# Photon Emission Modeling and Machine-Learning Assisted Pre-Silicon Optical Side-channel Simulation

Henian Li[1], Lang Lin[2], Norman Chang[2], Sreeja Chowdhury[2], Dylan Mcguire[2], Bozidar Novakovic[2], Kazuki Monta[3], Makoto Nagata[3], Ying-Shiun Li[2], Pramod M S[2], Piin-Chen Yeh[4], J.-S. Roger Jang[4], Chengjie Xi[1], Qiutong Jin[5], Navid Asadi[1], Mark Tehranipoor[1]
[1]University of Florida, {henian.li, chengjiexi}@ufl.edu, {nasadi, tehranipoor}@ece.ufl.edu
[2]Ansys, Inc., {firstname.lastname}@ansys.com
[3]Kobe University, kazuki.monta@it1.stin.kobe-u.ac.jp, nagata@cs.kobe-u.ac.jp
[4]National Taiwan University, r10946019@ntu.edu.tw, jang@csie.ntu.edu.tw
[5]University of California, Berkeley, qiutong-jin@berkeley.edu

***Abstract*—Optical side-channel analysis poses a significant threat to the security of integrated circuits (ICs) by enabling the disclosure of secret data, such as encryption keys. In this paper, for the first time, we present a multiphysics simulation framework of optical side-channel analysis from the layout database of a fabricated testchip. By leveraging accurate device models and electro-photonic physics, our framework models the photon emission behavior in ICs and enables the statistical correlation of emitted photon patterns with secret keys. Our framework enhances understanding of layout-level optical side-channel leakage and its implications, enabling IC designers to assess the risks associated with optical side-channel attacks and develop efficient countermeasures at the pre-silicon stage.**

***Index Terms*—Optical side-channel analysis, security key disclosure, layout-level analysis, photon emission modeling and simulation, machine learning, hardware security**

## I. Introduction

Side-channel information leakage [1] poses one of the most critical physical threats toward the security of generic hardware implementations of crypto cores and crypto primitives. Side-channel leakages including timing [1], power consumptions and noises [2], [3], electromagnetic emissions [4], and thermal emissions [5] are widely used to analyze and extract sensitive information from designs. Photon emissions, as a category of non-electromagnetic side-channels [6], is produced to facilitate side-channel analysis (SCA) in 2008 [7], optical SCA is recognized as a powerful category of cracking the crypto implementations and extracting the security assets (sensitive data, secret keys, etc.) from modern SoCs by observing photon emission patterns. Therefore, design verifications for optical side-channel leakages are critical to ensure a security-proven sign-off of secure and trustworthy ICs.

To counter the urgency of hardware security vulnerabilities, a critical gap exists in the absence of pre-silicon simulation methodologies for optical side-channel analysis. Addressing this, a simulation approach is needed that accurately models NMOS channel currents, integrates electro-photonic physics for photon emission simulation, and employs sophisticated postprocessing for data disclosure amidst design complexity, revealing insights into IC security under optical side-channel attack threats.

**Contributions:** To the best of our knowledge, this is the first work in literature that unravels these intricacies. In this work, we present a multiphysics simulation framework of optical SCA at the layout level. Our contributions include:

- We applied multiphysics transistor-level dynamic IR drop methodology and accurate photon emission modeling to derive the photon emission image of ICs at the pre-silicon stage.
- We performed correlation-based optical SCA at the pre-silicon stage, covering white-, grey-, and black-box attack scenarios.
- We developed tile-based segmentations for the photon emission map and built Machine Learning (ML) models for key-extraction optimizations.

