Chip-Package System Level Countermeasure Methodologies against Side-Channel Leakage Problems

門田, 和樹

(Degree)
博士（科学技術イノベーション）

(Date of Degree)
2024-03-25

(Date of Publication)
2025-03-01

(Resource Type)
doctoral thesis

(Report Number)
甲第8965号

(URL)
https://hdl.handle.net/20.500.14094/0100490190

Doctor Thesis

Chip-Package System Level Countermeasure Methodologies against Side-Channel Leakage Problems

（サイドチャネル漏洩問題に対するチップ・パッケージ・システムレベルの対策手段）

January 2024

Grasuate School of Science, Technology and Innovation,

Kobe University

Kazuki Monta

門田　和樹

Contents

1 Introduction 1
1.1 Background 1
1.2 Thesis outline 2

2 High resolution on-chip power noise evaluation technique 5
2.1 Introduction 5
2.2 Dynamic power supply monitoring 7
2.2.1 General architecture of SoC with on-chip monitors 7
2.2.2 On-chip monitor circuit 8
2.2.3 Dynamic IR-drop waveform 8
2.2.4 Dynamic PS monitoring and analysis principles 9
2.3 Evaluation setup 11
2.3.1 Test chip 11
2.3.2 Measurement setup 12
2.4 Results 14
2.4.1 Measurement results 14
2.4.2 Evaluation and example of diagnosis 15
2.5 Conclusion 17

3 Packaging technology for countermeasure against side-channel leakage 18
3.1 Introduction 18
3.2 CMOS power delivery with backside buried metal 19
3.3 Silicon demonstrator 22
3.3.1 Power delivery 22
3.3.2 Functionality 23
3.4 Measurement results 25
3.4.1 Passive impedance measurements 25
3.4.2 On-chip IR drop measurements 27
3.4.3 EM side-channel leakage measurements 29
3.5 Conclusion 32

4 Crypto core level side-channel leakage simulation 33
4.1 Introduction 33
4.2 Masking scheme 35
4.3 Side-channel analysis simulation 36
4.4 Side-channel evaluation metric 37
4.4.1 Measurement to disclosure 37
4.4.2 TVLA 38
4.5 Evaluation details and result 38
4.6 Discussion for a solution 47
4.7 Conclusion 48

5 SoC level side-channel leakage simulation 49
5.1 Introduction 49
5.2 EM emission modeling 51
5.2.1 Power supply current modeling with chip-package system (CPS) board model 51
5.2.2 On-chip power noise model 52
5.2.3 Near-field electro magnetic emission 55
5.3 Side-channel leakage simulation 56
5.3.1 Overview of SCLA simulation frame work 56
5.3.2 Identification of security sensitive register 58
5.3.3 Direct vector control 60
5.4 Silicon design flow and example 61
5.4.1 Silicon design flow 61
5.4.2 Silicon example and measurement 65
5.4.3 Silicon results 67
5.5 Conclusion 69

6 Innovation idea using side-channel leakage simulation technique 71
6.1 Introduction 71
6.2 Innovation idea 74
6.3 Analysis 78
6.4 Conclusion 83

7 Conclusion **85**

Acknowledgment **88**

References **89**

List of publication **100**

Journals 100

International Conferences 100

Awards 102

Section 1

Introduction

1.1 Background

The development of information and communication technology has enabled electronic devices around us to communicate a lot of information via the Internet. By storing, analysing and utilising these information, an advanced information and telecommunication society is being created to create new value and enrich people's lives. The vast amounts of data used here not only contain sensitive information such as personal data, but also are indispensable for the operation of services.

In order to use the convenient advanced information and telecommunication society without worry, it is essential to protect these data. The use of cryptography to ensure security of these data is drawing attention. The difficulty of stealing secret information from ciphertext generated by cryptography has been assessed by experts, and a list of secure cryptographic algorithms has been released.

However, even if a cryptographic algorithm's security has been guaranteed, there is the threat of physical attacks that exploit implementation vulnerabilities once implemented in an electronic device as a cryptographic module. Physical attacks include methods that analyse the electromagnetic waves emitted from the electronic device during the encryption operation (Side-channel attack, SC attack) and methods that inject disturbances into the electronic device from outside (Fault injection attack, FI attack). These attack methods have only been a field of research, but in recent years, cases of attacks on real products have been reported, and these attack have become a real threat. However, the threat of such physical attacks is not increasingly recognised and many products do not have enough tolerance against physical attack.

SC attacks, which exploit secret information by analysing SC information such as current consumption and electromagnetic waves generated as a side effect of the operation of cryptographic circuits, are relatively cheap and easy to attack. Therefore,

SC attacks are serious threat among physical attacks. Countermeasures against SC attacks are highly required.

1.2 Thesis outline

This paper discusses countermeasure techniques for suppressing SC leakage in chip-package systems, where the functions required for a system containing one (or more) chip and package are integrated and realised. In order to counter SC leakage, it is important to have an accurate understanding of the behaviour of power supply (PS) noise, which is the cause of side-channel leakage, and to develop countermeasure techniques. Therefore, this thesis reports the realisation of SC leakage countermeasures at the chip-package system level using three technologies: high-resolution evaluation technology for the PS noise that causes SC leakage [1], packaging technology to suppress SC leakage [2], and countermeasure technology based on SC leakage simulation [3,4]. The summary of these technologies are shown in Fig. 1-1. Previous works have reported on circuit and architecture level countermeasure technologies. However, a complete countermeasure technology has not been identified, and it is important to achieve a high security level by combining countermeasures at the circuit level, architecture level, and package level. Therefore, this paper aims to contribute to a higher level of security for Chip-Package System Level side-channel leakage countermeasures by proposing techniques for each layer, as illustrated in Fig. 1-2.

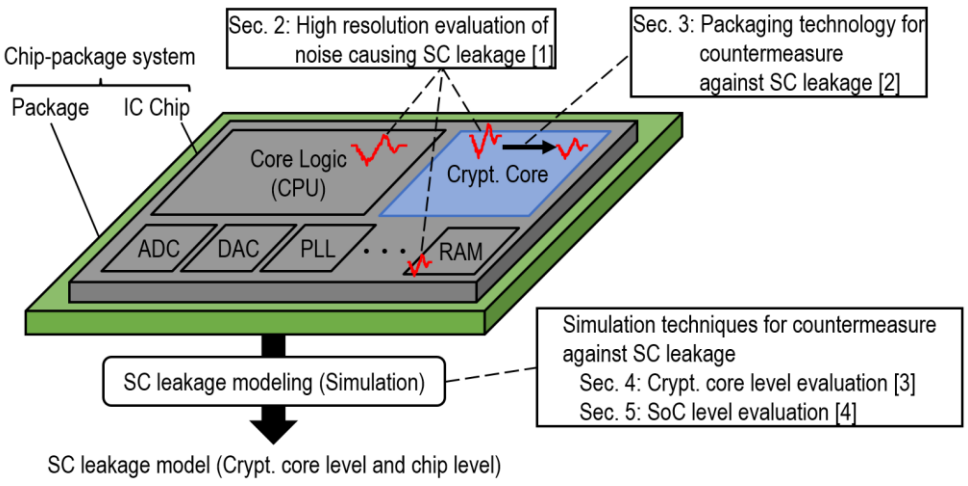


Fig. 1-1 Overview of this thesis.

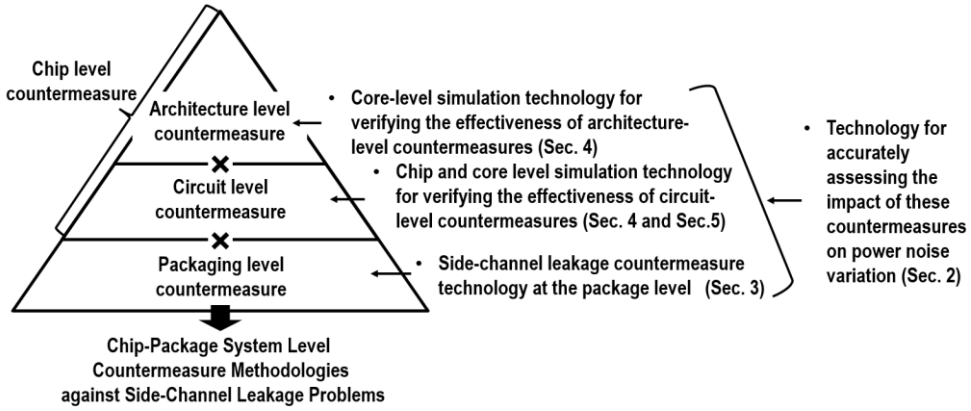


Fig. 1-2 Approaches in this paper for enhancing tolerance against Side-Channel Attacks at the Chip-Package System Level

First, as a high-resolution evaluation technique for PS noise that causes SC leakage, dynamic voltage drop waveforms in large-scale devices such as system-on-chip (SoC) and three-dimensional integrated circuits (3D-IC) were evaluated using on-chip monitor circuits and simulation. Accurate PS noise waveform acquisition using an on-chip monitoring (OCM) circuit resulted in a high degree of correlation between the number of switching nodes in the chip calculated from the acquired PS noise waveform and the number of switching nodes calculated in advance using logic simulation. This technique contributes to understand the behaviour of PS noise in cryptographic circuits, which is a source of side-channel leakage. It can also be applied to the diagnosis of circuits that consume power by generating toggles in the background without generating signal outputs in order to flatten and stabilise the PS. An IR-drop-based power-domain scenario-based testing and in-field diagnosis technique using OCM circuits is presented in Sect. 2.

As a packaging technology to suppress SC leakage, a PS noise suppression technology, that applies a PS network with backside buried wiring to a three-dimensional stacked chip, was proposed in Sect. 3. The backside buried wiring is a technology to reduce PS noise by forming a PS network using backside buried wiring. Cu wiring PS network is embedded in the backside of the silicon substrate and thereby realises low parallel wiring resistance and parasitic capacitance between the backside buried wiring and the silicon substrate. The proposed method suppresses dynamic voltage drop and achieves a reduction of approximately 59% in voltage fluctuations. The SC leakage suppression effect of this noise reduction effect was evaluated using a t-value representing statistical significance, and it was confirmed

that side-channel leakage was suppressed by a factor of 14 compared to the conventional implementation.

Next, as simulation techniques for side-channel leakage suppression, a highly accurate transistor-level SC leakage simulation method for cryptographic core analysis and a simulation method for large-scale circuits that achieves high speed without compromising accuracy were developed. SC leakage simulation is very important because it enables SC leakage evaluation before manufacturing and immediate revision if the desired SC leakage tolerance is not reached. However, at present, it has not reached a practical level due to issues with the accuracy and speed of the simulation. Therefore, in order to perform accurate simulation at the cryptographic core level, we discovered the problem of false detection of side-channel leakage evaluation by simulation at the transistor level and developed a simulation method to avoid false detection in Sect. 4. In addition, for SoC-level simulation, we proposed a simulation method to increase simulation speed while maintaining accuracy, as the simulation time has been increasing due to the recent increase in circuit size in Sect. 5.

Finally, as a business plan to utilise these technologies, the commercialisation of physical attack resistance evaluation technology using simulation was discussed in Sect. 6. Based on the social background and customer issues, a semiconductor integrated circuit (IC) chip design business with cryptographic modules equipped with high physical attack resistance was proposed and the business environment of the proposed business was analysed. The analysis revealed that at the current stage, when the threat of physical attacks is not strongly prevalent, it is very important to make customers aware of the threat of physical attacks at the business start-up stage. Once the threat has been successfully made aware and the first customers have used the service, the scale of the business can then be expanded through continuous research and development of simulation technology and raising the barriers to entry for new customers.

Section 2

High resolution on-chip power noise evaluation technique

2.1 Introducion

In IC-testing, test stimuli are sent to the inputs of the IC and its responses are compared with the expected responses by the test equipment. Automatic test pattern generator (ATPG) generates test stimuli. Traditional test generation approaches treated the entire IC as a single unit for the ATPG. The huge gate counts of today's digital circuits, especially SoCs and 3D-ICs, make traditional test generation approaches difficult. Therefore, nowadays, most SoCs and 3D-ICs are tested using a modular test approach [5]. Here, individual modules making up SoC/3D-IC (e.g. memory, processor, I/O interfaces) are tested separately.

ATPG has traditionally tried to maximise fault coverage per a test pattern and minimise the number of test patterns required, by cramping as much switching as possible into each test pattern, so that the corresponding test application time. As a result, switching activity during IC-testing is significantly higher than during functional operation [6]. To avoid excessive dynamic voltage drop caused by switching activity of the circuits during IC-testing, most ATPG tools support the generation of low power test patterns. However, when we use low-power ATPG without considerations, low-power ATPG is effective only for the modules under test (MUTs) [6]. One way to avoid (almost) random test stimuli for neighbour modules is gating scan chains or clock signals to shield neighbours. However, this will provide too optimistic test conditions and may lead false positives [7]. Therefore, authors in [6] propose to use an embedded programmable toggle generator (ePTG) to create realistic test conditions.

Recent SoC very large scale integration (VLSI) chips utilize embedded toggle generators to achieve various goals. These include (1) stabilizing voltage variations in the PS network of high-bandwidth wireline circuits [8], (2) emulating background switching

activity during IC-testing to create realistic test conditions [6], and (3) equalizing PS noise to enhance resiliency against power SC attacks [9]. These circuits are designed to consume intended power without producing direct outputs. In many-core heterogeneous architectures, some functional blocks within SoC VLSI chips must be completely deactivated to stay within the overall power budget. These deactivated areas, referred to as 'dark silicon' [10], change locations within the chip over time, based on the processing contexts.

It is difficult for traditional function-based testing to confirm the proper operation of the circuits without digital outputs. A mechanism that verifies the correct number of toggles in circuits without digital outputs, complementing the traditional function-based testing approach, is needed. Some previous works explored the integration of testing, on-chip monitoring, and PS noise analysis. In [11] and [12], authors mention the importance of monitoring PS noise during testing and show the results of both IR-drop simulation and measurement. These systems are capable of analyzing PS noise over multiple clock cycles. However, they are not suited for evaluating the toggle count within a single clock cycle. And also, there is no detailed comparison between the predicted switching count and the observed IR drop. SoC designers take into account both average and dynamic IR drops for timing closure and mitigating crosstalk noise.

This section introduces IR-drop-based power-domain scenario-based testing and in-field diagnosis technique using OCM circuits. It enables the precise estimation of the number of toggled gates by analyzing the dynamic IR-drop waveforms at the PS nodes of each power domain individually powered by a micro voltage regulator module (μVRM). This technique realizes an in-place detailed evaluation of toggles among the granularly defined power domains in SoC chips.

Various on-chip PS and substrate noise measurement techniques have been reported for different purposes in existing literature. A technique using built-in current sensing to detect faulty transistors in analog circuits is discussed in [13]. Another method visualizes dynamic IR drop distribution in a microprocessor and links them to fault mechanisms [14]. These on-chip measurements have significantly contributed to the precise understanding of PS noise and interference mechanisms. However, this paper focuses on the use of OCM for scenario-based testing and in-field diagnosis of power domains in circuit blocks without visible outputs, which is suitable for SoC VLSI chips with granular power managements.

2.2 Dynamic power-supply monitoring

2.2.1 General architecture of toggle pattern generation

As shown in Fig. 2-1(a), an SoC VLSI chip comprises several power domains for its functional cores. Each of these domains is managed by a µVRM at a direct current (DC) voltage level of V_{DD} to meet required operational performance and to isolate one power domain from other domains. Within a power domain, there might be an ePTG [6], designed to generate on-chip switching activities at programmable levels set by the user. The toggle generation program is digitally encoded and pre-stored in the status registers of ePTG. Although there is no digital output, power supply current, I_{DD}, is consumed and leads to a dynamic IR drop. Additionally, the chip is equipped with OCM functions for waveform capturing and processing.

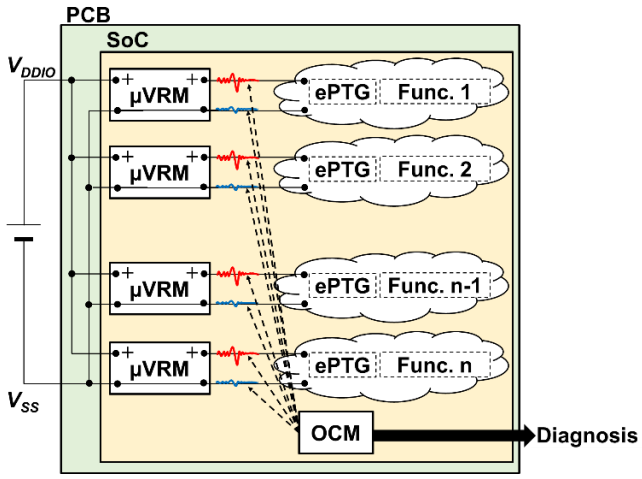


Fig. 2-1 SoC VLSI chip with multiple power domains includes ePTG and OCM for PS diagnosis[16]. (© 2021 IEEE)

The input channel of OCM is interconnected with the power (V_{DD}) and ground (V_{SS}) rail to capture waveforms of dynamic IR drops. These captured waveforms are subsequently processed and assessed in the following IR-drop based toggle diagnosis process. To probe and diagnose targeted power domains, the OCM is equipped with multiple input channels.

The ePTG's function is to regulate the PS current to a predetermined level of power consumption or to stabilize the PS current to avoid fluctuations of PS voltage. As shown in Sec. 2.1, this intentional toggle generation is utilized for various purposes in SoC VLSI chips [8][9][11]. For the purpose of generality, the ePTG is selected as a MUT which can controll switching activity within the logic gate cells.

2.2.2 On-chip monitor circuit

In the targeted power domain, the OCM captures the PS voltage waveforms. As shown in Fig. 2-2, the OCM circuits comprise a source follower (SF) to sence voltage level at its input, followed by a single-bit comparator that digitizes the SF's output. This process of iterative comparisons, as described in [14], allows both time and voltage to be discretized.

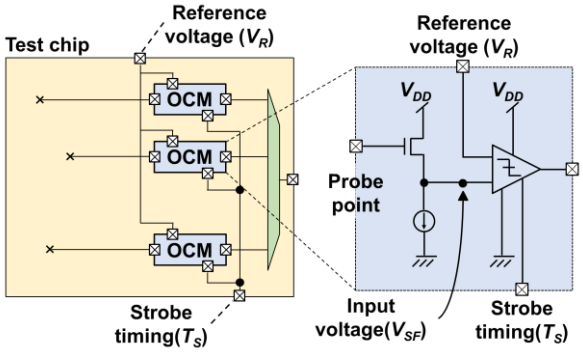


Fig. 2-2 The structure of OCM circuits [16]. (© 2021 IEEE)

The strobe timing, T_S, is synchronized with and incrementally shifted relative to the SoC's clock. Similarly, the reference voltage, V_R, is changed in a staircase way. At the timing of T_S, the comparator outputs a signal indicating whether the input voltage, V_{SF}, exceeds V_R. Through iterative comparative assessments by the comparator, the V_{SF}'s closest voltage level is searched in the staircase of V_R, and this procedure is then iterated at the next T_S. Finally, the time evolvement of approximated V_{SF} is a target voltage waveform. Prior to diagnosis, the relationship between input voltage and output value is calibrated using known linear or sinusoidal patterns.

2.2.3 Dynamic IR-drop PS waveform

The time-domain PS voltage, V_{DD}(t), is correlated with the PS current, I_{DD}(t), as described in equation (2-1), where Z_{DD} represents the impedance of PS network in a target power domain. Given that the domain is packed within the silicon area of digital standard cells, Z_{DD} is primarily influenced by the metal wirings that constitute the power rails. While off-chip impedance significantly affects the behavior of the overall system's power delivery networks, on-chip power domains can be effectively isolated by μVRMs.

$$V_{DD}(t) = Z_{DD} * \ I_{DD}(t) \qquad (2\text{-}1)$$

Though the V_{DD} side of the power rails is regulated by the μVRM, the V_{SS} side is typically connected to a p-type silicon substrate via p+ contacts and is commonly shared

across different power domains. As a result, the ground side's contribution to ZDD is almost negligible. On the other hand, Z_{DD} is primarily influenced by the resistance (R) exsisting in series with the V_{DD} side of the power rails, typically designed to be less than 1 Ω. The capacitance (C) alongside the power rails acts as a parallel shunt impedance for the PS current. This capacitance is estimated to be greater than 1 kΩ for AC components below 1 GHz, when we assume a parasitic capacitance of 1 pF. Therefore, the dynamic IR-drop voltage waveform, described in equation (2-1), accurately reflects I_{DD}(t) with a frequency-independent coefficient, R_{DD}, determined by the parasitic series resistance. In this section (Sect. 2), an R_{DD} of 0.25 Ω is assumed, to derive I_{DD} from V_{DD} captured by OCM.

2.2.4 Dynamic PS monitoring and analysis principles

By integrating the dynamic IR-drop waveforms over time, the total consumed charge within a power domain can be calculated, as Q_{DD} in equation (2-2) and illustrated in Fig. 2-3. The evoluation of $Q_{DD}(t_i)$ across successive time intervals t_i (i=0,1,2,…) reflects the sequence of toggle activities within logic cell operations. The duration of each time interval, t_{i+1} - ti, is selected to be an order of magnitude greater than the time resolution capability of the OCM's waveform capturing.

$$Q_{DD}(t_i) = \frac{1}{R_{DD}} \int_{t_i}^{t_{i+1}} |V_{DD}(t) - V_{CORE}| \, dt \qquad (2\text{-}2)$$

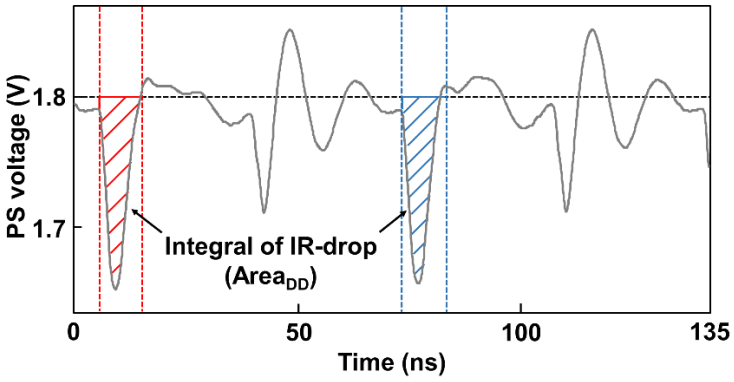


Fig. 2-3 Time integral of dynamic IR-drop waveforms by on-chip measurements [16]. (© 2021 IEEE)

The gate-level logic simulation result of a synchronous digital circuit is depicted in Fig. 2-4 to show the timings of net toggles. Three colors are employed to differentiate the

types of toggles. Following a clock edge, either rising or falling, toggls occurs first in the clock drivers and throughout the clock distribution network. Subsequently, digital data gets latched and captured within flip-flops or latches in registers. The final toggle type is occurred at the combinational logic cells.

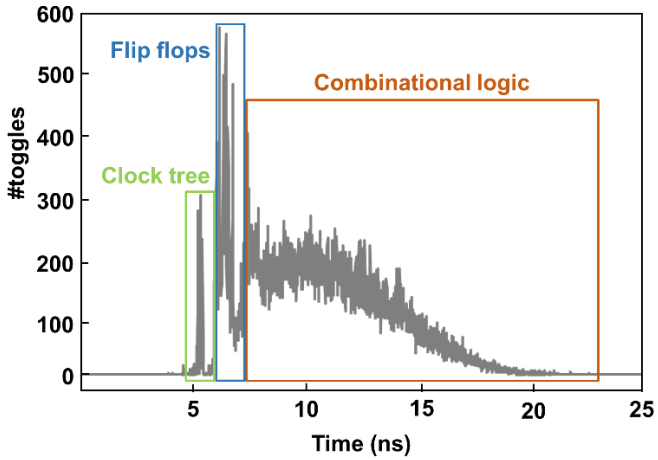


Fig.2-4 Three toggle types in one clock period [16]. (© 2021 IEEE)

In traditional synchronous digital IC design, it's typically assumed that toggles in clock network happen instantaneously. As a result, the range of toggle timings within the clock network and registers is narrow. We can assume that these first two types of toggles will be almost identical among different test scenarios. On the other hand, a broader distribution of toggles is expected in the combinational logic cells. This broader distribution is due to the different numbers of cascaded logic cells along the logical paths of different test scenarios. The amount of the third type of toggle is highly influenced by the test patterns.

The estimated charge consumption, $Q_{EST}(t_i)$, is calculated based on the counts of toggles in gate-level logic simulation. We assume that any change in a logic signal results from a single toggle in the preceding standard cell, approximately represented by a two-input NAND (NAND2) gate. Therefore, the total number of toggles, #toggles, is counted at the outputs of standard cells within target power domain. The charge consumption during a switching operation in a NAND2 cell, Q_{NAND2}, is evaluated in advance via transistor-level simulations. For each time interval t_i, #toggles is multiplied by Q_{NAND2} to calculate the corresponding $Q_{EST}(t_i)$, as shown in equation (2-3).

$$Q_{EST}(t_i) = Q_{NAND2} * \#\text{toggles}(t_i) \quad (2\text{-}3)$$

In the IR-drop-based toggle diagnosis depicted in Fig. 2-5, the evoluation of the charge consumption, Q_{DD}, derived from IR-drop waveform captured by OCM is

compared against the estimated charge consumption, Q_{EST}, in gate-level logic simulation. The trends of charge consumption among different timings and different test scenarios provides assurance of correct operation in digital circuits, even in the absence of digital outputs. Significant differences between Q_{DD} and Q_{EST} indicate potential issues. These issues can be either faults in the IC hardware or errors in the test program. These indications call for further detailed diagnostic investigations to determine the underlying cause. A particular example in Fig. 2-5 shows the deviation between Q_{DD} and Q_{EST} in test scenario #3. This indicates errors in either the test scenario or the digital circuit implementation. The practicality of this diagnos method will be shown through silicon measurements in the following section.

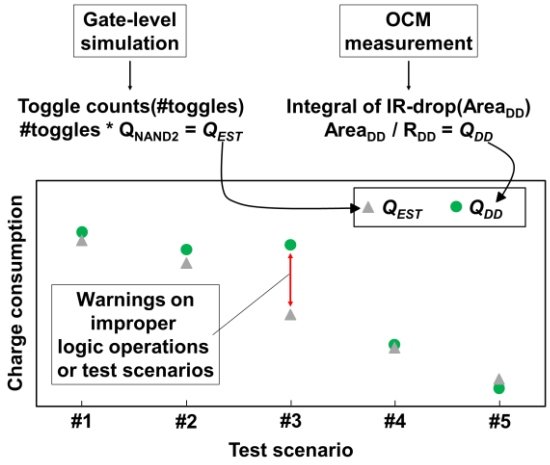


Fig. 2-5 Dynamic IR-drop-based PS diagnosis flow comparing gate-level simulation and on-chip measurements [1]. (© 2022 IEEE)

2.3 Evaluation setup

2.3.1 Test chip

We prepared a test chip using a commercially available 0.18 μm CMOS technology. This chip, as illustrated in Fig. 2-6(a) and Fig. 2-6(b), incorporates three digital blocks, reffered to as A, B, and C, along with an OCM system. The chip operates within a single power domain, powered directly from an external source. The digital blocks A, B, and C are designed as full-scan digital circuits equipped with IEEE Std 1500TM-2005 [15] core test wrappers. This structure allows each block to be independently tested, while sharing a common clock distribution and power delivery networks.

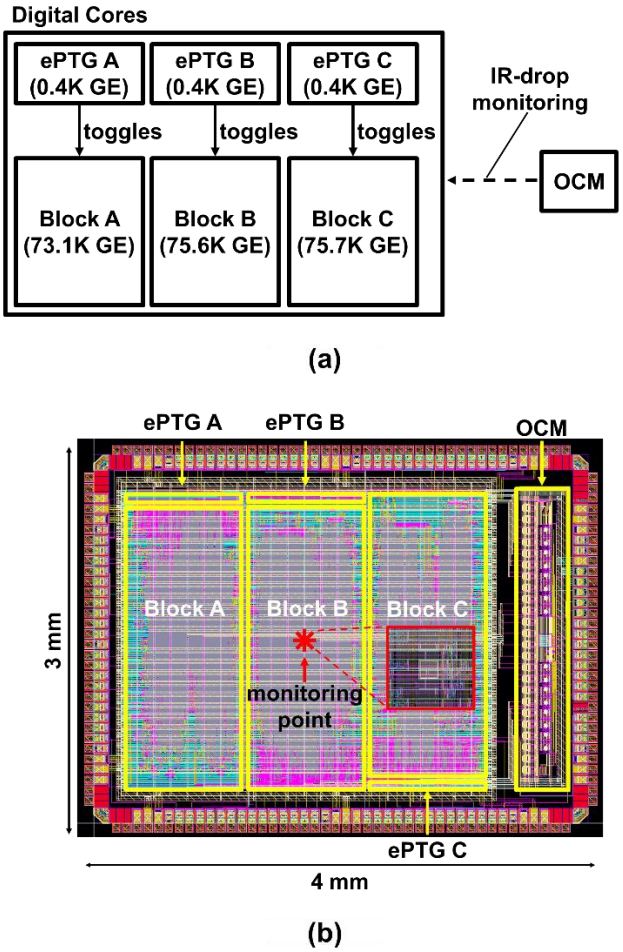


Fig. 2-6 (a) Block diagram and (b) layout of the test chip [1]. (© 2022 IEEE)

The OCM system is designed to be isolated from the digital blocks in terms of clocking and power delivery networks. The OCM channels are connected to various pairs of VDD and VSS nodes located near the digital blocks. For waveform capturing, one of the OCM channels within the core is digitally selected. In this study, the OCM system captures dynamic PS waveforms with a resolution of 100 ps and 100 μV.

