DesignCon 2020

A C-P-S Simulation Technique of Power-Noise Side Channel Leakage in Cryptographic Integrated Circuits

Makoto Nagata, Kobe University
nagata@cs.kobe-u.ac.jp

Akihiro Tsukioka, Kobe University
tsukioka@cs26.scitec.kobe-u.ac.jp

Norman Chang, ANSYS
norman.chang@ansys.com

Karthik Srinivasan, ANSYS
karthik.srinivasan@ansys.com

Abstract

Cryptographic algorithms are vulnerable to implementation attacks on side-channel (SC) leakage information. This paper introduces an efficient simulation technique of SC leakage at the full IC chip level. Tool chains and modeling flows will be explained in detail. The whole power delivery network (PDN) including Si substrate is captured in a chip power model (CPM) and then integrated in a chip-package-system board (C-P-S) model. The proposed technique was demonstrated with an advanced encryption standard (AES) Si test chip for SC leakage evaluation using correlation power analysis (CPA) over 1000 different plain texts through power delivery and Si substrate combined networks.

Key words: side-channel information leakage, hardware security, cryptographic device, power delivery network, power noise, electromagnetic emanation, chip power model

Author(s) Biography

Makoto Nagata received the B.S. and M.S. degrees in physics from Gakushuin University, Tokyo, in 1991 and 1993, respectively, and the Ph.D in electronics engineering from Hiroshima University, Hiroshima, in 2001. He was a research associate at Hiroshima University from 1994 to 2002, an associate professor of Kobe University from 2002 to 2009, and then promoted to a full professor. He is currently a professor of the graduate school of science, technology and innovation, Kobe University, Kobe, Japan. He is a senior member of IEEE and IEICE. Dr. Nagata is chairing Technology Directions subcommittee for International Solid-State Circuits Conference (ISSCC) since 2018. He served as a technical program chair (2010-2011), symposium chair (2012-2013) and an executive committee member (2014-2015) for Symposium on VLSI circuits, and also a chair for IEEE SSCS Kansai Chapter (2017-2018). He has been with a variety of technical program committees of international conferences. He is currently an associate editor for IEEE Transactions on VLSI Systems since 2015.

Akihiro Tsukioka received the B.S. and M.S. degrees in Graduate School of System Informatics from Kobe University in 2015 and 2017, respectively. He is currently pursuing the Ph.D. degree at the Graduate School of System Informatics of Kobe University.

Norman Chang co-founded Apache Design Solutions in February 2001 and currently serves as Chief Technologist at Semiconductor BU, ANSYS, Inc. Prior to Apache, Dr. Chang lead a group at Palo Alto HP Labs, focused on interconnect related signal/power integrity issues and contributing to the HP-Intel IA64 micro-processor design. Dr. Chang

received his BS, MS, and Ph.D. in Electrical Engineering and Computer Sciences from University of California, Berkeley. He holds fourteen patents and has authored over 50 technical papers. He also co-authored the popular book, "Interconnect Analysis and Synthesis", published by John Wiley & Sons, 2000. He is currently in the committee for ESDA-EDA and IEEE P2401.

Karthik Srinivasan is currently working as a Senior Corporate AE Manager for Analog & Mixed Signal Products at Semiconductor Business Unit, Ansys Inc. His work focus includes providing technical support and guidance to Field Applications Engineers and working closely with product development teams to plan for future roadmap items. He joined Apache Design Solutions in 2006 and has taken several roles as part of field AE team. He received a B.S. in Electronics and Telecommunication Engineering from University of Madras, India, and an M.S. in Electrical Engineering from the State University of New York, Buffalo in 2003 and 2005 respectively.

I. Introduction

Cryptographic devices need to be more resilient against side channel (SC) leakage for mission critical applications. The secret key is mathematically protected in a cryptographic algorithm, however, SC leakage could be a potential path of its revelation [1][2][3][4]. The fast power leakage modeling of a secure IC chip can be helpful to validate and to countermeasure against SC leakage.

The SC attacks, utilizing SC leakage by potential adversary, such as correlation power analysis (CPA) or even simple power analysis (SPA) utilize near-field electromagnetic (EM) radiation emanated from an IC chip or simply power consumption current at power supply pins flowing from the chip [5][6]. An experimental setup of SC leakage is sketched in Fig. 1 that facilitates the measurements of EM waves from an IC chip having cryptographic engines. The efficient way of SC leakage simulation is very much needed for the design of secure IC chips.

This paper introduces an efficient simulation technique of SC leakage at the full IC chip level. The tool chains and modeling flows are explained in detail. The whole power delivery network (PDN) including Si substrate is captured in a chip power model (CPM) and then integrated in a chip-package-system board (C-P-S) model [7][8].

The proposed technique was demonstrated to an advanced encryption standard (AES) Si test chip and evaluated for SC leakage using correlation power analysis (CPA) over a few thousand different plain texts through both power and substrate leakage channels [9][10]. A key idea to promote the C-P-S simulation for SC leakage analysis provides the way to efficiently update the CPM of a cryptographic device whenever its input plain text is altered. Once the CPM is created for a whole chip, its active part is replaced with power consumption current that is derived for each plain text, while the passive part involving PDN and Si substrate networks remains as it is (reused). This scheme is implemented in the CPM extraction flow and accelerates the creation of CPM and makes the whole SC simulation processes faster. The update of CPM is prepared for the set of different plain texts to explore SC attacks such as CPA.

