Indonesian Journal of Electrical Engineering and Computer Science
Vol. 22, No. 3, June 2021, pp. 1284~1294
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v22.i3.pp1284-1294

Low power circuit design using NCL based asynchronous method

Toi Le Thanh[1], Lac Truong Tri[2], Trang Hoang[3]
[1,2,3] Department of Electronics, Faculty of Electrical and Electronics Engineering, Ho Chi Minh City University of Technology (HCMUT), Ho Chi Minh City, Vietnam
[1,2,3]Vietnam National University Ho Chi Minh City, Ho Chi Minh City, Vietnam
[1]Faculty of Electrical and Electronics Engineering, Ho Chi Minh City University of Food Industry (HUFI), Tan Phu District, Vietnam

Article Info

Article history:

Received Oct 27, 2020
Revised Apr 1, 2021
Accepted Apr 6, 2021

Keywords:

Advanced encryption standard
Asynchronous method
Low power
Null convention logic
Synchronous method

ABSTRACT

The null convention logic (NCL) based circuit design methodology eliminates the problems related to noise, clock tree, electromagnetic interference and also reduces significant power consumption. In this paper, we would like to demonstrate the advantage of low power consumption of the NCL based asynchronous circuit design on a large design scale, thus we used the advanced encryption standard (AES) encryption design as an illustrative example. In addition, we also proposed two pipelined AES encryption models using the synchronous circuit design technique and the asynchronous circuit design technique based on NCL. Besides, these two models were realized by using version control system (VCS) tool to simulate and Design Compiler tool to synthesize parameters in power consumption, processing speed and area. The synthesis results of these two models indicated that power consumption of the NCL based asynchronous AES encryption model had a decrease of 71% compared with the synchronous AES encryption model. Moreover, we show the outstanding advantage of the power consumption of the NCL based asynchronous design model (a decrease of 91.12% and 93,23%) compared to the synchronous design model using clock gating technique and without using clock gating technique respectively.

Corresponding Author:

Trang Hoang
Faculty of Electrical and Electronics Engineering
Ho Chi Minh City University of Technology (HCMUT),
268 Ly Thuong Kiet, District 10, Ho Chi Minh City, Vietnam
Email: hoangtrang@hcmut.edu.vn

1. INTRODUCTION

In recent decades, the digital world has still been dominated by the strong development of the synchronous circuit design techniques. However, as integrated circuits require the increase of the processing speed and the decrease of the feature sizes and of power consumption, synchronous circuits become difficult to respond because of the clock related issues such as clock skews, glitches, layout complexity for clock distribution networks and especially increase of power [1]. Power consumption could be also one of the major concerns in a lot of applications such as wireless, laptops, cell phones, movable medical devices because of staying their battery life time [2]. In recent years, there have been researches about low power integrated circuits using synchronous design techniques such as low power and high performance the fast fourier transform (FFT) with different radices [3], low power pseudo-random number generator [4], low power wakes up receiver based on ultrasound communication for wireless sensor network [5], low power implementation of a high throughput multi core advanced encryption standard (AES) encryption architecture [6]. Although all above mentioned studies had indicated an improvement

in power consumption, this power consumption is mainly due to the switching power remaining high as the clock frequency increases. Therefore, we would propose a new method, the null convention logic (NCL) based asynchronous circuit design method without clock, to make a decrease of power. The method has benefits of eliminating all the clock related issues listed above.

In the mid 1990s, Karl Fant and Scott Brandt firstly proposed NCL which is a delay insensitive logic and the type of asynchronous logic. NCL initially dedicated to designing application specific integrated circuit and very large scale integration circuits with lower power, lower noise, and lower electromagnetic interference [1]. Many studies from transistor level to gate level based on NCL have shown superior performance compared to studies based on traditional Boolean logic [7]-[11]. In addition, NCL is being studied for various purposes such as ultralow power high performance portable digital systems [12], bus alternatives for asynchronous circuits [13], AES encryption and decryption [14], low power designs [15]-[17]. D. L. Oliveira *et al.* [18], the authors indicated the outstanding advantage of low power of the NCL based asynchronous design. However, authors only implemented to examine for small designs such as threshold gates. On the other hand, in [19], 1 bit, 4 bit and 8 bit NCL ripple carry adders have been designed and compared with the corresponding ripple carry adders implemented using conventional synchronous complementary metal–oxide–semiconductor (CMOS) level design methodologies. The synthesis results in [19] indicated that NCL circuits have a significant decrease (about 65%) in power consumption. Both above mentioned models in [18, 19] were carried out on a small scale designs. Thus, in this paper, we would like to use a large scale design to demonstate more clearly the low power advantage of the NCL based asynchronous design technique. We choose the AES encryption model as an example to implement because NCL has the advantage of securing cryptographic devices against side-channel attacks (SCA) and various power analysis attacks [20]. Although many authors have studied the AES algorithm [6], [14], [21], [22] by many various approaches, they have not shown advantages of the NCL based asynchronous design method compared with the other design method. In addition, we would like to propose two pipelined encryption models for the AES encryption using an asynchronous design method based on NCL and a synchronous design method. Both these AES encryption models are synthesized by design compiler tool with the same TSMC 65nm technology libraries. The comparison between these two methods in power consumption, area and processing speed is done. In addition, we also realize an extra comparison of the power between the NCL based asynchronous method and the synchronous design method using the clock gating technique and without using clock gating technique in [6] to prove some ideas why we choose the asynchronous design technique based on NCL for low power integrated circuit designs.

