Higher Order Side-Channel Attack
Resilient S-boxes

Liran Lerman
Quality and Security of Information Systems,
Département d'Informatique,
Université libre de Bruxelles
Belgium

Nikita Veshchikov
NXP Semiconductors
Belgium

Stjepan Picek
Delft University of Technology
Mekelweg 2
Delft, The Netherlands

Olivier Markowitch
Quality and Security of Information Systems,
Département d'Informatique,
Université libre de Bruxelles
Belgium

ABSTRACT

Masking schemes represent a well-researched and successful option to follow when considering side-channel countermeasures. Still, such measures increase the implementation cost in terms of power consumption, clock cycles, and random numbers generation. In fact, the higher the order of protection against side-channel adversaries, the higher the implementation cost of countermeasures. S-boxes represent the most vulnerable part in an implementation when considering side-channel adversary. In this paper, we investigate how to generate S-boxes that have improved resilience against varying orders of side-channel attacks while having minimal implementation costs. We examine whether S-boxes generated against a certain order of attack also represent a good solution when considering different order of attacks. We demonstrate that we successfully generated S-boxes resilient against a certain physical attack order but the improvements are small. As a result, S-boxes that are resilient against first order attacks stay resilient against higher-order attacks, which saves computational power during the design of higher-order side-channel attacks resilient S-boxes.

KEYWORDS

S-box construction, Genetic algorithms, Higher-order side-channel analysis, Correlation power analysis.

ACM Reference format:
Liran Lerman, Nikita Veshchikov, Stjepan Picek, and Olivier Markowitch. 2018. Higher Order Side-Channel Attack
Resilient S-boxes. In *Proceedings of CF '18: Computing Frontiers Conference, Ischia, Italy, May 8–10, 2018 (CF '18),* 6 pages.
DOI: 10.1145/3203217.3206428

'

1 INTRODUCTION

For decades, designers estimated the security level of a cryptographic algorithm independently of its implementation in a cryptographic device. Since the first publication on implementation attacks in 1996, the physical attacks have become an active research area [11]. A side-channel attack (SCA) represents a process that exploits physical leakages (measured on cryptographic devices) in order to extract sensitive information (e.g., the key used in a symmetric encryption algorithm). The ability to secure devices against side-channel attacks represents a critical requirement for the industry due to several publications on real-world physical attacks against (certified and uncertified) industrial products.

The Internet of Things (IoT) represents an attractive target for physical attacks (see e.g., Ronen et al. [21]) since the target device is in the vicinity of the adversary (which facilitates the analysis of physical properties). The widespread adoption of IoT, its extreme constraints (in terms of area and power consumption) as well as the hostile environments in which the IoT is manipulated raise the need of lightweight countermeasures against side-channel attacks. Following several works on this subject (see for example [4, 8, 10, 20]), this paper analyses the protection of the nonlinear part (called S-boxes) of block ciphers, which is often targeted by implementation attacks. More precisely, this paper focuses on lightweight countermeasures in which the S-boxes (also called (n, m) functions) are intrinsically more resilient against side-channel attacks.

In 2014, Picek et al. generated S-boxes of various sizes providing improved resistance to physical attacks [16]. They used genetic programming and genetic algorithms to evolve S-boxes minimising the transparency order metric that relates to the side-channel resistance of the S-boxes [19]. The main advantage of these approaches (compared to the exhaustive search) lies in the execution time of the search: exhaustive search generates $2^{m \cdot 2^n}$ different $n \times n$ S-boxes ($(2^n)!$ if we only consider permutations) while genetic algorithms optimise this search in an automatic way. At the same year, Picek et al. obtained two S-boxes of sizes 4×4 and 8×8 by exploiting genetic algorithms optimising the confusion coefficient property, which represents another metric related to the side-channel resistance of the S-boxes [18]. One year later, Picek et al. built a 4×4 S-box using genetic algorithms optimising the improved transparency order

CF '18, Ischia, Italy
© 2018 ACM. 978-1-4503-5761-6/18/05…$15.00
DOI: 10.1145/3203217.3206428

metric [6, 17]. Recently, Lerman et al. provided new S-boxes minimising the success probability of actual physical attacks [13]. They provided 4×4 and 5×5 S-boxes that possess increased resistance against various real-world attacks exploiting actual leakages.

In this paper, we focus on 4×4 S-boxes since we deem this size to have the most impact in the future design of lightweight ciphers. We aim to give an answer to the following question: "*Should we take into account the key enumeration during the design of S-boxes?*". In order to generate S-boxes with different orders of resilience against key enumeration, we use genetic algorithms. Such a technique proved to be a viable choice in previous works where it successfully generated cryptographically optimal 4×4 S-boxes with improved resilience against SCAs. It is possible to exhaustively search all optimal 4×4 S-boxes but the problem is the computational complexity of the evaluation of resilience against key enumeration. This makes exhaustive search difficult even for the smallest S-box sizes.

