Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-018-0574-2

A trigonometric sum sharp estimate and new bounds on the nonlinearity of some cryptographic Boolean functions

Qichun Wang[1] · **Pantelimon Stănică**[2]

Received: 28 February 2018 / Revised: 5 August 2018 / Accepted: 11 October 2018

Abstract
In this paper, we give a sharp estimate of a trigonometric sum which has several applications in cryptography and sequence theory. Using this estimate, we deduce new lower bounds on the nonlinearity of Carlet–Feng function, which has very good cryptographic properties with its nonlinearity bound being improved in numerous papers, as well as the function proposed by Tang–Carlet–Tang.

Keywords Carlet–Feng function · Tang–Carlet–Tang function · Trigonometric sum · Nonlinearity

Mathematics Subject Classification 11T71 · 11L03

1 Introduction

To resist the main known attacks, Boolean functions used in stream ciphers should be balanced, have high algebraic degree, high algebraic immunity, high nonlinearity and good immunity to fast algebraic attacks. It is known that constructing Boolean functions satisfying all these criteria is not an easy task.

Many classes of Boolean functions with optimum algebraic immunity had been introduced [2,9,12,13,24,25,30,32]. However, the nonlinearity of these functions is not good, and we do not know whether they can behave well against fast algebraic attacks. In 2008, Carlet and Feng [6] studied a class of functions which had been introduced by [14], and they found that these functions seem to satisfy all of the mentioned cryptographic criteria [6].

Communicated by C. Carlet.

✉ Qichun Wang
qcwang@fudan.edu.cn

Pantelimon Stănică
pstanica@nps.edu

1 School of Computer Science and Technology, Nanjing Normal University, Nanjing 210046, People's Republic of China

2 Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943-5216, USA

This is a breakthrough in the field of cryptographic Boolean functions. Based on the Carlet–Feng construction, some researchers proposed several classes of cryptographically significant Boolean functions [33,34,36,37,41,43].

To resist fast correlation attacks and linear approximation attacks [16,28], Boolean functions used in stream ciphers should have high nonlinearity. The maximum nonlinearity of n-variable Boolean functions is the same as the covering radius of the first order Reed–Muller code $RM(1,n)$, which is bounded above by $2^{n-1}-2^{n/2-1}$, and a function is bent if it achieves this bound [8,15]. For n odd, the nonlinearity is upper bounded by $2\lfloor 2^{n-2}-2^{n/2-2}\rfloor$ [21]. For odd $n \le 7$, it is known that the maximum nonlinearity is equal to the bent concatenation bound $2^{n-1}-2^{(n-1)/2}$ [1,18,29]. However, for odd $n > 7$, the covering radius of $RM(1,n)$ is still unknown [19,20,22,23,31]. For the maximum possible higher-order nonlinearities, we refer to [3,7,10,38,42].

From the cryptographic point of view, Boolean functions need to be balanced. It is still an open problem whether the maximum possible nonlinearity of 8-variable balanced functions is 118. We refer to [35] for more results on the nonlinearity of balanced functions. If we want Boolean functions to be cryptographically significant, e.g, balanced, with optimum algebraic immunity and good immunity to fast algebraic attacks, the problem of finding the maximum possible nonlinearity is still far away to be solved.

Using a Gauss sum, Carlet and Feng deduced a lower bound on the nonlinearity of the Carlet–Feng function by estimating the sum

$$S_n = \sum_{k=1}^{2^n-2} \left| \frac{\sin \frac{\pi k(2^{n-1}-1)}{2^n-1}}{\sin \frac{\pi k}{2^n-1}} \right| .$$

Using the same method, several improved bounds have been deduced in [5,17,36,39,41,43] by estimating the same sum S_n.

In 2013, Tang et al. [36] proposed two classes of Boolean functions with good cryptographic properties. They deduced a lower bound on the nonlinearity which is larger than all previously introduced bounds for similar functions. The key method in finding that bound relied yet again on an estimate of the above sum S_n.

It is of interest to give a sharp estimate of S_n and thus the best possible nonlinearity bound derived through this trigonometric sum. However, if we want to improve the bound further, then one must use a different method than the one based upon a trigonometric sum.

Moreover, the trigonometric sum S_n has applications in sequence theory, as well. For example, it can be used to investigate the imbalance properties of LFSR subsequences [40].

In this paper, we give a very precise estimate of S_n and prove that

$$\frac{0.36}{\pi(2^n-1)} < S_n - \left(\frac{2^n-1}{\pi} \left(n \ln 2 + \gamma + \ln \frac{8}{\pi} \right) - \frac{1}{\pi} - \frac{1}{2} \right) < \frac{0.72}{\pi(2^n-1)}.$$

Using these inequalities, we deduce new lower bounds on the nonlinearity of the Carlet–Feng function and the function proposed by [36].

2 Preliminaries

Let $\mathbb{F}_{2^n}$ the finite field of dimension n over the binary field $\mathbb{F}_2$. We denote by $\mathcal{B}_n$ the set of all n-variable Boolean functions from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$. Any Boolean function $f \in \mathcal{B}_n$ (with the usual identification of the finite field $\mathbb{F}_{2^n}$ with the vector space $\mathbb{F}_2^n$) can be uniquely represented as a multivariate polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]$,

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

which is called the *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. Let $1_f = \{x \in \mathbb{F}_{2^n} | f(x) = 1\}$ be the support of a Boolean function f, whose cardinality $|1_f|$ is called the *Hamming weight* of f. The *Hamming distance* between two functions f and g, denoted by $d(f, g)$, is the Hamming weight of $f + g$. Let $f \in \mathcal{B}_n$. The *nonlinearity* [4,11] of f is

$$nl(f) = \min_{\deg(g) \leq 1} d(f, g).$$

The *Walsh-Hadamard transform* of a given function $f \in \mathcal{B}_n$ is the integer-valued function over $\mathbb{F}_{2^n}$ 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 $tr(x)$ denotes the absolute trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. The nonlinearity of f can then be determined by

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

3 New bounds on the nonlinearity of some cryptographically significant Boolean functions

Nonlinearity is a quite important cryptographic criterion of Boolean functions in designing stream ciphers and block ciphers, which is desired to be as high as possible. It is still far away to be solved that what is the maximum possible nonlinearity of cryptographically significant Boolean functions. In the following, we will deduce new lower bounds on the nonlinearity of cryptographically significant Boolean functions.

3.1 New bound on the nonlinearity of the Carlet–Feng function

The Carlet–Feng function $CF \in \mathcal{B}_n$ is defined as the function with support

$$1_{CF} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^{n-1}-2}\},$$

where $\alpha \in \mathbb{F}_{2^n}$ is a primitive element. It is known that the Carlet–Feng function has quite good cryptographic properties: balancedness, high algebraic degree, high algebraic immunity, high nonlinearity and good immunity to fast algebraic attacks [6,27].