The rest of this paper is organized as follows: a description of the null convention logic and the general structure of the AES encryption algorithm are introduced briefly in section 2 and section 3. Then, section 4 and section 5 present respectively the proposed AES encryption models using the synchronous design method and the NCL based asynchronous design approach. Comparison between the two above mentioned methods and discussions are presented in section 6. The last section gives a conclusion of the proposed method.

2. NULL CONVENTION LOGIC (NCL)

NCL is a delay-insensitive paradigm used widely for designing asynchronous circuits in which the circuit will operate correctly regardless of the delay of the components and wires [9]. NCL circuits utilize dual-rail logic or quad-rail logic to achieve this purpose and NCL also uses two complete criteria which are the symbolic completeness of the expression and the completeness of the input [10]. A dual-rail signal, D is represented by 2 wires D0 and D1. The value of a dual-rail signal gets any value of the set {DATA0, DATA1, NULL} shown in the Table 1 [8]. Three logical states (NULL, DATA0 and DATA1) help dual-rail signals achieve the symbolic completeness of expression. The second criterion is the completeness of input showing that all outputs must not transit from null to data or data to null until all inputs have transited from null to data or data to null.

NCL uses a special type of gate, called a threshold gate, with hysteresis. There are 27 threshold gates with hysteresis in [9], [10] utilized in order to design NCL circuits. The general threshold gate is denoted as ThmnWn1n2. Here, n is the total number of inputs, m is the threshold value that means at least m of the n inputs must be asserted before the output becomes asserted, and w is the weight of the inputs with values n1, n2 respectively. Figure 1 illustrates the primary threshold gate. Figures 2 and 3 are examples of an NCL dual–rail EXOR and 1 bit register, respective.

Table 1. Dual-rail signal

Boolean logic	Dual–rail logic	Code D1	Code D0
0	DATA0	0	1
1	DATA1	1	0
	NULL	0	0
	ILLEGAL	1	1

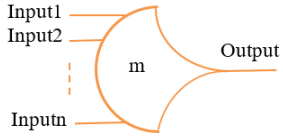

Figure 1. The primary threshold gate

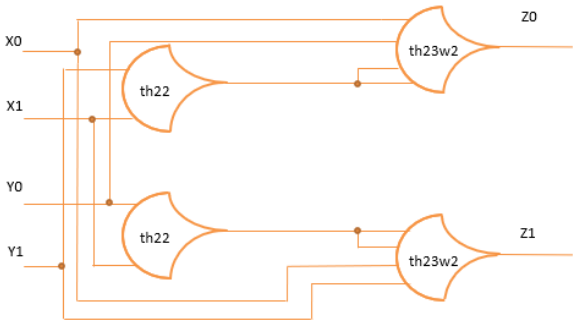

Figure 2. NCL dual–rail EXOR

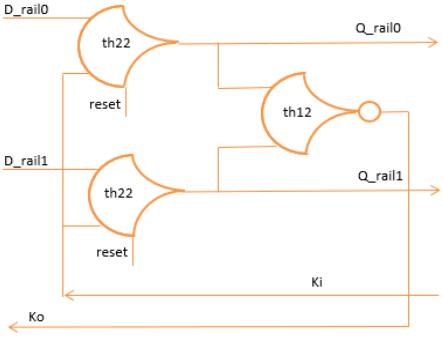

Figure 3. NCL dual–rail 1 bit register

3. THE AES ENCRYPTION FLOW

This section briefly presents 128-bit AES encryption (described in [21]) in which we use the key length of 128 bits. The flow of the AES encryption is implemented through five main function blocks: AddRoundKey, SubBytes, ShiftRows, MixColumns and KeyExpansion and they are arranged to perform through three basic steps shown in Figure 4. The implementation of the five functions mentioned above is presented and explained in detail in [14], [22].

– The first step is called as the initialization step in which the original plaintext is combined with the original key by the AddRoundKey transformation.
– The second step is named as the repeat encryption Step where the results from the first step are employed in order to sequentially perform functions such as SubBytes, ShiftRows, MixColumns and AddRoundKey. This step is also repeated nine times while the KeyExpansion transformation has to be performed in parallel with the AddRoundKey operation to create a key for this function.
– The final step is called as the output generation step where data output from the second step is executed through three sub-steps such as SubBytes, ShiftRows and AddRoundKey and the result of this step is ciphertext.