2.3.2 Measurement setup

This test chip is packaged in a ball grid array and mounted on a custom printed circuit board (PCB). It is connected to a commercially available field programmable gate array (FPGA) board (Xilinx AC701) and they are controlled by a PC. The demonstrator system is depicted in Fig. 2-7(a) and 2-7(b). The PC programs various test scenarios with some data stored on the FPGA board, and then transferred to the chip via an interface (I/F)

block. An external pulse generator supplies the system clock to both the FPGA and the test chip. The entire system, including digital circuits operation and on-chip IR-drop waveforms monitoring, is autonomously controlled by the PC.

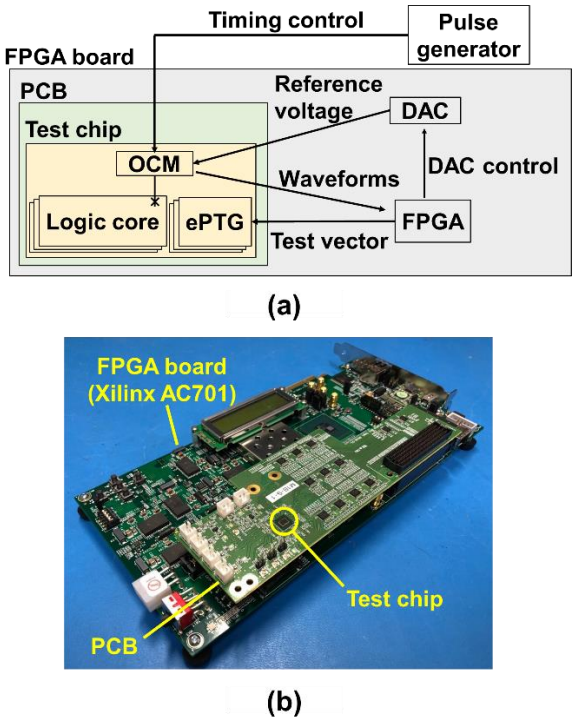


Fig. 2-7 (a) Block diagram showing the design hierarchy and (d) photo of the test system [16]. (© 2021 IEEE)

The test scenarios for the three digital blocks, depicted in Table 2-1, are prepared to intentionally induce varying levels of internal logic activity. A total of 15 test scenarios are designed, in which the digital cores load toggle data from their dedicated ePTG in one of two modes: 0 or 1/X as shown in Table1. In mode 0, the digital block becomes an MUT, where the ePTG is inactive and does not trigger toggling. On the other hand, in mode 1/X (where X equals 1, 2, 4, 8, 16), the digital block becomes neighbor module, where the ePTG generats stimuli that makes the digital block to toggle at every X clock cycles.

Table 2-1 Test scenarios [1] (© 2022 IEEE)

	#1	#2	#3	#4	#5	#6	#7	#8
Block A	1	0	1	1/2	0	1/2	1/4	0
Block B	1	1	0	1/2	1/2	0	1/4	1/4
Block C	0	1	1	0	1/2	1/2	0	1/4

	#9	#10	#11	#12	#13	#14	#15
Block A	1/4	1/8	0	1/8	1/16	0	1/16
Block B	0	1/8	1/8	0	1/16	1/16	0
Block C	1/4	0	1/8	1/8	0	1/16	1/16

2.4 Results

2.4.1 Measurement results

OCM captures a set of on-chip V_{DD} waveforms for all test scenarios at the monitoring point shown in Fig. 2-6(b). Power currents, which are summed among the cores, flow through the PS network resulting in an IR drop. This IR drop is observed as the V_{DD} voltage fluctuation at the monitoring point, typically appearing as shown in Fig. 2-3.

The ammount of charges, Q_{DD} and Q_{EST}, obtained from on-chip measurements and gate-level simulations respectively, are aligned against the prepared test scenarios (in Table 2-1), as shown in Figure 2-8. To ensure result consistency, two chips (chip α and chip β) are sampled for each test scenario. The trends generally agree with each other across a broad range of digital activities among different test scenarios.

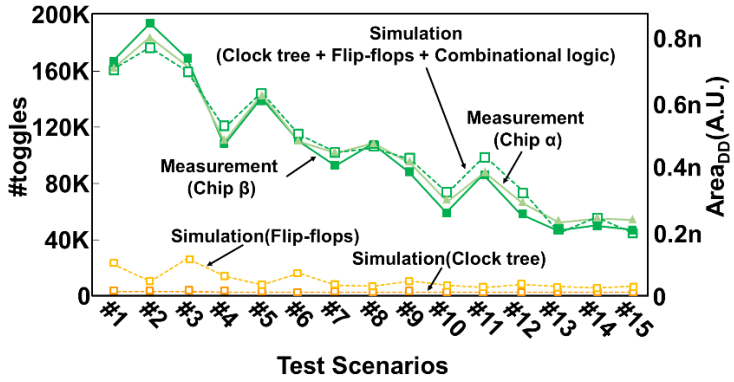


Fig. 2-8 Comparison of AreaDD(A.U.) (∝QDD) and #toggles (∝QEST) among test scenarios [1]. (© 2022 IEEE)

The switching activities of toggle types within the clock network and registers are calculated via simulation, and their respective contributions are shown in Fig. 2-8. The

result clearly shows that these toggles are only small part of the total toggling in the chip, as previously anticipated in Section 2.2.4. And also, they remain almost constant across different test scenarios.

In Fig. 2-9, Q_{DD} and Q_{EST} are analyzed and compared for both nominal and varying supply voltages. These comparisons reveal consistency in features across different chips. For a broad range of digital activities, the slopes of Q_{DD} and Q_{EST} remain almost unchanged. The slopes for chip α and chip β are identified to be around 17.1 fC/gate and 19.0 fC/gate respectively. Additionally, the response of these slopes to variations in V_{CORE} (+10% and -10% from the nominal voltage 1.8 V) is examined. This analysis accurately reflects the corresponding increase or decrease in power consumption current relative to the fluctuations in power supply voltage.

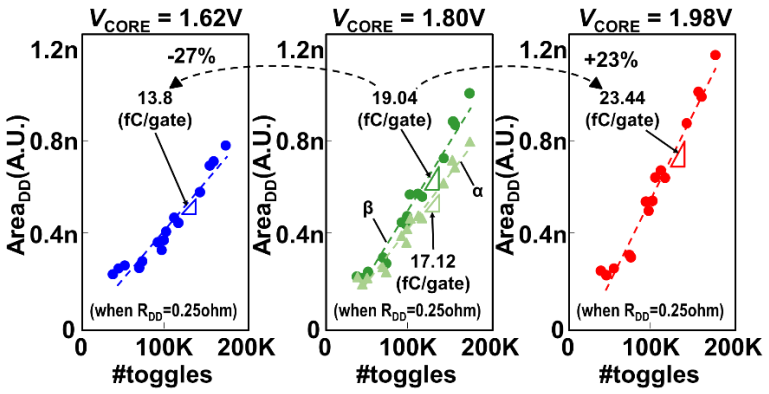


Fig. 2-9 Comparison of $Area_{DD}$(A.U.) ($\propto Q_{DD}$) and #toggles ($\propto Q_{EST}$) with variation of V_{CORE} voltage. [1] (© 2022 IEEE)

2.4.2Evaluation and example of diagnosis

By conducting transistor-level simulations, as shown in Fig. 2-10(a), with typical process, voltage, and temperature (PVT) conditions, the charge consumption for a NAND2 gate, Q_{NAND2}, is calculated to be approximately 33 fC (Fig. 2-10(b)). The slopes of Q_{DD} against the number of toggles measured for chip α and chip β are found to be nearly half of Q_{NAND2}. This observation suggests that the charge-based diagnosis method proposed can resolve down to the activity of a single NAND2 gate.

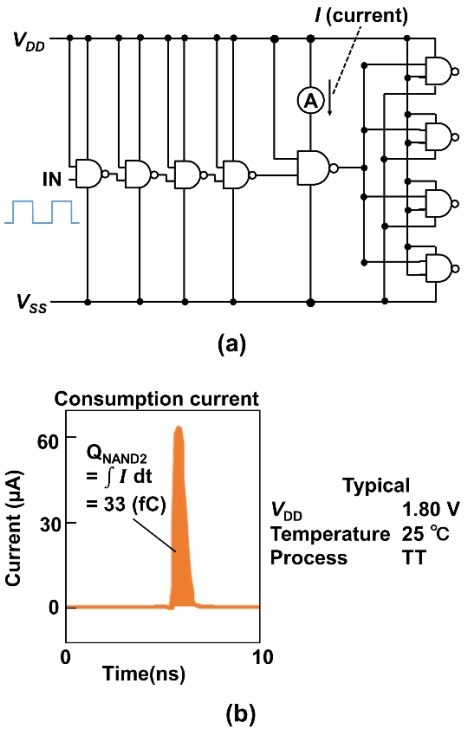


Fig. 2-10 (a) Evaluated circuits to derive Q_{NAND2} and (b) consumption current waveform of Q_{NAND2} with typical PVT condition. [1] (© 2022 IEEE)

The result of example diagnosis is shown in Fig. 2-11. Initially, a significant discrepancy was found in the test scenario #7 during the on-chip IR-drop-based PS diagnosis, as shown in Fig. 2-11 (left). This discrepancy came from an incorrect setup in the ATPG for ePTG for the test scenario #7. Subsequently, the test scenario #7 was revised and re-diagnosed, as shown in Fig. 2-11 (right). The correction in the ATPG setup is now verified by the comparison between Q_{EST} with Q_{DD}. If this diagnosis has not been conducted, the ePTG might have resulted in a smaller IR drop, potentially leading to erroneous responses in other circuits or false negative in IC-testing.

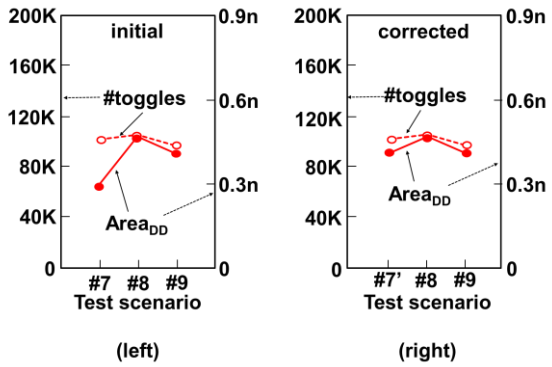


Fig. 2-11 On-chip IR-drop-based PS diagnosis,
(left) with initial set of ePTG test vectors,
(right) with corrected set of ePTG test vectors [1].
(© 2022 IEEE)

2.5 Conclusion

A technique for dynamic IR-drop-based PS scenario-based testing and in-field diagnosis is demonstrated using 0.18 µm CMOS test chips, which incorporate cryptographic functions and ePTG cores. This technique enables the precise monitoring of on-chip PS voltage waveforms, effectively capturing the evolution of charge consumption in a synchronous digital system. The evoluation of the charge consumption, Q_{DD}, derived from IR-drop waveform captured by OCM is compared against the estimated charge consumption, Q_{EST}, in gate-level logic simulation. Any discrepancy in charge consumption compared to a reference, either a golden sample or simulation data, indicates potential errors in either the test scenario or the digital circuit implementation. This helps to diagnose circuits designed to induce toggles or consume power without generating signal output, which equalize, flatten or stabilize power delivery in the background of primary circuits.

The proposed dynamic IR-drop-based PS diagnosis flow is realized by a high-resolution evaluation technique for PS noise by both simulation and measurement. This high-resolution PS noise evaluation technique contributes to understand the behaviour of PS noise in cryptographic circuits, which is a source of SC leakage.

Section 3

Packaging technology for countermeasure against side-channel leakage

3.1 Introduction

To maintain homogeneous as well as heterogeneous developments in VLSI systems, power and signal integrity (PSI) has been elaborately achieved. Capacitors play a crucial role in ensuring stable and efficient power delivery for high-performance circuits and also in mitigating unintended inter-circuit interference caused by power noise coupling. Demands for system performance enhancements are driving the requirement for higher density and increased total capacitance, as well as a more compact footprint and a lower profile. In addition, there is a growing requirement for higher voltage tolerance and reduced electrical impedance. These requisites are prompting advancements in silicon (Si) wafer processing and the development of post Si packaging technology platforms.

On-die capacitors with high density are realized using metal-insulator-metal (MIM) configurations. MIM is a structurte with thin layers within a metal stack or through deeply etched trenches filled with dielectric and metal. Package capacitors often utilize multi-layer ceramic capacitor (MLCC) surface mount discrete components (SMD). These are placed either under the IC chip, known as land side capacitors (LSC), or adjacent to the IC chip, referred to as die side capacitors (DSC). Both on-die and package capacitors are increasingly being integrated within the packaging interposer of high-performance large IC chips in mass production, such as microprocessors [17] and FPGAs [18]. This integration aims to achieve total capacitance and efficiently decoupled utilization of semiconductor manufacturing sites with different technological nodes. Various technology platforms among

literature include thin film multi-layers within a plastic interposer [19], MIM and deep trench (DT) capacitors on a silicon interposer [20][21], DT capacitors created via wafer-to-wafer bonding [22], among so on.

While most of those capacitor technologies are proposed for 2.5D interposer assemblies [23], further developments are expected for PSI in 3D VLSI systems [24][25][26]. In the rest of the Sect.3, we explain and demonstrate the deployment of capacitors throughout a 3D CMOS chip stack utilizing backside buried metal (BBM). And also, we show the advantages of 3D-embedded capacitance from a hardware security standpoint.

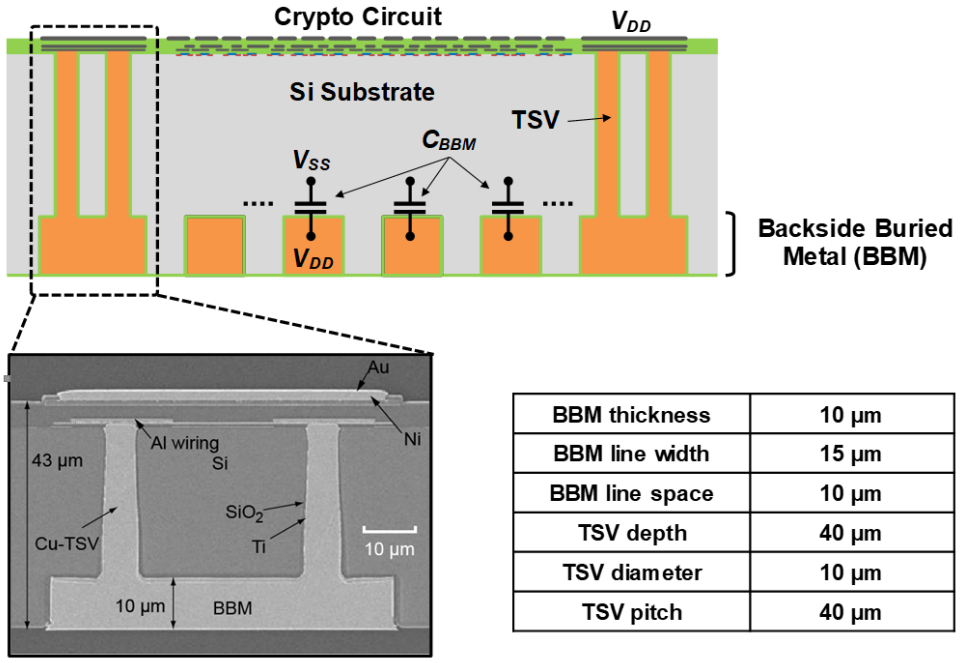
The backside of a silicon substrate is a valuable space for integrating passive elements, almost isolated from the design limitations imposed by the transistor technology on its front side. The BBM technique applied post-CMOS at wafer level enables to form thick and wide copper (Cu) stripes buried from Si backside [27]. Electrical connections between BBM and front metal are made via through Si vias (TSVs). This approach of dual-side metallization has realized the creation of a passive in-package low-impedance power delivery [28], as well as a monolithic CMOS chip featuring backside attack protection circuits [29]. The development of silicon backside technologies aligns with the trend towards enhancing near-core power supply functionality, such as the development of a monolithic power delivery network in scaled technologies approaching the 3 nm node [30][31] and the functional integration of in-package magnetic core inductors [32].

In the rest of Sect. 3, the use of backside Si for integrated passives and routings for power delivery in a secure 3D CMOS chip stack typically with cryptographic functions is demonstrated [33]. Section 3.2 shows power delivery network architecture using BBM. Section 3.3 details a demonstrator fabricated through wafer level processing and assembled in a system. Measurement results will be described in Sect. 3.4. A brief summary will be given in Sect. 3.5.

3.2 CMOS power delivery with BBM

The BBM routing, depicted in the cross-sectional view of Fig. 3-1, is created via post-CMOS processing at the wafer level. In digital ICs composed of standard CMOS logic cells, the V_{SS} (ground) nodes are connected to a p-type silicon wafer via silicon substrate contacts. Therefore, the BBM routing is exclusively allocated for the V_{DD} (power supply) side of the power delivery network (PDN), targeting the side and

bottom wall capacitances, C_{BBM}, which are distributed across the entire backside of the chip as shown in Fig. 3-1. This BBM distributed capacitor is designed for suppression of PS noise over a chip. The BBM PDN interfaces with the front side PDN through TSVs located only at the I/O pad areas along the die's edge, thereby avoiding any disturbance to the core transistors within the logic cell array. As depicted in Fig. 3-1, the BBM PDN features Cu that is over ten times thicker and wider than the typical top-layer metal wiring on the front side. This structure significantly reduces the on-chip PDN impedance, which is particularly beneficial for large-area digital IC chips that implement complex algorithms, such as public-key cryptography.



BBM thickness	10 μm
BBM line width	15 μm
BBM line space	10 μm
TSV depth	40 μm
TSV diameter	10 μm
TSV pitch	40 μm

Fig. 3-1. BBM structure (SEM photo form [29]) [2].

Fig. 3-2 depicts the 3D configuration of the BBM PDN. The backside of an upper tier is equipped with V_{DD} and V_{SS} BBM cross trunks directly connectted to the μbumps on the front side of the tier below. These μbumps are placed on Al pads and are arranged to align with the V_{DD} and V_{SS} top metal cross trunks at central region of the CMOS frontside. All the remaining parts of the BBM are allocated to the V_{DD} domain, where they form dense mesh structures to enhance PDN capacitance against Si substrate biased to V_{SS}. Both the V_{DD} and V_{SS} domains are interconnected tier-to-tier vertically through the BBM cross trunks and the TSVs located at the

periphery of the chip. As a result, the capacitance of the BBM PDN is uniformly distributed over the entire 3D stack.

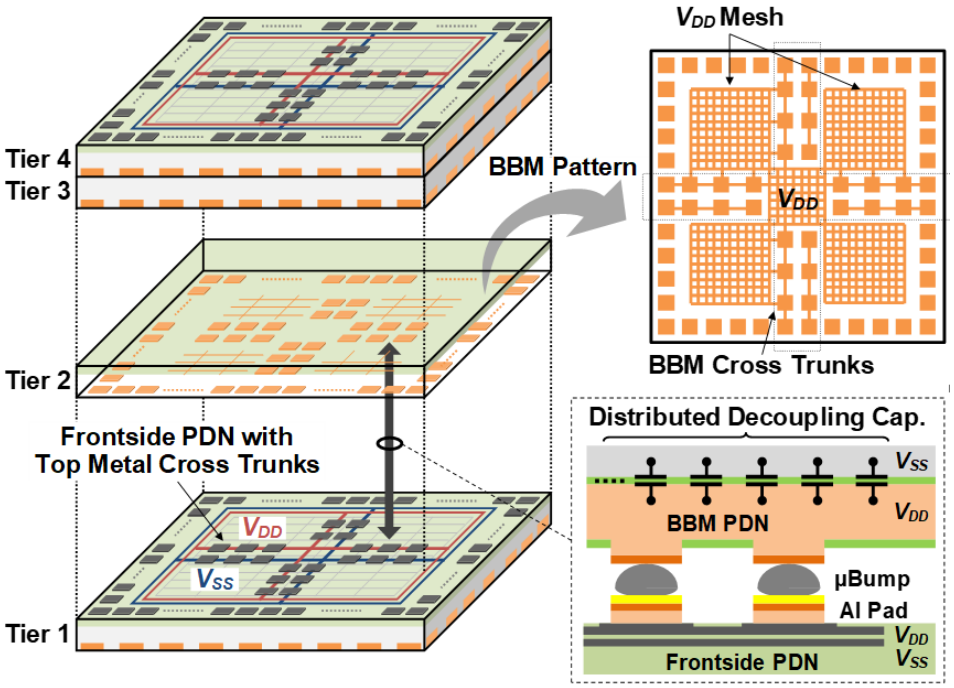


Fig.3-2. Proposed 3D stack with BBM PDN [2].

For the assembly process, flip-chip ball grid array packaging is utilized. The first chip faces to a fine-pitch plastic interposer, where μbumps located on the sirst chip's peripheral pads are directly contactted with the Al lands on an interposer. The other chips are stacked in a uniform manner. Fig. 3 shows both the structural view and the cross-sectional images of a four-tier 3D stack test sample. The BBM on the top tier becomes exposed once the stack is decapsulated. This top-tier BBM can be separated from the PDN and externally biased to a clean voltage, for the purpose to utilize top layer BBM as electromagnetic (EM) shielding.

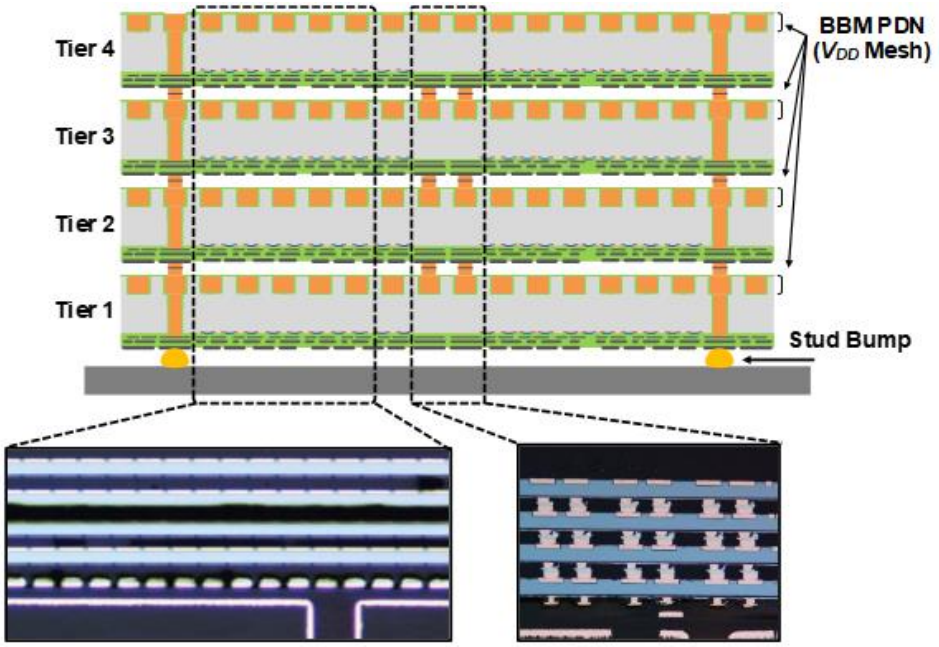


Fig. 3-3. Photos of 3D stacking structure with BBM PDN [2].

3.3 Silicon demonstrator details

3.3.1 Power delivery

The equivalent circuit of a single-chip implementation of the BBM PDN is depicted in Fig. 3-4(a). In this structure, a digital core is powered by an on-chip μVRM with the BBM capacitance, C_{BBM}, formed between the core V_{DD} and V_{SS}. Within the silicon demonstrator, cryptographic functions are implemented in the digital core. For enhanced power delivery efficiency, the chip is mounted face-down on a plastic interposer, allowing for the integration of land-side capacitors (C_{LS}). However, a series impedance resulting from routing and contacts (Z_{IP}) is an unavoidable aspect of this structure.

In a 3D stack structure shown in Fig. 3-4(b), chips equipped with BBM and TSVs are connected in a 3D stack. This structure aimes to optimize energy efficiency for parall cryptography operation. It should be noted that the capacitance of C_{BBM} for V_{DD} is incorporated in every tier, while the placement of C_{LS} is limited to the first tier. Thanks to the distributed capacitance of C_{BBM} and vertical PDN connections, the efficiency of C_{BBM} is not affected by the series impedance between stacked tiers.

Over the 3D stack, V_{SS} is uniformly maintained, while the V_{DD} of each tier is regulated by the μVRM. The V_{DD} voltage is produced in reference to V_{SS} which is a

global reference voltage. As a result, the BBM plays an important role in significantly lowering the parasitic impedance, primarily within the V_{DD} region. This contributes to an improvement of power delivery efficiency over the whole 3D stack.

While VSS is unified over the whole 3D stack, VDD on a respective tier is regulated by the µVRM or even halted in a power-down mode for logic circuits, where the VDD voltage is generated with respect to VSS as the global reference voltage. The BBM then lowers parasitic impedance primarily on the VDD domain and consequently improves the capacity of power delivery in the whole 3D chip stack.

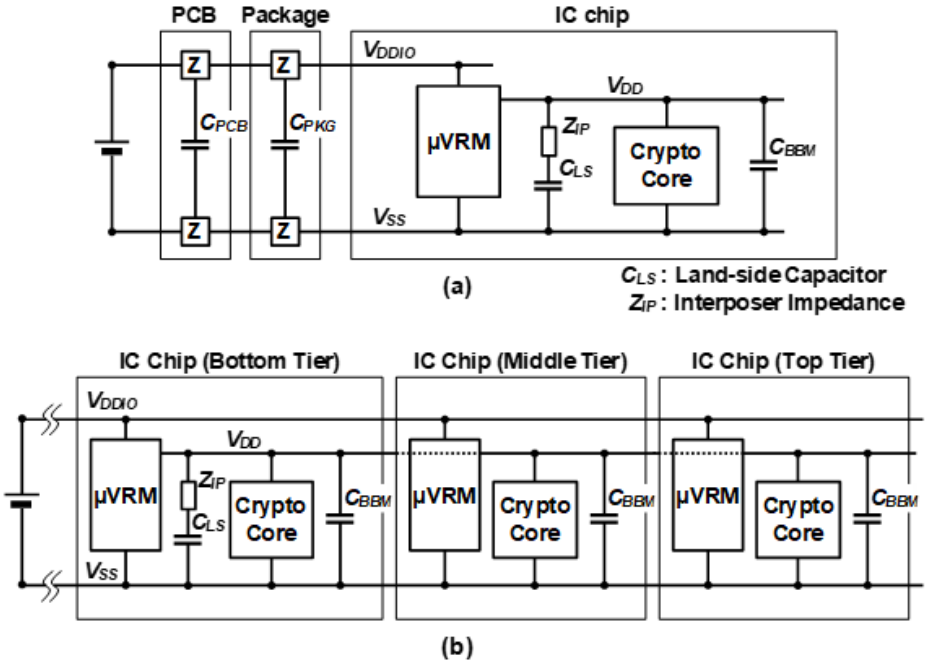
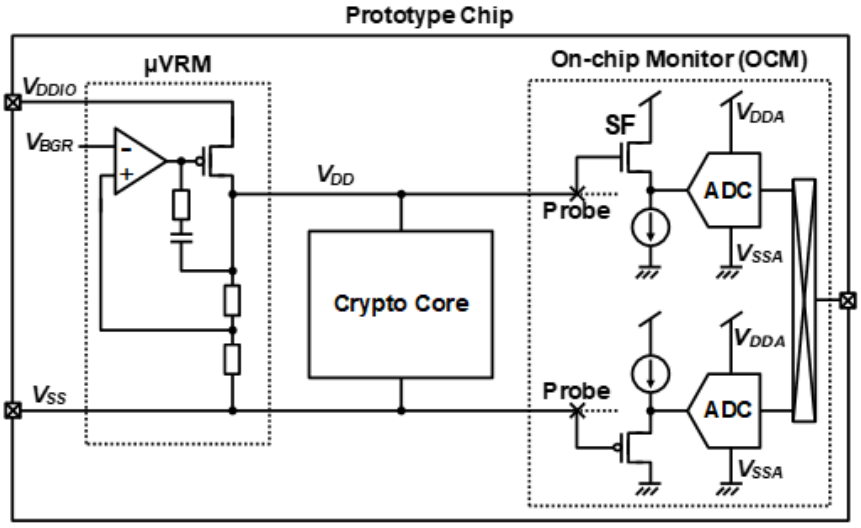


Fig. 3-4. Equivalent circuit of (a) single chip with BBM PDN, and (b) 3D stacked chip with BBM PDN [2].