## II. Background

### A. Photon Emissions in CMOS

Photon emissions within CMOS devices, notably more pronounced in the NMOS as compared to the PMOS counterparts, are attributed to several intrinsic factors such as electrons' higher mobility, larger currents, and favorable energy levels in the conduction band. Primarily, during the process of logic switching, the NMOS transistor emits photons most notably within its saturation region [8], [9]. The emitted photons bear a direct correlation to the level of device activity (e.g., the density of the channel current), providing a tangible representation of the operational dynamics. Notably, These photons can be effectively detected from chips' backside [10], [11] by specialized sensors, which are often integrated into emission microscopes such as the PHEMOS-1000 [12].

### B. Optical Side-Channel Attacks

Optical side-channel attacks, a significant concern in hardware security, capitalize on the inadvertent emission of light during the operation of integrated circuits (e.g., cryptographic operations). During the attack procedure, adversaries measure the emitted photons produced by the execution of cryptographic tasks, aiming to extract sensitive data like secret encryption keys. Optical SCA is classified based on different methodologies: simple photonic emission analysis (SPEA) [13], differen-

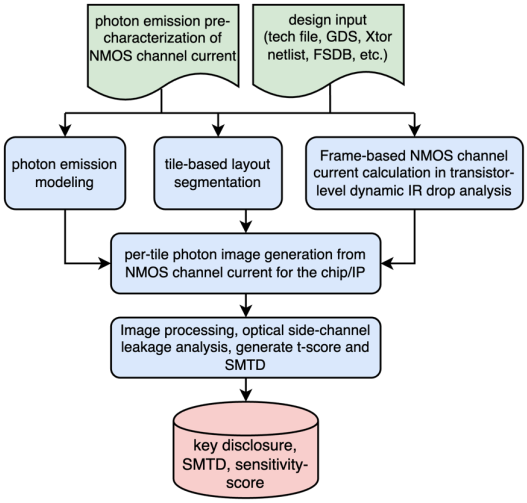



Fig. 1: Overall framework for pre-silicon optical side-channel leakage analysis.

tial photonic emission analysis (DPEA) [14], and correlation-based photon emission analysis (CPEA) [15]. The side-channel analysis in this paper is based on CPEA, which leverages correlation coefficients to quantify the correlation between predicted values and the actual photon emissions. To mitigate the side-channel concerns and ensure robust protections, thorough assessments and effective countermeasures at the design stage are essential.

### C. Related Work

There is a handful of work has been done on simulating the photon emission intensity at the pre-silicon stage. Existing work either *1)* utilizes a numerical approach to estimate the probability of photon emission and its intensity as *traces* input [16]–[18] based on circuits' logic behavior at RTL/gate-level, or *2)* utilizes a simpler model such as Hamming Weight (HW) model [15] for such estimation. However, none of them considers physical information and we propose the first photon emission behavior-based multiphysics simulation.

## III. Pre-Silicon Optical Side-Channel Simulation

### A. Threat Model

In this paper, we assume black-box and white-/grey-box attack scenarios on 16 bytes of AES-128 Sbox. While the white-/grey-box scenario assumes all/partial knowledge of the AES design details, the black-box scenario assumes only the physical access to the chip, e.g., after necessary polishing and thinning of the chip (assuming flip-chip packaging), a black-box attacker would need to scan through the entire layout, combine all the pieces of photon emission pictures taken, and obtain a comprehensive photon image to proceed with the optical side-channel leakage analysis. Note that even though the design is always a white-/grey-box to the designer, all scenarios are necessary for security assessments from the attacker's view to ensure effective protection.

### B. Proposed Framework

**Summary:** Our framework, depicted in Fig. 1, initiates with the simulation of NMOS device channel currents through a Fast Signal Database (FSDB) vector stimulus sourced from security encryption processes. Photon emission behavior, modeled from pre-characterized device curves, then simulates photon images based on the given pixel size. By segmenting the photon image into tiles with different sizing plans across two threat models, we perform correlation-based key disclosure analysis.

**Transistor-Level Dynamic IR Drop Analysis:** We exploit post-layout transistor-level dynamic IR drop analysis and then extract the vector-based transistor current profile [19]. Further, fast transient simulations can be done by combining the electrical model and physical model of the circuit under test.