Using a Gauss sum, Carlet and Feng [6] proved that

$$nl(CF) > 2^{n-1} - \frac{1}{2^n - 1} \left(\sum_{k=1}^{2^n-2} 2^{\frac{n}{2}} \left| \frac{\sin \frac{\pi k(2^{n-1}-1)}{2^n-1}}{\sin \frac{\pi k}{2^n-1}} \right| + 2^{n-1} \right). \tag{1}$$

By estimating the sum

$$S_n = \sum_{k=1}^{2^n-2} \left| \frac{\sin \frac{\pi k(2^{n-1}-1)}{2^n-1}}{\sin \frac{\pi k}{2^n-1}} \right|,$$

they deduced a lower bound on $nl(CF)$. After that, many improved bounds have been found by estimating the same sum [17,36,41,43].

In this section, we will give a very precise estimate of this sum S_n. Our estimate relies on Lemmas 3.1 and 3.2, whose proofs are included in the Appendix.

Lemma 3.1 *Let $N \geq 255$ and $N \equiv -1 \pmod 4$. Then*

$$\frac{0.53}{\pi N} < \sum_{k=1}^{\frac{N+1}{4}} \frac{1}{\sin \frac{\pi(2k-1)}{2N}} - \left(\frac{N}{\pi} \left(\ln(N+1) + \gamma + \ln \frac{8(\sqrt{2}-1)}{\pi} \right) + \frac{\sqrt{2}}{4} - \frac{1}{\pi} \right) < \frac{0.72}{\pi N}.$$

Lemma 3.2 *Let $N \geq 255$ and $N \equiv -1 \pmod 4$. Then*

$$-\frac{0.17}{\pi N} < \sum_{k=1}^{\frac{N+1}{4}-1} \frac{1}{\cos \frac{\pi k}{N}} - \left(\frac{N}{\pi} \ln\left(\sqrt{2}+1\right) - \frac{1}{2} - \frac{\sqrt{2}}{4} \right) < 0.$$

By Lemmas 3.1 and 3.2, we can then prove the following theorem.

Theorem 3.3 *For $n \geq 8$, we have*

$$\frac{0.36}{\pi(2^n-1)} < \sum_{k=1}^{2^n-2} \left| \frac{\sin \frac{\pi k(2^{n-1}-1)}{2^n-1}}{\sin \frac{\pi k}{2^n-1}} \right| - \left(\frac{2^n-1}{\pi} \left(n \ln 2 + \gamma + \ln \frac{8}{\pi} \right) - \frac{1}{\pi} - \frac{1}{2} \right) < \frac{0.72}{\pi(2^n-1)}.$$

Proof Clearly,

$$\begin{aligned} \sum_{k=1}^{2^n-2} \left| \frac{\sin \frac{\pi k(2^{n-1}-1)}{2^n-1}}{\sin \frac{\pi k}{2^n-1}} \right| &= 2 \sum_{k=1}^{2^{n-1}-1} \left| \frac{\sin \frac{\pi k(2^{n-1}-1)}{2^n-1}}{\sin \frac{\pi k}{2^n-1}} \right| \\ &= 2 \sum_{t=1}^{2^{n-2}} \left| \frac{\sin \frac{\pi(2^{n-1}-t)}{2^n-1}}{\sin \frac{\pi(2t-1)}{2^n-1}} \right| + 2 \sum_{t=1}^{2^{n-2}-1} \frac{\sin \frac{\pi t}{2^n-1}}{\sin \frac{2\pi t}{2^n-1}} \\ &= \sum_{t=1}^{2^{n-2}} \frac{1}{\sin \frac{\pi(2t-1)}{2(2^n-1)}} + \sum_{t=1}^{2^{n-2}-1} \frac{1}{\cos \frac{\pi t}{2^n-1}}. \end{aligned}$$

By the right inequalities of Lemmas 3.1 and 3.2, we have

$$\sum_{t=1}^{2^{n-2}} \frac{1}{\sin \frac{\pi(2t-1)}{2(2^n-1)}} < \frac{2^n-1}{\pi} \left(\ln(2^n) + \gamma + \ln \frac{8(\sqrt{2}-1)}{\pi} \right) + \frac{1}{4} \left(\sqrt{2} - \frac{4}{\pi} \right) + \frac{0.72}{\pi(2^n-1)},$$

and

$$\sum_{t=1}^{2^{n-2}-1} \frac{1}{\cos \frac{\pi t}{2^n-1}} < \frac{2^n-1}{\pi} \ln(\sqrt{2}+1) - \frac{1}{2} - \frac{\sqrt{2}}{4}.$$

Table 1 Comparison of the bounds on $nl(CF)$

n	Bound in [6]	Bound in [17]	Bound in [36]	Our bound	Exact value
8	70	79	86	92	112
10	366	396	416	426	484
12	1700	1780	1830	1848	1970
14	7382	7584	7700	7735	8036
16	30922	31409	31673	31741	32530
18	126927	128068	128658	128792	130442
20	515094	517704	519010	519277	523154
22	2076956	2082834	2085694	2086225	2094972
24	8344600	8357672	8363886	8364947	8384536
26	33459185	33487957	33501375	33503496	33545716

Therefore,

$$\sum_{k=1}^{2^n-2} \left| \frac{\sin \frac{\pi k(2^{n-1}-1)}{2^n-1}}{\sin \frac{\pi k}{2^n-1}} \right| < \frac{2^n-1}{\pi}\left(n\ln 2+\gamma+\ln\frac{8}{\pi}\right)-\frac{1}{\pi}-\frac{1}{2}+\frac{0.72}{\pi(2^n-1)}.$$

Similarly, by the left inequalities of Lemmas 3.1 and 3.2, we have

$$\sum_{k=1}^{2^n-2} \left| \frac{\sin \frac{\pi k(2^{n-1}-1)}{2^n-1}}{\sin \frac{\pi k}{2^n-1}} \right| > \frac{2^n-1}{\pi}\left(n\ln 2+\gamma+\ln\frac{8}{\pi}\right)-\frac{1}{\pi}-\frac{1}{2}+\frac{0.36}{\pi(2^n-1)},$$

and the result follows. □

By (1), we then have the following theorem.

Theorem 3.4 *For $n \geq 8$, we have*

$$nl(CF) > 2^{n-1}-\left(\frac{n\ln 2}{\pi}+\frac{1}{\pi}\left(\gamma+\ln\frac{8}{\pi}\right)\right)2^{\frac{n}{2}}-\frac{2^{n-1}}{2^n-1}.$$

Remark 3.5 The lower bound on $nl(CF)$ in Theorem 3.4 improves upon known bounds. In Table 1, we display the comparison of our bound with the previously known ones. By Theorem 3.3, using the standard Gauss sum method, it seems that one cannot improve upon our lower bound on $nl(CF)$.

