Leveraging On-Chip Voltage Regulators as a Countermeasure Against Side-Channel Attacks*

Weize Yu
University of South Florida
Tampa, Florida
weizeyu@mail.usf.edu

Orhun Aras Uzun
University of South Florida
Tampa, Florida
orhunuzun@mail.usf.edu

Selçuk Köse
University of South Florida
Tampa, Florida
kose@usf.edu

ABSTRACT

Side-channel attacks have become a significant threat to the integrated circuit security. Circuit level techniques are proposed in this paper as a countermeasure against side-channel attacks. A distributed on-chip power delivery system consisting of multi-level switched capacitor (SC) voltage converters is proposed where the individual interleaved stages are turned on and turned off either based on the workload information or pseudo-randomly to scramble the power consumption profile. In the case that the changes in the workload demand do not trigger the power delivery system to turn on or off individual stages, the active stages are reshuffled with so called *converter-reshuffling* to insert random spikes in the power consumption profile. An entropy based metric is developed to evaluate the security-performance of the proposed converter-reshuffling technique as compared to three other existing on-chip power delivery schemes. The increase in the power trace entropy with CoRe scheme is also demonstrated with simulation results to further verify the theoretical analysis.

Categories and Subject Descriptors

SEC1.3 [**Hardware Security**]: Device, circuit, and architecture techniques for security

Keywords

Side-channel attacks, on-chip voltage regulation, power efficiency

1. INTRODUCTION

Hardware security has become an important design metric during the past decade with the increase in the number of attacks at different hardware abstraction levels. Along with the other important metrics such as higher power efficiency, better performance, and lower noise, hardware security is also added as an important design objective in modern computing devices. It has been shown that software level countermeasures may not be sufficient to protect the encrypted data from an attacker who has physical access to the device under attack (DuA). Even flawless implementations of state-of-the-art encryption algorithms are typically vulnerable against hardware attacks. The primary reason is that the modern integrated circuits (ICs) heavily depend on complementary metal oxide semiconductor (CMOS) transistors which have switching characteristics that are easily analyzed to determine the underlying circuit functionality. The side channel leakage originating from the switching activity of transistors can be monitored with simple measurement equipment by an attacker. This side channel leakage can manifest itself in the form of power consumption profile, timing profile, electromagnetic emanations (EME), acoustic waveforms, and heat. An efficient implementation of side-channel attacks can retrieve the secret key from an AES algorithm in a couple of minutes whereas it can take up to 149 trillion years to crack a 128-bit AES key with a supercomputer [1].

Various techniques have been proposed to minimize the information leakage through side-channels. Most of the circuit-level countermeasures focus on modifying the power consumed by the logic circuits and/or memory (hereafter called as load circuits in the paper) to hide and/or mask the information from an attacker [2]. These techniques include leakage reduction, noise injection, frequent key update, and designing secure PUF and scan chain circuits [2]. There is, however, a limited amount of research that exploits the medium, *power delivery network*, through which a significant amount of leakage is emanated from. With the proliferation of on-chip voltage regulators in modern ICs, the on-chip power delivery network is no longer a mesh connection of metal wires but also includes active voltage regulators. The on-chip voltage regulators can potentially be used to scramble the power consumption monitored by an attacker with negligible power and area overhead.

A countermeasure based on on-chip voltage regulators has been recently proposed [3] where an interleaved switched capacitor (SC) voltage converter is utilized and individual stages are turned on and turned off based on the workload information. Activation and deactivation of each individual stage creates a current spike in the power consumption profile that is potentially monitored by an attacker. One primary shortcoming of this technique is that the number of active stages is determined based on the workload information and therefore the characteristics (timing and amplitude) of

*This work was supported in part by the National Science Foundation CAREER grant under contract No. CCF-1350451 and a research award from Cisco Systems.

DAC '15, June 07 - 11, 2015, San Francisco, CA, USA

http://dx.doi.org/10.1145/2744769.2744866.

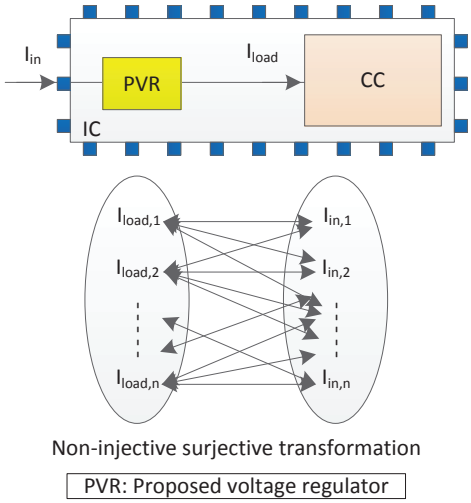

Figure 1: Proposed technique disrupts the one-to-one transformation and accomplishes a non-injective relationship between the load current and input current.

the artificial current spikes may provide critical information about the actual power consumption of the circuit. A significant amount of the workload information may eventually still leak with this technique [3].