**Photon Emission Modeling:** We model the drain current-dependent NMOS photon emission rate based on the theory of hot carrier scattering in the conduction band due to bremsstrahlung (braking radiation) as proposed in [20], which is an intraband process. While there is disagreement regarding the specific intraband process that dominates photon emission [21]–[23], studies of silicon MOSFETs strongly suggest that the measured photon emission spectra cannot be adequately explained by interband processes (e.g. direct c-v transitions) [22]. Starting with a conduction band electron accelerated by a field $E_x$, the probability that it obtains kinetic energy $U$ over mean free path $\lambda$ is formulated assuming a Maxwell-Boltzmann distribution [24]. The overall rate of photon emission is related to the number of electrons arriving at the high-field region, which is proportional to the drain current.

Since this paper's scope falls in emission intensities between similar transistors at equivalent operating points, we make additional assumptions of an ideal PN junction model with reasonable channel and drain doping to estimate the maximum electric field magnitude and gradient, we then conclude that the maximum electric field $E_m$ is on the order of $10^5$ V/cm, and the E-field gradient can be expressed as in Equation 1 below.

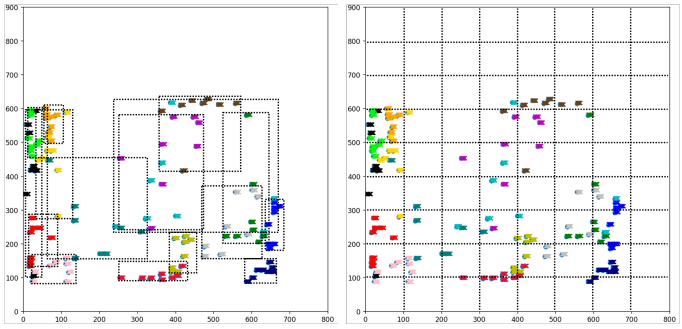
$$\frac{dE_x}{dx} \simeq \frac{E_m}{W_j} \tag{1}$$

where $W_j$ is the width of the depleted region in the channel. The expression for the energy-integrated photon emission rate is then shown in Equation 2.

$$I_{\nu_0,\infty}(I_{DS}) = 6.7 \times 10^{-22}[J \cdot S \cdot C^{-1}] I_{DS} \frac{qN_C}{m^*} \frac{q\lambda E_m W_j}{E_g} \cdot \frac{a}{\nu_0} e^{-(E_g+b)/qE_m\lambda}[s^{-1}] \tag{2}$$

where $I_{DS}$ is the drain current; $N_C$ is the impurity density; $m^*$ the electron effective mass; $\lambda$ the mean free path; $E_m$ the maximum electric field intensity in the channel; $E_g$ and $\nu_0$ the band gap energy and frequency, respectively; $a$ and $b$ are constants [20].

**Tile-Based Photon Emission Map:** For multiphysics simulations at the layout level, it is not feasible to include all the details from a complex design at extremely small scales (e.g., $< 1\mu m$) [5] due to the limitation of pre-silicon simulation cost



(a) (b)

Fig. 2: Schematic representations of two tile-based layout segmentations: (a) byte boundary-based tile sizing when POIs are known, and (b) uniform tile sizing (example tile size $100\mu m \times 100\mu m$) assuming black-box attackers. Various colors depict distinct Sbox bytes.

or physical detectors' resolutions. In this context, the design is partitioned into discrete pixels or clusters of pixels within proximity (i.e., tiles). Each pixel or tile can be harnessed to extract a localized photon emission pattern, facilitating subsequent side-channel analysis. In this work, based on real-life devices' specifications [25], we choose $10\mu m \times 10\mu m$ as the pixel size and apply various pixel clustering plans to form tiles, while they remain configurable to users.

