# Power Supply Noise Aware Evaluation Framework for Side Channel Attacks and Countermeasures

[ Invited Special Session Paper ]

Jianlei Yang Chenguang Wang Yici Cai Qiang Zhou
Tsinghua National Laboratory for Information Science and Technology
Department of Computer Science and Technology
Tsinghua University, 100084, Beijing, China
jerryyangs@gmail.com chenguang91@foxmail.com
caiyc@mail.tsinghua.edu.cn zhouqiang@tsinghua.edu.cn

***Abstract*—Side Channel Attack (SCA) aims to extract the secret information from cryptography chips by analyzing the leakage of physical parameters. Power analysis based SCA is a popular approach to obtain secret keys by monitoring the power consumption of cryptography chips. However, most SCA evaluation methods are performed on FPGA platforms while many parasitic physical effects cannot be revealed before the cryptography chips are taped out. Roughly ignoring these effects will significantly increase the attack difficulties due to the corresponding measurement noise. Power supply noise has been observed to be critical for power analysis based SCA. This paper demonstrates a power supply noise aware evaluation framework for practical side channel attack from cryptography system design to physical design. On-chip power delivery network is implemented among physical design stage. Consequently the supply noise of power network can be explored according to the post-layout implementation. Additionally, the countermeasures of cryptography chips could be enhanced by on-chip decapacitors placement due to its influences on the characteristics of power delivery network.**

***Keywords*—Power Supply Noise, Side Channel Attack, Countermeasures, Differential Power Analysis.**

## I. Introduction

In traditional cryptanalysis, a cipher is viewed as a black box operation that transforms the plaintext into the ciphertext through a secret key [1]. Many ciphers usually have no practical known weaknesses since the mathematical strength renders many modern ciphers rather invulnerable, and the only way to unlock the secret key is to evaluate all possible combinations. However, as long as the number of combinations is large enough that brute force search approaches are usually infeasible in terms of computing complexity [2]. In reality, however, the ciphers have to be physically implemented on specified devices, such as ATM, RFID tags, smart cards, smart mobiles and sensor nodes. If an attacker has physical access to the targeted device, any sensitive information which is otherwise hidden, can become available to the attacker. As many of these devices are easily available to the attackers, there also arises the need for introducing countermeasures in both hardware and software to prevent the information leakage.

This work was supported by the National Natural Science Foundation of China (NSFC) under Grant No.61274031.

Side-channel attack [3] aims to extract the secret information such as encryption key through the information that can be retrieved from the physical implementation of the cryptosystem in various forms such as power consumption profile, timing delay and electromagnetic radiation. Among them, power analysis attack has emerged as one of the most significant attacks and has been widely studied, such as Simple Power Analysis and Differential Power Analysis [4]. Power analysis attacks exploit the dependence between the measured instantaneous power consumption of a cryptographic device and the data/operation being processed/performed. Furthermore, this power profile is statistically correlated to power estimates using power models like Hamming Weight or Hamming Distance, and the confidential key being used for encryption/decryption can be retrieved by performing efficient correlation or stochastic involved techniques [5].

Power analysis attacks are performed by monitoring the currents flown through the power supply pads of cryptographic chips and usually some measurement noises are easily introduced into such power profile [6]. The measurement noise increases the difficulty of successfully mounting an SCA attack while usually a number of measurements are required to disclose the secret key. Consequently, SCA attacks largely depends on the Signal-to-Noise (SNR) ratio of the side channel information. The SNR is observed to be determined by the cryptographic algorithms and circuit implementations. From the viewpoint of countermeasures against power analysis attacks, many kinds of noise injection or masking techniques are introduced to hide the sensitive information by breaking the dependency between power consumption of devices and the intermediate values of the cryptographic algorithms [7].

Previous investigations are mostly focused on algorithmic or circuit level implementation, both on power analysis attacks and countermeasures [8]. Even though there exist many kinds of complicated masking and noise injection techniques, some advanced techniques are newly developed and observed to be able to reveal the hidden information, such as template attack [9] and stochastic model attack [10]. These approaches no longer try to reduce noise but exploit multivariate-Gaussian noise model to extract information present in a single sample, which could be regarded as a manner of machine learning. One remarkable accomplishment recently is an attacker named Segrids [11] by Frank Schuhmacher on DPA Contest v4

978-1-4799-6245-7/14/$31.00 ©2014 IEEE

[12]. For the AES-256 RSM implementation, Segrids could determine the correct key from one power trace within 5 milliseconds. It indicates that such Rotating Sbox Masking (RSM) scheme is somewhat vulnerable for attackers since the hidden leakages could be still detected by much more efficient machine learning involved techniques [13].

