International Journal on Applications in Electrical and Electronics Engineering
Volume 8 : Issue 2 : September 2022, pp 7 – 12 www.aetsjournal.com ISSN (Online) : 2395 - 3527

IMAGE CRYPTOGRAPHY DESIGN USING NANO AES ALGORITHM

S.JAYAPRIYA , R.RAJINI VISHWANITHA

Abstract— An electronic data encryption standard is known as Advanced Encryption Standard (AES).This standard is used in both software and hardware, and it is today one of the most widely used encryption techniques. Implementation of a symmetric cryptography algorithm with good security on a field-programmable gate array (FPGA). 8-bit data channels as well as five primary blocks are included in the proposed architecture. In our project, to keep the plain text, keys, and also intermediate data, we create two independent register banks, Key-Register and State-Register. Shift Rows are integrated into the State Register to save space. We carry out an efficient block of 8 bit containing the four internal registers that take and send a 8-bit to fit the Mix Column to an 8-bit data path. Advanced shared Sub-Bytes are also used for the key expansion and encryption process.

Keywords— Advanced Encryption Standard (AES), 8-bit,Save space

I. INTRODUCTION

Since the beginning of time, people have had two basic needs: (a) communication and information sharing, and (b) selective sharing. These two requirements have made the art of coding so that only a writer can read it. Even if encrypted messages fall into their hands, unauthorized persons will not be able to retrieve any information. Cryptography is the art and science of encrypting messages about the use of privacy in information security. The Advanced Encryption Standard (AES) is the most widely used and effective encryption method.AES is at least six times quicker than DES and detects three times faster.. Because the DES key size was too small, it needed to be changed. It was thought that it could be vulnerable to search keywords as the processing power grows. Three times DES was created to deal with this error, yet it proved to be lazy. The AES specifications are.

S.Jayapriya , *Department Of VLSI , Vandayar Engineering College, Pulavarnatham, Thanjavur.*
(Email : jayapriyasekar3296@gmail.com)

R.Rajini Vishwanitha M.E , *Department Of VLSI , Vandayar Engineering College, Pulavarnatham, Thanjavur.*

- Data in 128 bits, keys in 128/192/256 bits
- AES is secured and stronger than the Triple-DES.
- Provide all architectural info.
- Software that would be used in combination with HDL.

Operation of AES

AES would be an adaptive cypher rather than a Feistel cypher. A 'permission-exchange network' is used. Contains a series of interconnected operations, some of which require the replacement of a specific output (changed) and others which are more time consuming (permissions).The AES does all calculations in bytes instead of bits. So that, a 128-bit plaintext block is processed as if it were a 16-bit plaintext blocks by AES. These 16 bytes are split into four rows and four columns by using matrix. The number of iterations in AES could be modified, unlike DES, and is decided by a key size. For 128-bit keys, the AES algorithm uses ten rounds, twelve for 192-bit keys, and fourteen for 256-bit keys. For this, a one-of-a-kind 128-bit round key is employed.

II. RELATED WORKS

Power analysis impact is a severe danger to the security of FPGAs. Int. J. Internet Technol. Secured Trans., vol. 4, no. 1, pp. 12–25, M. Masoumi. Differential power analysis (DPA) attack, as well as a feasible and productive development of this threat over an FPGA implementation of the AES encryption algorithm. Such AES algorithms require high-speed VLSI designsX. Zhang and K. K. Parhi, IEEE Trans. Very Large Scale Integration (VLSI) Syst., vol. 12, no. 9, pp. 957–967. High-performance approaches for integrating an Advanced Encryption Standard (AES) technique using hardware.

III. PROPOSED NANO AES DEVELOPMENT

For both ASIC and FPGA stages, we utilize Verilog HDL to execute the suggested nano-AES multiplier. We planned a lightweight AES architecture for IoT gadgets with restricted assets. There was a 8-bit information way and two register banks for plain text, keys, and halfway outcomes in the plan. Inside the State-Register, Shift-Rows were employed to simplify the required logic.

