INTERNATIONAL JOURNAL OF CIRCUITS, SYSTEMS AND SIGNAL PROCESSING
DOI: 10.46300/9106.2021.15.29 Volume 15, 2021

Power consumption Improvements in AES decryption based on Null Convention Logic

Toi Le Thanh[1,2], Lac Truong Tri[1], Hoang Trang[1]
[1] Faculty of Electrical and Electronics Engineering, Ho Chi Minh City University of Technology (HCMUT), Vietnam National University Ho Chi Minh City, Vietnam
[2] Faculty of Electrical and Electronics Engineering, Ho Chi Minh City University of Food Industry (HUFI), Vietnam

Received: July 11, 2020. Revised: March 12, 2021. Accepted: April 1, 2021. Published: April 7, 2021.

Abstract—In this paper, we propose a new asynchronous method based on a Null Convention Logic (NCL) to improve power consumption for low power integrated circuits. The reason is because the NCL based designs do not use a clock, it eliminates the problems related to the clock and its power consumption reduces significantly. To show the advantages of the selected method, we propose two design models using the synchronous circuit design method, and the NCL based asynchronous circuit design method. To test these two design models conveniently, we also propose an extra automatic test model. In this study, the AES decryption is used as an example to illustrate both methods. The two above proposed AES decryption models are simulated and synthesized at the various corners by VCS and Design Compiler tool using TSMC standard cell libraries in 65nm technology. The synthesis results of the two above mentioned models indicated that the power consumption of the NCL based asynchronous circuit model is 3 times lower than that of the synchronous circuit model, and significantly improves (from 94% to 98%) compared with the results of the other authors. The processing speed of the NCL based asynchronous circuit paradigm is able to achieve a maximum speed.

Keywords—Advanced Encryption Standard (AES), Decryption, Synchronous method, Asynchronous method, Null Convention Logic.

I. INTRODUCTION

THE synchronous circuits always use clock pulses to control their operation, so the problems of the clock skew, clock tree, noise, and power consumption are the disadvantages of the synchronous circuits [1]. There have been many low power integrated circuits studied in recent years such as the application of FinFET technology for low power circuits [2], ten-core low power AES encryption models [3], low power wake-up receivers applied for wireless sensor network [4], low power and high-performance FFT with various radices [5], low power integrated circuits for automatic epilepsy seizure detection [6], and some relevant studies can be found in [7], [8], and [9]. However, all of them have not achieved a considerable level of optimization yet. This is because switching power is large in the synchronous circuits. To solve this problem, we propose an NCL based new asynchronous circuit design method in order to improve the power consumption in the integrated circuits. In addition, we use the AES decryption design as an example to illustrate the advantages of the proposed approach.

Karl Fant and Scott Brandt firstly proposed NCL in 1994. It is a delay-insensitive logic and pertains to asynchronous logic. NCL firstly targeted at designing very large scale integrated circuits and application specific integrated circuits with lower power, lower electromagnetic interference, and lower noise [1]. Today, NCL is studied for many purposes such as built-in self-test for multi threshold NCL asynchronous circuits [10], exploiting dual-rail register invariants for equivalence verification of NCL circuits [11], formal verification of completion-completeness for NCL circuits [12], the realization of FinFET using static NCL threshold gates [13] and low power consumption [14], [15].

The AES decryption is studied in various ways by many authors in [16], [17], [18], [19], and [20], but all of these studies have not shown the significant optimal design method for power consumption. In [19], and [21], the authors studied the AES decryption using the synchronous method, but the synthesis result of the power consumption was not implemented. Similar to [19], [21], the power consumption in [18], [22], [23], [24] is synthesized by various tools, but these results have not reached the most optimal level. In addition, the AES decryption studied by the NCL based asynchronous method [17] was only simulated by the VCS tool, but the result of the power consumption was not synthesized. Therefore, we propose realizing the AES decryption by using

the new asynchronous method based on NCL to demonstrate the power consumption improvement of the proposed method. In the study process, we implement two pipelined AES decryption models by using the synchronous method and the NCL based asynchronous method. Besides, we implement an extra automatic test model. Both of the two AES decryption models are simulated by the VCS tool and are synthesized by the DC tool with the same standard cell libraries in 65nm technology. Also, we make a comparison between two methods about power consumption, area, and operating speed to show the significant low power consumption of the proposed method.

The rest of this article is arranged as follows: a description of NCL and the general flow of the AES decryption algorithm are introduced briefly in Section 2 and Section 3. Then, Section 4 and Section 5 give out the proposed AES decryption models using the synchronous circuit design approach and the NCL based asynchronous circuit design approach. Subsequently, the automated test pattern, the simulation and synthesis results, and some comparisons between the two methods are presented in Section 6 and Section 7. Finally, Section 8 gives a conclusion of the advantage of the proposed method.

II. NULL CONVENTION LOGIC

NCL is not only a symbolically complete logic template, but also a template that is not sensitive to latency. The NCL based asynchronous circuits always operate correctly regardless of the component and wire delays [25], [26]. To achieve the goal mentioned above, NCL circuits employ quad-rail logic or dual-rail logic [26]. A traditional single-rail logic signal is made up of one rail whereas an NCL signal D is made up of two wires D0 and D1. A traditional logic signal is converted to a dual-rail signal as shown in Table. I [27]. Both D0 and D1 cannot be in state 1 simultaneously, because this is an illegal state.

Table. I Dual rail signal

code		
Dual-rail logic	D1	D0
DATA0	0	1
DATA1	1	0
NULL	0	0
ILEGAL	1	1

To implement NCL circuits, the threshold gates with hysteresis are used in designing asynchronous integrated circuits. 27 threshold gates are utilized to design NCL circuits presented in detail in [25]-[27]. A threshold gate is symbolized ThnmWm1m2. Whereas m is the total number of inputs, n is the threshold value that means at least n of m inputs must become '1' state before the output will become '1' state, w is the weight of the inputs with values m1, m2. Fig. 1 illustrates the fundamental threshold gate and Fig. 2 is a typical case of a 1-bit NCL register.

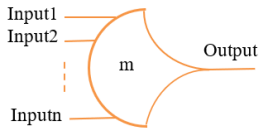

Fig. 1 The primary threshold gate

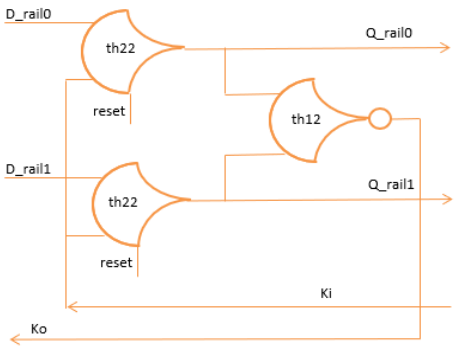

Fig. 2 1-bit NCL register

A common framework of an NCL asynchronous system in Fig. 3 consists of two NCL registers and a combinational logic circuit inserted between two registers [28]. The framework of the NCL asynchronous circuits is like the framework of the traditional synchronous circuits. The flow of data between combinational logic blocks is controlled by using registers. Thus, to design an NCL system, the designers can comply with the same primary stages of the synchronous designs. Additionally, when changing from the synchronous design flow to the asynchronous framework, NCL circuits are often the best option with the lowest conversion costs.