Simply exploiting masking schemes is observed to be not able to resolve the potential threats from advanced side channel attacks which are bringing more and more severe challengeable security problems. The possible reason is that even though the used masking strategies could hide partial information from cryptographic algorithms, but its underlying relationship or dependency still could be properly captured through deep mining on the measured physical parameters [14]. The most perfect solution of hiding leakage is to smooth the fluctuations of measured power profile so that the sensitive information could be removed as much as possible, that is, the power trace is pruned as a shape of constant profile with as little ripple as possible [15]. One promising strategy is to re-examine the physical effects on cryptographic chips implementation from the post-layout design [16]. Crypto chips are generally implemented as ASICs for practical use, but usually evaluated on FPGA platforms [17][18][19][20][21] which makes their physical characteristics could not be taken into consideration before ASICs are taped out.

Power delivery network of crypto chips has been observed to be playing a significant role in effecting the SNR of the measured supply current by causing nonlinear voltage drops on circuit cells [22][23]. Such an unideal phenomenon could intrinsically limit propagation of useful information to supply current. The role of PDN characterization in SCA has been studied in [24] for precise security analysis and design of secure crypto chips. However, the secure design methodology has been only evaluated on FPGA platforms. And consequently, the detailed characteristics of PDN is usually under typical assumptions to model the power supply noise because the physical parameters cannot be figured out by the FPGA users. Roughly assuming the PDN structures and characteristics might lead to inaccurate modeling on power supply noise and then mismatch the secure crypto chip designs. Hence, there is a strong necessary to model the realistic PDN and evaluate its accurate supply noise on circuit cells which is critical to satisfy the requirements of anti-SCA crypto chips design especially for ASIC.

In this work, we propose a power supply noise aware evaluation framework for side channel attacks. It provides a designer with more realistic measure of PDN characteristics for SCA exploration among physical design stages. Additionally, it can be easily integrated into the right level of protection by performing on-chip decapacitors placement and optimization, which helps a designer to properly adjust the characteristics of PDN and accomplish balanced protection across power supply noise. The reminder of the paper is organized as follows. Section II provides background and motivational observations on the impact of PDN on SCA. Detailed evaluation framework and preliminary simulation results are demonstrated in Section III. We conclude and provide future directions in Section IV.

## II. Background and Motivation

This section introduces some preliminary knowledge on SCA and typical countermeasures techniques. Our motivation is briefly discussed based on the role of power delivery network in crypto chips.

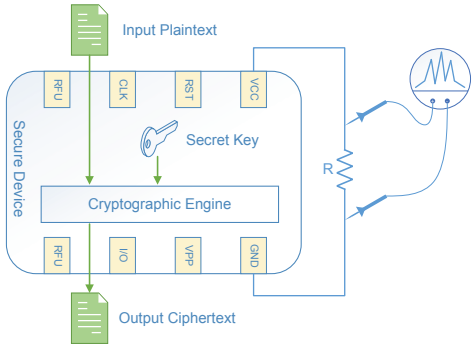



Fig. 1. Side channel attack by measuring power dissipation of a crypto device.

### A. Side Channel Attacks and Countermeasures

As shown in Fig. 1, a cryptographic device implements a cryptographic algorithm which takes plaintext and the key as inputs, and generates the ciphertext as encryption result. The internal secret key is not directly observable through the ports of the device. Power analysis attacks are introduced to reveal the key where a devices power consumption serves as the leaked information used to exploit the particular device. During the execution of a cryptographic algorithm on a particular device, information performing to the low-level instructions the algorithm is using may be revealed in the power traces that are retrieved. This in turn allows the attacker to identify the instructions being used, as well as branch statements to ultimately derive the cryptosystem and recover the key. A simple power model of a secure device could be defined according to the toggling profile of circuit logic [25] combined with the physical parameters of transistors, interconnect wires and circuit loads. In practice, the actual power component usually includes a noise component due to the unideal circuit implementation or measurement error.