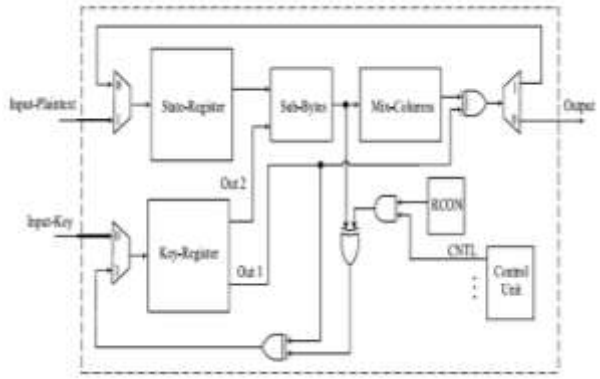


Figure 1: Proposed NANO AES Encrypter

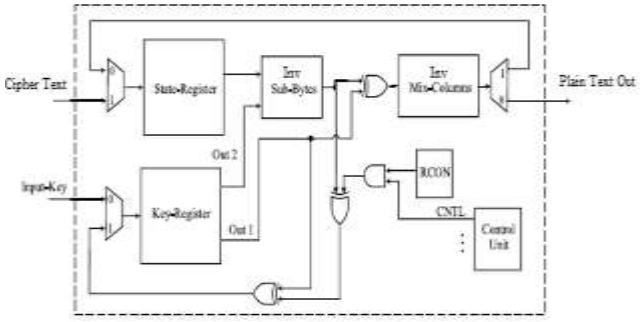


Figure 2 : Proposed NANO AES Decrypter

The camouflaged AES core and Clock gating are used to construct the encryption masks in the AES implementation. The AES core is hidden, and it performs 128-bit encryption. When compared to a totally unrolled technique, the operation is carried out in ten cycles, with each round being calculated once and to saving the space, the circuitry from each cycle is reused. The suggested masked AES is depicted in the diagram below. A random mask is used to mask the original data (plaintext).The data which being concealed are moved to the "Nano AES center," which encodes the covered information utilizing the mystery key. The module receives the result masked cipher-text and converts it to the desired cipher-text.

1) The Shift-Rows are incorporated into the State-Register to simplify the needed logic.
2) The Sub-Bytes block has been optimized and is shared with the key expansion and encryption stages.
3) Based on the layout of an 8-bit data stream, we create an efficient 8-bit module with Mix-Columns with 8-bit input and output. The Add-Round-Key command is then executed. As a result, the data are passed to Add-Round-Key byte by byte. For Key-Register, as for 32-bit Mix-columns, it is not necessary to record the data in registers or to increase the data stream to 32 bits.
4) It isn't important to save the outcomes in the registers or to expand the data stream to 32 bits for Key-Register, as it is for 32-bit Mix-columns.

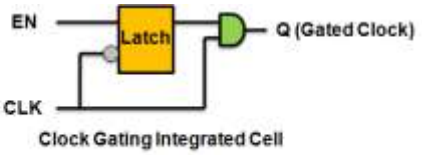
We employ the clock gating mechanism in numerous elements of the design to decrease dynamic force utilization. The clock gating is done individually to State-Register, Mix-Columns' internal registers, Key-Register, and RCON. Because in key expansion process , the blocks of two data which is disuse the key expansion phase, the clocks of the State-Register and the Mix-Columns are deactivated to conserve power during that phase. In Fig 2 show the Decrypter of the AES Design.

```
state = M
AddRoundKey(state, &w[0])
for i = 1 step 1 to 9
    SubBytes(state)
    ShiftRows(state)
    MixColumns(state)
    AddRoundKey(state, &w[i*4])
end for
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, &c.W[10])
```

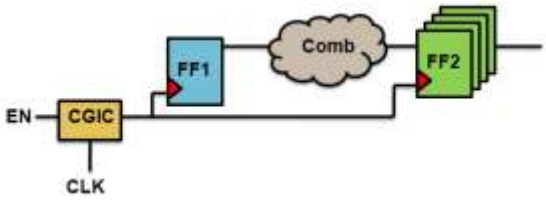
Pseudo code

1) CLOCK GATING:

Clock gating is a notable methodology for diminishing chip dynamic power. Two contemporary clock gating advances are ACG (Adaptive Clock Gating) and guidance level clock gating. The clock gating methodology limits not simply practical square changing movement in the expansion to static power in the inactive state, dynamic power is utilized in the working state . The functional block's clock can be enabled or disabled automatically using the modified ACG (Adjustable Clock Gating.) In synchronous circuits, clock gating is a typical method of reducing dynamic power dissipation. By trimming the clock tree and adding extra logic to a circuit, clock gating saves electricity.



