Contents lists available at ScienceDirect

Integration, the VLSI Journal

journal homepage: www.elsevier.com/locate/vlsi

Design-time exploration of voltage switching against power analysis attacks in 14 nm FinFET technology

Johann Knechtel [a,*], Tarek Ashraf [b,1], Natascha Fernengel [c], Satwik Patnaik [d,2], Mohammed Nabeel [a], Mohammed Ashraf [a], Ozgur Sinanoglu [a], Hussam Amrouch [e,1]

[a] Division of Engineering, NYU Abu Dhabi, PO Box 129188, Abu Dhabi, United Arab Emirates
[b] University of Stuttgart, Stuttgart 70174, Germany
[c] Department of Computer Science, Karlsruhe Institute of Technology, Karlsruhe 76131, Germany
[d] Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX, 77843, USA
[e] Chair of Semiconductor Test and Reliability (STAR) in the Computer Science, Electrical Engineering Faculty, University of Stuttgart, Stuttgart 70174, Germany

ARTICLE INFO

Keywords:
14 nm finFET
Library characterization
Power side-channel attack
Correlation power analysis
AES
Voltage switching
Design-time exploration
CAD flow

ABSTRACT

Given their non-invasiveness and demonstrated effectiveness, power analysis attacks (PAAs) are concerning and to be accounted for in modern circuit design. That is especially relevant for technology-dependent verification of PAA countermeasure implementations. Prior art proposed various countermeasures against PAAs, including masking and hiding, voltage switching, noise injection, etc. Aside from the proven working principles of such countermeasures, it is important to understand that their effectiveness is primarily technology- and implementation-dependent. Hence, before deployment, especially for integrated circuits, such countermeasures require accurate circuit-level studies.

This work investigates an industrial-grade 14 nm fin field-effect transistor (FinFET) technology at design-time in the context of PAAs. We leverage device-level measurement data from *Intel* high-volume manufacturing processes, build up accordingly well-characterized standard-cell libraries, and utilize a commercial-grade computer-aided design (CAD) flow for PAA evaluation at design-time. Our study is focused on (1) the effectiveness of voltage switching as a countermeasure, (2) the advanced encryption standard (AES) cipher as a representative circuit, and (3) the correlation power analysis (CPA) as an attack framework. We show that, to improve the resilience against the CPA attack in particular and to lower information leakage in general, specific voltage configurations are more promising than others for the 14 nm FinFET technology.

1. Introduction

To protect any sensitive data handled within integrated circuits (ICs), the use of ciphers is widely adopted, which are formally secure algorithms for encryption/decryption of data. Still, once attackers have direct access to ICs, they can monitor the physical interactions with the environment which are inevitably occurring for hardware. These interactions, also known as side-channel information leakage, can be exploited to, e.g., infer the secret key used for ciphers; related activities are known as side-channel attacks.

In this work, we focus on *power analysis attacks (PAAs)*, where attackers measure power traces and assess the underlying relationship to the cipher operations conducted within the hardware under attack. Among other side-channel attacks, PAAs are particularly concerning, owing to their non-invasiveness, low-cost implementation, and proven effectiveness [1]. Different versions of PAAs have been demonstrated, like the simple power analysis, the differential power analysis (DPA) [2], the correlation power analysis (CPA) [1], or the mutual information analysis [3]. Without loss of generality, we focus on the widely adopted, seminal CPA attack in this work.

* Corresponding author.
E-mail addresses: johann@nyu.edu (J. Knechtel), st180774@stud.uni-stuttgart.de (T. Ashraf), natascha.fernengel@student.kit.edu (N. Fernengel), satwik.patnaik@tamu.edu (S. Patnaik), mtn2@nyu.edu (M. Nabeel), ma199@nyu.edu (M. Ashraf), ozgursin@nyu.edu (O. Sinanoglu), amrouch@iti.uni-stuttgart.de (H. Amrouch).
URLs: https://wp.nyu.edu/johann/ (J. Knechtel), https://nyuad.nyu.edu/dfxlab (O. Sinanoglu), https://www.iti.uni-stuttgart.de/en/chairs/star (H. Amrouch).

[1] The work was done in part at Karlsruhe Institute of Technology, Germany.
[2] The work was done in part at NYU Abu Dhabi, UAE.

Various countermeasures against PAAs have been proposed and evaluated in a large body of prior art, including masking and hiding [4–6], voltage switching [7–10], noise injection [11,12], etc. Essentially, these countermeasures seek to de-correlate the observable power consumption from the sensitive cipher operations, to hinder PAAs. More specifically, masking and hiding re-organize the design such that sensitive operations are decomposed/split at the functional level as well as the circuit level, aiming for notions of formal security. However, the implementation of such schemes is expensive, as overheads are scaling quadratically with the related security requirements, making efficient implementations challenging [13]. Voltage switching can be supported via integrated voltage regulators (IVRs) [7]. IVRs are commonly employed in modern IC designs, as they can enable significant power savings. However, the efforts for IC verification as well as the need for system-level synchronization during switching periods represent some challenges when employing IVRs. Noise-injection schemes like doubling the registers and interposing random data into the paths [11], while effective in practice, also incur considerable area and power cost. Without loss of generality, we focus on voltage switching in this work.

Aside from the fact that the working principles of these various countermeasures have been thoroughly studied before, it is important to understand that their effectiveness is largely dependent on the used technology and the hardware implementation. Therefore, we argue that any countermeasure, especially before deployment in high-volume IC manufacturing, would require a circuit-level evaluation that must be based on accurate technology models along with commercial tool support. We note that some prior art, e.g., [5,6], relied on field-programmable gate array (FPGA) implementations for evaluation, which is not suitable to assess the resilience of an IC implementation, as there are fundamental differences in the hardware architectures of FPGAs and ICs. We also note that some prior art, e.g., [8], uses SPICE simulations for power analysis, which is limited to small circuits, due to considerable computational efforts.

This manuscript is not aiming to counter such or other prior art, but rather to contributes to the landscape as follows.

- We derive a well-calibrated model for an industrial-grade 14 nm FinFET technology from *Intel* quality production. This step is based on actual measurement data set and commercial tools, and the model matching is confirmed.
- We implement a CAD flow, also based on commercial tools, which allows for accurate and efficient design-time power analysis. This CAD flow is integrated with an open-source CPA attack, which we extend for a thorough exploration of the sampling space.
- Leveraging this integrated CAD and CPA framework, we investigate, without loss of generality, the security promises of voltage switching in detail for an AES circuitry implemented in an industrial-grade 14 nm FinFET technology. We derive related, practical guidelines for any security-concerned designer.