A workload-agnostic SC voltage converter management technique is proposed in this paper to minimize the information leakage via side-channels. Active converter stages are periodically or pseudo-randomly reshuffled with the inactive converter stages regardless of the changes in the workload demand.

Our contributions in this paper are as follows:

- A new on-chip voltage converter management technique, converter-reshuffling (CoRe), is proposed as a countermeasure against side-channel attacks
- The performance of CoRe is evaluated both theoretically and with simulation results
- A security-performance metric, power trace entropy, has been utilized to evaluate the security levels of four different on-chip power delivery schemes

The rest of the paper is organized as follows. Background information on on-chip voltage regulation is provided in Section 2. The treat model is explained in Section 3. A related state-of-the-art technique, converter-gating, is discussed in Section 4. The proposed workload-agnostic CoRe is explained in Section 5. The security-performance of CoRe technique is evaluated against three different power delivery schemes both theoretically and with simulation results in Section 6. The related work is summarized in Section 7 and the paper is concluded in Section 8.

2. BACKGROUND

On-chip voltage regulation is an area with vast amount of research to enable small, fast, efficient, robust, and high power-density voltage regulators on-die close to the load circuits [4,5]. On-chip voltage regulators provide faster voltage scaling, reduce the number of dedicated IO pins, and facilitate fine granularity power management techniques [4–7]. Three types of regulators are widely used in modern circuits: buck converters, switched capacitor (SC) converters, and low-dropout (LDO) regulators [8–10]. Buck converters can provide superior power efficiency over 95%; however, the on-chip area requirement is quite large due to the large passive LC filter [10, 11]. SC voltage converters utilize non-overlapping switches that control the charge-sharing between capacitors to generate a DC output voltage. Linear regulators provide superior line and load regulation but have inferior power efficiency limited to V_{out}/V_{in} [12, 13]. With the utilization of deep-trench capacitors, SC voltage converters can achieve high power densities such as 4.6 A/mm^2 [14]. SC voltage converters charge and discharge periodically, producing periodic spikes in the input current waveform and therefore reducing the correlation between the input and output current profiles as compared to LDO regulators.

Certain voltage regulator types allow a high correlation between the actual load current and the input current that may be monitored by an attacker to learn "*what is going on inside the chip.*" An injective (one-to-one) relationship should exist to determine $I_{load,n}$ by measuring $I_{in,n}$. When the IC does not employ on-chip voltage regulation, an injective relationship exists between the load current consumed by the cryptographic circuit (CC) and the input current to the IC (*i.e.*, $I_{load,n} = I_{in,n}$), as shown in Fig. 1. If the on-chip power delivery network can provide a non-injective relationship between the load and input current profiles, as illustrated in Fig. 1, (*i.e.*, a particular load current leads to *more than one* input current profile), the outside attacker can no longer obtain the internal information by measuring the input current. SC voltage converters charge and discharge periodically, produce spikes in the input current waveform, and therefore reduce the correlation between the input and output current profiles.

3. TREAT MODEL

The attack is assumed to be non-invasive and the attacker is assumed to have access to the circuit where s/he can monitor the side-channel leakage information. For example, the power consumption profile can be monitored by measuring the I/O pins dedicated to power/ground, shown as I_{in} in Fig. 1. Alternatively, the attacker can use near-field antennas to monitor the EM emanations. Additionally, the DuA is assumed to have on-chip voltage regulators.

4. REVIEW OF CONVERTER-GATING

Converter-gating (CoGa) is the adaptive activation and deactivation of certain stages of a multiphase on-chip SC voltage converter based on the workload information [3]. When the current demand increases (decreases), an additional passive (active) stage is activated (gated) to provide a higher (lower) load current without sacrificing power conversion efficiency. The additional stage that is being activated or gated is determined based on a pseudo-random number generator (PRNG) to scramble the input current consumption of the SC voltage converter (*i.e.*, I_{in} as shown in Fig. 1). Since each interleaved stage within an SC voltage converter is driven with a different phase of the input clock signal, each interleaved stage charges and discharges with a certain time shift. The amount of time shift depends on the frequency of the clock signal. For example, a timing shift of 0.5 μs can be achieved by activating the 4^{th} stage instead of the 0^{th} stage when an eight stage SC converter operates at 1 MHz.

