International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.3, 2015

REVIEW ARTICLE

ISSN: 2321-7758

LITERATURE ON ADVANCED ENCRYPTION STANDARD: A REVIEW

VINAY P. FIRAKE [1], Dr. A. M. PATIL[2]

[1]M. E. Student, [2]HoD Electronics and Telecommunication Dept., J. T. Mahajan College of Engg. Faizpur

Article Received: 30/04/2015

Article Revised on:06/05/2015

Article Accepted on:10/05/2015

ISSN:2321-7758
International Journal of Engineering Research-Online
A peer-reviewed, open access International scientific journal
www.ijoer.in

ABSTRACT

Advanced Encryption Standard (AES) is the mainly secure symmetric encryption method that has gained universal acceptance. The AES based on the Rijndael Algorithm is an resourceful cryptographic technique that includes age group of ciphers for encryption and inverse ciphers for decryption. Advanced security and speed of encryption/decryption is ensured by operations like Sub-Bytes (S-box)/Inv. Sub-Bytes (Inv. S-box), Mix-Columns/Inv. Mix-Columns and Key Scheduling. Extensive research has been conducted into development of S-box /Inv. S-Box and Mix-Columns/Inv. Mix-Columns on devoted ASIC and FPGA to speed up the AES algorithm and to decrease circuit area. This is an attempt, to survey in detail the work conducted in the abovementioned fields. The major centre of attention is on the FPGA implementations of optimized novel hardware architectures and algorithms.

Key Words—Advanced Encryption Standard (AES), FPGA, Block Cipher, Mix-column (MC), Inverse Mix-column (IMC), Su-bytes (S-Box), Inverse Sub-bytes (S-Box).

I. INTRODUCTION

With the development of Computer Network and Communication Technology, a great mass of data and information need to be exchanged by public communication networks. High efficiency and high safety of Data transmission become much more important. Communication and convey of data in the current days habitually necessitate the use of encryption. Above and beyond its uses in Military and Governments secret communication, Encryption is also used for shielding many kinds of national systems such as Internet e-commerce, Mobile networks, automatic teller machine transactions, copy protection (especially protection against reverse Engineering and Software piracy) and many more. Data encryption is achieved by subsequent a systematic algorithm called encryption algorithm[1], [5], [10]. An encryption algorithm provides secrecy, Authentication, Integrity and Non-repudiation. Secrecy is the necessity that information is kept secret from people who are not certified to access it. Certification is the sureness that the message indeed originates from the purported sender. Integrity is the requirement that information is unaltered and complete or that information is modified only by those users who have the right to do so. No repudiation means that the sender or receiver of a communication cannot reject having sent or received the message. National Institute of Standards and Technology (NIST) collected advanced encryption standard (AES) for efficient communication through public announcement [16]. Finally, the algorithm of Joan Daemen and Vincent Rijmen both are cryptographers in Belgium was selected as the standard for AES. The AES algorithm can resist any kinds of password attacks that all we have known with a strong practicability in information security and reliability. It has become the main information encryption algorithm now. The following presented review of an implementation of AES algorithm based on FPGA in order to speed data flow and reduce time for key generating. With the advent of new technologies in the field of FPGAs, they are increasingly preferred over ASICs. Advantages of FPGAs include the ability to re-program in the field to fix bugs[20], [21]. FPGA design flows support the use of third party EDA tools to perform design flow tasks such as static timing analysis, formal verification, and RTL and gate level simulation. Applications of FPGAs include digital signal processing, software defined radio, aerospace and defence systems, ASIC prototyping, medical imaging, computer vision, speech recognition, cryptography, bioinformatics, computer hardware emulation, radio astronomy, metal detection and a growing range of other areas.

This paper is organized as follows: Section 2 reviews the related works on FPGA. Section 3 discusses the performance summary and the conclusions arrived at in Section 4.