The adversary observes the *Vcc* pin of the chip to measure the power profile, while feeding inputs to the chip to perform secure transactions, such as encryption or decryption. A general technique to measure the power consumption of a chip is to connect a resistor in series with the power or ground input. The voltage difference across the resistor divided by the resistance reveals the current, which is used to compute the power dissipation. Take a smart card as example, several visible segmented parts clearly placed outside the chip, as shown in Fig. 1. A resistor can be attached across *Vcc* and *Gnd* pin to measure the voltage drop and compute the power dissipation in *Vcc*. The adversary feeds in $CLK$ and inputs through $I/O$ pin to the chip for the execution of the encryption program stored inside. While the program is running for different inputs, the voltage across *Vcc* and *Gnd* is recorded for analysis.

For measuring the power consumption of a chip, it requires several devices to recode power samples, including a computer to control the measurement, a high-sample-rate oscilloscope to measure and store the samples, a current probe to attached

on the power supply pin, and several inputs are fed to the chip. A trigger signal is used to synchronize measurements, and an inductive probe to connected at chips power supply pads. The crypto chip is fed different inputs to execute the encryption program and the power samples are recorded for analysis. After the adversary has recorded the power values for different inputs, where a fixed secret key is used for encryption or decryption, the power profiles are analyzed with the known input values to predict the unknown secret key.

Recently numerous power analysis approaches have been proposed for efficient SCA attacks. The Simple Power Analysis (SPA) is a visual inspection using only one or very few power traces, and Differential Power Analysis is a statistical test which examines a large number of power consumption signals to retrieve secret keys. And then, the Correlation Power Analysis technique based on the correlation between the real power consumption of the device and a power consumption model has been widely studied. All DPA and CPA attacks are based on a power consumption model such as Hamming weight model, the Hamming distance model, or the most recent switching distance leakage mode [26]. However, these models do no always fit totally to the real power consumption of a device practically. Template attack [9] is initially proposed from the the idea of using a reference device which is identical or very close to the attacked one. It builds a database stocking power consumption information dedicated to a type of device [27]. The stochastic model attack proposed in [10] can be considered as a combination of the attacks based on power consumption models (e.g. DPA, CPA) and the template attack. Template attack and stochastic model attack usually first performs profiling to learn and determine the details of the device implementation and noise distribution, and the perform key extraction to detect the secret key.

Power analysis attacks could possibly detect the secret key because of the dependency between the power consumption of devices and the intermediate values of the cryptographic algorithms. Therefore, we can prevent from such power analysis attacks by breaking this dependency relationship, which is regarded as countermeasures. Countermeasures against power analysis are distinguished hardware and software countermeasures. Hardware countermeasures aims to randomize the power consumption of the device while the dependency between the power consumption and the intermediate values could be hidden. It can be done by adding a random noise or desynchronizing power consumption signals with a time jitter or a random operation interrupts [28][29]. Software countermeasures can be implemented at the algorithm level without changing the power consumption characteristics of the cryptographic device. They usually exploit the masking techniques to randomize the intermediate values [30][31].

### B. On-Chip Power Delivery Network

A lumped model of power consumption measurement is detailed demonstrated in Fig. 2. Resister $R$, which is connected between the true ground and *Vss* pin on chip, is used to monitor the power dissipation. When there is a voltage change in $V_g$, the transistor *PMOS* and *NMOS* conduct the current, which discharges the $C_{load}$ capacitance, causing the current to flow through the *Vss* pin. Consequently, useful information is leaked when the circuit is clocked, changing the state of $C_{load}$, which

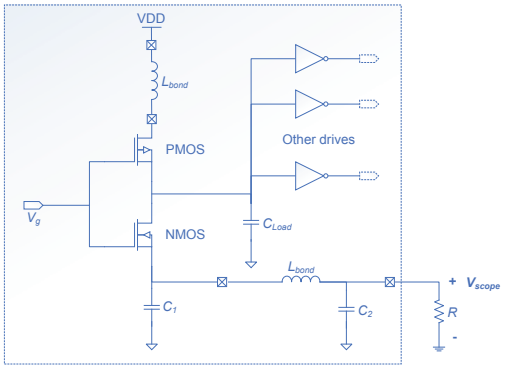



Fig. 2. Lumped modeling of power consumption measurement for crypto chip [32].