As shown in Fig. 2, tiles can be separately chosen for certain areas or evenly distributed with a uniform size under different circumstances. For white-/grey-box cases, the attacker can attempt to crack the sensitivity bytes individually or at least start by focusing on known localized areas/point-of-interests(POIs). Hence, we create tiles based on pixel clusters included in POI(e.g., byte instances) boundaries and proceed with side-channel analysis.

In black-box cases, image pieces (tiles) are evenly scanned from the entire layout or a roughly chosen big area and then combined into a whole picture. In this paper, we implement the proposed flow with the capability of sweeping the uniform tile sizing with a given range, we have the tile width $W_i \in \{80\mu m, 100\mu m, 120\mu m, ..., 400\mu m\}$ while height $H_i \in \{90\mu m, 110\mu m, 130\mu m, ..., 450\mu m\}$, thus, there are $20 \times 18 = 323$ combinations of sizing, where each plan has a different total amount of tiles.

**Layout-Level CPEA:** We apply 3000 plaintexts on AES-128 encryption, thus, for each tile based on 3000 simulated photon emission images, we attempt to correlate the tile-based lossless-extracted emission intensities with the Hamming Weight (HW) or Hamming Distance (HD) models of 16 bytes of AES-128 $10^{th}$ round AES-128 *SubBytes* output.

The design's optical side-channel vulnerability is evaluated through four metrics for each AES Sbox byte: *disclosed_byte_amount*, *simulation measurement-to-disclosure (SMTD)* for location dependency evaluation [26], *sensitivity_score* for each byte to evaluate its leakage level [26], and *mean_score* calculated from all 16 bytes' sensitivity scores to represent an overall leakage level. The metric *sensitivity_score* is calculated from Equation 3 [26]:

$$sensitivity\_score = \frac{2 - \frac{rank}{256} - \frac{N_{effective\_trace}}{N_{total\_trace}}}{2} \quad (3)$$

where *rank* is based on the ranking of the correct key at the end of analysis. A *sensitivity_score* $\geq 0.5$ means full-key disclosure of the design under assessment. If partial key bytes are disclosed due to countermeasures, the score is in a range of $[0, 0.5)$.

### C. ML Approaches for Model Optimization

In the context of uniform tile sizing (black-box), determining the optimal tile size for effective disclosures is challenging due to impracticalities in finely sweeping various tile sizes for multiple experiments, particularly within a large layout. To address this, we automated the entire flow and integrated machine learning (ML) approaches [27]. Our ML workflow predicts experimental results based on four metrics (Section III-B), explores optimal tile sizes, and provides visualizations for vulnerability assessment. Leveraging the adaptive meta-model of optimal prognosis (AMOP) and an evolutionary algorithm (EA), our approach dynamically refines the design space, progressing through stages of initialization, evaluation, termination, selection, and variation [28]. Sensitivity analysis, an essential part of the optimization process, involves establishing a dynamic meta-model and iterative refining using techniques like anisotropic Kriging and linear/quadratic fitting. The optimized meta-model's predictive accuracy is quantitatively evaluated using the coefficient of prognosis (CoP) [29] calculated by Equation 4:

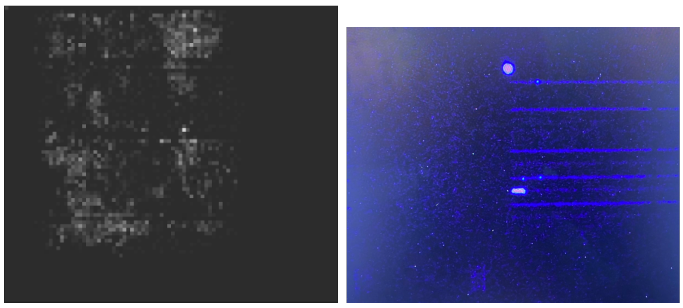
$$CoP = 1 - \frac{SS_E^{Prediction}}{SS_T} \quad (4)$$

where $SS_T$ is the total variation and $SS_E^{Prediction}$ is the sum of squared prediction errors. The closer CoP is to 1, the better accuracy the meta-model possesses.

