Exploiting On-chip Power Management for Side-Channel Security

Arvind Singh[1], Monodeep Kar[1], Sanu Mathew[2], Anand Rajan[2], Vivek De[2], and Saibal Mukhopadhyay[1]
Georgia Institute of Technology[1], and Intel Labs[2]

{rathorearvind19, monodeepkar}@gatech.edu, {sanu.mathew, anand.rajan, vivek.de}@intel.com, saibal@ece.gatech.edu

***Abstract*—The high-performance and energy-efficient encryption engines have emerged as a key component for modern System-On-Chip (SoC) in various platforms including servers, desktops, mobile, and IoT edge devices. A key bottleneck to secure operation of encryption engines is leakage of information through various side-channels. For example, an adversary can extract the secret key by performing statistical analysis on measured power and electromagnetic (EM) emission signatures generated by the hardware during encryption. Countermeasures to such side-channel attacks often come at high power, area, or performance overheads. Therefore, design of side-channel secure encryption engines is a critical challenge for high-performance and/or power-/energy efficient operations. This paper reviews that although low-power requirement imposes critical challenge for side-channel security, but circuit techniques traditionally developed for power management also present new opportunities for side-channel resistance. As a case study, we review the feasibility of using integrated voltage regulator and dynamic voltage frequency scaling normally used for efficient power management, for increasing power-side-channel resistance of AES engines. The hardware measurement results from test-chip fabricated in 130nm process are presented to demonstrate the impact of power management circuits on side-channel security.**

Keywords— Integrated Voltage Regulators, Side-channel Attacks, Countermeasures, Voltage Dithering, Cryptography

I. Introduction

The advent of pervasive computing has led to exponential growth of computing devices from servers to personal digital assistants to all the way to miniscule Internet-of-Things (IOTs) and Internet-of-Everything (IOE) devices [1]. Most of these devices are inter-connected through internet and sensitive data is monitored, processed and communicated in real-time over insecure physical channels. To secure the sensitive information, data is often encrypted using mathematically unbreakable cryptographic algorithms [2]. However, the hardware implementations [3-4] of these algorithms leak information in the form of power [5], electromagnetic emission (EM) [6] and timing [7] signatures when critical data is computed or communicated. An adversary, even with limited resources, can efficiently and inexpensively measure these signatures and perform statistical analyses, also known as side-channel analysis (SCA) [5], to reveal the secret encryption key. Several countermeasures proposed to secure hardware devices against SCA attacks implement techniques to eliminate/randomize data dependency in the measured side-channel signatures [8-17]. However, most of these countermeasures have appreciable power, area, and performance overheads and often require complete/partial re-design of the whole encryption hardware.

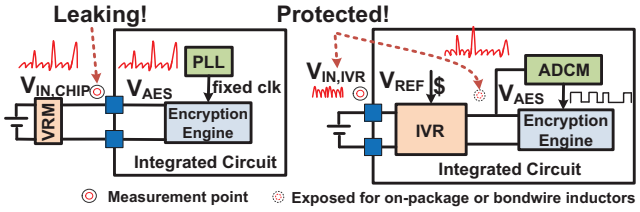


Fig 1. Exploiting integrated voltage regulators (IVR) and all-digital clock modulation (ADCM) for protection against power side-channel attacks: (a) traditional power delivery system and (b) on-chip integrated IVR+ADCM architecture to protect against SCA attacks.

Power management and low-power techniques such as distributed on-chip voltage regulation, dynamic voltage scaling (DVS) [18], dynamic voltage and frequency scaling (DVFS) [19] as well as clock and power gating are becoming very critical for energy-efficient digital circuits and architectures [20]. Integration of voltage regulation modules on-chip provides very fast response to transient events and reduces the overheads associated with switching of power states and therefore facilitates fine-grain power management for multiple DVFS domains. Adaptive clocking is another technique which eliminates timing/supply margins under variations, therefore improving system performance or reducing the total power [21, 22]. These techniques modulate/modify power side-channel leakage and therefore it is essential to understand their interaction with side-channel security of underlying cryptographic hardware [23-37].

This paper reviews the power, performance, area (PPA) and SCA resistance tradeoffs for unprotected encryption engines. Additionally, the impact of power management and low power techniques on the side-channel security of encryption engines is discussed. In particular, we discuss that side-channel resistance offered by integrated voltage regulators (IVRs) with some control loop modifications [23, 36] and random fast voltage dithering (RFVD), a DVFS like scheme enabled with IVR and all-digital clock modulation (ADCM) [24] (Fig. 1). Security-aware architectures exploiting these power management and low power techniques are developed and improvement in the SCA resistance is quantified with minimum-traces-to-disclosure (MTD) for correlation power analysis (CPA) [38] and test-vector leakage assessment (TVLA) [39] metric with measurement results from a test-chip fabricated in 130nm process. The analysis shows the potential of using traditional power management techniques like integrated voltage regulation and dynamic voltage/frequency scaling for improving power-side-channel attack resistance.

