Higher Order Side-Channel Attacks
Resilient S-boxes

Liran Lerman[1], Stjepan Picek[2], Nikita Veshchikov[3], and Olivier Markowitch[1]

[1] Quality and Security of Information Systems, Département d'Informatique,
Université libre de Bruxelles, Belgium
[2] Delft University of Technology, Mekelweg 2, Delft, The Netherlands
[3] NXP Semiconductors, Belgium

Abstract. Masking and hiding schemes represent a well-researched and successful option to follow when considering side-channel countermeasures. Still, such measures increase the implementation cost in term 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 minimising the 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.

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 [1]. 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 [2,3].

The Internet of Things (IoT) represents an attractive target for physical attacks (see e.g., Ronen et al. [4]) 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 term 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. This paper analyses the protection of the nonlinear part (called S-boxes) of 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 [5]. 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. The main advantage of these approaches (compared to the exhaustive search) lies in the execution time of the research: exhaustive search generates $2^{m \cdot 2^n}$ different $n \times n$ S-boxes[4] 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 [6]. One year later, Picek et al. built a 4×4 S-box using genetic algorithms optimising the improved transparency order metric [7]. Recently, Lerman et al. provided new S-boxes minimising the success probability of actual physical attacks [8]. 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 and 5×5 S-boxes since we deem those sizes to have the most impact in the future design of lightweight ciphers (as already reported by several papers [9–11]). We aim to give an answer to the following question: "*Should we take into account the key-enumeration during the design of S-boxes?*". 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. We also provide a new 5×5 S-box reaching a lower first order success rate compared to the previously published 5×5 S-boxes. 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. [8].

The rest of this paper is organised in the following way. Section 2 discusses the general notions about S-boxes, side-channel attacks, and search strategy. Section 3 presents the experimental setting, the experiments, and discusses the obtained results. Finally, Section 4 concludes the paper.

---

[4] $(2^n)!$ if we only consider permutations.

2 Background

This section provides general notions on S-boxes, their properties and bounds, as well as on physical attacks (e.g., physical leakages, correlation power analysis, and i-th order success rate).

2.1 General Notions

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 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 can be defined as a vector $F = (f_1, \cdots, f_m)$, where the Boolean functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$ 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. Since for every n, there exists a field $\mathbb{F}_{2^n}$ of order 2^n, we can endow the vector space $\mathbb{F}_2^n$ with the structure of that field. The addition of elements of the finite field $\mathbb{F}_{2^n}$ is denoted with "+", as usual in mathematics. 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.

2.2 S-box Properties

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., [12]):

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

The *nonlinearity* N_F of an (n, m)-function F equals the minimum nonlinearity of all its component functions $v \cdot F$, where $v \in \mathbb{F}_2^{m*}$ [12, 13]:

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

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:

$$D_F(a, b) = \{x \in \mathbb{F}_2^n : F(x) + F(x + a) = b\}. \tag{3}$$

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]:

$$\delta_F = \max_{a \neq 0, b} \delta(a, b). \tag{4}$$

2.3 S-box Bounds

The nonlinearity of any (n, m) function F is bounded above by the so-called *covering radius bound*:

$$N_F \leq 2^{n-1} - 2^{\frac{n}{2}-1}. \tag{5}$$

There exists a better bound when $m = n$ – the Sidelnikov-Chabaud-Vaudenay bound [15]:

$$N_F \leq 2^{n-1} - 2^{\frac{n-1}{2}}. \tag{6}$$

Eq. (6) is an equality if and only if F is an Almost Bent (AB) function.

Functions that have differential uniformity equal to 2 are called the Almost Perfect Nonlinear (APN) functions. Every AB function is also APN, but the converse does not hold in general. AB functions exist only in an odd number of variables, while APN functions also exist for an even number of variables. When discussing the differential uniformity for permutations, the best possible (and known) value is 2 for any odd n and also for $n = 6$. For n even and larger than 6, this is an open question.

To conclude, for 4×4 S-boxes, the best nonlinearity as well as differential uniformity equals 4. When discussing 5×5 S-box size, the best possible nonlinearity equals 12 and the best possible differential uniformity equals 2.

2.4 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):

$$\mathsf{F} : \mathcal{P} \times \mathcal{K} \to \mathcal{Y} \tag{7}$$
$$y = \mathsf{F}_k(p),$$

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).

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 crypto-graphic device manipulates the target value y, i.e.:

$$^jT_y = \mathsf{L}\left(y\right) + {}^j\epsilon_y, \tag{8}$$

$$= \mathsf{L}\left(\mathsf{F}_k\left(p\right)\right) + {}^j\epsilon_y, \tag{9}$$

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. [16]) since 1) they represent the most efficient attacks when the leakage model fit to the leakage function in univariate settings [17], and 2) we assume 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.

Correlation Power Analysis Correlation power analysis recover 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, correlation power analysis selects the secret key $\widehat{k}$ such that:

$$\widehat{k} \in \underset{k \in \mathcal{K}}{\arg\max} \left\| \rho\left(\widehat{\mathcal{T}}_{(k)}, \mathcal{T}\right) \right\|, \tag{10}$$

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

- $\mathcal{T} = \left[^1T, ..., {}^{N_a}T\right]$ represents a vector of N_a attack traces measured when the target device manipulates the S-box (where ^iT denotes the i-th measurement on the target device and N_a is the number of attack traces), and
- $\widehat{\mathcal{T}}_{(k)} = \left[\widehat{\mathsf{L}}(\mathsf{F}(k \oplus p_{[1]})), \dots, \widehat{\mathsf{L}}(\mathsf{F}(k \oplus p_{[N_a]}))\right]$ 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 ^iT.

