International Journal of Electronics Engineering (ISSN: 0973-7383
Volume 11 • Issue 1 pp. 263-268 Jan 2019-June 2019 www.csjournals.com

Survey on AES and Whirlpool Cryptographic Architectures

[1]Vignesh. O, [2]Rajakumari.V, [3]Divya. A
[1]Teaching Fellow, [2]PG Scholar, [3]Assistant Professor
Department of Electronics Engineering, MIT Campus, Anna University, Chennai, India

Abstract: In recent years the need for the effective and secure communications in both wired and wireless networks is becoming important. Cryptography provides a method for securing and authenticating the transmission of information over insecure channels. Advanced Encryption Standard (AES) is commonly known as the standard for symmetric key encryption. Hash functions are used as major blocks in numerous cryptographic applications. Many hardware based implementations of Encryption and Hash functions have been proposed on separate architecture. This paper presents literature study of various AES Encryption and Whirlpool Hash function architectures**.** It is also recommended that AES and Whirlpool have a similar structure of the operation. So this Encryption and Hash function can be combined into a single dynamically reconfigurable cryptographic architecture which requires less area and power than that of separate Encryption and Hash Function.
Keywords: Advanced Encryption Standard (AES), Rijndael algorithm, Symmetric key Encryption, Whirlpool Hash.

1. Introduction

With the arrival of high speed and easily accessible computers, there has been an increase in demand for effective methods to protect data despite what processing power an adversary may possess. [8] Some of the ancient cryptographic methods, such as DES, does not have a large enough key space to lend themselves to applications where high security is needed. To overcome this situation, A design proposed by Joan Daemon and Vincent Rijman, was the method that was selected, which they called Rijndael.
The Rijndael algorithm, which is known as the Advanced Encryption Standard (AES).It provides a symmetric key cryptography that allows for the encryption and decryption of fixed size(128 bit)blocks of data [11,12]. As a symmetric system, in order for communication to be possible, the secret key must be shared between the sender and receiver.

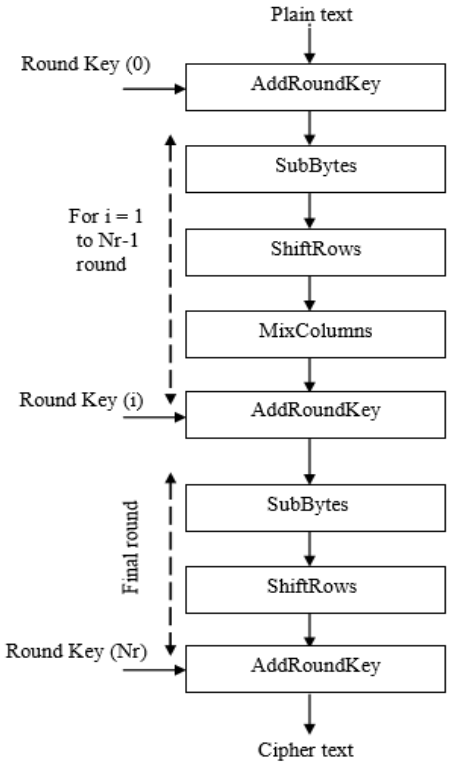

Figure 1. Block diagram of AES algorithm

The Rijndael algorithm was implemented using a 128-bit plaintext data and 128-bit key which produces 128-bit ciphertext [21]. It operates on the 128-bit data in 10 rounds [20]. Each round consisting of several

mathematic operations designed to obscure the data., a key expansion algorithm is used, in order to accommodate the several rounds using a single 128-bit key [22]. The major four steps involved in each round of encryption are as follows:

1. ShiftRow
2. Subbyte
3. MixColumns
4. AddRoundKey

The present value for the system is stored in the system state throughout the steps of encryption [25]. The system state begins with the contents of the plaintext of 128-bit variable, and ends with the ciphertext contents .One round of encryption operation is shown in Fig.1.

