Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 2, April : 2024

AN ENHANCED SECURITY FPGA AES ACCELERATOR WITH DUAL-HIDING ASYNCHRONOUS LOGIC FOR SIDE-CHANNEL ATTACK PREVENTION

Mr. Chinchinada Vijaya Srinivasa Rao, PG Scholar, Department of ECE, Sarojini Institute of Technology, Telaprolu, Andhra pradesh, India. chinchinadajagadishkumar99@gmail.com
Mr. Murali Dova, Associate Professor, Department of ECE, Sarojini Institute of Technology, Telaprolu, Andhra pradesh, India. dovamurali20@gmail.com,

***Abstract*:**
Data Security is considered to be a major factor and plays an important role in most of the applications such as e-commerce, internet banking, military, satellite, wireless communications, electronic gadgets, appliances, signal and digital image processing, etc. Cryptography is a technique which is used to keep the data safe and secretby changing it into a form so that unnecessary users cannot understand. This technique provides a strong, economical way to keep our data as a secret and helps in data integrity verification. Cryptography technique is facing issue from side channel attacks and unable to provide error free data. The proposed AES accelerator achieves vertical (amplitude) SCA hiding via an area-efficient dual-rail mapping approach and a zero-value (ZV) compensated substitution-box (S-Box), while enhancing the horizontal (temporal) SCA hiding of asynchronous logic operations via a timing-boundary-free input arrival time randomizer and a skewed-delay controller. This design will decrease the area overhead and provide strong resistance from side channel attacks. The proposed design is executed in Xilinx Vivado/Xilinx ISE and the output is verified using simulation results.
Keywords: Advanced encryption standard (AES), asynchronous logic design, delay randomizer, dual-hiding, side-channel attack (SCA), Data security, Cryptography.

Earlier work:
Large Internet-of-Things (IoT) marketplaces are driving EDGE computing [1], which requires edge devices to process/store more raw IoT data locally and only transfer/share essential IoT data among other edge devices and/or cloud servers. Edge devices must not only have low cost, high performance, and low power features but also high configurability and high security attributes in order to be suitable for a wide range of IoT applications. Secure field-programmable gate arrays (FPGAs), which offer dynamic reconfiguration and enable security and privacy in IoT, represent a promising choice for the latter characteristics. Although the architecture of an application-specific integrated circuit (ASIC) may be altered to offer more security, this takes longer to market since it needs a larger volume (>400 k) to keep costs down [2]. Additionally, due to FPGA's reconfigurability, the countermeasures may be intermittently updated as security threats occasionally change. The design of secure boot, memory, and key generation, malware analysis [3], access authentication, and data encryption are only a few of the factors that must be taken into account in order to create safe FPGAs. One of the primary problems with data encryption using hardware ciphers is the side-channel attack (SCA) [4], which uses physical leakage information (PLI) [5] released by FPGAs to disclose the secret key. Two forms of countermeasures, namely masking [7] and concealment [8], are typically used to combat SCAs. Masking makes an effort to link the PLI with the fictitious SCA models using random masks. In contrast, concealing makes an effort to uniformize or randomize the PLI so that the SCA cannot tell what beneficial information pertains to the secret key. Due to design limitations in FPGA designs, such as fixed mapping unit structure, restricted placement, and routing flexibility, FPGAs are difficult to defend against SCAs. Since FPGA lacks analog components and specialized routing control, several cutting-edge countermeasures like random rapid voltage dithering [9], nonlinear digital low-dropout regulator (LDO) [10], and current-domain signature attenuation [11] cannot be implemented. Although a number of reported FPGA topologies, including application-specific-inflexible FPGA (ASIF) [14],

SCAR-FPGA [13], and tree-based FPGA [12] may alleviate hardware security vulnerabilities, the design complexity is greater and the security has not yet been confirmed. Because they are straightforward and inexpensive, the majority of current FPGAs use a "by-design" strategy, such as adopting masking or concealing countermeasures to reduce SCAs. A true-random-number-generator is needed to guarantee the unpredictability of the masks in order for masking countermeasures to be effective. A low complexity masking countermeasure, such as rotating S-Boxes masking [15], can be achieved by compromising the masks' unpredictability, however doing so may compromise the SCA resistance [8]. A low-order masking countermeasure may not be completely safe against high-order SCAs (HoSCAs), even if the masks are chosen at random [16]. A high order masking countermeasure [17] that conceals a single value using many masks is necessary to protect against HoSCAs, but it is complicated and has substantial overheads. On the other hand, the PLI randomization or uniformization impact must be strong while not causing excessive area/energy overheads in order for hidden countermeasures to be successful. Vertical and horizontal concealing are two possible directions for hiding countermeasures. The vertical concealing seeks to flatten the PLI fluctuations by introducing complementary circuits, such as dual-rail logic [19], or compensating the PLI amplitude by using (redundant) compensators [18]. The unbalanced routing and the early propagation effect (EPE) [20] issues that make hardware ciphers susceptible to SCAs still plague complementary circuits, despite the fact that they can guarantee uniform switching activity. The horizontal concealing, on the other hand, attempts to desynchronize the PLI by randomizing the PLI in time. In order to enable both vertical hiding and horizontal hiding (collectively referred to as dual-hiding), dummy operations [21] and asynchronous-logic (asynchronous-logic) [22], [23] have been used; however, they suffer from either coarse-grain hiding attributes that limit the SCA's resistance or large area/energy overheads.

