IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Highly Secure Chaotic Based Dual-Hiding Asynchronous-Logic AES Accelerator Against SCA

1st SHIVARAJ CHANNABASAPPA
ECE Department
Sharnbasva University
Kalaburagi, Karnataka, India

2nd Prof. MAHESH R K
ECE Department
Asst. Professor, Sharnbasva University
Kalaburagi, Karnataka, India

***Abstract*— Most applications, including e-commerce, online banking, the military, satellite and wireless communications, electronic devices and appliances, etc., consider data security to be a major factor and give it significant weight. By transforming the data into a format that is difficult for unneeded people to understand, cryptography is a technique used to keep data secure and private. This method offers a reliable, affordable means of protecting our data secrecy and aids in data integrity verification. The side channel attacks that cryptography is subject to make it difficult to provide error-free data. The proposed AES accelerator improves the horizontal (temporal) SCA hiding of asynchronous logic operations using a timing-boundary-free input arrival time randomizer and a skewed-delay controller while achieving vertical (amplitude) SCA hiding via an area-efficient dual-rail mapping approach and a ZV compensated substitution-box (S-Box). Additionally, a chaotic sequence is used in between each step of the cypher text generation process. As a result, the design will reduce the area overhead, offer strong defence against side channel attacks, and increase the system dependability. The proposed design is implemented in Xilinx Vivado 2018.3, and final result of the simulation are used to validate the output.**

Keywords*— FPGA, Side Channel Attack(SCA), Advance Encryption System(AES), Xilinx Vivado 18.3.*

I. INTRODUCTION

Large Internet of Things (IoT) markets are what are driving EDGE computing, which necessitates that edge devices process and store more raw IoT data locally and only share or transfer necessary IoT data with other edge devices and/or cloud servers. In order to be suited for a variety of IoT applications, edge devices should not only have cheap cost, high performance, and low power qualities, but also high configuration and high security ones. A possible option for the latter features is secure field-programmable gate arrays (FPGAs), which provide security and privacy in IoT and offer dynamic reconfiguration. Although an application-specific integrated circuit (ASIC)'s architecture can be changed to provide better security, this takes longer to market because it requires a higher volume (>400 k) to keep costs down.

A further benefit of FPGA reconfigurability is that the counter measures can be sporadically updated as security threats shift over time. A few of the aspects that must be considered in the design are secure boot, memory, and key creation, malware analysis, access authentication, and data encryption. The side-channel attack (SCA), which leverages physical leakage information (PLI) released by FPGAs to reveal the secret key, is among the main issues with data encryption utilising hardware cyphers. The SCA consistently attempts to determine the secret key or plaintext by examining physical parameters like power consumption, execution time, EMR ("Electro Magnetic Radiation") of the final ciphertext, or from the intermediate output of encryption algorithms.

In order to combat SCAs, two types of countermeasures are commonly employed: masking and concealment. Masking uses arbitrary masks to attempt to connect the PLI with the made-up SCA models. Contrarily, hiding attempts to randomize or uniformize the PLI so that the SCA cannot determine which helpful information relates to the secret key.

FPGAs are challenging to defend against SCAs because of design restrictions in FPGA designs, such as set mapping unit structure, constrained placement, and routing flexibility. Innovative countermeasures like random quick voltage dithering, nonlinear digital low-dropout regulator (LDO), and current-domain signature attenuation cannot be used since FPGA lacks analogue components and specialized routing control. Although a number of reported FPGA topologies, such as application-specific-inflexible FPGA (ASIF), SCAR-FPGA, and tree-based FPGA may reduce hardware security vulnerabilities, the design complexity is higher and still security has not been verified. The bulk of modern FPGAs employ a "by-design" method, such as adopting masking or hiding countermeasures, to reduce SCAs because they are simple and affordable.

On the other side, for hidden countermeasures to work, the PLI randomization or uniformization impact must be significant while not generating excessive area/energy overheads. Two alternative directions for concealing countermeasures are vertical concealment and horizontal concealment. The vertical hiding attempts to reduce PLI fluctuations by adding complementary circuits, like dual-rail logic, or by reducing the PLI amplitude using (redundant)

compensators. Despite being able to guarantee uniform switching activity, complementary circuits nevertheless suffer from the unbalanced routing and early propagation effect (EPE) problems that make hardware cyphers susceptible to SCAs. By randomizing the PLI in time, the horizontal hiding,on the other side, seeks to desynchronize the PLI. Dummy operations and asynchronous-logic (asynchronous-logic) have been used to enable both vertical hiding and horizontal hiding (collectively referred to as dual-hiding), but they have the drawbacks of either large area/energy overheads or coarse-grain hiding attributes that limit the SCA's resistance.