will result in drawing current from all related gates. This is a general property of logic circuits and the changes can be observed at $V_{scope}$. Two types of information leakage from the data bus that have been observed are Hamming weight leakage and transition count leakage. Hamming weight information leaks when the dominant source of current is caused by the discharging of $C_{load}$. A situation where Hamming weight information leaks is when a pre-charged bus design is used. In this case, the number of zeros driven onto the pre-charged bus directly determines the amount of current that is being discharged. Transition count information leaks when the dominant source of current is due to the switching of the gates that are driven by the data bus. When the data bus changes state, many of the gates driven by the bus will briefly conduct current. Thus, the more bits that change state, the more power that is dissipated.

However, the exploited *Vdd* pin and *Vss* pin in Fig. 2 are usually unideal due to the PDN impedance existed. Especially for the measurement scope attached onto *Vss* pin, the resulted ground bounce will introduce significant noise which will largely complicates the following power analysis attacks. Not only the inductance effects from power supply pads shown in Fig. 2, but also the widely parasitic parameters across the whole power delivery network will dominate the impedance characteristics of such on-chip PDN. As shown in Fig. 3, the power probe is attached onto the power supply pins of crypto chip where the measurement will be introduced power supply noises due to the parasitic parameters of package and on-die power grid. On-chip PDN has been well studied recently for design, simulation and optimization [33]. With the trends of increasing power consumption and decreased power supply value, how to retain the switching speeds and satisfy the noise margin is becoming more and more challengeable. The resulted design margin of power supply noise will obviously degrade the measurement accuracy of power analysis attacks.

On-chip power delivery network has an important impact on the supply voltage obtained by working cells due to the parasitic effects of resistance, capacitance and inductance. The power grid impedance usually affects the total supply current absorbing by a chip. This changes the supply current profile when it passes through the PDN from inside the chip to the external pin for measurement. The effect causes distortion to the supply current waveforms. Such distortion can create

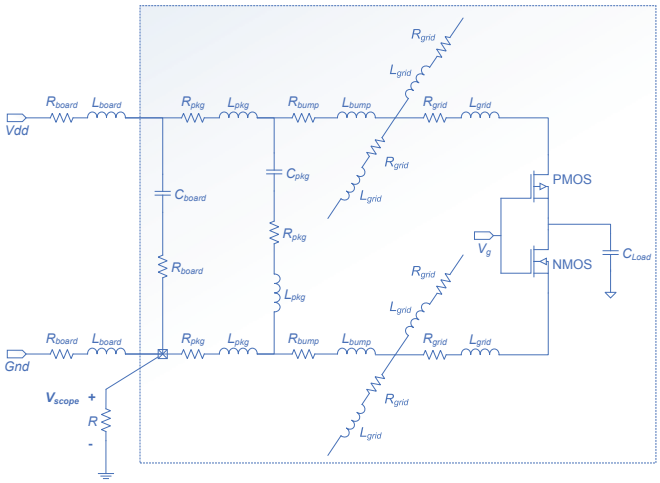



Fig. 3. SCA power measurement across power delivery network.

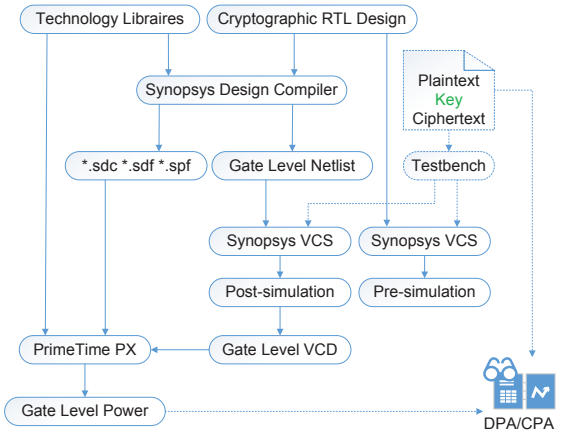



Fig. 4. General power analysis attack framework.

