Construction of Odd-Variable Resilient Boolean Functions with Optimal Degree*

SHAOJING FU*, BING SUN**, CHAO LI++ AND LONGJIANG QU++

* College of Computer
** College of Science
National University of Defense Technology
Changsha, 410073 P.R. China
++ Key Lab of Network Security and Cryptology
Fujian Normal University
Fuzhou, 350007 P.R. China

In this paper, we investigate the problem of obtaining new construction methods for resilient Boolean functions. Given \( n \) (\( n \) odd and \( n \geq 35 \)), we firstly provide degree optimized 1-resilient \( n \)-variable functions with currently best known nonlinearity. Then we extend our method to obtain \( m \)-resilient (\( m > 1 \)) Boolean functions with degree \( n - m - 1 \), we show that these Boolean functions also achieve currently best known nonlinearity. Finally, the algebraic immunity and immunity against fast algebraic attack of the obtained Boolean functions are investigated.

Keywords: stream cipher, Boolean function, resiliency, nonlinearity, algebraic immunity

1. INTRODUCTION

Resilient Boolean functions have wide applications in combiner model or filter model for stream ciphers [1-3]. By a \((n, m, d, x)\) function we mean \( n \)-variable \( m \)-resilient Boolean function with degree \( d \) and nonlinearity \( x \). A component is replaced by a “−” if it is not specified, e.g. \((n, m, −, −)\) means the degree and the nonlinearity are not specified. It is now well accepted that for a resilient Boolean function in stream ciphers, it must satisfy such properties as high nonlinearity, high algebraic degree. All of these parameters are important in resisting on different kinds of attacks, so the researches on cryptographic resilient Boolean function are paid more and more attention.

However, not all of these criteria can be satisfied simultaneously. As for concerning degree, Siegenthaler [3] proved that \( d \leq n - m - 1 \) for \((n, m, d, x)\) functions. The resilient Boolean functions which reach this bound, is called degree optimized resilient Boolean functions. As for concerning the nonlinearity, a lot of results which include nontrivial nonlinearity (upper) bounds have been published in [4-7].

Considering a Boolean function on \( n \)-variable with order of resiliency \( m \) (\( m > n/2 - 3/2 \)), generalized construction methods for \((n, m, −, −)\) resilient functions which attain maximum possible nonlinearity have been proposed in [6, 8], and these Boolean functions also have the optimal degree since there exists a relational expression \( 2^{m+2^\left\lfloor \frac{n}{2}-1\right\rfloor d} \mid W_f(u) \) which was proved in [7].

Unfortunately, for a Boolean function on \( n \)-variable with low order of resiliency \( m \)

Received March 3, 2010; revised January 6, 2011; accepted April 27, 2011.
Communicated by Wen-Guey Tzeng.
* This work was supported by the National Nature Science Foundation of China (No. 61103191), and Key Lab of Fujian Province University Network Security and Cryptology (No. 2011003).
(m < n/2 - 2), we do not have a common method to generate a function attaining both the maximum possible nonlinearity and upper bound of the degree although we have obtained some interesting results by computer search techniques [9-11]. As a result, constructions of (n, m, n - m - 1, -) Boolean function focus on generating a function attaining as high nonlinearity as possible (not maximum possible nonlinearity), and the problem can be classified into the following two cases.

(1) For even n, construct (n, m, n - m - 1, -) functions with high nonlinearity.
(2) For odd n, construct (n, m, n - m - 1, -) functions with high nonlinearity.

The first problem has been studied in [12-16]. The currently best known results are obtained in [16] by using the disjoint spectra functions. The second problem has been less studied. In [14], the author modify the Patterson-Wiedemann functions to construct balanced Boolean functions on n-variables having nonlinearity strictly greater than 2\(^{n-1} - \frac{2(n-1)}{2}\) for odd n. To the best of our knowledge, this is the known construction which provides functions of the second type with highest nonlinearity, though in certain cases, for small number of variables, the technique of [15] yields better results.

Apart from already considered cryptographic criteria such as nonlinearity, algebraic degree, and resiliency, it turned out that the Boolean function must also have a high order of algebraic immunity and immunity against fast algebraic attack [17-19], and the study on resilient Boolean functions which has strongest ability to resist algebraic attack and fast algebraic attack is of great importance [20-22].