This approach is of high importance since (as reported in this paper) the designers of S-boxes can concentrate only on the first order success probability of side-channel adversaries. Eventually, this paper highlights that the best S-box (which minimises the success probability of physical attacks) depends on the physical noise level in the leakages. This result demonstrates the requirement to select S-boxes as a function of the cryptographic device executing these S-boxes, and it confirms the assumption of Lerman et al. [13].

2 BACKGROUND

Let n, m be positive integers – $n, m \in \mathbb{N}^+$. We denote by $\mathbb{F}_2^n$ the n-dimensional vector space over $\mathbb{F}_2$ and by $\mathbb{F}_{2^n}$ the finite field with 2^n elements. The set of all n-tuples of elements in the field $\mathbb{F}_2$ is denoted by $\mathbb{F}_2^n$, where $\mathbb{F}_2$ is the Galois field with two elements. For any set S, we denote $S\backslash\{0\}$ by S^*. The usual inner product of a and b equals $a \cdot b = \bigoplus_{i=1}^n a_i b_i$ in F_2^n. The addition of elements of the finite field $\mathbb{F}_{2^n}$ is denoted with "+". Since we often identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ and when there is no ambiguity, the addition of vectors of $\mathbb{F}_2^n, n > 1$ is denoted with "+" as well. The Hamming weight $w_H(a)$ of a vector a, where $a \in \mathbb{F}_2^n$, is the number of non-zero positions in the vector. An (n, m)-function is any mapping F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. An (n, m)-function F is defined as a vector $F = (f_1, \cdots, f_m)$, where the Boolean functions $f_i : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ for $i \in \{1, \cdots, m\}$ are called the coordinate functions of F. The component functions of an (n, m)-function F are all the linear combinations of the coordinate functions with non all-zero coefficients.

2.1 S-box Properties and Bounds

An (n, m)-function F is balanced if it takes every value of $\mathbb{F}_2^m$ the same number 2^{n-m} of times.

The Walsh-Hadamard transform of an (n, m)-function F is (see e.g., [2]):

$$W_F(a, v) = \sum_{x \in \mathbb{F}_2^m} (-1)^{v \cdot F(x) + a \cdot x}, \; a, v \in \mathbb{F}_2^m. \tag{1}$$

The *nonlinearity* N_F of an (n, m)-function F equals the minimum nonlinearity of all its component functions $v \cdot F$, where $v \in \mathbb{F}_2^{m*}$ [15]:

$$N_F = 2^{n-1} - \frac{1}{2} \max_{\substack{a \in \mathbb{F}_2^n \\ v \in \mathbb{F}_2^{m*}}} |W_F(a, v)|. \tag{2}$$

The nonlinearity of any (n, n) function F is bounded above by the Sidelnikov-Chabaud-Vaudenay bound [5]:

$$N_F \leq 2^{n-1} - 2^{\frac{n-1}{2}}. \tag{3}$$

Eq. (3) is an equality if and only if F is an Almost Bent (AB) function.

Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$ with $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^m$. We denote:

$$D_F(a, b) = \left\{ x \in \mathbb{F}_2^n : F(x) + F(x + a) = b \right\}. \tag{4}$$

The entry at the position (a, b) corresponds to the cardinality of the difference table $D_F(a, b)$ and is denoted as $\delta(a, b)$. The *differential uniformity* δ_F is then defined as [14]:

$$\delta_F = \max_{a \neq 0, b} \delta(a, b). \tag{5}$$

Functions that have differential uniformity equal to 2 are called the Almost Perfect Nonlinear (APN) functions. The best possible nonlinearity and differential uniformity values for the 4×4 S-box size equal 4.

2.2 Side-Channel Attacks

We assume that the adversary wants to retrieve the secret key used when the cryptographic device (that executes a known encryption algorithm) encrypts known plaintexts and provides known ciphertexts. In order to find the key, the adversary targets a set of key-related information (called the *target intermediate values*) with a *divide-and-conquer approach*. The divide-and-conquer strategy extracts information on separate parts of the key (e.g., the adversary extracts each byte of the key independently) and then combines the results in order to get the full secret key. In the rest of the paper, we systematically use the term key to denote the target of our attacks, though in fact, we address one part of the key at a time.

During the execution of the encryption algorithm, the cryptographic device processes a function F (e.g., the S-box of the block cipher AES):

$$\begin{aligned} \mathsf{F} \colon \mathcal{P} \times \mathcal{K} &\rightarrow \mathcal{Y} \\ y &= \mathsf{F}_k(p), \end{aligned} \tag{6}$$

that outputs the target intermediate value y and where $k \in \mathcal{K}$ is a key-related information (e.g., one byte of the secret key), and $p \in \mathcal{P}$ represents information known by the adversary (e.g., one byte of the plaintext).

