IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 9, 2019, accepted October 8, 2019, date of publication October 14, 2019, date of current version October 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2947367

Constructing Two Classes of Boolean Functions With Good Cryptographic Properties

YINDONG CHEN[1,2,3], **LIU ZHANG**[1], **ZHANGQUAN GONG**[1], **AND WEIHONG CAI**[1,2,3]

[1]Department of Computer Science, Shantou University, Shantou 515063, China
[2]Guangdong Provincial Key Laboratory of Digital Signal and Image Processing Techniques, Shantou 515063, China
[3]Key Laboratory of Intelligent Manufacturing Technology, Ministry of Education, Shantou University, Shantou 515063, China

Corresponding author: Yindong Chen (ydchen@stu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61103244, Grant U1509213, Grant 61672303, Grant 61702318, and Grant 61902232, in part by the Science and Technology Planning Project of Guangdong Province under Grant 2016B010124012, Grant 2019B010116001, Grant 180917104960489, and Grant 190827105555406, in part by the Natural Science Foundation of Guangdong Province under Grant 2018A030313291, Grant 2018A030313438, and Grant 2018A030313889, in part by the Special Funds for Discipline and Specialty Construction of Guangdong Higher Education Institutions under Grant 2016KTSCX040, Grant 2016KQNCX056, Grant 2018KQNCX079, and Grant 2018GXJK048, in part by the STU Scientific Research Foundation for Talents under Grant NTF18006, Grant NTF18022, and Grant NTF18024, and in part by the National Training Program of Innovation and Entrepreneurship for Undergraduates under Grant 201910560015.

ABSTRACT Wu et al. proposed a generalized Tu-Deng conjecture over $\mathbb{F}_{2^{rm}} \times \mathbb{F}_{2^m}$, and constructed Boolean functions with good properties. However the proof of the generalized conjecture is still open. Based on Wu's work and assuming that the conjecture is true, we come up with a new class of balanced Boolean functions which has optimal algebraic degree, high nonlinearity and optimal algebraic immunity. The Boolean function also behaves well against fast algebraic attacks. Meanwhile we construct another class of Boolean functions by concatenation, which is 1-resilient and also has other good cryptographic properties.

INDEX TERMS Algebraic immunity, 1-resilient, nonlinearity, fast algebraic attacks, Tu-Deng conjecture, Boolean function.

I. INTRODUCTION

It is difficult to construct Boolean function satisfying all main criteria, including balancedness, optimal algebraic immunity (AI), high algebraic degree (deg), high nonlinearity, etc. At present, fast algebraic immunity (FAI) is usually computed by computer to evaluate the ability of Boolean functions to resist fast algebraic attack, but some work is to obtain accurate fast algebraic immunity or its lower bound by mathematical proof [1]–[4].

Researchers can construct Boolean functions with good properties or special properties, such as rotationally symmetric Boolean functions [5]–[9]. Liu summarized the recent work on Boolean functions constructed by decomposition methods based on additive or multiplicative groups over finite fields, which can effectively resist fast algebraic attacks in [10]. In 2009, Tu and Deng [11] presented a combinatorial conjecture (Tu-Deng conjecture) and constructed a class of balanced even-variable Boolean functions with optimal AI, optimal deg and very high nonlinearity. Subsequently, much work was done to prove the Tu-Deng conjecture [12]. However, this class of Boolean functions does not perform well against fast algebraic attack (FAA). The idea of Tu and Deng's construction enlightens many people. Tang et al. constructed a class of Boolean functions which satisfies all main criteria [13], and this class of functions is based on a new combinatorial conjecture, which was proved to be true in [14]. Based on a general conjecture similar to Tu-Deng conjecture mentioned in [15], Jin et al. proposed a construction of Boolean functions with optimal AI. Note that the additive group of a finite field used in constructing functions is $F_{2^k} \times F_{2^k}$. Therefore, in order to generalize the constructions in [11], [13], [15], a natural idea is to decompose finite field additive groups into different size additive groups. Wu et al. realized this idea in paper [16]. In the above constructions, parameters s defined as the power of the primitive elements in the support are added, and Boolean functions with the same good properties are added, but some functions are affine equivalent when s takes different values [17].

By decomposing the additive group of the finite field $F_{2^{(r+1)m}}$ into a direct sum of $F_{2^{rm}}$ and F_{2^m} where $r \geq 1$ is an odd integer and $m \geq 3$ is another integer, Wu et al.

The associate editor coordinating the review of this manuscript and approving it for publication was Junggab Son.

constructed two classes of $(r+1)m$-variable unbalanced Boolean functions in similar techniques as those in [11], [13], [15]. If the combination conjecture holds, these constructed functions can achieve optimal AI. In this paper, we present a class of balanced Boolean functions over $F_{2^{rm}} \times F_{2^m}$ which are proved to obtain optimal AI, optimal deg, high nonlinearity and good behavior against fast algebraci attack (FAA). Furthermore, we construct another class of Boolean functions with good cryptographic properties by concatenating with Wu's function proposed in [16].

The rest of the paper is organized as follows. In Section II, we recall some preliminaries required for the subsequent sections. In Section III, we propose a construction of balanced Boolean functions with optimal AI. In Section IV, a class of 1-resilient Boolean functions is presented. Section V concludes this paper.

II. PRELIMINARIES

An n-variable Boolean function is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Let $\mathbb{B}_n$ be the set of all n-variable Boolean functions. The support of Boolean function $f \in \mathbb{B}_n$ is defined as $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n | f(x) = 1\}$ and Hamming weight denoted by $\mathrm{wt}(f)$ is defined by the cardinality of the support. We say f is balanced if $\mathrm{wt}(f) = 2^{n-1}$. Let $\mathrm{wt}_p(i)$ the number of 1's in the binary expansion of i mod (2^p-1) where p represents the length of the binary extension and can take different values.

The Boolean function f over $\mathbb{F}_{2^n}$ can also be uniquely expressed by a univariate polynomial

$$f(x) = \sum_{i=0}^{2^n-1} \alpha_i x^i$$

where $\alpha_0, \alpha_{2^n-1} = 0 \in \mathbb{F}_2, \alpha_i \in \mathbb{F}_{2^n}$ for $1 \leq i < 2^n - 1$ such that $\alpha_i^2 = \alpha_{2i \pmod{2^n-1}}$. The algebraic degree $\deg(f)$ equals $\max\{wt(\bar{i})|\alpha_i \neq 0, 0 \leq i < 2^n)\}$, where $\bar{i}$ is the binary expansion of i. The algebraic degree of Affine functions is at most 1. The nonlinearity of f, expressed by $\mathcal{N}_f$, is the minium distance between f and all affine functions.

In fact, we can express Boolean functions more flexibly. We can decompose the additive group of F_{2^n} into $\mathbb{F}_{2^{n_1}} \times \mathbb{F}_{2^{n_2}}$ where $n = n_1 + n_2$ for two integers $n_1, n_2 \geq 1$, so every n-variable Boolean function is a mapping from $\mathbb{F}_{2^{n_1}} \times \mathbb{F}_{2^{n_2}}$ to $\mathbb{F}_2$. Thus f can be expressed as

$$f(x, y) = \sum_{i=0}^{2^{n_1}-1} \sum_{j=0}^{2^{n_2}-1} f_{i,j} x^i y^j, \quad f_{i,j} \in \mathbb{F}_{2^{[n_1,n_2]}}.$$

It can be easily deduced that

$$\deg(f) = \max\left\{ \mathrm{wt}_{n_1}(i) + \mathrm{wt}_{n_2}(j) \,\middle|\, f_{i,j} \neq 0 \right\}$$

where $0 \leq i \leq 2^{n_1}-1, 0 \leq j \leq 2^{n_2}-1$.