[3,1]The Whirlpool Hash Algorithm is a 512-bit hash function designed by Vincent Rijmen and Paulo S.L.M. Barreto. It employs a symmetric key block cipher based on AES, which is known as the Whirlpool Cipher. The Whirlpool uses block cipher for the compression function. The block cipher W shown in Fig.2 will perform the operation same as that of AES. Whirlpool hash function produces Variable length of inputs into fixed length of irreversible output [5].

The encryption algorithm involves the use of four different functions, or transformations which are used in each round are:

1. Shift Columns (SC)
2. Substitute Bytes (SB)
3. Mix Rows (MR)
4. Add Key Round (AK)

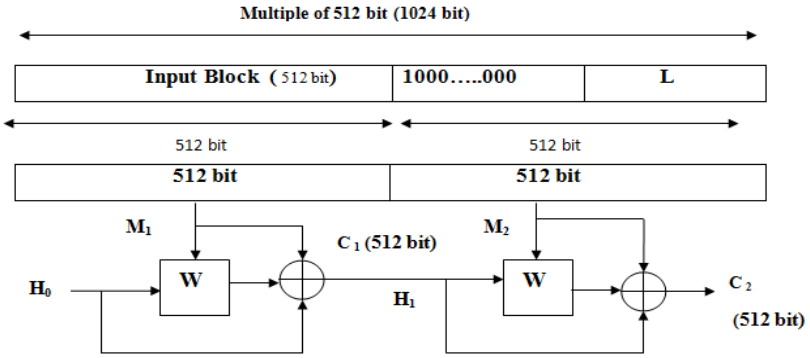

Figure. 2. Structure of whirlpool Hash function

2. Subbyte Transformation

In Subbyte transformation step the 16 input bytes are substituted by looking up a fixed table (S-box)[10,24]. The result is in a matrix of four rows and four columns for AES (128 bit) and eight rows and eight columns for Whirlpool Hash (512 bit). The S-box table varies for both AES and Whirlpool, but the implementation is same. Various architectures are available to implement S-box. Some of them are mentioned below.

2.1. Parallel S-Box

In Subbyte implementation, (16 x 16) S-box are used and these S-box involves the largest computation complexity in AES encryption process [19,16]. By applying pipelining and parallel processing technique higher throughput can be achieved in S-box. However it is difficult to apply the pipelining technique in LUT based S-box. So higher throughput can be achieved using parallel processing technique in S-box. In Subbytes round Each byte in State is replaced by the element in S-box LUT. In order to increase thethroughput sixteen S-box are divided in to eight groups. Each group consists of two bytes. All the eight groups are processed in parallel. Thereby effective execution delay of the Subbyte transformation round is decreased. Hence, the overall throughput of AES is increased.

International Journal of Electronics Engineering (ISSN: 0973-7383
Volume 11 • Issue 1 pp. 263-268 Jan 2019-June 2019 www.csjournals.com

2.2. DSE S-box

The idea is to use an onehot decoder to convert S-box inputs into onehot representation is shown in Fig.3 [17].The wire permutations are done as a nonlinear operations in lightweight cryptography algorithms. After that, the S-box output in onehot encoding is converted back into the original. it minimizes the activity inside the S-box circuit. So, DSE S-Box can reduce the power consumption. After decoding state, only one signal changes its value to go to the encoding state. The most of the Area is reduced because of the size of encoder and decoder circuits.