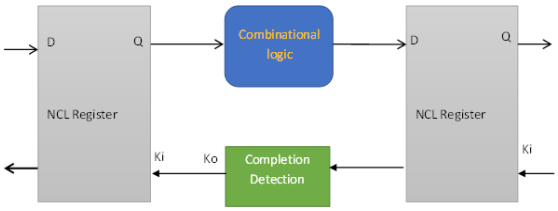

Fig. 3 NCL pipeline system

III. THE AES DECRYPTION BLOCK DIAGRAM

The encryption process converts a "plaintext" into a "ciphertext" through a key that conceals the original information. Otherwise, the decryption process is the inverse cipher process of the encryption process. It helps to restore plaintext from a ciphertext. During the decryption process, the ciphertext is transformed by functions such as AddRoundKey, InvSubBytes, InvShiftRows, and InvMixColumns to generate intermediate data called the state. The key cipher is transformed by the KeyExpansion function, as in the encryption process. However, the order of the round keys used during the decryption process is in the inverse order of the round keys in the encryption process, meaning that the 10th round key will be used first. The second key is the ninth-round key and so on, and the last key is the original key. The implementation of the five

functions mentioned above is illustrated in [17], [19], [29] and is employed through three stages as shown in Fig. 4.

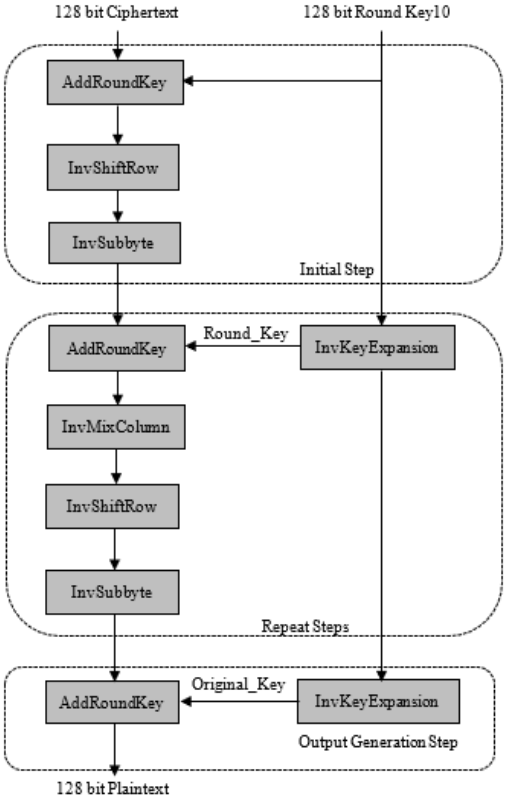

Fig. 4 The AES decryption block diagram [17], [19]

AddRoundKey transformation is an important stage in the decryption process. The ciphertext and the round key are distributed in the 4x4 byte matrices, in which each byte of the ciphertext is exored bitwise with the corresponding byte of the 10th round key of the encryption process. An example is shown in fig. 5.

69	C4	E0	D8	⊕	00	01	02	03	=	69	C5	E2	DB
6A	7B	04	30		04	05	06	07		6E	7E	02	37
D8	CD	B7	80		08	09	0A	0B		D0	C4	BD	8B
70	B4	C5	5A		0C	0D	0E	0F		7C	B9	CB	55
Ciphertext					Key round					State			

Fig. 5 AddRoundKey transformation

Then the result of this AddRoundKey transformation is continued to be implemented by InvShiftRows transformation. In this transformation, the first row of the state matrix is unchanged, while the second row is shifted right 1 byte, the third row is shifted right by 2 bytes and the fourth row is shifted right by 3 bytes. This transformation is illustrated in Fig.6.

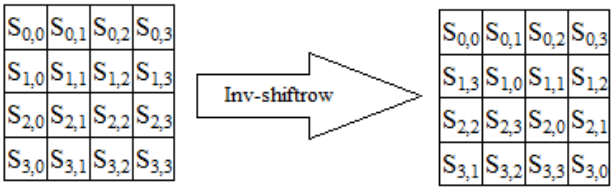

Fig. 6 InvShiftrows transformation

The final transformation of the initial step is InvSubbyte transformation as shown in Fig. 7. In this function, each byte of the state matrix which is the output of the previous invShiftrow transformation, is substituted by another byte specified in the AES algorithm. The table specifying alternative values for the InvSubByte function is called the inverse S-box table.

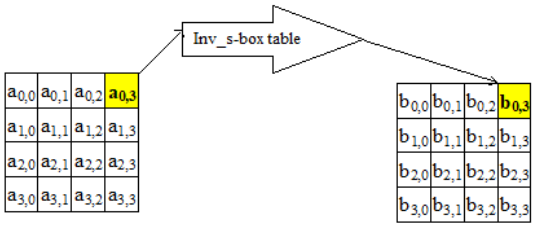

Fig. 7 Invsubbyte transformation

The next stage is the repeat decryption stage including four sub-steps implemented by four transformations. In addition to the three transformations in the first stage, the InvMixcolumns transformation is done by taking each column of the state matrix multiplying modulo (1) with a fixed polynomial (2) over GF(2^8) [17].

$$G(x) = x^4 + 1 \quad (1)$$

$$F(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E\} \quad (2)$$

Where 0B, 0D, 09, 0E is hexadecimal values.

As presented in [29], this can be inscribed as a matrix multiplication (3).

$$\begin{bmatrix} s'_{0,i} \\ s'_{1,i} \\ s'_{2,i} \\ s'_{3,i} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} s_{0,i} \\ s_{1,i} \\ s_{2,i} \\ s_{3,i} \end{bmatrix} \quad (3)$$

Where $0 \le i \le 3$

This repeat stage is reduplicated nine times, whereas the InvKeyExpansion alteration must be carried out in parallel with the AddRoundKey transformation to generate a key for this transformation.

The final stage is the output generation stage, where the result of the previous stage is implemented by AddRoundKey transformation with the original key to restore the plaintext.

IV. THE PROPOSED AES DECRYPTION MODEL USING THE SYNCHRONOUS DESIGN METHOD

The AES algorithm is symmetrical, so the decryption is performed in complete contrast to the encryption. The

decryption comprises 10 main rounds, 1 sub-round, 12 synchronous registers using 256-bit D flip-flop, a clock distributor, a signal to reset, and an 11-stage pipelined system.