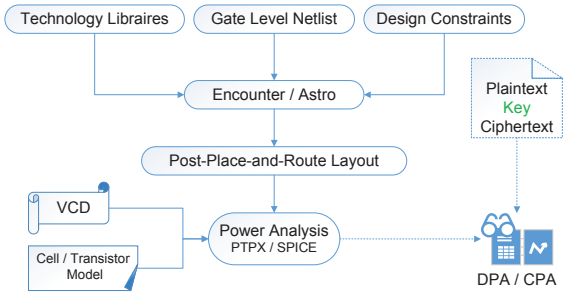



Fig. 5. DPA with physical implementation.

difficulty for SCA. For using CPA to crack the key on a cipher chip, the number of power traces required to extract the key is increasing in the presence of PDN. More importantly, due to the RLC properties of PDN, the masking effect differs with different impedance characteristics. Just like the circuit intrinsic noise can be viewed as a linear additive noise in SCA, PDN can be considered as a noise source which causes a non-linear distortion on power traces. It is necessary to consider the impacts of on-chip PDN when performing SCA and related countermeasures.

## III. Evaluation Framework

### A. The Proposed Evaluation Framework

Security applications usually include a range of possible architectural and electrical implementations, such as ASIC vs. FPGA, standard cell vs. full custom design. The choice of the platform has historically been dictated by performance, area, and power consumption, each of which can be measured accurately. Once the initial design point is fixed, designers consider a fine-grained space of possible solutions, and only at this point is security typically considered, often based mainly on empirical evaluation. The aim of this work is to bring security to the forefront of design stages for cryptosystems by associating it with co-simulation or co-analyasis. To achieve our goal, we propose a flexible and fully automated design flow based on standard CAD tools. The framework supports hierarchical design with considering power supply noise against side channel attacks.

Most previous evaluation techniques are based on FPGA platforms. The designers cannot take the physical parameters into consideration for evaluation the power supply noise on side channel attacks. From the viewpoint of software evaluation, a prior flow is shown in Fig. 4, some encryption or decryption operations are performed as testbench for evaluating the targeted RTL design of cryptographic algorithms. Since pre-simulation could be well performed, the RTL description are synthesized as gate level netlist according to specific technology library. And consequently the cell library information is accessible for designers. Then the post-simulation is available to be performed for evaluating the correctness of results of cryptographic algorithms. The caused circuit/logic transitions from cryptographic operations have a strong correlation with power consumption which could be measured by attackers. Several power analysis tools could calculate the cycle-to-cycle power consumption according to the gate level implementation, such as PrimeTime PX. Among such gate level simulation and power analysis, no physical structures have been taken into consideration including parasitic capacitances and resistance of circuit interconnects. Generally speaking, RTL and gate level evaluation is still a relative higher level compared with practical implementation.

Taking the evaluation into physical design level as shown in Fig 5, gate level netlist is synthesized using Encounter or Astro with several steps including floorplan, placement and routing according to specified technology libraries. Logic cells are properly placed and connected under the timing/power/area constraints. Post-place-and-route layout has more detailed geometric physical information, mainly including circuit cell implementation and wire interconnects. Consequently the power analysis can be performed with Pritime PX or SPICE by extracting the cell current characteristics, parasitic wire capacitance and resistance. Such power analysis on lower level implementations should be more accurate than higher level analysis since more detailed information is available and closer to practically implemented physical chips.

In practice, power delivery network can be also extracted for post-place-and-route layout simulation and analysis. However, the resulted power supply noise have to be specially

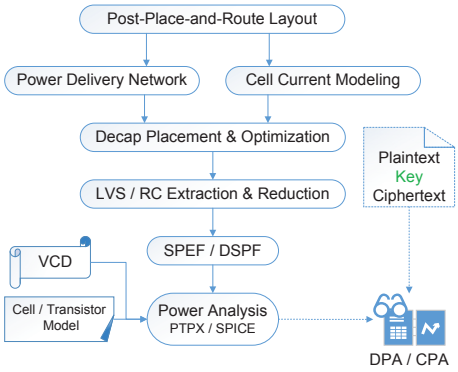



Fig. 6. DPA with considering PDN and decap optimization.

