S-Boxes from Binary Quasi-Cyclic Codes

Dusan Bikov, Iliya Bouyukliev, Stefka Bouyuklieva

Faculty of Mathematics and Informatics, Veliko Tarnovo University
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences

ACCT

June 20, 2016

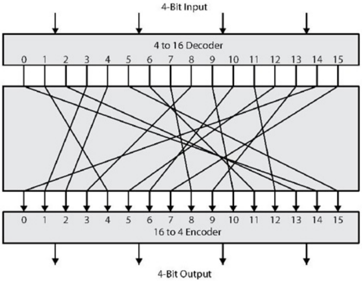
Outline

S-box (or vectorial Boolean function)

Vectorial Boolean function with n inputs and m outputs is

$$S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m.$$

It can be represented by the vector $(f_1, f_2, ..., f_m)$, where f_i are Boolean function in n variables, $i = 1, 2, ..., m$.
The functions f_i are called the coordinate functions of the S-box.



S-box (or vectorial Boolean function)

$$S : \mathbb{F}_2^n \to \mathbb{F}_2^m.$$

$S = (f_1, f_2, ..., f_m)$, where f_i are Boolean function in n variables.
The functions f_i can be represented by their Truth Tables (TT) and then we can consider the S-box S as a matrix

$$G(S) = \begin{pmatrix} TT(f_1) \\ TT(f_2) \\ \dots \\ TT(f_m) \end{pmatrix}$$

Fact.

An S-box S is invertible $\iff$ $m = n$ and the matrix $G(S)$ generates the simplex code S_n with a zero column.

S-box, linearity and nonlinearity

In order to study the cryptographic properties of an S-box related to the linearity, we need to consider all non-zero linear combinations of the coordinates of the S-box, denoted by:

$$S_b = b \cdot S = b_1 f_1 \oplus \cdots \oplus b_m f_m, where \quad b = (b_1, ..., b_m) \in \mathbb{F}_2^m$$

These are the component function of the S-box.

The linearity and nonlinearity of S are defined as:

$$Lin(S) = \max_{b \in \mathbb{F}_2^m \setminus \{0\}} Lin(b \cdot S), \qquad nl(S) = \min_{b \in \mathbb{F}_2^m \setminus \{0\}} nl(b \cdot S).$$

S-box, linearity and nonlinearity

- Linearity $Lin(f)$ of a Boolean function f is the maximum absolute value of an Walsh coefficient of f:

$$Lin(f) = \max_{a \in \mathbb{F}_2^n} |f^W(a)| \geq 2^{n/2}.$$

An Walsh coefficient is defined by

$$f^W(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f_a(x)} = 2^n - 2d_H(f, f_a),$$

where $f_a(x) = a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n$.

- The nonlinearity of a Boolean function f is given by

$$nl(f) = \min\{d_H(f, g) \mid g \ - \ \text{affine function}\} = 2^{n-1} - \frac{1}{2}Lin(f).$$

Obviously, the minimum linearity corresponds to maximum nonlinearity.

Nonlinearity and Walsh spectrum of f from linear codes

$$nl(f) = \min\{d_H(f, g) \mid g \ - \ \text{affine function}\}.$$

The set of the TT of all affine functions coincides with the set of the codewords of Reed-Muller code $RM(1, n)$, with a generator matrix

$$G(RM(1,n)) = \begin{pmatrix} TT(1) \\ TT(x_1) \\ \vdots \\ TT(x_n) \end{pmatrix}.$$

$$\Rightarrow nl(f) = d_H(TT(f), RM(1, n))$$

This means that to find nl and Lin of f we can use algorithms for calculating:

- distance from a vector to a code;
- minimum distance of a linear code.

S-box, differential uniformity

The differential uniformity δ of an $(n \times m)$ S-box S with $n \geq m$, is defined by:

$$\delta = \max_{\alpha \in \mathbb{F}_2^n \setminus \{0\}, \beta \in \mathbb{F}_2^m} |\{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \alpha) = \beta\}|$$

It is the largest value in its difference distribution table (DDT) not counting the first entry in the first row.

S should have a differential uniformity as low as is possible. It is known that $2^{n-m} \leq \delta \leq 2^n$.

For bijective S-boxes $(n = m)$ $\delta \geq 2$.