Let $x \cdot a$ be any inner product in $\mathbb{F}_2^n$, then the Walsh transform of $f \in \mathcal{B}_n$ is defined as

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

The nonlinearity of f can be expressed as

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |W_f(a)|.$$

Over $\mathbb{F}_{2^n}$, the Walsh transform can be defined as

$$W_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{tr}_1^n(ax)}$$

where $\mathrm{tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is a mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Furthermore, when $n = n_1 + n_2$ and f is a mapping from $\mathbb{F}_{2^{n_1}} \times \mathbb{F}_{2^{n_2}}$ to $\mathbb{F}_2$, then for $(a, b) \in \mathbb{F}_{2^{n_1}} \times \mathbb{F}_{2^{n_2}}$,

$$W_f(a, b) = \sum_{(x,y) \in \mathbb{F}_{2^{n_1}} \times \mathbb{F}_{2^{n_2}}} (-1)^{f(x)+\mathrm{tr}_1^{n_1}(ax)+\mathrm{tr}_1^{n_2}(by)}.$$

Definition 1 [18]: The algebraic immunity of a Boolean function $f \in \mathcal{B}_n$, expressed by $\mathrm{AI}(f)$*, is defined as*

$$\mathrm{AI}(f) = \min\left\{ \deg(g) \,|\, fg = 0 \text{ or } (f+1)g = 0,\ g \neq 0 \right\}.$$

The Boolean functions with $\mathrm{AI}(f) = \lceil n/2 \rceil$ are called optimal AI functions. To improve standard algebraic attacks, Courtois proposed the fast algebraic attacks(FAA) [19]. Liu proposed the concept of fast algebraic immunity to assess the ability to resist FAA.

Definition 2 [20]: The fast algebraic immunity of a Boolean function $f \in \mathcal{B}_n$, expressed by $\mathrm{FAI}(f)$*, is defined as*

$$\mathrm{FAI}(f) = \min\Big\{ 2\,\mathrm{AI}(f), \min\big\{ \deg(g) + \deg(fg) | 1 \leq \deg(g) < \mathrm{AI}(f) \big\}\Big\}.$$

III. BOOLEAN FUNCTION WITH VERY GOOD CRYPTOGRAPHIC PROPERTIES

Conjecture 1: [16] For any $0 \leq t \leq 2^m-2$, define

$$S_t = \left\{ (a, b) \,\middle|\, \begin{array}{l} 0 \leq a \leq 2^{rm}-2,\ 0 \leq b \leq 2^m-1, \\ ua + b \equiv t \pmod{2^m-1}, \\ \mathrm{wt}_{rm}(a) + \mathrm{wt}_m(b) \leq \frac{n}{2}-1, \end{array} \right\},$$

where u is an integer with $1 \leq u \leq 2^k-1$ and $\gcd(u, 2^m-1)=1$. Then $|S_t| \leq 2^{rm-1}$.

Let α be a primitive element of $\mathbb{F}_{2^{rm}}$ and $\beta = \alpha^{(2^{rm}-1)/(2^m-1)}$ as a primitive element of $\mathbb{F}_{2^m}$. For any integer $0 \leq s \leq 2^{rm}-2$, define

$$\Delta_s = \left\{ \alpha^i \,\middle|\, s \leq i \leq s + 2^{rm-1} - 1 \right\}.$$

Construction 1: Let $0 \leq s, l \leq 2^{rm}-2$ be integers. G is an n-variable Boolean function defined in $\mathbb{F}_{2^{rm}} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ by setting

$$\mathrm{supp}(G) = \left\{ (\gamma y^u, y) \,\middle|\, y \in \mathbb{F}_{2^m}^*, \gamma \in \Delta_s \backslash \{\alpha^s\} \right\} \bigcup \left\{ (0, y) \,\middle|\, y \in \mathbb{F}_{2^m}^* \right\} \bigcup \left\{ (x, 0) \,\middle|\, x \in \mathbb{F}_{2^{rm}} \backslash \Delta_l \right\}.$$

The bivariate representation of G over $\mathbb{F}_{2^{rm}} \times \mathbb{F}_{2^m}$ can be expressed as

$$G(x,y) = \begin{cases} g(\frac{x}{y^u}), & \text{if } x \cdot y \neq 0 \\ 1, & \text{if } x = 0,\ y \in \mathbb{F}_{2^m}^* \\ 1, & \text{if } x \in \mathbb{F}_{2^{rm}} \backslash \Delta_l,\ y = 0 \\ 0, & \text{otherwise} \end{cases}$$

where g is an (rm)-variable Boolean function and $\mathrm{supp}(g) = \Delta_s \setminus \{\alpha^s\}$, $0 \leq s \leq 2^{rm}-2$. For convenience, we denote tr_1^{rm} and tr_1^m by "Tr" and "tr" respectively, and denote $Q = 2^{rm}$, $q = 2^m$.

A. BALANCE

Theorem 1: The Boolean function G, defined in Construction 1, is balanced.

Proof: According to the definition of G, we can easily get

$$\begin{aligned} \mathrm{wt}(G) &= (2^{rm-1} - 1)(2^m - 1) + 2^m - 1 + 2^{rm-1} \\ &= 2^{(r+1)m-1} \\ &= 2^{n-1}. \end{aligned}$$

Thus the function G is balanced. ■

B. ALGEBRAIC IMMUNITY

Theorem 2: The Boolean function G, defined in Construction 1, has optimal AI when Conjecture 1 is true.

Proof: We need to prove that both G and $G+1$ don't have any nonzero annihilator whose degree is less than $n/2$ when Conjecture 1 is true.

Assume that h is an n-variable Boolean function with $\deg(G) < n/2$. Then h could be written over $\mathbb{F}_{2^{rm}} \times \mathbb{F}_{2^m}$ as

$$h(x,y) = \sum_{i=0}^{2^{rm}-1} \sum_{j=0}^{2^m-1} h_{i,j} x^i y^j,$$

where $h_{0,0}, h_{0,2^m-1}, h_{2^{rm}-1,0}, h_{2^{rm}-1,2^m-1} \in \mathbb{F}_2$, the other $h_{i,j} \in \mathbb{F}_{2^n}$. It is obvious that $h_{0,0} = 0$.

Because of $\deg(G) < n/2 \leq rm$, it deduces that $h_{i,j} = 0$ for any $\mathrm{wt}_{rm}(i) + \mathrm{wt}_m(j) \geq n/2$, which implies $h_{2^{rm}-a,j} = 0$ for any $0 \leq j \leq 2^m-1$. Therefore,

$$h(\gamma y^u, y) = \sum_{i=0}^{2^{rm}-2} \sum_{j=0}^{2^m-2} h_{i,j} x^i y^j + \sum_{i=0}^{2^{rm}-2} h_{i,2^m-1} x^i y^{2^m-1}.$$

Since $h(x,y) = 0$ for any $(x,y) \in \mathrm{supp}(G)$, we know that, for any $y \in \mathbb{F}_{2^m}^*$, $\gamma \in \Delta_s \backslash \{\alpha^s\}$, thus

$$\begin{aligned} h(\gamma y^u, y) &= \sum_{i=0}^{2^{rm}-2} \sum_{j=0}^{2^m-2} h_{i,j} \gamma^i y^{ui+j} + \sum_{i=0}^{2^{rm}-2} h_{i,2^m-1} \gamma^i y^{ui} \\ &= \sum_{k=0}^{2^m-2} y^k \Bigg(\sum_{i=0}^{2^{rm}-2} h_{i,k-ui(\mathrm{mod}\ 2^m-1)} \gamma^i \\ &\qquad + \sum_{j=0}^{\frac{2^{rm}-1}{2^m-1}-1} h_{\tilde{u}k+j,2^m-1} \gamma^{\tilde{u}k+j(2^m-1)} \Bigg) \\ &= \sum_{k=0}^{2^m-2} h_k(\gamma) y^k \\ &= 0 \end{aligned}$$

where $\tilde{u}$ is an integer and $u\tilde{u} \equiv 1 \pmod{2^m-1}$, $\tilde{u}k$ is also need to modulo (2^m-1). And

$$h_k(\gamma) = \sum_{i=0}^{2^{rm}-2} h_{i,k-ui(\mathrm{mod}\ 2^m-1)} \gamma^i + \sum_{j=0}^{\frac{2^{rm}-1}{2^m-1}-1} h_{\tilde{u}k+j,2^m-1} \gamma^{\tilde{u}k+j(2^m-1)}.$$