Table 1. Comparison of side channel analysis attack resistance offered by power management and low power techniques

Power Management/Low Power Technique	Complexity	Area	PAA resistance analysis
Switched Cap. (SC) VR + analog-LDO [25]	High	Moderate	Protection using SC-VR. No power attack analysis.
Random converter gating in multi-phase SC-VR [26]	High	High	Improvement in power trace entropy, no statistical power analysis
Fully Integrated Inductive VR [23, 27-28]	High	High	Power attack protection from control loop randomization
Integrated LDO [29-32]	Moderate	Low	PAA protection with integration effects and feedback loop losses
Random Dynamic Voltage Frequency Scaling (RDVFS) [33-34]	High	High	Max. N× increase in MTD where N number of V-F pairs
Dynamic Voltage Switching (DVS) [35]	Moderate	High	Broken with instantaneous frequency analysis

II. Background

After Paul Kocher introduced differential power analysis attacks almost two decades ago [5], there have been several countermeasures proposed to prevent the leakage of critical information through physical channels. These countermeasures are based on two basic principles – a) information hiding and b) information masking. Information hiding tries to break the relation between power consumption and intermediate computation of data achieved by reducing the signal-to-noise ratio (SNR) or equalizing the current drawn independent of input vectors. On the other hand, masking relies on randomization of key dependent intermediate data processing. Most of these countermeasures can be divided into architectural [8-10], logic [11-13] or physical design [14-16] aspects of hardware design. Architectural solutions target to achieve information hiding or masking or both with modification at the architecture level, for example, by inserting "no operations (NOPs)", random order execution of encryption instructions [8] and processing bitflipped data on dual core processor system to equalize the power consumption [9]. Same result can also be obtained with logic level modifications to the underlying security algorithm. For example, differential dynamic logic (DDL) families draw equal current independent of input vectors [11, 12]. However, DDL based countermeasures atleast double the required area and power, degrade the performance, and are not very friendly with ASIC design flows and require custom design of the encryption cores, therefore increasing the design verification and implementation time. Moreover, these countermeasures have been proven ineffective with higher order SCA attacks which exploit early propagation of signals resulting from timing differences [17]. At physical design level, most of the state-of-the-art countermeasures try to reduce the SNR either with direct noise injection during encryption or through some technique which modulates the current consumption during encryptions. Some of the popular physical design based countermeasures are switched capacitor current equalization [14], power-delivery-network (PDN) [15], noise injection and clock randomization [16].

One major drawback with most of the current countermeasures is that they require complete or partial redesign of the underlying security circuit. Recently, researchers have given significant attention to exploiting components and techniques used for power management and low power design [23-37] (Table 1) which can in principle lead to generic countermeasures, therefore not requiring any modification to the encryption core. Voltage regulators, an essential part of power delivery unit, have recently been shown to offer side-channel resistance arising from their inherent transformations [23-32]. These voltage regulators can be switching DC-DC inductive/capacitive regulators or linear regulators. Switching voltage regulators require passives and are complex in nature. However, because of large signal transformations, they are expected to offer higher resistance to SCA attacks as compared to linear regulators. Linear regulators, also known as low-drop-out regulators, do not require any large passives and are easier to design and integrate with digital process technology. In particular, digital low-drop-out (DLDO) regulators with limited sampling rate and quantization error of feedback loop offer higher SCA resistance compared to their analog counterparts [31]. Traditional low power techniques such as dynamic voltage frequency scaling (DVFS) which are generally implemented to improve the energy efficiency of low-power systems, have also been explored with respect to power attack. Countermeasures utilizing these techniques (random DVS or random fast DVFS [33-35]) have been demonstrated to increase the difficulty of a successful attack.

III. Power-Security Trade-off For Encryption Engines

Architectural modifications on encryption engines due to low-power-constraints can significantly affect the side-channel-vulnerability of the design. Table 2 shows comparison between a high-performance parallel AES design with 128-bit datapath, a low-performance serial AES with 8-bit datapath and an alternative lightweight crypto system SIMON with a bit-serial datapath [29]. For better understanding, the power/performance, and area are normalized to that of the parallel AES. Table 2 shows that the serialized AES design and the SIMON have lower area and power compared to the high-performance parallel AES, however the measurements to disclose (MTD) for CPA attack is also drastically lower than the parallel AES. This suggests that resource constrained

Table 2. Comparison of synthesis area, power, and performance of encryption engines with different power-constraints [29, 36].

