Efficient and Secure On-Chip Reconfigurable Voltage Regulation for IoT Devices

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

ABSTRACT

The emergence of internet of things (IoT) devices is challenging the conventional design targets for integrated systems such as performance, power efficiency, and cost. With the proliferation of IoT devices, ensuring safe operating margins will become more crucial due to the limited power budget and physical constraints. Additionally, IoT devices are vulnerable to hardware attacks as they may be easily accessible to an attacker. The limitations when combined with the cost constraints make the design of security measures for the IoT devices quite challenging. In this perspective paper, reconfigurable voltage regulators are investigated to simultaneously improve the overall power efficiency of the system and provide enhanced security against certain side-channel attacks. A brief survey of randomized reconfiguration of voltage regulators to scramble to power consumption profile is proposed. The randomized reconfiguration makes the the synchronization of the attack more difficult for the attacker, boosting the security benefits of conventional voltage regulators with negligible power and area overhead.

CCS Concepts

•**Hardware → Chip-level power issues;**

Keywords

Voltage regulation, power efficiency, hardware security, IoT

1. INTRODUCTION

With the advancement in the semiconductor technology in the last couple of years, the number of devices connected to the internet has increased significantly. It is projected that more than 50 billion internet of things (IoT) devices will be connected to the internet by the end of 2020, marking one of the fastest growing segment in the semiconductor industry [30]. The stringent design constraints for these IoT devices are challenging and changing the conventional design paradigms of power efficiency, area requirement, noise constraint, high performance, reliability, and security. Out of these design constraints, power management and security can be identified as the two primary challenges [30, 27].

Power management becomes challenging due to multiple factors stemming primarily from the limited available area, cost, power budget, and intermittent operation. In a system such as automotive, enterprise, and cloud services, several IoT devices are integrated, putting a significant constraint on the size and cost of these devices. The limited cost and size necessitate novel techniques for both battery technologies to increase the amount of charge that can be stored in unit area, circuit and architectural techniques to convert, regulate, and deliver the stored charge to the load circuits efficiently, and power management techniques and circuit architectures to increase performance per watt. The innovations in the battery technology to increase the amount of charge stored in unit area have been slower than the continuous demand for higher power consumption over the past decade. There is considerable amount of research on developing power management techniques to increase the performance per watt for IoT devices [30, 27]. In this paper, we will focus on circuit techniques that would potentially increase the power conversion efficiency from the battery to the load circuits as there is significant opportunity to increase the overall power efficiency of the system using a tailored power delivery system.

Security has also become a more important design constraint for IoT devices as these devices are highly accessible to malicious attacks (*i.e.,* side channel attacks) as compared to general purpose computing devices [30]. IoT devices should therefore provide sufficient level of security without significant area and performance overhead. To enhance security with negligible overhead, the existing components of a device can be designed and implemented in a security-aware fashion. As each active IoT device should house a voltage regulator/converter to either up/down convert/regulate the harvested energy or regulate the battery voltage to the load circuits, the leveraging of voltage regulators as a security primitive has been recently proposed [49]. We will investigate several voltage regulator topologies and summarize their propriety as a security primitive against certain side-channel attacks for IoT devices.

The rest of the paper is organized as follows. Background regarding on-chip voltage regulation and potential side-channel attacks is provided in Section 2. The most widely used three voltage regulator types are investigated in terms of their security and power efficiency characteristics for IoT devices in Section 3. The unique advantages and potential drawbacks

GLSVLSI '17, May 10–12, 2017, Banff, AB, Canada.

DOI: http://dx.doi.org/10.1145/3060403.3060496

of reconfigurable voltage regulators for IoT devices are explored in Section 4. Conclusions are offered in Section 6.

2. BACKGROUND

Ensuring a robust communication between several *things* is a key design constraint for IoT devices. Equally important is the efficient analysis, computation, storage of the data that are obtained from the environment or from other connected devices. To maintain a robust communication and efficient computation while also reducing the cost of the packaging, on-chip voltage regulation is more of a necessity than luxury for IoT devices [30].

