Silicon-correlated Simulation Methodology of EM Side-channel Leakage Analysis

Monta, Kazuki ; Lin, Lang ; Wen, Jimin ; Shrivastav, Harsh ; Chow, Calvin ; Chen, Hua ; Geada, Joao ; Chowdhury, Sreeja ; Pundir, Nitin ;…

(Citation)
ACM Journal on Emerging Technologies in Computing Systems,19(1):1-23

(Issue Date)
2022-12-09

(Resource Type)
journal article

(Version)
Version of Record

(URL)
https://hdl.handle.net/20.500.14094/0100485311

Silicon-correlated Simulation Methodology of EM Side-channel Leakage Analysis

KAZUKI MONTA, Kobe University, Graduate School of Science, Technology and Innovation
LANG LIN, JIMIN WEN, HARSH SHRIVASTAV, CALVIN CHOW, HUA CHEN, JOAO GEADA, and SREEJA CHOWDHURY, Ansys Inc., USA
NITIN PUNDIR, University of Florida, USA
NORMAN CHANG, Ansys Inc., USA
MAKOTO NAGATA, Kobe University, Graduate School of Science, Technology and Innovation

Cryptography hardware is vulnerable to side-channel (SC) attacks on power supply current flow and electromagnetic (EM) emission. This article proposes simulation-based power and EM side-channel leakage analysis (SCLA) techniques on a cryptographic integrated circuit (IC) chip in system level assembly. SCLA measures SC leakage metrics including T-score, SC leakage score, and the number of measurement traces to disclosure, leveraged by a secure system-on-chip design flow toward SC attack resiliency and SC leakage sign off. Power SCLA features the tracking of security sensitive registers within cryptographic logic paths and the automatic assignments of probe points on associated physical power nets. Power supply current traces are efficiently simulated for the large set of input payloads, with direct vector-based and vector-less random switching controls. EM SCLA evaluates magnetic fields created by every piece of metal wiring in metal stacks where power supply current of cryptographic processing flows. The EM emission and EM SCLA from the backside Si surface of an IC chip in flip-chip packaging are experimentally examined with a 0.13 μm test chip. The proposed simulation-based SCLA exhibits the SC leakage metrics of on-chip location and direction dependency as accurately as in the measurements.

CCS Concepts: • **Security and privacy → Side-channel analysis and countermeasures** • **Applied computing → Computer-aided design**;

Additional Key Words and Phrases: Cryptography hardware, integrated circuits, VLSI system, side-channel leakage, side-channel attack, silicon backside attack, electromagnetic emission, power supply noise, flip chip packaging

ACM Reference format:
Kazuki Monta, Lang Lin, Jimin Wen, Harsh Shrivastav, Calvin Chow, Hua Chen, Joao Geada, Sreeja Chowdhury, Nitin Pundir, Norman Chang, and Makoto Nagata. 2022. Silicon-correlated Simulation Methodology of EM Side-channel Leakage Analysis. *ACM J. Emerg. Technol. Comput. Syst.* 19, 1, Article 9 (December 2022), 23 pages.
https://doi.org/10.1145/3568957

Kazuki Monta and Lang Lin equally contributed (ECAs).
Nitin Pundir work has been done as an internship at Ansys.
Authors' addresses: K. Monta and M. Nagata, Kobe University, CS26, Graduate School of Science, Technology and Innovation, Kobe University, 1-1 Rokkodai-cho, Nada-ku, Kobe 657-8501 Japan; emails: monta@cs26.scitec.kobe-u.ac.jp, nagata@cs.kobe-u.ac.jp; L. Lin, J. Wen, H. Shrivastav, C. Chow, H. Chen, J. Geada, S. Chowdhury, and N. Chang, ANSYS, Inc., 2645 Zanker Road, San Jose CA 95134, USA; emails: {Lang.Lin, Jimin.Wen, harsh.shrivastav, Calvin.Chow, Hua.Chen, Joao.Geada, sreeja.chowdhury, Norman.Chang}@ansys.com; N. Pundir, University of Florida, 968 Center Dr., University of Florida, Gainesville, Florida 32611, USA; email: nitin.pundir@ufl.edu.

1550-4832/2022/12-ART9
https://doi.org/10.1145/3568957

1 INTRODUCTION

Side-channel attack (SCA) is a practical threat to cryptosystems. An attacker investigates the secret key of cryptography hardware by exploiting various analysis models on physical quantities that are inevitably observable during the operation. **Simple power analysis (SPA)** and **differential power analysis (DPA)** straightforwardly relate bit-wise operation with power supply current consumption of associated digital **integrated circuits (ICs)** [1]. **Correlation power analysis (CPA)** [2], which is the evolved version of DPA, assumes the **side-channel (SC)** leakage model that is tailored for the given cryptography algorithm and related to power supply current consumption of an IC chip. For example, the number of bit changes in a secret data register, often called Hamming distance, can be chosen as one of the quantities of interest in the crypto algorithm and correlated to the size of power consumption current at the timing of data access.

Here, **electromagnetic (EM)** radiation can be a more powerful alternative to an adversary [3–6], thanks to its near-noninvasive features. An attacker could capture more localized emanation of a silicon IC chip by using a small magnetic probe [7] and derive more detailed information with EM SC analysis. Pre-silicon simulation becomes more complicated for an IC chip designer to complete, since multi-physical approaches are inherently necessary. EM SC simulation therefore draws a high attention in the research community toward the design for high resiliency of cryptosystems.

Many works have been reported on logic and physical design countermeasures against SCAs. Some of them try to mitigate power SC correlation by power balancing or by randomizing intermediate values among logic paths [8–13]. The techniques are often tested through post-silicon evaluation, however, revealing three major downsides. First, the production of an **application specific IC (ASIC)** chip is time consuming and obviously costly. A **field-programmable gate array (FPGA)** device is used instead, however, while cryptography modules function in the same way as in a ASIC chip, their physical behaviors can be different if one investigates power supply current consumption. Second, it is not necessarily possible to designate the physical source of SC leakage, even though the presence of SC leakage is experimentally observed. Third, if an unexpected vulnerability is discovered at the post-silicon evaluation, then its respin with additional countermeasures should be enormously expensive, not only for the cost of manufacturing but also for the delay of time to market.

Therefore, the pre-silicon **side-channel leakage analysis (SCLA)** methodology has been keenly desired and investigated with a full-stack simulation approach. This will expedite the use of countermeasures in its design stage where the vulnerability of an IC chip to SC leakage is predicted and mitigated before going to tape out. A variety of simulation techniques for SCLA have been reported [14–24]; however, general problems still remain. The reduction of simulation time is essential to evaluate SC leakage for the large number of clock cycles in crypto processing. A public key cryptography needs thousands of clock cycles for SCLA of full key bytes. On the other hand, a symmetric key cryptography, e.g., **advanced encryption standard (AES)** requires millions of traces with different input payloads. The improvement of simulation accuracy is another challenge. The simulation of power supply currents is dominated by fully physical models of power delivery networks and transistors [20]. Here, the simulation time will almost explode as the number of transistors in an IC chip increases for the higher level of functionality. The SCLA simulation technique therefore needs to achieve the best balance of efficiency, accuracy and capacity to handle the full-chip and system level design database, and moreover, to cover multiple physical aspects of power as well as EM SC leakages.

In this article, we propose the fast simulation methodology of power and EM SCLA, which is applicable to **Systems of Chip (SoCs)** that include crypto hardware. This flow leverages a power noise solver and an EM solver as underlying physical simulation methods to simulate traces during cryptography module operation. And, this flow is optimized for collecting traces, which are

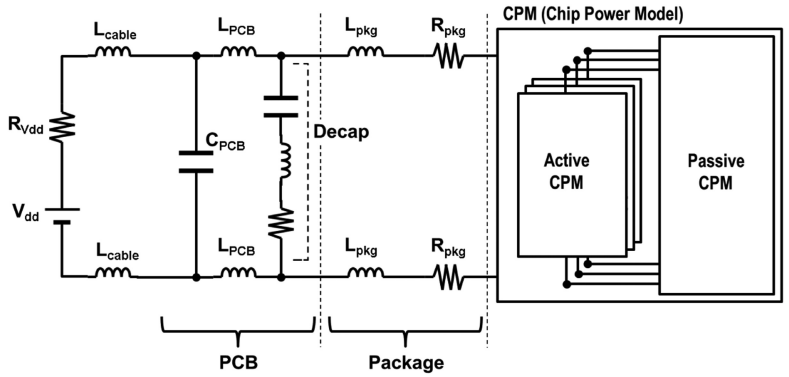


Fig. 1. Chip-package-system (CPS) board model for power supply current simulation.

analyzed in the subsequent SCLA flow by using a security-sensitive register extraction engine, an intelligent probe generation flow and a fast simulation methodology called the **direct vector control (DVC)**. In the subsequent SCLA stage, the SC leakage heatmap is produced to guide a designer to find vulnerable spots, and also to expedite the adoption of countermeasures. The whole simulation flow is verified for the correctness and accuracy of EM SCLA through detailed comparisons with silicon measurements.

The remaining part of this article is structured as follows. Section 2 describes the methods of on-chip power noise modeling and near-field EM emission modeling. Section 3 details the techniques to speed SC leakage simulation with a security-sensitive register extraction engine, an intelligent probe generation flow and DVC. In Section 4, the silicon design flow based on the SCLA is outlined and also exemplified by a prototype Si chip. The comparison between simulation and measurement results are also given. Section 5 concludes this article.

2 EM EMISSION MODELING

2.1 Power Supply Current Modeling with Chip-package-system (CPS) Board Model

Power SC leakage is rooted to the dynamic power supply current consumption by logic gate switching inside an IC chip. Full-chip power supply current flows over a **chip-package-system board (CPS)** integrated **power delivery network (PDN)** [20]. The system model includes a **printed circuit board (PCB)** and also cables for connecting to external power sources. The package model incorporates a plastic interposer with soldering bumps and balls in connection to chip pads and PCB lands, respectively. We assume here that an IC chip is equipped with cryptographic engines, and the chip model then involves dynamic power supply current during cryptographic operation.

The system-level model is constructed from the CPS involving a **chip power model (CPM)**, as shown in Figure 1. The CPM of an IC chip consists of a passive sub model representing an impedance network of an on-chip PDN and an active counterpart responsible for the power supply current during the operation of cryptographic circuits and represented in a **piece-wise linear (PWL)** time domain waveform. The creation of CPM will be detailed in the next section.

