Leveraging On-Chip Voltage Regulators Against Fault Injection Attacks

Ali Vosoughi
mvosough@ur.rochester.edu
Department of Electrical and Computer Engineering
University of Rochester
Rochester, New York

Selçuk Köse
selcuk.kose@rochester.edu
Department of Electrical and Computer Engineering
University of Rochester
Rochester, New York

ABSTRACT

The security implications of utilizing an on-chip voltage regulator as a countermeasure against fault injection attacks are investigated in this paper. The effect of the size of the capacitors and number of phases of the voltage regulator on the resilience of a cryptographic circuit against fault injection attacks are analyzed. The effectiveness of the proposed method in counteracting voltage glitch attacks is demonstrated with extensive simulations on the S-box of an advanced encryption standard (AES) cryptographic algorithm. Using a single phase on-chip voltage regulator, the number of faults generated by a voltage glitch attack is reduced by 5.45% as compared to unprotected S-box, and by 91.82% when number of phases increases to 32.

CCS CONCEPTS

• **Hardware → Integrated circuits**; **Power and energy**; **Energy distribution**; **Power conversion**; **Robustness**; **System-level fault tolerance**.

KEYWORDS

Hardware security; voltage regulator; fault injection attack; multi-phase voltage regulator

ACM Reference Format:
Ali Vosoughi and Selçuk Köse. 2019. Leveraging On-Chip Voltage Regulators Against Fault Injection Attacks. In *Great Lakes Symposium on VLSI 2019 (GLSVLSI '19), May 9–11, 2019, Tysons Corner, VA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3299874.3317978

1 INTRODUCTION

Side-channel attacks are an important class of attacks aimed at breaking the secrets of a cryptographic circuit (CC) and threatening the security of cryptographic devices. In side-channel attacks, the physical emanations leaked from an integrated circuit is used to obtain the correct key that is stored within a CC [1–4]. For example, the correct key of an AES cryptographic algorithm can be obtained in a few minutes with a side-channel attack, however, using the supercomputers and the brute force search can take 149 trillion years to get the correct key [5].

Active side-channel attacks are a class of side-channel attacks to obtain the correct key by making transient (or permanent) changes to the CC and analyzing the output of the CC under those changes. In these attacks, which are known as fault injection attacks, the attacker causes a fault in the CC in various ways and exploits the fault analysis tools, such as differential fault analysis (DFA) [6], safe error analysis (SEA) [7], and collision fault analysis (CFA) [8] to obtain the key.

There are various methods for fault injection, such as injecting faults by voltage glitch injection, voltage starving, overvoltaging, injecting intentional temperature variations, white light, and laser radiation to the CC [9, 10]. Different methods require a different level of attacker skills and equipment [9, 10]. Voltage glitch attack (VGA) is a fault injection method that the attacker creates a fault in the CC through a sudden change, positive or negative, in the supply voltage of a CC [9–13]. VGA is used in a fault injection attack on the RSA device in the presence of countermeasures in [12]. VGA is exerted to inject the faults in unprotected RFID tags in [11].

Various techniques have been proposed to counteract fault injection attacks. Information redundancy-based techniques such as error correcting codes are a class of countermeasures against fault injection attack by encoding information flowing through the CC [14, 15]. Spatial redundancy-based countermeasures are a class of countermeasures which use the duplication/multiplication of the hardware of the CC to ensure the accuracy of the output through majority voting, and temporal redundancy based countermeasures verify the output through repetition of (part of) the cryptographic algorithm in time. Even though these countermeasures are advantageous in countering fault injection attacks, spatial, temporal, and information redundancies will lead to increased power dissipation of CC, reduced throughput, and increased area of the CC [9, 10, 12, 16]. Alternatively, analog countermeasures, such as voltage, temperature, and frequency sensors, are used to detect malicious fault injection activities and to protect a CC by ceasing the operations if such an activity is detected [9, 12, 17]. Detection of dynamic supply voltage variations has been used in [18]. Timing detectors are used to detect the glitches in [17] as a digital solution to counteract the VGA within a specific voltage and clock range. To the best of the knowledge of the authors, the on-chip VR has never been used as an inherent countermeasure against fault injection attacks. This paper is the first work to utilize the existing resources of an on-chip VR as a countermeasure against voltage glitch attacks where the implications of on-chip VR and the number of phases are investigated in counteracting voltage glitch attacks.

