LETTER

Search for 9-Variable Boolean Functions with the Optimal Algebraic Immunity-Resiliency Trade-Off and High Nonlinearity

Yueying LOU[†], ***Nonmember and*** **Qichun WANG**[†,††a)], ***Member***

SUMMARY Boolean functions play an important role in symmetric ciphers. One of important open problems on Boolean functions is determining the maximum possible resiliency order of n-variable Boolean functions with optimal algebraic immunity. In this letter, we search Boolean functions in the rotation symmetric class, and determine the maximum possible resiliency order of 9-variable Boolean functions with optimal algebraic immunity. Moreover, the maximum possible nonlinearity of 9-variable rotation symmetric Boolean functions with optimal algebraic immunity-resiliency trade-off is determined to be 224.

key words: *Boolean function, algebraic immunity, resiliency, nonlinearity*

1. Introduction

Boolean functions play an important role in designing ciphers. When designing a Boolean function, the most important criteria are resiliency, algebraic degree, nonlinearity, algebraic immunity, etc. It is well-known that the algebraic immunity of n-variable Boolean functions is upper bounded by $\lceil \frac{n}{2} \rceil$. One of important open problems is determining the maximum possible resiliency order of Boolean functions with optimal algebraic immunity [1], [2]. According to the Siegenthaler's bound, given an n-variable Boolean function of algebraic degree ≥ 2, the sum of its algebraic degree and resiliency order is at most $n-1$. Moreover, the algebraic immunity of a Boolean function is less than or equal to its algebraic degree. Therefore, the resiliency order of a Boolean function with optimal algebraic immunity is bounded above by $n-1-\lceil \frac{n}{2} \rceil$. Then, a natural question is whether there exist n-variable Boolean functions with the optimal algebraic immunity $\lceil \frac{n}{2} \rceil$ and the maximum possible resiliency order $n-1-\lceil \frac{n}{2} \rceil$.

In [10], the authors studied the rotation symmetric Boolean functions on 5, 6, 7 variables by computer search and found some functions with very good cryptographic properties. In [4], the authors tested the algebraic immunity of these functions and found 7-variable Boolean functions with the optimal algebraic immunity 4 and the maximum possible resiliency order 2. Moreover, the authors constructed an 8-variable Boolean function with the optimal algebraic immunity 4, the maximum possible resiliency order 3, and a high nonlinearity 112.

There are exactly 2^{512} 9-variable Boolean functions, and 2^{60} of them are rotation symmetric. In [6], 9-variable rotation symmetric Boolean functions with nonlinearity 241 were found which solved an open question for almost three decades. In [7], Kavut and Y*ü*cel found 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class. However, all these functions are not balanced. Up until now, we still do not know whether there exist 9-variable Boolean functions with nonlinearity greater than 242, even cannot determine the existence of 9-variable balanced Boolean functions with nonlinearity greater than 240. As for higher order nonlinearities, a recent paper proved that the covering radius of the third-order Reed-Muller code RM(3, 7) is 20 which solved an open problem for around four decades [5].

It is natural to ask whether there exist 9-variable Boolean functions with the optimal algebraic immunity, the maximum possible resiliency order and a high nonrearity. In this letter, we search Boolean functions in the rotation symmetric class, and find 9-variable Boolean functions with the optimal algebraic immunity 5, the maximum possible resiliency order 3 and a high nonlinearity 224 which is the maximum possible nonlinearity of 9-variable rotation symmetric Boolean functions with optimal algebraic immunity-resiliency trade-off.

2. Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_2$. We denote by B_n the set of all n-variable Boolean functions, from $\mathbb{F}_2^n$ into $\mathbb{F}_2$.

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

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

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 $1_f = \{x \in \mathbb{F}_2^n | f(x) = 1\}$ be the support of a Boolean function f, whose cardinality $|1_f|$ is called the *Hamming*

Manuscript received December 19, 2023.
Manuscript revised February 5, 2024.
Manuscript publicized March 28, 2024.

[†]School of Computer and Electronic Information/School of Artificial Intelligence, Nanjing Normal University, Nanjing, 210023, P.R. China.
[††]Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai, 200433, China.
a) E-mail: qcwang@fudan.edu.cn

DOI: 10.1587/transfun.2023EAL2111

weight of f, and will be denoted by $wt(f)$. The *Hamming distance* between two functions f and g, denoted by $d(f,g)$, is the Hamming weight of $f+g$. We say that an n-variable Boolean function f is *balanced* if $wt(f)=2^{n-1}$.