The scope of our work is also illustrated in Fig. 1. The manuscript is structured as follows. In Section 2, we describe our approach to model an industrial-grade 14 nm FinFET technology from *Intel* quality production. In Section 3, we describe our commercial-tools-based CAD flow, which allows for design-time power analysis and thorough CPA attack runs for security evaluation. In Section 4, we present our experimental study, where we investigate the security promises of voltage switching in detail for an AES circuitry. We derive practical guidelines for any security-concerned designer using such industrial-grade 14 nm FinFET technology. Finally, in Section 5, we conclude.

2. Modeling and calibrating for a commercial 14 nm FinFET technology

To accurately model the FinFET technology, it is essential to perform calibrations with some existing commercial technology offered by the semiconductor industry. To achieve that, we employ the available

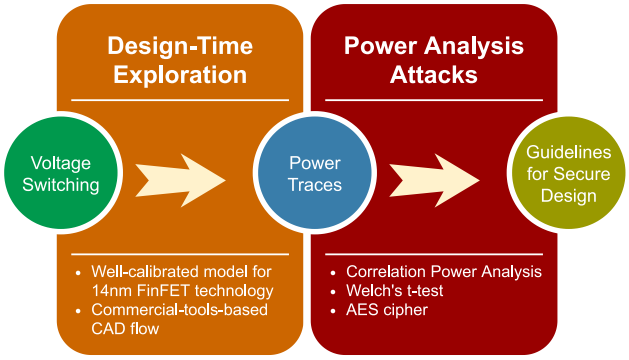

Fig. 1. The scope of this work is to study voltage switching as a countermeasure against PAAs, specifically for an industrial-grade 14 nm FinFET technology, and to derive conservative guidelines for secure design. This is achieved through design-time exploration of an exemplary AES circuitry, using a well-calibrated technology model within our integrated CAD flow. Since the data obtained from our flow is free of noise (unlike for attacks on devices in the field), we can provide conservative and well-founded security assessments.

measurement data from state-of-the-art *Intel* 14 nm FinFET technology obtained from a high-volume production-quality manufacturing process [14].

First, we use *Synopsys Sentaurus Process Technology CAD* [15], a commercial TCAD tool, to mimic the fabrication process of 14 nm FinFET using the same materials properties, layer dimensions, doping profile, etc. Then, we carefully tune key parameters in the FinFET device such as source/drain doping, sub-fin doping, source–drain series resistance, gate-metal work function, low-field mobility parameters, and high-field saturation parameters.

Next, we calibrate the industry-standard compact model for the FinFET technology, *BSIM-CMG* [16,17], using the *Intel* measurement data and additional data obtained from the previously calibrated TCAD transistor devices. The additional data contains, for instance, the electrical properties of transistors at various temperature and voltage biases. The calibrations are performed for both n-type and p-type FinFET devices and the output of this step is fully-calibrated transistor models that accurately match and reproduce the measurement data of the 14 nm *Intel* FinFET technology.

Finally, we perform TCAD mixed-mode simulations to further validate our calibrated transistor models (SBIM-CMG). In this validation phase, we compare the TCAD results of an inverter and ring oscillator circuits against the results of SPICE simulations. This step ensures to us that parasitics effects are accounted for in the calibration. Further details on the validation and calibration process are also available in [16].

In Fig. 2, we summarize our technology calibration. In Fig. 3, we demonstrate how SPICE simulations, using our calibrated FinFET model, reproduce *Intel* measurement data for both n-type and p-type FinFET devices. More specifically, in Fig. 3(a), we show the transfer characteristics represented by transistor drain current (I_{DS}) versus gate voltage (V_{GS}), and in Fig. 3(b), we show output characteristics represented by transistor drain current (I_{DS}) versus drain voltage (V_{DS}). In both cases, for both n-type and p-type transistors, the results from our calibrated FinFET models match very well the original 14 nm FinFET measurement data from *Intel* [14].

Having well-calibrated transistor models enables us to characterize standard-cell libraries that can be used within any design flow. To this end, we employ the open-source SPICE netlists for FinFET standard cells from *Silvaco* [18]. Using a commercial tool flow for standard-cell library characterization based on *Synopsys SiliconSmart* [19], we create the 14 nm FinFET library by employing our calibrated FinFET models. For every standard cell within the library, we consider 7 × 7 cases for

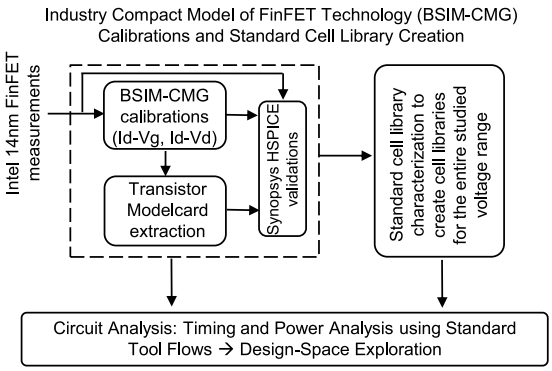

Fig. 2. The calibration process starts with the industry compact model of FinFET technology (BSIM-CMG), using measurement data from the production-quality Intel 14 nm node. The calibrated transistor models are then employed within standard tool flows for standard-cell library calibration. The calibration is performed at various operating voltages. Our libraries are fully compatible with the existing CAD tool flows.

input signal slews and output load capacitance, similar to what is done in existing commercial cell libraries.

To capture the impact of voltage scaling accurately, we repeat the library characterization for an entire voltage range from 0.8 V down to 0.3 V with 50 mV and 100 mV step sizes. All the created 14 nm FinFET standard-cell libraries for the varying voltages are fully compatible with existing CAD tool flows. Hence, we can directly use them, without any modifications, to perform accurate timing analysis and power analysis. For this work, we employ these libraries within our CAD flow to investigate the resiliency of AES against PAAs attacks under the effects of voltage scaling.

3. Integrated CAD and CPA framework

Next, we explain our integrated CAD and CPA framework that allows to evaluate ciphers (or any other circuitry module, for that matter) against PAAs (Fig. 4). The fundamentals of the framework are derived from [20].