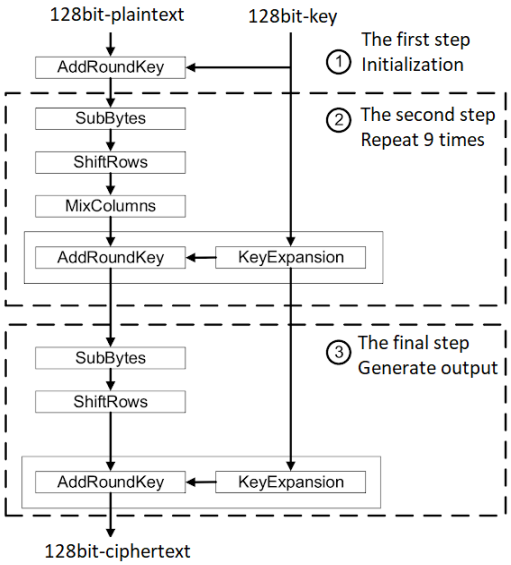

Figure 4. The AES encryption flow [23]

4. THE PROPOSED AES ENCRYPTION MODEL USING THE SYNCHRONOUS DESIGN METHOD

The synchronous AES encryption model illustrated in Figure 5 includes 11 rounds, 12 synchronous registers and a clock distributor pipelined by a twelve register system. Using an eleven-stage pipelined model also reduces the amount of logic in a clock cycle at the expense of more registers. That is the best way in order to reduce power consumption [24].

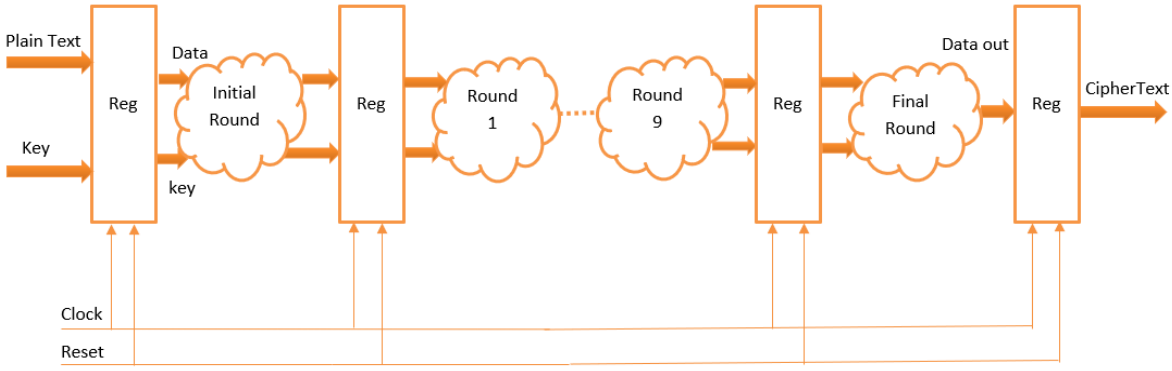

Figure 5. The synchronous AES encryption model

5. THE PROPOSED AES ENCRYPTION MODEL USING THE NCL BASED ASYNCHRONOUS DESIGN METHOD

The NCL based asynchronous AES encryption model is proposed and presented in this section. Figure 6 shows the asynchronous AES encryption model where the algorithm processes data blocks of 128 bits through the use of cipher keys with the lengths of 128 bits. Therefore, there are 11 rounds, 12 NCL registers and 11 completion detection circuits.

The Ko of the current register is connected to the Ki of the previous register and plays a role as an acknowledge and request signal. Initially, when reset signals in all NCL registers are turned on, the Null state is loaded into them, which causes Ko to transit from 0 to 1 state. Then Nulls are also loaded into computing blocks inside rounds, which causes signals in all rounds to Null. As a result, the circuit is on reset. When the output Q of a register returns complete Data, its Ko transits to 0 state and thus, drives Ki of the previous register to 0 state to wait for the Null wavefront [25]. Similarly, when the output Q of a register is already reset to a complete Null, its Ko will drive Ki of the previous register to 1 state to wait for the Data wavefront. Therefore, in an NCL system, two Data wavefronts will always be separated by the Null wavefront to avoid overwriting data. The structure of the initial round, round 1 to round 9, and the final round are shown in Figure 7, Figure 8, and Figure 9. In special cases, the first NCL register has no Ko signal because there is no round in front of it. The last NCL register has no next round so its Ko becomes Ki. A 128 bit NCL register comprising of 128 single bit NCL registers requires 128 completion signals. Since the maximum input threshold gate is the th_{44} gate, the number of logic levels in the completion component for a 128 bit register is given by $\log_4(128)=3,5$ [26] (approximately 4 levels) as shown in Figure 10. For the first register, it has no completion detection circuit depicted in Figure 11.

