Journal of Cryptographic Engineering
https://doi.org/10.1007/s13389-019-00220-8

REGULAR PAPER

Deep learning for side-channel analysis and introduction to ASCAD database

Ryad Benadjila[1] · Emmanuel Prouff[1] · Rémi Strullu[1] · Eleonora Cagli[2] · Cécile Dumas[2]

Received: 25 August 2018 / Accepted: 13 November 2019

Abstract
Recent works have demonstrated that deep learning algorithms were efficient to conduct security evaluations of embedded systems and had many advantages compared to the other methods. Unfortunately, their *hyper-parametrization* has often been kept secret by the authors who only discussed on the main design principles and on the attack efficiencies in some specific contexts. This is clearly an important limitation of previous works since (1) the latter parametrization is known to be a challenging question in machine learning and (2) it does not allow for the reproducibility of the presented results and (3) it does not allow to draw general conclusions. This paper aims to address these limitations in several ways. First, completing recent works, we propose a study of deep learning algorithms when applied in the context of side-channel analysis and we discuss the links with the classical template attacks. Secondly, for the first time, we address the question of the choice of the hyper-parameters for the class convolutional neural networks. Several benchmarks and rationales are given in the context of the analysis of a challenging masked implementation of the AES algorithm. Interestingly, our work shows that the approach followed to design the algorithm VGG-16 used for image recognition seems also to be sound when it comes to fix an architecture for side-channel analysis. To enable perfect reproducibility of our tests, this work also introduces an open platform including all the sources of the target implementation together with the campaign of electromagnetic measurements exploited in our benchmarks. This open database, named ASCAD, is the first one in its category and it has been specified to serve as a common basis for further works on this subject.

Keywords Side-channel analysis · Machine learning · Deep learning

1 Introduction

Side-channel analysis (SCA) is a class of cryptanalytic attacks that exploit the dependency between the execution of a cryptosystem implementation and the manipulated data (e.g. the power consumption or the timing) to recover some *leakage* about its secrets. It is often more efficient than a cryptanalysis mounted in the so-called *black-box model* where no leakage occurs. In particular, *continuous side-channel attacks* in which the adversary gets information at each invocation of the cryptosystem are especially threatening. Common attacks as those exploiting the running-time, the power consumption or the electromagnetic radiations of a cryptographic computation fall into this class. Many implementations of block ciphers have been practically broken by continuous side-channel analysis (see for instance [11,34,45,50]) and securing them has been a long-standing issue for the embedded systems industry.

Side-channel attacks exploit information which leak from the physical implementations of cryptographic algorithms. Since this leakage (e.g. the power consumption or the electromagnetic emanations) depends on some small part of the internally used secret key, the adversary may perform an efficient key-recovery attack to reveal this sensitive data. Among SCA, the family of so-called *profiling* attacks is actually the

✉ Emmanuel Prouff
emmanuel.prouff@ssi.gouv.fr

Ryad Benadjila
ryad.benadjila@ssi.gouv.fr

Rémi Strullu
remi.strullu@ssi.gouv.fr

Eleonora Cagli
eleonora.cagli@cea.fr

Cécile Dumas
cecile.dumasg@cea.fr

[1] ANSSI, Paris, France

[2] CEA, LETI, MINATEC Campus, 38054 Grenoble, France

Published online: 30 November 2019

most powerful one since the underlying adversary is assumed to priorly use an open copy of the final target to precisely tune all the parameters of the attack. It includes templates attacks [14] and Stochastic modelling (a.k.a. linear regression analysis) [17,58,59]. This attack strategy where the adversary precedes the attack by a supervised training phase may be viewed as a classical Machine Learning problem and a recent line of works has started to build connections between the world of side-channel analysis and the world of machine learning (with a particular focus on deep learning).

1.1 Related works

Several works have investigated the application of Machine Learning (ML) to defeat both unprotected [5,29,30,41,43] and protected cryptographic implementations [21,42]. These contributions focus mainly on two techniques: the *Support Vector Machine* (SVM) [16,64] and *Random Forest* (RF) [56]. Practical results on several datasets have demonstrated the ability of these attacks to perform successful key recoveries. Besides, authors in [29] have shown that the SVM-based attack outperforms the template attack when applied on highly noisy traces while [43] has experimentally argued that ML (and RF in particular) become(s) interesting if the amount of observations available for profiling is small while the dimension of the latter observations is high. Following the current trend in the Machine Learning area, more recent works have started to pay attention to deep learning (DL) algorithms like multi-layer perceptron networks (MLP) [46–48] or convolutional neural networks (CNN) [13,44]. Essentially, the conclusion of theses works is that DL offers a promising alternative to the state-of-the-art attacks, especially when the measurement dimension is high and/or the measured signal suffers from deformation like jittering (for CNN). However, the application context of these previous works is too weak or the amount of information on the involved deep learning techniques is too limited to draw solid conclusions for challenging contexts (e.g. where the target implementations include state-of-the-art countermeasures) and/or to improve these first attempts. Indeed, on one side, the series of papers [46–48] give partial information about the training and architecture of the deep learning models but it is limited to a comparison of MLP with other more classical approaches in the context of unprotected implementations of the AES-128 algorithm running on an old PIC 8-bit micro-controller. On the other side, papers [44] and [13] show that the Deep Learning approach may be applied to defeat classical countermeasures such as masking [44] or clock jittering [13] but they say nothing for the application of DL when both countermeasures are combined and, more importantly, they give very limited information about the training and the models architectures. This last point is an important limitation which does not allow for the reproducibility of the analyses and hence hampers the development of deep learning in the embedded security community. More generally, a common framework to study and compare the effectiveness of Machine Learning methods against secure embedded implementations of cryptographic algorithms is today missing.

1.2 Contributions

In this paper, our main objective is to conduct an in-depth study of the application of deep learning theory in the context of side-channel attacks. In particular, for the first time, we discuss several parametrization options and we present a large variety of benchmarks which have been used to either experimentally validate our choices or to help us to take the adequate decision.[1] The methodologies followed for the hyper-parameters' selection may be viewed as a proposal to help researchers to make their own choice for the design of new deep learning models. For most of the final choices made for the configuration of our models, we were not able to get a formal explanation and hence we of course do not claim that they are optimal. Since the current state of machine learning theory does not yet provide clear foundations to conduct such analyses, we think that having methodologies (even ad hoc) is a first necessary step which opens the way for further research in this domain. Our study also shows that convolutional neural networks are almost as efficient as multi-layer perceptron networks in the context of perfectly synchronized observations, and outperform them in presence of desynchronization/jittering. This suggests that CNN models should be preferred in the context of SCA (even if they are more difficult to train). When it comes to choose a base architecture for the latter models, our study shows that, surprisingly, the 16-layer network VGG-16 used by the VGG team in the ILSVRC-2014 competition [60] is a sound starting point (other public models like ResNet-50 [28] or Inception-v3 [63] are shown to be inefficient against masked implementations). It allows us to design architectures which, after training, are better than classical templates attacks even when combined with dimension reduction techniques like principal component analysis (PCA) [53]. By training (with 75 epochs) our CNN_{best} architecture on a subset of 50,000 700-dimensional traces of ASCAD database, we outperformed the other tested models on highly desynchronized traces while we achieved one of the best performances on small desynchronized traces.

[1] Some libraries (such as `hyperopt` or `hyperas`, [8]) could have been tested to automatize the search of accurate hyper-parameters in pre-defined sets. However, since they often perform a random search of the best parameters ([7]), they do not allow studying the impact of each hyper-parameter independently of the others on the side-channel attack success rate. Moreover, they have been defined to maximize classical machine learning evaluation metrics and not SCA ranking functions which require a batch of test traces.

Clearly, our analysis does not enable to draw strong conclusions on the optimization and selection of optimal networks in the context of side-channel analysis. It however shows the impact of each hyper-parameter on the model soundness.

All the benchmarkings have been done with the same target (and database) which corresponds to an AES implementation secured against first-order side-channel attacks and developed in assembly for an ATMega8515 component.[2] A signal-to-noise characterization has been done to validate that there is no first-order leakage. This project has been published in [4]. To enable perfect reproducing of our experiments and benchmarks, we also chose to publish the electromagnetic measurements acquired during the processing of our target AES implementation (available in [3]) together with example Python scripts to launch some initial training and attacks based on these traces. We think that this database may serve as a common basis for researchers willing to compare their new architectures or their improvements in existing models.

2 Preliminaries and theoretical foundations

2.1 Notations

Throughout this paper, we use calligraphic letters as $\mathcal{X}$ to denote sets, the corresponding upper-case letter X to denote random variables (random vectors $\mathbf{X}$ if with an arrow) over $\mathcal{X}$, and the corresponding lower-case letter x (resp. $\mathbf{x}$ for vectors) to denote realizations of X (resp. $\mathbf{X}$). Matrices will be denoted with bold capital letters. The i-th entry of a vector $\mathbf{x}$ is denoted by $\mathbf{x}[i]$, while the i-th observation of a random variable X is denoted by x_i. The *probability mass function* (aka the *probability distribution function*, pdf for short) of a *discrete* random variable $\mathbf{X}$ will be denoted by $f_{\mathbf{X}}$. It is defined for any possible realization $\mathbf{x}$ of $\mathbf{X}$ by $f_{\mathbf{X}}(\mathbf{x}) = \mathsf{P}[\mathbf{X} = \mathbf{x}]$. The symbol $\mathsf{E}[\ ]$ denotes the expected value, and might be subscripted by a random variable $\mathsf{E}_X[\ ]$, or by a probability distribution $\mathsf{E}_{f_X}[\ ]$, to specify under which probability distribution it is computed. Side-channel traces will be viewed as discrete realizations of a random column vector $\mathbf{L}$ with values in $[0, 2^{\omega} - 1]^D$ where D denotes the trace size (or dimension) and where ω depends on the vertical resolution of the oscilloscope used for the acquisitions (usually, we have $\omega \in \{8, 10, 12\}$). During their acquisition, a target sensitive variable $Z = \varphi(P, K)$ is handled, where P denotes some public variable, e.g. a plaintext chunk, and K the part of a secret key the attacker aims to retrieve. The value assumed by such a variable is viewed as a realization z of a discrete finite random variable Z defined over $\mathcal{Z}$ (e.g. $\mathcal{Z} = \{0, \ldots, 255\}$).

[2] We have validated that the code and the full project can be easily tested with the Chipwhisperer platform developed by C. O' Flynn [52].

2.2 Side-channel analysis

Side-channel analysis (SCA) aims at exploiting noisy observations $\mathbf{L}$ of the processing of an algorithm to recover its secret parameter. When the SCA adversary has the ability to use an open device (i.e. a device on which he can control, at least partially, all the inputs of the algorithm, including the secret parameters), a particular class of attacks named *profiling* may be executed.

2.2.1 Profiling SCA

A *profiling SCA* is composed of two phases: a profiling (or *characterization*, or *training*) phase, and an attack (or *matching*) phase.

During the profiling step, the attacker computes for every possible $k \in \mathcal{K}$ an estimation $\hat{\mathrm{g}}_k$ of the following conditional probability distribution function:

$$g_k : (\boldsymbol{\ell}, p) \mapsto \mathsf{P}[\mathbf{L} = \boldsymbol{\ell} | (P, K) = (p, k)]. \tag{1}$$

The estimation $\hat{\mathrm{g}}_k$ is deduced from on a so-called *profiling set* which is denoted by $\mathcal{D}_{\text{profiling}}$ and satisfies $\mathcal{D}_{\text{profiling}} \doteq \{\boldsymbol{\ell}_i, p_i, k_i\}_{i=1,\ldots,N_p}$ where N_p denotes the number of traces $\boldsymbol{\ell}_i$ acquired under known guessable chunks p_i and k_i of the cryptographic algorithm inputs. In the rest of this paper, the profiling set is viewed as the Cartesian product between the set a traces $\mathcal{L}$ and the set of corresponding inputs $\mathcal{Y}$.

Remark 1 In the context of side-channel analysis against block cipher implementations, it is common to label the observations/traces by an appropriate function $\varphi(p, k)$ instead of (p, k) (and both labellings are equivalent when the observations exactly correspond to the processing of $\varphi(\cdot)$ since p is assumed to be known). It will be the case for the database used in the rest of the paper where $\varphi(\cdot)$ corresponds to the AES sbox. Here the probability in the right-hand side of (1) may w.l.g. be rewritten $\mathsf{P}[\mathbf{L} = \boldsymbol{\ell} | \varphi(P, K) = z]$ and the profiling set may be rewritten $\mathcal{D}_{\text{profiling}} \doteq \{\boldsymbol{\ell}_i, z_i\}_{i=1,\ldots,N_p}$ with $\mathcal{L} = \{\boldsymbol{\ell}_i; i \leqslant N_p\}$ and $\mathcal{Y} = \{z_i; i \leqslant N_p\}$.

During the attack step, the adversary gets a new *attack set* $\mathcal{D}_{\text{attack}} \doteq \{\boldsymbol{\ell}_i, p_i\}_{i=1,\ldots,N_a}$ for which the secret parameter, say $k^{\star}$, is fixed but unknown. His goal is to recover the latter key. For such a purpose, it must be decided which of the pdf estimations $\hat{\mathrm{g}}_k$, $k \in \mathcal{K}$, is the most likely knowing the attack set. It is well known that, under realistic assumptions on the distributions' nature, the most efficient way to make such a decision is to follow a *Maximum Likelihood* strategy which amounts to estimate the following *likelihood* $\mathbf{d}_{N_a}[k]$ for every key candidate $k \in \mathcal{K}$, and then to select the key candidate that maximizes it:

$$\mathbf{d}_{N_a}[k] = \prod_{i=1}^{N_a} \frac{\mathsf{P}[\mathbf{L} = \boldsymbol{\ell}_i \mid (P, K) = (p_i, k)]}{f_{\mathbf{L}}(\boldsymbol{\ell}_i)} \times f_{P,K}(p_i, k), \tag{2}$$

which is obtained under the hypothesis that acquisitions are independent.[3] The estimation of the right-hand term of (2) is simply done by replacing the probabilities $\mathsf{P}[\mathbf{L} = \boldsymbol{\ell}_i | (P, K) = (p_i, k)]$ by their estimations $\hat{\mathrm{g}}_k(\boldsymbol{\ell}_i, p_i)$. The vector $\mathbf{d}_{N_a}$ is called *scores vector* and its kth coordinate is the score corresponding to key candidate k.

2.2.2 Leakage dimensionality issue

The potentially huge dimensionality of $\mathbf{L}$ may make the estimation of (1) a very complex problem. To circumvent it, the adversary usually priorly exploits some statistical tests (e.g. SNR or T-Test) and/or dimensionality reduction techniques (e.g. principal component analysis [53], linear discriminant analysis [19], kernel discriminant analysis [12]) to select points of interest or an opportune combination of them. Then, denoting $\varepsilon(\mathbf{L})$ the result of such a dimensionality reduction, the attack is performed as described previously with the simple difference that $\mathbf{L}$ and $\boldsymbol{\ell}_i$ are respectively replaced by $\varepsilon(\mathbf{L})$ and $\varepsilon(\boldsymbol{\ell}_i)$ in (1) and (2).

2.2.3 (Gaussian) Template attacks

Until now the most popular way adopted to estimate the conditional probability (1) is the one that led to the well-established Gaussian template attack [14]. It assumes that $\mathbf{L} \mid (P, K)$ (or equivalently $\varepsilon(\mathbf{L}) \mid (P, K)$ if a dimensionality reduction has been priorly applied) has a multivariate Gaussian distribution, and estimates the mean vector $\bar{\ }_{p,k}$ and the covariance matrix $\mathbf{6}_{p,k}$ for each possible $(p, k) \in \mathcal{P} \times \mathcal{K}$ (i.e. the so-called templates). In this way, for every (p, k), the pdf $\boldsymbol{\ell} \mapsto g_k(\boldsymbol{\ell}, p)$ defined in (1) is approximated by the Gaussian pdf $f_{\bar{\ }_{p,k}, \mathbf{6}_{p,k}}$. So, the Gaussian template attack is a strategy that makes use of a generative model. The same multivariate Gaussian assumption is the one that is made in *quadratic discriminant analysis* (QDA), which is a well-known generative strategy in the Machine Learning literature [19] to perform classification.

2.3 Machine learning and deep learning

In machine learning theory, the problem of estimating $\mathsf{P}[\mathbf{L} \mid (P, K) = (p, k)]$, for some $(p, k) \in \mathcal{Y}$ with $\mathcal{Y} \doteq \mathcal{P} \times \mathcal{K}$, is known as a *generation* problem[4] (a.k.a. *prediction* problem), while the estimation of $\mathsf{P}[(P, K) = (p, k) \mid \mathbf{L}]$ is referred to as a *classification problem* (see e.g. [9]).