GLSVLSI '19, May 9–11, 2019, Tysons Corner, VA, USA

ACM ISBN 978-1-4503-6252-8/19/05…$15.00
https://doi.org/10.1145/3299874.3317978

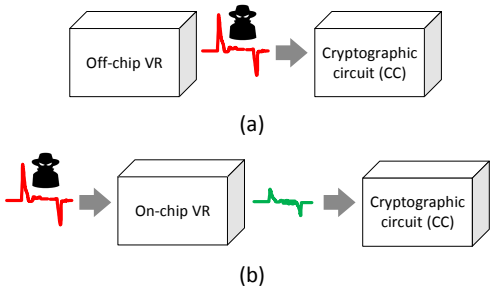

Figure 1: A voltage glitch attack to the CC a) without on-chip VR and b) with an on-chip VR.

The rest of this paper is as follows. In Section 2, the advantage of the on-chip VR on the resilience of CC against VGA is discussed and the effect of the capacitor size is analyzed. In Section 3, the effect of increasing the number of phases in the robustness of the CC to the VGA is investigated. In Section 4, extensive practical evaluations on the S-box of an AES with and without an on-chip VR is presented, followed by discussions on the overhead of the proposed countermeasure and conclusions.

2 ON-CHIP VR AGAINST VGA

An integrated circuit with an off-chip power supply is shown to be susceptible to side-channel analysis for key extraction [19]. The use of an on-chip voltage converter is shown to improve the security of CC against power and EM analysis attacks [20–24]. Intuitively, the on-chip VR is the first defense mechanism of a CC against side-channel attacks. Various topologies of VR, such as low-drop-out (LDO), buck, and switched capacitor (SC), have different responses against VGA based on the component selection and fabrication technology. These differences affect how the voltage glitch reaches the CC. Each VR, inherently acts as a low-pass filter that eliminates high-frequency inputs. A fault injection attack through voltage glitch to the CC in the presence of an on-chip VR and without on-chip VR is shown in Fig. 1. The f_{-3dB} frequency of the VR and related frequency response depend significantly on the design of the VR and the number of effective reactive elements (*i.e.* inductors and capacitors). For example, a buck VR has two reactive components and thus is at least a second-order low-pass filter, as shown in Fig. 2a, while an LDO has only one reactive component and is inherently a first-order low-pass filter, as shown in Fig. 2b. Therefore, the expected amount of attenuation of high-frequency inputs in the stop-band of the buck VR will be higher than LDO. A switched-capacitor (SC) VR, has one or more number of effective capacitors depending on the configuration, as shown in Fig. 2c. The first-order low-pass filter is selected as the equivalent model of the low-pass behavior of a VR, as shown in Fig. 3.

The amount of energy transferred by the capacitor C_{eq} to the output is equal to $\frac{1}{2}C_{eq}(\Delta V_{C_{eq}})^2$, where $\Delta V_{C_{eq}}$ is the voltage difference on the C_{eq}. If C_{eq} increases, the amount of voltage glitch energy transferred through the VR to the CC also increases. Alternatively, with larger C_{eq}, the cutoff frequency $f_{-3dB} = (2\pi R_{eq}(C_{eq} + C_{out}))^{-1}$ of VR is reduced. However, this is provided that the glitch frequency is higher than the cutoff frequency of the VR. With larger C_{eq}, the cutoff frequency f_{-3dB} is reduced and the filtering of the high frequency glitches is improved, while the amount of glitch energy transferred by the VR also increases with respect to $\frac{1}{2}C_{eq}(\Delta V_{C_{eq}})^2$. The relationship between the capacitance of the VR and the glitch energy transmitted to the CC is shown in Fig. 4.