The *nonlinearity* of $f \in B_n$ is

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

which is bounded above by $2^{n-1}-2^{n/2-1}$, and a function is said to be *bent* if it achieves this bound.

For any $f \in B_n$, define $AN(f) = \{g \in B_n \mid g \neq 0 \text{ and } f * g = 0\}$. The *algebraic immunity* of f, denoted by $AI(f)$, is defined as

$$AI(f) = \min\{\deg(g) \mid g \in AN(f) \cup AN(f+1)\}.$$

It is known that the algebraic immunity of an n-variable Boolean function is bounded above by $\lceil \frac{n}{2} \rceil$ [3], [8].

The *Walsh transform* of a given function $f \in B_n$ is the integer-valued function over $\mathbb{F}_2^n$ defined by

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

where $\omega \cdot x$ is the usual inner product. It is easy to see that a Boolean function f is balanced if and only if $W_f(0)=0$.

Let $f \in B_n$. f is called *resilient* of order d if and only if

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+w \cdot x} = 0,$$

for any $w \in \mathbb{F}_2^n$ satisfying $0 \leq wt(w) \leq d$ [1], [2], [9], [12].

$f \in B_n$ is a *rotation symmetric Boolean function (RSBF)* if for each input $x \in \mathbb{F}_2^n$, $f(\rho(x)) = f(x)$, where $\rho(x_1,x_2,\ldots,x_n) = (x_2,\ldots,x_n,x_1)$. A partition of inputs can be generated by $G_n(x) = \rho^k(x)$ $(k=1,2,\ldots,n)$, and the number of partitions is denoted by g_n. Let $\varphi(k)$ be Euler's function. It is known that the number of n-variable RSBFs is 2^{g_n}, where

$$g_n = \frac{1}{n} \sum_{k|n} \varphi(k) 2^{n/k}.$$

A partition can be represented by its representative element $\Lambda_{n,i}$, which is the lexicographically first element belonging to the partition. The *rotation symmetric truth table (RSTT)* of an RSBF f is denoted by the string

$$[f(\Lambda_{n,0}), f(\Lambda_{n,1}), \ldots, f(\Lambda_{n,g_n-1})].$$

The ANF of an RSBF can be divided into some partitions which can also be represented by its representative element $\Lambda_{n,i}$ associated with a monomial. If there is a '1' in the corresponding position of $\Lambda_{n,i} = (x_1,\ldots,x_n)$, then the variable is present in the monomial.

The $g_n \times g_n$ matrix ${}_n\mathcal{A}$ for an n-variable RSBF is defined as [11]

$${}_n\mathcal{A}_{i,j} = \sum_{x \in G_n(\Lambda_{n,i})} (-1)^{x \cdot \Lambda_{n,j}}.$$

The Walsh spectra of an RSBF can be calculated from the RSTT as

$$W_f(\Lambda_{n,j}) = \sum_{i=0}^{g_n-1} (-1)^{f(\Lambda_{n,i})} {}_n\mathcal{A}_{i,j}.$$

Moreover, the $g_n \times g_n$ matrix ${}_n\mathcal{B}$ is defined as

$${}_n\mathcal{B}_{i,j} = \bigoplus_{h \in G_n(\Lambda_{n,j})} h(\Lambda_{n,i}),$$

where $\Lambda_{n,i} = (x_1,\ldots,x_n)$ is a representative element, $G_n(\Lambda_{n,j})$ is a partition whose elements are monomials and $\Lambda_{n,j}$ is the representative monomial. This matrix can be used to deduce the RSTT of an RSBF.

3. Search for 9-Variable Boolean Functions with the Optimal Algebraic Immunity-Resiliency Trade-Off and High Nonlinearity

Let $f \in B_9$. It is well known that $AI(f) \leq 5$, and the sum of $deg(f)$ and the resiliency order is at most 8, according to the Siegenthaler's bound. Since $AI(f) \leq deg(f)$, if $AI(f)=5$, then $deg(f) \geq 5$ and the resiliency order of f is at most 3. In the following, we will search for 9-variable 3-resilient Boolean functions f with $AI(f)=5$ and a high nonlinearity in the RSBF class. In this case, $5 = AI(f) \leq deg(f) \leq 8-3 = 5$. That is, f must be of degree 5. Since the constant term of f has no effect on the considered properties, we always set it to be 0.