We note that there still exists a big gap between our bound and the exact value. However, our bound is the best possible deduced through the trigonometric sum and our estimates. If one wants to improve the bound further, one must use a different method, i.e., not through the trigonometric sum.

3.2 New bound on the nonlinearity of the function constructed by Tang–Carlet–Tang

Let $n = 2k \geq 4$ and α be a primitive element of $\mathbb{F}_{2^k}$. Let

$$\Delta_s = \{\alpha^s, \ldots, \alpha^{2^{k-1}+s-1}\}, \quad 0 \leq s < 2^k - 1.$$

Let g be the function of support Δ_s. The function $TTC \in \mathcal{B}_n$ introduced by Tang–Carlet–Tang in [36] is defined by

$$TTC(x, y) = g(xy).$$

This function has optimal algebraic immunity, good immunity to fast algebraic attacks and high algebraic degree. Tang et al. deduced a lower bound on the nonlinearity which is larger than all previously introduced bounds for similar functions. In the following, we will find a new lower bound on $nl(TTC)$.

We let $q = 2^k$. Let χ be the primitive character of $\mathbb{F}_q^*$ defined by $\chi(\alpha^j) = \zeta^j$ $(0 \le j \le q-2)$ and $\chi(0) = 0$, where $\zeta = e^{\frac{2\pi\sqrt{-1}}{q-1}}$. Let

$$G(\chi^\mu) = \sum_{x \in \mathbb{F}_q^*} \chi^\mu(x)(-1)^{tr(x)},\ 0 \le \mu \le 2^k - 2$$

be the Gauss sum [26] (recall that tr is the absolute trace of $\mathbb{F}_q$ over $\mathbb{F}_2$). By [36], we have

$$nl(TTC) = 2^{n-1} - \max_{0 \le s < 2^k - 1} |\Gamma_s|,$$

where

$$\Gamma_s = \frac{q}{2(q-1)} + \frac{1}{q-1} \sum_{\nu=1}^{q-2} G^2(\chi^\nu)\zeta^{-\nu s} \frac{\zeta^{-\nu \frac{q}{2}} - 1}{\zeta^{-\nu} - 1}.$$

Theorem 3.6 *For $k \ge 8$, we have*

$$nl(TTC) > 2^{n-1} - \left(\frac{k \ln 2}{\pi} + \frac{1}{\pi}\left(\gamma + \ln \frac{8}{\pi}\right)\right) 2^k + \frac{1}{\pi}.$$

Proof We have

$$\begin{aligned} nl(TTC) &= 2^{n-1} - \max_{0 \le s < 2^k - 1} \frac{1}{q-1} \left| \sum_{\nu=1}^{q-2} G^2(\chi^\nu)\zeta^{-\nu s} \frac{\zeta^{-\nu \frac{q}{2}} - 1}{\zeta^{-\nu} - 1} \right| - \frac{q}{2(q-1)} \\ &\ge 2^{n-1} - \frac{q}{q-1} \sum_{\nu=1}^{q-2} \left| \frac{\zeta^{-\nu \frac{q}{2}} - 1}{\zeta^{-\nu} - 1} \right| - \frac{q}{2(q-1)} \\ &= 2^{n-1} - \frac{q}{q-1} \sum_{\nu=1}^{q-2} \left| \frac{\zeta^{-\nu \frac{q}{4}} - \zeta^{\nu \frac{q}{4}}}{\zeta^{-\frac{\nu}{2}} - \zeta^{\frac{\nu}{2}}} \right| - \frac{q}{2(q-1)} \\ &= 2^{n-1} - \frac{q}{q-1} \sum_{\nu=1}^{q-2} \left| \frac{\sin \frac{\pi \nu \frac{q}{2}}{q-1}}{\sin \frac{\pi \nu}{q-1}} \right| - \frac{q}{2(q-1)}. \end{aligned}$$

Since $\sin \frac{\pi \nu \frac{q}{2}}{q-1} = \sin \frac{\pi \nu (\frac{q}{2} - 1)}{q-1}$, then by Theorem 3.3,

$$\sum_{\nu=1}^{q-2} \left| \frac{\sin \frac{\nu\pi \frac{q}{2}}{q-1}}{\sin \frac{\nu\pi}{q-1}} \right| < \frac{q-1}{\pi}\left(k \ln 2 + \gamma + \ln \frac{8}{\pi}\right) - \frac{1}{\pi} - \frac{1}{2} + \frac{0.72}{\pi(q-1)}.$$

Therefore,

$$nl(TTC) > 2^{n-1} - \left(\frac{k \ln 2}{\pi} + \frac{1}{\pi}\left(\gamma + \ln \frac{8}{\pi}\right)\right) 2^k$$

$$
\begin{aligned}
&+\frac{q}{q-1}\left(\frac{1}{\pi}+\frac{1}{2}-\frac{0.72}{\pi(q-1)}\right)-\frac{q}{2(q-1)}\\
&=2^{n-1}-\left(\frac{k\ln 2}{\pi}+\frac{1}{\pi}\left(\gamma+\ln\frac{8}{\pi}\right)\right)2^k+\frac{1}{\pi}+\frac{1}{\pi(q-1)}-\frac{0.72q}{\pi(q-1)^2}\\
&>2^{n-1}-\left(\frac{k\ln 2}{\pi}+\frac{1}{\pi}\left(\gamma+\ln\frac{8}{\pi}\right)\right)2^k+\frac{1}{\pi},
\end{aligned}
$$

and the theorem is shown. □

Remark 3.7 By Theorem 3.3, for any $C>0$,

$$
2^{n-1}-\frac{q}{q-1}\sum_{\nu=1}^{q-2}\left|\frac{\sin\frac{\pi\nu\frac{q}{2}}{q-1}}{\sin\frac{\pi\nu}{q-1}}\right|-\frac{q}{2(q-1)}<2^{n-1}-\left(\frac{k\ln 2}{\pi}+\frac{1}{\pi}\left(\gamma+\ln\frac{8}{\pi}\right)\right)2^k+\frac{1}{\pi}+C.
$$

That is, using the standard Gauss sum method, our lower bound on $nl(TTC)$ cannot be further improved.

4 Conclusion

In this paper, we give a very precise estimate of a trigonometric sum. Using that estimate, we deduce new lower bounds on the nonlinearity of the Carlet–Feng function and the function proposed by Tang et al. [36].

