On some methods for constructing almost optimal S-Boxes and their resilience against side-channel attacks

Reynier Antonio de la Cruz Jiménez

Institute of Cryptography, Havana University, Cuba.

djr.antonio537@gmail.com

Abstract

Substitution Boxes (S-Boxes) are crucial components in the design of many symmetric ciphers. The security of these ciphers against linear, differential, algebraic cryptanalyses and side-channel attacks is then strongly dependent on the choice of the S-Boxes. To construct S-Boxes having good resistive properties both towards classical cryptanalysis as well side-channel attacks is not a trivial task. In this article we propose new methods for generating S-Boxes with strong cryptographic properties and therefore study the resilience of such S-Boxes against side-channel attacks in terms of its theoretical metrics and masking possibility.

Keywords: S-Box, permutations, hamming weight, nonlinearity, differential uniformity, graph algebraic immunity, differential power analysis, transparency order, confusion coefficient, signal-to-noise ratio.

1 Introduction

Modern block ciphers are often iterations of several rounds. Each round (which must depend on the key) consists of a confusion layer and a diffusion layer. The confusion layers are usually formed by local nonlinear mappings (S-Boxes) while the diffusion layers are formed by global linear mappings mixing the output of the different S-Boxes. Block ciphers can be built using a well-known structure such as a Feistel network (and its variants) (see,e.g. [2]), a Substitution-Permutation network (SPN) [43], or a Lai-Massey structure [55]. Cryptographic properties of S-Boxes deal with the application of several logical attacks on ciphers, namely linear attack [34], the differential attack [34], the higher order differential attack [37] and algebraic attack [16] (which is not yet efficient but represents some threat and should keep in mind by designers of next generation of block ciphers). For this reason S-Boxes must satisfy various criteria for providing high level of protection against such attacks.

Besides the linear, differential and algebraic attacks, today the most prominent attacks on the cryptographic algorithms are based on supervision of physical processes in cryptographic device. In literature, this kind of attack has received the name of side-channel attacks (SCAs). Examples of such attacks are: Simple Power Analysis (SPA) [35], Differential Power Analysis (DPA) [35], Timing Analysis (TA) [36] , Correlation Power Analysis (CPA) [10], Mutual Information Attack (MIA)[18]. S-Boxes represent the most vulnerable part in an implementation when considering side-channel adversary and it is not a trivial task to construct S-Boxes having good resistive properties both towards classical cryptanalysis as well side-channel attacks.

The known methods for constructing S-Boxes can be divided into four main classes: algebraic constructions, pseudo-random generation, heuristic techniques and constructions from small to large S-Boxes. Each approach has its advantages and disadvantages respectively (see, e.g. [11, 30]). Motivated by specialist's work of Luxembourg's university Alex Biryukov, Léo Perrin and Aleksei Udovenko on cryptanalysis of the only known solution to the big APN problem [9] we propose (using the last approach) new constructions for generating S-Boxes with strong cryptographic properties and therefore study their resilience against side-channel attacks in terms of its theoretical metrics and masking possibility.

This article is structured as follows: In Section 2 we give the basic definitions. In Section 3 we present our design criteria and new methods for constructing S-Boxes with strong cryptographic properties. An algorithm to generate 8-bit permutations having strong properties and good theoretical DPA metrics, is presented in Section 4. In Section 5 we compare our

S-Boxes with other from the perspective of conventional cryptanalysis and theoretical DPA metrics. The possibility of combine our S-Boxes with the masking countermeasure against SCAs is studied in Section 6. Our work is concluded in Section 7.

2 Basic definitions and notations

Let V_n be n-dimensional vector space over the field GF(2), by $S(V_n)$ we denote the symmetric group on set of 2^n elements. The finite field of size 2^n is denoted by GF(2^n), where GF(2^n)=GF(2)[ξ]/$g(\xi)$, for some irreducible polynomial $g(\xi)$ of degree n. We use the notation $\mathbb{Z}/2^n$ for the ring of the integers modulo 2^n. There are bijective mappings between $\mathbb{Z}/2^n, V_n$ and GF(2^n) defined by the correspondences:

$$\left[a_{n-1} \cdot 2^{n-1} + \ldots + a_0\right] \quad \leftrightarrow \quad (a_{n-1}, \ldots, a_0) \quad \leftrightarrow \quad \left[a_{n-1} \cdot \xi^{n-1} + \ldots + a_0\right].$$

Using these mapping in what follows we make no difference between vectors of V_n and the corresponding elements in and $\mathbb{Z}/2^n$ and GF(2^n).

Throughout the article, we shall use the following operations and notations:

$a\|b$ - concatenation of the vectors a, b of V_l, i.e. a vector from V_{2l} ;
0 - the null vector of V_l ;
$\oplus$ - bitwise eXclusive-OR. Addition in GF(2^l);
$< a, b >$ - the scalar product of vectors $a = (a_{l-1}, \ldots, a_0), b = (b_{l-1}, \ldots, b_0)$ of V_l and is equal to $< a, b >= a_{l-1}b_{l-1} \oplus \ldots \oplus a_0b_0$;
$gcd(a, b)$ - the greatest common divisor of integers a and b;
$w_H(a)$ - the Hamming weight of a binary vector $a \in V_l$, i.e. the number of its nonzero coordinates;
$\otimes$ - finite field multiplication ;
$\Lambda \circ \Psi$ - a composition of mappings, where Ψ is the first to operate;
Ψ^{-1} - the inverse transformation to some bijective mapping Ψ.

Now, we introduce some basic concepts needed to describe and analyze S-Boxes with respect to linear, differential, algebraic attack and DPA attacks. For this purpose, we consider an n-bit S-Box Φ as a vector of Boolean functions:

$$\Phi = (f_{n-1}, \ldots, f_0), f_i : V_n \to V_1, i = 0, 1, \ldots n - 1. \tag{1}$$

For some fixed $i = 0, 1, \ldots, n-1$, every Boolean function f_i can be written as a sum over V_1 of distinct t-order products of its arguments, $0 \leq t \leq n-1$; this is called the algebraic normal form of f_i. Functions f_i are called coordinate Boolean functions of the S-Box Φ and it is well known that most of the desirable cryptographic properties of Φ can be defined in terms of their linear combinations (also-called S-Box component Boolean functions).

Definition 1. For each vector $a \in V_n$ the The Walsh-Hadamard transform $\mathcal{W}_f(a)$ of the n-variable Boolean function f is defined as

$$\mathcal{W}_f(a) = \sum_{x \in V_n} (-1)^{f(x) \oplus <a,x>}. \tag{2}$$

Definition 2. The nonlinearity $\mathcal{NL}(f)$ of the n-variable Boolean function f is defined as

$$\mathcal{NL}(f) = \min_{g \in \mathcal{A}_n} w_H(f \oplus g), \tag{3}$$

where $\mathcal{A}_n$ is the set of all n-variable affine Boolean functions and $w_H(f \oplus g)$ is the Hamming weight of the n-variable Boolean function $f \oplus g$. The nonlinearity $\mathcal{NL}(f)$ can be expressed as follows:

$$\mathcal{NL}(f) = 2^{n-1} - \frac{1}{2} \max_{a \in V_n \setminus \{0\}} |\mathcal{W}_f(a)| \tag{4}$$

Definition 3. For $a, b \in V_n$ the Walsh transform $\mathcal{W}_\Phi(a, b)$ of an n-bit S-Box Φ is defined as

$$\mathcal{W}_\Phi(a, b) = \sum_{x \in V_n} (-1)^{<b, \Phi(x)> \oplus <a,x>}. \tag{5}$$

Definition 4. The nonlinearity of an n-bit S-Box Φ, denoted by $\mathcal{NL}(\Phi)$, is defined as

$$\mathcal{NL}(\Phi) = \min_{a \in V_n \setminus \{0\}} \{\mathcal{NL}(a_{n-1} f_{n-1} \oplus \ldots \oplus a_0 f_0)\}, \tag{6}$$

where $\mathcal{NL}(a_{n-1}f_{n-1} \oplus \ldots \oplus a_0 f_0)$ is the nonlinearity of each of the component Boolean functions excluding the zero one.
The nonlinearity $\mathcal{NL}(\Phi)$ of an arbitrary n-bit S-Box Φ can be calculated as follows

$$\mathcal{NL}(\Phi) = 2^{n-1} - \frac{1}{2} \cdot \max_{a \neq 0, b \in V_n} |\mathcal{W}_{\Phi}(a, b)|. \tag{7}$$

From a cryptographic point of view S-Boxes with small values of Walsh coefficients offer better resistance against linear attacks.

Definition 5. The differential uniformity of an n-bit S-Box Φ, denoted by δ_Φ, is defined as

$$\delta_\Phi = \max_{a \neq 0, b \in V_n} \delta(a, b), \tag{8}$$

where $\delta(a, b) = |\{x \in V_n | \Phi(x \oplus a) \oplus \Phi(x) = b\}|$.

The resistance offered by an S-Box against differential attacks is related by the highest value of δ, for this reason S-Boxes must have a small value of δ-uniformity for a sufficient level of protection against this type of attacks.

The algebraic degree of the Boolean functions $f : V_n \to V_1$, denoted by $\deg f$, is the maximum order of the terms appearing in its algebraic normal form.

Definition 6. The minimum degree of an S-Box Φ, denoted by $\deg(\Phi)$, is defined as

$$\deg(\Phi) = \min_{a \in V_n \setminus \{0\}} \{\deg(a_{n-1}f_{n-1} \oplus \ldots \oplus a_0 f_0)\}. \tag{9}$$

In general, S-Boxes should have high minimum degree because S-Boxes with low degree are susceptible to algebraic attack, higher-order differential, interpolation, cube attacks etc.

Definition 7. The univariate polynomial representation of an n-bit S-Box Φ over $\mathrm{GF}(2^n)$, is defined in a unique fashion as

$$\Phi(X) = \sum_{i=0}^{2^n-1} \nu_i X^i, \nu_i \in \mathrm{GF}(2^n), \tag{10}$$

where coefficients $\nu_i, i = 0, \ldots, 2^n - 1$ can be obtained from the n-bit S-Box Φ by applying Lagrange's Interpolation theorem (see,[13],[49]).

