A Novel Methodology for Testing Hardware Security and Trust Exploiting On-Chip Power Noise Measurement

–Extended Version–

Daisuke Fujimoto[1]* Shivam Bhasin[2]† Makoto Nagata[1] Jean-Luc Danger[2]
[1]Graduate School of System Informatics, Kobe University, Japan
e-mail: nagata@cs.kobe-u.ac.jp
[2]COMELEC, Telecom Paristech, France
e-mal: danger@telecom-paristech.fr

Abstract— Testing of electronic components is indispensable to minimize malfunction and failure of complex electronic systems. Currently, functionality and performance of these electronic components are the main parameters tested. However, validation of performance is not enough when the applications are safety or security critical. Therefore the security and trust of devices must also be tested before validation for such applications. In this paper, we promote the use of On-Chip Power noise Measurements (OCM), in order to test security using side-channel techniques. We then propose for the first time a standard side-channel measurement setup using OCM. Finally, we provide some key ideas on methodology to integrate the validation of hardware security and trust in the standard testing flow, exploiting OCM.

1 Introduction

Modern integrated circuits (ICs) are becoming more and more prone to manufacturing defects with rapidly shrinking sub-micron technologies. Such defects arise from statistical flaws in mask and material deployed in the IC fabrication process. Therefore reliable testing and diagnosis of complex new ICs is crucial. Test helps in identifying faulty devices as well as providing key feedback to analyze and diagnose the source of defects. Diagnosis improves the design and the manufacturing process, resulting in lower cost, a higher yield and a shorter time-to-market. It is impossible to achieve 100% yield i.e. all the manufactured ICs cannot satisfy all the performance specifications under all specified conditions. Moreover the performance specification of critical applications like defense, medical, space etc. are very strict, which in turn also affect the overall yield.

*Daisuke Fujimoto is currently a researcher at YNU, Japan. email:fujimoto-daisuke-ht@ynu.ac.jp

†Shivam Bhasin is currently with Temasek Labortaries,NTU,Singapore. email: sbhasin@ntu.edu.sg

Security and Trust of ICs has been a hot topic of research over the last decade. By security here, we imply the resistance of cryptographic cores (crypto-cores) against physical or side-channel (SC) attacks. These attacks exploit physical implementations of otherwise (theoretically) secure cryptography. On the other hand, Trust of modern ICs is a fairly new research direction which focuses on detection of trojan in a manufactured IC. A trojan is any malicious circuit introduced during any step of the IC design process. For critical applications, security and trust are also a key performance specification which should be tested before shipping the IC. However, to our knowledge, there is no provision for integration of security evaluation in the standard testing flow. In this paper, we propose integration and use of On-Chip power noise Measurement (OCM) into ICs for critical applications.

The key problem with evaluation of security is that there is no standard measurement setup. From one measurement setup to another, the quality of acquired side-channel traces varies. Moreover, even with a fixed setup, the interesting points of leakage on an IC may change, specially for electromagnetic measurements. Thus it is hard to integrate side-channel evaluation in the test process. Side-channel measurements can also be potentially used for trojan detection, but this topic is still in early phase of research. If we are able to standardize the measurement of side-channel activity, then security and trust evaluation can be integrated into the standard test and diagnosis flow.

Our Contributions: We propose three major contributions in this paper.

1. Firstly, we demonstrate the use of OCM in the context of hardware security and SC measurements. We compare the quality of measurements from the OCM to compare with traditional methods (1-ohm, EM probes).

2. Next, for the first time, we propose a methodology to build a standard measurement setup for SC traces.

3. Finally, we put forward a methodology to integrate the evaluation of security and detection of trojans into the standard test flow.

The rest of the paper is organized as follows: Sec. 2 gives general background on hardware security. The basics of designing an OCM and its prototype system is detailed in Sec. 3 Next in Sec. 4, we show the advantages of using OCM for hardware security evaluation with real experiments on a cryptographic core in $0.18um$ technology. In Sec. 5 we propose a standard SC measurment setup using OCM. The methodology to integrate hardware security and trust evaluation in the standard test flow is detailed in Sec. 6. Finally conclusions are drawn in Sec. 7.

2 General Background

2.1 Hardware Security

Complex System on Chip (SoC) rely on embedded crypto-cores for security critical applications. However, just the inclusion of a crypto-core into a SoC does not guarantee security. Several threats and policies must be tested before declaring a device secure. One such threat, which we address here is SC Attacks (SCA [8, 4, 5]). SCA exploits unintentional leakage from the physical implementation of secure devices in form of power consumption, ElectroMagnetic (EM) emanation or timing.

The theory and application of SCA has been widely dealt in literature. On the other hand there is no clear indication on the standard measurement setup for SCA analysis. The most common method for power measurements is low-ohm method where a small low-noise resistor is inserted between the GND pin of the chip and the actual GND. This method is also called low-side measurement [8]. The alternate method called high-side measurement inserts a resistor between V_{cc} and the V_{cc} pin of the chip. Both these methods are low-cost and easy to implement but come with some demerits. The low-side measurement suffers from low signal strength while high-side measurement contains higher noise from the power supply. Thus the measurements from this method suffer from low signal-to-noise ratio (SNR). Also the inserted resistor (with some circuit inductance) acts as a low-pass filter, thus filtering signal in the higher frequencies. We will show later that even higher frequencies can contain useful and exploitable information.