Acknowledgements Qichun Wang would like to thank the financial support from the National Natural Science Foundation of China (Grant 61572189).

Appendix: Proof of Lemmas 3.1 and 3.2

In order to prove Lemmas 3.1 and 3.2, we introduce a function $g(x)=\frac{1}{\sin x}-\frac{1}{x}$, which we extend at 0 (observe that $\lim_{x\to 0}g(x)=0$) by $g(0)=0$. First, $g'(x)=-\dfrac{\cos x}{\sin^2 x}+\dfrac{1}{x^2}$, and observe that $\lim_{x\to 0}g'(x)=\frac{1}{6}$ and $g'(\frac{\pi}{4})=\frac{16}{\pi^2}-\sqrt{2}$. Further,

$$
g''(x)=\frac{1+\cos^2 x}{\sin^3 x}-\frac{2}{x^3},\quad g'''(x)=-\frac{(5+\cos^2 x)\cos x}{\sin^4 x}+\frac{6}{x^4}.
$$

Using standard methods from calculus, it is easy to prove that $g'''(x)>0$, for $0<x<\pi$.

Lemma 3.1 gives an estimate of $T_1=\displaystyle\sum_{k=1}^{\frac{N+1}{4}}\frac{1}{\sin\frac{\pi(2k-1)}{2N}}$. Our idea of the proof is as follows.

To deduce a precise estimate of T_1, we first consider the sum $T_2=\displaystyle\sum_{k=1}^{\frac{N+1}{4}}g\left(\frac{\pi(2k-1)}{2N}\right)$.

Since we have the equation

$$
\frac{\pi}{N}T_2=\sum_{k=1}^{\frac{N+1}{4}}G_k\left(\frac{\pi}{N}\right)+\frac{\pi}{2N}g\left(\frac{\pi}{2N}\right)-\frac{\pi}{2N}g\left(\frac{\pi(N+3)}{4N}\right)+\frac{\pi}{2N}\int_{\frac{\pi}{2N}}^{\frac{\pi(N+3)}{4N}}g(x)dx, \tag{2}
$$

where

$$G_k(t) = \frac{t}{2}\left(g\left(\frac{\pi(2k-1)}{2N}\right) + g\left(\frac{\pi(2k-1)}{2N}+t\right)\right) - \int_{\frac{\pi(2k-1)}{2N}}^{\frac{\pi(2k-1)}{2N}+t} g(x)dx,\ 0 \le t \le \frac{\pi}{N},$$

we can give a precise estimate of T_2 by estimating those terms in (4), and then a precise estimate of T_1 can be deduced. The proof of Lemma 3.2 is similar.

The following four lemmas estimate those terms in (4) one by one.

Lemma A.1 *Let* $k, N \ge 255$ *be integers with* $N \equiv -1 \pmod 4$ *and* $1 \le k \le \frac{N+1}{4}$. *If*

$$G_k(t) = \frac{t}{2}\left(g\left(\frac{\pi(2k-1)}{2N}\right) + g\left(\frac{\pi(2k-1)}{2N}+t\right)\right) - \int_{\frac{\pi(2k-1)}{2N}}^{\frac{\pi(2k-1)}{2N}+t} g(x)dx,\ 0 \le t \le \frac{\pi}{N},$$

then

$$\frac{\pi^2}{12N^2}\left(\frac{16}{\pi^2} - \sqrt{2} - \frac{1}{6}\right) - \frac{0.115\pi^3}{12N^3} < \sum_{k=1}^{\frac{N+1}{4}} G_k\left(\frac{\pi}{N}\right) < \frac{\pi^2}{12N^2}\left(\frac{16}{\pi^2} - \sqrt{2} - \frac{1}{6}\right) + \frac{0.231\pi^3}{12N^3}.$$

Proof Clearly, for $0 \le t \le \frac{\pi}{N}$, we have

$$2G_k'(t) = g\left(\frac{\pi(2k-1)}{2N}\right) - g\left(\frac{\pi(2k-1)}{2N}+t\right) + tg'\left(\frac{\pi(2k-1)}{2N}+t\right),$$

and

$$2G_k''(t) = tg''\left(\frac{\pi(2k-1)}{2N}+t\right).$$

Since $g'''(x) > 0$, for $0 < x < \pi$, $g''(x)$ is strictly increasing on the interval $(0, \pi)$. Then we have

$$tg''\left(\frac{\pi(2k-1)}{2N}\right) \le 2G_k''(t) = tg''\left(\frac{\pi(2k-1)}{2N}+t\right) \le tg''\left(\frac{\pi(2k+1)}{2N}\right).$$

Since $G_k(0) = G_k'(0) = 0$, we have

$$g''\left(\frac{\pi(2k-1)}{2N}\right)t^3 \le 12G_k(t) \le g''\left(\frac{\pi(2k+1)}{2N}\right)t^3.$$

Therefore,

$$\frac{\pi^3}{12N^3}\sum_{k=1}^{\frac{N+1}{4}} g''\left(\frac{\pi(2k-1)}{2N}\right) \le \sum_{k=1}^{\frac{N+1}{4}} G_k\left(\frac{\pi}{N}\right) \le \frac{\pi^3}{12N^3}\sum_{k=1}^{\frac{N+1}{4}} g''\left(\frac{\pi(2k+1)}{2N}\right).$$

Clearly,

$$\begin{aligned}\sum_{k=1}^{\frac{N+1}{4}} g''\left(\frac{\pi(2k+1)}{2N}\right) &< \frac{N}{\pi}\int_0^{\frac{\pi}{4}} g''(x)dx + g''\left(\frac{\pi(N-1)}{4N}\right) + g''\left(\frac{\pi(N+3)}{4N}\right)\\ &< \frac{N}{\pi}\left(\frac{16}{\pi^2} - \sqrt{2} - \frac{1}{6}\right) + g''\left(\frac{\pi}{4}\right) + g''\left(\frac{258\pi}{4\cdot 255}\right)\\ &< \frac{N}{\pi}\left(\frac{16}{\pi^2} - \sqrt{2} - \frac{1}{6}\right) + 0.231,\end{aligned}$$

and

$$\sum_{k=1}^{\frac{N+1}{4}} g''\left(\frac{\pi(2k-1)}{2N}\right) > \frac{N}{\pi}\int_0^{\frac{\pi}{4}} g''(x)dx - g''\left(\frac{\pi}{4}\right)$$
$$> \frac{N}{\pi}\left(\frac{16}{\pi^2} - \sqrt{2} - \frac{1}{6}\right) - 0.115,$$

and the result follows. □

Lemma A.2 *Let* $N \geq 255$. *Then*

$$\frac{\pi^2}{48N^2} \leq \frac{\pi}{2N} g\left(\frac{\pi}{2N}\right) - \int_0^{\frac{\pi}{2N}} g(x)dx \leq \frac{\pi^2}{48N^2} + \frac{\pi^4}{512N^3}.$$

