

SECURITY ENHANCEMENT OF INFORMATION USING MULTILAYERED CRYPTOGRAPHIC ALGORITHM

¹B.SATYA TULASI, ²P.VANI

¹M.TECH VLSI&ES, DEPT OF E.C.E, KAKINADA INSTITUTE OF ENGINEERING AND
TECHNOLOGY FOR WOMEN,KORANGI,ANDHRAPRADESH,INDIA,533461

²ASSISTANT PROFESSOR, KAKINADA INSTITUTE OF ENGINEERING AND TECHNOLOGY
FOR WOMEN,KORANGI,ANDHRAPRADESH,INDIA,533461

ABSTRACT:

The data which is being communicated can be protected in different ways. For securing sensitive data in various industries Modified Advanced Encryption Standard (MAES) is used. To address issues, an automated key generation, power reduction, optimization of hardware resources techniques and mathematically less operation involved methods are proposed and analyzed in this work by employing modified substitution box algorithms for more security in present communication systems. The new S-box is developed by using the galois field using the affine transformation properties. By using this S-box, the pipelining mechanism was applied to the various stages of MAES. The pipelining mechanism effectively applied to the mix-columns, shift rows and key expansion modules respectively. As these blocks run parallel, it will reduces the time consumption for encryption process, the reduction in time causes to effectively reduces the power consumption for MAES system. The experiments conducted using Xilinx is environment, the simulation results shows that the proposed method consumes lows hardware recourse utilization as well as power reduction compared to the conventional approaches.

Keywords: MAES, AES, Xilinx, cryptography .

1. INTRODUCTION

AES is short for Advanced Encryption Standard and is a United

States encryption standard defined in Federal Information Processing Standard (FIPS) 192, published in

November 2001. It was ratified as a federal standard in May 2002. AES is the most recent of the four current algorithms approved for federal use in the United States. One should not compare AES with RSA, another standard algorithm, as RSA is a different category of algorithm. Bulk encryption of information itself is seldom performed with RSA. RSA is used to transfer other encryption keys for use by AES for example, and for digital signatures. AES is a symmetric encryption algorithm processing data in block of 128 bits. A bit can take the values zero and one, in effect a binary digit with two possible values as opposed to decimal digits, which can take one of 10 values. Under the influence of a key, a 128-bit block is encrypted by transforming it in a unique way into a new block of the same size. AES is symmetric since the same key is used for encryption and the reverse transformation, decryption. The only secret necessary to keep for security is the key. AES may be configured to use different key-lengths, the

standard defines 3 lengths and the resulting algorithms are named AES-128, AES-192 and AES-256 respectively to indicate the length in bits of the key. Each additional bit in the key effectively doubles the strength of the algorithm, when defined as the time necessary for an attacker to stage a brute force attack, i.e. an exhaustive search of all possible key combinations in order to find the right one

Some background on AES In 1997 the US National Institute of Standards and Technology put out a call for candidates for a replacement for the ageing Data Encryption Standard, DES. 15 candidates were accepted for further consideration, and after a fully public process and three open international conferences, the number of candidates was reduced to five. In February 2001, the final candidate was announced and comments were solicited. 21 organizations and individuals submitted comments. None had any reservations about the suggested algorithm. AES is founded on solid

and well-published mathematical ground, and appears to resist all known attacks well. There's a strong indication that in fact no back-door or known weakness exists since it has been published for a long time, has been the subject of intense scrutiny by researchers all over the world, and such enormous amounts of economic value and information is already successfully protected by AES. There are no unknown factors in its design, and it was developed by Belgian researchers in Belgium therefore voiding the conspiracy theories sometimes voiced concerning an encryption standard developed by a United States government agency. A strong encryption algorithm need only meet only single main criteria:

- There must be no way to find the unencrypted clear text if the key is unknown, except brute force, i.e. to try all possible keys until the right one is found.

A secondary criterion must also be met:

- The number of possible keys must be so large that it is computationally infeasible to actually stage a successful brute force attack in short enough a time.

The older standard, DES or Data Encryption Standard, meets the first criterion, but no longer the secondary one – computer speeds have caught up with it, or soon will.

2. RELATED STUDY

In the SubBytes step, each byte in the matrix is updated using an 8-bit substitution box, the Rijndael S-box. This operation provides the non-linearity in the cipher. The S-box used is derived from the multiplicative inverse over $\text{GF}(2^8)$, known to have good non-linearity properties. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation. The S-box is also chosen The S-box is also chosen to avoid any fixed points

(and so is a derangement), and also any opposite fixed points.