Although CoGa makes the attackers' job more difficult by scrambling the power consumption profile and inserting additional spikes in the input current profile, the DuA would still be vulnerable under advanced attacks as the activation/deactivation occurs when there is a change in the

workload demand. Particularly, an attacker can effectively bypass the CoGa technique if an attack is performed such that the changes in the load current demand are not large enough to trigger CoGa to activate/deactivate interleaved stages. Furthermore, the input current profile that is monitored by an attacker would still be correlated with the actual current profile even if CoGa is triggered since the activation/deactivation occurs when there is a change in the workload demand.

5. CONVERTER-RESHUFFLING

A new control technique, converter-reshuffling (CoRe), is proposed to scramble the input current profile when the change in the load current is not sufficiently large to turn on or off a converter stage. In CoRe technique, a new set of voltage converter stages is periodically determined with a PRNG. Some of the active converter stages are then juggled accordingly with the inactive converter stages. In other words, some of the active stages are gated concurrently while the same number of inactive stages are turned on under constant load current demand.

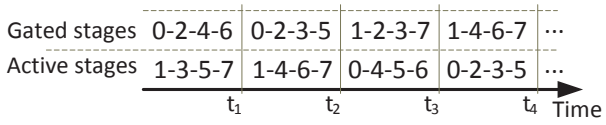

Figure 2: Active and gated converters are juggled with converter-reshuffling.

For example, the number of required active converter stages to efficiently provide a load current of 1 mA is four. Let's assume that these active stages are the 1^{st}, 3^{rd}, 5^{th}, and 7^{th} converter stages. With CoRe, some of these active stages are gated and the same number of inactive stages are simultaneously turned on, as shown in Fig. 2. After a certain time period, the converters are shuffled again while keeping the same number of converters active. Please note that CoRe technique can work with or without converter-gating regardless of whether or not the load current demand is sufficiently large to trigger converter-gating and lead to an additional stage to turn on.

The primary advantages of CoRe operation as a side-channel attack countermeasure are twofold. First, the input current profile is disrupted while turning on and off different converter stages. Secondly, the input current profile periodically exhibits a different signature since the phases of the active converter stages vary, generating a quite different input current signature. For example, an eight phase SC voltage converter with three active stages has $\binom{8}{3}$=56 activity patterns that would lead to 56 different input current signatures while delivering the same load current.

6. EVALUATION

6.1 Theoretical Proof of Converter Reshuffling

Entropy is a widely used property to quantify the security-performance of countermeasures against side-channel attacks [15]. In this paper, the power trace entropy (PTE) is utilized as a security-performance metric while ensuring a constant time trace entropy (TTE) to compare the security levels of different voltage regulation schemes [16]. PTE and TTE are, respectively, the uncertainty of the amplitude and timing of the spikes in the power consumption profile. It has been shown in [16] that TTE is zero without DVFS. When DVFS is activated, a constant non-zero TTE of 6.02 [16] is used in

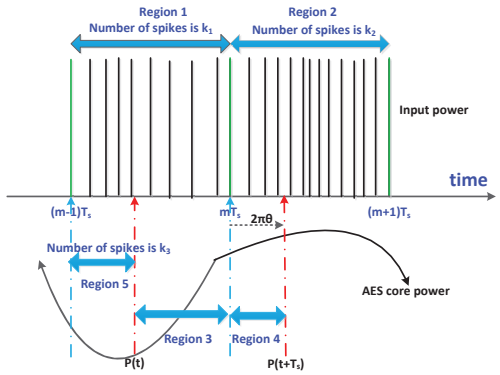

Figure 3: Relationship between the input power and AES core power.

the evaluation. Intuitively, TTE increases when the operating frequency changes over time as in the case of DVFS. We assume that the power consumption of an AES core is $P(t)$ at time t, the number of phases N changes between 30 and 100, the switching frequency and period of each phase are, respectively, f_s and T_s, the frequency of the input data for AES core is f_0, the phase difference between actual power consumption and sampling of the attacker is $2\pi\theta$. The relationship between the input power and AES core power while employing either CoGa or CoRe is illustrated in time domain in Fig. 3. Regions 3 and 4 are, respectively, the time periods in which the attacker observes part of the spikes that occur in Regions 1 and 2. The two consecutive power consumption profiles, as shown in Fig. 3, may contain different number of spikes k_1 and k_2 if the workload current demand changes. Assuming $k_2 > k_1$, the change in the number of spikes $f(\theta, P(t))(k_2 - k_1)$, as illustrated in Fig. 3 in Region 4, can be observed by an attacker and may provide critical information about the workload. $f(\theta, P(t))$ is the ratio of number of additional spikes in Region 4 over the total number of additional spikes in Region 2.