3.3.2 Functionality

Prototype IC chips are designed and fabricated using 0.13 µm 6-layer metal CMOS technology. The circuit configuration of the prototype chip is shown in Fig. 3-5. This chip incorporates several types of cryptographic algorithms as detailed in the table. The public-key cryptographic cores are based on elliptic curve cryptography. The number of 2-input NAND equivalent gates of those cryptographic cores range from 2.9 to 4.3 million and implemented within the same chip dimensions of 12 x 8 mm². These digital cores are powered either by a single µVRM

or dual μVRMs, positioned at the top left and bottom right corners of the chip, depending on the specific test scenario. And also, for comparative purposes, smaller-scale chips with 4 x 3 mm² dimension containing some test circuits are developed to assess the BBM capacitance.



Chip Name	Crypto Algorithm	Chip Size	Num. of Logic Gates	μVRM	OCM	BBM Mesh (Line / Space)
Public Key Crypto #1	ECC*1	12 mm x 8 mm	2.9 M	O	O	15 μm / 35 μm
Public Key Crypto #2	ECC*1	12 mm x 8 mm	3.9 M	O	O	15 μm / 35 μm
Public Key Crypto #3	ECC*1	12 mm x 8 mm	4.3 M	O	O	15 μm / 35 μm
Private Key Crypto	AES*2	4 mm x 3 mm	203.5 K	O	O	15 μm / 10 μm
Digital TEG Chip	-	4 mm x 3 mm	70.8 K	O	O	15 μm / 10 μm
Analog TEG Chip	-	4 mm x 3 mm	0.1 K	-	-	15 μm / 10 μm

*1 Elliptic Curve Cryptography *2 Advanced Encryption Standard

Fig.3-5. Circuit configuration of prototype chips [2].

Each chip contains an OCM function which enables the measurement of voltage fluctuations at the V_{DD} and V_{SS} nodes [25][28]. The OCM channel has a source follower (SF) for sensing the target voltage at its input and a following 11-bit successive approximation register (SAR) analog-to-digital converter (ADC) for converting the on-chip voltage into a digital format. The SF with n- and p-channel MOSFET are prepared for the core V_{DD}, nominally set at 1.5 V, and V_{SS}, at 0.0 V, to generate both negative and positive offset DC voltages at the SF's output. With offsets given by SF, the power noise voltages are aligned within the ADC's input voltage range.

Fig. 3-6 shows photos of both the frontside CMOS and the BBM on an identical chip. The cross trunks with μbump and the meshes of the BBM PDN are shown in enlarged images around the die center reasion.

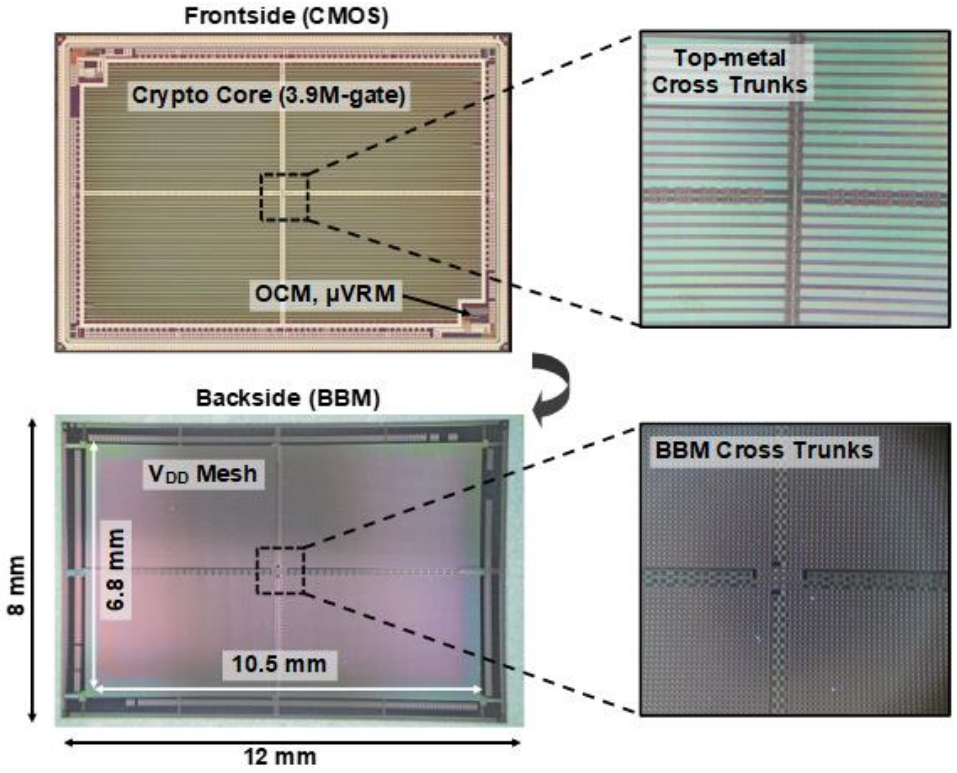


Fig.3-6. Photos of frontside CMOS and backside BBM of fabricated chip (public key crypto #2) [2].

3.4 Measurement results

3.4.1 Passive impedance measurements

The measurement results of capacitance between V_{DD} and V_{SS} for each standalone (not staccked) chip are shown in Fig.3-7. These measurements were conducted both with and without the BBM PDN. This capacitance includes the inherent capacitance, due to frontside CMOS circuits, and C_{BBM} which are separated out using linear regression and subsequently detailed in Fig. 3-8. The BBM mesh density varies between smaller and larger chips, resulting in capacitances of 0.25 nF/mm^2 and 0.18 nF/mm^2 respectively. For larger chips, the total distributed BBM capacitance over the 4 x 3 mm^2 dimension is 12.8 nF.

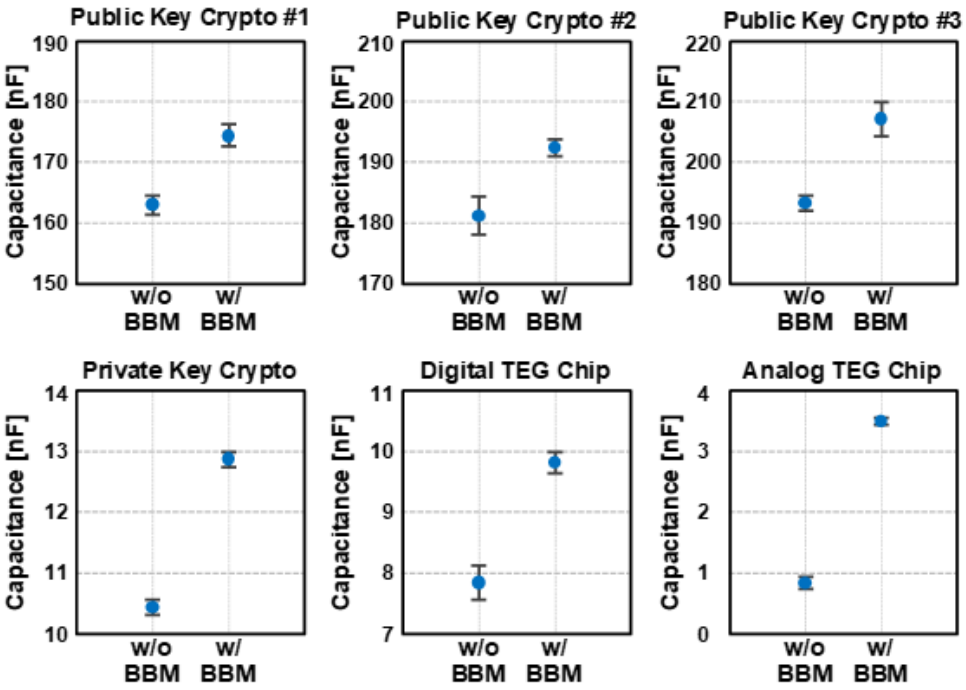


Fig. 3-7. Measured BBM capacitance of single chip [2].

Element	BBM	MOM	MIM	Gate Cap.
Unit Capacitance	Mesh #1 L=15 μm S=35 μm 0.18 fF/μm² / Mesh #2 L=15 μm S=10 μm 0.25 fF/μm²	≈ 1 fF/μm²	≈ 2 fF/μm²	≈ 4.2 fF/μm²
Density	≈ 100 % (Filled with meshes)	< 90 %	< 70 %	< 20 %
Capacitance per 1mm²	Mesh #1: 0.18 nF/mm² / Mesh #2: 0.25 nF/mm²	0.9 nF/mm²	1.4 nF/mm²	0.84 nF/mm²
Area Overhead	No area-overhead	All metal and device layers occupied	Top 2 metal layers occupied	M1 and device layers occupied

Fig. 3-8. Summary of BBM capacitance and comparison with other capacitive elements [2].

The capacitance formed by BBM is approximately 4x to 8x lower, relative to standard in-circuit structures like metal-on-metal (MOM) and MIM capacitors. However, it should be noted that the utilization of BBM capacitors avoids the need to sacrifice frontside core areas (area overhead). The area overhead is huge also in the method of transistor gate electrodes, though the method presents the highest capacitance. These comparative assessments are carried out through manual layouts and simulations using the physical design kits and rules of the given technology.

3.4.2 On-chip IR drop measurements

V_{DD} and V_{SS} waveforms are measured by OCM on the first tier during the operation of cryptographic engine, public-key crypto algorithm #2 in Fig. 3-5. As shown in Fig. 3-9, the waveforms are captured in different configurations: demonstrators with and without BBM, as well as in single and 3D chip stacks with 2 and 4 tiers. The vertical axis of the graph represents the voltage in steps of the least significant bit (LSB) of the ADC and incorporates the DC offset voltage of the SF. One LSB is equal to 0.73 mV in our setup. The horizontal axis is time and a sampling interval, controlled by an external data timing generator, is 1.0 ns.

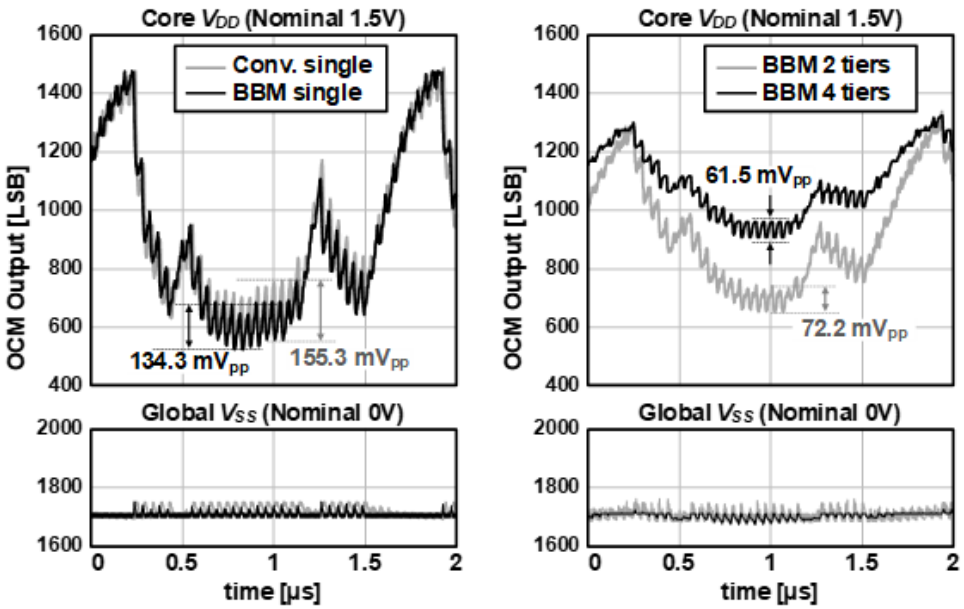


Fig. 3-9. Measured V_{DD} and V_{SS} waveforms during operation of public key crypto #2 [2].

Periodic voltage fluctuations on V_{DD}, known as dynamic IR drops, occur in syncchronization with clock and are linked to the internal processes of adding and multiplying binary data with the width of 256 bits or more. The large number of logic gates in these arithmetic functions toggle continuously for each clock cycle, which makes a maximum clock frequency limit of 30 MHz. Also, low-frequency voltage droops correspond to the logical activities within the algorithm. The results in Fig. 3-9 indicate that both periodic and low-frequency voltage variations are more effectively mitigated in 3D stacks with a greater number of tiers. In contrast, the voltage across V_{SS} nodes remains almost the nominal ground voltage, which shows the robust integration of V_{SS} networks within the stack. The utilization of BBM stripes in the V_{DD} domains is validated as effective.

The peak-to-peak voltage variation is extracted from the waveform data and is plotted in Fig. 3-10 for a comparison between conventional stacks and stacks with BBM. In the comparison of the dynamic IR drops on V_{DD} nodes, it is observed that a four-tier stack with BBM capacitors achieves a 59% reduction in these drops.

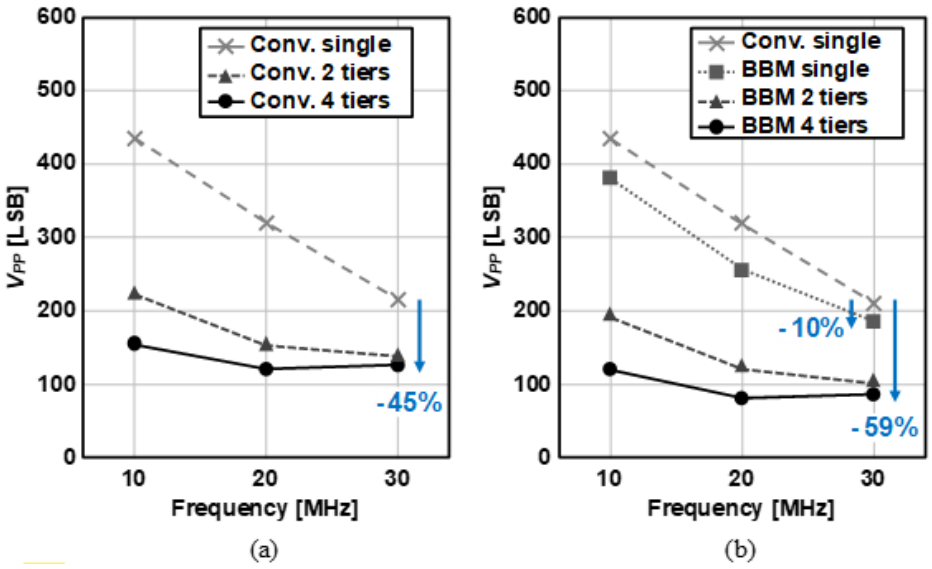


Fig. 10. Peak-to-peak values of VDD noise versus operation frequency in public key crypto #2. (a) conventional stacks and (b) proposed BBM stack [2].

The impact of BBM in decreasing series impedance is calculated to be approximately 42%, as shown in Figure 3-11. This impedance value is determined from the slopes of the DC voltage drops measured with changing clock frequency. During this evaluation, the cryptographic cores are inactive and only clock baffers toggle.

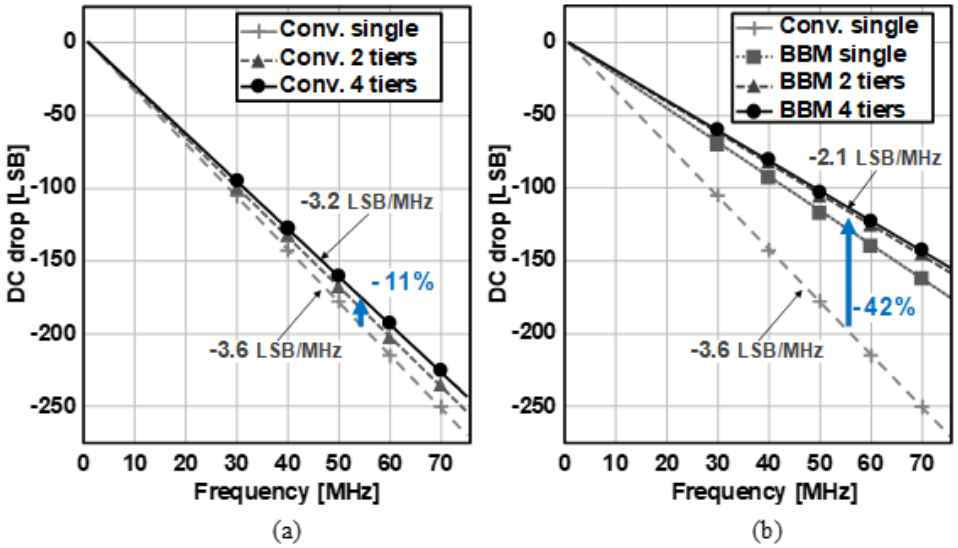


Fig. 3-11. Measured DC drop versus clock frequency when clock buffers are only operated. (a) conventional stack, and (b) proposed BBM stacks [2].

3.4.3 EM side-channel leakage measurements

The distributed BBM capacitance effectively reduces dynamic IR drop and it contributes to the reduction of electromagnetic SC leakage during cryptographic operations. The experimental setup for SC leakage evaluation is shown in Fig. 3-12. An EM probe sences local electromagnetic waves radiated from the demonstrator and the output from the EM probe is amplified and recorded by an oscilloscope. This local EM emission is primarily caused by the dynamic power current of the cryptographic core. Therefore, the EM emission is linked to internal logic operations that handle sensitive information. To assess how dependent EM waveforms during cryptographic processing are on secretdata, we employed the statistical t-test method on the gathered waveforms. A t-test value exceeding 4.5 indicates a statistical significance and the siginificance may lead to SC leakage. This SC leakage evaluation method leveraging t-test has been often used since the evaluation methodology is proposed and named as test vector leakage assessment (TVLA) methodology in [34].

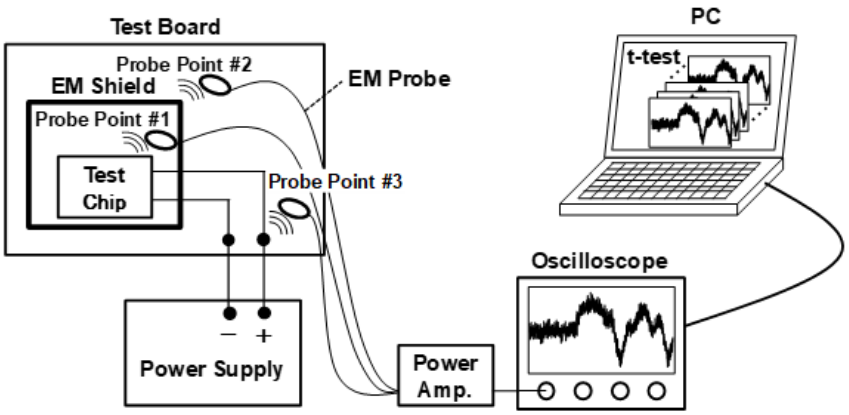


Fig. 3-12. Experimental setup for SC leakage evaluation [2].

T-test evaluation is conducted for two two large sets of EM traces emitted from the demonstrator during cryptographic core operation. In one set, a specific dataset is used consistently across all cases, while in the other, a new dataset is randomly generated for each input. EM measurements are alternately conducted for these two experimental set until the number of TM traces gathered reaches 20,000. Each EM trace stored in the oscilloscope is the trace after averaging five EM traces captured during iterative cryptographic operation.

First, we conducted measurements of local EM emissions at measurement point #1 indicated in Fig. 3-12, the point just above the stack. The single chip equipped with BBM has the highest SC leakage, as shown in Fig. 3-13. This result is reasonable considering that the power current consumed by the cryptographic core flows through the BBM is strongly coupled to the EM probe near the backside surface of the chip. The leakage is clearly suppressed with an increasing number of chips in a 3D stack. This can be attributed to the power noise suppression due to the BBM capacitance distributed throughout the stack. The number of EM traces required to achieve statistical significance in the four-chip BBM stack is approximately same as that for a single chip without BBM. Our experiments also verified that SC leakage is not suppressed in conventional multi-tier 3D stacks without BBM. Notably, when the single chip is shielded with Al sheat biased to clean voltage regulated from an external voltage source, as measured at point #1 in Fig. 3-12, the t-value does not exceed 4.5 even with 20,000 test cases.

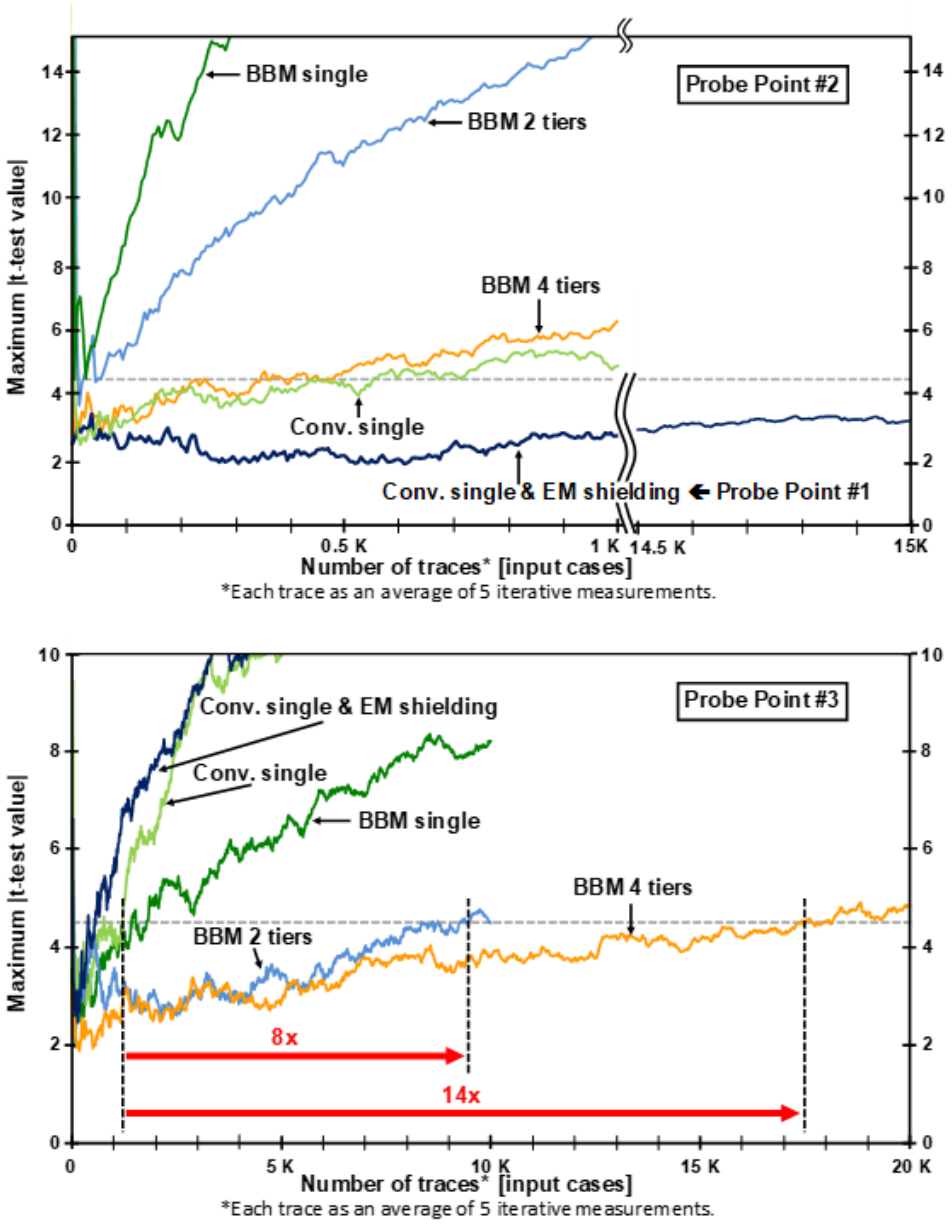


Fig. 3-13. T-test results of SC leakage measurements [2].

Second, EM measurements were conducted at the point #3 in Fig. 3-12, the point above the power supply terminals on the printed circuit board (PCB). This method allows for leakage evaluation by potential adversaries who may not have detailed knowledge of the internal structure of the device. The t-test values in Fig. 3-13 show a comparison between the conventional public-key cryptographic demonstrator and those with 3D BBM stacking. The leakage was effectively suppressed in the case of the four-tier BBM stack. This increased the number of EM traces required to reach t

test values greater than 4.5 by a factor of 14 compared to the conventional single chip. Similarly, an 8 times increase was observed in the two-tier BBM stack setup.

In the first setup, EM waves are emitted from the backside of the cryptographic chips, while in the second setup, they are generated on the board due to power current flowing from the on-die μVRMs, which have lowpass characteristics with a limited bandwidth. Although EM radiation is somewhat present in these measurements, the statistical significance among EM traces is significantly reduced by the distributed BBM capacitance.

3.5 Conclusion

The effectiveness of the BBM PDN in 3D CMOS stack has been assessed using Si demonstrators that incorporate cryptographic engines and OCM systems. Utilizing post-wafer BBM processing on 0.13-micrometer CMOS wafers, a capacitance of 12.8 nF was formed across the entire backside of the chip. These chips with BBM stacked in configurations of up to four layers was assembled using flip-chip packaging techniques.

One significant benefit of this BBM capacitance is the efficient reduction of dynamic IR drop in the power nodes of the stack. The reduction of approximately 59% in voltage variation was achieved. In terms of suppressing SC leakage, the 3D BBM-stacked structure achieved 14 times improvement compared to traditional single-chip.

The implementation of BBM PDN in 3D chip stacking introduces innovative option for enhancing the resilience against SC attack. This implementation level option should be used in the comboination with circuit level and algorithm level countermeasure techniques.

Section 4

Crypto core level side-channel leakage simulation

4.1 Introduction

Cryptographic hardware modules face a risk of SC analysis hat reveals secret data by analyzing a device's power consumption, such as Differential Power Analysis (DPA) [35]. Masking [36] is a countermeasure against SC attack widely adopted. It removes power consumption’s dependence on sencitive information by randomizing all intermediate values. Standard masking countermeasure offered provable security, assuming circuits are free from unintended signal transitions, such as glitches. However, completely eliminating glitches in circuits consist of CMOS standard logic cells is generally impossible.

To address this challenge, advanced masking techniques like Threshold Implementation (TI) [37] and Domain-Oriented Masking (DOM) [38] have been proposed. TI was the first technique integrating glitch tolerance into masking schemes. Subsequently, DOM was introduced, offering both a reduction in circuit size overhead and a decrease in required randomness, while keeping the same security level as TI. Both TI and DOM provide provable security under the assumption that power consumption of the shares inside cryptographich module is independent.

For SC leakage assessments, two measure metrics exist. The first is the Measurement to Disclosure (MtD), which determines the number of measurement or simulation waveforms required to extract secret information through SC analyses like DPA or Correlation Power Analysis (CPA) [39]. The second metric is TVLA [40], which is used to assess the potential for leakage. In TVLA, the t-test index is calculated to determine the statistical significance of differences between groups of divided measurement or simulation waveforms. TVLA is more sensitive than MtD

and it enables exploring of SC leakage resilient implementation without requiring a complete crptographic algorithm.

Generally, the effectiveness of countermeasures against SC attacks is assessed after Si manufacturing stage. However, post-silicon evaluation approach has two problems. Firstly, fabricating Application Specific Integrated Circuit (ASIC) chips for evaluation purposes is an expensive and time-consuming. If vulnerabilities to SC attacks are discovered during this stage, a re-spin with countermeasure is necessary, which substantially increases costs and extends timelines. As a workaround, Field Programmable Gate Arrays (FPGAs) are often used in stead of ASICs for evaluation. However, the power consumption profiles of FPGAs and ASICs vary, even when both of them execute the same cryptographic functions. The second issue is that while post-silicon evaluation can confirm the effectiveness of countermeasures, it is challenging to identify the source of leakage if unforeseen leakages occur. This makes it difficult for designers to implement countermeasures during the re-spin phase. Considering these factors, there is a clear need for a pre-silicon method of evaluating SC leakage.

Various pre-silicon SC leakage evaluation techniques have been reported [41,42,43,44,45,46,4748]. These methods can be categorized into two main types, one employing logic simulations and the other utilizing transistor-level simulations. Logic simulation, known for its high simulation speed, is particularly useful during the early stages of design. On the other hand, transistor-level simulations such as SPICE offer high accuracy but require more computational time. The choice between these simulations depends on the balance between the desired accuracy and the available time for simulation. SPICE is frequently chosen for in-depth or complex evaluations of SC leakage.

This paper discusses optimizing the Analysis Time-Step (ATS) creation within SPICE to improve simulation efficiency may lead to false positives when verifying the security order of masked circuits. While SPICE-generated analog waveforms are reliable for verifying timing-accurate circuits, the statistical variations in power supply noise amplitude in SPICE simulations may not be accurate for SC leakage evaluations. We use a simple nonlinear function designed with the DOM scheme as an example to explore the unpredictability in SPICE-based SC leakage evaluations.

The structure of the rest of the section 4 is as follows. Sect. 4.2 discusses the masking countermeasure against SCA. Sect. 4.3 explains quantitative metrics for SC leakage evaluation. Sect. 4.4 describes the methodology for SC leakage evaluation

using simulation techniques. In Sect. 4.5, we present our experimental setup and results, demonstrating the unpredictability of SPICE simulations in evaluating SC leakage of masked cryptographic circuits. The paper concludes in Sect. 4.6 with a discussion on potential solutions.

4.2 Masking scheme

Since the first report of SC analysis in 1999, numerous studies have focused on reducing SC leakage through various logical or physical design countermeasures. Physical design countermeasures focus on minimizing SC leakage through power balancing techniques [49,50], while logical countermeasures aim to disrupt the correlation between power consumption and sensitive information.