In this paper, based on the disjoint spectra functions theory in [16], we will provide a new method to construct degree optimized resilient Boolean functions with currently best known nonlinearity. Our construction can be seen as a future version of the construction in [23]. The rest of this paper is organized as follows. Section 2 provides basic definitions and notations. Section 3 presents a method to construct degree optimized 1-resilient Boolean function with nonlinearity > 2\(^{n-1} - \frac{2(n-1)}{2}\) when n is an odd number. In section 4, we extend the method to construct m-resilient function with nonlinearity > 2\(^{n-1} - \frac{2(n-1)}{2}\). In section 5, we study the algebraic immunity of the constructed functions and prove that our construction does not provide a maximum resistance against fast algebraic attacks. Section 6 concludes this paper.

2. RELATED WORKS

Let \(F_2\) be the finite field with 2 elements, the vector space of n-tuples of element from \(F_2\) is denoted by \(F_2^n\), \((F_2^n)^*\) be the set of all nonzero vector in \(F_2^n\). The addition operator over \(F_2\) is denoted by +, representing additions modulo 2. By \(B_n\) we mean the set of all Boolean functions on n variables. We interpret a Boolean function \(f(x_1, x_2, \ldots, x_n)\) as the output column of its truth table, that is, a string of length \(2^n\) having the form:

\[
\{f(0, 0, \ldots, 0), f(0, 0, \ldots, 1), \ldots, f(1, 1, \ldots, 1)\}.
\]

The weight of \(f\) is the number of ones in its output column, this is denoted by \(wt(f)\).

Definition 1  An n-variable Boolean function \(f\) is balanced iff \(wt(f) = 2^{n-1}\).
An $n$-variable function $f(x_1, \ldots, x_n)$ can be seen as a multivariate polynomial over $\mathbb{F}_2$, that is,

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq \{1,2,\ldots,n\}} a_I \prod_{i \in I} x_i$$

where the coefficients $a_I$ are in $\mathbb{F}_2$. This representation of $f$ is called the algebraic normal form (ANF) of $f$. The maximum cardinality of $I$ with $a_I \neq 0$ is called the algebraic degree, or simply the degree of $f$ and denoted by $\deg(f)$.

Boolean functions with degree at most one are called affine functions, affine functions with $f(0) = 0$ are called linear functions. The set of all $n$-variable affine functions is denoted by $A_n$, the set of all $n$-variable linear functions is denoted by $L_n$. The Walsh transform of an $n$-variable function $f$ is a real valued function defined as

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

where the dot product of vectors $x$ and $u$ is defined as $x \cdot u = x_1 u_1 + x_2 u_2 + \ldots + x_n u_n$. The nonlinearity of $f$ is defined as

$$NL(f) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^n} |W_f(u)|.$$ 

An $n$-variable Boolean function $f$ is called $t$-resilient if and only if its Walsh transform satisfies

$$W_f(u) = 0, \text{ for } 0 \leq wt(u) \leq m.$$ 

Let us now clearly clarify the exact upper bounds on the nonlinearity of resilient Boolean functions. It is known that for $n$ even, the maximum nonlinearity is $2^{n-1} - 2^{n/2-1}$ and the Boolean functions which attain this nonlinearity are called bent functions. However, the problem remains open for odd $n$. For the $n$-odd case, we here use the term $nlmax(n)$ to denote the maximum nonlinearity. The following results of the nonlinearity of an $(n, m, n-m-1, x)$ function have been provided in [13],

(1) If $n$ is even, and $m > n/2 - 2$, then $x \leq 2^{n-1} - 2^{m+1}$.
(2) If $n$ is even, and $m \leq n/2 - 2$, then $x \leq 2^{n-1} - 2^{n/2-1} - 2^m$.
(3) If $n$ is odd, and $nlmax(n) > 2^{n-1} - 2^{m+1}$, then $x \leq 2^{n-1} - 2^{m+1}$.
(4) If $n$ is odd, and $nlmax(n) \leq 2^{n-1} - 2^{m+1}$, then $x$ is the highest multiple of $2^{m+1}$ which is $\leq nlmax(n)$.

A nonzero $n$-variable Boolean function $g$ is called an annihilator of an $n$-variable Boolean function $f$ if $f \times g = 0$. We denote the set of all annihilators of $f$ by $AN(f)$.