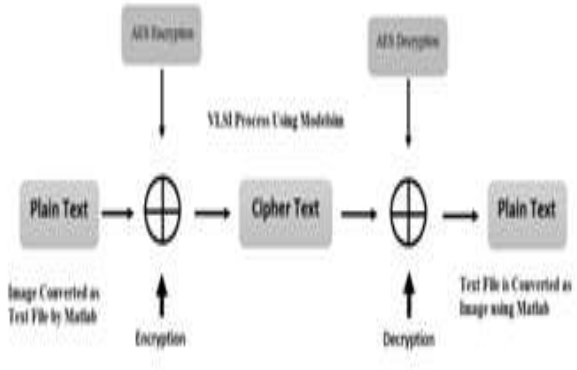
Clock Gating Integrated Cell



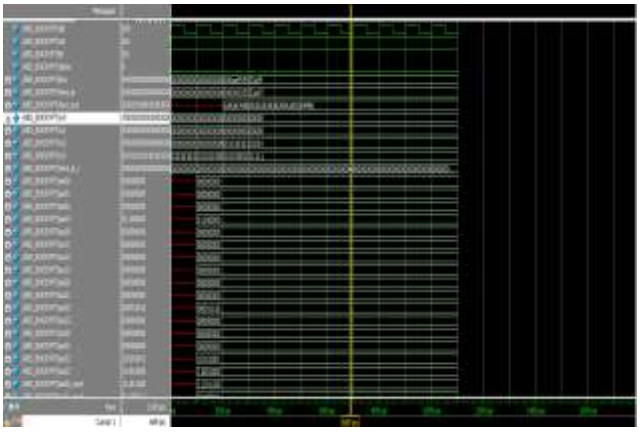
With the increased use of mobile devices like cellphones, PDAs, and MP3 players, there has been a lot of study on low-power design strategies. The continual lowering in the minimum feature size of transistors, resulting in increased device intensity and design complexity. Clock and data-path power dissipation account for the majority of a chip's total power consumption.

One of the most successful logics in RTL and design power dissipation is clock-gating.

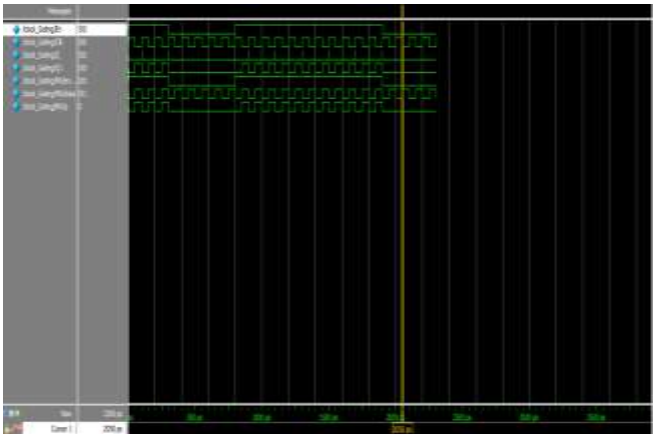
Because individual IP utilization fluctuates between applications, clock gating is an excellent strategy for decreasing dynamic power. Since not all IP centers are utilized constantly, there is a chance to lessen the force of the IP centers that aren't being utilized. Whenever an IP center isn't being used, clock gating effectively turns down the clock by consolidating (AND door) the clock with an entryway control signal, limiting power scattering from over the top charging and releasing of the unused circuits. One of the most successful logics in RTL and design power reduction is clock-gating. Clock gating would be a good way to cut down on dynamic power. Based on the proposed scheme, we will create a decryption scheme. Encryption and decryption will be done using for Image Encryption and Decryption. For this process, we will combine Matlab and VLSI .