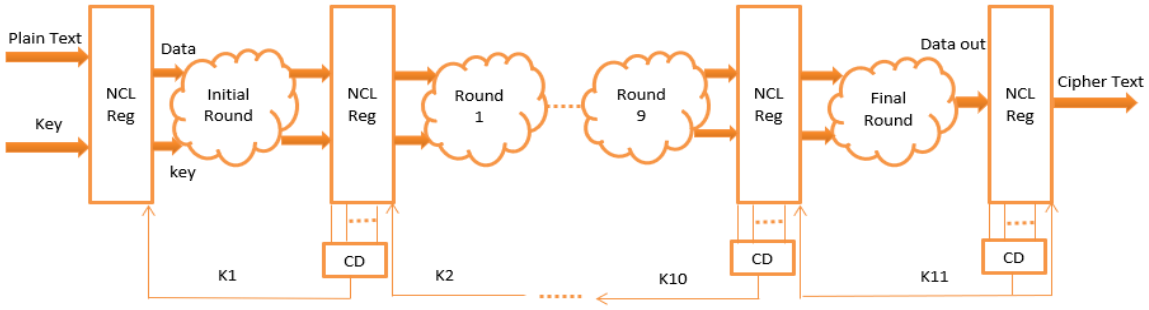

Figure 6. The asynchronous AES encryption model

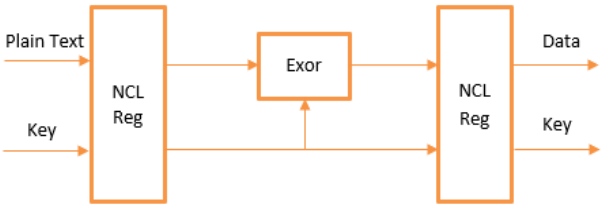

Figure 7. The structure of initial round

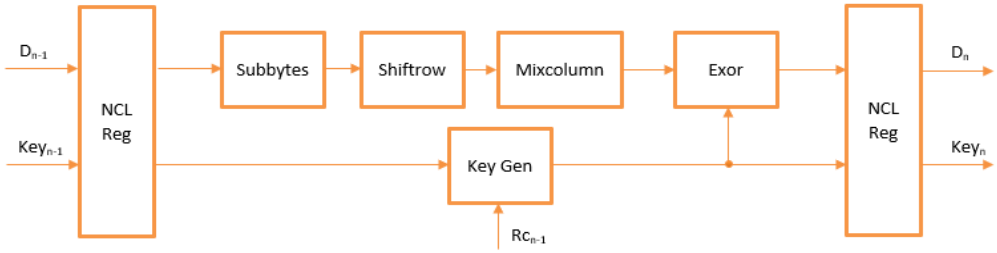

Figure 8. The structure of round 1-9

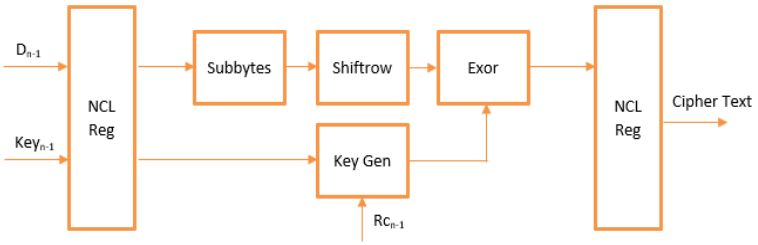

Figure 9. The structure of final round

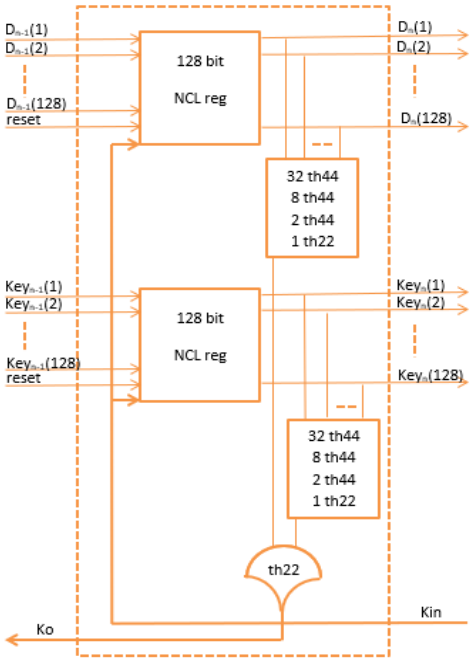

Figure 10. The structure of NCL 128 bits register and completion detection circuit

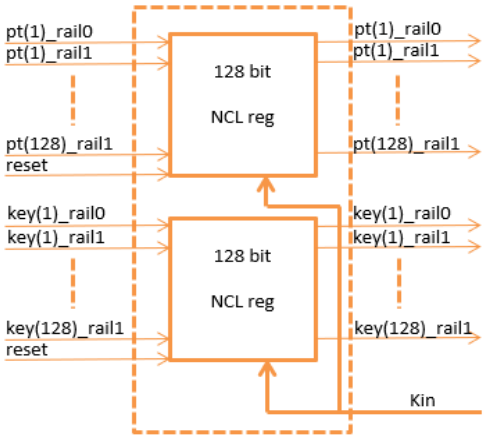

Figure 11. The structure of first NCL register

6. RESULTS AND DISCUSSION

The synchronous AES encryption model is simulated and synthesized for some parameters such as power consumption, processing speed and area by VCS tool and DC tool which use TSMC 65nm technology libraries. The simulation and synthesis results of the synchronous AES encryption model are depicted in Figure 12 and Figure 13. The maximum speed of the synchronous design model is shown in Figure 13 (c), where the maximum frequency is the frequency that the design still meets the timing. The function blocks in Figure 6 are also simulated and synthesized for the same parameters as in the synchronous AES encryption model by VCS, DC tool. In particularly, due to the lack of the NCL based asynchronous libraries, the synthesis results are also performed using the TSMC 65nm technology libraries shown in Figure 14.