Proof Let $F_1(t) = tg(t) - \int_0^t g(x)dx$, where $0 \leq t \leq \frac{\pi}{2N}$. Clearly, $F_1(0) = 0$ and $F_1'(t) = tg'(t)$. Therefore,

$$\frac{t^2}{2}\lim_{t\to 0} g'(t) \leq F_1(t) \leq \frac{t^2}{2} g'\left(\frac{\pi}{2N}\right).$$

That is,

$$\frac{\pi^2}{48N^2} \leq F_1(\frac{\pi}{2N}) \leq \frac{\pi^2}{8N^2} g'\left(\frac{\pi}{2N}\right).$$

We have

$$g'\left(\frac{\pi}{2N}\right) = \frac{4N^2}{\pi^2} - \frac{\cos(\frac{\pi}{2N})}{\sin^2(\frac{\pi}{2N})} = \frac{4N^2\sin^2(\frac{\pi}{2N}) - \pi^2\cos(\frac{\pi}{2N})}{\pi^2\sin^2(\frac{\pi}{2N})}$$
$$< \frac{4N^2\left(\frac{\pi^2}{4N^2} - \frac{\pi^4}{48N^4} + \frac{0.016\pi^6}{N^6}\right) - \pi^2\left(1 - \frac{\pi^2}{8N^2}\right)}{\pi^2\left(\frac{\pi^2}{4N^2} - \frac{\pi^4}{48N^4}\right)}$$
$$= \frac{\frac{1}{6} + \frac{0.256\pi^2}{N^2}}{1 - \frac{\pi^2}{12N^2}} < \frac{1}{6} + \frac{\pi^2}{64N},$$

and the result follows. □

Lemma A.3 *Let* $N \geq 255$. *Then*

$$\frac{144 - 9\sqrt{2}\pi^2}{32N^2} \leq \frac{3\pi}{4N} g\left(\frac{\pi(N+3)}{4N}\right) - \int_{\frac{\pi}{4}}^{\frac{\pi(N+3)}{4N}} g(x)dx < \frac{144 - 9\sqrt{2}\pi^2}{32N^2} + \frac{4.05\pi^2}{32N^3}.$$

Proof Let $F_2(t) = tg\left(\frac{\pi}{4} + t\right) - \int_{\frac{\pi}{4}}^{\frac{\pi}{4}+t} g(x)dx$, where $0 \leq t \leq \frac{3\pi}{4N}$. Clearly, $F_2(0) = 0$ and $F_2'(t) = tg'\left(\frac{\pi}{4} + t\right)$. Therefore,

$$\frac{t^2}{2} g'\left(\frac{\pi}{4}\right) \leq F_2(t) \leq \frac{t^2}{2} g'\left(\frac{\pi}{4} + \frac{3\pi}{4N}\right),$$

and

$$\frac{9\pi^2}{32N^2} g'\left(\frac{\pi}{4}\right) \leq F_2\left(\frac{3\pi}{4N}\right) \leq \frac{9\pi^2}{32N^2} g'\left(\frac{\pi}{4} + \frac{3\pi}{4N}\right).$$

Clearly, $g'\left(\frac{\pi}{4}\right) = \frac{16}{\pi^2} - \sqrt{2}$ and

$$\begin{aligned} g'\left(\frac{\pi}{4} + \frac{3\pi}{4N}\right) &= \frac{1}{(\frac{\pi}{4} + \frac{3\pi}{4N})^2} - \frac{\cos(\frac{\pi}{4} + \frac{3\pi}{4N})}{\sin^2(\frac{\pi}{4} + \frac{3\pi}{4N})} \\ &< \left(\frac{16}{\pi^2} - \frac{96}{\pi^2 N} + \frac{432}{\pi^2 N^2}\right) - \frac{\sqrt{2}(\cos\frac{3\pi}{4N} - \sin\frac{3\pi}{4N})}{(\cos\frac{3\pi}{4N} + \sin\frac{3\pi}{4N})^2} \\ &< \frac{16}{\pi^2} - \frac{96}{\pi^2 N} + \frac{432}{\pi^2 N^2} - \sqrt{2}\left(1 - \frac{9\pi}{4N}\right) \\ &< \frac{16}{\pi^2} - \sqrt{2} + \frac{0.45}{N}, \end{aligned}$$

and the result follows. □

Lemma A.4 *Let $N \geq 255$. Then*

$$\frac{0.165}{N^2} < g\left(\frac{\pi(N+3)}{4N}\right) - (\sqrt{2} - \frac{4}{\pi} - \frac{3\sqrt{2}\pi}{4N} + \frac{12}{\pi N}) < \frac{0.457}{N^2}.$$

Proof We have

$$\begin{aligned} g\left(\frac{\pi(N+3)}{4N}\right) &= \frac{\sqrt{2}}{1 + \sin\frac{3\pi}{4N} - 2\sin^2\frac{3\pi}{8N}} - \frac{\frac{4}{\pi}}{1 + \frac{3}{N}} \\ &= \sqrt{2} - \frac{4}{\pi} - \frac{\sqrt{2}\left(\sin\frac{3\pi}{4N} - 2\sin^2\frac{3\pi}{8N}\right)}{1 + \sin\frac{3\pi}{4N} - 2\sin^2\frac{3\pi}{8N}} + \frac{\frac{12}{\pi N}}{1 + \frac{3}{N}}. \end{aligned}$$

Clearly,

$$\frac{3\pi}{4N} - \frac{27\pi^2}{32N^2} - \frac{3\pi^3}{128N^3} < \frac{\sin\frac{3\pi}{4N} - 2\sin^2\frac{3\pi}{8N}}{1 + \sin\frac{3\pi}{4N} - 2\sin^2\frac{3\pi}{8N}} < \frac{3\pi}{4N} - \frac{27\pi^2}{32N^2} + \frac{113\pi^3}{128N^3},$$

and

$$\frac{12}{\pi N} - \frac{36}{\pi N^2} < \frac{\frac{12}{\pi N}}{1 + \frac{3}{N}} < \frac{12}{\pi N} - \frac{36}{\pi N^2} + \frac{108}{\pi N^3},$$

and the result follows. □

Those terms in (4) have been estimated by the above four lemmas. We then can give a proof for Lemma 3.1.