2.2.1 *Physical Characteristics.* Let ${}^jT_y$ be the j-th leakage (also known as trace) measured when the device manipulates the target value y. In the following, we represent each leakage with one real value measured when the analysed cryptographic device manipulates the target value y, i.e.:

$${}^jT_y = \mathsf{L}(y) + {}^j\epsilon_y, \tag{7}$$

$$= \mathsf{L}(\mathsf{F}_k(p)) + {}^j\epsilon_y, \tag{8}$$

where ${}^j\epsilon_y \in \mathbb{R}$ is the noise of the trace ${}^jT_y$ following for example the Gaussian distribution with zero mean and L is the (deterministic) leakage function. The function L can be *linear* (e.g., the weighted sum of each bit of the input value) or *nonlinear* (e.g., the weighted sum of products of bits of the input value). Evaluators often model linear leakage functions as the Hamming weight of the manipulated value y for software implementations.

A *side-channel attack* is a process during which an attacker analyses leakages measured on a target device in order to extract information on the secret value. Several side-channel attacks exist but we focus on classical attacks exploiting correlation power analysis (presented by Coron et al. [7]) since 1) they represent the most efficient attacks when the leakage model fits to the leakage function in univariate settings [1], and 2) we presume no assumption error and no estimation error (of the estimation of the leakage function) leading to the evaluation of the S-boxes with the worst-case (univariate) side-channel adversaries.

2.2.2 Correlation Power Analysis. Correlation power analysis (CPA) recovers the secret key from a cryptographic device by selecting the key that maximises the dependence between the actual leakage and the estimated leakage based on the assumed secret key. More precisely, CPA selects the secret key $\widehat{k}$ such that:

$$\widehat{k} \in \underset{k \in \mathcal{K}}{\arg\max} \left\| \rho \left(\widehat{\mathcal{T}}_{(k)}, \mathcal{T} \right) \right\|, \tag{9}$$

where $\|x\|$ denotes the Euclidean norm of x, $\rho(\mathcal{X}, \mathcal{Y})$ represents the Pearson's correlation between two vectors $\mathcal{X}$ and $\mathcal{Y}$, and:

- $\mathcal{T} = \left[{}^{1}T, ..., {}^{N_a}T\right]$ represents a vector of N_a attack traces measured when the target device manipulates the S-box (where ${}^{i}T$ denotes the i-th measurement on the target device and N_a is the number of attack traces), and
- $\widehat{\mathcal{T}}_{(k)} = \left[\widehat{\mathsf{L}}(\mathsf{F}(k \oplus p_{[1]}), \ldots, \widehat{\mathsf{L}}(\mathsf{F}(k \oplus p_{[N_a]})\right]$ refers to a vector of estimated leakages (with a leakage model $\widehat{\mathsf{L}}$) parametrised with the output of the S-box combining (with the exclusive-or operation denoted $\oplus$) an estimated key k and known plaintext $p_{[i]}$ associated to ${}^{i}T$.

2.2.3 i-th Order Success Rate. The designers of cryptographic devices measure the resistance of an implementation against a physical attack by using (among others) the first order Success Rate (1oSR) [22]. The first order success rate (also known as the first order success probability) represents the probability that the physical attack ranks the actual key in the first position of the list of keys sorted by the physical attack in decreasing order of likelihood. Similarly, the i-th order success rate denotes the probability that the physical attack ranks the actual key among the i first positions of the list of keys. This metric relates to a side-channel adversary applying key enumeration algorithms (in which the adversary outputs a set of keys from the most probable one to the least probable one).

3 RESILIENT S-BOXES AGAINST KEY ENUMERATION

This section extends the analysis of S-boxes (generated by genetic algorithms and reported in [13, 16, 17]) by considering side-channel adversaries exploiting a CPA with a key enumeration. More precisely, we aim to verify whether the generated S-boxes, that minimise the first order success rate, minimise also a higher order success rate. We also provide results of newly generated S-boxes taking into account the key enumeration during their design as well as the multiplicative complexity of such S-boxes.

3.1 Scenarios under Consideration

3.1.1 Leakages Generation. We generated synthetic leakages having 1 point related to the Hamming weight of the S-Box:

$${}^{j}T_{y} = \mathsf{L}(y) + {}^{j}\epsilon_{y} = \mathsf{HW}(\mathsf{SBox}(p \oplus k)) + {}^{j}\epsilon_{y}. \tag{10}$$

This leakage function models the measurements collected during the execution of (serial) software implementations (which represent a realistic scenario in IoT). We assume no estimation/assumption error, which leads the adversary to consider the Hamming weight model during the attack: $\widehat{\mathsf{L}}(\cdot) = \mathsf{L}(\cdot) = \mathsf{HW}(\cdot)$. We estimated the success rate by generating 100 000 sets of attack leakages.