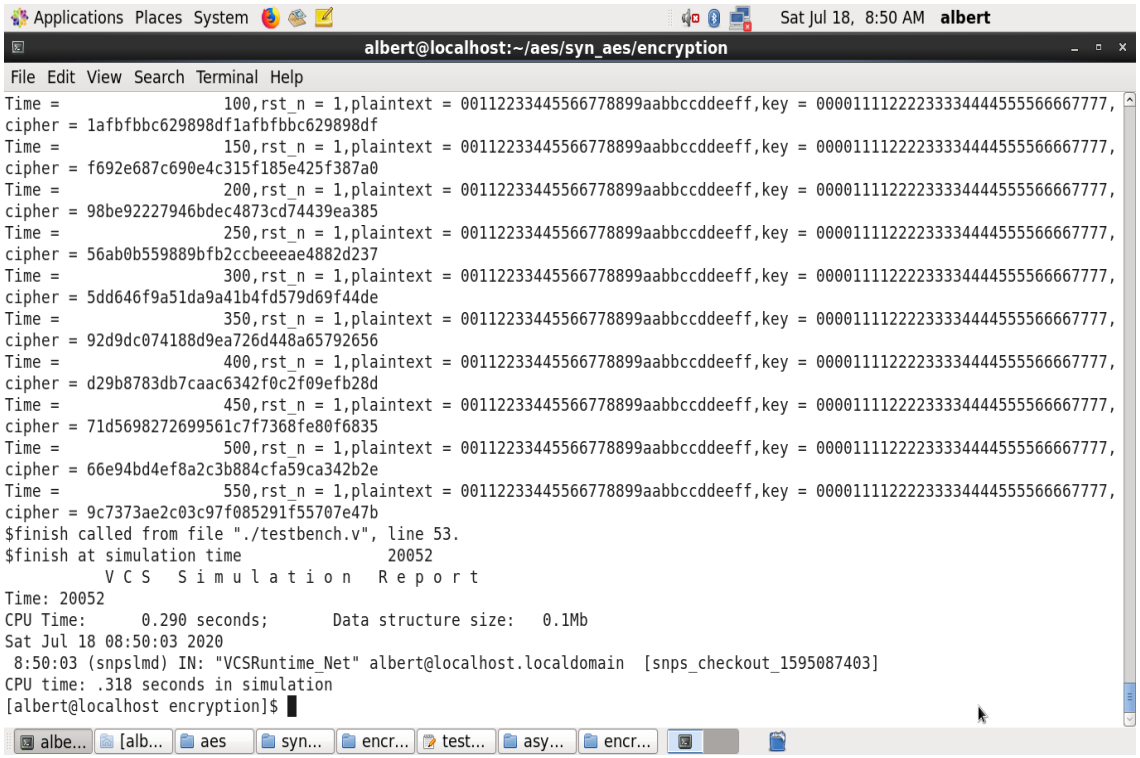

Figure 12. The simulation result of the synchronous AES encryption model

```
Number of nets:                       110987
Number of cells:                       87159
Number of combinational cells:         83933
Number of sequential cells:             2966
Number of macros/black boxes:              0
Number of buf/inv:                     11957
Number of references:                     25

Combinational area:             218599.679843
Buf/Inv area:                    17254.080677
Noncombinational area:           35328.000000
Macro/Black Box area:                0.000000
Net Interconnect area:      undefined  (No wire load specified)

Total cell area:                253927.679843
```

(a)

```
Global Operating Voltage = 1.32
Power-specific unit information :
    Voltage Units = 1V
    Capacitance Units = 1.000000pf
    Time Units = 1ns
    Dynamic Power Units = 1mW    (derived from V,C,T units)
    Leakage Power Units = 1pW


  Cell Internal Power  =   8.4162 mW   (78%)
  Net Switching Power  =   2.4173 mW   (22%)
                           ---------
Total Dynamic Power    =  10.8335 mW  (100%)

Cell Leakage Power     =   5.8524 uW
```

(b)

```
Timing Path Group 'clk'
-----------------------------------
Levels of Logic:              17.00
Critical Path Length:          0.85
Critical Path Slack:           0.00
Critical Path Clk Period:      0.95
Total Negative Slack:          0.00
No. of Violating Paths:        0.00
Worst Hold Violation:          0.00
Total Hold Violation:          0.00
No. of Hold Violations:        0.00
-----------------------------------
```

(c)

Figure 13. Extract reports on area, timing and power; (a) area report, (b) power report, and (c) timing report

```
Number of nets:                       546823
Number of cells:                      269439
Number of combinational cells:        212782
Number of sequential cells:              926
Number of macros/black boxes:              0
Number of buf/inv:                     15164
Number of references:                     23

Combinational area:             572166.720207
Buf/Inv area:                    22434.240800
Noncombinational area:               0.000000
Macro/Black Box area:                0.000000
Net Interconnect area:      undefined  (No wire load specified)

Total cell area:                572166.720207
```

(a)

```
Global Operating Voltage = 1.32
Power-specific unit information :
    Voltage Units = 1V
    Capacitance Units = 1.000000pf
    Time Units = 1ns
    Dynamic Power Units = 1mW    (derived from V,C,T units)
    Leakage Power Units = 1pW


  Cell Internal Power  =   2.4872 mW   (81%)
  Net Switching Power  = 567.8337 uW   (19%)
                           ---------
Total Dynamic Power    =   3.0550 mW  (100%)

Cell Leakage Power     =  10.5392 uW
```