$h_k(\gamma)$ is a polynomial to γ and have the elements in $\Delta_s \setminus \{\alpha^s\}$ as zeros. So the vector of coefficients can be expressed as

$$\begin{aligned} h_k &= \big(h_{0,k}, h_{1,k-u}, \cdots, h_{\tilde{u}k,0}, \\ &\quad \cdots, h_{2^m-2,k+u}, \cdots, h_{2^m-1+\tilde{u}k,0}, \cdots, h_{2^{rm}-2,k+u}\big) \\ &\quad + \big(0, \cdots, 0, h_{\tilde{u}k,2^m-1}, 0, \cdots, 0, \\ &\quad h_{2^m-1+\tilde{u}k,2^m-1}, 0, \cdots, 0, h_{2^{rm}-2^m+\tilde{u}k,2^m-1}, 0, \cdots, 0\big) \\ &= h_k^{(1)} + h_k^{(2)}. \end{aligned}$$

By now, the vector h_k is a codeword of the BCH code whose designed distance $\delta = 2^{rm-1}$. If it is nonzero, because of the BCH bound, then $\mathrm{wt}(h_k) \geq 2^{rm-1}$.

On the other hand, Since $\{(0,y) \mid y \in \mathbb{F}_{2^m}\} \subseteq \mathrm{supp}(G)$, then we have $h(0,y) = \sum_{i=0}^{2^m-1} h_{0,i} y^i = 0$. Its vector of coefficients is $h' = (h_{0,0}, h_{0,1}, \cdots, h_{0,2^m-1}) = 0$ as well as $\mathrm{wt}_m(k) \leq m-1 \leq n/2-1$ for any $0 \leq k \leq 2^m-1$. With this, if Conjecture 1 is true, we have $\mathrm{wt}(h_k) \leq 2^{rm}-1$, a contradiction happens that $h_k = 0$. Thus for any $0 \leq i \leq s^{rm}-1$, there are $h_{i,0} = h_{i,2^m-1}$ if $i \equiv \tilde{u}k \pmod{2^m-1}$, otherwise $h_{i,k-ui} = 0$.

And we have equation

$$\bigcup_{k=0}^{2^m-1} \Big\{ 0 \leq i \leq 2^{rm}-1 \,\Big|\, i \equiv \tilde{u}k \pmod{2^m-1} \Big\} = \Big\{ i \,\Big|\, 0 \leq i \leq 2^{rm}-1 \Big\}.$$

Therefore, $h(x,y)$ can be written as

$$\begin{aligned} h(x,y) &= \sum_{i=0}^{2^m-2} \Big(h_{0,i} x^i + h_{i,2^m-1} x^i y^{2^m-1} \Big) \\ &= \Big(1 + y^{2^m-1}\Big) \sum_{i=0}^{2^m-2} h_{i,0} x^i. \end{aligned}$$

Because $\deg(h) < n/2$, $\mathrm{wt}_{rm}(i) + \mathrm{wt}_m(2^m-1) < n/2$, which means $\mathrm{wt}_{rm}(i) < n/2 - m$. Consider the case of $x \in \mathbb{F}_{2^{rm}} \backslash \Delta_l$, $y = 0$. We get $h(x,0) = \sum_{i=0}^{2^m-2} h_{0,i} x^i = 0$, whose vector of coefficients is $h'' = (h_{0,0}, \cdots, h_{2^{rm}-2,0})$.

So if $h'' \neq 0$, with BCH bound we have $\mathrm{wt}(h'') \geq 2^{rm-1}$. Because $\mathrm{wt}_{rm}(i) < n/2 - m$, we also have

$$\mathrm{wt}(h'') \leq \sum_{k=0}^{n/2-m-1} \binom{rm}{k} < \sum_{k=0}^{\lfloor (rm-1)/2 \rfloor} \binom{rm}{k} < 2^{rm-1}.$$

A contradiction happens, so $h'' = 0$.

With all above, $h(x, y) = 0$, which means there is no nonzero annihilators whose degree less than $n/2$ for G. As to $G+1$, we can deduce the same result with similar proof. ■

C. NONLINEARITY

Lemma 1 [16]: Let T be an integer. Then,

$$2T\left(\frac{\ln T}{\pi}+0.163\right) < \sum_{i=1}^{T-1} \frac{1}{\sin \frac{i\pi}{2T}} < 2T\left(\frac{\ln T}{\pi}+0.263\right)+\frac{3\pi}{8T}.$$

Lemma 2: Let $0 \leq s \leq Q-2$ be an integer and

$$\Lambda_s = \sum_{\gamma \in \Delta_s \setminus \{\alpha^s\}} \sum_{y \in \mathbb{F}_q^*} (-1)^{\mathrm{Tr}(\gamma y)}.$$

If $r = 1$, then $|\Lambda_s| = 2^{m-1} - 1$.
If $r > 1$, then

$$|\Lambda_s| \leq \left(\frac{(n-2m)\ln 2}{\pi}+0.263\right) 2^{(n-m)/2} + 2^{m-1} + \frac{1}{2}.$$

Proof: Let $\xi \in \mathbb{C}$ be a $(Q-1)$-th root of unity and $\zeta = \xi^N$ where $N = (Q-1)/(q-1)$. χ_1 express the primitive multiplication character of $\mathbb{F}_Q^*$ and define the Gauss sums over $\mathbb{F}_Q$ as

$$G_1(\chi_1^{\mu}) = \sum_{x \in \mathbb{F}_Q^*} \chi_1^{\mu}(x)(-1)^{\mathrm{Tr}(x)}.$$

For $\mu = 0$, as we know, $G_1(\chi_1^0) = -1$ and $|G_1(\chi_1^0)| = Q^{1/2}$. For any $1 \leq \mu \leq Q-2$. Through Fourier inversion for any $0 \leq i \leq Q-2$, we have

$$(-1)^{\mathrm{Tr}(\alpha^i)} = \frac{1}{Q-1} \sum_{\mu=0}^{Q-2} G_1(\chi_1^{\mu}) \xi^{-i\mu}.$$

Hence we have

$$\begin{aligned}
\Lambda_s &= \sum_{i=s+1}^{s+Q/2-1} \sum_{j=0}^{q-2} (-1)^{\mathrm{Tr}(\alpha^{i+Nj})} \\
&= \frac{1}{Q-1} \sum_{i=s+1}^{s+Q/2-1} \sum_{j=0}^{q-2} \sum_{\mu=0}^{Q-2} G_1(\chi_1^{\mu}) \xi^{-\mu(i+Nj)} \\
&= \frac{1}{Q-1} \sum_{\mu=0}^{Q-2} G_1(\chi_1^{\mu}) \sum_{i=s+1}^{s+Q/2-1} \xi^{-i\mu} \sum_{j=0}^{q-2} \zeta^{-j\mu}
\end{aligned}$$

