rfloor = k_02^t - 2$, then $wt(f_{k_0-1} \oplus x_1) = 1$ or $2^t - 1$, which is contradictory to the fact that $\deg(f_{k_0-1}) \leq 1$. If $\lfloor \frac{k_0(2^n-1)}{d} \rfloor = k_02^t$, then $wt(f_{k_0} \oplus x_1) = 1$ or $2^t - 1$, which is contradictory to the fact that $\deg(f_{k_0}) \leq 1$.

By Claims 1 and 2, we have

$$|0_{f_\beta \oplus x_1}| - |1_{f_\beta \oplus x_1}| = 2^n - 1 - \lfloor \frac{(d-1)(2^n-1)}{d} \rfloor.$$

Therefore, $0 < wt(f_\beta \oplus x_1) < 2^{n-1}$ and $\deg(f_\beta \oplus x_1) \geq 2$. Hence, $\deg(f_\beta) \geq 2$ and the result follows. □

We now consider cryptographic properties of the functions in the same blended representation. Let f be the ANF of an n-variable Boolean function and $\alpha \in \mathbb{F}_{2^n}$ be a primitive element. Clearly, $wt(g_\alpha) = wt(f)$ and g_α is balanced if and only if f is balanced. If $|wt(f) - 2^{n-1}|$ is sufficiently large, then g_α and f have the same algebraic degree, algebraic immunity and nonlinearity. However, in general, cryptographic properties of g_α and f may be quite different. In fact, for any balanced function $f \in B_n$, we can find an $\alpha \in \mathbb{F}_{2^n}$ such that the function g_α defined by (2) has the optimum algebraic degree $n-1$, where $2^n - 1$ is a prime.

Proposition 3: Let $f \in B_n$ be balanced and $2^n - 1$ be a prime. Then there exists an $\alpha \in \mathbb{F}_{2^n}$ such that the function g_α defined by (2) has the optimum algebraic degree $n-1$.

Proof: Since $2^n - 1$ is a prime, there are exactly $\frac{2^n-2}{n}$ primitive polynomials of degree n and the product of these polynomials is $\sum_{i=0}^{2^n-2} x^i$. Clearly,

$$\sum_{i=0}^{2^n-2} x^i \nmid \sum_{j \in 1_f} x^j.$$

Therefore, there exists a primitive element $\alpha \in \mathbb{F}_{2^n}$ such that $\sum_{j \in 1_f} \alpha^j \neq 0$. Let $g_\alpha(x) = \sum_{i=0}^{2^n-1} a_i x^i$ be the univariate representation of the function defined by (2). Then g_α is balanced and $\deg(g_\alpha) \leq n-1$. For every $1 \leq i \leq 2^n-2$, we have

$$a_i = \sum_{j=0}^{2^n-2} g_\alpha(\alpha^j)\alpha^{-ij}.$$

Therefore,

$$a_{2^n-2} = \sum_{j=0}^{2^n-2} g_\alpha(\alpha^j)\alpha^{-(2^n-2)j} = \sum_{j=0}^{2^n-2} f(j)\alpha^j = \sum_{j \in 1_f} \alpha^j \neq 0,$$

and the result follows. □

IV. CONSTRUCTIONS OF BOOLEAN FUNCTIONS USING BLENDED REPRESENTATIONS

A. CONSTRUCTION 1

Let $g = Tr(x) \in B_n$ and $\alpha \in \mathbb{F}_{2^n}$ be a primitive element. Then the function f_α defined by (1) is

$$f_\alpha(x) = \begin{cases} 0 & \text{if } x = 0, \\ Tr(\alpha^{|x|-1}) & \text{otherwise}, \end{cases}$$

where $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ and $|x| = x_1 + 2x_2 + 2^2x_3 + \ldots + 2^{n-1}x_n$.

In Table 1, we give the cryptographic properties of $f_\alpha \in B_8$, where $p(x)$ denotes the primitive polynomial with $p(\alpha) = 0$ ($p(x)$ is given in an octal representation, for example,

TABLE 1. Cryptographic properties of $f_\alpha \in B_8$.

