Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Fully-Digital Randomization Based Side-Channel Security — Towards Ultra-Low Cost-per-Security

RINAT BREUER[1], FRANÇOIS-XAVIER STANDAERT[2], AND ITAMAR LEVI[1], (Member, IEEE).
[1]Faculty of Engineering, Bar-Ilan University, Ramat Gan, Israel (e-mail: {rinat.breuer, itamar.levi}@biu.ac.il, respectively)
[2]Université catholique de Louvain, ICTEAM/ELEN/Crypto Group, Belgium (e-mail: fstandae@uclouvain.be)

Corresponding author: Itamar Levi (e-mail: itamar.levi@biu.ac.il).

This research was supported in part by Israel Science Foundation (ISF) grant number 2569/21.

ABSTRACT In this paper we formulate and re-evaluate a recently proposed randomization-based side-channel protection mechanism. The strength of the construction lies with its ability to comply with standard digital design flows and that it provides a security parameter which directly links side-channel security metrics. A detailed leakage model is provided and investigated for the first time, and it is linked to electronic parameters of the randomization mechanism. We develop guidelines and optimization for concrete ASIC constructions, and sheds light on this ultra low-cost leakage-randomization mechanism. The proposed circuit is natural to be utilized without or on top of the popular masking countermeasures. It is demonstrated to be considerably more efficient in terms of attack data-complexity as compared to low-order masking (i.e., number of shares $d = 2$). In addition, seemingly it is a nice and necessary fit to increase the noise when a too low-noise environment is expected, which impedes masking's theoretical security. Finally, it is discussed that the proposed mechanism is natural to be embedded with masked designs for higher security-levels ($d > 2$) while lowering significantly their asymptotically quadratic area price-tag as d increase. Robustness results are provided along with post place & route cost estimations for both AES encryption and a more recently proposed permutation such as ISAP. Our design efficiently provides unprecedented three orders-of-magnitude signal-to-noise reduction with a total area-overhead of 21% and 46% for AES and Ascon-ρ, respectively. These factors are more cost-efficient than low-orders masked designs and such mechanisms are sometimes necessary when the inherent noise is not sufficient. However, the joint embedding of the proposed mechanism with masked designs potentially exponentially improve the security level they provide, all whilst enabling electronic-design friendly security mechanism.

INDEX TERMS Countermeasures, Hiding, Localization, Low-Cost, Masking, Power-Gating, Randomization circuits, Side-Channel Analysis, Security Order

I. INTRODUCTION

SIDE-channels analysis (SCA) attacks enable distinguishing internal secret values manipulated by the hardware, exploiting secret dependent internal computations which affect some physically measurable quantities, denoted by leakage. Such attacks have repeatedly underpinned the sensitivity of implemented cryptographic schemes. With this motivation, the National Institute of Standardization and Technology (NIST) competitions for future symmetric-key, e.g., Authenticated-Encryption [1] and public-key Post-Quantum schemes [2], consider SCA security as important factors. To date, various successful single leakage-trace SCA attacks were shown possible for public-key encryption/ digital signatures schemes, both on hardware and software implementations (see e.g., [3]–[5]).

Side-channel protection by masking countermeasures bare asymptotic quadratic cost factors with the desired security-level or #number of shares (d) dominated by vector-multiplications [6]–[11]. Masking implementations are also quite expensive and complicated due to randomness handling (refreshes) and their amount (generation) [11], [12]. However, considering all inherent masking assumptions take place, theoretically the masking approach provides exponential security with "only" polynomial-cost (quadratic) as d

increase. An important added value for embedding circuitry randomization mechanism, such as the ones promoted in this manuscript, is that in many cases the inherent level of noise required to comply with masking's statistical security bounds is insufficient. For example, we can consider the evaluation in [13] showing insufficient software implementations security levels which impedes fulfilling masking full potential. This implies that some underlying noise-embedding mechanism is a must for even standard edge/IoT devices which manifest a rather low noise-level. This is one of the motivations which highlights our goal: *designing an ultra low-cost leakage randomization mechanism which is electronic design automation friendly.*

Side-channel protection by noise addition is traditionally considered not-sufficient to provide *efficient* side-channel security. Moreover, such mechanisms are hard to link with concrete security parameters and metrics. Naively assuming that physical noise is linearly expensive with the security level, i.e., noise is assumed to be proportional to area utilization in conventional micro-electronics[1]. The last challenge of noise addition mechanisms is that non-conventional noise addition solutions are hard to embed within standard design-flows or require special IPs even if efficient [15]–[18].

In [19], [20] it has been demonstrated first, that it is possible to embed noise-generation on power lines with ultra-low electronic cost, utilizing standard electronic design tools and second, that such mechanisms can be added independently to very localized blocks, i.e., independently randomizing the leakage stemming from internal variables manipulation of small number of bits. Our previously proposed technique is based on localized embedding of randomizers which inflict uniform distribution of the side-channel leakage. These tiny randomizers were implemented utilizing standard power-gates (PGs) with a unique sizing methodology which is a reminiscence of Binary Weighted Resistor DAC (Digital to Analog Converter). The relative cost of the countermeasure is very low, especially for small values of the security parameter (number of PGs). Therefore, it was discussed as a perfect match to emulate noise in order to then amplify it with countermeasures which are exponential with the noise-level, i.e., masking. By doing so the overall cost can be significantly reduced owing to smaller masking *orders*.

In this paper we contribute in the following aspects: (1) we discuss how by smart PGs sizing tactics, relatively to the inherent loads of the circuit, it is possible to reduce the cost of such countermeasures and make them more secure, making them even more attractive, with or without masking on-top. (2) the paper elaborates on how to optimize and set parameters for the countermeasure giving a concrete security target, and (3) how to formally argue the achieved security level and perform security analysis. Finally, we provide a leakage model and support it with simulated ASIC measurements while connecting cryptographic SCA-security metrics, and projecting so advanced permutations such as Ascon-ρ (also utilized by ISAP).

The highlight achievements of the mechanism is that it enables concrete security levels: (e.g.,) three orders-of-magnitude signal-to-noise reduction with a total area-overhead of 21% and 46% for AES and Ascon-ρ, respectively. But more importantly, this security level is parametric for the security-architect use, as discussed below. Theoretically, these factors are more cost-efficient than any low-orders masked designs which can not achieve such security levels for example in cases the inherent noise is not sufficient. We underline that this is achieved whilst enabling electronic-design friendly security mechanism and no IP-based design nor digital-flow unsupported steps. Finally, the joint embedding of the proposed mechanism with masked designs potentially exponentially improve the security level they provide, as they are can randomize in the masked "share"-level.

Noteworthy, our results follow physical evidence from a complex 65nm ASIC chip in [20]. However, in this manuscript we provide analysis on the correct utilization of the technique supported by a model and an in depth analysis of the security it provides.

Paper organization. The manuscript starts with a short background discussion including a general-perspective and some necessary reminders in Section II. In Subsection II-A we provide a model for the randomizer's influence on the leakage, supported by general cost estimation, security optimization while discussing security tradeoffs. In Section III we follow with a more detailed security-tradeoffs evaluation while utilizing the SNR and the leakage distribution as the main tools for evaluation. The modeling effort and optimization is followed in Section IV with extracted ASIC transient/noise simulation data which enables evaluation of the concrete security of the mechanism, and a more concrete evaluation of the design parameters needed to achieve maximum security. Finally in Section VII the main conclusions are listed along with directions for future-work.