3.1.2 Target Functions. We focus on seven 4×4 S-boxes used by Joltik, Klein, Minalpher, Prince, Prøst, Present, and Rectangle. In the sequel, we refer to these (4×4) S-boxes as *unoptimised* S-boxes since the designers did not optimise these S-boxes with respect to minimising the success rate of physical attacks.

The *optimised* S-boxes represent nonlinear functions designed to minimise the first order success rate of physical attacks and already published in the side-channel literature. These optimised 4×4 S-boxes are the following: Evolved$_{CC}$ [18], Evolved$_{TO}$ [17], Evolved$_{SR1}$, and Evolved$_{SR2}$ [13]. Table 1 reports all these (unoptimised and optimised) S-boxes with their cryptographic properties. The *new optimised* S-boxes are nonlinear functions generated with genetic algorithm by taking into account the key enumeration and the noise level during the S-box generation. Table 2 provides the new optimised 4×4.

3.1.3 Search Strategy. As a search technique used to generate S-boxes, we use genetic algorithms (GAs) since it is a method that is easy to implement while being very efficient as reported in related work. Genetic algorithms are generic population-based metaheuristic optimization technique inspired by biological evolution [9]. Candidate solutions to the optimization problem play the role of individuals in a population, and the fitness function determines the quality of the solutions. Evolution of the population takes place after the repeated application of the above operators. In our algorithm, we encode solutions (S-boxes) as lists of values between 0 and $2^n - 1$ where n is the size of the S-box. We use 3-tournament selection where three solutions are randomly selected and the worst one is discarded. The remaining two solutions are used by the crossover operator (order crossover) to create a new offspring. The order crossover works by first randomly selecting two crossover points and copying everything between those two points from the first parent to the offspring. Then, starting from the second crossover point in the second parent, the unused numbers are copied in the order they appear in that parent [9]. We use the toggle mutation where we randomly select two values and swap them. The initial population is created uniformly at random and the population size equals 200 individuals. As a stopping criterion, we use the number of evaluations without improvement, which we set to 150 evaluations. To obtain S-boxes with as high as possible nonlinearity and as low as possible differential uniformity, we use the following fitness function:

$$fitness_t = N_F + (2^n - \delta_F)). \tag{11}$$

Then, only those solutions that have the best possible values of nonlinearity and differential uniformity are further evolved (while

Type	Name	MC	S-box
U	Joltik	6	E,4,B,2,3,8,0,9,1,A,7,F,6,C,5,D
	Klein	8	7,4,A,9,1,F,B,0,C,3,2,6,8,E,D,5
	Minalpher	8	B,3,4,1,2,8,C,F,5,D,E,0,6,9,A,7
	Prince	8	B,F,3,2,A,C,9,1,6,7,8,0,E,5,D,4
	Prøst	6	0,4,8,F,1,5,E,9,2,7,A,C,B,D,6,3
	Present	7	C,5,6,B,9,0,A,D,3,E,F,8,4,7,1,2
	Rectangle	6	6,5,C,A,1,E,7,9,B,0,3,D,8,F,4,2
O	Evolved$_{CC}$	7	6,4,7,8,0,5,2,A,E,3,D,1,C,F,9,B
	Evolved$_{TO}$	6	2,0,C,6,A,E,F,7,3,1,8,4,9,D,B,5
	Evolved$_{SR1}$	8	2,4,8,0,F,B,7,D,6,5,E,3,1,9,C,A
	Evolved$_{SR2}$	7	F,E,0,A,1,8,9,B,7,6,4,C,5,2,3,D

Table 1: Properties of S-boxes when considering correlation power analysis. Values of S-boxes are given in hexadecimal format. Notations O and U represent optimised and unoptimised S-boxes with respect to side-channel analysis. All S-boxes are optimal. The notation MC represents multiplicative complexity.

Name	MC	Or.	σ	S-box
Ev$_{4x4\_1oSR\_\sigma 0.5}$	8	1	0.5	1,9,4,5,B,6,D,A,C,0,3,F,2,7,8,E
Ev$_{4x4\_2oSR\_\sigma 0.5}$	8	2	0.5	8,1,F,A,4,9,6,7,0,3,E,B,2,C,D,5
Ev$_{4x4\_3oSR\_\sigma 0.5}$	7	3	0.5	1,F,2,0,D,C,8,7,5,9,3,B,4,6,E,A
Ev$_{4x4\_4oSR\_\sigma 0.5}$	7	4	0.5	0,8,C,1,F,B,9,D,7,E,6,A,2,3,5,4
Ev$_{4x4\_1oSR\_\sigma 2}$	8	1	2	9,C,3,5,F,E,1,2,7,B,0,4,D,6,A,8
Ev$_{4x4\_2oSR\_\sigma 2}$	7	2	2	D,1,2,E,3,8,A,9,5,B,6,C,4,7,F,0
Ev$_{4x4\_3oSR\_\sigma 2}$	8	3	2	6,5,E,2,1,A,B,8,C,9,D,4,3,7,F,0
Ev$_{4x4\_4oSR\_\sigma 2}$	8	4	2	7,8,D,4,3,2,E,5,C,6,9,A,B,0,F,1