Note that

$$\sum_{i=s+1}^{s+Q/2-1} \xi^{-i\mu} = \begin{cases} \frac{Q}{2} - 1, & \text{if } \mu = 0, \\ \xi^{-s\mu} \frac{1-\xi^{-\mu \frac{Q}{2}}}{1-\xi^{-\mu}} - \xi^{-s\mu}, & \text{otherwise.} \end{cases}$$

$$\sum_{j=0}^{q-2} \zeta^{-j\mu} = \begin{cases} q-1, & \text{if } \mu \equiv 0 \pmod{q-1}, \\ 0, & \text{otherwise.} \end{cases}$$

Then we have,

$$\begin{aligned}
\Lambda_s = &-\frac{(Q-2)(q-1)}{2(Q-1)} \\
&+ \frac{q-1}{Q-1} \sum_{\substack{\mu=0 \\ (q-1)|\mu}}^{Q-2} G_1(\chi_1^{\mu}) \left(\xi^{-s\mu} \frac{1-\xi^{-\mu\frac{Q}{2}}}{1-\xi^{-\mu}} - \xi^{-s\mu}\right).
\end{aligned}$$

If $r = 1$, it means $Q = q$, then

$$|\Lambda_s| = \left|-\frac{Q-2}{2}\right| = 2^{m-1} - 1.$$

If $r > 1$, then

$$\begin{aligned}
|\Lambda_s| &= \frac{(Q-2)(q-1)}{2(Q-1)} + \frac{(q-1)Q^{\frac{1}{2}}}{Q-1} \sum_{\substack{\mu=0 \\ (q-1)|\mu}}^{Q-2} \left|\frac{1-\xi^{-\mu\frac{Q}{2}}}{1-\xi^{-\mu}} - 1\right| \\
&= \frac{(Q-2)(q-1)}{2(Q-1)} + \frac{(q-1)Q^{\frac{1}{2}}}{Q-1} \sum_{\substack{\mu=0 \\ (q-1)|\mu}}^{Q-2} \left|\frac{1}{1+\xi^{-\frac{\mu}{2}}} - 1\right| \\
&= \frac{(Q-2)(q-1)}{2(Q-1)} + \frac{(q-1)Q^{\frac{1}{2}}}{Q-1} \sum_{\substack{\mu=0 \\ (q-1)|\mu}}^{Q-2} \left|\frac{1}{\xi^{\frac{\mu}{4}} + \xi^{-\frac{\mu}{4}}}\right| \\
&\leq \frac{q-1}{2} + \frac{(q-1)Q^{\frac{1}{2}}}{2(Q-1)} \sum_{k=1}^{N-1} \frac{1}{\sin \frac{k\pi}{2N}}.
\end{aligned}$$

With Lemma 1, we have

$$\begin{aligned}
|\Lambda_s| &\leq \frac{q-1}{2} + \frac{(q-1)Q^{\frac{1}{2}}}{2(Q-1)} \left(2N\left(\frac{\ln N}{\pi}+0.263\right)+\frac{3\pi}{8N}\right) \\
&< \frac{q-1}{2} + Q^{\frac{1}{2}}\left(\frac{\ln N}{\pi}+0.263\right) + \frac{3\pi(q-1)^2 Q^{\frac{1}{2}}}{8(Q-1)^2} \\
&< \left(\frac{(n-2m)\ln 2}{\pi}+0.263\right) 2^{(n-m)/2} + 2^{m-1} + \frac{1}{2}.
\end{aligned}$$

■

Lemma 3: Let $0 \leq s \leq Q-2$ be an integer and

$$\Gamma_s = \sum_{\gamma \in \Delta_s \setminus \{\alpha^s\}} \sum_{y \in \mathbb{F}_q^*} (-1)^{\mathrm{Tr}(\gamma y)+\mathrm{tr}(y^u)},$$

then

$$\begin{aligned}
|\Gamma_s| \leq &\left(\frac{(n-m)\ln 2}{\pi}+0.263\right) 2^{n/2} \\
&- \left(\frac{(n-2m)\ln 2}{\pi}+0.163\right) 2^{n/2-m} + \frac{3}{2}.
\end{aligned}$$

Proof: The definition of notations in this lemma is the same as that in Lemma 2. Let χ_2 be the primitive multiplication character of $\mathbb{F}_q^*$ and define the Gauss sums over $\mathbb{F}_q$ for any $0 \leq \nu \leq q-2$ as

$$G_2(\chi_2^{\nu}) = \sum_{x \in \mathbb{F}_q^*} \chi_2^{\nu}(x)(-1)^{\mathrm{tr}(x)}.$$

We also have $G_2(\chi_2^0) = -1$ and $|G_2(\chi_2)| = q^{1/2}$ for any $1 \leq \nu \leq q-2$. Through Fourier inversion for any $0 \leq i \leq q-2$ we have

$$(-1)^{\mathrm{tr}(\alpha^i)} = \frac{1}{q-1}\sum_{\nu=0}^{q-2} G_2(\chi_2^\nu)\zeta^{-i\nu}.$$

Hence, we have

$$\begin{aligned}\Gamma_s &= \sum_{i=s+1}^{s+Q/2-1}\sum_{j=0}^{q-2}(-1)^{\mathrm{Tr}(\alpha^i\beta^j)+\mathrm{tr}(\beta^{ju})}\\ &= \frac{1}{(Q-1)(q-1)}\sum_{\mu=0}^{Q-2}\sum_{\nu=0}^{q-2} G_1(\chi_1^\mu)G_2(\chi_2^\nu)\\ &\quad\times\sum_{i=s+1}^{s+Q/2-1}\xi^{-i\mu}\sum_{j=0}^{q-2}\zeta^{-j(\mu+u\nu)}.\end{aligned}$$

Note that

$$\sum_{j=0}^{q-2}\zeta^{-j(\mu+u\nu)} = \begin{cases} q-1, & \text{if } \mu+u\nu\equiv 0 \pmod{q-1};\\ 0, & \text{otherwise.}\end{cases}$$

Since $\mu+u\nu\equiv 0 \pmod{q-1}$ if and only if $\nu=0$ and $\mu = k(q-1)$ $(0\leq k\leq N-1)$, or $\nu\equiv q-1-\tilde{u}\mu \pmod{q-1}$ and $(q-1)\nmid\mu$, where $\tilde{u}u\equiv 1 \pmod{q-1}$. Thus we have

$$\begin{aligned}\Gamma_s &= \frac{1}{(Q-1)(q-1)}\\ &\quad\cdot\Bigg(\frac{(Q-2)(q-1)}{2}+(q-1)\sum_{\substack{\mu=1\\(q-1)\nmid\mu}}^{Q-2} G_1(\chi_1^\mu)\\ &\quad\times G_2(\chi_2^{q-1-\tilde{u}\mu})\Big(\xi^{-s\mu}\frac{1-\xi^{-\mu\frac{Q}{2}}}{1-\xi^{-\mu}}-\xi^{-s\mu}\Big)+(q-1)\\ &\quad\times\sum_{\substack{\mu=1\\(q-1)\mid\mu}}^{Q-2} G_1(\chi_1^\mu)(-1)\Big(\xi^{-s\mu}\frac{1-\xi^{-\mu\frac{Q}{2}}}{1-\xi^{-\mu}}-\xi^{-s\mu}\Big)\Bigg).\end{aligned}$$