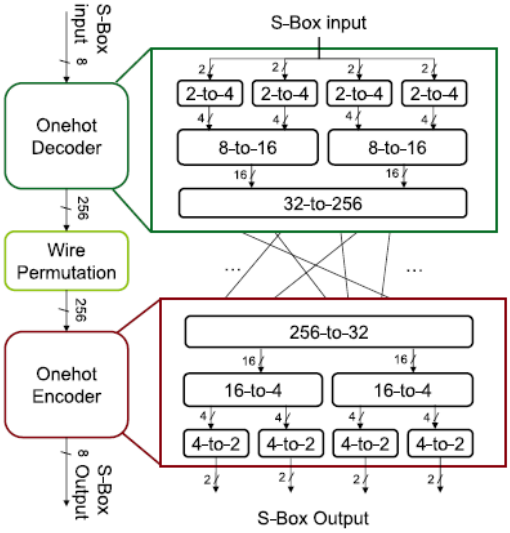

Figure 3. Structure of DSE S-box

3. Shift Row/Column

The Shift Rows step operation is the rows of the state in AES encryption. It cyclically shifts the bytes in each row by a certain manner. For AES, the first row remains constant. Each byte of the second row is shifted by one to the left [18]. Similarly, the third rows are shifted by two and fourth rows are shifted by three. For blocks of sizes 128 bits and 192 bits, the shifting pattern is the same. Row m is shifted circular left by m-1 bytes. In this way, each column of the output state of the Shift Rows step is composed of bytes from each column of the input state [8].

For Whirlpool the block size is 512 bits .Here the Shift operation is done in column wise. The shift column is done by downward circular shift of each column of State matrix except the first column. A one byte downward circular shift is performed for the second column. A two byte downward circular shift is performed for the third column and so on.

4. Mix Column/Row

In AES each column of bytes are transformed using a special mathematical function [8,2]. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another matrix consisting of new bytes. This step is not performed in the last round.
Whereas in Whirlpool hash function mix rows achieves diffusion within each row individually. Each byte of a row is mapped into a new value that is a function of all eight bytes in that row. This step also performed in the last round unlike AES.

4.1. Eight stage Parallel Mix Column

In AES encryption process within a single loop, Mix Column transformation produces 60% of execution delay[19]. So, throughput of the AES Encryption can be increased by introducing the parallelism in Mix Column transformation. Sixteen 2 bytes MixColumn-16 can be replaced by eight 2 bytes. At a time each MixColumns-2 processes only 2 bytes than processing a whole data block. So eight stages of MixColumn-2

are used in parallel to do the computation. As a result, Parallel Mix Column implementation increases throughput. In Mix Column the matrix multiplication is done. In 8 stage parallel Mix Column all the 128-bit data are seperated in to 8 groups. All the 8 group has two bytes and all the bytes are computed as parallel.

5. Key Expansion

The 16 bytes of the matrix are considered as 128 bits of plain text and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round [8].

5.1 AES Key Schedule Using Look-Ahead Technique

The initial 128-bit key is considered as four 32 bit words W0, W1, W2 and W3. An iterative algorithm computes the remaining 40 words each of length 32-bits using the following algorithm for ten rounds.

$$W4k = RW(W'4k-1) \oplus RC \oplus W4k-4 \quad (1.1)$$
$$W4k+1 = W4k \oplus W4k-3 \quad (1.2)$$
$$W4k+2 = W4k+1 \oplus W4k-2 \quad (1.3)$$
$$W4k+3 = W4k+2 \oplus W4k-1 \quad (1.4)$$

In this Section, the proposed approach for generation of round keys for decryption is given [13]. Consider the first four rounds (k = 1,…,4) for which, using conventional approach, from (1.1)–(1.4),after simplification (for k = 1,…,3)

$$W7 = RW(W3) \oplus A1 \quad (2.1)$$
$$W11 = RW(W7) \oplus A2 \quad (2.2)$$
$$W15 = RW(W11) \oplus A3 \quad (2.3)$$

Where,

$$A1 = RC1 \oplus A1 \quad (3.1)$$
$$A2 = RC2 \oplus A2 \quad (3.2)$$
$$A3 = RC3 \oplus A3 \quad (3.3)$$

Note that A1= W0 ⊕ W1 ⊕ W2 ⊕ W3, A2= W1 ⊕ W3, A3= W2 ⊕ W3
Following in a similar manner, for the remaining rounds k= 4–10, W19, W23,...,W43 can be calculated using the general expression

$$W4k+3 = RW(W4k-1) \oplus Ak \quad (4)$$
$$Ak = RC \oplus Ak' \quad (5)$$
$$Ak' = W4k-13 \text{ for } k = 4 \ldots 10 \quad (6)$$