***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) [18]. 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 [5,7,8]) 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

Leakages generation We generated synthetic leakages having 1 points related to the Hamming weight of the S-Box:

$$^{j}T_y = \mathsf{L}\left(y\right) + {}^{j}\epsilon_y = \mathsf{HW}\left(\mathsf{SBox}\left(p \oplus k\right)\right) + {}^{j}\epsilon_y. \tag{11}$$

This leakage function models the measurements collected during the execution of (serial) software implementations (which represent a realistic scenario in IoT) [19]. 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.

Target functions We focus on seven $4{\times}4$ S-boxes used by Joltik [20], Klein [21], Minalpher [22], Prince [23], Prøst [24], Present [25], and Rectangle [26].
    Regarding the $5{\times}5$ S-boxes, we focus on the S-boxes exploited by SC2000 [27] and Primate [28]. These 5×5 S-boxes have the best possible cryptographic properties: a nonlinearity of 12 and a differential uniformity of 2. In the sequel, we refer to these (4×4 and 5×5) 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 $4{\times}4$ S-boxes are the following: Evolved$_{CC}$ [6], Evolved$_{TO}$ [7], Evolved$_{SR1}$, and Evolved$_{SR2}$ [8]. The optimised 5×5 S-boxes are the following: Evolved$_{SR4}$, Evolved$_{SR7}$, Evolved$_{SR8}$, and Evolved$_{SR9}$ [8]. 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 and 5×5 S-boxes.

Search strategy As a search technique used to generate S-boxes, we use genetic algorithms (GAs) since it represents 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 and phenomena like mutation, recombination, and selection [29]. 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 as lists of values between 0 and $2^n - 1$ where n is the size of the S-box. Next, 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 [29]. Finally, 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 generations. In order to obtain S-boxes with as high as possible nonlinearity and as low as possible differential uniformity, we use the following expression:

$$fitness_t = N_F + (2^n - \delta_F)). \tag{12}$$

Then, only those solutions that have good enough values of cryptographic properties are further evolved (while retaining those cryptographic properties) so they have low SCA success probability, which gives us the fitness function used in our experiments:

$$fitness = fitness_t + (1 - SR). \tag{13}$$

We note that for 4×4 S-box size, we consider only S-boxes that are optimal: bijective, with nonlinearity and differential uniformity equal to 4 [30]. For 5×5 size, there are no such classification so we consider S-boxes that are either AB (having the best possible nonlinearity of 12 and differential uniformity of 2) or S-boxes with one step worse properties, i.e., nonlinearity of 10 and differential uniformity of 4.

Multiplicative complexity of S-boxes Multiplicative Complexity (MC) of an S-box is important for its secure implementation. Here we will refer to the

Size	Type	Name	N_F	δ_F	MC	S-box
4 × 4	U	Joltik	4	4	6	E,4,B,2,3,8,0,9,1,A,7,F,6,C,5,D
		KLEIN	4	4	8	7,4,A,9,1,F,B,0,C,3,2,6,8,E,D,5
		Minalpher	4	4	8	B,3,4,1,2,8,C,F,5,D,E,0,6,9,A,7
		PRINCE	4	4	8	B,F,3,2,A,C,9,1,6,7,8,0,E,5,D,4
		Prøst	4	4	6	0,4,8,F,1,5,E,9,2,7,A,C,B,D,6,3
		PRESENT	4	4	7	C,5,6,B,9,0,A,D,3,E,F,8,4,7,1,2
		RECTANGLE	4	4	6	6,5,C,A,1,E,7,9,B,0,3,D,8,F,4,2
	O	Evolved$_{CC}$	4	4	7	6,4,7,8,0,5,2,A,E,3,D,1,C,F,9,B
		Evolved$_{TO}$	4	4	6	2,0,C,6,A,E,F,7,3,1,8,4,9,D,B,5
		Evolved$_{SR1}$	4	4	8	2,4,8,0,F,B,7,D,6,5,E,3,1,9,C,A
		Evolved$_{SR2}$	4	4	7	F,E,0,A,1,8,9,B,7,6,4,C,5,2,3,D
5 × 5	U	SC2000	12	2	20	14,1A,07,1F,13,0C,0A,0F,16,1E,0D,0E,04,18,09,12 1B,0B,01,15,06,10,02,1C,17,05,08,03,00,11,1D,19
		Primate	12	2	10	01,00,19,1A,11,1D,15,1B,14,05,04,17,0E,12,02,1C 0F,08,06,03,0D,07,18,10,1E,09,1F,0A,16,0C,0B,13
	O	Evolved$_{SR4}$	10	4	20	0A,1C,01,13,04,08,12,10,06,05,03,0D,02,18,09,00 0F,1B,1A,11,14,1D,0B,0E,16,07,15,19,0C,17,1E,1F
		Evolved$_{SR7}$	10	4	20	1B,13,17,16,0B,0F,0D,1A,03,06,01,09,02,14,08,11 10,12,00,0A,1F,18,05,0C,1D,1C,04,07,0E,1E,15,19
		Evolved$_{SR8}$	12	2	10	00,0E,1C,16,19,01,0D,11,13,08,02,1D,1A,17,03,0A 07,0B,10,18,04,1E,1B,05,15,0C,0F,12,06,09,14,1F
		Evolved$_{SR9}$	12	2	10	00,07,0E,0B,1C,10,16,18,19,04,01,1E,0D,1B,11,05 13,15,08,0C,02,0F,1D,12,1A,06,17,09,03,14,0A,1F

Table 1: Properties of evolved 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. The notation N_F represents nonlinearity, δ_F differential uniformity, and MC multiplicative complexity.