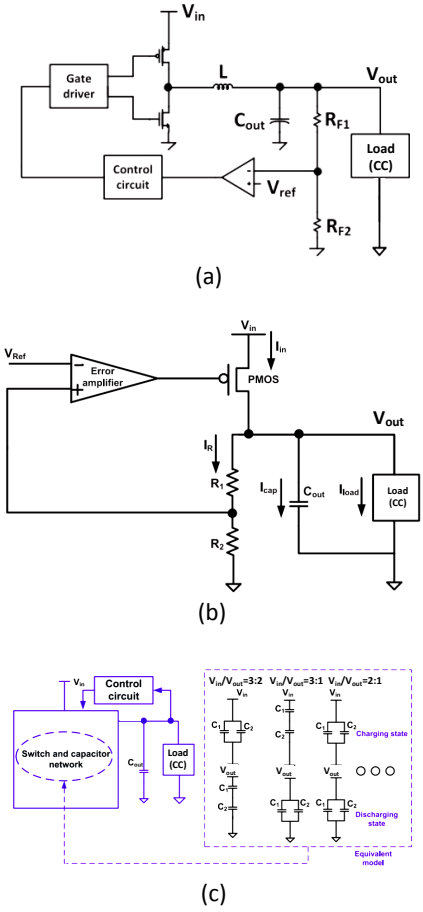

Figure 2: Schematic of a) a conventional Buck VR with two reactive components, b) a conventional LDO VR with one reactive component, and c) a conventional SC-VR with a capacitor network.

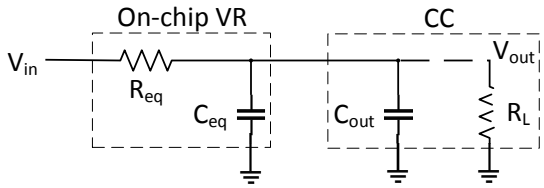

Figure 3: A general, simplified first-order model for behavior of a VR as a low-pass filter (LPF) for input signals. R_{eq} and C_{eq} are equivalent resistive and capacitive impedance of on-chip VR.

3 MULTI-PHASE VR AGAINST VGA

In addition to the topology, component selection, and scaling, the number of phases of a VR has a significant impact on the resilience of a CC against a VGA. The amount of energy inserted into a CC during a VGA can significantly change the success rate of attack[17].

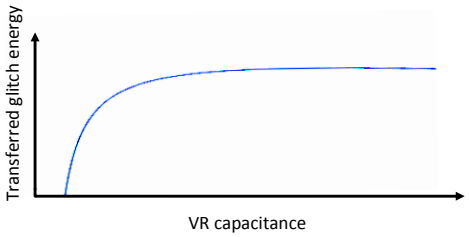

Figure 4: Relation of C_{eq} and voltage glitch transmitted to the CC. By increasing C_{eq}, the glitch transferred to the CC increases unto the cut-off frequency of the VR, where the increase of the C_{eq} makes a negligible impact on the transferred glitch energy.

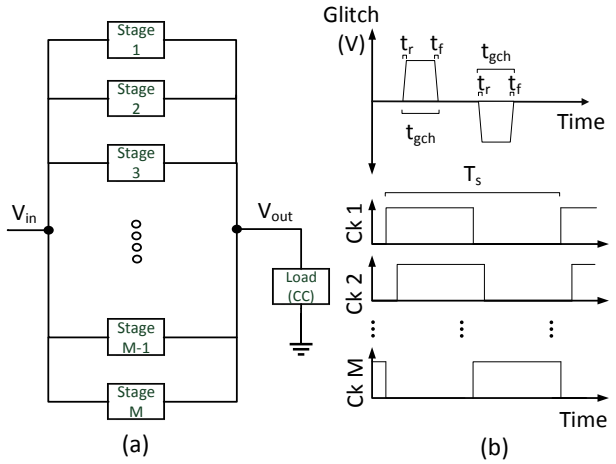

Figure 5: Schematic of a) an MPVR with M phases, and b) glitches of the VGA and clocks of the MPVR are depicted. The glitch has trapezoid shape with rise time t_r, fall time t_f, and duration t_{gch}.

The amount of energy depends on the duration and amplitude of a glitch[17]. For a switching circuit, the duration of a glitch attack changes the effectiveness of an attack [25].