The input power of CoGa $P_{in}^{CoGa}(t)$ observed by an attacker within a switch period T_s can be expressed as

$$P_{in}^{CoGa}(t) = k_1 P_0 + f(\theta, P(t))(k_2 - k_1)P_0, \quad (1)$$

where

$$k_1 = [\frac{\int_{(m-2)T_s}^{(m-1)T_s} P(t)dt}{\eta_0 P_0 T_s}], \quad (2)$$

$$k_2 = [\frac{\int_{(m-1)T_s}^{mT_s} P(t)dt}{\eta_0 P_0 T_s}], \quad (3)$$

η_0 is the power efficiency, P_0 is the output power of each individual converter phase, and m is the number of switch cycles that is a function of time t.

The input power of CoRe $P_{in}^{CoRe}(t)$ observed by an attacker within a switch period T_s can be expressed as

$$P_{in}^{CoRe}(t) = \alpha(\theta, P(t))P_0 + \beta(\theta, P(t))P_0, \quad (4)$$

where $\alpha(\theta, P(t))$ and $\beta(\theta, P(t))$ are the number of spikes that is monitored by an attacker, respectively, in Regions 3 and 4.

In differential power analysis (DPA) attacks, the attacker monitors the dynamic power consumption [16]. To obtain a useful level of PTE from CoGa and CoRe, the probability of detecting the changes in the power profile for each possible

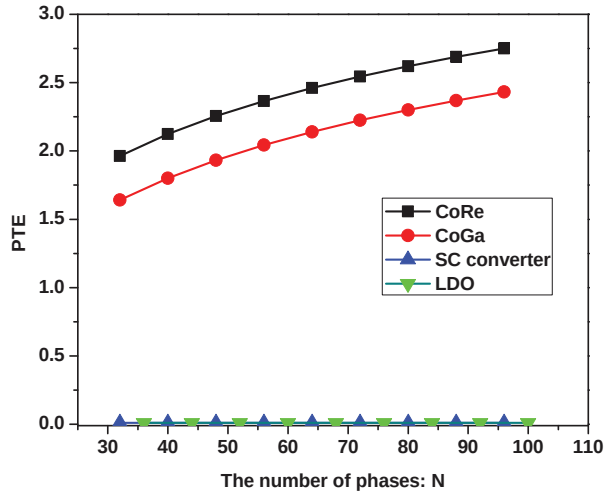

Figure 4: Relationship between the number of phases and the PTEs for four different kinds of voltage regulation schemes without employing DVFS.

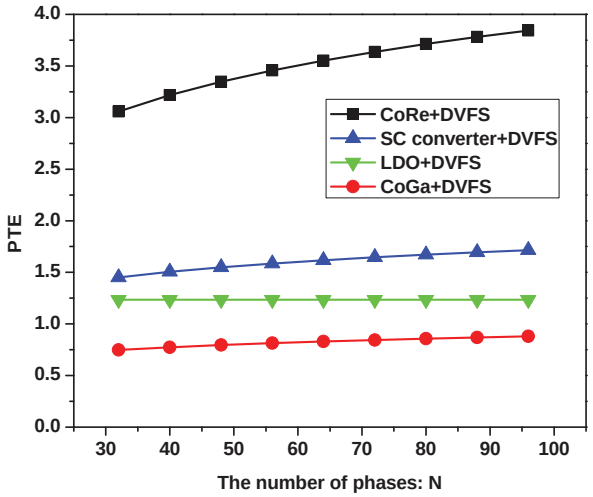

Figure 5: Relationship between the number of phases and the PTEs for four different kinds of voltage regulation schemes with DVFS enabled AES core.