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. [31], where their work gives a way to compute the MC for 4-bit and 5-bit Boolean functions. Note that in the case of some equivalence classes of 5-bit Boolean functions the MC estimate is the upper bound, thus we also PRESENT the upper bound of MC in our tables. 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.

Size	Name	N_F	δ_F	MC	Order	σ	S-box
4 × 4	Ev$_{4x4\_1oSR\_\sigma0.5}$	4	4	8	1	0.5	1,9,4,5,B,6,D,A,C,0,3,F,2,7,8,E
	Ev$_{4x4\_2oSR\_\sigma0.5}$	4	4	8	2	0.5	8,1,F,A,4,9,6,7,0,3,E,B,2,C,D,5
	Ev$_{4x4\_3oSR\_\sigma0.5}$	4	4	7	3	0.5	1,F,2,0,D,C,8,7,5,9,3,B,4,6,E,A
	Ev$_{4x4\_4oSR\_\sigma0.5}$	4	4	7	4	0.5	0,8,C,1,F,B,9,D,7,E,6,A,2,3,5,4
	Ev$_{4x4\_1oSR\_\sigma2}$	4	4	8	1	2	9,C,3,5,F,E,1,2,7,B,0,4,D,6,A,8
	Ev$_{4x4\_2oSR\_\sigma2}$	4	4	7	2	2	D,1,2,E,3,8,A,9,5,B,6,C,4,7,F,0
	Ev$_{4x4\_3oSR\_\sigma2}$	4	4	8	3	2	6,5,E,2,1,A,B,8,C,9,D,4,3,7,F,0
	Ev$_{4x4\_4oSR\_\sigma2}$	4	4	8	4	2	7,8,D,4,3,2,E,5,C,6,9,A,B,0,F,1
5 × 5	Ev$_{5x5\_1oSR\_\sigma1\_N_f12\_\delta_F2}$	12	2	10	1	1	1F,11,03,1E,06,09,1D,01,0C,0A,12,07,1B,1C,02,16 18,0F,14,10,05,13,0E,0B,17,08,19,15,04,1A,0D,00
	Ev$_{5x5\_2oSR\_\sigma1\_N_f12\_\delta_F2}$	12	2	10	2	1	1F,11,03,17,06,0A,0F,19,0C,12,14,10,1E,02,13,15 18,1B,05,1C,09,08,01,1A,1D,0E,04,0D,07,16,0B,00
	Ev$_{5x5\_3oSR\_\sigma1\_N_f12\_\delta_F2}$	12	2	10	3	1	1F,14,09,06,12,0F,0C,15,05,1B,1E,04,18,10,0B,07 0A,03,17,1A,1D,02,08,13,11,0D,01,19,16,1C,0E,00
	Ev$_{5x5\_4oSR\_\sigma1\_N_f12\_\delta_F2}$	12	2	10	4	1	1F,05,0A,11,14,1B,03,0D,09,1E,17,01,06,04,1A,19 12,18,1D,16,0F,10,02,1C,0C,0B,08,0E,15,07,13,00
	Ev$_{5x5\_1oSR\_\sigma1\_N_f10\_\delta_F4}$	10	4	10	1	1	1F,06,0C,1D,18,1A,1B,08,11,16,15,05,17,14,10,0E 03,1E,0D,04,0B,12,0A,07,0F,02,09,13,01,19,1C,00
	Ev$_{5x5\_2oSR\_\sigma1\_N_f10\_\delta_F4}$	10	4	20	2	1	00,1A,15,07,0B,0C,0E,05,16,03,18,1B,1C,0F,0A,01 0D,13,06,12,11,1D,17,10,19,09,1E,08,14,04,02,1F
	Ev$_{5x5\_3oSR\_\sigma1\_N_f10\_\delta_F4}$	10	4	20	3	1	00,12,05,13,0A,01,07,0B,14,08,02,18,0E,03,16,17 09,19,10,15,04,0C,11,1B,1C,1A,06,1D,0D,1E,0F,1F
	Ev$_{5x5\_4oSR\_\sigma1\_N_f10\_\delta_F4}$	10	4	20	4	1	1F,06,0C,17,18,05,0F,1C,11,09,0A,08,1E,01,19,15 03,1B,12,0E,14,04,10,1A,1D,07,02,0D,13,16,0B,00

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 (N_F), differential uniformity (δ_F), the order of the success rate as well as the standard deviation of the noise in the leakages.

Finally, 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. [30]. 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,

Name	Class
Joltik	G_8
KLEIN	G_4
Minalpher	G_4
PRINCE	G_{13}
Prøst	G_8
PRESENT	G_1
RECTANGLE	G_1
Evolved$_{CC}$	G_1
Evolved$_{TO}$	G_1
Evolved$_{SR1}$	G_0
Evolved$_{SR2}$	G_1
Ev$_{4x4\_1oSR\_\sigma 0.5}$	G_{14}
Ev$_{4x4\_2oSR\_\sigma 0.5}$	G_{14}
Ev$_{4x4\_3oSR\_\sigma 0.5}$	G_{15}
Ev$_{4x4\_4oSR\_\sigma 0.5}$	G_{15}
Ev$_{4x4\_1oSR\_\sigma 2}$	G_{13}
Ev$_{4x4\_2oSR\_\sigma 2}$	G_{14}
Ev$_{4x4\_3oSR\_\sigma 2}$	G_{13}
Ev$_{4x4\_4oSR\_\sigma 2}$	G_{14}

Table 3: Optimal 4×4 S-boxes and their equivalence classes (classes use the same order as presented by Turan et al. [31]).

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. [8]).