EM probes are also often used for precise and high quality SCA measurements [11]. Measurements using EM probes can be localized and low-noise. The bandwidth of EM measurements are often higher than low-resistor measurements and its limited only by the bandwidth of the probe. A major issue with EM measurements is the placement of the antenna. The leakage points changes from one design to another, which prevents from standardizing the measurement setup.

2.2 Trust

Globalization and cost motivation of the semiconductor industry has resulted in a recent problem of insertion of trojans in an IC [12]. A trojan can be introduced at any design step right from the Register Transfer Level (RTL) source code to lithographic masks fabrication. Along with several methods for trojan detection [3], side-channel analysis is also a potential method for trojan detection. Authors in [1] use principal component analysis (PCA) of SCA measurements to create the fingerprint of the activity. Few works observes leakage current [9]or dynamic current [10] or uses “sustained vector technique” [3] to detect trojans.

The main problem with the SC based trojan detection is the number of noise sources in SC measurements. As the equipment for SC measurements is not standardized, it is hard to distinguish activity of trojans in SC from other noise sources. This noise can come from various sources like measurement equipment, measurement environment, placement of EM probe, process variation (for newer technologies) etc. Therefore it is hard to blame any unusual activity on trojans only which introduces the notion of false positives and negatives. In other words, several trusted chips can be falsely rejected and vice-versa depending on the performance specifications. Due to aforementioned reasons, it is hard to integrate the trojan detection into standard test flow.

3 On-Chip Power Noise Measurement

The basic idea of an OCM system is depicted in Fig. 1. An embedded sampler of Fig. 1 enables on-chip waveform monitoring and works for the testing of hardware security. The circuit senses and samples the analog voltage of interest at the timing of sampling, and then buffers the sampled DC voltage to an output pin. The usage of high-voltage $(3.3V)$ I/O MOS transistors allows low-resistivity as well as low-leakage properties of sampling switch and capacitor. While the power supply voltage (V_{dd}) of cryptographic modules at $1.8V$ is directly sampled and buffered by a unity-gain amplifier (UGA Fig. 1(a)), the ground voltage (V_{ss}) or substrate voltage (V_{sub}) at $0.0V$ is level-shifted by a p-type source follower to match the input voltage range of a sampling head (Fig. 1(b)).

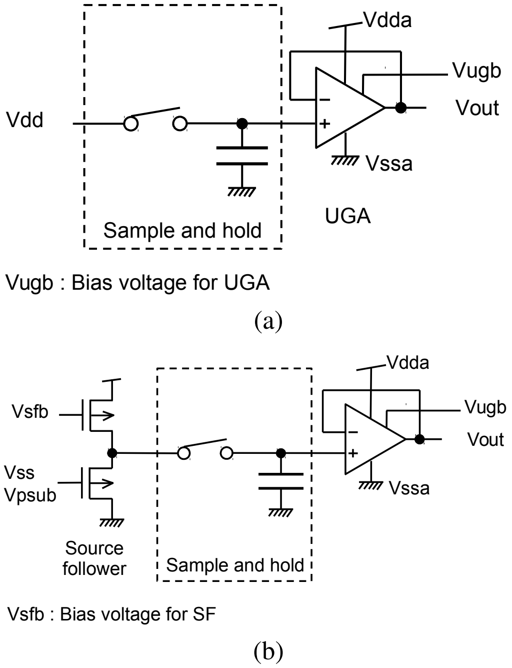


Figure 1: Basic structure of a OCM system with front-end probing for (a) V_{dd}, (b) V_{ss} and V_{psub}

This OCM is designed with a vision of integration into the testing flow. The proposed OCM realizes the best use of the digitization functionality of Automatic Test Equipment (ATE) while minimizes the cost of integration. The functions of high precision sample-timing generation and wide-voltage analog-to-digital conversion, that highly consumes power supply current and silicon areas as well, are covered by the ATE. Power noise waveforms sensitively respond to the variation of internal logic activities reflecting private information, or potentially including trojan (or malicious) logic operation. The changes in wave shapes can be quite small. However, they are finely captured by the embedded sampler and precisely digitized by the off-chip ATE with high measurement stability and reproducibility. This is of prime importance in the testing of ICs for hardware security and trust.

In contrast, an on-chip digitization of power and substrate noise waveforms was proposed in [2], where an embedded digitizer used a latched comparator in the back for quantizing the output voltage of a source follower. The sample timings and reference voltages are also on-chip generated. The on-chip digitization is essentially needed for the in-place diagnosis of power supply integrity and noise coupling, since the frequency-domain response of power delivery networks is only characterized after packaging and assembly with a printed circuit board.