Table 2: Properties of new optimised S-boxes when considering correlation power analysis. The genetic algorithms optimise each S-box as a function of its size, its nonlinearity, differential uniformity, the order of the success rate (denoted as “Or.”) as well as the standard deviation of the noise in the leakages. All presented S-boxes have optimal values of nonlinearity and differential uniformity.

Name	Class
Evolved$_{SR1}$	G_0
Present, Rectangle, Evolved$_{CC}$, Evolved$_{TO}$, Evolved$_{SR2}$	G_1
Klein, Minalpher	G_4
Prøst, Joltik	G_8
Prince, Ev$_{4x4\_1oSR\_\sigma 2}$, Ev$_{4x4\_3oSR\_\sigma 2}$	G_{13}
Ev$_{4x4\_1oSR\_\sigma 0.5}$, Ev$_{4x4\_2oSR\_\sigma 0.5}$, Ev$_{4x4\_2oSR\_\sigma 2}$, Ev$_{4x4\_4oSR\_\sigma 2}$	G_{14}
Ev$_{4x4\_3oSR\_\sigma 0.5}$, Ev$_{4x4\_4oSR\_\sigma 0.5}$	G_{15}

Table 3: Optimal 4×4 S-boxes and their equivalence classes (classes use the same order as presented by Turan et al. [23]).

retaining those cryptographic properties) so they have low SCA success probability, which gives us the fitness function used in our experiments:

$$fitness = fitness_t + (1 - SR). \tag{12}$$

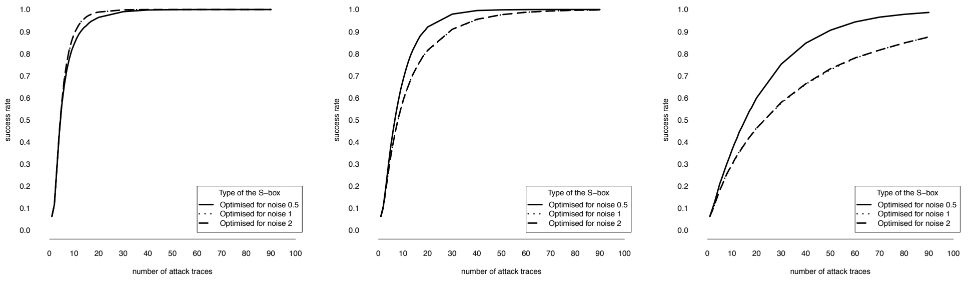
Since our search strategy preserves the bijectivity property and we consider only those S-boxes that have the best possible values of nonlinearity and differential uniformity, it is clear we consider only optimal S-boxes [12]. When considering the run time of our genetic algorithm, the most computationally intensive part is the calculation of SCA success probability. We note that for S-box sizes larger than 5×5, genetic algorithm becomes much less efficient option since it is difficult to generate solutions that have optimal values of nonlinearity and differential uniformity (for instance, for the 8×8 size, to the best of our knowledge, heuristic techniques never generated S-boxes with properties comparable to the AES S-box).

3.1.4 Multiplicative Complexity of S-boxes. Introduced in the context of side-channel attacks by Carlet et al., the multiplicative Complexity (MC) of an S-box is important for its secure implementation [3]. Here we will refer to the MC of an S-box as the minimum number of `AND` gates (or instructions in case of a software implementation) that one would need to implement the S-box. MC is important because the amount of randomness that one needs for masked implementation grows fast with the number of `AND` operations required for the implementation (i.e., it is easier to mask an `XOR` operation compared to `AND`). We estimate the MC of each S-box using equivalence classes presented in the work by Turan et al. [23], where their work gives a way to compute the MC for 4-bit Boolean functions. The results show that the multiplicative complexity for our new S-boxes is similar to the previously obtained ones, which points us that optimising S-boxes for different orders of attack does not bring a negative impact with respect to the MC.

In Table 3 we list the equivalence classes where all the investigated 4×4 S-boxes belong. In total, there are 16 optimal classes as defined by Leander and Poschmann. [12]. Interestingly, it can be seen that S-boxes optimized in previous works favours classes G_0 and G_1 while our new S-boxes are in classes G_{13}, G_{14}, and G_{15}. This could indicate that those classes have better side-channel resilience when considering various orders of attack.