	Norm. Area	Norm. Power	Latency (#cycles)	Norm. MTD
High performance parallel AES	1	1	1	1
Compact serial AES	0.1	0.4	125	0.05
SIMON	0.02	0.08	1150	0.05

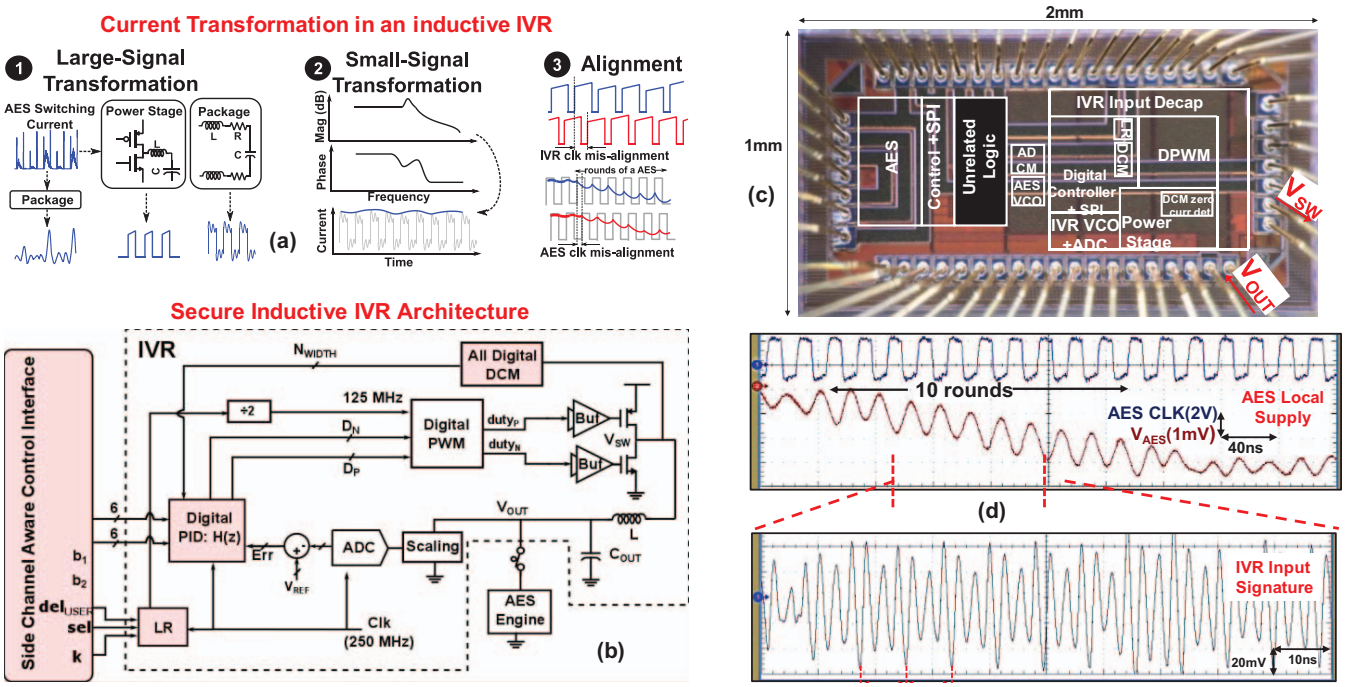


Fig 2. Security aware inductive IVR design (a) IVR transformations, (b) security-aware architecture, (c) 130nm test-chip and (d) sample measured V_{AES} and $V_{IN,IVR}$ waveforms for AES encryption [23, 36].

encryption engines are more vulnerable to power attacks i.e. a trade-off exist in the energy-security space of encryption hardware.

IV. Power Management Techniques And Power Attack

A. Power Management Techniques

With constant miniaturization of semiconductor devices, a variety of functional blocks are now integrated into modern microprocessors, system-on-chip (SoC) and portable systems. One major bottleneck preventing these systems from achieving high performance and energy efficiency is the quality of power delivered to these multi-functional dynamically varying loads. Traditional methods to manage power delivery with off-chip voltage regulation modules (VRM) has significant drawback due to printed-circuit-board (PCB) and package parasitics which incur appreciable power losses. Additionally, longer feedback loop slows down the transient response thus resulting in significant performance degradation. To facilitate energy-efficient power delivery, these VRMs have recently been integrated on-chip bringing power delivery units closer to the target loads [20]. This not only improves energy efficiency for the overall system but also improves the system performance.

