Data-Driven Noise Reduction for Power Side-Channel Attack Detection

Nipun Kaushik, *Student Member, IEEE,* Laurent Njilla, *Member, IEEE,* and John Hu, *Senior Member, IEEE*

***Abstract*—Power side-channel attacks (PSCA) pose unique design challenges for secure Internet-of-Things (IoT) devices. Real-time on-chip PSCA detection is highly desirable if it can detect a small attack resistor upon insertion quickly. However, existing PSCA detecting integrated circuits (IC) suffer from high power consumption, limited detection scope, and low detection sensitivity. This paper incorporates data-driven noise reduction (DDNR) method into PSCA detection ICs to overcome these problems. Thanks to DDNR's thermal noise reduction and speed advantage over majority vote averaging, the DDNR-assisted PSCA detection circuit achieved 39 μV of voltage sensitivity or 0.39 Ω of minimum detectable resistance, which are 64x and 2.56x reduction compared to prior art. The energy per detection ranges from 925 to 1700 pJ per detection, the worst-case of which is still 15% below the state-of-the-art. The PSCA circuit and the DDNR controller was designed and synthesized in a general-purpose 65 nm CMOS process. The superior energy-efficiency and detection sensitivity was also a result of avoiding over-design by targeting 95% true positive (TP) and true negative (TN) rates.**

***Index Terms*—Noise, PSCA, Hardware Security, Switched Capacitor Circuit,DDNR**

I. Introduction

Encrypting devices are used to jumble delicate information and save them from meddling oppugner. Research has exposed that there is often a relation between side channel and information being guarded. The information can exist on side channels such as power consumption [1]–[3], electromigration emanations [4]–[6],thermal signatures [7]–[9],optical [10], [11], timing [12], [13] and acoustic [14], [15]. Side channel attacks are a constant threat to security . This demands exacting demands for design of secure devices. In case of AES, the encryption engine power supply can provide the information about the secure operation. This sensitive information can be exposed by techniques like differential power analysis (DPA) [16], correlational power analysis (CPA) [17]. The main theme for power analysis is to monitor the current consumption by inserting a sense resistor in power supply or ground. This current signature is monitored over several iterations of encryption cycles. The adversary uses a known plain text as input to the device. The collected current signature is processed statistically to come up with the encryption key. Once the key is exposed

Manuscript received April 1st, 2022. This reseaerch was sponsored by the Air Force under PIA FA8750-19-3-1000. The U.S. Government is authorized to reproduce and distribute copies for Governmental purposes notwithstanding any copyright or other restrictive legends. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Air Force or the U.S. Government.

Nipun Kaushik and John Hu are with the School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, OK, 74078 USA (e-mail: nipun.kaushik@okstate.edu; john.hu@okstate.edu).

Laurent Njilla is with the Cyber Assurance Branch, Air Force Research Laboratory, Rome, NY, 13441 USA (e-mail: laurent.njilla@us.af.mil).

A. Background

Military electronics is also susceptible to various side channel attacks [18]. Information stored on electronic media can be exposed by conducting these attacks. Power and EM SCA's have revealed encryption keys [19], machine learning devices [20], Convolutional neural networks(CNN) [21], deep neural networks(DNN) [22] parameters. To make device more robust to SCA's various logical [23], [24] and circuit level countermeasures [25]–[30] have been proposed. However these methods cannot assure the safety of device under prolonged exposure. All the above mentioned techniques come at a cost of power, performance and area (PPA) [31]. This lead to work in *proactive* power [32]–[36] and EM [37], [38] SCA detection methods.

B. Detection circuits

Power side channel attack (PSCA) is typically conducted by inserting a sense resistor in power or ground path. Literature shows various techniques of detecting this sense resistor. Ring oscillators are used to sense power grid impedance [34].The comparison is based on detecting the phase difference of other nodes in a BGA package. The circuit provides high speed and low area. This circuit however has the limitation of limited coverage based on the location of sense resistor. Machine learning have used to detect power side channel attack [32]. ML models are trained and used to detect a PSCA. The circuit requires training of ML models along with high area and power overheads. A switched capacitor circuit has been shown in recent works to detect the attack surface [35]. The topology uses a switched capacitor amplifier with a compactor to digitize the signal. This circuit is generic to the location if insertion of the sense resistor. The topology detects the impedance of the power supply. It is done by generating an on chip current I_{force} to provide voltage signal to the amplifier. It provides low area, higher coverage through a simple implementation. The performance of comparator plays a vital role in this detection. Thermal noise limits the minimum sense resistor R_{sns} which can be detected [39] by this circuit. The noise distribution at the output of amplifier and input of comparator. Noise can lead to increased Type I and Type II errors. This decreases the detection accuracy of the circuit and leads to false detection.

