Finding an effective metric used for bijective S-Box generation by genetic algorithms

Tsonka Baicheva, Dusan Bikov, Yuri Borissov, Limonka Lazarova,
Aleksandra Stojanova, Liliya Stoykova, Stela Zhelezova

Introduction

In cryptography, S-box is a basic component of symmetric key algorithms which performs nonlinear substitution. S-boxes need to be highly nonlinear, so that the cipher can resist linear cryptanalysis.

Let $B = \{0, 1\}$ and $B^n = \{0, 1\}^n$. Every function $f : B^n \to B$ is called *Boolean function* of n variables:

$$B_n = \{f : B^n \to B\},\ |B_n| = 2^{2^n}.$$

Let f_1, f_2, ..., $f_m \in B_n$. Mapping $F : B^n \to B^m$ defined by the rule:

$$F(x) = (f_1(x), f_2(x), \ldots, f_m(x)),$$

is called *vectorial Boolean function* and f_1, f_2, ..., f_m are its coordinate functions.

S-boxes transform n-binary input into m-binary output. Let S be the substitution table of an n-binary input into m-binary output mapping, that is, if $B = \{0, 1\}$,

$$S : B^n \to B^m,\ x = (x_1, x_2, \ldots, x_n) \to y = (y_1, y_2 \ldots, y_m) = S(x)$$

S can be considered as a vectorial Boolean function, consisting of m individual n-variable Boolean functions f_1, f_2, ..., f_m, referred to as coordinate Boolean functions, where $f_k : B^n \to B$ and $f_k(x) = y_k \in B$, $k = 1, 2, \ldots, m$.

The main cryptographic interest has been with reversible, or *bijective*, S-boxes. An $(n \times n)$ S-box S is called bijective, if S is an invertible mapping over B^n. Bijective S-boxes represent permutations of their 2^n inputs.

For cryptographic Boolean functions, $nl(f)$ must be close to the maximum to prevent the system from attacks by linear approximations, correlation attacks, fast correlation attacks.

A Boolean function f on B_2^n is also uniquely determined by its Walsh-Hadamard transform. The Walsh-Hadamard transform f^W of f is an integer valued function defined by:

$$f^W(a) = \sum_{x \in B_2^n} (-1)^{f(x) + \langle a, x \rangle},$$

where $\langle a, x \rangle$ is scalar product.

Linearity $Lin(f)$ of the Boolean function f is defined by using Walsh-Hadamard transform with the following:

$$Lin\,(f) = \max_{a \in B_2^n} |f^W| \geq 2^{n/2}.$$

Linearity and nonlinearity of a Boolean function are connected by the relation:

$$nl\,(f) = 2^{n-1} - \tfrac{1}{2} Lin(f).$$

Walsh-Hadamard Transform spectrum of $f(x)$ is the set of all 2^n spectral coefficients for the elements in B^n.

WHT Spectrum Matrix is the matrix of WHT spectrum of all coordinate Boolean functions.

An S-box S is referred as a *Bent S-box*, if its WHT Spectrum Matrix is entirely flat. Bent S-box has the highest possible nonlinearity. It itself is not suitable for our purposes – it is not balanced and exists only for even $n \geq 2m$. From now on we will talk about bijective S-boxes.

The main criteria for cryptographically strong $(n \times n)$ S-box are:

- High nonlinearity;
- High algebraic degree;
- Balanced structure;
- Good autocorrelation properties.

Our task was to give some suggestions for finding an effective metric used for generation bijective optimal S-Box. Because of the given problem's complexity, our group considered different approaches and we gave a few suggestions for problem solving.

Group suggestions

Bear in mind given problem we focus on achieving good performance according to the nonlinearity criterion finding S-box close to Bent one.