input power value needs to be calculated. This probability $\gamma_i(\theta, P(t))$ for CoGa when $\theta \neq 0$ is

$$\gamma_i(\theta, P(t)) = \frac{\binom{[\theta N]-k_3}{i}\binom{[(1-\theta)N]-k_1+k_3}{k_2-k_1-i}}{\binom{N-k_1}{k_2-k_1}}, \quad (5)$$

$$i \in [A, B] = [max\{0, k_2 - k_3 - [(1-\theta)N]\}, min\{[\theta N] - k_3, k_2 - k_1\}], \quad (6)$$

where k_3 is the number of spikes in Region 5, as illustrated in Fig. 3. The PTE value for CoGa $PTE^{CoGa}_{DPA}(t)$ is therefore

$$PTE^{CoGa}_{DPA}(t) = -\sum_{i=A}^{B} \gamma_i(\theta, P(t)) log_2^{(\gamma_i(\theta,P(t)))}. \quad (7)$$

Note that if $\theta = 0$, the probability $\gamma_i(0, P(t)) = 1$ and the PTE for CoGa becomes 0. However, in practice, the switching frequency f_s is not constant, but has a narrow frequency range. It is quite difficult for an attacker to keep the value of θ as 0 all the time. Therefore, in the rest of the paper, we assume $\theta \neq 0$.

For CoRe, the probability function $\lambda_j(\theta, P(t))$ for achieving different input powers is

$$\lambda_j(\theta, P(t)) = \frac{\binom{N}{j}\binom{N}{k_1+k_2-j}}{\binom{N}{k_1}\binom{N}{k_2}}, \quad (8)$$

$$j \in [C, D] = [max\{0, k_1 + k_2 - N\}, min\{N, k_1 + k_2\}], \quad (9)$$

when $\theta \neq 0$. In (8), $j = i_1 + i_2$ where i_1 and i_2 are the number of spikes, respectively, in Regions 3 and 4. The constraints for (i_1, i_2) are $(i_1 \leq k_1, i_2 \leq k_2)$. Accordingly, the PTE of CoRe $PTE^{CoRe}_{DPA}(t)$ becomes

$$PTE^{CoRe}_{DPA}(t) = -\sum_{j=C}^{D} \lambda_j(\theta, P(t)) log_2^{(\lambda_j(\theta,P(t)))}. \quad (10)$$

The relationship between the number of phases and the PTE value for four different kinds of voltage regulation schemes is illustrated in Fig. 4 when load power demand varies from $(1/2)P_{max}$ to $(7/8)P_{max}$ where P_{max} is the maximum dynamic power consumption for AES core. As shown in Fig. 4, the PTE of CoRe is about 13% greater as compared to the PTE of CoGa and therefore CoRe provides better security than CoGa.

Dynamic voltage and frequency scaling (DVFS) is a popular technique which not only reduces power dissipation but also can improve the security level of AES core by increasing time trace entropy (TTE) [16]. Accordingly, the security implications of the proposed on-chip voltage regulation scheme is compared to the three other existing power delivery schemes in the presence of DVFS. When the AES core employs DVFS, we assume the random time delay between the input data and power consumption variation caused by DVFS is T_0. In other words, the input power would vary within 0 to T_0 after the input data completed. In the case of CoGa, the variations in the power consumption appear within the first switch period only after the input data has been processed. This can cause CoGa a non-zero PTE. The PTE for CoGa $PTE^{CoGa}_{DVFS}(t)$ with DVFS therefore becomes

$$PTE^{CoGa}_{DVFS}(t) = -(1 - \frac{T_s}{T_0}) log_2^{(1-\frac{T_s}{T_0})} - \sum_{[\theta N]=1}^{N-1} \sum_{i=A}^{B} \frac{T_s}{NT_0} \gamma_i(\theta, P(t)) log_2^{(\sum_{[\theta N]=1}^{N-1} \frac{T_s}{NT_0} \gamma_i(\theta,P(t)))}. \quad (11)$$

The PTE for CoRe is, however, quite different in the presence of DVFS. The input power of CoRe keeps reshuffling regardless of the workload demand and therefore always has a non-zero PTE. As a result, the PTE of CoRe $PTE^{CoRe}_{DVFS}(t)$ is much greater than the PTE of CoGa and can be shown as

$$PTE^{CoRe}_{DVFS}(t) = -\sum_{[\theta N]=1}^{N-1} \sum_{j=C}^{D} \frac{1}{N}(1 - \frac{T_s}{T_0})\lambda^1_j(\theta, P(t)) \times log_2^{(\sum_{[\theta N]=1}^{N-1} \frac{1}{N}(1-\frac{T_s}{T_0})\lambda^1_j(\theta,P(t)))} - \sum_{[\theta N]=1}^{N-1} \sum_{j=C}^{D} \lambda_j(\theta, P(t)) \times \frac{T_s}{NT_0} log_2^{(\sum_{[\theta N]=1}^{N-1} \frac{T_s}{NT_0} \lambda_j(\theta,P(t)))}. \quad (12)$$