$p(x)$	$\deg(f_\alpha)$	$\mathcal{AI}(f_\alpha)$	$nl(f_\alpha)$
435	7	4	108
561	7	4	104
551	7	4	108
455	7	4	108
747	7	4	108
717	7	4	106
453	7	4	106
651	7	4	100
545	7	4	108
515	7	4	108
543	7	4	104
615	7	4	96
537	7	4	100
765	7	4	108
703	7	4	104
607	7	4	100

the binary equivalent of 435 is 100011101 and the corresponding polynomial is $x^8+x^4+x^3+x^2+1$). Clearly, f_α has the optimum algebraic degree and the optimum algebraic immunity for all primitive polynomials of degree 8.

We do not know whether $f_\alpha \in B_n$ always have the optimum algebraic degree, which we leave as an open problem.

Let $f \in B_n$ and $D_c(f) = f(x) + f(x + c)$, where $c \in \mathbb{F}_2^n$. In [5], Carlet proved that

$$nl_r(f) \geq \frac{1}{2} \max_{c \in \mathbb{F}_2^n} nl_{r-1}(D_c(f)), \tag{3}$$

and

$$nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{c\in\mathbb{F}_2^n} nl_{r-1}(D_c(f))}. \tag{4}$$

In general, (4) can lead to efficient bounds. But it was unknown whether the following inequality always holds:

$$2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{c\in\mathbb{F}_2^n} nl_{r-1}(D_c(f))} \geq \frac{1}{2} \max_{c \in \mathbb{F}_2^n} nl_{r-1}(D_c(f)). \tag{5}$$

In [31], Mesnager *et al.* constructed a class of Boolean functions to show that the inequality (5) can not always hold for $r = 2$. However, it is still an open problem for $r \geq 3$. In the following, we show that the inequality (5) can not always hold for $r = 3$.

Proposition 4: Let $\alpha \in \mathbb{F}_{2^6}$ be a root of $x^6 + x + 1$ and $f_\alpha \in B_6$ be defined by

$$f_\alpha(x) = \begin{cases} 0 & \text{if } x = 0, \\ Tr(\alpha^{|x|-1}) & \text{otherwise.} \end{cases}$$

Let $f \in B_n$ and $f(x_1, \ldots, x_n) = f_\alpha(x_1, \ldots, x_6)$, where $n \geq 6$. Then

$$2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{c\in\mathbb{F}_2^n} nl_{r-1}(D_c(f))} < \frac{1}{2} \max_{c \in \mathbb{F}_2^n} nl_{r-1}(D_c(f)),$$

for $r = 3$.

Proof: Let $c = (c_1, \ldots, c_n) \in \mathbb{F}_2^n$. Then

$$\begin{aligned} D_c(f) &= f(x) \oplus f(x \oplus c) \\ &= f_\alpha(x_1, \ldots, x_6) \oplus f_\alpha(x_1 \oplus c_1, \ldots, x_6 \oplus c_6) = D_{\widetilde{c}}(f_\alpha), \end{aligned}$$

where $\widetilde{c} = (c_1, \ldots, c_6)$. It is easy to calculate that

$$nl_2(D_c(f_\alpha)) = \begin{cases} 0 & \text{if } c = 0, \\ 8 & \text{if } c \in B, \\ 12 & \text{otherwise,} \end{cases}$$

where $B =$

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

Therefore,

$$\begin{aligned} \sum_{c\in\mathbb{F}_2^n} nl_2(D_c(f)) &= 2^{n-6} * 2^{n-6} \sum_{\widetilde{c}\in\mathbb{F}_2^6} nl_2(D_{\widetilde{c}}(f_\alpha)) \\ &= (8*30 + 12*33) * 2^{2n-12} = 636 * 2^{2n-12}, \end{aligned}$$

and

$$\max_{c\in\mathbb{F}_2^n} nl_2(D_c(f)) = 2^{n-6} \max_{\widetilde{c}\in\mathbb{F}_2^6} nl_2(D_{\widetilde{c}}(f)) = 12 * 2^{n-6}.$$

Clearly,

$$\begin{aligned} &2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2*636*2^{2n-12}} \\ &\qquad = (32 - \sqrt{706}) * 2^{n-6} < 6 * 2^{n-6}, \end{aligned}$$

and the result follows. □

Remark 1: Let $f \in B_n$ and $f(x_1, \ldots, x_n) = f_\alpha(x_1, \ldots, x_6)$. Then by (3), $nl_3(f) > 6*2^{n-6}$. While by (4), we have $nl_3(f) > 5.4 * 2^{n-6}$. Clearly, the bound deduced by (3) is better than the bound deduced by (4), and the difference between these two bounds tends to infinity when $n \to \infty$.