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 [32], 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.
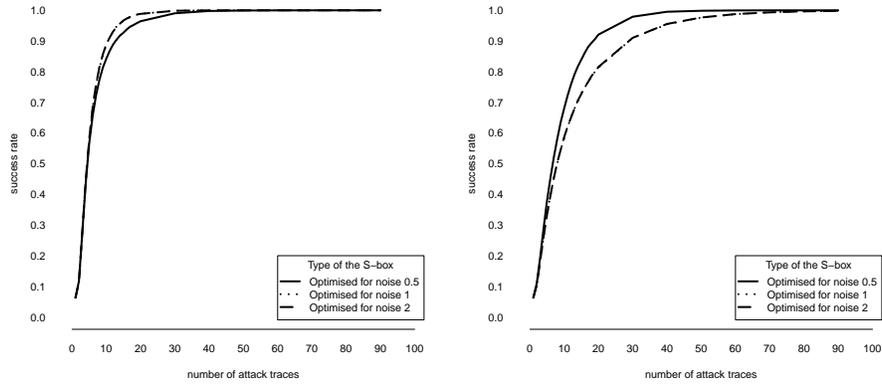
(a) $\sigma = \mathbf{0.5}$

(b) $\sigma = \mathbf{1}$
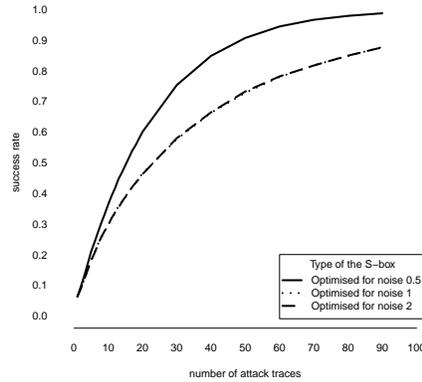
(c) $\sigma = \mathbf{2}$

Fig. 1: Success rate of correlation power analysis on $\mathbf{4 \times 4}$ S-boxes as a function of the number of attack traces. The standard deviation of the noise equals σ. The S-boxes have nonlinearity equal to $N_F = \mathbf{4}$ and differential uniformity equal to $\delta_F = \mathbf{4}$. Each S-box was generated by genetic algorithms minimising the first order success rate given a fixed noise level.
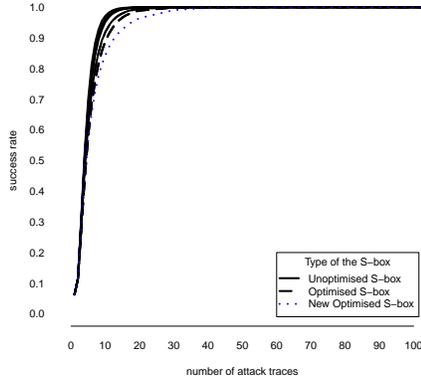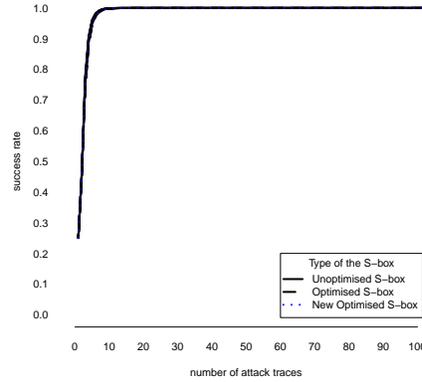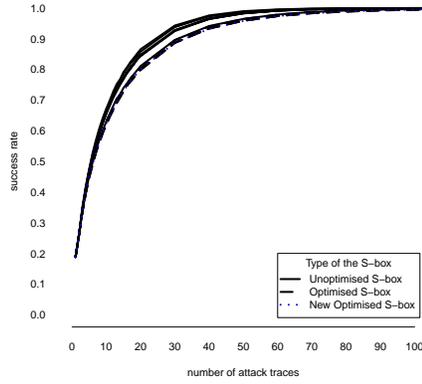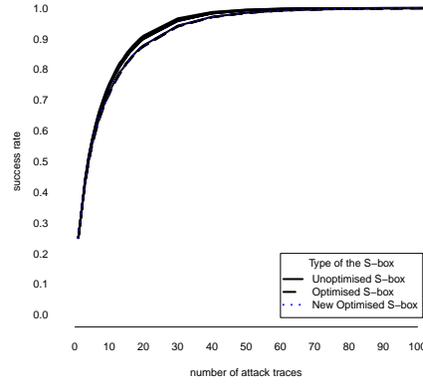
(a) First order success rate.
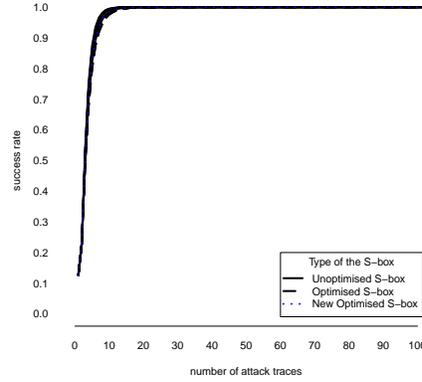
(b) Second order success rate.
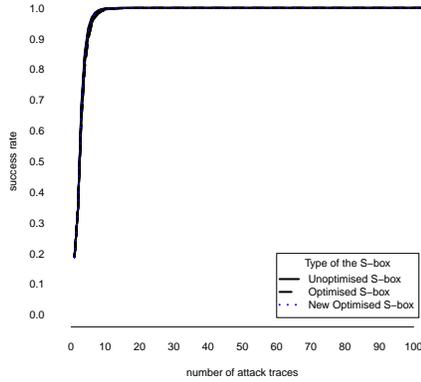
(c) Third order success rate.

(d) Fourth order success rate.