II. LITERATURE RELATED WORK UP TILL DATE

Considering the innumerable advantages of using a FPGA platform over others as can be noted, we have chosen to review AES implementations over FPGA exclusively. A new methodology for secret key block ciphers based on optimum number of pipeline stages has been proposed. The results of this work can be shown in table 1 of this paper for better understanding [1]. In this paper a novel high-speed non-pipelined architecture for implementing both encryption and decryption operations of the Rijndael algorithm on the same FPGA implementation has been proposed [2]. The results of this paper have been presented in table. A fully pipelined architecture for implementation of AES algorithm over FPGA has been presented in this paper [3]. A trade-off between cost and area has been achieved with a considerable reduction in area and improvement in throughput. A high-speed parallel pipelined architecture has been developed to build a hardware efficient design for the implementation of AES algorithm in this paper. It uses an efficient inter-round and intra-round pipeline design [4]. A Rijndael cipher for encryption using a basic 64-bit iterative architecture was developed and presented in this paper. The proposed architecture implemented on FPGA achieves high speed, low area and cost effectiveness[5]. Key scheduling unit has been added as a part of this work and the number of cycles required to encrypt text has been reduced and hardware optimization achieved. A hardware implementation of AES algorithm suitable for wireless military communication has been suggested in this work[6]. An optimized code was proposed for the Rijndael algorithm with 128-bit keys. A significant improvement in throughput and reduction of slices was achieved.

his paper proposes to combine both encryption and de-cryption on a single FPGA implementation with focus on low area and high throughput. The Rijndaels algorithm for 128-bit key is used on the fully pipelined AES encryptor /decryptor core proposed in this work [7]. In this work a 32-bit data path FPGA implementation of AES has been proposed. A significant improvement of 3.4 was achieved over the existing designs in terms of throughput [8]. This paper describes a FPGA implementation of Rijndael algorithm built using Reduced Residue of Prime Numbers or RRPN. The S-Box LUT entries form a set of Reduced Residue Prime Numbers which in turn forms a mathematical field. This makes the system resistant to algebraic attacks[9]. A high speed, non-pipelined FPGA implementation of AESCCMP has been proposed. Where in the CCMP consists of two modes, that is Counter mode for Data Privacy and CBC mode for authenticity [10]. Pipelining techniques have been used in the architectural optimization for the FPGA implementation of AES presented in this paper. Significant improvement in terms of speed has been achieved by processing multiple rounds simultaneously though cost in terms of area increased. Exclusion of Shift Row stage and on-the-fly key generation has been incorporated to enhance throughput[11]. FPGA implementation of AES algorithm has been presented in this paper. The encryption and decryption transformations have been performed using iterative design thus cutting hardware implementation costs. The result of this paper has been discussed in the Table 2 of this paper[12]. A high throughput design combining both encryption and decryption on a single FPGA architecture has been proposed in this paper. Low area and low cost was achieved [13]. In this paper hardware implementation of optimized area for block cipher AES has been proposed. Time sharing of resources and iteration architecture has been used to reduce the area [14]. This work proposes a new flexible AES architecture that performs both encryption and decryption. A key generation module that generates both encryption and decryption keys is provided. Flexibility is achieved so that key generation depends on the data and hence hardware need not be changed every time[15].

Efficiency and high throughput issues for FPGA implemen-tation of AESGCM have been addressed in this paper. Both the AES engine and the modular multiplication over G.F (2m) have been discussed. The Karatsubas algorithm has been used in the multiplication [16]. Designs achieving area, latency and bandwidth optimizations have been reviewed in this paper. A FPGA implementation of AES algorithm has been presented in this work incorporating these optimization techniques for better throughput and lower latency[17]. A new combinational logic to improve the efficiency of inner round pipelining has been developed in this paper. Composite field arithmetic reduced the area. A fully sub pipelined encrypter/decrypter with three sub stage pipelining per round has been used to achieve higher throughput[18]. Two new designs of FPGA implementation of AES algorithm, one achieving a very high throughput and the other with a very small area have been presented in this paper. The high throughput design supports continued throughput during key changes for both encryption and decryption processes[19]. FPGA implementation of AES algorithm presented in this paper use the content-addressable memory (CAM) based scheme to realize the high speed Sub-bytes block. The mix-columns block is implemented by the application of hardware sharing and the real time key generations are performed using a cost efficient Add Round Key architecture[20]. This paper uses a pipelined architecture only for the outer-round in the FPGA implementation of the AES algorithm. Very high throughput and efficiency are the merits of the proposed work[21]. A highly optimized, high performance efficient hardware realisation of the AES algorithm on FPGA has been proposed in this paper[22]. A throughput as high as 44.5Gbps has been achieved in the FPGA implementation of AES algorithm proposed in this paper. A fully pipelined architecture which uses a 128-bit cipher key has been proposed in it [23]. A high performance S-box implementation of AES algorithm over FPGA using reduced residue of prime numbers (RRPN) has been proposed in this work. The proposed design adds to the complexity and efficiency of the AES algorithm thus enhancing resistance to algebraic attacks [24]. This paper proposes a method for integrating AES encrypter and decrypter, thus developing low-complexity architecture. Hardware resources used in the Sub-Bytes module and mix columns module have been saved thus making it an efficient design for both encryption and decryption, suitable for PDAs, mobile phones and smart cards [25]. Speed enhancement has been achieved in this work by insertion of compact and flexible architecture for the Mix-column transformation operation. It also proposes to use a fixed coefficient multiplier for Mix-Column transform. High throughput is achieved by incorporating a change in the inner process order in round transformation [26].