II. BACKGROUND

Side-channel protection pose a significant challenge for hardware designers. It is a topic of vast research interest within the Circuits and Systems (CAS) society, reflecting basic limitations of available design-techniques and circuits for hardware-security aspects. It also reflects an inherent challenge for cryptographic designs and primitives seeded by parameters from the electronics. Typically, the needed parameters (noise, composability, leakage-distribution and leakages independence), are: (1) very slow to estimate by device-level simulations/noise-simulations and hard to argue otherwise (2) security-metrics are not automated/supported by Electronic Design Automation (EDA) flows. Therefore, a vast interest is observed in security communities in general and needs/requirements are already set by standardization organizations such as common-criteria [21], NIST/FIPS [22], ISO/IEC 15408, ISO/IEC 17825 and BSI. However, regu-

[1] A similar argument holds for algorithmic-noise [14]

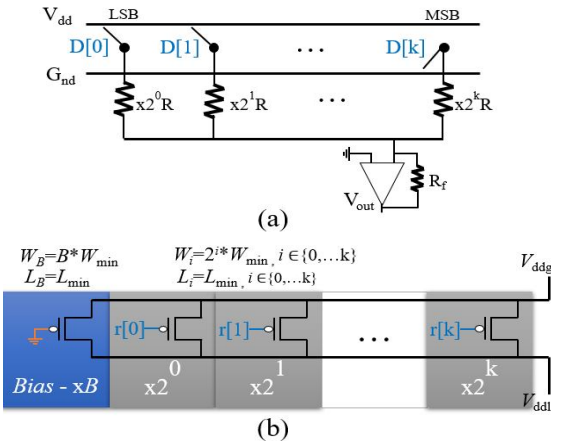


FIGURE 1: (a) BWR-DAC (b) PG based randomizer.

lations are changing slower than appearance of attacks and typically, some of the standards allow rather low-level of assurance and security in the context of (e.g.,) side-channel attacks [23].

Side-channel leakages encompass information related to internal computations within the hardware. Relating to leakage randomization mechanisms, it is understood that the desired modulated leakage should distribute uniformly to provide maximum entropy. Otherwise stated, "stretching" the inherent noise by utilizing randomization mechanisms, which in-turn reduces the effective Signal-to-Noise ratio (SNR) observed by an adversary. The main trade-offs are clearly area and energy cost.

SCA literature is packed by either (1) randomization mechanisms which are not natively standard for EDA-flows (e.g., [16]–[18]), (2) randomization mechanisms which are not provided with a parametric security level (e.g., [15]–[18]), and (3) naive logical-randomization by duplication of logic or PRNGs.

In [20] a randomization mechanism supported by a security-parameter from the physical implementation was proposed. Similarly to a security parameter such as the number of key bits from cryptography theory, the level of leakage randomization (or number of randomizer states which affect the uniformity of the leakage distribution and its variance) are parametrized with a very area/energy efficient methodology. It enables setting this parameter to match an SCA-security need as a function of circuitry parameters by designers (e.g. inherent resistances and loads of a technology). In [20] standard metrics were utilized to evaluate the SCA-security of a leaky cryptographic primitive. Namely the cryptographic SNR [24] and the Mutual-Information (MI) [25]–[29]. To keep the discussions in this manuscript simple, without the loss of generality, and the analysis comprehensive we stick with one metric, namely the SNR which is faster to compute and easily linked/comparable with prior-art.

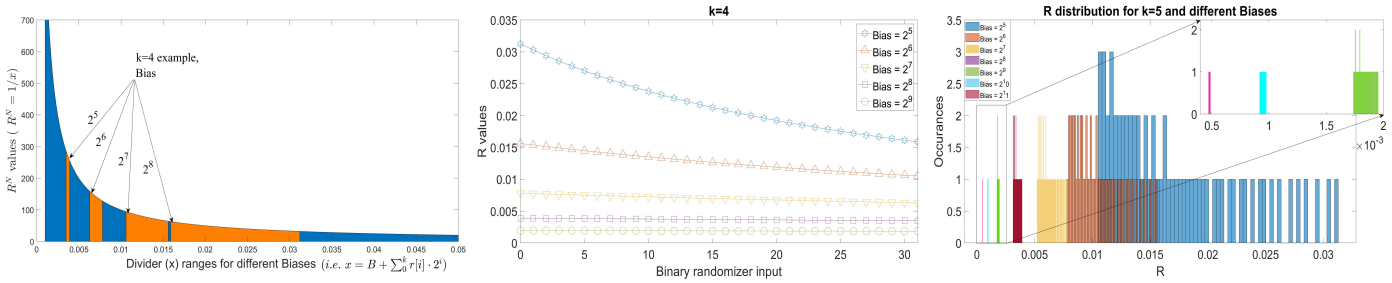
A. MODEL - SECURITY AND COST

The low-cost local randomizer demonstrated in [20] is a reminiscence and adaptation of the conventional device sizing in a Binary Weighted Resistor DAC (BWR-DAC); as schematically illustrated in Fig. 1a. Within this topology the $k+1$ random input bits of the randomizer, D, are weighting a $\{V_{dd}, G_{nd}\}$ connection per bit of a parallel resistors bank. The size of each of the resistors is proportional to a base-2 power series. Such weights distribute the output voltage uniformly across the full rail-to-rail voltage span. As illustrated in Fig. 1b, the proposed randomizer has its main similarity in the base-2 power series sizing of the $k+1$ Power-Gates in the bank. For keeping the discussion simple we set the transistors channel length to L_{min} while their width is increasing with $W_i = 2^i \cdot W_{min}$. The global and local power-lines, V_{ddg} and V_{ddl} are connected at both ends of the bank. The transistors, controlled by random input bits, r, modulate the effective resistance of the network. Perhaps the main difference within our construction is the existence of another parallel connected $Bias$ device. This difference is significant as discussed in what follow. In order to assure a safe-guard maximal resistance and to prevent power-starvation of the local logical-blocks supplied, the $Bias$ (B) always-on is therefore connected in parallel to the bank, illustrated with a blue background shading. The minimal and maximal effective resistance of this construction and their normalized equivalents (denoted by N) are:

$$\begin{aligned} R_{max} &= \frac{\rho L_{min}}{B} \;\; ; \;\; R_{min} = \frac{\rho L_{min}}{B + S_k} \\ R^N_{max} &= \frac{1}{B} \;\; ; \;\; R^N_{min} = \frac{1}{B + S_k} \end{aligned} \tag{1}$$

with $S_k = \sum_{i=0}^{k} 2^i = 2^{k+1} - 1 \approx 2^{k+1}$ and ρ being the device sheet resistance. The total area-utilization of the construction is proportional to $B + S_k$, i.e., exponential with the number of levels or the number of random input bits of the construction.

We begin with a mathematical model of the mechanism's resistance. Considering Fig. 2b, the normalized resistance values of the construction for all $r[k = 4 : 0]$ bits states is shown for different $Bias$ values $\in \{2^5, ..., 2^9\}$. Clearly, when the $Bias$ is small, the resistances, drawn from $1/(Bias + \sum_{i=0}^{k} r[i] \cdot 2^i)$, will take values not uniformly spread, as can be captured from the $Bias = 2^5$ curve. The larger the $Bias$ would the values be taken from the more linear section of a $1/(\alpha + x)$ curve, as shown for larger $Bias$es curves (and illustrated in Fig. 2a). Setting the $Bias$ value correctly enables a designer to control the distribution and set it to approximate a discrete uniform. Considering Fig. 2a, a side-effect is that as the $Bias$ size increase, the span of the effective resistance values (R on the Y axis) decrease, and so does the randomization variance. Fig. 2c shows the histograms of the modeled effective normalized resistance for a $k = 5$ scenario for several different $Bias$es. It is possible to see that as the $Bias$ increase in dimensions, the distribution becomes more uniform with this exemplary mathematical



(a) (b) (c)

FIGURE 2: Modeled behaviour: (a) R^N ranges for different $Bias$es (b) R values for all randomizer states, and (c) R distribution for different $Bias$es.

model. The zoomed-in subplot shows that $Bias = 2^7 = 2 \cdot S_k$ or $Bias = 4 \cdot S_k$ is quite sufficient to achieve a quasi uniform distribution.