Fig. 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 $\delta_F = 4$.
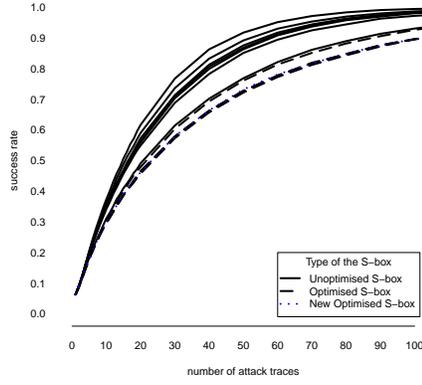
(a) First order success rate.
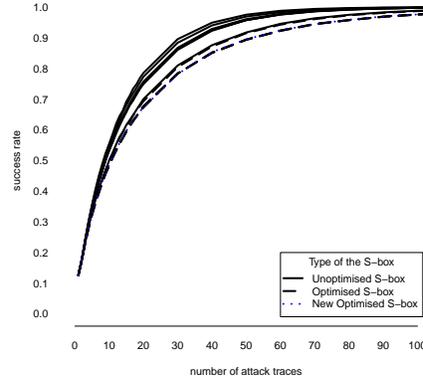
(b) Second order success rate.

(c) Third order success rate.

(d) Fourth order success rate.

Fig. 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 $\delta_F = 4$.

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.

We present new 5×5 S-boxes that have optimal cryptographic properties (nonlinearity equal to 12 and differential uniformity equal to 2) but require a high level of physical noise in order to be useful when compared to unoptimised S-boxes. Future work will focus on the generation of 5×5 S-boxes having good cryptographic properties as well as being resilient against side-channel attacks executed in the low noise level contexts. It would be of interest to understand why the physical noise level impacts the choice of the best S-box. Finally, since we recognise several classes for 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.

Acknowledgments

References

1. Kocher, P.C.: Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In Koblitz, N., ed.: Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings. Volume 1109 of Lecture Notes in Computer Science., Springer (1996) 104–113
2. Oswald, D., Strobel, D., Schellenberg, F., Kasper, T., Paar, C.: When reverse-engineering meets side-channel analysis - digital lockpicking in practice. In Lange, T., Lauter, K.E., Lisonek, P., eds.: Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers. Volume 8282 of Lecture Notes in Computer Science., Springer (2013) 571–588

3. Zhou, Y., Yu, Y., Standaert, F., Quisquater, J.: On the need of physical security for small embedded devices: A case study with COMP128-1 implementations in SIM cards. In Sadeghi, A., ed.: Financial Cryptography and Data Security - 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers. Volume 7859 of Lecture Notes in Computer Science., Springer (2013) 230–238

4. Ronen, E., Shamir, A., Weingarten, A., O'Flynn, C.: 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 (2017) 195–212

5. Picek, S., Batina, L., Jakobovic, D.: Evolving DPA-Resistant Boolean Functions. In Bartz-Beielstein, T., Branke, J., Filipic, B., Smith, J., eds.: Parallel Problem Solving from Nature - PPSN XIII - 13th International Conference, Ljubljana, Slovenia, September 13-17, 2014. Proceedings. Volume 8672 of Lecture Notes in Computer Science., Springer (2014) 812–821

6. Picek, S., Papagiannopoulos, K., Ege, B., Batina, L., Jakobovic, D.: Confused by Confusion: Systematic Evaluation of DPA Resistance of Various S-boxes. In Meier, W., Mukhopadhyay, D., eds.: Progress in Cryptology - INDOCRYPT 2014 - 15th International Conference on Cryptology in India, New Delhi, India, December 14-17, 2014, Proceedings. Volume 8885 of Lecture Notes in Computer Science., Springer (2014) 374–390

7. Picek, S., Mazumdar, B., Mukhopadhyay, D., Batina, L.: Modified Transparency Order Property: Solution or Just Another Attempt. In Chakraborty, R.S., Schwabe, P., Solworth, J.A., eds.: Security, Privacy, and Applied Cryptography Engineering - 5th International Conference, SPACE 2015, Jaipur, India, 2015, Proceedings. Volume 9354 of Lecture Notes in Computer Science., Springer (2015) 210–227

8. Lerman, L., Veshchikov, N., Picek, S., Markowitch, O.: On the construction of side-channel attack resilient s-boxes. In Guilley, S., ed.: Constructive Side-Channel Analysis and Secure Design - 8th International Workshop, COSADE 2017, Paris, France, April 13-14, 2017, Revised Selected Papers. Volume 10348 of Lecture Notes in Computer Science., Springer (2017) 102–119

9. Bertoni, G., Daemen, J., Peeters, M., Assche, G.V.: The keccak reference (2011) Submission to NIST (Round 3).

10. Andreeva, E., Bilgin, B., Bogdanov, A., Luykx, A., Mendel, F., Mennink, B., Mouha, N., Wang, Q., Yasuda, K.: PRIMATEs v1 Submission to the CAESAR Competition. http://competitions.cr.yp.to/round1/primatesv1.pdf (2014)

11. Borghoff, J., Canteaut, A., Gneysu, T., Kavun, E., Knežević, M., Knudsen, L., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S., Yaln, T.: PRINCE : A Low-Latency Block Cipher for Pervasive Computing Applications. In Wang, X., Sako, K., eds.: Advances in Cryptology: ASIACRYPT 2012. Volume 7658 of LNCS. Springer Berlin Heidelberg (2012) 208–225

12. Carlet, C.: Vectorial Boolean Functions for Cryptography. In Crama, Y., Hammer, P.L., eds.: Boolean Models and Methods in Mathematics, Computer Science, and Engineering. 1st edn. Cambridge University Press, New York, USA (2010) 398–469