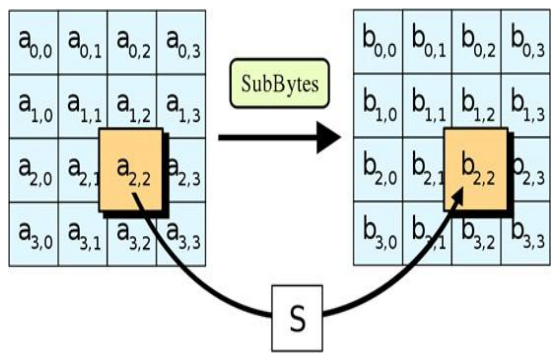


Fig.2.1. Sub-byte models.

The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. For the block of size 128 bits and 192 bits the shifting pattern is the same. In this way, each column of the output state of the ShiftRows step is composed of bytes from each column of the input state. (Rijndael variants with a larger block size have slightly different offsets). In the case of the 256-bit block, the first row is unchanged and the shifting for second, third and fourth row is 1 byte, 3 bytes and 4

bytes respectively—this change only applies for the Rijndael cipher when used with a 256-bit block, as AES does not use 256-bit blocks.

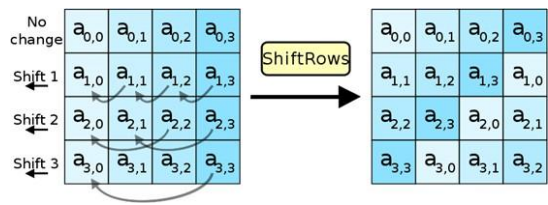


Fig.2.2.shift rows.

3. AN OVERVIEW OF PROPOSED SYSTEM

The usage of semiconductor devices has rapidly increased. Integrated Circuit (IC) has become the foremost part of every stream like military, government, commercialization, etc. Chip manufacturing cycle involves Specification, Architectural design, Functional and Logical design, Circuit design, Physical design, Fabrication, Packaging and Testing. Due to long supply chain, the manufacturing of an IC at one place was difficult and demands a large capital investment. So, fabrication of an IC is done at different places and monitoring such long process, the products are likely to be modified or inserted a malicious circuit into the

design by the attackers. Hardware Trojans [HTs] are malicious modification or insertion of harmful circuit into existing design. HTs can be implanted in security weaker parts of IC to disturb the original functionality of the circuit. Hardware Trojans can leak the secure information (Data leakers) or disturb the regular flow of the circuit (behaviour modifiers) or destroy the device or system's hardware or degrade the operation (reliability Impacts) [5]. HTs are small in size and activated by rare events. As the foot print for a Trojan may be very small, it becomes hard to verify or test for Trojan in circuit. Especially when there is no Trojan free reference available to compare against. Several methods are proposed to detect HTs, still it become an issue in IC security. Cryptography is used for protect data from attempt theft, theft or unauthorised use of data. Cryptographic chips are used for protecting Military secrets, Business

Data, and other high security fields, requires most secured chips.

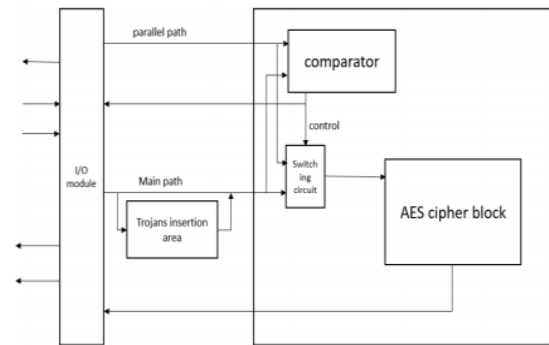


Fig.3.1. Block Diagram of Multipath Authentication model for AES crypto processor.

In proposed model there are two paths, main path and parallel path. Trojans are inserted in free area (alongside of data path) and are activated in rare conditions based on triggering signal (input data) to modify the data to produce malicious results. The authentication system comprises of both comparator and switching network. Any modifications happened to the data by the Trojans is observed by the comparator, which compares the main path data with entered input data through the parallel path. The output of the comparator gives as a status signal for the intimation of Trojan detection

and drives the control input of the switching circuit. The changes of main path data is observed, the comparator generates negative signal to the switch control for data change. The switch circuit terminates main path signals and connects parallel path signals to AES cipher, so the original results are achieved even though Trojan is activated.