LITERATURE SURVEY

A. Mokari, B. Ghavami and H. Pedram, "SCAR-FPGA : A novel side-channel attack resistant fpga," 2009 5th Southern Conference on Programmable Logic (SPL), 2009, pp. 177-182

In design of embedded systems for security applications, flexibility and tamper-resistance are two important factors to be considered. High frequency of updates and high costs of ASIC and their long design time urge us to use a secure FPGA as an alternative. In this paper a secure FPGA is proposed for secure implementation of crypto devices. The FPGA architecture is based on Asynchronous methodology and is resistant against multiple side channel attacks such as Power Attacks and Fault Attacks. AES algorithm implementation shows the native resistance of SCAR-FPGA.

Summary: In this paper a side channel attack resistant FPGA was introduced for protecting devices from side channel attacks. This involves power and fault attack resistant which can be done during AES in a FPGA.

Shan, Weiwei & Zhang, Shuai & He, Yunkun. (2017). Machine Learning based Side-Channel-Attack Countermeasure with Hamming-distance Redistribution and its application on AES. Electronics Letters. 53. 10.1049/el.2017.1460.

Side channel analysis (SCA) is effective to reveal the key of crypto devices by applying statistical analysis to a number of power traces, thus hardware countermeasure is necessary to protect the crypto circuits. A SCA-resistance methodology by machine learning trained power compensation module is proposed to compensate the probability of hamming distance (HD) of the intermediate data directly, to make it unable to be distinguished from correct and incorrect sub-key, thus providing resistance to SCA. The machine learning algorithm is used to find out the best HD redistribution mapping by using neural dynamic programming. Implemented on an AES-128 encryption algorithm circuit on a Xilinx Spartan-6 FPGA mounted on a SAKURA-G board, experimental SCA results show that it can provide more than 200 × measures to disclosure and still has no sign to reveal the advanced encryption standard (AES) sub-key. In addition, it has low power and area overhead and zero frequency overhead, thus is appropriate for hardware implementation of

SCA countermeasure.
Summary: In the proposed method, side channel analysis is done for power compensation using machine learning such that resistant from SCA can be done in AES.
M. Lecomte, J. Fournier and P. Maurine, "An On-Chip Technique to Detect Hardware Trojans and Assist Counterfeit Identification," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 25, no. 12, pp. 3317-3330, Dec. 2017.
This paper introduces an embedded solution for the detection of hardware trojans (HTs) and counterfeits. The proposed method, which considers that HTs are necessarily inserted on production lots and not on a single device, is based on the fingerprinting of the static distribution of the supply voltage (Vdd) over the whole surface of an integrated circuit. The measurement of this fingerprint is done through an array of sensors sensitive to the local Vdd value and fingerprint extraction is based on a novel variation model of CMOS logic performance. This model takes into account not only process variations but also the impact of the design (layout, supply routing, and so on). In addition to the fingerprinting process, this paper introduces an adaptive distinguisher to deal with the difficult problem of fixing the p-value on large sets of statistical tests. The efficiency of the whole detection methodology is experimentally demonstrated on a set of 24 FPGA boards.
Summary: In this paper an on-chip technique was proposed for detecting Hardware Trojans which helps in identifying similar attacks which was tested on different FPGA boards.
S. Seçkiner and S. Köse, "Preprocessing of the Physical Leakage Information to Combine Side-Channel Distinguishers," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 12, pp. 2052-2063, Dec. 2021.
The security and privacy of modern computing devices have become an important design metric with the unprecedented increase in the amount of personal information stored in the digital domain. Side-channel attacks have been demonstrated to be one of the primary threats for the security and privacy of these devices. Understanding the working principles of side-channel attacks has, therefore, become an important research problem. An efficient preprocessing technique is proposed in this work for an attack scenario where the amount of time to collect physical leakage (PL) and access to the device is limited. The proposed preprocessing technique utilizes different side-channel distinguishers to decrease the required number of PL measurements for a given success rate by enhancing the quality of the leakage signal. Two commonly used distinguishers, Pearson correlation and mutual information, are combined in this work. For the first time, combined distinguishers are used to improve the performance of both the preprocessing and the attack steps. The success rate of the proposed attack framework outperforms the conventional single distinguisher side-channel attacks by 33% and 30% for unmasked advanced encryption standard (AES) and masked AES, respectively.
Summary: In this paper to overcome the problem of information leakage due to side channel attacks preprocessing is done. By using this technique in AES a significant reduction is observed in terms of leakage information.
A. 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," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 3, pp. 376-387, 1 May-June 2019.
We propose a Profiling through Relevance-Learning (PRL) technique on Physical Leakage Information (PLI) to extract highly correlated PLI with processed data, as to achieve a highly efficient yet robust Side Channel Attack (SCA). There are four key features in our proposed PRL. First, variance analysis on PLI is implemented to determine the boundary of the clusters and objects of the clusters. Second, the nearest-neighbor k-NN variance clustering is used to reduce the sampling points of PLI by clustering the high variance sampling points and discarding the low variance sampling points of PLI measurements (traces). These clustered sampling points, which are highly correlated with the processed data, contain pertinent leakage information related to the secret key.