**Definition 2** For $f \in B_n$, the algebraic immunity of $f$ is the minimum degree of non-zero functions $g \in B_n$ such that $f \times g = 0$ or $(f + 1) \times g = 0$. Namely,

$$AI(f) = \min \{ \deg(g) | 0 \neq g \in AN(f) \cup AN(1 + f) \}.$$
Definition 3 For $f \in B_n$, we say $f$ has optimal immunity against fast algebraic attack if for Boolean function $g$, $h$ such that $fg = h$. Denoting by $e$ and $d$ the degree of $g$ and $h$ respectively, then $e + d \leq n - 1$ for any $e \in [1, \lceil n/2 \rceil] - 1$.

3. CONSTRUCTION OF $(n, 1, n - 2, \cdot)$ FUNCTIONS WITH NONLINEARITY $> 2^{n-1} - 2^{(n-1)/2}$

In this section, by concatenating of a resilient Boolean function and a highly nonlinear Boolean function, we obtain our new 1-resilient Boolean functions with high nonlinearity. In fact, construction of resilient functions by concatenating two Boolean functions has been investigated in many references [13-15]. These constructions use the Maiorana-McFarland (MM) functions, but the general MM-functions restrict high nonlinearity. Here we use the disjoint spectra functions to confine ourselves to considering only a special subclass of the MM-functions obtained by imposing a restriction on an injective, and then we concatenate the MM-functions with a 15-variable Boolean function. As a result, we derive a new degree optimized 1-resilient Boolean functions, and the nonlinearity of our constructed 1-resilient functions are higher than previous construction.

Algorithm 1

Input: Parameter $n$ ($n \geq 35$ odd).

Output: an $(n, 1, n - 2, \cdot)$ function with nonlinearity $> 2^{n-1} - 2^{(n-1)/2}$.

Procedure:

Step 1: Take $n \geq 35$ and $n$ odd, let $n^* = (n - 15)/2$.

Step 2: Let $X = (x_1, \ldots, x_n) \in F_2^n$, choose $D = \{i_0, i_1\}$ with $1 \leq i_0 < i_1 \leq n^*$. Let $D_2 = \{1 \leq i \leq n^* \mid i \in D\}$, and $g^*(x) = \prod_{x_i \in D_2} x_i$.

Step 3: Obtain the set $T_0$ as, $T_0 = \{c \cdot X \mid c \in F_2^n, w(c) > 1\}$.

Step 4: Let $(X_1, X_{n-k}) = X$, where $X_1 = (x_1, \ldots, x_{k}) \in F_2^k$, and $X_{n-k} = (x_{k+1}, \ldots, x_n) \in F_2^{n-k}$, $\mu(X_{n-k})$ denotes an $n^* - k$-variable Boolean function with nonlinearity $W_c$. Let $\delta = \lceil \log_2(n^* + 1) \rceil$, we construct $T_1$ as follows,

4.1 Case $\sum_{j=2}^{\delta} \binom{\delta}{j} \geq n^* + 1$, then $T_1 = \{c \cdot X_\delta + \mu(X_{n-k}) \mid c \in F_2^\delta, w(c) > 1\}$.

4.2 Case $\sum_{j=2}^{\delta} \binom{\delta}{j} < n^* + 1$, if $n^* - \delta$ is odd or if $n^* - \delta$ is a power of 2, then $T_1 = \{c \cdot X_{\delta+1} + \mu(X_{n-k}) \mid c \in F_2^{\delta+1}, w(c) > 1\}$.

4.3 Case $\sum_{j=2}^{\delta} \binom{\delta}{j} < n^* + 1$, if $n^* - \delta$ is even and $n^* - \delta$ is not a power of 2, then $T_1 = \{c \cdot X_{\delta} + \mu(X_{n-k}) \mid c \in F_2^\delta, w(c) > 0\}$ where $\mu(X_{n-k})$ is a balanced Boolean function obtained by Dobbertin’s iterative Construction.

Step 5: Let $\phi$ be an injective mapping from $F_2^n$ to $T_0 \cup T_1$, and $\exists \tau' \in F_2^n$ such that $\phi(\tau') = \sum_{x_i \in D} x_i$. Let $h(Z)$ be a 15-variable function with nonlinearity $2^{14} - 2^7 + 20$, and $h(0) = 0$. Denote by $g(Y, \tau') = (y_1 + r_1 + 1) \ldots (y_{n^*} + r_{n^*} + 1)$. 
**Step 6:** For \((Z, Y, X) \in F_2^{15} \times F_2^{n^*} \times F_2^{n^*}\), output \(f(Z, Y, X) = h(Z) + \sum_{\tau \in F_2^{n^*}} \xi(Y, \tau) \phi(\tau) + (z_1 + 1) \ldots (z_{15} + 1) \xi(Y, \tau^*) g^*(X)\).

