Sufficient conditions of five-valued spectra Boolean functions

Samed Bajrić

JOŽEF STEFAN INSTITUTE
Laboratory for Open Systems and Networks
Ljubljana, Slovenia

20th Central European Conference on Cryptology
June 24–26, 2020, Zagreb, Croatia

Outline

- Short introduction to Boolean functions
- 5-valued spectra Boolean functions
- Infinite families of five-valued spectra Boolean functions

Boolean functions: representation

- A *Boolean function* f in n variables is an $\mathbb{F}_2-$valued function on $\mathbb{F}_2^n$
- Unique representation of f as a polynomial over $\mathbb{F}_2$ in n variables of the form

$$f(x_1, \ldots, x_n) = a_0 + \sum_{1 \leq i \leq n} a_i x_i + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j + \ldots + a_{12\ldots n} x_1 x_2 \ldots x_n,$$

  where $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \mathbb{F}_2$, is called the *algebraic normal form (ANF)* of f

- The *algebraic degree* $deg(f)$ is the degree of the ANF

Boolean functions: representation

- Unique trace expansion of f defined on $\mathbb{F}_{2^n}$ as

$$f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n - 1}), \quad a_j \in \mathbb{F}_{2^{o(j)}},$$

where:

$Tr_1^n(x)$ is the *absolute trace* of x over $\mathbb{F}_{2^n}$ defined by $Tr_1^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}}$, for all $x \in \mathbb{F}_{2^n}$

Γ_n - the set of integers obtained by choosing one element in each cyclotomic coset of 2 modulo $2^n - 1$

$o(j)$ - the size of the cyclotomic coset of 2 modulo $2^n - 1$ containing j

$\epsilon = wt(f)$ modulo 2, where $wt(f) = \#\{x \in \mathbb{F}_{2^n} : f(x) = 1\}$

Boolean functions: cryptographic criteria

- To prevent the system from Massey's attack by the Berlekamp-Massey algorithm, a Boolean function should have a high algebraic degree
- To prevent the system from leaking statistical dependence between the input and output, a Boolean function should be balanced
- To prevent the system from linear attacks and correlation attacks, a Boolean function should be of high nonlinearity
- To prevent the system from algebraic attack, a Boolean function should have an optimal algebraic immunity

Boolean functions: applications

- In cryptography:
  - Ciphers CAST and Grain
  - Hash function HAVAL
- In discrete mathematics:
  - Strongly regular graphs
  - Reed-Muller and Kerdock codes
- In mobile networks:
  - Constant-amplitude codes for Code Division Multiple Access

Boolean functions: Walsh Hadamard transform

- The most important mathematical tool for the study of cryptographic properties of Boolean functions

- *The Walsh Hadamard transform (WHT)* of f is an integer valued function over $\mathbb{F}_2^n$ defined by

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

where $x \cdot \omega = x_1\omega_1 + x_2\omega_2 + \ldots + x_n\omega_n$

- For the Boolean functions defined on $\mathbb{F}_{2^n}$ it is defined by

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\lambda x)}, \qquad \lambda \in \mathbb{F}_{2^n}$$

Boolean functions: Walsh Hadamard transform

- The nonlinearity of $f(x)$ can be obtained via the Walsh transform as

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2}\text{max}_{\omega \in \mathbb{F}_2^n} \mid W_f(\omega) \mid$$

- The nonlinearity of $f(x)$ is always upper bounded by $2^{n-1} - 2^{\frac{n}{2}-1}$
- It can reach this value if and only if n is even, i.e., f is bent
- $f(x)$ is bent if and only if $\mid W_f(\omega) \mid = 2^{\frac{n}{2}}$, for all $\omega \in \mathbb{F}_2^n$

5-valued spectra Boolean functions

- The multiset $\{W_f(\lambda) : \lambda \in \mathbb{F}_{2^n}\}$ is called the Walsh–Hadamard spectrum of the Boolean function f
- If the Walsh Hadamard spectrum takes the values in $\{0, \pm 2^{\lambda_1}, \pm 2^{\lambda_2}\}$, then f is so-called 5-valued spectra Boolean function
- These functions may satisfy multiple cryptographic criteria
- Their design might contribute to a better understanding of other related combinatorial structures