Third, the information associated with the secret key is spread in several neighboring sampling points with different degrees of leakages. We analytically derive the Key-leakage relevance factor for each clustered sampling point to quantify the degree of leakage associated with the secret key. Fourth, by means of Hebbian learning, a weight proportional to the Key-leakage relevance factor is updated iteratively based on the values of relevance factor and traces of the sampling points. The converged weights which are being assigned to clustered sampling points are linked to their associated PLI to further increase the correlation of the PLI with the processed data. Therefore, the required number of PLI measurements, to reveal the secret key, can be reduced significantly. In addition, we analytically show that the computational complexity of our proposed PRL is O(n) when compared to the reported profiling techniques having O(n2) and O(n3) computational complexities. Based on the experiments of our proposed PRL performed on the PLI of AES-128 algorithm, the results depicting that the sampling points of PLI are reduced 87 percent after the k-NN variance clustering. The converged weight with learning error rate <;1 percent is attained with only 538 iterations. The robustness of our proposed PRL is examined with four different frequencies (embodying four noise levels), various reported profiling techniques and two hiding countermeasures applied on the PLI (vertical and horizontal hidings). Our proposed PRL successfully reduce 94.53-to-98.19 percent of traces when performing at four different frequencies. Based on the hiding countermeasures applied on the PLI, the weights converge at 7,517 iterations and the SCA requires only 523 traces to reveal the secret key. By comparing with reported techniques which require > 106 traces, our proposed PRL is ~2; 000x more efficient in performing SCA.

Summary: In this paper a Profiling through Relevance-Learning (PRL) technique on Physical Leakage Information (PLI) to extract highly correlated PLI with processed data, as to achieve a highly efficient yet robust Side Channel Attack (SCA) is proposed.

K. -S. Chong et al., "Side-Channel-Attack Resistant Dual-Rail Asynchronous-Logic AES Accelerator Based on Standard Library Cells," 2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), 2019, pp. 1-7.

We present a side-channel-attack (SCA) resistant Advanced Encryption Standard (AES) accelerator by means of asynchronous-logic (asynchronous) based on the standard library cells. To mitigate SCA, we adopt the dual-rail logic, and propose a delayed completion tree (to introduce delay variations) and the data flow control (to halt reset operation at the last round). We further perform a comprehensive SCA evaluation (with 7 attacking/power models) by means of power simulations. To the best of our knowledge, such comprehensive SCA evaluation has never been reported for other asynchronous AES or its sub-block designs. Based on the basis of 5k power simulations, we show that our proposed asynchronous AES accelerator are unbreakable. Our proposed asynchronous AES accelerator occupies 420μm×420μm @ 65nm CMOS and dissipates 2nJ/encryption @ 1.2V.

Summary: Here in this paper the author proposed an AES accelerator by asynchronous logic for side channel attack resistant. For doing so dual rail logic, delay completion tree and data flow control has been introduced.