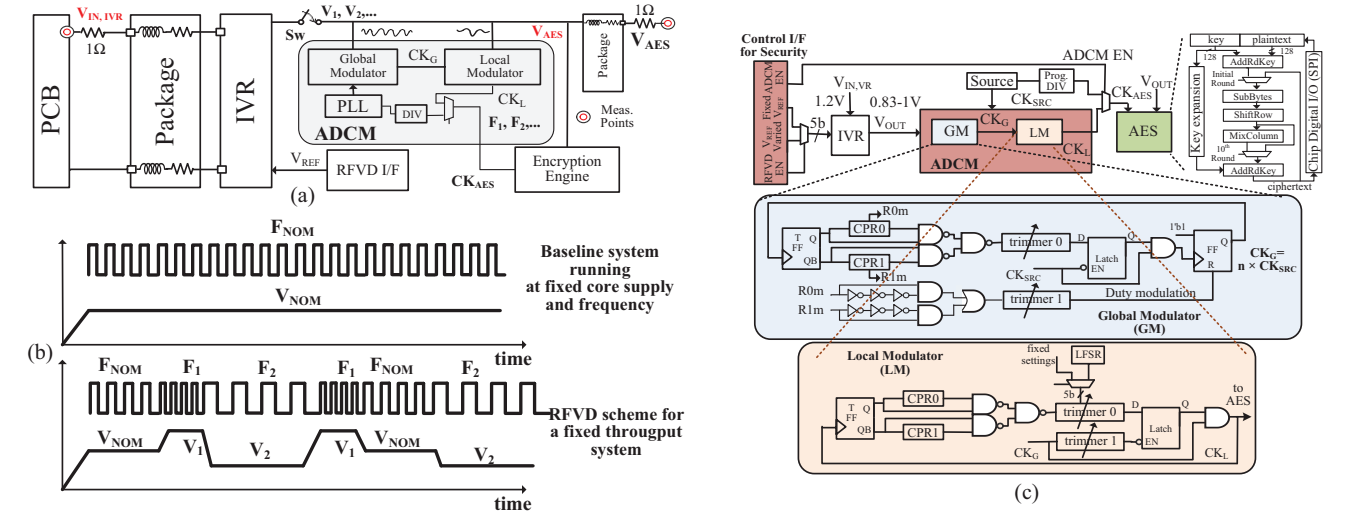
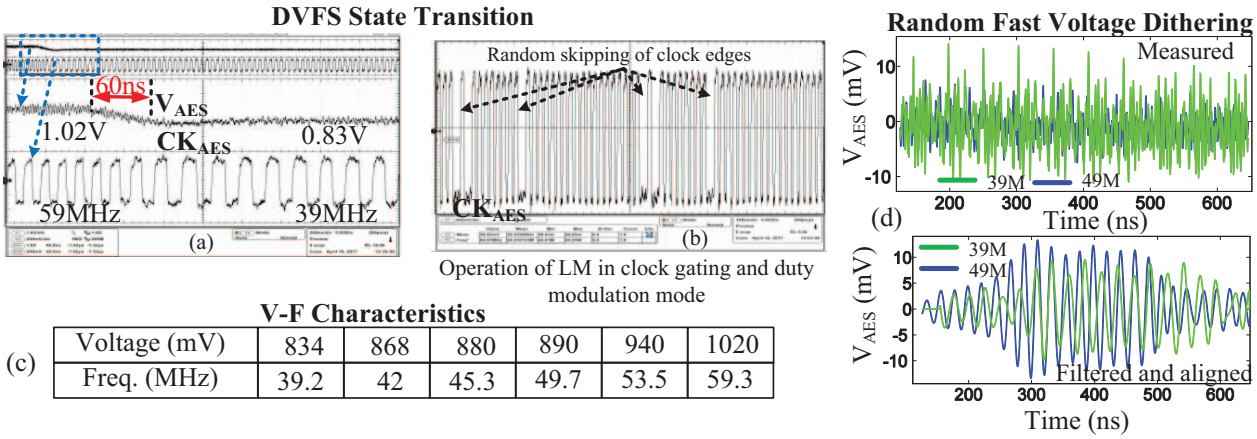


Fig 3. (a) DVFS/RFVD architecture for improved energy efficiency and SCA attack robustness, (b) RFVD for fixed system throughput and (c) block diagram of AES+IVR+ADCM system with security-aware control interface [24].