It is important to note that power supply current is observable at any position on CPS model for power SCLA. The voltage variation is induced on an on-chip PDN by the interaction of power supply current and its parasitic impedance, which is recognized as dynamic IR drop noise or power noise hereinafter. The same power supply current creates magnetic fields nearby metal wirings on the PDN, as the part of EM emission. There are several shunting paths for power supply currents

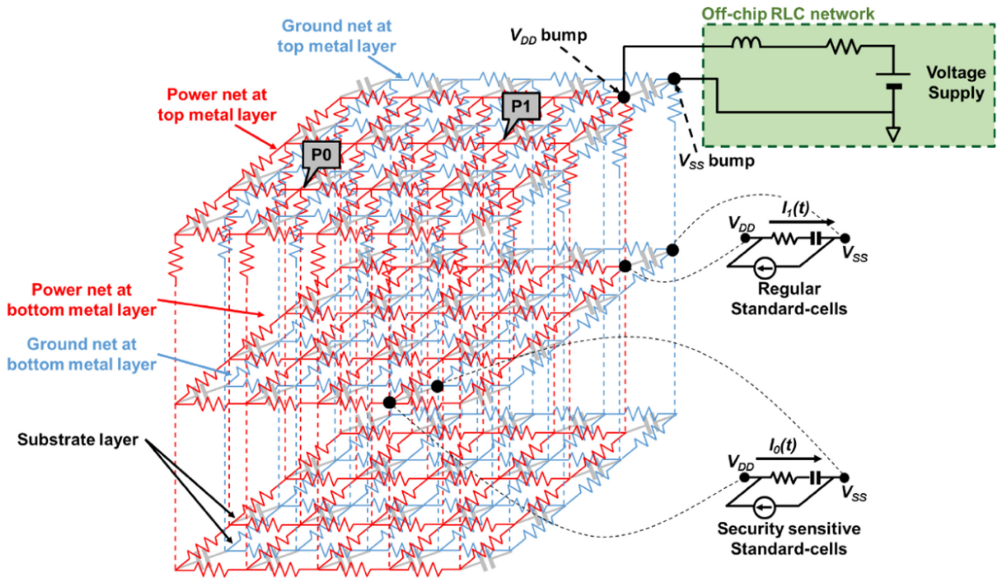


Fig. 2. Power-noise model of an on-chip PDN of an IC chip with security functionality.

to attenuate dynamic variations, and determining the frequency-domain response of the whole PDN impedance. In this article, the test device is evaluated with the clock frequency at 30 MHz, but power current consumed by digital circuits operating at 30 MHz has the frequency contents of 30 MHz and above. It means that parasitic impedance considered in this flow is important on SCLA evaluation, because it has high impact on the voltage variation (e.g., high-frequency contents of power currents are suppressed by low-pass filter consisting of PDN parasitic passive components).

2.2 On-chip Power Noise Modeling

Power SCLA relies on on-chip power noise simulation. This involves four elementary processes: (1) switching scenario creation, (2) parasitic passive component extraction, (3) cell-level current profile characterization, and (4) transient simulation. The whole simulation flow has been established for the dynamic power noise analysis in very large-scale digital ICs and evolved with its high-capacity solver to handle an SoC chip having millions of logic gates. The first Silicon correlation was reported in Reference [25]. The technical details and updates on the power noise solver can be found in Reference [26]. Here, the resistance, R, inductance, L, and capacitance, C, which are all parasitic to an on-chip PDN, are extracted from the physical layout of an IC chip and included in the CPS power noise simulation. The PDN is primarily formed by the topmost metal layers in a mesh structure covering the whole IC chip. On the other hand, the power supply current of a standard logic cell is individually connected to power and ground nodes at its placement position on the bottom metal layers of the on-chip PDN, respectively, as shown in Figure 2 [27]. While the correlation of power supply current with the data of interest is locally rooted to the logic cells that are associated with the data, the power supply current as a whole flow through the entire PDN over an IC chip and interact with RLC components parasitic to V_{DD} and V_{SS} domains of a full-chip PDN. In addition, the Si substrate of an IC chip is represented as a resistive-capacitive mesh model and attached to the PDN, that captures the distributions of p- and n-type implanted impurities as well as p-n junctions. The whole model in simulation creates chip-level power noise, and further, induces power SC leakage over an IC chip and its assembly.

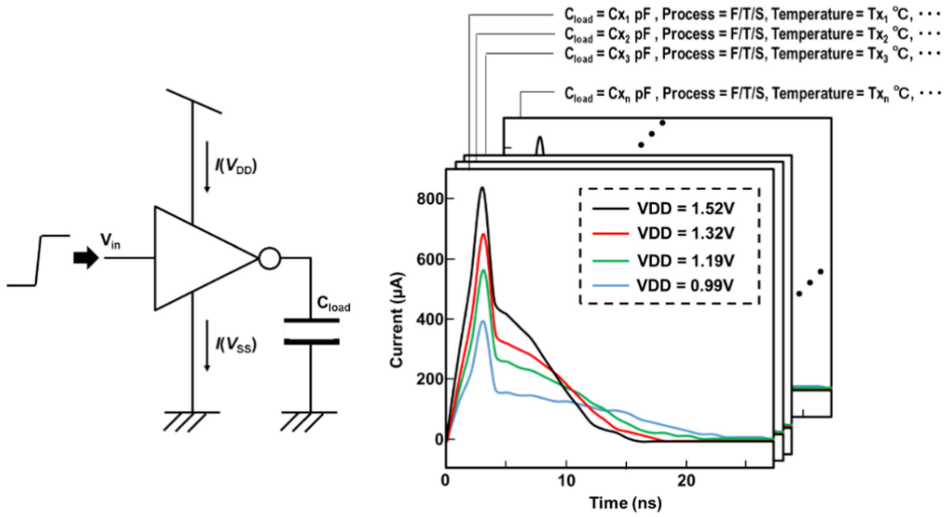


Fig. 3. Cell-level dynamic power supply current model under various operation conditions.

The total power consumption measured at the global voltage supply port is a function of demand currents from all logic gates in a design. The dynamic voltage drop at any virtual probing port (e.g., P0 and P1 in Figure 2) can be expressed as

$$V(\mathrm{t}) = I(t) * R + L\frac{dI(t)}{dt} + \frac{1}{C}\int I(t)dt, \tag{1}$$

where I(t) is the local dynamic current, while R, L, and C are derived from PDN physical layout. Our simulation methodology estimates the power supply current drawn by every logic gate in design, and includes the effects by intentional decap devices, intrinsic device capacitance, metal fills, and RLC parasitic elements over PDN grids. When an IC chip contains a cryptographic core, I(t) can be divided into two parts; (1) I_0(t) consumed by the security sensitive standard-cells and (2) I_1(t) by the other standard-cells, as shown in Figure 2. The ratio of I_0(t) to I_1(t) is regarded as the sort of **signal-to-noise ratio (SNR)**, which is an observable factor of significance determining SCLA. Here, I_1(t) has almost no correlation with sensitive information.

To simulate dynamic IR-drop waveforms, the time-domain power supply current and RLC parasitics of PDN grids are modeled [26]. Power supply current libraries of standard logic cells, input/output macro cells (IO macros), and IP macro blocks are prepared using transistor-level SPICE simulation before dynamic power noise simulation. The RLC parasitics are extracted from the physical layout of cells and blocks. Figure 3 shows the image of the cell-level current model of an inverter as an example. The dynamic current at V_{DD} pin and V_{SS} pin are captured by using SPICE simulation for every logic operation according to the truth table of a logic cell. To precisely model both linear and non-linear power behaviors of the cell, the power supply current library first defines a set of operating conditions during characterization. Then a heuristic interpolation method is employed to derive the power profile of other operating conditions including process corners, power supply voltage, temperature, input signal slew, signal load capacitance, multiple output states and so on. For IO macros or IP blocks, the switching states of interest can be modeled with pre-simulated time-domain PWL waveforms of power and ground switching current.

An SC attacker or an evaluator in general captures power noise waveforms at off-chip power pins on system assembly, which is easier than measuring power supply currents locally within an IC chip. As opposed to this, there is no constraint for probe allocations in simulation-based

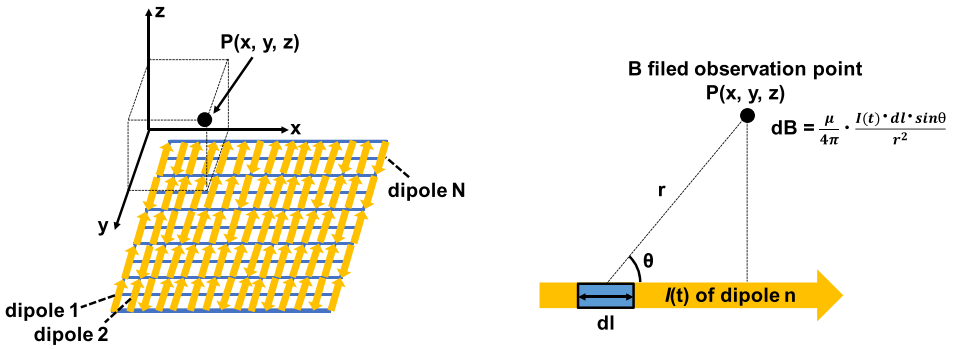


Fig. 4. Near-field EM emission modeling of an on-chip PDN wires as dipoles.

SCLA. In our power noise simulation flow, it is possible to place virtual measurement probes at any locations within an on-chip PDN. The virtual probes can be automatically placed on an on-chip PDN with a given distance, for instance as denoted by P0 and P1 in Figure 2. This feature allows a designer to visualize the distribution of SC leakage in the whole chip area, and moreover, to focus on the security vulnerable regions once a location-aware SC leakage heatmap is generated.

The traditional methods to simulate on-chip power consumption are categorized in two types; **register-transfer level (RTL)** simulation and transistor level one. The RTL level power current prediction is fast enough for SCLA in the architectural design exploration but not always suitable in the post layout evaluation, because the physical characteristics such as transistor's transient behaviors and PDN parasitics are not included. On the other hand, the transistor level one is regarded as the most accurate, however, leads to the exponential growth of simulation time with respect to the size of circuits. This is inappropriate in SCLA evaluation on the secure SoCs. Unlike these traditional methods, the proposed power noise simulation flow is more friendly to side-channel assessments, since it incorporates the physical attributes and keeps the computation time in a linear manner to the number of logic gates. In addition, the multi-threading computation over many core CPUs is also applicable, thanks to the parallelism in the power-library-based power noise simulation algorithm.