Multi-phase voltage regulator (MPVR) is a method in modern integrated circuits to increase the performance of power generation, power delivery and management of electronic systems, such as SoCs, and 3D integrated circuits. A block diagram of an MPVR with M interleaved stages is shown in Fig. 5. An MPVR is a discrete time sampling circuit due to the clocking that causes consecutive connections and disconnections to and from the input of VR. Assuming V_i^g as the voltage glitch when the stage i is connected to the input of VR, the total glitch energy transmitted by the VR to the CC E_{CC}^g at the end of period T_s is

$$E_{CC}^g = \frac{C_{tot}}{2M} \sum_{i=1}^{M} (V_i^g)^2 \tag{1}$$

where C_{tot} is total flying capacitance of an MPVR. The energy of the normal voltage of MPVR is not expressed in (1) since the effect of the normal output voltage is desirable for CC. If the glitch

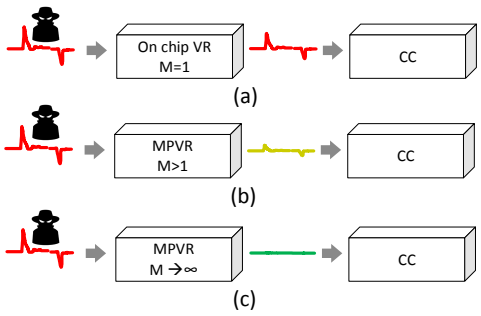

Figure 6: The power of a CC is provided by an on-chip VR. Defeating the glitch is raised by increasing M from a) $M = 1$, to b) $M > 1$, and further diminished by increasing to c) $M \to \infty$.

duration is significantly less than T_s, such that $M \gg \|\overrightarrow{V^g}\|_0$, then

$$\lim_{M \to \infty} E_{CC}^g \to 0. \tag{2}$$

The f_{-3dB} frequency of an MPVR will decrease by increasing M[26]. As a result of the decrease in f_{-3dB} frequency of MPVR, high frequency glitches at the input of MPVR will be reduced by increasing M. This smoothing in the voltage on CC results in reducing the effect of voltage glitch on CC, as shown in Fig.6.

4 PRACTICAL EVALUATIONS

Since the countermeasure is proposed against a VGA, the evaluation of the countermeasure requires the faults injected by voltage glitches. SCVR is a preferred choice over inductive counterparts due to the stability, area, and CMOS integrability considerations [27]. Moreover, an SC-MPVR with a high number of phases can be implemented by slicing larger capacitors and switches into smaller portions of capacitors and switches, and using a ring oscillator to generate interleaving clock phases [21, 27]. A 2:1 SC-MPVR is designed and simulated in Virtuoso Cadence at $60MHz$ ($T_s = 16.7\ nS$), $V_{in} = 2V$, $V_{out} = 1V$, and $M = \{1, \ldots, 32\}$. The schematic of the individual stages of VR, overall MPVR, and non-overlapping clocks are shown in Fig. 7. Switches S_1, S_3 are on for half of the period and switches S_2, S_4 are on for the rest of the period T_s. Furthermore, an S-box of AES [22] is implemented in 90 nm predictive technology model of [28] using the Virtuoso Cadence. Average power dissipation of the S-box is 256 μW, where the minimum and maximum load power is between 156.3 and 387.22 μW. In Section 2, the effect of increasing the size of the capacitor in a VR on the transition of glitches to the CC is theoretically discussed. As shown in Fig. 8, by increasing the size of the flying capacitor from 500 fF to 3 nF, the transferred energy of glitch into the CC is increased, however, this increase becomes marginal due to the filtering behavior of the VR.

The effect of increasing the switching frequency f_s of the on-chip VR on the voltage glitch on the CC is shown in Fig. 9. The resilience of the CC against VGA increases by increasing the switching frequency of the VR, and for all f_s frequencies, the resilience of the VR to VGA improves with increasing the number of phases.