Therefore,

$$\begin{aligned}|\Gamma_s| &\leq \frac{Q-2}{2(Q-1)}+\frac{Q^{\frac{1}{2}}q^{\frac{1}{2}}}{Q-1}\sum_{\substack{\mu=1\\(q-1)\nmid\mu}}^{Q-2}\left|\frac{1-\xi^{-\mu\frac{Q}{2}}}{1-\xi^{-\mu}}-1\right|\\ &\quad+\frac{Q^{\frac{1}{2}}}{Q-1}\sum_{\substack{\mu=1\\(q-1)\mid\mu}}^{Q-2}\left|\frac{1-\xi^{-\mu\frac{Q}{2}}}{1-\xi^{-\mu}}-1\right|\\ &< \frac{1}{2}+\frac{Q^{\frac{1}{2}}q^{\frac{1}{2}}}{Q-1}\sum_{\mu=1}^{Q-2}\left|\frac{1}{\xi^{\frac{\mu}{4}}+\xi^{-\frac{\mu}{4}}}\right|\\ &\quad-\frac{Q^{\frac{1}{2}}q^{\frac{1}{2}}-Q^{\frac{1}{2}}}{Q-1}\sum_{\substack{\mu=1\\(q-1)\mid\mu}}^{Q-2}\left|\frac{1}{\xi^{\frac{\mu}{4}}+\xi^{-\frac{\mu}{4}}}\right|.\end{aligned}$$

Hence,

$$|\Gamma_s| \leq \frac{1}{2}+\frac{Q^{\frac{1}{2}}q^{\frac{1}{2}}}{2(Q-1)}\sum_{\mu=1}^{Q-2}\frac{1}{\sin\frac{\mu\pi}{2(Q-1)}}-\frac{Q^{\frac{1}{2}}q^{\frac{1}{2}}-Q^{\frac{1}{2}}}{2(Q-1)}\sum_{k=1}^{N-1}\frac{1}{\sin\frac{k\pi}{2N}}.$$

By Lemma 1 we have, if $r=1$, i.e., $Q=q, N=1$, then

$$\begin{aligned}|\Gamma_s| &\leq \frac{1}{2}+\frac{q}{2(q-1)}\left(2(q-1)\Big(\frac{\ln(q-1)}{\pi}+0.263\Big)+\frac{3\pi}{8(q-1)}\right)\\ &< \frac{3}{2}+\left(\frac{m\ln 2}{\pi}+0.263\right)2^m.\end{aligned}$$

If $r>1$, then

$$\begin{aligned}&|\Gamma_s|\\ &\leq \frac{1}{2}+\frac{Q^{\frac{1}{2}}q^{\frac{1}{2}}}{2(Q-1)}\left(2(Q-1)\Big(\frac{\ln(Q-1)}{\pi}+0.263\Big)+\frac{3\pi}{8(Q-1)}\right)\\ &\quad-\frac{Q^{\frac{1}{2}}q^{\frac{1}{2}}-Q^{\frac{1}{2}}}{2Q-1)}2N\left(\frac{\ln N}{\pi}+0.163\right)\\ &< \frac{1}{2}+Q^{\frac{1}{2}}q^{\frac{1}{2}}\left(\frac{\ln Q}{\pi}+0.263\right)-\frac{Q^{\frac{1}{2}}}{q^{\frac{1}{2}}+1}\left(\frac{\ln N}{\pi}+0.163\right)\\ &\leq \frac{3}{2}+\left(\frac{(n-m)\ln 2}{\pi}+0.263\right)2^{\frac{n}{2}}\\ &\quad-\left(\frac{(n-2m)\ln 2}{\pi}+0.163\right)2^{\frac{n}{2}-m}.\end{aligned}$$

■

Lemma 4 [21]: Let h be the Carlet-Feng function in k variables, then for any $a\in\mathbb{F}_{2^k}^*$, there's

$$|W_h(a)| \leq \left(\frac{k\ln 2}{\pi}+0.485\right)2^{\frac{k}{2}+1}.$$

Theorem 3: Let G be the Boolean function defined in Construction 1. Then

$$\begin{aligned}\mathcal{N}_G \geq 2^{n-1} &- \left(\frac{(n-m)\ln 2}{\pi}+0.263\right)2^{\frac{n}{2}}\\ &-\left(\frac{(n-m)\ln 2}{\pi}+0.485\right)2^{\frac{n-m}{2}}\\ &+\left(\frac{(n-2m)\ln 2}{\pi}+0.163\right)2^{\frac{n}{2}-m}-\frac{1}{2}.\end{aligned}$$

Proof: We compute $W_G(a,b)$ for any $(a,b)\in\mathbb{F}_Q\times\mathbb{F}_q$. If $(a,b)=(0,0)$, then $W_G(0,0)=0$ since W_G is balanced. If $(a,b)\neq(0,0)$, we have

$$\begin{aligned}W_G(a,b) &= -2\sum_{(x,y)\in\mathrm{supp}(G)}(-1)^{\mathrm{Tr}(ax)+\mathrm{tr}(by)}\\ &= -2\sum_{\gamma\in\Delta_s\backslash\{\alpha^s\}}\sum_{y\in\mathbb{F}_q^*}(-1)^{\mathrm{Tr}(a\gamma y^u)+\mathrm{tr}(by)}\\ &\quad-2\sum_{y\in\mathbb{F}_q^*}(-1)^{\mathrm{tr}(by)}-2\sum_{x\in\mathbb{F}_Q\backslash\Delta_l}(-1)^{\mathrm{Tr}(ax)}.\end{aligned}$$

i). If $a=0, b\neq 0$, then

$$\begin{aligned}W_G(0,b) &= -2\sum_{\gamma\in\Delta_s\backslash\{\alpha^s\}}\sum_{y\in\mathbb{F}_q^*}(-1)^{\mathrm{tr}(by)}\\ &\quad-2\sum_{y\in\mathbb{F}_q^*}(-1)^{\mathrm{tr}(by)}-2\sum_{x\in\mathbb{F}_Q\backslash\Delta_l}1\\ &= -2\cdot(-1)\cdot(2^{rm-1}-1)-2\cdot(-1)-2\cdot 2^{rm-1}\\ &= 2^{rm}-2+2-2^{rm}\\ &= 0.\end{aligned}$$

ii). If $a \neq 0, b = 0$, then

$$\begin{aligned} W_G(a,0) &= -2 \sum_{\gamma\in\Delta_s\backslash\{\alpha^s\}} \sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{Tr}(a\gamma y^u)} \\ &\quad -2\sum_{y\in\mathbb{F}_q^*} 1 - 2 \sum_{x\in\mathbb{F}_Q\backslash\Delta_l} (-1)^{\mathrm{Tr}(ax)} \\ &= -2\cdot\Lambda_s - 2\cdot(2^m-1) + W_h(a). \end{aligned}$$

iii). If $ab \neq 0$, then

$$\begin{aligned} W_G(a,b) &= -2 \sum_{\gamma\in\Delta_s\backslash\{\alpha^s\}} \sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{Tr}(a\gamma y^u)+\mathrm{tr}(by)} \\ &\quad -2\sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{tr}(by)} - 2 \sum_{x\in\mathbb{F}_Q\backslash\Delta_l} (-1)^{\mathrm{Tr}(ax)} \\ &= -2\cdot\Gamma_s + 2 + W_h(a). \end{aligned}$$

So with Lemma 3 and Lemma 4, we have

$$\begin{aligned} &\max_{(a,b)\in\mathbb{F}_Q\times\mathbb{F}_q} |W_G(a,b)| \\ &= \max\left\{ \max_{a\in\mathbb{F}_Q} |W_G(a,0)|, \max_{(a,b)\in\mathbb{F}_Q^*\times\mathbb{F}_q^*} |W_G(a,b)| \right\} \\ &\leq \left(\frac{(n-m)\ln 2}{\pi} + 0.263\right) 2^{\frac{n}{2}+1} \\ &\quad + \left(\frac{(n-m)\ln 2}{\pi} + 0.485\right) 2^{\frac{n-m}{2}+1} \\ &\quad - \left(\frac{(n-2m)\ln 2}{\pi} + 0.163\right) 2^{\frac{n}{2}-m+1} + 1. \end{aligned}$$

Therefore,

$$\begin{aligned} \mathcal{N}_G &= 2^{n-1} - \frac{1}{2} \max_{(a,b)\in\mathbb{F}_Q\times\mathbb{F}_q} |W_G(a,b)| \\ &\geq 2^{n-1} - \left(\frac{(n-m)\ln 2}{\pi} + 0.263\right) 2^{\frac{n}{2}} \\ &\quad - \left(\frac{(n-m)\ln 2}{\pi} + 0.485\right) 2^{\frac{n-m}{2}} \\ &\quad + \left(\frac{(n-2m)\ln 2}{\pi} + 0.163\right) 2^{\frac{n}{2}-m} - \frac{1}{2}. \end{aligned}$$

■

D. ALGEBRAIC DEGREE

Theorem 4: Let G be the Boolean function defined in Construction 1, then $\deg(G) = n - 1$.