3.2 Impact of the Noise in the Generation of S-boxes

The first experiment analyses the impact of the noise during the generation of S-boxes by genetic algorithms. We focus on the first order success rate of CPA against 4×4 S-boxes. Figure 1 shows the success probability of CPA as a function of the number of attack traces in which the standard deviation of the noise equals 0.5, 1, and 2 (which leads to a signal-to-noise ratio of 4.27, 1.07, and 0.27). Interestingly, the generated S-boxes optimised by genetic algorithm for a noise level x minimise the success rate when the standard deviation of the physical noise in the leakages equals x. In other words, the noise level in the leakages impacts the selection of the best S-boxes, which stresses the usefulness of the selection of S-boxes as a function of the device executing the S-box operation (as reported by Lerman et al. [13]).

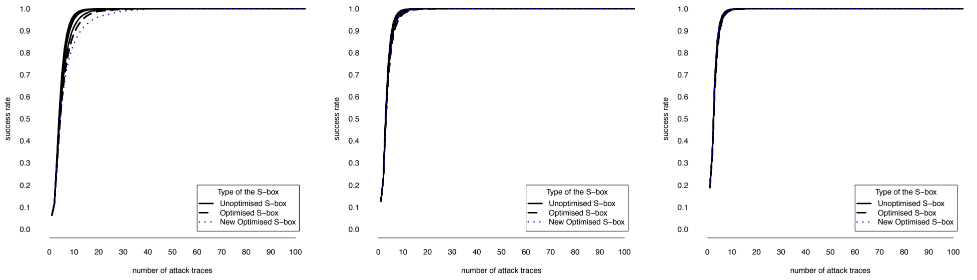


(a) $\sigma = 0.5$

(b) $\sigma = 1$

(c) $\sigma = 2$

Figure 1: Success rate of correlation power analysis on 4 × 4 S-boxes as a function of the number of attack traces. The standard deviation of the noise equals $\sigma = 1$. The S-boxes have nonlinearity equal to $N_F = 4$ and differential uniformity equal to $\delta_F = 4$. Each S-box was generated by genetic algorithms minimising the first order success rate given a fixed noise level.

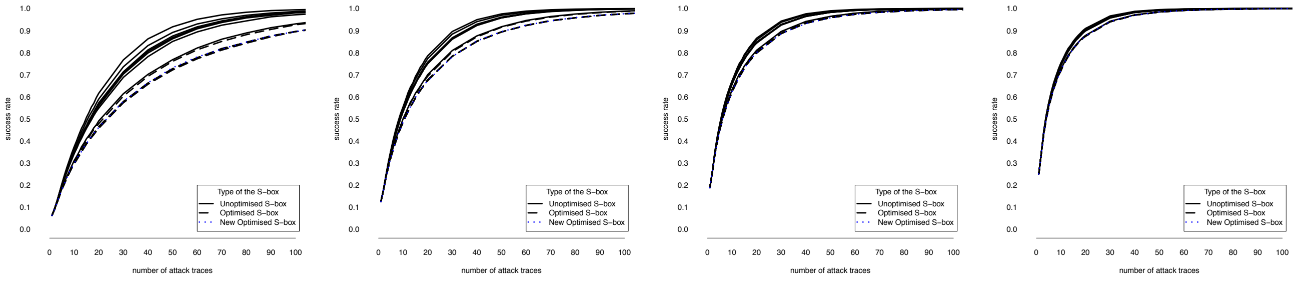


(a) First order success rate.

(b) Second order success rate.

(c) Third order success rate.

Figure 2: Success rates (different orders) of correlation power analysis on 4 × 4 S-boxes as a function of the number of attack traces. The standard deviation of the noise equals $\sigma = 0.5$. The S-boxes have nonlinearity equal to $N_F = 4$ and differential uniformity equal to $\delta_F = 4$.



(a) First order success rate.

(b) Second order success rate.

(c) Third order success rate.

(d) Fourth order success rate.

Figure 3: Success rate of correlation power analysis on 4 × 4 S-boxes as a function of the number of attack traces. The standard deviation of the noise equals $\sigma = 2$. The S-boxes have nonlinearity equal to $N_F = 4$ and differential uniformity equal to $\delta_F = 4$.

3.3 New Optimised vs. Optimised vs. Unoptimised S-boxes

This section compares the unoptimised 4×4 S-boxes with respect to optimised S-boxes. We focus on the first, second, third, and fourth order success rates. Figures 2 and 3 report the results by considering a standard deviation of the noise equal to 0.5 and 2 (which leads to a signal-to-noise ratio of 4.27 and 0.27). Interestingly, as already reported for the masking countermeasures, Figure 2 highlights that all the (optimised and unoptimised) 4 × 4 S-boxes provide similar success rate when the leakages contain a low noise. Figure 3 exhibits that the generated S-boxes, that minimise the first order success rate, minimise also a higher order success rate. We can see that the higher the order of the success rate, the lower the difference between the optimised and the unoptimised S-boxes.

