International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 3, ISSN No. 2455-2143, Pages 179-182
Published Online July 2022 in IJEAST (http://www.ijeast.com)

AN INNOVATIVE IMPLEMENTATION OF ENCRYPTION ALGORITHM ON FPGA IN MANY CORE ARCHITECTURES.

Dr. Gnanajeyaraman Rajaram,
M.E; Professor,
SBM College of Engineering and Technology,
Dindigul.

Jeyanthi.S,
M.E;Assistant Professor,
SBM College of Engineering and Technology,
Dindigul.

***Abstract*— In this paper, we grant the remodeling with the aid of "categorizes" of amenities—a category being explained as a group of amenities that share innovative operations and are mapped to the same key value based on Encryption schemes of sub-bytes transformation method. The sub-bytes transformation method is the high-speed standard Encryption module. AES Algorithm is synthesized by utilizing Verilog code and encountered into FPGA. We implement a new design of AES Algorithm in FPGA in many core Architectures which is an in-built one.**

***Keywords*— AES Algorithm, Sub-Bytes transformation, FPGA.**

I. INTRODUCTION

The acronym FPGA stands for Field Programmable Gate Array. It is an integrated circuit that can be automated with operator for determined application after it has been fabricated. Synchronous FPGAs consist of adaptive logic modules (ALMs) and logic elements (LEs) intertwined through configurable correlates with one another. The impediments innovate physical architecture of logic gates be modeled operating particular simulations. It is a unique one by comparing distinct categories of microcontrollers or Central Processing Units, whose layout is formed and secured by fabricator and further modifications cannot be implemented.

By implementing the high-speed algorithm of standard AES in FPGA, improving the data transmission engine, where the modification be used in pipelining for many cores network. Here a 128-bits, 192-bits and, 256-bits data key is introduced in the AES algorithm. The quantity of key relies upon the various dimensions of streams of Advanced Encryption Standard, for 10 streams we have 128-bits, for 12 streams 192-bits and for 14 streams be obtained 256-bit size.

Every stream consists of self-cryptographic simulations that combined with cipher key operating addition of round key, sub bytes exploitation, shifting and mixing of rows and columns to the plain content.

II. PROPOSED DESIGN ARCHITECTURE

At the input side plain text of 128-bit is taken which is encrypted with a 128-bit key. The input consists of a clock signal, a start signal, a reset signal, s-box, a mix column block (mixco_done) and a key generator (keygen_done) block. After performing all the encryption process steps cipher text of 128-bit is observed at the output side. In the simulation, the 128-bit key is secured for all 10 streams of the Advanced Encryption Standard simulation.

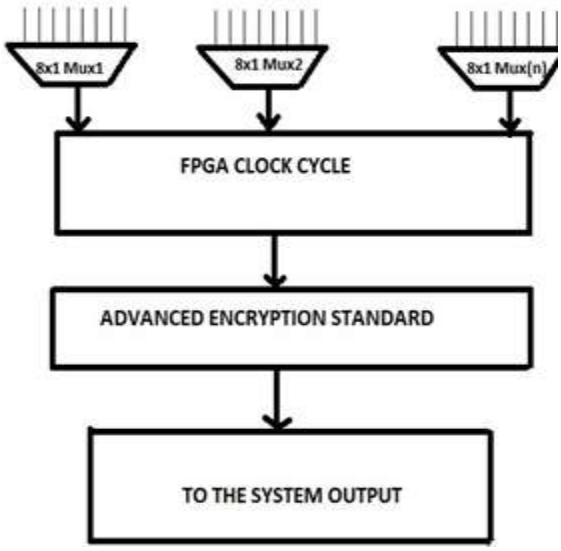

Fig. Modified FPGA architecture circuit for many cores in built systems

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 3, ISSN No. 2455-2143, Pages 179-182
Published Online July 2022 in IJEAST (http://www.ijeast.com)

Then implementing 1 to clock, start and, reset indications the 128-bit cipher text is scrutinized. The consumption of Slice Registers (SR) required more than 3987. The consumption of the number of Look Up Tables (LUTs) required are 4115. The consumption of the number of Input/Output (I/O) ports required are 269. The consumption of the number of Global Buffer (BUFG) required more.

Lack of security is available when number of Job Queues are switched on together. The Smallest Job count is neglected in the Priority when the Load balancer is added in the system. The consumption of cipher text is 128 keys only. The clock cycle is limited. The core in the implementation is limited to 100 cores only. The architecture uses pipelining and parallel processing to reduce the time cycle.

III. ADVANCED ENCRYPTION STANDARD

Encryption is the process of encoding messages (or information) in such a way that third parties cannot read it, but only authorized parties can.