Fig. 8 shows a general diagram of the synchronous AES decryption with a pipelined system. Functional blocks are simulated and synthesized for some parameters such as the power consumption, the processing speed, and area by VCS and DC tools using TSMC 65nm technology libraries.

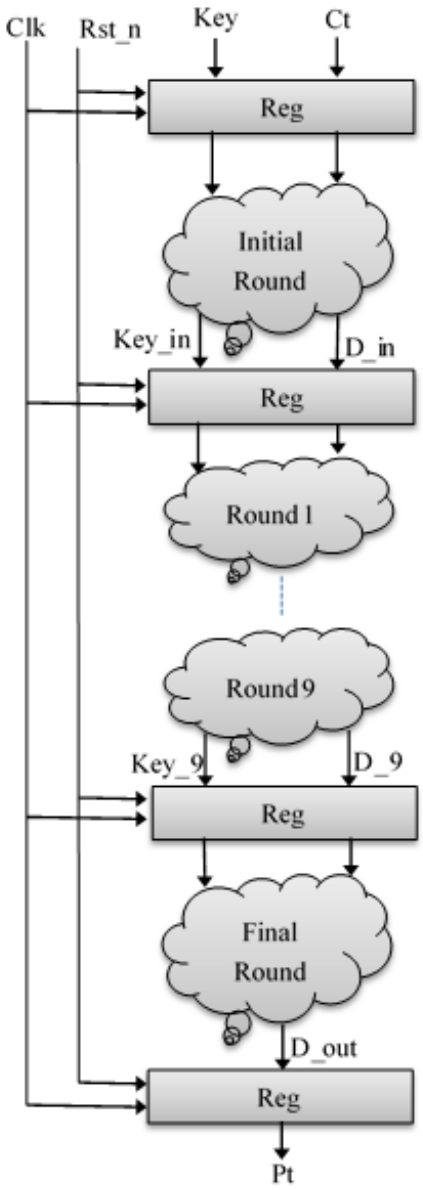

Fig. 8 The synchronous AES decryption model

V. THE PROPOSED AES DECRYPTION MODEL USING THE NCL BASED ASYNCHRONOUS DESIGN METHOD

The AES decryption process, which consists of 10 main rounds and 1 last round with the 128-bit ciphertext input combined with the 128-bit key creating the 128-bit plaintext, will be performed in contrast to the encryption process. The AES decryption block diagram is shown in Fig. 9. Both the synchronous and asynchronous decryption models are pipelined by a system of registers, which will be the best way to contribute to reducing power consumption. In addition, replacing a single functional unit with an 11-stage pipelined unit also reduces the amount of logic in a clock cycle at the expense of more registers [30].

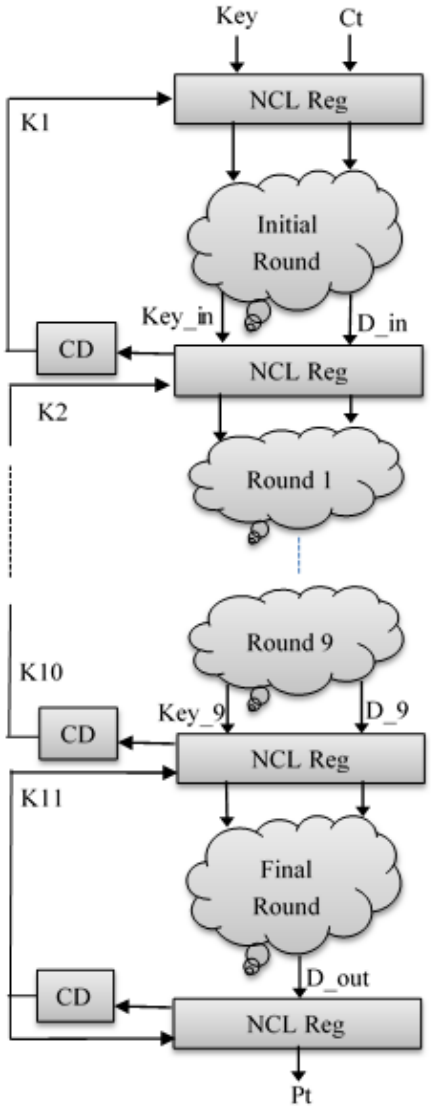

Fig. 9 The NCL based asynchronous AES decryption model

This first round consists of 4 functions in which data and the key are exored by the AddroundKey transformation, then the data are converted through the InvShiftrow function and the InvSubbyte function to create a new data. Fig. 10 shows the structure of the first round. The structure of the rounds from round 1 to round 9 shown in Fig. 11 has five functions such as AddRoundKey or Exor, InvMixcolumn, InvShiftRow, InvSubbyte, and InvKeyGen transformation. Especially, the last round only carries out the AddRoundKey transformation as shown in Fig. 12. The output of this round is the 128-bit plaintext.