We note that some prior art leverages similar principles, e.g., see [21,22]. However, an important distinction of ours from such prior art is the randomized-but-reproducible exploration of the power-distribution sampling space (not illustrated in Fig. 4, but explained in detail further below). This is essential for a fair and thorough assessment of any technology, circuitry, or system feature against PAAs. We demonstrate our framework for the seminal AES cipher and voltage switching in this work; however, our framework is not limited to those.

It is important to note that our notion of resilience is *not* based on any de-synchronization effects induced by voltage switching. While an attacker would have to handle these effects during measurements required for real-world attacks, here we instead evaluate the foundation of voltage switching, namely mixing of different power distributions, and the resulting role for resilience against PAAs.

Our framework requires the register-transfer level (RTL) description of the cipher and the standard-cell libraries of choice as inputs. After the successful termination of the framework, the user gets to know the minimum number of power traces needed to disclose the secret key. In general, a larger number of traces indicates that the underlying cipher RTL has a higher resilience against the launched attack. We explain the two major components of our integrated framework next.

3.1. Simulation-based power analysis

Initially, we synthesize the cipher RTL using the technology libraries of choice. We verify the functionality of the gate-level netlist using a Verilog testbench with user-defined sets of plaintexts and keys. We also confirm the functionality of the design using software simulation.

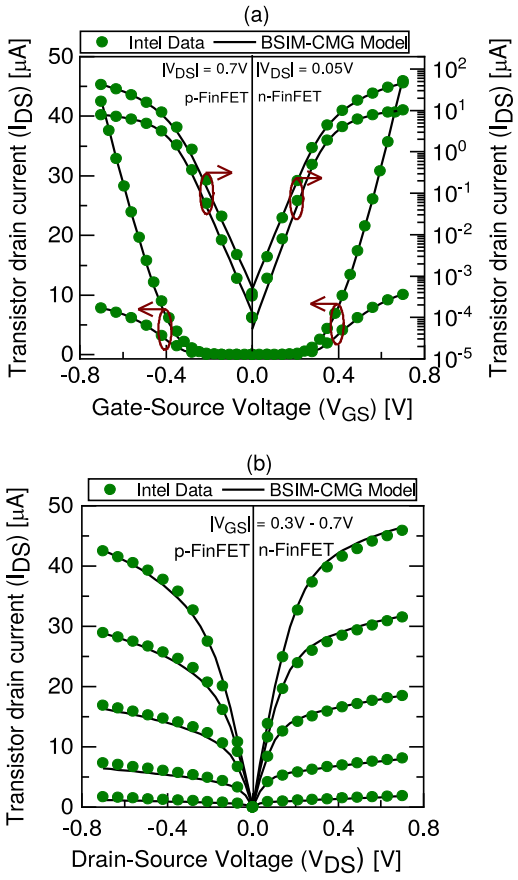

Fig. 3. 14 nm FinFET technology calibration for both n-type and p-type transistors. (a) and (b) demonstrate the excellent matching between our calibrated FinFET models and *Intel* 14 nm FinFET measurement data from both transfer and output characteristics, respectively, [16].

Next, we perform a gate-level simulation (GLS) and generate a Value Change Dump (VCD) file. This VCD file captures every node's switching activity for a user-defined time resolution (e.g., 1 ps). The VCD file is then used for power simulation of the synthesized gate-level netlist. To reduce computational efforts for power analysis without comprising the efficacy of PAAs, we can consider only the relevant time intervals, i.e., the last round of AES, which is known to be vulnerable [1].

Instead of performing full-scale timing simulations, which would also capture glitching activities, we leverage zero-delay simulations here. For such, all signal transitions occur simultaneously at the clock's active edge, which also simplifies the extraction of peak power values. As explained further below, we are indeed only interested in the switching power of specific registers, which occurs at the clock's active edge. Our power analysis can be considered conservative from a security standpoint since we ignore glitching noises, which naturally deteriorate any PAA. Depending on the countermeasure of interest, glitches may still have to be considered, e.g., for masking-based countermeasures. However, for our notion of voltage switching, glitches are not relevant. Related implications are further discussed in Section 4.

In short, we obtain the design-time power traces for the AES RTL in a step-wise manner while processing the texts and secret keys, and we extract the zero-delay, peak-power values for the sensitive registers of the last-round AES operations [1].

3.2. Correlation power analysis

The correlation power analysis (CPA) [1] is an effective attack. At its heart, the *Pearson correlation coefficient (PCC)* is leveraged to measure

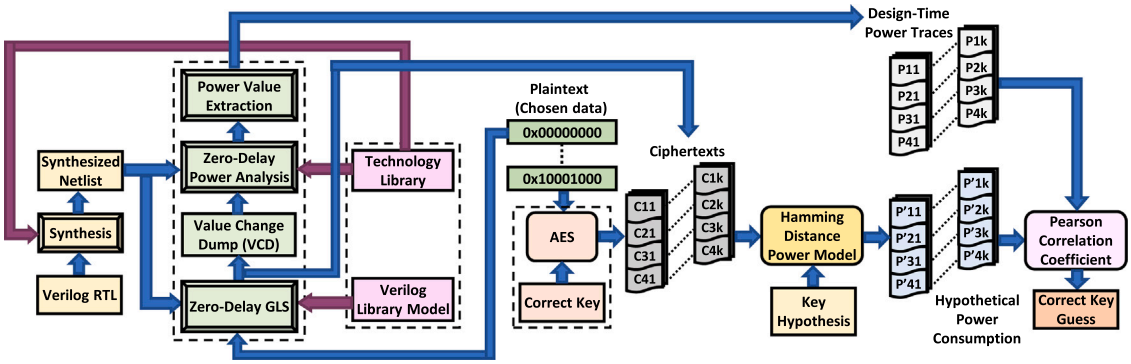

Fig. 4. Our integrated CAD and CPA framework. The left part illustrates the CAD stages, the center part illustrates the cipher/module under investigation (AES for this study), and the right part illustrates the CPA stages. The parts are intertwined as needed for design-time exploration against PAAs.

the relationship between predicted and actual power profiles [1]. In our framework, we follow a standard approach for the CPA, as detailed next.