Assuming a designer is correctly utilizing the mechanism, i.e., samples are drawn from the quasi-uniform region, we can evaluate the (ideal) leakage model distribution parameters. Next, we relate to the distribution of the leakage, in a general case regardless of the manipulated data, i.e., leakage variance due to the randomizer alone:

The modeled distribution is that of a finite Gaussian mixture, i.e., $f(x;\mu_0,...\mu_{2^{k+1}};\sigma_0,...\sigma_{2^{k+1}}) = \sum_{i=0}^{2^{k+1}} w_i \cdot \varphi_i(x,\mu_i,\sigma_i)$, $w_i \geq 0$, where $\sum_i w_i = 1$ and $\varphi_i(x,\mu_i,\sigma_i) = n(x,\mu_i,\sigma_i)$. For simplicity, let's assume that $\forall i,\ \sigma_i = \sigma$, let's further assume $w_i = 1/(2^{k+1}+1)$ (uniform random input assumption) and that $\mu_i = a + \frac{b-a}{2^{k+1}+1} \cdot i$ (i.e, BWR structure generates a uniform quantization of the span), then naturally:

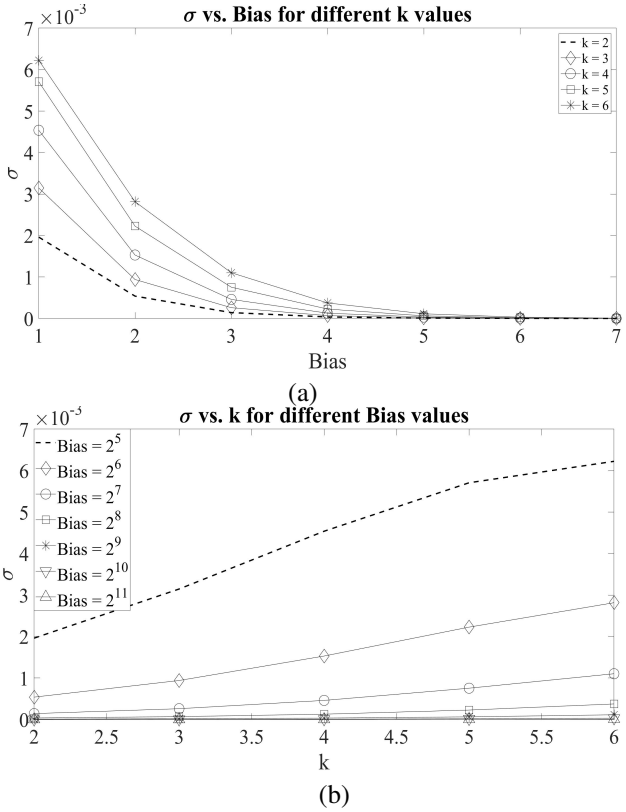
$$\mathsf{E}[f(x)] = \mu_{tot} = \sum_{i=0}^{2^{k+1}} w_i \cdot \mu_i = (b+a)/2 \qquad (2)$$

where b and a represent R_{min} and R_{max} from above. For the variance we can write,

$$\mathsf{V}[(f(x)] = \mathsf{E}[(f(x)-\mu)^2] = \sigma_{tot}^2 = (\sum_{i=0}^{2^{k+1}} w_i(\mu_i+\sigma_i)) - \mu \qquad (3)$$

where if assuming that $\forall i,\ \sigma_i \geq \mu_i$, we get the trivial but important relation $\sigma_{tot}^2 \approx (2^k)^2$, i.e., an exponential relation between σ_{tot} and k. Or, alternatively put, σ_{tot} is roughly proportional to $(R_{max} - R_{min})$. However, as discussed next such an ideal distribution is hard to get in practice due to physical limitations, and for relevant parameters span we roughly achieve a linear to low-order polynomial relation between σ_{tot} and k. E.g., in the device-level simulation section below (Section IV), a second-degree polynomial relation is observed approximately.

More generally, the developed model also corresponds to a leakage distribution with some manipulated data, The effective resistance from the power-supply, V_{ddg}, to ground of a logic block is the serial summation of the randomizer and the logic block resistance, $R + R_{logic}$. Assuming



(a)

(b)

FIGURE 3: Leakage std: (a) vs. $Bias$ size (b) vs. k. σ here denotes the total standard-deviation (σ_{tot}).

the logic block resistance is proportional to the Hamming Weight (HW), and that additive noise exist, we can write $R + \alpha \cdot \mathrm{HW}(data) + \mathcal{N}$. The leakage (i.e., current) will be proportional to this resistance owing to the constant and stable global voltage V_{ddg}.

For simplicity we can assume that $data$ manipulation changes only the mean of the leakage distribution. That is, $\Pr[l|data,r] = f(l;\mu_r + \alpha \cdot \mathrm{HW}(data),\sigma_i)$, where r denotes the randomizer's state $\in \{0..2^k-1\}$ and σ_i, reflects noise factors independent from the randomizer.

In order to evaluate the security-level provided by the mechanism, it is possible to compute and evaluate the

standard-deviation (σ_i) of the samples. Fig. 3a shows the effective (total) standard-deviation, σ_{tot}, versus the $Bias$ dimensions for different k values simulated in Matlab. Constants were set with standard values derived from circuit simulations, i.e., α and R values and Gaussian noise with SNR=10^{-2}. As discussed above in our more tentative explanation: for a set k value, increasing the $Bias$ reduces the computed σ_{tot}. However, the more interesting observation relates to Fig. 3b where on each curve we set a different $Bias$ and plot σ_{tot} versus k. As expected, the security-level of the mechanism increases with k increase. However, in order for our uniform-distribution assumption to approximately hold we demand that $Bias \geq 2S_k$, with this exemplary set of model parameters. Nevertheless, we do note that for practical scenarios, parameters values and sizes, and for cases of combining this protection mechanism with other approaches (such as masking), k is a very effective security-parameter as small values are required.

III. LEAKAGE MODELING AND SNR EVALUATION

We continue in this subsection with leakage modeling and computing a more 'standard' cryptographic SCA metric, the SNR [20], [24]. The SNR evaluates the univariate security level and it is a good and sound estimator in the statistical sense especially when the noise in the leakage is Gaussian. In our case the total noise is a modulation of a Gaussian noise over a discrete uniform distribution (i.e., a Mixture). The SNR which is a metric commonly used for security evaluation is still an indicative estimator for the security in our case. Moreover, a nice property of the SNR is that it directly indicates the level of informativeness in the leakage and closely connected to attack Success Rate and (e.g.,) correlation based attacks, CPA, [30], [31]. This is as opposed to detection-based approaches, such as T-test based, which only distinguish whether some information exist in a *specific* of a *random* scenario, regardless of its exploitation (various discussions appear in [32]–[34]). Therefore, this was the metric of choice here without the loss of generality regarding the results.