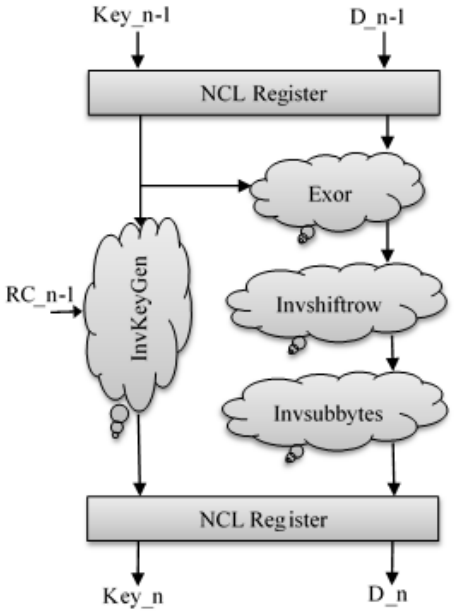

Fig. 10 The structure of the initial round

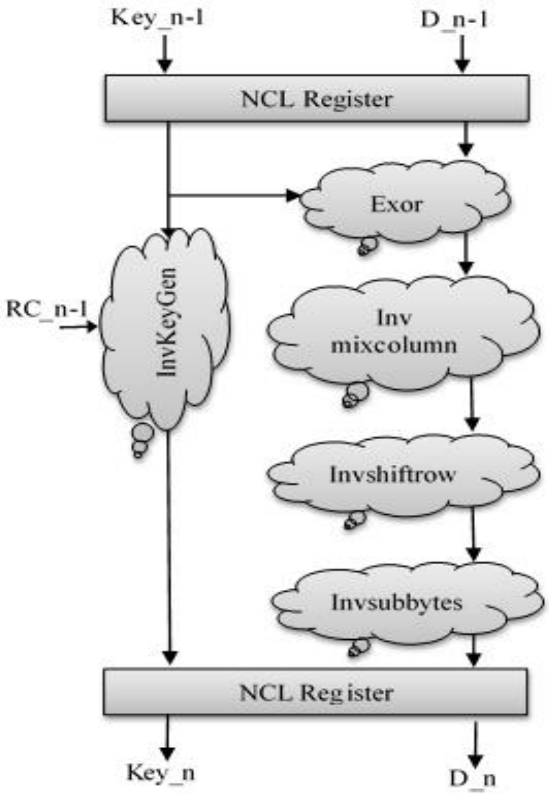

Fig.11 The structure of round 1 – round 9

The general structure of the NCL registers from register 1 to register 9 as shown in Fig. 13 includes two 128-bit NCL registers, two detection circuits for Data and Key, and a threshold gate th22. The output of th22 is carried to the input of the previous register. Particularly, the first NCL register has no detection circuit, illustrated in Fig. 14, and the last register has a data input and a data output.

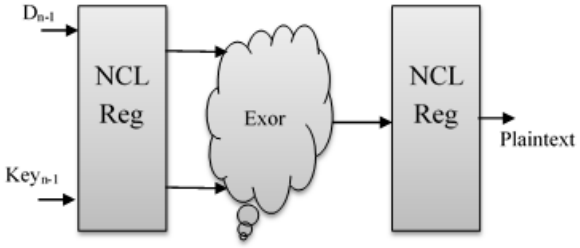

Fig. 12 The structure of the final round

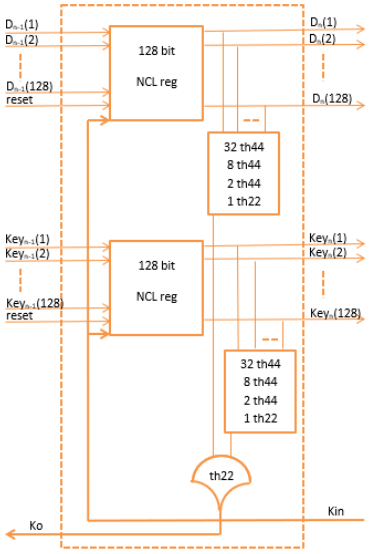

Fig. 13 The structure of an NCL 128-bit register and completion detection circuit

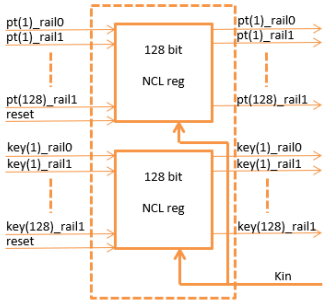

Fig. 14 The structure of the first NCL register

VI. THE PROPOSED AUTOMATIC TEST MODEL FOR THE AES DECRYPTION

To be able to test many cases, we propose the automatic test model as shown in Fig. 15. This model is only used to verify the results of both synchronous and asynchronous AES decryption. It includes an AES decryption block (HDL), an AES decryption block (Matlab), four memories to store data, and one comparison block. Mem1 is used to contain the ciphertext, Mem2 stores the key, Mem3 holds the results of the AES decryption block using Verilog language, and Mem4 accommodates the results of the AES decryption block using Matlab language (golden results). At first, ciphertext and key are taken the AES decryption block (Matlab) using Matlab

software to create golden data and the results are stored in Mem4. Then to create data from the AES decryption block (HDL), input data from mem 1 and mem 2 is loaded into the AES decryption block (HDL). Finally, the results of the AES decryption block (HDL) are compared to the results of the AES decryption block (Matlab). The result of the comparison is true if both data in mem 3 and mem 4 are the same and vice versa is false. By using this test model, just providing N data and key, N cases are executed and compared.

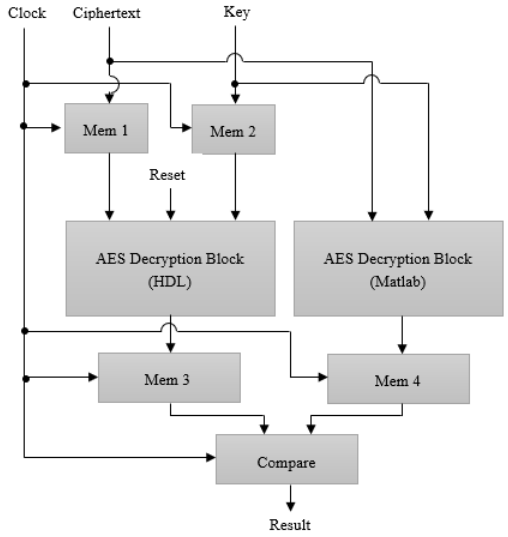

Fig. 15 The automatic test model

VII. RESULTS AND DISCUSSION

Both the synchronous and asynchronous AES decryption models are simulated by the VCS tool of Synopsys using TSMC 65nm technology libraries for two cases with Key and ciphertext in Table II.

Table. II Two test cases

	Case 1	Case 2
Cipher-text	128'h69c4_e0d8_6a7b_0430_d8cd_b780_70b4_c55a	128'h3514_3da5_c83d_bba6_8a49_cc93_4de9_3417
Key	128'h0001_0203_0405_0607_0809_0a0b_0c0d_0e0f	128'h524b_9651_adef_2154_010f_cbb5_4633_0477
Plain-text	128'h0011_2233_4455_6677_8899_aabb_ccdd_eeff	128'h524b_9651_adef_2154_010f_cbb5_4633_0478

The waveform of both models are displayed in the Fig. 16 and Fig. 17.