Proof of Lemma 3.1 By Lemma A.1, we have

$$\begin{aligned} &\sum_{k=1}^{\frac{N+1}{4}} G_k\left(\frac{\pi}{N}\right) \\ &= \frac{\pi}{2N}\left(2\sum_{k=1}^{\frac{N+1}{4}} g\left(\frac{\pi(2k-1)}{2N}\right) - g\left(\frac{\pi}{2N}\right) + g\left(\frac{\pi(N+3)}{4N}\right)\right) - \int_{\frac{\pi}{2N}}^{\frac{\pi(N+3)}{4N}} g(x)dx \\ &< \frac{\pi^2}{12N^2}\left(\frac{16}{\pi^2} - \sqrt{2} - \frac{1}{6}\right) + \frac{0.231\pi^3}{12N^3}. \end{aligned}$$

Since $\int_0^{\frac{\pi}{4}} g(x)dx = \ln \frac{8(\sqrt{2}-1)}{\pi}$, we have

$$\frac{\pi}{N}\sum_{k=1}^{\frac{N+1}{4}} g\left(\frac{\pi(2k-1)}{2N}\right) < \ln\frac{8(\sqrt{2}-1)}{\pi} + \frac{\pi^2}{12N^2}\left(\frac{16}{\pi^2}-\sqrt{2}-\frac{1}{6}\right) + \frac{0.231\pi^3}{12N^3} + \frac{\pi}{2N}g\left(\frac{\pi}{2N}\right)$$
$$-\int_0^{\frac{\pi}{2N}} g(x)dx + \int_{\frac{\pi}{4}}^{\frac{\pi(N+3)}{4N}} g(x)dx - \frac{3\pi}{4N}g\left(\frac{\pi(N+3)}{4N}\right) + \frac{\pi}{4N}g\left(\frac{\pi(N+3)}{4N}\right).$$

Then by Lemmas A.2, A.3 and A.4, we have

$$\begin{aligned}\frac{\pi}{N}\sum_{k=1}^{\frac{N+1}{4}} g\left(\frac{\pi(2k-1)}{2N}\right) &< \ln\frac{8(\sqrt{2}-1)}{\pi} + \frac{\pi^2}{12N^2}\left(\frac{16}{\pi^2}-\sqrt{2}-\frac{1}{6}\right) + \frac{0.231\pi^3}{12N^3}\\ &\quad+\frac{\pi^2}{48N^2} + \frac{\pi^4}{512N^3} - \frac{144-9\sqrt{2}\pi^2}{32N^2}\\ &\quad+\frac{\pi}{4N}\left(\sqrt{2}-\frac{4}{\pi}-\frac{3\sqrt{2}\pi}{4N}+\frac{12}{\pi N}+\frac{0.457}{N^2}\right)\\ &< \ln\frac{8(\sqrt{2}-1)}{\pi} + \frac{\pi}{4N}\left(\sqrt{2}-\frac{4}{\pi}\right) + \frac{0.052}{N^2}.\end{aligned}$$

Clearly, $\sum_{k=1}^{\frac{N+1}{4}} \frac{1}{2k-1} < \frac{1}{2}\ln(N+1) + \frac{\gamma}{2} + \frac{1}{3(N+1)^2}$, where γ is Euler–Mascheroni's constant. Therefore,

$$\begin{aligned}&\frac{\pi}{N}\sum_{k=1}^{\frac{N+1}{4}} \frac{1}{\sin\frac{\pi(2k-1)}{2N}}\\ &\quad< \ln(N+1)+\gamma+\frac{2}{3(N+1)^2} + \ln\frac{8(\sqrt{2}-1)}{\pi} + \frac{\pi}{4N}\left(\sqrt{2}-\frac{4}{\pi}\right) + \frac{0.052}{N^2}\\ &\quad< \ln(N+1)+\gamma+\ln\frac{8(\sqrt{2}-1)}{\pi} + \frac{\pi}{4N}\left(\sqrt{2}-\frac{4}{\pi}\right) + \frac{0.72}{N^2}.\end{aligned}$$

Similarly, we can prove the left inequality of Lemma 3.1, and the result follows. □

To prove Lemma 3.2, we need two more lemmas.

Lemma A.5 *Let* $N \geq 255$, $N \equiv -1 \pmod 4$, *and* $1 \leq k \leq \frac{N+1}{4} - 1$ *be an integer. Let*

$$H_k(t) = \frac{t}{2}\left(g\left(\frac{\pi(N-2k)}{2N}\right) + g\left(\frac{\pi(N-2k)}{2N}+t\right)\right) - \int_{\frac{\pi(N-2k)}{2N}}^{\frac{\pi(N-2k)}{2N}+t} g(x)dx,\ 0 \leq t \leq \frac{\pi}{N}.$$

Then

$$\frac{\pi^2}{12N^2}\left(\sqrt{2}-\frac{12}{\pi^2}\right) - \frac{0.49\pi^3}{12N^3} < \sum_{k=1}^{\frac{N+1}{4}-1} H_k\left(\frac{\pi}{N}\right) < \frac{\pi^2}{12N^2}\left(\sqrt{2}-\frac{12}{\pi^2}\right) + \frac{0.61\pi^3}{12N^3}.$$

The proof of Lemma A.5 is quite similar to the proof of Lemma A.1, so we omit it here.

Lemma A.6 *Let* $N \geq 255$ *and* $N \equiv -1 \pmod 4$. *Then*

$$\frac{\ln 2}{2} - \frac{1}{N+1} - \frac{1.25}{(N-1)^2} < \sum_{k=1}^{\frac{N+1}{4}-1} \frac{1}{N-2k} < \frac{\ln 2}{2} - \frac{1}{N+1} - \frac{1.23}{(N-1)^2}.$$

Proof We have

$$\sum_{k=1}^{N-1} \frac{1}{k} = \ln(N-1) + \gamma + \frac{1}{2(N-1)} - \frac{1}{12(N-1)^2} + \frac{1}{120(N-1)^4} - \frac{\theta_1}{252(N-1)^6},$$

$$\sum_{k=1}^{\frac{N-1}{2}} \frac{1}{k} = \ln(\frac{N-1}{2}) + \gamma + \frac{1}{2(\frac{N-1}{2})} - \frac{1}{12(\frac{N-1}{2})^2} + \frac{1}{120(\frac{N-1}{2})^4} - \frac{\theta_2}{252(\frac{N-1}{2})^6},$$

$$\sum_{k=1}^{\frac{N+1}{4}} \frac{1}{k} = \ln(\frac{N+1}{4}) + \gamma + \frac{1}{2(\frac{N+1}{4})} - \frac{1}{12(\frac{N+1}{4})^2} + \frac{1}{120(\frac{N+1}{4})^4} - \frac{\theta_3}{252(\frac{N+1}{4})^6},$$

where γ is Euler–Mascheroni's constant and $0 < \theta_i < 1, i = 1, 2, 3$. Clearly

$$\sum_{k=1}^{\frac{N+1}{4}-1} \frac{1}{N-2k} = \left(\sum_{k=1}^{N-1} \frac{1}{k} - \frac{1}{2} \sum_{k=1}^{\frac{N-1}{2}} \frac{1}{k} \right) - \left(\sum_{k=1}^{\frac{N-1}{2}} \frac{1}{k} + \frac{2}{N+1} - \frac{1}{2} \sum_{k=1}^{\frac{N+1}{4}} \frac{1}{k} \right).$$