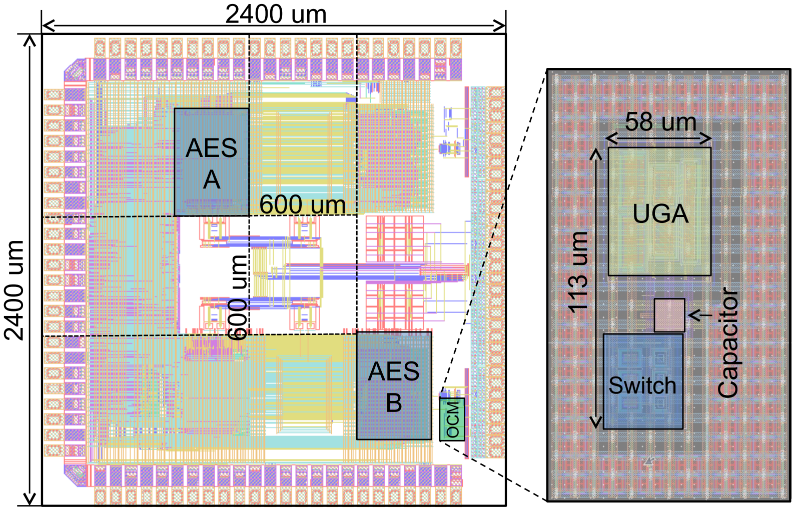
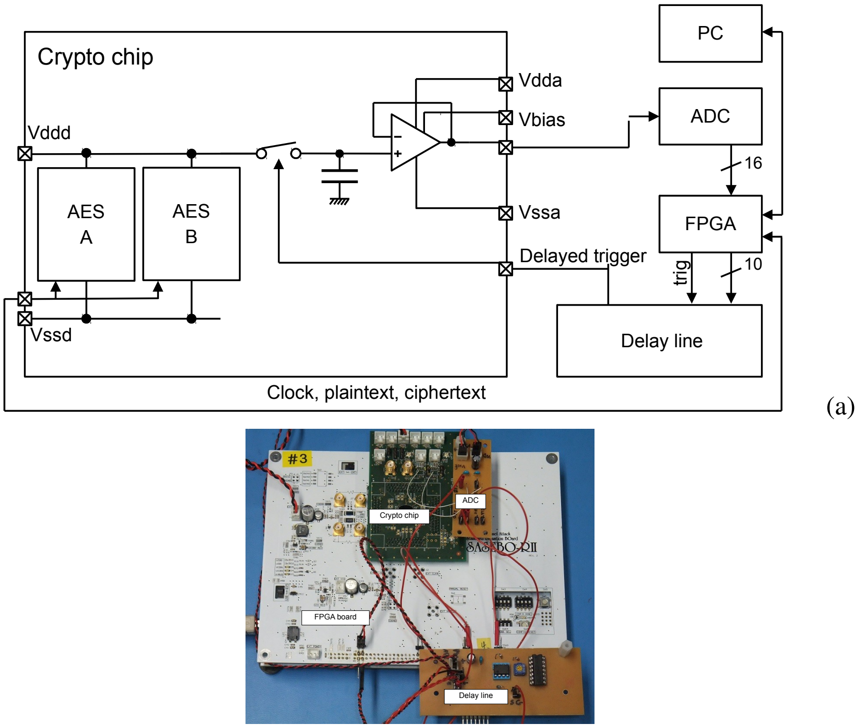


Figure 2: Internal structure of the test chip

3.1 Prototype Test System

For practical validation, we designed a test chip, using $0.18um$ CMOS technology, with the embedded sampler and cryptographic modules as shown in Fig. 2. We chose Advanced Encryption Standard (AES) for the demonstration of on-chip power noise evaluation. The AES core is a very basic hardware implementation which computes one round per clock cycle and the sbox is computed in glue logic using composite field. There are no physical countermeasures present in the AES to permit fair evaluations. The sampler has input channels to probe the V_{dd} node of AES modules at two different locations in a die, sharing a single power delivery network. The channel is selectively activated for monitoring. The power domain of the sampler at $3.3V$ is separated from the domain of cryptographic modules at $1.8V$. This isolates power and ground nodes of samplers from those of the target of interest, for stabilizing the measurements by eliminating the undesired power noise coupling.

The prototype test system is built as in Fig. 3. The sample timing given to the sampler is generated by an on-board delay line device (DL) with a synchronous and controlled delay to the system clock (CLK) of AES cores. The buffered output DC voltage from the sampler converted into a digital code by an on-board analog-to-digital converter (ADC). A field programmable gate array (FPGA) device is programmed to control the DL and ADC devices for waveform capturing and also to transfer the digital codes to an external personal computer (PC) for further data processing. The FPGA also handles the data to/from the AES cores.



(a)

(b)

Figure 3: Block diagram of the prototype system

4 OCM and Hardware Security

In this section, we analyze the measurements performed by OCM from a hardware security view point. The main objective is to check the vulnerability of the tested block against SCA. We compare the measurements from OCM with that of 1-ohm resistor and EM probe. We first perform "Leakage Analysis" ***i.e.*** the amount of exploitable information present in the measurements when in time-domain. We precisely compute the SNR of the measurement with respect to the input of the AES core. SNR is computed as:

$$SNR = \frac{\mathsf{Var}\left[\mathbb{E}\left[T|X\right]\right]}{\mathbb{E}\left[\mathsf{Var}\left[T|X\right]\right]}, \tag{1}$$

where T denotes measured waveforms and X represent a chosen part of the corresponding plaintext (in this case 1 out of 16 bytes). A high SNR [7] indicates a possible leakage which may be exploited by an attacker. To attest the ease of attackability of the measurement, we use Correlation Power Analysis (CPA [4]). Let us denote a random variable L representing the side-channel leakage (*e.g.*, power consumed) while computing $Z = f(X.K)$. K is the n-bit secret key. A standard side-channel attack tries to find correct key $k^\star$ for which Z and L have maximum dependency. Since L is noisy, several measurements of Z are required to estimate L. For hardware implementation, the leakage L generally depends on the *Hamming distance (HD) model*. It expresses at first-order the power consumption of CMOS gates in electronic devices as the sum of total number of bit transitions. The leakage can be expressed as:

$$L = HD(Z, R) + N = HW(Z \oplus R) + N\,,$$

where N is the noise, and R is the reference state. $HW(X)$ is the *Hamming Weight function* which returns the number of bits set to 1 in binary representation of X. CPA computes the *Pearson Correlation Coefficient* ρ between the SC measurements T and the predicted leakages L.