The remaining part of this paper is organized as follows. Section II introduces the basics of side channel leakage analysis. Section III describes CPM and C-P-S simulation frameworks. Section IV details the proposed simulation flow. Section V draws a brief conclusion.

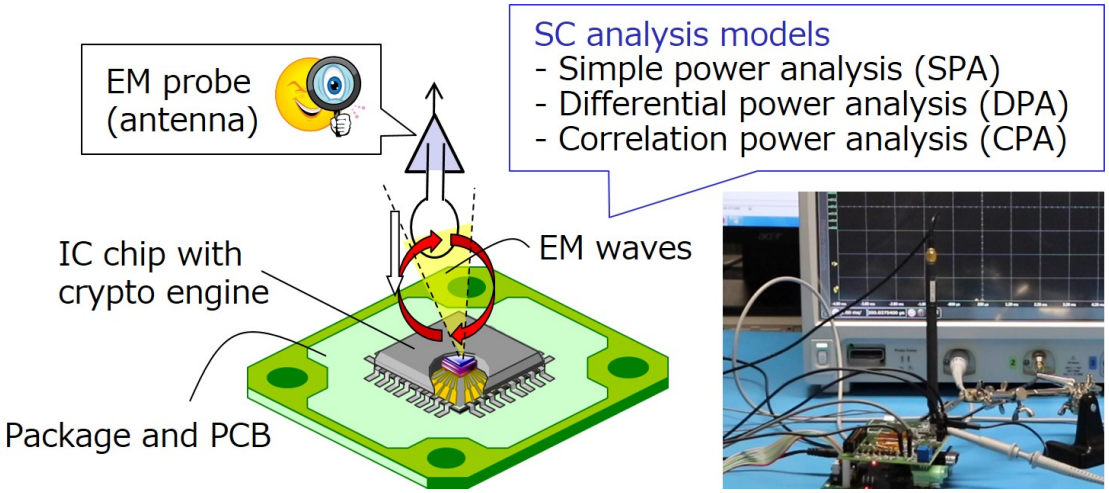

Figure 1: View of SC leakage measurement (Copyright IEEE 2019 [5].)

II. SC information leakage

A typical operation of an AES core is outlined in Fig. 2. The signal chain is prepared for a byte-wise crypto computation, and the entire operation includes 16 chains in parallel among 16 bytes when the AES core is designed for a 128-bit secret key length. The chain also adopts round based architecture, where the whole AES encryption processing completes in 10 rounds. All the rounds other than the last one include the mixture of key shuffling.

It is known that there is a strong correlation among the secret key byte and Hamming distance in its data register. One of the most powerful SC attacks focuses on the last round of AES processing, where the mixture of a shuffled key does not occur. The Hamming distance represents the number of bits flipped in the output data register in the last round of AES processing. The larger Hamming distance leads to the larger power current consumption and therefore induces the higher voltage drop, if we measure power supply noise of an IC chip embedding the AES core. This fact directly relates the C-P-S power noise simulation with the SC leakage analysis.

Power delivery networks including decoupling capacitors and power supply voltage regulators alter the level of SC leakage on a printed circuit board (PCB) or even in a package with multiple IC chips and components. In addition, a flip-chip packaging technology is often used among IC chips for a small footprint, where the backside of a silicon IC chip is exposed, even with being covered by epoxy on its backside surface [11]. This makes SC leakage worse, and requires involving a Si substrate network model for the C-P-S power noise simulation.

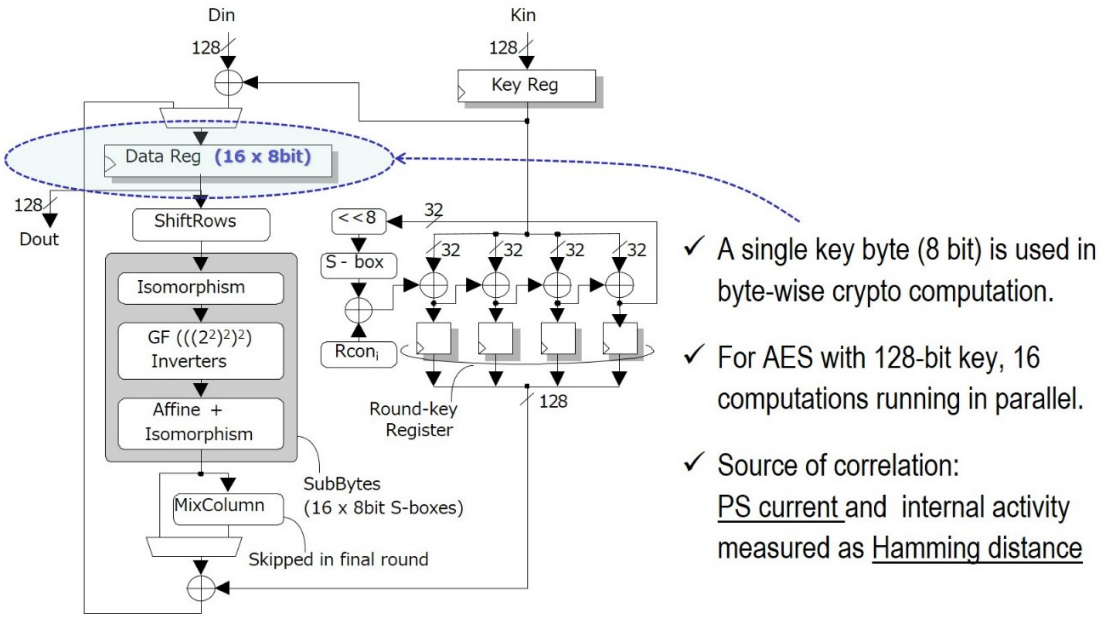

Figure 2: AES cryptographic core architecture.