When utilizing an on-chip VR, the security of the CC against VGA can be further enhanced by increasing the number of interleaved stages, as shown in Fig. 10. For a glitch with 10 ns duration

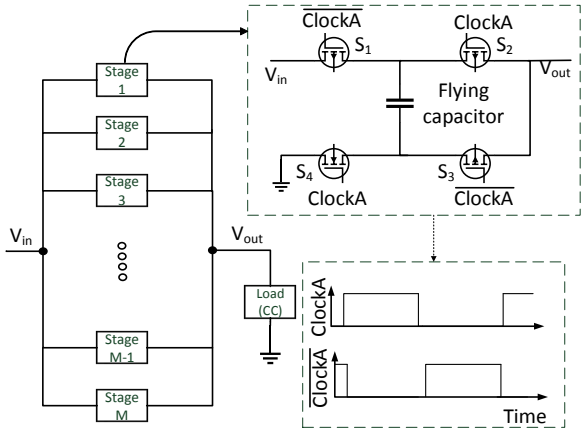

Figure 7: A 2:1 SC-VR with M stages is shown. Non-overlapping clocks A and B and switches $< S_1, S_3 >$ are connected for $T_s/2 - \epsilon$, and switches $< S_2, S_4 >$ are conducting for $T_s/2 - \epsilon$ remaining, where ϵ is the time assigned to ensure non overlapping clocks.

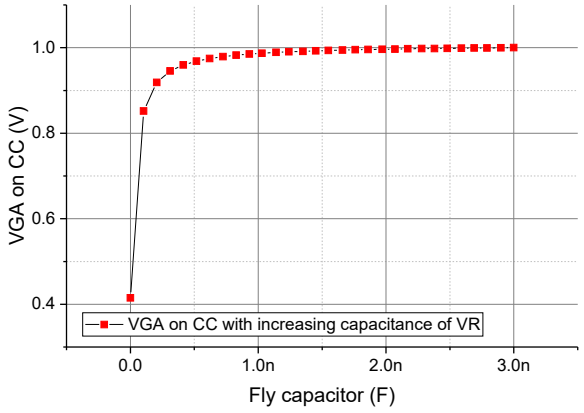

Figure 8: Implication of the capacitive impedance of the on-chip VR on the glitch transferred to the CC. By increasing the size of fly capacitor, the voltage glitch transmitted to the CC is increased before up to f_{-3dB} frequency of the voltage regulator.

on an S-box operating at 100 MHz, the attenuation in the glitch amplitude is doubled with 32 interleaved phases, while the practical span of a voltage glitch on a CC is half the cycle of the operating frequency [25]. Except for the voltage-starving attacks, the proposed countermeasure increases the resistance of the CC to a wide range of glitch durations.

As shown in Fig. 11, by increasing the number of phases of an on-chip VR, the resilience of CC against fault injection attack is improved, as theoretically discussed in Section. 3. By describing the faulty output as any result at the output of CC other than the expected one, the success of the VGA on the CC is defined as [29]

$$\%Glitch\ attack\ success = \frac{\#\ Faults}{\#\ All\ tests} \times 100. \quad (3)$$

Using (3) and repeatedly simulating the VGA on the S-box of an AES and counting the number of the faulty outputs using a comparator

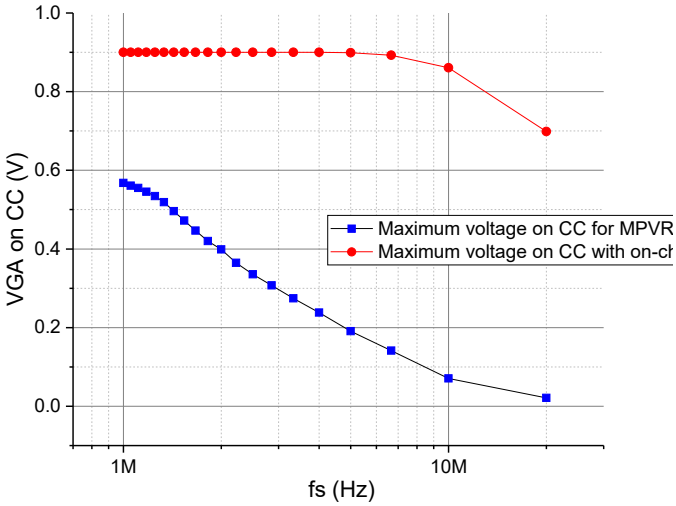

Figure 9: The maximum effect of VGA on CC for different clock frequencies f_s of VR is shown. For all frequency ranges, The resilience of MPVR with $M = 32$ (depicted by squares) against VGA is higher than that of for a CC with on-chip VR ($M = 1$).