13. Nyberg, K.: On the construction of highly nonlinear permutations. In Rueppel, R., ed.: Advances in Cryptology - EUROCRYPT' 92. Volume 658 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (1993) 92–98

14. Nyberg, K.: 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. Volume 547 of Lecture Notes in Computer Science., Springer (1991) 378–386

15. Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis. In De Santis, A., ed.: Advances in Cryptology — EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia, Italy, May 9–12, 1994 Proceedings, Berlin, Heidelberg, Springer Berlin Heidelberg (1995) 356–365

16. Coron, J., Kocher, P.C., Naccache, D.: Statistics and Secret Leakage. In Frankel, Y., ed.: Financial Cryptography, 4th International Conference, FC 2000 Anguilla, British West Indies, February 20-24, 2000, Proceedings. Volume 1962 of Lecture Notes in Computer Science., Springer (2000) 157–173

17. Batina, L., Gierlichs, B., Prouff, E., Rivain, M., Standaert, F., Veyrat-Charvillon, N.: Mutual information analysis: a comprehensive study. J. Cryptology 24(2) (2011) 269–291

18. Standaert, F., Malkin, T., Yung, M.: A unified framework for the analysis of side-channel key recovery attacks. In Joux, A., ed.: Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings. Volume 5479 of Lecture Notes in Computer Science., Springer (2009) 443–461

19. Barthe, G., Dupressoir, F., Faust, S., Grégoire, B., Standaert, F., Strub, P.: Parallel implementations of masking schemes and the bounded moment leakage model. In Coron, J., Nielsen, J.B., eds.: Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I. Volume 10210 of Lecture Notes in Computer Science. (2017) 535–566

20. Jean, J., Nikolić, I., Peyrin, T.: Joltik (2014) CAESAR submission.

21. Gong, Z., Nikova, S., Law, Y.W.: KLEIN: A new family of lightweight block ciphers. In Juels, A., Paar, C., eds.: RFID. Security and Privacy - 7th International Workshop, RFIDSec 2011, Amherst, USA, June 26-28, 2011, Revised Selected Papers. Volume 7055 of Lecture Notes in Computer Science., Springer (2011) 1–18

22. Sasaki, Y., Todo, Y., Aoki, K., Naito, Y., Sugawara, T., Murakami, Y., Matsui, M., Hirose, S.: Minalpher (2014) CAESAR submission.

23. Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S., Yalçin, T.: PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In Wang, X., Sako, K., eds.: Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings. Volume 7658 of Lecture Notes in Computer Science., Springer (2012) 208–225

24. Kavun, E.B., Lauridsen, M.M., Leander, G., Rechberger, C., Schwabe, P., Yalcin, T.: Prøst (2014) CAESAR submission.

25. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In Paillier, P., Verbauwhede, I., eds.: Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings. Volume 4727 of Lecture Notes in Computer Science., Springer (2007) 450–466

26. Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., Verbauwhede, I.: RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. SCIENCE CHINA Information Sciences 58(12) (2015) 1–15

27. Shimoyama, T., Yanami, H., Yokoyama, K., Takenaka, M., Itoh, K., Yajima, J., Torii, N., Tanaka, H.: The block cipher SC2000. In Matsui, M., ed.: Fast Software Encryption, 8th International Workshop, FSE 2001 Yokohama, Japan, April 2-4, 2001, Revised Papers. Volume 2355 of Lecture Notes in Computer Science., Springer (2001) 312–327

28. Andreeva, E., Bilgin, B., Bogdanov, A., Luykx, A., Mendel, F., Mennink, B., Mouha, N., Wang, Q., Yasuda, K.: PRIMATEs v1.02 (Sept 2014) CAESAR submission.

29. Eiben, A.E., Smith, J.E.: Introduction to Evolutionary Computing. Springer-Verlag, Berlin Heidelberg New York, USA (2003)

30. Leander, G., Poschmann, A.: On the Classification of 4 Bit S-Boxes. In Carlet, C., Sunar, B., eds.: Arithmetic of Finite Fields. Volume 4547 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2007) 159–176

31. Turan, M.S., Peralta, R.: The multiplicative complexity of boolean functions on four and five variables. In Eisenbarth, T., Öztürk, E., eds.: Lightweight Cryptography for Security and Privacy - Third International Workshop, LightSec 2014, Istanbul, Turkey, September 1-2, 2014, Revised Selected Papers. Volume 8898 of Lecture Notes in Computer Science., Springer (2014) 21–33

32. Standaert, F., Veyrat-Charvillon, N., Oswald, E., Gierlichs, B., Medwed, M., Kasper, M., Mangard, S.: The world is not enough: Another look on second-order DPA. In Abe, M., ed.: Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings. Volume 6477 of Lecture Notes in Computer Science., Springer (2010) 112–129