III. C-P-S power noise simulation

A chip-package-system board (C-P-S) integrated power delivery network (PDN) is generalized in the equivalent circuit representation of Fig. 3. The power traces on a PCB will be modeled by a full wave solver for the multi-port S parameters and then reduced to lumped RLGC circuits for the frequency range of interest. The package can also be modeled in S parameters while often further simplified in the inductance in series (L_{wire}) since Au bonding wires between the pads and lands of IC chip and package, respectively, are mainly represented by inductance. The chip internally has dense networks of resistive/inductive and capacitive elements parasitic to active devices (MOS transistors and associated junction capacitors/diodes) and passive components (multiple layer metallic wirings.) The chip model in the PDN model of Fig. 3 is equivalently represented by a single-order RC low pass circuit representing power supply line impedance (Z_{DD}), including the effect of decoupling capacitors, decaps (C_{Decap}).

A chip power model (CPM) of Fig. 4 compactly represents passive power delivery impedance networks of an IC chip and active power supply current during the operation of internal circuits. The C-P-S simulation includes the CPM of a target chip with added power and ground impedance networks within a chip to the system-level PDN in order to stimulate the whole response. Power noise simulation is then achieved in the time domain and provides power supply current and voltage waveforms at any node of interest within the PDN. It is noted that the PDN part of CPM can be shared among active parts of the model for digital circuits with independent operational sequences, or namely, with different switching scenarios even in a single power domain. Those active models will run in parallel in a single passive PDN model during the C-P-S simulation.

The CPM for a whole chip is represented with dense mesh grids of resistive and capacitive networks for power supply (V_{DD}), ground (V_{SS}) and silicon substrate (V_{SUB}) nodes, as depicted in Fig. 5. The inductive networks may also be included for extremely high frequency designs. The grids involve parasitic resistive elements to the wirings of power and signal nets, capacitive ones to the explicit devices of MOS transistors, analog capacitors and resistors. The silicon substrate network includes junction capacitances to wells, trench capacitances to side walls, and resistive branches to doped wells as well as to a bulk material. Silicon-on-insulator (SOI) types of substrate engineering can also be captured. The whole network is applied with a model reduction technique and reduced to a SPICE compatible compact CPM, and connected to external models for circuit simulation.

A digital integrated circuit is generally composed of standard logic cells given by Silicon foundry. The active part of CPM includes current source models of Fig. 6 for the cells that are distributed in the whole network of Fig. 3. Each standard logic cell is pre-characterized by circuit simulation (SPICE) with transistor-level netlist, for the set of power supply currents ($I(t)$) dynamically drawing from a power source, with parametric conditions of load capacitance parasitic to the input fan in as well as output fan out and associated wirings, and also for environmental conditions of such as power supply voltage variation and temperature changes. Additionally, parasitic capacitance (C_{esc}) and resistance (R_{esr}) associated with transistor channels of the cell itself are also extracted

from physical layout, to form a Norton equivalent current source model. The static capacitance (C_{pg}) between V_{DD} and V_{SS}, which are attributed mostly to well junctions, is also included. The power current and parasitic components of individual standard logic cells are stored in a power library and called during the creation of CPMs.

The active part of CPM is self-timed for each gate-level model to restore power supply currents ($I(t)$) according to switching scenarios of C-P-S simulation. The currents are summed up by and interacted with the whole parasitic PDN model of Fig. 3. The switching scenario reflects the timing and transition of logical values that are all recorded beforehand in gate-level logic simulation in a file that is called toggle records or value change dump.

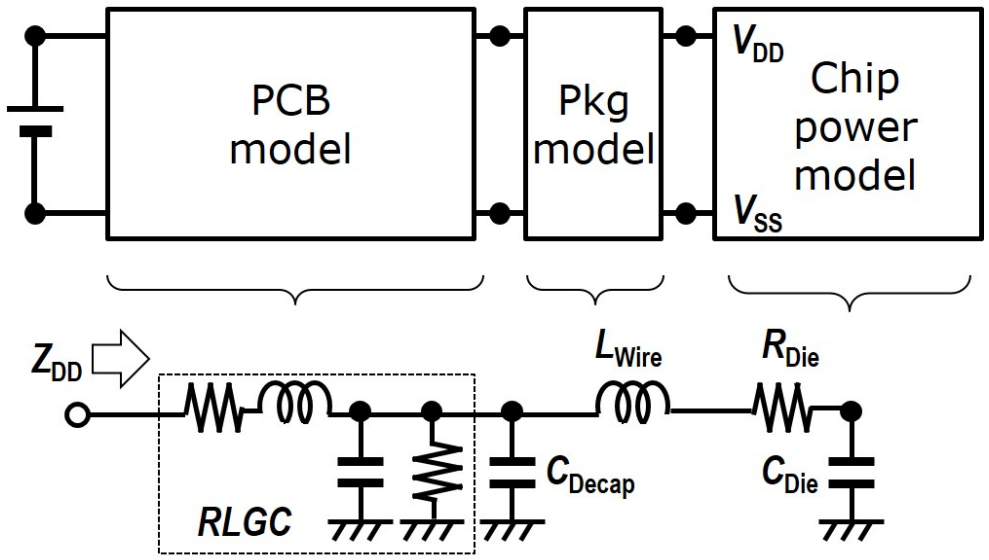

Figure 3: C-P-S model expressing PDN (Copyright IEEE 2016 [7].)