Definition 8. Let U be a non-empty subset of V_{2n}, then the annihilating set of U is defined as $\{p \in \mathrm{GF}(2)[z_1, \ldots, z_{2n}] | p(U) = 0\}$.

Definition 9. The algebraic immunity of U is defined as

$$\mathcal{AI}(U) = \min \Big\{ \deg p \Big| 0 \neq p \in \mathrm{GF}(2)[z_1, \ldots, z_{2n}], p(U) = 0 \Big\}.$$

Definition 10. The graph algebraic immunity of n-bit S-Box Φ, denoted by $\mathcal{AI}_{gr}(\Phi)$, is defined as

$$\mathcal{AI}_{gr}(\Phi) = \min \Big\{ \deg p \Big| 0 \neq p \in \mathrm{GF}(2)[z_1, \ldots, z_{2n}], p(gr(\Phi)) = 0 \Big\}, \quad (11)$$

where $gr(\Phi) = \{(x, \Phi(x)) | x \in V_n\} \subseteq V_{2n}$.

Thus we focus on the graph algebraic immunity of S-Box Φ and also on the parameter $r_{\Phi}^{(AI_{gr}(\Phi))}$ referred to as the number of all the independent equations in input and output values of the S-Box Φ, i.e., equations of the form $p(x, \Phi(x)) = 0 \; \forall x \in V_n$.

Definition 11. An element $a \in V_n$ is called a fixed point of an n-bit S-Box Φ if $\Phi(a) = a$.

Definition 12. Two n-bit S-Boxes Φ_1 and Φ_2 are affine/linear equivalent if there exist a pair of invertible affine/linear permutation $A_1(x)$ and $A_2(x)$, such that $\Phi_1(x) = A_2 \circ \Phi_2 \circ A_1(x)$.

Definition 13. The Transparency Order of an S-Box Φ, denoted by $\mathsf{TO}(\Phi)$, is defined as

$$\begin{aligned} \mathsf{TO}(\Phi) = \max_{b \in V_n} \Big(& |n - 2w_H(b)| - \frac{1}{2^{2n} - 2^n} \times \\ & \sum_{a \in V_n \setminus \{0\}} \Big| \sum_{c \in V_n, w_H(c)=1} (-1)^{<c,b>} \mathcal{W}_{\Phi(x) \oplus \Phi(x \oplus a)}(0, c) \Big| \Big). \end{aligned} \quad (12)$$

The smaller the transparency order metric, the higher is its resistance the S-Box Φ to DPA attacks.

Definition 14. The DPA Signal-to-Noise Ratio of an S-Box Φ, denoted by $\mathsf{SNR(DPA)}(\Phi)$, is defined as

$$\mathsf{SNR(DPA)}(\Phi) = n 2^{2n} \Big(\sum_{a \in V_n} \Big(\sum_{i=0}^{n-1} \mathcal{W}_{f_i}(a) \Big)^4 \Big)^{-\frac{1}{2}}, \quad (13)$$

where $f_i, i = 0, \ldots, 7$ are the coordinate Boolean functions of the S-Box Φ.

The $\mathsf{SNR}(\mathsf{DPA})$, proper to each S-Box Φ, fully characterizes the DPA discrimination power. The lower the $\mathsf{SNR}(\mathsf{DPA})$ metric of Φ , the better resistance to DPA attacks.

Definition 15. The confusion coefficient of of an S-Box Φ, denoted by $\mathsf{CC}(\Phi)$, is defined as

$$\mathsf{CC}(\Phi) = \sigma^2[\overline{\kappa}] = \sigma^2[\kappa(k_i, k_j) | \forall i < j], \tag{14}$$

where $\sigma^2[\cdot]$ is the variance, $\overline{\kappa}$ denote the list $[\kappa(k_i, k_j) | \forall i < j]$, $\kappa(k_i, k_j) = \mathrm{E}_p\Big[\Big(\mathrm{L}(\Phi(k_i \oplus p)) - \mathrm{L}(\Phi(k_i \oplus p))^2\Big)\Big]$, k_i and k_j are the i-th and the j-the value of the key, p - is some known plaintext, L represents the leakage function and E is the mean operator.

According to [45], the S-Box Φ with higher $\mathsf{CC}(\Phi)$ metric leads to a higher resistance against SCAs.

3 General S-Box Design Criteria

Our goal is to find bijective S-Boxes that satisfy the following criteria (which in what follows are called almost optimal):

1. Absence of fixed points;
2. Maximum value of minimum degree ;
3. Maximum graph algebraic immunity with the minimum number of equations;
4. Minimum value of δ-uniformity limited by parameter listed above;
5. Maximum value of nonlinearity limited by parameter listed above.

For example,when $n = 8$ an almost optimal permutation Φ without fixed points has:

- $\deg(\Phi) = 7$;
- $\mathcal{AI}_{gr}(\Phi) = 3$ with $r_\Phi^{(3)} = 441$;
- $\delta_\Phi \leq 8$;
- $\mathcal{NL}(\Phi) \geq 100$.

Also, we concentrate on generating 8-bit almost optimal S-Boxes that have good values of transparency order property, $\mathsf{SNR}(\mathsf{DPA})$ and confusion coefficient respectively. By good values, we mean such values that are better than those found in currently used 8-bit S-Boxes. Although it is well known that, improving the aftermentioned metrics is a good defense strategy, we do recognize that this cannot be counted as a countermeasure (see, [14]). Thus, we are looking for 8-bit S-Boxes having good resistive properties both towards classical cryptanalysis as well side-channel attacks with some given level of masking.

3.1 Constructing almost optimal S-Boxes from smaller ones and finite field multiplication

Now, we present some methods for constructing S-Boxes having almost optimal cryptographic properties using smaller ones and finite field multiplication. In cryptography, it is very common to build an S-Box from smaller ones, usually an 8-bit S-Box from variuos 4-bit S-Boxes. Several S-Boxes of block ciphers have been designed in this fashion (see, [4, 5, 21, 46, 51, 52]). In many cases, such a structure is used not only to allow an efficient implementation of the S-Box in software (hardware) or using a bit-sliced approach, but also to protect S-Boxes implemented in this way against SCAs. The implementation cost of our S-Boxes in hardware is outside the scope of this work. The main components that we need for constructing ours S-Boxes are described below

Let be $n = 2k$ a natural number, where $k \geq 2$. Choosing:

- The permutation polynomial (PP) $\mathcal{P}_d(x) = x^d$ over $GF(2^k)$ (denoting for the sake of simplicity $\mathcal{I} = \mathcal{P}_{2^k-2}(x)$) where d is a positive integer such that $gcd(d, 2^k - 1) = 1, d \neq 1, 2^s$ and $s < k$;
- Non-bijective k-bit funtions ψ, ψ_1, ψ_2 which have no pre-image for 0;
- Arbitrary permutations $h, h_1, h_2 \in S(V_k)$.

We construct the following $2k$-bit vectorial Boolean functions $\mathcal{F}, \mathcal{G}, \mathcal{H}$ from V_{2k} to V_{2k} as follows

Construction of $\mathcal{F}$

For the input value $(l\|r) \in V_{2k}$ we define the corresponding output value $\mathcal{F}(l\|r) = (l_1\|r_1)$ where,

$$l_1 = \mathcal{P}_d(l \otimes \psi_1(r));$$
$$r_1 = h(r) \otimes \psi_2(l_1).$$

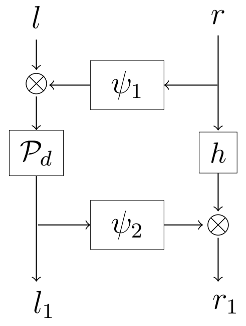

Figure 1: High level structure of $\mathcal{F}$

Construction of $\mathcal{G}$

For the input value $(l\|r) \in V_{2k}$ we define the corresponding output value $\mathcal{G}(l\|r) = (l_1\|r_1)$ where,

$$l_1 = h(l \otimes \psi(l \otimes r));$$
$$r_1 = \mathcal{I}(r) \otimes \psi(l \otimes r).$$

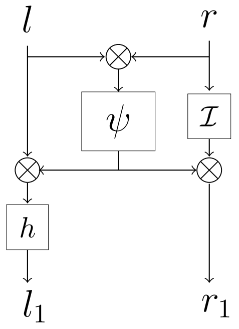

Figure 2: High level structure of $\mathcal{G}$

Construction of $\mathcal{H}$

For the input value $(l\|r) \in V_{2k}$ we define the corresponding output value $\mathcal{H}(l\|r) = (l_1\|r_1)$ where,

$$l_1 = \begin{cases} h_1(l), & \text{if } r = 0; \\ \mathcal{P}_d(l \otimes r), & \text{if } r \neq 0; \end{cases}$$
$$r_1 = \begin{cases} h_2(r), & \text{if } l_1 = 0; \\ l_1 \otimes \mathcal{P}_d(r), & \text{if } l_1 \neq 0. \end{cases}$$

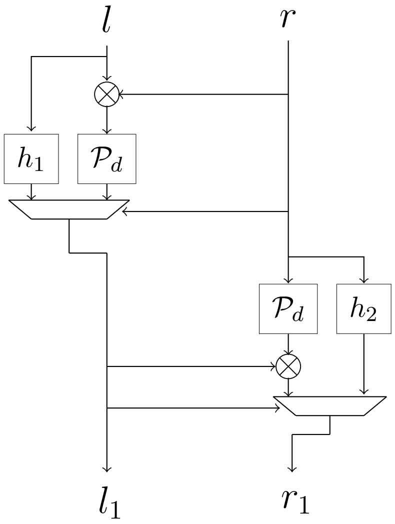

Figure 3: High level structure of $\mathcal{H}$

As shown in Figure 1, the construction of $\mathcal{F}$ is similar to a 2-round combination of a Misty-like and Feistel structure where the XORs have been replaced by finite field multiplications. Figure 2 shows us, that the construction of $\mathcal{G}$ share similarities with 1-round Lai-Massey structure replacing in the latter the XORs by finite field multiplications. The high level structure of $\mathcal{H}$ is shown at Figure 3, as we can see, the construction of $\mathcal{H}$ represent a particular version of $\mathcal{F}$ which has some advantages over the latter (see, Section 4.1). The non-bijective k-bit functions $\psi, \psi_i, i = 1, 2$ (which have no pre-image for 0) and the special nonlinear components of $\mathcal{H}$ where chosen in such a way to make all these structures invertible. Moreover, from the next constructions:

- $\mathcal{F}^{-1}(l_1 \| r_1) = l \| r$ where $r = h^{-1}(r_1 \otimes \mathcal{I}(\psi_2(l_1))), l = \mathcal{P}_d(l_1) \otimes \mathcal{I}(\psi_1(r))$;
- $\mathcal{G}^{-1}(l_1 \| r_1) = l \| r$ where $l = h^{-1}(l_1) \otimes \mathcal{I}(\psi(h^{-1}(l_1) \otimes \mathcal{I}(r_1)))$,
  $r = \mathcal{I}(r_1 \otimes \mathcal{I}(\psi(h^{-1}(l_1) \otimes \mathcal{I}(r_1))))$;
- $\mathcal{H}^{-1}(l_1 \| r_1) = l \| r$ where $r = \left\{ \begin{array}{ll} h_2^{-1}(r_1), & \text{if } l_1 = 0; \\ l_1 \otimes \mathcal{P}_d(r_1), & \text{if } l_1 \neq 0; \end{array} \right., l = \left\{ \begin{array}{ll} h_1^{-1}(l_1), & \text{if } r = 0; \\ \mathcal{P}_d(l_1 \otimes r), & \text{if } r \neq 0. \end{array} \right.$

we can easy derive the bijectivity of the S-Boxes $\mathcal{F}, \mathcal{G}, \mathcal{H}$ which is a necessary design criteria for SPN ciphers and quite useful for Feistel and Lai-Massey ciphers.

4 Generating almost optimal 8-bit S-Boxes having good theoretical DPA metrics

When $n = 8$, in correspondence with the suggested constructions of $\mathcal{F}, \mathcal{G}, \mathcal{H}$ we need to construct; the 4-bit non-bijective functions $\psi, \psi_i, i = 1, 2$, the 4-bit permutations $h, h_i, i = 1, 2 \in S(V_4)$ and the PP $\mathcal{P}_d(x) = x^d$ over GF(2^4) where $d \in \{7, 11, 13, 14\} \setminus \{1, 2, 4, 8\}$. Taking into account that in GF(2^4), the values of d are all in the same cyclotomic class (notice that for $n > 4$ this fact is not always true) in what follows we shall work with the inversion function $\mathcal{I}$ over the finite field GF(2^4)=GF(2)[ξ]/$g(\xi)$, constructing the latter with the irreducible polynomial $g(\xi) = \xi^4 + \xi + 1$.

The main advantage offered by constructions of $\mathcal{F}, \mathcal{G}$ and $\mathcal{H}$ is that its allows to perform a search based on random generation of 4-bit non-bijective functions and 4-bit permutations for finding almost optimal 8-bit S-Boxes having good theoretical DPA metrics. For this purpose we propose the following generic algorithm:

Step 1. Select one of the three constructions $\mathcal{F}, \mathcal{G}$ or $\mathcal{H}$;

Step 2. In dependency of the selected construction, generate randomly the 4-bit components (ψ_1, ψ_2, h) or (ψ, h) or (h_1, h_2);

Step 3. For already generated 4-bit components, (ψ_1, ψ_2, h) or (ψ, h) or (h_1, h_2) construct the S-Box;

Step 4. Test this permutation for all criteria 1-5. If the choosen substitution satisfies all of them except criterion 1 then go to **Step 5**. Otherwise repeat **Step 2**;

Step 5. Apply affine/linear equivalence to the obtained permutation in order to achieve the required property 1;

Step 6. Compute the parameters $\mathsf{TO}, \mathsf{SNR}(\mathsf{DPA}), \mathsf{CC}$ for the S-Box obtained in the previous step. If $(\mathsf{TO} < 7.860)\&(\mathsf{SNR}(\mathsf{DPA}) < 9.600)\&(\mathsf{CC} > 0.111)$ then go to **Step 7**. Otherwise repeat **Step 2**;

Step 7. Output of the algorithm. A nonlinear bijective mapping with the desired properties.

Let us point out that the values of transparency order, SNR(DPA) and confusion coefficient specified in the step 6 of the previous algorithm were select in such a way to ensure that our S-Boxes have at least better theoretical DPA metrics than the AES's S-Box.

Our algorithm was implemented in SAGE [50] and has been applied to a large number of random 4-bit permutations and random non-bijective 4-bit functions (which have no pre-image for 0). As a result we have obtained affine nonequivalent almost optimal 8-bit permutations based on construction of $\mathcal{F}$ without fixed points with the following parameters

- minimum degree — 7;
- graph algebraic immunity — 3 (with 441 equations);
- 8 — uniform;
- nonlinearity in range of 100 up to a value of 104.

While the construction of $\mathcal{G}$ is able to produce almost optimal afine nonequivalent 8-bit S-Boxes without fixed points with

- minimum degree — 7;
- graph algebraic immunity — 3 (with 441 equations);
- 6 and 8 — uniform;
- nonlinearity in range of 100 up to a value of 104.

The best result have been achieved by the construction of $\mathcal{H}$, which generate almost optimal affine nonequivalent 8-bit S-Boxes without fixed points having the parameters listed below

- minimum degree — 7;
- graph algebraic immunity — 3 (with 441 equations);
- 6 and 8 — uniform;
- nonlinearity in range of 100 up to a value of 108.

Some 8-bit permutations generated by constructions of $\mathcal{F}, \mathcal{G}$ and $\mathcal{H}$ in correspondence with the previous algorithm have been listed in the appendix section. These S-Boxes exhibit good theoretical DPA metrics.

4.1 Relations, advantages and disadvantages between and $\mathcal{H}$

As stated in Section 3.1 the construction of $\mathcal{H}$ represent a version of $\mathcal{F}$ which has some advantages and disadvantages over $\mathcal{F}$. In fact, directly from these constructions we can easy obtain that, when $h = \mathcal{P}_d, \psi_1(z) = \psi_2(z) = \left\{ \begin{smallmatrix} c, \text{if } z = 0; \\ z, \text{if } z \neq 0. \end{smallmatrix} \right.$, $c \in \mathrm{GF}(2^k)\backslash\{0\}$, the constructions of $\mathcal{F}$ and $\mathcal{H}$ are the same, when in the latter $h_1(z) = \mathcal{P}_d(z \otimes c), h_2(z) = \mathcal{P}_d(z) \otimes c$. From practical point of view the main difference between these structures comes from the cryptographic quality of the permutations that they produce. For example, when $n = 8$ we have no found any S-Box generated by $\mathcal{F}$ with graph algebraic immunity — 3 and nonlinearity more than 104 while the construction of $\mathcal{H}$ does it, solving at the same time the open question raised in [32] about existence of such permutations. It shoult be noted that even when the construction of $\mathcal{H}$ can be weak against SCAs due to the use of an "if" operation (see, [27, 28, 35]) we can apply the Cycloatomic or Parity-Split methods described in [13] for masking 8-bit S-Boxes generated by $\mathcal{H}$ in GF(2^8). However, due to its multiplicative complexity (33 and 22 nonlinear field multiplications respetively) in GF(2^8) the issue of finding more efficient methods of masking for construction of $\mathcal{H}$ is left as future work.

5 Comparing our S-Boxes with other from the perspective of conventional cryptanalysis and theoretical side-channel metrics

In Table 1 we show the cryptographic parameters on some classes of currently 8-bit S-Boxes used in different modern block ciphers. As it can be seen the Scream S-Box highlight the best values of transparency order, SNR(DPA) and confusion coefficient respectively. It should be noted that the Scream cipher was designed to be side-channel resistant with masking (see, [23]). However, this S-Box is not almost optimal with respect the chosen criteria decribed in Section 3. Only Kuznyechik and Belt (relaxing slightly the condition on the minimum degree) S-Boxes satisfies our design criteri. But even when these permutations have good theoretical DPA metrics at the time of writing we have no found any dth-order ($d > 1$) masked version of aftermentioned S-Boxes in the public available literature. However, in [38] was proposed a method of masking which can be applied to any SPN block cipher and therefore the whole Kuznyechik cipher can be protected using this approach or using the Cycloatomic or Parity-Split methods [13] for masking the Kuznyechik S-Box. The remainder S-Boxes compiled in this table can be masking using different methods described in [15, 21, 33, 46].