- Change the initial parent pool

  Genetic algorithms represent the heuristic approaches for S-box generation. Each genetic algorithm start with an initial parent pool of bijective S-boxes, P_1, P_2, ..., P_t,. Till now it is used as P_i random or AES S-boxes.

$$\begin{matrix} b_{0,0} & b_{0,1} & & b_{0,2^n-1} \\ b_{1,0} & b_{1,1} & & b_{1,2^n-1} \\ \vdots & \vdots & \dots & \vdots \\ b_{2^n-1,0} & b_{2^n-1,1} & & b_{2^n-1,2^n-1} \end{matrix}$$

Figure 1: S-box – a vectorial Boolean function

$$\begin{matrix} w_{0,0} & w_{0,1} & & w_{0,2^n-1} \\ w_{1,0} & w_{1,1} & & w_{1,2^n-1} \\ \vdots & \vdots & \dots & \vdots \\ w_{2^n-1,0} & w_{2^n-1,1} & & w_{2^n-1,2^n-1} \end{matrix}$$

Figure 2: WHT Spectrum Matrix of S

We propose exponential S-boxes as the initial parent pool. Exponential S-boxes are proven to have good cryptographic properties [1].

- Change the cost function

  In genetic algorithms it's necessary to be able to evaluate how *good* a potential solution is relative to other potential solutions. The *fitness function* is responsible for performing this evaluation and returning a *fitness value*, that reflects how optimal the solution is. In the considered algorithm fitness value is based on two functions: fitness – measuring S-box nonlinearity and cost – measuring flatness of WHT Spectrum Matrix, i.e. how close is it to Bent one. For now cost function is evaluated by:

$$\sqrt[p]{\sum_{j=0}^{2^n-1} |w_{i,j} - w_{i,j+1}|^p}$$

  for $p \geq 1$. The lower its value is the better the solution is.

  ◦ The cost function can be computed by using the maximum of the differences between the spectral coefficients of each coordinate function.

  Let Δ_i be the maximal difference of $i^{-\text{th}}$ coordinate:

$$\Delta_i = \{|w_{i,j} - w_{i,j+k}| : j \in (0, 2^n - 1), j + k \leq 2^n - 1\}.$$

  We can calculate the maximal difference for given S-box as:

$$\Delta_S = \max \Delta_i,\ i \in (1, 2^n - 1).$$

WHT Spectrum Matrix of Bent S-box is entirely flat, so $\Delta_{Bent} = 0$. If $\Delta_{S_1} \approx \Delta_{S_2}$ then the second condition can be used. The vectors of maximal differences for two S-boxes (Δ_1, Δ_2,..., Δ_{2^n-1}) of S_1 and (Δ_1, Δ_2,..., Δ_{2^n-1}) of S_2 are considered and the $\Delta_i = 0$ values are counted and the S-box which has more $\Delta_i = 0$ is chosen as a good one.

◦ Another cost function can be computed by using the dispersion of the WHT spectrum of each coordinate function. Statistical dispersion is zero if all the data are the same and increases as the data become more diverse.

Let a_0, a_1,..., a_{2k} be possible values of the WHT spectrum matrix and $p_{i,j}$ be the probability of appearing a_j in the i^{-th} column. Then the mathematical expectation is

$$E(w_i) = \sum_{j=0}^{2k} a_j p_{i,j}.$$

The dispersion of the i^{-th} column of the WHT matrix with respect to the bent WHT Spectrum ($2^{\frac{n}{2}}$) is:

$$D(w_i) = E(w_i^2) - (2^{\frac{n}{2}}) = \sum_{j=0}^{2k} a_j^2 p_{i,j} - 2^n.$$

The dispersion of the S-Box is:

$$D(S) = \frac{1}{2^n - 1} \sum_{i=1}^{2^n-1} D(w_i).$$

Smaller dispersion means flatter spectrum and better S-box.

- Examine smaller S-Boxes

  Natural requirement for 4 bit S-boxes is an optimal resistance against linearity and differential cryptoanalysis.The optimal values for $Lin(S)$ and $Diff(S)$ are known for dimension $n = 4$, but they aren't determined for higher dimension. More precisely, for any bijective mapping $S : B_2^4 \to B_2^4$ we have $Lin(S) \geq 8$ and $Diff(S) \geq 4$.

