On the Construction of Side-Channel Attack Resilient S-boxes

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

[1] Quality and Security of Information Systems, Département d'Informatique,
Université libre de Bruxelles, Belgium

[2] KU Leuven ESAT/COSIC and imec, Kasteelpark Arenberg 10, B-3001
Leuven-Heverlee, Belgium

Abstract. Side-channel attacks exploit physical characteristics of implementations of cryptographic algorithms in order to extract sensitive information such as the secret key. These physical attacks are among the most powerful attacks against real-world crypto-systems. In recent years, there has been a number of proposals how to increase the resilience of ciphers against side-channel attacks. One class of proposals concentrates on the intrinsic resilience of ciphers and more precisely their S-boxes. A number of properties has been proposed such as the transparency order, the confusion coefficient and the modified transparency order. Although results with those properties confirm that they are (to some extent) related with the S-box resilience, there is still much to be investigated. There, the biggest drawback stems from the fact that even S-boxes with the best possible values of those properties have only slightly improved side-channel resistance. In this paper, we propose to construct small sized S-boxes based on the results of the measurements of the actual physical attacks. More precisely, we model our S-boxes to be as resilient as possible against non-profiled and profiled physical attacks. Our results highlight that we can design 4×4 and 5×5 S-boxes that possess increased resistance against various real-world attacks.

Keywords: S-box construction, Lightweight cryptography, Genetic algorithms, Side-channel analysis, Correlation power analysis, Template attacks.

1 Introduction

The pervasive presence of interconnected lightweight devices has lead to a massive interest in security features provided among others by cryptography. For decades, designers estimated the security level of a cryptographic algorithm independently of its implementation in a cryptographic device. However, since the publication on implementation attacks in the mid-nineties, the physical attacks have become an active research area by analysing physical leakages measured on the target cryptographic device [1]. The rationale is that there is a relationship between the manipulated data (e.g., the secret key), the executed operations and the physical properties observed during the execution of the cryptographic algorithm by a device. A side-channel attack (SCA) represents a process that exploits leakages in order to extract sensitive information such as the key. This paper analyses the non-linear part (called S-boxes) of ciphers, which is often targeted by implementation attacks. Note that other functions could be analysed, which constitutes an interesting future work.

Three categories of countermeasures against physical attacks exist: masking, hiding and leakage resiliency. Masking blinds sensitive operations (manipulating key-related information) using random numbers and hiding minimises the signal-to-noise ratio in the leakage by shuffling operations or adding a noise generator. Leakage resiliency regularly updates the secret key in order to prevent the aggregation of information from several leakages. The extreme constraints of Radio-Frequency Identification based on chip (in short RFID tags) as well as the hostile environments in which the RFID tags are manipulated raise the need of lightweight countermeasures against side-channel attacks minimising the power consumption, the clock cycles, and the used random numbers.

In 2014, Picek *et al.* generated S-boxes of various sizes providing high resistance to physical attacks without the need of extra random numbers (like masking or shuffling) during the execution of cryptographic primitives [2]. More precisely, 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 exhaustive search) lies in the execution time of the research: exhaustive search generates 2^{2^n} different $n \times n$ S-boxes[3] while genetic algorithms optimise this research 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 (representing another metric related to the side-channel resistance of the S-boxes) [3]. Finally, Picek *et al.* built a 4×4 S-box using genetic algorithms optimising an improved transparency order [4].

Our Contributions The success probability (also known as success rate) represents the probability of an adversary to extract the sensitive information from physical leakages measured on the target device. This (security) metric provides the strength of a strategy against an implementation. Surprisingly, all the previous works generated S-boxes by optimising the properties (e.g., confusion coefficient) related with the side-channel resilience, but up to now no one explored whether it is possible to design S-boxes with the success rate as a metric, i.e., by obtaining it already in the design phase of the S-boxes and not only a posteriori.

In this paper, we shed new insights on the generation of S-boxes by focusing on a security metric that is directly related to the strength of a side-channel adversary. More precisely, we provide several S-boxes minimising the success probability of two well-known side-channel attacks called (non-profiled) correlation power analysis and (profiled) template attacks. Correlation power analysis represents the state-of-the-art when considering non-profiled attacks while template

[3] $(2^n)!$ if we only consider permutations.

attacks are the most powerful physical attacks from an information theoretic point of view.

Furthermore, we present the first 5×5 S-boxes minimising the security metric that can be directly exploited in cryptographic primitives.

Differing from previous works, we also consider S-boxes where their inverse has good resilience against side-channel attacks. This approach is of high importance since the attacker can concentrate either on the first round and the plaintext or the last round and the ciphertext (in which case the inverse of the S-box is targeted) during the side-channel attack phase.

Finally, to depict the increased resilience of our new S-boxes, we also design S-boxes that provide the worst resilience regarding the considered physical attacks as well as the considered devices. Following the kleptography concept [5], these results highlight that malicious designers of cryptographic primitives can weaken a target device (or family of devices) by carefully selecting an S-box (that still has good cryptographic properties) for the cipher.

We provide all the new (4×4 and 5×5) S-boxes in Table 1 and in Table 2 taking into account respectively non-profiled attacks and profiled attacks. Our results can be of major value (1) for industry that wants to (easily and quickly) increase the protection of the executed cryptographic primitive according to the considered device, and (2) for the scientific community that can pursue research on lightweight countermeasures with different optimisation goals.

Cautionary Note This paper relates to the protection of one low-cost party in a communication protocol that involves (for example) an RFID tag and an RFID reader. More precisely, we assume that an RFID tag (having strong cost constraints) requires lightweight countermeasures (provided in this paper) while the RFID readers (implementing the same cryptographic primitive or its inverse) can be protected with more expensive means such as masking and shuffling. Indeed, in this paper we provide S-boxes having good resilience against side-channel attacks when we implement these S-boxes in a specific device (such as an RFID tag) while this protection could be undermined (by a physical attack) when they are implemented in other devices (such as RFID readers) having different physical characteristics. Note however that our approach can be generalised to protect several devices at the same time, which constitutes a future work.

Outline This paper is organised as follows. Section 2 starts with the basic notions of relevant cryptographic properties and side-channel attacks. Moreover, this section discusses about the evaluation procedure from the side-channel attacks perspective. Next, Section 3 presents our search strategy as well as the obtained results. Finally, Section 4 provides conclusions of the paper and gives several directions for future works.