In this section we model the Hamming Weight leakages of an 8-bit secret variable, we follow by modulating these leakages by the effective resistance which is the outcome of the BWR-sizing based randomizer (Fig. 1b). All simulations are performed with a sample set of 10^7 leakages and in each leakage-cycle the k-bits of the randomizer $\in \{2, \dots 6\}$ are drawn uniformly at random. The noise level of the inherent physical noise, i.e., σ_i $\forall i$, takes a reasonable range of $\{10^{-3}, \dots 10^{1}\}$[2]. For all scenarios the Bias was set to 2^{k+2} so as to abide an approximately uniform resistance distribution from above.

Fig. 4 shows the resulting SNR. All x- and y-axis in the figures are in log-scale. Fig. 4a illustrates the achievable SNR versus k for different noise-levels and Fig. 4b plots

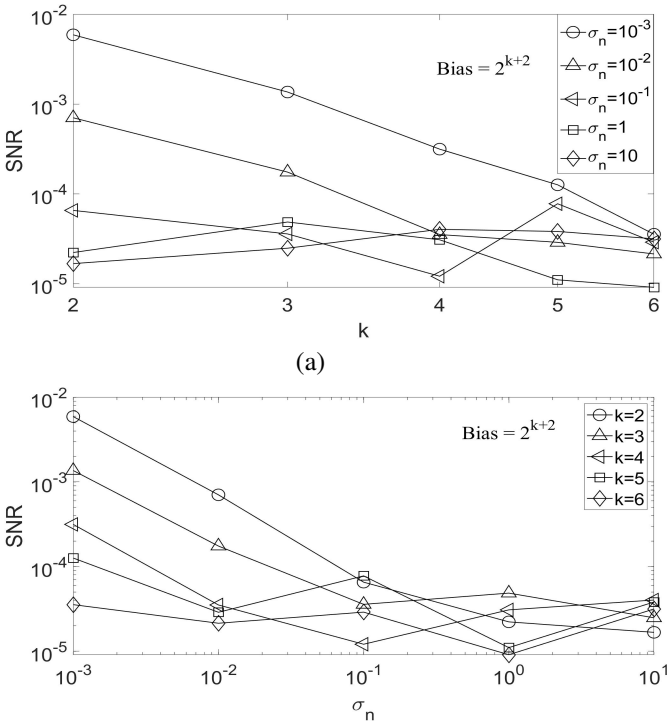


FIGURE 4: SNR: (a) vs. k (b) vs. σ_n.

the SNR versus the noise-level for different k-values. As shown, for a given noise-level, the security increases linearly in a log-log scale with the security parameter. Clearly, it is more easy to capture this behaviour with small k-values. However, for large inherent noise level it saturates as the sample-set of 10^7 traces is not enough and, as explained above, the span of the distribution saturates. In addition, considering Fig. 4b, especially for low block-inherent noise-level, σ_n the randomizer affect is very significant, reducing the SNR from 10^{-2} with $k = 2$ (low level of added security) to $0.5 \cdot 10^{-5}$ with only $k = 6$. These parameters (k = 2 to 6) in terms of implementation cost are quite negligible for practical scenarios as discussed and demonstrated on a secured full AES test-chip in 65nm [20]; they occupy less than 25% of the total area.

IV. SIMULATED ASIC-MODEL CORRESPONDENCE

In this section we follow with linking the mathematical model and the modeled security parameter to a model derived from an industrial Process Design-Kit PDK simulation environment. Our evaluation environment is seeded by physical extracted parameters, we next relate to Fig. 5a. We investigate here a 65nm PDK devices with a Power-Management Kit (PMK) supporting the PGs required. We start with a k = 4 scenario (i.e., 5 parallel PGs) with power-grid resistance and capacitance (R_{ext}, C_{ext}) and internal power-delivery network capacitance of V_{ddl} (C_{int}) evaluated post-extraction from the physical block, as illustrated on the figure. The underlying logic (Logic) protected is a simple 4-bit Present

[2]for simplicity denoted on figures by σ_n to highlight it is the inherent noise component

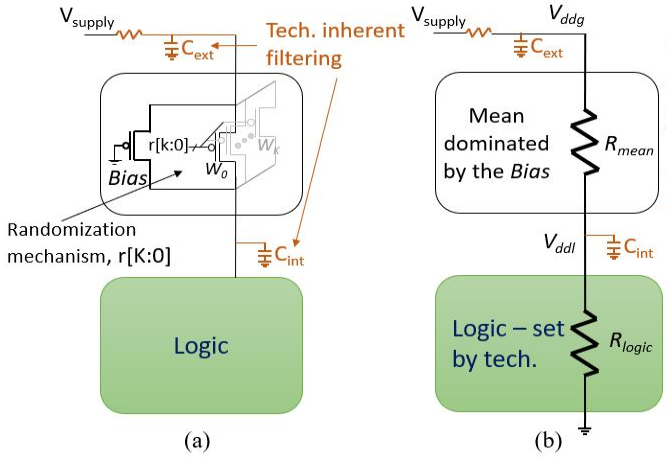


FIGURE 5: Schematic illustration: (a) with parasitic elements (b) with internal dominating effective resistances.

algorithm synthesized Sbox (results can be easily generalized to other Sboxes). The entire Logic block also incorporates input and output registers, another Sbox at the output reflecting a physical-load and key-addition at the inputs.

Considering Fig. 5b in this evaluation environment the Logic load (both resistive and capacitive) are technological parameters which are generally set by the technology provider. We denote by R_{logic} the *on* resistance of the logical block in a given state. We further relate to the mean resistance of the randomization mechanism (R_{mean}). This latter parameter is dominated by the $Bias$ device.

Before we follow with experimental results we list several conflicting effects which are induced due to a reduction in R_{mean}, i.e., increase $Bias$ size:

- ***Negative***: It increases the average signal or alternatively increases the voltage drop (ΔV) over R_{logic}. This in turn increases the exploitable signal.
- ***Negative***: It reduces the total randomized leakage variance as discussed in the previous section.
- ***Positive***: It increase the leakage uniformity as discussed in the previous section.
- ***Positive***: A physical/ technological effect is that it increases both C_{int} and C_{ext} and therefore increases filtering effects which generally lowers the exploitable signal.

Referring to Fig. 6a, we have performed a transient/transient noise simulation of the aforementioned circuitry. The clock frequency was set to 500MHz (following Cadence Genus Synthesis). The figure shows the local voltage (V_{ddl}) span where the nominal is 1.2V on the left (blue) y-axis. The global current, driven through the mechanism to the main power supply (V_{ddg}) is also showed on each of the plots corresponding with the right y-axis (orange), spanning around $200uA$. Withing the entire operation throughout time, the randomizer state (r[4:0]) was swept through all possible states (i.e., denoted on the lower part of the figure by the increasing vectors from '00000' to '11111'). In each state of the randomizer, 100 internal clock-cycles i.e., Sbox operations take place, where the variable y represent the 4 bit output of the circuitry vary. From top to bottom on the figure, the plots correspond to cases where a group of {0, 2, 4, 5} power-gates are assigned with fresh randomness every six clock-cycles or $12ns$, meaning Randomness-Throughput (RT) is 5bits/$12ns$. On the top plot where all transistors are open, it is clear that the leakages vs. time seams consistent (randomization is not on). In this case the voltage drop is minimal. As we progress and utilize more randomization bits, going down in the plots tiling, the maximal voltage