(b)

```
Timing Path Group (none)
-----------------------------------
Levels of Logic:              43.00
Critical Path Length:          2.91
Critical Path Slack:         uninit
Critical Path Clk Period:       n/a
Total Negative Slack:          0.00
No. of Violating Paths:        0.00
Worst Hold Violation:          0.00
Total Hold Violation:          0.00
No. of Hold Violations:        0.00
-----------------------------------
```

(c)

Figure 14. Extract reports on area, power and timing; (a) area report, (b) power report, and (c) timing report

Because the synopsys DC tools do not support critical timing path for asynchronous designs, the maximum delay computation is based on the formula below [27]:

$$TDD = 2 * (Tcomb + Tcomp) = 5.82\ (ns)$$

where,
T_{DD}: is the average delay.
T_{comb}: is the combinational delay.
T_{comp}: is the delay of the completion components.
Beside the above mentioned synthesis results, the NCL based asynchronous AES encryption model is also simulated by VCS tool with the same data and key in the synchronous AES encryption model and gives the same simulation results as depicted in Figure 15.

Comparison between the synchronous circuit model and the NCL based asynchronous circuit model is presented in Table 2. Although both methods are simulated and synthesized by using the same TSMC 65nm technology libraries, the cycle time T=10 ns and supply voltage V_{dd}=1.32 V, the verifications of the area, power of the NCL based asynchronous circuit compared with the synchronous circuit is consistent with the theory. In Table 2, the area of the synchronous circuit (253927 μm^2) is smaller than the area of the asynchronous circuit (572167 μm^2). That is because of the appearance of the complete detection circuit in a pipelined NCL asynchronous system. Whereas power consumption of the synchronous circuit (10.8394 mW) is larger than that of the asynchronous circuit (3.0653 mW) because switching power of the synchronous circuit model is larger than that in the NCL based asynchronous circuit model. In term of processing speed, 171 MHz for asynchronous design is slower than 1050 MHz for the counterpart, but the synchronous design is harder to achieve that maximum speed because of clock related issues. The synthesis results mentioned above are obtained by using the same 65nm technology libraries in the asynchronous and synchronous approaches

```
File  Edit  View  Search  Terminal  Help
and may be used and disclosed only as authorized in a license agreement
controlling such use and disclosure.

20:21:41 (snpslmd) OUT: "VCSCompiler_Net" albert@localhost.localdomain  [snps_checkout_1595042501]
The design hasn't changed and need not be recompiled.
If you really want to, delete file simv.daidir/.vcs.timestamp and
run VCS again.

20:21:41 (snpslmd) IN: "VCSCompiler_Net" albert@localhost.localdomain  [snps_checkout_1595042501]
20:21:42 (snpslmd) OUT: "VCSRuntime_Net" albert@localhost.localdomain  [snps_checkout_1595042502]
Chronologic VCS simulator copyright 1991-2017
Contains Synopsys proprietary information.
Compiler version M-2017.03-SP2_Full64; Runtime version M-2017.03-SP2_Full64;  Jul 17 20:21 2020
VCD+ Writer M-2017.03-SP2_Full64 Copyright (c) 1991-2017 by Synopsys Inc.
Time =                    0,rst_n = 0,d_rail1 = 0011223344556677889 9aabbccddeeff,d_rail0 = ffeeddccbbaa9988776655443322110
0,k_rail1 = 0000111122223333444455556666777 7,k_rail0 = ffffeeeeddddccccbbbbaaaa99998888,cipher_rail1 = 0000000000000000000
0000000000000,cipher_rail0 = 0000000000000000000000000000000000
Time =                    5,rst_n = 1,d_rail1 = 0011223344556677889 9aabbccddeeff,d_rail0 = ffeeddccbbaa9988776655443322110
0,k_rail1 = 0000111122223333444455556666777 7,k_rail0 = ffffeeeeddddccccbbbbaaaa99998888,cipher_rail1 = 9c7373ae2c03c97f085
291f55707e47b,cipher_rail0 = 638c8c51d3fc3680f7ad6e0aa8f81b84
$finish called from file "./testbench.v", line 59.
$finish at simulation time                505
           V C S   S i m u l a t i o n   R e p o r t
Time: 505
CPU Time:      1.540 seconds;       Data structure size:   4.7Mb
Fri Jul 17 20:21:43 2020
20:21:43 (snpslmd) IN: "VCSRuntime_Net" albert@localhost.localdomain  [snps_checkout_1595042502]
CPU time: 1.576 seconds in simulation
```

Figure 15. the simulation results of the asynchronous AES encryption model

Table 2. Comparison between two methods of area, power and speed

Specification	Area (μm^2)	Total Power (mW)	Speed (MHz)
Asynchronous design (NCL)	572,167	3.0653	171
Synchronous design	253,927	10.8394	1,050
Ratio (Asyn/Syn)	2.2533	0.2828	0.1629

From Figure 16, it is observed that the higher frequency operates, the more power dissipation of synchronous circuit consumes. In particular, power consumption of the synchronous circuit is 3.5 times higher than that of the asynchronous circuit at 100 Mhz frequency. This is because as the frequency increases, the synchronous circuit will switch more, which causes the switching power to increase significantly. In addition, because the asynchronous circuit does not use the clock and the switching power is consumed only when DATA and NULL wavefront are being processed [27], the power consumption of asynchronous circuit does not change much. In order to highlight the low power advantage of the NCL based asynchronous design, we compare it with the synchronous method using clock gating technique in term of power in Table 3.