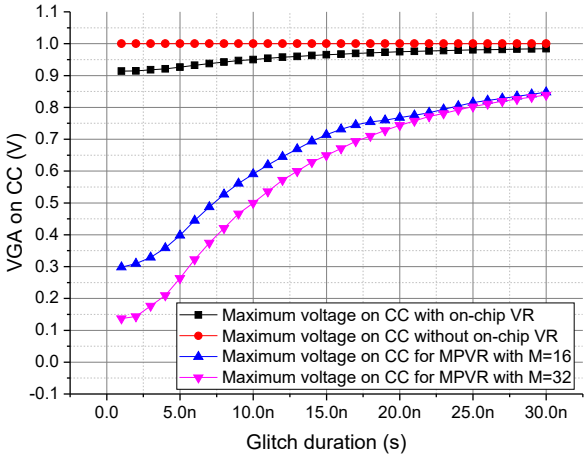

Figure 10: Relation of glitch duration and maximum effect of VGA on CC with glitch duration $\{1ns, 3ns, \ldots, 31ns\}$, for CC with various MPVRs $M = \{1, 16, 32\}$ (depicted by triangles and squares), and for CC without on-chip VR (depicted by circles).

and a counter [30], the success rate of fault occurrence in the presence of an MPVR is obtained, as shown in Fig. 12. The success of the VGA is reduced by increasing the number of phases. While the fault coverage for the unprotected S-box is 0%, the fault coverage is 5.45% with an on-chip VR, and the fault coverage reaches 91.82% with an increase in the number of phases to 32.

5 DISCUSSION

Assuming that the CC already has an on-chip VR, the throughput overhead on the CC is zero. Even though the increase in the number of phases of the VR is advantageous for the security purposes,

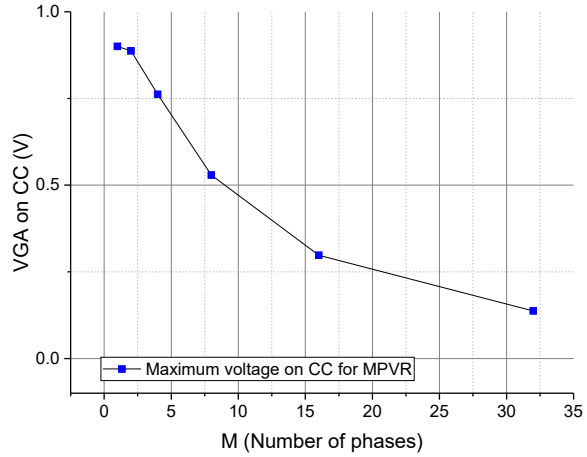

Figure 11: VGA on CC with on-chip VR for $M = \{1, 2, 4, 8, 16, 32\}$, when a glitch with amplitude $V_{glitch} = \pm 2$, duration $t_r = t_f = 500ps$, and $t_{gch} = 1\ ns$ is applied.

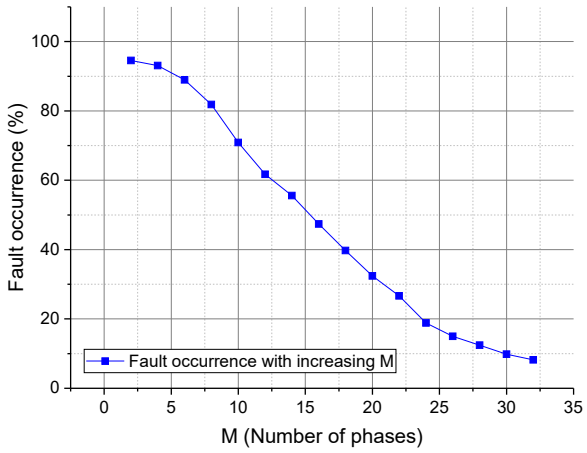

Figure 12: Fault occurrence versus number of phases for an MPVR for various number of phases. Glitch input is applied to an S-box with MPVR and an S-box without MPVR, while the result is compared and number of faults is counted using a counter.

with the increase in the number of phases the conduction losses in switches, buffers, and drivers will be increased [31]. Moreover, the design of clock generators with higher resolution is an overhead in the design of MPVR with higher M. Efficiency and area overheads of the on-chip VR with a various number of stages are listed in Table 1. The ripple at the output V_{rip} is a function of output current, switching frequency of VR, the equivalent series resistance of capacitors of VR, and M, and decreases by increasing the number of phases [31]. Efficiency and area overheads of the on-chip VR with a various number of stages and ring-oscillator are listed in Table 1.