The fully pipelined architecture with high throughput for data security applications has been proposed in this work. The hardware is implemented on FPGA[27]. 32-bit bus width architecture for implementation of AES algorithm on FPGA has been proposed in this work. Higher speed was achieved using pipelining whilst Sub-bytes method was implemented using both composite field and fixed ROM techniques[28]. In this paper three novel composite field arithmetic (C.F.A) S-Boxes of field GF ((22)2)2 for the implementation of AES algorithm have been derived and the best of them chosen by algorithmic and architectural optimizations. The design with minimal area cost and highest throughput was chosen[29] An efficient high speed hardware implementation of AS algorithm has been presented in this paper. Composite field arithmetic in normal bases has been used and novel key expansion ar-chitecture is also presented. Key variation during encryption is also supported by the proposed architecture [29]. A significant increase in throughput of about 230 architecture proposed in by using a block and key size of 512-bits.The architecture for AS algorithm was implemented on FPGA. High resistance to cryptanalysis attacks was achieved with only a minimal increase in area cost[30]. In this paper an extension of a public key cryptosystem has been proposed to support a private key cryptosystem. A new arithmetic unit has been developed in which the polynomial modular multiplication of ECC is extended to compute the polynomial arithmetic operations over binary extended field of AES. Higher hardware efficiency was achieved [31]. A higher throughput/area was achieved in the architecture proposed .The paper proposes a FPGA implementation for data storage encryption [32].

III. PERFORMANCE SUMMARY

In an effort to summarize the work conducted in the relevant field so far we have chosen only the most suitable results of FPGA implementations. These results are summarized in the table 3. LUTs are Look Up Tables, CLBs are Con-figurable Logic Blocks, enc./dec. is encryption/decryption, RRPN is Reduced Residue Prime Numbers, CBC is (cipher Block Chaining) mode, CFB is (cipher feedback) mode, CTR (counter) mode.

TABLE I: PERFORMANCE SUMMARY OF STATE OF THE ART

Name /year	Process/ comment	Number of gates	requency/ throughput
P. Chodowiec 2001[1]	Enc. Pipelined approach	12.6k CLB	95 MHz/ 12.2 Gbit/s
M. McLoone 2001[3]	Enc. Pipelined approach	2.7kCLB + 82 RAM	54.4 MHz/ 6.95 Gbit/s
N. Sklavos 2002[6]	Enc./Dec. —-	2358 CLB	22 MHz/ 259 Mbit/s
N. Sklavos 2002[15]	Enc./Dec. Pipelined approach	17.3k CLB	28.5 MHz/ 3.65 Gbit/s
J. H. Shim 2002[22]	Enc./Dec. —-	2580 CLB	38.8 MHz/ 452 Mbit/s
Refix sever 2004[9]	Enc./Dec. Block RAM	4189 CLB + 4RAM	28.5 MHz/ 1.19 Gbit/s
Monica Liber 2007 [5]	Enc. Round loop unrolling	1643 slices	91.5 MHz/ 224.2 Mbit/s
Chi-Wu Huang 2007[16]	Enc. Block RAM	148 slices + RAM	287 MHz/ 647Mbps
SwinderKaur 2007[17]	Enc./Dec. pipelining	6279 Slices/	119.954MHz 1.18 Gbps
Banraplangjyr 2009[32]	Enc./Dec. iterative	6211 Slices	142.5MHz/ 1458 Mbps
A. M. Borkar 2011[12]	Enc./Dec. CFB mode	1853 Slices/	140.390MHz 352 Mbits/sec
Alex planto 2012[25]	Enc./ Dec. iterative	4779 Slices	240 Mbit/s 184 Mbit/s
Hoang Trang 2012[26]	Enc./ Dec. iterative approach	1993 Slices	1188 Mbit/s 422 Mbit/s