Operation of LM in clock gating and duty modulation mode

(c) **V-F Characteristics**

Voltage (mV)	834	868	880	890	940	1020
Freq. (MHz)	39.2	42	45.3	49.7	53.5	59.3

Fig 4. All-digital clock modulation (ADCM) operation: (a) worst case voltage transition from 1.02V to 0.834V occurs in 60ns with ADCM modulating clock even during the transition, ensuring correct operation, (b) additional random shifts added to clock edges from LFSR controlled trimmer inside LM, (c) V-F characteristics, and (d) measured and aligned waveforms for RFVD traces [24].

Dynamic voltage scaling (DVS) [18] and dynamic voltage frequency scaling (DVFS) [19] are widely used in modern SoCs in conjunction with voltage regulation modules to adapt to varying workloads. With these techniques, significant power can be saved under light workload conditions, making battery operated devices (smartphones, laptops, etc) last longer with a single charge. One major drawback associated with traditional DVFS architectures which utilize PLL and wait for PLL re-lock (usually much higher with respect to high speed functional clocks) to switch between different DVFS states is the performance and power overheads, preventing DVFS controllers to frequently switch between power states to save power. Therefore, there has been significant interest in developing all-digital clock modulation (ADCM) circuits to enable fast frequency changes. The clock modulation circuits also provide the additional advantage of increased tolerance to supply noise [21, 22].

We present illustrative design of on-chip power management circuits composed of IVR and ADCM to perform on-chip voltage regulation to reduce supply noise and enable fast DVFS. Measurement results are presented from a 130nm CMOS test-chip with a fully integrated inductive IVR (125MHz, 11.6nH inductor) powering a 128-bit AES engine [40, 41]. An inductive IVR consists of a power stage followed by an integrated L-C filter (Fig. 2). Several forms of integrated inductors have been used in high frequency IVRs, including on-chip/on-package implementation with metal traces, bondwires, etc. This design utilizes 2 bondwires to construct the inductor from an LCC package. Digital PWM control with a PID compensator is used for ease of integration into digital process nodes. This IVR can provide very fast output voltage transitions of 230mV/80ns and responds quickly to large load transients (80ns for 5mA to 65mA load step) with resistive-transient-assist technique [40, 41].

An on-chip integrated all-digital clock modulation (ADCM) circuit is utilized to enable single-cycle adaptation to any transitions in IVR output voltage [Fig. 3(a&b)] [21]. ADCM circuit is powered by output of IVR and utilizes two clock modulators – global modulator (GM) and local modulator (LM) [Fig. 3(c)]. GM consists of two critical path replicas and responds to any global noise or DC variations in the supply while LM, having similar structure, takes output clock of GM and modulates the clock edges in presence of local supply noise (clock stretching in duty modulation mode and clock skipping in clock gating mode). The ADCM circuit is supplied with a voltage-controlled-oscillator (VCO) generated 600MHz clock which determines the resolution and therefore sensitivity of GM generated clock with respect to supply noise. DVFS is implemented for a target AES encryption engine utilizing fast output voltage transitions from IVR and 1-cycle response of ADCM circuit. The reference word to the IVR controller can be varied depending on the dynamic workload and IVR responds by changing the output voltage. The ADCM circuit responds to these changes at cycle-by-cycle speed [Fig. 4(a&b)]. Fig. 4(c) shows the output voltage levels generated by IVR (0.834V to 1.02V) and corresponding clock frequencies generated by the ADCM circuit (39.2MHz to 59.3MHz) for the AES digital core. This DVFS state transition is achieved in only 60ns and the clock output is valid even during the transition. The area and power overheads associated with ADCM circuit are very small (9000µm2 and 102.4µW [21]).

B. Power Attack

Several low-power circuit techniques have the potential to improve resistance to power attack as well as satisfy the energy-efficiency requirement of the encryption engines. For example, as IVRs isolate the local supply nodes of the digital logic from the IVR input, they can be potentially exploited for improvement in power side-channel resistance. In this section, we review the SCA resistance offered by IVR and random fast voltage dithering scheme enabled by IVR in conjunction with ADCM circuit.