2.3 Near-field Electromagnetic Emission Modeling

Power supply current induces magnetic fields according to Maxwell's equations. To characterize near-field EM emission, a dipole-moment method is universally applied to wire segments and metal planes carrying power supply current [28–31]. An image of near field EM emission modeling is given in Figure 4. An on-chip PDN wire segment is represented as a dipole moment and then the associated B field, B(t), at the observation point P is calculated according to the Biot-Savart raw of Equation (2). The total B(t) is computed by summing the contributions by every dipole (dipole 1, dipole 2, ..., dipole N) arranged in a lattice within an IC chip. It is also updated for the time-domain change in power supply current I(t) to approximate the near-field EM traces. The equation also uses the permeability, μ_0, the length of wire segments, *dl*, the distance vector *r* and the angle between dipole point and observation point, θ

$$B(t) = \frac{\mu_0}{4\pi} \sum_{k=1}^{N} \int \frac{I_k(t) \bullet dl_k \bullet \sin\theta_k}{r_k^2} \tag{2}$$

The EM observation points can be freely planned in a spherical space from an IC chip in assembly, however, often placed near their surface. The power and EM noise solver can accommodate almost unlimited number of EM observation points up to being bounded by the computation

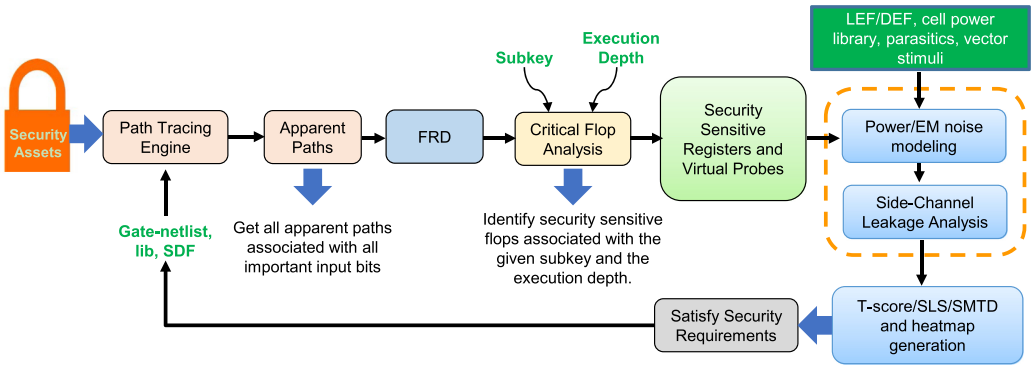


Fig. 5. Overall flow of the pre-silicon side-channel assessment method for secure SoC design.

facility, however, we have reasonably set the number of EM observation points as 1,024, which approximately costs the simulation time of 3 h for 10K traces (Table 1) in this article. The number of probes can easily explode with the more detailed meshes in the three-dimensional field analysis. In contrast, one can remain in the same number of 1,024 probes (as mesh nodes) while exploit multiple simulation runs hierarchically from the coarse resolution to the fine one to search and focus on the area of interest.

The distribution of EM emission and also EM SC leakage heatmap can be simulated with the fine grains of power wire segments within an IC chip and also in its assembly. These results help a designer to optimize the physical layout of an IC chip and also to choose the physical structure of assembly, for the higher level of protections against power and EM SCAs. The EM magnitudes in simulation with the B(I(t)) calculation and those in Silicon measurements are not necessarily matched, because the simulation does not include the noise in experimental environment as well as the effect of off-chip electronic components. The simulation in this article will not estimate the absolute magnitude of EM noise, while reveal the correlations and more importantly explore the locations of strong side-channel leakage in the SCLA at the pre-silicon stage. The proposed flow based on the Biot-Savart raw is sufficiently efficient and trustworthy from this purpose.

3 SIDE-CHANNEL LEAKAGE SIMULATION

3.1 Overview of SCLA Simulation Framework

The proposed power and EM SCLA simulation framework is outlined in Figure 5. For a data leakage problem verified through SC leakage assessment, it is important to recognize what data to be protected. The "security assets" of a design can flow through a chain of logic gates and registers in a secure IC chip. At the gate-level netlist of the design, all gate instances affected by such security assets are defined as security sensitive registers and nets, which have to be carefully examined for data leakage. This step is the starting point of our simulation framework.

We leverage the **static timing analysis (STA)** to parse the entire logic core of crypto design to create a **forward reachability database (FRD)** of the design at the gate netlist level. The design input to our flow includes the gate-level netlist, the logic cell timing model file in liberty format, and the timing constraint file in **standard delay format (SDF)**. Effectively, FRD stores the reachable registers at every execution depth for all the input ports. Subsequently, FRD is used to get all potentially accessible registers at any execution depth in a constant runtime penalty. From the obtained list of registers, security-sensitive registers are identified using **critical flop analysis (CFA)**. These security-sensitive registers are grouped at the chip-layout level to perform the SC validation.

The extracted security-sensitive registers are those registers in the design that leak the most SC information about the secret byte when compared to other registers in the design. By isolating the power signature from security-sensitive registers, we substantially increase the SNR ratio in the power traces by reducing intrinsic noise from other registers. The rest of the registers are irrelevant, since they carry little SC information about the secret key byte critical for performing the attack. From a practical perspective, the attacker may just have access to the global power consumption of the device, but highly motivated attackers may resort to pre-processing of data to reduce noise (environment and intrinsic) and even sensing regional power SC leakages other than global ones. For design engineers with complete access to the gate-level and layout-level design of the chip, the proposed framework assumes a white-box approach to pre-silicon SC assessment. The framework enables the complete coverage of SC leakage and further facilitates the amplification of SNR associated with secret key bytes in a noiseless environment. If the design engineer also intends to estimate **measurement-to-disclosure (MTD)** from a post-silicon SCLA perspective, then our framework allows the SC leakage of non-sensitive registers or a realistic silicon noise profile to be further included.

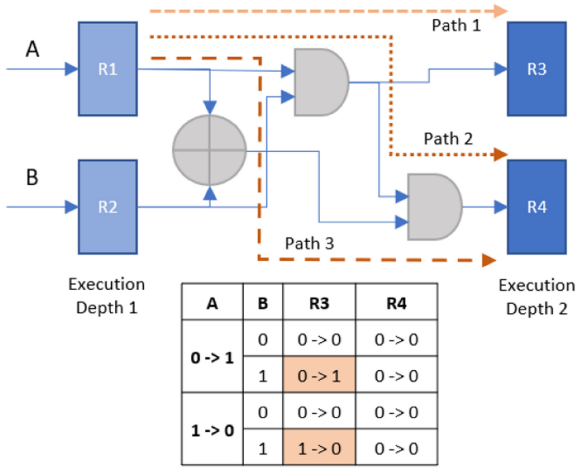
The physical model of the logic core can be built with layout files in LEF/DEF format, wire parasitics files, cell power supply current model files, and the vector stimuli file in **value change dump (VCD)** format. Then a power noise solver computes the dynamic IR drop traces at any location on the logic core's PDN. Further, an EM solver is used to get the dynamic EM traces at a near-field plain of the IC chip.

To compute a large number of traces, we have proposed a simulation trace reduction approach called "direct vector control." Finally, power noise and EM traces are post-processed by the SCLA flow for the SC assessment with heatmaps and scores. Since our flow can identify the location-dependent SC leakage down to a gate-instance granularity, a failure of SC scoring result can be fixed at the gate-netlist level.

3.2 Identification of Security-sensitive Registers

3.2.1 Fast-path Tracing. The first step of the framework is to analyze the flow of information between input and output ports by examining all STA paths and tracking all the registers along these paths. We recursively take all the important input bits and traverse through all the static paths until we hit the output ports. We assume that registers along these paths are the ones that would be impacted by the switching of the input bit. For example, Figure 6 shows the illustration of our tracking for two execution depths, where registers pairs (R1, R2) and (R3, R4) are at the execution depths 1 and 2, respectively. When we track static paths from input bit A, we get three paths and two endpoints (R3 and R4). We assume the switching of A could result in the switching of R3 and R4 at execution depth 2, but this may not always be true, as depicted by the truth table in Figure 6. It can be seen that switching of A from 0→1 or 1→0 impacts the R3 register, but the value of R4 remains unchanged. This happens because the same registers may be impacted by other input bits on the same execution depth, in this case, input B. That is why the paths reported by our tracing technique are called apparent paths.

Other schemes of information flow analysis at the gate-netlist level, i.e., SCRIPT [32] and GLIFT [33], are more accurate as they can sensitize these apparent paths to report exact registers that will be impacted by the switching of the input bit. However, they incur a large penalty on the computation time. For example, GLIFT requires the generation of shadow logic, which is an NP-complete problem and could be very challenging for large circuits. In contrast, SCRIPT requires the recursive conversion of registers from full scan to partial scan and repeated masking and unmasking to enable and disable the propagation of faults. This could be challenging, since it needs a specialized **automatic test pattern generation (ATPG)** to support this feature or if the design has large execution depths.



A	B	R3	R4
0 -> 1	0	0 -> 0	0 -> 0
	1	0 -> 1	0 -> 0
1 -> 0	0	0 -> 0	0 -> 0
	1	1 -> 0	0 -> 0

Fig. 6. Illustration of apparent paths between two execution depths.

We realized that the speed and scalability of the framework can be improved for SC assessment by simply considering all the apparent paths and avoiding sensitization of the paths. We came to this decision to improve the SNR ratio of power traces to focus on SCLA. This can be effectively achieved by considering all the registers that could potentially be affected by the switching of input bits. Once the list of such sensitive registers associated with each input bit is collected at each execution depth, the list could be further pruned by following critical flop analysis, thereby improving the overall SNR of the power traces.

Information about all the apparent paths and registers is stored in the FRD. To minimize the storage space, we only trace timing paths associated with every important input bit in the design. The important inputs used in the tracing comprise of: (1) Secret Assets: Any secret bit that the organization wants to keep hidden and the attacker wants to reveal, e.g., keys in AES; (2) Non-secret Inputs: Any input bit that is not secret, and we assume the attacker can control, e.g., plaintexts bits in AES. All other input ports that do not satisfy the criteria are excluded from our tracing engine, e.g., clock, reset, start, enable signals.

The biggest hurdle in generating the FRD is the path explosion problem, due to an exponential increase in the number of static paths as the execution depth increases. This causes a significant increase in the assessment time and memory required to generate and store the FRD. To solve this problem, we dropped the combinational paths from our FRD and only stores a unique set of "driver" and "sink" registers at every execution depth. We define "sink" registers as all those registers at the current execution depth to where a static path exists from all the "driver" registers from the previous execution depth. For example, in Figure 6 for the input bit A at the execution depth 2, the "driver" register is R1 and "sink" registers are R3 and R4.