Thus, the words W7, W11,W15, ...,W43 can be obtained from the given 128-bit keyW0, W1, W2 and W3 using (2)–(6) without needing to compute all the intermediate words. Further, Ak as needed in (2.1)–(2.3) and (5) for k = 1,…, 10 can be computed in parallel with the SBox look-up (used to obtain W4k−1 from W4k−1) so that the critical path for each of these ten steps is SBox+XOR. The word W4k+2for k = 1–10 from the already available words W4k−1 and W4k+3 can be computed as follows:

$$W4k+2 = W4k+3 \oplus W4k-1 \quad (7)$$

The words W4k and W4k+1 can be obtained using (1.1) and (1.2) respectively. It can be seen that W4k can be obtained after one EXOR delay after RW (RotWord) (W4k−1)is available since W4k−4⊕RC can be computed beforehand. Thus, W4k and W4k+3 are availablesimultaneously.Next,W4k+2 andW4k+1 can be obtained after one EXOR operation as given by (7) and (1.2). This, however, can take place concurrently with the first stage execution of next round key computation unit. Thus, all the round keys are available after a delay of 10(S−BOX + XOR) + XOR.

6. Comparison of AES and Whirlpool

The comparison of both AES and Whirlpool hash function is shown in Table 1.

Table 1: Comparison of AES and Whirlpool Hash

	WHRLPOOL	**AES**
Block size(bits)	512	128
Key size(bits)	512	128,192,256
Matrix structure	Row based mapping	Column based mapping
No. of Rounds	10	10
Key Expansion	Same as W round function	Dedicated Key expansion algorithm
SBox	Recursive structure	Multiplicative inverse in GF(28) + affine transformation
Shift Operation	Column wise shift	Row wise Shift
Mix Operation	Right multiplication by 8×8 circulant matrix	Left multiplication by 4×4 circulant matrix
Addround constant	Successive entries of the S-box for 10 rounds	32 bit round constant for ten rounds

From the above analysis, it is observed that Key Expansion is same for both AES Encryption and Whirlpool Hash function whereas the other blocks in Whirlpool differ slightly from that of AES as mentioned below [6]. Subbyte Transformation step is similar for both AES and Whirlpool except that of (16 X 16) S-box values stored in the LUT will vary [4].

- Shift operation in AES takes place row wise whereas in Whirlpool it is done in column manner.
- Mix column step in AES multiplies the input with constant matrix ([I] × [C]), but in Whirlpool constant matrix is multiplied with the input ([C] × [I]) and hence it is termed as Mix row. Constant Matrix also different for both AES and Whirlpool.

7. Conclusion

In this article various AES and Whirlpool architectures are analyzed and observed that both have similar operation. So, they can be combined for security applications which require the use of both Encryption and Hash function**.** The combined architecture of AES encryption and whirlpool hash function requires less area and power compared to the individual architecture of AES and Whirlpool hash algorithm.

References

[1] P. Kitsos and O. Koufopavlou,"whirlpool hash function: architecture and VLSI implementation", Conference:Circuits and Systems (ISCAS) Proceedings of the International Symposium on,vol. 2,2004.
[2] Xinmiao Zhang, and Keshab K. Parhi,"High-Speed VLSI Architectures for the AES Algorithm", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 12, no. 9,pp. 957-967, 2004.
[3] William Stallings, "The Whirlpool Secure Hash Function", Cryptologia,pp. 55-67,2006.
[4] Norbert Pramstaller, Christian Rechberger, and Vincent Rijmen,"A Compact FPGA Implementation of the Hash Function Whirlpool", Proceedings of the ACM/SIGDA 14th international symposium on Field programmable gate arrays,Pages159-166, 2006.
[5] Akashi Satoh,"ASIC Hardware Implementations for 512-bit Hash Function Whirlpool", IEEE International Symposium on Circuits and Systems,2008.
[6] Jianhua He , Hu Chen , Huaqiang Huang, "The Integrated Implementation of Whirlpool and AES on FPGA", Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics (PrimeAsia),2010.
[7] Bin Liu et al.,"A High-Performance Area-Efficient AES Cipher on a Many-Core Platform", Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR),2011.
[8] B.A. Forouzan and D. Mukhopadhyay, "Cryptography and Network Security", 2nd Ed.,Tata McGraw Hill, New Delhi,2012.
[9] Tuan Anh Pham et al., "Area and Power optimization for AES encryption module implementation on FPGA", Proceedings of the 18th International Conference on Automation & Computing, Loughborough University,Leicestershire, UK,2012.
[10] Ahmed Fathy Abd Elfatah et.al.,"Optimized Hardware Implementation of the Advanced Encryption Standard Algorithm",8th International Conference on Computer Engineering & Systems (ICCES), 2013.