SCA Resistance with IVR

Being a switching VR, transformations of inductive IVR can be useful for side-channel protection (Fig. 2) [23, 36]. The continuous switching of the power stage creates a strong pulsating current signature at the IVR input and impedes the

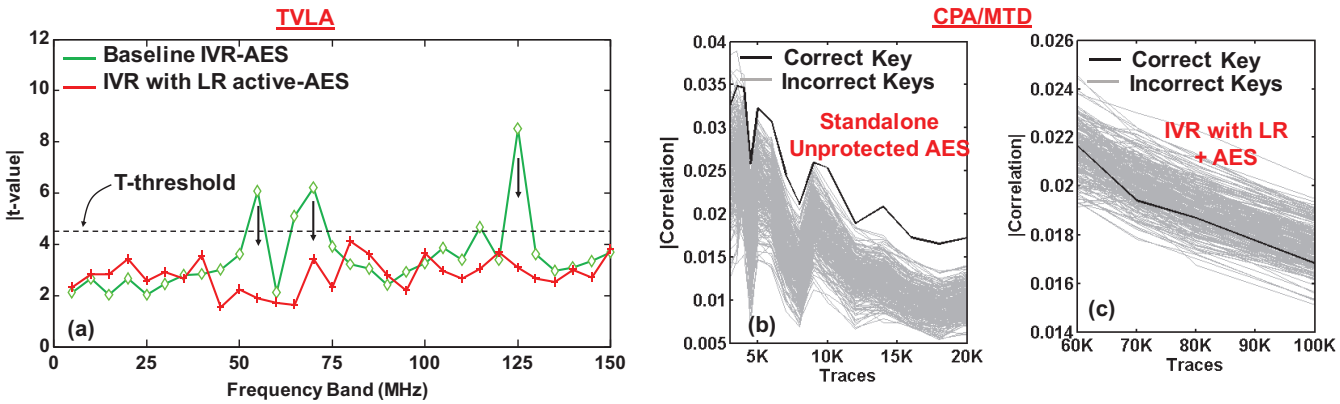


Fig 4. (a) TVLA analysis shows no leakage when LR is activated, CPA analysis for (b) unprotected AES and (c) with LR ON. When LR is ON, there is no successful CPA even with 100K measured traces [23, 36].

adversary in triggering a side-channel measurement. Similarly the asynchronous relation between the IVR switching clock and the digital clock impedes the attacker to properly align the measured signatures.

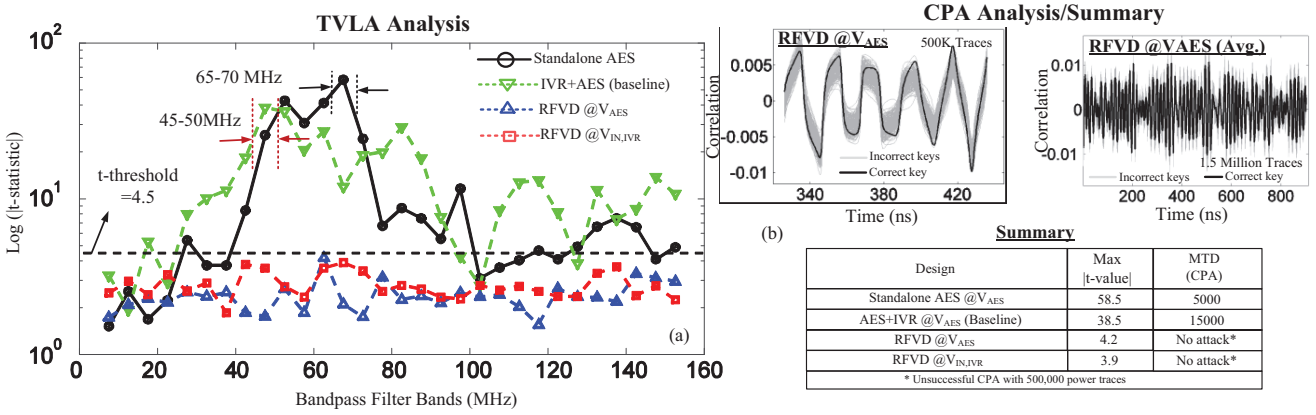
The coefficients of the digital PID filter and the limit-cycling behavior of the control loop in discontinuous conduction mode is used to improve the PSCA resistance. We can use an all-digital loop-randomizer (LR) which randomly delays the clock (using a maximal length LFSR) driving the power stage of the IVR and randomizes all three transformations [23, 36].

The standalone AES engine shows successful CPA with an MTD of 5000. Without activating LR, no successful CPA was observed with 100000 traces. However test-vector-leakage-assessment (TVLA) shows leakage with 10000 test vectors. After turning on the LR, not only no successful CPA was observed with 100000 traces, but the TVLA leakage disappears as well (Fig. 4). Turning on the LR increases the output ripple at the IVR output with 3.33% degradation in F_{MAX} and 5% increase in total power consumption of the IVR.