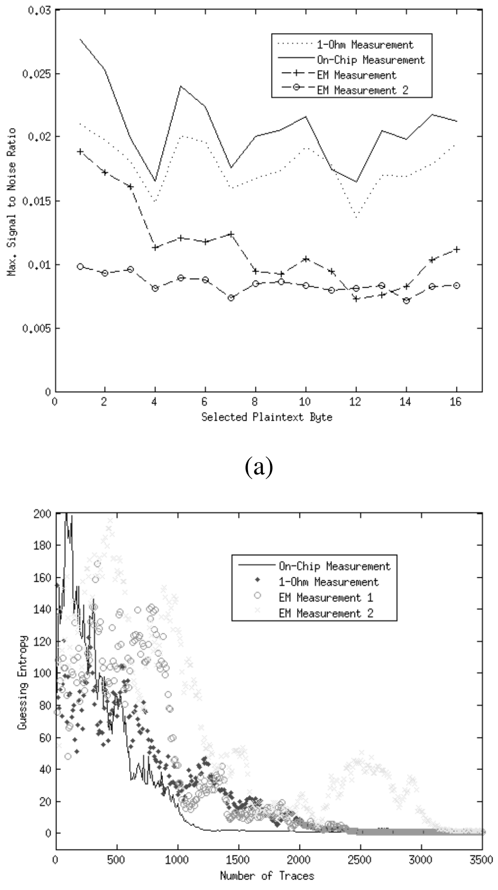
$$CPA = \rho\left[T; L\right]\ .$$

The second characteristic, called "High-Frequency Analysis", also uses CPA but to see the impact of measurement setup in the frequency domain. In this part, we show the range of frequencies where the captured measurement leaks information. The main motivation behind this analysis is to check if OCM based measurement captures high-frequency leakage, which is otherwise hard to capture.

4.1 Leakage Analysis

We acquired $50,000$ traces for an AES module running at clock frequency of 24 MHz. The mesurements were taken from the OCM, 1-ohm measurement (low-side) and two EM measurements from different locations. For each measurement set, we computed the SNR as defined in Eq. (1). In AES, the algorithm is designed in a way such that the data is handled as bytes. Since the input vector of AES is 128 bits or 16 bytes, we compute 16 SNR curves, one for each input byte. Fig. 4(a) shows the maximum SNR for the 16 input bytes for the four sets of measurements. We can clearly see that for all 16 bytes the OCM provides a higher SNR than other methods.

Next we mount an attack on first byte of the secret key associated with the AES. We compute the average rank of the correct key or its guessing entropy, on the output of 5 attacks for each measurement set. In this case, the faster the rank converges to 1, the higher is the attackability, which also means that the measurements carry more information. For the same AES core, we attacked measurements from different sources



(a)

(b)

Figure 4: Comparison of (a) maximum SNR obtained, (b) guessing entropy from different measurements

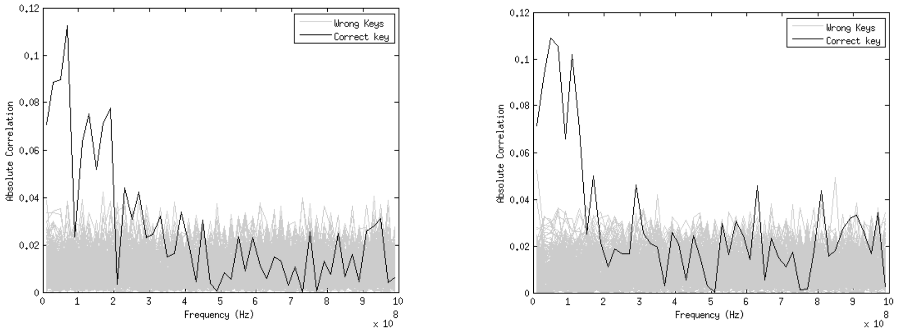
and plotted the average rank of the correct key in Fig. 4(b). It can be observed that OCM-based traces are easier to attack as they reveal the key in about 1200 measurements only. 1-ohm, and EM 1 need around 2000 measurements while EM 2 need 3100 measurements. Thus, from the three experiments we can conclude that OCM provides the best SNR or captures maximum information out of all the measurement techniques. Therefore it can be considered as the best-case measurement which can be obtained.

4.2 High-Frequency Analysis

Another interesting parameter for SCA is the range of frequencies where leakage is present. In general, depending on the measurement setup some information is not captured or lost. For instance, in the 1-ohm method, the 1-ohm resistance along with the circuit capacitance acts as a low-pass filter, which filters out high-frequency component of leakage. Similarly, for the EM measurements, the range of frequencies captured will directly depend on the bandwidth of the used EM probe. Fig. 5 shows the result of CPA on a key byte of AES using the FFT of previously captured measurements. This CPA is slightly different from last experiment and computed as:

$$CPA = \rho \left[abs(FFT(T)); L \right] .$$

Unlike 1-ohm based measurements, OCM show good leakage at lower and higher frequencies. At higher frequencies, 1-ohm method might be noisy which motivates the need of OCM in high-performance chips. Moreover we can observe some leakage around 300 MHz, 620 MHz, 800 Mhz and 1 GHz i.e. the leakage from all the frequencies is captured. Thus OCM can also be promoted for SC measurements from high-performance chips which operate at multiple GHz of clock. Please note that the leakage frequencies will depend on the device, but OCM is capable of capturing it across range of frequencies.



