LETTER

28nm asynchronous area-saving AES processor with high Common and Machine Learning Side-Channel Attack resistance.

Qingyun Zou¹, Xiaoxin Cui^{1, a)}, Zhenhui Dai¹, Yisong Kuang¹, Yi Zhong¹, Chenglong Zou¹, and Xiaole Cui²

Abstract An asynchronous Advanced Encryption Standard (AES) cryptographic processor for low-area and side-channel attack (SCA) resistant applications is introduced. To reduce the area and power, two Substituting Byte blocks (S-Boxes) are reused in key expansion and the data encryption module, respectively. To mitigate SCA, we adopt asynchronous dual-rail logic with dual-rail balanced logic and new dual-rail spacer latch. Common and Machine learning (ML) SCA simulations are performed to validate SCA resistance. To the best of our knowledge, we are the first ones to perform the ML SCA evaluations on asynchronous AES. Simulation results with 200K power traces demonstrate that our asynchronous AES is immune to the attacks. Our proposed asynchronous AES occupies an area of 0.016 mm² in TSMC 28nm technology and consumes 1nJ per encryption at a supply voltage of 0.9V.

key words: Advanced Encryption Standard (AES), asynchronous circuit, side-channel attack (SCA)

Classification: Integrated circuits

1. Introduction

Security problem draws more attention in the Internet of things (IoT) system. Encryption algorithms such as Advanced Encryption Standard (AES) [1] can be adopted to avoid the data being obtained by others on the internet. AES transforms plaintext into ciphertext with a cryptographic key. The transformation composes of ten-round operations. Each round iteration includes S-Box, Shift-Row, Mix-Column, and Add-Round except for the last round which does not include Mix-Column. The most complicated operation is S-Box, whose implementation includes two different types, a look-up table, or Galois-field (GF) arithmetic. Implementing S-Box with GF arithmetic is more area-efficient than a look-up table [2].

In an embedded system, it is vital to take the AES cryptographic processor into overall consideration. On one hand, to meet the area-saving demand, a processor

with only two GF arithmetic S-Boxes is superior although it reduces the throughput. On the other hand, the AES cryptographic processor will be vulnerable if it is physically attacked. SCA can reveal the key on the basis of the relationship between the chip power and the processed data [3]. Concerning the ability to resist SCA, asynchronous circuits such as the dual-rail ones are more powerful than the synchronous circuit [4]. Hence, our design exploits redesigned asynchronous logic to improve the SCA resistance of AES. We also perform comprehensive SCA evaluations including common and ML SCA simulations. As far as we know, we are the first ones to perform ML SCA evaluations on asynchronous AES.

2. Circuits adopted in our asynchronous AES design.

Asynchronous circuits can be classified into four types: self-timed circuit, Speed-Independent circuit, Delay-Insensitive circuit, and Quasi-Delay-Insensitive (QDI) circuit according to the delays of wires and gates [5, 6, 7]. To improve the SCA resistance, the dual-rail four-phase handshake style circuit, one kind of QDI circuit, is adopted in our design. In the dual-rail protocol, each bit is encoded with two bits $d.t$ and $d.f$ in Fig.1(a). The condition that $d.t$ and $d.f$ both are 1 is not allowed in the dual-rail protocol in Fig.1(b). Furthermore, the four-phase protocol refers to a process introduced in Fig. 1(a). Considering that logic 1 represented by $d.t=1$ and $d.f=0$ is transmitted, the value is then acknowledged by a low-to-high transition of the *Ack* signal. Once $d.t$ and $d.f$ both return to zero, the *Ack* signal will be also reset to 0, indicating the empty state of the transmission channel. Then a pair of new data can be loaded on this channel.

Fig. 1 (a) Waveform of the asynchronous dual-rail protocol. (b) The rule of dual-rail encoding of QDI.

¹Ministry key laboratory of Microelectronics devices and Circuits, Peking University, Beijing 100871, China.

² School of Electronic and Computer Engineering, Peking University, Shenzhen 100101, China.

a) cxx@pku.edu.cn

Muller C-element is essential in asynchronous circuits. Dual-rail unit consists of *C-element* and other basic units in Delay-insensitive Min-term Synthesis (DIMS) QDI dual-rail way. The *C-element* is implemented with standard cells represented by the schematic in Fig. 2(a). The truth table of the *C-element* is shown in Fig. 2(b). Its function is $out = AB + out(A + B)$.