II. PROPOSED WORK

The block design of proposed dual-hiding asynchronous logic AES accelerator is shown in Fig. 1, and it includes input-output flip-flops with sync-logic state machines, a pre round TBF input arrival-time randomizer, a single- to dual-rail conversion module, and an asynchronous-logic core. The inputs and outputs are stored in the input-output flip-flops with sync-logic state machines that make up the sync-asynchronous interface circuit. Essentially, the purpose of the pre round TBF input arrival-time randomizer is to randomise the start of the dual-rail asynchronous-logic operation and to safeguard the preround operation from SCA. The primary computing engine of AES is the asynchronous-logic core, which is composed of a number of building elements, including dual-rail core modules (S-Box, Shift-Row, MixColumn, etc.) and rings of asynchronous-logic pipeline [latches with competition detection (CD)].

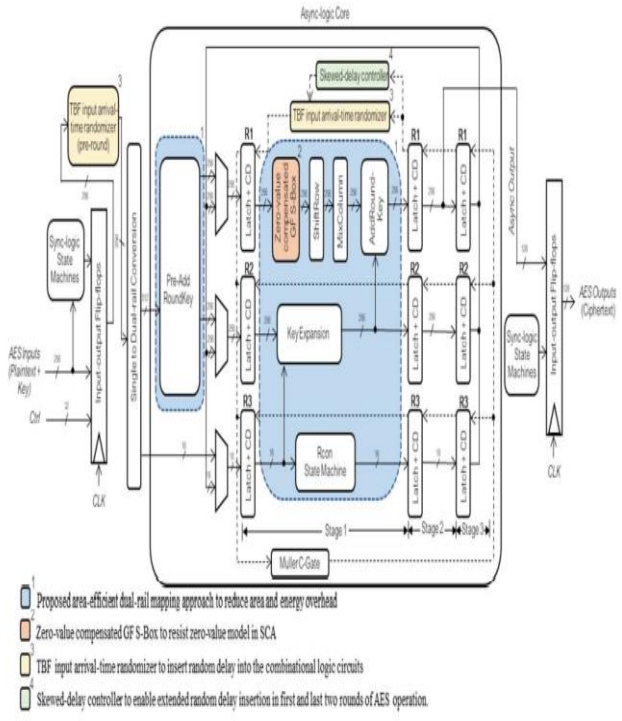

Fig. 1 Block Diagram of a Proposed Dual-Hiding Asynchronous-Logic AES Accelerator