Nowadays, deep neural networks are the privileged tool to address the classification problem, and they can be exploited in a discriminative way. In such a case, which corresponds to our choice, they aim at directly constructing an approximation $\hat{\mathrm{g}}$ of the function $\mathrm{g} : \boldsymbol{\ell}, p \mapsto (\mathsf{P}[(P, K) = (p, k) \mid \mathbf{L} = \boldsymbol{\ell}])_{k \in \mathcal{K}}$. It may be observed that g is directly linked to the pdfs in (1) through the following relation which comes as a direct consequence of Bayes Theorem:

$$\mathrm{g}(\boldsymbol{\ell}, p) = \big(g_k(\boldsymbol{\ell}, p) \times f_{P,K}(p, k) / f_{\mathbf{L}}(\boldsymbol{\ell})\big)_{k \in \mathcal{K}}. \tag{3}$$

The classification of a new leakage $\boldsymbol{\ell}$ observed for an input p is done afterwards by processing $\mathbf{y} = \hat{\mathrm{g}}(\boldsymbol{\ell}, p)$ and by choosing the key candidate $\hat{k}$ (or equivalently the label in the formalism of Machine Learning) such that $\hat{k} = \mathrm{argmax}_{k \in \mathcal{K}} \mathbf{y}[k]$. If the key-discrimination is done from several, say N_a, pairs $(\boldsymbol{\ell}_i, p_i)$ then the maximum likelihood approach is followed as in (2):

$$\mathbf{d}_{N_a}[k] = \prod_{i=1}^{N_a} \mathbf{y}_i[k], \tag{4}$$

where $\mathbf{y}_i$ denotes the output of (the model function) $\hat{\mathrm{g}}$ input with the pair $(\boldsymbol{\ell}_i, p_i)$. It may be checked that (4) is a simple rewriting of (2) obtained by using (3).

Remark 2 In cases where the SCA targets a particular processing in the form $\varphi(P, K)$, this leads to search for an approximation $\hat{\mathrm{g}}'$ of the function $\boldsymbol{\ell}, p \mapsto (\mathsf{P}[\varphi(P, K) = z \mid \mathbf{L} = \boldsymbol{\ell}, P = p])_{z \in \mathcal{Z}}$. The output of the model $\hat{\mathrm{g}}'$ when input with $(\boldsymbol{\ell}, p)$ is then a vector $\mathbf{y}'$ indexed by the values $z = \varphi(p, k)$ for k ranges over $\mathcal{K}$. To build a second vector $\mathbf{y}$ indexed by the key candidates k it suffices to process $\mathbf{y}[k] = \mathbf{y}'[\varphi(p, k)]$ for the input p and for every $k \in \mathcal{K}$.

Remark 3 Another formulation of the classification problem could consist in directly looking for an estimation of the pdf $\mathsf{P}[K \mid \mathbf{L}, P]$: the deep neural networks will here be trained to classify the key candidates knowing the public input of the cryptographic primitive and the information leakage. However, even if this formulation may seem more natural (it perfectly matches the problem we want to resolve), it implies that the deep neural networks must not only recover the statistical dependency between the values of the manipulated data and the leakage, but also the function that links it to the key (e.g. the function $\varphi^{-1}(\cdot, P)$). Since the latter function may be complex (e.g. can be affinely equivalent to the inverse of

[3] In Templates Attacks the profiling set and the attack set are assumed to be different, namely the traces $\boldsymbol{\ell}_i$ involved in (2) have not been used for the profiling.

[4] The name *generative* is due to the fact that it is possible to generate synthetic traces by sampling from such probability distributions.

an sbox), this can made the task of the deep neural networks harder, whereas the function φ is often already known by the adversary.

Deep Learning is a branch of machine learning whose characteristic is to avoid any manual feature extraction step from the model construction work-flow. For example, in deep learning the dimensionality issue discussed in Sect. 2.2.2 is not necessarily tackled out by preprocessing a dimensionality reduction function ε. As described below, the cascade of multiple layers that characterize DL models is indeed in charge of directly and implicitly extracting interesting features and of estimating the classifying model $\hat{\mathrm{g}}$. This approximation is searched in a family of functions (aka *models* in the machine learning terminology) specified *a priori* by the data analyst according to the specificities of the problem which is tackled out.

We conclude this subsection by recalling some basic definitions and notions about neural networks and their training.

Neural networks A neural network has an *input layer* (the identity over the input datum $\boldsymbol{\ell}$), an *output layer* (the last function, whose output $\mathbf{y}$ is an estimation of the vector of conditional probabilities) and all other layers are called *hidden* layers. The so-called *neurons*, that give the name to the architecture, are the computational units (also named *nodes*) of the network and essentially process a scalar product between the coordinates of its input and a vector of *trainable weights* (or simply *weights*) that have to be *trained*. Each layer processes some neurons and the outputs of the neuron evaluations will form new input vectors for the subsequent layer. The numbers of layers in the neural networks, the dimension of the elementary units or the algebraic nature of the nonlinear layers form the *architecture* of the network and define the family of functions/models. The identification of the best approximating function in this family is made by solving a minimization problem with respect to a metric which is specific to the application.

Training of neural networks In a privileged setting, the *training phase* (i.e. the automatic tuning of the weights of the neurons) is done *via* an iterative approach which locally applies the (Stochastic) Gradient Descent algorithm [24] to minimize a *loss function* quantifying the *classification error* of the function $\hat{\mathrm{g}}$ over a training set which is a part of the profiling set. The cross-entropy [25,40] metric is a classical (and often by default) choice in classification problems. It is smooth and decomposable, and therefore amenable to optimization with standard gradient-based methods. However, other metrics may be investigated and can potentially lead to better results [49,61]. A training is said to be *full batch learning* if the full training database is processed before one update. At the opposite, if a single training input is processed at a time then the approach is named *stochastic*. In practice, one often prefers to follow an approach in between, called *mini-batch learning*, and to use small *batch* (aka group) of training inputs at a time during the learning. The size of the mini-batch is generally driven by several efficiency/accuracy factors which are e.g. discussed in [25] (e.g. optimal use of the multi-core architectures, parallelization with GPUs, trade-off between regularization effect and stability, etc.).

An iteration over all the training datasets during the Stochastic Gradient Descent is called an *epoch*. The number of epochs is an important parameter to tune because small values may lead to under-fitting (the number of steps of the Gradient Descent is not sufficient and the model is too poor to capture a trend in the training dataset) and high values may lead to over-fitting (the model is too complex, it perfectly fit the training dataset but is not able to generalized its predictions to other datasets).

Several extensions and variants of the Stochastic Gradient Descent have been proposed in the context of deep learning. These variants, called *optimizers*, aim to adapt the *learning rate* (the step size) of the Gradient Descent during the training process. More details about the specification of neural networks will be given in the dedicated Sects. 3 and C, but we will not go further on the optimization approaches and the interested reader may refer to [24].

Hyper-parameters All the parameters that define an architecture (called *architecture hyper-parameters* or simply *architecture parameters*), together with some other parameters that govern the training phase (called *training hyper-parameters* or simply *training parameters*), have to be carefully set by the attacker.[5] This point will be discussed in Sect. 3.3.

2.4 Model assessment and selection

2.4.1 Evaluation methodology

In the machine learning community, several evaluation frameworks are commonly applied to assess the performances of a model or to select the best parameters that suit to a parametrized family of models. These methods aim to provide an estimator of the performance of a metric (e.g. the accuracy) which does not depend on the choice of the training set $\mathcal{D}_{\text{train}}$ (on which the model is trained) and of the test set $\mathcal{D}_{\text{test}}$ (on which the model is tested) but only on their size.

The so-called *t-fold cross-validation* [20] is currently the preferred evaluation method. Let c be a metric, $\hat{\mathrm{g}}$ a model to evaluate, and $\mathcal{D}_{\text{profiling}} = (\mathcal{L}, \mathcal{Y})$ a dataset with labels, the outline of the method is the following:

[5] When no ambiguity is present we will call simply *hyper-parameters* the architecture ones.

1. [optional] randomize the order of the labelled traces in $\mathcal{D}_{\text{profiling}}$,
2. split the samples and their corresponding labels into t disjoint parts of equal size $(\mathcal{L}_1, \mathcal{Y}_1), \ldots, (\mathcal{L}_t, \mathcal{Y}_t)$. For each $i \in [1..t]$, do:
   (a) set $\mathcal{D}_{\text{test}} \doteq (\mathcal{L}_i, \mathcal{Y}_i)$ and $\mathcal{D}_{\text{train}} \doteq (\bigcup_{j\neq i} \mathcal{L}_j, \bigcup_{j\neq i} \mathcal{Y}_j)$,
   (b) (re-)train[6] the model $\hat{\mathsf{g}}$ on $\mathcal{D}_{\text{train}}$,
   (c) compute the performance metric by evaluating the model on $\mathcal{D}_{\text{test}}$:

$$\mathsf{c}_i = \mathsf{c}(\hat{\mathsf{g}}, \mathcal{D}_{\text{test}}), \tag{5}$$

3. return the mean $\frac{1}{t}\sum_{i=1}^{t} \mathsf{c}_i$.

It is known that the t-fold cross-validation estimator is an unbiased estimator of the generalization performance. Its main drawback is its variance which may be large and difficult to estimate [6,10]. In this paper (Sects. 3 and C), we perform a 10-fold cross-validation for each selection of the model parameters. The choice of $t = 10$ results in a trade-off between evaluation complexity and accuracy, since for each choice of parameters the model is trained 10 times with a substantial computing time, and the generalization performance estimator is computed among 10 values on different training sets, reducing the uncertainty on the evaluation metrics. The dataset $\mathcal{D}_{\text{profiling}}$ on which is performed the cross-validation is a fixed subset comprised of 50,000 labelled traces, split at each iteration into $N_{\text{train}} = 45,000$ labelled traces for $\mathcal{D}_{\text{train}}$ and $N_{\text{test}} = 5,000$ labelled traces for $\mathcal{D}_{\text{test}}$.

2.4.2 Evaluation metrics

We evaluate the performance of our models with three different metrics, which are: the *rank function*, the *accuracy* and the *computational time*.

The rank function is a commonly used metric in SCA for assessing the performance of an attack. Let us denote by $k^\star \in \mathcal{K}$ the key that has been used during the acquisition of the dataset $\mathcal{D}_{\text{profiling}}$. The *rank function* corresponding to a model $\hat{\mathsf{g}}$ trained with the dataset $\mathcal{D}_{\text{train}}$ and tested with the dataset $\mathcal{D}_{\text{test}}$ is defined by:

$$\mathsf{rank}(\hat{\mathsf{g}}, \mathcal{D}_{\text{train}}, \mathcal{D}_{\text{test}}, n) = |\{k \in \mathcal{K} \mid \mathbf{d}_n[k] > \mathbf{d}_n[k^\star]\}|, \tag{6}$$

where $\mathbf{d}_n[k]$ is the score for the candidate k as defined in (4) (replacing $\mathcal{D}_{\text{attack}}$ by $\mathcal{D}_{\text{test}}$ and N_a by n) and estimated from a modelling of the conditional probability done with $\mathcal{D}_{\text{train}}$ and a test done with the n first traces in $\mathcal{D}_{\text{test}}$. For example, if $k^\star$ has the highest score (resp. the lowest score), then its rank is 0 (resp. $|\mathcal{K}|-1$). Note that in this definition, the rank function depends on the choices of the training and test datasets. To get a better measure of the rank for given cardinalities N_{train} and N_{test} of $\mathcal{D}_{\text{train}}$ and $\mathcal{D}_{\text{test}}$ respectively, it is therefore more suitable to estimate its mean over several pairs of datasets:[7]

$$\mathsf{RANK}_{N_{\text{train}},n}(\hat{\mathsf{g}}) = \mathsf{E}[\mathsf{rank}(\hat{\mathsf{g}}, \mathcal{D}_{\text{train}}, \mathcal{D}_{\text{test}}, n)], \tag{7}$$

where the mean is defined over all the datasets $\mathcal{D}_{\text{train}}$ and $\mathcal{D}_{\text{test}}$, respectively, of cardinality N_{train} and N_{test}, and where n is assumed to be bounded above by N_{test}. For any pair of cardinalities, an approximation of the mean can be obtained by cross-validation as detailed previously just by replacing c in (5) by the rank function $\mathsf{rank}(\cdot)$. This is exactly what has been done for the benchmarks discussed in Sect(s). 3 and C. More precisely, the following attack has been repeated $t = 10$ times and the average rank of the correct key is plotted: (1) select a training set of fixed size N_{train} and (2) compute the evolution of the rank of the correct key when the model is tested with an increasing number n of traces in $\mathcal{D}_{\text{test}}$ (of size N_{test}).

A second metric which is commonly used in machine learning is the accuracy. With the same previous notations, we can define it as:

$$\mathsf{acc}(\hat{\mathsf{g}}, \mathcal{D}_{\text{train}}, \mathcal{D}_{\text{test}}) = \frac{|\{(\boldsymbol{\ell}_i, p_i, k^\star) \in \mathcal{D}_{\text{test}} \mid k^\star = \text{argmax}_{k\in\mathcal{K}}\, \mathbf{y}_i[k]\}|}{|\mathcal{D}_{\text{test}}|}, \tag{8}$$

where we recall that $\mathbf{y}_i$ denotes the $|\mathcal{K}|$-dimensional output $\hat{\mathsf{g}}(\boldsymbol{\ell}_i, p_i)$. Then, similarly as for the rank function but for possibly unbounded size of $\mathcal{D}_{\text{test}}$, we can define from (8) an *Expected Accuracy of the model* (ACC) by:

$$\mathsf{ACC}_{N_{\text{train}}}(\hat{\mathsf{g}}) = \mathsf{E}[\mathsf{acc}(\hat{\mathsf{g}}, \mathcal{D}_{\text{train}}, \mathcal{D}_{\text{test}})],$$

where the mean is defined over all the datasets $\mathcal{D}_{\text{train}}$ of size N_{train} and all the datasets $\mathcal{D}_{\text{test}}$ (with unbounded size).[8]

Finally, our selection of parameters is also guided by the *computational time* of the model training. The mean of the training time is computed in the same manner as the other evaluation metrics during the 10-fold cross-validation.

2.4.3 About the profiling set-up

Our implementations of machine learning algorithms have been developed with Keras library [15] (version 2.1.1) or

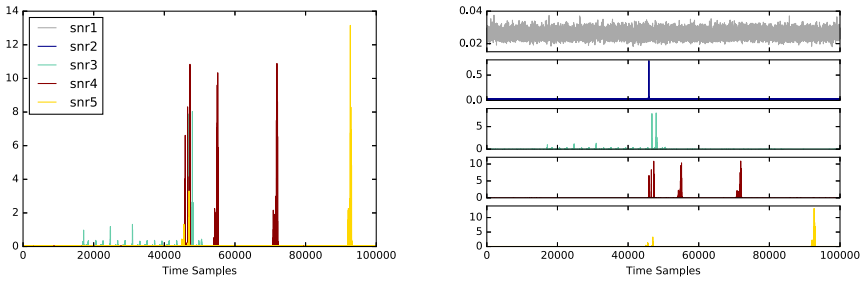
[6] We insist here on the fact that the model is trained from scratch at each iteration of the loop over t.

[7] and also different values of $k^\star$ if this is relevant for the attacked algorithm.

[8] Another metric, the *prediction error* (PE), is sometimes used in combination with the accuracy: it is defined as the expected error of the model over the training sets; $\mathsf{PE}_{N_{\text{train}}}(\hat{\mathsf{g}}) = 1 - \mathsf{ACC}_{N_{\text{train}}}(\hat{\mathsf{g}})$.

Name	Definition of Z
$snr1$	$\text{sbox}(p[3] \oplus k[3])$
$snr2$	$\text{sbox}(p[3] \oplus k[3]) \oplus r_{\text{out}}$
$snr3$	r_{out}
$snr4$	$\text{sbox}(p[3] \oplus k[3]) \oplus r[3]$
$snr5$	$r[3]$

(a) details of the SNR processings in 1b



(b) SNRs for various intermediate values related to processing the third sbox output

Fig. 1 SNR characterization for the third sbox output manipulation

directly with Tensorflow library [1] (version 1.4.0). We run the trainings over ordinary computers equipped with 16 GB of RAM and gamer market GPUs Nvidia GTX 1080 Ti. The computation of all the benchmarks took approximately 12 days by using 3 GPU cards.

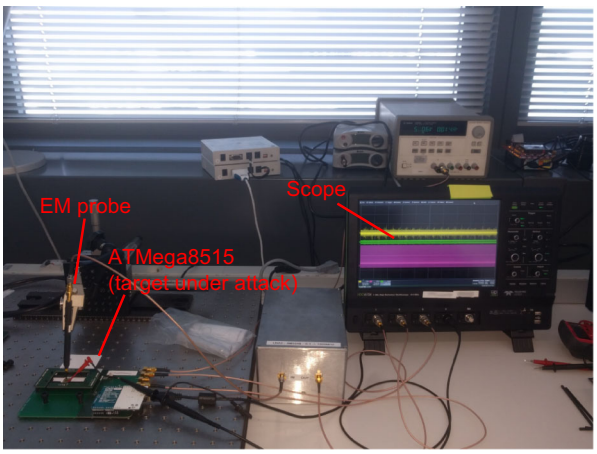
2.5 Target of the attacks experiments and leakage characterization

For our attack experiments, we targeted a Software protected AES implementation running over an 8-bit AVR architecture. More precisely, the device is an ATMega8515.