In Table 2 we compare our results with the state-of-the-art in design of cryptographically strong S-Boxes obtained by different available methods. This comparison shows that our construction produces 8-bit permutations with the same properties reported in [1, 17, 20, 29, 30, 32, 39, 40, 41, 53] and other with the best parameters reported in the public available literature for nonlinearity and graph algebraic immunity respectively. Table 2 also shows that our S-Boxes have better resistence to algebraic and DPA at-

S-Boxes class/Cryptographic properties	Bijection	$\mathcal{NL}$	δ	deg	$\mathcal{AI}_{gr}\left(r^{(\mathcal{AI}_{gr})}\right)$	TO	SNR(DPA)	CC
AES S-Box [43]	Yes	112	4	7	2(39)	7.860	9.600	0.111
Belt S-Box [6]	Yes	102	8	6	3(441)	7.833	8,318	0.169
Clefia S-Box S_0 [52]	Yes	100	10	6	3(441)	7.745	9.662	0.109
FOX S-Box [54]	Yes	96	16	6	3(441)	7.788	9.342	0.121
Iceberg S-Box [51]	Yes	96	8	7	3(441)	7.812	10.254	0.089
Khazad S-Box [4]	Yes	96	8	7	3(441)	7.80	8.860	0.141
Kuznyechik S-Box [25]	Yes	100	8	7	3(441)	7.835	9.571	0.112
Picaro S-Box [46]	No	94	4	2	3(441)	7.843	8.557	0.147
Scream S-Box [23]	Yes	96	8	6	3(441)	7.589	7.921	0.194
Zorro S-Box [21]	Yes	96	10	6	3(441)	7.806	9.260	0.124

Table 1: Crytptographic parameters on some classes of currently used 8-bit S-Boxes

Methods/Cryptographic properties	$\mathcal{NL}$	δ	deg	$\mathcal{AI}_{gr}\left(r^{(\mathcal{AI}_{gr})}\right)$	TO	SNR(DPA)	CC
Gradient descent method [32]	104	8	7	3(441)	7.823	9.208	0.149
GA/HC [41]	100	NR	NR	NR	NR	NR	NR
GaT [53]	104	NR	NR	NR	NR	NR	NR
GA1 [31]	106	6	6	2(32)	7.850	9.458	0.108
	108	6	6	2(34)	7.849	9.768	0.119
GA2 [31]	110	6	7	2(36)	7.855	9.850	0.109
	112	6	7	2(38)	7.858	9,866	0.118
Hill Climbing [40]	100	NR	NR	NR	NR	NR	NR
Hybrid Heuristic Methods [29]	102	6	4	3(441)	7.833	8.650	0.102
	104	6	4	3(441)	7.824	8.467	0.108
Simulated Annealing [17]	102	NR	NR	NR	NR	NR	NR
SpImmAlg [30]	104	6	7	3(441)	7.822	9.038	0.128
Spectral-linear and spectral-difference methods [39]	104	6	7	3(441)	NR	NR	NR
Tweaking [20]	106	6	7	2(27)	7.854	9.481	NR
S-Box $\mathcal{F}_1$ [this work]	100	8	7	3(441)	7.780	5.873	0.402
S-Box $\mathcal{F}_2$ [this work]	102	8	7	3(441)	7.758	6.384	0.331
S-Box $\mathcal{G}_1$ [this work]	104	8	7	3(441)	7.786	7.400	0.230
S-Box $\mathcal{G}_2$ [this work]	104	6	7	3(441)	7.800	8.380	0.165
S-Box $\mathcal{H}_1$ [this work]	106	6	7	3(441)	7.834	8.644	0.152
S-Box $\mathcal{H}_2$ [this work]	108	6	7	3(441)	7.838	9.335	0.121

Table 2: A comparison between the cryptographic properties of 8-bit permutations produced by different modern generation methods (NR means "not reported")

tacks in terms of graph algebraic immunity, transparency order, SNR(DPA) and confusion coefficient than other permutations while having comparable classical cryptographic properties.

6 Higher-Order Masking of 8-bit S-Boxes obtained by construction of $\mathcal{F}$ and $\mathcal{G}$

In this section we study the possibility of combine ours 8-bit S-Boxes having almost optimal cryptographic properties and good values of transparency order, SNR(DPA) and confusion coefficient with the classical masking countermeasure against SCAs. The principle of the so-called masking scheme is to randomly split every sensitive intermediate variable occurring in the computation into $d+1$ shares, where d is called the masking order and plays the role of a security parameter.

In connection with [13], to design a higher-order masking scheme for any n-bit S-Box Φ, we need to express it as a sequence of field multiplications and additions over GF(2^n). This representation is based on four kinds of operations over GF(2^n): additions, scalar multiplications, squares, and nonlinear multiplications. Masking is efficient for the three first kinds, the latter operations are linear (resp. affine) over V_n, and in this case the masking overhead will solely correspond to d times the original operation complexity. In the case of nonlinear multiplications, the masking scheme is more expensive: it costs $(d+1)^2$ field multiplications, $2d(d+1)$ XORs and the generation of $d(d+1)/2$ random n-bit values. Masking an n-bit S-Box Φ processing can hence be done by masking every affine function and every nonlinear multiplication independently. We refers to [13] for a detailed explanation of how this can be done for each category. As defined in [13], the masking complexity of any n-bit S-Box Φ, denoted by $\mathcal{MC}(\Phi)$, is the minimal number of nonlinear multiplications required to evaluate its polynomial representation over GF(2^n). Denoting by $\mathcal{M}_k^n$ as the class of exponents α such that X^α has a masking complexity equal to k we summarizes in Table 3 the results (obtained in [13]) for the cyclotomic classes $C_\alpha = \{\alpha \cdot 2^j \mod (15) \,|\, j = 0, 1, 2, 3.\}$ in $\mathcal{M}_k^4$.

k	Cyclotomic classes in $\mathcal{M}_k^4$
0	$C_0 = \{0\}, C_1 = \{1, 2, 4, 8\}$
1	$C_3 = \{3, 6, 12, 9\}, C_5 = \{5, 10\}$
2	$C_7 = \{7, 11, 13, 14\}$

Table 3: Cyclotomic classes for $n = 4$ w.r.t. the masking complexity k.

S-Boxes should have a simple expression as a polynomial in order to be efficiently masked (see, [46, 21]). Keeping our design criteria described in Section 3 and choosing in the suggested constructions (in the first two) $h = \mathcal{I}$ we obtain the following two candidates which are not expressed directly as a polynomial of the form (7), but as the concatenation two bivariate functions over GF(2^4):

1. $\mathcal{F}_3(l\|r) = \left(\left(l \otimes \psi_1(r)\right)^{14}\Big\|\left(r^{14} \otimes \psi_2((l \otimes \psi_1(r))^{14}\right)\right) \oplus 6,$

2. $\mathcal{G}_3(l\|r) = \left(\left(l \otimes \psi(l \otimes r)\right)^{14}\Big\|\left(r^{14} \otimes \psi(l \otimes r)\right)\right) \oplus 252,$

where the 4-bit non-bijective functions ψ_1, ψ_2 and ψ (which have no preimage for 0) having the following polynomial representations $\psi_1(X) = 1+11X+6X^2+3X^3+12X^4+12X^6+6X^8+X^9+X^{12}, \psi_2(X) = 14+X+14X^{15}$ and $\psi(X) = 4 + X + 13X^2 + 11X^3 + X^{14}$ were randomly generated. It can be easily checked that ψ_1, ψ_2 and ψ can be computed with 1,3 and 2 field multiplications respectively. We summarizes in Table 4, the values obtained for $\mathcal{MC}(\mathcal{F}_3)$ and $\mathcal{MC}(\mathcal{G}_3)$ and the look-up tables of these S-Boxes and its cryptographic parameters are listed in the appendix section.

	# nonl. multiplications	# additions	# squarings	# random 4-bit values
Unmasked $\mathcal{F}_3$	10	8	8	0
Unmasked $\mathcal{G}_3$	9	3	4	0
dth-order masked $\mathcal{F}_3$	$10(d+1)^2$	$(20d+8)(d+1)$	8(d+1)	5d(d+1)
dth-order masked $\mathcal{G}_3$	$9(d+1)^2$	$(18d+3)(d+1)$	4(d+1)	$\frac{9}{2}d(d+1)$

Table 4: Number of operations

Taking into account that the number of field of multiplications for any 4-bit non-bijective function and any 4-bit permutation is lower bounded by 0 and upper bounded by 3,4 respectively (see, [13]), we obtain the following bounds for 8-bit S-Boxes produced by construction of $\mathcal{F}$ and $\mathcal{G}$:

$$4 \leq \# \text{ nonl. mult. of } \mathcal{F} \leq 15, 5 \leq \# \text{ nonl. mult. of } \mathcal{G} \leq 12. \tag{15}$$

As we can see from (15), 8-bit S-Boxes with only 4 and 5 nonlinear multiplications over GF(2^4) can be constructed using the schemes of $\mathcal{F}$ and $\mathcal{G}$ respectively, but our experiments have shown that these permutations are not almost optimal with respect to the chosen criteria.

Finally, in Table 5 we compare our results with some candidates having a given level of masking. As we can see our S-Boxes exhibits better values of fields multiplications than S-Boxes of Clefia, Iceberg and Khazad respectively, having at the same time stronger cryptographic properties but

S-Box class	# nonl. multiplications
AES's S-Box [21] AES's S-Box [33]	4 (GF(2^8)) 5 (GF(2^4))
Clefia S-Box [15]	10 (GF(2^8))
Iceberg S-Box [21]	18 (GF(2^4))
Khazad S-Box [21]	18 (GF(2^4))
Picaro S-Box [46]	4 (GF(2^4))
Zorro S-Box [21]	4 (GF(2^4))
$\mathcal{F}_3$ S-Box [this work]	10 (GF(2^4))
$\mathcal{G}_3$ S-Box [this work]	9 (GF(2^4))

Table 5: Comparison of 8-bit S-Boxes w.r.t. # nonl. multiplications.

at the cost of a worse number of nonlinear multiplications compared with the AES [33], Picaro [46] and Zorro S-Boxes [21].

7 Conclusion

In this work we have presented some new schemes based on the well-known Feistel and Lai-Massey structures for constructing S-Boxes of dimension $n = 2k, k \geq 2$. The main cores of our constructions are: the inversion in GF(2^k), the k-bit non-bijective functions (which have no pre-image for 0) and the k-bit permutations. Combining these components with the finite field multiplication, we provide new cryptographically strong 8-bit S-Boxes having good values of transparency order, $\mathsf{SNR}(\mathsf{DPA})$, confusion coefficient and acceptable masking complexity over GF(2^4) respectively. There are several questions (theoretical results, hardware and bit-sliced implementations, efficient methods of masking) about the constructions suggested in this work which are left as future work.

References

[1] Agievich S., Afonenko A.: Exponential s-boxes. Cryptology ePrint Archive, Report 2004/024, 2004. http://eprint.iacr.org/2004/024.