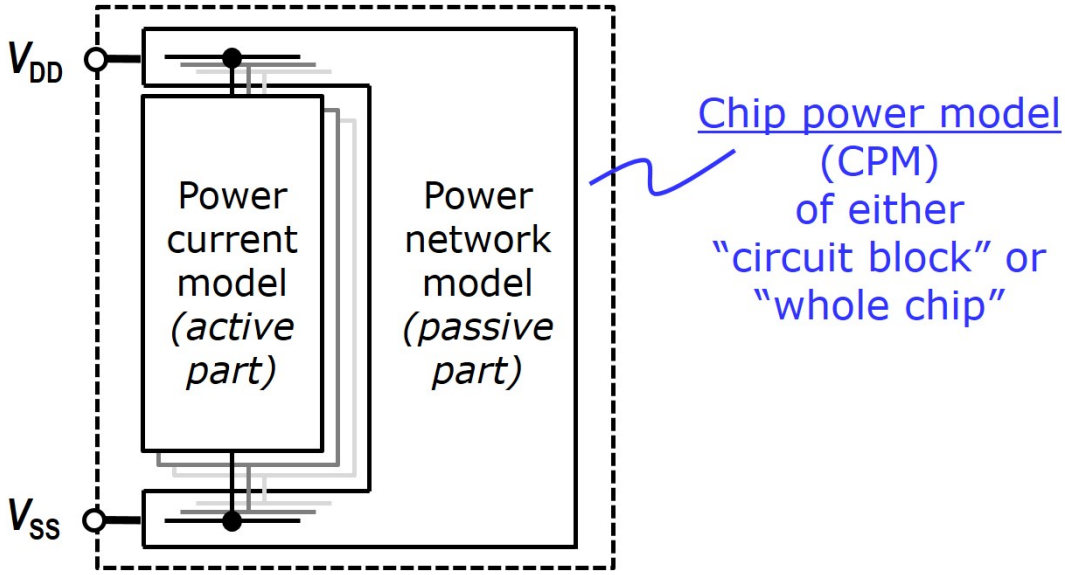

Figure 4: Chip power model (Copyright IEEE 2016 [7].)

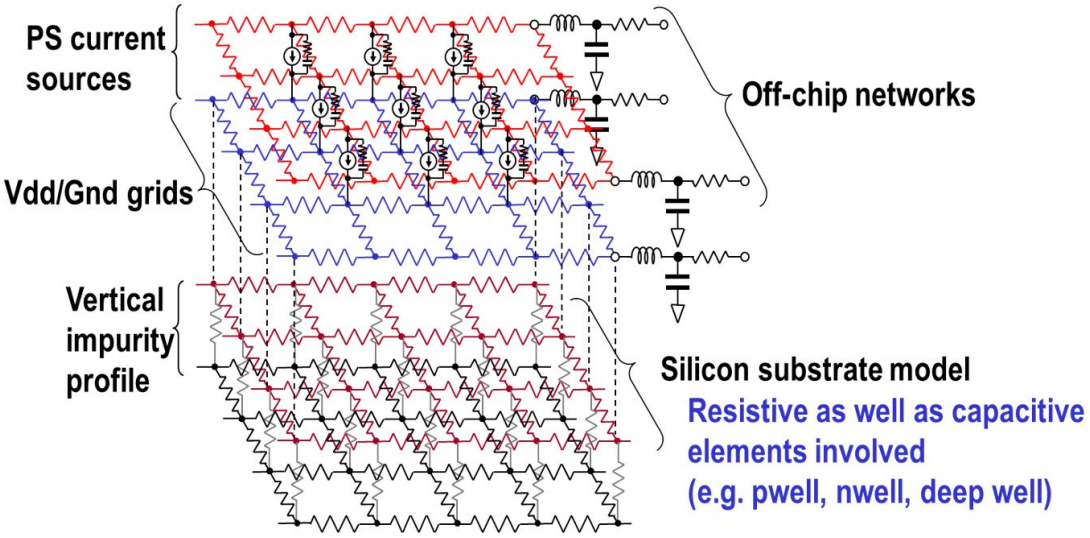

Figure 5: Full chip presentation of chip power model (Copyright IEEE 2016 [7].)