(a)

(b)

Figure 5: CPA in frequency domain on (a) 1-Ohm measurements, (b) OCM

5 Standard SC Measurement Setup using OCM

In Sec. 3, we argued that OCM has the potential application for SC measurement. The environment noise does not affect the measurements as the signal is measured on chip. On the other hand, the process variation stays constant for a given technology which can be pre-charaterized by the vendor. Therefore measurements using OCM are the *best-case* measurements. Moreover, we demonstrated that OCM provides the best

SNR as well as frequency components of the leakage in Sec. 4. With these features in mind, we can propose OCM as a candidate for standard SC measurement setup. OCM can be configured to measure various entities on chip. The most common target for OCM is the V_{dd} pin of the concerned IP. This method gives a good signal but cannot be standardized as the quality of signal will depend on the respective placement and routing of OCM and the target IP. The second method is measurement of substrate noise. It has been shown in [6] that by measuring the substrate noise one can easily monitor the activity of the target chip. Moreover, the substrate noise stays uniform almost all over the chip except for the areas very approximate to an operating circuits where the noise strengths are in steep attenuation with the distance. The substrate noise can be measured anywhere as the total of contributions by all circuits on a die. Therefore there is no specific restriction on respective placement and routing of OCM and the target IP. Thus an OCM measuring side-channel activity through substrate noise is an ideal candidate for standardized SC measurement setup.

A common and tedious task in evaluation labs is the search of best leakage point on or around the IC. This is not only a time-taking task but prevents labs from automating their evaluation tools. With the OCM integrated in security-critical ICs, evaluation labs will have a common interface and setup for SC leakage. Once the SC measurement is autoamted, the analysis part which involves statistical computations is not hard to automate. The proposed OCM is simple to design and its size is rather small *i.e.* $6400m^2$, which limits the area overhead of the integration of OCM. Further research in directions to reduce the size of OCM will continue to motivate the integration of OCM in security-critical ICs.

Note: A common argument against integration of OCM in security-critical ICs is its exploitation by attackers. Indeed, if the attacker has access to OCM, it can be exploited for attacks. To solve this problem, we propose integration of OCM with a kill-switch. The kill-switch allows the designer to deactivate the OCM premanently at will. It will firstly disconnect the OCM completely from the measurement point and then deactivate permenantly the S/H circuit to ensure no misuse of OCM is performed. For instance, if the OCM is needed during the testing and certification phase, the designer can deactivate the OCM after testing/certification and before shipping to the market. A detail review of the security policies for deactivated OCM remains out of the scope of this paper.

5.1 Potential application of OCM for TRUST

OCM can also find potential application in trojan detection on fabricated ICs using SC measurement. A common scenario is when an untrusted manufacturer modifies the mask of the chip before fabrication to add malicious activity [12]. Like any SC-based trojan detection technique, OCM based trojan detection needs a golden model. The appropriate way to obtain a golden model is still an open question and applies to all trojan detection techniques based on SC. However, the main drawback in SC-based trojan detection remains the presence of measurement noise due to environmental factors. The main problem with the SC based trojan detection is the number of noise sources in SC measurements. As the equipment for SC measurements is not standardized, it is hard to distinguish activity of trojans in SC from other noise sources. This noise can come from various sources like measurement equipment, measurement environment, placement of EM probe, process variation (for newer technologies) etc. Therefore it is hard to blame any unusual activity on trojans only, which introduces the notion of false positives and negatives. Using a standard SC measurement setup based on OCM, one can solve this problem.

Using measurements from OCM, we now propose a methodology for trojan detection. The main principle is to compare measured SC traces with a golden reference. The methodology unrolls in three steps:

1. **Calibration:** The first step involves verification of the OCM i.e. check if the OCM is not compromised by a trojan. Since OCM is composed of analog components, the output response to a known input signal can be characterized properly. If the OCM for a chip under test outputs an expected response, the detection moves to the second step else the chip is marked faulted or untrusted.

2. **Measurements:** This step involves measurement of precise SC waveforms using the OCM for known inputs.

3. **Detection:** The third and the final step compares measured waveforms with golden reference to detect trojans in chip under test.

In some cases, complex SC metrics like Difference of Means (DoM) and Principle Component Analysis (PCA) can be used to compare waveforms. The best metric in this case is still an open topic of research, along with methods to obtain the golden reference. This technique only addresses a small class of trojans which can be observed in SC. To detect other trojans like bug-based trojans, this detection technique must be coupled with other techniques based on logic analysis etc.

Our designed prototype did not had any trojan inserted, which prevents us from providing practical results. Nevertheless our methodology can find useful application in testing for TRUST. Future extention of this work can look into practical application of OCM into trojan detection.

5.2 Estimation of Minimum Size of Detectable Trojan

In this part, we aim to determine the minimum size of trojan that is detectable by the proposed OCM. As previously proposed, the trojan is detected by comparing power consumption measured against a reference. This means the detection efficiency will depend on the reliability or accuracy of OCM measurement. To detect a trojan, the trojan should consume greater than the measurement error of the OCM. The measurement error can come from several factors like voltage variation, process variation etc. In the following, we do not consider process variation, which is out of scope of this paper.