[2] Avanzi R. A Salad of Block Ciphers.: The State of the Art in Block Ciphers and their Analysis. Cryptology ePrint Archive, Report 2017/1171, 2017. http://eprint.iacr.org/2017/1171.

[3] Armknecht, F., Krause, M.: Constructing single and multioutput Boolean functions with maximal algebraic immunity. In: Bugliesi, M., Preneel, B., Sassone, V.,Wegener, I. (eds.) ICALP 2006, Part II. of LNCS, vol. 4052, pp. 180-191. Springer,Heidelberg (2006).

[4] Barreto, P., Rijmen, V.: The Khazad legacy-level block cipher. Primitive submitted to NESSIE (2000).

[5] Barreto, P., Rijmen, V.: The Whirlpool hashing function. In: First open NESSIE Workshop, Leuven, Belgium. Volume 13. (2000)

[6] Belarusian State University, National Research Center for Applied Problems of Mathematics and Informatics. "Information technologies. Data protection. Cryptographic algorithms for encryption and integrity control.". State Standard of Republic of Belarus (STB 34.101.31-2011), 2011.

[7] Biryukov, A., De Cannière, C.: Block ciphers and systems of quadratic equations.In: Johansson, T. (ed.) FSE. 2003. of LNCS, vol. 2887, pp. 274-289. Springer, Heidelberg (2003)

[8] Biryukov, A., Perrin L., and Udovenko A.: Reverse engineering the S-Box of streebog, kuznyechik and STRIBOBr1. In Marc Fischlin and Jean-Sébastien Coron, editors, Advances in Cryptology - EUROCRYPT 2016, Part I, volume 9665 of LNCS, pages 372-402. Springer, Heidelberg, May 2016.

[9] Biryukov, A., Perrin L., and Udovenko A.: Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem. In Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II,pages 93-122, 2016.

[10] Brier E., Clavier C., and Olivier F.: Correlation Power Analysis with a Leakage Model // Proceedings of Cryptographic Hardware and Embedded Systems 2004, LNCS 2004, p. 157-173, Springer-Verlag, 2004.

[11] Canteaut, A., Duval, S., Leurent, G.: Construction of Lightweight S-Boxes using Feistel and MISTY structures. In Dunkelman, O., Keliher, L., eds.: Selected Areas in Cryptography 2015. of LNCS. Springer International Publishing (2015).

[12] Carlet, C.: Vectorial Boolean functions for cryptography. Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge University Press, 2010.

[13] Carlet c Goubin L., Prouff E., Quisquater M., and Rivain M.: Higher-order masking schemes for s-boxes. In Anne Canteaut, editor, FSE, volume 7549 of LNCS, pages 366-384. Springer, 2012.

[14] Chakraborty K., Sarkar S., Maitra S., Mazumdar B. Mukhopadhyay D., Prouff E.: Redefining the transparency order. Cryptology ePrint Archive, Report 2014/367, 2014. http://eprint.iacr.org/2014/367.

[15] Coron J.S, Roy A., and Vivek S.: Fast evaluation of polynomials over binary finite fields and application to side-channel countermeasures. CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings, pages 170-187, 2014.

[16] Courtois, N. T., and Pieprzyk, J.: Cryptanalysis of Block Ciphers with Overdefined Systems of Equations, http://eprint.iacr.org/2002/044/,2002.

[17] Clark J.A., Jacob J.L., and Stepney S.: The design of s-boxes by simulated annealing. New Generation Computing Archive, 23(3), September 2005.

[18] Gierlichs B., Batina L., Tuyls P. , and Preneel B.: Mutual information analysis // International Workshop Cryptographic Hardware and Embedded System , p. 426-442., 2008.

[19] Feistel H.: Cryptography and computer privacy. Scientific American, 228(5):15-23, 1973.

[20] Fuller J. and Millan W.: Linear redundancy in s-boxes. In FSE'03, volume 2887 of of LNCS, pages 74-86.Springer, 2003.

[21] Gérard, B., Grosso, V., Naya-Plasencia, M., Standaert, F.X.: Block ciphers that are easier to mask: how far can we go? In: Cryptographic Hardware and Embedded Systems-CHES 2013. Springer (2013) 383-399.

[22] Grosso V., Leurent G., Standaert, F.X., Varici K.: LS-designs: Bitslice encryption for efficient masked software implementations. In Carlos Cid and Christian Rechberger, editors, FSE 2014, volume 8540 of LNCS, p 18-37. Springer, Heidelberg, March 2015.

[23] Grosso V., Leurent G., Standaert, F.X., Varici K, Journault F.D.A., Gaspar L., and Kerckhof S.: SCREAM & iSCREAM Side-Channel Resistant Authenticated Encryption with Masking. Candidate for the CAESAR Competition. See also http://perso.uclouvain.be/fstandae/SCREAM/, 2014.

[24] Golić J. Dj.: Fast low order approximation of cryptographic functions. In Advances in Cryptology EUROCRYPT'96, volume 1070 of of LNCS, p.p 268-282. Springer Verlag, 1996.

[25] GOST R 34.11-2012 Information technology. Cryptographic protection of information. Hash function. Moscow, Standartinform, 2012.

[26] Guilley S., Hoogvorst P. and Pacalet R.: Differential power analysis modeland some results. In CARDIS, pages 127-142, 2004.

[27] Hodgers P., Regazzoni F., Gilmore R., Moore C. , Oder T.: Safe Crypto. Secure Architectures of Future State-of-the-Art in Physical Side-Channel Attacks and Resistant Technologies Emerging cryptography. Report by European Commission.

[28] Hogenboom J.: Principal Component Analysis and Side-Channel Attacks - Master Thesis.

[29] Isa H., Jamil N., and Z'aba M. (2016).: Hybrid Heuristic Methods in Constructing Cryptographically Strong S-boxes. International Journal of Cryptology Research 6(1): (2016)

[30] Ivanov G., Nikolov N., and Nikova S.: Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm. Cryptography and Information Security in the Balkans Volume 9540 of the series of LNCS pp 31-42.

[31] Ivanov G, Nikolov N., and Nikova S.: Reversed genetic algorithms for generation of bijective S-Boxes with good cryptographic properties. IACR Cryptology ePrint Archive (2014), Report 2014/801, http://eprint.iacr.org/2014/801.pdf.

[32] Kazymyrov O.V., Kazymyrova V.N., Oliynykov R.V.: A method for generation of high-nonlinear S-Boxes based on gradient descent, Mathematical Aspects of Cryptography, 2014, Volume 5, Issue 2, pp. 71-78.

[33] Kim H., S. Hong, and J. Lim.: A fast and provably secure higher-order masking of AES s-box. In B. Preneel and T. Takagi, editors. CHES 2011 - 13th International Workshop, Nara, Japan. Proceedings, volume 6917 of LNCS. Springer, 2011,pages 95-107.

[34] Kim J.: Combined Differential, Linear and Related-Key Attacks on Block Ciphers and MAC Algorithms. IACR Cryptology ePrint Archive (2006), Report 2006/451,http://eprint.iacr.org/2006/451.pdf.

[35] P. Kocher, Jaffe J., and Jun B.: Introduction to Differential Power Analysis and Related Attacks Technical Report // Cryptography Research Inc., 1998. Available athttp://www.cryptography.com/resources/whitepapers/DPA-technical.html

[36] Paul C. Kocher.: Timing attacks on implementations of Diffie-Hellman,RSA, DSS and other systems // In Neal Koblitz, editor, Advances in Cryptology - Proceedings of CRYPTO 1996, number 1109 in LNCS, 104-113. Springer-Verlag, 1996.

[37] Knudsen, L. R.: Truncated and Higher Order Differentials. In FSE, B. Preneel,Ed., vol. 1008 of of LNCS. Springer Berlin Heidelberg, 1995, pp. 196-211.

[38] Matveev, S. GOST 28147-89 masking against side channel attacks. In: Pre-proceedings of CTCrypt'14-Moscow, Russia.

[39] Menyachikhin A.: Spectral-linear and spectral-difference methods for generating cryptographically strong S-Boxes. In: Pre-proceedings of CTCrypt'16-Yaroslavl, Russia, 2016. p.232-252.

[40] Millan W.: How to improve the nonlinearity of bijective s-boxes. In Australian Conference on Information Security and Privacy 1998, volume 1438, pages 181-192. Springer Verlag, 1998.

[41] Millan W., L. Burnett, G. Carter, A. Clark, and E. Dawson.: Evolutionary heuristics for finding cryptographically strong s-boxes. In ICICS'99, volume 1726 of of LNCS, pages 263-274. Springer, 1999.

[42] Millan W. L.: Low order approximation of cipher functions. In Cryptography: Policy and Algorithms Conference, Proceedings, volume 1029 of of LNCS, pp. 144-155. Springer Verlag, 1996.

[43] NIST. Advanced Encryption Standard. Federal Information Processing Standard (FIPS) 197,November 2001.

[44] Nyberg K.: Differentially uniform mappings for cryptography. In Helleseth, T. (ed.), Advances in Cryptology - EUROCRYPT'93, vol.765 of of LNCS, pp. 55-64. Springer Berlin Heidelberg, 1994.

[45] Picek S., K. Papagiannopoulos K., Ege B., Batina L., and Jakobovic D.:"Confused by confusion: Systematic evaluation of DPA resistance of various s-boxes", in Progress in Cryptology - INDOCRYPT 2014 - 15th International Conference on Cryptology in India, New Delhi, India, December 14-17, 2014, Proceedings, ser.LNCS, W. Meier and D. Mukhopadhyay, Eds., vol. 8885. Springer,2014, pp. 374-390.

[46] Piret G., Roche T,, and Carlet C.: PICARO - a block cipher allowing efficient higher-order side-channel resistance. In Feng Bao, Pierangela Samarati, and Jianying Zhou, editors, ACNS, volume 7341 of Lecture Notes in Computer Science, pages 311-328. Springer, 2012.

[47] Prouff E.: DPA Attacks and S-boxes. In FSE, pages 424-441, 2005.