Encryption never prohibits hacking but disallows the cyberpunk goes through the encrypted information. In an **Encryption origination**, whether the report or data that is encrypted utilizing an encryption algorithm, converting with indecipherable **CIPHER TEXT**. This is usually done with the use of an **Encryption** Key, which specifies how the message is to be **BLOCKED**.

CIPHER- TEXT

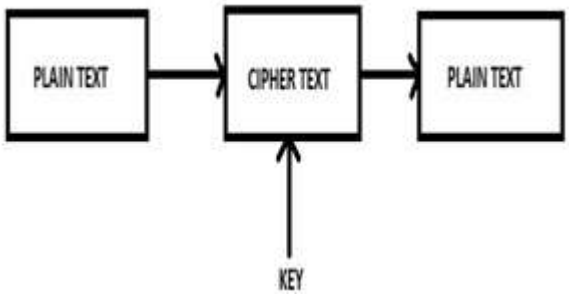

Fig. Cipher Text

Most of the cryptography involves very advanced Mathematical functions used for securing data. The sole purpose of the algorithms developed for cryptography is to hide data from the attacker or middleman. In this article, we will understand the concept in cryptography named symmetric encryption.

The cryptographic terms are:

- **Plain text:** The plain text is an innovative information or data is concealed and none can go through it through a cryptographic encryption algorithm.
- **Cipher text:** It is the output of Cryptographed function after implementing key and plain context. This information must be implemented in deciphered operation.
- **Key:** The key is small quantity of information or interconnected coupling information after implementing input with plain co-text into cryptographed operation results in cipher-content. The key is encrypted and the architecture is brazened to everyone.

IV. SUB-BYTES TRANSFORMATION

The three variants of AES are based on different key sizes (128, 192, and 256 bits). This paper denotes the 128-bit version of the Advanced Encryption Standard key timeline, contributes the adequate environment comprehending the 192- and 256-bits.

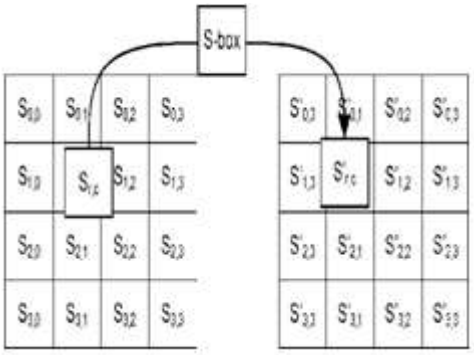

Fig. Sub-bytes transformation

At the end, we'll include a note the other variants, and how they differ from the 128-bit version.

A. SUB-BYTES

	0	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
40	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig. S-Box Table

The Sub-Bytes phase of AES involves splitting the input into bytes and passing each through a Substitution Box or S-Box.

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 3, ISSN No. 2455-2143, Pages 179-182
Published Online July 2022 in IJEAST (http://www.ijeast.com)

Unlike Data Encryption Standard, Advanced Encryption Standard implement identical S-Box for all datas.
From the above Table, the data input is broken into two 4-bit semi slots. The initial semi slot denotes the row and the second semi slot denotes the column.
For example, the S-Box transformation of 35 or 0x23 can be found in the cell at the intersection of the row labelled 20 and the column labelled 03. Since decimated value 35 becomes 0x26 or decimation 38.

B. SHIFT-ROWS

In the Shift-Rows phase of AES, each row of the 128-bit internal state of the cipher is shifted. Currently, the rows spotlight the conventional modeling of the inward position in Advanced Encryption Standard, denoted 4x4 matrix in every slot consists of a data. Inward position of the datas are secured in the matrix straddling rows from left to right and down columns.
In the Shift-Rows operation, each of these rows is shifted to the left by a set amount: their row number starting with zero. The upper row is stabilized, moreover, another row is evolved by one after another.

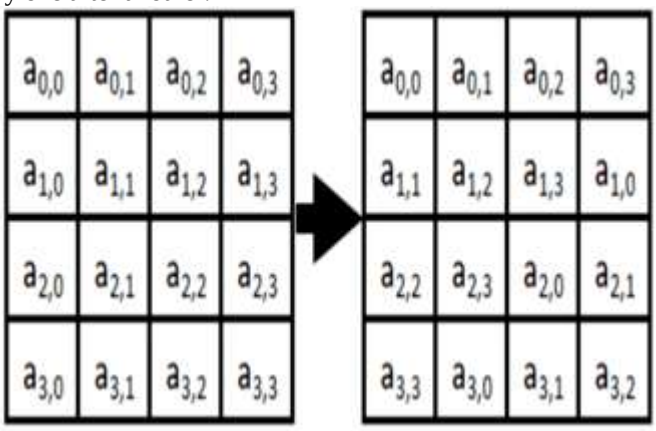

Fig. Shift rows Operation

In the Figure, the first number in each cell refers to the row number and the second refers to the column. The initial upper row (row 0) is stabilized, row 1 shifts left by one, and so on.