Fig. 2 (a) Symbol and schematic of Muller *C-element*. (b) Truth table of *c-element*.

2.1 Dual-rail balanced asynchronous circuit

The DIMS dual-rail asynchronous circuit has an innate ability to balance the power consumption, and we further redesigned the dual-rail logic to improve SCA resistance in our design. The dual-rail AND unit and dual-rail XOR unit, comprised of standard cells, are designed as follows in Fig. 3(a) and Fig. 3(b). The dual-rail AND is composed of four *Muller C-element* circuits, two buffers, and two OR3 circuits. To keep a power-balanced data path, the buffers attached to the ground (GND) keep the same size as the *Muller C-element* circuit. The structure of the dual-rail OR circuit in Fig.3(c) is similar to AND. In this way, every data path between each input and each output of these units consumes almost the same energy, which ensures independence between the consuming power and the logic operation. Compared with the recent asynchronous dual-rail AES work [7], this design can improve security by ensuring the power balance between different data paths.

Fig. 3 (a) Dual-rail balanced AND logic. (b) Dual-rail balanced XOR logic. (c) Dual-rail balanced OR logic.

2.2 New dual-rail spacer latch

Some articles have addressed that the dual-rail spacer latch is safer than the ordinary dual-rail latch [8]. However, we adopt a new dual-rail spacer latch which is

simpler than [8]. The structure of the spacer latch is shown in Fig. 4. The ports *d.t_in*, *d.f_in*, *d.t_out* and *d.f_out* are the dual-rail style like Fig.1. The function of the port *Ack* is the same as *Ack* in Fig1. b. The spacer latch is reset to an empty state before a write operation even though the previously stored data are the same as the data written. The data transformation of the spacer latch has four conditions in Table I. When data transforms from 0 to 0, the dual-rail encode transforms from 01 to 00 to 01 so *d.f* has two changes including from 0 to 1 and from 1 to 0. Here, all the four transformations have been considered and the dual-rail encodes of those conditions always go through both 0 to 1 and 1 to 0 changes as listed in Table I, so each transformation has the same toggle rate. Therefore, the dynamic power is not correlated to the data transformation in the spacer latch. However, the ordinary latch has a 2-bit change only when the previous data are different from the written data so the dynamic power consumed in the latch correlates with the data transformation. In a word, the spacer latch is suitable for security designs in spite of more power and area.

Fig. 4 Structure of the adopted spacer latch

Table I Data transformations of the spacer latch

Four cases of writing	The dual-rail data transformation	d.t	d.f
From 0 to 0	01 to 00 to 01		1 to 0 and 0 to 1
From 0 to 1	01 to 00 to 10	0 to 1	1 to 0
From 1 to 1	10 to 00 to 10	1 to 0 and 0 to 1	
From 1 to 0	10 to 00 to 01	1 to 0	0 to 1

3. Implementation of our asynchronous AES cryptographic processor

We propose a 2-S-Box architecture that is area-efficient and less power-consuming for the 128-bit AES core in Fig. 5(a). Our design includes GF-S-Box, Shift-Row, Mix_Column, Serializer (get a sequence of bytes from input), Key expansion unit, and Dual-rail spacer latch. The structure is modeled after the design of [9]. We adopt the asynchronous dual-rail style and replace

registers with dual-rail spacer latch, which differs from [9]. Besides, all the computation circuits are made up of dual-rail balanced logic, which makes our design more secure than [9]. Overall, the encryption process is divided into four dual-rail spacer power-balanced pipelines. The key expansion unit is just one dual-rail spacer power-balanced pipeline. Each pipeline is composed of combination logic (*comb*), completion checking logic and a dual-rail spacer latch in Fig.6. The combination logic is based on dual-rail balanced units. The completion checking logic checks if the inputs and outputs of combination logic are valid, which controls the previous and status of output pipeline. The dual-rail spacer latch stores the processed data. The signal *ackout* indicates the data are already stored while the signal *ackin* shows the data has been captured by the pipeline. All the critical data paths in pipeline including (*din.t-dout.t*, *din.t-dout.f*, *din.f-dout.f* and *din.f-dout.t*) are designed to consume the same power by redesigning the dual-rail balanced unit, C-elements and dual-spacer latches. Hence, every data path between key and ciphertext and between plaintext and ciphertext is power-balanced to guarantee data independence with power. The SCA resistance is improved a lot by the method.