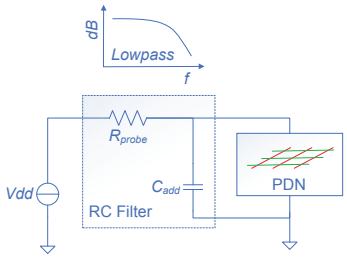



Fig. 7. Regarding decap placement and optimization as RC filter to smooth the total power consumption.

taken into consideration, that is, to perform power analysis under the impacts of power supply noise. As shown in Fig. 6, co-simulation and analysis with power supply noise requires that power grid simulation is first performed to obtain the IR-drop and then the supply voltage delivered to circuit cells could be figured out. The current behaviors of all circuit cells could be re-modeled under the supply voltage variations to fit the power supply noises. Especially decapacitance placement and optimization is a must to reduce the power supply noise, which usually largely changes the impedance characteristics of power delivery network. This is also exploited to improve the countermeasures, which will be detailed discussed in the next subsection. After the power delivery network with additional decap optimization has been fixed, following steps of LVS and RC extraction are conducted to provide the detailed parasitic parameters of post-layout (SPEF or DSPF file). Then Prime-Time PX is used to perform cycle-by-cycle power analysis according to the obtained circuit activity information (VCD file. If the circuit has been flatten as transistors connected, then transistors level SPICE simulation will be performed to calculate a more accurate power trace. At last, the input plaintext and output ciphertext will be adopted as a reference combined with the obtained power trace to perform differential power analysis or correlation power analysis with the attempts of determining each bit of the secret key.

### B. Countermeasures Enhancement

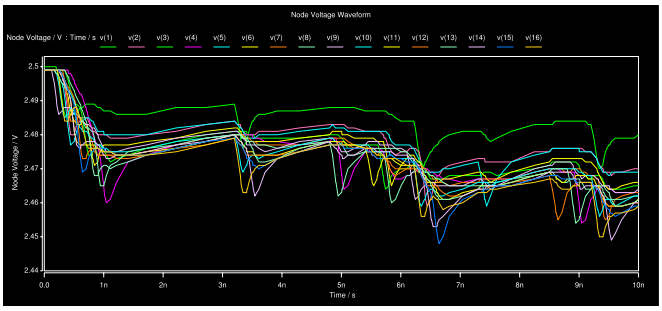
The decapacitors indeed could be placed on board outside the crypto chips to stabilize the power supply voltage. However, simply adding decapacitors on board level is not enough so that several optimization techniques for on-chip decapacitors have been widely studied, which are much more complicated than off-chip decapacitors problems. Additionally, off-chip parasitic parameters usually cannot disturb the power measurement by introducing voltage noises due to the measurement probe is typically attached onto package pins of chips. That is, only the parasitic parameters distributed among package level or on-chip level will significantly degrade the power measurement accuracy.

Without loss of generality, considering power delivery network as $RC$ circuit network is yet typical to demonstrate our ideas when inductive effect is not significant due to the technology nodes. As shown in Fig. 7, $R_{probe}$ is the SCA resistance to measure power consumption for power analysis attacks. Aiming to enhance the ability of anti-SCA attacks, we perform decapacitance placement and optimization both on meeting the design margin requirements of supply voltages and smoothing the ripple of measured voltage on $R_{probe}$. We abstract the additional decapacitance resulted by decapacitance placement and optimization as a lumped $C_{add}$ shown in Fig. 7. As we have known, the behavior of $R_{probe}$ with $C_{add}$ is shown to be a $RC$ filter with low pass property, which contributes to reduce the power supply noise by smooth the voltage ripples on high frequency.