  Our suggestion is to examine the behavior of the genetic algorithm on 4×4 S-boxes and compare the results with the already known optimal ones [3].

This can give verification of the method and some suggestions for the cost function.

- New approach

  It is considered Quasigroups as a tool for construction of optimal S-boxes.

  Let $(Q, *)$ be a finite binary groupoid, i.e. an algebra with one binary operation $*$ on the non-empty set Q and $a, b \in Q$. A finite binary groupoid $(Q, *)$ is called a quasigroup if for all ordered pairs $(a, b) \in Q$ there exist unique solutions $x, y \in Q$ of the equations $x * a = b$ and $a * y = b$. This implies the cancellation laws for quasigroup i.e. $x * a = x' * a \Rightarrow x = x'$ and $a * y = a * y' \Rightarrow y = y'$.

  Any quasigroup is possible to be presented as a multiplication table known as Cayley table. Removing the topmost row and the leftmost column of the Cayley table of a quasigroup, results in a Latin square.

  Assuming that $(Q, *)$ is a given quasigroup, for a fixed element $l \in Q$, called leader, the transformation $e_l : Q^r \to Q^r$ is as follows:

$$e_l\left(a_0, a_1, \ldots, a_{r-1}\right) = \left(b_0, b_1, \ldots, b_{r-1}\right) \Leftrightarrow \begin{cases} b_0 = l * a_0 \\ b_i = b_{i-1} * a_i, 1 \leq i \leq r-1 \end{cases}.$$

  The representation of finite quasigroups $(Q, *)$, of order n, where $n \geq 2$ and $n = 2d$ as vector valued Boolean functions, can be used. Every Boolean function $f : F_2^m \to F_2$, can be uniquely written in its Algebraic Normal Form (ANF), by which the algebraic degree can be immediately read off. According to their algebraic degree quasigroups can be divided in two classes, class of linear quasigroups and class of non-linear quasigroups. The class of linear quasigroups has a maximal algebraic degree 1, and all other quasigroups (which maximal algebraic degree is bigger than 1) belong to the class of non-linear.

  Our suggestion is to consider quasigroups as a tool for construction of optimal S-boxes. An algorithm for construction of optimal 4×4 S-box already exists [2]. Cryptographically strong $6 \times 4, 8 \times 8$ and other types of S-boxes could be produced by extending the above algorithm. First, the number of rounds and leaders which are necessary to produce Q-S-boxes with the same quality as already known ones, should be obtained and then, should be determined which of them belong to the class of optimal ones regarding to linear and differential characteristics of S-boxes.

Conclusions

S-boxes play a fundamental role for the security of nearly all modern block ciphers. They are basically used to hide the relationship between the plain text and the cipher text. The S-boxes form the only non-linear part of a block cipher. Therefore, S-boxes have to be chosen carefully to make the cipher resistant against all kinds of attacks. In particular there are well studied criteria that a good S-box has to fullfill to make the cipher resistant against diferential, linear and algebraic cryptoanalyses.

An open problem in cryptography is finding an $(n \times n)$ bijective S-box with nonlinearity nl bounded above by $2^{n-1} - 2^{\frac{n}{2}-1}$, where n is even, to prevent the system from attacks by linear approximations, correlation attacks, fast correlation attacks etc. The proposed problem is in close relation with this, so it is also very difficult problem for solving (AES have $n = 8$ and it is not clear that this kind S-box can be optimal in this dimension). We hope our work helps for moving things a little bit forward.

References

[1] S. Agievich, A. Afonenko, Exponential S-boxes, Cryptology ePrint Archive, Report 2004/024 (2004).

[2] D.Gligoroski, H.Mihajloska, Construction of Optimal 4-bit S-boxes by Quasigroups of Order 4, SECURWARE 2012, The Sixth International Conference on Emerging Security Information, Systems and Technologies (2012), 163–168.

[3] G. Leander, A. Poschmann, On the Classification of 4 Bit S-Boxes, In: Arithmetic of Finite Fields, Lecture Notes in Computer Science Volume 4547 (2007), 159–176.