Clearly, there exist 1 partition of Hamming weight one, 4 partitions of Hamming weight two, 10 partitions of Hamming weight three, 14 partitions of Hamming weight four and 14 partitions of Hamming weight five. Since $deg(f)=5$, the search space of our RSBFs on 9 variables is of size around $2^{1+4+10+14+14} = 2^{43}$.

We sort the rows and columns of ${}_9\mathcal{B}_{60\times 60}$ by the Hamming weight of the representative terms, and consider the sub-matrix ${}_9\mathcal{B}_{60\times 43}$ whose columns correspond to the representative terms in the ANF of degree between 1 and 5, which can be used to compute the RSTT for a RSBF of degree 5. We divide the matrix vertically into 3 parts: the first 15 columns (corresponding to the representative terms in the ANF of degree between 1 and 3), the next 14 columns (corresponding to the representative terms of degree 4) and the last 15 columns (corresponding to the representative terms of degree 5). A randomly chosen 9-variable RSBF of degree 5 corresponds to some columns of ${}_9\mathcal{B}_{60\times 43}$ which can be represented by a vector of integers (b_0, b_1, b_2), where $0 \leq b_0 \leq 2^{15}-1$, $0 \leq b_1 \leq 2^{14}-1$ and $1 \leq b_2 \leq 2^{14}-1$. We divide the matrix horizontally into 4 equal parts and pre-compute the xor of each section for each input which is stored in the three-dimensional array $B[3][4][2^{15}]$: 3 vertical sections, 4 horizontal sections and all the possible chosen columns (15 or 14 bits).

The matrix ${}_9\mathcal{A}_{60\times 60}$ is divided horizontally into 4 sections, each of 15 rows, which can be represented by a vector of integers (a_0, a_1, a_2, a_3), where $0 \le a_i \le 2^{15}-1$. The sum of the rows is pre-computed for each section and is stored in the three-dimensional array $A[4][2^{15}][60]$: 4 sections, 2^{15} possible inputs and 60 columns. We then search for the 9-variable RSBFs satisfying the following condition

$$Wal_f(i) = \begin{cases} 0 & \text{if } 0 \le i \le 15, \\ \le M & \text{if } 16 \le i \le 59, \end{cases}$$

where M is the least number such that there exists a 9-variable RSBF satisfying the condition. We design a search algorithm as the following Algorithm 1 to find 9-variable RSBFs with the resiliency order 3 and a high nonlinearity.

Using Algorithm 1, we perform an exhaustive search in 48 hours on a 3.2 GHz computer with 8 GB of RAM, and find that there does not exist any 9-variable RSBF with the resiliency order 3 and the nonlinearity greater than 224. Moreover, there are exactly 235362 9-variable RSBFs with the resiliency order 3 and the nonlinearity 224. Algebraic immunity is an easy-control criterion and many functions among them are with the optimal algebraic immunity. We choose randomly a function from them and find that it has the optimal algebraic immunity 5. We provide the truth table of it as follows, where the numbers are in hexadecimal (e.g. 7=0111).

7B8A849D847597E285747A63976AB80D
85767A617A89691E966A698D9A9545F2
D0272F783EC978433EC9C196689347BC
C33C69C9699685B6969996366566BA49

Algorithm 1 Search for 9-variable RSBFs with the resiliency order 3 and a high nonlinearity