Proof: Let $f, h : \mathbb{F}_{2^{rm}} \times \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ be both n-variable Boolean functions with the following support.

$$\begin{cases} \mathrm{supp}(f) &= \left\{(\gamma y^u, y) \,\middle|\, y \in \mathbb{F}_{2^m}^*, \gamma \in \Delta_s\right\}, \\ \mathrm{supp}(h) &= \left\{(0,0)\right\} \bigcup \left\{(\alpha^s y^u, y) \,\middle|\, y \in \mathbb{F}_{2^m}^*\right\} \bigcup \\ & \quad \left\{(0,y) \,\middle|\, y \in \mathbb{F}_{2^m}^*\right\} \bigcup \left\{(x,0) \,\middle|\, x \in \mathbb{F}_{2^{rm}}^* \backslash \Delta_l\right\}. \end{cases}$$

It is obvious that $G = f + h$. And f is the function constructed by Jin et al. [15], of which $\deg(f) \leq n - 2$. So we just need to consider $\deg(h)$. From Lagrange's interpolation formula, we get

$$\begin{aligned} &h(x,y) \\ &= (x^{2^{rm}-1}+1)(y^{2^m-1}+1) \\ &\quad + \sum_{\substack{(\alpha^s b^u, b) \\ b\in\mathbb{F}_{2^m}^*}} \left((x+\alpha^s b^u)^{2^{rm}-1}+1\right)\left((y+b)^{2^m-1}+1\right) \\ &\quad + \sum_{\substack{(0,b) \\ b\in\mathbb{F}_{2^m}^*}} (x^{2^{rm}-1}+1)\left((y+b)^{2^m-1}+1\right) \\ &\quad + \sum_{\substack{(a,0) \\ a\in\mathbb{F}_{2^{rm}}^*\backslash\Delta_l}} \left((x+a)^{2^{rm}-1}+1\right)(y^{2^m-1}+1) \\ &= x^{2^{rm}-1}y^{2^m-1} + \sum_{b\in\mathbb{F}_{2^m}^*} x^{2^{rm}-1}(y+b)^{2^m-1} \\ &\quad + \sum_{b\in\mathbb{F}_{2^m}^*} \left((x+\alpha^s b^u)^{2^{rm}-1} + (y+b)^{2^m-1}(x+\alpha^s b^u)^{2^{rm}-1}\right) \\ &\quad + \sum_{a\in\mathbb{F}_{2^{rm}}^*\backslash\Delta_l} \left((x+a)^{2^{rm}-1} + y^{2^m-1}(x+a)^{2^{rm}-1}\right). \end{aligned}$$

Expanding these terms, we have

$$\begin{aligned} &h(x,y) \\ &\quad = x^{2^{rm}-1}y^{2^m-1} \\ &\qquad + \sum_{b\in\mathbb{F}_{2^m}^*} (x+\alpha^s b^u)^{2^{rm}-1} + \sum_{a\in\mathbb{F}_{2^{rm}}^*\backslash\Delta_l} (x+a)^{2^{rm}-1} \\ &\qquad + \sum_{b\in\mathbb{F}_{2^m}^*} \sum_{i=0}^{2^m-1} \sum_{j=0}^{2^{rm}-1} \binom{2^{rm}-1}{j}\binom{2^m-1}{i} \alpha^{sj} b^{uj+i} \\ &\qquad \times x^{2^{rm}-1-j} y^{2^m-1-i} \\ &\qquad + \sum_{b\in\mathbb{F}_{2^m}^*} x^{2^{rm}-1} \sum_{i=0}^{2^m-1} \binom{2^m-1}{i} b^i y^{2^m-1-i} \\ &\qquad + \sum_{a\in\mathbb{F}_{2^{rm}}^*\backslash\Delta_l} y^{2^m-1} \sum_{j=0}^{2^{rm}-1} \binom{2^{rm}-1}{j} a^j x^{2^{rm}-1-j}. \end{aligned}$$

Finally, we get

$$\begin{aligned} h(x,y) &= \sum_{b\in\mathbb{F}_{2^m}^*} (x+\alpha^s b^u)^{2^{rm}-1} + \sum_{a\in\mathbb{F}_{2^{rm}}^*\backslash\Delta_l} (x+a)^{2^{rm}-1} \\ &\quad + \sum_{b\in\mathbb{F}_{2^m}^*} \sum_{i=1}^{2^m-1} \sum_{j=1}^{2^{rm}-1} \binom{2^{rm}-1}{j}\binom{2^m-1}{i} \alpha^{sj} b^{uj+i} \\ &\quad \times x^{2^{rm}-1-j} y^{2^m-1-i} \\ &\quad + \sum_{b\in\mathbb{F}_{2^m}^*} y^{2^m-1} \sum_{j=1}^{2^{rm}-1} \binom{2^{rm}-1}{j} \alpha^{sj} b^{uj} x^{2^{rm}-1-j} \\ &\quad + \sum_{a\in\mathbb{F}_{2^{rm}}^*\backslash\Delta_l} y^{2^m-1} \sum_{j=1}^{2^{rm}-1} \binom{2^{rm}-1}{j} \alpha^j x^{2^{rm}-1-j}. \end{aligned}$$

By now, we can see when $j = 1$, the coefficent of $y^{2^m-1}x^{2^{rm}-1-j}$ is

$$\sum_{b\in\mathbb{F}_{2^m}^*}\binom{2^{rm}-1}{1}\alpha^s b^u+\sum_{a\in\mathbb{F}_{2^{rm}}^*\setminus\Delta_l}\binom{2^{rm}-1}{1}a,$$

which is nonzero obviously. So $\deg(h) = n-1$, which means $\deg(G) = n-1$. ■

E. IMMUNITY AGAINST FAST ALGEBRAIC IMMUNITY

G is the Boolean function defined in Construction 1. We fix $s = l = 0$, select some values of the parameters r, m, u, and use computer to get the value of the pair (e, d) with $e < n/2$ and $e + d < n$ in order to judge where there is a function h satisfying $\deg(h) < e$ and $\deg(hG) \le d$ exists. The result is

i). Let $n = 12$, $r = 3$, $m = 3$, there do not exist such pair with $e + d \le n-2$ for any possible u, meaning $\mathrm{FAI}(G) = n-1$.

ii). Let $n = 16$, $r = 3$, $m = 4$, there do not such pair with $e + d \le n-2$ for $u = 7, 11, 13, 14$, meaning $\mathrm{FAI}(G) = n-1$. When $u = 1, 2, 4, 8$, there do not exist such pair with $e+d \le n-3$, meaning $\mathrm{FAI}(G) = n-2$.

So that we can say the function G in Construction 1 has good resistance to FAA.

IV. CONSTRUCTING BOOLEAN FUNCTIONS BY CONCATENATION

A. CONSTRUCTION

Before, Wu et al. constructed a class of balanced Boolean functions as follows.