2.5.1 About the implementation

To maximize our control on the code executed by the device, we choose to implement the AES in assembly language. We developed two versions which merely aim at defeating first-order SCA attacks (i.e. attacks exploiting a single temporal leakage without (re-)combining of temporal points). The first one makes use of the classical *table re-computation* method (see e.g. [2,34,55] for a detailed description). The AES state is secured with 16 different masks for the linear parts and, for the SubBytes processing, the same pair of input and output masks is used for each state element. The outlines of the implementation are summed up in Algorithm 1 in "Appendix B". A Signal-to-Noise Ratio (SNR)[9] has been done (1) to validate that there is no first-order leakage ($snr1$ in Fig. 1b) and (2) to identify where the target values and the masks are leaking ($snr2 - snr5$ in Fig. 1b). To help evaluators to perform elementary attacks against the first two bytes of the AES state during the first round, the corresponding masks of the linear parts ($r[1]$ and $r[2]$ in Algorithm 1) have been fixed to 0.

Attack experiments reported in the rest of the paper only target the output of the third sbox processing during the first round (namely $\text{sbox}^\star[\text{state0}[3]] \doteq \text{sbox}(p[3] \oplus k[3]) \oplus r_{\text{out}}$ with $i = 3$ in Algorithm 1).[10]



SCA acquisition setup

2.5.2 About the acquisition phase

The side-channel observations were obtained by measuring the electromagnetic (EM) radiations emitted by the device. To this aim, a sensor made of several coils of copper was plugged into a low-noise amplifier. To sample measurements, a digital oscilloscope was used with a sampling rate of 2G samples per second. We insist on the fact that the temporal acquisition window was set to record the first round of the AES only. As the MCU clock was quite stable, the resynchronization of the measurements was not difficult and resulted in a campaign of 100,000 traces composed of 100,000 time samples. Among them, we chose to finally extract only 60,000 traces after validating that it was sufficient to accurately realize all our benchmarks (see e.g. Sect. C.2). To identify the leakage samples related to the secure processing of $\text{sbox}(p[3] \oplus k[3])$, several SNRs have been processed. Their definition is given in Table 1a.

[9] The SNR is sometimes named F-Test to refer to its original introduction by Fischer [18]. For a noisy observation L_t at time sample t of an event Z, it is defined as $\mathsf{Var}[\mathsf{E}[L_t \mid Z]]/\mathsf{E}[\mathsf{Var}[L_t \mid Z]]$.

[10] Another possibility would have been to target $\text{state0}[3] = \text{sbox}(p[3] \oplus k[3]) \oplus r[3]$ which is manipulated at the end of Step 8] in Algorithm 1.

It may be observed in Fig. 1b that $snr1$ (in grey) is very low, which essentially shows that there is no first-order leakage on the unmasked sbox output $\text{sbox}(p[3] \oplus k[3])$. The leakages on the sbox output masked with $r[3]$ and on the mask $r[3]$ itself are relatively high ($snr4$ and $snr5$ respectively). The SNR $snr4$ shows three peaks because the sbox output with mask $r[3]$ is not only manipulated during the SubBytes step but also during the ShiftRows and the MixColumns. Eventually, one can also observe a leakage on the sbox output masked with r_{out} and on the mask r_{out} itself ($snr2$ and $snr3$). Since this leakage is smaller than that for the sbox with mask $r[3]$, we found it more challenging and preferred to focus on it in our attack experiments.

For the reasons explained in previous paragraph, we chose to enshorten the initial traces (composed of 100,000 samples) and to only keep, for each trace, the 700 samples in the interval [45400..46100] which contains information on the two pairs of $(\text{sbox}(p[3] \oplus k[3]) \oplus r[3], r[3])$ and $(\text{sbox}(p[3] \oplus k[3]) \oplus r_{\text{out}}, r_{\text{out}}))$ (see Fig. 15 in "Appendix A" for a zoom on the SNRs in the target intervals[11]).

To enable perfect reproducing of our experiments and benchmarks, we published the electromagnetic measurements acquired during the processing of our target AES implementation (available in [3]) together with example Python scripts to launch some initial training and attacks based on these traces. See Section B for details about this open database.

3 Convolutional neural networks

3.1 Core principles and constructions

Convolutional Neural Networks (CNNs) involved in our studies are based on 5 types of layers that are briefly recalled hereafter:

- *The Fully-Connected layers* (FC for short), denoted by λ, are expressible as affine functions: denoting $\mathbf{x}$ the D-dimensional input of an FC, its output is given by $\mathbf{Ax}+\mathbf{B}$, being $\mathbf{A} \in \mathbb{R}^{C \times D}$ a matrix of weights and $\mathbf{B} \in \mathbb{R}^{C}$ a vector of biases. These weights and biases are the trainable weights of the FC layer.[12]
- *Convolutional layers* (CONV for short) are linear layers, denoted by γ, that share weights across space. To apply it to an input, n_{filter} small column vectors, called *convolutional filters*, of size W (aka *kernel size*) are slid over the input by some amount of units, called *stride*.[13] The column vectors form a window[14] which defines a linear transformation of the W consecutive points of the data into a new vector $\mathbf{x}$. When the window slides over the last points, the input trace can be either padded with 0 resulting in a vector $\mathbf{x}$ which has the same number of points than the input data (*same* padding) or the data is not padded and the window only slides over the valid part of the data, resulting in a vector $\mathbf{x}$ smaller than the input trace (*valid* padding). The coordinates of the window (viewed as a matrix) are among the trainable weights which are constrained to be unchanged for every input. This constraint aims to allow the CONV layer to learn shift-invariant features. The reason why several filters are applied is that we expect each filter to extract a different kind of characteristic from the input. As one goes along convolutional layers, higher-level abstraction features are expected to be extracted. These high-level features are arranged side-by-side over an additional data dimension, the so-called *depth*.[15] This is this geometric characteristic that makes CNNs robust to temporal deformations [36].
- *Pooling layers* (POOL for short) are nonlinear layers, denoted by δ, that reduce the spatial size by making some filters slide across its input. Filters are 1-dimensional, characterized by a length W and a stride, that is usually chosen equal to W. They do not contain trainable weights and only slide across the input to select a segment, then a pooling function is applied: the most common pooling functions are the *max pooling* which outputs the maximum values within the segment and the *average pooling* which outputs the average of the coordinates of the segment.
- *Activation layers* (ACT for short) are composed of a single nonlinear real function that is applied independently to each coordinate of its input. Several activation functions have been used in deep learning and currently the so-called ReLU is preferred. It processes $\max(0, x)$ to each coordinate x. The ACT layer preceded by the Batch Normalization layer below is denoted α.
- *Batch Normalization layers* (BN for short) have been introduced in [31] by Ioffe Szegedy to reduce the so-called *internal covariate shift* in neural networks and to eventually allow for the usage of higher learning rates. The reasoning behind the soundness of this layer is well argued in [25].

[11] Note that some peaks appearing in Fig. 1b have not been selected.

[12] They are called *Fully-Connected* because each i-th input coordinate is *connected* to each j-th output via the $\mathbf{A}[i, j]$ weight. FC layers can be seen as a special case of the linear layers where not all the connections are necessarily present. The absence of some (i, j) connections can be formalized as a constraint for the matrix $\mathbf{A}$ consisting in forcing to 0 its (i, j)-th coordinates.

[13] Amount of units by which a filter shifts across the trace.

[14] *patches* in the machine learning language.

[15] Ambiguity: Neural networks with many layers are sometimes called *Deep Neural Networks*, where the *depth* corresponds to the number of layers.

– The *softmax*[16] layer (SOFT for short), denoted by s, applies the following processing to each coordinate of its input $\mathbf{x}$: $\mathsf{s}(\mathbf{x})[i] = \frac{e^{\mathbf{x}[i]}}{\sum_j e^{\mathbf{x}[j]}}$.

Eventually, the main block of a CNN is a CONV layer γ directly followed by a BN layer and an ACT layer α. The former locally extracts information from the input thanks to filters and the latter increases the complexity of the learned classification function thanks to its nonlinearity. After some $(\alpha \circ \gamma)$ blocks, a POOL layer δ is usually added to reduce the number of neurons: $\delta \circ [\alpha \circ \gamma]^{n_{\text{conv}}}$. This new block is repeated n_{blocks} times in the neural network until obtaining an output of reasonable size. Then, n_{dense} FC layes λ are introduced in order to obtain a global result which depends on the entire input. To sum-up, a common convolutional network can be characterized by the following formula:[17]

$$\mathsf{s} \circ [\lambda]^{n_{\text{dense}}} \circ [\delta \circ [\alpha \circ \gamma]^{n_{\text{conv}}}]^{n_{\text{blocks}}}. \tag{9}$$

3.2 A brief overview of current CNN architectures

The first successful CNN network, best known as LeNet, was developed in the nineties and was mostly applied to handwritten digit recognition [37,38]. The last version of the network, LeNet-5 [38], is a small architecture which operates on images of 32×32 pixels split into 10 classes. The architecture is comprised of 2 convolutional layers with, respectively, 6 and 16 filters of size 5×5, and 3 final dense layers of, respectively, 120, 84 and 10 units. Each convolutional layer is followed by an average pooling layer and the activation function is the hyperbolic tangent. The network achieved an accuracy of nearly 99% on the test dataset.

CNN networks gained popularity with their breakthrough as a contender in the Imagenet Large Scale Visual Recognition Challenge (ILSVRC, [57]) and since 2012, deep CNN networks have constantly established new records in computer vision [28,35,60,62]. ILSVRC is an image classification challenge which provides each year a labelled dataset of roughly 1,000,000 images of 200×200 pixels split into 1000 classes. Candidates train and validate their algorithm on the provided dataset and submit it to the competition. Then algorithms are evaluated with an (unknown) test dataset and they are ranked according to two metrics, the top-1 accuracy and the top-5 accuracy, where the top-5 accuracy is the fraction of the test dataset for which the correct label is among the best 5 predictions returned by the algorithm.

The first CNN architecture presented at ILSVRC challenge in 2012 [35] obtained a great success in the competition by outperforming all the challengers with a top-5 accuracy rate of 84.7% (against 73.8% for the second-best entry). This CNN network, well-known as AlexNet, has 8 layers, with 5 convolutional layers dispatched in 3 blocks and 3 dense layers of 4096 units each. The convolutional layers have 3,96,256 and 384 filters of size 11×11, 5×5 and 3×3. Each block has a final max pooling layer and ReLU activation functions are used instead of hyperbolic tangents (as in LeNet). The subsequent winner of ILSVRC challenge, ZFNet [65], improved the previous architecture by reducing the size of the first convolutional layer to 7×7 and by increasing the number of filters to 1024 for the last convolutional layers; it achieved a top-5 accuracy of 85.2%.

The trend of reducing the size of the filters by increasing the depth of the network was later confirmed to be a successful strategy. The runner-up architecture of the ILSVRC 2014 challenge, VGGNet [60], obtained a 92.7% top-5 accuracy with an architecture comprised of (up to) 16 convolutional layers of 512 filters of size 3×3 distributed in 5 blocks (for the VGG-19 version).

The winner of ILSVRC 2014, GoogLeNet [62], also used a deep network architecture with a total of 27 layers, but managed to decrease the number of parameters to train by using a new element in the architecture, the Inception module, which is a stack of small size convolutional layers (1×1, 3×3, 5×5) with few parameters. Furthermore, the last dense layers are replaced by an average pooling layer, which also decreases the number of parameters to train. GoogLeNet obtained a top-5 accuracy rate of 93.3% with 12 times fewer parameters than AlexNet.

Finally, deep residual networks recently grow in popularity with the success of ResNet at ILSVRC 2015 [28]. These architectures manage to overcome the degradation problem that occurs when the depth of the network increases. They rely on residual units that learn for each layer the residual function $\mathcal{F}(x) = \mathcal{H}(x) - x$ where x is the input of the layer and $\mathcal{H}(x)$ is the desired function of the layer. The top of the networks also have an average pooling layer like GoogLeNet. ResNet has up to 152 layers and achieves a 96.6% top-5 accuracy at ILSVRC 2015, winning the challenge.

3.3 Determining an architecture

Essentially, the strategy we have followed to finalize a choice of hyper-parameters is composed of three consecutive steps. First, we perform some ad hoc preliminary tests to select a base model with fixed architecture parameters, namely a CNN_{base} model in the form (9), and then we analyse the performances we can obtain with such a model while making the training hyper-parameters vary. In a third time, and after fixing the best solutions for the training hyper-parameters, we

[16] To prevent underflow, the log-softmax is usually preferred if several classification outputs must be combined.

[17] where each layer of the same type appearing in the composition is not to be intended as exactly the same function (e.g. with same input/output dimensions), but as a function of the same form.

made the network hyper-parameters vary in order to optimize the architecture, called CNN_{best}.

This strategy has also been conducted in the context of multi-layer perceptron networks. The setting process leads to the MLP_{best} architecture given in C.

3.3.1 Choice of the CNN_{base}

To get a first idea about the kind of architectures relevant in our context, we chose to test some of state-of-the-art CNN architectures listed in previous section:[18] VGG-16 [60], ResNet-50 [28] and Inception-v3 [63]. Our purpose was not to compare their efficiency after some specific tuning but was to check whether one of them seems straightforwardly more adapted to our context than the others. Results are summed up in Fig. 2 where we have plotted the evolution of the mean rank of the correct key-hypothesis according to the number of epochs. Results are obtained with a 10-fold cross-validation.

Clearly, ResNet-50 and Inception-v3 do not seem to succeed in extracting key-dependent information for the observations whereas VGG-16 does very well. Based on these preliminary results, we chose to apply the same design principles as in VGG-16 architecture and we investigated the impact on several parameters' configuration on the side-channel attack efficiency.

We moreover added the following rules, which are today classical in literature and enable us to limit the number of different configurations to test.

Rule 1 *CONV layers in the same block have exactly the same configuration (to keep the global volume constant).*

Rule 2 *Each pooling has dimension* 2 *(and hence divides the size of the input by* 2*).*

Rule 3 *The number of filters* $n_{filters,i}$ *in a CONV layer of the* i*th block (starting from* $i = 1$*) satisfies for* $i \geq 2$*:*

$$n_{filters,i} = \min(n_{filters,1} \times 2^{i-1}, 512).$$

Remark 4 The core idea behind Rule 3 is to keep the global amount of information treated by the different layers as constant as possible. Since each pool layer divides the input dimension by 2, the number of filters is itself multiplied by 2 to compensate it. This idea is inspired by VGG-16.

Rule 4 *All the CONV layers have the same kernel size.*

An example of the tested CNN architecture CNN_{base} is given in Fig. 30 in "Appendix D". For the initial configuration of our CNN_{base} model used to test the impact of the different hyper-parameters, we select the following values: the number

[18] Straightforwardly customized to apply on 1-dimensional inputs of 700 units and outputs of 256 units.

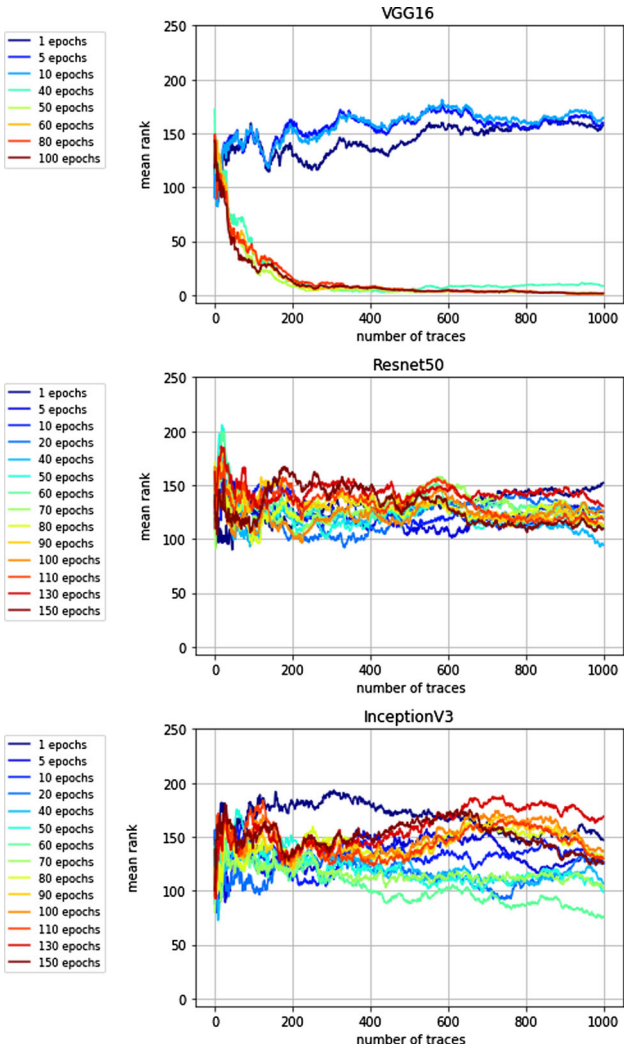


Fig. 2 Mean ranks (y-axis) w.r.t. the number of test traces (x-axis) obtained for VGG-16, ResNet-50 and Inception-v3 and for different epochs

of blocks of CONV layers n_{blocks} is equal to 4, there is only one CONV layer by block ($n_{\text{conv}} = 1$), the number of filters for the first block $n_{filter,1}$ is equal to 64, each filter has kernel size 3 (*same* padding) with ReLU activation functions and a max pooling layer for each block ($W = 2$). CNN_{base} has $n_{\text{dense}} = 2$ final dense layers of 4, 096 units.