2 Background

2.1 Cryptographic Properties of S-boxes

Let $\mathbb{F}_2^n$ be the vector space that contains all the n-bit binary vectors. Let F be a substitution box (denoted S-box). S-boxes provide the confusion property in cryptographic primitives by substituting values from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ (denoted as an S-box $n \times m$ as well as an (n, m)-function). The S-box can be seen as a vector of m Boolean functions $[\mathsf{F}_1, \mathsf{F}_2, ..., \mathsf{F}_m]$ where each Boolean function represents a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.

We denote the inner product of two vectors $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1})$ as $a \cdot b$ (which is equal to $a \cdot b = \oplus_{i=1}^n a_i b_i$). The Hamming weight of a vector $a \in \mathbb{F}_2^n$ (denoted $\mathsf{HW}(a)$) represents the number of non-zero positions in the vector.

The **nonlinearity** N_F of an (n, m)-function F is equal to the minimum nonlinearity of all non-zero linear combinations $v \cdot \mathsf{F}$, with $v \neq 0$, of its coordinate functions F_i, i.e.:

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

where $\|x\|$ symbolises the absolute value of x, and $W_{\mathsf{F}}(a, v)$ represents the Walsh-Hadamard transform of F that is equal to:

$$W_{\mathsf{F}}(a, v) = \sum_{x \in \mathbb{F}_2^m} (-1)^{v \cdot \mathsf{F}(x) + a \cdot x}, \ a \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m. \tag{2}$$

The nonlinearity N_F of any (n, n)-function F must satisfy the inequality:

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

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

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

$\delta(a, b)$ denotes the cardinality of $\mathsf{D}(a, b)$ and

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

Almost Bent (AB) functions contain an equality in Eq. (3) while when a function is differentially 2-uniform, it is called Almost Perfect Nonlinear (APN) function. Every AB function is also APN, but the other direction 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. Furthermore, the maximal algebraic degree of AB functions equals $(n + 1)/2$ while for the inverse APN equals $n - 1$. We refer to the following papers [6, 7] for the interested readers about the theory of Boolean functions and S-boxes.

Leander and Poschmann define optimal 4-bit S-boxes as being bijective, with the minimal possible linearity (or, maximal possible nonlinearity) and with a minimal differential uniformity. For optimal 4×4 S-boxes, both N_F and the differential uniformity are equal to 4 [8]. PRESENT considers S-boxes from the 16 classes suggested by Leander and Poschmann [8], but some lightweight ciphers use 4×4 S-boxes with different cryptographic conditions. For instance, the authors of the PRINCE cipher impose several additional criteria on the 4×4 S-box and therefore they accept only 8 out of the 16 classes [9].

When considering 5×5 S-boxes, the cryptographic properties one can obtain differ with regards to the choice of the S-box. As a first example, we consider the Keccak S-box for which both the nonlinearity and differential uniformity are equal to 8 [10]. Note that those values are relatively far from the optimal ones. Furthermore, the algebraic degree of Keccak is low, and it actually equals the minimal possible algebraic degree for a nonlinear function. However, the Keccak S-box has an extremely efficient hardware implementation. The S-box used in Ascon [11] is an affine transformation of the Keccak S-box in order to remove the fixed points and to increase the differential branch number value. On the other hand, the PRIMATEs S-box [12] is based on an almost bent permutation, which means it has a nonlinearity equal to 12 and a differential uniformity equal to 2, while the algebraic degree equals 2.

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 following, we systematically use the term key to denote the target of our attacks, though, in fact, we address one byte 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)

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

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

Physical Characteristics Let ${}^{j}T_i$ be the j-th leakage (also known as trace) measured when the device manipulates the target value y_i. In the following, we represent each leakage with a vector of real values (of length n_s) measured at different instants on the analysed device. We denote ${}^{j}_{t}T_i$ the j-th leakage (associated to the target value y_i) measured at time t such that:

$${}^{j}_{t}T_i = {}_{t}\mathsf{L}\left(\mathsf{F}_k\left(p\right)\right) + {}^{j}_{t}\epsilon_i, \tag{7}$$

where ${}^{j}_{t}\epsilon_i \in \mathbb{R}$ is the noise of the trace ${}^{j}_{t}T_i$ following for example a Gaussian distribution with zero mean, and ${}_{t}\mathsf{L}$ is the (deterministic) leakage function at time t. The function ${}_t\mathsf{L}$ 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_i 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 such as the Correlation Power Analysis (CPA) [13] and Template Attack (TA) [14]. We refer to the work of Chakraborty *et al.* [15] for a detailed description of the improved transparency order metric and to the work of Fei *et al.* introducing the confusion coefficient that evaluates the resistance of S-boxes against side-channel attacks in a theoretical point of view [16,17].

Correlation Power Analysis CPA 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, CPA selects the secret key $\widehat{k}$ such that:

$$\widehat{k} \in \underset{k\in\mathcal{K}}{\arg\max} \left\| \rho\left(\widehat{\mathcal{T}}_{(k)}, \mathcal{T}\right) \right\|, \tag{8}$$

where $\rho\left(\mathcal{X}, \mathcal{Y}\right)$ represents the Pearsons correlation between 2 lists $\mathcal{X}$ and $\mathcal{Y}$, and:

- $\mathcal{T} = \left[{}^1T, ..., {}^{N_a}T\right]$ represents a list of N_a 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
- $\widehat{\mathcal{T}}_{(k)} = \left[\widehat{\mathsf{L}}(\mathsf{F}(k \oplus p_{[1]}), ..., \widehat{\mathsf{L}}(\mathsf{F}(k \oplus p_{[N_a]})\right]$ refers to a list 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 ${}^iT$.

Template Attacks (Gaussian) Template attacks assume that $\Pr\left[{}^jT_i \mid y_i\right]$ follows a Gaussian distribution $\mathcal{N}(\hat{\mu}_i, \hat{\Sigma}_i)$ for each value y_i where $\hat{\mu}_i \in \mathbb{R}^{n_s}$ and $\hat{\Sigma}_i \in \mathbb{R}^{n_s \times n_s}$ are respectively the sample mean and the sample covariance matrix of the traces associated to y_i. In what follows we assume that the noise is independent of y_i in unprotected contexts. This property allows to estimate the same physical noise (represented by Σ) for all the target values.