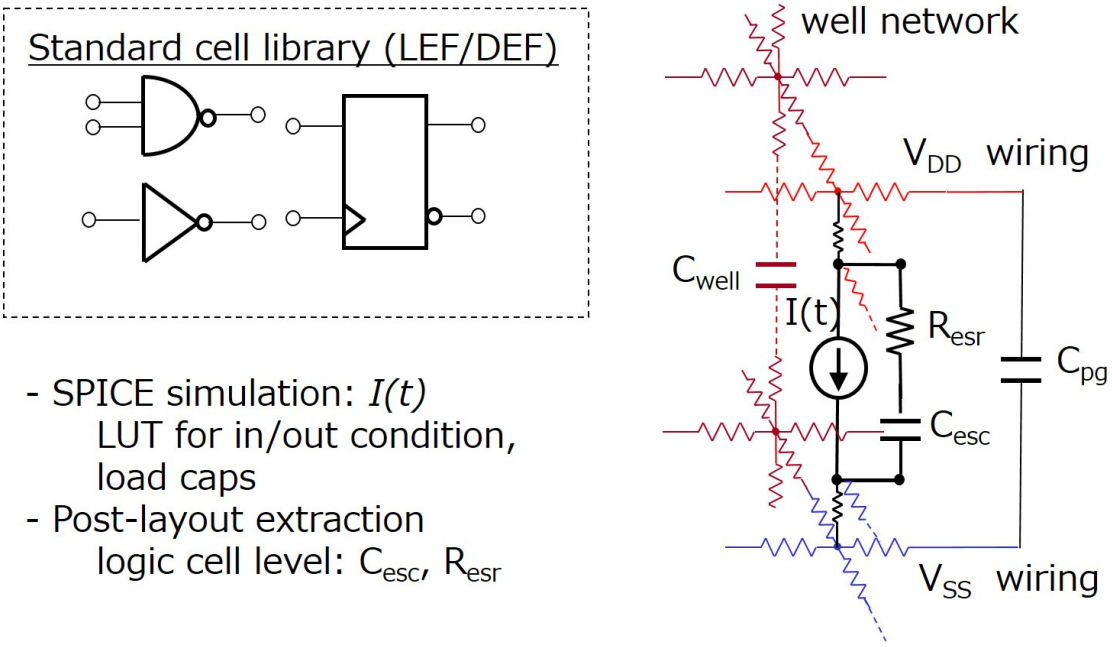

Figure 6: Standard logic cell model (Copyright IEEE 2016 [7].)

IV. SC leakage simulation

The SC leakage of AES, as a typical example of a secret key cipher, is analyzed through the correlation power analysis (CPA) of Fig. 7. The Hamming distance in the last round of AES encryption processing (Fig. 2) is correlated with the size of power supply voltage drop measured on the V_{DD} node of the AES core. The distribution of drops is outlined in the inset figures, with more than 10k, randomly generated 16-byte plain texts given to the AES core for a single secret key of 16 bytes. The power supply noise waveform differs for each input since the size of power supply consumption current varies with internal logic toggles. The larger distribution of voltage drops among the eight possible Hamming distance will more rapidly disclose the internal secret key bytes. Therefore, the most important parameter in the analysis is the number of test vectors (with different plain texts as payloads) to finely correlate the voltage drops in the last round of AES processing with the secret key bytes. This number can be a security indicator of a given cryptographic engine. The larger number requires the larger simulation costs and also for the higher cost burdened to the adversary. The detailed algorithms of CPA are given in the references [4].

The proposed SC simulation flow is given in Fig. 8. Initially, the whole PDN including Si substrate is modeled in the passive part of CPM. Secondly, the active part of CPM is generated for a digital circuit according to its toggle records. The active part is replaced for subsequent set of input test vectors (or payloads). Once a secret key (target key) is given, a set of plain texts are prepared to setup test vectors for the SC leakage simulation of AES core. A key idea to promote the C-P-S simulation for SC leakage analysis provides the way to efficiently update the CPM of a cryptographic device whenever its input plain text is altered. Once the CPM is created for a whole chip, its active part is replaced with power consumption current that is derived for each plain text, while the passive part involving PDN and Si substrate networks remains as it is (reused). This scheme is implemented in the CPM extraction flow and accelerates the creation of CPM and makes the whole SC simulation processes faster. The update of CPM is prepared for the set of different plain texts to explore SC analyses such as CPA.

The detailed tool chain is summarized in Fig. 9. Since the AES core is designed with standard logic cells, a gate-level logic simulator analyzes its operation and records all the toggling (switching) actions during the whole sequence of AES processing. The active part of CPM can be produced according to the toggle records with using the pre-characterized power current models among every gate in the AES core. It is noted that the active part of the model needs to be created for each test vector. The power noise waveforms are then simulated in C-P-S including the updated CPMs of AES core for the set of test vectors and correlated with the secret key bytes. A full-chip level CPM is combined with external models of those components and then passively represents the frequency domain response. Also the CPM for a cryptographic circuit will be integrated with the other CPMs of different circuit entities such as a microprocessor and memory macros. This allows to include the active background noise (total power currents) in the analysis of SC leakage in a practical system-on-chip integration.

The test vehicle of Fig. 10 is tested with the SC leakage simulation flow. The proposed efficient chip power modeling methodology is applied to an AES test chip fabricated in a 0.13 μm CMOS technology. The difference of peak amplitudes among the randomly selected plain texts exhibits the source of SC leakage. The simulated power noise waveforms in the last round of AES processing for 1.5k payloads are pictured in Fig. 11. The simulated waveforms clearly reveal the voltage drops to be used for CPA, for the duration of 15 ns that corresponds to a half clock cycle in the last round. When we increase the number of waveforms with random plain texts to more than 3k, the whole 16 bytes of the secret key is considered resolved, as demonstrated in Fig. 12. The rank of the assumed key bytes remains 1st for further large number of waveforms in our trial up to 10k.

The simulation becomes so exhaustive if we use a full-transistor level netlist of the AES core that the inclusion of parasitic passive components will not be feasible. It is estimated to need more than three months for a thousand test cases with the netlist only with transistors (without parasitic components). On the other hand, the simulation time is greatly reduced once we apply the chip model technique that appropriately involves the parasitic components and even in the C-P-S model integration. In the proposed simulation flow, the acceleration of 21.2 times is achieved if we compare the simulation time including the update of the active part of CPM to the case where all part of the model is re-created as in the traditional flow, as shown in Fig. 13. This implies that the C-P-S simulation purely captures SC leakage mechanisms inherent to a given design and technology.