3.3.2 Choice of the hyper-parameters in SCA context

The goal of the following benchmarks is twofold. First, it is to study, for the architecture CNN_{base} presented in previous section and for our dataset, the impact of each (hyper)-parameter on the accuracy and SCA-efficiency. Secondly, it is to choose the final hyper-parameters for a new CNN model (hopefully) better than the original one and hence called CNN_{best}. The number of the latter parameters being too large for an exhaustive test of all the possible configurations, we chose

Table 1 Benchmarks summary

Parameter	Reference	Metric	Range	Choice
Training parameters				
Epochs	–	Rank versus time	10, 25, 50, 60, . . . , 100, 150	Up to 100
Batch size	–	Rank versus time	50, 100, 200	200
Architecture parameters				
Blocks	n_{blocks}	Rank, accuracy	[2..5]	5
CONV layers	n_{conv}	Rank, accuracy	[0..3]	1
Filters	$n_{\text{filters},1}$	Rank versus time	$\{2^i; i \in [4..7]\}$	64
Kernel size	–	Rank	{3, 6, 11}	11
FC layers	n_{dense}	Rank, accuracy versus time	[0..3]	2
ACT function	α	Rank	ReLU, Sigmoid, Tanh	ReLU
Pooling layer	–	Rank	Max, Average, Stride	Average
Padding	–	Rank	Same, Valid	Same

to arbitrarily follow a predetermined sequence of tests. Note that the same CNN_{base} architecture is used for each benchmarking (which each focuses on a single hyper-parameter). For completeness, we also validated the soundness of our choices when the observations are desynchronized.

The desynchronizations of the traces are simulated by generating for each trace a random number δ in $[0..N_{\max}]$ and by shifting the original trace of δ points to the left. The samples added to a trace by this processing directly come from the corresponding full trace in `ATMega8515_raw_traces.h5`. For a chosen value $N_{\max}$ we then generate a new dataset $\mathcal{D}_{N_{\max}}$ from the original one.

Our goal was not to find the optimal configuration/training strategies but was to identify one of them making sense in our context and leading to accurate results. Other choices are certainly possible and we let the question of determining the most pertinent strategy as an open problem for further studies on this subject. The roadmap followed for our benchmarks is summarized in Table 1. Since our goal is to improve the SCA efficiency, i.e. to have the correct hypothesis ranked first with the minimum of traces during the matching/test phase, we always privileged rank-flavoured criteria for parameters selection.

3.3.3 Training parameters

The tuning of some training parameters is inherited by the analogous study in MLP context (see "Appendix C"). In particular we fixed the training set size to 50,000,[19] and chose to use the RMSProp optimizer with a learning rate of 10^{-5}.

Number of epochs and batch size For our campaigns, we did not observe any over-fitting (relatively to our rank function) when the number of epochs is increasing. As a direct consequence, the quality of the trained model in terms of our rank function never decreases when the number of epochs increases. Based on this observation, the following benchmarks aim to get the best trade-off between the SCA-efficiency and the training duration/time as a function of the number of epochs and the training batch size.

The first benchmark series are obtained by training CNN_{base} with different values of epoch and batch size. The results in Fig. 3 show that the SCA-efficiency is enhanced not only when the number of epochs increases but also when the batch decreases. We consider that as a natural behaviour since the number of gradient descents (and thus the number of steps in the solving of the minimization problem) increases linearly with the number of epochs and linearly with $(|\mathcal{D}_{\text{train}}|/batch\_size)$. However, as a counterpart, the training duration linearly increases with the number of gradient descent steps, as well. We selected one of the best trade-off, namely 100 epochs and a batch size equal to 200.[20] This choice will allow us to test the impact of the other parameters in our CNN experiments while keeping the training time acceptable.

The following benchmark validates, for a batch size equal to 200, that the previous observation (namely the fact that the SCA-efficiency increases with the number of epochs) stays true when traces are desynchronized.

With CNN_{base} and with 5000 traces, we manage to obtain a mean rank close to 20 for a maximal desynchronization value $N_{\max} = 50$, and a mean rank close to 40 for a maximal desynchronization value $N_{\max} = 100$. These results highlight the

[19] Leading to 10 training sets of size 45,000 and 10 test sets of size 5000 to perform the 10-fold cross-validation.

[20] Having 50 epochs and a batch size equal to 50 is also a good trade-off, but between two options that seem equivalent, we chose to prefer the solution with the highest number of epochs.

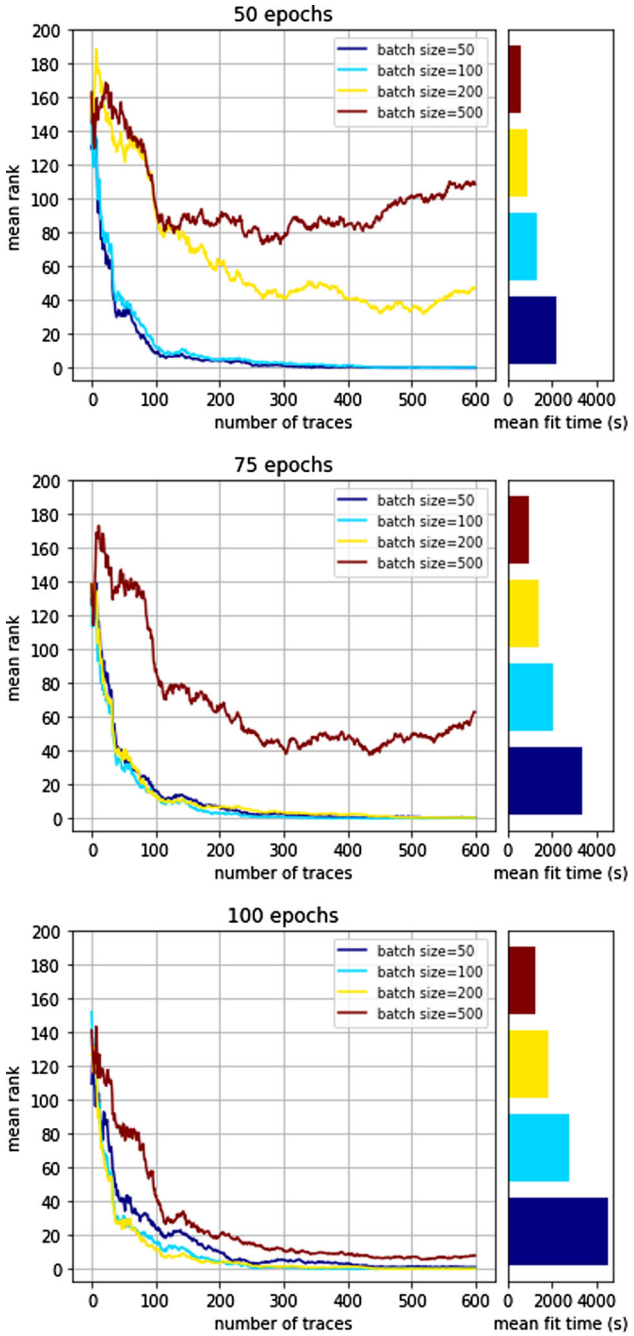


Fig. 3 Mean ranks and training time of CNN_{base} with different values of epochs and batch sizes

success of CNN architectures in the context of desynchronized traces, as studied in [13]. Results of Fig. 4 also show the impact of the epoch parameter on the SCA-efficiency with the desynchronization amount: an epoch value of 100 is enough without desynchronization, but it does not yield to the best performance when traces are desynchronized.

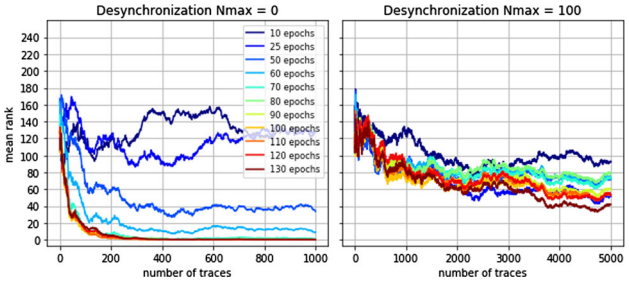


Fig. 4 Mean ranks of CNN_{base} for a desynchronization in {0, 100} and different numbers of epochs

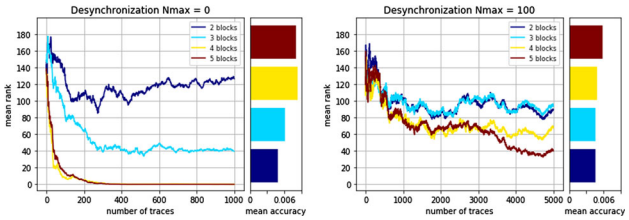


Fig. 5 Mean ranks (left-hand side) and mean accuracy (right-hand side) of CNN_{base} for a desynchronization in {0, 100} and several numbers of blocks

3.3.4 Architecture parameters

In each case, we study the parameters in the context of 256 classes.

Number of layers The architecture of our CNN_{base} suggests to divide the study of the number of layers in two phases: in a first time we make the number n_{blocks} of blocks vary where a block is composed of convolutional layers followed by a single pooling layer. In this phase we consider, for each block, only $n_{\text{conv}} = 1$ convolutional layer per block (which is the configuration of our CNN_{base} model). In a second time, we look for the optimal number n_{conv} of convolutional layers per block assuming that this number is fixed to for all the blocks and that the number of blocks equals 4.

Results of the first phase are plotted in Fig. 5. As expected, we notice that the SCA-efficiency increases with the number of blocks. A difference can be observed in the mean rank between 4 blocks and 5 blocks in presence of desynchronization. This fact can be explained in term of dimension of the input layer before applying the dense layers. The input trace has dimension 700, i.e. contains 700 temporal features, corresponding to its time samples. When 5 blocks are used, 5 max pooling layers of stride 2 are applied, and the temporal input dimension is divided by $2^5 = 32$, resulting in an input for the first dense layer composed of 21 temporal features times 512 abstract features (43 temporal features times 512 abstract ones if only 4 blocks). The temporal fea-

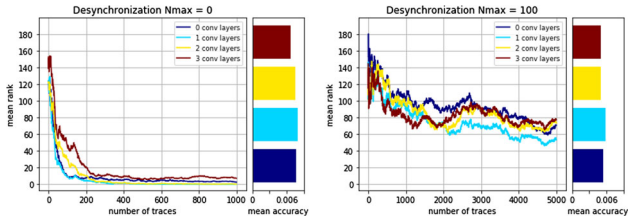


Fig. 6 Mean ranks (left-hand side) and mean accuracy of CNN_{base} for a desynchronization in {0, 100} and different numbers of CONV layers per block

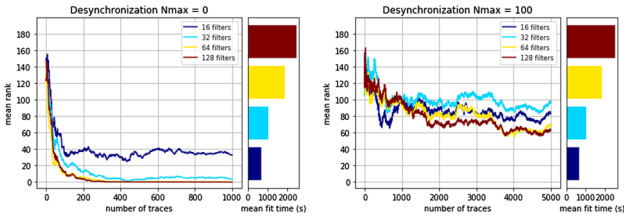


Fig. 7 Mean ranks (left-hand side) and mean training time (right-hand side) of CNN_{base} for a desynchronization in {0, 100} and different values of initial number of filters

tures are those which are directly impacted by the temporal noisy effect of desynchronization. So the less they are the more the model is robust to desynchronization. This explains why adding blocks increases the SCA-efficiency in presence of desynchronization. Thus, we choose $n_{\text{blocks}} = 5$ as best parameter. However, in our further benchmarks we keep the value $n_{\text{blocks}} = 4$; choosing this mid range value allows us to have a better understanding of the impact of the other parameters on the SCA-efficiency.

Results of the second phase are plotted in Fig. 6. We observe that optimal performances are obtained with only one CONV layer per block, even if the SCA-efficiency seems to be dimly impacted by n_{conv}. This is probably due to the fact that increasing number of layers, the number of trainable weights increases as well. To observe a benefit we should let models with more weights train longer, but for our benchmark we fixed the number of epochs (100 in our experiment). So not only we do not observe any benefit in augmenting the n_{conv}, but actually we observe performances slightly decreasing for an under-fitting phenomenon due to the lack of epochs. Observing results obtained with $n_{\text{conv}} = 0$, we verify the fact that the performance of the network is impacted by desynchronization when no CONV layer at all is exploited. The claim of CONV layers overcoming desynchronization issue by extracting patterns in the trace is then verified. Those conclusions are perfectly in line with [54] which observes that CONV layers play a minor role when the observations traces are perfectly synchronized.

Number of filters Following Rule 3, the aim of the next benchmark is to test several values for the number of filters in the CONV layers of the first block (denoted $n_{filters,1}$ in Rule 3). Figure 7 shows that increasing the number of filters also increases the SCA-efficiency. However, it also obviously increases the time of the training which leads us to look at a good trade-off between efficiency and computational time.

Kernel size We here study the impact of the kernel size (aka the dimension of the convolutional filters) on the model efficiency. In parallel, we compare two different approaches which either consist in combining several convolutional layers with small dimension or in selecting one unique convolutional layer with high dimension.

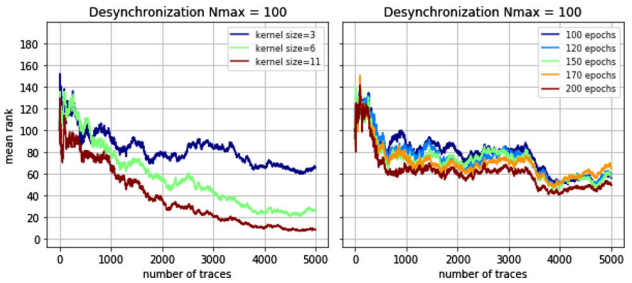


Fig. 8 Mean ranks with different kernel sizes (left-hand side) and mean ranks with 3 layers of dimension 3 in each block for different epochs (right-hand side) of CNN_{base}, for a desynchronization amount of 100

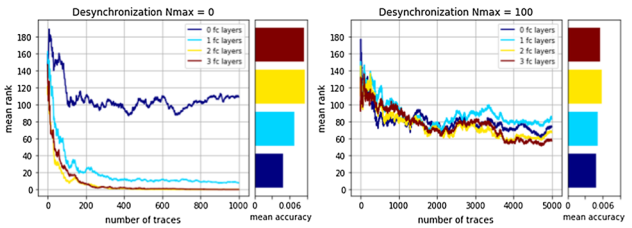


Fig. 9 Mean ranks (left-hand side) and mean accuracy (right-hand side) of CNN_{base} for a desynchronization in {0, 100} and various numbers of final fully-connected layers

Unexpectedly, as shown in Fig. 8, the kernel size significantly impacts the SCA-efficiency. We obtain a mean rank below 10 with a desynchronization amount of 100 by increasing the size of the filters to 11, whereas we only obtain a mean rank of 40 by increasing the number of convolutional layers to 3 for each block with filters of size 3. For a complete comparison we also increased the number of epochs to 200 in our second experiment but it clearly does not improve the efficiency in the same scale than the kernel size. This behaviour is very different than the one expected if we refer to recent results in computer vision where the trend is to increase the number of layers with filters of small size.