[48] Leander G., Poschmann A.: On the classification of 4 bit S-Boxes. of LNCS, 2007, vol. 4547, pp. 159-176.

[49] Lidl, R., and Niederreiter, H.: Finite Fields,vol. 20 of Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.

[50] Sage Mathematics Software (Version 8.1). (2018) http://www.sagemath.org.

[51] Standaert, F.X., Piret, G., Rouvroy, G., Quisquater, J.J., Legat, J.D.: ICEBERG : An Involutional Cipher Efficient for Block Encryption in Reconfigurable Hardware. In Roy B., Meier W., eds. FSE. Volume 3017 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2004) 279-298.

[52] Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA. In FSE, Springer (2007) 181-195

[53] Tesař P.: A New Method for Generating High Non-linearity S-Boxes. Radioengineering - 2010. V. 19, NO. 1. - p. 23-26.

[54] Vaudenay S., Junod P.: Device and method for encrypting and decrypting a block of data. United States Patent (20040247117), see also ”Fox, a New Family of Block Ciphers” http://crypto.junod.info/sac04a.pdf, 2004.

[55] Xuejia Lai and James L. Massey.: A proposal for a new block encryption standard. In Ivan Damgard, editor, Advances in Cryptology EUROCRYPT’ 90, volume 473 of LNCS, pages 389-404. Springer, Heidelberg, May 1991.