One primaly logical countermeasure is masking [36], which effectively disrupt the correlation between power consumption and confidential data by dividing security-critical logic values into various shares. The effectiveness of a masking scheme against SC attack is typically evaluated using probing model proposed by Ishai *et al.* [51]. The model measures the number of probes an attacker would require to get secret information from the masking scheme. A cryptographic module that can secure against an attack using d probes is considered to have d-th order security. The number of probes in this d-probing model corresponds to the attack order in DPA CPA [52,53].

Earlier masking schemes' security were mathematically proven based on certain assumptions about the hardware. However, authors in [54] showed that standard masking schemes fail to counter SC attacks when glitches, unintentional togles at the output of a gate, occur in digital circuits. These glitches are inevitable in circuits based on standard logic cells. Consequently, modern masking approaches like TI [37] and DOM [38] have been developed with tolerance for these glitches. DOM attains the same security level as TI while requiring a smaller circuit footprint and fewer fresh random bits [38]. Both of these masking schemes provide provable security under the condition that information leakage is the linear sum of leakages from individual shares, known as the independent leakage assumption.

However, some works [55,56] have shown that physical layout and measurement setup might decrease the security effectiveness of these glitch-resistant masking schemes. These works have demonstrated a reduction in security order through experiments on FPGAs and have suggested possible causes. Factors such as

proximity of placement, on-chip PDN, and off-chip PDN are said to create nonlinear interactions among the independent shares, which lower the security order. The exact mechanisms behind this secutiry order reduction remain unclear, making it challenging to implement hardware masking schemes without reducing their security order. A deeper understanding of the sources of this security order reduction is essential to develop methods for effectively implementing masking schemes without reducing their security level.

4.3 Side-channel analysis simulation

Simulation-based security evaluations are crucial for hardware designers to pinpoint vulnerabilities and confirm security requirements during the design phase. There are a variety of simulation methods for assessing SC leakage as reported in several works [41,42,343,44,45,46,47,51]. Some methods employ gate-level logic simulations combined with specific power consumption models for standard logic cells, which allow for high-speed evaluation. Others rely on detailed transistor-level circuit simulations, such as SPICE simulators, which deliver electrically precise results but are limited by the circuit size they can handle due to computational capacity. Due to its high accuracy, SPICE is particularly valuable for SC leakage assessments in complex scenarios, such as verifying SC leakage in Boolean masking circuits resistant to glitches. This kind of accurate analysis with SPICE can unravel complex causes behind SC leakages, which provide insights for enhancing hardware security.

SPICE, an open-source tool for simulating electrical performance of circuits, was initially introduced by the University of California, Berkeley in 1973 [57]. Since its first release, Berkeley SPICE has undergone multiple revisions to enhance both its accuracy and the size of circuits it can handle. Nowadays, various companies have developed commercial versions of SPICE-based transistor-level simulation tools. Throughout these revisions and developments, selecting an appropriate ATS has been one of the most importanr point to ensure convergence, accuracy, and efficiency. Berkeley SPICE’s variable time-step transient analysis utilizes either the trapezoidal or Gear integration method, adjusting the ATS internally based on local truncation error [58]. The ATS dynamically changes during a simulation, becoming finer when there are steeper voltage (or current) changes over time among the circuit's internal nodes, as depicted in Fig.4-1. While users can preset a maximum ATS to balance

analysis accuracy with computation time, the minimum ATS is automatically constrained by the algorithm to ensure convergence. Modern SPICE-based transistor-level simulators, offered by various companies with distinct internal calculation algorithms, are widely trusted by IC designers, often without in-depth consideration of these internal mechanisms. As these simulators are not open-source, it's challenging for IC designers to fully understand the algorithms used inside the tools.

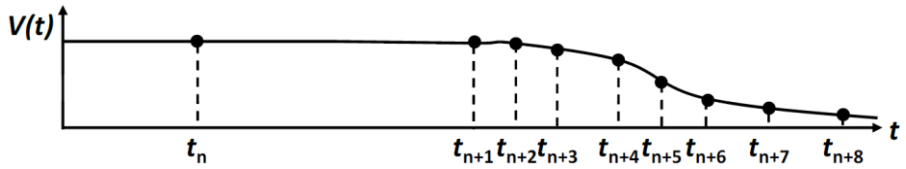


Fig. 4-1. A variable time-step in SPICE [3]. (© 2023 IEEE)

In this paper, we show that power noise waveforms generated by SPICE simulation may not always be accurate for evaluating SC leakage, despite their reliability in verifying circuits with precise timing. ATS of SPICE simulation can lead to false-positive in the security order assessment of masked circuits.

4.4 Side-channel evaluation metric

For evaluating SC leakage, power traces from simulations or actual measurements are analyzed using specific SC analysis metrics to determine a circuit's security level. The most straightforward metric is known as MtD, which measure the resilience of a circuit against known types of attacks to confirm its security level. Alternatively, in a method referred to as TVLA, statistical hypothesis testing is employed to identify any leakage in an implementation [59,60]. TVLA has become popular in security evaluations. The details of these two metrics are explained below. Understanding the characteristics of MtD and TVLA and chosing them properly considering these characteristics is important for accurate and efficient security assessment.

4.4.1 Measurement to disclodure

MtD is a fundamental metric for evaluating SC leakage, especially in assessing a circuit's resilience against established SC attacks like DPA and CPA. MtD determines the minimum number of waveforms required to completely reveal sensitive

information. While commonly employed for SC leakage evaluations, MtD faces three challenges. Firstly, the accuracy of MtD results relies on the suitability of leakage models for each cryptographic algorithm. An improper leakage model can lead to false negative in SC leakage evaluation. Secondly, conducting SC leakage assessments using MtD reqires long time, especially for evaluating crypto modules with countermeasures. In some cases, the MtD value could escalate to several hundred thousand or even millions. The third issue is that MtD results are confined to known attack methods. Thus, if a new attack method emerges, a re-evaluation of the circuit's security is necessary.

4.4.2 TVLA

TVLA uses a statistical method Welch's t-test to evaluate SC leakage by checking for significant differences between the statistical moments of two data sets. In this process, measured or simulated waveforms are categorized into two groups based on an intermediate value. The outcome is calculated using the formula (4-1):

$$t = \frac{\mu_1 - \mu_2}{\sqrt{\frac{{\sigma_1}^2}{N_1} + \frac{{\sigma_2}^2}{N_2}}} \quad (4\text{-}1)$$

where N1 and N2 are the number of traces, μ1, μ2 represent the mean values, and σ1, σ2 are standard deviations respectively. The methodology to compute a higher order t-value is detailed in [60]. A t-value exceeding 4.5 suggests a significant statistical discrepancy between the two sets, indicating a potential correlation between data and waveforms that could be exploited by an attacker. The effectiveness of countermeasure against SC attacks are typically certified by a t-value not surpassing 4.5. Although a t-value above 4.5 doesn't mean an existence attack revealing seacret information, its high sensitivity compared to the MtD make the metric popular in SC leakage evaluations.

4.5 Evaluation details and results

For our study, we selected a simple nonlinear function F(x,y,z)=x&y^z implemented with DOM scheme as our target circuit. This arithmetic function was incorporated into data paths involving data registers first, and then synthesized into a logical circuit netlist, as depicted in Fig. 4-2. Subsequently, the core was finalized through place-and-route tools to shape its physical layout. To assess the security

order of this circuits, SPICE simulation was employed. The standard parasitic exchange format (SPEF) is utilized to integrate parasitic elements among metallic wiring for signal interconnections and the PDN in VLSI logic circuits. After completing the place-and-route phase, we extracted parasitic details from the layout and annotated them as SPEF in the netlist. This procedure enables SPICE to generate precise analog waveforms.

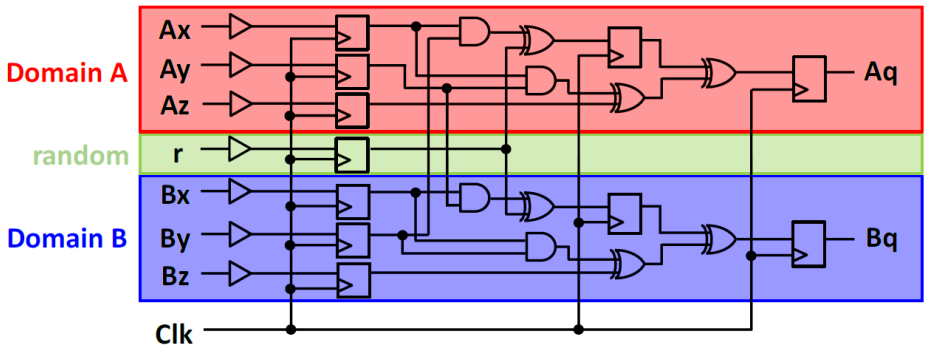


Fig. 4-2. Target circuits (F(x,y,z)=x&y^z) [3]. (© 2023 IEEE)

We demonstrate that the statistical variance in power noise amplitude produced by SPICE simulations may not accurately reflect the security level of masked cryptographic circuits. This is shown using four different verification scenarios. The maximum Analysis Time-Step (ATS) is set at either 1 ps or 10 ps. The Strobe Time-Step (STS), used for reading out time-domain simulated waveforms, is consistently set at 10 ps. Our hypothesis is that the ATS, internally calculated by the SPICE simulator, might induce statistical variations in the waveform data and these variations significantly impact the verification of security levels in cryptographic circuits, even though they are minor for timing accuracy verification. An example of such a statistical discrepancy influenced by ATS is shown in Fig.4-3. The possibility of false-positive results in security assessments can arise if there is a linkage between ATS and the logical values within a circuit. Considering that ATS is affected by fluctuations in voltage and current within the circuit as mentioned above in Sect. 4-3, it is quite possible that ATS and the logic inside the circuit are correlated.

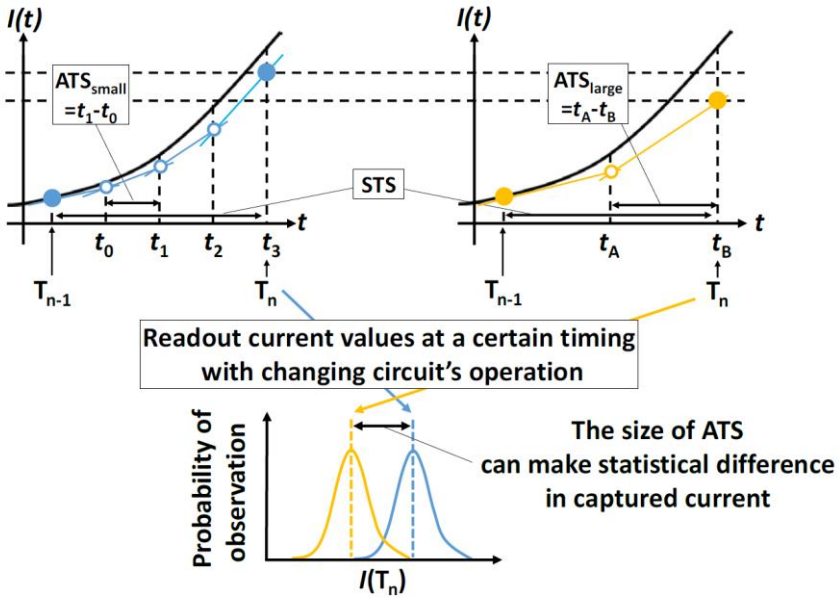


Fig. 4-3. Statistical difference caused by analysis time-step [3]. (© 2023 IEEE)

A. Verification scenario 1

The evaluation results of this verification scenario are the basis for the hypothesis that internal ATS calculations could lead to fault in security evaluation. In this scenario, the core of a masked aritjmetic function is connected to V_{DD} and V_{SS} through wiring and resistances as depicted in Fig. 4-4. SPICE simulations generate I_{VDD} waveforms while changing input data. These waveforms are divided into two sets based on the unmasked value of the function (either zero or one) for TVLA. First, we set the maximum ATS in SPICE to 10 ps. Though the arithmetic function is protected by 1st-order DOM, the first-order t-value unexpectedly becomes over the threshold of 4.5, as illustrated in Fig.4-5 (left). Subsequently, we set the maximum ATS to 1 ps for more precise simulations and repeat the analysis. In this evaluation, the results align with our expectations, indicating no leakage. It is important to note that the TVLA test for second-order security detects leakage in both cases, as depicted in Fig.4-5 (right). These results suggest that ATS can influence security verification outcomes, leading to the hypothesis that ATS in SPICE simulations could result in false positives during security order verifications.

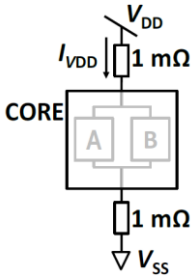


Fig. 4-4. The core connected to VDD and VSS [3]. (© 2023 IEEE)

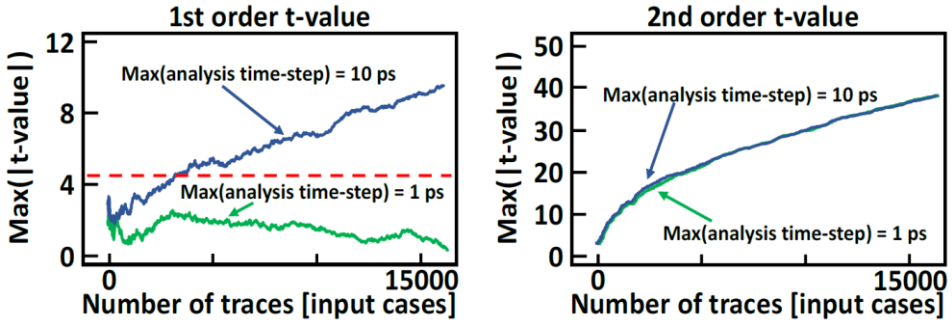


Fig. 4-5. 1st order (left) and 2nd order (right) t-test results
of verification scenario 1 with changing the maximum ATS [3]. (© 2023 IEEE)

B. Verification scenario 2

In the rest of verification scenarios, we replicated the arithmetic core to assess each instance for SC leakage to demonstrate that the ATS in SPICE simulation could lead to false-positive results in security order verification using the t-test method. First, the PDNs of these cores were connected to ideal voltage, as depicted in Fig.4-6, and this PDN structure is reffered to as ideal PDN. We assigned input data sequences, named dataset1 and dataset2, to CORE1 and CORE2 respectively. The current waveforms of each core during their arithmetic operations, I_{VDD_CORE1} and I_{VDD_CORE2}, are captured through SPICE simulations with a maximum ATS of 10ps. We first categorize the waveforms of each core into two groups based on the unmasked output values of dataset1 for the t-test evaluation. Subsequently, we conduct the t-test again on the same waveforms, but this time partitioned according to the unmasked outputs of dataset2. These evaluation results are reffered to as "t-value based on dataset1" and "t-value based on dataset2". It is important to note that the t-values of I_{VDD_CORE1} based on dataset2 and t-value of I_{VDD_CORE2} based on dataset1 should not surpass the threshold of 4.5 since dataset1 and dataset2 do not influence the operations of core2 and core1 respectively. However, considering the findings from

the first verification scenario using a maximum ATS of 10ps, we estimate that both I_{VDD_CORE1}'s t-value based on dataset1 and I_{VDD_CORE2}'s t-value based on dataset2 will exceed the 4.5. The results shown in Figure 4-7 confirm that our predictions are correct.

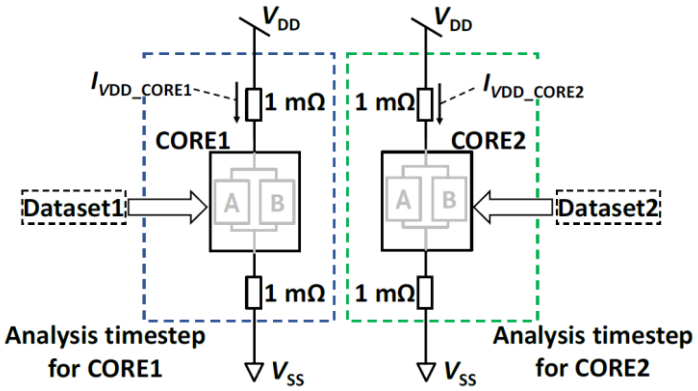


Fig. 4-6. Ideal PDN of 2 cores [3]. (© 2023 IEEE)

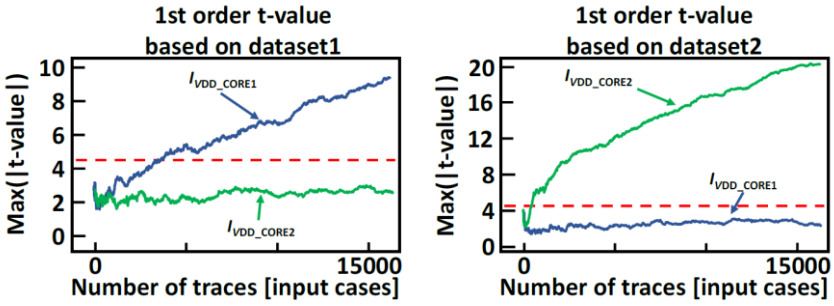


Fig. 4-7. 1st order t-test results of verification scenario 2.
t-value based on dataset1(left) and dataset2(right) [3]. (© 2023 IEEE)

C. Verification scenario 3

In the second verification scenario, two cores with ideal PDN were assessed for SC leakage and its results were same as expected. However, an ideal PDN setup like the one illustrated in Fig.4-6 does not accurately reflect actual ASIC design. In actual physical layouts, PDNs of multiple cores are interconnected through nodes that are separated from the ideal voltage source by the parasitic components of the PDN. For the third scenario, we connect the PDNs of both cores as displayed in Fig.4-8. The 0 ohm resisances represent the parasitic elements of the PDN that isolate the ideal voltage sources from the connection nodes of the two cores. This setup is referred to

as “realistic PDN”. The only difference between the ideal PDN shown in Fig.4-4 and the realistic PDN in Fig.4-8 is the presence or absence of these 0 ohm resistances, and these PDN configurations are equivalent from a circuit designer’s perspective. However, the results of this third scenario, shown in Fig.4-9, differ from those of the second scenario. In this case, the t-values for I_{VDD_CORE1} based on dataset2 and I_{VDD_CORE2} based on dataset1 surpass the threshold 4.5. This is unexpected since dataset1 and dataset2 are not supposed to influence the operations of core2 and core1, respectively. This discrepancy suggests a potential false-positive in security order verification using SPICE simulation.

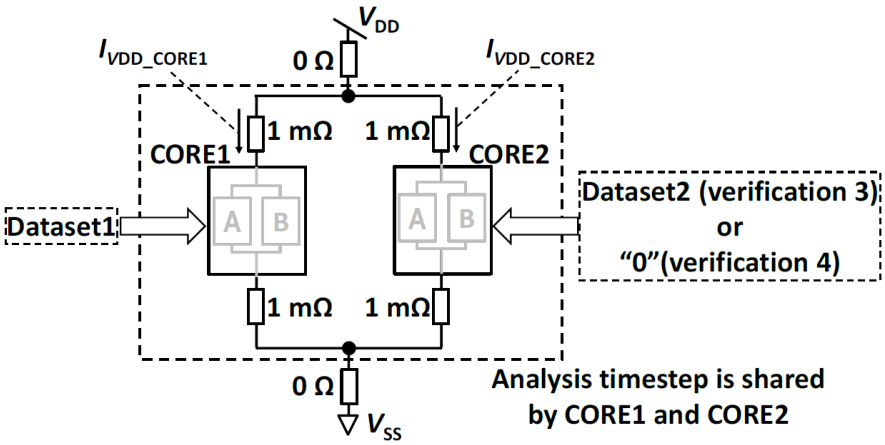


Fig. 4-8. Realistic PDN of 2 cores [3]. (© 2023 IEEE)

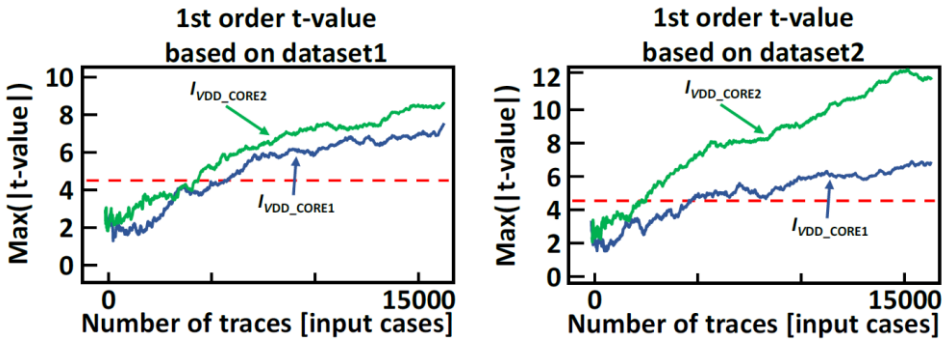


Fig. 4-9. 1st order t-test results of verification scenario 3
when the maximum ATS is 10 ps.
t-value based on dataset1(left) and dataset2(right) [3]. (© 2023 IEEE)

To validate whether the ATS in SPICE simulations leads to false-positive security evaluations shown in Fig.4-9, we replicate the evaluation with reducing the maximum ATS from 10 ps to 1 ps. We hypothesized that this smaller maximum ATS would limit ATS variations, which prevents false-positive results in security assessments. Fig.4-10 shows the results of this revised evaluation. In these results, neither the t-value of I_{VDD_CORE1} based on dataset2 nor the t-value of I_{VDD_CORE2} based on dataset1 surpass the threshold 4.5, which aligns with our expectations. This observation is also consistent for the t-values of I_{VDD_CORE1} based on dataset1 and the t-value of I_{VDD_CORE2} based on dataset2, indicating that reducing the maximum ATS eliminates the false-positive outcomes in previous security order verifications.

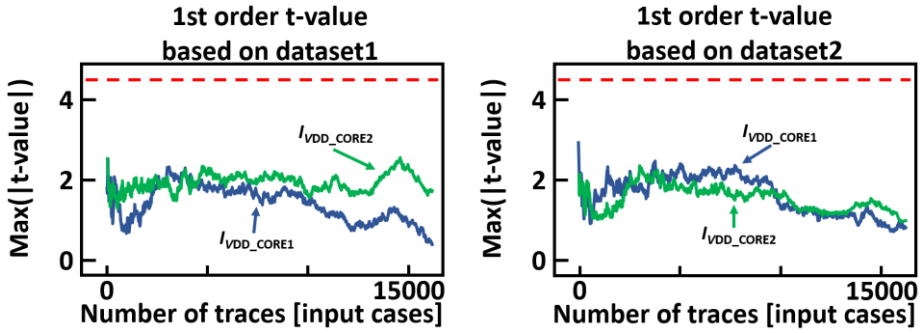


Fig. 10. 1st order t-test results of verification scenario 3
when the maximum ATS is 1 ps.
t-value based on dataset1(left) and dataset2(right) [3]. (© 2023 IEEE)

Based on the discussions in verification scenarios 1, 2, and 3, it has now become evident that when PDN node of core1 and core2 is connected at a point isolated from an ideal voltage source by parasitic elements, ATS becomes uniform for both cores. This shared ATS can result in false-positive outcomes during the security order verification of masked cryptographic circuits. On the other hand, when each core is powered separately by an ideal source, ATS is generated independently for CORE1 and CORE2. We also demonstrate that reducing the maximum ATS in SPICE simulations can be an effective strategy for eliminating such false positives in security evaluations. Though, it's crucial to remember that a smaller ATS leading to longer simulation times. The implications of simulation costs will be further discussed in Sect. 4.5.E.

D. Verification scenario 4

In a further verification scenario designed to gain a better understanding, CORE1 is assessed using dataset1, while CORE2 is assessed with a constant "0" input for all ports except the clock signal, as illustrated in Fig.4-8. The waveforms for this test are generated using a SPICE simulation with maximum ATS set to either a 10 ps or 1 ps, and the t-test evaluation is conducted with dividing the waveforms into two sets based on the unmasked output from dataset1. Fig.4-11 shows the results of this evaluation. Considering the results of verification scenario 3, we expected false-positive occurs in security order verification when the maximum ATS is 10 ps and does not occur when the maximum ATS is 1 ps. The result with a 1 ps maximum ATS differed from our expectation. In verification scenario 3, I_{VDD_CORE2} varied due to CORE2's internal operations and the ATS shared with CORE1. In this verification scenario 4, I_{VDD_CORE2} is influenced only by the ATS, because CORE2's inputs are always set to 0. This difference explains the discrepancy in the security order verification resultss between scenarios. When the maximum ATS is reduced from 10 ps to 1 ps, the statistical variation in the power noise amplitude due to ATS changes is reduces. In scenario 3, this reduced variation is hidden by the noise generated by internal logic fluctuations. However, in this verification scenario 4, the power noise variation due to ATS changes directly affects the t-value due to the lack of change in logic values.

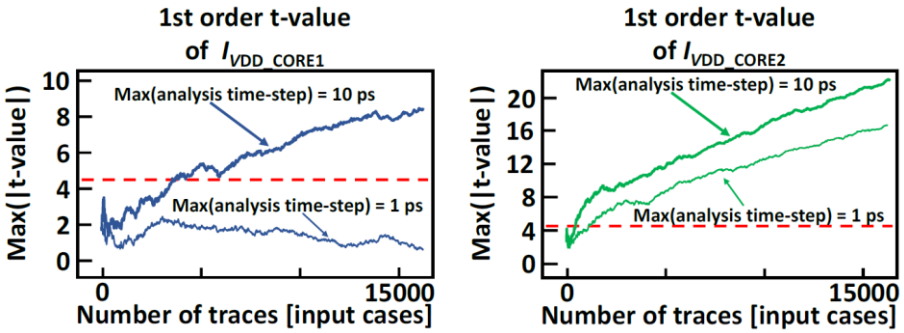


Fig. 11. 1st order t-test result of verification scenario 4.
I_{VDD_CORE1}(left) and I_{VDD_CORE2} (right) [3]. (© 2023 IEEE)

E. Summary among verification scenarios

The setups and results of evaluaions for all verification scenarios in section 4.5 are summarized in Table 4-1. Firstly, it was demonstrated how the amplitude of power noise is influenced by ATS, and how ATS-induced variations in power noise

amplitude could lead to false-positive results in SC leakage evaluation. Subsequently, in verification scenarios 3 and 4, we showed that ATS becomes uniform across multiple cores or domains in realistic PDN setups, which may lead to false-positives in the security order verification of masking circuits. It was also shown that reducing the maximum ATS could prevent these false-positives. Nevertheless, as verification scenario 4 indicated, making the maximum ATS small is not a perfect method to eliminate false-positives. The combined impact of power noise amplitude variations due to ATS and other fuctors influences the occurence of false-positives. These additional factors include power noise from surrounding circuits, fluctuations in power noise due to logical transitions within a target core, and signal jitter. This concept aligns with the considerations of SNR in security evaluations.

Tabale 4-1 Summary of evaluations in this section [3] (© 2023 IEEE)

Verification scenario	Input dataset for CORE2	Maximum ATS [ps]	ATS of 2 cores (PDN of 2cores)	Simulation CPU time [hours]	Verification results
1-1 (Fig.5 (10ps))	—	10	—	4.0	False positive
1-2 (Fig.5 (1ps))	—	1	—	21.3	As expected
2 (Fig.7)	Dataset2	10	Independent (Ideal PDN)	12.1	As expected
3-1 (Fig.9)	Dataset2	10	Common (Realistic PDN)	5.1	False positive
3-2 (Fig.10)	Dataset2	1	Common (Realistic PDN)	26.3	As expected
4-1 (Fig.11 (10ps))	“0”	10	Common (Realistic PDN)	5.1	False positive
4-2 (Fig.11 (1ps))	“0”	1	Common (Realistic PDN)	26.1	False positive

In Section 4.5.C, we showed that during the verification of an ideal PDN, ATS calculations are specific to each core. On the other hand, in a verification of a realistic PDN, the ATS becomes a shared factor across two cores. This is reinforced by comparing the CPU time required for simulation in verification scenarios 2 and 3-1. It was observed that the simulation for scenario 2 consumed approximately double the time compared to scenario 3-1. This discrepancy is explainable by the fact that in scenario 3-1, the ATS is shared between two cores, whereas in scenario 2,

each core has its own ATS. Furthermore, it is crucial to note that simulations conducted with a maximum ATS of 1 ps require significantly more time, about five times longer in our case, compared to those with a maximum ATS of 10 ps. Simulations with a maximum ATS of 1 ps require more than 20 hours though our target arithmetric core is small.

4.6 Discussion for a solution

The investigations conducted using four verification scenarios reveal that when utilizing SPICE simulations without careful consideration for SC leakage assessment of masked circuits, false positives can occu. To mitigate such occurrences, we propose three potential solution options.

A. Solution option 1

One approach is to employ MtD as the SC leakage evaluation metric, instead of the TVLA. The high sensitivity of the t-test in TVLA might lead to false positives. Although MtD is less sensitive and may help in avoiding false positives, its requirement for the full cryptographic algorithm and a larger set of waveforms could pose significant challenges in terms of SPICE simulation time. This could make employing MtD impractical for SC leakage evaluation using SPICE simulation. Additionally, MtD's effectiveness varies depending on the type of DPA attack, such as CPA.