2.1 On-chip voltage regulation

Over the past decade, fortunately, there is significant amount of research focusing on the development of fully integrated on-chip voltage regulators to down-convert and regulate the voltage at the point-of-load for general purpose computing devices [41, 21, 31, 39, 15, 4, 1, 16, 19]. There are several advantages of on-chip voltage regulation. First, the number of dedicated pins for power/ground can be reduced as the power is delivered at a higher voltage and lower current level, liberating some of the pins which can be used for signaling and other purposes. Second, the response time to transient changes in the load is improved as the voltage regulator is physically closer to the load circuits, reducing the parasitic impedance in between. Additionally, the control loop of a voltage regulator is faster due to the lower parasitic impedances, improving the response time. Third, power management techniques such as dynamic voltage scaling can be performed faster (*i.e.,*fine granular), potentially paving the way for significantly improving power efficiency for devices that perform intermittent computation. Fourth, more number of voltage levels can be generated that are tailored for different heterogeneous techniques that can be housed in a single IoT device. This will potentially reduce the cost of multiple voltage regulators integrated at the package, each of which generates a different voltage level that is delivered through dedicated pins [18, 5].

The number of on-chip voltage regulators on a single die also increases significantly owing to the high power densities that can be achieved by leveraging advanced capacitance technologies such as the trench capacitors that are available for DRAM cells in certain processes. For example, IBM's high end server processor Power8 houses hundreds of digital low dropout regulators that are sprinkled throughout the die [9]. Intel also utilizes multi-phase buck converters that have output stages distributed across the die [5] in the Haswell processor. The number of voltage regulators in IoT devices has also increased recently as ARM [26], Intel [6, 25], and Samsung [24] have fabricated prototype IoT devices with multiple integrated voltage regulators.

There is considerable amount of recent research on voltage regulators with reconfigurable topologies [29, 8, 43, 23, 22, 37, 5]. The primary objectives of reconfigurable voltage regulators are to maintain a high power conversion efficiency for a wider range of output currents and enable multiple voltage conversion ratios with the same circuitry that can generate different supply voltage levels [37, 8]. More than half of the voltage regulator designs presented in ISSCC'16 have reconfigurable features [8, 43, 7, 20]. The reconfigurable voltage regulators either change some of the connections at runtime to change the voltage conversion ratio Vout=Vin [29, 8, 43] or turn-on and turn-off certain regulator stages to save power during low power modes of operation [23, 22, 37, 5].

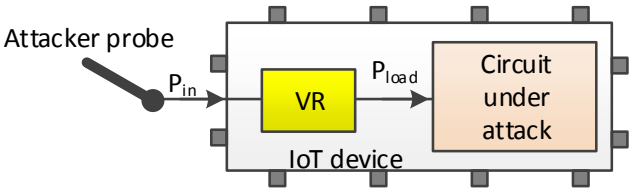

Figure 1: On-chip voltage regulators can disrupt the correlation between the leakage power consumption P_{out} and the monitored power consumption P_{in} by a malicious attacker.

2.2 Side-channel attacks

Non-invasive side-channel attacks are performed to extract information from an integrated circuit (IC) or a smart card by monitoring different physical leakage sources such as power consumption, timing information, temperature, electromagnetic (EM) emanations, and acoustic waves while loading/executing/storing information. The side-channel leakage of a circuit depends on and contains information about i) the data that the circuit is processing and ii) the operations that the circuit is performing while processing data. Due to the low cost and non-invasive nature, side-channel attacks pose a serious threat to the security of personal, commercial, and military information. Unfortunately, IoT devices are inherently more vulnerable to side-channel attacks as compared to general purpose devices as IoT devices are typically more accessible to an attacker.

Power analysis attacks are a widely used side-channel attack that exploits the data dependence of the power consumption profile due to the asymmetric power consumption of the $(0 \rightarrow 1)$ and $(1 \rightarrow 0)$ transition in CMOS circuits. The power delivery network of an IC has a significant impact on the side-channel power leakage profile [44, 11, 33]. Thus, the design of power delivery network has a significant impact on the side-channel power leakage profile. A security-aware power delivery network therefore greatly enhances the trustworthiness of critical systems. Several countermeasures have been proposed against power analysis attacks which typically either significantly increase the power consumption [36] or cause considerable area overhead [10]. The role of the on-chip power delivery network against power analysis attacks has been investigated in [44].