A Success rates for 5×5 S-boxes

When considering 5×5 size, we observe similar behaviour (having a nonlinearity equal to $N_F = 12$ and a differential uniformity equal to $\delta_F = 2$) in which the standard deviation of the physical noise equals 2 and 4, leading to a signal-to-noise ratio of 0.32 and 0.08, respectively. Still, 5×5 S-boxes generated by genetic algorithms (with $N_F = 12$ and $\delta_F = 2$) provide a higher resiliency against side-channel adversary (compared to other unoptimised S-boxes) when the leakages contain a high level of physical noise. In other words, the higher the level of noise, the higher the resiliency of these optimised 5×5 S-boxes against physical attacks. Finally, we observe that optimised 5×5 S-boxes (taking into account only the first order success rate during the generation of the S-boxes) provide similar success rates to the new optimised S-boxes (taking into account the order of the success rate during the generation of the S-boxes). In the case of 5×5 S-boxes with nonlinearity equal to 10 and differential uniformity equal to 4, we see that the new optimised S-box reach a lower first order success rate compared to the previously published 5×5 S-boxes. Still, all the 5×5 S-boxes (with $N_F = 10$ and $\delta_F = 4$) provide similar results when considering higher-order success rate.
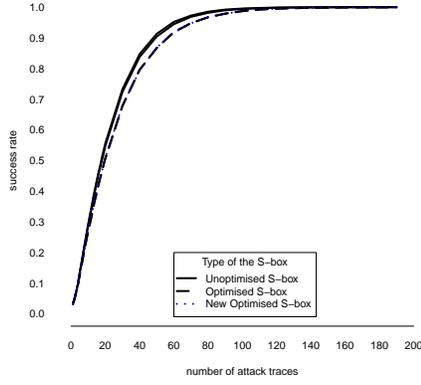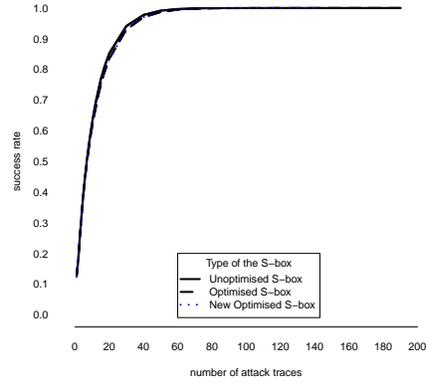
(a) First order success rate.
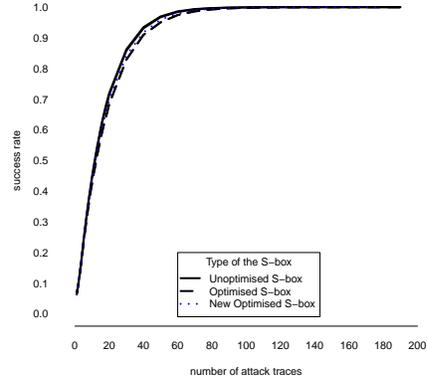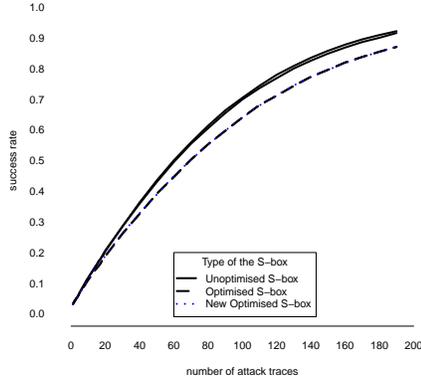
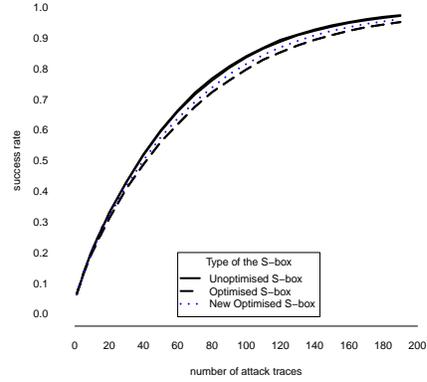(b) Second order success rate.
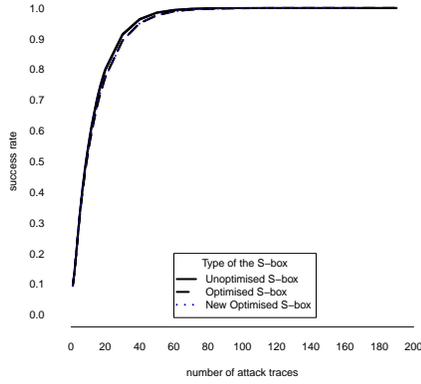
(c) Third order success rate.

(d) Fourth order success rate.