We estimate the measurement error of our chip by measuring the power consumption of the same operation when repeated 10.000 times. The AES core has a gate count of $43,877$, which suffers a voltage drop of $31mV$ over a period (one round) of $23ns$ i.e. $43877/23$ or 1908 $gates/ns$. We estimated the maximum measurement error in voltage drop of the OCM, based on our simulations. This error turned out to be $1.2mV$ (at 6σ) at DC level or $12mV$ for the AES core. Thus we can detect a trojan of $(1908 * 1.2)/31.7$ i.e. 72 gates/ns at DC level or as small as 0.16% of the original circuit. Similarly, we can detect a trojan of 722 gates/ns (1.6%) at AES operation which has a measurement error of $12mV$ in the voltage drop. Further reduction of measurement error by application of advanced analog design techniques is an open question.

6 Methodology for Testing of Hardware Security and Trust using ATE

6.1 Test Environment

The OCM can be configured for the testing of IC chips for hardware security and trust, as depicted in Fig. 6. The sampler with multiple input channels is integrated into automated test environment (ATE) with mixed signal extensions, where an entire body of IC functionality including cryptography is to be fully tested. An IC chip (device) under test (DUT) passes a Go/NoGo or a PASS/FAIL gauge as long as the output data stream by the DUT in response to an input test vector matches the pre-registered data as the value of expectation. A cryptographic module is inspected with the identical set of input test vectors for a large number of IC chips in the ATE, as a part of manufacturing. A well selected set of test vectors thoroughly cover a wide range of operation scenarios of an IC chip and to potentially activate suspicious trojan hardware. The choice of set vectors totally depends on the target. This mostly covers the trojans inserted by an untrusted chip manufacturer in some of the wafers by changing the lithographic mask.

The test vector also configures the OCM function, where the single channel of interest is selectively connected to the sampler. A waveform acquisition window is placed in the test vector to capture time-domain voltage variation during the operation of a cryptographic module. The sampler strobes the voltage of the selected channel at the sample timing issued by the ATE, and outputs the voltage to the digitizer for subsequent analog-to-digital conversion. The sample timing includes a stepped delay relative to the system clock, and the delay is also controlled by the ATE. The entire test vector is iterated while the delay is stepped with a fixed amount of time. The iteration continues until the delay covers the whole of a waveform acquisition window.

The acquisition of waveforms is performed in parallel to the inspection of full functionalities of an IC chip. The waveforms associated with a given set of test vectors are then further processed to evaluate the level of side-channel leakage and the deviation of waveforms from the reference.

6.2 Test Flow

The flow of an IC testing incorporates on-chip waveform capturing for power noise evaluation, as given in Fig. 7. The sampler is first calibrated in its voltage gain when a DUT becomes ready for testing in the ATE. n test vectors are then loaded in the ATE for inspecting full functionality of the DUT. The waveform acquisition window of j samples is also specified for the i^{th} test vector and registered in the control program of the ATE. j and i are chosen as a good time-accuracy trade-off. The Go/NoGo is

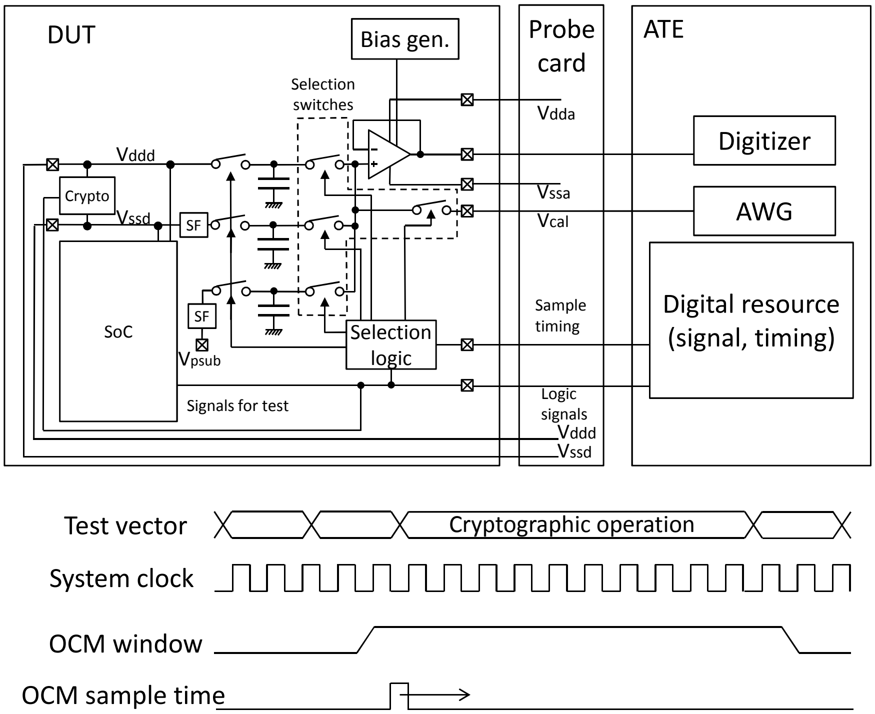


Figure 6: Block diagram of OCM integrated with ATE

then judged after the collection of response by the DUT including the waveform by the OCM.