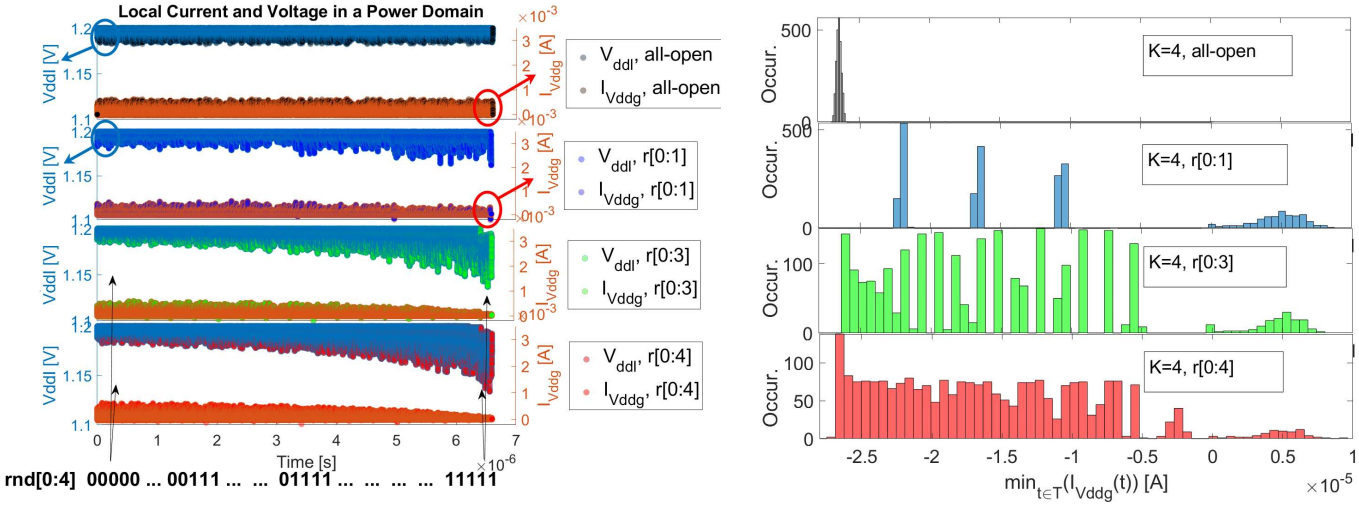


FIGURE 6: Local Currents and Voltages of the k=4 design: (a) vs. the level of randomization (b) leakage distributions.

drop is appearing with the state of r[4:0]='11111' (maximal resistance), similarly the reduction of the current.

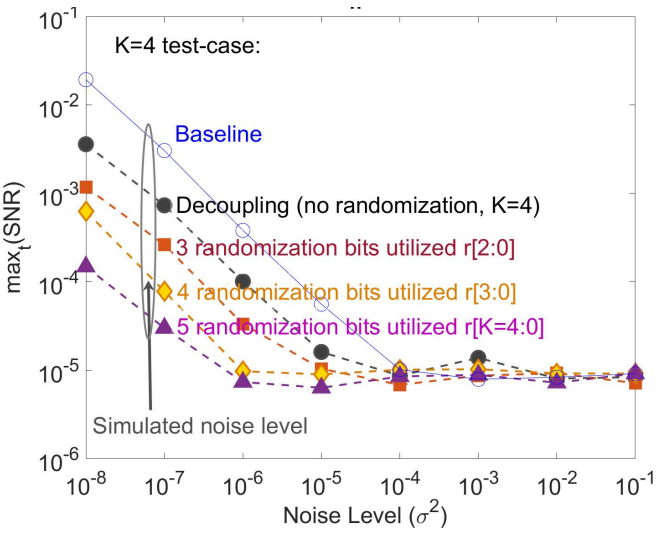
It is noteworthy that the maximal voltage drop is about $50mV$ which is expected due to the fact that power-gating library devices are designed to drive large currents. In fact, these characteristics are and should be verified by-design utilizing standard UCF/CPF design-flows. In Fig. 6b the leakage distribution of the minimum current (in each clock-cycle) is shown per each of these settings[3]. The important and interesting aspect which we can observe is that as more and more bits are utilized by the randomizer, the leakage distributes more and is becoming more and more uniform as discussed above. However, clearly a designer needs to set k as such that different leakage lobes overlap. Therefore, the baseline noise and the $Bias$ size are important parameter.

A complementing view of the transient-noise simulation, from which noise-level can be computed, is the noiseless simulation. Transient-noise simulations of large blocks are compute-intensive and therefore, after evaluating the noise level, it is possible to compute the SNR from such noiseless leakages. In this case, the inherent noise level (σ) is set within the analysis tool (e.g., python). Fig. 7a shows the maximum SNR achieved over time, max_t(SNR) with $5{\cdot}10^6$ traces (denoted by leakages). As the distributions indicate, the more randomization is consumed by the mechanism the SNR reduces. As compared to a baseline curve (no protection), the traces from randomization-disabled (all-open) design already provide a considerable SNR reduction by a factor of about 8. At the other extreme, a more than 2 orders of magnitude SNR reduction is achieved with as little as k=5. In this case the $Bias$ size was set to be x2^0 similarly to the minimum device of the network. As discussed, following the transient-noise simulation of the circuitry, it is easy to estimate the actual noise level as indicated on the figure with an ellipse.

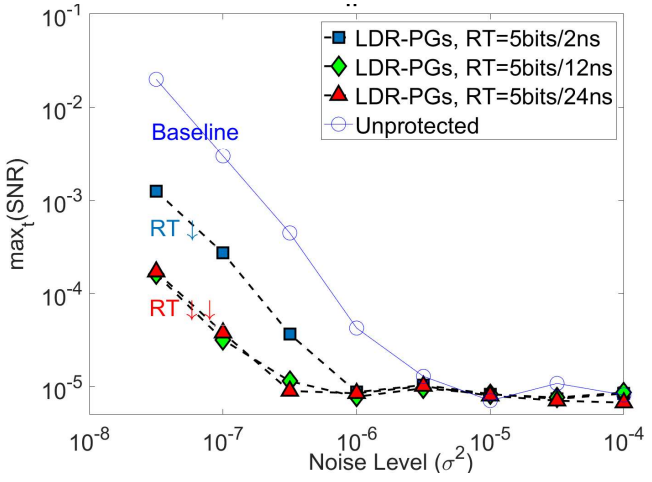
Another interesting point relates to the randomness-throughput (RT) as illustrated by Fig. 7b: PGs which are mainly built to power-on/off cores reflect large input capacitance and are therefore slow to react on inputs change. In this sense, if RT is increased, in essence the randomizer might not suffice to settle on the new state and in-turn the effective randomness bandwidth is "cut". An alternative view is that the span of the distribution reduces if RT is larger than the switching-time of the PG. Therefore, per PDK a designer will need to find the minimum RT to enable correct operation. These values in fact exist within standard PMK by the on-to-off timing characteristics of the PGs. As shown on the figure, with RT of 5bits/12ns (i.e. fresh randomness in each sixth cycle), the mechanism operate as required and provide maximum security (minimum SNR). It is important to stress that, reducing RT more will, at some stage, reduce security as an adversary will captures more consequent traces at the same randomized state.