During the attack step, the adversary classifies the list $\left[{}^1T, ..., {}^{N_a}T\right]$ by using:

$$\hat{k} \in \underset{k\in\mathcal{K}}{\arg\max} \prod_{j=1}^{N_a} \Pr\left[{}^jT \mid k, p_j\right] \times \Pr\left[k, p_j\right], \tag{9}$$

$$\approx \underset{k\in\mathcal{K}}{\arg\max} \prod_{j=1}^{N_a} \hat{\Pr}\left[{}^jT \mid y_i = \mathsf{F}_k(p_j); \hat{\theta}_i\right] \times \hat{\Pr}\left[y_i = \mathsf{F}_k(p_{[j]})\right], \tag{10}$$

where $\hat{\theta}_i$ denotes the two parameters $\{\hat{\mu}_i, \hat{\Sigma}_i\}$.

The designers of cryptographic devices measure the resistance of an implementation against a physical attack by using (among others) the first order Success Rate (SR) [18]. The success rate (also known as the success probability) represents the probability that the physical attack extracts the secret key.

3 Experiments

Table 1 and Table 2 display all the generated 4×4 and 5×5 S-boxes taking into account respectively the correlation power analysis and the template attacks. We note that all presented 4×4 S-boxes also have maximal possible algebraic degree that is equal to 3. For the 5×5 size, algebraic degree varies from 2 to 4 where we note that for all optimal S-boxes it equals 2 (since optimal 5-bit S-boxes are actually AB functions, meaning that the algebraic degree is upper bounded with $\frac{n+1}{2}$ that equals to 3). Note that our new 5×5 S-boxes have better nonlinearity and differential uniformity values than Keccak or Ascon, but we can easily adapt our strategy to output S-boxes with any combinations of values.

In order to compare our generated S-boxes we used the following existing S-boxes:

- 4×4 S-boxes: Evolved$_{\mathrm{CC}}$ [3], Evolved$_{\mathrm{TO}}$ [4], Klein [19], PRESENT [20] and PRINCE [9];
- 5×5 S-boxes: ASCON [11], Keccak (Ketje, Keyak) [21] and PRIMATE [22].

The S-boxes Evolved$_{\mathrm{CC}}$ and Evolved$_{\mathrm{TO}}$ were also generated using genetic algorithms while taking into account theoretical metrics (i.e., the confusion coefficient and the modified transparency order) in order to estimate their resistance against side-channel attacks.

3.1 Search Strategy

We use a genetic algorithm (GA) exploiting simple variation operators and solution encodings. We follow this line of research in an effort to make our search process as fast as possible as well as to make comparison with previous works as fair as possible. We encode solutions as lists of values between 0 and $2^n - 1$ where n is the size of the S-box. Note that this representation (i.e., permutation encoding) is highly efficient since this ensures that solutions are bijections (which is a necessary condition we enforce on our S-boxes).

We use the tournament selection mechanism in order to avoid the need to tune the crossover rate parameter. We work with the 3-tournament selection which is the option that offers the fastest convergence [23]. This mechanism selects three solutions randomly and discards the worst solution. Then, from the remaining two solutions, the crossover operator creates a new offspring. For variation operators, we use the Toggle mutation and the Order crossover. In the Toggle mutation we randomly select two values and swap them. The Order crossover (OX) works by first randomly selecting two crossover points and copying everything between those two points from the first parent to the offspring.

Size	Name	N_F	δ_F	Strategy	S-box
4×4	Evolved$_{SR1}$	4	4	F	2,4,8,0,F,B,7,D,6,5,E,3,1,9,C,A
	Evolved$_{SR2}$	4	4	$F+I$	F,E,0,A,1,8,9,B,7,6,4,C,5,2,3,D
	Evolved$_K$	4	4	K	0,F,1,9,B,5,8,2,E,3,C,6,D,4,A,7
5×5	Evolved$_{SR1}$	8	6	F	1E,07,15,02,0E,09,19,04,17,12,0B,08,1C,0A,1D,06 0C,1B,05,0D,00,14,18,1F,10,13,11,1A,01,16,03,0F
	Evolved$_{SR2}$	8	6	$F+I$	15,02,1F,0A,19,11,1B,12,08,0E,0C,07,06,0F,10,16 13,00,17,09,1D,18,0D,03,04,1A,14,1C,05,1E,01,0B
	Evolved$_{SR3}$	10	6	$F+I$	1D,15,03,02,1C,0A,0C,09,11,10,1F,0D,18,14,19,16 06,12,0F,17,01,04,13,1B,0B,07,0E,05,1A,1E,00,08
	Evolved$_{SR4}$	10	4	$F+I$	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$_{SR5}$	8	6	F	04,17,1C,18,07,00,12,19,0E,14,10,15,06,13,1F,08 1A,11,0C,0B,05,1E,0F,01,02,1D,1B,09,0D,03,0A,16
	Evolved$_{SR6}$	8	4	F	09,05,1E,1C,0D,16,14,06,07,1D,01,10,03,02,13,1F 1B,15,08,18,04,00,0F,1A,0A,12,0B,0E,19,17,11,0C
	Evolved$_{SR7}$	10	4	F	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	F	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	$F+I$	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
	Evolved$_K$	8	4	K	15,07,06,03,18,0E,04,01,0C,05,0A,16,1F,1D,19,13 12,0F,11,1B,09,1A,17,10,08,0B,00,14,02,1C,1E,0D

Table 1: Properties of evolved S-boxes when considering correlation power analysis. Values of S-boxes are given in hexadecimal format. Strategy F represents S-boxes optimised for the success rate. Strategy $F+I$ represents S-boxes optimised in the forward direction as well as their inverse. Strategy K represents S-boxes optimised for the kleptography concept.

Then, starting from the second crossover point in the second parent, the unused numbers are copied in the order they appear in that parent [23]. The initial population is created uniformly at random and the population size equals 100. As a termination criterion, we use the number of evaluations without improvement, which we set here to 100 generations.