First, we derive the predicted power profiles using a power model. Since registers consume a significant portion of dynamic power during signal transitions, considering the *Hamming distance (HD)* for the registers' output before and after switching is established as the *HD power model* [1]. This predictive modeling is repeated for all possible key candidates; the results are also known as *hypothetical power values* that are related to the respective key hypotheses. Note that we need to consider only the registers holding the intermediate texts for the vulnerable last-round operation to build up the HD power model [1]. Finally, the design-time the hypothetical power values are correlated via PCC, and the hypothesis with the highest PCC is thought to represent the correct key.

In other words, we stepwise correlate the following two assets: (a) the set of design-time power values arising from using the actual, secret key for the vulnerable AES operations, and (b) all the different sets comprising all possible hypothetical power values, which mimic the power consumption of the same AES operations for all possible key candidates. Note that all the sets in (b) have to be individually correlated with (a); there are as many correlation results as there are sets or key hypotheses in (b). Then, the set in (b) corresponding to the highest correlation score describes the hypothetical power values matching best with the actual power consumption of the AES operations using the secret key—the related key hypothesis is thus considered to be correct key.

Acting as designers, we can directly verify the key hypothesis. As an attacker, however, one would have to study the trend in correlation throughout multiple trials, and once a stable and significant trend for correlation appears, one deducts with certain confidence that the key hypothesis should be correct [1].

While conducting the above steps would be sufficient for an actual attack, for the exploration in this study, we have to conduct multiple trials while varying the secret key, the texts, the selection of power traces, and the voltages. Related details are given next, in Section 4.1.

4. Experimental investigation

4.1. Setup

4.1.1. Synthesis and simulations

We use *Synopsys VCS* for functional simulations at RTL and gate level, *Synopsys DC* for logic synthesis, and *Synopsys PrimeTime PX* for power simulations; all tool versions are from 2018.

For the AES circuit, we leverage a publicly available RTL, which works on 128-bit keys and texts, and uses look-up tables for the AES substitution box [23]. For synthesis and power simulations, we employ the 14 nm FinFET technology libraries described in Section 2. Without loss of generality, we use the operating frequency $f = 100$ MHz.

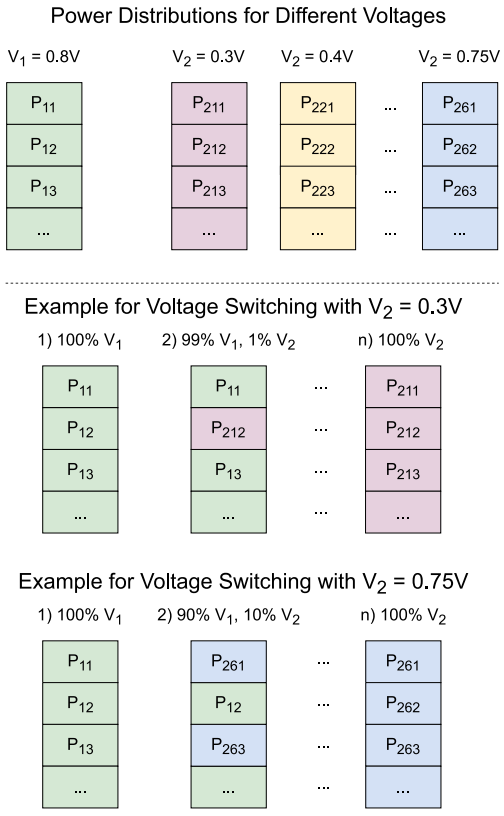

Fig. 5. Conceptional examples for voltage switching. Voltages V_{DD_1}, V_{DD_2} are labeled V_1, V_2 here for simplicity. Based on the individual power distributions obtained through simulation for different voltages, voltage switching at the system level is mimicked by mixing these power distributions. Note that voltage switching is realized stepwise and independently for the different, fixed pairs of V_1, V_2.

4.1.2. Voltage switching

To enable a thorough study on the impact of voltage switching, we carefully investigate switching using a broad range of voltage configurations. Our approach is outlined in Fig. 5, and we describe it in some detail next.

First, we apply different supply voltages for the whole AES circuit during independent runs for power simulations, after which we collect the corresponding power traces for each voltage and corresponding library separately (as outlined in Section 3–3.1). The considered voltages are: 0.8 V, 0.75 V, 0.7 V, 0.6 V, 0.5 V, 0.4 V, 0.3 V.

Now, we can study voltage switching for varying-sized sets of texts processed by the AES circuit. We stepwise consider the full spectrum of switching, i.e., we investigate all possible configurations ranging from

100% of the texts processed using V_{DD_1}, over, e.g., 99% processed using V_{DD_1} and 1% processed using V_{DD_2}, all the way to 100% processed using V_{DD_2}. Note that the granularity for switching is tuned according to our initial experiments—for voltage configurations with a large difference $|V_{DD_1} - V_{DD_2}|$, we found that employing very fine granularities (down to 0.1%) is required, whereas for smaller differences, coarser granularities suffice (e.g., 10%). Also note that, while observing the selected granularity, we do switch randomly, i.e., any number of consecutive texts may or may not be processed using the same voltage.

For simplicity, we always switch between 0.8 V and one other, fixed voltage, i.e., we consider pairings $\{V_{DD_1}, V_{DD_2}\}$ with $V_{DD_1} = 0.8V$ as common baseline voltage, where $V_{DD_2} \neq V_{DD_1}$. Since we keep V_{DD_2} fixed to one particular voltage for each set of experiments, we have to conduct independent runs for each set, across all the considered voltage configurations.

Note that, for each voltage configuration, we conduct three batches of randomized switching, and all reported results are accordingly averaged.

To mimic voltage switching at the system level, we mix the separately obtained power distributions, whereas some IVR circuitry would be leveraged in practice.

As indicated, our evaluation of resilience is *not* based on any desynchronization effects induced by voltage switching. While an attacker would have to handle these effects during measurements required for real-world attacks, here we rather evaluate the foundation of voltage switching, namely different power distributions, and their impact on resilience.

4.1.3. CPA attack

We leverage and extend the open-source C/C++ framework of [24]; we provide our version in [23]. All CPA runs are executed on a high-performance computing (HPC) facility, with 14-core *Intel* Broadwell processors (Xeon E5-2680) running at 2.4 GHz, and 4 GB RAM are guaranteed (by the Slurm HPC scheduler) for each CPA run.