The STA tool allows us to perform multi-threading to get a set of "sink" registers from the provided set of "driver" registers in one go and thus helps us to save a lot of time in the generation of the FRD. For the input bit A, as shown in Figure 6, three static paths and two "sink" registers exist at execution depth 2. In practical design circuits, the number of static paths between two execution depths is much higher than the limited set of "sink" and "driver" registers. Thus, saving all information (combination gates) about these paths becomes infeasible for designs with a large number of input bits and high execution depths. To make an important clarification, we are not at all ignoring the power consumption and glitch effects from combination gates in the SC assessment flow. These sets of grouped registers along the datapath of a cryptography design store the targeted

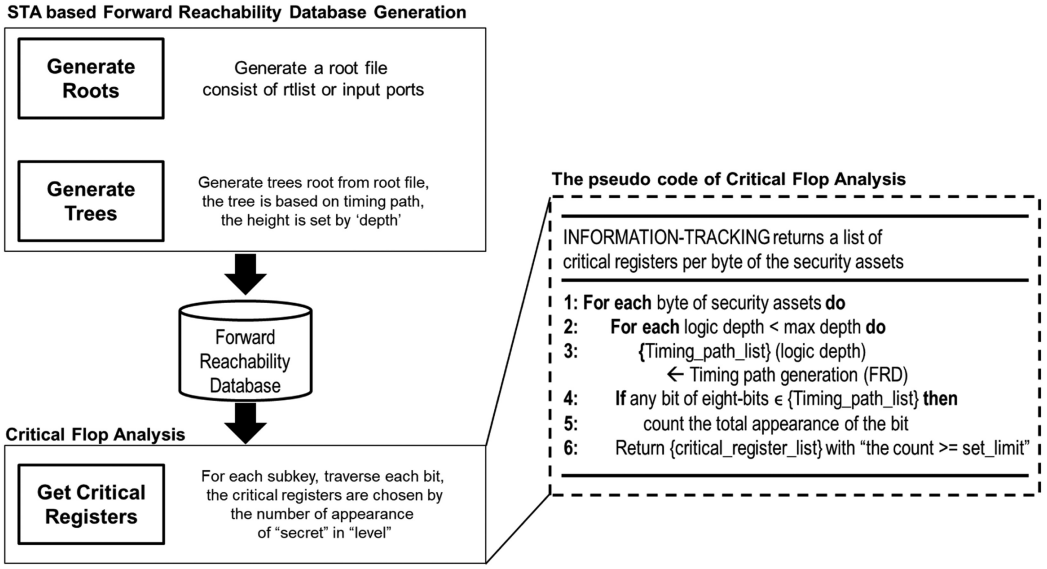


Fig. 7. Critical flop analysis to extract security-sensitive registers from the set of reachable registers.

data values at a particular execution depth for correlation SC analysis, as we explained before. In general, we estimate the complexity of computation in FRD to be O(n) for exploring n nodes within each sequential depth in parallel among the n sequential ones.

3.2.2 Critical Flop Analysis. To identify security-sensitive registers of a design, we propose the methodology of tracing the security assets (e.g., a secret key byte of a cryptographic block) at each specific execution cycle. The execution cycle under test is taken as the input to our simulation framework to provide the flexibility to focus on a particular design execution cycle. For example, in the case of AES, an adversary may specifically target the first or the last round. In our framework, CFA, as seen in Figure 7, is used to equivalently realize the goal. CFA takes the subkey and the execution depth as input and provides a list of security-sensitive registers in the FRD. We interchangeably use the words "flop" and "register" to represent the 1-bit memory elements in the gate-level netlist. CFA takes the attacker's perspective and assumes the SC leakage on the subkey using SCAs such as CPA or DPA. CFA also assumes that the attacker has some information about the implementation to target a particular execution time frame. By controlling the input plaintext and performing the correlation-based attacks, the given security-sensitive registers assist in leaking secret bytes with minimally necessary power traces.

The SCLA evaluator can control some input to the system, e.g., plaintext, which then gets combined with the secret (key), for example, substitution, mix column, shift rows, and XOR operations in AES. And due to the confusion property of the cryptographic algorithms, multiple bits of the non-secret and secret inputs should be impacting the same flops. Based on this information, we define two properties to extract the security-sensitive registers.

Property 1. *Flop should be impacted by both secret and non-secret input at the execution depth under analysis.*

Property 2. *Multiple bits of secret and non-secret input should impact the flop at the execution depth under analysis.*

As seen in Figure 7, for each byte of security-sensitive assets, all the registers in the FRD are evaluated whether above two properties are met or not to classify certain registers as

security-sensitive registers at the particular execution depth. For this, the design engineer needs to set the limit of how many secrets and non-secret input bits should be impacting the register to classify it as "security sensitive". This set limit could vary with different types of implementation and design under analysis. For the given test case of AES implementation, we set the limit to eight due to the size of sbox registers. The complexity of computation for accessing any information regarding critical flops would be O(n) if we assume the table look-up algorithm to the FRD that is generated beforehand.

In this flow, we leverage FRD provided by STA-based fast-path tracing, which is explained in Section 3.2.1. This FRD contains the information of all the registers that could potentially be affected by the switching of input bits. And CFA extracts the registers that manipulate the security assets by assessing all registers in the FRD. The extracted registers reachable by the security assets are then targeted for searching any leakage. With this flow, we can search all the source of leakage and can avoid overlooking a leakage that a designer is not expecting.

3.3 Intelligent Probe Generation Flow

It becomes a daunting simulation task if one tries to cover all SC leakage locations for a large SoC design. At the first glance, the probe location near the security sensitive registers has the highest priority of validating the SC leakage. The metal stacks nearby these source locations would be of secondary interests to know how the leakage propagates and whether a chip pad location can leak information to favor an actual silicon attack. Finally, it is very hard to completely ignore the PDN grid locations far away from those security sensitive registers to miss any unexpected leakage mechanism such as weak PDN design of a long routing and power-noise coupling effects.

In our framework, we leverage the critical flop analysis result from the previous section to further decide the best probe locations by ranking the power SC leakage from a representative set of cryptographic vectors. Peak power and power variation of each instance among thousands of vectors will be used to determine the ranking of security-sensitive instances, which are the identified registers plus the driver driving the security sensitive nets. Lower activity instances in the security critical list would be ranked lower, so less important to be probed. Instances with low power variation value are also not likely to leak data, so less important to be probed. An empirical score called $P_{\text{normalized}}$ of each instance is shown in Equation (3):

$$P_{\text{normalized}} = P_1 * P_{\text{peaknormalized}} + (1 - P_1) * P_{\text{varnormalized}}, \tag{3}$$

Where P1 is defined by the user, $\text{P}_{\text{peaknormalized}}$ is the normalized cell peak power, and $\text{P}_{\text{varnormalized}}$ is the normalized variation of the cell power. $\text{P}_{\text{peakmormalized}}$ is defined in Equation (4) as

$$P_{\text{peaknormalized}} = (P_{\text{peak}} - P_{\text{peakmin}})/(P_{\text{peakmax}} - P_{\text{peakmin}}), \tag{4}$$

where the P_{peakmax} is the maximum P_{peak} of all the instances running through thousands of plaintexts, and P_{peakmin} is similarly defined. $P_{\text{varnormalized}}$ is also derived in the same way. $P_{\text{peaknormalized}}$ and $P_{\text{varnormalized}}$ has the range between 0.1 and 10 and are derived from the distribution of P_{peak} and P_{var}. Finally, a user can limit the maximum number of virtual probes for layout-level SCLA, just for bounding the computation efforts. Starting from the top-one critical instance, the snapping to a pre-generated virtual probe on the corresponding $\{V_{\text{DD}}, V_{\text{SS}}\}$ PDN of the top or preassigned metal layer of a design can be identified by calculating the minimum effective point-to-point resistance from $\{V_{\text{DD}}, V_{\text{SS}}\}$ nodes of the instance. Then other instances are kept assigned with probes until the user limit has reached. If two instances share the same probe, then the flow can automatically annotate them intelligently.

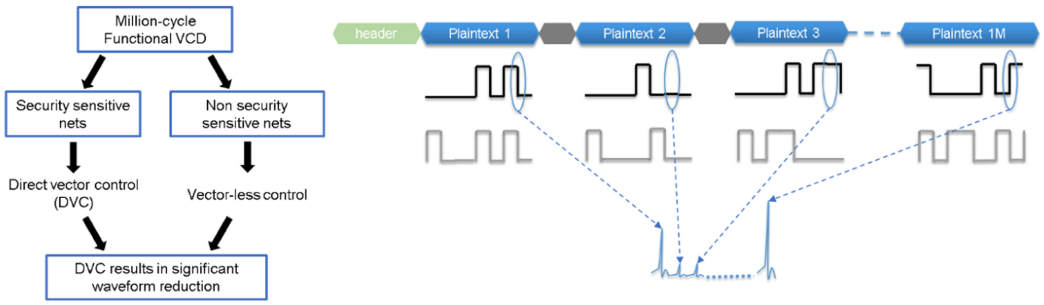


Fig. 8. Direct vector control technique to control the SNR of side-channel assessment in simulation.

3.4 Direct Vector Control

To approximate the silicon MTD, thousands or even millions of input payloads are needed to generate time-domain power supply current traces, which is not computationally feasible for circuit-level simulators. In this work, we have proposed a simulation trace reduction approach to enabling the simulation of dynamic power-noise and EM traces with a large number of stimuli vectors. We coined this reduction approach as "direct vector control" method as described in Figure 8. Given the knowledge of chip functionality, the designer would know the security assets of the design and provide a list of security sensitive nets. For example, such list of nets can be an interface data bus carrying secret data, or the multi-bit flip-flops holding the private key of a cryptographic core. Using design information and logic simulation data, the list of security sensitive nets from the design are annotated by our flow and stimulated with a "direct vector control" file. This file is a set of vectors to iterate all possible combination of states for the list of sensitive nets. Such states are applied on the targeted gates of the design, and logically coherent states are propagated through the rest of the logic cores in our simulation engine. Further, to mimic the noise in the background of SoC chip, the remaining nets for security analysis are controlled with a vector-less approach to reduce computation overhead in million-cycle simulation, where a physically co-located group of nets will randomly switch according to a user-defined toggle rate. To realistically approximate the SNR of system-level power supply current, we also constrained the vector-less blocks with a power target for each cycle. There is non-correlated noise by the logic circuits auxiliary and peripheral to crypto cores in an SoC, which influences the SNR in the chip-level evaluation of SCLA. The full-chip power supply current simulation in this article essentially and efficiently involves both correlated and non-correlated gate activities with the use of DVC and vector-less control, respectively. The direct vector control file, together with cell liberty files, timing window file, and the power library files are used to generate the electrical model of the design. Every input plain payload only needs to simulate a few **point-of-interest (POI)** cycles (e.g., the last round of AES) to get the corresponding power noise waveforms for SCLA.