## IV. Experimental Results on AES-128

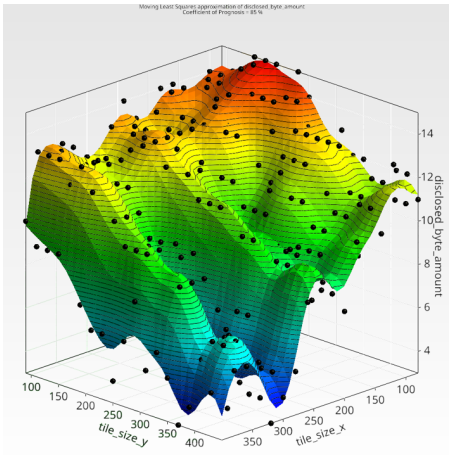
### A. Experimental Setup

We performed our layout-level experiments on an $800\mu m \times 900\mu m$ AES-128 implementation [26], [30]. Targeting 16 Sbox bytes at the $10^{th}$ round, we first simulate 3000 photon emission images from 3000 plaintexts based on $10\mu m \times 10\mu m$ pixel, and derive tile-based *traces* differently. For the white-/grey-box scenario, our *traces* are from 16 bytes' bounding box area.



(a) (b)

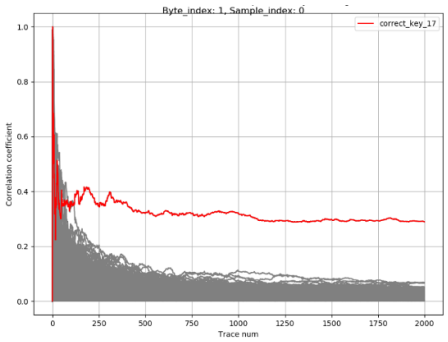
Fig. 3: (a) Simulated photon emission image vs. (b) real-life image example captured by PHEMOS-1000 [12].




(a)

```
#byte_index disclosed disclosed_probes_num
top_correlated_probe_name top_correlated_sample_index
top_correlation_coefficient effective_trace_num
effective_probe_name sensitivity_score
sidechannel_leakage_score
0 True 2 probe9_0 0 0.2012 207 probe9_0 0.9655 1.0000
1 True 3 probe1_0 0 0.1176 683 probe1_0 0.8862 1.0000
2 True 3 probe4_3 0 0.1947 287 probe4_3 0.9522 1.0000
3 True 2 probe8_1 0 0.2270 135 probe8_1 0.9775 1.0000
4 True 1 probe3_3 0 0.0815 2325 probe3_3 0.6125 1.0000
5 True 1 probe0_3 0 0.0499 2964 probe0_3 0.5060 1.0000
6 True 2 probe6_3 0 0.2466 121 probe6_3 0.9798 1.0000
7 True 5 probe2_3 0 0.1865 530 probe2_3 0.9117 1.0000
8 False 0 - -1 0.0000 -1 - 0.2882 0.3425
9 True 2 probe0_2 0 0.0838 2713 probe0_5 0.5478 1.0000
10 True 2 probe9_2 0 0.0848 1925 probe9_2 0.6792 1.0000
11 True 1 probe0_4 0 0.0915 2990 probe0_4 0.5017 1.0000
12 True 3 probe4_3 0 0.1093 2164 probe4_3 0.6393 1.0000
13 True 2 probe7_0 0 0.1615 319 probe7_0 0.9468 1.0000
14 True 2 probe5_3 0 0.2176 126 probe5_3 0.9790 1.0000
15 True 3 probe4_3 0 0.1705 412 probe4_3 0.9313 1.0000
```

(b)




(c)

Fig. 4: Exploration on uniform emission-image segmentations: (a) tile sizes vs. *disclosed_byte_amount*, (b) the explored best candidate's disclosure report, (c) correlation coefficient example from the best candidate.