The WHT of $f(x) = g(x) + \prod_{j=1}^{l} Tr_1^n(u_j x)$

Lemma

Let n and l $(l < 2^n - 1)$ be the positive integers and $u_j \in \mathbb{F}_{2^n}^*$, where $j = 1, \ldots, l$. Let $g(x)$ be a Boolean function defined over $\mathbb{F}_{2^n}$. Define the Boolean function $f(x)$ by

$$f(x) = g(x) + \prod_{j=1}^{l} Tr_1^n(u_j x). \tag{1}$$

Then, for every $a \in \mathbb{F}_{2^n}$,

$$\begin{aligned} W_f(a) \quad = \quad & \frac{1}{2^{l-1}}[(2^{l-1}-1)W_g(a) + W_g(a+u_1) + W_g(a+u_2) + \ldots + W_g(a+u_l) - \\ & W_g(a+u_1+u_2) - W_g(a+u_1+u_3) - \ldots - W_g(a+u_{l-1}+u_l) + \\ & W_g(a+u_1+u_2+u_3) + W_g(a+u_1+u_2+u_4) + \ldots + W_g(a+u_{l-2}+u_{l-1}+u_l) \\ & \vdots \\ & +(-1)^{l-1} W_g(a+u_1+\ldots+u_{l-2}+u_{l-1}+u_l)]. \end{aligned}$$

The WHT of $f(x) = g(x) + \prod_{j=1}^{l} Tr_1^n(u_j x)$

Proof.

For $i_1, i_2, \ldots, i_{l-1} \in \{0,1\}$ and $u_j \in \mathbb{F}_{2^n}^*$ define the sets

$$T_{(i_1,i_2,\ldots,i_{l-1})} = \{x \in \mathbb{F}_{2^n} | Tr_1^n(u_1 x) = i_1, Tr_1^n(u_2 x) = i_2, \ldots, Tr_1^n(u_{l-1} x) = i_{l-1}\},$$

and denote

$$S_{(i_1,i_2,\ldots,i_{l-1})}(a) = \sum_{x \in T_{(i_1,i_2,\ldots,i_{l-1})}} (-1)^{g(x)+Tr_1^n(ax)},$$

$$Q_{(i_1,i_2,\ldots,i_{l-1})}(a+u_l) = \sum_{x \in T_{(i_1,i_2,\ldots,i_{l-1})}} (-1)^{g(x)+Tr_1^n((a+u_l)x)}.$$

The Walsh Hadamard transform of $f(x)$ can be computed as

$$\begin{aligned} W_f(a) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(ax)} = \ldots \\ &= W_g(a) - S_{(1,1,\ldots,1,1)}(a) + Q_{(1,1,\ldots,1,1)}(a+u_l). \end{aligned}$$

The WHT of $f(x) = g(x) + \prod_{j=1}^{l} Tr_1^n(u_j x)$

Proof.

Note that

$$W_g(a) = S_{(0,0,\ldots,0,0)}(a) + S_{(0,0,\ldots,0,1)}(a) + \ldots + S_{(1,1,\ldots,1,1)}(a)$$

Similarly, we get

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 & 1 \\ 1 & -1 & 1 & \ldots & 1 & -1 \\ 1 & 1 & -1 & \ldots & -1 & -1 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 1 & -1 & -1 & \ldots & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} S_{(0,0,\ldots,0,0)}(a) \\ S_{(0,0,\ldots,0,1)}(a) \\ S_{(0,0,\ldots,1,0)}(a) \\ \vdots \\ S_{(1,1,\ldots,1,1)}(a) \end{pmatrix} = \begin{pmatrix} W_g(a) \\ W_g(a+u_1) \\ W_g(a+u_2) \\ \vdots \\ W_g(a+u_1+\ldots+u_{l-1}) \end{pmatrix}.$$

The coefficient matrix is a Hadamard matrix of order 2^{l-1}. Since for the Hadamard matrix holds $H \cdot H^T = n \cdot I_n$, we can easily compute $S_{(1,1,\ldots,1,1)}(a)$ and get the final result. □

5-valued spectra functions via Niho bent functions

Theorem

Let $f(x) = g(x) + \prod_{j=1}^{l} Tr_1^n(u_j x)$, *where* $n = 2m$ *is a positive integer,* $l < 2^n - 1, u_j \in \mathbb{F}_{2^n}^*$. *Let* $g(x) = Tr_1^m(\lambda x^{2^m+1}),\ \lambda \in \mathbb{F}_{2^m}^*$ *be the monomial Niho quadratic bent function with the Walsh Hadamard transform given by*

$$W_g(a) = -2^m(-1)^{Tr_1^m(\lambda^{-1}a^{2^m+1})}.$$

If

$$Tr_1^n(\lambda^{-1}u_1^{2^m}u_2) = 1,\ and$$

$$Tr_1^n(\lambda^{-1}u_1^{2^m}u_3) = \ldots = Tr_1^n(\lambda^{-1}u_{l-1}^{2^m}u_l) = 0,$$

then f is a 5-valued spectra function with the Walsh spectrum $\{0, \pm 2^m, \pm 2^{m+1}\}$.

