Applied Mathematics Letters 24 (2011) 2093–2096

Contents lists available at ScienceDirect

Applied Mathematics Letters

journal homepage: www.elsevier.com/locate/aml

Balanced $2p$-variable rotation symmetric Boolean functions with maximum algebraic immunity

Shaojing Fu [a,b,*], Chao Li [c], Kanta Matsuura [b], Longjiang Qu [c]

[a] College of Computer, National University of Defense Technology, Changsha, China
[b] Institute of Industrial Science, University of Tokyo, 4-6-1 Komaba, Tokyo, Japan
[c] College of Science, National University of Defense Technology, Changsha, China

ARTICLE INFO

Article history:
Received 14 April 2010
Received in revised form 8 June 2011
Accepted 8 June 2011

Keywords:
Stream cipher
Rotation symmetry
Boolean function
Algebraic immunity

ABSTRACT

In this paper, we study the construction of Rotation Symmetric Boolean Functions (RSBFs) which achieve a maximum algebraic immunity (AI). For the first time, a construction of balanced $2p$-variable (p is an odd prime) RSBFs with maximum AI was provided, and the nonlinearity of the constructed RSBFs is not less than $2^{2p-1} - \binom{2p-1}{p} + (p-2)(p-3) + 2$; this nonlinearity result is significantly higher than the previously best known nonlinearity of RSBFs with maximum AI.

1. Introduction

The pseudo-random generators using Boolean functions in stream ciphers have been the objects of a lot of cryptanalyses. This has led to efficient implementations of Boolean functions with a large number of variables combined with some desirable properties. But the technology restricts the possibilities. In fact, a Boolean function of 38 input variables, which is rather small, will fit into the largest available physical memory block. Thus we must choose a complex function, which possesses properties that enable a straightforward implementation.

Rotation Symmetric Boolean Functions (RSBFs) represent really good candidates on this point. Boolean functions which are invariant under the action of the cyclic group C_n are called rotation symmetric Boolean functions. These functions have been analyzed in [1] where the authors studied the nonlinearity of these Boolean functions and found encouraging results. This study has been extended in [2,3], and important properties of RSBFs have been demonstrated.

In recent years algebraic attacks [4,5] have become an important tool in cryptanalysis of symmetric cipher systems. A new cryptographic property for designing Boolean functions to resist this kind of attacks, called algebraic immunity (AI), has been introduced [6,7]. Since then several classes of Boolean functions with large AI have been investigated and constructed against the algebraic attack [8–11].

The highest nonlinearity of even-variable RSBFs with maximum AI was presented in [12], where the authors use majority function and toggled its outputs at the inputs of the orbits of weight $\lceil n/2 \rceil$ and $\lfloor n/2 \rfloor$ to obtain RSBFs with nonlinearity higher than $2^n - \binom{n-1}{n/2} + 4$. But [12] cannot provide balanced even-variable RSBFs. We here work in the construction of balanced RSBFs with maximum AI; the nonlinearity of our constructed $2p$-variable RSBFs can be higher than the previous constructions (only our construction ensures balance).

* Corresponding author at: College of Computer, National University of Defense Technology, Changsha, China.
E-mail address: shaojing1984@yahoo.cn (S. Fu).

0893-9659/$ – see front matter
doi:10.1016/j.aml.2011.06.004

2. Preliminaries

An n-variable Boolean function $f(x_1, x_2, \ldots, x_n)$ can be seen as a multivariate polynomial over $\mathbb{F}_2$, that is, $f(x_1, x_2, \ldots, x_n) = \sum_{I \subseteq \{1,2,\ldots,n\}} a_I \prod_{i \in I} x_i$, where $a_I \in \mathbb{F}_2$. The maximum cardinality of I with $a_I \neq 0$ is called the algebraic degree, or simply the degree of f and denoted by $\deg(f)$. The Walsh transform of f is a real-valued function defined as $W_f(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x\cdot w}$, and the nonlinearity of f is defined as

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

The support of f is denoted by $\mathrm{supp}(f) = \{x | f(x) = 1\}$, and the weight of f is the cardinality of $\mathrm{supp}(f)$ (abbr $wt(f)$), and f is called a balanced Boolean function iff $wt(f) = 2^{n-1}$.

A nonzero n-variable Boolean function g is called an annihilator of f if $f * g = 0$, we denote the set of all annihilators of f by $\mathrm{AN}(f)$. The algebraic immunity (AI) of f is defined as $\mathrm{AI}(f) = \min\{\deg(g) | 0 \neq g \in \mathrm{AN}(f) \cup \mathrm{AN}(1+f)\}$. It is known [5] that for any n-variable function, the maximum possible AI is $\lceil n/2 \rceil$.

For $x_i \in \mathbb{F}_2$, we define $\rho_n^k(x_i) = x_{i-k}$ if $i > k$, and $\rho_n^k(x_i) = x_{i+n-k}$ if $i \leq k$. Then we can extend the definition of ρ_n^k on vectors as $\rho_n^k(x_1, \ldots, x_n) = (\rho_n^k(x_1), \ldots, \rho_n^k(x_n))$. And f is called a rotation symmetric Boolean function if and only if $f(\rho_n^k(x_1, x_2, \ldots, x_n)) = f(x_1, x_2, \ldots, x_n)$ for any $0 \leq k \leq n-1$.