The probability function $\lambda_j^1(\theta, P(t)))$ is the same as $\lambda_j(\theta, P(t)))$ if $k_2 = k_1$. Similarly, the PTEs of a conventional SC voltage converter PTE_{DVFS}^{SC} and an LDO regulator PTE_{DVFS}^{LDO} with DVFS are

$$PTE_{DVFS}^{SC} = -(1 - \frac{T_s}{T_0})log_2^{(1-\frac{T_s}{T_0})} - \frac{T_s}{T_0}log_2^{(\frac{T_s}{T_0}\frac{1}{max\{k_1,k_2\}})}, \quad (13)$$

$$PTE_{DVFS}^{LDO} = -(1 - \frac{T_s}{T_0})log_2^{(1-\frac{T_s}{T_0})} - \frac{T_s}{T_0}log_2^{(\frac{T_s}{T_0}\frac{f_s}{f_{clock}})}, \quad (14)$$

where f_{clock} is the clock frequency of the AES core.

The PTEs of the aforementioned four different voltage regulation schemes for different number of voltage converter stages are illustrated in Fig. 5 when DVFS is employed. In Fig. 5, the load power consumption varies from $(1/2)P_{max}$ to $(7/8)P_{max}$ where P_{max} denotes the maximum dynamic power consumption for AES core. The clock frequency is selected between 250 MHz and 450 MHz and the TTE value is 6.02 in [16]. The switching frequency for CoGa and CoRe is 30 MHz.

The PTE of CoRe increases ∼40% when DVFS is activated. The primary reason for this enhancement is that the reshuffling behavior is workload-agnostic and DVFS further enhances the scrambling behavior. The PTE of SC voltage converter and LDO regulator also increases to a non-zero value with DVFS, but still much smaller than the PTE of CoRe. Alternatively, the PTE of CoGa reduces ∼64% in the presence of DVFS. Therefore, CoRe technique provides significantly higher security as compared to other power delivery schemes when DVFS is activated.

6.2 Circuit level evaluation

The control circuit of CoGa is modified to add the CoRe capability to the proposed system. A load current of 0.7 mA, as shown in Fig. 6a, is delivered with CoGa and CoRe schemes. Four out of eight stages are required to be active to provide 0.7 mA load current. When CoGa scheme is utilized, 0^{th}, 2^{nd}, 4^{th} and 6^{th} stages are active while providing a constant 0.7 mA load current. In the CoRe scheme, the active converter stages are joggled with gated stages after 10 clock periods, as shown in Fig. 2. The input current profiles of converter-gating and converter-reshuffling are shown in Fig. 6c. As shown in the zoomed Figs. 6d, 6e, 6f, and 6g, the input current spikes of the CoGa scheme exhibit a similar behavior (shown in red) whereas the input current spikes of the CoRe scheme have random timing and amplitude variations (*i.e.*, increased TTE and PTE, respectively). Both CoRe and CoGa techniques provide a robust output voltage as shown in Fig. 6b. This analysis validates that CoRe technique can scramble the power consumption profile monitored by an outside attacker even if the load current variations are not large enough to trigger CoGa technique and eventually increases the TTE and PTE values.

7. RELATED WORK

Various techniques have been proposed as a countermeasure against various types of side-channel attacks both at the circuit and architectural levels. To reduce the dependency of the side-channel leakage on the actual power consumption profile, leakage reduction techniques have been proposed. Dummy multiplication operations have been performed for timing attacks against RSA to minimize the leakage in the timing channel in [17], significantly increasing the power consumption. The actual power consumption profile can be smoothened by using different CMOS logic families to provide a more balanced pull-up and pull-down power consumption such as current-mode logic [18] or asynchronous logic [19]. Random or pseudo-random noise has been inserted in the side-channel leakage to make the analysis more difficult for an attacker in [20]. Although the number of required side-channel leakage measurements increases quadratically with decreasing SNR of the side-channel information [21], advanced techniques can be used to average out the injected noise [22]. Frequently updating the secret key is also proposed in [22] to add another level of difficulty for the attacker. One of the primary disadvantages of the existing techniques is the power and area overhead. Although some of these techniques are successful against certain side-channel attacks, power and area overheads typically make them quite costly [16].