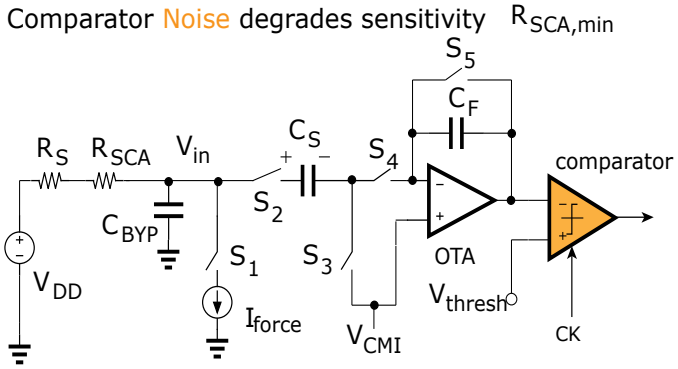

Fig. 1: Circuit description

C. Contribution of this work

This work introduces the first PSCA detection circuit employing data driven reduction technique (DDNR) [40].

1) The input voltage sensitivity was improved by 64x and 42x with and without the DDNR technique
2) The energy per detection was reduced from 2000 pJ to 925-1700 pJ. The energy saving comes primarily from the use of a smaller stimulus current I_{force}.
3) Compared to other noise reduction techniques through averaging, DDNR provides faster detection time and increases the throughput by ...

This work introduces the first PSCA detection circuit employing data driven reduction technique [40]. It provides high detection accuracy with minimal power and area overhead. This alleviate the limitation due to thermal noise yielding high sensitivity. This low noise performance allows the circuit to use low on chip current I_{force}. The circuit provides high detection accuracy reducing false detection rates. The circuit demonstrates low energy per detection as compared to other works. The techniques enhances detection of minimum sense resistor R_{sns} which results in higher security.

II. Circuit description

The switched capacitor uses on chip current to detect a sense resistor in the power of the secure device. This signal chain consists of a switched capacitor amplifier followed by a comparator to digitize the signal for further use. This signal can generate a flag to notify the system of an attack and stop the secure operation.

Figure 1 the topology and the critical point of comparator decision. The circuit can result in false detection due to the presence of thermal noise the the time of detection resulting in decreased accuracy.

Equation 1 [39] shows the a direct relation between minimum detectable R_{sns} and circuit parameters. The noise distribution of comparator and the track & hold circuit limit the R_{min}. The current I_{force} refers to the on chip stimulus current. The current is used to generate the potential difference for the input of the amplifier with R_{sns}.The significance level $f(\alpha, \beta)$ = 0.5 (a.k.a 95% confidence level) is chosen for high accuracy to reject null hypothesis. The total combined noise ($\overline{\sigma^2}$) the noise from THA and input referred noise of the comparator. This noise arises from two different sources and thus assumed to be uncorrelated. G refers to the gain of the THA, for this case it is set to 30. For high confidence of 95% we can do the following things in order to improve R_{min}.

1) Increase I_{force} which requires higher power, energy per detection and area.
2) Decrease noise(σ)

Typical methods of reducing noise include increasing the size (W/L). This results in higher area which is not desirable. Noise performance can also be improved by high I_{bias}. This comes at a cost of more power consumption increasing energy per detection. Averaging can be reduce noise without high area and power consumption. The logic can be implemented in digital block. Digital logic consumes lower area, it is very compact and doesn't require big devices (W/L). It operates at low power which is highly desirable for low energy consumed per detection. The area and power overhead of this approach are minimal as compared to other existing methods of noise reduction. This leads to implementation of DDNR in PSCA.