4 SILICON DESIGN FLOW AND EXAMPLE

4.1 Silicon Design Flow

The design flow of Figure 9 exploits the simulation-based power and EM SCLA, targeting the realization of a security-oriented SoC with cryptographic functionality. The proposed SCLA technique statistically estimates the potentiality of SC leakage with a large set of payloads input to cryptographic cores and also visualizes the distribution of SC leakage levels over a full chip area, which all help designers to finely tune physical layouts.

We assume that the RTL design is given by a trusted design team through architectural exploration of cryptographic hardware, and then proceeds to the logic and circuit-level design stage.

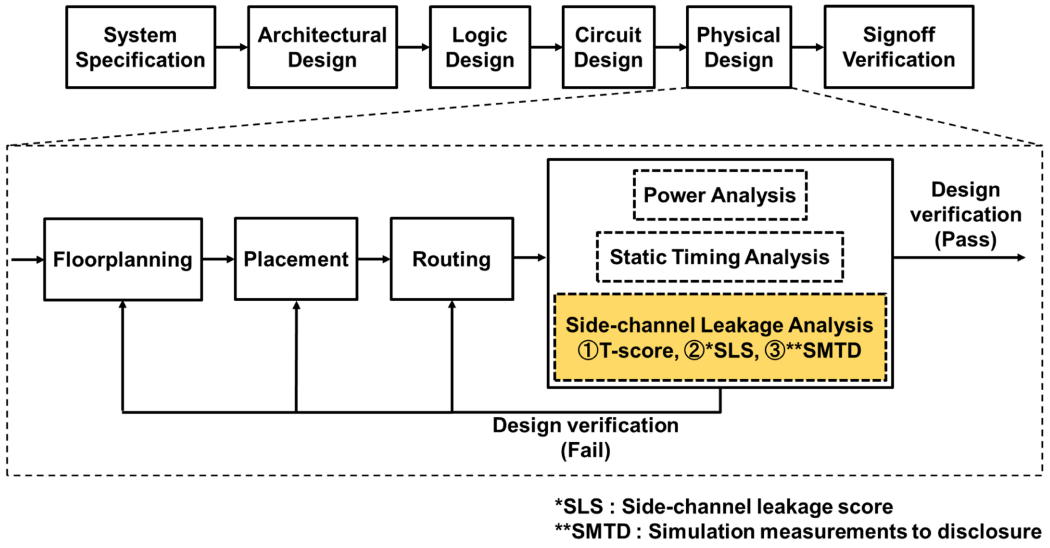


Fig. 9. Overview of general VLSI design flow and the position of our SCL simulation.

After the initial trial of full-chip physical implementation by **place-and-route (PNR)** and some physical rule checks, the first SCLA is applied on the design data. The results will be annotated to the design through another round of PNR with some intentional constraints and inclusion of additional devices, and then followed by the second or further SCLA. The iterations will be performed to the required level of SC leakage tolerance before the signoff verification stage.

The SCLA derives quantitative SC leakage metrics by processing a set of simulated power traces in respective analysis modes at every probe point designated in the full chip area. According to the security exploration sequence, we initially calculate T-score numbers at every probing points and scan the whole chip area to evaluate the possible presence of SC leakage. We then leverage the **SC leakage score (SLS)** and the **simulation measurements to disclosure (SMTD)** to deeply identify the root position of SC leakage with the assumption of SC leakage models tailored for a given crypto algorithm. The statistical analysis are not necessarily applicable to the simulation results with too small physical quantities (e.g., nA or nV), which are hidden by noise in actual measurements. Our simulation flow is able to perform noisy simulation as explained in Section 3.4, which approximates the practical leakages in the presence of noise in SoC, and thus we can apply these analysis modes in simulation. The analysis modes are defined as follows.

T-score

Welch's t-test is a hypothesis testing that determines if two populations are statistically different, and provides the statistical number, T-score, from the following Equation (5), where the traces in the first and second group of acquisition are represented by W_1 and W_2, with the size of N_1 and N_2, respectively:

$$\text{T-score} = \frac{\mu(W_1) - \mu(W_2)}{\sqrt{\frac{\sigma^2(W_1)}{N_1} + \frac{\sigma^2(W_2)}{N_2}}}. \tag{5}$$

There is a known SC analysis scheme of the **test vector leakage assessment (TVLA)** that is fully related with Welch's t-test [34, 35]. The measured or simulated traces are divided into two groups under some conditions. For example, the first one uses a fixed payload (plain text) that is given to a cryptographic core for every operation, while the second one assumes a different

payload randomly chosen for every operation. Statistical moments are considered insignificantly different among these two groups when T-score does not exceed the threshold value of 4.5. On the other hand, the correlation might exist between the intermediate state of cryptographic operation and power traces, when T-score is much higher than 4.5. Here, it is not necessary to mean that any secret information will be derived from the traces, while declaring the presence of correlation and the sensitivity to SC analysis. TVLA can be more sensitive than other assessment methods, and advantageous in investigating the existence of potential leakage sources for any kind of cryptographic algorithm. It is also noted that simulation excludes "white noise" unlike in measurements, thus the smaller number of traces in simulation reaches the certain confidence level of statistical significance that is comparable to measurements.

SC leakage score (SLS)

We have proposed SLS as a metric to measure the level of correlation between power supply currents and secret information. A white-box approach is taken in this analysis, where the SC leakage model is predefined with the design of cryptographic core data paths, according to the given cryptographic algorithm. A secret key is also known as a correct key in the analysis. An 8-bit number in a byte is chosen as a guessed value of subkey and calculated for its correlation coefficient against a given set of power supply current traces obtained by simulation or by measurements. This calculation is executed for every possible subkey value in a brute force manner. The SLS is then derived as the ratio between the correlation coefficient of the correct subkey to the maximum correlation coefficient among all subkey values as shown in Equation (6):

$$\mathrm{SLS} = \frac{\rho\left(X\{correct_{key}\}, Y\right)}{MAX\left[\rho\left(X\{key_{guess1}\}, Y\right), \rho\left(X\{key_{guess2}\}, Y\right), \ldots, \rho\left(X\{key_{guessN}\}, Y\right)\right]}. \tag{6}$$

The function X represents the leakage model on each guessed key, while Y represents the set of measured or simulated traces during cryptographic operation with a unique correct key. The correlation coefficient, ρ, between the guessed key and the traces is calculated according to Equation (7):

$$\rho(\mathrm{X}, \mathrm{Y}) = \frac{cov(X, Y)}{\sigma X \cdot \sigma Y}. \tag{7}$$

From the literature of CPA, given all possible key guesses, the predicted Hamming weight (or distance) of power model would result in the highest correlation with the key guesses matching the correct key. Here, we are normalizing the correlation coefficient to the correct key guess by using SLS. The trend of leakage level is visualized by SLS when the number of simulation traces increases, further, compared among different locations within an IC chip. The closer the value of SLS to 1, the higher the vulnerability detected. A designer can investigate the root location of SC leakage and then modify the physical layout of an IC chip under design.

Simulation measurements to disclosure (SMTD)

As the sign-off index verifying SC leakage, SMTD reveals the minimum number of traces to completely disclose all the subkey bytes in a secret key. Since the number of traces in SMTD can reach hundreds of thousands or even millions, the computational cost becomes too large in a general circuit-level simulation flow. Instead, the DVC technique (Section 3.4) only enables the simulation-based SC leakage sign off, by efficiently accelerating the simulation with the smallest compromise in accuracy.

In summary, these SCLA metrics are used in respective three design stages. (1) A crypto core will be evaluated with T-score in the initial step, with a certain number of simulation power traces. The potential vulnerability will be logically examined and then flagged for the further

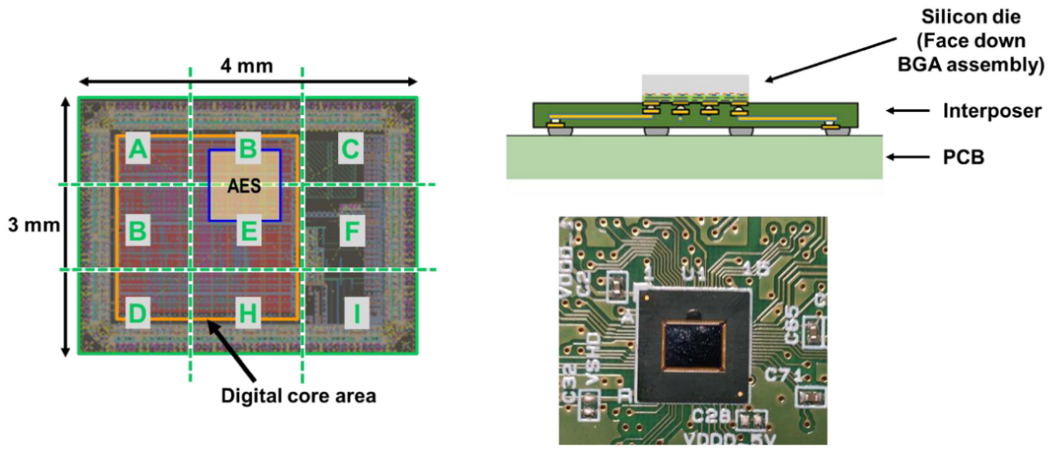


Fig. 10. Silicon example (chip layout, image of implementation, and photo of silicon example).

physical implementation, along with the definition of SC leakage models through such as power or EM correlation. (2) An IC chip layout with the crypto core will be then in-depth evaluated with SLS by assuming the correlation, with the incremental increase of simulation traces. The root positions of SC leakage will be examined and then eliminated or mitigated by means of physical design changes. (3) After the iteration of SLS exploration, the full IC chip layout will be verified with SMTD for SC leakage sign off. The number of simulation traces can be maximized in this stage. Even though our simulation flow is able to perform noisy simulation, the number of simulation traces required could be lower than that required in practice (e.g., SMTD could be lower than MTD). However, for the purpose of producing a heatmap to guide a designer to find vulnerable spots, this pessimistic condition stays meaningful.

4.2 Silicon Example and Measurement Setup

A test chip was developed in a 0.13 μm CMOS technology, and assembled on PCB in flip-chip BGA packaging (Figure 10). The chip is composed of AES circuits as well as additional digital circuits that control and interface to AES core, and thus resembles an SoC. The full-chip SCLA is tested both by simulation and measurements on an AES core with the key length of 128 bits (16 bytes). It is important to note that the backside surface of an IC chip is open for an adversary to access any place for SC leakage measurements, in particular for EM emission that is no longer shielded by metal layers stacked on the frontside. We are focusing on the backside EM SCLA of an IC chip in the following experiments.