We assume a classical threat model, i.e., the attacker can measure power traces at will and also understands which power values belong to which texts that are being processed. While the attacker understands that voltage switching is applied as a countermeasure, s/he does not know which particular text is processed using which voltage.[3] Furthermore, the attacker has only external physical access, but no invasive probing capabilities.

While our power traces are obtained at design-time and are thus void of any environmental noise (e.g., arising from the measurement equipment), the traces gathered by an attacker would be subjected to such noise. In other words, we are *not* taking the attacker's perspective here, but rather the designer's perspective, where we leverage the CPA attack to conduct a conservative and robust security evaluation at design-time.

Initially, we generate and store the following assets: six random, 128-bit keys; 5000 random, 128-bit plain-texts; and, separately for each key, the corresponding 5000 cipher-texts, also 128 bits long each. We keep these sets of keys and texts the same across the whole study, i.e., for all voltage configurations.

To guide the CPA attack exhaustively through the various sets of voltage-variable power traces, we apply the following sampling strategy.[4] We start with a small number of traces being selected from the larger overall set of traces collected, and we choose such small subsets

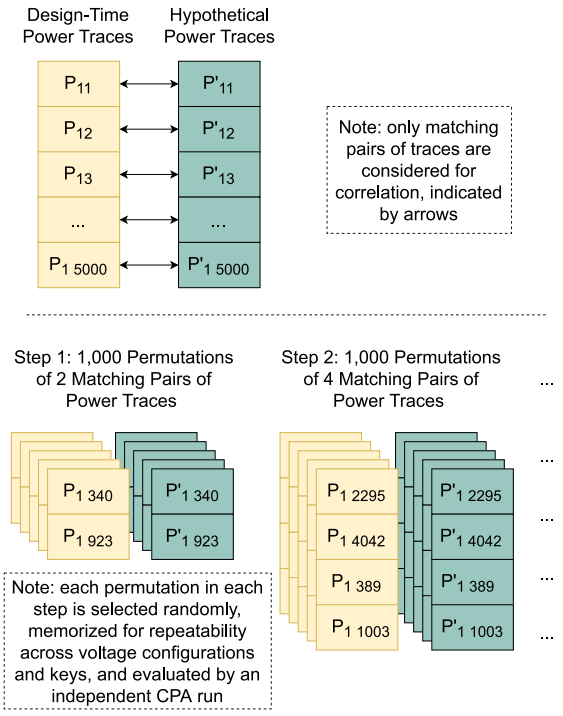

Fig. 6. All experiments utilize the outlined, thorough sampling of power traces, to determine the number of traces to disclosure with high confidence.

of traces multiple times, in order to conduct multiple, independent CPA runs. Then, we stepwise increase the number of traces being selected, and we repeat that procedure of selecting multiple subsets and conducting related CPA runs. By doing so, we explore different subsets with more and more traces being made available for the CPA attack. Such an approach is essential for a robust assessment of how many traces are needed to disclose a secret key.

The sampling approach is exemplified in Fig. 6. Throughout 2500 steps, we randomly pick for each step 1000 sets of matching pairs of design-time power values and hypothetical power values. Matching pairs mean that the power values arise from the same texts being processed, which is a prerequisite for PCC, or for any correlation for that matter.

Each of 2500 steps requires an independent, separate CPA run. As indicated, each step covers 1000 sets (through an independent CPA run), more specifically 1000 permutations of all 5000 available pairs of design-time and hypothetical power values, where each step $s + 1$ considers two more pairs per permutation over prior step s. In total, this results in 2,500,000 permutations being considered, step by step, through individual CPA runs on those subsets of power values. For a fair comparison, these permutations are all memorized, stored, and re-applied when conducting the CPA runs for different keys as well as for different voltage configurations.

In short, using the above strategy, we ensure (1) a thorough sampling of all power traces for robust inferences about how many traces are needed for key disclosures, and, more importantly, (2) that any differences observed in CPA resilience are *not* due to the outlined randomized nature of sampling, but rather indeed due to different voltage configurations (and different keys).

4.2. Results

4.2.1. Overview

The goal of this work is to investigate the resilience offered by voltage switching in an industrial-grade 14 nm FinFET technology.

[3] To uphold this assumption, it is essential that the voltage configurations cannot be trivially differentiated, i.e., the power distributions arising from using the different voltages must be sufficiently interspersed. This holds true for all the configurations considered in this study, as long as the ratio of switching is accordingly tuned. See Section 4.2.2 for more details.

[4] This strategy is conducted separately for each configuration of voltage switching—voltage switching and sampling of power traces are independent procedures of our framework.

Table 1
Results for baseline voltage $V_{DD_1} = 0.8$ V.

Key	#TTD(99.9%)	μ(P)	σ(P)	CV(P)
1	1008	1.868E−03	5.15E−05	2.77%
2	920	1.870E−03	5.40E−05	2.88%
3	874	1.873E−03	5.26E−05	2.80%
4	856	1.824E−03	5.43E−05	2.98%
5	970	1.881E−03	5.21E−05	2.76%
6	1032	1.862E−03	5.31E−05	2.85%
μ(#TTD)	943	–	–	–
σ(#TTD)	71.74	–	–	–
CV(#TTD)	7.61%	–	–	–

From this study, security-concerned designers can obtain guidance for proper implementation of voltage switching as a countermeasure against PAAs in general and the seminal CPA attack in particular.

The main observations from the empirical study are as follows. First, the larger the difference $|V_{DD_1} - V_{DD_2}|$, the less we need to switch from the baseline voltage V_{DD_1} to V_{DD_2} in order to raise the resilience against the CPA attack to a specific, comparable level. Second, the larger the difference, however, the larger the information leakage in terms of Welch's t-test scores.

The first observation is because of the fact that, for a larger difference of voltages, the difference in power consumption is significantly larger as well, given that $P \propto (\alpha \times C \times V_{DD}^2 \times f)$.[5] The resulting pronounced variances for power values hinder the effectiveness of the PCC formalism underlying of the CPA attack, suggesting to leverage largely different voltages to advance security.

The second, more important observation, however, suggests that the voltage difference should be limited. This is because for overly large differences, there is information leakage arising for the largely varying power values. While the seminal CPA attack is not leveraging this kind of information leakage—on the contrary, the CPA attack is rather hindered by the less clear correlations of voltage-variable power values with AES operations—more advanced attacks, e.g., based on machine learning, might leverage this leakage. Note that the second observation also relates to the assumption that an attacker cannot trivially differentiate the power distributions. This assumption only holds true for limited voltage differences where the resulting power distributions remain sufficiently interspersed.