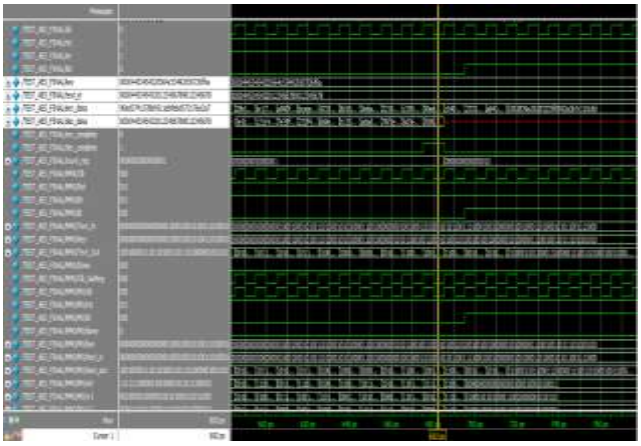
IV. SIMULATION RESULTS



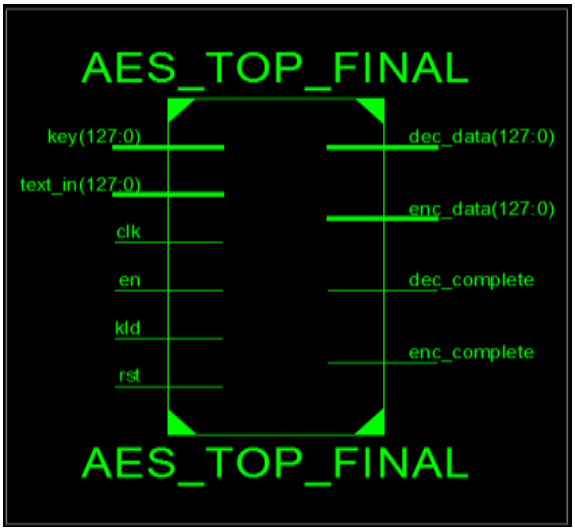
NANOAES Encrypter with clock Gating

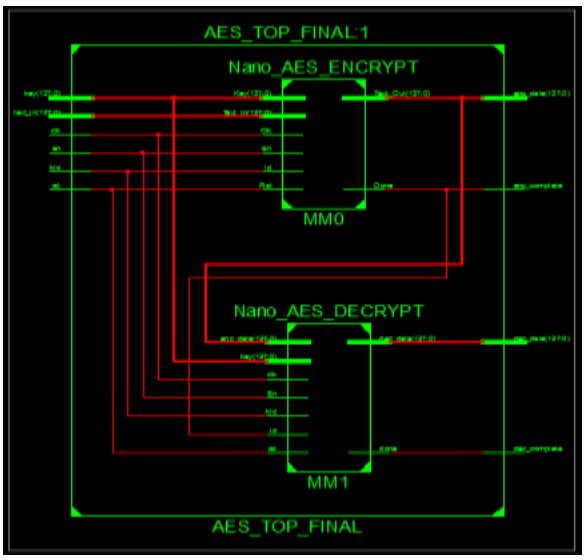


Clock Gating

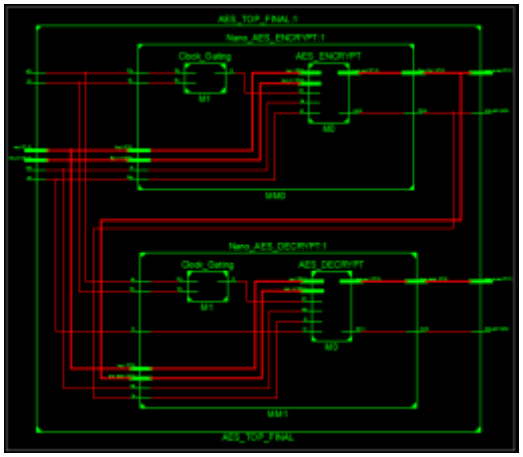


Final Encryption & Decryption



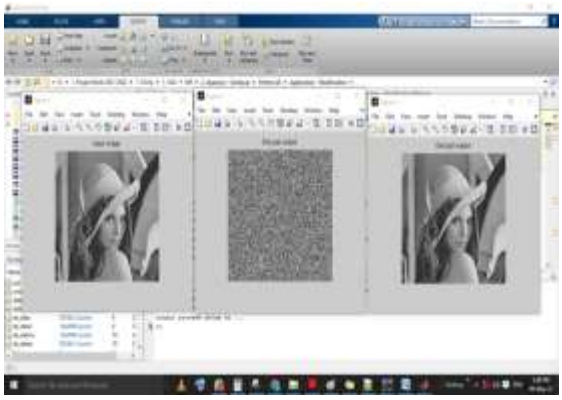


RTL View of AES MAIN Module



Inner View of TOP AES DESIGN

1)IMAGE ENCRYPTION & DECRYPTION RESULTS

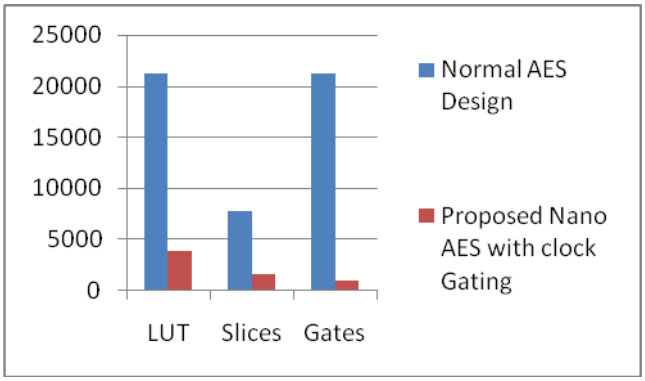


V. COMPARISON AND ANALYSES

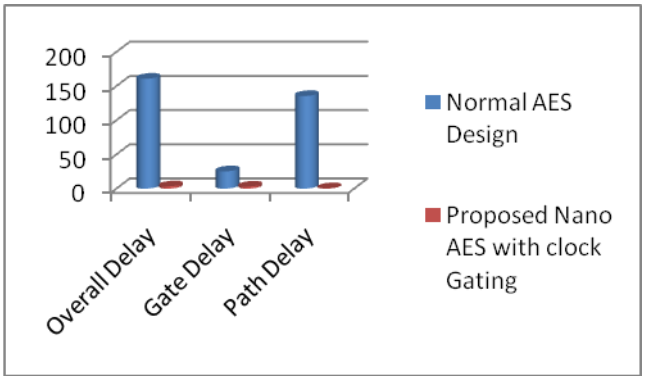
The suggested AES design concepts are built in Verilog HDL, generated with Xilinx for various bit sizes, and the latency and area are compared. As seen in Fig. 4, AES Design with clock Gating has the smallest area and has the shortest latency when compare to AES as the number of bits increases. The results demonstrate that using Clock gating Nano AES for inclusion achieves the suggested Design's overall minimum area.

S. No	Method Name	Area			Delay		
		Slice	Flip Flops	LUT	Max Delay	Gate Delay	Path Delay
1	Normal AES Design	7734	21207	21207	160.860ns	25.302ns	135.558ns
2	Proposed Nano AES with Clock Gating	1670	1066	3900	3.405ns	2.923ns	0.482ns

Comparison Chart



Area Analysis



Delay Analysis

VI. CONCLUSION

Nano AES is a symmetric encryption technology with great security that is frequently used in a range of applications and networks. As a result, AES is an excellent solution for IoT devices of all sizes. We used a lightweight AES architecture to develop a resource-constrained IoT device. In this post, we created a resource-constrained IoT device using a lightweight AES architecture. The