We first describe the encryption process of our proposed asynchronous-logic AES accelerator. Upon receiving the AES inputs, the input–output flip-flops will pass the inputs into the asynchronous-logic core via the TBF input arrival-time randomizer and the single- to dual-rail conversion module. The TBF input arrival-time randomizer is our proposed countermeasure to protect the First round SCA attack. The single- to dual-rail conversion module converts the single-rail data of the AES inputs into their corresponding dual-rail data. In the asynchronous-logic core, the dual-rail data first undergo a preround key addition, followed by 14 rounds of AES transformation in rings of asynchronous-logic pipelines. Each ring of the asynchronous-logic pipelines is made up of three latches with CD. Lack serves as the handshake signal to control the latch, allowing either a valid data or a null to pass through.
Lack serves as the handshake signal to control the latch, allowing either a valid data or a null data to pass through. When the Lack signal is asserted (logic “1”), the latch will wait for a valid data, and once the valid data have arrived, the latch will hold the valid data. When the Lack signal is negated (logic “0”), the latch will wait for a null data, and once the null data have arrived, the latch will hold the null data. Each valid–null data sequence constitutes one round of AES transformation. There are three rings of asynchronous-logic pipeline, R1–R3 rings. The R1 ring performs AES round transformation, the R2 ring performs key expansion, and the R3 ring controls fourteen rounds of AES transformation via Rcon state machine.
Key expansion is done by the R2 ring, while the R3 ring uses the Rcon state machine to handle 14 rounds of AES transformation. The R1 ring performs AES round transformation. Data from the Pre-Add Round Key module will first be sent to the latches in Stage 1 via the multiplexers when the encryption process is initiated. The MUXes will be switched to create three rings, R1-R3, based on the latches in Stage 1 successfully receiving the data. To fully build an asynchronous cyclic data transmission, we require at least three stages for each ring. The data is passed from Stage 1 to Stage 2, Stage 2 to Stage 3, and Stage 3 back to Stage 1 in order to create each ring. The propagation of the valid and null data in Stages 1-3 is controlled by the handshake Lack signals of the latches, which are represented by the dotted lines in Fig. 1. All of the Lack signals will be synchronized by the Muller C-Gate in Stage 1. Before starting a new round of AES transformation, this synchronization in Stage 1 makes sure that the AES data, AES key, and Rcon are all updated and stored in the latches. The valid and null data cycle through Stages 1-3 ten times during the asynchronous-logic AES transformation process. The asynchronous-logic process will be stopped by the Rcon state machine after the tenth round, and the cipher text will be saved in the R1 latch in Stage 2 so that the input-output flip-flops can recover it. After 14 clock cycles, the sync-logic state machines will direct the flip-flops to retrieve the data kept in the latches. Therefore, essentially, our asynchronous-logic AES accelerator is globally synchronous locally asynchronous, assuming that the AES encryption will be complete within 14 clock cycles.

A. Area-Efficient Dual-Rail Mapping:

A conventional dual-rail cell that consists of a true rail and a false rail needs at least twice as many gates as a single-rail cell. In their proposal, dual-rail cells with 5 inputs would all be combined into a single, 6-input LUT. There are two-input XOR,OR,NAND,XNORAND & NOR gates in these dual-rail cells. Our suggested mapping method is substantially more space-efficient and only requires one LUT.

B. ZV Compensated GF S-Box:

The hardware implementation of S-Boxes is essential for minimizing the space and PLI dissipation. A GF S-Box is area-efficient; however, it has the ZV SCA issue. A ZV compensated GF S-Box is suggested in order to take advantage of the GF S-Box's tiny area characteristics while still avoiding the ZV problem. The addition of two MUXes solves the ZV issue. The initial MUX checks to see if the S-Box input is zero and, if it is, passes a dummy data p into the S-Box.

Whether the S-box input is zero is also determined by the second MUX. If the answer to that question is "yes," the second MUX will wait for the dummy data to travel through the circuits until it finds q in the output of GF(24), where q is the predicted output of GF(24) when the S-Box input is p. Ensure that q is the GF(24) output of p's equivalent nonzero dummy value, p, which can be any nonzero value. We select the values of p and q for our suggested ZV adjusted S-Box, with p being "8" and q being "1." When q is found, the second MUX will retransmit the proper output, which is zero, to the subsequent circuits.

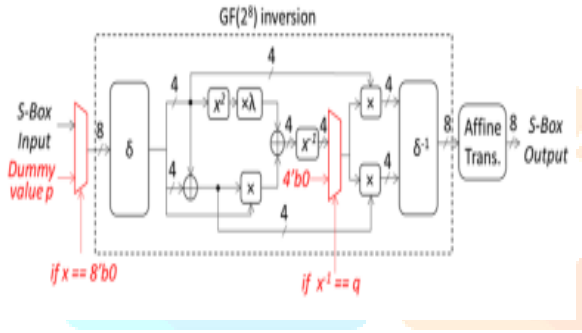

Fig. 2: Shows A Suggested ZV-Compensated GF S-Box.

C. TBF Input Arrival-Time Randomizer

We suggest a TBF input arrival-time randomizer to introduce random delays to the local handshake signals that regulate the "release" of the data into dual-rail core modules in order to boost the horizontal concealment feature.