Fig. 5 Architecture of the asynchronous AES cryptographic processor.

Fig. 6 Dual-rail spacer pipeline.

GF arithmetic rather than look-up table is utilized to improve area efficiency. The operation of S-Box in GF includes a Multiplicative Inversion in $GF(2^8)$ and affine transformation [2]. However, the operation in $GF(2^8)$ is expensive. Thus, the inputs are mapped to a composite-field of $GF(2^4)^2$ using a mapping transformation, where the computation involves 4-bit logic [10]. After a series

of operations, $GF(2^4)^2$ multiplications, additions, squaring and inverse computation, the output is mapped back into $GF(2^8)$. Finally, an affine transformation performed by matrix multiplication and addition is followed.

Interface ports and layout view of the asynchronous AES cryptographic processor are shown in Fig. 7. The layout is designed carefully to ensure that the wire paths between the dual-rail circuits are almost the same length. Otherwise, the parasitic effects of the wire will undermine the power balance of dual-rail spacer pipeline. The design is based on standard library cells in TSMC 28nm CMOS technology at a supply voltage of 0.9V.

Fig. 7 (a) Input and output ports of the AES cryptographic processor. (b) Layout view of the asynchronous AES cryptographic processor.

The waveform in Fig.8 depicts the data transformation of the input and output ports in Fig.7(a) during one complete asynchronous AES encryption. The signal *Initialize* is used to reset the asynchronous AES in Fig.8. The encryption begins when *Start* is high. Then the asynchronous AES requests for *Key* which is encoded in the dual-rail protocol by setting *Key_req* high. After the *Key* is received, *Key_req* returns to low. Afterward, the asynchronous AES requests for *Plaintext* encoded in the dual-rail protocol by setting *Plaintext_req* high, which is the same as the transmission of *Key*. When *Ciphertext* turns from empty to valid, *Ciphertext_ack* becomes high, which indicates one encryption of asynchronous AES is done.

Fig. 8 Waveform of an asynchronous AES encryption.

4. Simulation of side-channel attack

We perform an SCA simulation by collecting power traces from Synopsys power compiler. We sampled 200K power traces at 0.4ns (2.5GHz) with a 24-bit dynamic range. At last, the Value Change Dump(VCD) file is almost 10Tbytes, which takes two weeks to get these samples. Although the simulation power traces are not real physical power traces, they can be a reasonable assessment for the realistic scenario, because we have extracted the parasitic capacitance from the layout to perform the simulation. If the circuit can resist SCA with a certain number of simulation power traces, it can resist SCA with more real tested power traces in consideration of the real noise interference and process variation [7].

4.1 Common SCA simulations

Common SCA can be divided into Differential Power Analysis (DPA) and Correlation Power Analysis (CPA) [11, 12]. CPA can be further classified into sub-types due to different leakage models. In addition to the correlation, common SCA needs to assume the power trace with a certain leakage model. The leakage model includes certain kinds of models such as Hamming Weight (HW), Hamming Distance (HD), and Switch distance (SD) [13]. Several simulations including CPA and DPA are performed on our asynchronous AES, in which the attack point is selected at the first round of asynchronous AES encryption. Two randomly selected power traces are depicted in Fig. 9(a). The traces are different in the peak value and time. Fig. 9(b), (c), (d) depicts the correlations between the leakage information and the processed data according to the HW, HD, SD for the first byte of the key, respectively. It is evident that the sub-key is not deciphered because the correlations do not have an obvious bias. Compared with the unprotected AES that can not resist common SCA with 5K power traces according to [7], our asynchronous AES can resist common SCA with 200K power traces.