B. CONSTRUCTION 2

Let $hw \in B_n$ be the hidden weighted bit function. That is,

$$hw(x) = \begin{cases} 0 & \text{if } x = 0, \\ x_{wt(x)} & \text{otherwise,} \end{cases}$$

where $wt(x) = x_1 + x_2 + \ldots + x_n$. Then the function defined by (2) is

$$g_\alpha(x) = \begin{cases} 0 & \text{if } x = 0, \\ hw(i_1, \ldots, i_n) & \text{if } x = \alpha^i, \end{cases} \tag{6}$$

where $0 \leq i \leq 2^n-2$ and $i+1 = i_1+2i_2+2^2i_3+\ldots+2^{n-1}i_n$.

TABLE 2. Cryptographic properties of g_α and nonlinearities of functions in [8], [37].

n	$\deg(g_\alpha)$	$\mathcal{AI}(g_\alpha)$	$nl(g_\alpha)$	$nl(CF)$	$nl(MCF)$
8	7	4	112	112	108
9	8	5	232	232	
10	9	5	484	484	476
11	10	6	984	980	
12	11	6	1994	1970	1982
13	12	7	4004	3988	
14	13	7	8074	8036	8028
15	14	8	16216	16212	

TABLE 3. Behavior of the function g_α against Fast algebraic attacks.

n	8	9	10	11	12	13
(d,e)	(1,6)	(1,8)	(1,8)	(1,10)	(1,10)	(1,12)
	(2,5)	(2,7)	(2,8)	(2,8)	(2,9)	(2,11)
	(3,4)	(3,6)	(3,7)	(3,8)	(3,8)	(3,10)
		(4,5)	(4,6)	(4,7)	(4,8)	(4,8)
				(5,6)	(5,7)	(5,8)
						(6,7)
$\min\{d+e\}$	7	9	9	10	11	12

In Table 2, one can find some cryptographic properties of this function $g_\alpha \in B_n$. As a comparison, in that table, we also give the nonlinearity of the Carlet-Feng function which denoted by $nl(CF)$, and the nonlinearity of the even-variable balanced function proposed by [37] which denoted by $nl(MCF)$. Clearly, the function f has very good cryptographic properties: balancedness, optimum algebraic degree, optimum algebraic immunity and high nonlinearity (higher than the Carlet-Feng function and the function proposed by [37]).

Let $\deg(g_1) = d < \mathcal{AI}(g_\alpha)$ and $g_\alpha \cdot g_1 = g_2$. To resist the fast algebraic attacks, $\deg(g_2)$ is expected to be as high as possible for any g_1 of low degree. Let $\deg(g_2) = e$. For $8 \leq n \leq 13$, in Table 3, we give the lowest possible values of (d, e). Clearly, $d+e = n$ for $n = 9$, and $d+e \geq n-1$ for $n = 8, 10, 11, 12, 13$. This is the optimum case for an n-variable Boolean function to resist the fast algebraic attacks [28].

Example 5: Taking $n = 12$, we get the function $g_\alpha \in B_{12}$, where α is a root of $x^{12} + x^{10} + x^9 + x^8 + x^6 + x^2 + 1$. We have $\deg(g_\alpha) = 11$, $\mathcal{AI}(g_\alpha) = 6$, $nl(g_\alpha) = 1994$ and g_α has the optimum behavior against fast algebraic attacks. As a comparison, the nonlinearity of the Carlet-Feng function CF is 1970, and the nonlinearity of the function MCF proposed by [37] is 1982. The function g_α is balanced and with the optimum algebraic degree, optimum algebraic immunity and optimum behavior against fast algebraic attacks. It has the highest nonlinearity among all those known functions with the above properties. The truth table of g_α can be found in Appendix, where the numbers are in hexadecimal.

V. CONCLUSION

In this paper, we study blended representations of Boolean functions, and construct two classes of quite interesting Boolean functions. We hope that our work would attract more researchers to be interested in blended representations.