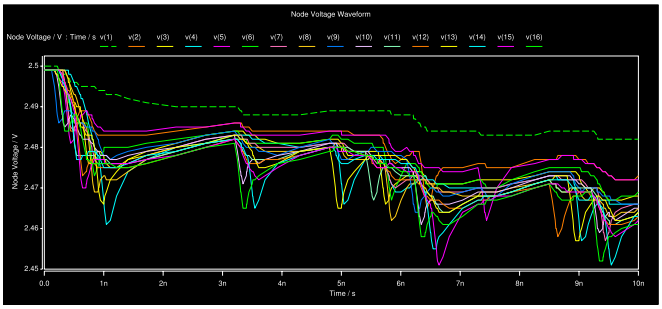
Experimental results for simulating a small power grid case are shown in Fig. 8, which evaluates the lumped abstraction decap $C_{add}$ attached nearby power supply pad. Fig. 8(a) shows the power grid with no additional decapacitor, that is, $C_{add}$ equals zero. The green dash line is the measured voltage of SCA resistance $R_{probe}$, which has certain overlap with other grid nodes. If a small decap $C_{add}$ is attached, the nodes voltage waveform is shown in Fig. 8(b), where the green dash line is easy to be distinguished with other curves. That is to say, the voltage fluctuation is partially removed due to the low pass property. If an even large decap $C_{add}$ is attached, the node voltage waveform is shown in Fig. 8(c) for a longer run period. The green bold line is the voltage on $R_{probe}$, where it is much more smooth than before. The measured IR-drop on SCA resistance $R_{probe}$ will be smoothed as a relative steady waveform, that is, a certain range of frequencies have been removed. It should be noticed that only a lumped decap is adopted in our experiments while the impedance characteristic of realistic power grid is much more complicated. By properly adopting the well-studied decap placement and optimization algorithms, the power supply noise could be effectively reduced especially for the IR-drop on $R_{probe}$.

## IV. Conclusion

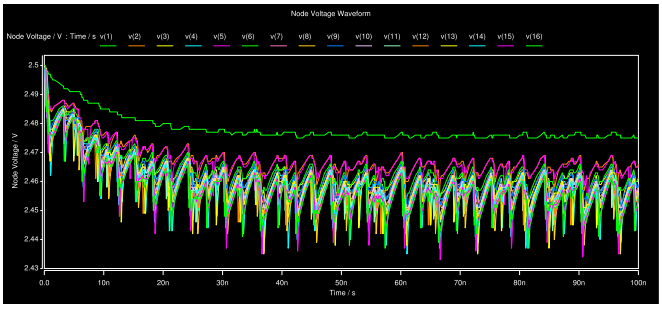
Previous power analysis attacks are usually evaluated on FPGA platforms. But the significant impact of power supply noise has never been well considered which will bring substantial measurement errors consequently more difficulties for successful attacks. In this paper, a power noise aware evaluation framework is proposed based on standard EDA tools. Post-place-and-route layout is implemented to explore more detailed physical parameters, mainly including the impedance characteristics of power delivery network. This software based evaluation framework provides a flexible and practical exploration approach for more efficient side channel attacks. Meanwhile, power delivery involved decapacitance placement and optimization is shown to be available for countermeasures




(a) Without additional decapacitor where $C_{add}$ equals zero.




(b) With additional decapacitor of small $C_{add}$.




(c) With additional decapacitor of large $C_{add}$ and longer run cycles.

Fig. 8. Voltage waveform of grid nodes. The measured IR-drop on $R_{probe}$ could be obtained from *Vdd* minus. An additional decap is attached nearby power supply pad.

enhancement, which ensures the anti-SCA attacks have another kind of novel approach to strengthen the security of cryptographic chips.

## REFERENCES


[1] B. Preneel, C. Paar, and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*. Springer, 2009.

[2] Cryptographic Key Length Recommendation, BlueKrypt, 2014. [Online]. Available: http://www.keylength.com

[3] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Advances in Cryptology, CRYPTO*. Springer, 1996, pp. 104–113.

[4] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology, CRYPTO*. Springer, 1999, pp. 388–397.

[5] T.-H. Le, C. Canovas, and J. Clédière, "An overview of side channel analysis attacks," in *Proceedings of ACM Symposium on Information, Computer and Communications Security*, 2008, pp. 33–43.

[6] K. Tiri, "Side-channel attack pitfalls," in *44th ACM/IEEE Design Automation Conference*, 2007, pp. 15–20.

[7] Z. Chen, A. Sinha, and P. Schaumont, "Using virtual secure circuit to protect embedded software from side-channel attacks," *IEEE Transactions on Computers*, vol. 62, no. 1, pp. 124–136, 2013.

[8] I. Verbauwhede, *Secure integrated circuits and systems*. Springer, 2010.