Comments: 1. One equation and explanation about noise affecting accuracy. 2. Previous methods of reducing noise are undesirable. (increasing WL, increasing Ibias)

$$\therefore R_{SNS,min} = \frac{f(\alpha,\beta)}{I_{force}} \sqrt{\sigma^2_{THA,in} + \frac{\sigma^2_{comp}}{G^2}} \tag{1}$$

A. Majority Voting with DDNR

Data driven noise reduction (DDNR) [41] was introduced in analog to digital (ADC) designs. The techniques uses majority voting get more samples and increase true detection. The topology takes more number of samples per conversion by holding the final result. The number of samples are related to reduction of input referred noise (σ) at input of the comparator as

$$\frac{\sigma}{\sqrt{N}} \tag{2}$$

Figure 2 shows different approaches of averaging. Errors occurs for the values near the comparator threshold. More number of samples are taken for the same value to improve decision confidence. Majority voting samples a fixed number of times before providing the final result. It is based on majority of the comparator output. This impacts the noise at comparator input resulting in reduced sigma. This is important for PSCA detection as it results in detecting lower R_{sns}. DDNR has a dynamic operation for this topology as it will provide a final decision if the majority reaches earlier (3 out of 5) for N=5.

B. Integrating DDNR with PSCA

The switched capacitor circuit implies DDNR by adding a digital block overlooking comparator output. Figure 3 shows integration of DDNR with the existing circuit. Internal clock is generated by a slow or fast signal depending on the delay. If a *Fast* is received earlier than delay DDNR is not activated. This means the result is resolved with high accuracy. It happens when R_{sns} far away from the detection threshold of the

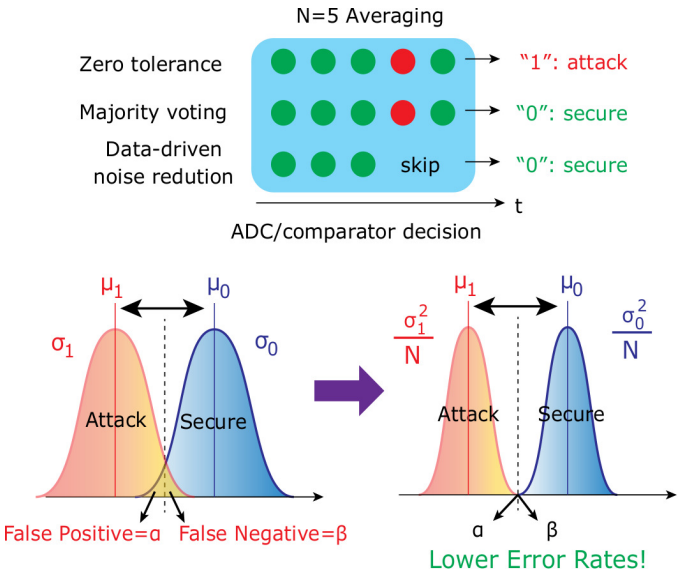

Fig. 2: Improvement in noise by averaging

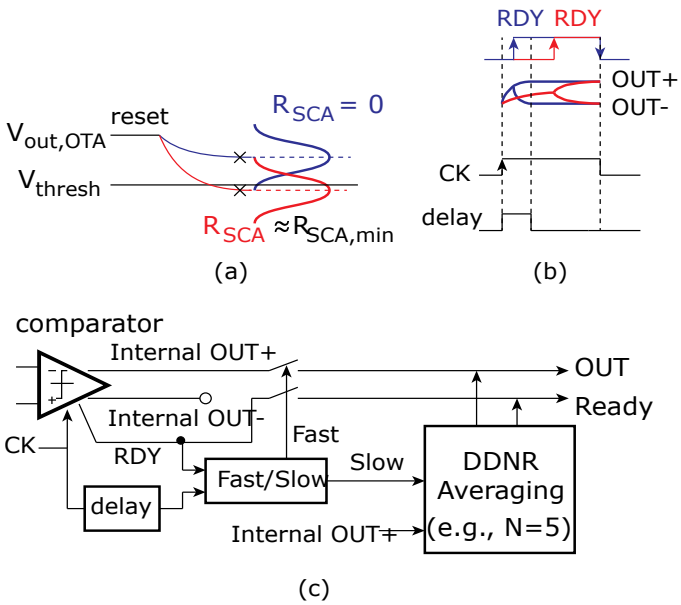

Fig. 3: Integration of DDNR in PSCA

compartor. The decision is made with high accuracy for very low/high values. If a *Slow* is received, it means that the value of R_{sns} is close to the detection threshold. This is the region for high errors during detection. The final decision is held, while DDNR samples the output of comparator. The number of samples are related to noise reduction in the circuit. More number of samples (N) can lead to higher noise performance at the cost of delay in the final output. The circuit can be optimized for early exit if the majority is received early. This leads to higher throughput with less detection time. Skipping cycles also lead to lower energy per detection saving power.