Finally, we evaluate the effect of $Bias$ up-sizing. Fig. 8a shows the leakage distribution as the $Bias$ increases (from

[3]the maximum and average leakages shows similar distributions



(a)



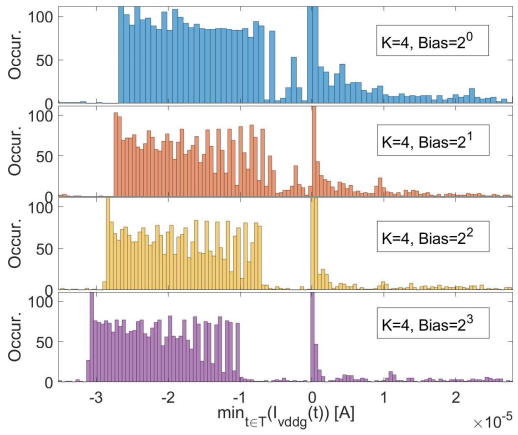
(b)

FIGURE 7: max(SNR) vs. σ for: (a) varying level of randomization (b) varying RT.

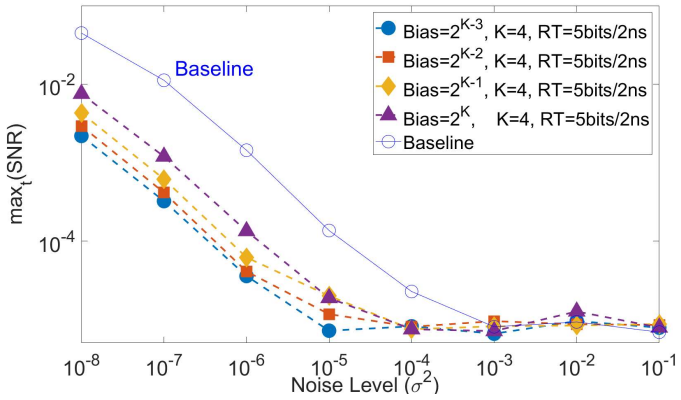
the top to the bottom plot), whereas Fig. 8b is showing the corresponding SNR levels of the different designs. In this example the RT was set to 5-bits/2ns. As discussed above, though theoretically we would like to increase the $Bias$ to maintain a perfectly uniform distribution, for concrete technological parameters its negative effects outweigh the positive ones: both the total leakage variance reduces and generally the leakage signal increases. The significance of these effects is observed by clear SNR reduction in Fig. 8b where the blue circle-denoted curve with the smallest $Bias$ size provides minimum SNR.

V. COST VS. SECURITY PARAMETER

Generally, area utilization cost factor of the masking countermeasure is in the range of d to d^2 [6]–[12] where, it depends on the implementation and level of serialization/parallelism and the ratio between linear and non-linear Boolean gates used to represent the algorithm. It also depends on how



(a)



(b)

FIGURE 8: Bias influence: (a) leakage distributions (b) max(SNR) vs. σ.

efficiently refreshes and masked multiplication gadgets are implemented. While multiplication gates complexity is of d^2, the best known randomness complexity ranges between $\lceil d^2/4 \rceil$ and $\lfloor (d(d-1)/2 \rfloor$. Simply put, even the lowest security-order, $d = 2$, best masking design will not cost less than 200% in area utilization and steeply increasing with d. On the other hand, the proposed randomization technique provides exceptionally low area utilization figures with a significant (and parametric) security-level. That is, with only K=3, it provides three orders of magnitude SNR reduction and a cost of $\sim$20% increment in area-utilization, or for higher security level with K=5 only 36% (further lowering the SNR) for a fully parallel AES as illustrated in Table 1. The table lists the different cost factors associated with two exemplary symmetric ciphers, the AES and Ascon-ρ[4], both of 128 bits. For the AES case, it was partitioned into power-domains (PDs) accounting naturally to 8-bit internal variables taking up 30 PDs for a fully parallel rounded implementation. The efficient Sboxes representation used was Canright's composite tower-field base one (GF($(2^2)^2)^2$) [36]. Taking the same tactic for the ISAP algorithm we have synthesized a fully parallel round of the Ascon-ρ permutation while grouping two Keccak Sboxes together per PD [37]. Area utilization values are listed in the table for: (1) vanilla (no protection) synthesized and placed and routed designs, (2) the partitioned and per-PD added overheads (e.g., spacing for power rings encircling PDs) and the cost of the randomization mechanism, randomness storage and power-gating, and (3) the total overheads for each of the blocks is also listed, accounting for the additions of the PDs and randomization mechanism for all PDs in a block. I.e., the AES required about 30 PDs and the Ascon permutation required about 40 PDs. As shown, the overheads are computed in the last rows of the table for different K values. In fact, the value of K=3 for the AES, was manufactured and tested (as demonstrated in [20]) and denoted by a * in the table. This design provided SNR levels even lower than the modeled/simulated values, which we refer to here as upper-bounds. This is natural as the analysis performed here was quite conservative; i.e., only accounting for a single block without *algorithmic noise* or other noise factors which are present in a complete system, and not considering measurement equipment limitations (noise and resolution). For K=5, which provides (pessimistic) SNR values of down to 10^{-5}, we list an area overhead of just 36%. For ISAP and K=5, area overhead increases to 79% owing to the very small Keccak Sboxes as compared to the AES ones. As an example, Fig. 9 illustrates a Cadence Innovus pre-placement power-grid layout for 8 PDs, illustrating area overheads and area-utilization required for a k=4 randomization mechanism.

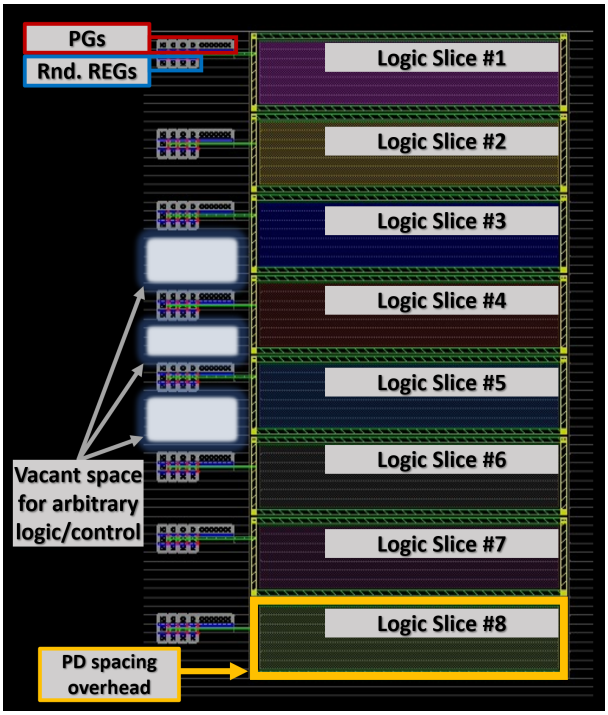


FIGURE 9: Illustration: exemplary power grid layout configuration (partial); fully automated and CPF/UPF flows supported.

[4]instantiated also by ISAP-A [35]

Area [μm^2]	Vanilla	K=0	K=1	K=2	K=3*	K=4	K=5	K=6
2 · 5bit Keccak Sbox	2·17	2·17	2·17	2·17	2·17	2·17	2·17	2·17
8bit AES Sbox	120	120	120	120	120	120	120	120
Per power-domain (PD) Overhead	0	7	7	7	7	7	7	7
Randomization mechanism	0	0	5	8	14	21	29	41
Total randomization and PD overhead	0	210	360	450	630	840	1080	1440
Total Area AES (fully parallel Rounded)	3000	3210	3360	3450	3630	3840	4080	4440
Total Area ISAP-A 128b (Ascon-ρ) fully-parallel Rounded	1820	2100	2300	2420	2660	2940	3260	3740
AES overhead	0%	7%	12%	15%	21%*	28%	36%	48%
ISAP-A 128 perm. overhead	0%	15%	26%	33%	46%	61%	79%	105%

TABLE 1: Area cost of the randomization mechanism for AES and ISAP-round vs. K.