In our experiments, we maximise the nonlinearity while minimising the differential uniformity as well as the success probability (denoted SR), hence the subtraction from 2^n value and 1, respectively:

$$\mathsf{fitness} = N_F + (2^n - \delta_F)) + (1 - \mathsf{SR}). \tag{11}$$

We give equal weights to both N_F and δ_F since our experiments show there is no statistically significant difference in those two cases[4].

[4] Note that in general case of a fitness function it is possible to sacrifice one parameter in order to boost another. However, in our case it is impossible to sacrifice the

Size	Name	N_F	δ_F	Strategy	S-box
4 × 4	EvolvedTA$_{SR1}$	4	4	F	`0,5,7,C,A,6,2,4,9,8,B,F,D,E,1,3`
	EvolvedTA$_{SR2}$	4	4	$F+I$	`4,2,D,E,B,1,6,5,7,8,3,A,F,0,C,9`
	EvolvedTA$_{SR3}$	4	4	F	`9,4,5,D,3,0,1,F,B,2,C,7,E,8,A,6`
	EvolvedTA$_{SR4}$	4	4	$F+I$	`4,0,6,7,1,2,A,F,5,3,C,E,D,9,B,8`

5 × 5	EvolvedTA$_{SR1}$	8	6	F	`1F,15,01,0C,14,1D,12,00,1A,09,08,17,05,0E,0B,0d`
					`04,18,1B,0A,13,11,06,1E,10,19,16,02,0F,07,03,1c`

	EvolvedTA$_{SR2}$	10	6	$F+I$	`07,14,1D,11,12,02,06,13,19,0F,09,0C,1C,15,0A,08`
					`01,0B,1F,0D,03,17,1E,05,04,1B,0E,00,1A,18,10,16`

	EvolvedTA$_{SR3}$	12	2	F	`1F,01,02,1A,04,1B,15,0C,08,1E,17,07,0B,1C,18,09`
					`10,0D,1D,06,0F,13,0E,14,16,03,19,0A,11,05,12,00`

	EvolvedTA$_{SR4}$	12	2	$F+I$	`1F,01,02,1E,04,0E,1D,15,08,13,1C,05,1B,14,0B,06`
					`10,0F,07,1A,19,12,0A,03,17,0D,09,11,16,18,0C,00`

	EvolvedTA$_{SR5}$	10	4	F	`01,13,11,16,0F,03,08,10,0B,1A,02,1B,0C,1E,17,12`
					`19,0D,14,00,05,04,18,07,1F,1D,06,15,0A,1C,0E,09`

	EvolvedTA$_{SR6}$	8	4	$F+I$	`1F,15,18,05,01,06,08,0B,12,02,17,0D,03,1C,04,16`
					`0F,1B,09,13,0C,11,1E,1A,00,19,0A,07,1D,14,0E,10`

Table 2: Properties of S-boxes Evolved for ATMega 328 microcontroller using template attacks. Values of S-boxes are given in hexadecimal format. Strategy F represents S-boxes optimised for the success rate. Strategy $F+I$ represents S-boxes optimised in the forward direction as well as their inverse.

Regarding the complexity of our search strategy, on average one generation (100 individuals) needs around 1 second to evolve. In that estimation we include the cost of the evaluation of the cryptographic properties, but not the cost of the evaluation of the attack strategy. We note that although here we work with GA, our methodology is not exclusive for that algorithm, but it could work with any other heuristics that supports the permutation encoding. Naturally, it is to be expected that in such case one could also need to change the fitness function and the stopping criterion. For further details about genetic algorithms, we refer readers to the work of Eiben and Smith [23].

3.2 Results for Correlation Power Analysis

We generated synthetic leakages by considering that the leakage function equals to the Hamming weight and the leakage model (of the adversary) also equals to the Hamming weight (i.e., the adversary has a perfect knowledge on how the device leaks information). We use the same level of noise of 0.5 variance representing a signal-to-noise ratio (1) of 2.13 when considering 4 × 4 S-boxes,

nonlinearity N_F in order to improve the success rate due to the fact that $N_F \in \mathbb{N}$ and $\mathsf{SR} \in \mathbb{R}$ and $0 < \mathsf{SR} < 1$. In other words the minimal step in values of N_F is 1, while 1 is the maximum increase that the SR can get, thus, the whole $\mathsf{fitness}$ will decrease if N_F decreases while boosting the SR.