Number of fully-connected final layers

For this benchmark, we train four versions of CNN_{base} with different numbers of fully-connected final layers. Each of these dense layers has 4096 units. We observe from Fig. 9 that the network requires at least one dense layer when the

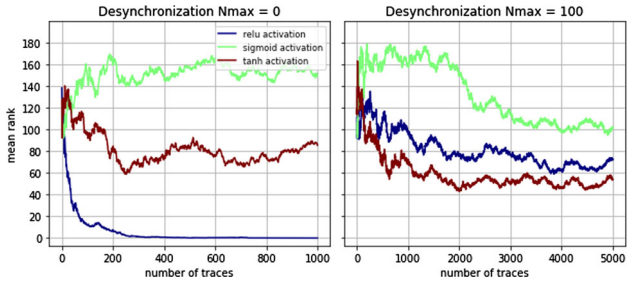


Fig. 10 Mean ranks of CNN_{base} for a desynchronization in $\{0, 100\}$ and activation function in $\{ReLU, tanh, sigmoid\}$

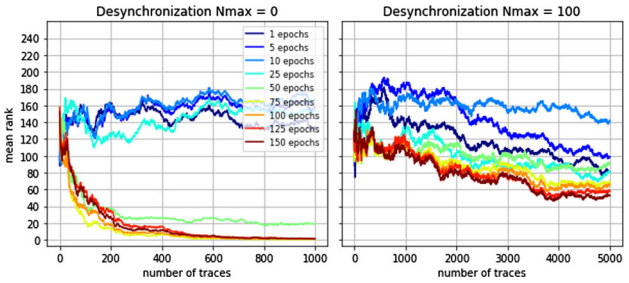


Fig. 11 VGG-16 mean ranks for a desynchronization amount in $\{0, 100\}$ and different numbers of epochs

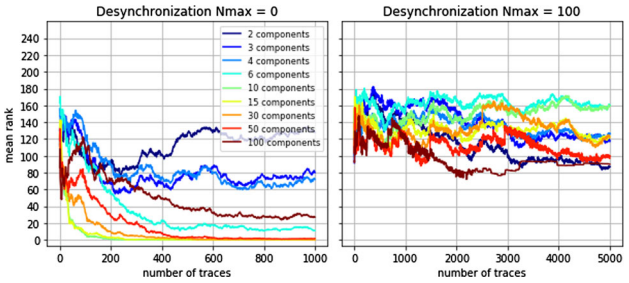


Fig. 12 Template Attacks mean ranks for a desynchronization amount in $\{0, 100\}$ and different values of PCA reduction

traces are synchronized. Roughly speaking, this suggest that, for SCA attacks, the QDA part of CNN networks is simulated by dense layers, while convolutional layers essentially extract information (e.g. by combining leakage points and/or by dealing with the desynchronization). The results also confirm that the number of dense layers increases the SCA-efficiency. Hence, fully connected layers are a critical part of the CNN network in the context of SCA and shall be not removed. This differs from the recent trend in computer vision where dense layers are replaced by an average pooling layer and it explains the poor results of Inception-v3 and ResNet-50 in our experiments (Fig. 2).

Activation functions For the three tested activation functions, Fig. 10 shows that only ReLU can afford a good efficiency for SCA when desynchronization is below 50. Therefore, we recommend the usage of ReLU activation function for CNN architecture.

Pooling layer and padding We observed that the choice of the pooling layer and the padding played a minor role in the attack success rate. Among the tested options, we eventually selected a the *Average* pooling layer and a padding option equal to *same*. More information about the related benchmarking may be found in "Appendix E".

CNN_{best} At the end of these benchmarks, we are able to define the best CNN architecture based on our selection of the parameters. Therefore, we define CNN_{best} as the CNN architecture with 5 blocks and 1 convolutional layer by block, a number of filters equal to (64, 128, 256, 512, 512) with kernel size 11 (*same* padding), ReLU activation functions and an average pooling layer for each block. The CNN has 2 final dense layers of 4096 units. CNN_{best} is trained with a batch size equal to 200 by using RMSprop optimizer with an initial learning rate of 10^{-5}. According to previous benchmarks and results of Fig. 4, a number of epochs above 130 is necessary to obtain the best results with CNN_{base} on desynchronized traces. In our experiments on CNN_{best}, we noticed that a training with 75 epochs is sufficient. For robustness and because it had an acceptable computing time impact, we eventually chose to benchmark until a number of epochs equal to 100.

4 Attack comparisons on desynchronized traces

In this section, we perform on desynchronized traces a last comparison of the efficiency of the four models studied throughout this article, namely: VGG-16, PCA-QDA (aka template attacks) and CNN_{best}. For completeness, we also report on comparisons with a MLP model trained by following an approach similar to that described in Sect. 3 for CNN models (see "Appendix C" for more details). As in the previous sections, models are evaluated with a 10-fold cross-validation on 50, 000 traces.

VGG-16 We train VGG-16 with different numbers of epochs. The size of the batch is equal to 200 and we use RMSprop optimizer with a initial learning rate of 10^{-5}. The results for different desynchronization values are plotted in Fig. 11. As expected, the SCA-efficient increases with the number of epochs and we select 150 epochs for this model.

Template attacks As described in Sect. 14, we first perform an unsupervised PCA on the 700 samples of the traces in the dataset $\mathcal{D}_{\text{profiling}}$ and we apply a QDA on the resulting components. Fig. 12 shows the impact of the desynchronization on the efficiency of template attacks. We note that the attack fails for a desynchronization amount equal to 100. When no desynchronization is added, best results are obtained when only 10 components are kept after the PCA.

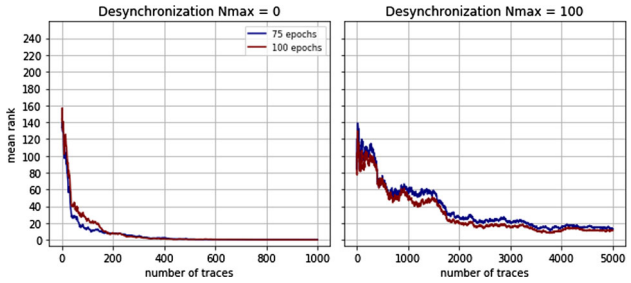


Fig. 13 Mean ranks of CNN_{best} for a desynchronization amount in {0, 100}

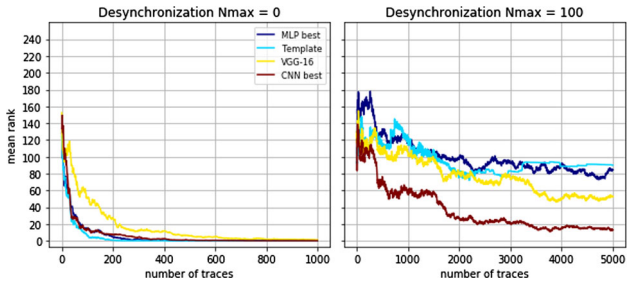


Fig. 14 Mean ranks of the best models for a desynchronization amount in {0, 100}

CNN_{best} Finally, we evaluate CNN_{best} with the parameters described in the previous subsection. Results are displayed in Fig. 13.

Summarize of the results In Fig. 14, we compare the best results obtained from the models. CNN_{best} outperforms all the other models on desynchronized traces with only 75 epochs. VGG-16 has decent results too, but with an higher number of epochs. CNN_{best} and template attacks combined to a PCA have similar results with synchronized traces, however this second model performs poorly with desynchronization. MLP_{best} has good performances on synchronized traces, but is very sensitive to desynchronization.[21]

5 Conclusions and perspectives

In this paper, we have conducted a thorough study of the application of deep learning theory in the context of side-channel attacks. In particular, we have discussed several parametrization options and we have presented a large variety of benchmarks which have been used to either experimentally validate our choices or to help us to take the adequate decision. The methodologies followed for the hyper-parameters selection may be viewed as a proposal to help researchers to make their own choice for the design of new deep learning models. They also open the way for further research in this domain. Since convolutional neural networks are shown almost similarly efficient as multi-layer perceptron networks in the context of perfectly synchronized observations but outperform them in presence of desynchronization/jittering, our study suggests that CNN models should be preferred in the context of SCA (even if they are more difficult to train). When it comes to choose a base architecture for the latter models, our study shows that the 16-layer network VGG-16 used by the VGG team in the ILSVRC-2014 competition [60] is a sound starting point (other public models like ResNet-50 [28] or Inception-v3 [63] are shown to be inefficient). Our results show that VGG-16 allows to design architectures which, after training, are better than classical Templates Attacks even when combined with dimension reduction techniques like principal component analysis (PCA) [53]. Clearly, our analysis does not enable to draw strong conclusions on the optimization and selection of optimal networks in the context of side-channel analysis. It however shows the impact of each hyper-parameter on the model soundness. All the benchmarkings have been done with the same target (and database) which corresponds to an AES implementation secured against first-order side-channel attacks and developed in assembly for an ATMega8515 component. This project has been published in [4]. To enable perfect reproducing of our experiments and benchmarks, we also chose to publish the electromagnetic measurements acquired during the processing of our target AES implementation (available in [3]) together with example Python scripts to launch some initial training and attacks based on these traces. We think that this ASCAD database may serve as a common basis for researchers willing to compare their new architectures or their improvements in existing models. In this paper, we did not address the question of model optimality in the context of side-channel attacks. We think that this subject, together with the extension of our study to masking schemes which are not a simple Boolean sharing, is a promising avenue for further research.

A signal-to-noise characterization of the target operations

See Fig. 15.

[21] For the sake of completeness, we have also tested the SCANet model introduced in [54]. This did not yield to good performances on our dataset: we have obtained a mean rank of approximatively 128 for each of our desynchronizations 0, 50 and 100.

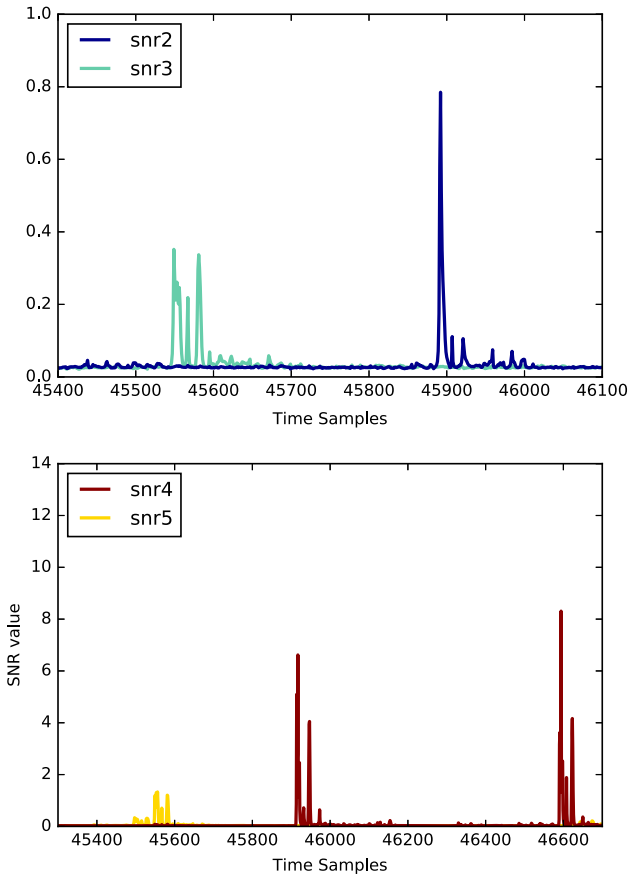


Fig. 15 SNRs for various intermediate values related to the processing of $\text{sbox}(p[3] \oplus k[3])$ in the interval [45400..46100]

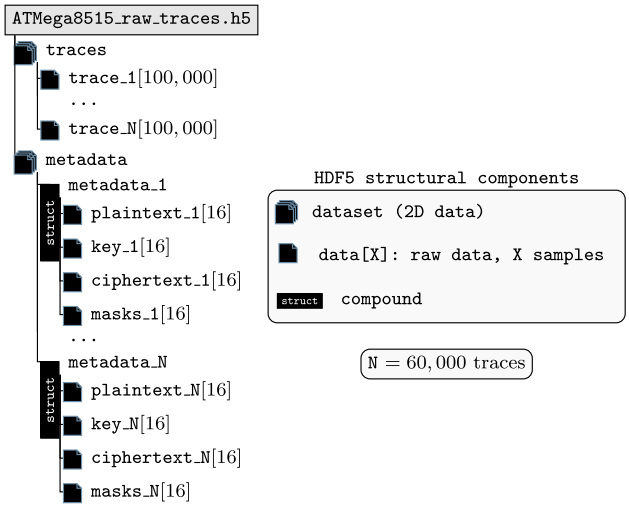


Fig. 16 Structure of the `ATMega8515_raw_traces.h5` HDF5 data file

B The new ASCAD database

B.1 Trace format

For the storage of the observations and the metadata (plaintext/ciphertext/key/mask values), we chose to use the current version 5 of the *Hierarchical Data Format* (HDF5). The latter one is a multi-purpose hierarchical container format capable of storing large numerical datasets with their metadata. The specification is open and the tools are open source. The development of HDF5 is done by the HDF Group, a non-profit corporation [26]. A HDF5 file contains a POSIX-like hierarchy of numerical arrays (aka datasets) organized within groups and subgroups. Effectively, HDF5 may be seen as a file system within a file, where files are datasets and folders are groups. Moreover, HDF5 also supports lossless compression of datasets. To manipulate our HDF5 files we used the `h5py` python package [27].

Our HDF5 file `ATMega8515_raw_traces.h5` is composed of two datasets within two groups: `metadata` and `traces`. The type of the latter one is HDF5 `Scalar Dataset` (i.e. may be viewed as a 2-dimensional array of 8-bit integers, the first dimension being the observation index, the second dimension being a time index and 8-bit integer being the type of the measure). The type of `metadata` is HDF5 `Compound Dataset` which is similar to a `struct` in `C` language. The `members` of the compound dataset `metadata` are *plaintext*, *ciphertext*, *key* and *mask* which all are arrays of 16 unsigned 8-bit integers. The 14 first elements of the *mask* array correspond to the masks $r[3], \cdots, r[16]$ in Algorithm 1 and the two last elements respectively correspond to r_{in} and r_{out} (as explained before the masks $r[1]$ and $r[2]$ have been forced to 0 for test/validation purpose). We give an overview of this structure on Fig. 16.

B.2 MNIST database and adaptations to SCA

Our raw traces format, as described in the previous subsection, is a classical representation of data for SCA analysis. This however suffers from some issues when considering it in the light of ML analysis:

- When considering a classification problem, one wants to get explicit and distinct classes where each trace is sorted (i.e. labelled) to help with the profiling phase.
- From the traces in `ATMega8515_raw_traces.h5`, it is not clear which dataset is to be used for training, and which is to be used for the tests and the accuracy computation.
- Finally, the raw `ATMega8515_raw_traces.h5` file does not contain explicit *labels* for the SCA classification problem, though these can be computed given the *plaintext* and *key* metadata.

The **MNIST database** [39] is a reference in the ML image classification community, allowing any new machine learn-

ing algorithm to be fairly compared to the state-of-the-art results. The efficiency of a new algorithm is tested against the classification of 28×28 pixels greyscale, normalized and centered images of handwritten digits. The database is split in groups, each one containing data and labels:

1. The *training dataset* group (50, 000 samples) contains the samples used during the training phase. This group is composed of the raw images in a file, and their labels with the same index in another file.
2. Similarly, the *test dataset* group (10,000 samples) is composed of the raw images in a file, and their labels with the same index in another file.

Following the path of the MNIST database, we propose a novel approach that fits the needs of testing ML algorithms against the SCA classification problems described in previous sections. We provide a database ASCAD with labelled datasets that will allow the *SCA community to objectively compare the efficiency of ML and DL methods*. To fit the SCA context, we have adapted the so-called MNIST training and test concepts to the more appropriate *profiling* and *attack* semantics as introduced and described in Sect. 2.2.1.[22]

The database information is extracted from the raw data file `ATMega8515_raw_traces.h5`, and its structure is presented on Fig. 17. For the sake of efficiency and simplicity, the HDF5 file format has been kept for our ASCAD database. The new file `ASCAD.h5` is composed of:

- two main groups: `Profiling_traces` for profiling which contains N_p information, and `Attack_traces` for attacking which contains N_a information.[23] In our case, over the 60, 000 labelled traces, we have chosen $N_p = 50,000$ and $N_a = 10,000$.
- In each main group, we find three HDF5 datasets;
  - the `traces` dataset contains the raw traces zoomed in on the 700 samples window of interest: the [45400..46100] interval containing the relevant information as previously described (only keeping the relevant samples in the traces allows to have a reasonably sized database),
  - the `labels` dataset contains the labels (following the ML classification meaning) for each trace. In our case, the value of the byte $\text{sbox}(p[3] \oplus k[3])$ is the label of interest, leading to 256 possible classes (the sequel of the article discusses this choice, and compares it to other possible classes such as using the Hamming weight of $\text{sbox}(p[3] \oplus k[3])$. In Remark 2, we explain how this labelling over the outputs of the sbox processing can be simply converted into a labelling over the different key candidates. It is to be noted that the masks *are not used* when computing the labels.
  - The `metadata` dataset contains the information related to each trace in a HDF5 compound (aka structure), taken from `ATMega8515_raw_traces.h5` almost without any modification (an additional field is added, see below). From a strict ML perspective, this metadata is useless since the labels are the only necessary information to check the efficiency of an algorithm. These data are however useful from a SCA perspective since the *plaintext* byte $p[3]$ is necessary to extract the estimated $\hat{k}[3]$ from the label values, and the real value of the key byte $k[3]$ is useful for the key ranking with regard to each class probability. Even though only $p[3]$ and $k[3]$ are useful for key ranking, we have decided to keep all the other metadata (the other *plaintext* and *key* bytes, the *ciphertext* and the *masks*) for the sake of completeness: the size of this metadata is very reasonable. Finally, a *desync* field is added to the compound structure: this `uint32` field represents the optional random desynchronization applied to the traces, which simulates a jitter as explained hereafter.