APPENDIX

The truth table of g_α in Example 5:

72A9	337E	A0E0	924B	92DE	235B
3C77	6F95	6CBB	4C01	F9F0	8C60
712F	C441	67A5	B84D	428B	30B4
EA2A	DE58	402C	58E5	2747	83A5
45F8	73A0	AE6E	CF79	9B98	3B9C
2077	DD06	EFF3	BE31	F15F	954B
5361	E161	1619	9437	CB7E	732A
CD3B	A64D	BBD8	8790	3DE2	61C4
D7C6	0237	D0B8	79FF	B6A6	43A2
0E85	C5B8	3678	3C2D	F82A	2E0F
D6FE	61E4	AC0C	5BE2	8301	8175
10A2	D0F9	12AC	8C10	6E94	DD28
E8D4	E2D8	A2FD	6258	E49B	B636
24D5	E2C2	4522	D049	88B0	B329
0B0D	5030	92E7	CA29	6222	0635
6FD8	3CBF	F48C	8276	437C	AB4F
0C98	1791	A7F9	B098	09DE	153E
603D	2485	6AD1	33D9	97A8	71B1
DA86	3F49	2EED	B59E	F5E7	449A
F00A	D78C	5065	A379	B953	BF18
0943	0086	47FC	A74B	7157	F54D
8630	13F9	2DA0	F7A4	75AE	9884
585F	13D7	A85E	803C	F6B1	3B5F
7D17	E6EF	C3A3	194A	8989	F21E
021A	2C4E	2777	A9BA	69AB	4A1C
81EB	9677	26EA	3910	11E3	D443
A19D	1CCC	51A1	1DE3	6E68	F372
ADDB	4B1D	3537	30BF	78AA	F366
7E35	DBAD	ECFB	707A	6EEB	4198
1579	E92C	D9AB	E1B9	E5C9	B894
43A1	AD3B	758E	9005	00D7	3F45
37E1	9289	EEF5	C10E	3235	EBA1
DF2F	3C9F	FCE4	3D79	2B80	1A64
62EF	663D	FF9D	8823	5C49	F4A2
93AF	E25E	F995	3F96	9B2B	06EC
BAB8	1C26	9860	12BB	4479	B15D
1C79	759B	E20A	857C	F287	A7AD
106D	B822	4894	118A	CF87	6469
047A	DE13	AC60	1B8A	8CE5	899E
7BF2	DA2C	9138	6CF1	3400	F83B
5BBC	4E75	DB5E	1BE7	D7D8	020D
6B92	9F3A	E1D8	6DE0	21ED	4A88
2783	A0F7	EEF2	4266		

REFERENCES

[1] R. E. Bryant, "On the complexity of VLSI implementations and graph representations of Boolean functions with application to integer multiplication," *IEEE Trans. Comput.*, vol. 40, no. 2, pp. 205–213, Feb. 1991.

[2] C. Carlet, "Boolean functions for cryptography and error correcting codes," in *Boolean Models and Methods Mathematics Computer Science and Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2010, pp. 257–397. Available:. [Online]. Available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html

[3] C. Carlet, "On the higher order nonlinearities of algebraic immune functions," *Advances in Cryptology—CRYPTO*. New York, NY, USA: Springer, 2006, pp. 584–601.

[4] C. Carlet. (2006). *The Complexity of Boolean Functions From Cryptographic Viewpoint*. [Online]. Available: http://dblp.unitrier.de/db/conf/dagstuhl/P6111.html

[5] C. Carlet, "Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 1262–1272, Mar. 2008.

[6] C. Carlet, "Comments on Constructions of cryptographically significant Boolean functions using primitive polynomials," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4852–4853, Jul. 2011.

[7] C. Carlet, D. K. Dalai, K. C. Gupta, and S. Maitra, "Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3105–3121, Jul. 2006.

[8] C. Carlet and K. Q. Feng, "An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," in *Advances in Cryptology—ASIACRYPT* (Lecture Notes in Computer Science), vol. 5350. Berlin, Germany: Springer, 2008, pp. 425–440.

[9] C. Carlet and S. Mesnager, "Improving the upper bounds on the covering radii of binary Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 162–173, Jan. 2007.

[10] C. Carlet and D. Tang, "Enhanced Boolean functions suitable for the filter model of pseudo-random generator," *Des., Codes Cryptogr.*, vol. 76, no. 3, pp. 571–587, 2015.

[11] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: Elsevier, 1997.

[12] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 2729. Springer-Verlag, 2003, pp. 176–194.

[13] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 2656. Springer-Verlag, 2003, pp. 345–359.

[14] Y. Crama and P. L. Hammer, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[15] T. W. Cusick, P. Stănică, *Cryptographic Boolean Functions and Applications*, Amsterdam, The Netherlands: Elsevier, 2009.