Therefore,

$$\sum_{k=1}^{\frac{N+1}{4}-1} \frac{1}{N-2k} = \frac{\ln 2}{2} + \frac{1}{2} \ln \left(1 + \frac{2}{N-1}\right) - \frac{1}{N-1} - \frac{1}{N+1} + \frac{5}{12(N-1)^2}$$
$$- \frac{2}{3(N+1)^2} - \frac{23}{120(N-1)^4} + \frac{16}{15(N+1)^4} + \frac{96\theta_2 - \theta_1}{252(N-1)^6} - \frac{512\theta_3}{63}.$$

Clearly

$$\frac{2}{N-1} - \frac{2}{(N-1)^2} < \ln \left(1 + \frac{2}{N-1}\right) < \frac{2}{N-1} - \frac{2}{(N-1)^2} + \frac{8}{3(N-1)^3},$$

and the result follows. □

We then can give a proof for Lemma 3.2.

Proof of Lemma 3.2 By Lemma A.5, we have

$$\sum_{k=1}^{\frac{N+1}{4}-1} H_k\left(\frac{\pi}{N}\right)$$
$$= \frac{\pi}{2N} \left(2 \sum_{k=1}^{\frac{N+1}{4}-1} g\left(\frac{\pi(N-2k)}{2N}\right) + g\left(\frac{\pi}{2}\right) - g\left(\frac{\pi}{4} + \frac{3\pi}{4N}\right) \right) - \int_{\frac{\pi}{4}+\frac{3\pi}{4N}}^{\frac{\pi}{2}} g(x)dx$$
$$< \frac{\pi^2}{12N^2} \left(\sqrt{2} - \frac{12}{\pi^2}\right) + \frac{0.61\pi^3}{12N^3}.$$

Since $\int_{\frac{\pi}{4}}^{\frac{\pi}{2}} g(x)dx = \ln \frac{\sqrt{2}+1}{2}$, we have

$$\frac{\pi}{N} \sum_{k=1}^{\frac{N+1}{4}-1} g\left(\frac{\pi(N-2k)}{2N}\right) < \frac{\pi^2}{12N^2}\left(\sqrt{2}-\frac{12}{\pi^2}\right) + \frac{0.61\pi^3}{12N^3} + \ln\frac{\sqrt{2}+1}{2} - \frac{\pi}{2N} g\left(\frac{\pi}{2}\right) + \frac{3\pi}{4N} g\left(\frac{\pi}{4}+\frac{3\pi}{4N}\right) - \int_{\frac{\pi}{4}}^{\frac{\pi}{4}+\frac{3\pi}{4N}} g(x)dx - \frac{\pi}{4N} g\left(\frac{\pi}{4}+\frac{3\pi}{4N}\right).$$

Then by Lemmas A.3 and A.4, we have

$$\begin{aligned}
&\frac{\pi}{N} \sum_{k=1}^{\frac{N+1}{4}-1} g\left(\frac{\pi(N-2k)}{2N}\right) \\
&< \frac{\pi^2}{12N^2}\left(\sqrt{2}-\frac{12}{\pi^2}\right) + \frac{0.61\pi^3}{12N^3} + \ln\frac{\sqrt{2}+1}{2} - \frac{\pi}{2N}\left(1-\frac{2}{\pi}\right) \\
&+ \frac{144-9\sqrt{2}\pi^2}{32N^2} + \frac{4.05\pi^2}{32N^3} - \frac{\pi}{4N}\left(\sqrt{2}-\frac{4}{\pi}-\frac{3\sqrt{2}\pi}{4N}+\frac{12}{\pi N}+\frac{0.165}{N^2}\right) \\
&< \ln\frac{\sqrt{2}+1}{2} + \frac{2}{N} - \frac{\pi}{2N} - \frac{\sqrt{2}\pi}{4N} + \frac{0.37}{N^2}.
\end{aligned}$$

By Lemma A.6, $\sum_{k=1}^{\frac{N+1}{4}-1} \frac{2}{N-2k} < \ln 2 - \frac{2}{N+1} - \frac{2.46}{(N-1)^2}$. Therefore,

$$\begin{aligned}
\frac{\pi}{N} \sum_{k=1}^{\frac{N+1}{4}-1} \frac{1}{\cos\frac{\pi k}{N}} &= \frac{\pi}{N} \sum_{k=1}^{\frac{N+1}{4}-1} \frac{1}{\sin\frac{\pi(N-2k)}{2N}} \\
&< \ln 2 - \frac{2}{N+1} - \frac{2.46}{(N-1)^2} + \ln\frac{\sqrt{2}+1}{2} + \frac{2}{N} - \frac{\pi}{2N} - \frac{\sqrt{2}\pi}{4N} + \frac{0.37}{N^2} \\
&< \ln(\sqrt{2}+1) - \frac{\pi}{2N} - \frac{\sqrt{2}\pi}{4N}.
\end{aligned}$$

Similarly, we can show the left inequality of Lemma 3.2, and the result follows. □

References

1. Berlekamp E.R., Welch L.R.: Weight distributions of the cosets of the (32, 6) Reed-Muller code. IEEE Trans. Inf. Theory **18**(1), 203–207 (1972).
2. Braeken A., Preneel B.: On the algebraic immunity of symmetric Boolean functions. In: Progress in Cryptology-Indocrypt 2005, LNCS 3797, pp. 35–48. Springer, New York (2005).
3. Carlet C.: The complexity of Boolean functions from cryptographic viewpoint (2006). http://dblp.uni-trier.de/db/conf/dagstuhl/P6111.html.
4. Carlet C.: Boolean functions for cryptography and error correcting codes, chapter of the monography. In: Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press, Cambridge (2010). http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.
5. Carlet C.: Comments on constructions of cryptographically significant boolean functions using primitive polynomials. IEEE Trans. Inf. Theory **57**(7), 4852–4853 (2011).
6. Carlet C., Feng K.: An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. In: Advances in Cryptology—ASIACRYPT 2008, LNCS 5350, pp. 425–440. Springer, New York (2008).