IV. CONCLUSION

The Advanced Encryption Standard algorithm is a sym-metric block cipher that can process data blocks of 128 bits through the use of cipher keys with lengths of 128, 192, and 256 bits. An efficient FPGA implementation of 128 bit block and 128 bit key AES algorithms has been presented in this paper. The design is implemented on Xilinx and altera using different kind of FPGA such as Spartan 3E. these designs are tested with the sample vectors provided by FIPS 197. FPGA implementation offers ultra high speed with low latency. The results of the researches compared with one together. It is shown that the improved architecture produces significant contribution in terms of speed and latency and optimize the silicon area and power consumption.

ACKNOWLEDGMENT

we are likes to gratefully acknowledge to all the staff member of electronics and Telecommunication department in J. T. Mahajan College of Engineering, Faizpur for allowing us to conduct the research using its all kinds of facilities.

REFERENCES

[1] P. Chodowiec, P. Khuon and K. Gaj, ”Fast Implementations of Secret-Key Block Ciphers Using Mixed Inner and Outer Round Pipelining”, Proc. ACM/SIGDA Int. Symposium on Field Programmable Gate Arrays, FPGA’01, Monterey, 2011.

[2] Refik Sever, A. NeslinI smailoglu, Yusuf C. Tekmen, Murat Askar, Burak Okcan,”A High

speed FPGA Implementation of the Rijndael Algorithm", Proceedings of the EUROMICRO Systems on Digital System Design (DSD04),IEEE, pp.358-362, 2004.

[3] Nazar A. Saqib, Francisco Rodrguez-Henrquez and Arturo Daz-Prez," AES Algorithm Implementation An efficient approach for Sequential and Pipeline Architectures ", Proceedings of the Fourth Mexican International Conference on Computer Science (ENC03),IEEE, pp. 126 130, 2003.

[4] DeenKotturi, Seong-Moo Yoo, and John Blizzard, AES Crypto Chip Utilizing High-Speed Parallel Pipelined Architecture, IEEE, Vol. 5, pp. 4653-4656, 2005.

[5] Monica Liberatori, Fernando Otero, J. C. Bonadero, Jorge Castifieira,"AES-128 cipher. High speed, low cost fpgaimplementation", IEEE,2007.

[6] Banraplang Jyrwa, Roy Paily, "An Area-Throughput Efficient FPGA implementation of Block Cipher AES algorithm",IEEE, 2009.

[7] Nalini C. Nagaraj, Dr. Anandmohan P.V. and Poornaiah D.V, "An FPGA Based Performance Analysis of Pipelining and Unrolling of AES Algorithm", IEEE, pp.477-482, 2006.

[8] Chi-Wu Huang, Chi-Jeng Chang, Mao-Yuan Lin, Hung-Yun Tai, "Com-pact FPGA Implementation of 32-bits AES Algorithm Using Block RAM", IEEE, pp.126-129, 2007.

[9] Muhammad H. Rais, and Syed M. Qasim,"FPGA Implementation of Rijndael Algorithm using Reduced Residue of Prime Numbers", IEEE, pp.1-4,2009.

[10] C. Sivakumar and A .Velmurugan,"High Speed VLSI Design CCMP AES Cipher for WLAN (IEEE 802.11i)", IEEE, pp.398-403,2007.

[11] Swinder Kaur, Prof. Renu Vig,"Efficient Implementation of AES Al-gorithm in FPGA Device", International Conference on Computational Intelligence and Multimedia Applications, IEEE ,Volume.2,pp.179-187, 2007.

[12] Mr. Atul M. Borkar, Dr. R. V. Kshirsagar, Mrs. M. V. Vyawahare, "FPGA Implementation of AES Algorithm,IEEE,Vol.3,pp.401-405,2011.