8 Appendix

8.1 Some S-Boxes generated by our constructions

<table>
<tr><th colspan="16">S-Box $\mathcal{F}_1$</th><th colspan="16">S-Box $\mathcal{F}_2$</th></tr>
<tr><td colspan="16">$\mathcal{NL}(\mathcal{F}_1) = 100, \delta(\mathcal{F}_1) = 8, \deg(\mathcal{F}_1) = 7, \mathcal{AI}_{gr}(\mathcal{F}_1) = 3, r_{\mathcal{F}_1}^{(3)} = 441,$
$\mathsf{TO}(\mathcal{F}_1) = 7.780, \mathsf{SNR(DPA)}(\mathcal{F}_1) = 5.873, \mathsf{CC}(\mathcal{F}_1) = 0.402$</td><td colspan="16">$\mathcal{NL}(\mathcal{F}_2) = 102, \delta(\mathcal{F}_2) = 8, \deg(\mathcal{F}_2) = 7, \mathcal{AI}_{gr}(\mathcal{F}_1) = 3, r_{\mathcal{F}_1}^{(3)} = 441$
$\mathsf{TO}(\mathcal{F}_2) = 7.758, \mathsf{SNR(DPA)}(\mathcal{F}_2) = 6.384, \mathsf{CC}(\mathcal{F}_2) = 0.331$</td></tr>
<tr><td>f1</td><td>fa</td><td>fd</td><td>f9</td><td>f7</td><td>f8</td><td>f5</td><td>fe</td><td>f2</td><td>f4</td><td>fc</td><td>f0</td><td>f3</td><td>fb</td><td>ff</td><td>f6</td><td>cf</td><td>c6</td><td>c2</td><td>c8</td><td>c0</td><td>c3</td><td>c5</td><td>cc</td><td>c1</td><td>ce</td><td>c9</td><td>c4</td><td>ca</td><td>cd</td><td>c7</td><td>cb</td></tr>
<tr><td>a1</td><td>87</td><td>dc</td><td>d6</td><td>15</td><td>dd</td><td>e6</td><td>90</td><td>ee</td><td>8d</td><td>30</td><td>e4</td><td>ba</td><td>54</td><td>98</td><td>3e</td><td>ef</td><td>f1</td><td>74</td><td>bd</td><td>56</td><td>7e</td><td>6d</td><td>fd</td><td>88</td><td>64</td><td>fb</td><td>0b</td><td>43</td><td>46</td><td>4d</td><td>00</td></tr>
<tr><td>41</td><td>e8</td><td>89</td><td>6f</td><td>6c</td><td>93</td><td>d4</td><td>c0</td><td>ef</td><td>5d</td><td>c3</td><td>ea</td><td>6b</td><td>5a</td><td>9c</td><td>ab</td><td>df</td><td>0a</td><td>1e</td><td>9b</td><td>e1</td><td>47</td><td>84</td><td>8b</td><td>6b</td><td>40</td><td>4b</td><td>0d</td><td>a7</td><td>9a</td><td>a2</td><td>8e</td></tr>
<tr><td>c1</td><td>08</td><td>18</td><td>06</td><td>2f</td><td>b3</td><td>b2</td><td>36</td><td>1e</td><td>13</td><td>9e</td><td>d9</td><td>d2</td><td>4d</td><td>3b</td><td>05</td><td>3f</td><td>09</td><td>a9</td><td>4c</td><td>58</td><td>8d</td><td>d3</td><td>a1</td><td>83</td><td>16</td><td>57</td><td>59</td><td>d9</td><td>b7</td><td>de</td><td>41</td></tr>
<tr><td>31</td><td>52</td><td>28</td><td>eb</td><td>6e</td><td>75</td><td>26</td><td>c8</td><td>2e</td><td>60</td><td>73</td><td>c5</td><td>64</td><td>aa</td><td>46</td><td>a4</td><td>5f</td><td>3d</td><td>d0</td><td>ea</td><td>97</td><td>87</td><td>fc</td><td>f6</td><td>77</td><td>a5</td><td>e7</td><td>8c</td><td>ab</td><td>82</td><td>ed</td><td>75</td></tr>
<tr><td>e1</td><td>a8</td><td>24</td><td>27</td><td>04</td><td>ad</td><td>d3</td><td>47</td><td>0a</td><td>43</td><td>76</td><td>bc</td><td>b8</td><td>50</td><td>a9</td><td>49</td><td>9f</td><td>5a</td><td>28</td><td>19</td><td>25</td><td>5e</td><td>b4</td><td>67</td><td>b5</td><td>18</td><td>04</td><td>2c</td><td>ee</td><td>b6</td><td>85</td><td>e5</td></tr>
<tr><td>71</td><td>80</td><td>0e</td><td>d7</td><td>8c</td><td>cc</td><td>e7</td><td>96</td><td>1f</td><td>10</td><td>9f</td><td>d5</td><td>e2</td><td>85</td><td>19</td><td>3a</td><td>2f</td><td>f3</td><td>11</td><td>54</td><td>e4</td><td>1c</td><td>53</td><td>5d</td><td>89</td><td>a3</td><td>f0</td><td>eb</td><td>13</td><td>3e</td><td>80</td><td>6c</td></tr>
<tr><td>21</td><td>86</td><td>8b</td><td>e3</td><td>1a</td><td>9a</td><td>e0</td><td>97</td><td>69</td><td>16</td><td>37</td><td>de</td><td>34</td><td>33</td><td>45</td><td>99</td><td>0f</td><td>61</td><td>91</td><td>5b</td><td>24</td><td>79</td><td>63</td><td>51</td><td>95</td><td>60</td><td>d1</td><td>f5</td><td>3b</td><td>38</td><td>9d</td><td>20</td></tr>
<tr><td>91</td><td>00</td><td>2c</td><td>0f</td><td>0c</td><td>b5</td><td>2b</td><td>3f</td><td>66</td><td>a7</td><td>70</td><td>b9</td><td>79</td><td>23</td><td>4b</td><td>44</td><td>1f</td><td>52</td><td>7c</td><td>49</td><td>0c</td><td>dc</td><td>f7</td><td>db</td><td>d5</td><td>2b</td><td>4e</td><td>ec</td><td>e9</td><td>f8</td><td>08</td><td>e6</td></tr>
<tr><td>51</td><td>17</td><td>12</td><td>df</td><td>be</td><td>da</td><td>bb</td><td>48</td><td>03</td><td>8a</td><td>b7</td><td>7d</td><td>db</td><td>4f</td><td>38</td><td>3c</td><td>8f</td><td>b3</td><td>a8</td><td>45</td><td>93</td><td>7d</td><td>2e</td><td>ad</td><td>d2</td><td>f2</td><td>96</td><td>f9</td><td>be</td><td>71</td><td>ae</td><td>fe</td></tr>
<tr><td>61</td><td>0b</td><td>1b</td><td>e5</td><td>14</td><td>bf</td><td>d0</td><td>42</td><td>0d</td><td>40</td><td>3d</td><td>4a</td><td>d8</td><td>35</td><td>32</td><td>a3</td><td>7f</td><td>b1</td><td>b8</td><td>6a</td><td>68</td><td>aa</td><td>dd</td><td>e8</td><td>33</td><td>15</td><td>9c</td><td>1d</td><td>b9</td><td>31</td><td>d8</td><td>6e</td></tr>
<tr><td>d1</td><td>a0</td><td>5c</td><td>2d</td><td>6a</td><td>7e</td><td>62</td><td>cb</td><td>2a</td><td>88</td><td>57</td><td>7c</td><td>b0</td><td>a5</td><td>a2</td><td>55</td><td>6f</td><td>55</td><td>d4</td><td>2a</td><td>35</td><td>37</td><td>5c</td><td>73</td><td>3a</td><td>22</td><td>d6</td><td>86</td><td>23</td><td>8a</td><td>bb</td><td>4a</td></tr>
<tr><td>b1</td><td>1c</td><td>58</td><td>6d</td><td>8e</td><td>ce</td><td>67</td><td>82</td><td>ed</td><td>53</td><td>cf</td><td>78</td><td>e9</td><td>83</td><td>94</td><td>59</td><td>bf</td><td>30</td><td>da</td><td>14</td><td>e3</td><td>42</td><td>34</td><td>e2</td><td>1a</td><td>44</td><td>1b</td><td>39</td><td>d7</td><td>f4</td><td>99</td><td>2d</td></tr>
<tr><td>81</td><td>1d</td><td>02</td><td>20</td><td>09</td><td>c7</td><td>b6</td><td>72</td><td>7f</td><td>a6</td><td>bd</td><td>b4</td><td>74</td><td>4e</td><td>ac</td><td>4c</td><td>4f</td><td>a0</td><td>29</td><td>e0</td><td>05</td><td>ac</td><td>fa</td><td>62</td><td>69</td><td>98</td><td>9e</td><td>26</td><td>36</td><td>a6</td><td>0e</td><td>06</td></tr>
<tr><td>01</td><td>56</td><td>84</td><td>63</td><td>22</td><td>9d</td><td>9b</td><td>39</td><td>65</td><td>5f</td><td>cd</td><td>c4</td><td>ec</td><td>8f</td><td>c2</td><td>95</td><td>af</td><td>70</td><td>ba</td><td>94</td><td>78</td><td>50</td><td>27</td><td>7b</td><td>17</td><td>90</td><td>10</td><td>03</td><td>48</td><td>92</td><td>b2</td><td>21</td></tr>
<tr><td>11</td><td>5b</td><td>07</td><td>c6</td><td>29</td><td>7a</td><td>68</td><td>77</td><td>25</td><td>af</td><td>92</td><td>ca</td><td>7b</td><td>ae</td><td>c9</td><td>5e</td><td>ff</td><td>65</td><td>01</td><td>bc</td><td>3c</td><td>32</td><td>81</td><td>66</td><td>7a</td><td>02</td><td>07</td><td>12</td><td>a4</td><td>72</td><td>b0</td><td>0b</td></tr>
<tr><th colspan="16">S-Box $\mathcal{G}_1$</th><th colspan="16">S-Box $\mathcal{G}_2$</th></tr>
<tr><td colspan="16">$\mathcal{NL}(\mathcal{G}_1) = 104, \delta(\mathcal{G}_1) = 8, \deg(\mathcal{G}_1) = 7, \mathcal{AI}_{gr}(\mathcal{G}_1) = 3, r_{\mathcal{G}_1}^{(3)} = 441,$
$\mathsf{TO}(\mathcal{G}_1) = 7.786, \mathsf{SNR(DPA)}(\mathcal{G}_1) = 7.400, \mathsf{CC}(\mathcal{G}_1) = 0.23$</td><td colspan="16">$\mathcal{NL}(\mathcal{G}_2) = 104, \delta(\mathcal{G}_2) = 6, \deg(\mathcal{G}_2) = 7, \mathcal{AI}_{gr}(\mathcal{G}_2) = 3, r_{\mathcal{G}_2}^{(3)} = 441$
$\mathsf{TO}(\mathcal{G}_2) = 7.80, \mathsf{SNR(DPA)}(\mathcal{G}_2) = 8.38, \mathsf{CC}(\mathcal{G}_2) = 0.165$</td></tr>
<tr><td>d9</td><td>d3</td><td>dc</td><td>df</td><td>d2</td><td>db</td><td>da</td><td>d0</td><td>d5</td><td>de</td><td>d8</td><td>dd</td><td>d1</td><td>d7</td><td>d4</td><td>d6</td><td>f1</td><td>f6</td><td>fb</td><td>fd</td><td>f4</td><td>f5</td><td>f7</td><td>f0</td><td>fa</td><td>ff</td><td>f3</td><td>f9</td><td>f2</td><td>fe</td><td>f8</td><td>fc</td></tr>
<tr><td>19</td><td>6c</td><td>7f</td><td>b5</td><td>a1</td><td>9f</td><td>e5</td><td>5d</td><td>ec</td><td>8c</td><td>51</td><td>1d</td><td>ba</td><td>2f</td><td>9d</td><td>0f</td><td>91</td><td>5d</td><td>19</td><td>55</td><td>52</td><td>dd</td><td>b4</td><td>b9</td><td>00</td><td>65</td><td>6a</td><td>a0</td><td>d4</td><td>78</td><td>67</td><td>1a</td></tr>
<tr><td>b9</td><td>85</td><td>7a</td><td>52</td><td>53</td><td>9a</td><td>ef</td><td>f1</td><td>e2</td><td>13</td><td>91</td><td>f5</td><td>b1</td><td>63</td><td>25</td><td>35</td><td>c1</td><td>82</td><td>a7</td><td>db</td><td>13</td><td>24</td><td>eb</td><td>2d</td><td>a9</td><td>aa</td><td>d2</td><td>ea</td><td>43</td><td>29</td><td>84</td><td>b0</td></tr>
<tr><td>99</td><td>fe</td><td>ce</td><td>03</td><td>fc</td><td>73</td><td>42</td><td>e6</td><td>95</td><td>c6</td><td>83</td><td>05</td><td>45</td><td>12</td><td>56</td><td>b3</td><td>d1</td><td>9d</td><td>2e</td><td>06</td><td>0e</td><td>4f</td><td>8f</td><td>8d</td><td>c2</td><td>a2</td><td>69</td><td>8b</td><td>2a</td><td>94</td><td>96</td><td>4a</td></tr>
<tr><td>e9</td><td>8f</td><td>9e</td><td>55</td><td>5c</td><td>fa</td><td>ea</td><td>32</td><td>9c</td><td>62</td><td>ca</td><td>ff</td><td>c2</td><td>be</td><td>a2</td><td>1e</td><td>71</td><td>4d</td><td>85</td><td>66</td><td>42</td><td>e7</td><td>35</td><td>5b</td><td>e6</td><td>57</td><td>0a</td><td>0b</td><td>64</td><td>44</td><td>d3</td><td>02</td></tr>
<tr><td>09</td><td>74</td><td>a7</td><td>b4</td><td>ae</td><td>f4</td><td>e4</td><td>3b</td><td>7e</td><td>0e</td><td>97</td><td>4b</td><td>cb</td><td>26</td><td>20</td><td>30</td><td>01</td><td>a8</td><td>30</td><td>70</td><td>5f</td><td>7f</td><td>8a</td><td>c4</td><td>3c</td><td>e4</td><td>de</td><td>d8</td><td>36</td><td>a3</td><td>d6</td><td>53</td></tr>
<tr><td>f9</td><td>47</td><td>c3</td><td>0c</td><td>f2</td><td>6e</td><td>02</td><td>94</td><td>2e</td><td>c7</td><td>54</td><td>8e</td><td>22</td><td>44</td><td>ee</td><td>bc</td><td>e1</td><td>0c</td><td>1c</td><td>5e</td><td>77</td><td>22</td><td>04</td><td>cf</td><td>1f</td><td>ca</td><td>5a</td><td>3e</td><td>56</td><td>47</td><td>34</td><td>cb</td></tr>
<tr><td>39</td><td>86</td><td>66</td><td>01</td><td>58</td><td>71</td><td>21</td><td>7b</td><td>98</td><td>84</td><td>ab</td><td>c4</td><td>48</td><td>68</td><td>a0</td><td>36</td><td>81</td><td>4c</td><td>c0</td><td>ce</td><td>d5</td><td>b6</td><td>63</td><td>49</td><td>ab</td><td>c5</td><td>6e</td><td>68</td><td>dc</td><td>33</td><td>39</td><td>26</td></tr>
<tr><td>59</td><td>f7</td><td>93</td><td>5f</td><td>f3</td><td>4f</td><td>4c</td><td>7c</td><td>92</td><td>65</td><td>ac</td><td>cf</td><td>c5</td><td>1c</td><td>b7</td><td>e7</td><td>b1</td><td>59</td><td>37</td><td>99</td><td>6f</td><td>14</td><td>2b</td><td>e5</td><td>2f</td><td>3a</td><td>a6</td><td>6d</td><td>16</td><td>ad</td><td>17</td><td>3b</td></tr>
<tr><td>69</td><td>72</td><td>82</td><td>b2</td><td>aa</td><td>6b</td><td>1f</td><td>ed</td><td>3d</td><td>0a</td><td>5a</td><td>11</td><td>bf</td><td>4a</td><td>eb</td><td>5b</td><td>31</td><td>e3</td><td>87</td><td>28</td><td>05</td><td>58</td><td>83</td><td>ed</td><td>89</td><td>cc</td><td>b7</td><td>ba</td><td>7a</td><td>0d</td><td>75</td><td>e2</td></tr>
<tr><td>29</td><td>76</td><td>77</td><td>50</td><td>87</td><td>f6</td><td>4d</td><td>38</td><td>e0</td><td>80</td><td>ad</td><td>c0</td><td>0d</td><td>27</td><td>a8</td><td>34</td><td>11</td><td>93</td><td>ae</td><td>54</td><td>98</td><td>ec</td><td>9f</td><td>ef</td><td>b3</td><td>40</td><td>7b</td><td>be</td><td>e0</td><td>6b</td><td>a5</td><td>45</td></tr>
<tr><td>49</td><td>43</td><td>a6</td><td>a3</td><td>3e</td><td>c8</td><td>16</td><td>5e</td><td>33</td><td>07</td><td>96</td><td>f8</td><td>b6</td><td>24</td><td>28</td><td>04</td><td>21</td><td>da</td><td>5c</td><td>4e</td><td>48</td><td>bc</td><td>c8</td><td>bf</td><td>86</td><td>50</td><td>c6</td><td>4b</td><td>1d</td><td>80</td><td>9a</td><td>bb</td></tr>
<tr><td>c9</td><td>4e</td><td>cc</td><td>2c</td><td>37</td><td>90</td><td>3c</td><td>57</td><td>23</td><td>06</td><td>f0</td><td>17</td><td>67</td><td>46</td><td>e3</td><td>00</td><td>61</td><td>88</td><td>bd</td><td>1b</td><td>8e</td><td>a4</td><td>af</td><td>9b</td><td>ac</td><td>18</td><td>7e</td><td>07</td><td>9c</td><td>74</td><td>76</td><td>3d</td></tr>
<tr><td>89</td><td>41</td><td>a5</td><td>2b</td><td>75</td><td>6d</td><td>15</td><td>e1</td><td>31</td><td>c1</td><td>88</td><td>1a</td><td>6a</td><td>e8</td><td>bb</td><td>b8</td><td>41</td><td>9e</td><td>d0</td><td>15</td><td>12</td><td>7d</td><td>6c</td><td>72</td><td>23</td><td>27</td><td>8c</td><td>cd</td><td>10</td><td>d9</td><td>d7</td><td>c3</td></tr>
<tr><td>a9</td><td>14</td><td>9b</td><td>3a</td><td>fb</td><td>7d</td><td>0b</td><td>78</td><td>2a</td><td>64</td><td>8d</td><td>8a</td><td>40</td><td>60</td><td>a4</td><td>1b</td><td>51</td><td>73</td><td>e9</td><td>25</td><td>46</td><td>2c</td><td>e8</td><td>92</td><td>7c</td><td>38</td><td>32</td><td>df</td><td>20</td><td>79</td><td>0f</td><td>95</td></tr>
<tr><td>79</td><td>fd</td><td>cd</td><td>2d</td><td>3f</td><td>61</td><td>08</td><td>70</td><td>af</td><td>b0</td><td>8b</td><td>81</td><td>6f</td><td>10</td><td>bd</td><td>18</td><td>a1</td><td>62</td><td>3f</td><td>60</td><td>b8</td><td>97</td><td>03</td><td>1e</td><td>09</td><td>b5</td><td>c7</td><td>08</td><td>ee</td><td>90</td><td>c9</td><td>b2</td></tr>
</table>