**Theorem 1** \(f(Z, Y, X)\) is an \((n, 1, n - 2, NL(f))\) function with

\[
NL(f) \geq 2^{n^*} - 2^{n^* - 2} - 108 \cdot W^* - 2^3,
\]

where \(W^* = 2^{n^*} - 2^{n^* - 2} W_{\delta} + 1\) for step 4.1; \(W^* = 2^{n^*} - 2^{n^* - 2} W_{\delta, 1}\) for step 4.2; \(W^* = 2^{s_{n^*}} - 1\) for step 4.3.

**Proof:**

(1) We prove that the definition of \(\phi\) is reasonable. It is obvious that \(|T_0| = \sum_{j=2}^{n^*} \left( \begin{array}{c} n^* \\ j \end{array} \right)\). According to the definition of \(T_i\), we have

\[
|T_0| + |T_1| \geq \sum_{j=2}^{n^*} \left( \begin{array}{c} n^* \\ j \end{array} \right) + n^* + 1 = 2^{n^*}.
\]

thus, the injective mapping \(\phi\) exists.

(2) We prove that \(\deg(f) = n - 2\).

Note that the degree of \(h(Z)\) is no more than 15, and the degree of \(\sum_{\tau \in F_2^{n^*}} \xi(Y, \tau) \phi(\tau)\) is less than \(n - 15\), so

\[
\deg(f) = \deg((z_1 + 1) \ldots (z_{15} + 1) \xi(Y, \tau^*) g^*(X)) = n - 2.
\]

(3) \(f\) is 1-resilient.

First, we study the Walsh transform of \(f\), for any \((c, b, a) \in F_2^{15} \times F_2^{n^*} \times F_2^{n^*}\), then

\[
W_f(c, b, a) = \sum_{Z, Y, X} (-1)^{f(Z, Y, X) + cZ + bY + aX}
\]

\[
= \sum_{Z=0, Y=\tau^*, X=\tau}(1) g^*(X) + \sum_{i=a} x_i + b \tau^* + aX + \sum_{Z=0, Y=\tau^*, X=\tau}(1) \sum_{i=0}^\tau \{Y_i \phi(\tau_i) + bY + aX \}
\]

\[
+ \sum_{Z=\tau^*, Y=\tau^*, X=\tau}(1) (Y^*_i \phi(\tau^*_i) + bY + aX)
\]

\[
= (-1)^{b \tau^*} \sum_{X\in F_2^{n^*}} (-1) g^*(X) + \sum_{i=a} x_i + aX
\]

\[
+ \sum_{Z=\tau^*, Y=\tau^*, X=\tau}(1) (Y^*_i \phi(\tau^*_i) + bY + aX)
\]

\[
+ \sum_{Z=\tau^*, Y=\tau^*, X=\tau}(1) (Y^*_i \phi(\tau^*_i) + bY + aX)
\]

If \(0 \leq w(c, b, a) \leq 1\), then \(0 \leq w(a) \leq 1\), which follows that

\[
\sum_{X\in F_2^{n^*}} (-1) g^*(X) + \sum_{i=a} x_i + aX = 0, \quad \sum_{X\in F_2^{n^*}} (-1) \phi(\tau_i) + aX = 0,
\]

so \(|W_f(c, b, a)| = 0\), according to Relation (1), then \(f\) is 1-resilient function.
(4) The nonlinearity is calculated as follows,

\[
W_f(c, b, a) = \sum_{Z \neq 0, Y, X} (-1)^{h(Z)+\sum_{Y,Z} \xi(Y,z)\phi(\tau)+c Z+b Y+a X} + \sum_{Z=0, Y, X} (-1)^{\sum_{Y,Z} \xi(Y,z)\phi(\tau)+c Z+b Y+a X}.
\]

\[
= \sum_{Z \neq 0, Y, X} (-1)^{h(Z)+\sum_{Y,Z} \xi(Y,z)\phi(\tau)+c Z+b Y+a X} + \sum_{Z=0, Y, X} (-1)^{\sum_{Y,Z} \xi(Y,z)\phi(\tau)+c Z+b Y+a X} + (-1)^{b \tau} \sum_{X \neq 0} [(-1)^{\sum_{X \neq 0} \phi(\tau)+a X} - (-1)^{a X}].
\]