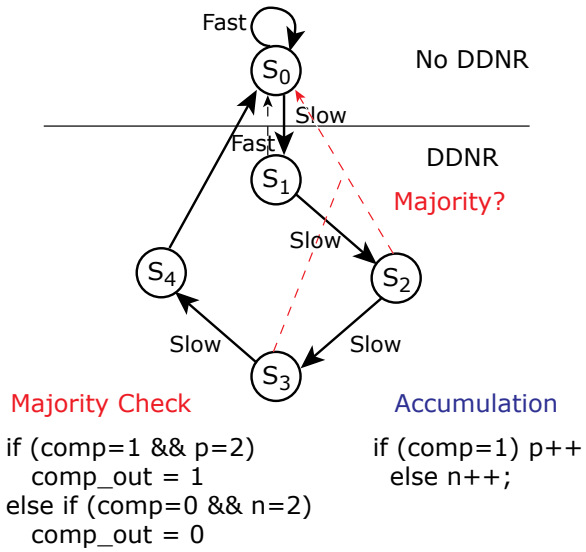

Fig. 4: State machine for DDNR

C. Bubble diagram of the state machine

The state machine shown in figure 4 shows the steps for state transition of this design. This scheme uses a maximum of 5 samples. If a majority is reached before 5 (for e.g. 3) the remaining samples are skipped producing the output. If a *Fast* is received first, it indicates successful resolution of the value. The DDNR is not activated in this case and it stays in S_0. If a *Slow* is received first, it means the value of R_{sns} is close the comparator detection threshold. DDNR is activated, that value of output is stored and machine moves to the next state S_1. The machine moves to the next states until it reaches and early exit condition of N=3. If the all output are negative or positive, it exits the state and produces the output. If no majority is reached, the output is the final result of majority from 5 states. The type of operation ensure speed and accuracy as compared to majority voting all the time. If majority voting is ON during the whole time for N=5, the machine provides final decision after all the 5 cycles. This impacts throughput and detection time as explained in simulation result section.

III. Simulation Results

The circuits are designed in standard 65nm CMOS process. The digital block is synthesised by Verilog code. This is separately tested for performance before integration with the analog part.The whole system comprises of analog front end for sensing and digital DDNR.

A. Increased noise performance with DDNR

Figure 5 shows the impact of averaging through majority voting, DDNR and no averaging. The performance of the PSCA detection was limited by the thermal noise at the point of digitization. The addition of averaging boosts the confidence of final decision. DDNR gives the noise performance similar to majority voting but it also provides higher detection speed. Higher speed comes due to skipping cycles if a decision is made early. The The ideal case should have pulse shape, this brings the performance the closer to an ideal case.