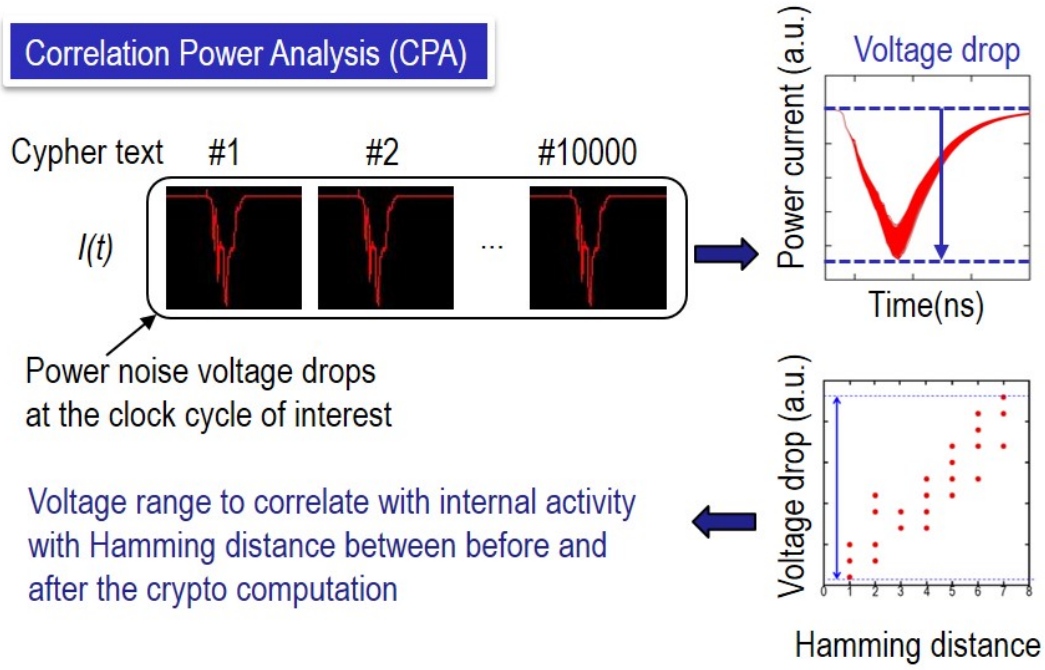

Figure 7: AES SC simulation (Copyright ACM 2019 [9].)

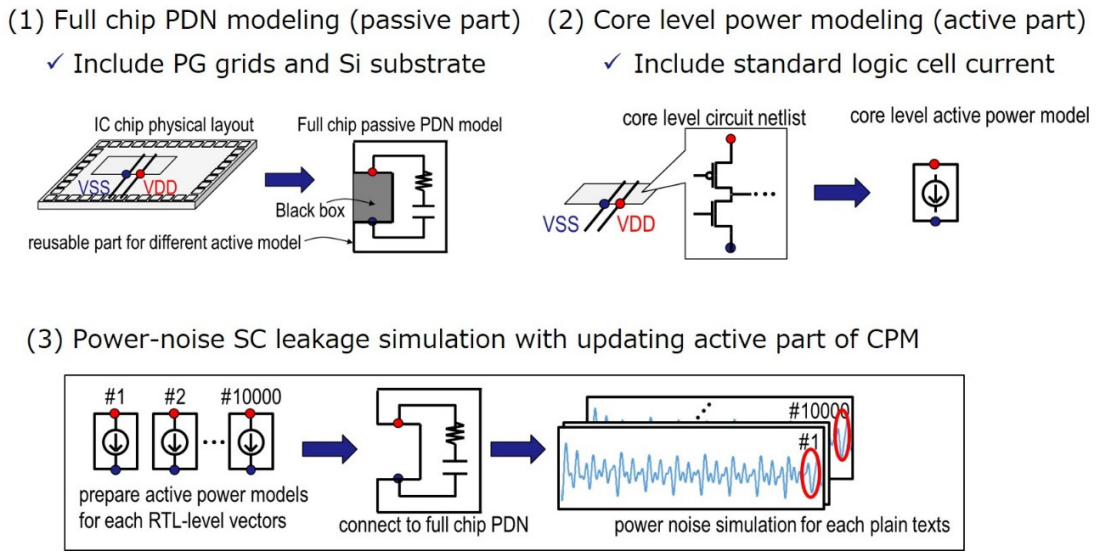

Figure 8: Proposed SC simulation flow (Copyright ACM 2019 [9].)