B. Solution option 2

An alternative method is to employ a power noise simulator different from SPICE, such as the simulation technique proposed in reference [45]. However, given the complexity and difficulty in implementing hardware masking schemes without reducing their security order and the need for in-depth understanding of leakage from masked circuits, SPICE remains the most important tool due to its high accuracy.

C. Solution option 3

The final approach involves creating an appropriate SPICE simulation setup for evaluating security order of masked circuit. This section, section 4.4, demonstrates that ATS creation within SPICE, which is optimized for efficiency and accuracy, could lead to false positives in verifying the security order of masked circuits. We

provide a discussion and evaluation results on how to eliminate these false positives caused by ATS. However, at this stage, it is not clear whether other internal calculations in SPICE other than ATS may also contribute to false positives. This research aims to encourage further exploration and development of simulation methods suitable for SC leakage verification in masked cryptographic circuits.

4.7 Conclusion

Masking is an effective countermeasure methodology against SC attacks, which provides provable security within specific assumption. However, some previous works suggested that the physical layout and measurement setups may lower the effectiveness of masking schemes when the countermeasure is implemented to hardware. Consequently, SPICE, known for its accuracy, is expected to be used for finding out the reason of this security order reduction and for verifying SC leakage in masked circuits at the design phase. Nevertheless, this section (section 4) reveals that inappropriate use of SPICE can lead to erroneous results in SC leakage verification. The evaluation results with the series of verification scenarios demonstrates that SPICE's internal time-step optimization for efficiency can generate false positives. We showed that it is dangerous to apply SPICE simulations to security evaluations without carefull consideration, and also provided strategies to mitigate these false positives.

Section 5

SoC level side-channel simulation

5.1 Introduction

SC attack is a significant threat to cryptographic systems. In a SC attack, an attacker deduces a cryptosystem's secret key by analyzing physical quantities that are observable during the system's operation. Simple power analysis (SPA) and DPA link bit-wise operations to the power supply current consumption of digital integrated circuits (ICs) [61]. An advanced form of DPA, known as CPA [66], utilizes a SC leakage model specifically tailored to the target cryptographic algorithm and correlats the model with the power supply current consumption of an IC chip. For example, Hamming distance, which means the number of bit changes in a secret data register, is often used in cryptographic algorithms and can be correlated with the magnitude of power consumption current during data access.

Attackers can use EM radiation as a stronger alternative, which has a feature of almost noninvasive [63,64,65,66]. Also, attackers can capture localized emanations from a silicon IC chip using small magnetic probes [67], which may give attackers more detailed information through EM SC analysis. For IC chip designers, pre-silicon simulation becomes increasingly complex, because of it needs a multi-physical approach. Consequently, EM SC simulation has garnered significant attention in the research community, focusing on designing cryptographic systems with enhanced resilience.

Many researches have been conducted on logical and physical design countermeasures against SCAs. These works include strategies like power balancing and randomization of intermediate values in logic paths [68,69,70,71,72,73]. While post-silicon evaluations are common for evaluating these techniques, there are three significant problems. Firstly, manufacturing ASICs is both costly and time-consuming. Although FPGAs are sometimes used as an alternative to ASIC, their power consumption characteristics can differ from ASICs even when FPGA and

ASIC conduct an identical cryptographic function. Secondly, identifying the specific physical source of SC leakage can be challenging, despite observable evidence of leakage. Thirdly, if vulnerabilities are uncovered during post-silicon evaluations, employing new countermeasures requires expensive and time-consuming respins.

These backgrounds lead the growing need for a pre-silicon SC Leakage Analysis (SCLA) method. Such a method may allow for the anticipation and mitigation of SC vulnerabilities in IC chips during the design phase before fabrication. Though numerous simulation techniques for SCLA have been eproposed [74,75,76,77,78,79, 80, 81, 82, 83, 84], there are still some issues. One major issue is simulation time, particularly vital for evaluating SC leakage over the numerous clock cycles involved in cryptographic processing. Public key cryptography, for instance, needs thousands of clock cycles for a comprehensive SCLA, while symmetric key cryptography like AES might require millions of traces with varying inputs. Another challenge lies in enhancing simulation accuracy. Accurate simulations demand fully physical models of transistors and power delivery networks, but as transistor counts increase for more complex functions, simulation time increases dramatically. Therefore, SCLA simulation techniques with an optimal balance between efficiency, accuracy, and capacity are needed. Also, the ability of handling comprehensive chip and system-level design databases and encompassing multiple physical aspects of both power and electromagnetic SC leakages is required.

In this section (section 5), we propose a rapid simulation method for power and electromagnetic SCLA. The method employs both a power noise solver and an electromagnetic solver for simulating traces during the operation of cryptographic modules. This process is specifically tailored for gathering traces for further analysis in SCLA, utilizing a security-sensitive register extraction engine, an innovative probe generation process, and an efficient simulation method known as Direct Vector Control (DVC). In the subsequent phase of SCLA, a heatmap of SC leakage is generated, assisting designers in pinpointing vulnerable areas and anabling the imediate implementation of countermeasures. The entire simulation process is validated for accuracy and correctness by the comparison against actual silicon measurements in electromagnetic SCLA.

The structure of the rest of this section is as follows. Section 5.2 explains on-chip power noise modeling and near-field electromagnetic emission modeling methods. Section 5.3 elaborates on ideas to accelerate SC leakage simulation, incorporating techniques like security-sensitive register extraction, intelligent probe generation, and

DVC. Section 5.4 discusses the silicon design flow based on SCLA, illustrated with a prototype silicon chip, and compares simulation results with actual measurements. Section 5.5 concludes Section 5.

5.2 EM emission modeling

5.2.1 Power supply current modeling with chip-package-system (CPS) board model

Power SC leakage is due to the fluctuating power supply current caused by logic gate operations within an IC chip. This current flows through the comprehensive PDN of Chip-Package-System (CPS) including the PCB and cables for external power connections [80]. The package structure is made up of a plastic interposer with solder bumps and balls, connecting the chip pads to the PCB. It's assumed that the IC chip is equipped with cryptographic engines and the model involves dynamic power supply currents during cryptographic activities.

A system-level model, shown in Fig. 5-1, is composed of the CPS including a Chip Power Model (CPM). The CPM of an IC chip is divided into a passive component, which describes the impedance network of the on-chip PDN, and an active part that accounts for the power supply currents during cryptographic circuit operations, presented as piece-wise linear (PWL) waveforms in the time domain. The development of the CPM is discussed in section 5.2.2.

It should be noted that power supply currents can be captured at any point in the CPS model during power SCLA. Voltage fluctuations in the on-chip PDN, caused by the combination of power supply currents and parasitic impedance, are identified as dynamic IR drop noise or power noise. The same power supply currents generate magnetic fields around metal wirings in the PDN, contributing to electromagnetic emissions. Multiple paths exist within the PDN for power supply currents to mitigate dynamic variations, and these significantly influence the frequency-domain response of the entire PDN impedance.

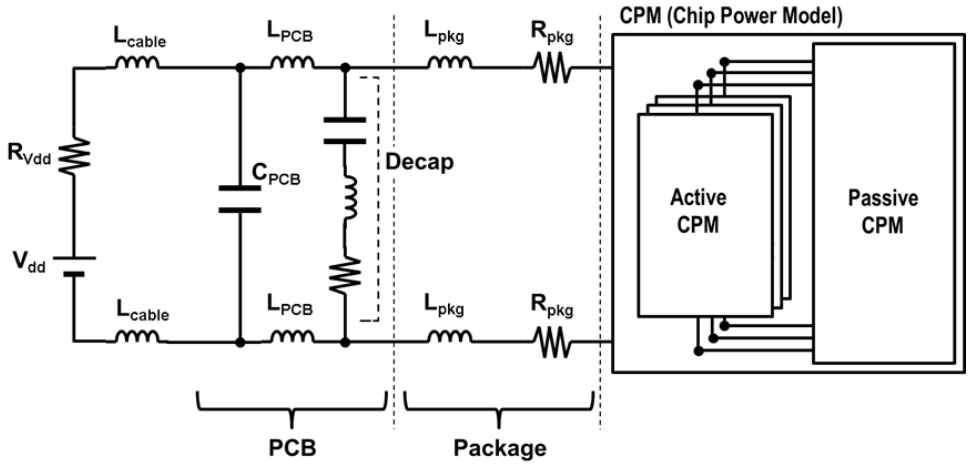


Figure 5-1: Chip-package-system (CPS) board model
for power supply current simulation [4].

5.2.2 On-chip power noise modeling

Power SCLA depends on the accurate simulation of on-chip power noise. This involves extracting the parasitic resistance (R), inductance (L), and capacitance (C) of the on-chip PDN from the IC chip's layout, which are then incorporated into the CPS power noise simulation. The PDN typically consists of the upper metal layers arranged in a mesh pattern that covers the entire chip. In contrast, each standard logic cell's power supply current is connected to the power and ground nodes at its specific location on the lower metal layers of the PDN, as depicted in Fig. 5-2 [85]. Although the direct correlation of power supply current to data is localized to logic cells processing the data, the overall current flows through the entire PDN across the chip, interacting with the parasitic RLC components within the V_{DD} and V_{SS} domains of the PDN. Furthermore, the silicon substrate of the IC chip is modeled as a resistive-capacitive mesh linked to the PDN. This mesh accounts for the distribution of p- and n-type dopants and p-n junctions. The comprehensive model used in simulations produces chip-level power noise, which leads to power SC leakage at both the IC chip and its entire assembly.

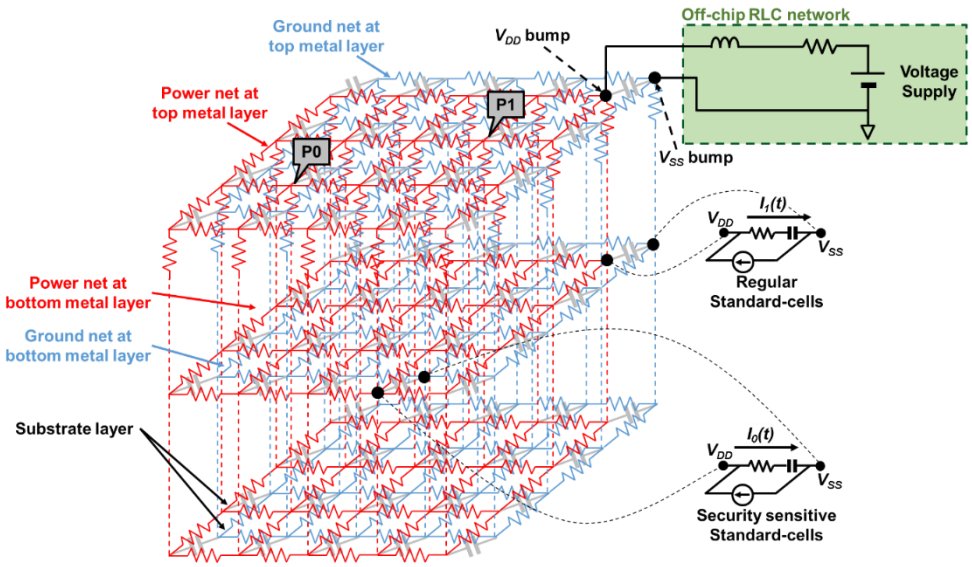


Fig. 5-2: Power-noise model of on-chip PDN
of an IC chip with security functionality [4].

The global power consumption of an IC chip, measured at the voltage supply port, is influenced by the current demands from every logic gate within a design. The dynamic voltage drop at any selected probing point (such as P0 and P1 in Fig. 5-2) can be described by the function:

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

where I(t) is the local dynamic current, and R, L, and C are parameters extracted from the physical configuration of the PDN. Our simulation approach calculates the power supply current drawn by each logic gate, considering the influences of intentional decoupling capacitors, inherent device capacitance, metal fills, and the parasitic RLC elements distributed across the PDN grid. When a cryptographic core is integrated into the chip, I(t) consists of two types of currents; 1) I_0(t), the current used by security-sensitive standard cells, and 2) I_1(t), the current consumed by the remaining standard cells, as illustrated in Fig. 5-2. Since I_1(t) generally not correlating with sensitive data, the ratio of I_0(t) relative to I_1(t) can be considered as SNR, which is a crucial observable in determining SCLA results.

For simulating dynamic IR-drop waveforms, we model time-domain power supply currents and the RLC parasitics of the PDN grids [86]. Libraries of power supply currents for standard logic cells, input/output macro cells (IO macros), and intellectual property (IP) macro blocks are established through transistor-level SPICE

simulations prior to dynamic power noise simulation. RLC parasitics are extracted from the physical layout of an IC design. Fig. 5-3 depicts an example of a cell-level current modeling for an inverter, where dynamic currents at V_{DD} and V_{SS} pins are determined by SPICE simulation for each logic operation, corresponding to the logic cell's truth table. To accurately model both linear and non-linear power behavior of the cell, the power supply current library initially identifies a range of operational conditions for characterization. Subsequently, a heuristic interpolation method is applied to generate the power profiles for other operational conditions, including variations in process corners, power supply voltage, temperature, input signal slew, signal load capacitance, and multiple output states. For IO macros and IP blocks, the switching states of interest are modeled with pre-simulated time-domain PWL waveforms of power and ground switching currents.

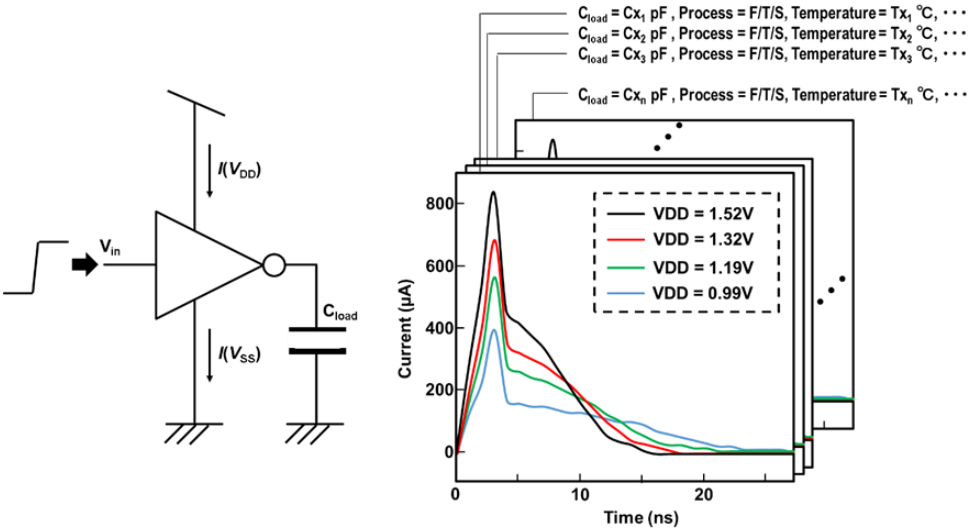


Figure 5-3: Cell-level dynamic power supply current model under various operation conditions [4].

An SC attacker or an SC leakage evaluator typically records power noise waveforms at the off-chip power pins on a system's assembly. This is much easier than measuring power supply currents directly within the IC chip. However, when conducting simulation-based SCLA, there are no such restrictions in placing probes. In our approach to simulating power noise, virtual measurement probes can be strategically positioned at any point within the on-chip PDN. These probes, which can be automatically located on the top metal layer at specific intervals, like P0 and

P1 shown in Fig. 5-2, enable designers see the distribution of SC leakage across the entire chip. This capability is crucial for identifying and focused analysis of the areas of a chip that are most vulnerable to security breaches immediately after a location-aware SC leakage heatmap is produced.

5.2.3 Near-field electromagnetic emmision

Power supply currents cause magnetic fields as formulated by Maxwell's equations. The characterization of near-field EM emission frequently employs the dipole-moment method for wire segments and metal planes that carry the power supply current [87,88,89,90]. This method is depicted in Fig. 5-4, where an on-chip PDN wire segment is modeled as a dipole moment. The magnetic field B(t) at an observation point P is then calculated using the Biot-Savart law following Eq. (2). This involves summing the contributions of every dipole (dipole 1, dipole 2, ..., dipole N) arranged within an IC chip. The total B(t) is also updated in accordance with the time-domain variation in the power supply current, I(t), to accurately simulate near-field EM traces. The equation considers factors like the permeability μ_0, the length of wire segments dl, the distance vector r, and the angle θ between the dipole point and the observation point.

$$\mathrm{B(t)} = \frac{\mu_0}{4\pi} \sum_1^N \int \frac{I(t) \cdot dl \cdot \sin\theta}{r^2} \qquad (2)$$

EM observation points can be strategically positioned in a space around an IC chip, though they are often placed close to its surface. By simulating with fine-grained power wire segments within an IC chip and its assembly, both the distribution of EM emissions and EM side-channel leakage heatmaps can be accurately modeled. The results from these simulations are important for designers to optimize the physical layout of IC chips and to select the most secure physical structures for assemblies, for enhancing protection against both power and EM side-channel attacks.

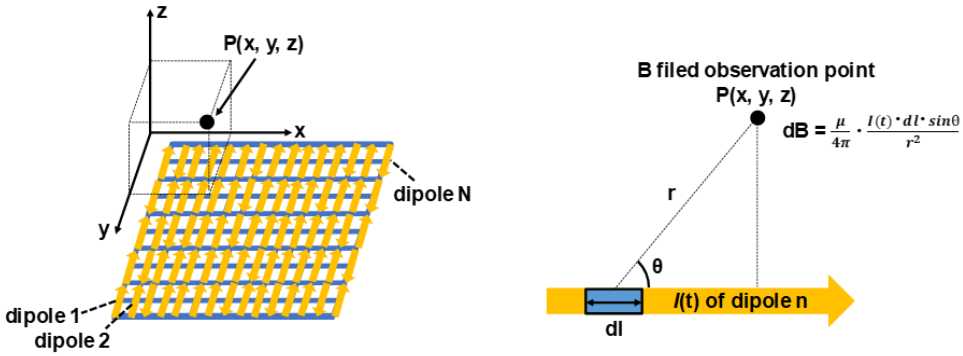


Fig. 5-4: Near-field EM emission modeling of on-chip PDN wires as dipoles [4].

5.3 Side-channel leakage simulation

5.3.1 Overview of SCLA simulation framework

The overview of the power and EM SCLA simulation framework we propose is shown in Fig. 5-5. The important point to resolve data leakage issues assessed through SCLA is the identification of the specific data to be protected. Such data, referred to as "security assets," flows through a sequence of logic gates and registers within a security IC chip. Within the gate-level netlist of the design, all gate instances impacted by these security assets are classified as "security sensitive registers and nets." These elements should be carefully assessed to prevent data leakage. This identification process is the initial phase of our simulation framework.

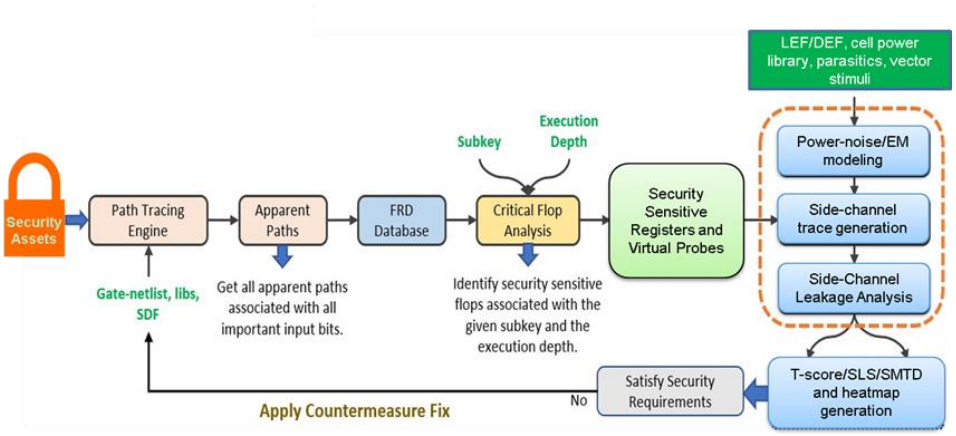


Figure 5-5: Overall flow of the pre-silicon side-channel assessment method for secure SoC design [4].

In our approach, we utilize static timing analysis (STA) to analyze the entire cryptographic core for creating a forward reachability database (FRD) at the gate netlist level. Our process requires the gate-level netlist, the logic cell timing model file in liberty format and the timing constraint file in standard delay format (SDF) as input. The FRD efficiently records all registers that are reachable at every stage of execution for every input port. This database is then employed to identify all potentially accessible registers at given execution depth. Through critical flop analysis (CFA), we pinpoint security-sensitive registers from this list of registers. These security-sensitive registers are grouped at the chip layout level for subsequent SC analysis.

These identified security-sensitive registers are the most likely sources of SC information leakage about the secret byte, in comparison to other registers. Isolating their power signatures enhances the SNR in power traces by reducing the noise of non security sensitive registers. These non security sensitive registers are less relevant to SC. Considering practical scenarios, an attacker might only access the global power consumption, but motivated attackers could try to preprocess data to minimize noise, including environmental and intrinsic noise, and even capture local power SC leakages.

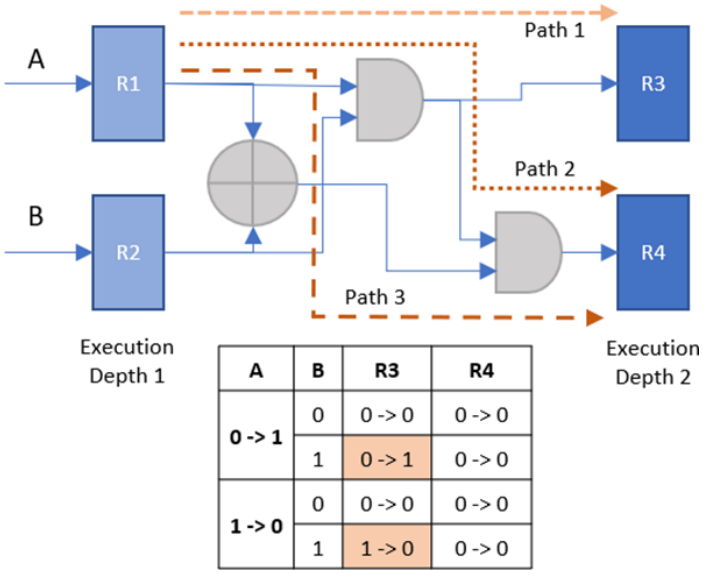
The proposed framework adopts a white-box approach for pre-silicon SCLA, which is ideal for design engineers with complete access to the gate-level and layout-level design of the chip. This framework enables SCLA with high sensitivity by amplifing SNR related to secret key bytes. If the engineer also aims to estimate MtD from a post-silicon SCLA perspective, proposed framework can incorporate SC leakage from non security sensitive registers or a realistic silicon noise profile.

The physical model of the logic core is constructed using LEF/DEF layout files, extracted parasitics files, cell power current model files, and the vector stimuli file in value change dump (VCD) format. A power noise solver then calculates dynamic IR drop traces over the PDN of the logic core, and an EM solver generates dynamic EM traces at a virtual probe point.

To obtain a large number of traces, we propose a simulation trace reduction method named “direct vector control.” Post-processing of traces for SC assessment, generating heatmaps and scoring, is handled by the SCLA flow. This process pinpoints location-dependent SC leakages down to the granularity of a gate instance and it enables gate-netlist level revision in case of SC leakage verification fails.

5.3.2 Identification of security sensitive register

Proposed framework begins with analyzing the data flow between input and output ports, evaluating all STA paths and saving each register encountered along these paths. Every security sensitive input bit is traced by following static paths to their output ports. This process is baced on the understanding that registers located along these paths are likely influenced by changing in the input bit. For example, as shown in Fig. 5-6, proposed tracking identifies register pairs (R1, R2) and (R3, R4) at execution depths 1 and 2, respectively. In tracing paths from input bit A, three paths leading to endpoints (R3 and R4) are identified. It is assumed that shifts in A might trigger corresponding changes in R3 and R4 at execution depth 2, though this is not always the case, as shown in the truth table in Fig. 5-6. A switch in A from 0->1 or 1->0 impacts R3 but leaves R4's value constant. This occurs because the same registers may be influenced by other input bits at the same execution depth, as with input B in this scenario. Thus, the paths identified through our tracing technique are termed "apparent paths."



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. 5-6: Illustration of apparent paths between two execution depths [4].

In the proposed framework, information flow analysis at the gate-netlist level is conducted as a important step in identifying security-sensitive elements in cryptography designs. Unlike the SCRIPT [91] and GLIFT [92], which precisely identify affected registers by sensitizing paths, we avoid such detailed path examination for computation efficiency. SCRIPT and GLIFT significantly increase

computational time. For instance, GLIFT demands the creation of shadow logic, a complex task for large circuits, while SCRIPT necessitates frequent register conversions and masking and unmasking operations, challenging without specialized ATPG support.

Proposed framework's efficiency is optimized for SCLA by considering all apparent paths without path sensitization. This approach effectively enhances the SNR of power traces for SCLA by considering all registers potentially affected by security sensitive input bits. We identify security-sensitive registers at each execution depth by pruning the list via critical flop analysis to further boost power trace SNR.

The FRD stores all apparent paths and registers. To minimize storage space, the flow tracks only crucial input bits in the design. This includes secret assets like cryptographic keys and non-secret inputs, which attacker can controle, like plaintexts in AES. And non-relevant inputs like clock or reset signals are excluded. The FRD faces a path explosion issue with increasing execution depths which leads a crusial problem in evaluation time and memory requirement. This path explosion issue is resolved by storing unique “driver” and “sink” register sets at each execution depth. Here, "sink" registers are identified as the set of registers at a given execution depth, which are connected to paths from all "driver" registers located at the preceding execution depth. For example, in Fig. 5-6, input bit A at execution depth 2 identifies R1 as the driver and R3 and R4 as sink registers.

The STA tool enables multi-threading in identifying sink registers from driver registers and saves much time in FRD generation. The number of static paths between execution depths exceeds the limited set of driver and sink registers. For example, there are three static paths and two “sink” registers for input bit A at execution depth 2, as ahown in Fig. 5-6. Therefore, storing detailed information about these paths becomes impractical for complex designs. Our framework does not neglect power consumption and glitch effects from combinational gates in SCLA flow. Instead, it groups registers along a cryptographic design's datapath to store target data values at specific execution depths for SCLA.

To identify security-sensitive registers, we trace security assets (e.g., a cryptographic block's secret key byte) at each execution cycle. CFA helps identifying these security-sensitive registers, taking the subkey and execution depth as inputs as shown in fig. 5-7. In the assessment of AES, execution depth should be correspond to the first round or last round of AES operation because an adversary may specifically target these rounds. CFA assumes an attacker's perspective such as targeting specific

execution timeframes and using correlation-based attacks like CPA or DPA to leak secret bytes with minimal power traces.

SCLA evaluators can manipulate some system inputs, like plaintext in AES, which is combined with the secret key and impacts flops due to cryptographic algorithms' confusion property. We define properties to extract security-sensitive registers:

Property 1: A flop should be influenced by both secret and non-secret inputs at the analyzed execution depth.

Property 2: Multiple bits of these secret and non-secret inputs should impact the flop at the analyzed execution depth.

As depicted in Fig. 5-7, registers satisfying these properties at a specific execution depth are identified as security-sensitive registers. The design engineer sets property which varies with the implementation type and design under analysis. For our AES test case, we set this limit to eight bits considering sbox register sizes.

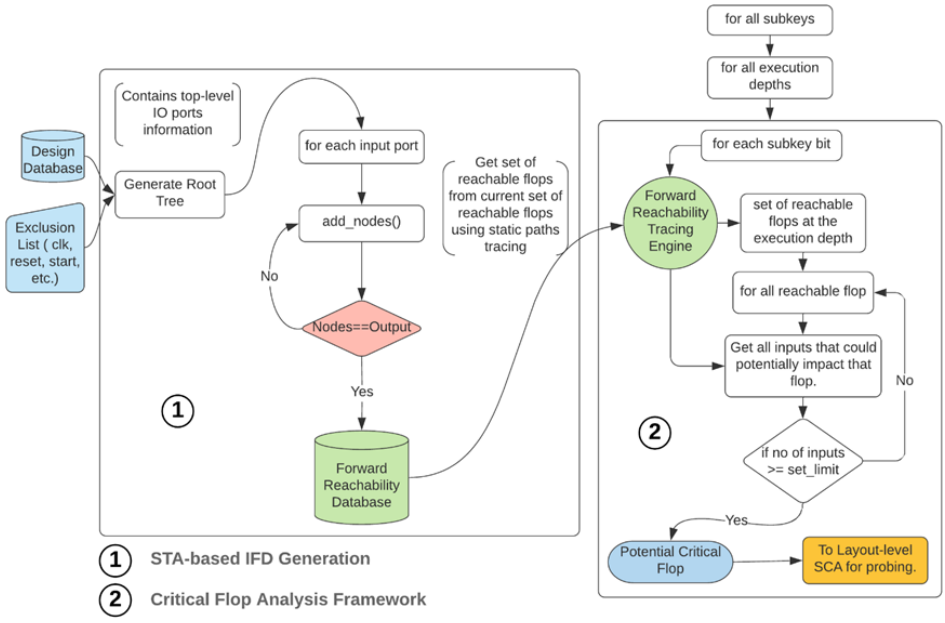


Fig. 5-7: Critical flop analysis to extract security-sensitive registers from the set of reachable registers [4].