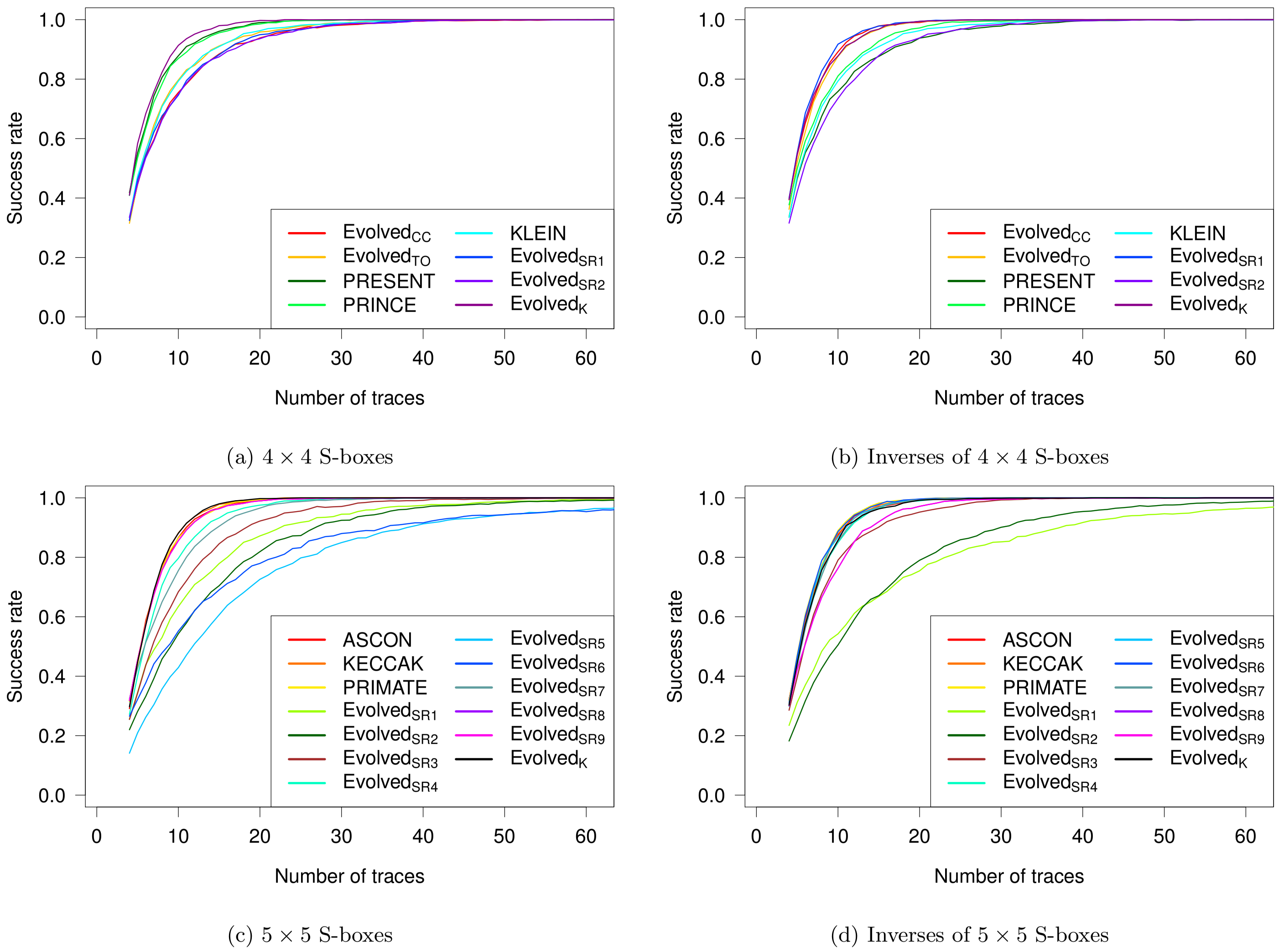
and (2) of 2.58 when considering 5×5 S-boxes. It is worth to note that the order of the (generated) S-boxes sorted by the resistance against SCA are not influenced by the signal-to-noise ratio.

Figure 1 provides the success rate of CPA on the (three) new generated S-boxes as well as their inverses. The first observation is that the nonlinearity of an S-box and its delta uniformity are not the (only) metrics impacting side-channel attacks (e.g., all the 4×4 S-boxes have the same nonlinearity and delta uniformity but differ from the point of view of side-channel). Furthermore, the generated S-boxes (by taking into account only the forward direction) as well as the already known S-boxes are weak (in a side channel point of view) when considering adversary targeting the last round of the cipher (i.e., attacking the inverse of the S-boxes). However, the generated S-boxes taking into account such adversary provide good side-channel resistance in forward and in inverse direction. The new 4×4 S-box $\mathrm{Evolved}_{\mathrm{SR2}}$ happens to be the best generated S-box among all of the considered S-boxes. In a kleptography point of view, the generated 4×4 $\mathrm{Evolved}_{\mathrm{K}}$ turns out to be the best: it has good cryptographic properties and it is the easiest S-box to attack using side-channel information. Note that the S-boxes $\mathrm{Evolved}_{\mathrm{CC}}$ and $\mathrm{Evolved}_{\mathrm{TO}}$ differ from a side-channel point of view. The rationale is that the confusion coefficient and the modified transparency order are not equivalent, as already reported by Lerman *et al.* [24].

Regarding the 5×5 S-boxes, we generated several S-boxes having different cryptographic properties (by varying the value of the differential uniformity and the nonlinearity metrics). This palette of S-boxes gives rise to 9 S-boxes having different levels of resistance against side-channel attacks. All the generated S-boxes provide a higher resistance compared to the existing (considered) S-boxes while having good cryptographic properties. This allows the designer to choose S-boxes among several S-boxes with cryptographic properties that fit his requirements.

3.3 Results for Template Attacks

A set of 80 000 power traces was collected on an 8-bit Atmel (ATMega 328) microcontroller at a 16 MHz clock frequency. The power consumption of the device was measured using an Agillent Infiniium 9 000 Series oscilloscope that was set up to acquire 200 MSamples/s. In order to measure the device's power consumption we inserted a 10 Ω resistor placed between the ground pin of the microcontroller and the ground of the power supply. In order to reduce noise in traces we used averaging, thus each power trace represents an average of 64 single acquisitions. Our target device executes AES using a constant 128-bit key and random plaintexts. We target the first round of the cipher and focus on the first byte of the key. We extracted the leakage function ${}_t\mathsf{L}$ of the device by averaging all traces associated to the same target value and by selecting the 8 instants that are the most (linearly)nonlinearityated with the target value. We used the extracted leakage function during our simulations with a small



(a) 4 × 4 S-boxes

(b) Inverses of 4 × 4 S-boxes

(c) 5 × 5 S-boxes

(d) Inverses of 5 × 5 S-boxes

Fig. 1: Success rate of correlation power analysis on 4 × 4 and 5 × 5 S-boxes.

additional Gaussian noise[5] having a standard deviation of 5×10^{-6}. This leads to a signal-to-noise ratio of 0.40 and 0.37 for the best point when considering respectively an 4×4 S-box and an 5×5 S-box. It is worth to note that we do not claim in this paper that this profiled attack represents the optimal physical attack against the analysed implementation. Other profiled attacks could provide higher success rates [25]. In other words, our purpose here is to provide S-boxes resilient against *chosen* profiled attacks.