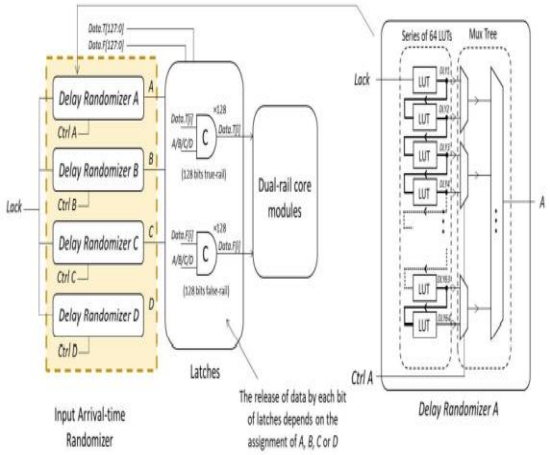

Fig. 3 Block diagram of our proposed TBF input arrival-time randomizer.

D. Internal Circuitries of a Delay Randomizer.

The proposed TBF input arrival-time randomizer as depicted in Fig. 3 above consists of four delay randomizers (delay randomizers A, B, C, and D). As illustrated in Fig. 3, each delay randomizer is composed of a set of 64 LUTs and a MUX tree, allowing the inserted delay to range from 1 to 64 unit-delays. Our suggested asynchronous-logic AES accelerator uses the Ctrl signal as a primary input, which acts as a random signal to determine how many unit delays will be incurred. We produce the Ctrl signal based on plaintext for the first encryption via external XOR operations and depends on prior ciphertext for the following encryptions using external XOR operations to achieve randomization. This work is done for simplicity and our SCA evaluation purpose alone. The data input arrival time for dual-rail core modules is altered by the delay randomizers A–D attach to the latches. Each bit of the latch in our asynchronous-logic design can "release" data independent, meaning that each bit of data may have various input arrival timings. Since our suggested TBF input arrival-time randomizer has four delay randomizers, we can divide the latches into four groups of 128 bits true-rail and 128 bits false-rail by assigning the outputs of each delay randomizer to specific latches via wire connections. Such an assignment is referred to as the TBF input arrival-time randomizer's configuration.

E. Skewed-Delay Controller:

SCA evaluations often only apply to FR or LR activities. Therefore, it is inefficient to apply large delay modifications to every round. Therefore, we suggest increasing the delay variations just in the 1st and last two rounds. Our suggested skewed-delay controller is shown in Fig. 4 along with the previously shown TBF input arrival-time randomizer. A state machine and two MUXes make up our suggested skewed-delay controller. In order to avoid a delay glitch, two MUXes are used. In the sequence of LUTs and MUX tree, the initial MUX acts as the stabilizing MUX and stabilizes all interior nodes. In the second-through-eighth rounds of AES operation, the bypass MUX allows the handshake signal (Lack) to be bypassed without causing input delay. AES operation is carried out in rounds, and the state machine keeps track of the no. of handshake signals.

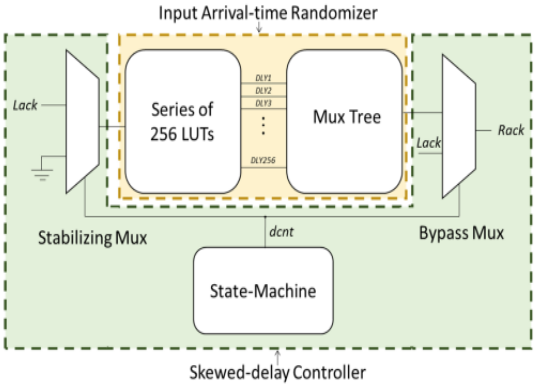

Fig. 4: Block Diagram of Our Proposed Skewed-Delay Controller

F. Chaotic encryption:

A chaotic system has the required security criteria because of its inherent properties, such as pseudo-randomness, instability, and sensitivity to the system's initial conditions and parameters. Fig. 5 depicts the general Chaotic encryption scheme. In order to help in image scrambling, a sequence is then used. Chaotic encryption now has a greater level of security due to the verifiable characteristics of sequence reconstruction and prediction.

Additional categories for recent chaos-based image encryption methods include generalized Fibonacci chaos, fractional calculus, chaotic logistic maps, hyper chaos, fuzzy cellular neural networks, coupling map lattices with mixed multi-chaoses, dynamic chaos and matrix convolution, true random numbers, cyclic shift, chaotic logistic maps, fuzzy cellular neural networks, and fuzzy cellular neural networks.