Fig. 9 (a) Two random power traces. (b) Correlation between the power and the processed data by HW. (c) Correlation between the power and the processed data by HD. (d) Correlation between the power and the processed data by SD

4.2. ML SCA simulations

Also, some Machine Learning (ML) methods like multi-layer perceptron networks (MLP) [14, 16, 18] and convolutional neural networks (CNN) [15, 16, 17, 18] can be exploited to perform SCA on cryptographic circuits. The CNN and MLP SCA have been simulated on our asynchronous AES, whose models are built from the unprotected synchronous AES power trace. The unprotected synchronous AES which is designed with the synchronous circuit has the same architecture as our asynchronous AES. We use 10k power traces of the unprotected synchronous AES to train the models. The inputs of CNN and MLP are power trace while the output of CNN and MLP are the sub-key in the training. The two models are trained by 75 epochs. Once the training is finished, these models are built.

Our selected MLP architecture is 4 hidden layers with 256 neurons and at the learning rate of 0.001. Our selected CNN architecture is made up of 5 convolution layers, 5 average pooling layers, 3 fully connected layers, and a learning rate of 0.001 [19]. They are the most optimal choices because they have the best validation and test accuracies on the unprotected AES according to our experiments. The performances of the two models are shown as follows in Fig. 10 when they are attacking the unprotected AES with 10K power traces required by the same method as the asynchronous AES simulation. The two models can both achieve high accuracies to predict the key, which proves that our models are effective to attack the unprotected AES.

Fig. 10 (a) MLP training and validation accuracy on the unprotected AES. (b) CNN training and validation accuracy on the unprotected AES.

The MLP and CNN are trained with a label of the key for our asynchronous AES SCA simulations, which adopts the same network structure as that attacking the unprotected AES. The two models' performances are shown in Fig.11(a) and Fig.11(b). Because their validation accuracies are almost zero without high variation during the training in Fig. 11(a) and Fig.11(b), validation accuracies look flat. It demonstrates that improving the models' accuracies during training is hard

and the chosen models do not work well in attacking our AES. The two models do not classify the key bytes correctly (blue dots represent right classifications and the accuracy $\frac{1}{256} \approx 0.3\%$ is close to random) in Fig.12, which proves our asynchronous AES can not be deciphered by MLP and CNN SCA with 200K traces. Therefore, compared with unprotected AES, our asynchronous AES has higher SCA resistance than the unprotected AES. The ML SCA resistance has improved by 200K/10K=20 times.

Fig. 11 (a) MLP training and validation accuracy on our AES. (b) CNN training and validation accuracy on our AES.

Fig. 12 (a) CNN SCA test accuracy. (b) MLP SCA test accuracy.

Table II Comparison with the state of art ML SCA evaluations

	The kinds of ML SCA	MTD	Countermeasures
[24]	MLP	>10M	Current-domain signature attenuation
[25]	CNN	<200K	Rotating S-box Masking
[26,27]	The specific training algorithm	>1.5M	ML-based HD redistribution compensation
Ours	MLP, CNN	>200K	Asynchronous balanced dual-rail circuit with the new spacer latch

Table II shows a comparison with the state-of-the-art ML SCA evaluations. As a large number of power traces have been collected in these works (simulations or actual power traces from test chip), they have not realigned power traces with alignment methods such as phase-only Correlation (POC) and amplitude-only correlation (AOC) [20, 21, 22, 23], which is the same as our SCA evaluations. Our evaluation results cover a wider range of ML SCA including MLP and CNN than others. Compared with other designs, we focus on asynchronous circuit unit optimization. It is a bottom-level circuit optimization for security. It is testified that the proposed asynchronous dual-rail balanced circuit with the new

spacer latch is effective in improving the resistance of different ML SCAs and has high MTD (measurement-to-disclosure).

5. Comparison with the state of art designs

At last, we compare the previous asynchronous AES counterparts with our proposed AES cryptographic processor regarding SCA resistance, energy, and area in Table III. As is shown in Table III, our work performs better in area and SCA evaluations, despite that the ciphering time is longer. This is caused by two reasons. One is that only two S-Boxes are used, which limits bandwidth and speed. The other is that the spacer latch is reset to zero before being updated, which is more time-consuming than an ordinary dual-rail latch. Besides, compared with [7] that adopted the asynchronous dual-rail circuit and delayed completion and performed only common SCA simulations with 5k power traces, we redesigned the asynchronous circuit units such as dual-rail balanced circuits and dual-rail spacer latch and performed both common SCA and ML SCA with 200K power traces. Although these balanced gates and spacer latch increase area, our design outperforms in area compared with [7,28,29] because we reduce the number of S-boxes from 20 to 2.