8. CONCLUSIONS

A new on-chip power management technique, converter-reshuffling (CoRe), is proposed as a power efficient countermeasure against side channel attacks. A theoretical proof based on the power trace entropy (PTE) analysis is developed to compare CoRe with three other existing on-chip power delivery schemes. CoRe performs better than the other schemes with or without DVFS. The PTE of CoRe significantly increases when DVFS is activated whereas other techniques may have degraded PTE levels with DVFS.

9. REFERENCES

[1] M. Arora, "How Secure is AES Against Brute Force Attacks?," 2012. [Online]. Available: http://www.eetimes.com/document.asp?doc_id=1279619.

[2] M. Rostami, F. Koushanfar, and R. Karri, "A Primer on Hardware Security: Models, Methods, and Metrics," *Proceedings of the IEEE*, Vol. 102, No. 8, pp. 1283–1295, August 2014.

[3] O. A. Uzun and S. Kose, "Converter-Gating: A Power Efficient and Secure On-Chip Power Delivery System," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, Vol. 4, No. 7, pp. 169–179, June 2014.

[4] E. Alon and M. Horowitz, "Integrated Regulation for Energy-Efficient Digital Circuits," *IEEE Journal of Solid-State Circuits*, Vol. 43, No. 8, pp. 1795–1807, August 2008.

[5] W. Kim, M. S. Gupta, G.-Y. Wei, and D. Brooks, "System Level Analysis of Fast, Per-Core DVFS Using On-Chip Switching Regulators," *Proceedings of the IEEE International Symposium on High Performance Computer Architecture*, pp. 123–134, February 2008.

[6] L. Benini, A. Bogliolo, and G. De Micheli, "A Survey of Design Techniques for System-Level Dynamic Power Management," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 8, No. 3, pp. 299–316, March 2000.

[7] S. Kose and E. G. Friedman, "Distributed On-Chip Power Delivery," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, Vol. 2, No. 4, pp. 704–713, December 2012.