We feel that our ASCAD database is versatile enough to check the efficiency and accuracy of ML and DL algorithms applied to side-channel analysis, and we also aim at providing general purpose `python` scripts that will ease the process of:

- creating new databases following the same structure to attack other outputs in other AES rounds (with data extracted from `ATMega8515_raw_traces.h5` or any other similarly structured HDF5 file),
- modifying the profiling and attack datasets sizes and index to check their effect,
- adding a parametrized desynchronization to the traces to check the efficiency of the algorithm against jitter, and its impacts on the hyper-parameters. See the sequel of the article for a discussion on this.

As a benchmarking baseline, we will actually provide three HDF5 files that form our reference database:

- `ASCAD.h5`, which contains profiling and attack datasets as previously described. The traces are synchronized and there is no jitter,
- `ASCAD_desync50.h5`, which contains traces with a 50 samples window maximum jitter.

[22] Additionally, beware that in this paper training and testing are used in the context of cross-validation and are subsets of the profiling dataset $\mathcal{D}_{\text{profiling}}$.

[23] We recommend to perform the cross-validation only with the profiling set.

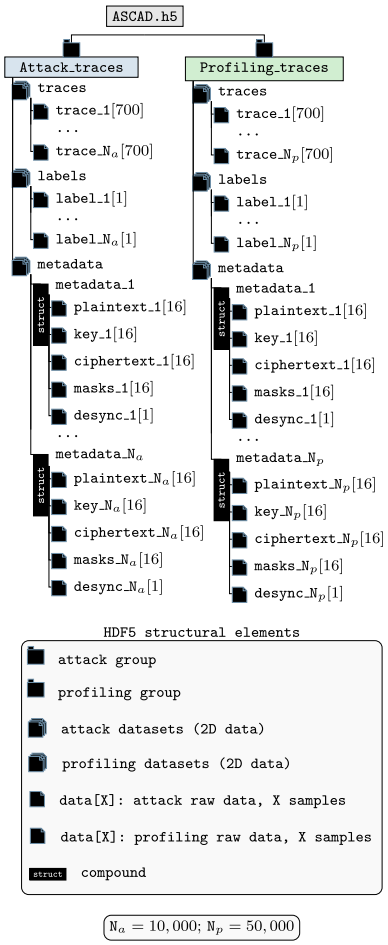


Fig. 17 Structure of the `ASCAD.h5` HDF5 data file

– `ASCAD_desync100.h5`, which contains traces with a 100 samples window maximum jitter.

The method used to simulate the jitter is described in 3.3.2.

C Multi-layer perceptrons (MLP)

C.1 Core principles and constructions

Multi-Layer Perceptrons (MLPs) are associated with a model/function $\hat{g}$ that is composed of multiple linear functions and some nonlinear *activation functions* which are efficiently-computable and whose derivatives are bounded and efficient to evaluate. In short, an MLP can be defined as follows:

$$\hat{g} : \boldsymbol{\ell} \mapsto \hat{g}(\boldsymbol{\ell}) = \mathsf{s} \circ \lambda_n \circ \alpha_{n-1} \circ \lambda_{n-1} \circ \cdots \circ \lambda_1(\boldsymbol{\ell}) = \mathbf{y} \,, \tag{10}$$

where:

Algorithm 1: Secure AES Implementation with Table Recomputation

Input : a 16-byte plaintext $(p[1], \cdots, p[16])$, an 18-byte mask vector $(r[1], \cdots, r[16], r_{\text{in}}, r_{\text{out}})$, and a 16-byte master key $(mk_1, \cdots, mk_{16})$

Output: a 16-byte ciphertext $(c_1, \cdots, c_{16})$

steps] function **MaskedAES:**

```
// SBox recomputation
for i = 0 to 255 do
1]    sbox*[i] ← sbox[i ⊕ r_in] ⊕ r_out
// Initialization
for i = 1 to 16 do
2]    state0[i] ← p[i] ⊕ r[i]
3]    state1[i] ← r[i]
4]    key[i] ← mk_i
// AES processing
for round = 1 to 10 do
      /* Key scheduling                                   */
5]    (key[1], ··· , key[16]) ←
       KeyScheduling(key[1], ··· , key[16])
      for i = 1 to 16 do
            /* AddRoundKey and SubBytes                   */
6]          state0[i] ← (state0[i] ⊕ key[i] ⊕ r_in) ⊕ state1[i]
7]          state0[i] ← sbox*[state0[i]]
8]          state0[i] ← (state0[i] ⊕ state1[i]) ⊕ r_out
      /* ShiftRows                                        */
9]    (state0[1], ··· , state0[16]) ←
       ShiftRows(state0[1], ··· , state0[16])
10]   (state1[1], ··· , state1[16]) ←
       ShiftRows(state1[1], ··· , state1[16])
      /* MixColumns except for the last round
         */
      if round ≠ 10 then
11]         (state0[1], ··· , state0[16]) ←
             MixColumns(state0[1], ··· , state0[16])
12]         (state1[1], ··· , state1[16]) ←
             MixColumns(state1[1], ··· , state1[16])
// Last AddRoundKey
13](key[1], ··· , key[16]) ← KeyScheduling(key[1], ··· , key[16])
for i = 1 to 16 do
14]   c_i ← (state0[i] ⊕ key[i]) ⊕ state1[i]
// Return the ciphertext
return (c_1, ..., c_16)
```

– the λ_i functions are the so-called *Fully-Connected* (FC) layers and are expressible as affine functions: denoting $\mathbf{v}$ the D-dimensional input of an FC, its output is given by $\mathbf{A}\boldsymbol{\ell} + \mathbf{B}$, being $\mathbf{A} \in \mathbb{R}^{C \times D}$ a matrix of weights and $\mathbf{B} \in \mathbb{R}^{C}$ a vector of biases.
– the α_i are the so-called *activation functions* (ACT): an activation function is a nonlinear real function that is applied independently to each coordinate of its input (e.g. the ReLU activation function processes $\max(0, x)$ to each coordinate x),

– s is the so-called *softmax* function (SOFT): $\mathsf{s}(\boldsymbol{\ell})[i] = \frac{e^{\boldsymbol{\ell}[i]}}{\sum_j e^{\boldsymbol{\ell}[j]}}$.

In the rest of the paper, $\texttt{MLP}(n_{\text{layer}}, n_{\text{units}}, \alpha)$ will denote an MLP architecture with n_{layer} layers, n_{units} units (a.k.a. nodes or neurons) and α as activation function for each hidden layer. Such an MLP corresponds to (10) with $\alpha_i = \alpha$ for every i, with $n = n_{\text{layer}}$, and with λ_i defined for $D = C = n_{\text{units}}$ if $i \in [2...n_{\text{layer}}-1]$ and for $(C, D) = (n_{\text{units}}, 700)$ if $i = 1$ and $(C, D) = (256, n_{\text{units}})$ for $i = n_{\text{layer}}$ (indeed inputs of the model are 700-dimensional leakage traces while the outputs are in [0..255]).

C.2 Choice of the hyper-parameters

As explained in Sect. 3.3, the strategy we applied to tune the hyper-parameters is divided into three steps. First we fix a base architecture that we denote MLP_{base} corresponding to $\texttt{MLP}(6, 200, \mathit{ReLU})$, the 6-layers MLP with 200 units and the ReLU activation function for each layer. Secondly we tune the training parameters, leading to the parametrization of a procedure $\texttt{Training}(n_{\text{epochs}}, \mathit{batch\_size}, \mathit{optimizer}, \mathit{learning\_rate})$. Then, different variations of MLP_{base} are tested by studying the impact of each architecture parameter on the model efficiency after training with the procedure fixed during previous step. The full strategy aims at providing us with an architecture MLP_{best} and a training procedure that are good w.r.t. the evaluation metrics listed in Sect. 2.4.2.

C.2.1 Training parameters

This subsection aims at studying how the mean rank of the side-channel attack involving the trained model is impacted by the length of the training dataset, the number of epochs, the batch size and the learning rates/optimizers.

First we evaluate the impact of the size N_{train} of the training set on the success of a neural network based SCA. We performed a 10-fold cross-validation with different sizes of dataset, while keeping a constant computational time during the training step for fair comparison. This is done by adapting the number of epochs to the number of traces in the dataset. We expect that the performance of the model increases with the size of the training set until a certain threshold that determined the optimal number of traces. The neural network used for this experiment is MLP_{base} trained with RMSProp optimizer, learning rate 10^{-5} and batch size 100. The initialization of the weights is performed from an uniform distribution of mean 0 as defined in Glorot and Bengio's article [22]. Figure 18 shows the mean rank function for different sizes of training set. Our empirical results on the full `ATMega8515_raw_traces.h5` show that approximately 50, 000 training traces are required for a full success

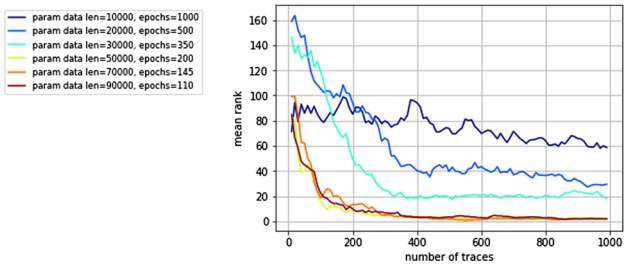


Fig. 18 Mean rank function (7) after 10-fold cross-validation of MLP_{base} with $\texttt{Training}(\cdot, 100, \text{RMSProp}, 10^{-5})$ for different sizes of training set, for an increasing number n of test traces and for different epochs chosen to keep the overall computation time roughly constant

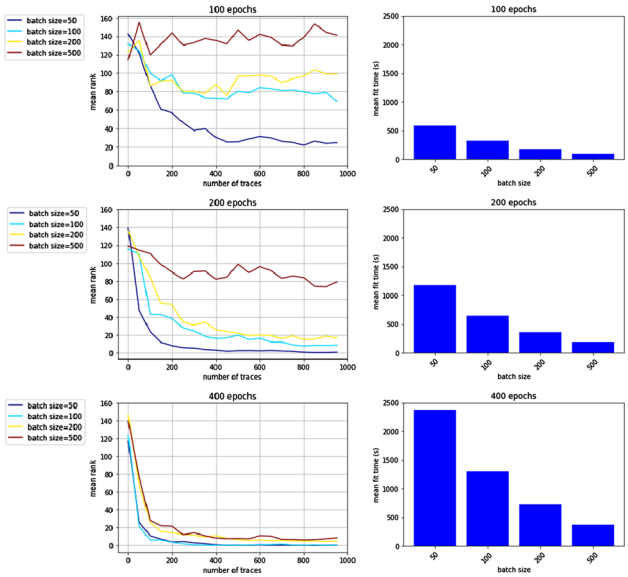


Fig. 19 Mean ranks and training time of $\text{MLP}_{\text{base}} = \texttt{MLP}(6, 200, \mathit{ReLU})$ trained with $\texttt{Training}(n_{\text{epochs}}, \mathit{batch\_size}, \text{RMSProp}, 10^{-5})$ for varying values of n_{epochs} and $\mathit{batch\_size}$

of the attack/test in less than 1000 traces. That is why ASCAD is composed of a training set $\mathcal{D}_{\text{profiling}}$ of size 50, 000 and an attack set $\mathcal{D}_{\text{attack}}$ of size 10,000. Based on these results, the benchmarks in the rest of the paper were performed on ASCAD profiling traces $\mathcal{D}_{\text{profiling}}$.

Then we select the best values for the number of epochs and the batch size of the training step. Figure 19 shows the empirical results for different values n_{epochs} with a 10-fold cross-validation on $\mathcal{D}_{\text{profiling}}$. We notice that the number of epochs has a significant impact on the rank functions. Taking into account the trade-off between computation time and SCA-efficiency, best results are obtained by choosing 400 epochs and a batch size equal to 500 or 200 epochs and a batch size equal to 100. However, it appears that we have a best accuracy and a best stability on the rank functions with the latter pair of parameters, which leads us to select these values for the rest of our benchmarks on MLP. We insist on the fact that theses values are obtained as a trade-off that

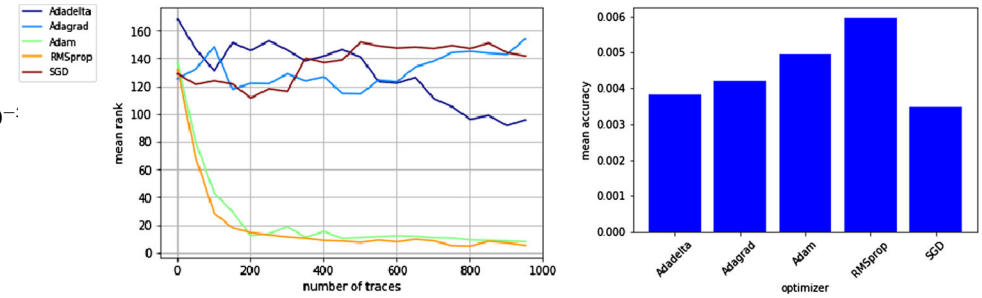


Fig. 20 Mean ranks and accuracy of $\text{MLP}_{\text{base}} = \texttt{MLP}(6, 200, ReLU)$ trained with $\texttt{Training}(200, 100, optimizer, 10^{-}$ for different optimizers

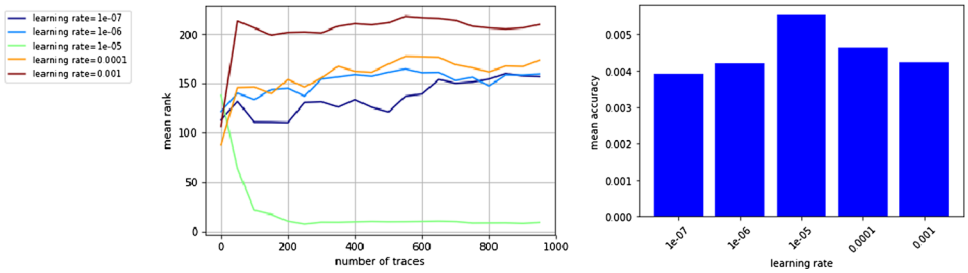


Fig. 21 Mean ranks and accuracy of $\text{MLP}_{\text{base}} = \texttt{MLP}(6, 200, ReLU)$ with RMSProp optimizer and different values of learning rate

allows us to perform multiple cross-validations in a reasonable amount of time. When the batch size parameter is fixed to 100 we can obtained better results by increasing the number of epochs and consequently the training time. Therefore in the case of a single SCA attack in a given amount of time, we recommend to fix the batch size to 100 and to increase progressively the number of epochs after 200 until the dedicated amount of time for the training step is reached (in our experimental results we did not notice any improvement in the SCA-efficiency after 800 epochs).

The last training parameters that we tune are the gradient descent optimization method (also called optimizer) and the learning rate. Empirical results in Figs. 20 and 21 show that these parameters also have a high impact on the success of the attack. We managed to obtain good results with $optimizer = RMSProp$ and a learning rate equal to 10^{-5} (which confirms the soundness of the choices made for experiments reported in Figs. 18 and 19).

C.2.2 Architecture parameters

As described in previous subsection, an MLP architecture is characterized by three architecture hyper-parameters: the number of layers, the number of units of each layer and the activation functions. In this section, we use the training procedure $\texttt{Training}(200, 100, RMSProp, 10^{-5})$ determined in previous section and we come back on our MLP_{base} initial choice to challenge its hyper-parameters.

First we evaluate the optimal number of layers with a fixed number of nodes: models $\texttt{MLP}(n_{\text{layers}}, 200, ReLU)$ are trained for different values $n_{\text{layers}} \in [3..11]$. Figure 22 plots the mean rank function, the mean accuracy and the average training time. All the mean rank functions converge to 0 when the number of traces increases. However, the 6-layers MLP has a slight advantage on less than 600 traces and has the best mean accuracy.

Then we evaluate the optimal number of units per layer. Small values lead to simple models that are not powerful enough to represent the dataset trends and high values lead to complex models that are difficult to train and are more susceptible to over-fitting. We limit our empirical study to MLPs with the same number of units by layer. Figure 23 shows the obtained results. With the previously fixed training parameters, the performance of the attack seems to increase once the number of units per layer equals or exceeds 200.

Finally we study the effect of the activation function on the performance of the neural network. Since its introduction in Deep Learning, Rectified Linear Units (ReLUs) have proved to be the best suitable choice for a number of problems, and most specifically in image recognition [23,32,51]. The obtained networks have sparse representation, and the simple definition of the $ReLU(x) = \max(0, x)$ activation function allows quick computations. Figure 24 plots the experimental results obtained with $\texttt{MLP}(6, 200, \alpha)$ for different activation functions α. The best results are obtained with $ReLU$, $tanh$ and $softsign$ which is a variation of $tanh$. We select $ReLU$ activation function since it provides state-of-the-art results and its computation time is below the two other functions.