Table III Comparison with other state of art asynchronous AES processors

	[29]	[28]	[30]	[7]	This work
Process(nm)	130	130	180	65	28
Number of S-Box	20	20	Not cited	Not cited	2
Ciphering Time(ns)	850 (425)*	300 (150)*	6400 (2311)*	200	520 (1207)*
Voltage(v)	1.2	1.2	--	1.2	0.9
Energy/per encryption(n J)	10.2 (2.6)*	1.6 (0.4)*	76.0 (9.9)*	2.0	1.0 (5.4)*
Area without pads(mm ²)	0.49 (0.123)*	0.64 (0.16)*	0.430 (0.056)*	0.176	0.016 (0.086)*
SCA evaluation	No	No	DPA	CPA, DPA	CPA, DPA, MLP, CNN
MTD (without trace alignment)	No	No	>33K	>5K	>200K

(*)normalized data regarding the 65nm technology process

6. Conclusion

This work implements an area-saving and high SCA resistant asynchronous AES cryptographic processor in QDI dual-rail way. Only two S-Boxes are employed to minimize the area. Dual-rail balanced logic and a new spacer latch are utilized to enhance SCA resistance. Also,

we have carefully designed the layout to ensure the same data path length between dual-rail units. Moreover, different common SCA simulations including DPA and CPA, and ML SCA simulations including MLP and CNN are carried out on our design. The simulation results show that our asynchronous dual-rail AES cryptographic processor exhibits high SCA resistance, which demonstrates that the asynchronous dual-rail balanced circuit with our new dual-rail spacer latch is competitive in improving the SCA resistance of AES. Compared with other asynchronous AES works, our design outperforms them in area and security.

Acknowledgments

This work was supported by the National Key Research and Development Program of China (Grant No. 2018YFB2202605), National Natural Science Foundation of China (Grant No. 61421005) and 111 Project (B18001).