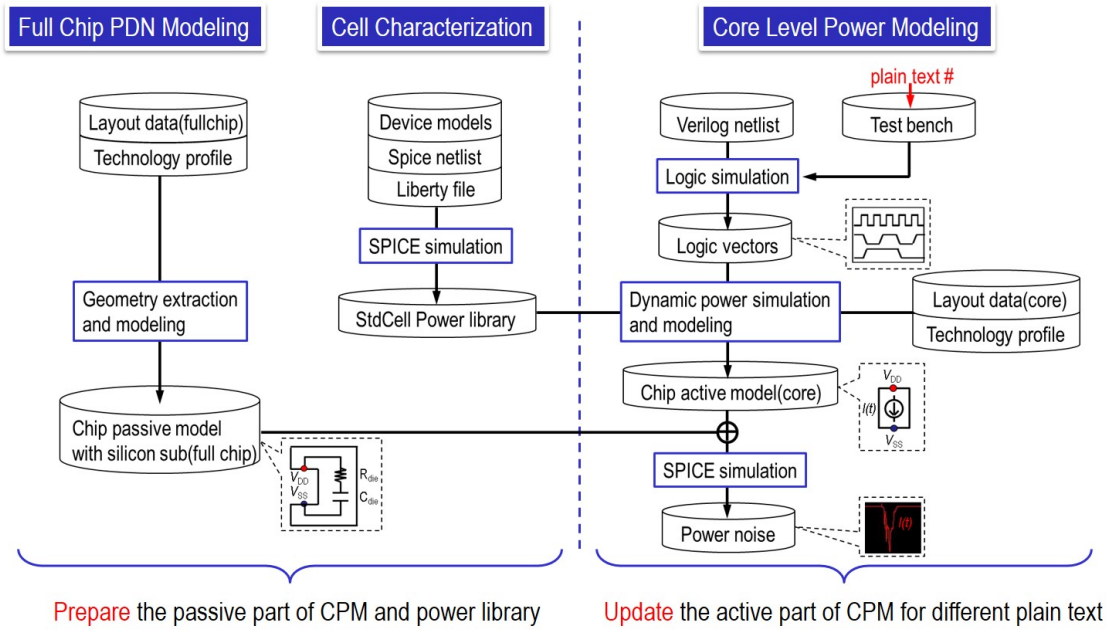

Figure 9: AES SC simulation tool chain diagram (Copyright ACM 2019 [9].)

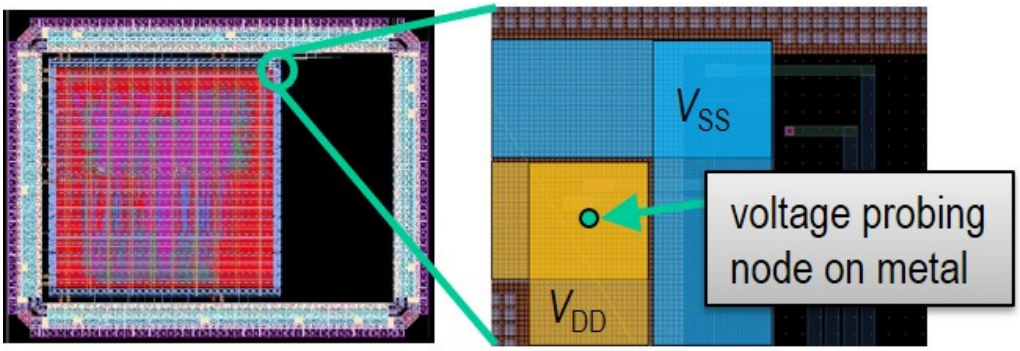

Figure 10: AES test chip example (Copyright ACM 2019 [9].)

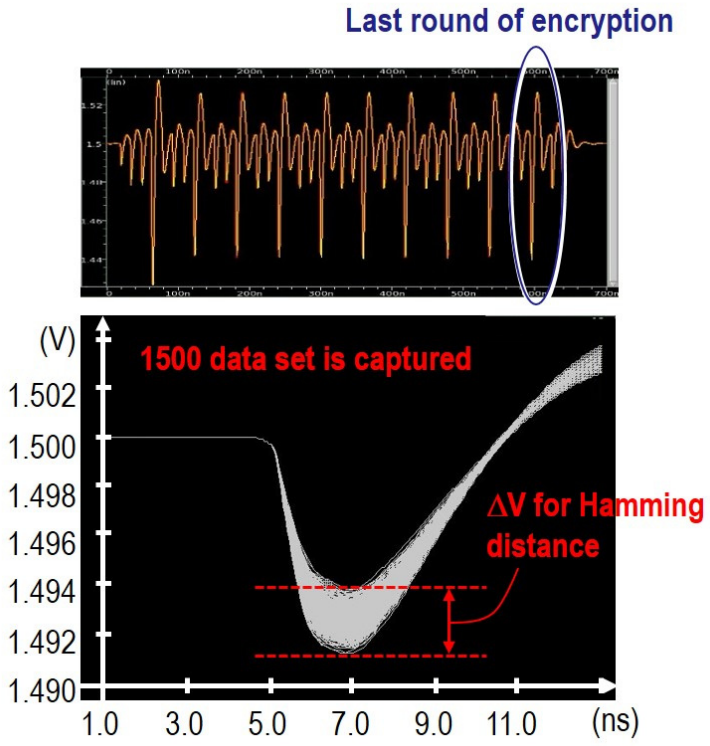

Figure 11: AES SC simulation (Copyright ACM 2019 [9].)

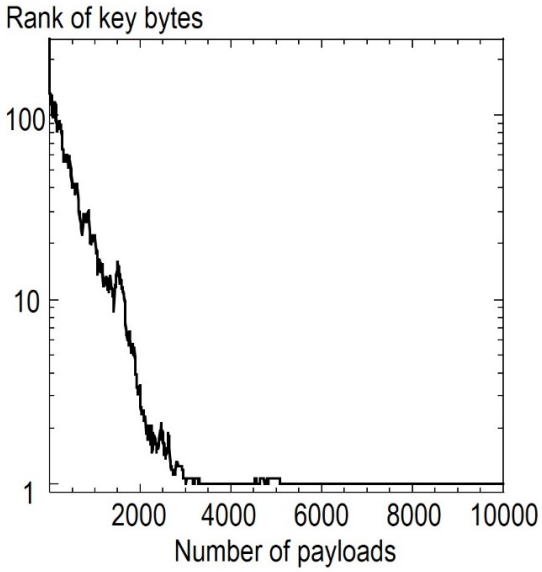

Figure 12: CPA on simulated power noise waveforms of AES.