4 CONCLUSION

Providing side-channel countermeasures represents a complex task when considering the IoT. The rationale is that the IoT has extreme constraints in terms of area and power consumption. In this paper, we investigate lightweight side-channel countermeasures minimising the implementation costs. More precisely, we investigate whether the key enumeration should be considered when designing side-channel attacks resilient S-boxes. Genetic algorithms provide S-boxes that reduce the success probabilities of side-channel adversaries while keeping the same power consumption, clock cycles, and multiplicative complexity as an unprotected S-box.

The results exhibit that there is no advantage to take into account the key enumeration in order to build higher order resilient S-boxes. In other words, S-boxes minimising the first order success rate, minimise also a higher order success rate. Consequently, the designers of S-boxes can save computational power by only focusing on the first order success probability of physical attacks. As a future work, since we recognise several classes for the 4 × 4 size that seem to be favoured by our search strategy, we plan to conduct additional experiments where we concentrate only on the S-boxes belonging to those classes.

REFERENCES

[1] Lejla Batina, Benedikt Gierlichs, Emmanuel Prouff, Matthieu Rivain, François-Xavier Standaert, and Nicolas Veyrat-Charvillon. 2011. Mutual Information Analysis: a Comprehensive Study. *J. Cryptology* 24, 2 (2011), 269–291. DOI: http://dx.doi.org/10.1007/s00145-010-9084-8

[2] Claude Carlet. 2010. Vectorial Boolean Functions for Cryptography. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering* (1st ed.), Yves Crama and Peter L. Hammer (Eds.). Cambridge University Press, New York, USA, 398–469.

[3] Claude Carlet, Louis Goubin, Emmanuel Prouff, Michaël Quisquater, and Matthieu Rivain. 2012. Higher-Order Masking Schemes for S-Boxes. In *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers (Lecture Notes in Computer Science)*, Anne Canteaut (Ed.), Vol. 7549. Springer, 366–384. DOI: http://dx.doi.org/10.1007/978-3-642-34047-5_21

[4] Claude Carlet, Emmanuel Prouff, Matthieu Rivain, and Thomas Roche. 2015. Algebraic Decomposition for Probing Security. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I (Lecture Notes in Computer Science)*, Rosario Gennaro and Matthew Robshaw (Eds.), Vol. 9215. Springer, 742–763. DOI: http://dx.doi.org/10.1007/978-3-662-47989-6_36

[5] Florent Chabaud and Serge Vaudenay. 1995. Links between differential and linear cryptanalysis. In *Advances in Cryptology — EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia, Italy, May 9–12, 1994 Proceedings*, Alfredo De Santis (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 356–365.

[6] Kaushik Chakraborty, Sumanta Sarkar, Subhamoy Maitra, Bodhisatwa Mazumdar, Debdeep Mukhopadhyay, and Emmanuel Prouff. 2017. Redefining the transparency order. *Des. Codes Cryptography* 82, 1-2 (2017), 95–115. DOI: http://dx.doi.org/10.1007/s10623-016-0250-3

[7] Jean-Sébastien Coron, Paul C. Kocher, and David Naccache. 2000. Statistics and Secret Leakage. In *Financial Cryptography, 4th International Conference, FC 2000 Anguilla, British West Indies, February 20-24, 2000, Proceedings (Lecture Notes in Computer Science)*, Yair Frankel (Ed.), Vol. 1962. Springer, 157–173. DOI: http://dx.doi.org/10.1007/3-540-45472-1_12

[8] Jean-Sébastien Coron, Arnab Roy, and Srinivas Vivek. 2015. Fast evaluation of polynomials over binary finite fields and application to side-channel countermeasures. *J. Cryptographic Engineering* 5, 2 (2015), 73–83. DOI: http://dx.doi.org/10.1007/s13389-015-0099-9

[9] A. E. Eiben and J. E. Smith. 2003. *Introduction to Evolutionary Computing*. Springer-Verlag, Berlin Heidelberg New York, USA.

[10] Vincent Grosso, Emmanuel Prouff, and François-Xavier Standaert. 2014. Efficient Masked S-Boxes Processing - A Step Forward -. In *Progress in Cryptology - AFRICACRYPT 2014 - 7th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 28-30, 2014. Proceedings (Lecture Notes in Computer Science)*, David Pointcheval and Damien Vergnaud (Eds.), Vol. 8469. Springer, 251–266. DOI: http://dx.doi.org/10.1007/978-3-319-06734-6_16

[11] Paul C. Kocher. 1996. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings (Lecture Notes in Computer Science)*, Neal Koblitz (Ed.), Vol. 1109. Springer, 104–113. DOI: http://dx.doi.org/10.1007/3-540-68697-5_9

[12] G. Leander and A. Poschmann. 2007. On the Classification of 4 Bit S-Boxes. In *Arithmetic of Finite Fields*, Claude Carlet and Berk Sunar (Eds.). Lecture Notes in Computer Science, Vol. 4547. Springer Berlin Heidelberg, 159–176.