Let us define $G_n(x_1, x_2, \ldots, x_n) = \{\rho_n^k(x_1, x_2, \ldots, x_n) | 0 \leq k \leq n-1\}$, that is, the orbit of $(x_1, x_2, \ldots, x_n)$ under the action of ρ_n^k. In [3] it was shown that the Walsh transform of an RSBF f takes the same value for all elements belonging to the same orbit, i.e.,$W_f(u) = W_f(v)$ if $v \in G_n(u)$. For analyzing the Walsh spectrum of RSBFs, the Krawtchouk polynomial should be studied at first. Krawtchouk polynomial [13] of degree i is defined by $K_i(k, n) = \sum_{j=0}^{i} (-1)^j \binom{k}{j} \binom{n-k}{i-j}$. The following lemmas are known results about Krawtchouk polynomial $K_i(x, n)$.

Lemma 1 (*[10]*).
1. *$K_0(k, n) = 1$, $K_1(k, n) = n - 2k$, $\binom{n}{k} K_i(k, n) = \binom{n}{i} K_k(i, n)$;*
2. *For even n,*

$$K_i(n/2, n) = \begin{cases} 0, & i \text{ odd}, \\ (-1)^{i/2} \binom{n/2}{i/2}, & i \text{ even}. \end{cases}$$

Lemma 2 (*[9]*). *The equality $\sum_{i=0}^{r} K_i(k, n) = K_r(k-1, n-1)$ holds for any $0 \leq r \leq n$ and $n, k \geq 1$; If n is even, then $|K_{\frac{n}{2}-1}(k, n-1)| \leq \frac{1}{n-1} \binom{n-1}{n/2}$ holds for any $1 \leq k \leq n-2$.*

3. Construction of balanced 2p-variable RSBFs with maximum AI

From now on, we will assume that $n = 2p$ and p is an odd prime. We start with some basic technical discussion. For any $u \in \mathbb{F}_2^{2p}$, it is clear that the cardinality $|G_n(u)|$ has four values: $1, 2, p, 2p$; and for $wt(u) = p$, the cardinality $|G_n(u)|$ only has two values: $2, 2p$. It is clear that $|G_n(u)| = 2$ if and only if $u = (1, 0, 1, 0, \ldots, 1, 0)$. Now we denoted by Num the number of orbits with cardinality $2p$ and weight p, note that $\mathrm{Num} \cdot 2p + 1 \times 2 = \binom{2p}{p}$, then we have $\mathrm{Num} = \frac{\binom{2p}{p} - 2}{2p}$ and $2 \mid (\mathrm{Num} - 1)$.

Lemma 3. *Let $N = p - 3$ and $v_k \in \mathbb{F}_2^n (1 \leq k \leq N)$, $\mathrm{supp}(v_k) = \left\{1, 2, \ldots, \frac{n}{2} - 1\right\} \cup \{n/2 + k\}$. Then there exists a set $D \subseteq \mathbb{F}_2^{2p} (|D| = \binom{2p}{p}/2 + 2p^2 - 7p - 1)$ such that $\cup_{1 \leq k \leq N} G_n(v_k) \subseteq D$, and for any $x \in D$, $\bar{x} \in D$.*

Proof. Let us denoted by Ω_1 the sets of orbits $\{G_n(x) | \bar{x} \notin G_n(x)\} \cup \{G_n(\bar{x}) | \bar{x} \notin G_n(x)\}$, denoted by Ω_2 the sets of orbits $\{G_n(x) | \bar{x} \in G_n(x)\}$. Denoted by $t_1 = |\Omega_1|/2$, and $t_2 = |\Omega_2|$, then $2t_1 + t_2 = \mathrm{Num}$.

It is easy to show that there exists integer x_1, and x_2 such that $2x_1 + x_2 = \frac{\mathrm{Num}-1}{2} + N$, and we can obtain D by select $2x_1$ orbits from Ω_1 (all $G_n(v_k)$ and $G_n(\bar{v}_k)$ should be chose) and x_2 orbits from Ω_2. Thus, we finish the proof. □

Proposition 4 (*[14]*). *Let n be even and let $a_1, \ldots, a_{\binom{n}{n/2}}$ be an ordering of all vectors of weight $n/2$ in $\mathbb{F}_2^n$. For every $i \in \{1, 2, \ldots, \binom{n}{n/2}\}$, let us denote by A_i the flat $\{x \in \mathbb{F}_2^n | \mathrm{supp}(x) \subseteq \mathrm{supp}(a_i)\}$ and by A_i° the flat $\{x \in \mathbb{F}_2^n | \mathrm{supp}(a_i) \subseteq \mathrm{supp}(x)\}$.*

Let I, J and K be three disjoint subsets of $\{1, 2, \ldots, \binom{n}{n/2}\}$. Assume that, for every $i \in I$, there exists a vector $b_i \neq a_i$ such that $b_i \in A_i \setminus [\cup_{i^* < i} A_{i^*}]$. Assume that, for every $j \in J$, there exists a vector $c_i \neq a_i$ such that $c_i \in A_i^\circ \setminus [\cup_{i^* < i} A_{i^*}^\circ]$.

Then the function with support set $\{x \in \mathbb{F}_2^n | wt(x) > n/2\} \cup \{a_i | i \in J \cup K\} \cup \{b_i | i \in I\} \setminus \{c_i | i \in J\}$ has the maximum AI.

The main purpose of this section is to construct balanced RSBF with maximum AI by Proposition 4. In [9], some constructions to satisfy Proposition 4 have been given. However, their construction cannot give any RSBFs. Before giving