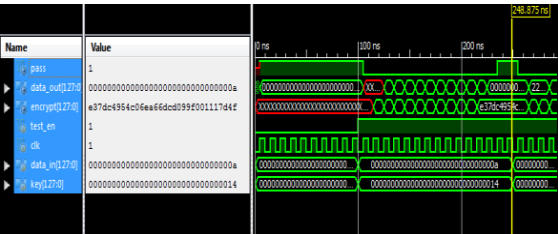


Fig.4.1. simulation output

Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slice Registers	1244	35200	3%
Number of Slice LUTs	19329	17600	109%
Number of fully used LUT-FF pairs	1033	19540	5%
Number of bonded IOBs	514	100	514%
Number of Block RAM/FIFO	21	60	35%
Number of BUFG/BUFGCTRLs	1	32	3%

Fig.4.2. design summary

LUT6:I1->O	1	0.043	0.350	D1/p8/Mxor_b11_nxt_0_xo<0>_SW0_SW0 (N4994)
LUT6:I5->O	32	0.043	0.743	D1/p8/Mxor_b11_nxt_0_xo<0> (D1/b11b<0>)
LUT6:I0->O	1	0.043	0.000	D1/p9_q9/Mram_c23 (D1/p9_q9/Mram_c23)
MUXF7:I1->O	1	0.178	0.000	D1/p9_q9/Mram_c2_f7_0 (D1/p9_q9/Mram_c2_f71)
MUXF8:I0->O	2	0.128	0.355	D1/p9_q9/Mram_c2_f8 (D1/p9/b12_sb<1>)
LUT5:I4->O	6	0.043	0.523	D1/p9/Mxor_b12_ak_1_xo<0>1 (D1/p9/b12_ak<1>)
LUT5:I0->O	4	0.043	0.422	D1/p9/Mmux_b12_ak[6]_b12_ak[6]_mux_419_OUT51 (D1
LUT6:I4->O	1	0.043	0.350	D1/p9/Mxor_b22_nxt_4_xo<0>_SW0_SW0 (N5974)
LUT6:I5->O	32	0.043	0.480	D1/p9/Mxor_b22_nxt_4_xo<0> (D1/b22i<4>)
LUT6:I1->O	1	0.043	0.000	D1/p10_q2/Mram_c3 (D1/p10_q2/Mram_c2)
MUXF7:I1->O	1	0.178	0.000	D1/p10_q2/Mram_c_f7_0 (D1/p10_q2/Mram_c_f71)
MUXF8:I0->O	1	0.128	0.350	D1/p10_q2/Mram_c_f8 (D1/p10/b20_sb<0>)
LUT2:I1->O	1	0.043	0.000	D1/p10/Mxor_m3_0_xo<0>1 (temp<104>)
FDR:D		-0.000		data_out_104

Total		38.635ns	(9.731ns logic, 28.904ns route)	
			(25.2% logic, 74.8% route)	

Fig.4.3. Time summary

Rijndael algorithm consists of encryption, decryption and key schedule algorithm. The main operations of the encryption algorithm among the three parts of Rijndael algorithm include: bytes substitution (SubBytes), the row shift (ShiftRows), column mixing (MixColumns), and the round key adding (AddRoundKey).

EXTENSION RESULTS

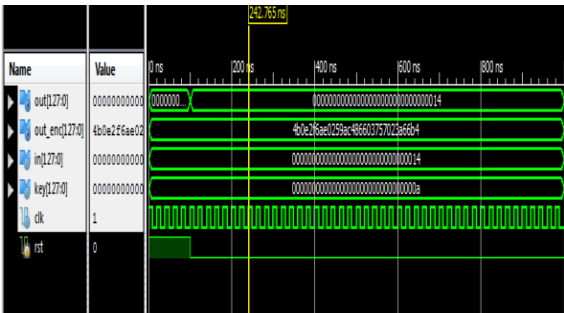


Fig.4.4.simulation output

Device Utilization Summary (estimated values)				
Logic Utilization	Used	Available	Utilization	
Number of Slice LUTs	8648	17600		49%
Number of fully used LUT-FF pairs	0	8648		0%
Number of bonded IOBs	514	100		514%
Number of BUFG/BUFGCTRLs	1	32		3%

Fig.4.5. design summary

LUT6:I0->O	1	0.043	0.350	e1/r1/r5/m3/m6/Mxor_b<3>_xo<0>1 (e
LUT5:I4->O	4	0.043	0.630	e1/r1/r5/Mxor_roundout_88_xo<0>1 (
LUT6:I0->O	5	0.043	0.626	e1/r1/r6/m1/s6/s1/Mxor_out_temp<3>
LUT6:I1->O	1	0.043	0.350	e1/r1/r6/m3/m4/Mxor_b<3>_xo<0>1 (e
LUT6:I5->O	4	0.043	0.630	e1/r1/r6/Mxor_roundout_99_xo<0>1 (
LUT6:I0->O	5	0.043	0.636	e1/r1/r7/m1/s4/s1/Mxor_out_temp<3>
LUT6:I0->O	1	0.043	0.350	e1/r1/r7/m3/m6/Mxor_b<3>_xo<0>1 (e
LUT6:I4->O	4	0.043	0.630	e1/r1/r7/Mxor_roundout_88_xo<0>1 (
LUT6:I0->O	5	0.043	0.626	e1/r1/r8/m1/s6/s1/Mxor_out_temp<3>
LUT6:I1->O	1	0.043	0.350	e1/r1/r8/m3/m4/Mxor_b<3>_xo<0>1 (e
LUT6:I5->O	4	0.043	0.630	e1/r1/r8/Mxor_roundout_99_xo<0>1 (
LUT6:I0->O	5	0.043	0.636	e1/r1/r9/m1/s4/s1/Mxor_out_temp<3>
LUT6:I0->O	1	0.043	0.350	e1/r1/r9/m3/m5/Mxor_b<3>_xo<0>1 (e
LUT3:I2->O	7	0.043	0.556	e1/r1/r9/Mxor_roundout_91_xo<0>1 (
LUT6:I2->O	5	0.043	0.362	e1/r1/r10/Mxor_roundout_91_xo<0>1
obuf:I->O		0.000		out_enc_91_obuf (out_enc<91>)