3. ON-CHIP VOLTAGE REGULATORS FOR SECURITY AND EFFICIENCY

Recently, on-chip voltage voltage regulators have attracted significant attention as a countermeasure against power analysis attacks [35, 11, 33, 14, 34, 12, 13]. While conventional voltage regulators provide a certain level of security against power analysis attacks, reconfigurable voltage regulators have been investigated as a countermeasure to further enhance security [45, 46, 48, 47]. The reason why on-chip voltage regulators naturally increase security against power analysis attacks is that they serve as a circuit block that can modify the media communication channel between the attacker and the circuit under attack, as shown in Fig. 1. IoT devices typically house at least one voltage regulator. When

these existing voltage regulators are designed in a security-aware fashion as a countermeasure against side-channel attacks, the power, performance, area, and design time overheads can be significantly reduced while ensuring a higher level of security.

Three types of voltage regulators are widely used in modern ICs to down-convert the voltage; namely low dropout (LDO) regulator, switched capacitor voltage converters, and buck converters. The related tradeoffs of these voltage regulator topologies are explained in the following subsections.

3.1 Leveraging low dropout regulators

LDO regulators are linear voltage regulators with a quite low dropout voltage (*i.e.,* voltage difference between input voltage V_{in} and output voltage V_{out} of the regulator). Although the power efficiency of LDO regulators is limited to V_{out}/V_{in}, when the dropout voltage is small, these regulators can achieve over 90% efficiency. Recently, digital LDO (D-LDO) regulators have attracted significant attention from the industry [9].

LDO regulators can effectively be utilized as a countermeasure against power analysis, as shown in [33, 34, 14] where the authors model the transfer function of the LDO regulator both in frequency and time domains. Although LDO regulators can increase the immunity against side-channel attacks, LDO regulators may still leak information regarding the operating frequency of the circuit-under-attack [48].

3.2 Leveraging buck converters

Buck converters utilize a second order inductor-capacitor (LC) filter to remove the high frequency components of the input switching signal and generate a DC output voltage with a certain amount of ripple voltage. The input switching signal is typically generated by a pulse width modulator (PWM) [40] to adaptively control the duty cycle of the switching signal to regulate the output voltage level. Buck converters can provide quite high power conversion efficiency even when the voltage conversion ratio (*i.e.*, V_{out}/V_{in}) is low. The primary problem with buck converters for on-chip integration is the inductor which requires a large chip area with a reduced quality-factor [42]. The inductors can be implemented at the package right above the IC, as performed recently by Intel [5].

Buck converters have also been explored as a potential side-channel attack countermeasure [11, 12, 13]. The delay loop and the compensator pole-zero locations are controlled to increase the security of the buck converter, however, with some power conversion efficiency degradation. The required number of measurements to disclose (MTD) the correct key from an AES encryption engine has increased over 400 times with a security-aware design of buck converter [12]. Although the buck converters can increase the security against power analysis attacks, certain level of information related to the supply voltage of the circuit-under-attack can still leak to the attacker if the attacker analyzes the slope of the inductor current [48].

3.3 Leveraging switched capacitor voltage converters

SC voltage converters utilize a flying capacitor network and several switches that control the charge transfer from the input node to the flying capacitor and from the flying capacitor to the output node. When the charging of the flying capacitor from the input node and the discharging to the output node occur at a considerably high frequency, a steady voltage with certain amount of ripple can be generated at the output node. Similar to buck converters, the power efficiency of SC converters can be quite high even when the voltage conversion ratio V_{out}/V_{in} is low. With the recent advancements in capacitor density improvements, high power density SC converters can be integrated on-chip without significant area overhead [2, 32].

SC converters can also provide increased security against power analysis attacks similar to LDO and buck converters [37, 49, 45, 46, 47]. The main advantage of SC converters over LDO and buck converters is that SC converters neither leak the supply voltage nor the clock frequency of the circuit-under-attack. This advantage is important when a type of voltage/frequency scaling (VFS) scheme is employed as a countermeasure against power analysis attacks where the leakage if either supply voltage level or the frequency can nullify the VFS based countermeasures [48].