C. MIX-COLUMNS

Like the Shift-Rows phase of AES, the Mix-Columns phase provides diffusion by mixing the input around. Unlike Shift-Rows, Mix-Columns performs operations splitting the matrix by columns instead of rows.

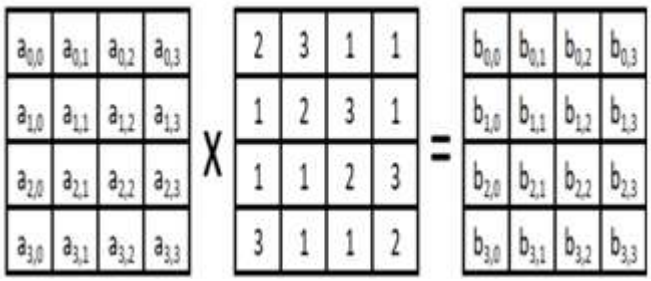

Fig. Mix columns operation

A visual representation of the Mix-Columns operation is shown above. The multiplication has the characteristic of working autonomously in every column of pioneer matrix, i.e., when the first column is multiplied by the matrix, triggers the first column of output matrix.

D. INVERSE- S BOX

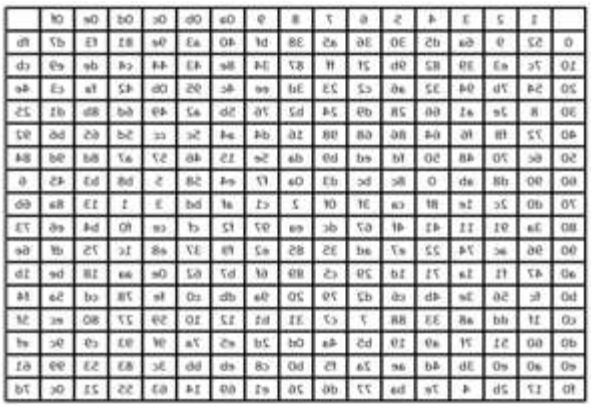

Fig. Inverse S-box

This was done by minimizing the correlation between linear transformations of input/output bits with the time latency. To strengthen S-box from algebraic attacks the affine transformation was added.

V. CONCLUSION

Thus, the modeling of innovative encrypted algorithm on FPGA in many core architectures is performed with concurrent operations through pipelining with secured manner. However, the data is encrypted and the FPGA clock cycle reduces the latency in every pipelined operation.

VI. REFERENCE

[1]. Ahmed, W.E. (2019) On Rijndael Byte-Sub Transformation. Applied Mathematics, 10, 113-118. https://doi.org/10.4236/am.2019.103010.

[2]. Gérault, D.; Lafourcade, P.; Minier, M.; Solnon, C. Revisiting AES related key differential attacks with constraint programming. Inf. Process. Lett. **2018**, 139, 24–29.

[3]. Zodpe, H.; Sapkal, A. An Efficient AES Implementation using FPGA with Enhanced Security Features. J. King

Saud Univ. Eng. Sci. **2018**, in press.

[4]. Gamido, H.V.; Sison, A.M.; Medina, R.P. Implementation of Modified AES as Image Encryption Scheme. Indones. J. Electr. Eng. Inform. (IJEEI) **2018**, 6, 301–308.

[5]. Saha, R.; Geetha, G.; Kumar, G.; Kim, T.-H. RK-AES: An Improved Version of AES Using a New Key Generation Process with Random Keys. Secur. Commun. Netw. **2018**, 2018, 1–11.

[6]. Reyes, E.M.D.L. Modified AES Cipher Round and Key Schedule. In Proceedings of the 2018 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), Bangkok, Thailand, 21–24 October 2018.

[7]. Chowdhury, A.R.; Mahmud, J.; Raihan, A.; Kamal, M.; Hamid, A. MAES: Modified Advanced Encryption Standard for Resource Constraint Environments.In Proceedings of the IEEE Sensors Applications Symposium (SAS), Seoul, Korea, 12–14 March 2018; pp. 2–7.

[8]. Amit Kumar, Manoj kumar, P. Balramudu (2017), "Implementation of AES algorithm using VHDL", IEEE 978-1-5090-4890- 8/17.

[9]. Soufiane Oukili, Seddik Bri (2017), "High speed efficient Advanced Encryption Standard implementation", IEEE 978-1- 5090-4260-9/17.