Summarized results for good 8-bit S-boxes

S-box	NL	DU	AD	Techniques
AES (Daemen et al., 2002)	112	4	7	*
Camellia(Aoki et al., 2001)	112	4	7	*
ARIA (Kwon et al., 2004)	112	4	7	*
HyRAL (Hirata, 2010)	112	4	7	*
Hierocrypt-HL(Ohkuma 2001)	112	4	7	*
CLEFIA-S_1(Shirai et al., 2007)	112	4	7	*
Tran et al., 2008	112	4	7	Gray S-Box
Hussain et al., (2013)	112	4	7	Lin. Fractional Trans.
Li et al., 2012	112	4	5	Conversion $\mathbb{F}_2^9 \rightarrow \mathbb{F}_2^8$
GA2 (Ivanov, Nikolov, Nikova 2016)	112	6	7	Reversed Genetic Algorithms
Yang et al., 2011	112	6	7	**
Yang et al., 2011	110	4	7	**

* Base on Multiplicative Inverse, x^{-1} in $\mathbb{F}_2^8$

** Theorem of Permutation Polynomials

Quasi-Cyclic Codes

A code is said to be quasi-cyclic if every cyclic shift of a codeword by s positions results in another codeword ($s \geq 1$).

$K = \mathbb{F}_{2^n}$ - a finite field, $2^n - 1 = m \cdot r$
α - a primitive element of K, $\beta = \alpha^r$
$\Rightarrow \;\; G = \langle \beta \rangle < K^*$ is a cyclic group of order m,
$G, \alpha G, \alpha^2 G, \ldots, \alpha^{r-1} G$ are all different cosets of G in K^*.

For $a \in \mathbb{Z}_r$ we define the circulant $m \times m$ matrix:

$$C_a = \begin{pmatrix} Tr(\alpha^a) & Tr(\alpha^a \beta) & \cdots & Tr(\alpha^a \beta^{m-1}) \\ Tr(\alpha^a \beta^{m-1}) & Tr(\alpha^a) & \cdots & Tr(\alpha^a \beta^{m-2}) \\ & & \vdots & \\ Tr(\alpha^a \beta) & Tr(\alpha^a \beta^2) & \cdots & Tr(\alpha^a) \end{pmatrix}.$$

The matrices C_a correspond to the different cosets of G in K^*.

Quasi-Cyclic Codes

The code $C(M)$ whose nonzero codewords are the rows of the matrix

$$M = \begin{pmatrix} C_0 & C_1 & \dots & C_{r-1} \\ C_{r-1} & C_0 & \dots & C_{r-2} \\ & & \vdots & \\ C_1 & C_2 & \dots & C_0 \end{pmatrix} \tag{1}$$

is equivalent to the simplex $[2^n - 1 = mr, n, 2^{n-1}]$ code S_n.

We consider the $(2^n - 1) \times 2^n$ matrix $\overline{M} = (0 \ M)$ and its corresponding $[2^n, n, 2^{n-1}]$ code $C(\overline{M}) = (0 \ S_n)$.

Constructions of S-boxes

$$\overline{M} = \left(\begin{array}{cc} 0 & \\ \vdots & M \\ 0 & \end{array} \right), \quad M = \left(\begin{array}{cccc} C_0 & C_1 & \dots & C_{r-1} \\ C_{r-1} & C_0 & \dots & C_{r-2} \\ & & \vdots & \\ C_1 & C_2 & \dots & C_0 \end{array} \right) \sim S_n.$$

Any generator matrix of $C(\overline{M})$ can be considered as an invertible S-box.

Since all these S-boxes generate the same code $C(\overline{M})$, they have the same linearity and nonlinearity.

First construction:

- We take the first ml rows of the matrix $\overline{M}$ such that the obtained matrix G_m has rank n, with one zero column in the beginning.
- Then we investigate all S-boxes $G_m\pi$ where $\pi \in S_r$ is a permutation of the circulants $C_0, C_1, \ldots, C_{r-1}$.

This construction is natural but the second one is more important for us because it gives better results.

Constructions of S-boxes

Second construction:

- Now we consider the matrix:

$$MR = \left(\begin{array}{c|c} 1 & 11\ldots1 \\ \hline 0 & G_m \end{array}\right) \tag{2}$$

  This matrix generates a code which is equivalent to $RM(1,n)$ but has the structure of a quasi-cyclic code.

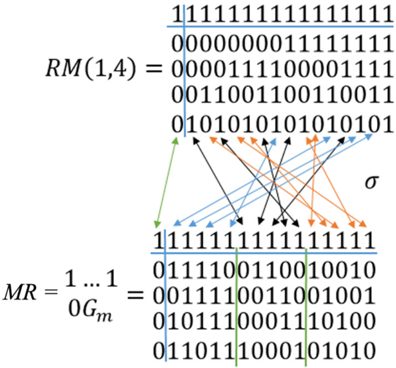
- We again use the matrices $G_m\pi$ but now we compute the minimum distance d of the code generated by the matrix:

$$\left(\begin{array}{c|c} 1 & 11\ldots1 \\ \hline 0 & G_m \\ 0 & G_m\pi \end{array}\right).$$

- If σ is a permutation which maps the Reed-Muller code $RM(1,n)$ to the code with a generator matrix MR then d is the nonlinearity of the S-box represented by the matrix $\sigma^{-1}(G_m\pi)$.