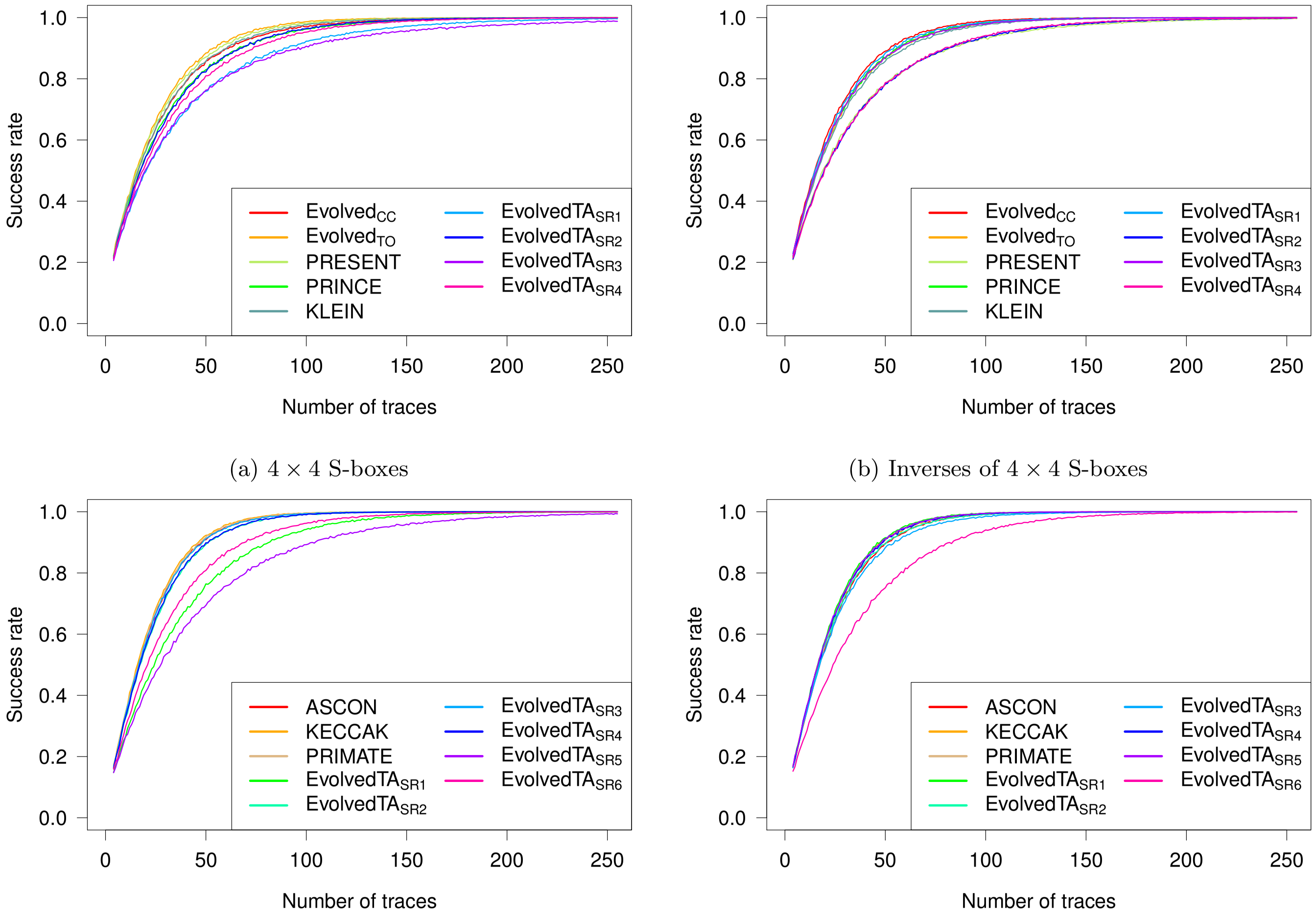
Figure 2 shows the success rate of template attacks on the considered S-boxes. We can notice that Figure 2a and Figure 2b show results similar to the results that we obtain in the previous section: when we consider well-known S-boxes or newly generated S-boxes (while considering only the forward strategy) the corresponding inverse S-boxes show them weaker against side-channel attacks. The 4×4 EvolvedTA$_{\mathrm{SR2}}$ S-box that was generated by taking into account the S-box and its inverse gives the best result: it is as good as PRESENT S-box in terms of its inverse and it is one of the best among well known 4×4 S-boxes (in the forward direction) with the exception of 4×4 EvolvedTA$_{\mathrm{SR1}}$ that was designed to be good in the forward direction (but not as an inverse). In terms of 5×5 S-boxes, 5×5 EvolvedTA$_{\mathrm{SR5}}$ provides the best result in forward direction. In the inverse direction, EvolvedTA$_{\mathrm{SR6}}$ outperforms all the known S-boxes. Note that it is still difficult to create resilient S-boxes while having good cryptographic properties and being better than existing S-boxes in both forward and inverse directions. However, we deem that we can still create a more resilient 5×5 S-box against template attacks since 5×5 S-boxes provide a large set of possible solutions.

3.4 Discussion

The previous sections report the improvement of the success probability of physical attacks on 4×4 and 5×5 S-boxes. Our results highlight that the improvement is more significant for the 5×5 S-boxes than for the 4×4 S-boxes. The reason relies on the fact that 5×5 S-boxes have a wider range of obtainable values for the success rate property when compared with 4×4 S-boxes.

Figure 3 provides the success rate on each S-box targeted by an adversary exploiting the plaintext (by attacking the forward S-box used in the first round of the cryptographic primitive) and the ciphertext (by attacking the inverse S-box used in the the last round of the primitive). Plots on these figure correspond to the maximum of the two attacks (between the attack on an S-box and on its inverse). The results highlight the usefulness of our approach by providing new S-boxes outperforming well known S-boxes in several contexts. More precisely, the 4×4 Evolved$_{\mathrm{SR2}}$ and the 5×5 Evolved$_{\mathrm{SR2}}$ S-boxes provide the best results against correlation power analysis while the 4×4 EvolvedTA$_{\mathrm{SR4}}$ and the 5×5 EvolvedTA$_{\mathrm{SR6}}$ S-box provide the best results against template attacks.

[5] A small amount of noise is necessary in order to avoid numerical issues during template attacks.