The experimental setup is overviewed in Figure 11. An EM probe is precisely placed by a probe positioner, which is controlled by PC software in three-dimensional coordinates and also in the orientation with respect to the IC chip on the stage. The Si die with the thickness of 350 μm is flipped and electrically mounted on a plastic interposer, while its backside is not coated by any material such as resin. Since the probe coil is covered by plastic molding, the minimum probe height from the backside surface of the chip is offset by its thickness of 400 μm. The vertical distance of the backside EM probe coil to the frontside circuits is therefore effectively calculated to be 750 μm. Horizontally, the SCLA is performed on every probe position in the array of 3×3 locations and also on the probe orientation for magnetic fields in x and y axes. The labels defined in Figures 10 and 11, respectively, represent the probe positions from point A to point H as well as the probe orientations of Bx and By. These structural notations and quantities are consistent among measurement setups and simulation models, and associated parameters and costs are

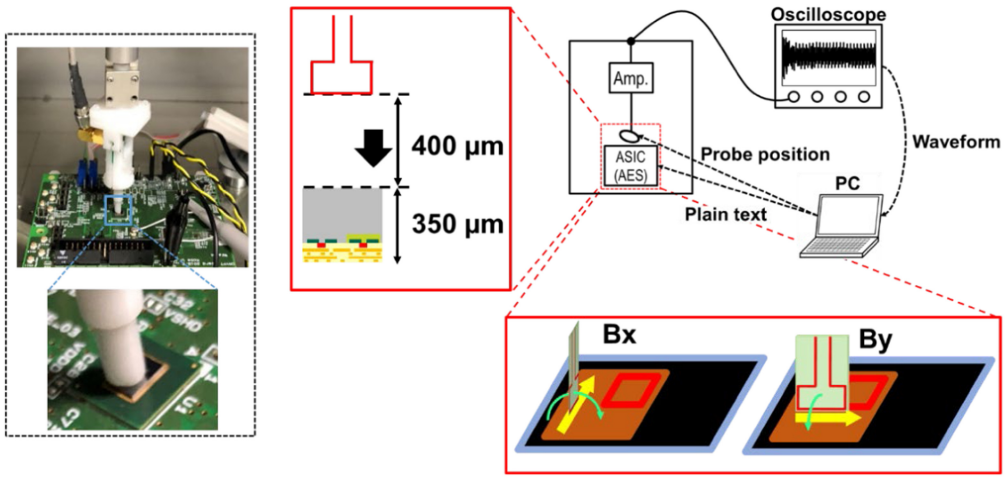


Fig. 11. Measurement setup.

Table 1. Summary of Measurement and Simulation Setup

	Simulation	Measurement
SC physical media	Power noise EM noise (Bx, By)	EM noise (Bx, By)
SC attack surface	Si die backside of BGA assembly	Si die backside of BGA assembly
Equipment	Server #CPU : 100 Memory(peak) : 7 GB (Intel Xeon Gold 6148 CPU @ 2.40 GHz)	Oscilloscope Analog sample rate : 20 GSa/sec PC system memory : 4 GB (Keysight MSO9404A)
Cost of time	Simulation time : 3 hours / 10K traces including ·1024 probe points × 2 probe orientation ·Power noise and EM noise → effective cost of time : 0.5 msec/wave	Measurement time : 198 hours / 10K traces including ·averaging 15 iterative measurements for 1 trace ·9 probe points × 2 probe orientation ·EM noise → effective cost of time : 4.0 sec/wave
Trace length	50 points × 0.59 ns/point → 29.5 ns/wave (focused on single round of interest)	15985 points × 0.025ns/point → 399.6 ns/wave (covering full rounds)
SC leakage analysis	Power noise : T-test, SLS, SMTD EM : T-test, SLS, SMTD	EM : T-test, SLS, SMTD

summarized in Table 1. By averaging 15 iterative measurements for a single trace in a measurement, we alleviate the influence of experimental noise. There are 1,024 virtual points evenly placed in simulation grids and compared to 9 probe points in measurements. The comparisons in this article were made for the magnetic fields in simulation and the induced electromotive forces by measurements. Their relation is generally expressed in the following equation with the probe calibration factor F involving the conductance and conversion of a given prove:

$$\mathrm{H\,[dB\ uA/m]} = \mathrm{V\,[dB\ uV]} + \mathrm{F\,[dB\ S/m]}. \tag{8}$$

Table 2. Comparison Table with Three Recent Works

	On-chip power current simulation method	EM noise calculation	Simulation technique for SCLA evaluation	Simulation cost
This Work	Simulation with cell-level current model	Theoretical equations	1. Identification of security-sensitive registers (section 3.2) 2. Intelligent probe generation flow (section 3.3) 3. Direct vector control (section 3.4)	0.54 sec/trace (1024 EM waves from 100K current probes)
[36]	Simulation with cell-level current model	Theoretical equations	-	0.72 sec/trace (30K power current probes)
[37]	Transistor level SPICE simulation	EM analysis tool	-	-
[38]	Transistor level SPICE simulation	Theoretical equations	1. Focused on target round 2. Node reduction	14.9 sec/trace (10201 EM waves from 798 current probes)

We here conclude from the linear relation of Equation (8) that the correlation can be evaluated for the simulated magnetic fields and the measured electromotive force with an EM probe having F.

The AES core in the IC chip has 800k instances and 3M node count with a single power domain. It is included in the full-chip level digital PNR along with some other digital blocks, however, mostly packed in the area over B and E regions. The clock frequency is 30 MHz and 50 sampling points per a clock period are analyzed. In simulation, VCD file contains 11M cycles of vectors for the testbench in the sequence of resetting, functional and IO activities. For SCLA purpose, we chopped the VCD file and stitched only the POI cycles for 10k input payloads. Besides, we leverage parallel processing to simulate side-channel traces by the time-chunking method. With 100 CPUs (Intel Xeon Gold 6148 CPU @ 2.40 GHz), the flow can finish simulating and analyzing both power noise and EM SC leakage of 10k traces at 1,024 virtual probes within about 3 h.

Our proposed simulation flow is compared with some recent works as in Table 2 [36–38]. Transistor-level SPICE is used for power current simulation in References [37, 38], that can be capable of solely evaluating a crypto core itself while difficult for full-chip level analysis once it is integrated on SoC. It is of interest in References [36, 37] that EM noise calculation is performed using the result coming from on-chip power current simulation, and then used for EM side-channel analysis. However, such the concatenating scheme works at the crypto core level. On the contrary, the simulation framework in this article unifies the power current simulation, the magnetic field calculation and SCLA in a single simulator kernel. This unification paves the way to realize the top-down cross-domain simulation approach that targets an SoC (Sections 3.1–3.4), featuring the logic-level tracking of security sensitive parts as well as the system-level location-dependent power and EM side-channel analyses. The highest simulation efficacy is then achieved in this work, as the simulation time of 0.5 s per a given plain text (a payload or a trace) for 1,024 EM waves calculated from 100K current probes internally to the AES core on an IC chip in assembly.

4.3 Silicon Results at Full System Level

We first evaluate the strength of EM emission both in simulation and measurements. Two-dimensional B field heatmaps in the area of BGA packaging interposer is shown in Figure 12.

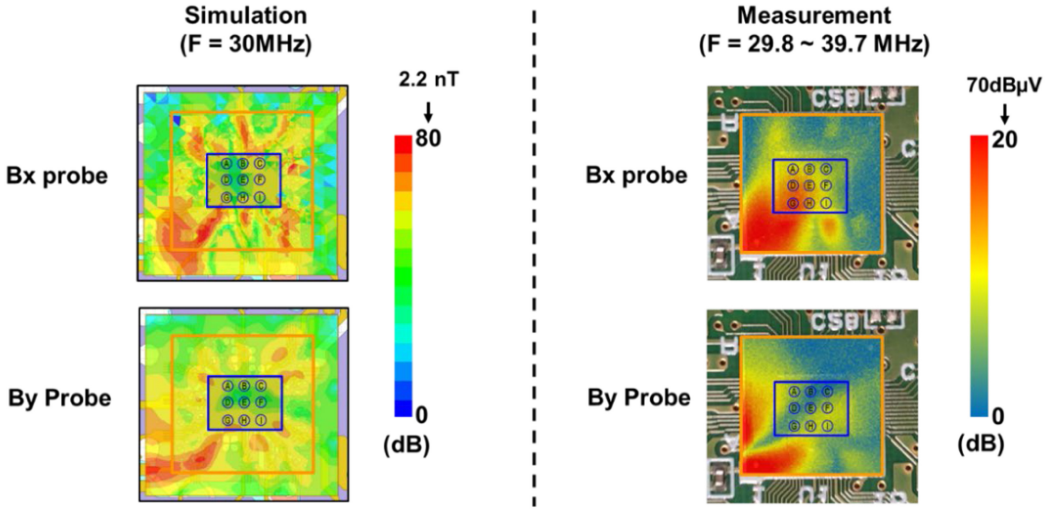


Fig. 12. Heatmap of CPS board level EM emission.

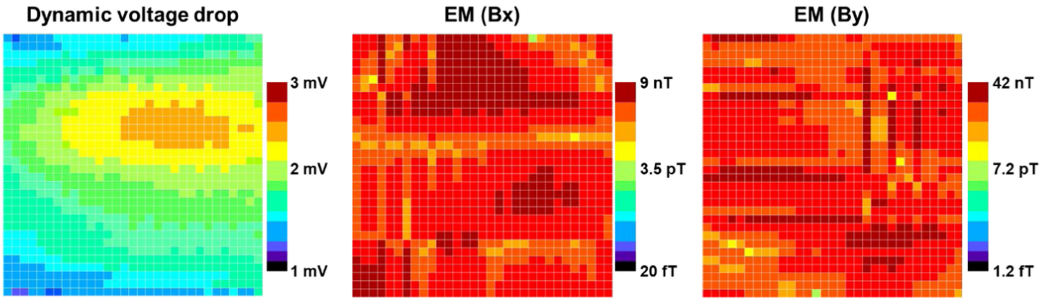


Fig. 13. On-chip heatmap of on-chip dynamic voltage drop and near-field EM emission.