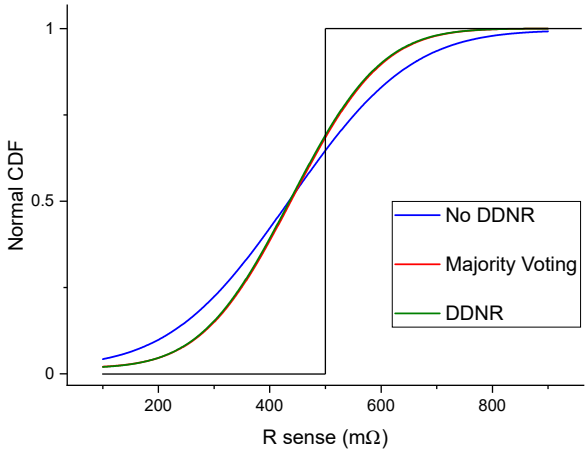

Fig. 5: Before and after comparison of DDNR, No DDNR and majority voting

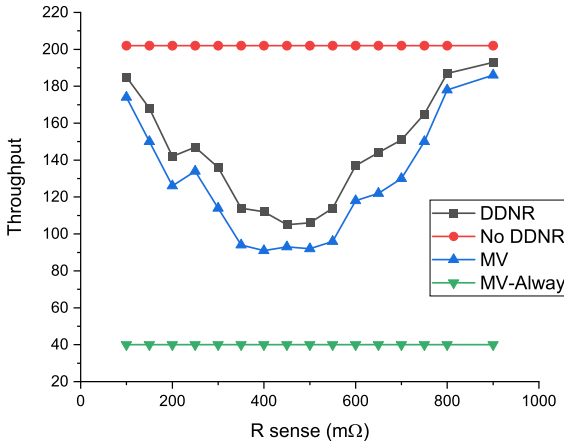

Fig. 6: Comparison of throughput with different techniques

B. Throughput

Consider starting paragraphs with Figure 6. Same for other places.

Figure 6 shows the comparison of different approaches for detection. The addition of averaging comes at a cost of throughput impact. In case of majority voting all for e.g. (N=5), every decision is done after counting majority of the full 5 samples. This causes a slew in final output. With no noise reduction, the system has higher throughput. This results in limited R_{min} sensing and higher detection errors. The use of DDNR optimizes this delay by producing the output if majority is achieved early, for e.g. 3 out of 5. This step decreases the throughput when the value of R_{sns} is close to the detection threshold. It shows that DDNR is not active in the beginning & end. It is because the errors are lower if the value is far away from the threshold of the comparator. It is activated only in the region of high error to collect more samples and provide accurate results covering the whole spectrum effectively.

Show the data point on plot.

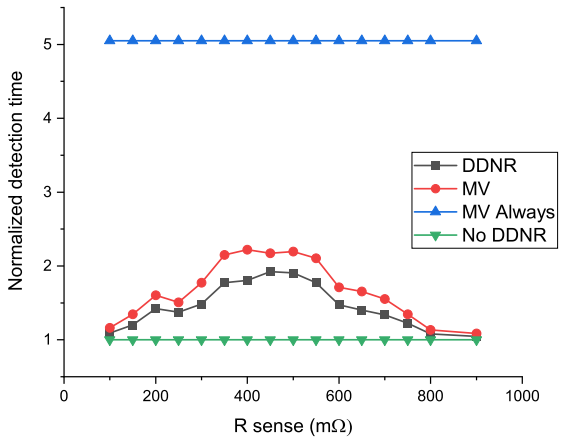

Fig. 7: Comparison of detection time

TABLE I: Area estimation of synthesized DDNR block

Digital Logic	Instances	Area	Area(%)
Sequential	17	128.16	53
Inverter	9	9.7	4
Logic	46	104	43

C. Speed and detection time

Figure 7 shows the comparison of different techniques. The detection time without the addition of averaging is higher. This however results in lower detection accuracy due to false detection. Averaging introduces a slight delay at the cost of higher accuracy. Averaging in this PSCA design is optimized to provide accuracy and speed. The normalized detection time is highest if majority voting is ON throughout the operation. Detection time in case of DDNR decreases in high error zone as it is activated. If R_{sns} away from the detection threshold the circuit works at higher speed.

Show the data point.

The table I shows the result of DDNR block synthesis, it shows a break down of area with type of logic. This circuit provides a low area and low power which is optimal for existing PSCA detection methodology.

Table **??** shows the comparison of this approach with other works. It provides low energy/detection with high accuracy. It shows a high $RSCA_{min}$ detection capability with low Type 1/2 errors. This circuit is also generic to the location of the sense resistor which means it would capture resistor inserted at any power trace. This circuit can also operate at a very low I_{force} because of high noise performance. The are of the circuit can also be optimized by placing the sampling MIMCAP on top of other mixed signal circuitry. The detection time varies due to the dynamic DDNR activation providing high speed and accuracy depending on the case.

Fill out the NR. Shrink the column width somehow.

IV. Conclusion

The work proposes the first PSCA circuit with a noise reduction technique. This reduces the error rate resulting in

high detection accuracy with low power operation. The circuit produces high voltage sensitivity by decreasing thermal noise. It increases the minimum sense resistor limit resulting in a very low energy per detection. The circuits are deigned in 65nm CMOS technology which can be scaled with latest technology. The solution is generic to the location sense resistor insertion which makes it easier to integrate with a secure device.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual international cryptology conference*. Springer, 1999, pp. 388–397.