Benchmarks reported in this section confirms that the architecture $\texttt{MLP}(6, 200, ReLU)$ leads to good compromise efficiency *versus* computational time when trained with the following parameters: $\texttt{Training}(200, 100, RMSProp, 10^{-5})$. In the rest of this paper, this architecture is denoted MLP_{best}. We insist on the fact that MLP_{best} has a decent

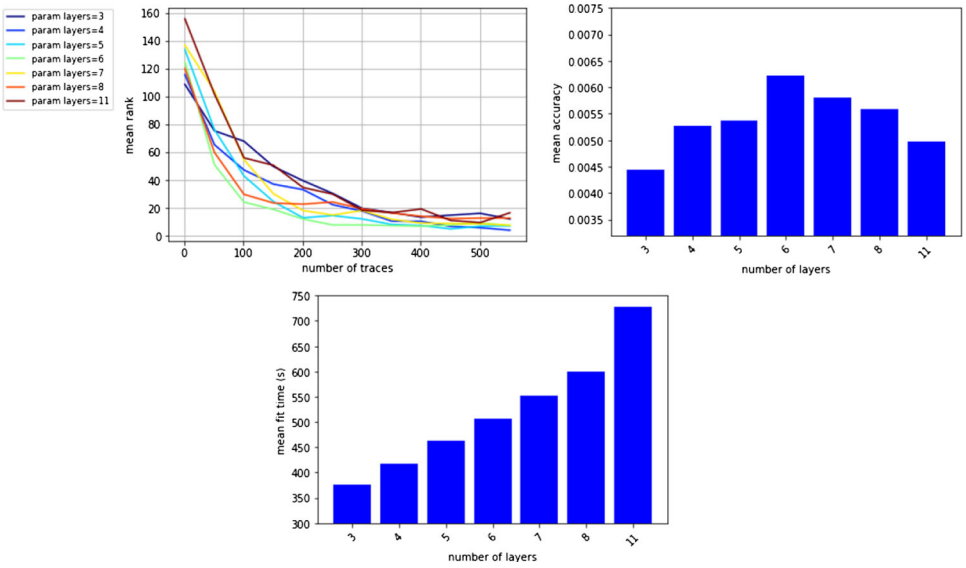


Fig. 22 Mean ranks, mean accuracy and mean training time of $\texttt{MLP}(n_{\text{layers}}, 200, ReLU)$ with different numbers of n_{layers}

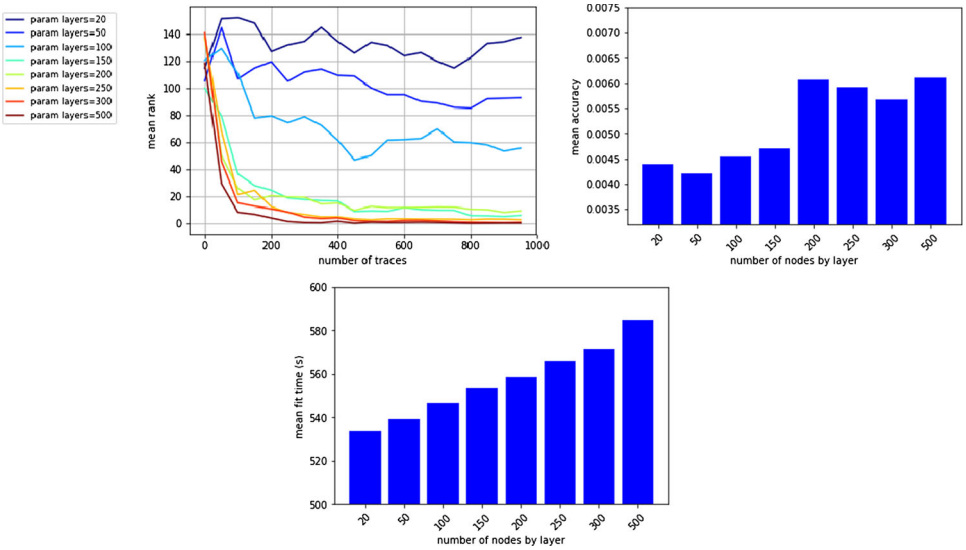


Fig. 23 Mean ranks, mean accuracy and mean training time of $\texttt{MLP}(6, n_{\text{units}}, ReLU)$ with different n_{units}

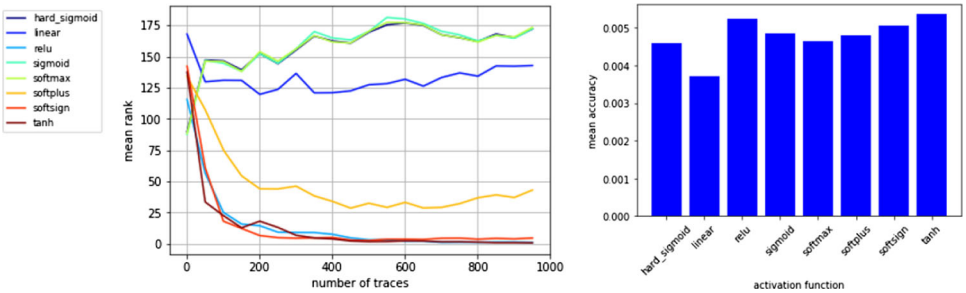


Fig. 24 Mean ranks of $\texttt{MLP}(6, 200, \alpha)$ with different activation functions

SCA-efficiency with 200 epochs but the latter efficiency continues to improve when the number of epochs increases until 800 epochs (in our experiments we did not notice any significant improvement after 800 epochs). Hence, depending on the amount of time allocated to the training of MLP_{best}, it may be interesting to increase the number of epochs in the range [200..800].

C.3 Open discussions

C.3.1 Self-normalizing neural networks

Recently, a new type of MLP called Self-Normalizing Neural Networks (SNN) has been introduced in [33]. It aims to improve the robustness of MLPs against perturbation during

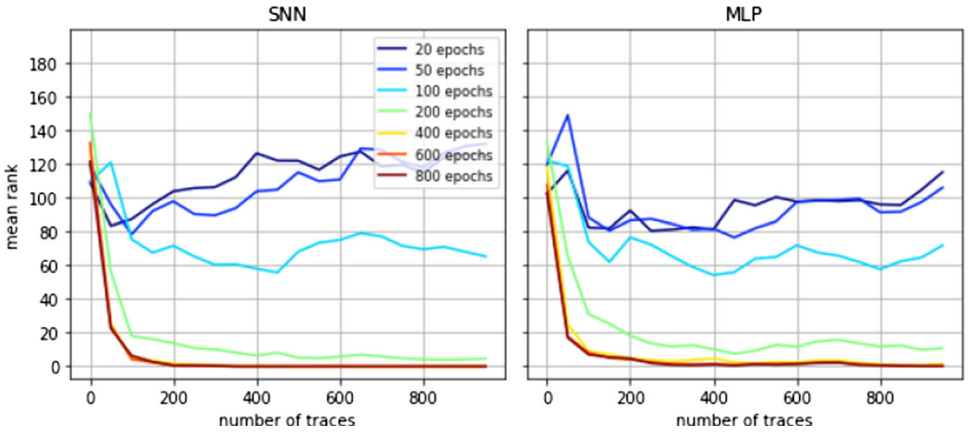


Fig. 25 Mean ranks and accuracy of a SNN and MLP_{best} with different numbers of epochs

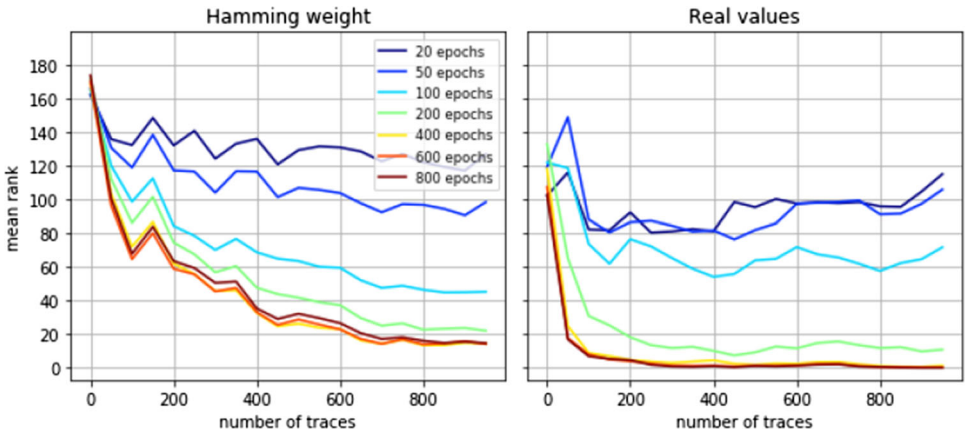


Fig. 26 Mean ranks of MLP_{best} with Hamming weights as labels and MLP_{best} with real values as labels

the training step and to reduce the variance of the training error. Its architecture is a slight variation of the standard MLP architecture: the activation function, called "scaled exponential linear units" (SELU) is given by:

$$selu(x) = \lambda \begin{cases} x & \text{if } x > 0 \\ \alpha e^x - \alpha & \text{if } x \leq 0 \end{cases}. \tag{11}$$

Furthermore, the initialization of the weights is performed from a standard normal distribution. These two modifications imply that the neural network is self-normalizing, i.e. the mean and variance of the activation functions across the different layers stay within small pre-defined intervals. This new architecture outperformed standard MLPs on a number of benchmarks, including MNIST.

We test on the ASCAD a SNN architecture with 6 layers and 200 units for each layer and we compare it with MLP_{best}. Experimental results in Fig. 25 show that rank functions are very similar between the two architectures. This highlights the fact that there does not seem to be any significant improvement with the SNN architecture in the context of SCA. The accuracy is slightly higher with SNN as expected in a Machine Learning perspective, however it does not have an influence on the overall rank function.

C.3.2 Hamming weight versus identity labelling

We test our MLP_{best} architecture on the SCA dataset with a labelling of the traces modified to take the Hamming weight of the sensitive value instead of the real value itself. This strategy of data labelling reduces the number of classes to predict (9 values for the Hamming weight instead of 256 values for a byte). Consequently, the model trained on the new dataset is less complex than the model trained on the full values. We also modify the computation of the rank function in (2) by taking into account the distribution of the Hamming weight values. In Fig. 26, the corresponding rank functions are plotted. They show that the new labelling strategy is less interesting. Indeed, even if the Hamming weight model is less complex and requires a smaller number of epochs for the training step, the conditional probability approximated by the neural network is less discriminating (which is a consequence of the reduced number of classes). Moreover, the weighting coefficients in (2) (deduced from the Hamming

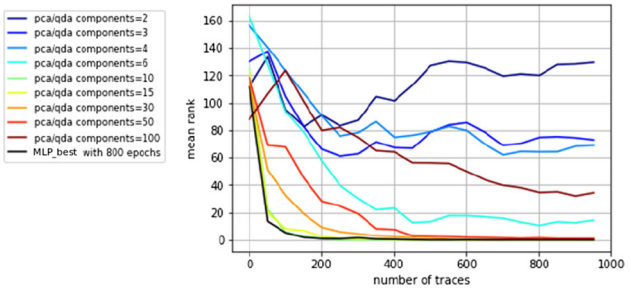


Fig. 27 Mean ranks of a PCA on n components followed by a QDA

weight distribution for uniform data) may increase the variance of the rank (viewed as a random variable) since e.g. an error on a value with Hamming weight 0 or 8 accounts for $\binom{8}{4} = 70$ times an error on a value of Hamming weight 4. Eventually, assuming that the deterministic part of the leakage corresponds to an Hamming weight may be an incorrect abstraction and induces error in the modelling.

C.3.3 Comparison with template attacks

We compare MLP_{best} with standard template attacks (aka quadratic discriminant analysis, or QDA in the machine learning community). We first perform an unsupervised dimension reduction to extract meaningful features. For this task we use a classical PCA which is parametrized by the number of components to extract. Then the classification task is performed with a QDA (i.e. Template Attacks). Note that, contrary to QDA, neural networks do not require the preprocessing feature extraction step since this task is realized by the first layers of the networks. Figure 27 shows the results obtained with different numbers of components extracted from the PCA.

C.3.4 First-order attacks

By using the mask values contained in the ASCAD, it is possible to compute the masked output after the first round AES Sbox:

$$z = \text{sbox}(p[3] \oplus k[3]) \oplus r_{\text{out}}$$

where z is the sensitive value and $p[3]$, $k[3]$, r_{out} are the plaintext byte, the key byte and the mask byte.

Therefore, we can mount a first-order SCA by labelling the traces with the masked output values and we can test the performance of MLP_{best} in this weaker context. The results in Fig. 28 show that, without any modification in the architecture and the training parameters, MLP_{best} easily succeeds in this attack. The rank functions converge to 0 with 20 epochs and only 4 traces are required to determine the correct key. We also managed to obtain an accuracy of 0.028, and we did not notice any over-fitting with 200 epochs.

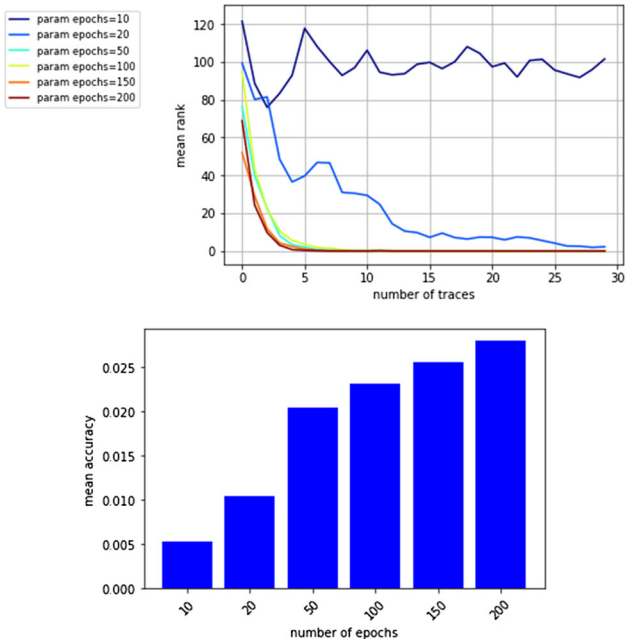


Fig. 28 Mean ranks and accuracy of MLP_{best} on a first-order SCA

C.4 Efficiency results on ASCAD database

We trained MLP_{best} on ASCAD Database with and without desynchronization and with different numbers of epochs. As shown in Fig. 29, MLP is very sensitive to desynchronization and increasing the number of epochs is not enough to get better results.

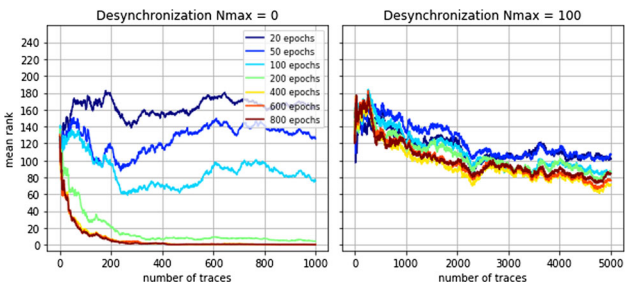


Fig. 29 Mean ranks of MLP_{best} for a desynchronization amount in $\{0, 100\}$ and different values of epochs

D Example of tested CNN architecture

See Fig. 30.

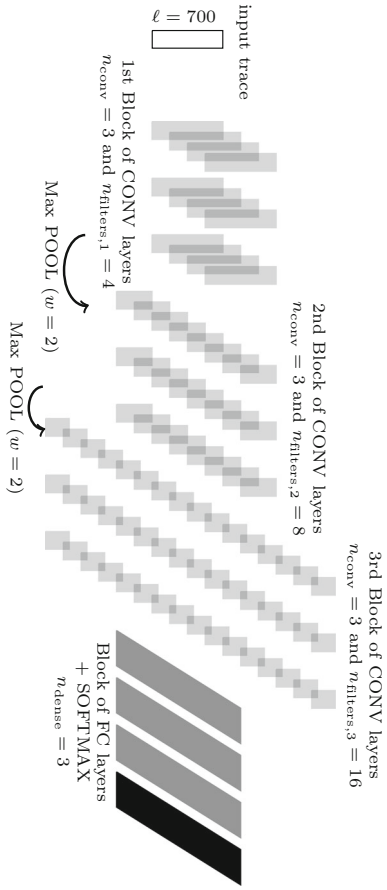


Fig. 30 Example of our CNN_{base} architecture

E CNN: Supplementary materials for t7he hyper-parameters' choice

Pooling Layer and Padding We tested three different options for all the pooling layers of CNN_{base}: max pooling, average pooling, and *stride pooling*[24]. Contrary to standard CNN architectures used in computer vision that rely on max pooling, we obtained our best results with average pooling layers (Fig. 31).

Padding Finally we tested two configurations of padding. Results in Fig. 32 show that this parameter does not have a significant impact on the SCA-efficiency.

[24] Stride pooling consists in taking the first value on each input window defined by the stride.