In short, there are trade-offs for voltage switching which necessitate such an empirical study during design-time, in particular before application of voltage switching in production. Next, we discuss our findings in more detail.

4.2.2. Detailed results and discussion

In Table 1, we report the results considering only the baseline voltage $V_{DD_1} = 0.8V$. The main metric here, as well as in the remaining experiments, is *number of traces to disclosure (#TTD)*, which we report with a confidence of 99.9%. Recall that we leverage 1000 permutations per step during our sampling approach; these 1000 permutations, evaluated through individual CPA runs each, correspond to the 1000 runs required for the 99.9% confidence on assessing #TTD.

We further report the (rounded) mean and standard deviation for #TTD, which describe the variations induced by different keys. However, note that we focus on the mean #TTD in the remainder; key-induced variations are not of particular interest here.[6] In any case, we point out the following: (1) these differences observed across keys establish themselves as relatively consistent trends across all experiments; (2) our observations are interpreted considering mean values. Thus, our findings on voltage switching are not undermined in any way by key-induced variations.

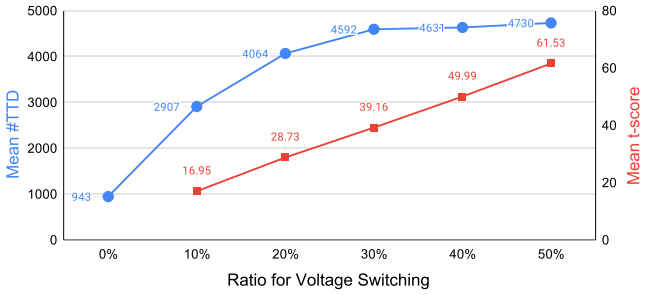

Fig. 7. Mean #TTD and mean t-scores versus the ratio for voltage switching, with $V_{DD_1} = 0.8V, V_{DD_2} = 0.75V$. The more we switch, the more resilient the circuit becomes against the CPA attack, but also the more information leakage is arising from the power values corresponding to different voltages.

We also report the mean μ(P), the standard deviation σ(P), and the coefficient of variation CV(P) for the underlying power values; these metrics serve to characterize the distribution of the power values. The coefficient of variation $CV = \sigma/\mu$ puts the variability of a distribution into its proper context, i.e., the mean value. The CV values in Table 1 are put into context further below.

In Table 2, we report the results when voltage switching is applied. As indicated, we consider a large range of voltages V_{DD_2} to switch to.

The first finding is that all considered voltage configurations can help to increase the resilience against the CPA attack by $\approx 5\times$ over the baseline resilience (Table 1). The mean ratio of how much we have to switch is essentially dictated by the targeted-at mean #TTD $\approx$ 5000, which we utilize for all configurations to enable a fair comparison. That is, different configurations require different degrees of switching to achieve a specific, comparable resilience against the CPA attack; the smaller the difference between the two voltages, the more switching is required.

The second finding is that for any voltage configuration, switching more would generally increase the resilience, albeit also introducing more information leakage. We have also studied this aspect for $V_{DD_2} = 0.75$ V in more detail, with the related results illustrated in Fig. 7.

Toward the third finding, we note the following two aspects: (1) the mean PCC between the randomly (but reproducibly) selected power values from the individual distributions associated with the two different voltages is relatively low; (2) the mean CV for the combined distribution of the selected power values (which is the only one observable by an actual attacker) is relatively large, i.e., compared to the CV values for the baseline configuration (Table 1), but still sufficiently low to maintain the interspersed nature of the underlying power distributions.

These aspects serve to explain the increased resilience against the CPA attack—correlating hypothetical power values, which exhibit relatively low correlation to begin with, with the more varied power

[5] The switching activities α are dictated by the AES keys and texts processed, as captured through *Synopsys VCS* in our flow. Given that the same keys and texts are processed, the activities are also the same.

[6] For more context on key-induced variations, note the following. Recall that our experiments are tailored for a fair and thorough comparison and, as such, for these experiments considering different keys, we ensure that the very same (but initially randomized) texts are leveraged for all experiments. Thus, the resulting differences in #TTD are due to varying distributions of bit-level flips across the last-round texts, which can impact the effectiveness of the CPA attack by definition. Still, we caution that such findings should *not* motivate to favor specific, seemingly "resilient keys" for actual applications—such outcomes are highly dependent on the architecture, RTL, and gate-level implementation of the cipher, as well as the selection of plain-/cipher-texts. There are studies investigating the role of keys and texts more formally, e.g., based on notions of collision and statistical modeling [25], which are out of scope for this work.

Table 2
Results for voltage switching with $V_{DD_1} = 0.8$ V.

	Mean ratio	#TTD			Combined power distribution			Individual power distributions	
V_{DD_2}	V_{DD_2}/V_{DD_1}	μ	σ	CV	Mean μ	Mean σ	Mean CV	Mean PCC	Mean t-score
0.3 V	1.05%	4984	38.22	0.77%	1.813E−03	1.75E−04	9.46%	0.2993	659.54
0.4 V	1.42%	4953	73.43	1.48%	1.843E−03	1.79E−04	9.71%	0.2937	562.62
0.5 V	2.03%	4920	135.02	2.74%	1.839E−03	1.77E−04	9.63%	0.3060	462.23
0.6 V	3.52%	4927	111.58	2.26%	1.833E−03	1.70E−04	9.27%	0.3138	345.79
0.7 V	11.50%	4939	49.73	1.01%	1.808E−03	1.63E−04	9.01%	0.3213	22.95
0.75 V	50.00%	4730	116.31	3.52%	1.736E−03	1.37E−04	7.86%	0.3600	61.53

The "Combined Power Distribution" refers to the actual distribution after voltage switching is applied, whereas the "Individual Power Distributions" refer to the individual distributions obtained for the respective voltages.

distributions resulting from voltage switching is more difficult by definition.

The role of these aspects on the resilience against the CPA attack can also be quantified, namely via the Spearman correlation, which is defined as the PCC between the rank variables. Unlike the PCC itself, that can only assess linear relationships (which is sufficient for correlating actual power values and hypothetical power values within the CPA framework), the Spearman correlation is more generic as it can assess any monotonic relationship. For example, the Spearman correlation between #TTD and PCC is −0.8162, representing a strong reciprocal correlation; this confirms that more traces are needed for less correlated power distributions. Furthermore, the Spearman correlation between #TTD and CV is 0.7532, representing a strong correlation as well; this confirms that more traces are needed for more varied power distributions.