[2] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks: Revealing the secrets of smart cards*. Springer Science & Business Media, 2008, vol. 31.

[3] M. Randolph and W. Diehl, "Power side-channel attack analysis: A review of 20 years of study for the layman," *Cryptography*, vol. 4, no. 2, p. 15, 2020.

[4] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The em side—channel (s)," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2002, pp. 29–45.

[5] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2001, pp. 251–261.

[6] J. Longo, E. De Mulder, D. Page, and M. Tunstall, "Soc it to em: electromagnetic side-channel attacks on a complex system-on-chip," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2015, pp. 620–640.

[7] P. Gu, D. Stow, R. Barnes, E. Kursun, and Y. Xie, "Thermal-aware 3d design for side-channel information leakage," in *2016 IEEE 34th International Conference on Computer Design (ICCD)*. IEEE, 2016, pp. 520–527.

[8] M. Hutter and J.-M. Schmidt, "The temperature side channel and heating fault attacks," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2013, pp. 219–235.

[9] R. J. Masti, D. Rai, A. Ranganathan, C. Müller, L. Thiele, and S. Capkun, "Thermal covert channels on multi-core platforms," in *24th {USENIX} Security Symposium ({USENIX} Security 15)*, 2015, pp. 865–880.

[10] J. Ferrigno and M. Hlaváč, "When aes blinks: introducing optical side channel," *IET Information Security*, vol. 2, no. 3, pp. 94–98, 2008.

[11] F. Stellari, A. Tosi, F. Zappa, and S. Cova, "Cmos circuit analysis with luminescence measurements and simulations," in *32nd European Solid-State Device Research Conference*. Citeseer, 2002, pp. 495–498.

[12] D. Brumley and D. Boneh, "Remote timing attacks are practical," *Computer Networks*, vol. 48, no. 5, pp. 701–716, 2005.

[13] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Annual International Cryptology Conference*. Springer, 1996, pp. 104–113.

[14] E. Toreini, B. Randell, and F. Hao, "An acoustic side channel attack on enigma," *School of Computing Science Technical Report Series*, 2015.

[15] M. E. Smid and D. K. Branstad, "Data encryption standard: past and future," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 550–559, 1988.

[16] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," *Journal of Cryptographic Engineering*, vol. 1, no. 1, pp. 5–27, 2011.

[17] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2004, pp. 16–29.

[18] M. Mehlberg, "Protecting military electronics ... - intelligent aerospace," Oct 2021. [Online]. Available: https://www.intelligent-aerospace.com/military/article/16544745/protecting-military-electronics-avionics-from-sidechannel-attacks

[19] C. O'Flynn and Z. D. Chen, "Chipwhisperer: An open-source platform for hardware embedded security research," in *International Workshop on Constructive Side-Channel Analysis and Secure Design*. Springer, 2014, pp. 243–260.

[20] L. Wei, B. Luo, Y. Li, Y. Liu, and Q. Xu, "I know what you see: Power side-channel attack on convolutional neural network accelerators," in *Proceedings of the 34th Annual Computer Security Applications Conference*, 2018, pp. 393–406.

[21] W. Hua, Z. Zhang, and G. E. Suh, "Reverse engineering convolutional neural networks through side-channel information leaks," in *2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC)*. IEEE, 2018, pp. 1–6.

[22] H. Yu, H. Ma, K. Yang, Y. Zhao, and Y. Jin, "Deepem: Deep neural networks model recovery through em side-channel information leakage," in *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2020, pp. 209–218.

[23] K. Tiri, D. Hwang, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "Prototype ic with wddl and differential routing–dpa resistance assessment," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2005, pp. 354–365.

[24] W. Yu and S. Köse, "A lightweight masked aes implementation for securing iot against cpa attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 11, pp. 2934–2944, 2017.

[25] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity," *IEEE Trans. Circuits Syst. I*, vol. 65, no. 10, pp. 3300–3311, 2018.