4. RECONFIGURABLE VOLTAGE REGULATION FOR IOT DEVICES

IoT devices may perform different functionalities such as image capturing and processing, computation, monitoring the environment with different sensors, and communication. Performing these diverse functions within a single IoT device may necessitate a heterogeneous integration of different technologies in a single die using 3-D or 2.5-D integration. Each technology can operate optimally at a specific supply voltage level. Delivering various levels of supply voltage to diverse technologies can be facilitated by reconfigurable voltage regulators. Reconfigurable voltage regulation is particularly beneficial for IoT devices (as compared to general purpose computing devices) due to their intermittent operation. The voltage regulator can provide supply voltage at a specific level to a circuit block during its intermittent operation and can change voltage conversion ratio at runtime to generate a different voltage level to power another circuit block.

We investigate reconfigurable voltage regulators for IoT devices in terms of power efficiency, cost, and security implications in the following subsections.

4.1 Power efficiency benefits of reconfigurable regulators

The primary benefit of reconfigurable voltage regulation is the increased power conversion efficiency under a wide range of load power consumption from idle to high-power modes of operation. One technique to realize a reconfigurable voltage regulator is to turn-on and turn-off certain stages of a multi-phase switched capacitor or buck converter [5] or activate and deactivate a certain number of stages of parallel connected LDO regulators [17, 38]. One of the challenges in IoT devices is to generate a stable supply voltage from a battery which delivers a variety of voltage levels based on the amount of charge stored [8, 43]. A high power conversion efficiency and robust supply voltage can be easily generated with a reconfigurable voltage regulator without sacrificing the speed of the transient load response[8].

Another objective of reconfigurable voltage regulators is to improve the transient response speed by reconfiguring the regulator during the transients. When the load current

demand increases abruptly, the voltage regulator can configure itself with a higher voltage conversion ratio during the transients and reconfigure to the actual conversion ratio immediately after the transient [37]. Another reason for the load voltage drop is an abrupt change in the input voltage level. Accordingly, an SC reconfigurable voltage regulator is proposed in [3] that adaptively changes the voltage conversion ratio to mitigate the output voltage drop during input voltage changes. Since IoT devices may encounter instant changes both in the input voltage of the regulator and in the load current demand, reconfigurable voltage regulators would potentially enhance the robustness of IoT devices.

4.2 Cost benefits of reconfigurable regulators

The output voltage of a battery and the power generated by energy harvesting circuitry vary significantly over time depending, respectively, on the remaining charge of the battery and the input power to the energy harvesting circuitry. To generate a stable voltage level to be delivered to the active circuits, specialized interface circuitry is typically utilized [28, 6]. With reconfigurable voltage regulators, the design specifications can be considerably relaxed for the output of the battery voltage. Accordingly, the specialized circuits that up- or down-convert the voltage level, which the voltage regulator can handle, may no longer be needed for a robust operation.

4.3 Security benefits of reconfigurable regulators

Although reconfigurable voltage regulators have been proposed to enhance the power conversion efficiency and increase the response speed, a major side-benefit of reconfiguring a voltage regulator is the increased security against side-channel attacks. Noteworthy is that an attacker exploits the dependence of the power consumption of the circuit on the processed secret key. The reconfiguration of the voltage regulator topology at runtime disrupts the correlation between the input and output power of the regulator. Reconfiguring the voltage regulator therefore adds a non-trivial time-dependent parameter to the power consumption signature, significantly increasing the number of measurements that is required by an attacker to determine the secret key [37, 49].

Converter-gating (CoGa) technique based on a multi-phase SC based reconfigurable voltage regulator is proposed as a countermeasure against power analysis attacks in [37]. The number of active SC stages is determined that maximizes the power conversion efficiency based on the workload requirement. Given the number of active stages that maximizes the power efficiency, a pseudo random number generator (PRNG) then decides which stages need to be active. Since each regulator stage is driven by a different phase of the input clock signal, the signature of input power profile of the regulator has spikes with delay uncertainty. Although a delay uncertainty of $\sim$20 ns is added to the input power signature in [37], this delay uncertainty can be increased by modifying the switching frequency of the SC voltage regulator.