SCA Resistance with Random Fast Voltage Dithering

As discussed above, IVR with control loop randomization with LR can protect the input of IVR ($V_{IN,IVR}$) against side-channel attack, however, it doesn't offer any resistance at local supply node of AES (V_{AES}). V_{AES} may be accessible to external world for on-package or bondwire based inductors/passives. In this subsection, we demonstrate that we can offer enhancement in side-channel security for V_{AES} node also with random fast voltage dithering (RFVD) [24].

The concept of varying supply voltage of a target circuit around a nominal voltage is known as voltage dithering. As described in the Fig. 3(a&b), the RFVD scheme is very similar to DVFS and is implemented by randomly varying the reference word to the IVR controller in fast intervals (every 20 encryptions). IVR generates the corresponding output level and ADCM adjusts its clock output instantaneously thus introducing random shifts in the AES clock edges. As a result, both instantaneous frequency and phase of the AES clock are randomized. LFSR controlled tunable trimmer inside LM introduces additional randomness when enabled [Fig. 3(c) & 4(b)]. Randomness in clock edges translates to randomness in power consumption in amplitude and time direction ($P = \alpha.f.\frac{1}{2}CVDD^2$). Fig. 4(d) shows the measured, aligned and filtered waveforms for V_{AES} when RFVD scheme is enabled. Due to randomization, the waveforms are distorted and cannot be aligned correctly. Moreover, the variation in power is not



Design	Max |t-value|	MTD (CPA)
Standalone AES @V_{AES}	58.5	5000
AES+IVR @V_{AES} (Baseline)	38.5	15000
RFVD @V_{AES}	4.2	No attack*
RFVD @$V_{IN,IVR}$	3.9	No attack*

* Unsuccessful CPA with 500,000 power traces

Fig 6. (a) TVLA analysis across bands shows that leakage is suppressed when RFVD is enabled and (b) no successful CPA with 500K measurements. Even averaging 30 measurements with modified RFVD scheme did not produce any successful CPA [24].

only dependent on switching activity but also on supply voltage (VDD) and frequency of operation (f). Therefore, the correlation power analysis across several measurements is expected to become difficult (or not at all possible) when RFVD is enabled.

Fig. 6 shows the TVLA and CPA analysis results for AES with RFVD enabled. The baseline (AES+IVR) design shows very high leakage, expected for unprotected design while with RFVD, no leakage was detected at either V_{AES} or $V_{IN,IVR}$ as t-statistic goes below 4.5, showing a reduction of 9× with respect to baseline. Similarly, a successful attack was observed for baseline AES+IVR design with 15000 traces while no attack was successful when RFVD was enabled. Since adversary can average out multiple measurements for an encryption to remove random noise from the measured traces, RFVD scheme was modified to have the plaintext dependent reference word generation. With the modified scheme, no successful CPA was observed even with averaging of 30 measurements for 50,000 unique plaintexts (1.5 million total measurements) [24].

V. Conclusion

This paper discussed a fast DVFS scheme enabled with on-chip integrated IVR and ADCM circuit. Moreover, with measurement results from 130nm test-chip, it was shown that low power circuit techniques can not only improve energy efficiency of security circuits but also offer robustness against power side-channel analysis attacks. Security aware design techniques need to be adopted for tuning these low-power techniques to enhance side-channel security. Furthermore, dynamic activation of security aware control logic in presence of an adversary can minimize power and performance overheads associated with these techniques.

Acknowledgment

This material is based on work supported in part by Intel Corp. and National Science Foundation (CNS# 1218745).

VI. References

[1] J. Gubbi, et. al., “Internet of Things (IoT): A vision, architectural elements, and future directions”, Future Gen. Info. Systems’13.

[2] R. Weber, et. al., “Internet of Things – New security and privacy challenges”, Computer Law & Security Review’10.

[3] R. Roman, et. al., “A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes”, Mobile Networks & Applications’07.

[4] P. Chodowiec, et. al., “Very Compact FPGA Implementation of the AES Algorithm”, CHES’03.

[5] P. Kocher et. al. “Differential Power Analysis”, Advances in cryptology—CRYPTO’99.

[6] K. Gandolfi, et. al., “Electromagnetic analysis: Concrete results”, CHES’01.

[7] P. Kocher, et. al., “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems”, CRYPTO’96.

[8] Y. Bo, et. al., “An AES chip with DPA resistance using hardware-based random order execution”, Chinese Institute of Electronics, 2012.