S-Box $\mathcal{F}_3$

$\mathcal{NL}(\mathcal{F}_3) = 100, \delta(\mathcal{F}_3) = 8, \deg(\mathcal{F}_3) = 7, \mathcal{AI}_{gr}(\mathcal{F}_3) = 3, r^{(3)}_{\mathcal{F}_3} = 441,$
$\mathsf{TO}(\mathcal{F}_3) = 7.773, \mathsf{SNR(DPA)}(\mathcal{F}_3) = 6.509, \mathsf{CC}(\mathcal{F}_3) = 0.316$

1d	1f	1c	12	14	18	13	11	10	19	16	17	1a	15	1b	1e
5d	3f	3c	2c	5c	ee	90	31	02	0f	ce	70	af	cc	64	cf
3d	0c	04	94	34	f5	52	0b	83	8c	e5	22	dc	e4	b0	ec
cd	e2	e3	03	c3	4c	87	e9	f8	f2	bc	37	92	b3	da	b2
0d	84	80	50	00	69	33	8e	ca	c4	f9	93	74	f0	42	f4
bd	48	46	f6	b6	23	6b	40	ae	a8	73	eb	88	76	51	78
ed	f3	fa	8a	ea	a4	c8	ff	66	63	44	08	53	4a	77	43
ad	d1	db	bb	ab	57	45	d3	79	71	97	65	e1	9b	0e	91
8d	c0	c2	32	82	bf	0a	c5	e7	e0	6f	5a	20	62	a3	60
9d	59	5f	7f	9f	cb	24	56	30	39	8b	d4	49	8f	fc	89
4d	a6	a1	61	41	9a	be	a2	d5	d6	2a	fe	c6	21	3b	26
6d	b7	b8	e8	68	72	f1	b4	4b	47	d2	c1	07	d8	96	d7
fd	6a	67	c7	f7	d0	e6	6c	b1	ba	a0	86	3a	a7	28	aa
2d	95	99	d9	29	81	7c	98	54	55	01	ac	b5	09	ef	05
dd	7b	7e	4e	de	38	a9	7a	2f	2b	58	b9	fb	5e	85	5b
7d	2e	25	a5	75	06	df	27	9c	9e	36	4f	6e	35	c9	3e

S-Box $\mathcal{G}_3$

$\mathcal{NL}(\mathcal{G}_3) = 100, \delta(\mathcal{G}_3) = 8, \deg(\mathcal{G}_3) = 7, \mathcal{AI}_{gr}(\mathcal{G}_3) = 3, r^{(3)}_{\mathcal{G}_2} = 441$
$\mathsf{TO}(\mathcal{G}_3) = 7.753, \mathsf{SNR(DPA)}(\mathcal{G}_3) = 6.629, \mathsf{CC}(\mathcal{G}_2) = 0.302$

fc	f8	fe	f1	fd	f6	f3	f7	f5	f4	f9	fb	f2	ff	f0	fa
2c	6e	d1	8e	2d	e7	a8	8b	61	68	1b	02	6b	4b	07	42
0c	e5	0e	44	25	82	22	19	58	28	52	69	13	24	33	32
5c	3a	c0	12	85	7d	45	80	ad	88	75	a2	35	5f	8a	08
1c	18	0d	03	a4	a3	81	91	3f	6d	86	53	26	04	93	0f
9c	4d	74	6f	b4	a0	64	30	cd	cf	99	36	3b	34	b6	eb
ac	77	5d	3d	4e	bd	9d	50	83	90	57	be	43	54	14	aa
7c	ea	b8	c3	00	c9	c2	23	0a	da	e2	7b	39	98	ca	b0
8c	1e	4f	55	9a	5b	0b	c1	11	84	c5	41	a1	2e	1a	1f
6c	ee	ed	e3	b3	2b	1d	06	65	a6	d0	e6	5e	ab	16	20
cc	bf	df	2f	7e	c6	92	db	2a	3e	97	47	9b	7a	62	9f
3c	94	a5	95	c8	49	e4	37	78	48	5a	46	e8	d6	4a	79
4c	ae	38	ce	51	a9	31	8f	9e	b9	a7	de	d8	c7	40	af
ec	59	dd	e1	d5	d9	d2	ba	72	56	66	8d	05	6a	29	09
bc	d4	17	73	10	63	96	70	71	60	01	76	b2	e0	d7	c4
dc	89	87	cb	b5	15	d3	e9	b1	ef	b7	21	bb	27	7f	67

S-Box $\mathcal{H}_1$

$\mathcal{NL}(\mathcal{H}_1) = 106, \delta(\mathcal{H}_1) = 6, \deg(\mathcal{H}_1) = 7, \mathcal{AI}_{gr}(\mathcal{H}_1) = 3, r^{(3)}_{\mathcal{H}_1} = 441,$
$\mathsf{TO}(\mathcal{H}_1) = 7.834, \mathsf{SNR(DPA)}(\mathcal{H}_1) = 8.644, \mathsf{CC}(\mathcal{H}_1) = 0.152$

1b	d4	6b	e6	a6	e4	96	59	29	94	69	19	2b	d6	5b	a4
47	88	d7	57	62	06	f6	f7	ff	31	c0	1e	c1	6f	54	ae
d0	0f	db	7a	75	b9	12	18	83	5f	d1	39	ce	51	cf	aa
af	58	23	cc	f2	a8	93	1d	45	3c	9b	0b	42	bb	ef	08
ea	d5	6d	14	60	41	53	f8	2c	36	80	79	f5	27	b1	cd
c9	d2	35	a5	f1	bf	4b	3d	ec	9d	01	cb	16	1c	4a	d8
64	32	04	33	e0	97	05	26	63	c2	55	81	48	20	d3	49
38	e9	07	7f	34	c4	b5	df	e3	e8	8e	30	1f	7e	de	e5
f3	9a	eb	fd	73	fb	e1	dd	5a	3f	90	9e	b7	b4	c8	4c
02	6c	72	ac	24	87	e2	a7	7c	8a	0d	17	76	43	c6	ad
b6	2f	9f	0a	bd	dc	6a	a1	f0	da	8b	37	86	d9	4e	fe
7d	0e	b8	03	40	82	66	6e	15	78	13	ed	44	2d	2a	f4
95	09	67	a2	70	b3	91	71	61	ca	e7	4d	50	89	3a	a9
21	8d	c5	25	9c	5d	bc	28	10	2e	7b	b0	ba	0c	99	74
5e	92	84	a3	fc	11	65	00	f9	68	ab	c7	fa	c3	b2	52
8c	85	ee	3e	3b	1a	a0	46	be	98	77	8f	5c	4f	56	22

S-Box $\mathcal{H}_2$

$\mathcal{NL}(\mathcal{H}_2) = 108, \delta(\mathcal{H}_2) = 6, \deg(\mathcal{H}_2) = 7, \mathcal{AI}_{gr}(\mathcal{H}_2) = 3, r^{(3)}_{\mathcal{H}_2} = 441$
$\mathsf{TO}(\mathcal{H}_2) = 7.838, \mathsf{SNR(DPA)}(\mathcal{H}_2) = 9.335, \mathsf{CC}(\mathcal{H}_2) = 0.121$

1b	58	81	db	94	8d	41	02	98	17	d7	4d	ce	0e	54	c2
9e	dd	ad	c3	7b	d3	75	b3	05	65	bd	0b	15	cd	a3	6b
e1	fb	38	b9	93	f2	9a	7a	59	d1	73	50	12	b0	31	d8
13	d6	a0	90	19	e4	2b	e6	5d	5f	d4	6f	29	a2	92	6d
4c	77	53	8f	80	30	c7	ab	e3	78	ec	a4	5c	c8	14	3f
3b	9c	7d	7e	6a	ee	18	9f	f9	88	ed	8b	69	0c	0f	fa
e9	36	83	32	91	0d	aa	87	1f	95	bc	24	20	09	b8	ae
6c	f0	35	ea	f1	c5	c4	2f	01	eb	1a	34	2e	df	00	de
96	10	16	48	79	2c	45	4e	43	21	72	7f	27	74	2a	1d
c1	7c	5e	dc	e2	07	99	fe	bb	42	85	c0	60	a7	25	39
c9	b1	e5	57	e0	f8	a9	03	fd	06	4a	b4	52	1e	ac	4f
33	51	c6	f5	68	11	28	62	bf	cc	22	ff	5b	b5	86	8c
be	5a	cb	a6	0a	26	76	37	e7	f6	4b	9b	67	da	b7	8a
b6	97	70	2d	08	d9	46	ca	a1	b2	84	ef	55	63	3e	fc
44	ba	e8	04	82	cf	f7	56	a5	3c	23	d0	6e	71	9d	49
64	3d	8e	61	f3	3a	f4	d2	47	af	d5	40	1c	66	89	a8