architecture had an 8-bit data route and two register banks of saving plain text, keys, and interim outputs. Inside the State-Register, Shift-Rows were employed to simplify the required logic. Further developed encryption for the Sub-Bytes and the key expansion process were likewise remembered for the plan. We additionally planned 8-digit info and result blend Columns, which is an extraordinary square for lower-region plan.

REFERENCES

[1] K. Fu and J. Blum, "Controlling for cybersecurity risks of medical device software," Commun. ACM, vol. 56, no. 10, pp. 35–37, Oct. 2013.

[2] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and privacy for implantable medical devices," IEEE Pervasive Comput., vol. 7, no. 1, pp. 30–39, Jan./Mar. 2008.

[3] M. Rostami, W. Burleson, A. Jules, and F. Koushanfar, "Balancing security and utility in medical devices?" in Proc. 50th ACM/EDAC/IEEE Int. Conf. Design Autom., May/Jun. 2013, pp. 1–6.

[4] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," Proc. IEEE, vol. 102, no. 8, pp. 1174–1188, Aug. 2014.

[5] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," IEEE Security Privacy, vol. 8, no. 1, pp. 81–85, Jan./Feb. 2010.

[6] M. Mozaffari-Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging frontiers in embedded security," in Proc. 26th Int. Conf. VLSI Design, Jan. 2013, pp. 203–208.

[7] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of things," Computer, vol. 44, no. 9, pp. 51–58, Sep. 2011.

[8] T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker, "Challenges in access right assignment for secure home networks," in Proc. USENIX Conf. Hot Topics Secur., 2010, pp. 1–6.