Table 3 shows that the NCL-based asynchronous circuit design method produces 91.12% less power consumption than the synchronous method using clock gating technique. In addition, the NCL-based asynchronous circuit design method generates 93.23% less power consumption than the counterpart without

using clock gating technique. Furthermore, compared to ultra low power encryption in [28], our work also shows a 27.60% improvement.

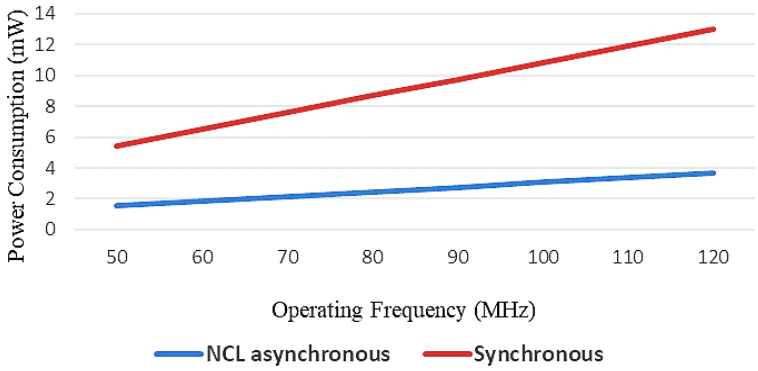

Figure 16. Power consumption for various frequencies

Table 3. Comparison of the power consumption of the methods

Specification	Area (μm^2)	Total Power (mW)	Speed (MHz)
NCL based Asynchronous design (our work)	572167	3.0653	171
Synchronous design with Clock Gating [6]		34.5277	667
Synchronous design without Clock Gating [6]		45.2924	667
Ultra low power Encryption [28]	211600	4.234	125

7. CONCLUSION

The NCL based asynchronous circuit design method not only has low power potential in small scale circuits but also has low power potential in large scale circuits. In this paper, we have demonstrated this potential through implementing two AES encryption models by using the synchronous circuit design technique and the NCL based asynchronous circuit design technique. Despite the lack of libraries and supporting tools, we recognize that the results of power consumption show the advantages of the NCL based asynchronous circuit design method over the synchronous circuit design method. If the power criterion of the integrated circuits is preferred, the NCL based asynchronous integrated circuit design method will be a promising candidate. Our future works will focus on analysis and synthesis of NCL based asynchronous circuits by using the dedicated libraries in order to validate convincingly low power property for the NCL based asynchronous circuit design method.

ACKNOWLEDGEMENTS

We acknowledge the support of time and facilities from Ho Chi Minh City University of Technology (HCMUT), VNU-HCM for this study.

REFERENCES

[1] J. Wu, "Null convention logic applications of asynchronous design in nanotechnology and cryptographic security," Docotoral dissertation, Department Electrical and Computer Engineering, Missouri University of Science and Technology, USA, 2012.

[2] B. Padmavathi, B. T. Geetha and K. Bhuvaneshwari, "Low power design techniques and implementation strategies adopted in VLSI circuits," *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, 2017, pp. 1764-1767, doi: 10.1109/ICPCSI.2017.8392017.

[3] Md. Z. Hussain and K. N. Parvin, "Low power and high performance FFT with different radices," *International Journal of Reconfigurable and Embedded Systems*, vol. 8, no. 2, pp. 99-106, 2019, doi: 10.11591/ijres.v8.i2.pp99-106.

[4] M. Saber and M. M. Eid, "Low power pseudo-random number generator based on lemniscate chaotic map," *International Journal of Electrical and Computer Engineering*, vol.11, no. 1, pp. 863-871, Feb. 2021, doi: 10.11591/ijece.v11i1.pp863-871.

[5] 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," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 1, pp. 21-29, 2020, doi: 10.11591/eei.v9i1.1654.