5.3.3 Direct vector control

In the proposed SCLA flow, we address the challenge of efficiently generating time-domain power supply current traces for approximating the silicon MtD, which typically requires thousands or millions of traces. Simulating such a large number of

traces is computationally challenging for circuit-level simulators. To overcome this, we have developed a simulation trace reduction technique, referred to as the “direct vector control”, as shown in Fig. 5-8. This method relies on the understanding of a chip's functionality to identify and list the security-sensitive nets within the design. Such nets might include an interface data bus transmitting secret data or the flip-flops holding a cryptographic core's private key.

Using design details and logic simulation data, proposed approach annotates the list of security-sensitive nets and these nets are then stimulated using a "direct vector control" file, which iterates through all possible state combinations for these sensitive nets. The states applied to targeted gates are logically propagated throughout the design's logic nodes. To simulate the background noise of an IC chip, the remaining nets, non security sensitive nets, are randomly switched using a vector-less method. This method reduces computational load over simulation cycles, where a group of physically close nets will toggle at a user-defined rate. Additionally, to accurately represent the SNR of system-level power supply current, vector-less blocks are constrained with a power target for each cycle.

The direct vector control file, combined with cell liberty files, timing window file, and power library files, forms the electrical model of the design. For each input data, only a few point-of-interest (POI) cycles need to be simulated (e.g., the final round of AES) to acquire the necessary power noise waveforms for SCLA.

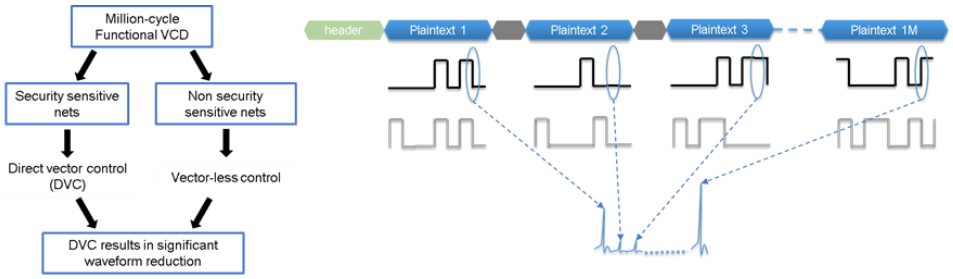


Figure 5-8: Direct vector control technique to control the SNR of side-channel assessment in simulation [4].

5.4 Silicon design flow and example

5.4.1 Silicon design flow

Fig. 5-9 shows the design flow incorporating simulation-based power and EM SCLA, focusing on the development of secure IC chips with cryptographic functions.

The proposed SCLA method statistically evaluates the risk of SC leakage by analyzing a large set of traces during cryptographic operations. This flow helps designers in optimizing physical layouts by visualizing the distribution of SC leakage levels across the entire chip.

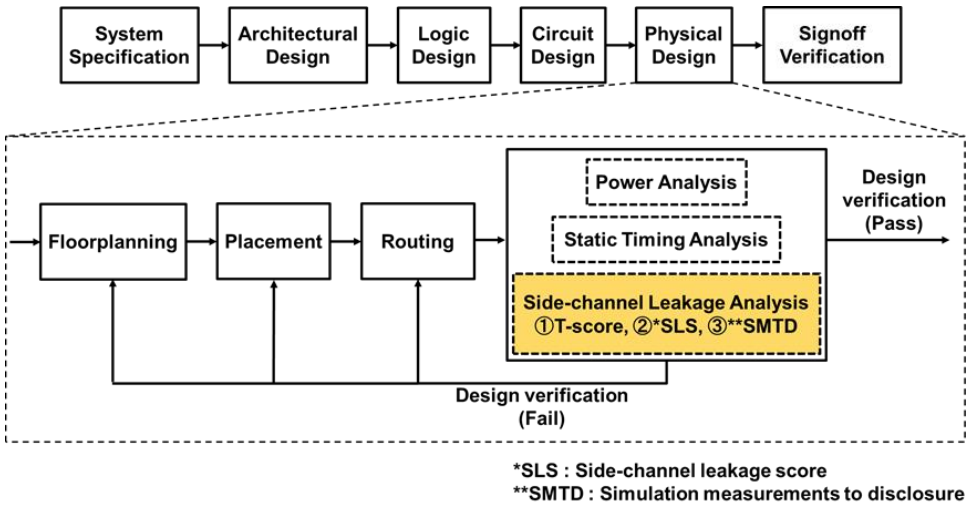


Fig. 5-9: Overview of general VLSI design flow and the position of our SCL simulation [4].

The flow begins with a RTL netlist, assumed to be a reliable design after thorough architectural exploration of the cryptographic hardware and logic and circuit design. The initial full-chip place and route (PNR) is conducted to convert RTL netlist to physical design. Following the initial PNR and physical rule checks, the first SCLA is applied to the design data. Based on the results, the design undergoes a second round of PNR with specific constraints and the addition of extra devices. Then, subsequent rounds of SCLA is conducted. These iterative processes continue until the design meets the required SC leakage tolerance level.

The SCLA employs quantitative metrics to analyze simulated power traces and assesses SC leakage at distributed probe points across the full chip area. The initial step in the security exploration sequence involves calculating T-score at each probe point, scanning the entire chip to identify potential SC leakage areas. Subsequently, the SC leakage score (SLS) and simulation measurements to disclosure (SMTD) are used to pinpoint the exact sources of SC leakage, based on SC leakage models specifically tailored to the cryptographic algorithm being used. These analysis modes are essential for accurately determining and addressing the root causes of SC leakage

in the chip design. Bellows are definitions of these analysis modes.

T-score

Welch's t-test is a statistical hypothesis test that evaluates the significance of the difference between two populations. The T-score is calculated using the following formula (3). It compares two sets of data, W1 and W2, each with a respective size of N1 and N2.

$$\mathrm{T-score} = \frac{\mu(W1)-\mu(W2)}{\sqrt{\frac{\sigma^2(W1)}{N1}+\frac{\sigma^2(W2)}{N2}}} \qquad (3)$$

This test is utilized in TVLA to assess SC leakage tolerance of cryptographic modules [89,90]. In TVLA, traces are divided into two sets under specific conditions. For instance, one set may consistently use the same input payload for each cryptographic operation, while the other set applies a random payload each time. When the T-score does not surpass a threshold of 4.5, it implies negligible statistical differences between these two groups. A higher T-score suggests a possible correlation between the intermediate values in cryptography function and the power traces. This indicates vulnerability to SC attacks, but not necessarily revealing secret information. TVLA, being more sensitive than other methods, is effective for identifying potential leakage sources across different cryptographic algorithms. It's important to note that simulations do not include "white noise", unlike measurements, which means fewer traces are needed in simulations to achieve a level of statistical significance comparable to actual measurements.

SC-leakage score (SLS)

We propose another metric SLS to quantify the correlation between power supply currents and confidential data. This approach is based on a white-box analysis, where the SC leakage model is assumed in advance according to the design and data paths of the cryptographic core, aligned with the specific cryptographic algorithm. In this analysis, evaluators know the actual secret key as the correct key. We use an 8-bit portion of a byte as a hypothetical subkey value and calculate its correlation coefficient against a set of power supply current traces, either simulated or measured. This calculation is repeated for each potential subkey value in a comprehensive manner. SLS is then determined by the ratio of the correlation coefficient of the correct subkey to the highest correlation coefficient among all hypothesized subkey

values, as expressed in equation (4):

$$\mathrm{SLS} = \frac{\rho(X\{correct_{key}\},Y)}{MAX[\rho(X\{key_{guess1}\},Y),\rho(X\{key_{guess2}\},Y),\cdots,\rho(X\{key_{guessN}\},Y)]} \quad (4)$$

Here, the function X denotes the leakage model for each guessed key, while Y denotes the set of measured or simulated traces during cryptographic operations using the unique correct key. The correlation coefficient ρ between the guessed key and the traces is calculated as equation (5):

$$\rho(\mathrm{X},\mathrm{Y}) = \frac{cov(X,Y)}{\sigma X \cdot \sigma Y} \quad (5)$$

In CPA literature, among all possible key guesses, the predicted Hamming weight or distance of the power model is expected to show the highest correlation with the traces when the key guesses match the correct key. The SLS normalizes the correlation coefficient to the correct key guess. The trend of leakage level is visualized through SLS as the number of simulation traces increases, and this trend is compared across various locations within an IC chip. The closer the SLS value is to 1, the more significant the detected vulnerability. This enables designers to pinpoint the source of SC leakage and modify the physical layout of the IC chip.

SMTD

SMTD is a crucial index for confirming the presence of side-channel leakage, indicating the least number of traces required to fully reveal subkey bytes within a secret key. Due to the large number of traces needed for SMTD, often reaching hundreds of thousands or even millions, the computational cost in a general circuit-level simulation process such as SPICE becomes excessively high. To address this issue, we employ the DVC technique detailed in Section 5.3.3, which significantly reduces the simulation time for SCLA while maintaining a minimal compromise on accuracy.

These SCLA metrics should be strategically utilized across three distinct stages of design. In the first stage, a cryptographic core is initially evaluated using the T-score metric, based on a limited number of simulation power traces. Any identified

potential vulnerabilities are logically analyzed and flagged for subsequent physical implementation. This step also involves defining side-channel leakage models, which may include power or electromagnetic correlation. The second stage involves an in-depth evaluation of the IC chip layout containing the cryptographic core, using the SLS. This step assumes a correlation and progressively increases the number of simulation traces. The primary focus here is to identify and address or mitigate the root causes of SC leakage through physical design modifications. Finally, in the third stage, after iterative SLS analysis, the complete IC chip layout undergoes verification using SMTD as the sign-off verification for SC leakage. In this stage, the number of simulation traces can be maximized.

5.4.2 Silicon example and measurement setup

For the demonstration, a test chip using 0.13 µm CMOS technology was fabricated and implemented on a PCB using flip-chip BGA packaging, as depicted in Fig. 5-10. The chip with 128-bit AES core was evaluated for SC leakage, both through simulation and experimental measurements. In this demonstration, EM emission is measured at the backside surface of the IC chip.

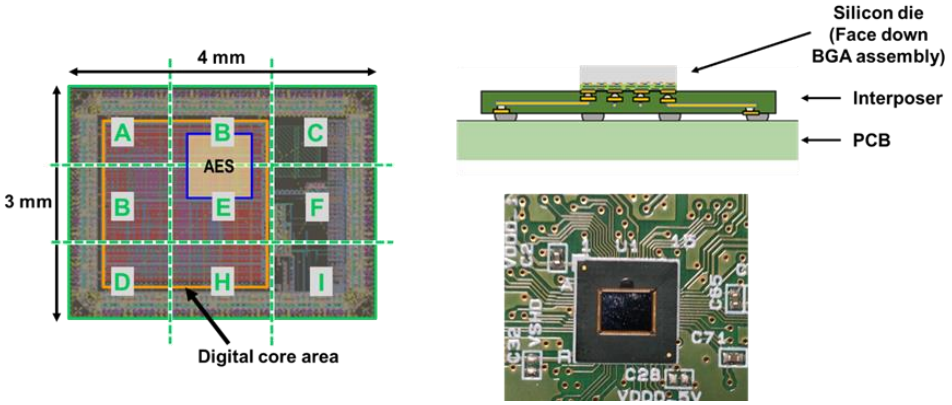


Fig. 5-10: Silicon example (chip layout, image of implementation and photo of silicon example) [4].

The experimental setup, depicted in Fig. 5-11, involves the utilization of an EM probe precisely positioned by PC-controlled software. The probe is positioned in three-dimensional space and can be oriented with respect to the IC chip. The silicon die, with a thickness of 350 µm, is flipped onto a plastic interposer. The backside surface is not covered by any material. The minimum height of the probe from the

chip's backside is offset by the 400 µm thickness of the probe's plastic molding, making the effective distance between the probe coil and the frontside circuits about 750 µm. SCLA tests were conducted in a 3 x 3 array of probe positions, along with measurements of magnetic fields in the x and y axes. Probe positions are labeled from A to H. And probe orientation labeled as Bx and By are consistent across measurement setups and simulation models.

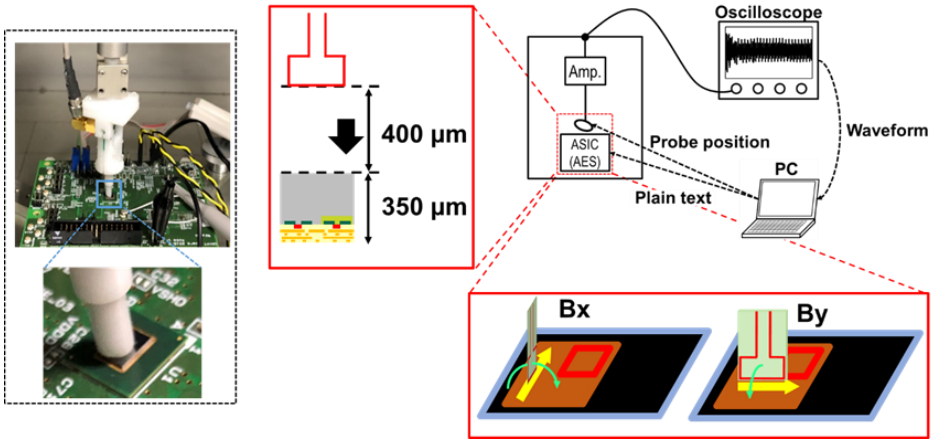


Fig. 5-11: Measurement setup [4].

	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/trace	Measurement time : 198 hours / 10K traces including ・9 probe points × 2 probe orientation ・EM noise → effective cost of time : 4.0 sec/trace
Trace length	50 points × 0.59 ns/point → 29.5 ns/trace (focused on single round of interest)	15985 points × 0.025ns/point → 399.6 ns/trace (covering full rounds)
SC leakage analysis	Power noise : T-test, SLS, SMTD EM : T-test, SLS, SMTD	EM : T-test, SLS, SMTD

Fig. 5-12: Summary of Measurement and simulation setup [4].

The AES core within the chip, consisting of 800k instances and 3 million nodes, is incorporated into a full-chip level digital PNR with other digital blocks. The AES

core occupies areas over B and E regions and its operating clock frequency is set at 30 MHz. Simulation analyzed 50 sampling points per clock cycle. For simulation purposes, an 11 million cycle VCD file is prepared first, and then this file is chopped and stitched to focuse only on the POI cycles including 10k cycles. Parallel processing is employed to simulate SC traces efficiently using a time-chunking method. Utilizing 100 CPUs (Intel(R) Xeon(R) Gold 6148 CPU @ 2.40GHz), the process of simulating and analyzing both power noise and EM SC leakage from 10k traces at 500 virtual probes is completed in approximately 3 hours. As summarized in Fig. 5-12, the time cost for a single measurement trace is about 8,000 times greater than its simulation counterpart. This is mainly due to the simulation's inherent parallelism and the DVC's focus on a single POI cycle.

5.4.3 Silicon results

First, SLS is employed to detect EM SC leakages within the die area of a test chip, as depicted in Fig. 5-13. The plot demonstrates the general trend of correlation-based leakage by comparing SLS across nine different probe locations with respect to the number of EM traces. The SLS is computed for each subkey byte using equation (4) and then averaged over 16 bytes. In contrast, the MTD plots explicitly indicate the complete disclosure of the full 8-bit correct subkey at certain locations. However, values less than 8.0 on the vertical axis (except for 0.0) are less significant as they include bits that cannot be distinguished from the disclosed bits. The SLS trend is observable even with a smaller number of traces, which is beneficial for early detection of SC leakage.

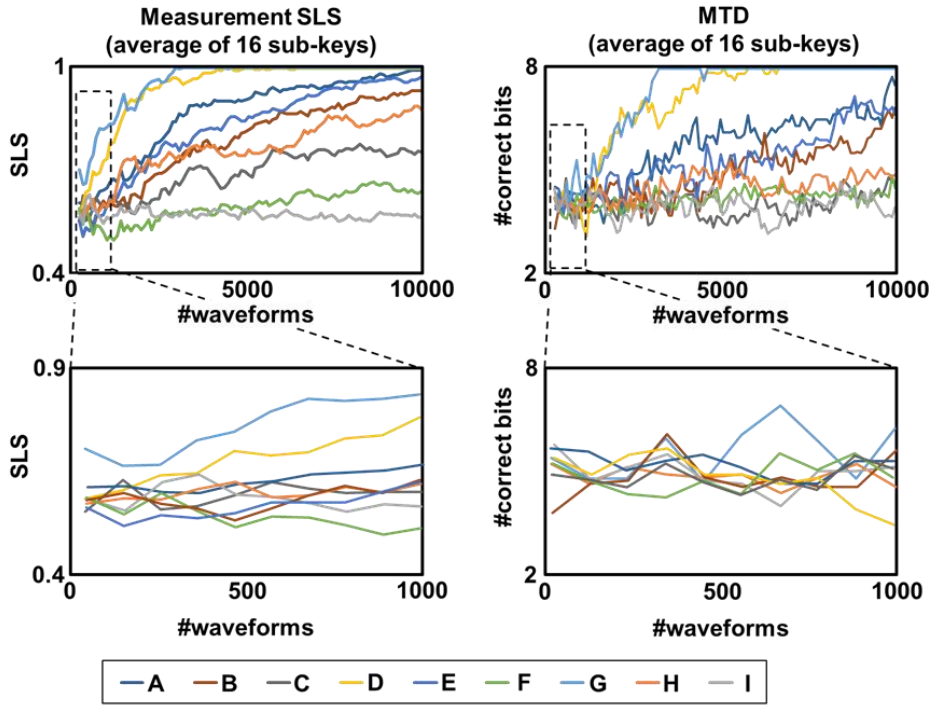


Figure 5-13: Comparison of two SCLA technique's feature [4].

Fig. 5-14 contrasts near-field EM SCLA metrics of SLS and MTD between simulation and measurements. The magnetic field traces captured in Bx and By directions are utilized for this analysis. Their directivity validates the proper treatment of near-field EM radiations. With in 10k traces, the full 128-bit correct key is revealed through EM SC leakage. The simulation accurately reflects the location dependency observed in measurements, particularly in areas with high SC leakage at points A, D, and G for Bx and points E, F, G, H, I for By. Conversely, lower leakage areas are more apparent in the By direction, especially in the upper area of the die at points A, B, and C. The general trends of EM SCLA results in measurement are well replicated in the simulation-based EM SCLA.

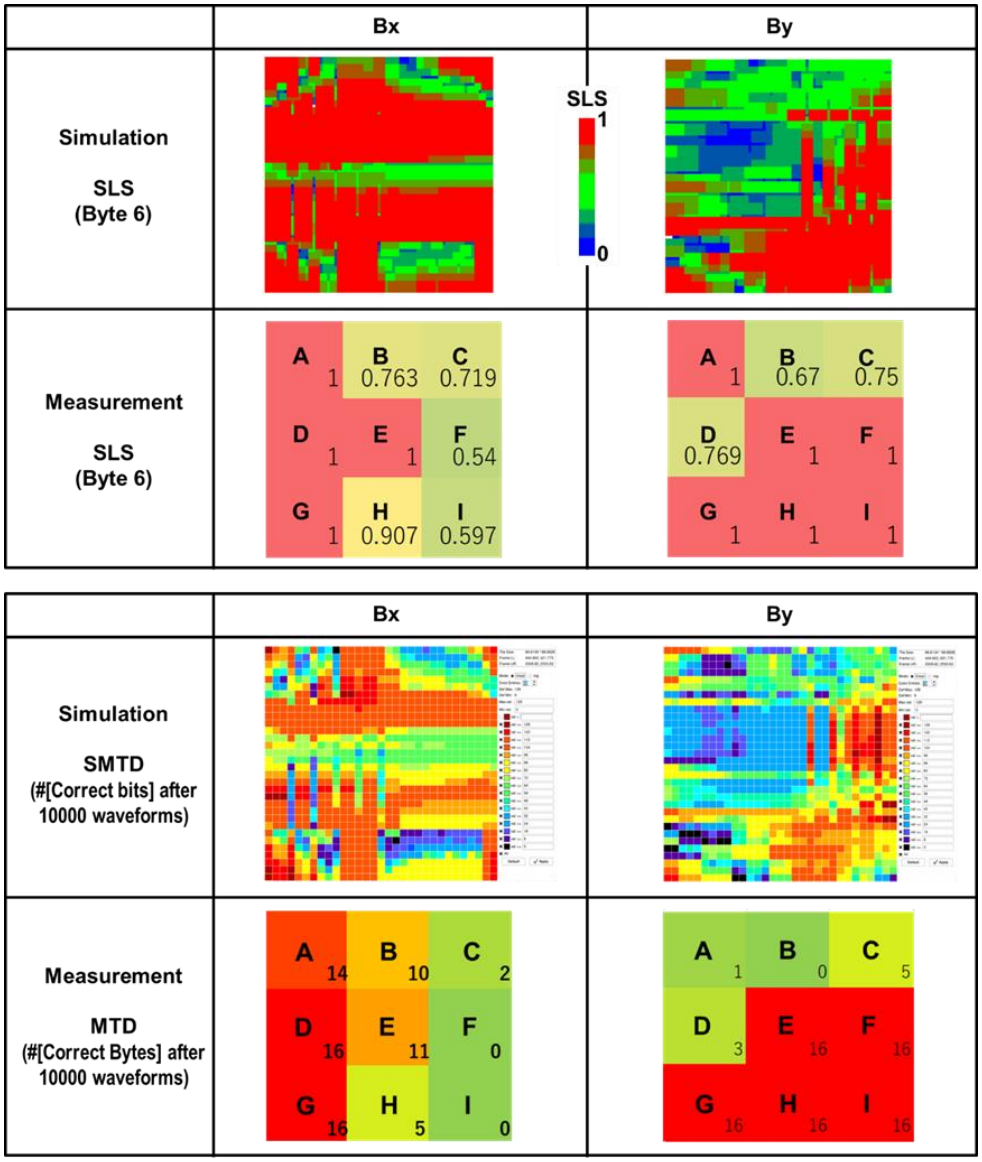


Fig. 5-14: Comparison of two simulation results and measurement result [4].

5.5 Conclusion

We proposed simulation-based power and EM SCLA techniques. The correctness of the technique was validated with a 0.13 µm AES prototype chip in flip-chip packaging and system-level assembly. The backside of the silicon die is utilized as the EM emission surface. On-chip dynamic power noise and near-field EM emission are accurately simulated with chip-level power supply current and system-level PDN models. Power and EM SC leakages are effectively analyzed with 1k on-chip virtual

probes and 10k input payloads, assessing t-score, SLS, and MTD. Simulation results correlate well with silicon measurements for backside EM SC leakage, achieving a simulation speed 8,000 times faster than measurements in exploring location and direction-dependent EM SC leakage in an IC chip. The design flow incorporating the proposed simulation-based SCLA helps designer to assess SC leakage vulnerability at the design stage and enables them to revise the design immediately.

Section 6

Innovation idea using side-channel leakage simulation

6.1 Introduction

The advancements in information and communication technology (ICT) have siginificantly changed people's lives. Since the mid-1990s, the widespread use of computers, mobile phones, and the internet led to a significant shift in how we access and share information. This era, often referred to as the digital era, is the beginning of a society highly reliant on digital technology for communication, information search and online transactions.

In recent years, this kind of change has been further accelerated by the utilization of artificial intelligence (AI) and continued developments in ICT. We are now moving towards a society where the integration of physical and digital spaces is becoming seamless. In this advanced digital society, technologies like AI, IoT, and big data analytics are enabling real-time analysis and feedback, enhancing the efficiency of various processes and improving the quality of life.

Such a transition increases the value of digital data and the importance of security. As our reliance on digital data continues to grow, protecting these data from cyber threats and ensuring privacy becomes crucial. Thus, the evolution of society with advanced ICT brings a heigh requirement for robust security measures to protect digital data in an increasingly interconnected world.

Cryptography is a key technology for securely protecting and utilizing digital data. Hence, cryptographic algorithms used for encryption, decryption, hashing, and the generation and verification of digital signatures are strictly assessed for security by numerous experts. The security of cryptographic techniques is based on the computational difficulty of problems such as the factorization of large composite

numbers or the difficulty of discrete logarithm problems for large numbers. However, the security level of cryptographic technologies can be degraded due to increased computing power and the discovery of new algorithms that can efficiently solve these problems. Therefore, the security level of cryptographic technologies needs to be periodically reviewed in response to advancements in technology. For instance, Data Encryption Standard (DES) was considered secure in the 1970s, but due to increased computational capabilities and new cryptoanalytical attack methods, it was found to be vulnerable and was replaced in 2002 by Advanced Encryption Standard (AES), which offers higher security and faster processing. Thus, experts continue to evaluate security level of existing cryptographic algorithms. These evaluations are conducted by organizations such as the National Institute of Standards and Technology (NIST) in the United States and the Cryptography Research and Evaluation Committees (CRYPTREC) in Japan. These institutions publish and regularly update lists of recommended cryptographic algorithms.

Cryptography can be used to secure digital data exchanged over networks against unauthorized access, misuse, or alteration. Moreover, the cryptographic algorithms are strictly evaluated and recommended lists of cryptographic algorithms providing robust countermeasures against cryptoanalytical attacks are published. As a result, attacks such as eavesdropping, tampering, or cryptoanalytical attack that threaten software security on networks are highly challenging. Even though the seculity level of used cryptographic algorithms are strictly eavaluated by experts, the threat of physical attacks exploiting vulnerabilities of electronic devices, where these algorithms are implemented, exists as shown in Fig. 6-1. Such physical attacks include SC attacks, where secret information is exploited by analyzing SC information such as electromagnetic noise emitted during circuit operation, and fault injection attacks, where intentional malfunctions are induced by injecting noise into circuits. These physical attacks are significant security risk and therefore the need for countermeasures not only against software security threats but also against hardware security threats.

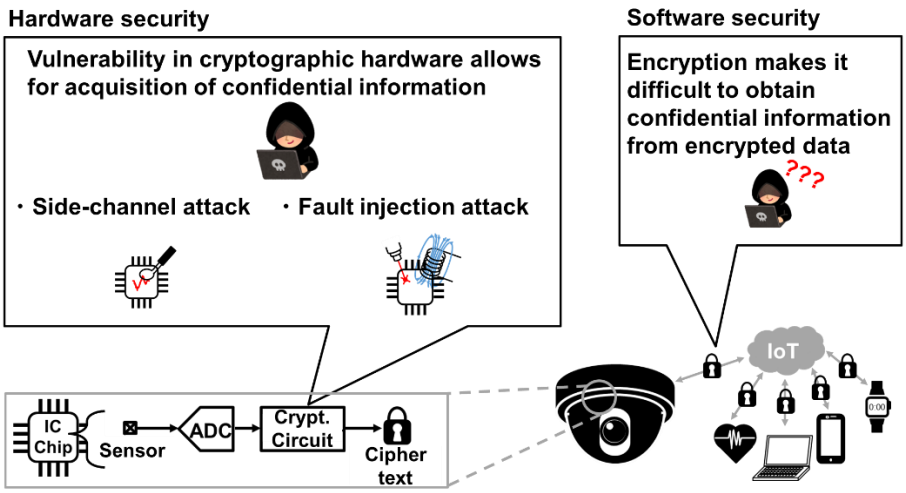


Fig. 6-1 Hardware security threats of digital data

There are reports of successful SC attacks and fault injection attacks on products in the commercial market. For example, in 2010, it was reported that secret information could be extracted through a SC attack on NXP's chips, "Mifare Classic" and "Mifare DESFire cards," utilized in the IC cards. Also, in 2021, successful SC attacks for Intel's microprocessors and Google's "Titan Security Key," employed for two-factor authentication were reported. There are some notable reports of fault injection attacks including the attack on Sony's PlayStation Vita in 2019, the attacks on electronic key authentication systems used by various car manufacturers in 2020, and the attack on Apple's AirTag in 2022. These examples show that both SC attacks and fault injection attacks are not just theoretical risks but are actual threats to products in the market.

As shown above, the threat of hardware security to actual products is becoming more realistic. However, addressing these hardware security threats is challenging for electronic device manufacturers lacking sufficient technical expertise. Therefore, the proposed business idea, "Design of Semiconductor IC Chips with Cryptographic Modules Resistant to Physical Attacks," aims to assist electronic device manufacturers in developing devices secured against physical attacks. This involves helping them establish specifications for countermeasures against physical attacks and resolving issues in the design of such countermeasures.

The proposed project is envisioned as a new project within "Secafy". Secafy, established in February 2023 by the authors, is a start-up company from Kobe

University. The company's mission is " Leveraging Secafy's strengths in 'Hardware Security Evaluation Technology' and 'Hardware Noise Evaluation Technology' to guarantee the security of hardware devices and contributing to the realization of a securer and safer ICT Society."

6.2 Innovation idea

As the importance of countermeasures against physical attacks increases, electronic device manufacturers, recognizing the threat of such attacks, may try to sell devices equipped with semiconductor IC chips resilient against physical attack. To manufacture and sell such electronic devices, they need to specify the required level of resistance to physical attacks for each product and the associated costs. Then, they must design semiconductor IC chips with these countermeasures. In this process, electronic device manufacturers face two primary issues: "Lack of technical expertise in defining specifications for the resistance of cryptographic modules to physical attacks" and "Absence of a suitable partner capable to design cryptographic modules with physical attack resistance" as depicted in Fig. 6-2. The details of these issues will be explained below.