6 CONCLUSION

In this paper, the application of an on-chip VR as a countermeasure against fault injection attack is proposed as a solution to enhance the resilience of the CC against a VGA. The effect of the number of phases in the MPVR on the robustness of the circuit against VGA is analyzed. The effectiveness of the proposed countermeasure on an S-box of an AES is evaluated. The faults generated by the VGA on CC are reduced by 5.45% with a single phase on-chip VR, and by 91.82% with an MPVR with 32 phases, as compared to unprotected S-box of an AES device. The throughput, power, and area overhead of the proposed technique are negligible due to the utilization of the existing VR as a power supply, while the area and power overhead of the MPVR are increased, respectively, by 5.1% and 1% when the number of interleaved phases is 32.

Table 1: Efficiency and area overhead of MPVR.

M	1	2	4	8	16	24	32
Ar.%	0	2.62	3.93	4.58	4.9	5.02	5.07
Eff.%	84.4	84.54	84.68	84.9	85.56	86.0	85.41

ACKNOWLEDGMENTS

This work is supported in part by the NSF CAREER Award under Grant CCF-1350451, in part by the NSF Award under Grant CNS-1715286, in part by SRC Contract NO: 2017-TS-2773, and in part by the Cisco Systems Research Award.

REFERENCES

[1] F. Standaert, E. Peeters, G. Rouvroy, and J. Quisquater, "An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays," *Proceedings of the IEEE*, Vol. 94, No. 2, pp. 383–394, February 2006.
[2] E. Karimi, Z. H. Jiang, Y. Fei, and D. Kaeli, "A Timing Side-Channel Attack on a Mobile GPU," *IEEE International Conference on Computer Design*, pp. 67–74, October 2018.
[3] H. Kumar *et al.*, "Towards Increasing the Difficulty of Reverse Engineering of RSFQ Circuits," *IEEE Transactions on Applied Superconductivity*, pp. 1–1, March 2019.
[4] M.A. Vosoughi and S. Köse, "Combined Distinguishers to Enhance the Accuracy and Success of Side Channel Analysis," *IEEE International Symposium on Circuits and Systems*, pp. 1–5, May 2019.
[5] M. Arora, "How Secure is AES Against Brute Force Attacks?," 2012. [Online]. Available: http://www.eetimes.com/document.asp?doc_id=1279619.
[6] G. Piret and J. J. Quisquater, "A Differential Fault Attack Technique Against SPN Structures, with Application to the AES and KHAZAD," *Cryptographic Hardware and Embedded Systems*, pp. 77–88, September 2003.
[7] S. M. Yen and M. Joye, "Checking Before Output May Not Be Enough Against Fault-Based Cryptanalysis," *IEEE Transactions on Computers*, Vol. 49, No. 9, pp. 967–970, September 2000.
[8] J. Blömer and V. Krummel, "Fault Based Collision Attacks on AES," *Fault Diagnosis and Tolerance in Cryptography*, pp. 106–120. October 2006.
[9] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, "The Sorcerer's Apprentice Guide to Fault Attacks," *Proceedings of the IEEE*, Vol. 94, No. 2, pp. 370–382, January 2006.
[10] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures," *Proceedings of the IEEE*, Vol. 100, No. 11, pp. 3056–3076, April 2012.
[11] M. Hutter, J. M. Schmidt, and T. Plos, "Contact-Based Fault Injections and Power Analysis on RFID Tags," *European Conference on Circuit Theory and Design*, pp. 409–412, August 2009.
[12] C. Aumüller *et al.*, "Fault Attacks on RSA with CRT: Concrete Results and Practical Countermeasures," *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 260–275, August 2002.
[13] K. Tobich *et al.*, "Voltage Spikes on the Substrate to Obtain Timing Faults," *Euromicro Conference on Digital System Design*, pp. 483–486, March 2013.
[14] A. Sarker, M. M. Kermani, and R. Azarderakhsh, "Hardware Constructions for Error Detection of Number-Theoretic Transform Utilized in Secure Cryptographic Architectures," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 27, No. 3, pp. 738–741, March 2019.
[15] M. M. Kermani and R. Azarderakhsh, "Reliable Architecture-Oblivious Error Detection Schemes for Secure Cryptographic GCM Structures," *IEEE Transactions on Reliability*, pp. 1–9, December 2018.