[11] Ali A. Abed et al., "FPGA Implementation of a Modified Advanced Encryption Standard Algorithm", The First International Conference of Electrical, Communication, Computer, Power and Control Engineering ICECCPCE,2013.
[12] J.Balamurugan et al,"High Speed Low Cost Implementation of Advanced Encryption Standard on FPGA", 2nd International Conference on Current Trends in Engineering and Technology, ICCTET,2014.
[13] Rashmi R. Rachh , P. V. Ananda Mohan, B. S. Anami , "Implementation of AES Key Schedule Using Look-Ahead Technique", Circuits System Signal Process,Springer,vol.33, pp.3663–3670,2014.
[14] H.Mangalam et al., "Power efficient and high performance VLSI architecturefor AES algorithm", Journal of Electrical Systems and Information Technology,pp. 178–183,2015.
[15] Qihui Zhang,Jian Cao,Dunshan Yu, Xixin Cao,Xing Zhang,Yin Ye, Botao Chen , "A Low Energy High through-put Asynchronous AES for secure smart cards", IEEE International Conference on Electron Devices and Solid-State Circuits (EDSSC), pp. 487-490,2015.
[16] Shreenivas Pai.N et.al.,"Logic Optimization Of AES S- Box", International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) International Institute of Information Technology (I²IT), Pune,2016.
[17] Duy-Hieu Bui et al.,, "AES Datapath Optimization Strategies for Low-Power Low-Energy Multi security-Level Internet-of-Things Applications", IEEE transactions on very large scale integration systems,vol.25, no. 12,2017.
[18] Rizky Riyaldhia , Rojalia , Aditya Kurniawanb, "Improvement of advanced encryption standard algorithm with shift row and s.box modification mapping in mix column', 2nd International Conference on Computer Science and Computational Intelligence , ICCSCI,2017.
[19] S. Sridevi Sathya Priya , P. Karthigai Kumar,N. M. Sivamangai, V. Rejula, "High Throughput AES Algorithm Using Parallel Subbytes and MixColumn", Wireless Pers Commun,Springer, vol.95,pp.1433–1449,2017.
[20] Subhadeep Banik, Andrey Bogdanov, Francesco Regazzoni, "Compact circuits for combined AES encryption/decryption", J Cryptogr Eng, Springer,2017.
[21] V.-P. Hoang et.al.,"Design of ultra-low power AES encryption cores with silicon demonstration in SOTB CMOS process",ELECTRONICS LETTERS ,Vol. 53 No. 23 pp. 1512–1514,2017
[22] Vatchara_Saicheur_ Krerk Piromsopa, "An implementation of AES-128 and AES-512 on Apple mobile processor", 14th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON),2017.
[23] Sridevi Sathya Priya, Palanivel Karthigaikumar,N. M. Siva Mangai, P. Kirti Gaurav Das,"High Throughput AES Encryptor Using MUX Based Sub Pipelined S-Box", Wireless Pers Commun,Springer, vol.94, pp. 2259–2273,2017.
[24] Pon. Partheeban,V. Kavitha 2, "Dynamic key dependent AES S-box generation with optimized quality analysis", Cluster Computing,Springer,2018.
[25] T. Manojkumar , P. Karthigaikumar, Varatharajan Ramachandran,'An Optimized S-Box Circuit for High Speed AES Design with Enhanced PPRM Architecture to Secure Mammographic Images', Journal of Medical Systems,Springer,2019.