As explained, the resilience against the CPA attack is increasing the more we switch and the larger the voltage difference is. For such cases, however, information leakage is often increasing as well, as evident from Welch's t-test scores in both Table 2 and Fig. 7. Note that Welch's t-test can assess whether there is information leakage at all, which may be exploited by some attacks, but it does not provide any insight on success rates of actual attacks.[7]

Thus, from a formal point of view, possibly seeking resilience going beyond the CPA attack, we would rather want to employ small voltage differences and small switching ratios. Indeed, an outstanding t-score minima is observed for $V_{DD_2} = 0.7$ V, where the voltage difference is still sufficiently small while the switching ratio is already considerably relaxed/reduced compared to the case of $V_{DD_2} = 0.75$ V (where 4.35× more switching was required for comparable CPA resilience). Importantly, although such a setting impacts the resilience against the CPA attack in general, it does *not* undermine the resilience against a specific level of attack effort (i.e., #TTD). This is especially true once a slightly increased switching ratio is considered again.

Thus, we have investigated this most promising scenario further, by considering more frequent switching. Indeed, already from 12% switching onward, the CPA attack always failed to infer the correct key even when provided all 5000 traces (across all the different keys).

This constitutes another, fourth finding, namely that this specific configuration is most promising for voltage switching as a countermeasure within the considered 14 nm FinFET technology, both from an empirical and a formal perspective.

Finally, it is important to recall that this study is based on zero-delay power simulations using commercial tools. Therefore, our results are void of any noise. Moreover, aside from empirical data based on CPA attack runs, we provide formal insights based on Welch's t-test. This implies two considerations as follows. First, for actual attacks in the field—assuming the same operation conditions—an attacker cannot do any better than what we observe. Accordingly, our findings serve well as accurate but conservative guidelines, e.g., for tailoring schemes like dynamic key management [27]. Second, for actual voltage switching in the field, our findings and guidelines may be over-constrained, i.e., once noise or other detrimental effects play out, a less stringent switching than what we consider here may offer the same level of resilience in practice. Most, if not all, IVR circuitry can be configured at run-time as needed, allowing to later on reduce such overheads arising for over-constrained switching requirements.

[7] It is said that, for a t-score below 4.5, the circuit is leakage-free and thus cannot be attacked by PAAs [26]. Accordingly, our reported results are *not* for leakage-free scenarios, which is also clearly demonstrated by the fact that the related CPA attack runs are, on average, successful.

5. Conclusion

In this work, we have investigated the resilience of an industrial 14 nm FinFET technology against power analysis attacks. We have leveraged device-level measurement data from manufacturing cycles, built up correspondingly well-characterized standard-cell libraries for different supply voltages, and utilized a commercial-grade CAD flow for power and attack evaluation at design-time.

Without loss of generality, our study is focused on voltage switching for an AES circuit and its resilience against the seminal CPA attack. We have shown that there are trade-offs for voltage switching, which clearly necessitate such an empirical study. More specifically, the resilience against the CPA attack is increasing the more we switch as well as the larger the difference is for the voltages being switched between, but the information leakage is often increasing at the same time. The specific configuration $V_{DD_1} = 0.8$ V, $V_{DD_2} = 0.7$ V was found to be a "sweet spot" that is most promising from both formal and empirical perspective. Randomly switching more than 12% of the AES operations to V_{DD_2} was hindering CPA attacks altogether.

While specific to the AES circuit implemented using the 14 nm FinFET technology, these findings are robust and conservative. The former is because we carefully conduct batches of randomized-but-reproducible CPA runs, to explore the whole sample space of power traces in a comprehensive manner. The latter is because the findings are based on technology-accurate, design-time data obtained from zero-delay power simulations. Furthermore, we consider the AES circuit as stand-alone module, without any potential side-effects of other modules' activities undermining our analysis. Assuming the same operation conditions, an attacker in the field cannot do any better than what we observe here. Accordingly, our findings serve well as practical guidelines for secure design or for system-level design/configuration parameters, e.g., key refresh rates.

CRediT authorship contribution statement

Johann Knechtel: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration. **Tarek Ashraf:** Methodology, Software, Validation, Formal analysis, Investigation, Data curation, Visualization. **Natascha Fernengel:** Methodology, Software, Validation, Formal analysis, Investigation, Data curation, Visualization. **Satwik Patnaik:** Conceptualization, Methodology, Software, Validation, Investigation, Data curation, Writing – original draft. **Mohammed Nabeel:** Conceptualization, Methodology, Software, Validation, Investigation, Data curation. **Mohammed**

Ashraf: Conceptualization, Methodology, Software, Validation, Investigation, Data curation. **Ozgur Sinanoglu:** Conceptualization, Resources, Writing – original draft, Supervision, Funding acquisition. **Hussam Amrouch:** Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported in part by the Center for Cyber Security (CCS) at New York University Abu Dhabi (NYUAD) and in part by the German Research Foundation (DFG), project "ACCROSS: Approximate Computing aCROss the System Stack" and in part by the Office of Naval Research under Grant N00014-18-1-2672. Parts of this work were carried out on the High Performance Computing facility at NYUAD. The work of S. Patnaik at NYUAD was supported by the Global Ph.D. Fellowship of NYU New York and NYUAD.

References

[1] E. Brier, C. Clavier, F. Olivier, Correlation power analysis with a leakage model, Proc. Cryptogr. Hardw. Embed. Sys. 1 (2004) 6–29, http://dx.doi.org/10.1007/978-3-540-28632-5_2.

[2] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, Proc. Adv. Cryptol. 38 (1999) 8–397.

[3] B. Gierlichs, L. Batina, P. Tuyls, B. Preneel, Mutual information analysis, Proc. Cryptogr. Hardw. Embed. Sys. 42 (2008) 6–442.

[4] X. Li, C. Yang, J. Ma, Y. Liu, S. Yin, Energy-efficient side-channel attack countermeasure with awareness and hybrid configuration based on it, Trans. VLSI Syst. 25 (2017) 3355–3368, http://dx.doi.org/10.1109/TVLSI.2017.2752212.