[9] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Concurrent structure independent fault detection schemes for the Advanced Encryption Standard," IEEE Trans. Comput., vol. 59, no. 5, pp. 608–622, May 2010.

[10] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A low-power high performance concurrent fault detection approach for the composite field S-box and inverse S-box," IEEE Trans. Comput., vol. 60, no. 9, pp. 1327–1340, Sep. 2011.

[11] N. Ahmad, R. Hasan, and W. M. Jubadi, "Design of AES S-box using combinational logic optimization," in Proc. IEEE Symp. Ind. Electron. Appl. (ISIEA), Oct. 2010, pp. 696–699.

[12] S. Banik, A. Bogdanov, and F. Regazzoni, "Exploring energy efficiency of lightweight block ciphers," in Proc. Int. Conf. Sel. Areas Cryptogr. Sackville, NB, Canada: Springer, 2015, pp. 178–194.

[13] H. K. Kim and M. H. Sunwoo, "Low power AES using 8-bit and 32-bit datapath optimization for small Internet-of-Things (IoT)," J. Signal Process. Syst., vol. 91, nos. 11–12, pp. 1283–1289, 2019.

[14] V.-P. Hoang, V.-L. Dao, and C.-K. Pham, "An ultra-low power AES encryption core in 65 nm SOTB CMOS process," in Proc. Int. SoCDesign Conf. (ISOCC), Oct. 2016, pp. 89–90.

[15] X. Zhang and K. K. Parhi, "High-speed VLSI architectures for the AES algorithm," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 12, no. 9, pp. 957–967, Sep. 2004.

[16] C. Paar, "Efficient VLSI architectures for bit-parallel computation in Galois fields," Ph.D. dissertation, Inst.

Dept. Experim. Math., Univ. Duisburg-Essen, Duisburg, Germany, 1994.

[17] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact Rijndael hardware architecture with S-box optimization," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur. Gold Coast, QLD, Australia: Springer, 2001, pp. 239–254.

[18] E. N. Mui, R. Custom, and D. Engineer, "Practical implementation of Rijndael S-box using combinational logic," Custom R&D Engineer Texco Enterprise, Tech. Rep., 2007. [Online]. Available: http://www. geocities.ws/dariuskrail20/Practical_Implementation_of_ Rij dael_SBox_Using_Combinational_Logic.pdf

[19] Federal Information Processing Standards Publication 197, Advanced Encryption Standard FIPS PUB 97, 2001, pp. 1–51.

[20] A. Reyhani-Masoleh, M. Taha, and D. Ashmawy, "New area record for the AES combined S-box/inverse S-box," in Proc. IEEE 25th Symp. Comput. Arithmetic (ARITH), Jun. 2018, pp. 145–152.

[21] K. Shahbazi and S.-B. Ko, "High throughput and area-efficient FPGA implementation of AES for high-traffic applications," IET Comput. Digit. Techn., vol. 14, no. 6, pp. 344–352, Nov. 2020.

[22] P. Hamalainen, T. Alho, M. Hannikainen, and T. D. Hamalainen, "Design and implementation of low-area and low-power AES encryption hardware core," in Proc. 9th EUROMICRO Conf. Digit. Syst. Design (DSD), 2006, pp. 577–583.

[23] S. Mathew et al., "340 mV–1.1 V, 289 Gbps/W, 2090-gate Nano AES hardware accelerator with area-optimized encrypt/decrypt GF(24)2 polynomials in 22 nm tri-gate CMOS," IEEE J. Solid-State Circuits, vol. 50, no. 4, pp. 1048–1058, Apr. 2015.

[24] A. Shreedhar et al., "Low gate-count ultra-small area nano advanced encryption standard (AES) design," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), May 2019, pp. 1–5.

[25] V.-P. Hoang, V.-L. Dao, and C.-K. Pham, "Design of ultra-low power AES encryption cores with silicon demonstration in SOTB CMOS process," Electron. Lett., vol. 53, no. 23, pp. 1512–1514, Nov. 2017.

[26] C. Hocquet et al., "Harvesting the potential of nano-CMOS for lightweight cryptography: An ultra-low-voltage 65 nm AES coprocessor for passive RFID tags," J. Cryptograph. Eng., vol. 1, no. 1, pp. 79–86, Apr. 2011.