[16] D. K. Dalai, K. C. Maitra, and S. Maitra, "Cryptographically significant Boolean functions: Construction and analysis in terms of algebraic immunity," in *Proc. Int. Workshop Fast Softw. Encryption* in Lecture Notes in Computer Science, vol. 3557. Springer-Verlag, 2005, pp. 98–111.

[17] D. K. Dalai, S. Maitra, and S. Sarkar, "Basic theory in construction of Boolean functions with maximum possible annihilator immunity," *Des., Codes Cryptogr.*, vol. 40, no. 1, pp. 41–58, Jul. 2006.

[18] K. Feng, Q. Liao, and J. Yang, "Maximal values of generalized algebraic immunity," *Des., Codes Cryptogr.*, vol. 50, no. 2, pp. 243–252, Feb. 2009.

[19] R. Gode and S. Gangopadhyay, "Third-order nonlinearities of a subclass of Kasami functions," *Cryptogr. Commun.*, vol. 2, no. 1, pp. 69–83, Apr. 2010.

[20] P. Hawkes and G. G. Rose, "Rewriting variables: The complexity of fast algebraic attacks on stream ciphers," in *Advances in Cryptology—CRYPTO*, (Lecture Notes in Computer Science), vol. 3152. Springer-Verlag, 2004, pp. 390–406.

[21] X. D. Hou, "Some results on the covering radii of Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 39, no. 2, pp. 366–378, Mar. 1993.

[22] D. E. Knuth, *The Art of Computer Programming, Fascicle 1: Bitwise Tricks & Techniques; Binary Decision Diagrams*, vol. 4. Reading, MA, USA: Addison-Wesley, 2009.

[23] J. Li, C. Carlet, X. Zeng, C. Li, L. Hu, and J. Shan, "Two constructions of balanced Boolean functions with optimal algebraic immunity, high nonlinearity and good behavior against fast algebraic attacks," *Des., Codes Cryptogr.*, vol. 76, no. 2, pp. 279–305, Aug. 2015.

[24] N. Li and W.-F. Qi, "Construction and analysis of Boolean functions of $2t + 1$ variables with maximum algebraic immunity," in *Advances in Cryptology—ASIACRYPT* (Lecture Notes in Computer Science), vol. 4284. Springer-Verlag, 2006, pp. 84–98.

[25] N. Li, L. Qu, W.-F. Qi, G. Feng, C. Li, and D. Xie, "On the construction of Boolean functions with optimal algebraic immunity," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 1330–1334, Mar. 2008.

[26] K. Limniotis and N. Kolokotronis, "Boolean functions with maximum algebraic immunity: Further extensions of the Carlet–Feng construction," *Des., Codes Cryptogr.*, vol. 86, no. 8, pp. 168–1706, Aug. 2018.

[27] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, "Secondary constructions of Boolean functions with maximum algebraic immunity," *Cryptogr. Commun.*, vol. 5, no. 3, pp. 179–199, Sep. 2013.

[28] M. Liu, Y. Zhang, and D. Lin, "Perfect algebraic immune functions," in *Advances in Cryptology—ASIACRYPT* (Lecture Notes in Computer Science), vol. 7658. Springer-Verlag, 2009, pp. 172–189.

[29] M. S. Lobanov, "Exact relations between nonlinearity and algebraic immunity," *J. Appl. Ind. Math.*, vol. 3, no. 3, pp. 367–376, 2009.

[30] W. Meier, E. Pasalic, and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 3027. Springer-Verlag, 2004, pp. 474–491.

[31] S. Mesnager, G. McGrew, J. Davis, D. Steele, and K. Marsten, "A comparison of Carlet's second-order nonlinearity bounds," *Int. J. Comput. Math.*, vol. 94, vol. 3, pp. 427–436, 2017.

[32] S. Mesnager and G. Cohen, "Cyclic codes and algebraic immunity of Boolean functions," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Apr./May 2015, pp. 1–5.

[33] E. Pasalic, "Almost fully optimized infinite classes of Boolean functions resistant to (fast) algebraic cryptanalysis," in *Proc. Int. Conf. Inf. Secur. Cryptol.*, in Lecture Notes in Computer Science, vol. 5461, Springer-Verlag, 2009, pp. 399–414.