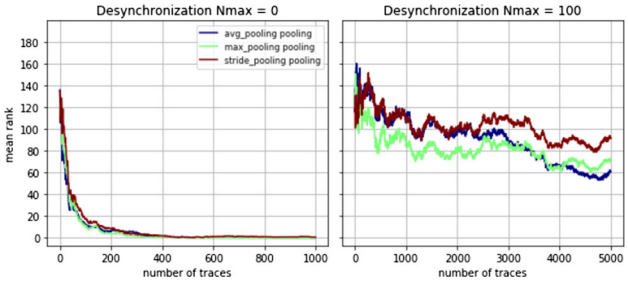


Fig. 31 For a desynchronization amount in {0, 100} and different pooling layers (either max or average or stride pooling), the mean ranks of CNN_{base}

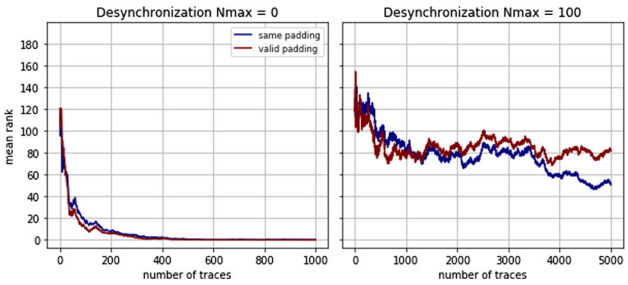


Fig. 32 For a desynchronization amount in {0, 100} and a padding option either set to *same* or to *valid*, the mean ranks of CNN_{base}

References

1. Abadi, M., Agarwal, A., Barham, P., Brevdo, E., Chen, Z., Citro, C., Corrado, G.S., Davis, A., Dean, J., Devin, M., Ghemawat, S., Goodfellow, I., Harp, A., Irving, G., Isard, M., Jia, Y., Jozefowicz, R., Kaiser, L., Kudlur, M., Levenberg, J., Mané, D., Monga, R., Moore, S., Murray, D., Olah, C., Schuster, M., Shlens, J., Steiner, B., Sutskever, I., Talwar, K., Tucker, P., Vanhoucke, V., Vasudevan, V., Viégas, F., Vinyals, O., Warden, P., Wattenberg, M., Wicke, M., Yu, Y., Zheng, X.: TensorFlow: Large-scale machine learning on heterogeneous systems (2015). https://www.tensorflow.org/. Software available from tensorflow.org
2. Akkar, M.L., Giraud, C.: An Implementation of DES and AES, Secure against Some Attacks. In: Ç. Koç, D., Naccache, D., Paar, C. (eds.) Cryptographic Hardware and Embedded Systems–CHES 2001. Lecture Notes in Computer Science, vol. 2162, pp. 309–318. Springer, Berlin (2001)
3. ANSSI: Ascad database (2018). https://github.com/ANSSI-FR/ASCAD
4. ANSSI: secaes-atmega8515 (2018). https://github.com/ANSSI-FR/secAES-ATmega8515
5. Bartkewitz, T., Lemke-Rust, K.: Efficient template attacks based on probabilistic multi-class support vector machines. In: Mangard, S. (ed.) Smart Card Research and Advanced Applications CARDIS. Lecture Notes in Computer Science, vol. 7771, pp. 263–276. Springer, Berlin (2013). https://doi.org/10.1007/978-3-642-37288-9_18
6. Bengio, Y., Grandvalet, Y.: Bias in estimating the variance of k-fold cross-validation. In: Duchesne, P., Rémillard, B. (eds.) Statistical modeling and analysis for complex data problems, pp. 75–95. Springer, Berlin (2005)
7. Bergstra, J., Bengio, Y.: Random search for hyper-parameter optimization. J. Mach. Learn. Res. **13**((Feb)), 281–305 (2012)
8. Bergstra, J., Yamins, D., Cox, D.D.: Hyperopt: a python library for optimizing the hyperparameters of machine learning algorithms.

In: Proceedings of the 12th Python in Science Conference, pp. 13–20 (2013)
9. Bishop, C.M.: Pattern Recognition and Machine Learning. Springer, Berlin (2006)
10. Breiman, L., et al.: Heuristics of instability and stabilization in model selection. Ann. Stat. **24**(6), 2350–2383 (1996)
11. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: Joye, M., Quisquater, J.J. (eds.) Cryptographic Hardware and Embedded Systems–CHES 2004. Lecture Notes in Computer Science, vol. 3156, pp. 16–29. Springer, Berlin (2004)
12. Cagli, E., Dumas, C., Prouff, E.: Kernel discriminant analysis for information extraction in the presence of masking. In: K. Lemke-Rust, M. Tunstall (eds.) Smart Card Research and Advanced Applications-15th International Conference, CARDIS 2016, Cannes, France, 7–9 November 2016, Revised Selected Papers, Lecture Notes in Computer Science, vol. 10146, pp. 1–22. Springer, Berlin (2016). https://doi.org/10.1007/978-3-319-54669-8_1
13. Cagli, E., Dumas, C., Prouff, E.: Convolutional neural networks with data augmentation against jitter-based countermeasures - profiling attacks without pre-processing. In: W. Fischer, N. Homma (eds.) Cryptographic Hardware and Embedded Systems-CHES 2017-19th International Conference, Taipei, Taiwan, September 25–28 2017, Proceedings, Lecture Notes in Computer Science, vol. 10529, pp. 45–68. Springer, Berlin (2017). https://doi.org/10.1007/978-3-319-66787-4_3
14. Chari, S., Rao, J., Rohatgi, P.: Template attacks. In: Kaliski Jr., B., Koç, Ç., Paar, C. (eds.) Cryptographic Hardware and Embedded Systems-CHES 2002. Lecture Notes in Computer Science, vol. 2523, pp. 13–29. Springer, Berlin (2002)
15. Chollet, F., et al.: Keras (2015). https://github.com/fchollet/keras
16. Cortes, C., Vapnik, V.: Support-vector networks. Mach. Learn. **20**(3), 273–297 (1995). https://doi.org/10.1007/BF00994018
17. Doget, J., Prouff, E., Rivain, M., Standaert, F.X.: Univariate side channel attacks and leakage modeling. J. Cryptogr. Eng. **1**(2), 123–144 (2011)
18. Fisher, R.A.: On the mathematical foundations of theoretical statistics. Philos. Trans. R. Soc. Lond. Ser. A. **222**, 309–368 (1922). https://doi.org/10.1098/rsta.1922.0009
19. Fisher, R.A.: The use of multiple measurements in taxonomic problems. Ann. Eugen. **7**(7), 179–188 (1936)
20. Friedman, J., Hastie, T., Tibshirani, R.: The Elements of Statistical Learning. Springer Series in Statistics, vol. 1. Springer, New York (2001)
21. Gilmore, R., Hanley, N., O'Neill, M.: Neural network based attack on a masked implementation of AES. In: IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2015, Washington, DC, USA, 5–7 May 2015, pp. 106–111. IEEE Computer Society (2015). https://doi.org/10.1109/HST.2015.7140247
22. Glorot, X., Bengio, Y.: Understanding the difficulty of training deep feedforward neural networks. In: Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics, pp. 249–256 (2010)
23. Glorot, X., Bordes, A., Bengio, Y.: Deep sparse rectifier neural networks. In: Proceedings of the Fourteenth International Conference on Artificial Intelligence and Statistics, pp. 315–323 (2011)
24. Goodfellow, I., Bengio, Y., Courville, A.: Deep Learning. MIT Press, Cambridge (2016)
25. Goodfellow, I.J., Bengio, Y., Courville, A.C.: Deep Learning. Adaptive Computation and Machine Learning. MIT Press, Cambridge (2016)
26. Group, H.: The hdf group. https://www.hdfgroup.org/
27. Group, H.: HDF5 For Python. http://www.h5py.org/
28. He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for image recognition. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 770–778 (2016)
29. Heuser, A., Zohner, M.: Intelligent machine homicide-breaking cryptographic devices using support vector machines. In: W. Schindler, S.A. Huss (eds.) Constructive Side-Channel Analysis and Secure Design-Third International Workshop, COSADE 2012, Darmstadt, Germany, 3–4 May 2012. Proceedings, Lecture Notes in Computer Science, vol. 7275, pp. 249–264. Springer, Berlin (2012). https://doi.org/10.1007/978-3-642-29912-4_18
30. Hospodar, G., Gierlichs, B., Mulder, E.D., Verbauwhede, I., Vandewalle, J.: Machine learning in side-channel analysis: a first study. J. Cryptogr. Eng. **1**(4), 293–302 (2011). https://doi.org/10.1007/s13389-011-0023-x
31. Ioffe, S., Szegedy, C.: Batch normalization: accelerating deep network training by reducing internal covariate shift. CoRR (2015). arXiv:1502.03167
32. Jarrett, K., Kavukcuoglu, K., LeCun, Y., et al.: What is the best multi-stage architecture for object recognition? In: 2009 IEEE 12th International Conference on Computer Vision, pp. 2146–2153. IEEE (2009)
33. Klambauer, G., Unterthiner, T., Mayr, A., Hochreiter, S.: Self-normalizing neural networks (2017). arXiv preprint arXiv:1706.02515
34. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) Advances in Cryptology-CRYPTO'99. Lecture Notes in Computer Science, vol. 1666, pp. 388–397. Springer, Berlin (1999)
35. Krizhevsky, A., Sutskever, I., Hinton, G.E.: Imagenet classification with deep convolutional neural networks. Commun. ACM **60**(6), 84–90 (2017). https://doi.org/10.1145/3065386
36. LeCun, Y., Bengio, Y., et al.: Convolutional networks for images, speech, and time series. The Handbook of Brain Theory and Neural Networks **3361**(10), 1995 (1995)
37. LeCun, Y., Boser, B., Denker, J.S., Henderson, D., Howard, R.E., Hubbard, W., Jackel, L.D.: Backpropagation applied to handwritten zip code recognition. Neural Comput. **1**(4), 541–551 (1989)
38. LeCun, Y., Bottou, L., Bengio, Y., Haffner, P.: Gradient-based learning applied to document recognition. Proc. IEEE **86**(11), 2278–2324 (1998)
39. LeCun, Y., Cortes, C., Burges, C.J.: The MNIST database of handwritten digits. http://yann.lecun.com/exdb/mnist/
40. LeCun, Y., Huang, F.J.: Loss functions for discriminative training of energy-based models. In: R.G. Cowell, Z. Ghahramani (eds.) Proceedings of the Tenth International Workshop on Artificial Intelligence and Statistics, AISTATS 2005, Bridgetown, Barbados, 6–8 January 2005. Society for Artificial Intelligence and Statistics (2005). http://www.gatsby.ucl.ac.uk/aistats/fullpapers/207.pdf
41. Lerman, L., Bontempi, G., Markowitch, O.: Power analysis attack: an approach based on machine learning. IJACT **3**(2), 97–115 (2014). https://doi.org/10.1504/IJACT.2014.062722
42. Lerman, L., Medeiros, S.F., Bontempi, G., Markowitch, O.: A machine learning approach against a masked AES. In: Friedman, J., Hastie, T., Tibshirani, R. (eds.) The Elements of Statistical Learning. Springer Series in Statistics, vol. 1, pp. 61–75. Springer, New York (2014). https://doi.org/10.1007/978-3-319-08302-5_5
43. 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: S. Mangard, A.Y. Poschmann (eds.) Constructive Side-Channel Analysis and Secure Design-6th International Workshop, COSADE 2015, Berlin, Germany, 13–14 April 2015. Revised Selected Papers, Lecture Notes in Computer Science, vol. 9064, pp. 20–33. Springer, Berlin (2015). https://doi.org/10.1007/978-3-319-21476-4_2
44. Maghrebi, H., Portigliatti, T., Prouff, E.: Breaking cryptographic implementations using deep learning techniques. In: C. Carlet, M.A. Hasan, V. Saraswat (eds.) Security, Privacy, and Applied Cryptography Engineering-6th International Conference, SPACE 2016, Hyderabad, India, 14–18 December 2016. Proceedings, Lec-

ture Notes in Computer Science, vol. 10076, pp. 3–26. Springer, Berlin (2016). https://doi.org/10.1007/978-3-319-49445-6_1
45. Mangard, S., Pramstaller, N., Oswald, E.: Successfully attacking masked AES hardware implementations. In: Rao, J., Sunar, B. (eds.) Cryptographic Hardware and Embedded Systems-CHES 2005. Lecture Notes in Computer Science, vol. 3659, pp. 157–171. Springer, Berlin (2005)
46. Martinasek, Z., Dzurenda, P., Malina, L.: Profiling power analysis attack based on MLP in DPA contest V4.2. In: 39th International Conference on Telecommunications and Signal Processing, TSP 2016, Vienna, Austria, 27–29 June 2016, pp. 223–226. IEEE (2016). https://doi.org/10.1109/TSP.2016.7760865
47. Martinasek, Z., Hajny, J., Malina, L.: Optimization of power analysis using neural network. In: Francillon, A., Rohatgi, P. (eds.) Smart Card Research and Advanced Applications-12th International Conference, CARDIS 2013, Berlin, Germany, 27–29 November 2013. Revised Selected Papers, Lecture Notes in Computer Science, vol. 8419, pp. 94–107. Springer, Berlin. https://doi.org/10.1007/978-3-319-08302-5_7
48. Martinasek, Z., Malina, L., Trasy, K.: Profiling power analysis attack based on multi-layer perceptron network. Comput. Probl. Sci. Eng. **343**, 317 (2015)
49. McAllester, D.A., Hazan, T., Keshet, J.: Direct loss minimization for structured prediction. In: J.D. Lafferty, C.K.I. Williams, J. Shawe-Taylor, R.S. Zemel, A. Culotta (eds.) Advances in Neural Information Processing Systems 23: 24th Annual Conference on Neural Information Processing Systems 2010. Proceedings of a Meeting Held 6–9 December 2010, Vancouver, British Columbia, Canada, pp. 1594–1602. Curran Associates, Inc., Red Hook (2010). http://papers.nips.cc/paper/4069-direct-loss-minimization-for-structured-prediction
50. Messerges, T.: Using second-order power analysis to attack DPA resistant software. In: Koç, Ç., Paar, C. (eds.) Cryptographic Hardware and Embedded Systems-CHES 2000. Lecture Notes in Computer Science, vol. 1965, pp. 238–251. Springer, Berlin (2000)
51. Nair, V., Hinton, G.E.: Rectified linear units improve restricted Boltzmann machines. In: Fürnkranz, J., Joachims, T. (eds.) Proceedings of the 27th International Conference on Machine Learning (ICML-10), 21–24 June 2010, Haifa, Israel, pp. 807–814. Omnipress, Madison (2010)
52. O'Flynn, C., Chen, Z.D.: Chipwhisperer: An open-source platform for hardware embedded security research. In: E. Prouff (ed.) Constructive Side-Channel Analysis and Secure Design-5th International Workshop, COSADE 2014, Paris, France, 13–15 April 2014. Revised Selected Papers, Lecture Notes in Computer Science, vol. 8622, pp. 243–260. Springer, Berlin (2014). https://doi.org/10.1007/978-3-319-10175-0_17
53. Pearson, K.: On lines and planes of closest fit to systems of points in space. Philos. Mag. **2**(11), 559–572(1901)
54. Picek, S., Samiotis, I.P., Heuser, A., Kim, J., Bhasin, S., Legay, A.: On the Performance of Deep Learning for Side-channel Analysis. IACR Cryptology. ePrint Archive **2018**, 004 (2018). http://eprint.iacr.org/2018/004
55. Prouff, E., Rivain, M.: A generic method for secure SBox implementation. In: Kim, S., Yung, M., Lee, H.W. (eds.) WISA. Lecture Notes in Computer Science, vol. 4867, pp. 227–244. Springer, Berlin (2008)
56. Rokach, L., Maimon, O.: Data Mining with Decision Trees: Theroy and Applications. World Scientific Publishing Co., Inc, River Edge (2008)
57. Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S., Huang, Z., Karpathy, A., Khosla, A., Bernstein, M., et al.: Imagenet large scale visual recognition challenge. Int. J. Comput. Vis. **115**(3), 211–252 (2015)
58. Schindler, W.: Advanced stochastic methods in side channel analysis on block ciphers in the presence of masking. J. Math. Cryptol. **2**, 291–310 (2008)
59. Schindler, W., Lemke, K., Paar, C.: A Stochastic model for differential side channel cryptanalysis. In: Rao, J., Sunar, B. (eds.) Cryptographic Hardware and Embedded Systems–CHES 2005. Lecture Notes in Computer Science, vol. 3659. Springer, Berlin (2005)
60. Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition (2014). arXiv preprint arXiv:1409.1556
61. Song, Y., Schwing, A.G., Zemel, R.S., Urtasun, R.: Direct loss minimization for training deep neural nets. CoRR (2015). arXiv:1511.06411
62. Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., Erhan, D., Vanhoucke, V., Rabinovich, A.: Going deeper with convolutions. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1–9 (2015)
63. Szegedy, C., Vanhoucke, V., Ioffe, S., Shlens, J., Wojna, Z.: Rethinking the inception architecture for computer vision. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 2818–2826 (2016)
64. Weston, J., Watkins, C.: Multi-class support vector machines. Technical Report CSD-TR-98-04, Royal Holloway, University of London (1998)
65. Zeiler, M.D., Fergus, R.: Visualizing and understanding convolutional networks. In: European Conference on Computer Vision, pp. 818–833. Springer (2014)