The frequency components at the clock frequency of 30 MHz given to the AES core are compared for the simulated B field and the measured voltage. In simulation, the CPS model including CPM of AES core and IO cells produces the near-field EM emission. In measurements, an EM probe is scanned over the packaging area and measuring magnetic fields during AES operation. The voltage induced on the coil of EM probe is multiplied with the system gain dominated by the coupling coefficient, the conversion coefficient and the gain of a preamplifier as well as an oscilloscope. It is shown that the points of significance for EM emission are almost consistent among simulation and measurements, as observed in both heatmaps, which qualitatively proves the directivity and location dependency of the EM emission analysis in close combination with the power supply current modeling. In this figure, we show results in the frequency domain, though the time domain waveforms are also important for SCAs. This is because the time domain waveforms necessarily involve frequency region of interest typically from DC to a few GHz. We claim here that there are agreements between EM emission by the simulation with a CPS board model and that by the near-field EM measurements.

Next, on-chip heatmaps are simulated as in Figure 13 for the **dynamic voltage drop (DVD)** and near-field EM emission within the die area. DVD hot spots are very constraint within the placement area of AES core. In contrast, EM maps look spread and flattened, and exhibit no

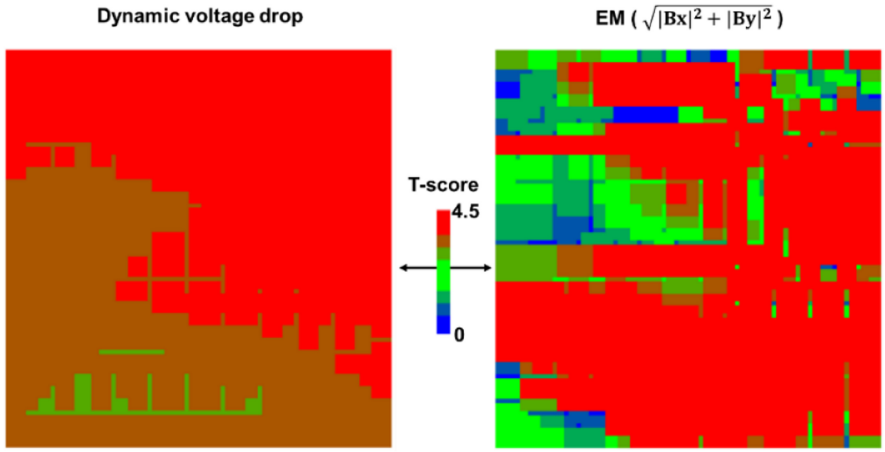


Fig. 14. T-score heatmap of power-noise (left) and EM (right) SCLA with violation locations in red hotspots.

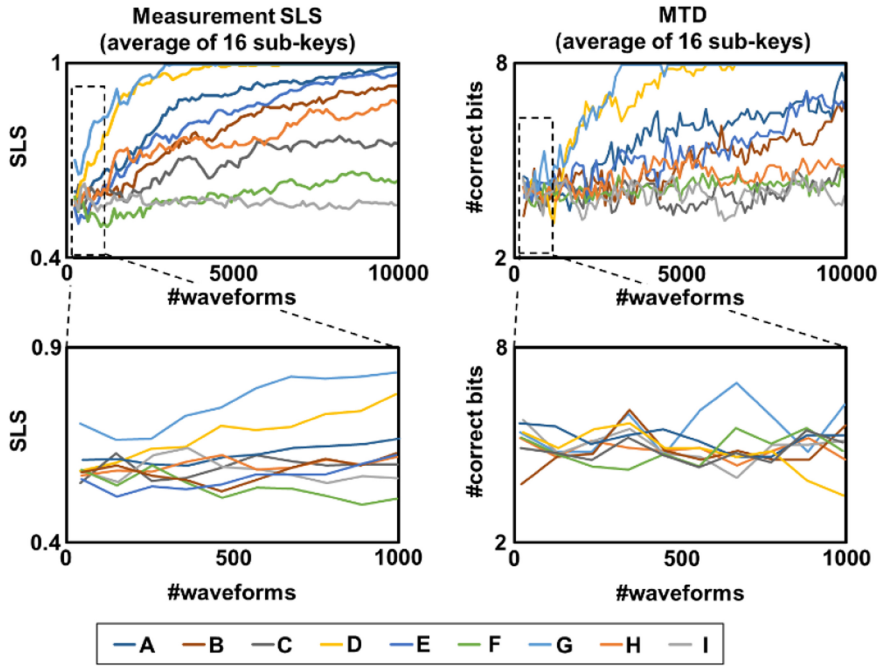


Fig. 15. Comparison of two SCLA technique's feature.

specific area correspondence to the core. This comes naturally from the fact that EM emission is induced by power supply current that is distributed over the chip and system PDNs. Here, we observe that the full-system level modeling and associated solver capacity is demanded for the quantitatively simulation of IC-chip power noise and EM emission for **power integrity (PI)** and **EM compatibility (EMC)** analysis, respectively. On the one hand, power and EM SCLA requires more logic content-oriented modeling while, on the other hand, it can be constraint within a die area, as will be discussed in the following subsection.

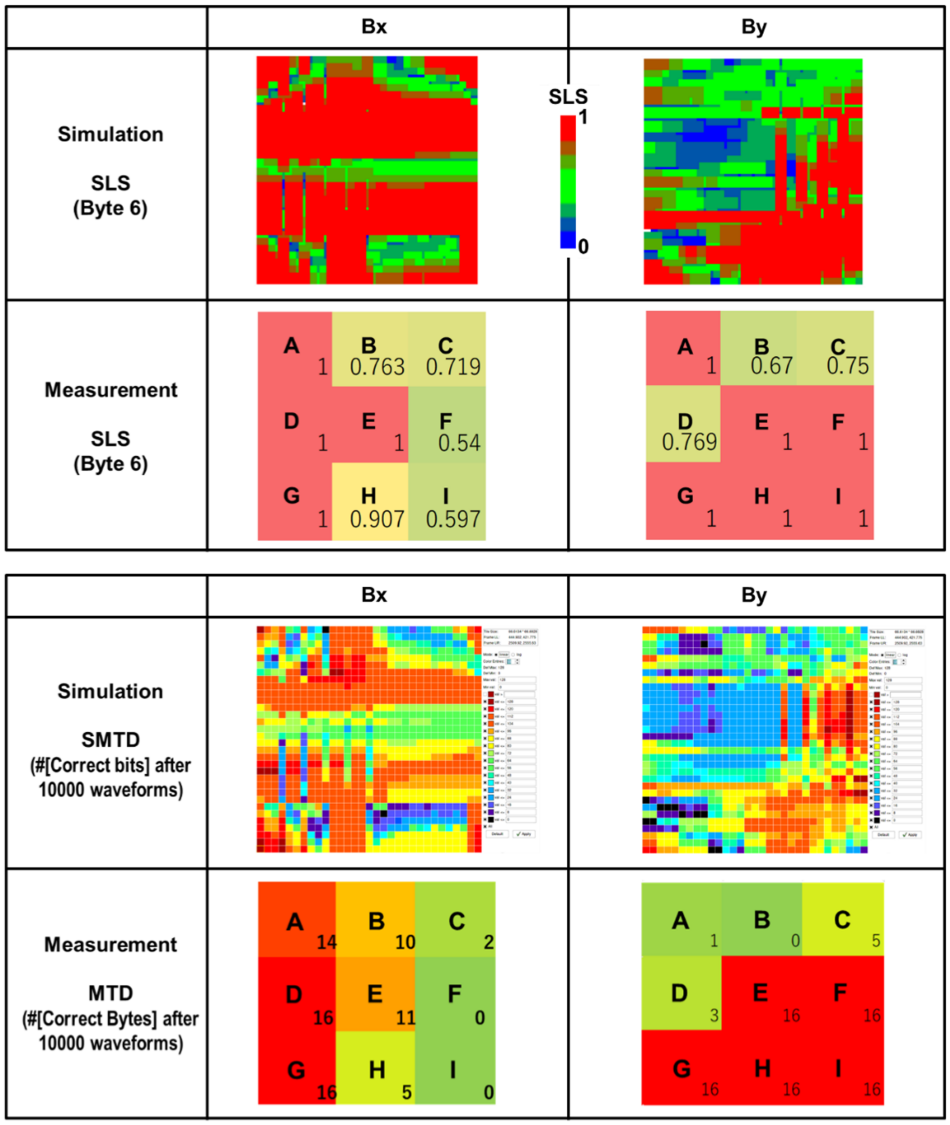


Fig. 16. Comparison of two simulation results and measurement result.

4.4 Silicon Results at IC Chip Level

The SCLA simulation is evaluated with the test chip. The T-score heatmap by simulation for power noise and EM traces are shown in Figure 14. There are huge physical areas of potentially high leakage where T-score exceeds 4.5 at each position of analysis. This leads to designer's consciousness for potential SC leakage.

We apply SLS for the detection of EM SC leakages within the die area of the test chip, as shown in Figure 15. The general trend of correlation-based leakage is revealed in the plot of SLS with respect to the number of EM traces and compared among the 9 different probe locations. The SLS is calculated for each subkey byte according to Equation (3) and then averaged over the 16 bytes. In contrast, the MTD plots absolutely manifests the full 8-bit correct subkey disclosures

at some locations, however, its number in the vertical axis of smaller than 8.0 (except for 0.0) is less meaningful, since it includes false positive bits indistinguishable from the disclosed bits. In addition, the trend of SLS is recognizable even with the smaller number of traces, which is useful for the detection of SC leakage.

These results suggest the importance of EM SCLA simulation flow. The near-field EM SCLA with the metric of SLS and MTD are compared among simulation and measurements, as shown in Figure 16. The magnetic field traces captured in Bx and By directions are used for the analysis, respectively, where their directivity proves the proper treatment of near-field EM radiations. The number of traces up to 10k reveal the full 128-bit correct key through the EM SC leakage. The simulated location dependency well match measurements, if we see the high SC leakage areas among points A, D, and G for Bx and also the points E, F, G, H, I for By. In the contrary, the low leakage is clearer in By direction in the upper area of the die, as simulated in points A, B and C. While there are imperfect correspondence due probably mainly to the position variations in our measurements, the general sketches are nicely reproduced by the simulation-based EM SCLA.

5 CONCLUSION AND FUTURE WORK

Simulation-based power and EM SCLA techniques are proposed and demonstrated with a 0.13 μm AES IC chip in flip-chip packaging and system-level assembly. The backside of Si die is treated as the EM emission surface. On-chip dynamic power noise and near-field EM emission are finely simulated with chip-level power supply current and system-level PDN models. Power and EM SC leakages are efficiently analyzed for 1,024 EM waves from 100k on-chip virtual current probes with 10k input payloads, and the SC metrics of t-score, side-channel leakage score, and measurements to disclosure are evaluated. Silicon measurements and simulation are well correlated for the backside EM SC leakage in the exploration of location- and direction-dependent EM SC leakage in an IC chip. The design flow of an IC chip deploys the proposed simulation-based SCLA for the exploration of SC attack resiliency and SC leakage sign off. The future works include the actual implementation of secure IC chips through the design flow and the evaluation of high SC leakage mitigation by countermeasures.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun. 1999. Differential power analysis. In *Proceedings of the Annual International Cryptology Conference*. Springer, 388–397.