For the black-box scenario, our *traces* are based on uniformly segmenting every photon emission image with a certain tile size, which is tested through 323 sizings (see Section III-B).

The overall CPEA framework and ML flow are implemented on CentOS Linux release 7.9.2009 (Core), with 80x Intel(R) Xeon(R) Gold 6148 CPU @ 2.40GHz, and the available memory size is 754 GB.

### B. Optical Side-Channel Simulation Results

Taking the transient current profile, we utilize our photon emission models to calculate the energy-integrated photon current (number of emitted photons per time unit) $I_{\nu_0,\infty}$ for each *Iavg*, the $I_{\nu_0,\infty}$ is then saved as photon emission images with the resolution of $10\mu m \times 10\mu m$ (different pins' $I_{\nu_0,\infty}$ within the same pixel boundary is accumulated). Fig. 3a shows a simulated image based on plaintext 1 out of 3000 images in total. Fig. 3b is an example real-life photon emission image showing the similarity to our simulated ones (with higher resolution) in contrast. For each certain tile experiment out of either 16 tiles (white-/grey-box) or the tile amount calculated from one of 323 uniform tile-sizing plans (black-box), we perform lossless processing to extract the corresponding grey value and recorded them from 3000 plaintexts as our final *traces*, which are proceeded with CPEA to acquire the leakage information.

From our AMOP-based meta-modeling, tile-size exploration can be significantly improved for black-box attack scenarios. We trained this model with experimental results from 323 combinations of tile-size arrangement plans: we have the width of tile size $W_i \in \{80\mu m, 100\mu m, 120\mu m..., 400\mu m\}$ while tile's height $H_i \in \{90\mu m, 110\mu m, 130\mu m, ..., 450\mu m\}$. Fig. 4a shows the results from setting optimization goal to *disclosed_byte_amount* with a CoP of 85%. When maximizing the goal, the EA algorithm explored a best candidate of $80\mu m \times 170\mu m$ uniform tile size (the peak in Fig. 4a), which turns out to disclose 15 bytes as shown in its disclosure report (Fig. 4b). Fig. 4c shows an example result of correlation coefficients vs. number-of-traces, it indicates that in the best candidate's uniform tile-sizing, byte #1 has a strong disclosure with an SMTD of $< 140$. The above-mentioned explorations are automated and configurable, which allows users to verify the leakiest points/scenarios of their design.

**Out-of-Model Leakage due to Current Coupling**: In byte-boundary-based experiments, byte-bounding boxes theoretically crack their corresponding key byte with a low noise ratio, meanwhile, they may have weak disclosures of neighbor bytes with overlapping boxes. However, our observations revealed an unexpected phenomenon: traces from one known byte's boundary not only disclosed the chosen byte itself but also, in some cases, disclosed other bytes with no overlapping boundaries. This suggests the possibility of bypassing countermeasures by exploiting out-of-model leakages [31], primarily due to current coupling in our case: as we derived our photon emission images from transistor-level dynamic IR drop simulations, the drop and bounce at VDD/VSS can result in coupling between different byte boundaries' current. For example, byte 7's NMOS VSS pin current is not entirely determined by its logic behavior, but also a function of VDD/VSS drop and bounce, which are shared across the chip and in our case, correlated and disclosed a non-overlapping byte 5's content. To the best of our knowledge, this is the first time that the effect of IR drop on SCA has been observed and discussed [31].

## V. Conclusion

In conclusion, for the first time, our paper presents a multi-physics optical side-channel simulation framework at the pre-silicon stage. Through transistor-level dynamic IR simulations on an AES-128 implementation, we model photon emission behavior physically and derive the emission images based on distinct tile-based segmentation methodologies. The proposed ML-optimized framework facilitates the key disclosure evaluation and paves the way for enhanced understanding and mitigation of optical side-channel vulnerabilities in cryptographic systems.