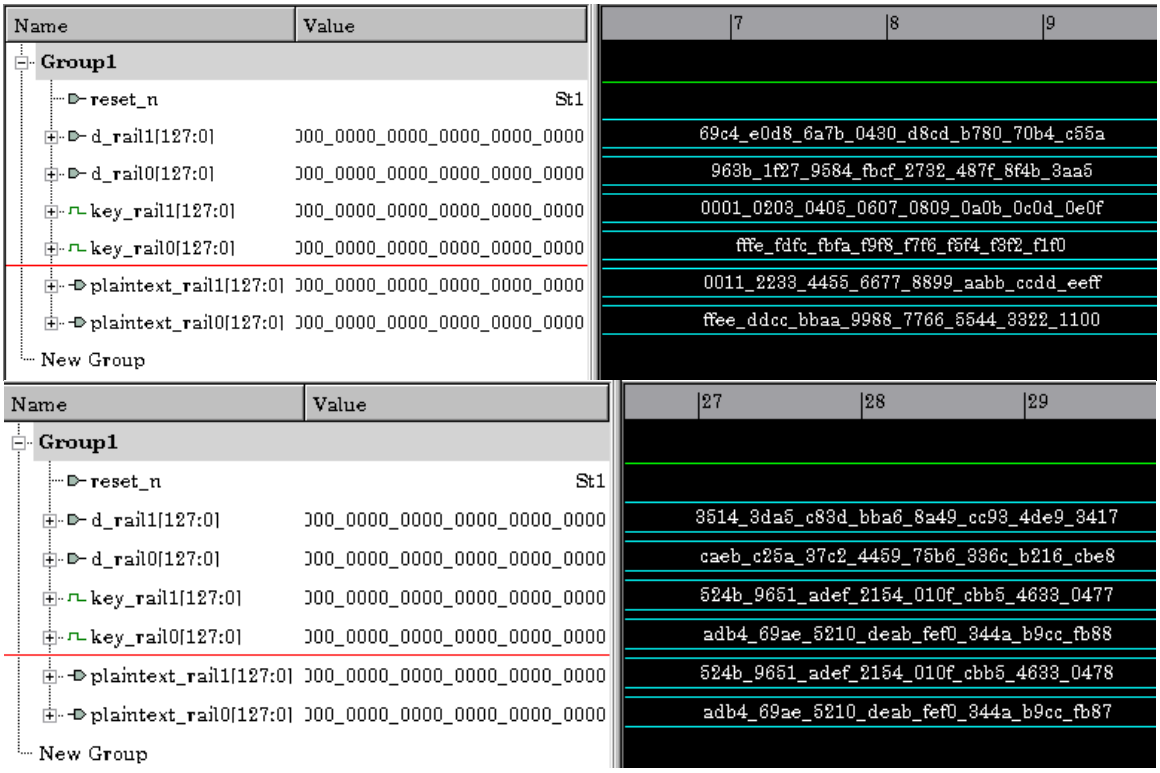

Fig. 16 The waveform of the asynchronous NCL AES decryption model

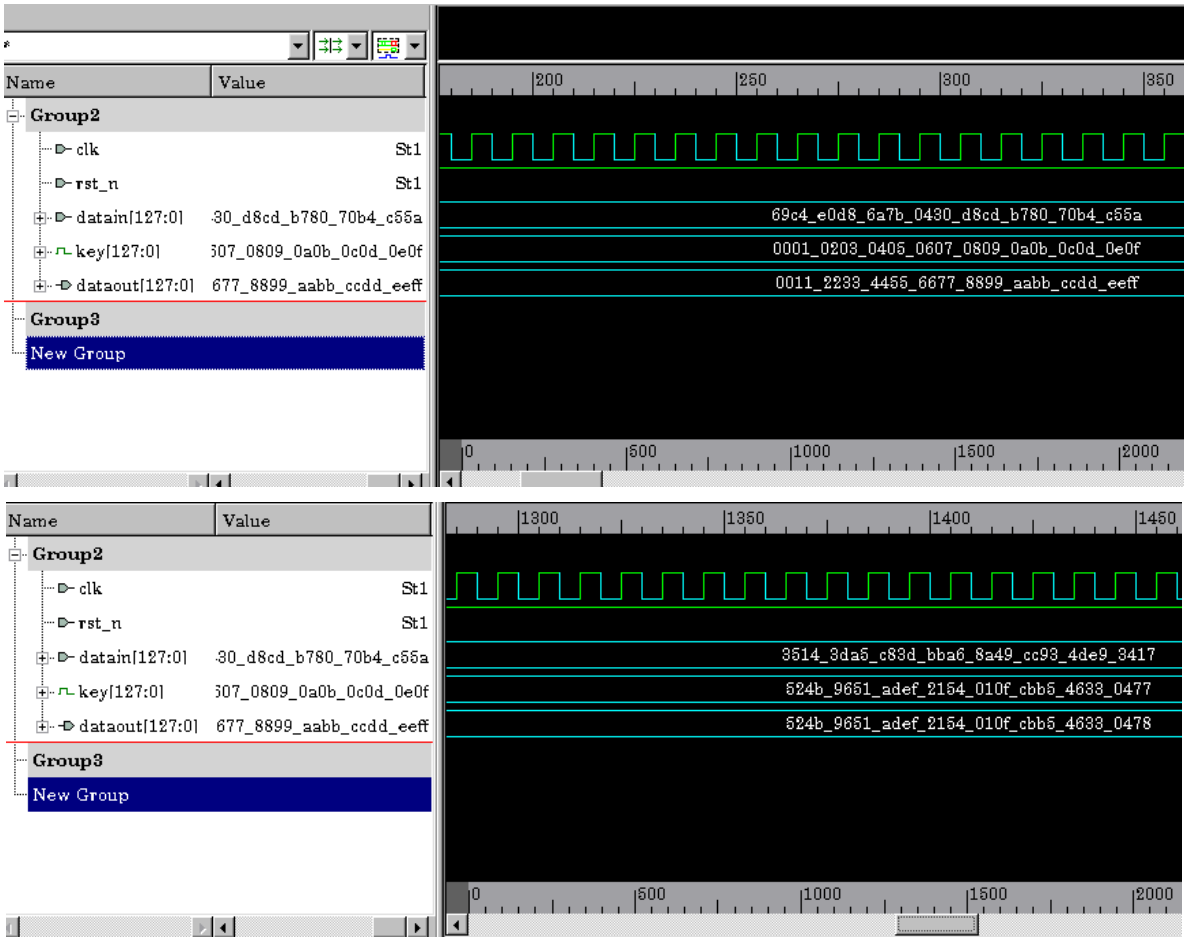

Fig. 17 The waveform of the synchronous AES decryption model

Ciphertext and Key are two input signals. When rst_n = '0' (low active), the output is reset at the '0' state. Similar to the synchronous design, a pair of NULL alternated between a pair of Data is one of the conditions to implement the pipeline in the NCL based asynchronous designs. The simulation results in an automated test environment for both the synchronous and NCL based asynchronous AES decryption models are shown in Fig. 18 and Fig. 19.

Both synchronous and NCL asynchronous AES decryption models are synthesized by the Design Compiler tool of Synopsys using TSMC 65nm technology libraries. Some libraries used for synthesis are listed as follows:

scadv12_cln65lp_hvt_ff_1p32v_0c.lib,
scadv12_cln65lp_hvt_ff_1p32v_125c.lib,
scadv12_cln65lp_hvt_ff_1p32v_m40c.lib.