Example I

Let $n = 8$ so that $m = 4$, and $\mathbb{F}_{2^8}$ be generated by the primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$ and α be a primitive element of $\mathbb{F}_{2^8}$.

Take $\lambda = 1, u_1 = \alpha^2, u_2 = \alpha^{10}, u_3 = \alpha^5, u_4 = \alpha^{24}$. Then,

$$Tr_1^8((\alpha^2)^{16}\alpha^{10}) = 1, \;\; Tr_1^8((\alpha^2)^{16}\alpha^5) = Tr_1^8((\alpha^2)^{16}\alpha^{24}) = 0,$$
$$Tr_1^8((\alpha^{10})^{16}\alpha^5) = Tr_1^8((\alpha^{10})^{16}\alpha^{24}) = Tr_1^8((\alpha^5)^{16}\alpha^{24}) = 0.$$

The function

$$f(x) = Tr_1^4(x^{17}) + Tr_1^8(\alpha^2 x)Tr_1^8(\alpha^{10}x)Tr_1^8(\alpha^5 x)Tr_1^8(\alpha^{24}x),$$

is 5-valued with the Walsh spectrum $\{0, \pm 2^4, \pm 2^5\}$.

5-valued spectra functions via Gold-like monomial functions

Theorem

Let $f(x) = g(x) + \prod_{j=1}^{l} Tr_1^n(u_j x)$, *where* $n = 2m$ *is a positive integer,* $l < 2^n - 1, u_j \in \mathbb{F}_{2^n}^*$. *Let* $g(x) = Tr_1^{4m}(\lambda x^{2^m+1})$, *where* $m \geq 2$ *and* $\lambda \in \mathbb{F}_{2^{4m}}^*, \lambda + \lambda^{2^{3m}} = 1$ *be the Gold-like monomial bent function with the Walsh Hadamard transform given by*

$$W_g(a) = 2^{2m}(-1)^{Tr_1^{4m}(\lambda a^{2^m+1})}.$$

If

$$Tr_1^{4m}(\lambda(u_1^{2^m}u_2 + u_1 u_2^{2^m})) = 1, \ and$$

$$Tr_1^{4m}(\lambda(u_1^{2^m}u_3 + u_1 u_3^{2^m})) = \cdots = Tr_1^{4m}(\lambda(u_{l-1}^{2^m}u_l + u_{l-1} u_l^{2^m})) = 0,$$

then f *is a 5-valued spectra function with the Walsh spectrum* $\{0, \pm 2^m, \pm 2^{m+1}\}$.

Example II

Let $n = 8$ so that $m = 2$, and $\mathbb{F}_{2^8}$ be generated by the primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$ and α be a primitive element of $\mathbb{F}_{2^8}$.

Take $\lambda = \alpha^{17}, u_1 = \alpha, u_2 = \alpha^3, u_3 = \alpha^2, u_4 = \alpha^{15}$. Then, $\alpha^{17} + (\alpha^{17})^{2^6} = 1$, and

$$\begin{aligned} Tr_1^8(\alpha^{17}(\alpha^7 + \alpha^{13}) &= 1 \\ Tr_1^8(\alpha^{17}(\alpha^6 + \alpha^{17})) &= Tr_1^8(\alpha^{17}(\alpha^{19} + \alpha^{61}) = Tr_1^8(\alpha^{17}(\alpha^{14} + \alpha^{11})) = \\ Tr_1^8(\alpha^{17}(\alpha^{27} + \alpha^{63})) &= Tr_1^8(\alpha^{17}(\alpha^{23} + \alpha^{62})) = 0. \end{aligned}$$

The function

$$f(x) = Tr_1^8(\alpha^{17}x^5) + Tr_1^8(\alpha x)Tr_1^8(\alpha^3 x)Tr_1^8(\alpha^2 x)Tr_1^8(\alpha^{15}x)$$

is 5-valued with the Walsh spectrum $\{0, \pm 2^4, \pm 2^5\}$.

Further work

- Specify the necessary conditions for constructing 5-valued spectra Boolean functions defined by (1) and their Walsh spectrum distributions.

Hvala za pozornost!

Questions: samed@e5.ijs.si