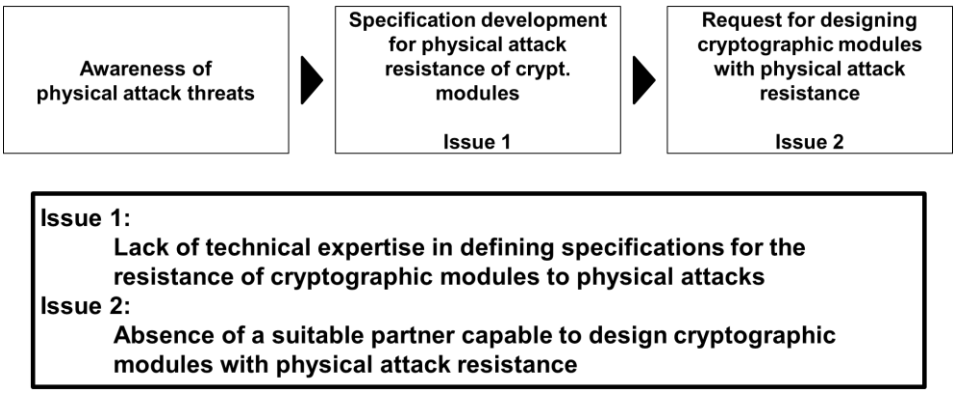


Fig. 6- 2 Issues for customers arising when electronic device manufacturers recognize the importance of hardware security

To make specifications for cryptographic modules resistant to physical attacks, it is necessary to consider the types of physical attacks that must be countered, based on factors such as the value of the data handled by each electronic device and usage environment of the device, and the required level of resistance against these attacks.

Also, because of the continuous evolvement of attack methods, it is crucial to constantly update information on the latest physical attack techniques. However, electronic device manufacturers, newly aware of the threat of physical attacks, often lack these knowledges. Consequently, they face difficulties in determining the appropriate level of physical attack resistance for each of their products or semiconductor IC chips. This is the first issue, "Lack of technical expertise in defining specifications for the resistance of cryptographic modules to physical attacks".

In the typical semiconductor IC chip design and manufacturing process, many electronic device manufacturers first development specification of the IC chip and then communicate these specifications to a turnkey provider to request the development of semiconductor IC chips, as illustrated in Fig. 6-3. The turnkey provider either designs in-house or outsources the design to a design house to create the design data. It is rare for turnkey providers to manufacture chips internally; instead, foundries typically manufacture the chips. When electronic device manufacturers plan to develop semiconductor IC chips with cryptographic modules resistant to physical attacks, they face the second issue, "Absence of a partner capable to design cryptographic modules with physical attack resistance", at the stage of requesting a turnkey provider to develop the IC chip. Turnkey providers and design houses lack the technical expertise to design IC chips equipped with cryptographic modules that are resistant to physical attacks.

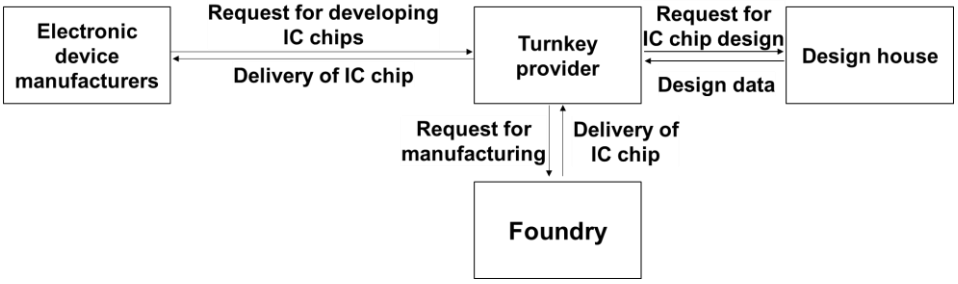


Fig. 6- 3 Semiconductor IC chip process from design to manufacturing

To solve these issues which electronic device manufacturers face, the proposed business offers two services: "Assistance in defining specifications for physical attacks on electronic devices and semiconductor IC chips" and "Designing cryptographic modules with high resistance to physical attacks."

Firstly, I'll explain the assistance service for defining specifications against physical attacks. A key consideration in formulating resistance to physical attacks is the fact that if the attacker's resources for conducting the attack are limitless, it's not possible to completely prevent the attack. Therefore, in assisting with specification development, it is essential to clearly define the types and levels of attacks each product needs to counter and to establish the appropriate level of physical attack resistance for each product.

The variation in types of physical attacks arises from combinations of three elements: "attack methods," "physical phenomena used in the attack," and "targets of the attack." The level of each physical attack depends on three factors: "the attacker's technical skills," "the performance of the equipment used in the attack," and "the duration of the attack". The types and levels of attacks to be countered should be decided baced on the value of the data handled by each electronic device and the environment in which the device is used. This is because the cost (both monetary and time) attackers are willing to invest varies depend on the value of the data, and the physical attacks feasiblility may be limited by the environment in which the product is used.

Therefore, by clearly defining the types of attacks that need countermeasures and the required levels of resistance for these attacks, considering the environment in which each product is used and the value of the data handled by the device, the proposed service supports the definition of specifications for physical attacks. This service solves the issue of "lack of technical expertise in defining specifications for resistance of cryptographic modules to physical attacks" faced by electronic device manufacturers.

The second service is to design cryptographic modules with high resistance to physical attacks. This service leverages the expertise gained from designing and evaluating cryptographic modules that have been fortified against physical attacks, as well as the physical attack resistance evaluation techniques using simulations discussed in Chapters 4 and 5. The service provides the desgn deta of cryptographic modules with high resistance to physical attacks and provide the design data.

Fig. 6-4 shows the process from specification development to sales of IC chips using the proposed service, "Designing cryptographic modules with high resistance to physical attacks." A key feature of this service is the pre-silicon verification of physical attack resistance during the design phase. This allows for comparison of physical attack resistance based on the presence or absence of countermeasures and

the differences in countermeasure techniques. There is a trade-off between physical attack resistance and overheads such as operational speed, circuit area, and power consumption. Therefore, specifications like power consumption and area need to be considered in addition to physical attack resistance during the design phase. Using this service, physical attack resistance of cryptographic modules with different countermeasure techniques can be verified at the design stage, enabling the achievement of the targeted security level at optimal overhead. Thus, this design service, which utilizes simulation-based physical attack resistance evaluation techniques, addresses the issue of "Absence of a partner capable to design cryptographic modules with physical attack resistance."

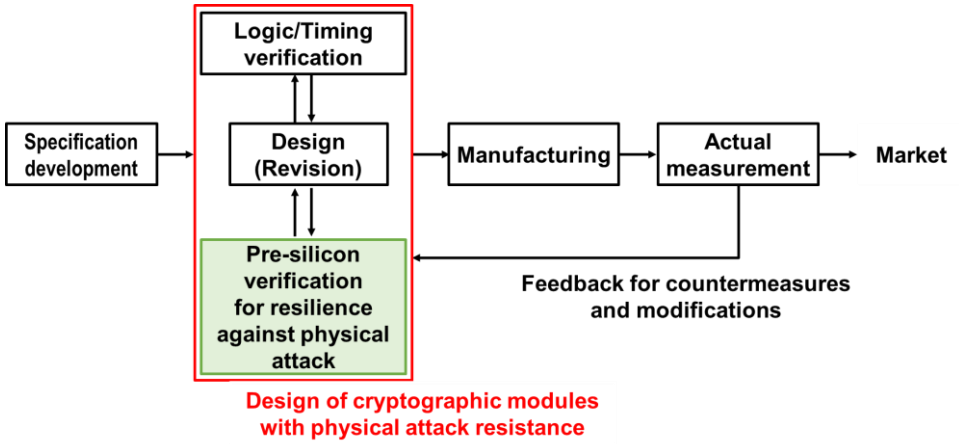


Fig.6- 4: Semiconductor IC chip process from specification to sales with the proposed design service.

This design service utilizing simulation-based physical attack resistance evaluation techniques not only achieves the specified level of resistance at optimal cost but also reduces the time and financial costs to reach that level of resistance. Without the proposed service, physical attack resistance could not be evaluated during the design stage, which makes actual measurements after fabrication is the only way to verify the effectiveness of countermeasures. As shown in the flow without proposed service in Fig. 6-5, if the expected level of physical attack resistance is not achieved, it is necessary to investigate the cause and repeat the process from design to actual measurement. However, with the proposed service, problems can be identified during the design verification and revision can be done before the manufacturing. As a result, as illustrated in Fig. 6-6, significant reductions

in time and financial costs are achieved by the service and it is a substantial benefit to customers.

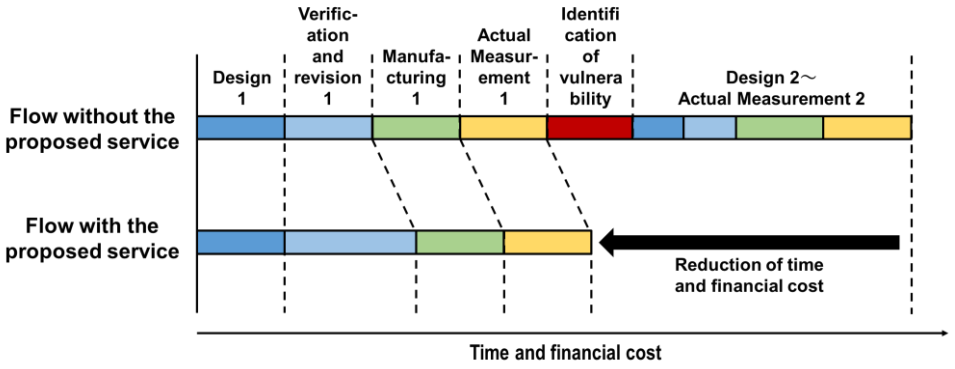


Fig. 6-5: Cost reduction image with cryptographic module design service featuring physical attack resistance

As described above, the two services of "Assistance in defining specifications for physical attacks on electronic devices and semiconductor IC chips" and "Designing cryptographic modules with high resistance to physical attacks" resolve issues faced by electronic device manufacturers. These issues are “a lack of technical expertise in specifying cryptographic modules with physical attack resistance” and “the absence of providers for designing such modules.” By utilizing these services, electronic device manufacturers can clearly define the required level of physical attack resistance for each semiconductor IC chip and achieve this resistance level with optimal overhead. Furthermore, compared to the traditional approach, these services enable a reduction in the time and financial costs involved in achieving the specified level of physical attack resistance. Therefore, the business providing these services are highly valuable to customers.

6.3 Analysis

In this section, we conducted both external and internal environmental analyses to clearify the strengths and weaknesses of the proposed business and to consider its strategic direction. Here, the results of the 5 Forces analysis and the VRIO (Value, Rarity, Imitability, Organization) analysis are presented. Finally, based on the

findings of both the external and internal environmental analyses, the business strategy will be discussed.

・Five Forces Analysis

The Five Forces analysis is a framework for understanding the profitability of an industry by analyzing five competitive factors: rivalry within the industry, the threat of new entrants, the suppliers' power, the power of buyers, and the threat of substitutes. Below is a detailed analysis of each of these factors specifically for the industry focused on designing cryptographic modules with resistance to physical attacks.

- Rivalry within the industry
  Currently, there are no companies, either in Japan or internationally, offering design services specifically focused on physical attack resistance. However, some large companiess like NXP Semiconductors in the Netherlands have both hardware security research and design departments. Such companies may have the capability to design cryptographic modules with physical attack resistance internally.
- The threat of new entrants
  Designing devices with cryptographic modules that are resistant to physical attacks requires expertise in various specialized fields, such as circuit design, noise simulation for large-scale circuits, and noise analysis with an understanding of cryptographic modules. These diverse technical requirements create a high barrier to entry into this industry. On the other hand, companies that possess expertise in each of these individual fields exist, suggesting the possibility that these companies could develop technologies in other areas and potentially enter this market.
- The power of suppliers
  Suppliers in the industry are vendors of IC chip design tools and noise simulation tools. The tool vendor industry has kept growing through repeated mergers and acquisitions by a few companies and these companies accumulate expertise over a long period. This has led to an oligopolistic market, resulting in these sellers possessing strong power.

- The power of buyers
  Buyers are electronic device manufacturers that require devices equipped with cryptographic modules resistant to physical attacks. At the beginning of the business, it can be difficult to encourage buyers to use the services because customer's issues have not yet become apparent, resulting in strong power for the buyers. However, given the absence of competition in this specific area, once issues become more recognized through activities to make them aware the necessity of hardware security the power of the buyers is likely to weaken.
- The threat of substitutes
  Among IP vendors that provide cryptographic cores, there are companies providing cryptographic core IPs with logical measures against physical attacks. Examples of such companies include Secure-IC in France and Rambus in the United States. Some of these companies think that logical countermeasures alone are sufficient to provide adequate resistance to physical attacks. If this thought is correct, cryptographic core IPs with logical countermeasures could potentially become substitutes for our proposed solutions.

The market opportunities and threats that have been revealed through this Five Forces analysis is discussed below.

The primary opportunity lies in the absence of competition within the industry. Although the small number of buyers due to the lack of apparent issues electronic device manufacturers will face is a challenge for the proposed business, success in making customer challenges apparent would be advantageous. This is because the high technical barriers to entry and the abcense of competitors at present creat a situation without price competition and not posing a strong threat from buyers.

On the other hand, there are three main threats.

The first threat is the existence of large companies like NXP Semiconductors in the Netherlands, which have both hardware security research and design departments internally. Even if such companies have separate departments for hardware security research and design, challenges in communication and misunderstanding between these different specialized departments can make the design of countermeasures complex. Therefore, having various specialized technical skills within a single organization, as Secafy does, is a strength, and enhancing these strengs can mitigate

competition with companies that have internal hardware security research and design departments.

The second threat is the possibility of cryptographic core IPs with logical countermeasures against physical attack becoming a substitute. While there is a thought that logical countermeasures alone can sufficiently provide physical attack resistance, all countermeasures inherently come with overheads. Thus, selecting optimal countermeasures including circuit implementation is crucial. Also, there is an example that even logical countermeasures thought to be secure against physical attacks have been found to be vulnerable when implemented in circuitry. Therefore, logical countermeasure against physical attacks should not be seen as a threat of substitute but rather as complementary to the proposed business.

The final threat is the power of supplyers, IC chip design tool vendors and simulation tool vendors. In general, tool vendor industry is known as oligopolistic market, implying strong power of supplyer. However, the environment for tool usage is gradually changing such as emergence of pay-per-use license services and open-source design tools. The proposed business plans to use these services and tools to mitigate the power of supplyers. Currently, there are no pay-per-use services for simulation tools like those for design tools. Additionally, having a license in-house is necessary to protect intellectual property. Therefore, service pricing must consider the cost of tool licensing fees for simulation tools to ensure profitability.

・VRIO Analysis

We conducted a VRIO analysis to assess the sustainability of the business.

- Value

  In an advanced ICT society where digital data is highly valuable, securing these dogital data against physical attacks becomes increasingly crucial. However, due to technical complexities, it's challenging for electronic device manufacturers to design cryptographic modules with physical attack resistance. Our proposed service enables customers to overcome these technical issues and manufacture devices equipped with such modules, hence offering high value.

- Rarity

  Companies providing design services focused on physical attack resistance are rare, both domestically and internationally. Moreover, our business model, which supports electronic device manufacturers from specification setting to design, is feasible due to our specialized knowledge and expertise, making it a rare and strong aspect of our proposed business.

- Imitability

  Designing cryptographic modules with resistance to physical attacks requires a combination of specialized technical skills, including circuit design, noise simulation for large-scale circuits, and noise analysis with an understanding of cryptographic modules. These specialized skills required for simulation in physical attack resistance evaluation make it difficult to imitate. Additionally, Secafy enhances its imitability by improving its simulation techniques through comparisons with actual physical attack resistance evaluations, leveraging its various in-house technologies.

- Organization

  Secafy's team consists of five members with expertise in circuit design, noise simulation, and noise analysis of cryptographic modules, or experience in launching new business projects. This composition of highly skilled technicians and members capable of transforming technology into business makes the team a strength in conducting business utilizing technical advantages. Another strength is the small team size enabling fast decision-making and in-depth discussions. However, the low recognition of the company and lack of credibility are weaknesses. Therefore, it is crucial to conduct sales activities that enhance recognition of Secafy's technical capabilities and the importance of physical attack resistance and to build a solid track record in the business.

・Summary of the analisys

Based on the external and internal environmental analyses, I consider the strategy for the proposed business.

As the evolvement of an advanced ICT society, the demand in digital data security are increasing. Although the current awareness of physical attack threats is low, our interviews with domestic and international companies and research into certification programs reveal a growing awareness of the threat of physical attacks and the importance of countermeasures. In this context, our proposed business, which resolves technical issues for customers and enables the manufacturing of devices equipped with cryptographic modules resistant to physical attacks, holds high economic value. Additionally, Scafy's wide range of specialized technical skills are both rare and difficult to imitate. To maintain these strengths as a sustainable competitive advantage, it is essential to continually improve our expertise by leveraging the diverse technologies within our organization.

However, sales activity and preparing tools are weaknesses for the proposed business. In preparing tools, the high cost of tool licensing fees is a challenge to business profitability. We plan to reduce costs by utilizing pay-per-use license services and open-source design tools for design activities to address this issue. For simulation tools, where cost reduction is difficult, we will consider financial strategies with taking this weakness into account. In sales activities, the challenges are low awareness of physical attack threats and the company's low recognition and credibility. Therefore, at the initial stage of the business, we will focus on sales activities, actively participating in exhibitions and conferences to raise awareness of the threats and importance of physical attack countermeasures, while also promoting our research achievements and technical capabilities to enhance the company's recognition and credibility.

6.4 Conclusion

In the advanced ICT society, the social impact of utilizing digital data has significantly increased. This implies that the economic and social losses, incurred by companies, individuals, and society, due to unauthorized acquisition or misuse of digital data are also expanding. Therefore, in the advanced ICT society, it is crucial to protect digital data from unauthorized access and misuse using security technologies. Cryptographic technology is employed for data protection, but when implemented in electronic devices, physical attacks utilizing device vulnerabilities are threat to hardware security. However, when electronic device manufacturers try to produce devices equipped with countermeasures against these threats, they face two

challenges: a lack of technical expertise in specifying the physical attack resistance of cryptographic modules and the absence of a suitable partner capable to design cryptographic modules with physical attack resistance. In this chapter, I propose a business project for designing semiconductor IC chips equipped with cryptographic modules that have high resistance to physical attacks, aiming to contribute to the realization of an advanced information society where people can use technology with confidence.

In the analysis of this proposed project, external and internal environmental analyses were conducted. The demand and interest in digital data security are growing in an advanced ICT society. Within this context, the proposed business, which resolves customers' technical issues and enables the manufacturing of devices with cryptographic modules resistant to physical attacks, offers high value to customers. Additionally, Secafy’s wide range of specialized technical skills are both rare and difficult to imitate. To sustain these strengths as competitive advantages, it is essential to continually improve expertise by leveraging the diverse technologies within the organization. Issues include the high cost of tool licensing fees and low awareness of the threat of physical attacks. To address the high licensing fees, pay-per-use license services and the use of open-source tools are necessary, while promotion activity is required to increase awareness of the physical attack threat.

Section 7

Conclusion

In the advanced ICT society being realized through the advancement of information and communication technology, the societal impact of utilizing digital data has significantly increased. This implies a corresponding rise in economic and social losses, for businesses, individuals, and society, due to unauthorized acquisition or misuse of digital data. Therefore, in an advanced ICT society, it is crucial to protect digital data from unauthorized access and misuse using security technologies. While encryption is used to protect digital data, its implementation in electronic devices can make them vulnerable to physical attacks. These attacks include SC attacks and fault injection attacks. Such attacks have also been carried out against actual products and drawing attention as a very serious threat. Consequently, countermeasures against physical attacks have become an urgent need.

This paper discusses countermeasure technologies to suppress SC leakage in chip package systems, which integrate the functions into one (or multiple) chips and package as a system. For SC leakage mitigation, it is important to precisely understand the behavior of power noise causing SC information leaks, and to develop countermeasure technologies. Therefore, this paper reports on high-resolution power noise evaluation technologies, packaging technologies to suppress side-channel leaks, and countermeasure technologies based on SC leakage simulations. Additionally, we have considered business plan using these technologies.

In Section 2, we discussed on-chip high-resolution PS noise evaluation techniques. We proposed an " IR-drop-based power-domain scenario-based testing and in-field diagnosis" enabled by on-chip high-resolution evaluation of PS noise. We designed and manufactured test chips and demonstrated proposed diagnosis. This approach is complementary to traditional IC testing and can diagnose circuits that consume power and stabilize the PS by generating toggles in the background without producing signal outputs.

In Section 3, we presented noise suppression techniques for PS networks using BBM in 3D stacked chips as a countermeasure against SC attack. This technique

forms PS networks with BBM to reduce PS noise. By embedding Cu wiring networks on the silicon substrate's backside, we achieved low-impedance power delivery and distributed parasitic capacitance between the BBM and the silicon substrate. The proposed method suppressed dynamic voltage drops, reducing voltage fluctuations by approximately 59%. The effect of this noise reduction on suppressing SC leaks was evaluated using the statistical significance t-value, confirming 14x mitigation in SC leaks compared to conventional implementations.

Section 4 and 5 reported simulation technologies for SC leakage evaluation. SC leakage simulation is crucial as it enables pre-silicon evaluation of SC leaks and immediate revisions if necessary. However, current simulations face accuracy and speed issues and are not reaching a practical level yet. Therefore, in Section 4, we first report false-positive problem in SC leakage evaluation through transistor-level simulations and then developed a simulation method that avoids the problem. In Section 5, we proposed a method to speed up simulations for VLSI circuits while maintaining accuracy.

Finally, in Section 6, the business idea using simulation technologies for SC leakage evaluation was discussed. Considering the social background and issues customers will face, we proposed a business project for designing IC chips equipped with cryptographic modules highly resistant to physical attacks and analyzed the business environment for the proposed project. The analysis revealed that at the current stage, where the threat of physical attacks is not perceived as strong, it is crucial to make customers aware of these threats during the business launch phase. Once the threat is recognized and the first customers start using the service, the business can expand by continuously researching and developing simulation technologies and increasing the barriers to new entry.

Acknowledgement

My greatest appreciation goes to my supervisor, Professor Makoto Nagata, for his long-term support, patient guidance, and advice on this research throughout my time as his student.

I am profoundly thankful to Associate Professors Takuji Miki and Nobuhiro Fuke of Kobe University Graduate School of Science, Technology and Innovation for their earnest guidance and support throughout the progression of this study.

I deeply appreciate Professor Noriyuki Miura of Osaka University and Mr. Takaaki Okidono for their suitable guidance and advice concerning this research.

I am grateful to Ms. Michi Tanaka and Ms. Miki Yamazaki for making my daily life in the research lab comfortable through their meticulous attention to administrative and accounting matters.

I also extend my deep gratitude to Dr. Koh Watanabe and Dr. Hiroki Sonoda of Kobe University Graduate School of Science, Technology and Innovation for their constant support and for offering various perspectives. Likewise, I thank everyone in the research lab and the Kobe University Graduate School of Science, Technology and Innovation along with all related parties.

The study of on-chip high-resolution PS noise evaluation techniques was supported by the Interuniversity Microelectronics Centre (imec) and Aristotle University of Thessaloniki. I offer my special thanks to Dr. Eric Jan Marinissen, Professor Alkis Hatzopoulos, Mr. Leonidas Katselas and Mr. Ferenc Fodor.

The research of transistor-level simulation for SC leakage evaluation was supported by COSIC, KULeuven. I offer my special thanks to Professor Ingrid Verbauwhede, Assistant Professor Josep Balasch and Dr. Danilo Sijacic.

The study of Simulation-based power and EM SCLA techniques was supported by ANSYS. I offer my special thanks to Dr. Norman Chang, Dr. Lang Lin, Dr. Jimin Wen and Dr. Sreeja Chowdhury.

Lastly, I express my profound gratitude to my family for their support in my life.

References

[1] Kazuki Monta, Leonidas Kataselas, Ferenc Fodor, Takuji Miki, Alkis Hatzopoulos, Makoto Nagata, Erik Jan Marinissen, "Testing Embedded Toggle Generation Through On-Chip IR Drop Measurements," in IEEE Design & Test, vol. 39, no. 5, pp. 79-87, Oct. 2022.

[2] Kazuki Monta, Hiroki Sonoda, Takaaki Okidono, Yuuki Araga, Naoya Watanabe, Haruo Shimamoto, Katsuya Kikuchi, Noriyuki Miura, Takuji Miki, Makoto Nagata, "3-D CMOS Chip Stacking for Security ICs Featuring Backside Buried Metal Power Delivery Networks with Distributed Capacitance," IEEE Transactions on Electron Devices, vol. 68, no. 4, pp. 2077-2082, Apr. 2021.

[3] Kazuki Monta, Makoto Nagata, Josep Balasch, Ingrid Verbauwhede, "ON THE UNPREDICTABILITY OF SPICE SIMULATIONS FOR SIDE-CHANNEL LEAKAGE VERIFICATION OF MASKED CRYPTOGRAPHIC CIRCUITS," ACM/IEEE Design Automation Conference (DAC 2023), Jul. 2023. (San Francisco).

[4] Kazuki Monta, Lang Lin, Jimin Wen, Harsh Shrivastav, Calvin Chow, Hua Chen, Joao Geada, Sreeja Chowdhury, Nitin Pundir, Norman Chang, Makoto Nagata, "Silicon-correlated Simulation Methodology of EM Side-channel Leakage Analysis," ACM Journal on Emerging Technology in Computing System, vol. 19, no. 1, Article 9, Jan. 2023, 23 pages.

[5] Yervant Zorian et al., 'Testing Embedded-Core Based System Chips', IEEE International Test Conference (ITC1998), Washington, D.C, October 1998, pp. 130-143, DOI 10.1109/TEST.1998.743146

[6] L.Katselas et al., 'On-Chip Toggle Generators to Provide Realistic Conditions during Test of Digital 2D-SoCs and 3D-SICs', IEEE International Test Conference (ITC'18), Oct. 2018, doi: 10.1109/TEST.2018.8624803

[7] E.J. Marinissen and S. Deutsch, “Controlled toggle rate of non-test signals during modular scan testing of an integrated circuit,” Dec. 16 2014, US Patent 8,914,689. [Online]. Available: https://www.google.com/patents/US8914689

[8] Y.Komatsu et al., "A 0.25–27-Gb/s PAM4/NRZ Transceiver With Adaptive Power CDR and Jitter Analysis," in IEEE Journal of Solid-State Circuits, vol. 54, no. 10, pp. 2802-2811, Oct. 2019, doi: 10.1109/JSSC.2019.2920082.

[9] C.Wang et al., "Power Profile Equalizer: A Lightweight Countermeasure against Side-Channel Attack," 2017 IEEE International Conference on Computer Design (ICCD), Boston, MA, 2017, pp. 305-312, doi: 10.1109/ICCD.2017.54

[10] H.Esmaeilzadeh et al.,"Dark silicon and the end of multicore scaling," 2011 38th Annual International Symposium on Computer Architecture (ISCA), San Jose, CA, 2011, pp. 365-376.

[11] J. Saxena et al., "A case study of ir-drop in structured at-speed testing," International Test Conference, 2003. Proceedings. ITC 2003., 2003, pp. 1098-1104, doi: 10.1109/TEST.2003.1271098.

[12] Z. Abuhamdeh et al.,"Characterize Predicted vs Actual IR Drop in a Chip Using Scan Clocks," 2006 IEEE International Test Conference, 2006, pp. 1-8, doi: 10.1109/TEST.2006.297656.

[13] Y.Lechuga et al.,"Built-in dynamic current sensor for hard-to-detect faults in mixed-signal ICs," Proceedings 2002 Design, Automation and Test in Europe Conference and Exhibition, Paris, France, 2002, pp. 205-211, doi: 10.1109/DATE.2002.998271.

[14] M.Nagata et al., "A built-in technique for probing power supply and ground noise distribution within large-scale digital integrated circuits," in IEEE Journal of Solid-State Circuits, vol. 40, no. 4, pp. 813-819, April 2005, doi: 10.1109/JSSC.2005.845559.

[15] IEEE Std 1500 Working Group, 'IEEE Standard Testability Method for Embedded Core-based Integrated Circuits', IEEE Std 1500-2005, published August 29, 2005, DOI 10.1109/IEEESTD.2005.96465

[16] K.Monta et al., "Testing Embedded Toggle Pattern Generation Through On-Chip IR Drop Monitoring," 2021 IEEE European Test Symposium (ETS), 2021, pp. 1-4, doi: 10.1109/ETS50041.2021.9465391.

[17] Yongki Min, Reynaldo Olmedo, Michael Hill, Kaladhar Radhakrishnan, Ke mal Aygun, Mostafa Kabiri-Badr, Rahul Panat, Sriram Dattaguru, Haluk B alkan, "Embedded Capacitors in the Next Generation Processor," in Procee dings of 2013 IEEE 63rd Electronic Components and Technology Confere nce (ECTC), pp. 1225-1229, May 2013.

[18] Myongseob Kim, Henley Liu, Dima Klokotov, Anna Wong, Thomas To, J

onathan Chang, "Performance Improvement for FPGA due to Interposer M etal Insulator Metal Decoupling Capacitors (MIMCAP)," in Proceedings of 2020 IEEE 70th Electronic Components and Technology Conference (EC TC), pp. 386-392, May 2020.