Because the Design Compiler tool currently supports only the synchronous designs, the synthesis results in terms of area, power, and delay are proper. While the synthesis results of the NCL based asynchronous designs have to be recomputed to get accurate results, the power consumption and the cycle time are computed from (4) [30].

$$P_{total} = P_{dynamic} + P_{static} \quad (4)$$

Where, $P_{dynamic} = P_{switching} + P_{internal}$

$$P_{switching} = \alpha.C_L.f.V_{dd}^2$$

α: the active factor

C_L: the load capacitance

f: the switching frequency

V_{dd}: supply voltage

For NCL based asynchronous designs, the frequency f is used to provide Data or Null. Thus, the Design Compiler tool only calculates the appropriate power, when the clock signal is added to the design. This clock signal is used to control the delivery of data with a predefined frequency and is only added when measuring power, i.e the measurement of area and delay have no clock.

The terms speed and delay are the same as in the synchronous design. The cycle of the NCL based asynchronous design is determined by (5) the cycle with the greatest delay [31].

$$T_{dd} = 2*(T_{comb} + T_{comp}) \quad (5)$$

T_{dd}: the processing time of Null/Data

T_{comb}: the delay of the combinatorial circuit

T_{comp}: the delay of the complete detection circuit

The synthesis results of the synchronous and NCL based asynchronous AES decryption paradigm pipelined are presented in Table. III.

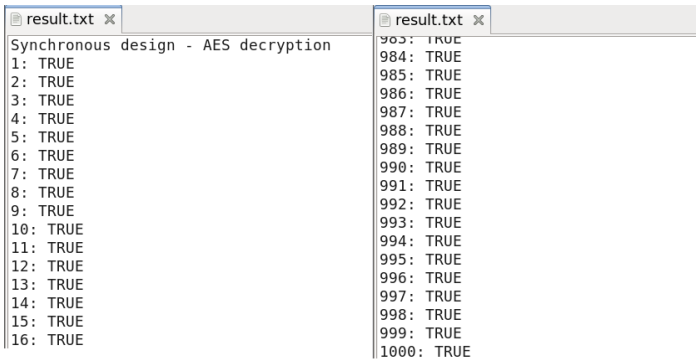

Fig. 18 The automated test result of the synchronous AES decryption model

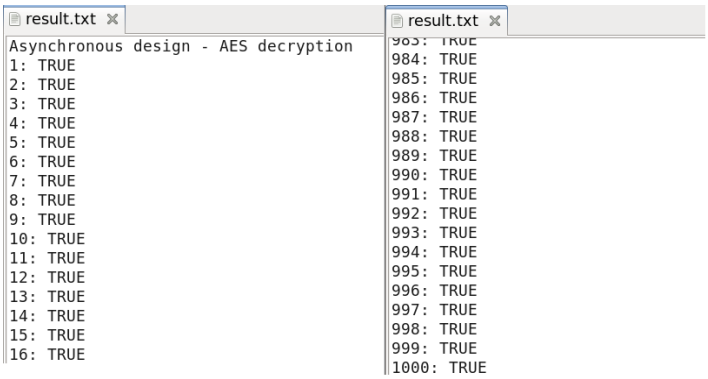

Fig. 19 The automated test result of the NCL asynchronous AES decryption model

Table. III The comparative synthesis results of the synchronous and asynchronous aes decryption paradigm

AES decryption		**65ff_m4**	**65ff_0c**	**65ff_125**
Area (μm^2)	Asyn	872251	872489	871714
	Syn	265810	265772	265794
	Asyn/syn	3.2815	3.2828	3.2797
Power (mW)	Asyn	2.7086	2.7307	3.4065
	Syn	11.7256	11.8045	12.4047
	Syn/Asyn	4.3290	4.3229	3.6415
Max Speed (MHz)	Asyn	149	142	131
	Syn	930	900	830
	Syn/Asyn	6.2416	6.3380	6.3359

The total area of the NCL based asynchronous design is 3.3 times larger than that of the synchronous design, which is also the biggest disadvantage of most NCL based asynchronous designs. Currently, there are many studies on different NCL CMOS models to reduce area [32]. Therefore, the result of the area can be improved using the NCL library with other CMOS models.

The power consumption of the NCL based asynchronous design is much smaller (roughly a quarter) than that of the synchronous design. There is a significant decrease in power consumption because while the NCL based asynchronous circuits only switch when DATA and NULL are being processed, the clocked Boolean circuits switch every clock pulse [28]. Therefore, as the synchronous circuits work at a higher frequency, the larger the number of switching times, the greater the power consumption is illustrated in Fig. 20. The low power consumption is one of the most outstanding advantages of the NCL based asynchronous circuit design method. Besides, the power consumption in the NCL based asynchronous designs is improved much more by using other techniques such as Sleep Convention Logic (SCL) [33], Multi-threshold CMOS [34].

Large delay in the NCL based asynchronous designs reduces the operating frequency compared with the synchronous designs. However, because the NCL based asynchronous designs do not use the clock, they easily achieve a maximum speed. In contrast, the synchronous designs are

difficult to achieve a maximum speed because it requires designers to analyze timing closely and calculate the delay avoiding clock-related issues. Reducing delay or improving the speed has also been studied through optimal methods such as early completion [35], Null Cycle Reduction (NCR) [36], threshold combinational reduction [37].

Fig. 20 shows the influence of the frequency on power consumption. As the frequency increases, the switching process in the synchronous circuit will be faster, which results in more power consumption. Meanwhile, the NCL based asynchronous designs do not use a clock, switching power will be less affected.

To show the highlight of the NCL based asynchronous design method, we compare the power consumption between the NCL based asynchronous design and the other low power synchronous designs. All of the designs are measured with the operating frequency at 100 MHz.

Table. IV Comparison of proposed ncl aes decryption and existing counterpart

Design	Power (mW)
NCL asynchronous (Our work)	2.7307
[24]	49
[18]	170
[38]	4.0

Table. IV shows that the power consumption in our work is much lower than the power consumption in the other works. Particularly, there is a significant improvement of power consumption in our work, in which the power consumption reduces by 94.43% and 98.39% compared to [18], [24] respectively. When compared with the low power 8-bit AES core architecture in [38], the power consumption in our work is 31.73% less than its power consumption.