Total		17.309ns	(1.290ns logic, 16.019ns route)	
			(7.5% logic, 92.5% route)	

Fig.4.6. Time summary.

parameter	proposed	extension
Simulation output	After 10 cycles	After 1 cycle due to pipelining
Slice LUTs	19329	8648
Area utilization	109%	49%
Time consumed	36.6ns	17.3ns

4. CONCLUSION

A FPGA implementation of area-optimized AES algorithm which meets the actual application is proposed in this paper. After being coded with Verilog Hardware Description Language, the waveform simulation of the new algorithm was taken in platform. Ultimately, a synthesis simulation of the new algorithm has been done. The result shows that the design with the pipelining technology and special data transmission mode can optimize the chip area effectively. Meanwhile, this design reduces power consumption to some extent, for the

power consumption is directly related to the chip area. Therefore the encryption device implemented in this method can meet some practical applications. As the S-box is implemented by look-up-table in this design, the chip area and power can still be optimized. So the future work should focus on the implementation mode of S-box. Mathematics in Galois field (28) can accomplish the bytes substitution of the AES algorithm, which could be another idea of further research. In this paper, we present a modified version of AES for Resource-Constraint Environments. A new Substitution Box is proposed which works over the Galois Field (24) by constructing an unique affine transformation equation. One notable feature of MAES is extending the battery life of low powered devices by consuming less amount of energy. The proposed method shows 18.35% efficiency when encrypted packets are transmitted using the proposed MAES to the sink node and the number of transmitted packets has

increased. In addition, 29.983 milliseconds is found in terms of latency. In future, the security issue and space complexity will be considered to make the proposed modification more applicable. Also, we plan to investigate multipath routing scheme while transmitting the encrypted data to the sink node. We will further delve to integrate Public Key Cryptosystem, specially Elliptic-curve cryptography (ECC) to achieve comparable efficiency in terms of number of packet transmission and latency with better security.

REFERENCES

- [1] Madakam, Somayya, R. Ramaswamy, and Siddharth Tripathi. "Internet of Things (IoT): A literature review." *Journal of Computer and Communications* 3, no. 05 (2015): p.164.
- [2] Wang, Yong, Garhan Attiebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." *IEEE Communications Surveys Tutorial* (2006).
- [3] Veeramallu, B., S. Sahitya, and Ch LavanyaSusanna. Veeramallu, B., S. Sahitya, and Ch LavanyaSusanna. "Confidentiality in Wireless sensor Networks." *International Journal of Soft Computing and Engineering (IJSCE)* ISSN: 2231-2307, Volume-2, Issue-6, January 2013.
- [4] Eisenbarth, Thomas, and Sandeep Kumar. "A survey of lightweight cryptography implementations." *IEEE Design & Test of Computers* 24.6 (2007).
- [5] Banik, Subhadeep, Andrey Bogdanov, and Francesco Regazzoni. "Exploring energy efficiency of lightweight block ciphers." *International Conference on Selected Areas in Cryptography*. Springer, Cham, 2015.
- [6] Bogdanov, Andrey, et al. "PRESENT: An ultra-lightweight block cipher." *CHES*. Vol. 4727. 2007.
- [7] Borghoff, Julia, et al. "PRINCEa low-latency block cipher for pervasive computing applications." *International Conference on the Theory and Application of*

Cryptology and Information Security. Springer, Berlin, Heidelberg, 2012.

[8] Beaulieu, Ray, et al. “The SIMON and SPECK lightweight block ciphers.” Design Automation Conference (DAC), 52nd ACM/EDAC/IEEE. IEEE, 2015.

[9] Suzaki, Tomoyasu, et al. “TWINE: A Lightweight Block Cipher for Multiple Platforms.” Selected Areas in Cryptography. Vol. 7707. 2012.