PROPOSED METHOD

Fig. 2 depicts the block diagram of our dual-hiding asynchronous logic AES accelerator, comprising input–output flip-flops with sync-logic state machines, a preround TBF input arrival-time randomizer, single- to dual-rail conversion module, and an asynchronous-logic core. The input–output flip-flops with sync-logic state machines serve as the sync–asynchronous interface circuit, storing the inputs (plaintext and keys) and outputs (ciphertext). The preround TBF input arrival-time randomizer is essentially to randomize the commencement of the dual-rail asynchronous-logic operation and to protect the preround operation from SCA. The asynchronous-logic core is the main AES computing engine, having various building blocks such as rings of asynchronous-logic pipeline [latches with competition detection (CD)] and dual-rail core modules (S-Box, Shift-Row, MixColumn, etc.).

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 2, April : 2024

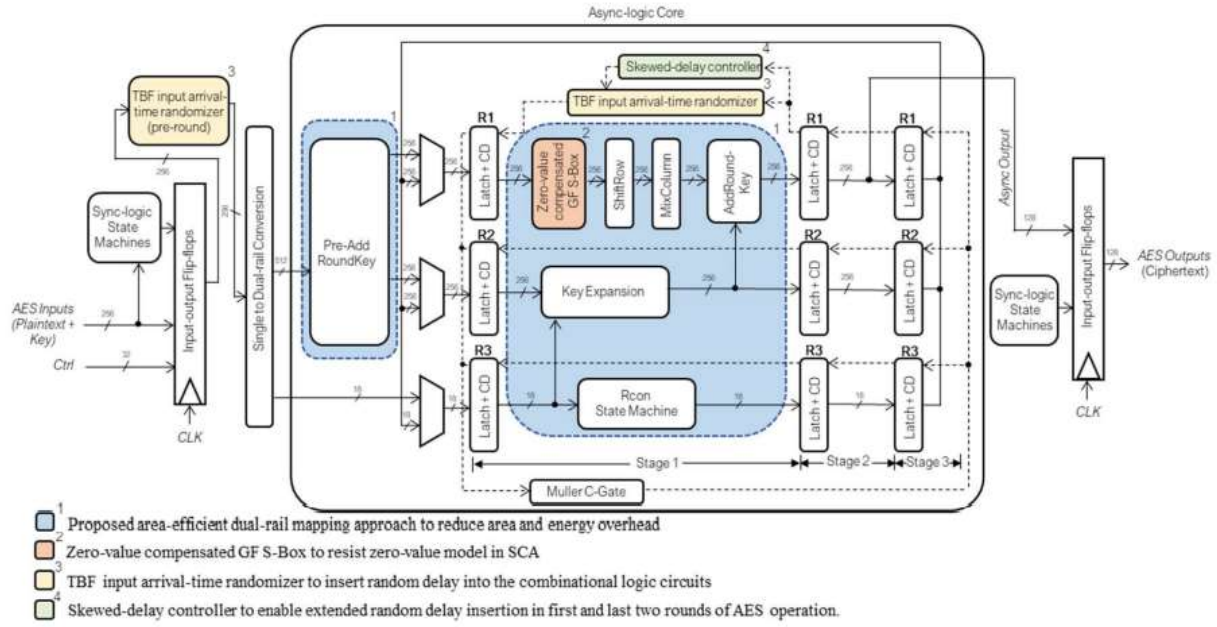

Fig. 1: Block diagram of our dual-hiding asynchronous-logic AES accelerator

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 FR SCA attack (see technical discussion later). 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 (Pre-AddRoundKey), followed by ten 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 (for evaluation) or a null data (for reset) 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 (i.e., latches labeled with R1–R3, respectively, in Fig. 3). The R1 ring performs AES round transformation (S-Box, ShiftRow, MixColumn, and AddRoundKey), the R2 ring performs key expansion, and the R3 ring controls ten rounds of AES transformation via Rcon state machine.

When the encryption is started, the latches in Stage 1 will first receive the data from Pre-AddRoundKey module via the multiplexers (MUXes). Based on the successful receival of the data by the latches in Stage 1, the MUXes will be switched to establish three rings, R1–R3. For each ring, we need a minimum of three stages (i.e., Stages 1–3 in Fig. 3) to form a complete asynchronous cyclic data propagation [41]. Particularly, each ring is formed by passing the data from Stage 1 to Stage 2, Stage 2 to Stage 3, and Stage 3 back to Stage 1 again. The dotted lines in Fig. 3 represent the handshake Lack signals of the latches (in each ring), thus controlling the propagation of the valid and null data in Stages 1–3. The Muller C-Gate will synchronize all the Lack signals (from the latches of R1–R3) in Stage 1. This synchronization in Stage 1 is to ensure that the AES data, AES key, and Rcon are all updated/stored in the latches in Stage 1 before a new round of AES transformation is initiated. Ten rounds of asynchronous-logic AES transformation are performed with the valid and null data cycling through Stages 1–3. After the tenth round, the Rcon state machine will stop the asynchronous-logic operation, and the ciphertext will be stored in the R1 latch in Stage 2, ready to be

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 2, April : 2024

retrieved by the input–output flip-flops. The sync-logic state machines will control the flip-flops to fetch the data stored in the latches after ten clock cycles. Hence, conceptually, our asynchronous-logic AES accelerator is globally synchronous, locally asynchronous (GSLA), with the assumption that the AES encryption will be finished within ten clock cycles.