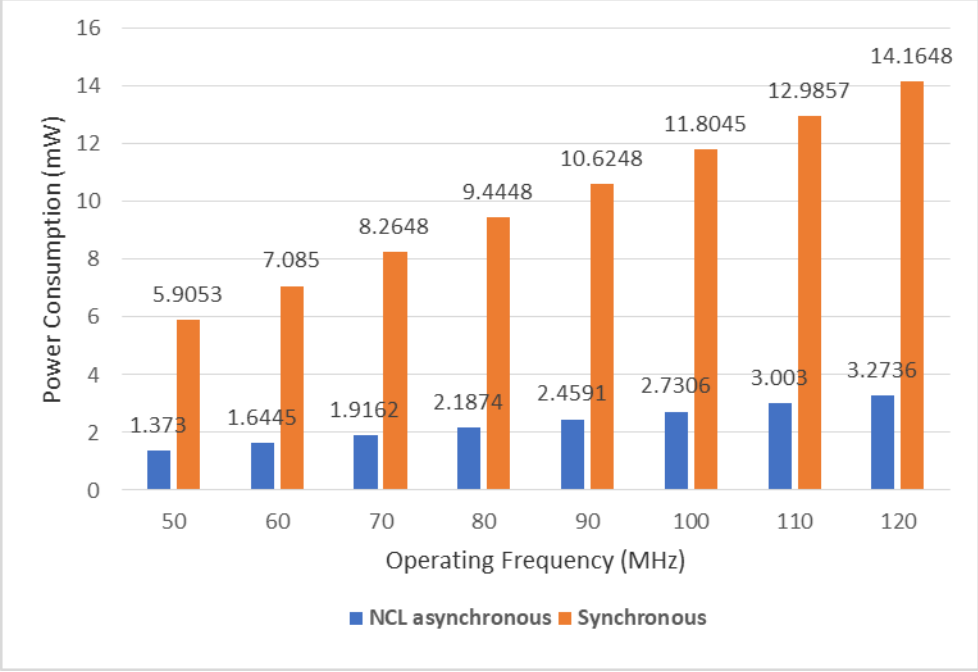

Fig. 20 The influence of the frequency on power consumption

VIII. CONCLUSION

In this research, we proposed the two AES decryption models using two different methods which are the synchronous method and the NCL based asynchronous method. Besides, the automated test paradigm for both AES decryption models mentioned above is also proposed to help test functionality correctly. The pipelining technique is applied for the synchronous and NCL based asynchronous circuit models to improve speed in the low power design field. It is obvious that the NCL based asynchronous method gives the integrated circuits a reduced amount of power consumption (about three times) compared with the synchronous method and a significant improvement (from 94% to 98%) compared with the results of the other authors. Moreover, the NCL based asynchronous designs do not utilize the clock pulse, so they are able to achieve a high processing speed. In terms of area, this is a disadvantage of the NCL based asynchronous designs. In the digital circuit designs, if the low power criterion is the first choice, the NCL based asynchronous circuit design method will be an excellent candidate. Although we use the same TSMC standard cell libraries in 65nm technology for both models, the low power advantages of the NCL based asynchronous design technique are still evident. In future work, we will design an NCL CMOS

library system to synthesize for NCL based asynchronous designs. At that time, the synthesis results of area, power, and delay will be fully promising.

ACKNOWLEDGEMENTS

This research is funded by Ho Chi Minh City University of technology (HCMUT), VNU-HCM, under grant number BK-SDH-2021-1980906.

References

[1] J. Wu, "Null Convention Logic applications of asynchronous design in nanotechnology and cryptographic security," 2012.

[2] S. Birla, "Ultra-low power finfet SRAM cell with improved stability suitable for low power applications," *Int. J. Electron. Telecommun.*, vol. 65, no. 4, pp. 603–609, 2019, doi: 10.24425/ijet.2019.129819.

[3] P. Dong, H. K. Nguyen, V. Hoang, and X. Tran, "Low-Power Implementation of a High-Throughput Multi-core AES Encryption Architecture," 2020.

[4] Y. C. Wong, S. H. Tan, R. S. S. Singh, H. Zhang, A. R. Syafeeza, and N. A. Hamid, "Low power wake-up receiver based on ultrasound communication for wireless sensor network," *Bull. Electr. Eng. Informatics*, vol. 9, no. 1, pp. 21–29, 2020, doi: 10.11591/eei.v9i1.1654.

[5] M. Z. Hussain and K. N. Parvin, "Low power and high performance FFT with different radices," *Int. J. Reconfigurable Embed. Syst.*, vol. 8, no. 2, p. 99, 2019, doi: 10.11591/ijres.v8.i2.pp99-106.

[6] S. Rafiammal, D. Najumnissa, G. Anuradha, S. K. Mohideen, P. K. Jawahar, and S. A. Mutalib, "A low power and high performance hardware design for automatic epilepsy seizure detections.," *Int. J. Electron. Telecommun.*, vol. 65, no. 4, pp. 707–712, 2019, doi: 10.24425/ijet.2019.130254.

[7] C. Zhang, Y. Zheng, and R. Chen, "A New Environment Parameter Monitoring System Based on ZigBee Protocol," vol. 13, 2019.

[8] N. Scheidt and M. Adda, "Framework of confidence values during digital forensic investigation processes," *WSEAS Trans. Syst. Control*, vol. 15, pp. 228–234, 2020, doi: 10.37394/23203.2020.15.24.

[9] E. A. Popov and Y. V. Shornikov, "Modeling and simulation of electric power systems as hybrid systems in ISMA," *WSEAS Trans. Syst. Control*, vol. 14, pp. 57–64, 2019.

[10] B. Sparkman, S. C. Smith, and J. Di, "Built-In Self-Test for Multi-Threshold NULL Convention Logic Asynchronous Circuits," in *Proceedings of the IEEE VLSI Test Symposium*, 2020, vol. 2020-April, doi: 10.1109/VTS48691.2020.9107627.

[11] S. N. Le, S. K. Srinivasan, and S. C. Smith, "Exploiting Dual-Rail Register Invariants for Equivalence Verification of NCL Circuits," in *Midwest Symposium on Circuits and Systems*, 2020, vol. 2020-Augus, pp. 21–24, doi: 10.1109/MWSCAS48704.2020.9184477.

[12] S. N. Le, S. K. Srinivasan, and S. C. Smith, "Formal Verification of Completion-Completeness for NCL Circuits," *Midwest Symposium on Circuits and Systems*, vol. 2020-Augus. pp. 25–28, 2020, doi: 10.1109/MWSCAS48704.2020.9184603.

[13] A. A. Sakib, A. A. Akib, and S. C. Smith, "Implementation of FinFET Based Static NCL Threshold Gates: An Analysis of Design Choice," in *Midwest Symposium on Circuits and Systems*, 2020, vol. 2020-Augus, pp. 37–40, doi: 10.1109/MWSCAS48704.2020.9184629.

[14] N. Le Huy and P. Beckett, "Null convention logic primitive element architecture for ultralow power high performance portable digital systems," *Proc. 2017 IEEE Reg. Symp. Micro Nanoelectron. RSM 2017*, pp. 167–170, 2017, doi: 10.1109/RSM.2017.8069157.

[15] Renuka Mandar Sovani, "Near and Sub-Threshold Null Convention Logic Design for Low-power Digital Signal Processing Applications," 2016.

[16] Jāmi'at al-Qāhirah. Kullīyat al-Handasah. Computer Engineering Department and Institute of Electrical and Electronics Engineers, "Ultra Low-Power Encryption/Decryption Core for Lightweight IoT Applications," p. 238.