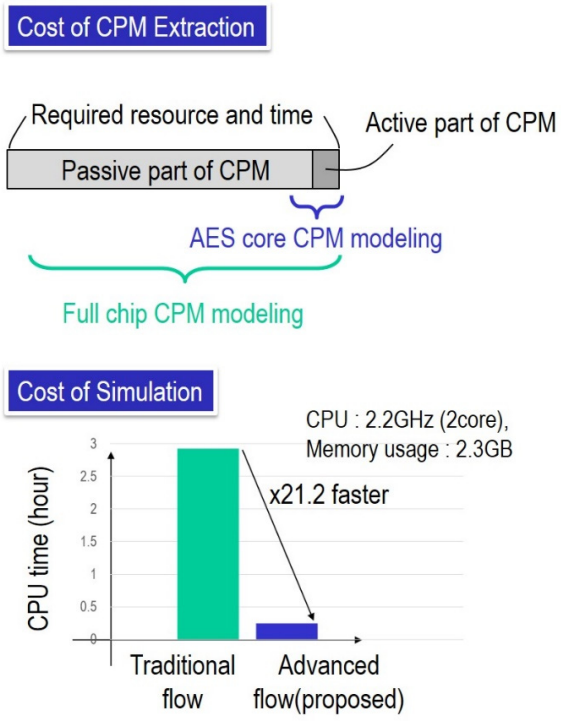

Figure 13: AES SC simulation cost (Copyright ACM 2019 [9].)

V. Conclusion

Power-noise SC leakage simulation technique was established and applicable to general cryptographic ICs. The technique can be explored for private-key and public-key crypto algorithms with diversified countermeasures at physical design. Advanced C-P-S simulation flow uses a full-chip CPM that is created one time, and then the active power current is updated. Core-level active power modeling is separated from full chip-level passive part modeling. Whole crypto operation including pre- and post-data processing time are simulated. It is demonstrated that the proposed technique achieves 21.2 times faster modeling/simulation of private-key crypto engine, in a half clock cycle (15 ns) of the last round of AES operation for SC analysis. Further studies will be pursued for countermeasure design of cryptographic engines against SC attacks.

References

[1] P. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems,” CRYPTO 1996, Lecture Notes in Computer Science, vol. 1109, pp. 104–113, Aug. 1996.

[2] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” CRYPTO 1999, Lecture Notes in Computer Science, vol. 1666, pp. 388–397, Aug. 1999.

[3] “Secure Integrated Circuits and Systems,” I. Verbauwhede, Ed., Springer, 2010 (ISBN 978-0-387-71829-3).

[4] “Hardware Security and Trust, Design and Deployment of Integrated Circuits in a Threatened Environment,” N. Sklavos, R. Chaves, G. D. Natale, and F. Regazzoni, Eds., Springer, 2017 (ISBN 978-3-319-44316-4).”

[5] M. Nagata, "On-Chip Protection of Cryptographic ICs Against Physical Side Channel Attacks (Invited)," in Proceedings of the 13th IEEE International Conference on ASIC (ASICON 2019), #C1-1, pp. 1-4, Oct. 2019.

[6] M. Nagata, T. Miki, N. Miura, "On-Chip Physical Attack Protection Circuits for Hardware Security (Invited), "Proceedings of the IEEE Custom Integrated Circuits Conference (CICC 2019), #15-5, pp. 1-6, Apr. 2019.

[7] M. Nagata, "Noise Simulation in Mixed-Signal SoCs (Invited Tutorial)," 2016 IEEE International Solid-State Circuits Conference (ISSCC 2016), Tutorial, T8, Jan. 2016.

[8] A. Tsukioka, N. Yamamoto, R. Korenaga, M. Nagata, K. Srinivasan, N. Chang, Y-S. Li, M. Takahashi, "Active Power Noise Modeling toward Design for EMI Compliance of IC Chips," 2017 DesignCon, Jan. 2017.

[9] A. Tsukioka, M. Nagata, K. Srinivasan, S. Wan, L. Lin, Y-S. Li, N. Chang, "A Full System Simulation Technique of Power-noise Side Channel Leakage in Cryptographic Integrated Circuits," ACM/IEEE Design Automation Conference (DAC 2019), Designer Track Reviewed #18.6, June 2019.

[10] A. Tsukioka, M. Nagata, K. Srinivasan, S. Wan, L. Lin, Y-S. Li, N. Chang, “A Fast Side-channel Leakage Simulation Technique Based on IC Chip Power Noise Modeling,” in Proceedings of the 2019 IEEE International Symposium on Electromagnetic Compatibility, Signal & Power Integrity (EMC+SIPI 2019), Abstract reviewed paper, TH-PM-3-4, July 2019.

[11] D. Fujimoto, M. Nagata, T. Katashita, A. Sasaki, Y. Hori, A. Satoh, "A Fast Power Current Analysis Methodology Using Capacitor Charging Model for Side Channel Attack Evaluation," 2011 IEEE Intl. Symp. Hardware-Oriented Security and Trust (HOST 2011), #P35, pp. 87-92, June 2011.