[9] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Cryptographic Hardware and Embedded Systems*. Springer, 2003, pp. 13–28.

[10] W. Schindler, K. Lemke, and C. Paar, "A stochastic model for differential side channel cryptanalysis," in *Cryptographic Hardware and Embedded Systems, CHES*. Springer, 2005, pp. 30–46.

[11] DPA Contest. [Online]. Available: http://www.dpacontest.org

[12] Segrids. [Online]. Available: http://www.segrids.com

[13] A. Moradi, S. Guilley, and A. Heuser, "Detecting hidden leakages," in *Applied Cryptography and Network Security*. Springer, 2014, pp. 324–342.

[14] L. Lerman, G. Bontempi, and O. Markowitch, "Side channel attack: an approach based on machine learning," *Center for Advanced Security Research Darmstadt*, pp. 29–41, 2011.

[15] H. Vahedi, S. Gregori, Y. Zhanrong, and R. Muresan, "Power-smart system-on-chip architecture for embedded cryptosystems," in *Third IEEE/ACM/IFIP CODES+ISSS'05*, 2005, pp. 184–189.

[16] F. K. Gürkaynak, "Post layout results are required," CHES, Tech. Rep., 2009.

[17] T. Katashita, A. Satoh, T. Sugawara, N. Homma, and T. Aoki, "Development of side-channel attack standard evaluation environment," in *IEEE European Conference on Circuit Theory and Design, ECCTD.*, 2009, pp. 403–408.

[18] T. Katashita, Y. Hori, H. Sakane, and A. Satoh, "Side-channel attack standard evaluation board SASEBO-W for smartcard testing," *Power*, vol. 3, p. 400, 2012.

[19] Side-Channel Attack Standard Evaluation Board (SASEBO), 2014. [Online]. Available: http://www.risec.aist.go.jp/project/sasebo

[20] C. O'Flynn and Z. D. Chen, "Chipwhisperer: An open-source platform for hardware embedded security research." *IACR Cryptology ePrint Archive*, p. 204, 2014.

[21] ChipWhisperer, open source hardware project, Assembla. [Online]. Available: https://www.assembla.com/spaces/chipwhisperer/wiki

[22] M. Saint-Laurent and M. Swaminathan, "Impact of power-supply noise on timing in high-frequency microprocessors," *IEEE Transactions on Advanced Packaging*, vol. 27, no. 1, pp. 135–144, 2004.

[23] E. Alon, "Measurement and regulation of on-chip power supply noise," Ph.D. dissertation, Stanford University, 2006.

[24] X. Wang, W. Vueh, D. B. Roy, S. Narasimhan, and Y. Zheng, "Role of power grid in side channel attack and power-grid-aware secure design," in *50th ACM/EDAC/IEEE DAC*, 2013, pp. 1–9.

[25] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[26] E. Peeters, F.-X. Standaert, and J.-J. Quisquater, "Power and electromagnetic analysis: Improved model, consequences and comparisons," *Integration, the VLSI journal*, vol. 40, no. 1, pp. 52–60, 2007.

[27] P. N. Fahn and P. K. Pearson, "IPA: A new class of power attacks," in *Cryptographic Hardware and Embedded Systems, CHES*. Springer, 1999, pp. 173–186.

[28] C. Clavier, J.-S. Coron, and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures," in *CHES*, 2000, pp. 252–263.

[29] S. Mangard, "Hardware countermeasures against DPA – a statistical analysis of their effectiveness," in *Topics in Cryptology, CT-RSA*. Springer, 2004, pp. 222–235.

[30] L. Goubin and J. Patarin, "DES and differential power analysis the duplication method," in *Cryptographic Hardware and Embedded Systems, CHES*. Springer, 1999, pp. 158–172.

[31] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in *Advances in Cryptology, CRYPTO*. Springer, 1999, pp. 398–412.

[32] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Investigations of power analysis attacks on smartcards," in *USENIX workshop on Smartcard Technology*, 1999.

[33] G. Bai, S. Bobba, and I. N. Hajj, "Simulation and optimization of the power distribution network in vlsi circuits," in *Proceedings of IEEE/ACM ICCAD*, 2000, pp. 481–486.