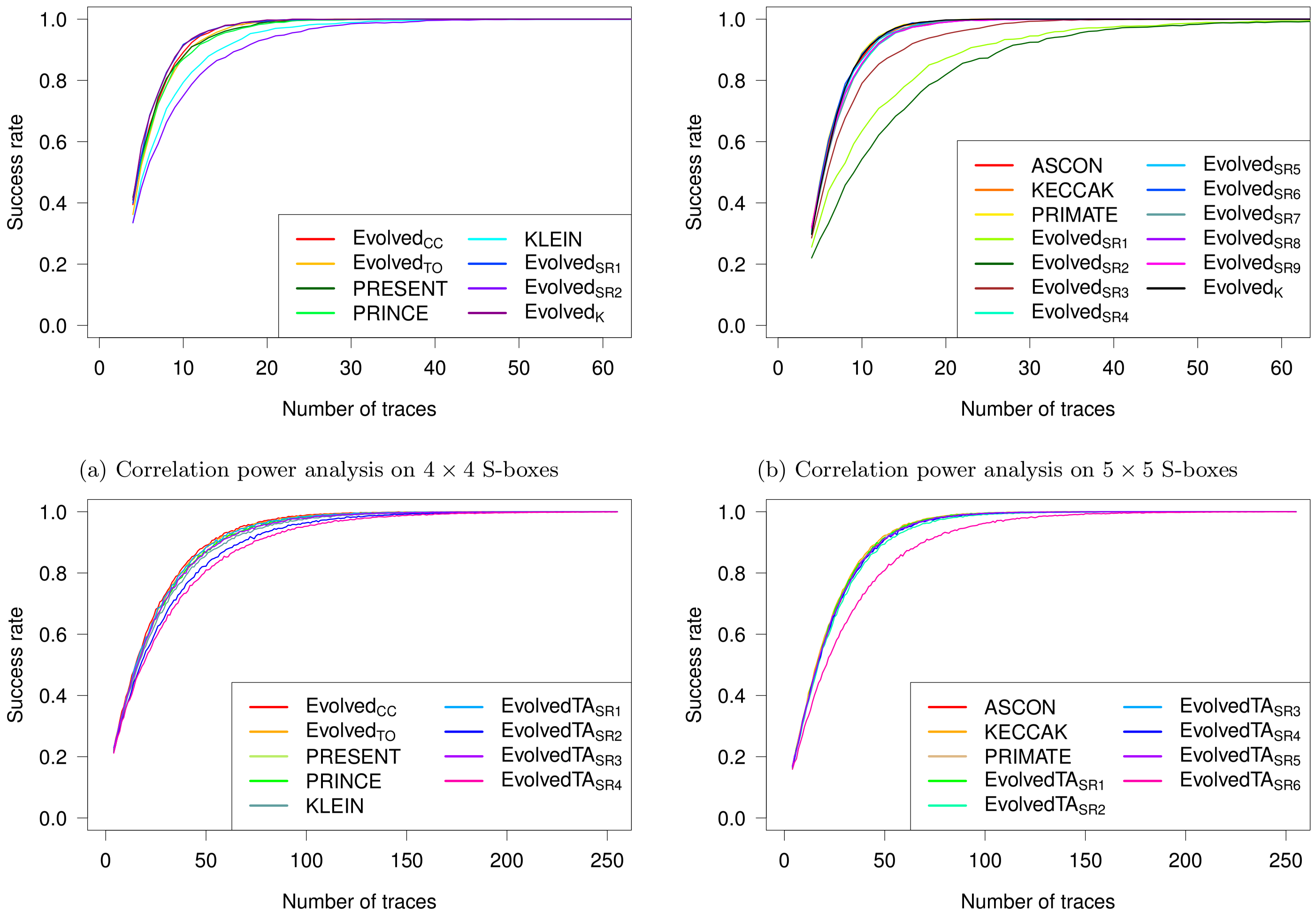
(a) 4 × 4 S-boxes

(b) Inverses of 4 × 4 S-boxes

(c) 5 × 5 S-boxes

(d) Inverses of 5 × 5 S-boxes

Fig. 2: Success rate of template attacks on 4 × 4 and 5 × 5 S-boxes.



(a) Correlation power analysis on 4 × 4 S-boxes

(b) Correlation power analysis on 5 × 5 S-boxes

(c) Template attacks on 4 × 4 S-boxes

(d) Template attacks on 5 × 5 S-boxes

Fig. 3: Maximum success rate between attacks on the first round (S-box) and last round (inverse of the S-box) of an algorithm.

Note also that all our results report the success rate of adversaries targeting *one* nibble of the key. It is worth to note that, in practice, adversaries extract the *full* secret key. As a result, a small-scale decrease of the first order success rate of an attack on one nibble leads to a significant reduction of the success probability of the attack on the full key. Therefore, designers of cryptographic primitives should consider optimisation methods minimising the success rate of physical attacks against S-boxes. As an example, let us take two 4 × 4 S-boxes with similarly close success rates: Evolved_K and the S-box of PRESENT. During a CPA using 15 attack traces, Evolved_K results in success rate of 0.9820 while the S-box of PRESENT gives the success rate of 0.9605 (difference of about 0.02). However, it is important to note that this success rate corresponds to an attack on one 4-bit nibble. During an attack on a full cipher with 80-bit key, the adversary repeats the attack on each nibble (i.e., 20 times). Thus, the success rate of a complete attack results in the success rate of 0.4466 on the PRESENT S-box and 0.6954 in case of Evolved_K which is a significant increase even though the success rates of attacks on one nibble are very close.

4 Conclusions and Future Work

In this paper, we investigate the design of S-boxes containing inherent resilience against various real-world physical attacks. The main difference between our work and the previous works lies in the design process of the S-boxes: previous works design S-boxes optimising metrics (e.g., confusion coefficient) that (according to the authors of these metrics) relate to the side-channel resilience while we take into account (during the design phase of the S-boxes) the quality of the generated S-boxes against actual physical adversaries. The rationale of our approach is that we remove the unnecessary step of connecting the value of a certain property (e.g., confusion coefficient) to a certain type of attack. Our results also highlight that such measures (e.g., confusion coefficient) can indicate the resilience but should not be used as a definitive guide in order to estimate the success probability of physical attacks [3, 24]. As a result, we provide the first S-boxes in which the countermeasure is automatically tailored for the device used by the implementers.

Our outcomes also generalise the results of previous works (that focus on the case where the adversary knows only the plaintexts) by considering that the adversary can target the first round (i.e., the S-box) as well as the last round (i.e., the inverse of the S-box) of the primitive when the adversary knows the plaintexts and the ciphertexts.

We conduct our analysis for S-boxes of sizes 4 × 4 and 5 × 5 since (1) we deem those sizes to have the most impact in the future design of lightweight ciphers, and (2) our results confirm that it is possible to design S-boxes with better resilience against various classes of side-channel attacks.