[17] D. V Supriya and R. Niranjan, "Realization of AES Encryption and Decryption Based On Null Convention Logic," pp. 77–81, 2015.

[18] L. P. Kumar and A. K. Gupta, "Implementation of speech encryption and decryption using advanced encryption standard," *2016 IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. RTEICT 2016 - Proc.*, pp. 1497–1501, 2017, doi: 10.1109/RTEICT.2016.7808081.

[19] A. Muhammad Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data," *Cryptogr. Netw. Secur.*, no. June, 2017, [Online]. Available: https://www.researchgate.net/publication/317615794.

[20] R. Srividya and B. Ramesh, "Implementation of AES using biometric," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 5, pp. 4266–4276, 2019, doi: 10.11591/IJECE.V9I5.PP4266-4276.

[21] S. Quirem and B. K. Lee, "AES decryption using warp-synchronous programming," in *2012 IEEE 31st International Performance Computing and Communications Conference, IPCCC 2012*, 2012, pp. 203–204, doi: 10.1109/PCCC.2012.6407714.

[22] K. L. Tsai, Y. L. Huang, F. Y. Leu, I. You, Y. L. Huang, and C. H. Tsai, "AES-128 based secure low power communication for LoRaWAN IoT environments," *IEEE Access*, vol. 6, pp. 45325–45334, Jul. 2018, doi: 10.1109/ACCESS.2018.2852563.

[23] M. P. Priyanka, E. L. Akshmi Prasad, and A. R. Reddy, "Fpga Implementation Of Image Encryption And Decryption Using AES 128-Bit Core."

[24] M. Janveja *et al.*, "Design of Efficient AES Architecture for Secure ECG Signal Transmission for Low-power IoT Applications," Apr. 2020, doi: 10.1109/RADIOELEKTRONIKA49387.2020.9092417.

[25] A. J. Albert and S. Ramachandran, "Static implementation of a null convention logic based exponent adder," *Int. J. Appl. Eng. Res.*, vol. 10, no. 3, pp. 7601–7614, 2015.

[26] A. Caberos, S. C. Huang, and F. C. Cheng, "Area-

efficient CMOS implementation of NCL gates for XOR-AND/OR dominated circuits," *Asia Pacific Conf. Postgrad. Res. Microelectron. Electron.*, vol. 2017-Octob, pp. 37–40, 2018, doi: 10.1109/PRIMEASIA.2017.8280358.

[27] B. G. Fawzy, M. M. Abutaleb, M. I. Eladawy, and M. Ghoneima, "Strong Indication Full-Adder Circuit for NULL Convention Logic Automation Flows," *Isc. 2018 - 18th Int. Symp. Commun. Inf. Technol.*, no. Iscit, pp. 416–421, 2018, doi: 10.1109/ISCIT.2018.8588000.

[28] M. C. Chang, P. H. Yang, and Z. G. Pan, "Register-Less NULL Convention Logic," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 64, no. 3, pp. 314–318, 2017, doi: 10.1109/TCSII.2016.2557812.

[29] S. M. Noor and E. B. John, "Resource Shared Galois Field Computation for Energy Efficient AES/CRC in IoT Applications," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 4, pp. 340–348, Oct. 2019, doi: 10.1109/TSUSC.2019.2943878.

[30] D. M. H. Neil H. E. Weste, *CMOS VLSI Design A Circuits and Systems Perspective*, vol. 58, no. 12. 2014.

[31] A. J. Albert and S. Ramachandran, "NULL convention floating point multiplier," *Sci. World J.*, vol. 2015, 2015, doi: 10.1155/2015/749569.

[32] F. A. Parsan and S. C. Smith, "CMOS implementation comparison of NCL gates," *Midwest Symp. Circuits Syst.*, pp. 394–397, 2012, doi: 10.1109/MWSCAS.2012.6292040.

[33] P. Palangpour and S. C. Smith, "Sleep Convention Logic using partially slept function blocks," *Midwest Symp. Circuits Syst.*, pp. 17–20, 2013, doi: 10.1109/MWSCAS.2013.6674574.

[34] L. Zhou, R. Parameswaran, F. A. Parsan, S. C. Smith, and J. Di, "Multi-threshold NULL convention logic (MTNCL): An ultra-low power asynchronous circuit design methodology," *J. Low Power Electron. Appl.*, vol. 5, no. 2, pp. 81–100, 2015, doi: 10.3390/jlpea5020081.

[35] S. C. Smith and J. Di, *Designing asynchronous circuits using NULL convention logic (NCL)*, vol. 23. 2009.

[36] S. C. Smith, R. F. DeMara, J. S. Yuan, M. Hagedorn, and D. Ferguson, "Speedup of Delay-Insensitive Digital Systems Using NULL Cycle Reduction," *Proc. 10th Int. Work. Log. Synth.*, pp. 185–189, 2001.

[37] S. C. Smith, R. F. DeMara, J. S. Yuan, M. Hagedorn, and D. Ferguson, "Delay-insensitive gate-level pipelining," *Integr. VLSI J.*, vol. 30, no. 2, pp. 103–131, 2001, doi: 10.1016/S0167-9260(01)00013-X.

[38] V.-L. Dao, V.-P. Hoang, A.-T. Nguyen, and Q.-M. Le, "A Compact, Low Power AES Core on 180nm CMOS Process."

Toi Le Thanh was born in Tay Ninh province, Vietnam. He received his M.S. degree from the Ho Chi Minh City University of Technology, Vietnam, in 2006. He has been a Lecturer of Electrical and Electronic Engineering at the University of Food Industry, Ho Chi Minh City, Vietnam, since 2003. His current research interests include asynchronous IC design and power electronics.

Lac Truong Tri was born in Tien Giang province, Vietnam. He received the Bachelor of Engineering in Electronics-Telecommunication Engineering major from Ho Chi Minh City University of Technology. He is studying Master of Science degree in Electronics Engineering from Ho Chi Minh City University of Technology. His field of research interest is in the domain of Null Convention Logic, Asynchronous Design Method.

Trang Hoang was born in Nha Trang city, Vietnam. He received the Bachelor of Engineering, and Master of Science degree in Electronics-Telecommunication Engineering from Ho Chi Minh City University of Technology in 2002 and 2004, respectively. He received the Ph.D. degree in Microelectronics-MEMS from CEA-LETI and University Joseph Fourier, France, in 2009. From 2009–2010, he did the postdoctorate research in Orange Lab-France Telecom. Since 2010, he is lecturer at Faculty of Electricals–Electronics Engineering, Ho Chi Minh City University of Technology. His field of research interest is in the domain of FPGA implementation, Speech Recognizer, IC architecture, MEMS, fabrication.