Construction 2 [16]: Define a class of Boolean Functions $F_u : \mathbb{F}_{2^{rm}} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$,

$$F(x,y)=\begin{cases} f(\frac{x}{y^u}), & x\cdot y\neq 0\\ w(x), & y=0\end{cases}$$

where f, w are both rm-variable Boolean functions with $\mathrm{supp}(f) = \Delta_s$, $\mathrm{supp}(w) = \Delta_l$, $0 \le s, l \le 2^{rm}-2$.

What we do next is to construct a new class Boolean functions by concatenating Boolean functions G and F, which are defined in Construction 1 and Construction 2, respectively.

Construction 3: Let u, v satisfy $\gcd(uv, 2^m-1) = 1$, *F_u, G_v be the Boolean functions mentioned above and F_u, G_v as n-variable function over $\mathbb{F}[x_1, x_2, \ldots, x_n]$. Then the Boolean function by concatenating F_u and G_v is*

$$H_{u,v}(x_1, x_2, \ldots, x_{n+1}) = (1+x_{n+1})F_u + x_{n+1}G_v.$$

B. PROPERTIES

Theorem 5: Let $H_{u,v}$ be the $(n+1)$-variable Boolean functions in Construction 3. Then $H_{u,v}$ is balanced.

Proof: Obviously, $H_{u,v} = F_u$ if $x_{n+1} = 0$, otherwise $H_{u,v} = G_v$. Therefore, we have

$$|\,\mathrm{wt}(H_{u,v})| = |\,\mathrm{wt}(F_u)| + |\,\mathrm{wt}(G_v)| = 2^{n-1} + 2^{n-1} = 2^n.$$

So, $H_{u,v}$ is balanced. ■

Theorem 6: Let $H_{u,v}$ be the $(n+1)$-variable Boolean functions in Construction 3. Then we have

$$\deg(H_{u,v}) \ge \deg(F_u) \ge n-1.$$

Lemma 5 [22]: Given that f, g are n-variable Boolean functions, which $\mathrm{AI}(f) = d_1$, $\mathrm{AI}(g) = d_2$. *Let h be the Boolean function by concatenation of f, g. Then* $\mathrm{AI}(h) = \min\{d_1, d_2\} + 1$ *if $d_1 \neq d_2$ or* $d_1 \le \mathrm{AI}(h) \le d_1 + 1$.

With Lemma 5, we can deduce a theorem as follows.

Theorem 7: Let $H_{u,v}$ be the $(n+1)$-variable Boolean function in Construction 3. Assume that Conjecture 1 is true, then $n/2 \le \mathrm{AI}(H_{u,v}) \le n/2 + 1$.

Theorem 8: Let $H_{u,v}$ be the $(n+1)$-variable Boolean function in Construction 3. Then the nonlinearity of $H_{u,v}$ is

$$\begin{aligned}\mathcal{N}_{H_{u,v}} \ge 2^n &- \left(\frac{(n-m)\ln 2}{\pi}+0.263\right)2^{\frac{n}{2}+1}\\ &-\left(\frac{(n-m)\ln 2}{\pi}+0.485\right)2^{\frac{n-m}{2}+1}\\ &+\left(\frac{(n-2m)\ln 2}{\pi}+0.163\right)2^{\frac{n}{2}-m+1}-\frac{5}{2}.\end{aligned}$$

Proof: From last section, we have

$$\begin{aligned}\mathcal{N}_{G_v} \ge 2^{n-1} &- \left(\frac{(n-m)\ln 2}{\pi}+0.263\right)2^{\frac{n}{2}}\\ &-\left(\frac{(n-m)\ln 2}{\pi}+0.485\right)2^{\frac{n-m}{2}}\\ &+\left(\frac{(n-2m)\ln 2}{\pi}+0.163\right)2^{\frac{n}{2}-m}-\frac{1}{2}.\end{aligned}$$

On the other hand, Wu et al. [16] showed us that

$$\begin{aligned}\mathcal{N}_{F_u} \ge 2^{n-1} &- \left(\frac{(n-m)\ln 2}{\pi}+0.263\right)2^{\frac{n}{2}}\\ &-\left(\frac{(n-m)\ln 2}{\pi}+0.485\right)2^{\frac{n-m}{2}}\\ &+\left(\frac{(n-2m)\ln 2}{\pi}+0.163\right)2^{\frac{n}{2}-m}-2.\end{aligned}$$

According to the fact $\mathcal{N}_{H_{u,v}} \ge \mathcal{N}_{F_u} + \mathcal{N}_{G_v}$ we have

$$\begin{aligned}\mathcal{N}_{H_{u,v}} \ge 2^n &- \left(\frac{(n-m)\ln 2}{\pi}+0.263\right)2^{\frac{n}{2}+1}\\ &-\left(\frac{(n-m)\ln 2}{\pi}+0.485\right)2^{\frac{n-m}{2}+1}\\ &+\left(\frac{(n-2m)\ln 2}{\pi}+0.163\right)2^{\frac{n}{2}-m+1}-\frac{5}{2}.\end{aligned}$$

■

At the end, we test the immunity against FAA of $H_{u,v}$. We fix $s = l = 0$, select the values of the parameters r, m, u, v with $\gcd(uv, 2^m-1) = 1$, and use computer to get the value of the pair (e, d) with $e < n/2$ and $e + d < n$ in order to judge whether there is a function h satisfying $\deg(h) < e$ and $\deg(hF) \le d$ exists. Results are as follows:

i). Let $n + 1 = 13$, $r = 3$, $m = 3$, there do not exist such pair with $e+d \le n-3$ for any possible (u, v), meaning $\mathrm{FAI}(H) = n-2$.

ii). Let $n+1 = 17$, $r = 3$, $m = 4$, we test some pair (u, v), for instance, when $(u, v) = (1, 2)$ or $(1, 2)$, there do not exist such pair with $e + d \leq n - 3$, meaning $\mathrm{FAI}(H) = n - 2$. And when $(u, v) = (1, 7)$ or $(2, 7)$, there do not eixst such pair with $e+d \leq n-2$, meaning $\mathrm{FAI}(H) = n - 1$.

So that we can say the function $H_{u,v}$ in Construction 3 has good resistance to FAA.

C. DISCUSSION ON 1-RESILIENT

$H_{u,v}$ is the $(n+1)$-variable Boolean function defined in Construction 3. Then its Walsh transform is

$$W_{H_{u,v}}(a, b, c) = W_{F_u}(a, b) + (-1)^c W_{G_v}(a, b),$$

where $a \in \mathbb{F}_{2^{rm}},\ b \in \mathbb{F}_{2^m},\ c \in \mathbb{F}_2$. So we have some results.

i). If $a = 0,\ b = 0,\ c = 0$, since $H_{u,v}$ is balanced, then

$$W_{H_{u,v}}(0, 0, 0) = 0.$$

ii). If $a = 0,\ b = 0,\ c = 1$, then

$$W_{H_{u,v}}(0, 0, 1) = W_{F_u}(0, 0) - W_{G_v}(0, 0) = 0.$$

iii). If $a = 0,\ b \neq 0,\ c = 0$, then

$$\begin{aligned}
&W_{H_{u,v}}(0, b, 0)\\
&= W_{F_u}(0, b) + W_{G_v}(0, b)\\
&= -2 \sum_{\gamma\in\Delta_s\setminus\{\alpha^s\}} \sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{tr}(by)} - 2\sum_{x\in\Delta_l} 1\\
&\quad - 2 \sum_{\gamma\in\Delta_s\setminus\{\alpha^s\}} \sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{tr}(by)} - 2\sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{tr}(by)}\\
&\quad - 2 \sum_{x\in\mathbb{F}_Q\setminus\Delta_l} 1\\
&= 2^{rm} - 2^{rm}\\
&\quad + \big(-2\cdot(-1)\cdot(2^{rm-1}-1) - 2\cdot(-1) - 2\cdot 2^{rm-1}\big)\\
&= 0.
\end{aligned}$$