The calibration of the sampler is performed by capturing a known sinusoidal waveform from an arbitrary waveform generator (AWG) of the ATE, while all the functions of an IC chip except for the sampling are halted. The amplitude and distortion of the sinusoid captured as such, the highest signal-to-noise ratio environment of a DUT are processed for two purposes. First, the ratio of amplitudes for the current DUT with the reference data is derived as a calibration coefficient. Second, the amplitude and distortion of the DUT are examined in the statistical distribution among the past DUTs including the golden samples. When they are in the position of outliers, the DUT is considered under suspicious attacks of the counterfeit, modification, or rebirth, to the OCM function.

The reference waveforms are statistically provided as an integrated database of captured waveforms among the past DUTs, regarding:

- sinusoids for calibration
- power noise for evaluation.

While the past DUTs should be genuine and treated as golden devices in the initial

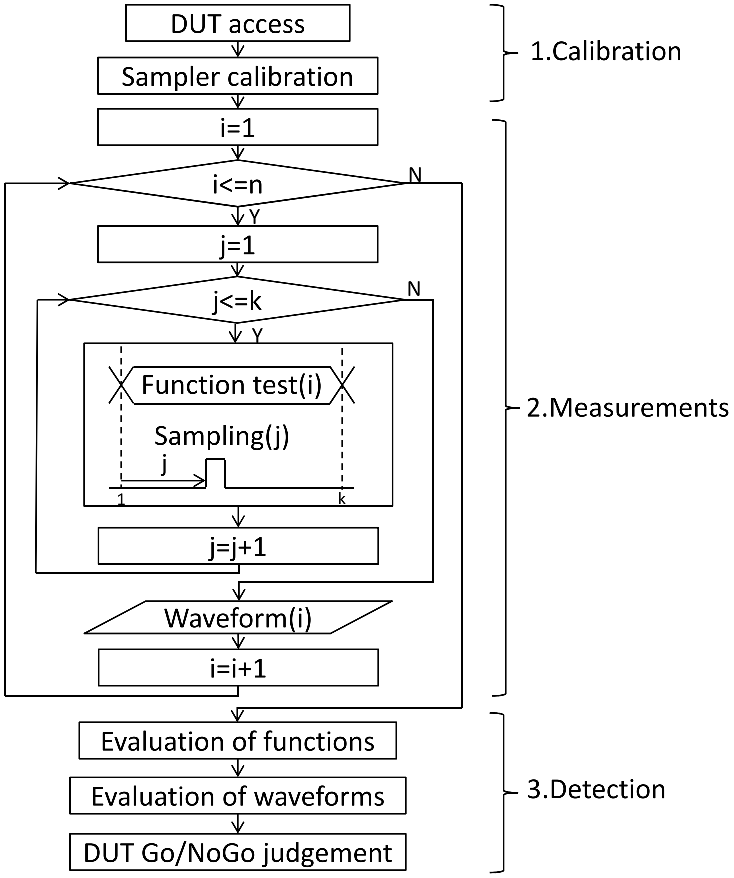


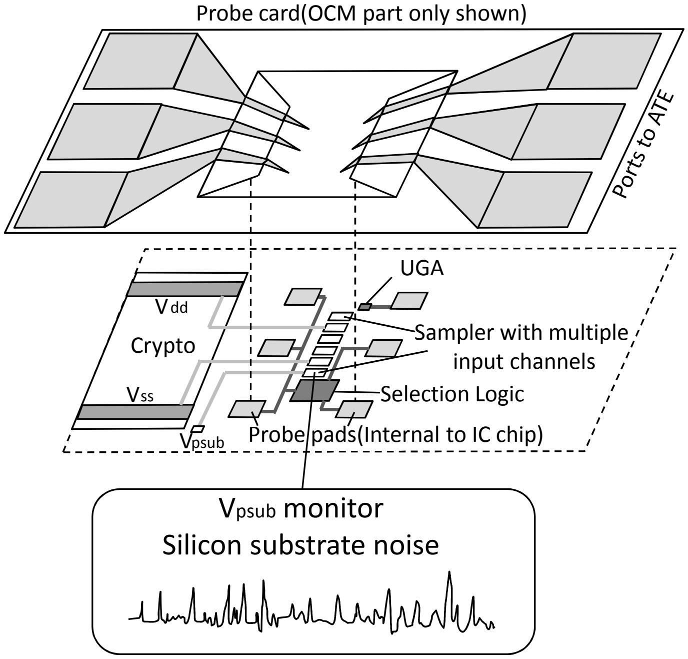
Figure 7: Test Flow

place, the data base is updated with as long as no false results in the testing is found. The average and variance of the waveforms are recorded in the database in association with each test vector and restored as the reference data for comparison in every testing.

The process and device parameter variations primarily impacts on the static offset or DC variations of power supply current as well as voltage. On the other hand, the dynamic or AC components of power noise are highly sensitive to the change in in internal logic activities rather than the parameter variations. The sinusoidal calibration of OCM thus suppresses the uncertainty of dynamic power noise measurements and ensures the waveform based evaluation in the testing of security.

6.3 Test Cost

The cost of incorporating OCM function needs to be minimized in the test strategy of an IC chip, although it is the only way providing the best SNR for hardware security and trust. The silicon area of the sampler is roughly estimated to be $6400um^2$ from the prototype layout of Fig. 2 with the extension of multiple input channels. This size is as negligibly small as a single metal access pad due to the simplified construction of the sampler. However, the cost inflates when an IC chip actually integrates the sampler for embodying OCM functionality.