References

- [1] National Institute of Standards and Technology, Advanced Encryption Standard (AES) (2001) FIPS PUB 197.
- [2] Canright D: "A Very Compact S-Box for AES," *Cryptographic Hardware and Embedded Systems (CHES)* (2005) (DOI: 10.1007/11545262_32).
- [3] S. B. Ors et al., "Power-analysis attack on an ASIC AES implementation," *Proc. ITCC.*, vol. 2, pp. 546-552, Apr. 2004.
- [4] Sparso, J., and Furber, S: *Principles of Asynchronous Circuit Design: A System Perspective* (Kluwer Academic Publishers, Boston, 2001) 177.
- [5] Peter A. Beerel, Recep O. Ozdag, Marcos Ferretti: *A Designer's Guide to Asynchronous VLSI* (Cambridge University, California 2010) 97.
- [6] E. Yahya and L. Fesquet: "Asynchronous design: A promising paradigm for electronic circuits and systems," *IEEE International Conference on Electronics, Circuits and Systems* (2009) 339 (DOI: 10.1109 / ICECS.2009.5411009).
- [7] Chong, K. S, et al: "Side-Channel-Attack Resistant Dual-Rail Asynchronous-Logic AES Accelerator Based on Standard Library Cells," *IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST)* (2019) 1 (DOI: 10.1109/AsianHOST47458.2019.9006690).
- [8] Sokolov, D, et al: "Design and analysis of dual-rail circuits for security applications," *IEEE Transactions on Computers* (2005) 449 (DOI: 10.1109 / TC.2005.61).
- [9] P. Hämäläinen, T. et al: "Design and implementation of low-area and low-power AES encryption hardware core," 9 *EUROMICRO Conference on Digital System Design (DSD'06)* (2006) 577 (DOI: 10.1109/DSD.2006.40).
- [10] Morioka S. and Satoh A: "An Optimized S-Box Circuit Architecture for Low Power AES Design," *Cryptographic Hardware and Embedded Systems (CHES)* (2002) (DOI: 10.1007/3-540-36400-5_14).
- [11] Brier E., Clavier C., Olivier F: "Correlation Power Analysis with a Leakage Model. *Cryptographic Hardware and Embedded Systems*" (CHES) (2004) 3156 (DOI: 10.1007/978-3-540-28632-5_2).
- [12] A. Chakraborty, et. al: "Correlation power analysis attack against STTMRAM based cyptosystems," *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, (2017) 171 (DOI: 10.1109/HST.2017.7951835).
- [13] Kocher, P. C. , J. Jaffe , and B. Jun . *Differential Power Analysis*. (Springer US, 2007) 1.
- [14] H. Liu, et. al: "AES Key Recovery Based on Switching Distance Model," *International Symposium on Electronic Commerce and Security (ISECS)* (2010) 218 (DOI: 10.1109/ISECS.2010.55).
- [15] Martinasek Z, et. al: "Profiling Power Analysis Attack Based on Multi-layer Perceptron Network." *Computational Problems in Science and Engineering. Lecture Notes in Electrical Engineering*, Springer, Cham (2015) (DOI: 10.1007/978-3-319-15765-8_18).
- [16] Benadjila, R., Prouff, E., Strullu, R. et al: "Deep learning for side-channel analysis and introduction to ASCAD database, " *J Cryptogr Eng* 163 (2020) (DOI: 10.1007/s13389-019-00220-8).
- [17] Cagli E, et. al: "Convolutional Neural Networks with Data Augmentation Against Jitter-Based Countermeasures," *Cryptographic Hardware and Embedded Systems (CHES)* (2017) (DOI: 10.1007/978-3-319-66787-4_3).
- [18] R. Gilmore, et. al: "Neural network based attack on a masked implementation of AES," *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* (2015) 106 (DOI: 10.1109/HST.2015.7140247).
- [19] Lecun, Y, and Y. Bengio: "Convolutional Networks for Images, Speech, and Time-Series." *Handbook of Brain Theory & Neural Networks* (1995).
- [20] G. M. James, "Curve Alignment by Moments," *Annals of Applied Statistics* 480 (2007) (DOI: 10.1214/07-aos127).
- [21] N. Debande, et. al: "Re-synchronization by moments": An efficient solution to align Side-Channel traces," *IEEE International Workshop on Information Forensics and Security (WIFS)* (2011) 1 (DOI: 10.1109/WIFS.2011.6123143).
- [22] Homma N, et. al: "High-Resolution Side-Channel Attack Using Phase-Based Waveform Matching," *Cryptographic Hardware and Embedded Systems (CHES)* (2006) (DOI: 10.1007/11894063_15).
- [23] Debande, N., et al. "Side Channel Analysis enhancement: A proposition for measurements resynchronisation." *Labh*.
- [24] D. Das, et. al: "Deep Learning Side-Channel Attack Resilient AES-256 using Current Domain Signature Attenuation in 65nm CMOS," *IEEE Custom Integrated Circuits Conference (CICC)*, (2020) 1 (DOI: 10.1109/CICC48029.2020.9075889).
- [25] T. Kubota, et. al: "Deep Learning Side-Channel Attack Against Hardware Implementations of AES," *Euromicro Conference on Digital System Design (DSD)* (2019) 261 (DOI: 10.1109/DSD.2019.00046).
- [26] W. Shan, et. al: "Machine Learning Assisted Side-Channel-Attack Countermeasure and Its Application on a 28-nm AES Circuit," in *IEEE Journal of Solid-State Circuits* (2020) 794 (DOI: 10.1109/JSSC.2019.2953855).
- [27] W. Shan, et. al: "Machine learning based side-channel attack countermeasure with hamming-distance redistribution and its application on advanced encryption standard," *Electron. Lett.*, (2017) 926 (DOI: 10.1049/el.2017.1460).
- [28] G. F. Bouesse, et al: "A clock-less low-voltage AES Cryptographic processor," *European Solid-State Circuits Conference (ESSCIR)*, (2005) 403 (DOI: 10.1109/ESSCIR.2005.1541645).
- [29] N. El-meligy, et al: "130nm Low power asynchronous AES core," *IEEE International Symposium on Circuits and Systems (ISCAS)*, (2017) 1 (DOI: 10.1109/ISCAS.2017.8050832).
- [30] B. Yu, et al: "A low cost, low power AES ASIC with high DPA resisting ability," *IEEE Asian Solid-State Circuits Conference (ASSCC)* (2009) 285 (DOI: 10.1109/ASSCC.2009.5357254).