One of the drawbacks of CoGa technique is that if the attacker performs an attack while keeping the power consumption of the circuit too low to trigger any change in the number of required voltage regulator stages, CoGa technique can be bypassed. Converter-reshuffling (CoRe) technique is proposed in [49] to overcome this drawback by periodically shuffling the active and inactive stages while keeping the number of active stages the same. When there is a considerable change in the power consumption, the number of active stages is increased and shuffling operation continues. A time delayed CoRe technique is proposed by adding another PRNG in [45] to make the synchronization with the regulator frequency more difficult for the attacker, increasing the security against machine learning based side-channel attacks. In a conventional multi-phase SC regulator, all of the flying capacitors are discharged to the output node after every switching cycle. A charge withheld CoRe technique is proposed in [46] to charge a higher number of flying capacitors than needed and randomize the discharging of those flying capacitors to the output node by discharging them a couple of cycles later.

5. DISCUSSION

The reconfigurable voltage regulators increase the power trace entropy (PTE) value of the voltage regulator 40 to 60% as compared to conventional voltage regulators. Additionally, there is a risk of bypassing and nullifying the security benefits of the voltage regulators if the attacker knows the impedance characteristics of the voltage regulator. Although the impedance characteristics strongly depend on the workload information and loosely on the environmental conditions, a simple voltage regulator model can be used. In such a case, the attacker can post-process the monitored power signature data based on the voltage regulator characteristics and increase the correlation between the input and output power profiles of the voltage regulator (*i.e.*, reduce the PTE). Although the process, temperature, and environmental (PTE) variations affect the impedance characteristics of the voltage regulators, their impact on the attacker might be quite limited.

Reconfigurable voltage regulators, however, do not depend on the PTE variations or on the changes in the workload to alter the regulator characteristics, but depend strongly on the reconfiguration of the topology that changes the impedance characteristics at runtime. As explained in Section 4.3, randomness can also be inserted during the reconfiguration process without sacrificing the power efficiency. Since reconfigurable voltage regulation simultaneously improves the power conversion efficiency and security, unlike most of the countermeasures, the power overhead of the reconfigurable voltage regulation is negligible.

6. CONCLUSION

Maintaining high power efficiency while enhancing security is the primary design challenge that IoT devices face. On-chip voltage regulators can be leveraged as a countermeasure against power analysis attacks with negligible area and power overhead. Different voltage regulator topologies are investigated based on their power efficiency and security. The power efficiency and security benefits of the voltage regulators can be significantly enhanced with reconfigurable voltage regulation. Various techniques that utilized reconfigurable voltage regulators for both power efficiency and security are investigated. The reconfiguration can be performed in a randomized fashion to provide increased security while conserving the power efficiency benefits.

7. ACKNOWLEDGMENTS

The author would like to thank Dr. Weize Yu for his help. This work is supported in part by the National Science Foundation CAREER award under Grant CCF-1350451, by the USF Presidential Fellowship, by a Cisco Research Award, and by a seed grant from Florida Center for Cybersecurity (FC^2).

8. REFERENCES

[1] E. Alon and M. Horowitz. Integrated regulation for energy-efficient digital circuits. *IEEE Journal of Solid-State Circuits*, 43(8):1795–1807, August 2008.

[2] 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. In *Proceedings of the IEEE International Applied Power Electronics Conference and Exposition*, pages 692–699, March 2013.

[3] T. M. Andersen et al. A feedforward controlled on-chip switched-capacitor voltage regulator delivering 10w in 32nm soi cmos. In *International Solid-State Circuits Conference*, pages 1–3, February 2015.

[4] 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*, 8(3):299–316, March 2000.

[5] E. A. Burton et al. Fivr - fully integrated voltage regulators on 4^{th} generation intel core socs. In *Proceedings of the IEEE International Applied Power Electronics Conference and Exposition*, pages 432–439, March 2014.

[6] S. Carreon-Bautista, L. Huang, and E. Sanchez-Sinencio. An autonomous energy harvesting power management unit with digital regulation for iot applications. *IEEE Journal of Solid-State Circuits*, 51(6):1457–1475, June 2016.

[7] P. R. D. Lutz and B. Wicht. A 10mw fully integrated 2-to-13v-input buck-boost sc converter with 81.5% peak efficiency. In *International Solid-State Circuits Conference*, pages 224–225, February 2016.

[8] W. J. et al. A 60%-efficiency 20nw-500μw tri-output fully integrated power management unit with environmental adaptation and load-proportional biasing for iot systems. In *International Solid-State Circuits Conference*, pages 154–155, February 2016.