Note that if \( g^* (X) + \sum_{i \in D} x_i + a \cdot X \neq \sum_{i \in D} x_i + a \cdot X \) if and only if \( \prod_{i \in D} x_i = 1 \), then \( |g^* (X)| + 2^2 \), which follows

\[
\|( -1)^{b \tau} \sum_X [(-1)^{g^* (X) + \sum_{X \neq 0} \phi(\tau)+a X} - (-1)^{a X}] \| \leq 2^3,
\]

then

\[
|W_f(c, b, a)| \leq \sum_{Z, Y, X} (-1)^{h(Z)+\sum_{Y,Z} \xi(Y,z)\phi(\tau)+c Z+b Y+a X} + 2^3 \leq |W(Z)|. \sum_{Y, X} (-1)^{h(Z)+c Y+a X} + 2^4.
\]

Note that the nonlinearity of \( h(Z) \) is \( 2^{14} - 2^7 + 20 \), and that

\[
\sum_{Y, X} (-1)^{h(Z)+c Y+a X} = \sum_{Y, X} (-1)^{\sum_{X \neq 0} \phi(\tau)+a X} = 2^{n'} + \sum_{\phi(\tau) \in T_1} (-1)^{b \tau} \sum_X (-1)^{\phi(\tau)+a X},
\]

then according to Relation (1), we finish the proof. 

\[\square\]

\( W^* \) should be small to insure \( f \) having a high nonlinearity, so \( W^*_c \) should be as small as possible. Note that the highest nonlinearity of 15-variable Boolean function is \( 2^{14} - 2^7 + 20 \) [24], and that the highest nonlinearity of 9-variable Boolean function is \( 2^8 - 2^3 + 2 \) [9]. Then by direct sum with bent functions, we can get the highest nonlinearity for odd variable Boolean function with the number of variable 11, 13, \( \geq 17 \). So, we have

(1) If \( 2 | n' - k \), then \( W^*_c = 2^{n'-k+1} - 2^{n'+k}/2 \);

(2) If \( 2 | n' - k \) and \( n' - k > 15 \), then \( W^*_c = 2^{n'+k} - 2^{(n'-k)/2} + 20 \cdot 2^{(n'+k-15)/2} \);

(3) If \( 2 | n' - k \) and \( 9 \leq n' - k < 15 \), then \( W^*_c = 2^{n'+k} - 2^{(n'-k)/2} + 2^{(n'+k-9)/2} \);

(4) If \( 2 | n' - k \) and \( n' - k < 9 \), then \( W^*_c = 2^{n'+k} - 2^{(n'-k)/2} \).
Table 1. The nonlinearity of 1-resilient Boolean function.

<table>
<thead>
<tr>
<th>(n)</th>
<th>Algorithm 1</th>
<th>[14]</th>
</tr>
</thead>
<tbody>
<tr>
<td>37</td>
<td>(2^{37} - 2^{18} + 13308)</td>
<td>–</td>
</tr>
<tr>
<td>39</td>
<td>(2^{39} - 2^{19} + 47356)</td>
<td>–</td>
</tr>
<tr>
<td>41</td>
<td>(2^{41} - 2^{20} + 108540)</td>
<td>(2^{41} - 2^{20} + 52224)</td>
</tr>
<tr>
<td>43</td>
<td>(2^{43} - 2^{21} + 258556)</td>
<td>(2^{43} - 2^{21} + 104448)</td>
</tr>
<tr>
<td>45</td>
<td>(2^{45} - 2^{22} + 544768)</td>
<td>(2^{45} - 2^{22} + 208896)</td>
</tr>
</tbody>
</table>

At the end of this section, we compare the nonlinearity obtained by [14] and our Construction in the Table 1, and it clearly shows the superiority of our method compared to the method in [14], “–” mean the construction fails.

4. CONSTRUCTION OF \((n, m, n - m - 1, \neg)\) FUNCTIONS WITH NONLINEARITY > \(2^{n-1} - 2^{(n-1)/2}\)

Note that the algorithm for 1-resilient functions can be extended to construct higher order resilient Boolean functions directly. However, in this case, we need find more nonlinear functions, then Algorithm 1 may be invalid. So, we will have the following improved algorithm for \(m > 1\).

Algorithm 2

Input: Parameter \(n\) (\(n\) odd and \(n \geq 35\)) and \(m > 1\).

Output: an \((n, m, n - m - 1, \neg)\) function with nonlinearity > \(2^{n-1} - 2^{(n-1)/2}\).