[2] Eric Brier, Christophe Clavier, and Francis Olivier. 2004. Correlation power analysis with a leakage model. In *Cryptographic Hardware and Embedded Systems*, MarcJoye and Jean-Jacques Quisquater (Eds.). Springer, 16–29.

[3] K. Gandolfi, C. Mourtel, and F. Olivier. 2001. Electromagnetic analysis: Concrete results. In *Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES'01)*. Springer, 251–261.

[4] J. Quisquater and D. Samyde. 2001. Electromagnetic analysis (EMA): Measures and counter-measures for smart cards. In *Proceedings of the International Conference on Research in Smart Cards (E-smart'01)*. Springer, 200–210.

[5] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi. 2002. The EM side-channel(s). *Cryptogr. Hardw. Embed. Syst., Lecture Notes Comput. Sci.* 2523 (2002), 29—45.

[6] D. Réal, F. Valette, and M. Drissi. 2009. Enhancing correlation electromagnetic attack using planar near-field cartography. In *Proceedings of the Design, Automation, and Test in Europe (DATE'09)*, 628–633.

[7] E. Peeters, X. Standaert, and J. Quisquater. 2007. Power and electromagnetic analysis: Improved model, consequences and comparisons. *VLSI J. Integr.* 40, 1 (2007), 52—60.

[8] K. Tiri and I. Verbauwhede. 2004. A logic level design methodology for a secure DPA resistant asic or fpga implementation. In *Proceedings of the IEEE Design, Automation, and Test in Europe (DATE'04)*. 246–251.

[9] C. Tokunaga and D. Blaauw. 2010. Securing encryption systems with a switched capacitor current equalizer. *IEEE J. Solid-State Circ.* 45, 1 (2010), 23—31.

[10] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi. 1999. Towards sound approaches to counteract power-analysis attacks. In *Proceedings of the Conference on Advances in Cryptology (CRYPTO'99)*. Springer, 398—412.

[11] L. Goubin and J. Patarin. 1999. DES and differential power analysis the "duplication" method. In *Proceedings of the Conference on Cryptographic Hardware and Embedded Systems (CHES'99)*. Springer, Berlin. https://doi.org/10.1007/3-540-48059-5_15

[12] S. Nikova, C. Rechberger, and V. Rijmen. 2006. Threshold implementations against side-channel attacks and glitches. In *Information and Communications Security,* P. Ning, S. Qing, and N. Li, (Eds.). Springer, Berlin, 529–545.

[13] H. Gross, S. Mangard, and T. Korak. 2016. Domain-oriented masking: Compact masked hardware implementations with arbitrary protection order. *Cryptology ePrint Archive*, Report 2016/486. Retrieved from http://eprint.iacr.org/2016/486.

[14] Shivam Bhasin, Jean-Luc Danger, Tarik Graba, Yves Mathieu, Daisuke Fujimoto, and Makoto Nagata. 2014. Physical security evaluation at an early design-phase: A side-channel aware simulation methodology. In *Proceedings of the Conference on Engineering Simulations for Cyber-Physical Systems (ES4CPS'14)*. ACM.

[15] Dina Kamel, Mathieu Renauld, Denis Flandre, and Francois-Xavier Standaert. 2014. Understanding the limitations and improving the relevance of SPICE simulations in side-channel security evaluations. *J. Cryptogr. Eng.* 4, 3 (2014), 187–195.

[16] Francesco Regazzoni, Thomas Eisenbarth, Axel Poschmann, Johann Groschadl, Frank K. Gurkaynak, Marco Macchetti, Zeynep Toprak Deniz, Laura Pozzi, Christof Paar, Yusuf Leblebici, and Paolo Ienne. 2009. Evaluating resistance of MCML technology to power analysis attacks using a simulation-based methodology. *Trans. Comput. Sci. IV, Special Issue Secur. Comput.* 4 (2009), 230–243.

[17] Kris Tiri and Ingrid Verbauwhede. 2005. Simulation models for side-channel information leaks. In *Proceedings of the Design Automation Conference (DAC'05)*. ACM, 228–233.

[18] D. Šijačić, J. Balasch, and I. Verbauwhede. 2020. Sweeping for leakage in masked circuit layouts. In *Proceedings of the Design, Automation and Test in Europe Conference and Exhibition (DATE'20)*. IEEE, 915–920.

[19] D. Šijačić, J. Balasch, B. Yang, S. Ghosh, and I. Verbauwhede. 2020. Towards efficient and automated side- channel evaluations at design time. *Journal of Cryptographic Engineering* 10 (2020), 305–319. https:// doi.org/10.1007/s13389-020-00233-8

[20] A. Tsukioka, K. Srinivasan, S. Wan, L. Lin, Y.-S. Li, N. Chang, and M. Nagata. 2020. A fast side-channel leakage simulation technique based on IC chip power modeling. *IEEE Lett. Electromag. Compat. Pract. Appl.* 1, 4 (2020), 83–87.

[21] J. Knechtel, E. B. Kavun, F. Regazzoni, A. Heuser, A. Chattopadhyay, D. Mukhopad- hyay, S. Dey, Y. Fei, Y. Belenky, I. Levi, et al. 2020. Towards secure composition of integrated circuits and electronic systems: On the role of EDA. In *Proceedings of the Design, Automation, and Test in Europe (DATE'20).*

[22] Francesco Regazzoni, Alessandro Cevrero, Francois-Xavier Standaert, Stephane Badel, Theo Kluter, Philip Brisk, Yusuf Leblebici, and Paolo Ienne. 2009. A design flow and evaluation framework for dpa-resistant instruction set extensions. In *Proceedings of the Conference on Cryptographic Hardware and Embedded Systems (CHES'09)*. Springer, 205–219.

[23] L. Lin, Dinesh Selvakumaran, Deqi Zhu, Norman Chang, Calvin Chow, Makoto Nagata, and Kazuki Monta. 2020. Fast and comprehensive simulation methodology for layout-based power-noise side-channel leakage analysis. In *Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES'20)*, 133–138. DOI: 10.1109/iSES50453.2020.00038

[24] Lang Lin, Deqi Zhu, Jimin Wen, Hua Chen, Yu Lu, Norman Chang, Calvin Chow, Harsh Shrivastav, Chia-Wei Chen, Kazuki Monta, and Makoto Nagata. 2021. Multiphysics simulation of EM side-channels from silicon backside with ML-based auto-POI Identification. In *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST'21).*

[25] Shen Lin et al. 2004. Full-chip vectorless dynamic power integrity analysis and verification against 100uV/100ps-resolution measurement. In *Proceedings of the IEEE Custom Integrated Circuits Conference*, 509–512. DOI: 10.1109/CICC.2004.1358869

[26] Ansys RedHawk-SC Digital Power Integrity Signoff. 2022. Retrieved from https://www.ansys.com/ja-jp/products/semiconductors/ansys-redhawk-sc.

[27] L. Lin, D. Selvakumaran, D. Zhu, N. Chang, C. Chow, M. Nagata, and K. Monta. 2020. Fast and comprehensive simulation methodology for layout-based power-noise side-channel leakage analysis. In *Proceedings of the IEEE International Symposium on Smart Electronic Systems*, 144–149.

[28] Z. Yu, J. Koo, J. A. Mix, K. Slattery, and J. Fan. 2010. Extracting physical IC models using near-field scanning. In *Proceedings of the IEEE International Symposium on Electromagnetic Compatibility (EMC'10)*, 317–320.

[29] Z. Yu, J. A. Mix, S. Sajuyigbe, K. P. Slattery, and J. Fan. 2013. An improved dipole-moment model based on near-field scanning for characterizing near-field coupling and far-field radiation from an IC. *IEEE Trans. Electromag. Compat.* 55, 1 (2013), 97–108, DOI: 10.1109/TEMC.2012.2207726

[30] Y. Vives-Gilabert, C. Arcambal, A. Louis, F. de Daran, P. Eudeline, and B. Mazari. 2007. Modeling magnetic radiations of electronic circuits using near-field scanning method. *IEEE Trans. Electromag. Compat.* 49, 2 (2007), 391–400. DOI: 10.1109/TEMC.2006.890168

[31] D. Baudry, C. Arcambal, A. Louis, B. Mazari, and P. Eudeline. 2007. Applications of the near-field techniques in EMC Investigations. *IEEE Trans. Electromag. Compat.* 49, 3 (2007), 485–493. DOI: 10.1109/TEMC.2007.902194

[32] A. Nahiyan, J. Park, M. He, Y. Iskander, F. Farahmandi, D. Forte, and M. Tehranipoor. 2020. Script: A cad framework for power side-channel vulnerability assessment using information flow tracking and pattern generation. *ACM Trans. Des. Autom. Electron. Syst.* 25, 3 (2020). https://doi.org/10.1145/3383445

[33] W. Hu, D. Mu, J. Oberg, B. Mao, M. Tiwari, T. Sherwood, and R. Kastner. 2014. Gate-level information flow tracking for security lattices. *ACM Trans. Des. Autom. Electron. Syst.* 20, 1 (2014), 1–25.

[34] J. Cooper, E. DeMulder, G. Goodwill, J. Jaffe, G. Kenworthy, and P. Rohatgi. 2013. Test vector leakage assessment (TVLA) methodology in practice. In *Proceedings of the International Cryptographic Module Conference.*

[35] G. Goodwill, B. Jun, J. Jaffe, and P. Rohatgi. 2011. A testing methodology for side-channel resistance validation. In *Proceedings of the NIST Non-Invasive Attack Testing Workshop.*

[36] D. Poggi, T. Ordas, A. Sarafianos, and P. Maurine. 2022. Checking robustness against EM side-channel attacks prior to manufacturing. *IEEE Trans. Comput.-Aided Design Integr. Circ. Syst.* 41, 5 (2022), 1264–1275. DOI: 10.1109/TCAD.2021.3092297

[37] D. Das, et al. 2022. EM SCA white-box analysis-based reduced leakage cell design and pre-silicon evaluation. *IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems* 41, 11 (2022), 4927–4938. DOI: 10.1109/TCAD.2022.3144369

[38] A. Kumar, C. Scarborough, A. Yilmaz, and M. Orshansky. 2017. Efficient simulation of EM side-channel attack resilience. *In Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 123–130. DOI: 10.1109/ICCAD.2017.8203769

Received 15 December 2021; revised 10 October 2022; accepted 13 October 2022