Probe card(OCM part only shown)
Ports to ATE
UGA
V dd
Crypto
Sampler with multiple input channels
Selection Logic
Vss
Vpsub
Probe pads(Internal to IC chip)
Vpsub monitor
Silicon substrate noise

Figure 8: Layout image of OCM with ATE

We propose two essential techniques of Fig. 8 to minimize the cost of incorporation. Firstly instead of metal access pads, a probe card (see Fig. 8) can be used for accessing the sampler and associated registers for configuration through internal pads. This eliminates the consumption of I/O pins of an IC chip, while limiting the usage of the sampler to testing purposes. Second, the probing points are restricted to substrate taps near the sampler and also to power I/O pads often in the periphery of an IC chip. It is known that the substrate noise waveforms carry secret information at the almost equivalent level of leakage to power noise ones [6]. This eliminates the need of probe wiring into the internal nodes of cryptographic modules, and more importantly, decouples the incorporation of OCM functionality from system-on-chip integration including cryptography. Both techniques also alleviate the design of chips.

Another metric is the run-time cost of OCM functionality. The DUT iterates its operation with a test vector, while the sampler captures a single waveform by successive sampling with stepped delays covering a waveform acquisition window. When we choose the time step of $0.1ns$, a hundred iterations take place for a waveform acquisition of a single clock cycle of $10ns$ in the operation at 100 MHz. This cost of time consumption is essential to the waveform acquisition, while making 10-GHz range high-speed analog-to-digital conversion unused.

7 Conclusions

In this paper, we make an attempt to bring IC testing and hardware security on the same page. First, we motivate the use of on-chip power noise measurement or OCM module in side-channel measurement. As shown by our experiments, OCM provides side-channel measurements with best possible SNR and leakage at high-frequencies. Then we propose a standard side-channel measurement setup owing to the the possibility of measurement at substrate-level. Next we integrate the evaluation of hardware security and trust with the standard test flow, using ATE, all thanks to OCM measurement at substrate. Extention to practical trojan detection and analysis of impact of process variation will be covered in further research.

This paper makes an initial attempt to include hardware security and trust into performance parameters for testing. Further attention from the test community can really help evolve this domain.

Acknowledgments

This work was strongly supported by the project **SPACES** (Security evaluation of Physically Attacked Cryptoprocessors in Embedded Systems).

References

[1] Dakshi Agrawal, Selcuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi, and Berk Sunar. Trojan Detection using IC Fingerprinting. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, SP '07, pages 296–310, Washington, DC, USA, 2007. IEEE Computer Society.

[2] N. Azuma, T. Makita, S. Ueyama, M. Nagata, S. Takahashi, M. Murakami, K. Hori, S. Tanaka, and M. Yamaguchi. In-system diagnosis of rf ics for tolerance against on-chip in-band interferers. In *Test Conference (ITC), 2013 IEEE International*, pages 1–9, Sept 2013.

[3] Mainak Banga and Michael S. Hsiao. A Novel Sustained Vector Technique for the Detection of Hardware Trojans. In *Proceedings of the 2009 22nd International Conference on VLSI Design*, VLSID '09, pages 327–332, Washington, DC, USA, 2009. IEEE Computer Society.

[4] Éric Brier, Christophe Clavier, and Francis Olivier. Correlation Power Analysis with a Leakage Model. In *CHES*, volume 3156 of *LNCS*, pages 16–29. Springer, August 11–13 2004. Cambridge, MA, USA.

[5] Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi. Template Attacks. In *CHES*, volume 2523 of *LNCS*, pages 13–28. Springer, August 2002. San Francisco Bay (Redwood City), USA.

[6] Daisuke Fujimoto, Daichi Tanaka, Noriyuki Miura, Makoto Nagata, Yu-Ichi Hayashi, Naofumi Homma, Shivam Bhasin, and Jean-Luc Danger. Side-Channel Leakage on Silicon Substrate of CMOS Cryptographic Chip. In *HOST*, IEEE Computer Society, May 2014. Arlington, USA.

[7] Suvadeep Hajra and Debdeep Mukhopadhyay. SNR to Success Rate: Reaching the Limit of Non-Profiling DPA. Cryptology ePrint Archive, Report 2013/865, 2013. `http://eprint.iacr.org/2013/865/`.

[8] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In *Proceedings of CRYPTO'99*, volume 1666 of *LNCS*, pages 388–397. Springer-Verlag, 1999.

[9] Reza Rad, Jim Plusquellic, and Mohammad Tehranipoor. Sensitivity analysis to hardware Trojans using power supply transient signals. In *Proceedings of the 2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, HST '08, pages 3–7, Washington, DC, USA, 2008. IEEE Computer Society.

[10] Hassan Salmani and Mohammad Tehranipoor. Layout-aware switching activity localization to enhance hardware trojan detection. *IEEE Transactions on Information Forensics and Security*, 7(1):76–87, 2012.

[11] Laurent Sauvage, Olivier Meynard, Sylvain Guilley, and Jean-Luc Danger. ElectroMagnetic Attacks Case Studies on Non-Protected and Protected Cryptographic Hardware Accelerators. In *IEEE EMC, Special session #4 on Modeling/Simulation Validation and use of FSV*, July 25-30 2010. Fort Lauderdale, Florida, USA (`http://emc2010.org/`).

[12] U.S. Department Of Defense. Defense science board task force on high performance microchip supply. `http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf`.