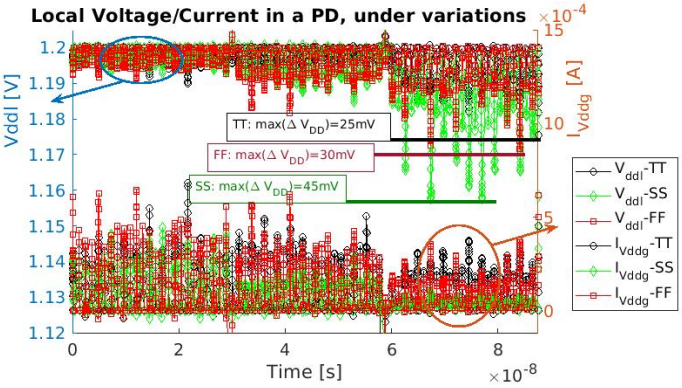


FIGURE 10: Randomizer operation under process variations

VI. ROBUSTNESS

Throughout the analysis performed we have evaluated the robustness of our design at various supply voltages (ranging 0.9 V to nominal 1.2 V) and temperatures in the range of -20°C to 70°C in simulation. However, the trends received were fully anticipated by the power-gates .lib characterization: owing to the dimensions of the PG cells, they are designed to provide minimal IR drops which can be simulated and accounted for by design and (e.g.,) adapt timing requirements accordingly owing to the randomizaer's worst-case which induces the largest propagation delay. As for one example Fig. 10 shows the local voltage and current flowing to a PD while operating with different randomizer's states. We have computed the worst case voltage-drops (ΔV_{DD}) at different process design corners (i.e., slow-slow SS, typical-typical TT, fast-fast FF, and all combinations) in a monte-carlo run representing the 6σ distribution point. Generally, the monte-carlo {SS, TT, FF} corresponding values are lower than the ones illustrated on the figure. The maximum voltage drop of a 65mV was captured with a SS corner, 60mV for the FF corner where the TT one was about 40mV. These values pinpoint the robustness of the mechanism to maintain a relatively low IR drop. Such drops only enforce us to select different .lib files for the timing analysis with a maximum change of 100mV in characterization which is supported by-design for the standard-cells and highlights small to moderate timing changes. All these results support the verifiability and EDA-applicability of such a methodology.

VII. CONCLUSIONS AND FUTURE-WORK

side-channels analysis (SCA) attacks have repeatedly underpinned the sensitivity of implemented cryptographic schemes. Launching massive efforts by the National Institute of Standardization and Technology (NIST) for both secured Lightweight Authenticated-Encryption and public-key Post-Quantum schemes as well as efforts for evaluation metrics and criteria and availability of security-embedding design tools.

Security solutions which are seeded by security-parameters derived directly from the hardware should naturally provide far more cost effective solutions than mathematical-only solutions. In this research we exemplify such a scenario which can significantly reduce the price-tag of SCA secure designs. I.e. generally, a 3 orders of magnitude SNR reduction, increases adversary's data-complexity with the same factor; if the proposed mechanism is utilized alone, its hardware overheads are negligible, that is for k values of up to 6 we have witnessed area cost of merely up to 48% of the entire area which is much lower than any masking-based countermeasure with minimal security order (d=2). In addition, a d=2 masking can theoretically provide a d'th power in data-complexity with the SNR^{-1} (or noise) at the base. Implying that the proposed mechanism can be more efficient stand-alone than masking for low-orders. If higher security levels are required, and e.g., if masking is evaluated to be used simultaneously, such a factor can quadratically reduce area/energy cost of the entire system as the masking order (d) can be linearly reduced with the SNR decrease. Another important aspect is that in low-noise scenarios some underlying noise-embedding mechanism is anyway a must for masked designs as demonstrated in [13], pinpointing the importance of the proposed mechanism. Therefore, the proposed design support our objective of demonstrating a fully-digital randomization based SCA security mechanism which provides a state-of-the-art cost-per-security in the class of EDA supported and security-modelled solutions.

A natural future work would be to evaluate the proposed approach embedded on-top or along masked circuitry and to tailor different combining apparatus to more efficiently reduce the cost of SCA protection. Moreover, an important direction would be to provide ameliorated tools on-top of commercial PDKs to enable faster integration as described in this paper. As such, even-though the approach presented

here can be easily embedded by any experienced engineer in the field, our goal would be to open-source improved parsing and embedding flows easily automated at the RTL level and for place & route tools.

ACKNOWLEDGMENT

This research was funded by Israel Science Foundation (ISF) grant number 2569/21. François-Xavier Standaert is a senior research associate of the Belgian fund for scientific research (FNRS-F.R.S.). Work funded in part by the European Union through the ERC project SWORD (724725).

REFERENCES

[1] M. S. Turan, K. McKay, D. Chang, C. Calik, L. Bassham, J. Kang, J. Kelsey *et al.*, "Status report on the second round of the nist lightweight cryptography standardization process," *National Institute of Standards and Technology Internal Report*, vol. 8369, no. 10.6028, 2021.

[2] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y.-K. Liu, C. Miller, D. Moody, R. Peralta *et al.*, "Status report on the second round of the nist post-quantum cryptography standardization process," *US Department of Commerce, NIST*, 2020.

[3] R. Primas, P. Pessl, and S. Mangard, "Single-trace side-channel attacks on masked lattice-based encryption," in *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2017, pp. 513–533.

[4] D. Park, G. Kim, D. Heo, S. Kim, H. Kim, and S. Hong, "Single trace side-channel attack on key reconciliation in quantum key distribution system and its efficient countermeasures," *ICT Express*, vol. 7, no. 1, pp. 36–40, 2021.

[5] E. Karabulut, E. Alkim, and A. Aysu, "Single-trace side-channel attacks on ω-small polynomial sampling: With applications to ntru, ntru prime, and crystals-dilithium," in *2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2021, pp. 35–45.

[6] G. Cassiers, B. Grégoire, I. Levi, and F.-X. Standaert, "Hardware private circuits: From trivial composition to full verification," *IEEE Transactions on Computers*, 2020.

[7] T. Moos, A. Moradi, T. Schneider, and F.-X. Standaert, "Glitch-resistant masking revisited-or why proofs in the robust probing model are needed," *Cryptology ePrint Archive*, 2018.

[8] G. Cassiers and F.-X. Standaert, "Provably secure hardware masking in the transition-and glitch-robust probing model: Better safe than sorry," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 136–158, 2021.

[9] H. Gross and S. Mangard, "A unified masking approach," *Journal of cryptographic engineering*, vol. 8, no. 2, pp. 109–124, 2018.

[10] A. Duc, S. Faust, and F.-X. Standaert, "Making masking security proofs concrete," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2015, pp. 401–429.

[11] B. Bilgin, L. De Meyer, S. Duval, I. Levi, and F.-X. Standaert, "Low and depth and efficient inverses: a guide on s-boxes for low-latency masking," *IACR Transactions on Symmetric Cryptology*, vol. 2020, no. 1, pp. 144–184, 2020.

[12] K. Papagiannopoulos, "Low randomness masking and shuffling: An evaluation using mutual information," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 524–546, 2018.

[13] O. Bronchain and F.-X. Standaert, "Breaking masked implementations with many shares on 32-bit software platforms: or when the security order does not matter," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 202–234, 2021.