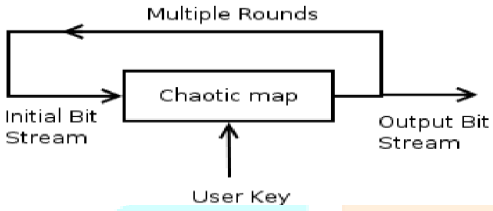

Fig. 5: Chaotic encryption scheme

Chaos is a good for cryptosystems because of characteristics like topological transitivity, ergodicity, and sensitivity to beginning circumstances. Cryptosystems work with finite integers, whereas chaotic systems work with real numbers. This is the main distinction between the two types of systems.

After several iterations, a small change in input results in a significant change in output. Additionally, if the key value is slightly altered, the cypher image is completely altered.

III. RESULTS & DISCUSSIONS

A. RTL Schematic Diagram:

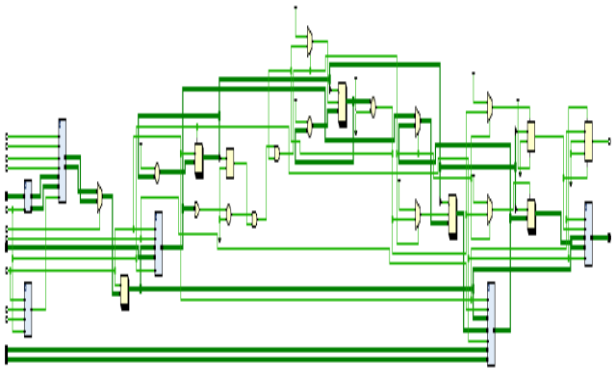

Fig. 6: RTL Schematic Diagram for a Proposed Dual-Hiding Asynchronous-Logic AES Accelerator

The Fig. 6 shows the RTL Schematic Diagram for a Proposed Dual Hiding Asynchronous Logic AES Accelerator.

B. RTL schematic of Skew Delay Generator

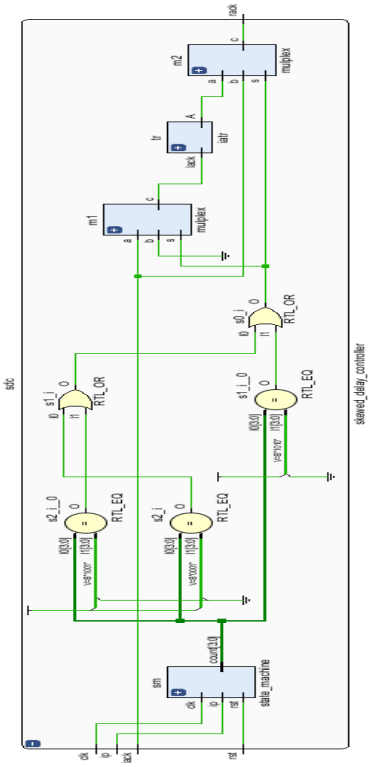

Fig. 7 RTL schematic of Skew Delay Generator.

The RTL schematic of Skew Delay Generator is shown in Fig. 7 which is used to prevent delay glitches with the help of two Mux's.

C. Simulation results:

Fig. 8 Output Waveform for A Proposed Dual-Hiding Asynchronous-Logic AES Accelerator

D. Area:

Name	Slice LUTs (134600)	Slice Registers (269200)	Bonded IOB (400)	BUFGCTRL (32)
AES_encryption_top	1895	1572	273	2
ins1 (AES_AR)	100	128	0	0
ins2 (AES_FR)	1777	1037	0	0