Area-Efficient Dual-Rail Mapping Approach

A common dual-rail cell, which comprises a true-rail and a false-rail, requires at least 2× the number of gates (as compared to a single-rail cell). They propose to integrate any dual-rail cells with less than five inputs into one 6-input LUT. These dual-rail cells include two-input AND, OR, NAND, NOR, XOR, and XNOR gates. Our proposed mapping approach needs just one LUT, much more area-efficient.

ZV Compensated GF S-Box

The hardware implementation of S-Boxes is crucial in reducing the area and PLI dissipation. Although a GF S-Box is area-efficient, it suffers from the ZV SCA problem. In order to enjoy the small area properties of GF S-Box and yet to prevent the ZV problem, a ZV compensated GF S-Box is proposed. The ZV problem is prevented by adding two MUXes The first MUX detects whether the S-Box input is zero and passes a dummy data p into the S-Box if it is true. The second MUX detects whether the S-box input is zero too. If yes, the second MUX will wait for the dummy data to pass through the circuits, until the second MUX detects q in the output of GF(24), where q is the expected output of GF(24) when the S-Box input is p. p can be any nonzero dummy value, while making sure that q is the corresponding GF(24) output of p. For our proposed ZV compensated S-Box, we choose p to be “8” while its corresponding q is “1.” Once q is detected, the second MUX will put back the correct output, which is zero into the subsequence circuits.

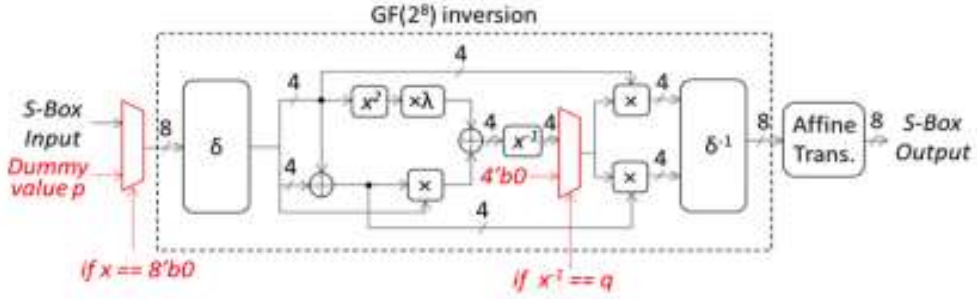

Fig. 2: Proposed ZV compensated GF S-Box

TBF Input Arrival-Time Randomizer

To increase the horizontal hiding feature, we propose a TBF input arrival-time randomizer to insert random delays to the local handshake signals (Lack) which control the “release” of the data into dual-rail core modules.

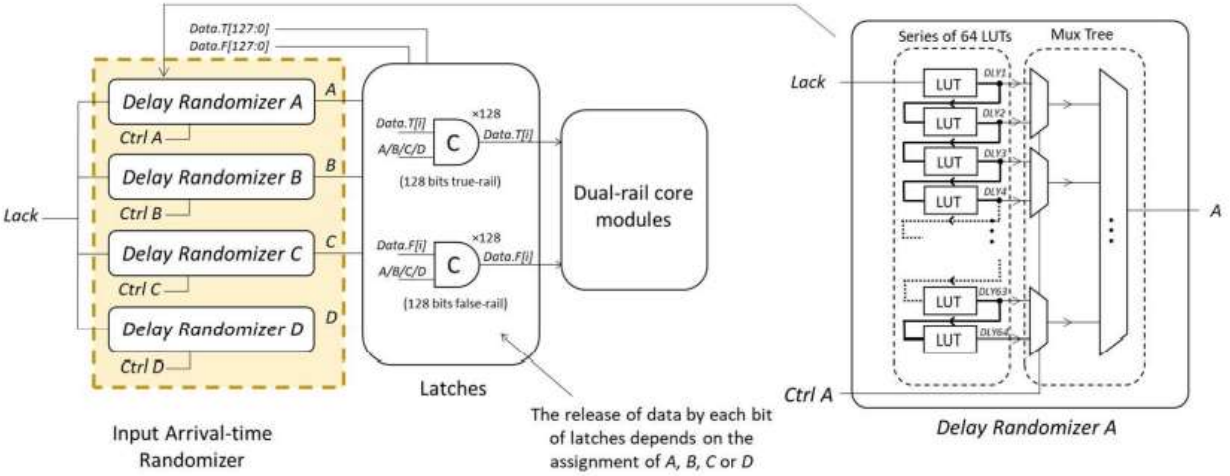

Fig. 3: (a) Block diagram of our proposed TBF input arrival-time randomizer. (b) Internal circuitries

of a delay randomizer.