## REFERENCES


[1] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Advances in Cryptology — CRYPTO '96*, N. Koblitz, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 104–113.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology — CRYPTO' 99*, M. Wiener, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397.

[3] T. Zhang, J. Park, M. Tehranipoor, and F. Farahmandi, "Psc-tg: Rtl power side-channel leakage assessment with test pattern generation," in *2021 58th ACM/IEEE Design Automation Conference (DAC)*, 2021, pp. 709–714.

[4] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (ema): Measures and counter-measures for smart cards," in *Smart Card Programming and Security*, I. Attali and T. Jensen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 200–210.

[5] N. Chang, D. Zhu, L. Lin, D. Selvakumaran, J. Wen, S. Pan, W. Xia, H. Chen, C. Chow, and G. Chen, "Ml-augmented methodology for fast thermal side-channel emission analysis," in *2021 26th Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2021, pp. 463–468.

[6] C. Lavaud, R. Gerzaguet, M. Gautier, O. Berder, E. Nogues, and S. Molton, "Whispering devices: A survey on how side-channels lead to compromised information," *Journal of Hardware and Systems Security*, vol. 5, pp. 143–168, 2021.

[7] J. Ferrigno and M. Hlavac, "When aes blinks: Introducing optical side channel," *Information Security, IET*, vol. 2, pp. 94 – 98, 10 2008.

[8] S. Tajik, E. Dietz, S. Frohmann, H. Dittrich, D. Nedospasov, C. Helfmeier, J.-P. Seifert, C. Boit, and H.-W. Hübers, "Photonic side channel analysis of arbiter pufs," *Journal of Cryptology*, vol. 30, 04 2016.

[9] B. G. Streetman, S. Banerjee *et al.*, *Chapter 4: Excess Carriers in Semiconductors, Solid State Electronic Devices*. Prentice hall New Jersey, 2000, vol. 4.

[10] N. Vashistha, M. T. Rahman, O. P. Dizon-Paradis, and N. Asadizanjani, "Is backside the new backdoor in modern socs?: Invited paper," in *2019 IEEE International Test Conference (ITC)*, 2019, pp. 1–10.

[11] N. Asadizanjani, M. Rahman, and M. Tehranipoor, *Physical Inspection and Attacks: An Overview*, 02 2012.

[12] PHEMOS-1000 Emission Microscope, Hamamatsu Photonics, https://www.hamamatsu.com/eu/en/product/semiconductor-manufacturing-support-systems/failure-analysis-system/C11222-16.html.

[13] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J.-P. Seifert, "Simple photonic emission analysis of aes," in *Cryptographic Hardware and Embedded Systems – CHES 2012*, E. Prouff and P. Schaumont, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 41–57.

[14] J. Krämer, D. Nedospasov, A. Schlösser, and J.-P. Seifert, "Differential photonic emission analysis," in *Constructive Side-Channel Analysis and Secure Design*, E. Prouff, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 1–16.

[15] H.-S. Wang, Z.-Y. Xu, Y. Zhang, K.-Y. Chen, and L.-A. Wu, "Correlation photonic emission attacks against aes algorithm," in *Proceedings of the 2016 5th International Conference on Advanced Materials and Computer Science*. Atlantis Press, 2016/06, pp. 512–517. [Online]. Available: https://doi.org/10.2991/icamcs-16.2016.106

[16] E. Carmon, J.-P. Seifert, and A. Wool, "Photonic side channel attacks against rsa," in *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2017, pp. 74–78.

[17] G. M. Bertoni, L. Grassi, and F. Melzani, "Simulations of optical emissions for attacking aes and masked aes," in *Security, Privacy, and Applied Cryptography Engineering*, R. S. Chakraborty, P. Schwabe, and J. Solworth, Eds. Cham: Springer International Publishing, 2015, pp. 172–189.