Fig. 9 Area Analysis for a Proposed Work

E. Delay:

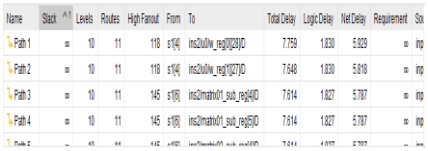

Fig. 10 Delay Analysis for a Proposed Work

F. Power:

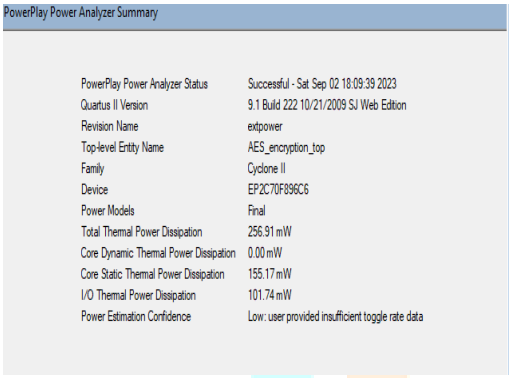

Fig. 11 Power Analysis for a Proposed Work

G. Comparison Table in Terms of Area, Delay, Power:

TABLE 1: Comparison Table in Terms of Area, Delay, Power

	Area (LUT's)	***Delay (ns)***	***Power(mW)***
Existing	2950	8.236	257.16
Proposed	1895	7.759	256.91

The above Table 1 depicts the comparison table in terms of area, delay, power for an existing & proposed work.

IV. CONCLUSION:

We have suggested an asynchronous-logic chaotic AES accelerator that uses "by-design" to provide fine-grain dual-hiding (horizontal and vertical) to reduce SCA while still achieving minimal area/energy overheads. The area-efficient dual-rail mapping technique, the ZV compensated S-Box, the TBF input arrival-time randomizer, and the skewed-delay controller were all included in our suggested asynchronous-logic AES accelerator to offer a low overhead for security design. Along with this, we have included chaotic sequence, which will make it more difficult for data to leak while enhancing data security. We thoroughly compared the various configurations of our proposed TBF input arrival-time randomizer, and then we chose the most secure one to be employed for our asynchronous-logic AES accelerator. In accordance to the evaluation's findings, our suggested asynchronous-logic accelerator can endure SCA with respect to area and energy overhead.

In future to increase the data's security and dependability, various new technologies can be incorporated into embedded systems, such as machine learning, artificial intelligence, IOT, medical, consumer, industrial, telecommunication, automotive, home appliances, commercial, aerospace, and military applications.

REFERENCES

[1] S. Seçkiner and S. Köse, "Preprocessing of the physical leakage information to combine side-channel distinguishers," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., early access, Oct. 26, 2021

[2] W. J. Jun and T. S. Fun, "A New Image Encryption Algorithm Based on Single S-Box and Dynamic Encryption Step," in IEEE Access, vol. 9, pp. 120596-120612, 2021

[3]. A. Pammu, K.-S. Chong, Y. Wang, and B.-H. Gwee, "A highly efficient side channel attack with profiling through relevance-learning on physical leakage information," IEEE Trans. Dependable Secure Comput., vol. 16, no. 3, pp. 376–387, May 2019

[4] K.-S. Chong et al., "Dual-hiding side-channel-attack resistant FPGAbased asynchronous-logic AES: Design, countermeasures and evaluation," IEEE J. Emerg. Sel. Topics Circuits Syst., vol. 11, no. 2, pp. 343–356, Jun. 2021.

[5] W. Shan, S. Zhang, and Y. He, "Machine learning based side-channelattack countermeasure with Hamming-distance redistribution and its application on advanced encryption standard," Electron. Lett., vol. 53, no. 14, pp. 926–928, Jul. 2017.

[6] M. Lecomte, J. Fournier, and P. Maurine, "An on-chip technique to detect hardware trojans and assist counterfeit identification," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 25, no. 12, pp. 3317–3330, Dec. 2017.

[7] A. Mokari, B. Ghavami, and H. Pedram, "SCAR-FPGA: A novel sidechannel attack resistant FPGA," in Proc. 5th Southern Conf. Program. Log. (SPL), Sao Carlos, Brazil, Apr. 2009, pp. 177–182.

[8] S. Mangard, O. Elisabeth, and T. Popp, Power Analysis Revealing the Secret of Smart Cards. Cham, Switzerland: Springer, 2007.

[9] 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, Feb. 2019.

[10] R. Kumar et al., "A time-/frequency-domain side-channel attack resistant AES-128 and RSA-4K crypto-processor in 14-nm CMOS," IEEE J. Solid-State Circuits, vol. 56, no. 4, pp. 1141–1151, Apr. 2021. [11] D. Das et al., "EM and power SCA-resilient AES-256 through >350× current-domain signature attenuation and local lower metal routing," IEEE J. Solid-State Circuits, vol. 56, no. 1, pp. 136–150, Jan. 2021.