[34] P. Rizomiliotis, "On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 4014–4024, Aug. 2010.

[35] O. Rothaus, "On bent functions," *J. Combin. Theory Ser. A*, vol. 20, no. 3, pp. 300–305, 1976.

[36] J. Schatz, "The second order Reed-Muller code of length 64 has covering radius 18 (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 27, no. 4, pp. 529–530, Jul. 1981.

[37] D. Tang, C. Carlet, and X. Tang, "Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 653–664, Jan. 2013.

[38] D. Tang, C. Carlet, X. Tang, and Z. Zhou, "Construction of highly nonlinear 1-resilient Boolean functions with optimal algebraic immunity and provably high fast algebraic immunity," *IEEE Trans. Inf. Theory*, vol. 63, no. 9, pp. 6113–6125, Sep. 2017.

[39] Z. Tu and Y. Deng, "A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity," *Des., Codes Cryptogr.*, vol. 60, no. 1, pp. 1–14, Jul. 2011.

[40] Q. Wang, C. Carlet, P. Stănică, and C. H. Tan, "Cryptographic properties of the hidden weighted bit function," *Discrete Appl. Math.*, vol. 174, pp. 1–10, Sep. 2014.

[41] Q. Wang and T. Johansson, "A note on fast algebraic attacks and higher order nonlinearities," in *Proc. Int. Conf. Inf. Secur. Cryptol.*, in Lecture Notes in Computer Science, vol. 6584. Springer-Verlag, 2011, pp. 84–98.

[42] Q. Wang, T. Johansson, and H. Kan, "Some results on fast algebraic attacks and higher-order non-linearities," *IET Inf. Secur.*, vol. 6, no. 1, pp. 41–46, Mar. 2012.

[43] Q. Wang and P. A. Stănică, "New bounds on the covering radius of the second order Reed-Muller code of length 128," *Cryptogr. Commun.*, vol. 11, no. 2, pp. 269–277, Mar. 2019.

[44] Q. Wang and P. A. Stănicsă, "A trigonometric sum sharp estimate and new bounds on the nonlinearity of some cryptographic Boolean functions," *Des., Codes Cryptogr.*, vol. 87, no. 8, pp. 1749–1763, Aug. 2019.

[45] Q. Wang, J. Peng, H. Kan, and X. Xue, "Constructions of cryptographically significant Boolean functions using primitive polynomials," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 3048–3053, Jun. 2010.

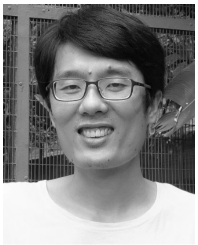
[46] Q. Wang, C. H. Tan, and T. F. Prabowo, "On the covering radius of the third order Reed–Muller code RM(3, 7)," *Des., Codes Cryptogr.*, vol. 86, no. 1, pp. 151–159, Jan. 2018.

[47] Q. Wang, C. H. Tan, and P. A. Stănic̦ "Concatenations of the hidden weighted bit function and their cryptographic properties," *Adv. Math. Commun.*, vol. 8, no. 2, pp. 153–165, 2014.

[48] Q. Wang and C. H. Tan, "Properties of a family of cryptographic Boolean functions," in *Proc. Int. Conf. Sequences Appl.*, in Lecture Notes in Computer Science, vol. 8865. Springer-Verlag, 2012, pp. 34–46.

[49] Q. Wang and C. H. Tan, "A new method to construct Boolean functions with good cryptographic properties" *Inf. Process. Lett.*, vol. 113, nos. 14–16, pp. 567–571, Jul./Aug. 2013.

[50] X. Zeng, C. Carlet, J. Shan, and L. Hu, "More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 6310–6320, Sep. 2011.



QICHUN WANG received the Ph.D. degree in computer science from Fudan University, Shanghai, China, in 2011. From February 2012 to August 2017, he was with the National University of Singapore as a Research Scientist. In 2017, he joined Nanjing Normal University, where he is currently a Full Professor. He is also with the Hunan University of Science and Engineering as an Adjunct Professor. His research interests include cryptography and coding theory.

CAIHONG NIE was born in 2000. She is currently pursuing the B.S. degree with the School of Mathematical Sciences, Nanjing Normal University.

YOULE XU received the B.S. degree in computer science from Hebei University, in 2017. He is currently pursuing the M.S. degree with the School of Computer Science and Technology, Nanjing Normal University.