Procedure:

Step 1: Let \(n' = (n - 15)/2\). Choose \(D = \{l_0, l_1, \ldots, l_m\}\) with \(1 \leq l_0 < l_1 < \ldots < l_m \leq n'\). Let \(D_a = \{1 \leq i \leq n' \mid i \notin D\}\), and \(g^*(X) = \prod_{i \in D_a} x_i\) and obtain the set \(T_0\) as, \(T_0 = \{c \cdot X_{n'} \mid c \in \mathbb{F}_2^{n'}, \text{wt}(c) > m\}\).

Step 2: Find \(s \geq 1\) and \(k_1, \ldots, k_s\) satisfies \(\min \sum_{i=1}^{s} 2^{k_i} (2^{n' - k_i} - 2W_{k_i})\); \(\sum_{i=1}^{s} \left(\sum_{j=0}^{k_i} \binom{k_i}{j}\right)\).

Then Case \(\sum_{i=1}^{s} \left(\sum_{j=m+1}^{k_i} \binom{k_i}{j}\right) \leq \sum_{i=1}^{s} \left(\sum_{j=1}^{k_i} \binom{k_i}{j}\right)\).

Then \(T_i = \{c \cdot X_{n'}' + \mu(X_{n'}^*) \mid c \in \mathbb{F}_2^{n'-k_i}, \text{wt}(c) > m\}\),

where \(\mu(X_{n'}^*)\) is an \(n' - k_i\)-variable balanced Boolean function with nonlinearity \(W_{k_i}\).

Case \(\sum_{i=1}^{s} \left(\sum_{j=m+1}^{k_i} \binom{k_i}{j}\right) < \sum_{i=1}^{s} \left(\sum_{j=1}^{k_i} \binom{k_i}{j}\right)\) \(\leq \sum_{i=1}^{s} \left(\sum_{j=m}^{k_i} \binom{k_i}{j}\right)\) For \(1 \leq i \leq s\),

Then \(T_i = \{c \cdot X_{n'}' + \mu(X_{n'}^*) \mid c \in \mathbb{F}_2^{n'-k_i}, \text{wt}(c) > m - 1\}\),

where \(\mu(X_{n'}^*)\) is an \(n' - k_i\)-variable balanced Boolean function with nonlinearity \(W_{k_i}\).
Case \[\sum_{i=1}^{s} \left( \sum_{j=m}^{k_i} \binom{k_i}{j} \right) \leq \sum_{j=m}^{m} \left( \binom{m}{j} \right) \leq \sum_{i=1}^{s} \left( \sum_{j=m-1}^{k_i} \binom{k_i}{j} \right) \] For \(1 \leq i \leq s\),

\[T_k = \{ c \cdot X_i' + \mu(X_i') | c \in F_2^{n-k}, \text{wt}(c) > m - 2 \},\]

where \(\mu(X_i')\) is a \(n^* - k_i\)-variable 1-resilient Boolean function with maximum non-linearity \(W_{k_i}\).

\[
\sum_{i=1}^{s} \left( \sum_{j=m}^{k_i} \binom{k_i}{j} \right) \leq \sum_{j=m}^{m} \left( \binom{m}{j} \right) \leq \sum_{i=1}^{s} \left( \sum_{j=m-1}^{k_i} \binom{k_i}{j} \right) \quad \text{for } 1 \leq i \leq s,
\]

\[T_k = \{ c \cdot X_i' + \mu(X_i') | c \in F_2^{n-k}, \text{wt}(c) > p - 2 \},\]

where \(\mu(X_i')\) is a \(n^* - k_i\)-variable \(m - p + 1\)-resilient Boolean function with non-linearity \(W_{k_i}\).

\[
\sum_{i=1}^{s} \left( \sum_{j=m}^{k_i} \binom{k_i}{j} \right) \leq \sum_{j=m}^{m} \left( \binom{m}{j} \right) \leq \sum_{i=1}^{s} \left( \sum_{j=m-1}^{k_i} \binom{k_i}{j} \right) \quad \text{for } 1 \leq i \leq s,
\]

\[T_k = \{ c \cdot X_i' + \mu(X_i') | c \in F_2^{n-k}, \text{wt}(c) > 0 \},\]

where \(\mu(X_i')\) is a \(n^* - k_i\)-variable \(m-1\)-resilient Boolean function with nonlinearity \(W_{k_i}\).

**Step 3:** Let \(T = \bigcup_{k=0}^{D} T_k\) and \(\phi\) be an injective mapping from \(F_2^n\) to \(T\) such that \(\exists \tau^*, \phi(\tau^*) = \sum_{i=1}^{s} x_i\).