[14] E. Peeters, F.-X. Standaert, N. Donckers, and J.-J. Quisquater, "Improved higher-order side-channel attacks with fpga experiments," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2005, pp. 309–323.

[15] T. Güneysu and A. Moradi, "Generic side-channel countermeasures for reconfigurable devices," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2011, pp. 33–48.

[16] P. Corsonello, S. Perri, and M. Margala, "An integrated countermeasure against differential power analysis for secure smart-cards," in *2006 IEEE International Symposium on Circuits and Systems*. IEEE, 2006, pp. 4–pp.

[17] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "High efficiency power side-channel attack immunity using noise injection in attenuated signature domain," in *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2017, pp. 62–67.

[18] A. Singh, M. Kar, J. H. Ko, and S. Mukhopadhyay, "Exploring power attack protection of resource constrained encryption engines using integrated low-drop-out regulators," in *2015 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*. IEEE, 2015, pp. 134–139.

[19] I. Levi, A. Fish, and O. Keren, "Low-cost pseudoasynchronous circuit design style with reduced exploitable side information," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 1, pp. 82–95, 2017.

[20] I. Levi, D. Bellizia, D. Bol, and F.-X. Standaert, "Ask less, get more: Side-channel signal hiding, revisited," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 67, no. 12, pp. 4904–4917, 2020.

[21] P. K. Infrastructure and T. P. Profile, "Common criteria for information technology security evaluation," *National Security Agency*, 2002.

[22] R. Snouffer, A. Lee, and A. Oldenhoeft, "A comparison of the security requirements for cryptographic modules in fips 140-1 and fips 140-2," BOOZ-ALLEN AND HAMILTON INC MCLEAN VA, Tech. Rep., 2001.

[23] V. Lomne, "Common criteria certification of a smartcard: a technical overview," *International Workshop on Cryptographic Hardware and Embedded Systems, tutorial*.

[24] S. Mangard, T. Popp, and B. M. Gammel, "Side-channel leakage of masked CMOS gates," in *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005, Proceedings*, 2005, pp. 351–365.

[25] E. Prouff and M. Rivain, "Theoretical and practical aspects of mutual information based side channel analysis," in *International Conference on Applied Cryptography and Network Security*. Springer, 2009, pp. 499–518.

[26] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, "Mutual information analysis," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2008, pp. 426–442.

[27] N. Veyrat-Charvillon and F.-X. Standaert, "Mutual information analysis: how, when and why?" in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2009, pp. 429–443.

[28] O. Bronchain, J. M. Hendrickx, C. Massart, A. Olshevsky, and F.-X. Standaert, "Leakage certification revisited: Bounding model errors in side-channel security evaluations," in *Annual International Cryptology Conference*. Springer, 2019, pp. 713–737.

[29] F.-X. Standaert, T. G. Malkin, and M. Yung, "A unified framework for the analysis of side-channel key recovery attacks," in *Annual international conference on the theory and applications of cryptographic techniques*. Springer, 2009, pp. 443–461.

[30] S. Guilley, H. Maghrebi, Y. Souissi, L. Sauvage, and J.-L. Danger, "Quantifying the quality of side channel acquisitions," *COSADE, February*, 2011.

[31] T. Unterluggauer, T. Korak, S. Mangard, R. Schilling, L. Benini, F. K. Gürkaynak, and M. Muehlberghuber, "Leakage bounds for gaussian side channels," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2017, pp. 88–104.

[32] B. J. Gilbert Goodwill, J. Jaffe, P. Rohatgi *et al.*, "A testing methodology for side-channel resistance validation," in *NIST non-invasive attack testing workshop*, vol. 7, 2011, pp. 115–136.

[33] F.-X. Standaert, "How (not) to use welch's t-test in side-channel security evaluations," in *International conference on smart card research and advanced applications*. Springer, 2018, pp. 65–79.

[34] F. Bache, C. Plump, and T. Güneysu, "Confident leakage assessment—a side-channel evaluation framework based on confidence intervals," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2018, pp. 1117–1122.

[35] C. Dobraunig, M. Eichlseder, S. Mangard, F. Mendel, B. Mennink, R. Primas, and T. Unterluggauer, "Updates on NIST Lightweight Authenticated Encryption Standardization Competition: Isap v2. 0," 2020.

[36] D. Canright and D. A. Osvik, "A more compact aes," in *International Workshop on Selected Areas in Cryptography*. Springer, 2009, pp. 157–169.

[37] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1. 2: Lightweight authenticated encryption and hashing," *Journal of Cryptology*, vol. 34, no. 3, pp. 1–42, 2021.

RINAT BREUER received her B.Sc. from the Faculty of Engineering Bar-Ilan University in 2020, following which she has started her M.Sc. studies. Rinat's interests are hardware-security and digital electronic design. She is currently working as a physical-design engineer with Amazon Israel.

FRANCOIS-XAVIER STANDAERT was born in Brussels, Belgium in 1978. He received the Electrical Engineering degree and PhD degree from the Universite catholique de Louvain, respectively in 2001 and 2004. In 2004-2005, he was a Fulbright visiting researcher at Columbia University, Department of Computer Science, Crypto Lab (hosted by Tal G. Malkin and Moti Yung) and at the MIT Medialab, Center for Bits and Atoms (hosted by Neil Gershenfeld). In 2006, he was a founding member of IntoPix s.a. From 2005 to 2008, he was a post-doctoral researcher of the Belgian Fund for Scientific Research (FNRS-F.R.S.) at the UCL Crypto Group and a regular visitor of the two aforementioned laboratories. Since 2008 (resp. 2017), he is associate researcher (resp. senior associate researcher) of the Belgian Fund for Scientific Research (FNRS-F.R.S). Since 2013 (resp. 2018), he is associate professor (resp. professor) at the UCL Institute of Information and Communication Technologies, Electronics and Applied Mathematics (ICTEAM). In 2010, he was program co-chair of CHES (which is the flagship workshop on cryptographic hardware). In 2021, he was program co-chair of EUROCRYPT (one of the flagship IACR conferences). In 2011, he was awarded a Starting Independent Research Grant by the European Research Council. In 2016, he has been awarded a Consolidator Grant by the European Research Council. From 2017 to 2022, he will be board member (director) of the International Association for Cryptologic Research (IACR). He gave an invited talk at Eurocrypt 2019. His research interests include cryptographic hardware and embedded systems, physical security issues including side-channel fault attacks, and the design analysis of cryptographic primitives that can cope with physical attack vectors.

ITAMAR LEVI received his B.Sc. and M.Sc. degrees in Electrical and Computer Engineering as a part of a direct excellence student track from Ben-Gurion University in 2012 and 2013, respectively. He completed his Ph.D. at Bar-Ilan University in 2017. He was a research-associate in UCLouvain, Belgium until 2019 with the UCLouvains Crypto-Group and currently he is a Computer-Engineering Faculty member at Bar-Ilan University, in Ramat Gan, Israel. He is also a member of Emerging Nanoscale Circuits and Systems Labs (EnICS), at BIU. Dr. Levi's current research interests are digital circuit design, embedded systems security, security evaluation analysis for cryptographic devices, side-channel and fault-injection countermeasures, and cryptographic implementations. As part of his activities, he has authored/co-authored over 50 journal articles and international conference papers and 7 patent applications, he co-authored a book on "Dual-Mode-Logic: A New Paradigm for Digital IC Design" and serves in several Technical Committees of IEEE Circuits and Systems Society and Hardware Security journals and conferences.