[9] E. Fluhr et al. The 12-core power8 processor with 7.6 tb/s io bandwidth, integrated voltage regulation, and resonant clocking. *IEEE Journal of Solid-State Circuits*, 50(1):10–23, January 2015.

[10] D. Hwang, K. Tiri, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede. Aes-based security coprocessor ic in 0.18-um cmos with resistance to differential power analysis side-channel attacks. *IEEE Journal of Solid-State Circuits*, 41(4):781–792, April 2006.

[11] M. Kar, D. Lie, M. Wolf, V. De, and S. Mukhopadhyay. Impact of inductive integrated voltage regulator on the power attack vulnerability of encryption engines: A simulation study. In *Proceedings of the IEEE Custom Integrated Circuits Conference*, pages 1–4, September 2014.

[12] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay. Exploiting fully integrated inductive voltage regulators to improve side channel resistance of encryption engines. In *Proceedings of the IEEE/ACM International Symposium on Low Power Electronics and Design*, pages 130–135, August 2016.

[13] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay. Improved power-side-channel-attack resistance of an aes-128 core via a security-aware integrated buck voltage regulator. In *International Solid-State Circuits Conference*, February 2017.

[14] M. Kar, A. Singh, A. Rajan, V. De, and S. Mukhopadhyay. What does ultra low power requirements mean for side-channel secure cryptography? In *Proceedings of the IEEE International Conference on Computer Design*, pages 686–689, October 2016.

[15] W. Kim, D. Brooks, and G.-Y. Wei. A fully-integrated 3-level dc-dc converter for nanosecond-scale dvfs. *IEEE Journal of Solid-State Circuits*, 47(1):206–219, January 2012.

[16] W. Kim, M. S. Gupta, G.-Y. Wei, and D. Brooks. System level analysis of fast, per-core dvfs using on-chip switching regulators. In *Proceedings of the IEEE International Symposium on High Performance Computer Architecture*, pages 123–134, February 2008.

[17] S. Kose. Regulator-gating: Adaptive management of on-chip voltage regulators. In *Proceedings of the ACM/IEEE Great Lakes Symposium on VLSI*, pages 105–110, May 2014.

[18] S. Kose and E. G. Friedman. Distributed on-chip power delivery. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 2(4):704–713, December 2012.

[19] 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*, 21(4):680–691, April 2013.

[20] J. G. L. L. G. Salem and P. P. Mercier. A flying-domain dc-dc converter powering a cortex-m0 processor with 90.8% efficiency. In *International Solid-State Circuits Conference*, pages 234–235, February 2016.

[21] 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*, 39(1):3–14, January 2004.

[22] W. Lee, Y. Wang, and M. Pedram. Optimizing a reconfigurable power distribution network in a multicore platform. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 34(7):110–1123, July 2015.

[23] W. Lee et al. Power conversion efficiency characterization and optimization for smartphones. In *Proceedings of the IEEE/ACM International Symposium on Low Power Electronics and Design*, pages 103–108, July-August 2012.

[24] Y. J. Lee et al. A 200ma digital low-drop-out regulator with coarse-fine dual loop in mobile

application processors. In *Proceedings of the IEEE International Solid-State Circuits Conference*, pages 150–151, February 2016.

[25] X. Liu, L. Huang, K. Ravichandran, and E. Sánchez-Sinencio. A highly efficient reconfigurable charge pump energy harvester with wide harvesting range and two-dimensional mppt for internet of things. *IEEE Journal of Solid-State Circuits*, 51(5):1302–1312, May 2016.

[26] J. Myers et al. A subthreshold arm cortex-m0+ subsystem in 65 nm cmos for wsn applications with 14 power domains, 10t sram, and integrated voltage regulator. *IEEE Journal of Solid-State Circuits*, 51(1):31–44, January 2016.

[27] A. M. Nia and N. K. Jha. A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing*, 2017.

[28] Y. K. Ramadass and A. P. Chandrakasan. A battery-less thermoelectric energy harvesting interface circuit with 35 mv startup voltage. *IEEE Journal of Solid-State Circuits*, 46(1):333–341, January 2011.