7. Carlet C., Mesnager S.: Improving the upper bounds on the covering radii of binary Reed-Muller codes. IEEE Trans. Inf. Theory **53**(1), 162–173 (2007).
8. Carlet C., Mesnager S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**(1), 5–50 (2016).
9. Carlet C., Dalai D.K., Gupta K.C., Maitra S.: Algebraic immunity for cryptographically significant Boolean functions: analysis and construction. IEEE Trans. Inf. Theory **52**(7), 3105–3121 (2006).
10. Cohen G., Honkala I., Litsyn S., Lobstein A.: Covering Codes. North-Holland, Amsterdam (1997).
11. Cusick T.W., Stănică P.: Cryptographic Boolean Functions and Applications, 2nd edn. Elsevier, New York (2017).
12. Dalai D.K., Maitra K.C., Maitra S.: Cryptographically significant Boolean functions: construction and analysis in terms of algebraic immunity. In: Proceedings of FSE 2005, LNCS 3557, pp. 98–111. Springer, New York (2005)
13. Dalai D.K., Maitra S., Sarkar S.: Basic theory in construction of Boolean functions with maximum possible annihilator immunity. Des. Codes Cryptogr. **40**(1), 41–58 (2006).
14. Feng K., Liao Q., Yang J.: Maximum values of generalized algebraic immunity. Des. Codes Cryptogr. **50**(2), 243–252 (2009).
15. Gangopadhyay S., Mandal B., Stănică P.: Gowers U_3 norm of some classes of bent Boolean functions. Des. Codes Cryptogr. **86**(5), 1131–1148 (2018).
16. Golić J.D.: Linear cryptanalysis of stream ciphers. In: Fast Software Encryption—FSE 1994, LNCS 1008, pp. 154–169. Springer, New York (1994).
17. Hakala R.M., Nyberg K.: On the nonlinearity of the discrete logarithm in $\mathbb{F}_2^n$. In: SEquences and Their Applications–SETA 2010, LNCS 6338, pp. 333–345. Springer, New York (2010).
18. Hou X.D.: Covering radius of the Reed-Muller code $R(1, 7)$—a simpler proof. J. Comb. Theory Ser. A **74**(2), 337–341 (1996).
19. Hou X.D.: On the covering radius of $R(1, m)$ in $R(3, m)$. IEEE Trans. Inf. Theory **42**(3), 1035–1037 (1996).
20. Hou X.D.: The Covering Radius of $R(1, 9)$ in $R(4, 9)$. Des. Codes Cryptogr. **8**(3), 285–292 (1996).
21. Hou X.D.: On the norm and covering radius of the first order Reed-Muller codes. IEEE Trans. Inf. Theory **43**(3), 1025–1027 (1997).
22. Kavut S., Yücel M.D.: 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class. Inf. Comput. **208**(4), 341–350 (2010).
23. Kavut S., Maitra S., Yücel M.D.: Search for Boolean functions with excellent profiles in the rotation symmetric class. IEEE Trans. Inf. Theory **53**(5), 1743–1751 (2007).
24. Li N., Qi W.F.: Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity. In: Advances in Cryptology–ASIACRYPT 2006, LNCS 4284, pp. 84–98. Springer, New York (2006).
25. Li N., Qu L., Qi W., Feng G., Li C., Xie D.: On the construction of Boolean functions with optimal algebraic immunity. IEEE Trans. Inf. Theory **54**(3), 1330–1334 (2008).
26. Lidl R., Niederreiter H.: Introduction to Finite Fields and Their Applications. Cambridge University Press, Cambridge (1986).
27. Liu M., Zhang Y., Lin D.: Perfect algebraic immune functions. Advances in Cryptology–ASIACRYPT 2012, LNCS 7658, pp. 172–189. Springer, New York (2012).
28. Meier W., Staffelbach O.: Fast correlation attacks on stream ciphers. In: Advances in Cryptology–EUROCRYPT ’88, LNCS 330, pp. 301–314. Springer, New York (1988).
29. Mykkeltveit J.J.: The covering radius of the (128, 8) Reed-Muller code is 56. IEEE Trans. Inf. Theory **26**(3), 359–362 (1980).
30. Pasalic, E.: Almost fully optimized infinite classes of Boolean functions resistant to (Fast) algebraic cryptanalysis. In: Proceedings of ICISC 2008, LNCS 5461, pp. 399–414. Springer, New York (2009).
31. Patterson N.J., Wiedemann D.H.: The covering radius of the (215, 16) Reed-Muller code is at least 16276. IEEE Trans. Inf. Theory **29**(3), 354–356 (1983).
32. Qu L., Feng K., Liu F., Wang L.: Constructing symmetric Boolean functions with maximum algebraic immunity. IEEE Trans. Inf. Theory **55**(5), 2406–2412 (2009).
33. Rizomiliotis P.: On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation. IEEE Trans. Inf. Theory **56**(8), 4014–4024 (2010).
34. Tan C., Goh S.: Several classes of even-variable balanced Boolean functions with optimal algebraic immunity. Trans. Fundam. Electron. Commun. Comput. Sci. **94**(1), 165–171 (2011).
35. Tang D., Maitra S.: Construction of n-variable ($n \equiv 2 \bmod 4$) balanced Boolean functions with maximum absolute value in autocorrelation spectra $< 2^{n/2}$. IEEE Trans. Inf. Theory **64**(1), 393–402 (2018).
36. Tang D., Carlet C., Tang X.: Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. IEEE Trans. Inf. Theory **59**(1), 653–664 (2013).

37. Tu Z., Deng Y.: A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. Des. Codes Cryptogr. **60**(1), 1–14 (2011).
38. Wang Q., Stănică P.: New bounds on the covering radius of the second order Reed–Muller code of length 128. Cryptogr. Commun. (2018). https://doi.org/10.1007/s12095-018-0289-2.
39. Wang Q., Tan C.H.: Properties of a family of cryptographic Boolean functions. In: SEquences and Their Applications–SETA 2014, LNCS 8865, pp. 34–46. Springer, New York (2012).
40. Wang Q., Tan C.H.: Proof of a conjecture and a bound on the imbalance properties of LFSR subsequences. Discret. Appl. Math. **211**, 217–221 (2016).
41. Wang Q., Peng J., Kan H., Xue X.: Constructions of cryptographically significant Boolean functions using primitive polynomials. IEEE Trans. Inf. Theory **56**(6), 3048–3053 (2010).
42. Wang Q., Tan C.H., Prabowo T.F.: On the covering radius of the third order Reed-Muller code $RM(3, 7)$. Des. Codes Cryptogr. **86**(1), 151–159 (2018).
43. Zeng X., Carlet C., Shan J., Hu L.: More balanced Boolean functions with optimal algebraic immunity, and good nonlinearity and resistance to fast algebraic attacks. IEEE Trans. Inf. Theory **57**(9), 6310–6320 (2011).