We take the first ml rows of the matrix M (1) such that the obtained matrix G_m has rank $n = 4$:

$$
G_m = \begin{array}{ccc} 30 & 12 & 18 \\ 15 & 6 & 9 \\ 23 & 3 & 20 \\ 27 & 17 & 10 \\ \downarrow & \downarrow & \downarrow \\ C_0 & C_1 & C_2 \end{array} = \begin{array}{c|c|c} 11110 & 01100 & 10010 \\ 01111 & 00110 & 01001 \\ 10111 & 00011 & 10100 \\ 11011 & 10001 & 01010 \\ \downarrow & \downarrow & \downarrow \\ C_0 & C_1 & C_2 \end{array}
$$



If σ is a permutation which maps $RM(1,4) \leftrightarrow \sigma(MR)$, then d is the nonlinearity of the S-box represented by the matrix $\sigma^{-1}(G_m)$.

Algorithm 1. The linearity *Lin* of the S-box

Algorithm 1 Linearity of an S-box

Input: STT - $m \times 2^n$ matrix of TT, coordinate f of $(G_m\pi), \sigma^{-1}(G_m\pi)$
Output: Lin of S-box, or exit if $Lin > BorderLin$

for i from 1 to m do $t[i] \leftarrow i + 1$;
for j from 0 to $2^n - 1$ do $TT[j] \leftarrow 0$ end for;
$i \leftarrow 1; Lin \leftarrow 0$;
while $(i \neq m + 1)$ do
  for j from 0 to $2^n - 1$ do
    $TT[j] \leftarrow TT[j] \oplus STT[i][j]$;
    if $(TT[j] = 1)$ then $PPT[j] \leftarrow -1$ *else* $PPT[j] \leftarrow 1$ end if;
  end for;
FastWalshTransform(PTT);
Lin=FindMaxElementFWT(PTT);
  if($Lin > BorderLin$) then return; end if;
$t[0] \leftarrow 1; t[i-1] = t[i]; t[i] \leftarrow i + 1; i = t[0]$;
end while

The second construction

Using the cyclic structure of the matrices, we can fasten the algorithm for computing the linearity.

Proposition.

Consider the matrices $A = (A_0, A_1, \ldots, A_{r-1})$ and $B = (B_0, B_1, \ldots, B_{r-1})$, where A_i and B_i are $m \times m$ circulant matrices, $i = 0, 1, \ldots, r-1$. If $a_0, a_1, \ldots, a_{m-1}$ are the rows of A, and $b_0, b_1, \ldots, b_{m-1}$ are the rows of B, then $d(a_i, b_j) = d(a_{i+1}, b_{j+1})$ for $0 \leq i, j \leq m-1$ (we consider $i+1$ and $j+1$ modulo m).

Corollary.

The first m coordinate functions of the S-box $\sigma^{-1}(G_m\pi)$ from the second construction have the same Walsh distributions.

Our result

Algorithm 1 - $2^n \times n \times 2^n$ operation
Algorithm 2 - $\frac{2^n}{m} \times n \times 2^n$ operation

For 4 bit S-box ($n = 4$, $m = 5$, $r = 3$) we obtain three optimal S-boxes (according the definition of an optimal S-box[Leander, Poschmann 2007], S is a bijection, $Lin = 8$, $\delta = 4$).

We have done the exhaustive search for $n = 8$, $m = 17$, $r = 15$, the results are presented in the table:

Number of S-box	NL	DU	AD
15	112	4	7
601	108	4, 6	7

Our result

Walsh distribution of the constructed S-box ($n = 8,\ m = 17,\ r = 15$)

32	28	24	20	16	12	8	4	0	-4	-8	-12	-16	-20	-24	-28	-32
1275	2040	5100	4080	4080	4080	5100	4080	4591	8160	4080	6120	4590	2040	4080	2040	0

Also we get S-box for $n = 8,\ m = 15,\ r = 17$ with $nl = 112$ they other properties are not optimal $\delta = 16,\ AD = 5$.
Walsh distribution ($n = 8,\ m = 15,\ r = 17$):

32	16	0	-16
10200	4080	30600	20400

For 16-bit S-box we obtain S-box with $lin = 512$, $nl = 2^{16-1} - \frac{lin}{2} = 32512$

Thank you