iv). If $a \neq 0, b = 0, c = 0$, then

$$\begin{aligned}
&W_{H_{u,v}}(a, 0, 0)\\
&= W_{F_u}(a, 0) + W_{G_v}(a, 0)\\
&= -2 \sum_{\gamma\in\Delta_s} \sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{Tr}(a\gamma y^u)} - 2\sum_{x\in\Delta_l} (-1)^{\mathrm{Tr}(ax)}\\
&\quad - 2 \sum_{\gamma\in\Delta_s\setminus\{\alpha^s\}} \sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{Tr}(a\gamma y^u)}\\
&\quad - 2\sum_{y\in\mathbb{F}_q^*} 1 - 2 \sum_{x\in\mathbb{F}_Q\setminus\Delta_l} (-1)^{\mathrm{Tr}(ax)}\\
&= -2 \sum_{\gamma\in\Delta_s} \sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{Tr}(a\gamma y^u)} - 2 \sum_{\gamma\in\Delta_s\setminus\{\alpha^s\}} \sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{Tr}(a\gamma y^u)}\\
&\quad - 2\cdot(2^m - 1).
\end{aligned}$$

If $r = 1$ (i.e. $\mathrm{Tr} = \mathrm{tr}$), then

$$\begin{aligned}
&W_{H_{u,v}}(a, 0, 0)\\
&= -2 \sum_{\gamma\in\Delta_s} \sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{Tr}(a\gamma y^u)}\\
&\quad - 2 \sum_{\gamma\in\Delta_s\setminus\{\alpha^s\}} \sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{Tr}(a\gamma y^u)} - 2\cdot(2^m - 1)\\
&= -2\cdot 2^{m-1}\cdot(-1) - 2\cdot(2^{m-1}-1)\cdot(-1) - 2\cdot(2^m-1)\\
&= 0.
\end{aligned}$$

Therefore, from the discussion above we have the following theorem.

Theorem 9: Let $H_{u,v}$ be the $(n+1)$-variable Boolean function in Construction 3. Then $H_{u,v}$ is 1-resilient if $r = 1$.

V. CONCLUSION

In this paper, we present a class balanced Boolean functions which has optimal AI, high nonlinearity and optimal algebraic degree. This Boolean function also behaves well against FAA. Then we constructed a class of 1-resilient Boolean functions with good cryptographic properties by concatenate our function to Wu's function. Finally we should indicate that the ability of these two constructions against FAA still need further research.

REFERENCES

[1] D. Tang, R. Luo, and X. Du, "The exact fast algebraic immunity of two subclasses of the majority function," *IEICE Trans. Fundam.*, vol. E99-A, no. 11, pp. 2084–2088, Nov. 2016.

[2] 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.

[3] Y. Chen, L. Zhang, F. Guo, and W. Cai, "Fast algebraic immunity of $2^m + 2$ & $2^m + 3$ variables majority function," *IEEE Access*, vol. 7, pp. 80733–80736, 2019.

[4] Y. Chen, L. Zhang, J. Xu, and W. Cai, "A lower bound of fast algebraic immunity of a class of 1-resilient Boolean functions," *IEEE Access*, vol. 7, pp. 90145–90151, 2019.

[5] Y. Chen and P. Lu, "Two classes of symmetric Boolean functions with optimum algebraic immunity: Construction and analysis," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2522–2538, Apr. 2011.

[6] Y. Chen, F. Guo, H. Xiang, W. Cai, and X. He, "Balanced odd-variable RSBFs with optimum AI, high nonlinearity and good behavior against FAAs," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E102-A, no. 6, pp. 818–824, 2019.

[7] Y. Chen, F. Guo, and J. Ruan, "Constructing odd-variable RSBFs with optimal algebraic immunity, good nonlinearity and good behavior against fast algebraic attacks," *Discrete Appl. Math.*, vol. 262, pp. 1–12, Jun. 2019.

[8] Y. Chen, L. Lin, L. Liao, J. Ruan, F. Guo, and W. Cai, "Constructing higher nonlinear odd-variable RSBFs with optimal AI and almost optimal FAI," *IEEE Access*, vol. 7, pp. 133335–133341, 2019.

[9] Y. Chen, L. Liao, F. Guo, and W. Cai, "Constructing odd-variable rotation symmetric Boolean functions with optimal AI and higher nonlinearity," *IEEE Access*, vol. 7, pp. 143866–143875, 2019.

[10] Z. Liu and B. Wu, "Recent results on constructing Boolean functions with (potentially) optimal algebraic immunity based on decompositions of finite fields," *J. Syst. Sci. Complex.*, vol. 32, no. 1, pp. 356–374, 2019.

[11] 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.

[12] Y. Chen, F. Guo, Z. Gong, and W. Cai, "One note about the Tu-Deng conjecture in case w(t)=5," *IEEE Access*, vol. 7, pp. 13799–13802, 2019.

[13] 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.

[14] G. Cohen and J.-P. Flori, "On a generalized combinatorial conjecture involving addition mod $2^k - 1$," Cryptol. ePrint Arch., Tech. Rep. 2011/400, 2011. [Online]. Available: http://eprint.iacr.org/

[15] Q. Jin, Z. Liu, B. Wu, and X. Zhang, "A combinatorial condition and Boolean functions with optimal algebraic immunity," *J. Syst. Sci. Complex.*, vol. 28, no. 3, 725-742, 2015.

[16] B. Wu, Q. Jin, Z. Liu, and D. Lin, "Constructing Boolean functions with potentially optimal algebraic immunity based on additive decompositions of finite fields," in *Proc. IEEE Int. Symp. Inf. Theory*, Honolulu, HI, USA, Jun./Jul. 2014, pp. 1361–1365.

[17] Y. Chen, L. Zhang, D. Tang, and W. Cai, "Translation equivalence of Boolean functions expressed by primitive element," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E102-A, no. 4, pp. 672–675, Apr. 2019.

[18] W. Meier, E. Pasalic, and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2004, pp. 474–491.

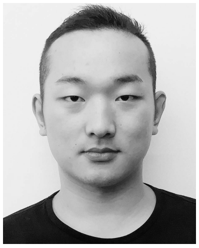
[19] N. T. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 2729. Berlin, Germany: Springer, 2003, pp. 176–194.

[20] M. Liu, D. Lin, and D. Pei, "Fast algebraic attacks and decomposition of symmetric Boolean functions," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4817–4821, Jul. 2011.

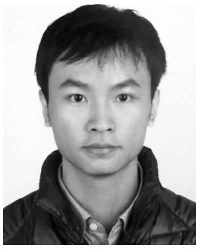
[21] M. Liu, Y. Zhang, and D. Lin, "Perfect algebraic immune functions," in *Proc. 18th Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer-Verlag, 2012, pp. 172–189.

[22] 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.

YINDONG CHEN was born in Jieyang, Guangdong, China, in 1983. He received the B.S. degree in mathematics from the South China University of Technology, in 2005, and the Ph.D. degree in computer science from Fudan University, in 2010. He is currently an Associate Professor with Shantou University, China. His research interests include cryptology and information security.



LIU ZHANG was born in Xinyang, Henan, China, in 1995. He received the B.S. degree in computer science from Xinyang Normal University, in 2017. He is currently pursuing the master's degree with Shantou University, China. His research interests include cryptology and information security.



ZHANGQUAN GONG was born in Nanning, Guangxi, China, in 1991. He received the M.S. degree in computer science from Shantou University, in 2017. His research interests include cryptology and information security.

WEIHONG CAI was born in Chaozhou, Guangdong, China, in 1963. He received the Ph.D. degree in computer science from the South China University of Technology, in 2012. He is currently a Professor with Shantou University, China. His research interests include network and communications, and information security.