Fig. 4(a) depicts our proposed TBF input arrival-time randomizer which comprises four delay randomizers (i.e., delay randomizers A, B, C, and D). Each delay randomizer is made up of a series of 64 LUTs and of a MUX tree allowing the inserted delay to vary from 1 to 64 unit-delays, as depicted in Fig. 7(b). The Ctrl signal is a primary input, serving as a random signal to our proposed asynchronous-logic AES accelerator that defines the number of unitdelays to be incurred. For simplicity and our SCA evaluation purpose only, we generate the Ctrl signal based on plaintext via external XOR operations for the first encryption and based on the previous ciphertext via external XOR operations for the subsequent encryptions to achieve randomness. The delay randomizers A–D are connected to the latches, thus manipulating the input arrival time of the data to dual-rail core modules. In our asynchronous-logic design, each bit of latch can "release" data independently, i.e., each bit of data may have different input arrival times. Since there are four delay randomizers in our proposed TBF input arrival-time randomizer, we may group the latches (128-bits true-rail + 128-bits false-rail) into four groups, by assigning the outputs of each delay randomizer to particular latches through wire connections. We denote such assignment as the configuration of TBF input arrival-time randomizer.

Skewed-Delay Controller

In general, the SCA evaluations only apply to the FR or LR operations. Hence, applying wide delay variations to all the rounds is not efficient. Hence, we propose to increase the delay variations only at the first and last two rounds. Fig. 11 depicts our proposed skewed-delay controller (marked in green) coupled with the TBF input arrival-time randomizer depicted in Fig. 7 previously. Our proposed skewed-delay controller comprises a state-machine and two MUXes. The two MUXes are used to prevent a delay glitch. The first MUX is the stabilizing MUX, stabilizing all the internal nodes in the series of LUTs and MUX tree. The second MUX is the bypass MUX where the handshake signal (Lack) can be bypassed without incurring input delay during the second–eighth rounds of AES operation. The state machine counts the number of handshake signal, which is corresponding to the number of rounds of AES operation.

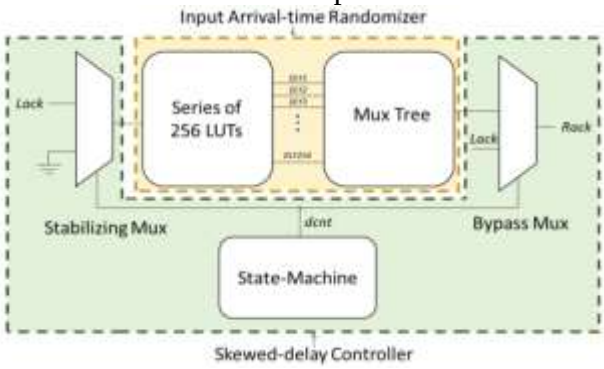

Fig. 4: Block diagram of our proposed skewed-delay controller

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 2, April : 2024

Results:

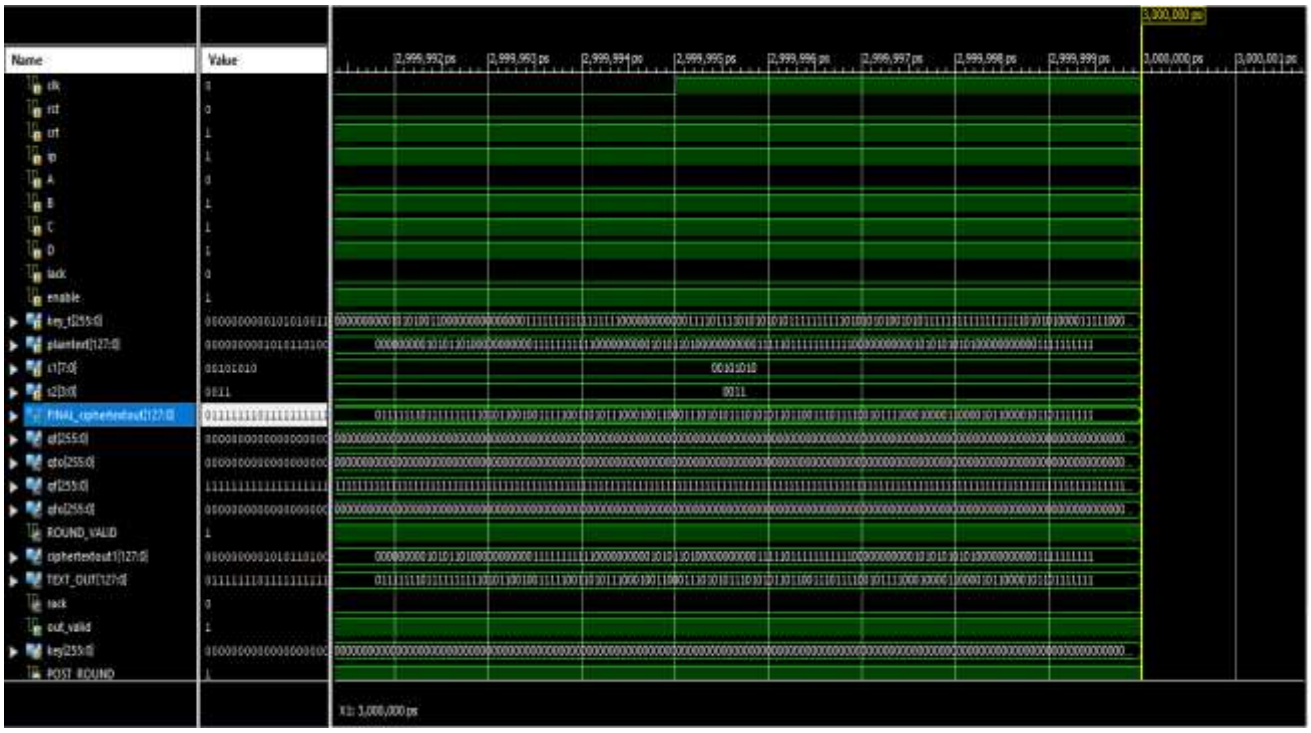

Fig: 5 Simulation Results

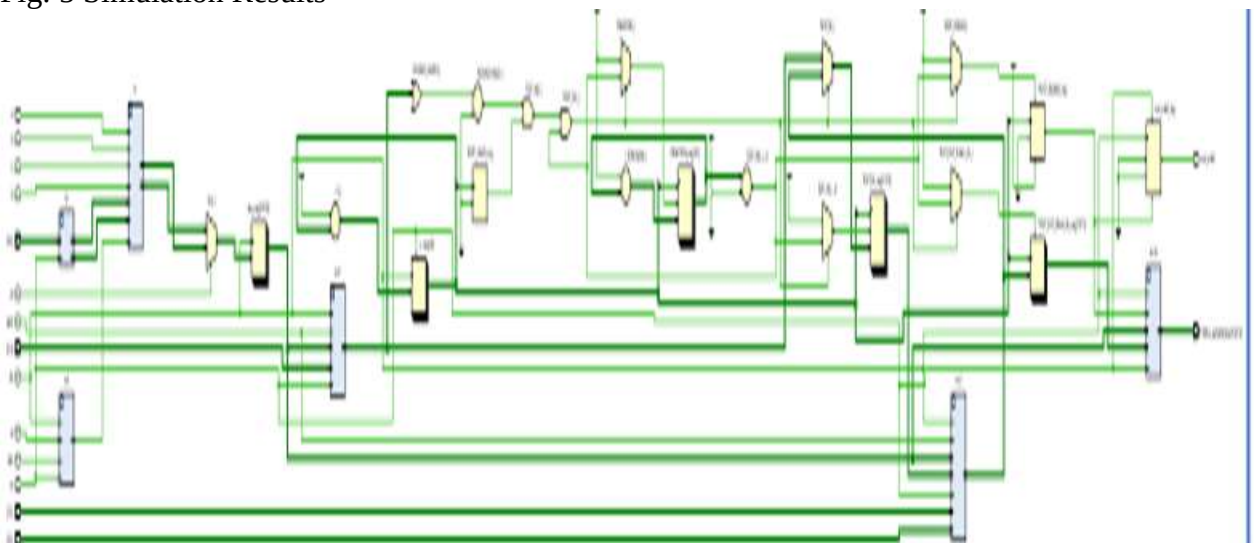

Fig 6: Fig: RTL schematic

Evaluation table for Area, Delay:

	Area (LUT's)	**Delay (ns)**
Proposed	2914	8.248

CONCLUSION

We have proposed an asynchronous-logic AES accelerator for secure FPGAs, by using "by-design" approaches in FPGA to enable a fine-grain dual-hiding (horizontal and vertical) to mitigate SCA and yet to achieve low area/energy overheads. Our proposed asynchronous-logic AES accelerator incorporated our area-efficient dual-rail mapping approach, ZV compensated S-Box, TBF input arrival-time randomizer, and skewed-delay controller to enable a low overhead-for-security design. We have comprehensively evaluated our proposed TBF input arrival-time randomizer with different configurations and selected the most secure configuration to be used for our asynchronous-logic AES accelerator. The evaluation results have shown that our proposed asynchronous-logic accelerator can

withstand SCA with 20 million traces, which is the most secured FPGA-based design, with area and energy overhead of 4.3× and 1.5×, respectively. Based on our figure of merit (Area × Energy/MTD(All)×106), our proposed design featured only 0.3, which is 403× smaller than the sync-logic WDDL and 95× smaller than the reported asynchronous-logic design.

REFERENCES

[1] Y.-W. Hung, Y.-C. Chen, C. Lo, A. G. So, and S.-C. Chang, "Dynamic workload allocation for edge computing," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 29, no. 3, pp. 519–529, Mar. 2021.
[2] S. Bhunia and M. Tehranipoor, Hardware Security: A Hands-on Learning Approach. Amsterdam, The Netherlands: Elsevier, 2019.
[3] 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.
[4] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," J. Cryptograph. Eng., vol. 1, no. 1, pp. 5–27, Apr. 2011.
[5] 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, doi: 10.1109/TVLSI.2021.3115420.
[6] A. 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.
[7] C. H. Gebotys, "A table masking countermeasure for low-energy secure embedded systems," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 14, no. 7, pp. 740–753, Jul. 2006.
[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.
[12] E. Amouri, S. Bhasin, Y. Mathieu, T. Graba, and J.-L. Danger, "Countering early propagation and routing imbalance of DPL designs in a tree-based FPGA," in Proc. Int. Conf. IC Design Technol. (ICICDT), Leuven, Belgium, Jun. 2015, pp. 1–4.
[13] 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.
[14] M. A. Qureshi and H. Parvez, "Design-space exploration between FPGA and ASIF," in Proc. 9th Int. Symp. Reconfigurable Commun.-Centric Syst. Chip (ReCoSoC), Montpellier, France, May 2014, pp. 1–5. [15] M. Nassar, Y. Souissi, S. Guilley, and J.-L. Danger, "RSM: A small and fast countermeasure for AES, secure against 1st and 2nd-order zerooffset SCAs," in Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE), Dresden, Germany, Mar. 2012, pp. 1173–1178.
[16] G. Dabosville, J. Doget, and E. Prouff, "A new second-order side channel attack based on linear regression," IEEE Trans. Comput., vol. 62, no. 8, pp. 1629–1640, Aug. 2012.
[17] M. Rivain and E. Prouff, "Provably secure higher-order masking of AES," in Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst., Santa Barbara, CA, USA, 2010, pp. 413–427.
[18] 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.
[19] S. Guilley, L. Sauvage, J.-L. Danger, T. Graba, and Y. Mathieu, "Evaluation of power-constant dual-rail logic as a protection of cryptographic applications in FPGAs," in Proc. 2nd Int. Conf. Secure Syst. Integr. Rel. Improvement, Yokohama, Japan, Jul. 2008, pp. 16–23.
[20] A. Moradi and V. Immler, "Early propagation and imbalanced routing, how to diminish in FPGAs," in Cryptographic Hardware and Embedded Systems (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2014, pp. 598–615.
[21] S. Attari, A. R. Shahmirzadi, M. Salmasizadeh, and I. Gholampour, "Finite state machine based countermeasure for cryptographic algorithms," in Proc. 14th Int. Conf. Inf. Secur. Cryptol. (ISCISC), Shiraz, Iran, Sep. 2017, pp. 58–63.
[22] S. Kotipalli, Y.-B. Kim, and M. Choi, "Asynchronous advanced encryption standard hardware with random noise injection for improved sidechannel attack resistance," J. Electr. Comput. Eng., vol. 2014, pp. 1–13, Jan. 2014.
[23] K.-S. Chong et al., "Side-channel-attack resistant dual-rail asynchronous-logic AES accelerator based on standard library cells," in Proc. Asian Hardw. Oriented Secur. Trust Symp. (AsianHOST), Xi'an, China, Dec. 2019, pp. 1–7.