[18] H. Wang, D. Ji, Y. Zhang, K. Chen, J. Chen, and Y. Wang, "Optical side channel attacks on singlechip," in *Proceedings of the 2015 International Conference on Industrial Technology and Management Science*. Atlantis Press, 2015/11, pp. 364–369. [Online]. Available: https://doi.org/10.2991/itms-15.2015.87

[19] Totem and Totem-SC, Ansys, https://www.ansys.com/products/semiconductors/ansys-totem.

[20] S. Tam and C. Hu, "Hot-electron-induced photon and photocarrier generation in silicon mosfet's," *IEEE Transactions on Electron Devices*, vol. 31, no. 9, pp. 1264–1273, 1984.

[21] N. Akil, S. Kerns, D. Kerns, A. Hoffmann, and J.-P. Charles, "A multimechanism model for photon generation by silicon junctions in avalanche breakdown," *IEEE Transactions on Electron Devices*, vol. 46, no. 5, pp. 1022–1028, 1999.

[22] J. Bude, N. Sano, and A. Yoshii, "Hot-carrier luminescence in si," *Physical review. B, Condensed matter*, vol. 45, pp. 5848–5856, 04 1992.

[23] A. Lacaita, F. Zappa, S. Bigliardi, and M. Manfredi, "On the bremsstrahlung origin of hot-carrier-induced photons in silicon devices," *IEEE Transactions on Electron Devices*, vol. 40, no. 3, pp. 577–582, 1993.

[24] A. Toriumi, M. Yoshimi, M. Iwase, Y. Akiyama, and K. Taniguchi, "A study of photon emission from n-channel mosfet's," *IEEE Transactions on Electron Devices*, vol. 34, no. 7, pp. 1501–1508, 1987.

[25] J. Phang, D. Chan, S. Tan, W. Len, K. Yim, L. Koh, C. Chua, and L. Balk, "A review of near infrared photon emission microscopy and spectroscopy," in *Proceedings of the 12th International Symposium on the Physical and Failure Analysis of Integrated Circuits, 2005. IPFA 2005.*, 2005, pp. 275–281.

[26] L. Lin, D. Zhu, J. Wen, H. Chen, Y. Lu, N. Chang, C. Chow, H. Shrivastav, C.-W. Chen, K. Monta, and M. Nagata, "Multiphysics simulation of em side-channels from silicon backside with ml-based auto-poi identification," in *2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2021, pp. 270–280.

[27] OptiSLang, Ansys, https://www.ansys.com/products/connect/ansys-optislang.

[28] Y. Im, H. Jo, C. Oh, Y.-S. Cho, J. Yoo, H. Lee, M. Lee, and V. K. Yaddanapudi, "Thermal model simplification of mobile device with adaptive metamodel of optimal prognosis (amop)," in *2022 21st IEEE Intersociety Conference on Thermal and Thermomechanical Phenomena in Electronic Systems (iTherm)*, 2022, pp. 1–6.

[29] T. Most and J. Will, "Sensitivity analysis using the metamodel of optimal prognosis," in *Proceedings of the Weimar Optimization and Stochastic Days 8.0*, 11 2011, pp. 24–25.

[30] K. Monta, L. Lin, J. Wen, H. Shrivastav, C. Chow, H. Chen, J. Geada, S. Chowdhury, N. Pundir, N. Chang, and M. Nagata, "Silicon-correlated simulation methodology of em side-channel leakage analysis," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 19, 10 2022.

[31] T. D. Cnudde, B. Bilgin, B. Gierlichs, V. Nikov, S. Nikova, and V. Rijmen, "Does coupling affect the security of masked implementations?" Cryptology ePrint Archive, Paper 2016/1080, 2016, https://eprint.iacr.org/2016/1080. [Online]. Available: https://eprint.iacr.org/2016/1080