[5] T. Moos, A. Moradi, T. Schneider, F.X. Standaert, Glitch-resistant masking revisited, Trans. Cryptogr. Hardw. Embed. Sys. 2019 (2019) 256–292, http://dx.doi.org/10.13154/tches.v2019.i2.256-292.

[6] S. Takemoto, Y. Nozaki, M. Yoshikawa, Evaluation of the hiding-countermeasure prince using differential power analysis, in: Proc. Conf. Cons. Electr., Vol. 16, 2019, pp. 4–0165.

[7] M. Kar, A. Singh, S.K. Mathew, A. Rajan, V. De, S. Mukhopadhyay, Reducing power side-channel information leakage of AES engines using fully integrated inductive voltage regulator, J. Sol.-St. Circ. 53 (2018) 2399–2414.

[8] F. Zhang, B. Yang, B. Yang, Y. Zhang, S. Bhasin, K. Ren, Fluctuating power logic: SCA protection by V_{DD} randomization at the cell-level, in: Proc. Asian Hardw.-Orient. Sec. Trust Symp, 2019, pp. 1–6.

[9] S. Yang, P. Gupta, M. Wolf, D. Serpanos, V. Narayanan, Y. Xie, Power analysis attack resistance engineering by dynamic voltage and frequency scaling, Trans. Embed. Comput. Syst. (2012) 11, http://dx.doi.org/10.1145/2345770.2345774.

[10] R.P. Pothukuchi, S.Y. Pothukuchi, P.G. Voulgaris, J. Torrellas, Maya: falsifying power sidechannels with operating system support, 2019, CoRR abs/1907.09440 http://arxiv.org/abs/1907.09440[arXiv:1907.09440].

[11] D. Bellizia, S. Bongiovanni, P. Monsurrò, G. Scotti, A. Trifiletti, F.B. Trotta, Secure double rate registers as an RTL countermeasure against power analysis attacks, Trans. VLSI Syst. 26 (2018) 1368–1376, http://dx.doi.org/10.1109/TVLSI.2018.2816914.

[12] D. Das, S. Maity, S.B. Nasir, S. Ghosh, A. Raychowdhury, S. Sen, ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity, Trans. Circ. Sys. 65 (2018) 3300–3311.

[13] H. Gross, S. Mangard, T. Korak, An efficient side-channel protected AES implementation with arbitrary protection order, in: H. Handschuh (Ed.), Topics in Cryptology – CT-RSA 2017, 2017, pp. 95–112.

[14] S. Natarajan, M. Agostinelli, S. Akbar, M. Bost, A. Bowonder, V. Chikarmane, S. Chouksey, A. Dasgupta, K. Fischer, Q. Fu, T. Ghani, M. Giles, S. Govindaraju, R. Grover, W. Han, D. Hanken, E. Haralson, M. Haran, M. Heckscher, R. Heussner, P. Jain, R. James, R. Jhaveri, I. Jin, H. Kam, E. Karl, C. Kenyon, M. Liu, Y. Luo, R. Mehandru, S. Morarka, L. Neiberg, P. Packan, A. Paliwal, C. Parker, P. Patel, R. Patel, C. Pelto, L. Pipes, P. Plekhanov, M. Prince, S. Rajamani, J. Sandford, B. Sell, S. Sivakumar, P. Smith, B. Song, K. Tone, T. Troeger, J. Wiedemer, M. Yang, K. Zhang, A 14 nm logic technology featuring 2nd-generation finfet, air-gapped interconnects, self-aligned double patterning and a 0.0588 μm^2 SRAM cell size, in: Proc. Int. Elec. Devices Meeting, 2014, pp. 3.7.1–3.7.3.

[15] Synopsys, Synopsys technology computer aided design (TCAD), 2020b, https://www.synopsys.com/silicon/tcad.html.

[16] S. Mishra, H. Amrouch, J. Joe, C.K. Dabhi, K. Thakor, Y.S. Chauhan, J. Henkel, S. Mahapatra, A simulation study of NBTI impact on 14-nm node finfet technology for logic applications: Device degradation to circuit-level interaction, Trans. Electron. Dev. 66 (2019) 271–278.

[17] BSIM. Group, BSIM-CMG model, 2020, http://bsim.berkeley.edu/models/bsimcmg.

[18] Silvaco, Si2, Open-source FinFET standard cell library, 2019, https://silvaco.com/news/silvaco-and-si2-release-unique-free-15nm-open-source-digital-cell-library/.

[19] Synopsys, Standard cell library characterization, 2020a, https://www.synopsys.com/implementation-and-signoff/signoff/siliconsmart.html.

[20] J. Knechtel, S. Patnaik, M. Nabeel, M. Ashraf, Y.S. Chauhan, J. Henkel, O. Sinanoglu, H. Amrouch, Power side-channel attacks in negative capacitance transistor, IEEE Micro. 40 (2020) 74–84, http://dx.doi.org/10.1109/MM.2020.3005883.

[21] S. Bhasin, J.L. Danger, T. Graba, Y. Mathieu, D. Fujimoto, M. Nagata, Physical security evaluation at an early design-phase: A side-channel aware simulation methodology, in: Proc. ES4CPS, 2013, pp. 13–20, http://dx.doi.org/10.1145/2589650.2559628.

[22] D. Šijačić, J. Balasch, B. Yang, S. Ghosh, I. Verbauwhede, Towards efficient and automated side-channel evaluations at design time, J. Crypt. Eng. 10 (2020) 305–319, http://dx.doi.org/10.1007/s13389-020-00233-8.

[23] J. Knechtel, Correlation power attack, 2019–2020, https://github.com/DfX-NYUAD/CPA extended from [7] as retrieved in March 2019.

[24] Y. Fei, et al., Side channel analysis library, 2013, https://tescase.coe.neu.edu/?current_page=SOURCE_CODEsoftware=aestool.

[25] Y. Fei, A. Ding, J. Lao, L. Zhang, A statistics-based success rate model for DPA and CPA, J. Cryptogr. Eng. 5 (2015) 227–243.

[26] T. Schneider, A. Moradi, Leakage assessment methodology - a clear roadmap for side-channel evaluations, 2015, https://eprint.iacr.org/2015/207.

[27] M. Taha, P. Schaumont, Key updating for leakage resiliency with application to AES modes of operation, Trans. Inf. Forens. Sec. 10 (2014) 519–528.