[13] Liran Lerman, Nikita Veshchikov, Stjepan Picek, and Olivier Markowitch. 2017. On the Construction of Side-Channel Attack Resilient S-boxes. In *Constructive Side-Channel Analysis and Secure Design - 8th International Workshop, COSADE 2017, Paris, France, April 13-14, 2017, Revised Selected Papers (Lecture Notes in Computer Science)*, Sylvain Guilley (Ed.), Vol. 10348. Springer, 102–119. DOI: http://dx.doi.org/10.1007/978-3-319-64647-3_7

[14] Kaisa Nyberg. 1991. Perfect Nonlinear S-Boxes. In *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings (Lecture Notes in Computer Science)*, Vol. 547. Springer, 378–386. DOI: http://dx.doi.org/10.1007/3-540-46416-6_32

[15] Kaisa Nyberg. 1993. On the construction of highly nonlinear permutations. In *Advances in Cryptology - EUROCRYPT' 92*, RainerA. Rueppel (Ed.). Lecture Notes in Computer Science, Vol. 658. Springer Berlin Heidelberg, 92–98.

[16] Stjepan Picek, Lejla Batina, and Domagoj Jakobovic. 2014. Evolving DPA-Resistant Boolean Functions. In *Parallel Problem Solving from Nature - PPSN XIII - 13th International Conference, Ljubljana, Slovenia, September 13-17, 2014. Proceedings (Lecture Notes in Computer Science)*, Thomas Bartz-Beielstein, Jürgen Branke, Bogdan Filipic, and Jim Smith (Eds.), Vol. 8672. Springer, 812–821. DOI: http://dx.doi.org/10.1007/978-3-319-10762-2_80

[17] Stjepan Picek, Bodhisatwa Mazumdar, Debdeep Mukhopadhyay, and Lejla Batina. 2015. Modified Transparency Order Property: Solution or Just Another Attempt. In *Security, Privacy, and Applied Cryptography Engineering - 5th International Conference, SPACE 2015, Jaipur, India, 2015, Proceedings (Lecture Notes in Computer Science)*, Rajat Subhra Chakraborty, Peter Schwabe, and Jon A. Solworth (Eds.), Vol. 9354. Springer, 210–227. DOI: http://dx.doi.org/10.1007/978-3-319-24126-5_13

[18] Stjepan Picek, Kostas Papagiannopoulos, Baris Ege, Lejla Batina, and Domagoj Jakobovic. 2014. 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 (Lecture Notes in Computer Science)*, Willi Meier and Debdeep Mukhopadhyay (Eds.), Vol. 8885. Springer, 374–390.

[19] Emmanuel Prouff. 2005. DPA Attacks and S-Boxes. In *Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers (Lecture Notes in Computer Science)*, Henri Gilbert and Helena Handschuh (Eds.), Vol. 3557. Springer, 424–441. DOI: http://dx.doi.org/10.1007/11502760_29

[20] Jürgen Pulkus and Srinivas Vivek. 2016. Reducing the Number of Non-linear Multiplications in Masking Schemes. In *Cryptographic Hardware and Embedded Systems - CHES 2016 - 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings (Lecture Notes in Computer Science)*, Benedikt Gierlichs and Axel Y. Poschmann (Eds.), Vol. 9813. Springer, 479–497. DOI: http://dx.doi.org/10.1007/978-3-662-53140-2_23

[21] Eyal Ronen, Adi Shamir, Achi-Or Weingarten, and Colin O'Flynn. 2017. IoT Goes Nuclear: Creating a ZigBee Chain Reaction. In *2017 IEEE Symposium on Security and Privacy, SP 2017, San Jose, CA, USA, May 22-26, 2017*. IEEE Computer Society, 195–212. DOI: http://dx.doi.org/10.1109/SP.2017.14

[22] François-Xavier Standaert, Tal Malkin, and Moti Yung. 2009. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. In *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings (Lecture Notes in Computer Science)*, Antoine Joux (Ed.), Vol. 5479. Springer, 443–461. DOI: http://dx.doi.org/10.1007/978-3-642-01001-9_26

[23] Meltem Sönmez Turan and René Peralta. 2014. The Multiplicative Complexity of Boolean Functions on Four and Five Variables. In *Lightweight Cryptography for Security and Privacy - Third International Workshop, LightSec 2014, Istanbul, Turkey, September 1-2, 2014, Revised Selected Papers (Lecture Notes in Computer Science)*, Thomas Eisenbarth and Erdinç Öztürk (Eds.), Vol. 8898. Springer, 21–33. DOI: http://dx.doi.org/10.1007/978-3-319-16363-5_2