[29] Y. K. Ramadass, A. A. Fayed, and A. P. Chandrakasan. A fully-integrated switched-capacitor step-down dc-dc converter with digital capacitance modulation in 45 nm cmos. *IEEE Journal of Solid-State Circuits*, 45(12):2557–2565, December 2010.

[30] S. Ray, Y. Jin, and A. Raychowdhury. The changing computing paradigm with internet of things: A tutorial introduction. *IEEE Design and Test of Computers*, 33(2):76–96, February 2016.

[31] S. Rusu et al. A 65-nm Dual-Core Multithreaded Xeon® Processor with 16-MB L3 Cache. *IEEE Journal of Solid-State Circuits*, 42(1):17–25, January 2007.

[32] S. R. Sanders, E. Alon, H.-P. Le, M. D. Seeman, M. John, and V. W. Ng. The road to fully integrated dc-dc conversion via the switched-capacitor approach. *IEEE Transactions on Power Electronics*, 28(9):4146–4155, September 2013.

[33] A. Singh, M. Kar, J. H. Ko, and S. Mukhopadhyay. Exploring power attack protection of resource constrained encryption engines using integrated low-dropout regulators. In *Proceedings of the IEEE/ACM International Symposium on Low Power Electronics and Design*, pages 134–139, July 2015.

[34] A. Singh, M. Kar, A. Rajan, V. De, and S. Mukhopadhyay. Integrated all-digital low-dropout regulator as a countermeasure to power attack in encryption engines. In *Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust*, pages 145–148, May 2016.

[35] V. Telandro, E. Kussener, A. Malherbe, and H. Barthelemy. On-chip voltage regulator protecting against power analysis attacks. In *Proceedings of the IEEE International Midwest Symposium on Symposium on Circuits and Systems*, pages 507–511, August 2006.

[36] C. Tokunaga and D. Blaauw. Securing encryption systems with a switched capacitor current equalizer. *IEEE Journal of Solid-State Circuits*, 45(1):23–31, January 2010.

[37] 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*, 4(7):169–179, June 2014.

[38] O. A. Uzun and S. Kose. Regulator-gating methodology with distributed switched capacitor voltage converters. In *Proceedings of the IEEE Computer Society Annual Symposium on VLSI*, pages 13–18, July 2014.

[39] V. Pinon, B. Allard, and C. Garnier. High Frequency Monolithic DC/DC Converter for System-on-Chip Power Management. In *Proceedings of the IEEE International Symposium on Power Semiconductor Devices and ICs*, pages 1–4, June 2006.

[40] I. Vaisband, M. Azhar, S. Kose, and E. G. Friedman. Digitally controlled pulse width modulator for on-chip power management. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 22(12):2527–2534, December 2014.

[41] I. Vaisband, R. Jakushokas, M. Popovich, A. V. Mezhiba, S. Köse, and E. G. Friedman. *On-Chip Power Delivery and Management, Fourth Edition*. Springer, 2016.

[42] G. Villar-Pique, H. J. Bergveld, and E. Alarcon. Survey and benchmark of fully integrated switching power converters: Switched-capacitor versus inductive approach. *IEEE Transactions on Power Electronics*, 28(9):4156–4167, September 2013.

[43] D. S. W. Jung and D. Blaauw. A rational-conversion-ratio switched-capacitor dc-dc converter using negative-output feedback. In *International Solid-State Circuits Conference*, pages 218–219, February 2016.

[44] 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 *Proceedings of the IEEE/ACM Design Automation Conference*, pages 1–9, May 2013.

[45] W. Yu and S. Kose. Time-delayed converter-reshuffling: An efficient and secure power delivery architecture. *IEEE Embedded Systems Letters*, 7(3):73–76, September 2015.

[46] W. Yu and S. Kose. Charge-withheld converter-reshuffling (core): A countermeasure against power analysis attacks. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 63(5):438–442, May 2016.

[47] W. Yu and S. Kose. A voltage regulator-assisted lightweight aes implementation against dpa attacks. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 63(8):1152–1163, August 2016.

[48] W. Yu and S. Kose. Exploiting voltage regulators to enhance various power attack countermeasures. *IEEE Transactions on Emerging Topics in Computing*, March 2017.

[49] W. Yu, O. A. Uzun, and S. Kose. Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks. In *Proceedings of the IEEE/ACM Design Automation Conference*, pages 1–6, June 2015.