[13] Gael Rouvroy, Francois-Xavier Standaert, Jean-Jacques Quisquater and Jean-Didier Legat,"Compact and Efficient Encryption/Decryption Module for FPGA Implementation of the AES Rijndael VeryWell Suited for Small Embedded Applications",ITCC04,IEEE,Vol.2,pp.583-587,2004.

[14] Ahmed Rady, Ehab EL Sehely, A.M. EL Hennawy,"Design and Implementation of area optimized AES algorithm on reconfigurable FPGA",IEEE,pp.35-38, 2007.

[15] H.Li,"Efficient and flexible architecture for AES",IEEE,Vol.153(6),pp.533-538,2006.

[16] Gang Zhou, Harald Michalik, Laszlo Hinsenkamp,"Efficient and High-Throughput Implementations of AES-GCM on FPGAs", ICFPT,IEEE,pp.185-192,2007.

[17] Nicholas Weaver and John Wawrzynek, "High Performance, Compact AES Implementations in Xilinx FPGAs",2002.

[18] Sumanth Kumar Reddy, R.Sakthivel, P Praneeth,"VLSI Implementation of AES Crypto Processor for High Throughput", IJAEST,Vol.6(1),pp.022-026, 2011.

[19] Tim Good and Mohammed Benaissa,"AES on FPGA from the fastest to the smallest", Springer Berlin Heidelberg,pp.427-440.

[20] Chih-Peng Fan, Jun-Kui Hwang,"FPGA implementations of high throughput Sequential and Fully pipelined aes algorithm", International Journal of Electrical Engineering, Vol.15(6),PP. 447-455, 2008.

[21] Yulin Zhang, Xinggang Wang, "Pipelined Implementation of AES En-cryption Based on FPGA", IEEE,pp.170-173, 2010

[22] Muhammad H. Rais and Syed M. Qasim,"Efficient Hardware Re-alization of Advanced Encryption Standard Algorithm using Virtex-5 FPGA", International Journal of Computer Science and Network Security, Vol.9(9),pp.201-205, 2009.

[23] Muhammad H. Rais and Syed M. Qasim,"Efficient FPGA Realization of S-Box using Reduced Residue of Prime Numbers", International Journal of Computer Science

and Network Security, Vol.10(1),pp. 754-757, 2010.

[24] Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kay-atanavar, (2009)”FPGA Implementation of AES Encryption and Decryp-tion”, International Conference on Control, Automation, Communication and Energy Conservation, 2009.

[25] M. Rajaram, J. Vijaya,”High Speed Pipelined AES with Mixcolumn Transform”, European Journal of Scientific Research, 2011.

[26] Gurmail Singh, Rajesh Mehra, ”FPGA Based High Speed and Area efficient Aes Encryption for Data Security”, International Journal of Research and Innovation in Computer Engineering(IJCTA), Vol.1(2), pp.53-56, 2011 .

[27] Tanzilur Rahman, Shengyi Pan, Qi Zhang, ”Design of a High Through-put 128-bit AES (Rijndael Block Cipher)”,International Multi Conference of Engineers and Computer Scientists,IEEE,vol.2, 2010.

[28] M. M. Wong, M. L. D. Wong, A. K. Nandi, and I. Hijazin,”Construction of Optimum Composite Field Architecture for Compact High-Throughput AES S-Boxes”, IEEE, Vol.1(99),pp.1-5, 2011.

[29] HadiSamiee, RezaEbrahimiAtani, HamidrezaAmindavar,”A Novel Area-Throughput Optimized Architecture for the AES Algorithm”, Interna-tional Conference on Electronic Devices, Systems and Applications (ICEDSA),IEEE, pp.29-32, 2011.

[30] Abidalrahman Mohmad,Yaser Jararweh, Lorai Tawalbeh,”AES-512: 512-Bit Advanced Encryption Standard Algorithm Design and Evalua-tion”, IEEE, pp.292-297, 2011.

[31] Yi Wang and Renfa Li,”A Unified Architecture for Supporting Oper-ations of AES and ECC”, Fourth International Symposium on Parallel Architectures, Algorithms and Programming, IEEE, pp.185-189, 2011.

[32] Shakil Ahmed, Khairul mizam Samsudin, Abdul Rahman Ramli, Fakhrul Zaman Rokhani,”Effective Implementation of AES-XTS on FPGA”, IEEE, pp 184-186. 2011.