Input: The two arrays $A[4][2^{15}][60]$ and $B[3][4][2^{15}]$
Output: 9-variable RSBFs with the resiliency order 3 and a high nonlinearity

```
for b0 = 0 → 2^15 − 1 do
    for b1 = 0 → 2^14 − 1 do
        for b2 = 0 → 2^14 − 1 do
            a0 ← B[0][0][b0]
            a1 ← B[0][1][b0] ⊕ B[1][1][b1]
            a2 ← B[0][2][b0] ⊕ B[1][2][b1] ⊕ B[2][2][b2]
            a3 ← B[0][3][b0] ⊕ B[1][3][b1] ⊕ B[2][3][b2]
            flag ← 0
            for k = 0 → 15 do
                sum ← A[0][a0][j] + A[1][a1][j] + A[2][a2][j] + A[3][a3][j]
                if sum ≠ 0 then
                    flag ← 1
                    break
                end if
            end for
            if flag = 0 then
                max ← 0
                for k = 16 → 59 do
                    sum ← A[0][a0][j] + A[1][a1][j] + A[2][a2][j] + A[3][a3][j]
                    if |sum| > max then
                        max ← |sum|
                    end if
                end for
            end if
            if max = 64 then
                rstt1[i++] = [b0, b1, b2]
            end if
            if max < 64 then
                rstt2[j++] = [b0, b1, b2]
            end if
        end for
    end for
end for
```

Though there exist many cryptographically significant RSBFs, its ratio to the whole space is very low. We do not know whether there exist a 3-resilient 9-variable Boolean function with optimum algebraic immunity and a nonlinearity > 224, which we leave as an open problem.

Open problem: Does there exist a 3-resilient 9-variable Boolean function with optimum algebraic immunity and a nonlinearity > 224?

4. Conclusion

In this letter, we search Boolean functions in the rotation symmetric class, and find 9-variable Boolean functions with the optimal algebraic immunity 5 and the maximum possible resiliency order 3. Moreover, the maximum possible nonlinearity of 9-variable rotation symmetric Boolean functions with optimal algebraic immunity-resiliency trade-off is determined to be 224.

A natural open question is whether there exist 9-variable Boolean functions with optimal algebraic immunity 5, resiliency order 3 and a nonlinearity greater than 224, which we leave as an open problem.

Acknowledgments

The authors would like to thank the financial support from the National Natural Science Foundation of China (Grant 62172230) and National Natural Science Foundation of Jiangsu Province (No. BK20201369).

References

[1] C. Carlet, Boolean Functions for Cryptography and Coding Theory, Cambridge University Press, 2021.
[2] T.W. Cusick and P. Stănică, “Cryptographic Boolean Functions and Applications, Elsevier–Academic Press, 2009.
[3] N. Courtois and W. Meier, “Algebraic attacks on stream ciphers with linear feedback,” Advances in Cryptology – EUROCRYPT 2003, LNCS 2656, pp.345–359, Springer–Verlag, 2003.

[4] D.K. Dalai, K.C. Gupta, and S. Maitra, "Results on algebraic immunity for cryptographically significant Boolean functions," INDOCRYPT 2004, LNCS 3348, pp.92–106, Springer–Verlag, 2004.

[5] J. Gao, H. Kan, Y. Li, and Q. Wang, "The covering radius of the third-order Reed-Muller code RM(3,7) is 20," IEEE Trans. Inf. Theory, vol.69, no.6, pp.3663–3673, 2023.

[6] S. Kavut, S. Maitra, and M.D. Yücel, "Search for Boolean functions with excellent profiles in the rotation symmetric class," IEEE Trans. Inf. Theory, vol.53, no.5, pp.1743–1751, 2007.

[7] S. Kavut and M.D. Yücel, "9-variable boolean functions with nonlinearity 242 in the generalized rotation symmetric class," Information and Compututation, vol.208, no.4, pp.341–350, 2010.

[8] W. Meier, E. Pasalic, and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," Advances in Cryptology - EUROCRYPT 2004, LNCS 3027, pp.474–491, Springer–Verlag, 2004.

[9] T. Siegenthaler, "Correlation immunity of Nonlinear combining functions for cryptographic applications," IEEE Trans. Inf. Theory, vol.30, no.5, pp.776–780, 1984.

[10] P. Stănică and S. Maitra, "Rotation symmetric Boolean functions count and cryptographic properties," Discrete Applied Mathematics, vol.156, no.10, pp.1567–1580, 2008.

[11] P. Stănică, S. Maitra, and J. Clark, "Results on rotation symmetric bent and correlation immune Boolean functions," Fast Software Encryption 2004, LNCS 3017, pp.161–177, Springer–Verlag, 2004.

[12] G.Z. Xiao and J.L. Massey, "A spectral characterization of correlation-immune combining functions," IEEE Trans. Inf. Theory, vol.34, no.3, pp.569–571, 1988.