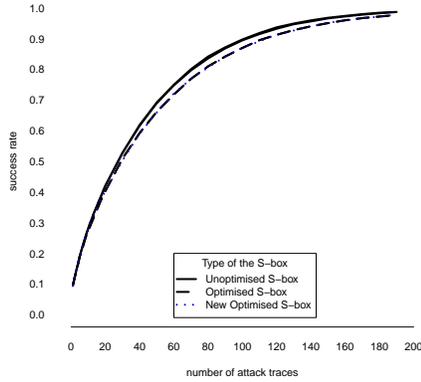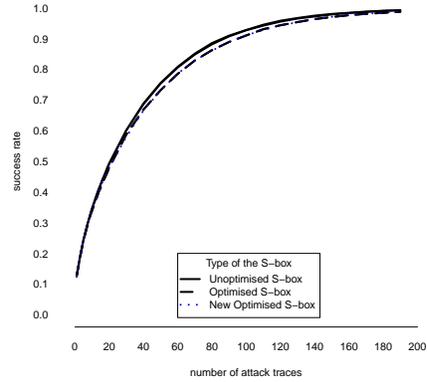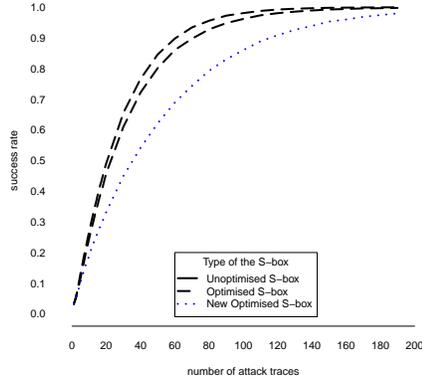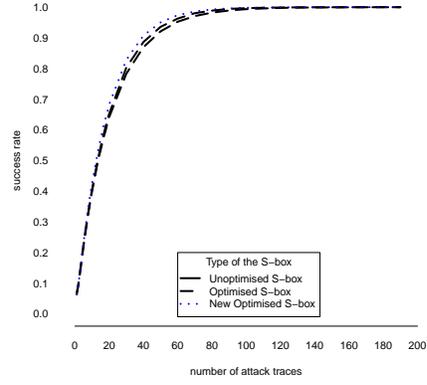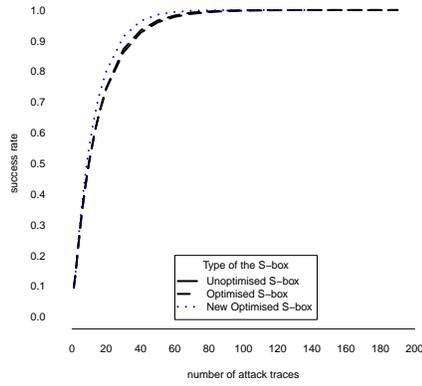Fig. 4: Success rate of correlation power analysis on $\mathbf{5 \times 5}$ S-boxes as a function of the number of attack traces. The standard deviation of the noise equals $\sigma = \mathbf{2}$. The S-boxes have nonlinearity equal to $N_F = \mathbf{12}$ and differential uniformity equal to $\delta_F = \mathbf{2}$.
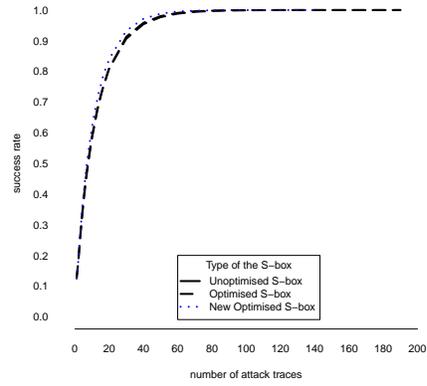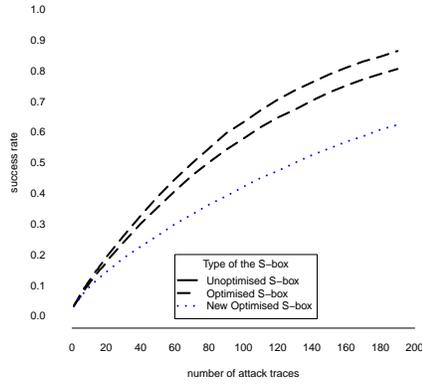
(a) First order success rate.

(b) Second order success rate.

(c) Third order success rate.

(d) Fourth order success rate.

Fig. 5: Success rate of correlation power analysis on $\mathbf{5} \times \mathbf{5}$ S-boxes as a function of the number of attack traces. The standard deviation of the noise equals $\sigma = \mathbf{4}$. The S-boxes have nonlinearity equal to $N_F = \mathbf{12}$ and differential uniformity equal to $\delta_F = \mathbf{2}$.

(a) First order success rate.

(b) Second order success rate.
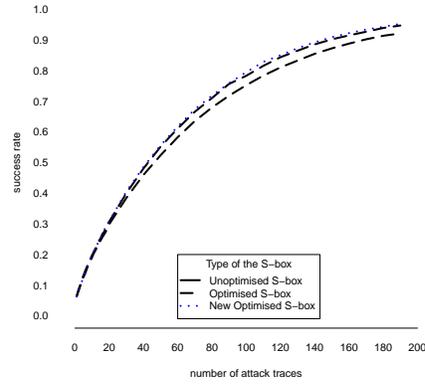
(c) Third order success rate.

(d) Fourth order success rate.

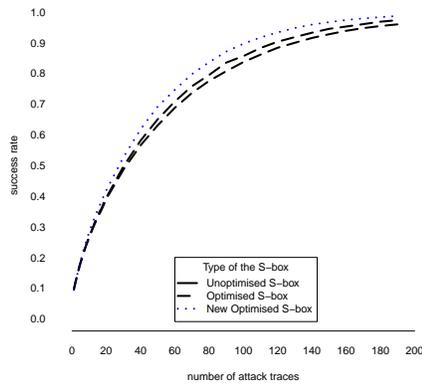Fig. 6: Success rate of correlation power analysis on $\mathbf{5} \times \mathbf{5}$ S-boxes as a function of the number of attack traces. The standard deviation of the noise equals $\sigma = \mathbf{2}$. The S-boxes have nonlinearity equal to $N_F = \mathbf{10}$ and differential uniformity equal to $\delta_F = \mathbf{4}$.
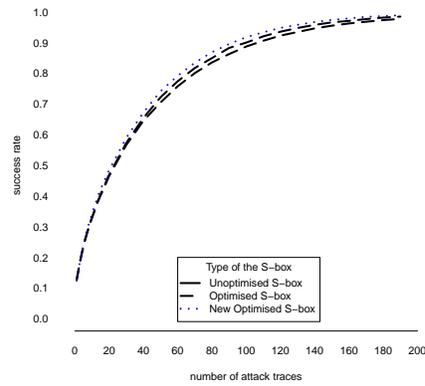
(a) First order success rate.

(b) Second order success rate.

(c) Third order success rate.

(d) Fourth order success rate.

Fig. 7: Success rate of correlation power analysis on $\mathbf{5} \times \mathbf{5}$ S-boxes as a function of the number of attack traces. The standard deviation of the noise equals $\sigma = \mathbf{4}$. The S-boxes have nonlinearity equal to $N_F = \mathbf{10}$ and differential uniformity equal to $\delta_F = \mathbf{4}$.