**Step 4:** Output Boolean function

\[f(Z, Y, X) = h(Z) + \sum_{\tau \in \mathcal{T}} \zeta(Y, \tau) \phi(\tau) + (z_1 + 1) \ldots (z_{15} + 1) g(Z, \tau^*) g(X),\]

where \(h(Z)\) be a 15-variable Boolean function with nonlinearity \(2^{14} - 2 + 20\) and \(h(0) = 0\), \(\zeta(Y, \tau) = (y_1 + r_1 + 1) \ldots (y_{15} + r_{15} + 1)\). Similarly as the proof of Theorem 1, we can show the following Theorem 2.

**Theorem 2** The \(f\) constructed in Algorithm 2 is an \((n, m, n - m - 1, NL(f))\) function, and the nonlinearity \(NL(f)\) satisfies

\[
NL(f) \geq 2^{n-1} - 2^{m+1} + (20 \cdot 2^{m+1} - 108 \cdot \sum_{k=1}^{s} 2^k (2^{n - k} - 2W_{k_i})) - 2^{m+1}.
\]

In Table 2, we list the nonlinearity of \((n, m, n - m - 1, -)\) functions corresponding to different constructions, “-” means that the construction is failed.

From Table 2, we can learned that: given \(n\), both [14] and our construction are often not valid for large resiliency orders. However, our construction adapts for more cases and provide better nonlinearity.
Table 2. The nonlinearity of \( m \)-resilient Boolean function.

<table>
<thead>
<tr>
<th>( m )</th>
<th>( n )</th>
<th>Algorithm 1</th>
<th>[21]</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>39</td>
<td>( 2^{39} - 2^{37} + 54104 )</td>
<td>–</td>
</tr>
<tr>
<td>2</td>
<td>41</td>
<td>( 2^{41} - 2^{43} + 108816 )</td>
<td>–</td>
</tr>
<tr>
<td>2</td>
<td>43</td>
<td>( 2^{43} - 2^{45} + 323148 )</td>
<td>–</td>
</tr>
<tr>
<td>2</td>
<td>45</td>
<td>( 2^{45} - 2^{47} + 870072 )</td>
<td>( 2^{40} - 2^{43} + 417792 )</td>
</tr>
<tr>
<td>2</td>
<td>47</td>
<td>( 2^{47} - 2^{49} + 1847288 )</td>
<td>( 2^{43} - 2^{47} + 835584 )</td>
</tr>
<tr>
<td>3</td>
<td>45</td>
<td>( 2^{45} - 2^{47} + 424684 )</td>
<td>–</td>
</tr>
<tr>
<td>3</td>
<td>49</td>
<td>( 2^{49} - 2^{51} + 850668 )</td>
<td>–</td>
</tr>
<tr>
<td>3</td>
<td>51</td>
<td>( 2^{51} - 2^{53} + 2587372 )</td>
<td>–</td>
</tr>
<tr>
<td>3</td>
<td>53</td>
<td>( 2^{53} - 2^{55} + 4472108 )</td>
<td>( 2^{52} - 2^{56} + 3342336 )</td>
</tr>
<tr>
<td>4</td>
<td>51</td>
<td>( 2^{51} - 2^{53} + 3404844 )</td>
<td>–</td>
</tr>
</tbody>
</table>

5. ALGEBRAIC IMMUNITY AND IMMUNITY AGAINST FAST ALGEBRAIC ATTACKS

It seems quite difficult to achieve all of the necessary criteria such as high resiliency, high nonlinearity, high algebraic degree, high algebraic immunity and immunity against fast algebraic attacks. However, high resilient functions are only used in the combiner model stream ciphers. For application in filter model stream ciphers, one order resiliency is enough. A general construction of 1-resilient Boolean functions with maximum algebraic immunity was first provided in [20]. Recently, [22] provided 1-resilient functions with maximum algebraic immunity by a primary construction, when the number of variables \( n \) equals to 6, 8, 10, 12; Then in [21], the authors presents a construction for a class of 1-resilient Boolean functions with maximum algebraic immunity on any even number of variables by correlation classes. In this section, we just study the algebraic immunity and immunity against fast algebraic attacks of Boolean function in Algorithm 1.