[9] J. A. Ambrose, et. al. , “MUTE-AES: A multiprocessor architecture to prevent power analysis based side channel attack of the AES algorithm”, ICCAD’08.

[10] F. Ghellar, et. al., “A novel AES cryptographic core highly resistant to differential power analysis attacks”, Integ. Circuits & System Design’08

[11] J. Kaps, et. al., “DPA resistant AES on FPGA using partial DDL”, FCCM’10.

[12] E. Amouri, et. al, ”Balancing WDDL dual-rail logic in a tree-based FPGA to enhance physical security”, FPL’14.

[13] T. Popp, et. al., “Evaluation of the masked logic style MDPL on a prototype chip”, CHES’07.

[14] C. Tokunaga, et. al., “Secure AES engine with a local switched-capacitor current equalizer”, ISSCC’09.

[15] X. Wang, et. al., “Role of power grid in side channel attack and power-grid-aware secure design”, DAC’13.

[16] R. Menicocci, et. al., “Experiments on two clock countermeasures against power analysis attacks”, MIXDES’14.

[17] D. Suzuki and M. Saeki, "Security evaluation of DPA countermeasures using Dual-Rail Pre-Charge logic style," CHES’06.

[18] P. Pillai, et. al., “Real-time dynamic voltage scaling for low-power embedded operating systems”, SIGOPS’01.

[19] G. Semeraro, et. al., “Energy-efficient processor design using multiple clock domains with dynamic voltage and frequency scaling”, HPCA’02.

[20] N. Kurd, et al. "Haswell: A family of IA 22 nm processors." JSSC’15.

[21] K. Chae, et. al., “All-Digital Adaptive Clocking to Tolerate Transient Supply Noise in a Low-Voltage Operation”, TCASII’12.

[22] M. Floyd, et. al., “Adaptive Clocking in the POWER9TM Processor for Voltage Droop Protection”, ISSCC’17.

[23] M. Kar, et. al. "Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator," ISSCC’17.

[24] A. Singh, et. al., “Improved power side-channel attack resistance of a 128-bit AES engine with random fast voltage dithering”, ESSCIRC’17.

[25] V. Telandro, et. al., “On-chip voltage regulator protecting against power analysis attacks”, MWCAS’06.

[26] O. A. Uzun et. al., "Converter-Gating: A Power Efficient and Secure On-Chip Power Delivery System," JETCAS’14.

[27] M. Kar. et. al., “Impact of inductive integrated voltage regulator on the power attack vulnerability of encryption engines: A simulation study”, CICC’14.

[28] M. Kar, et. al., “Exploiting Fully Integrated Inductive Voltage Regulators to Improve Side-channel Resistance of Encryption Engines”, ISLPED’17.

[29] A. Singh et. al., "Exploring power attack protection of resource constrained encryption engines using integrated low-drop-out regulators," ISLPED’15.

[30] A. Singh et. al., "Integrated all-digital low-dropout regulator as a countermeasure to power attack in encryption engines," HOST’16.

[31] A. Singh, et. al., “Reducing Side-Channel Leakage of Encryption Engines Using Integrated Low-Dropout Voltage Regulators”, accepted at HaSS’17.

[32] D. Das, et. al., “High efficiency power side-channel attack immunity using noise injection in attenuated signature domain”, HOST’17.

[33] S. Yang, et al. "Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach." DATE’05.

[34] K. Baddam, et. al., “Evaluation of Dynamic Voltage and Frequency Scaling as a Differential Power Analysis Countermeasure”, VLSID’05.

[35] R Korkikian, et. al., “Instantaneous frequency analysis”, Cryptology’13.

[36] M. Kar, et. al., “Low power requirements and side-channel protection of encryption engines: Challenges and opportunities”, ISLPED’17.

[37] M. Kar, et. al., “What does ultra low power requirements mean for side-channel secure cryptography?”, ICCD’16.

[38] E. Brier, et. al., “Correlation power analysis with a leakage model”, CHES’04.

[39] https://csrc.nist.gov/CSRC/media/Events/Non-Invasive-Attack-Testing-Workshop/documents/08_Goodwill.pdf.

[40] M. Kar, et. al., “An all-digital fully integrated inductive buck regulator with a 250-MHz multi-sampled compensator and a lightweight auto-tuner in 130-nm CMOS”, JSSC’17.

[41] M. Kar, et. al., “An integrated inductive VR with a 250MHz all-digital multisampled compensator and on-chip auto-tuning of coefficients in 130nm CMOS”, ESSCIRC’16.