[16] S. A. Aftabjahani and A. Das, "Robust Secure Design by Increasing the Resilience of Attack Protection Blocks," *International Verification and Security Workshop*, pp. 13–18, July 2017.

[17] N. Beringuier-Boher *et al.*, "Voltage Glitch Attacks on Mixed-Signal Systems," *Euromicro Conference on Digital System Design*, pp. 379–386, August 2014.

[18] H. B. Le, X. D. Do, S. G. Lee, and S. T. Ryu, "A Long Reset-Time Power-On Reset Circuit with Brown-Out Detection Capability," *IEEE Transactions on Circuits and Systems II: Express Briefs*, Vol. 58, No. 11, pp. 778–782, November 2011.

[19] S. Saab, A. Leiserson, and M. Tunstall, "Key Extraction From the Primary Side of a Switched-Mode Power Supply," *IEEE Asian Hardware-Oriented Security and Trust*, pp. 1–7, December 2016.

[20] W. Yu, O. A. Uzun, and S. Köse, "Leveraging On-Chip Voltage Regulators as a Countermeasure Against Side-Channel Attacks," *Design Automation Conference*, pp. 1–6, June 2015.

[21] 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. 2, pp. 169–179, June 2014.

[22] W. Yu and S. Köse, "Exploiting Voltage Regulators to Enhance Various Power Attack Countermeasures," *IEEE Transactions on Emerging Topics in Computing*, Vol. 6, No. 2, pp. 244–257, April 2018.

[23] A. W. Khan, T. Wanchoo, G. Mumcu, and S. Köse, "Implications of Distributed On-Chip Power Delivery on EM Side-Channel Attacks," *International Conference on Computer Design*, pp. 329–336, October 2017.

[24] M. Kar *et al.*, "8.1 Improved Power Side-Channel Attack Resistance of an AES-128 Core via a Security-Aware Integrated Buck Voltage Regulator," *International Solid-State Circuits Conference*, pp. 142–143, February 2017.

[25] A. Djellid-Ouar, G. Cathebras, and F. Bancel, "Supply Voltage Glitches Effects on CMOS Circuits," *International Conference on Design and Test of Integrated Systems in Nanoscale Technology*, pp. 257–261, September 2006.

[26] O. Garcia, P. Zumel, A. De Castro, and J. A. Cobos, "Effect of the Tolerances in Multi-Phase DC-DC Converters," *Power Electronics Specialists Conference*, pp. 1452–1457, June 2005.

[27] Y. Lu, J. Jiang, and W. Ki, "Design Considerations of Distributed and Centralized Switched-Capacitor Converters for Power Supply On-Chip," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, Vol. 6, No. 2, pp. 515–525, June 2018.

[28] NIMO Group Arizona State University, "Predictive Technology Model (PTM)," 2008. [Online]. Available: http://ptm.asu.edu/.

[29] N. Selmane, S. Guilley, and J. L. Danger, "Practical Setup Time Violation Attacks on AES.," *Seventh European Dependable Computing Conference*, pp. 91–96, May 2008.

[30] E. Karimi, M. Haghbayan, A. Rahmani, M. Tabandeh, P. Liljeberg, and Z. Navabi, "Accelerated On-chip Communication Test Methodology Using a Novel High-Level Fault Model," *IEEE 9th International Symposium on Embedded Multicore/Many-core Systems-on-Chip*, pp. 283–288, September 2015.

[31] M. D. Seeman and S. R. Sanders, "Analysis and Optimization of Switched-Capacitor DC-DC Converters," *IEEE Transactions on Power Electronics*, Vol. 23, No. 2, pp. 841–851, March 2008.