[19] Tomoyuki Akahoshi, Daisuke Mizutani, Kei Fukui, Seigo Yamawaki, Hide hiko Fujisaki, Manabu Watanabe, Masateru Koide, "Development of CPU Package Embedded with Multilayer Thin Film Capacitor for Stabilization of Power Supply," in Proceedings of 2017 IEEE 67th Electronic Compone nts and Technology Conference (ECTC), pp. 179-184, May 2017.

[20] Bing Dang, Michael Shapiro, Paul Andry, Cornelia Tsang, Edmund Sprogi s, Steven Wright, Mario Interrante, Jonathan Griffith, Van Truong, Luc Gu erin, Roger Liptak, Daniel Berger, John Knickerbocker, "Three-Dimensiona l Chip Stack with Integrated Decoupling Capacitors and Thru-Si Via Inter connects," IEEE Electron Device Letters, vol. 31, no. 12, pp. 1461-1463, Dec. 2010.

[21] S.Y. Hou, H. Hsia, C.H. Tsai, K.C. Ting, T.H. Yu, Y.W. Lee, F.C. Chen, W.C. Chiou, C.T. Wang, C.H. Wu, Douglas Yu, "Integrated Deep Trench Capacitor in Si Interposer for CoWoS Heterogeneous Integration," in Tech nical Digest of IEEE International Electron Devices Meeting (IEDM), pp. 19.5.1-19.5.4, Dec. 2019.

[22] Eunseok Song, Dan Oh, Seung-Yong Cha, Jaejune Jang, Taejoo Hwang, G youngbum Kim, Jongkook Kim, Sunghwan Min, Kilsoo Kim, Dae-Woo Ki m, Seungwook Yoon, "Power Integrity Performance Gain of a Novel Integ rated Stack Capacitor (ISC) Solution for High-end Computing Applications, " in Proceedings of 2020 IEEE 70th Electronic Components and Technolo gy Conference (ECTC), pp. 1358-1362, May 2020.

[23] Prathap Muthana, Arif Ege Engin, Madhavan Swaminathan, Rao Tummala, Venkatesh Sundaram, Boyd Wiedenman, Daniel Amey, Karl H. Dietz, So unak Banerji, "Design, Modeling, and Characterization of Embedded Capa citor Networks for Core Decoupling in the Package," IEEE Trans. Advanc ed Packaging, vol. 30, no. 4, pp. 809-822, Nov. 2007.

[24] Ioannis Savidis, Selcuk Kose, Eby G. Friedman, "Power Noise in TSV-Ba sed 3-D Integrated Circuits," IEEE J. Solid-State Circuits, vol. 48, no.2, p p. 587-597, Feb. 2013.

[25] Makoto Nagata, Satoshi Takaya, Hiroaki Ikeda, "In-Place Signal and Powe

r Noise Waveform Capturing Within 3-D Chip Stacking," IEEE Design an d Test, Vol. 32, No. 6, pp. 87-98, Nov. 2015.

[26] Paul D. Franzon, Erik Jan Marinissen, Muhannad S. Bakir (Eds.), “Handb ook of 3D Integration, Volume 4: Design, Test, and Thermal Management,” Wiley, Weinheim (2019).

[27] Yuuki Araga, Makoto Nagata, Hiroaki Ikeda, Takuji Miki, Noriyuki Miura, Naoya Watanabe, Haruo Shimamoto, Katsuya Kikuchi, "A Thick Cu Lay er Buried in Si Interposer Backside for Global Power Routing," IEEE Tra nsactions on Components, Packaging and Manufacturing Technology, Vol. 9, No. 3, pp. 502-510, Mar. 2019.

[28] Takuji Miki, Makoto Nagata, Akihiro Tsukioka, Noriyuki Miura, Takaaki Okidono, Yuuki Araga, Naoya Watanabe, Haruo Shimamoto, Katsuya Kiku chi, "Over-the-top Si Interposer Embedding Backside Buried Metal PDN t o Reduce Power Supply Impedance of Large Scale Digital ICs," in Proce edings of IEEE 2019 International 3D Systems Integration Conference (3D IC 2019), #B5L-B, pp.1-4, Oct. 2019.

[29] Takuji Miki, Makoto Nagata, Hiroki Sonoda, Noriyuki Miura, Takaaki Oki dono, Yuuki Araga, Naoya Watanabe, Haruo Shimamoto, Katsuya Kikuchi, "Si-Backside Protection Circuits Against Physical Security Attacks on Fli p-Chip Devices," IEEE Journal of Solid-State Circuits (JSSC), vol. 55, no. 10, pp. 2747-2755, Oct. 2020.

[30] Divya Prasad, S. S. Teja Nibhanupudi, Shidhartha Das, Odysseas Zografos, Bilal Chehab, Satadru Sarkar, Rogier Baert, Alex Robinson, Anshul Gupt a, Alessio Spessot, Peter, Debacker, Diederik Verkest, Jaydeep Kulkarni, B rian Cline and Saurabh Sinha, “Buried Power Rails and Back-side Power Grids: Arm® CPU Power Delivery Network Design Beyond 5nm,” in Tec hnical Digest of IEEE IEDM 2019, pp. 19.1.1-19.1.4, Dec. 2019.

[31] Md Obaidul Hossen, Bharani Chava, Geert Van der Plas, Eric Beyne, Mu hannad S. Bakir, “Power Delivery Network (PDN) Modeling for Backside-PDN Configurations with Buried Power Rails and μTSVs,” IEEE Transact ions on Electron Devices, vol. 67, no. pp. 11-17, Jan. 2020.

[32] Xiao Sun, Hesheng Lin, Dimitrios Velenis, John Slabbekoorn, Giacomo Ta lmelli, Pieter Bex, Tom Sterken, Rudy Lauwereins, Christoph Adelmann, Andy Miller, Geert Van der Plas, Eric Beyne, “3D Heterogeneous Packag e Integration of Air/Magnetic Core Inductor: 89%-Efficiency Buck Convert

er with Backside Power Delivery Network," in Digest of Technical Papers, 2020 Symposia on VLSI Technology and Circuits, TH1.2, June 2020.

[33] Hiroki Sonoda, Kazuki Monta, Takaaki Okidono, Yuuki Araga, Naoya Watanabe, Haruo Shimamoto, Katsuya Kikuchi, Noriyuki Miura, Takuji Miki, Makoto Nagata, "Secure 3D CMOS Chip Stacks with Backside Buried Metal Power Delivery Networks for Distributed Decoupling Capacitance," in Technical Digest of IEEE IEDM 2020, Dec. 2020.

[34] Jeremy Cooper, Gilbert Goodwill, Joshua Jaffe, Gary Kenworthy, Pankaj Rohatgi, "Test Vector Leakage Assessment (TVLA) methodology in practice," International Cryptographic Module Conference, Sept. 2013.

[35] P. C. Kocher et al., "Differential power analysis," in Advances in Cryptology - CRYPTO '99, ser. LNCS, M. J. Wiener, Ed., vol. 1666. Springer, 1999, pp. 388–397.

[36] S. Chari et al., "Towards sound approaches to counteract power-analysis attacks," in Advances in Cryptology — CRYPTO' 99, M. Wiener, Ed. Springer, 1999, pp. 398–412.

[37] S. Nikova et al., "Threshold implementations against side-channel attacks and glitches," in Information and Communications Security, P. Ning, S. Qing, and N. Li, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 529–545.

[38] H. Gross et al., "Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order," Cryptology ePrint Archive, Report 2016/486, 2016.

[39] E. Brier et al., "Correlation Power Analysis with a Leakage Model," In CHES 2004, volume 3156 of LNCS, pages 16–29. Springer, August 2004.

[40] J. Cooper et al., "Test Vector Leakage Assessment (TVLA) methodology in practice," International Cryptographic Module Conference, 2013.

[41] Shivam Bhasin et al., "Physical security evaluation at an early design-phase: A side-channel aware simulation methodology," In Christian Berger and Ina Schaefer, editors, Engineering Simulations for Cyber-Physical Systems - ES4CPS 2014, page 13. ACM, 2014

[42] Francesco Regazzoni et al., "Evaluating resistance of MCML technology to power analysis attacks using a simulation-based methodology," Transactions on Computational Science IV, Special Issue on Security in Computing, 4:230-243, 2009.

[43] Kris Tiri et al., “Simulation models for side-channel information leaks,” I n William H. Joyner Jr., Grant Martin, and Andrew B. Kahng, editors, D esign Automation Conference - DAC 2005, pages 228-233. ACM, 2005.

[44] D. Šijačić et al., “Towards efficient and automated side-channel evaluation s at design time,” Journal of Cryptographic Engineering, pages 1–15, 202 0.

[45] A. Tsukioka et al., “A fast side-channel leakage simulation technique base d on ic chip power modeling,” IEEE Letters on Electromagnetic Compatib ility Practice and Applications, 2020.

[46] Francesco Regazzoni et al., “A design flow and evaluation framework for dpa-resistant instruction set extensions,” In Christophe Clavier and Kris Gaj, editors, Cryptographic Hardware and Embedded Systems - CHES 200 9, volume 5747 of LNCS, pages 205-219.Springer, 2009.

[47] L. Lin et al., "Fast and Comprehensive Simulation Methodology for Layo ut-Based Power-Noise Side-Channel Leakage Analysis," 2020 IEEE Interna tional Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), 2 020, pp. 133-138.

[48] Daisuke Fujimoto et al., “A fast power current analysis methodology usin g capacitor charging model for side channel attack evaluation,” In Hardwa re-Oriented Security and Trust - HOST 2011, pages 87–92. IEEE, 2011.

[49] K. Tiri et al., “A logic level design methodology for a secure DPA resist ant asic or fpga implementation”. In IEEE DATE, pages 246–251, 2004.

[50] C. Tokunaga et al., “Securing Encryption Systems with a Switched Capaci tor Current Equalizer,” IEEE JSSC, vol. 45, no. 1, pp. 23-31, 2010.

[51] Y. Ishai et al., “Private Circuits: Securing Hardware against Probing Attac ks,” In D. Boneh, editor, Advances in Cryptology - CRYPTO 2003, volu me 2729 of Lecture Notes in Computer Science, pages 463–481. Springer Berlin Heidelberg, 2003.

[52] S. Faust et al., “Protecting Circuits from Leakage: the Computationally-Bo unded and Noisy Cases,” In H. Gilbert, editor, Advances in Cryptology E UROCRYPT 2010, volume 6110 of Lecture Notes in Computer Science, p ages 135–156. Springer Berlin Heidelberg, 2010.

[53] M. Rivain et al., “Provably Secure Higher-Order Masking of AES,” In S. Mangard and F.-X. Standaert, editors, Cryptographic Hardware and Embe dded Systems, CHES 2010, volume 6225 of Lecture Notes in Computer

Science, pages 413–427. Springer Berlin Hei delberg, 2010.

[54] Stefan Mangard et al., “Side-channel leakage of masked CMOS gates”, A. J. Menezes, Ed., CT-RSA 2005, LNCS 3376, Springer Verlag, 2005, pp. 351–36.

[55] I. Levi et al., “Reducing a Masked Implementation's Effective Security Or der with Setup Manipulations And an Explanation Based on Externally-A mplified Couplings.” IACR Trans. Cryptogr. Hardw. Embed. Syst. 2019 (2 019): 293-317.

[56] De Cnudde et al., “Does Coupling Affect the Security of Masked Implem entations?,” In: Guilley, S. (eds) Constructive Side-Channel Analysis and Secure Design. COSADE 2017. Lecture Notes in Computer Science(), vol 10348. Springer, Cham.

[57] Nagel, L. W et al., SPICE (Simulation Program with Integrated Circuit E mphasis), Memorandum No. ERL-M382, University of California, Berkeley, Apr. 1973.

[58] Nagel, L. W, SPICE2: A Computer Program to Simulate Semiconductor C ircuits, Technincal Report No. UCB/ERL M520, Electronics Research Labo ratory, University of California, Berkeley, May 1975.

[59] Gilbert Goodwill et al., “A testing methodology for side channel resistanc e validation,” NIST non invasive attack testing workshop, 2011.

[60] Schneider, T. et al., A. Leakage assessment methodology – A clear roadm ap for side-channel evaluations. In Cryptographic Hardware and Embedded Systems - CHES 2015 (2015), T. Güneysu and H. Handschuh, Eds., vol. 9293 of LNCS, Springer, pp. 495–513.

[61] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis”. In Annual I nternational Cryptology Conference, pp. 388–397, Springer, 1999.

[62] Eric Brier, Christophe Clavier, and Francis Olivier. 2004. Correlation Pow er Analysis with a Leakage Model. In Cryptographic Hardware and Embe dded Systems, Marc Joye and Jean-Jacques Quisquater (Eds.). Springer, 16 –29

[63] Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic analysis: Concrete r esults. In: Ko¸c, C¸ .K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 251–261. Springer, Heidelberg (2001)

[64] Quisquater, J., Samyde, D.: Electromagnetic analysis (EMA): Measures an d counter-measures for smart cards. In: Attali, S., Jensen, T. (eds.) E-smar

t 2001. LNCS, vol. 2140, pp. 200–210. Springer, Heidelberg (2001)

[65] D. Agrawal, B. Archambeault, J.R. Rao, P. Rohatgi, “The EM Side-Chann el(s).” In Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, vol 2523, pp. 29-45, 2002.

[66] R´eal, D., Valette, F., Drissi, M.: Enhancing Correlation Electromagnetic A ttack Using Planar Near-Field Cartography. In: DATE 2009, pp. 628–633 (2009)

[67] Peeters, E., Standaert, X., Quisquater, J.: Power and electromagnetic analy sis: Improved model, consequences and comparisons. Integration, the VLSI Journal 40(1), 52–60 (2007)

[68] K. Tiri, I. Verbauwhede, “A logic level design methodology for a secure DPA resistant asic or fpga implementation”. In IEEE DATE, pages 246–2 51, 2004.

[69] C. Tokunaga and D. Blaauw, “Securing Encryption Systems with a Switch ed Capacitor Current Equalizer,” IEEE JSSC, vol. 45, no. 1, pp. 23-31, 2 010.

[70] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, “Towards sound approac hes to counteract power-analysis attacks,” in Advances in Cryptology — CRYPTO’ 99, M. Wiener, Ed. Springer, 1999, pp. 398–412.

[71] Goubin L., Patarin J. (1999) DES and Differential Power Analysis The “Duplication” Method. In: Koç Ç.K., Paar C. (eds) Cryptographic Hardwar e and Embedded Systems. CHES 1999. Lecture Notes in Computer Scien ce, vol 1717. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-480 59-5_15

[72] S. Nikova, C. Rechberger, and V. Rijmen, “Threshold implementations aga inst side-channel attacks and glitches,” in Information and Communications Security, P. Ning, S. Qing, and N. Li, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 529–545.

[73] H. Gross, S. Mangard, and T. Korak, “Domain-Oriented Masking: Compac t Masked Hardware Implementations with Arbitrary Protection Order,” Cry ptology ePrint Archive, Report 2016/486, 2016, http://eprint.iacr.org/2016/4 86.

[74] Shivam Bhasin, Jean-Luc Danger, Tarik Graba, Yves Mathieu, Daisuke Fuj imoto, and Makoto Nagata. Physical security evaluation at an early design -phase: A side-channel aware simulation methodology. In Christian Berger

and Ina Schaefer, editors, Engineering Simulations for Cyber-Physical Sys tems - ES4CPS 2014, page 13. ACM, 2014.

[75] Dina Kamel, Mathieu Renauld, Denis Flandre, and Francois-Xavier Standa ert. Understanding the limitations and improving the relevance of SPICE s imulations in side-channel security evaluations. J. Cryptographic Engineerin g, 4(3):187-195, 2014.

[76] Francesco Regazzoni, Thomas Eisenbarth, Axel Poschmann, Johann Grosch adl, Frank K. Gurkaynak, Marco Macchetti, Zeynep Toprak Deniz, Laura Pozzi, Christof Paar, Yusuf Leblebici, and Paolo Ienne. Evaluating resistan ce of MCML technology to power analysis attacks using a simulation-bas ed methodology. Transactions on Computational Science IV, Special Issue on Security in Computing, 4:230-243, 2009.

[77] Kris Tiri and Ingrid Verbauwhede. Simulation models for side-channel inf ormation leaks. In William H. Joyner Jr., Grant Martin, and Andrew B. K ahng, editors, Design Automation Conference - DAC 2005, pages 228-233. ACM, 2005.

[78] D. Šijačić, J. Balasch, and I. Verbauwhede. Sweeping for leakage in mask ed circuit layouts. In 2020 Design, Automation & Test in Europe Confere nce & Exhibition (DATE), pages 915–920. IEEE, 2020.

[79] D. Šijačić, J. Balasch, B. Yang, S. Ghosh, and I. Verbauwhede. Towards efficient and automated side-channel evaluations at design time. Journal of Cryptographic Engineering, pages 1–15, 2020.

[80] A. Tsukioka, K. Srinivasan, S. Wan, L. Lin, Y.-S. Li, N. Chang, and M. Nagata. A fast side-channel leakage simulation technique based on ic chip power modeling. IEEE Letters on Electromagnetic Compatibility Practice and Applications, 2020.

[81] J. Knechtel, E. B. Kavun, F. Regazzoni, A. Heuser, A. Chattopadhyay, D. Mukhopad- hyay, S. Dey, Y. Fei, Y. Belenky, I. Levi, et al. “Towards se cure composition of integrated circuits and electronic systems: On the role of EDA,” DATE 2020.

[82] Francesco Regazzoni, Alessandro Cevrero, Francois-Xavier Standaert, Steph ane Badel, Theo Kluter, Philip Brisk, Yusuf Leblebici, and Paolo Ienne. A design flow and evaluation framework for dpa-resistant instruction set ext ensions. In Christophe Clavier and Kris Gaj, editors, Cryptographic Hardw are and Embedded Systems - CHES 2009, volume 5747 of LNCS, pages

205-219.Springer, 2009.

[83] L. Lin, Dinesh Selvakumaran, Deqi Zhu, Norman Chang, Calvin Chow, Makoto Nagata, and Kazuki Monta, "Fast and Comprehensive Simulation Methodology for Layout-Based Power-Noise Side-Channel Leakage Analysis," 2020 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), 2020, pp. 133-138, doi: 10.1109/iSES50453.2020.00038.

[84] Lang Lin, Deqi Zhu, Jimin Wen, Hua Chen, Yu Lu, Norman Chang, Calvin Chow, Harsh Shrivastav, Chia-Wei Chen, Kazuki Monta and Makoto Nagata, " Multiphysics Simulation of EM Side-Channels from Silicon Backside with ML-based Auto-POI Identification," 2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2021. (This paper has been accepted and will be published.)

[85] L. Lin, D. Selvakumaran, D. Zhu, N. Chang, C. Chow, M. Nagata, K. Monta, “Fast and Comprehensive Simulation Methodology for Layout-Based Power-Noise Side-Channel Leakage Analysis,” IEEE International Symposium on Smart Electronic Systems, pp. 144-149, 2020.

[86] ANSYS RedHawk-SC, https://www.ansys.com/products/semiconductors/

[87] Z. Yu, J. Koo, Mix, J A and Slattery, K and J. Fan, “Extracting physical IC models using near-field scanning”, In IEEE International Symposium on Electromagnetic Compatibility (EMC), pp. 317-320, 2010.

[88] Z. Yu, J. A. Mix, S. Sajuyigbe, K. P. Slattery and J. Fan, "An Improved Dipole-Moment Model Based on Near-Field Scanning for Characterizing Near-Field Coupling and Far-Field Radiation From an IC," in IEEE Transactions on Electromagnetic Compatibility, vol. 55, no. 1, pp. 97-108, Feb. 2013, doi: 10.1109/TEMC.2012.2207726.

[89] Y. Vives-Gilabert, C. Arcambal, A. Louis, F. de Daran, P. Eudeline and B. Mazari, "Modeling Magnetic Radiations of Electronic Circuits Using Near-Field Scanning Method," in IEEE Transactions on Electromagnetic Compatibility, vol. 49, no. 2, pp. 391-400, May 2007, doi: 10.1109/TEMC.2006.890168.

[90] D. Baudry, C. Arcambal, A. Louis, B. Mazari and P. Eudeline, "Applications of the Near-Field Techniques in EMC Investigations," in IEEE Transactions on Electromagnetic Compatibility, vol. 49, no. 3, pp. 485-493, Aug. 2007, doi: 10.1109/TEMC.2007.902194.

[91] A. Nahiyan, J. Park, M. He, Y. Iskander, F. Farahmandi, D. Forte, M. Te hranipoor, “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) (May 2020). https://doi.org/10.11 45/3383445, https://doi.org/10.1145/3383445

[92] W. Hu, D. Mu, J. Oberg, B. Mao, M. Tiwari, T. Sherwood, R. Kastner. “Gate-level information flow tracking for security lattices”. ACM Transacti ons on Design Automation of Electronic Systems (TODAES) 20(1), 1–25 (2014)

[93] J. Cooper, E. DeMulder, G. Goodwill, J. Jaffe, G. Kenworthy, and P. Roh atgi, “Test Vector Leakage Assessment (TVLA) methodology in practice,” International Cryptographic Module Conference, 2013.

[94] G. Goodwill, B. Jun, J. Jaffe, and P. Rohatgi, “A testing methodology for side channel resistance validation”, NIST non-invasive attack testing work shop, 2011.

List of publications

Journals

[1] Kazuki Monta, Lang Lin, Jimin Wen, Harsh Shrivastav, Calvin Chow, Hua Chen, Joao Geada, Sreeja Chowdhury, Nitin Pundir, Norman Chang, Makoto Nagata, "Silicon-correlated Simulation Methodology of EM Side-channel Leakage Analysis," ACM Journal on Emerging Technology in Computing System, vol. 19, no. 1, Article 9, Jan. 2023, 23 pages.

[2] Kazuki Monta, Leonidas Kataselas, Ferenc Fodor, Takuji Miki, Alkis Hatzopoulos, Makoto Nagata, Erik Jan Marinissen, "Testing Embedded Toggle Generation Through On-Chip IR Drop Measurements," in IEEE Design & Test, vol. 39, no. 5, pp. 79-87, Oct. 2022.

[3] Kazuki Monta, Hiroki Sonoda, Takaaki Okidono, Yuuki Araga, Naoya Watanabe, Haruo Shimamoto, Katsuya Kikuchi, Noriyuki Miura, Takuji Miki, Makoto Nagata, "3-D CMOS Chip Stacking for Security ICs Featuring Backside Buried Metal Power Delivery Networks With Distributed Capacitance," IEEE Transactions on Electron Devices, vol. 68, no. 4, pp. 2077-2082, Apr. 2021.

International Conferences

[4] Kazuki Monta, Makoto Nagata, Josep Balasch, Ingrid Verbauwhede, " ON THE UNPREDICTABILITY OF SPICE SIMULATIONS FOR SI DE-CHANNEL LEAKAGE VERIFICATION OF MASKED CRYPTO GRAPHIC CIRCUITS," ACM/IEEE Design Automation Conference (DAC 2023), Jul. 2023. (San Francisco)

[5] Takuya Wadatsumi, Rikuu Hasegawa, Kazuki Monta, Takaaki Okidono, Takuji Miki, Makoto Nagata, "A Si-Interposer with Buried Cu Metal

Stripes and Bonded to Si-Substrate Backside for Security IC Chips," in Proceedings of the IEEE 73rd Electronic Components and Technology Conference (ECTC 2023), pp. 951-954, June 2023. (Orlando)

[6] Kazuki Monta, Takumi Matsumaru, Takaaki Okidono, Takuji Miki, Makoto Nagata, "Side-Channel Leakage Evaluation of Multi-Chip Cryptographic Modules," Workshop on Nano Security at DATE2023, Apr. 2023. (Antwelp)

[7] Takuya Wadatsumi, Kohei Kawai, Rikuu Hasegawa, Kazuki Monta, Takuji Miki, Makoto Nagata, "Characterization of Backside ESD Impacts on Integrated Circuits," IEEE International Reliability Physics Symposium (IRPS 2023), #P22, Mar. 2023. (Monterey)

[8] Kazuki Monta, Makoto Nagata, Lang Lin, Jimin Wen, Preeti Gupta, Norman Chang, "RTL DESIGN SECURITY VERIFICATION FOR RESISTING POWER SIDE-CHANNEL ANALYSIS," ACM/IEEE Design Automation Conference (DAC 2022), Engineering Tracks, Jul. 2022. (San Francisco)

[9] Koh Watanabe, Takuya Wadatsumi, Kazuki Monta, Mai Aoi, Misaki Komatsu, Ryota Sakai, Satoshi Tanaka, Takuji Miki, Makoto Nagata, "Near Field Measurements of Sub-Millimeter-Wave Noise Emission from Digital Integrated Circuits," in Proceedings of the 13th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMC Compo 2021), pp. 45-47, Mar. 2022. (online)

[10] Lang Lin, Deqi Zhu, Jimin Wen, Hua Chen, Yu Lu, Norman Chang, Calvin Chow, Harsh Shrivastav, Chia-Wei Chen, Kazuki Monta, Makoto Nagata, "Multiphysics Simulation of EM Side-Channels from Silicon Backside with ML-based Auto-POI Identification," in Proceedings of the 2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 270-280, Dec. 2021.

[11] Lang Lin, Deqi Zhu, Kazuki Monta, Makoto Nagata, Calvin Chow, N

orman Chang, "Enabling Secure SoC Design by Fast Power-noise & EM Side-channel Emission Analysis," in Proc. 26th DesignCon 2021, Aug. 2021. (San Jose)

[12] Kazuki Monta, Leonidas Kataselas, Ferenc Fodor, Alkis Hatzopoulos, Makoto Nagata, Erik Jan Marinissen, "Testing Embedded Toggle Pattern Generation Through On-Chip IR Drop Monitoring," in Proceedings of the 26th IEEE European Test Symposium (ETS 2021), #S1-2, pp. 1-4, May 2021. (Virtual conference)

[13] Hiroki Sonoda, Kazuki Monta, Takaaki Okidono, Yuuki Araga, Naoya Watanabe, Haruo Shimamoto, Katsuya Kikuchi, Noriyuki Miura, Takuji Miki, Makoto Nagata, "Secure 3D CMOS Chip Stacks with Backside Buried Metal Power Delivery Networks for Distributed Decoupling Capacitance," in Proceedings of the 66th IEEE International Electron Device Meeting (IEDM 2020), #31.5, pp. 1-4, Dec. 2020. (Virtual conference)

[14] Lang Lin, Dinesh Selvakumaran, Deqi Zhu, Norman Chang, Calvin Chow, Makoto Nagata, Kazuki Monta, "Fast and Comprehensive Simulation Methodology for Layout-Based Power-Noise Side-Channel Leakage Analysis," in Proceedings of 2020 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), pp. 144-149, Dec. 2020. (Virtual conference)

[15] Makoto Nagata, Kazuki Monta, Akihiro Tsukioka, Lang Lin, Dinesh Selvakumaran, Norman Chang, Calvin Chow, "Fast and Comprehensive Layout-Based, Side-Channel Leakage Simulation with Simulation-to-Disclosure Metering," ACM/IEEE Design Automation Conference (DAC 2020), Designer Track #71.1, Jul. 2020. (Virtual conference)

Awards

[16] ハードウェアセキュリティフォーラム 2022 優秀ポスター賞, 電子情報通信学会 / ハードウェアセキュリティ研究専門委員会, 2023

[17] 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) BEST Paper Awards, IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2022.

[18] 研究会優秀若手講演賞 "電源ノイズシミュレーションによるサイドチャネル漏洩評価手法の検討", 電子情報通信学会 / 集積回路研究会, 2022

[19] 若手優秀賞 "大規模集積回路向け電源ノイズシミュレーションを用いた暗号モジュールのサイドチャネル漏洩評価", 電子情報通信学会 / ハードウェアセキュリティ研究専門委員会, 2021

[20] IEEE EDS Kansai Chapter MFSK Award, "Secure 3D CMOS Chip Stacks with Backside Buried Metal Power Delivery Networks for Distributed Decoupling Capacitance", IEEE EDS Kansai Chapter, 2021

[21] 第 19 回 IEEE EDS Japan Joint Chapter Student Award, "Secure 3D CMOS Chip Stacks with Backside Buried Metal Power Delivery Networks for Distributed Decoupling Capacitance", 2021

[22] Best Paper Award of the 6th IEEE International Symposium on Smart Electronic Systems (iSES), "Fast and Comprehensive Simulation Methodology for Layout-Based Power-Noise Side-Channel Leakage Analysis", IEEE / Computer society, Technical Committee on VLSI, 2020

[23] 若手優秀賞 "電源ノイズシミュレーションを用いた暗号モジュールのサイドチャネル漏洩評価", 電子情報通信学会 / ハードウェアセキュリティ研究専門委員会, 2020

[24] 若手研究会優秀ポスター賞 "オンチップモニタを用いた暗号モジュールにおけるサイドチャネル漏洩の評価", 電子情報通信学会 / 集積回路研究会, 2019

Doctor Thesis, Kobe University

“Chip-Package System Level Countermeasure Methodologies against Side-Channel Leakage Problems”, 103 pages

Submitted on January, 22, 2024

The date of publication is printed in cover of repository version published in Kobe University Repository Kernel.