[26] D. Das, J. Danial, A. Golder, N. Modak, S. Maity, B. Chatterjee, D. Seo, M. Chang, A. Varna, H. Krishnamurthy *et al.*, "27.3 EM and Power SCA-resilient AES-256 in 65nm CMOS Through $>350\times$ Current-Domain Signature Attenuation," in *2020 IEEE Int. Solid-State Circuits Conference - (ISSCC)*. IEEE, 2020, pp. 424–426.

[27] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "36.2 an em/power sca-resilient aes-256 with synthesizable signature attenuation using digital-friendly current source and ro-bleed-based integrated local feedback and global switched-mode control," in *2021 IEEE International Solid-State Circuits Conference (ISSCC)*, vol. 64. IEEE, 2021, pp. 499–501.

[28] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Improved power/EM side-channel attack resistance of 128-bit AES engines with random fast voltage dithering," *IEEE J. Solid-State Circuits*, vol. 54, no. 2, pp. 569–583, 2018.

[29] A. Singh, M. Kar, V. C. K. Chekuri, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Enhanced power and electromagnetic sca resistance of encryption engines via a security-aware integrated all-digital ldo," *IEEE Journal of Solid-State Circuits*, vol. 55, no. 2, pp. 478–493, 2019.

[30] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, 2009.

[31] D. Das, S. Ghosh, A. Raychowdhury, and S. Sen, "Em/power side-channel attack: White-box modeling and signature attenuation countermeasures," *IEEE Design & Test*, vol. 38, no. 3, pp. 67–75, 2021.

[32] F. Kenarangi and I. Partin-Vaisband, "Exploiting machine learning against on-chip power analysis attacks: Tradeoffs and design considerations," *IEEE Trans. Circuits Syst. I*, vol. 66, no. 2, pp. 769–781, 2019.

[33] D. Utyamishev and I. Partin-Vaisband, "Real-time detection of power analysis attacks by machine learning of power supply variations on-chip," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 1, pp. 45–55, 2020. [Online]. Available: https://dx.doi.org/10.1109/TCAD.2018.2883971

[34] N. Gattu, M. N. Imtiaz Khan, A. De, and S. Ghosh, "Power side channel attack analysis and detection," in *2020 IEEE/ACM Int. Conf. Comput. Aided Design ICCAD*, 2020, pp. 1–7.

[35] N. Kaushik and J. Hu, "A switched-capacitor power side-channel attack detection circuit in 65-nm CMOS," in *2020 IEEE Int. Symp. Circuits Syst. (ISCAS)*, 2021, pp. 1–5.

[36] R. Munny and J. Hu, "Power side-channel attack detection through battery impedance monitoring," in *2021 IEEE Int. Symp. on Circuits Systems (ISCAS)*, 2021, pp. 1–5.

[37] D.-H. Seo, M. Nath, D. Das, B. Chatterjee, S. Ghosh, and S. Sen, "Pg-cas: Patterned-ground co-planar capacitive asymmetry sensing for mm-range em side-channel attack probe detection," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2021, pp. 1–5.

[38] N. Miura, D. Fujimoto, D. Tanaka, Y.-i. Hayashi, N. Homma, T. Aoki, and M. Nagata, "A local EM-analysis attack resistant cryptographic engine with fully-digital oscillator-based tamper-access sensor," in *Symp. VLSI circuits Tech. Dig.* IEEE, 2014, pp. 1–2.

[39] N. Kaushik and J. Hu, "Performance and noise trade-off for sc-based power side-channel attack detection circuits," in *2021 IEEE Int. Midwest Symp. on Circuits Systems (MWSCAS)*, 2021, pp. 770–773.

[40] P. Harpe, E. Cantatore, and A. van Roermund, "A 10b/12b 40 ks/s sar adc with data-driven noise reduction achieving up to 10.1b enob at 2.2 fj/conversion-step," *IEEE J. Solid-State Circuits*, vol. 48, no. 12, pp. 3011–3018, 2013.

[41] P. Harpe, E. Cantatore, and A. Van Roermund, "A 10b/12b 40 ks/s sar adc with data-driven noise reduction achieving up to 10.1b enob at 2.2 fj/conversion-step," *IEEE Journal of Solid-State*

Circuits, vol. 48, no. 12, pp. 3011–3018, 2013. [Online]. Available: https://dx.doi.org/10.1109/jssc.2013.2278471