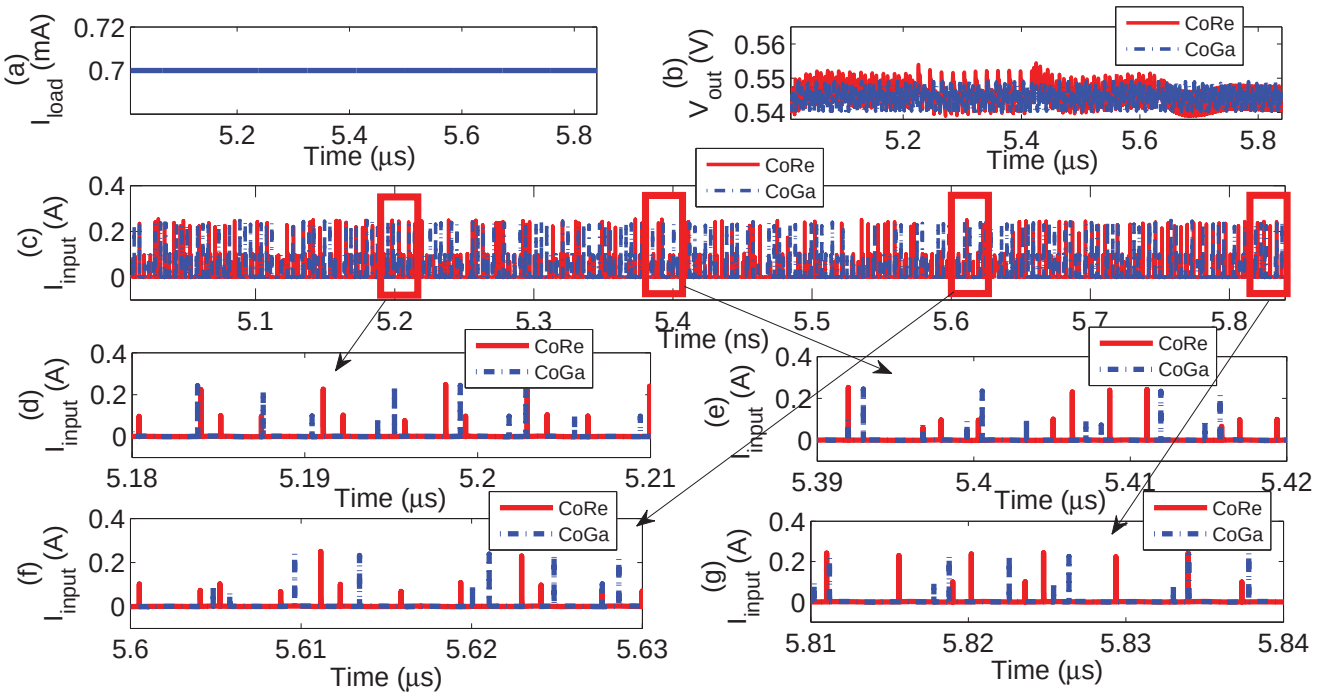

Figure 6: Converter-gating (CoGa) and converter-reshuffling(CoRe) are compared. a) Load current profile, b) output voltage, and c) corresponding input current profile of CoGa and CoRe schemes. The amplitude and timing of the input current spikes are scrambled when CoRe scheme is used whereas CoGa scheme cannot scramble the input current profile under a constant load current, as shown in d), e), f), and g).

[8] V. Kursun and E. G. Friedman, *Multi-Voltage CMOS Circuit Design*, John Wiley & Sons, 2006.

[9] G. Rincon-Mora, *Analog IC Design with Low-Dropout Regulators (LDOs)*, McGraw-Hill Publishers, 2009.

[10] C. F. Lee and P. K. Mok, "A Monolithic Current-Mode CMOS DC-DC Converter with On-Chip Current-Sensing Technique," *IEEE Journal of Solid-State Circuits*, Vol. 39, No. 1, pp. 3–14, January 2004.

[11] V. Kursun, S. G. Narendra, V. K. De, and E. G. Friedman, "Analysis of Buck Converters for On-Chip Integration with a Dual Supply Voltage Microprocessor," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 11, No. 3, pp. 514–522, June 2003.

[12] G. A. Rincon-Mora, *Current Efficient, Low Voltage, Low Drop-out Regulators*, Ph.D. thesis, Georgia Institute of Technology, 1996.

[13] S. Kose, S. Tam, S. Pinzon, B. McDermott, and E. G. Friedman, "Active Filter Based Hybrid On-Chip DC-DC Converters for Point-of-Load Voltage Regulation," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 21, No. 4, pp. 680–691, April 2013.

[14] T. M. Andersen *et al.*, "A 4.6 W/mm^2 power density 86% efficiency on-chip switched capacitor DC-DC converter in 32 nm SOI CMOS," *Proceedings of the IEEE International Applied Power Electronics Conference and Exposition*, pp. 692–699, March 2013.

[15] B. Kopf and D. Basin, "An information-theoretic model for adaptive side-channel attacks," *CCS*, pp. 286–296, October 2007.

[16] S. Yang, W. Wolf, N. Vijaykrishnan, D.N. Serpanos, and Y. Xie, "Power Attack Resistant Cryptosystem Design: A Dynamic Voltage and Frequency Switching Approach," *Design, Automation and Test in Europe*, pp. 64–69, March 2005.

[17] P. Rakers, L. Connell, T. Collins, and D. Russell, "Secure Contactless Smartcard ASIC with DPA Protection," *IEEE Journal of Solid-State Circuits*, Vol. 36, No. 3, pp. 559–565, March 2001.

[18] A. Cevrero, F. Regazzoni, M. Schwander, S. Badel, P. Ienne, and Y. Leblebici, "Power-Gated MOS Current Mode Logic (PG-MCML): A Power Aware DPA-resistant Standard Cell Library," *Proceedings of the IEEE/ACM Design Automation Conference*, pp. 1014–1019, May 2011.

[19] W. Cilio, M. Linder, C. Porter, J. Di, D. R. Thompson, and S. C. Smith, "Mitigating Power- and Timing-Based Side-Channel Attacks Using Dual-Spacer Dual-Rail Delay-Insensitive Asynchronous Logic," *Microelectronics Journal*, Vol. 44, No. 3, pp. 258–269, March 2013.

[20] J. A. Ambrose, R. G. Ragel, and S. Parameswaran, "Randomized Instruction Injection to Counter Power Analysis Attacks," Vol. 11, No. 3, pp. 69:1–69:27, March 2012.

[21] C. Clavier, J.-S. Coron, and N. Dabbous, *Differential Power Analysis in the Presence of Hardware Countermeasures*, Springer, 2000.

[22] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to Differential Power Analysis," *Journal of Cryptographic Engineering*, Vol. 1, No. 1, pp. 5–27, 2011.