Several directions for future works exist. For example, an interesting perspective would be to work with involutive S-boxes. Ciphers with involutive S-boxes have smaller area cost than those having separate S-boxes for encryption and decryption. The main difficulty of this future work lies in the definition of a new search strategy in order to stay only in the involutive S-boxes search space. Other future works may explore additional criteria for the fitness function such as the size of an S-box in hardware (e.g., by counting the number of gates).

Another direction of future work considers other physical attacks like stochastic attacks [26], mutual information analysis [27] and machine learning attacks [28–30]. Going even one step further, a designer could find S-boxes that (1) possess improved resilience against more than one type of attack, and (2) could be implemented in several devices (having different leakage functions).

Finally, the new proposed S-boxes can be combined with (more expensive) side-channel countermeasures such as masking. One of the easiest generic masking scheme (called *table re-computation*) computes a table look-up which associates to each masked input the output of the masked S-box [31]. Designers can easily combine this masking scheme with the new S-boxes. Other masking schemes tailored to the new S-boxes can also be applied, and constitute an interesting future work in order to investigate the resistance of physical cryptographic implementations generated by genetic algorithms against side-channel attacks.

Acknowledgments

L. Lerman is funded by the Brussels Institute for Research and Innovation (Innoviris) for the SCAUT project. S. Picek was supported in part by Croatian Science Foundation under the project IP-2014-09-4882.

References

1. Kocher, P.C.: Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. [32] 104–113
2. 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
3. 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
4. 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
5. Young, A.L., Yung, M.: The dark side of "black-box" cryptography, or: Should we trust capstone? [32] 89–103

6. Carlet, C.: Boolean Functions for Cryptography and Error Correcting Codes. In Crama, Y., Hammer, P.L., eds.: Boolean Models and Methods in Mathematics, Computer Science, and Engineering. 1st edn. Cambridge University Press, New York, NY, USA (2010) 257–397
7. 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, NY, USA (2010) 398–469
8. 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
9. 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
10. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Keccak. In Johansson, T., Nguyen, P., eds.: Advances in Cryptology EUROCRYPT 2013. Volume 7881 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2013) 313–314
11. Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M.: Ascon (2014) CAESAR submission, `http://ascon.iaik.tugraz.at/`.
12. 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) `http://competitions.cr.yp.to/round1/primatesv1.pdf`.
13. 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
14. Chari, S., Rao, J.R., Rohatgi, P.: Template attacks. In Jr., B.S.K., Koç, Ç.K., Paar, C., eds.: Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers. Volume 2523 of Lecture Notes in Computer Science., Springer (2002) 13–28
15. Chakraborty, K., Sarkar, S., Maitra, S., Mazumdar, B., Mukhopadhyay, D., Prouff, E.: Redefining the transparency order. In: WCC2015-9th International Workshop on Coding and Cryptography 2015. (2015)
16. Fei, Y., Luo, Q., Ding, A.A.: A statistical model for DPA with novel algorithmic confusion analysis. In Prouff, E., Schaumont, P., eds.: Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings. Volume 7428 of Lecture Notes in Computer Science., Springer (2012) 233–250
17. Fei, Y., Ding, A.A., Lao, J., Zhang, L.: A statistics-based success rate model for dpa and cpa. Journal of Cryptographic Engineering **5**(4) (2015) 227–243
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, 2009. Proceedings. Volume 5479 of Lecture Notes in Computer Science., Springer (2009) 443–461
19. 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

20. 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
21. Bertoni, G., Daemen, J., Peeters, M., Assche, G.V.: The keccak reference (2011) Submission to NIST (Round 3).
22. Andreeva, E., Bilgin, B., Bogdanov, A., Luykx, A., Mendel, F., Mennink, B., Mouha, N., an Kan Yasuda, Q.W.: PRIMATEs v1.02 (Sept 2014) CAESAR submission.
23. Eiben, A.E., Smith, J.E.: Introduction to Evolutionary Computing. Springer-Verlag, Berlin Heidelberg New York, USA (2003)
24. Lerman, L., Markowitch, O., Veshchikov, N.: Comparing sboxes of ciphers from the perspective of side-channel attacks. In: 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST). (Dec 2016) 1–6
25. Lerman, L., Poussier, R., Bontempi, G., Markowitch, O., Standaert, F.: Template attacks vs. machine learning revisited (and the curse of dimensionality in side-channel analysis). In Mangard, S., Poschmann, A.Y., eds.: Constructive Side-Channel Analysis and Secure Design - 6th International Workshop, COSADE 2015, Berlin, Germany, April 13-14, 2015. Revised Selected Papers. Volume 9064 of Lecture Notes in Computer Science., Springer (2015) 20–33
26. Schindler, W., Lemke, K., Paar, C.: A stochastic model for differential side channel cryptanalysis. In Rao, J.R., Sunar, B., eds.: Cryptographic Hardware and Embedded Systems - CHES 2005, 7th International Workshop, Edinburgh, UK, August 29 - September 1, 2005, Proceedings. Volume 3659 of Lecture Notes in Computer Science., Springer (2005) 30–46
27. Gierlichs, B., Batina, L., Tuyls, P., Preneel, B.: Mutual information analysis. In Oswald, E., Rohatgi, P., eds.: Cryptographic Hardware and Embedded Systems - CHES 2008, 10th International Workshop, Washington, D.C., USA, August 10-13, 2008. Proceedings. Volume 5154 of Lecture Notes in Computer Science., Springer (2008) 426–442
28. Lerman, L., Bontempi, G., Markowitch, O.: Side Channel Attack: an Approach Based on Machine Learning. In: Second International Workshop on Constructive SideChannel Analysis and Secure Design, Center for Advanced Security Research Darmstadt (2011) 29–41
29. Hospodar, G., Gierlichs, B., Mulder, E.D., Verbauwhede, I., Vandewalle, J.: Machine learning in side-channel analysis: a first study. J. Cryptographic Engineering **1**(4) (2011) 293–302
30. Lerman, L., Bontempi, G., Markowitch, O.: Power analysis attack: an approach based on machine learning. IJACT **3**(2) (2014) 97–115
31. Messerges, T.S.: Securing the AES finalists against power analysis attacks. In Schneier, B., ed.: Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings. Volume 1978 of Lecture Notes in Computer Science., Springer (2000) 150–164
32. 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)