[6] P. -K. Dong, H. K. Nguyen, V. -P. Hoang and X. -T. Tran, "Low-power implementation of a high-throughput multi-core AES encryption architecture," *2020 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, 2020, pp. 74-77, doi: 10.1109/APCCAS50809.2020.9301668.
[7] K. Haulmark, W. Khalil, W. Bouillon and J. Di, "Comprehensive comparison of null convention logic threshold gate implementations," *2018 New Generation of CAS (NGCAS)*, 2018, pp. 37-40, doi: 10.1109/NGCAS.2018.8572223.
[8] B. G. Fawzy, M. M. Abutaleb, M. I. Eladawy and M. Ghoneima, "Strong indication full-adder circuit for null convention logic automation flows," *2018 18th International Symposium on Communications and Information Technologies (ISCIT)*, 2018, pp. 416-421, doi: 10.1109/ISCIT.2018.8588000.
[9] A. J. Albert and S. Ramachandran, "Static implementation of a null convention logic based exponent adder," *International Journal of Applied Engineering Research,* vol. 10, no. 3, pp. 7601-7614, 2015.
[10] A. Caberos, S. Huang and F. Cheng, "Area-efficient CMOS Implementation of NCL Gates for XOR-AND/OR dominated circuits," *2017 IEEE Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics (PrimeAsia)*, 2017, pp. 37-40, doi: 10.1109/PRIMEASIA.2017.8280358.
[11] P. Metku, K. K. Kim, and M. Choi, "Novel area-efficient null convention logic based on CMOS and gate diffusion input (GDI) hybrid," *Journal of Semiconductor Technology and Science*, vol. 20, no. 1, pp. 127-134, 2020, doi: 10.5573/JSTS.2020.20.1.127.
[12] N. Le Huy and P. Beckett, "Null convention logic primitive element architecture for ultralow power high performance portable digital systems," *2017 IEEE Regional Symposium on Micro and Nanoelectronics (RSM)*, 2017, pp. 167-170, doi: 10.1109/RSM.2017.8069157.
[13] M. Howard, N. Mize and J. Di, "Investigation and comparison of bus alternatives for asynchronous circuits," *SoutheastCon 2018*, 2018, pp. 1-2, doi: 10.1109/SECON.2018.8478988.
[14] D. V. Supriya and M. R. Niranjan, "Realization of AES encryption and decryption based on null convention logic," *International Research Journal of Engineering and Technology*, vol. 2, no. 7, pp. 77-81, 2015.
[15] R. M. Sovani, "Near and sub-threshold null convention logic design for low-power digital signal processing applications," Master Thesis, School of Electrical and Computer Engineering. RMIT University, Australia, 2016.
[16] N. Kulkarni, "Energy-efficient digital circuit design using threshold logic gates," Doctoral Dissertation, Arizona State University, USA, 2015.
[17] N. Le Huy, A. S. Holland and P. Beckett, "Silicon on insulator null convention logic based asynchronous circuit design for high performance low power digital systems," *2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom)*, 2018, pp. 111-115, doi: 10.1109/SIGTELCOM.2018.8325772.
[18] D. L. Oliveira, O. Verducci, L. A. Faria and T. Curtinhas, "A novel κ convention logic (NCL) gates architecture based on basic gates," *2017 IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, 2017, pp. 1-4, doi: 10.1109/INTERCON.2017.8079680.
[19] A. Vakil, K. P. Jayadev, S. Hegde and D. Koppad, "Comparitive analysis of null convention logic and synchronous CMOS ripple carry adders," *2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 2017, pp. 1-5, doi: 10.1109/ICECCT.2017.8117926.
[20] S. D. Putra, A. S. Ahmad, S. Sutikno, Y. Kurniawan, and A. D. W. Sumari, "Revealing AES encryption device key on 328P microcontrollers with differential power analysis," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 6, pp. 5144-5152, December 2018, doi: 10.11591/ijece.v8i6.pp5144-5152.
[21] A. M. Abdullah, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," *Cryptography and Network Security*, 2017.
[22] D. Swathi, P. Gangadhar, and D. V. Supriya, "Designing of s-box based on null convention logic," *International Research Journal of Engineering and Technology*, vol. 2, no. 8, pp. 71–76, 2015.
[23] L. P. Kumar and A. K. Gupta, "Implementation of speech encryption and decryption using advanced encryption standard," *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2016, pp. 1497-1501, doi: 10.1109/RTEICT.2016.7808081.
[24] N. H. E. Weste and D. M. Harris, *CMOS VLSI design a circuits and systems perspective*, 4th Edition, London, U.K.: Addison Wesley, Pearson, 2010.
[25] L. D. Tran, G. I. Matthews, P. Beckett and A. Stojcevski, "Null convention logic (NCL) based asynchronous design - fundamentals and recent advances," *2017 International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom)*, 2017, pp. 158-163, doi: 10.1109/SIGTELCOM.2017.7849815.
[26] R. Sankar, *et al*., "Implementation of static and semi-static versions of a bit-wise pipelined dual-rail NCL 2S complement multiplier," *2007 IEEE Region 5 Technical Conference*, 2007, pp. 228-233, doi: 10.1109/TPSD.2007.4380386.
[27] A. J. Albert and S. Ramachandran, "Null convention floating point multiplier," *The Scientific World Journal*, 2015, doi: 10.1155/2015/749569.
[28] A. Zaky, E. Elmitwalli, M. Hemeda, Y. Ismail and K. Salah, "Ultra low-power encryption/decryption core for lightweight iot applications," *2019 15th International Computer Engineering Conference (ICENCO)*, 2019, pp. 39-43, doi: 10.1109/ICENCO48310.2019.9027471.

BIOGRAPHIES OF AUTHORS

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, Null Convention Logic (NCL) based asynchronous circuit design method and power electronics.

Lac Truong Tri was born in Tien Giang province, Vietnam. He received the Bachelor of Engineering degree in Electronics - Telecommunication Engineering major in Ho Chi Minh City University of Technology in 2020. 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.