Note that the ANF of the functions in Algorithm 1 is

\[
f(Z, Y, X) = h(Z) + \sum_{\tau \in F_2^n} \xi(Y, \tau) \phi(\tau) \times (z_1 + 1) \ldots (z_{15} + 1) \xi(Y, \tau) g^*(X).\]

If we multiplied \( f(Z, Y, X) \) by \( (z_1 + 1) \), we have

\[
f \times (z_1 + 1) = h(Z) \times (z_1 + 1) + \sum_{\tau \in F_2^n} \xi(Y, \tau) \phi(\tau) \times (z_1 + 1).
\]

Note that the highest degree of \( \phi(\tau) \) is \( n^* - 3 \), which indicates that \( \deg(f(Z, Y, X) \times (z_1 + 1)) \leq n - 17 \). So, our functions are not good to resist fast algebraic cryptanalysis.

As for algebraic attack, let \( h(Z) \) be nonzero annihilators of \( h(Z) \) with low degree, and \( \psi(\tau) \) be annihilators of \( \phi(\tau) \), then,

\[
g(Z, Y, X) = \sum_{\tau \in F_2^n} \xi(Y, \tau) \psi(\tau) \times h(Z)
\]

is an annihilator of \( f(Z, Y, X) \).

Since some \( \phi(\tau) \) is not linear, we can simply the \( g(Z, Y, X) \) by selecting \( \psi(\tau) = 0 \) for \( \tau \).
\[ \not \in T_0, \text{ then } g(Z, Y, X) = \sum_{\tau \in T_0} g(Y, \tau)(\phi(\tau) + 1) \times h(Z). \]

Note that \( \text{deg}(\phi(\tau) + 1) = 1 \), then the degree of such an annihilator is less than \( n^* + 9 = (n + 1)/2 + (\text{deg}(h(Z))) - 7 \). That means if the algebraic immunity of \( h(Z) \) is low, then our functions will also not resist algebraic attack. However, we do not know the algebraic immunity of \( h(Z) \).

6. CONCLUSION AND OPEN PROBLEM

In this paper, we considered the problem of obtaining new construction methods for cryptographically significant Boolean functions. We firstly provide 1-resilient \( n \)-variable (\( n \geq 35 \), odd) functions with nonlinearity \( > 2^{n-1} - 2^{(n-1)/2} \). Then for resiliency \( m > 1 \), we give an improved method to obtain \( m \)-resilient Boolean functions with degree \( n - m - 1 \) and nonlinearity \( > 2^{n-1} - 2^{(n-1)/2} \). For both \( m = 1 \) and \( m > 1 \), our construction provide odd-variable resilient Boolean functions with currently best known nonlinearity.

However, our method is only successful for some small \( m \), it is still an open problem to find new algorithms to get an \((n, m, n - m - 1, -)\) functions for general \( m \leq n/2 - 2 \). Furthermore, there are still some problems need to be studied such as the upper bound of nonlinearity \((n, m, n - m - 1, -)\) resilient Boolean functions for general \( n \geq 15 \), we have the conjecture about the upper bound of nonlinearity as follow.

**Conjecture 1** If \( n \geq 15 \) be odd and \( m \leq (n - 1)/4 - 3 \), then nonlinearity \((n, m, n - m - 1, -)\) functions satisfies

\[ \text{NL}(f) \leq 2^{n-1} - 2^{(n-1)/2} + \frac{20}{128} 2^{(n-1)/2}. \]

REFERENCES


Shaojing Fu (付紹靜) received the Ph.D. degree in Applied Mathematical from National University of Defense Technology in 2010. He is currently an Assistant Professor in College of Computer, National University of Defense Technology, Changsha, China. His research fields include cryptography and information security.

Bing Sun (孫兵) received the Ph.D. degree in Applied Mathematical from National University of Defense Technology in 2009. He is currently an Assistant Professor in Department of Mathematics and System Science, National University of Defense Technology, Changsha, China. His research fields include cryptography and coding theory.

Chao Li (李超) received the B.A. degree in Mathematics in 1987 from the University of Information Engineering of China, the M.S. degree in Mathematics in 1990 from the University of Science and Technology of China, and the Ph.D. degree in Engineering in 2002 from the National University of Defense Technology of China. Since December 2001, he has been a Professor in the Department of Mathematics and System Science, National University of Defense Technology. His research fields include: coding theory, cryptography and sequences.

Longjiang Qu (屈龍江) received his Ph.D. degree in 2007 in Mathematics from the National University of Defense Technology, Changsha, China. He is now an Associate Professor in the Department of Mathematics and System Science, National University of Defense Technology of China. His research fields include cryptography and coding theory.