International Journal for Innovative
Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 5th Mar 2021. Link :http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=ISSUE-03

DOI: 10.48047/IJIEMR/V10/I03/22

Title **DESIGN A HIGH SPEED PIPELINED AUTHENTICATED ENCRYPTION USING EMLD FOR SECURE COMMUNICATION**

Volume 10, Issue 03, Pages: 146-152

Paper Authors

THAMALAPAKULA RAMYA, Y.BHASKARA RAO

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

DESIGN A HIGH SPEED PIPELINED AUTHENTICATED ENCRYPTION USING EMLD FOR SECURE COMMUNICATION

[1] THAMALAPAKULA RAMYA, [2] Y.BHASKARA RAO
[1]M.Tech Scholar, Dept of ECE, Malineni Lakshmaiah Women's Engineering College, Guntur - Prathipadu Rd, Pulladigunta, Andhra Pradesh
[2]Associate professor, Dept of EEE, Malineni Lakshmaiah Women's Engineering College, Guntur - Prathipadu Rd, Pulladigunta, Andhra Pradesh

ABSTRACT: In this paper design a high speed pipelined authenticated encryption using EmLD for secure communication is implemented. In this inputs are taken as A and B. These inputs are assigned in the form of bits. 16 Byte state RF is performed. S-Box LUT is used to substitute the bits. All these are saved in working register. EmLD is used to encrypt and decrypt the data for better security. SPRP will perform the operation randomly for high speed. This article is implemented using Xilinx 14.7 ISE design tool. From results, RTL schematic, Technology schematic and output waveforms are given in detail manner. Hence, this project gives effective results and provides high security.

KEYWORDS:SPRP (Strong Pseudorandom Permutation), ELmD (Encrypt-Linear mix-Decrypt), S-BOX (Substitute Box), LUT (Look Up Table).

I. INTRODUCTION

Several fields in the web communication need general service for trading large portions of data. Some portion data is transmitted through dedicated channels between two users. The role of cryptography enters here to monitor and protect the data while transferring. The cryptography guarantees communication across the defective channel by employing secret codes. It also gives assurance regarding authentication of users. It clearly distinguishes between approved and unapproved persons. One of the well-known cryptography technique is Authenticated Encryption system [1].

In AES generally four standard transformation techniques are used. The four transformations are round Key, substitution of bytes, shift row and mix columns.

Security is the most significant issue in communication networks to protect private data of every individual. Many types of cryptography techniques have been proposed each one is remarkably suitable for specific applications. Another type of cryptography technique discussed earlier is hash functions do not use any keys for performing encryption of data [2]. It is not suitable for the applications where security is primitive. The purpose of security can be obtained using public key encryption because it uses two keys for scrambling and unraveling.

One key is used for validation of the user and other is used for deciphering of text. In intersecting network sender initiates transfer of data. The public key is used to verify the message whether it is encoded or not. In case of unscrambled message, it stops sending it to other client. The protection of data deserves some changes to data [3]. The public key encryption is responsible for secured transmission, user authentication, traffic checking, non-repudiation and investigation of unauthorized users. Encryption using computers is most powerful technique among many discovered algorithms on data systems.

A cryptography algorithm is said to be the most powerful algorithm only when it has evident proof of adverse attack and essential changes that have been made to act against that kind of attacks. A method introduce for providing utmost security is key schedule. In this schedule, different keys are extracted from private key, which are used for encryption in each round in order to conceal information from interpreting and changing. The computation of different keys for various stages can be done using computers.

There is a chance of disclosing data by trespassers to other association who may reveal mystery data or alter it according to their wish. When we want to send data using particular encryption technique we should first aware of total structure used in it. Then only we can block intruders from attacking our info systems. Cryptography gives assurance that data could not be interpreted or analyzed by any unauthorized persons except the user destined for that. It has the ability to block the trespasser from striking data which is protected.

In cryptography initially information is encrypted by using some familiar technique by giving proper command. In fast developing environment, information is not simply messages that are transferred between two users, it is lot more than that. Advanced data systems are double complex than normal ones. Some examples of advanced data systems are open data (online papers, blogs) and payer driven affiliations (data fetched by any person), private systems like individual collection of on-line content and websites run by individuals and secret organizations like military data, medicinal related data , online libraries which is accessed only by few authorized users [4-5]. The protection of this kind of data systems is in pace in present scenario.

Private key or secret key cryptography is utilized to address the difficulty in key transferring. In this secret key technique only one mystery key is exploited for both scrambling and decomposing. In public key encryption public key is utilized for composing and mystery key is used for decomposing of text. Among two techniques secret key is a faster and widely used algorithm. Therefore secret (parallel) key is used in to enhance the speed of substitution of bytes in AED. A programming scheme called as T-box used for computation, which includes sub bytes and Mix columns steps in encryption as well as Inv sub bytes and Inv mix columns in decryption.

At present day's cryptography significant role in communication networks. In this technique plain or clear which is need to be transmitted is converted to unreadable form called cipher text. After message received the receiver decrypts it to actual plain text. The Cryptography is concerned with the following properties:

Confidentiality: The information sent via channels must be not interpreted by any person.

Integrity: No one can change original information.

Non- repudiation: No need to control the desire to transmit the messages

Authentication: Correct validation of sender and receiver during communication.

II. AUTHENTICATED ENCRYPTION SYSTEM (AE)

A communication can be made secure and protective by using cryptography. The two main text types that encounter in cryptography are clear text and scrambled text. The plain text is nothing but original information in user's own language, which he wants to send and cipher text is the encoded or scrambled form of plain text. The study of various techniques used for the safe communication is called cryptography.

Symmetric and Asymmetric key are two main algorithms that are employed in cryptography. In secret key the sender and recipient at both ends of communication channel use same key for scrambling and unscrambling the data. It keeps the information confidential, which is the fundamental goal of cryptography. In other one asymmetric Key the sender and receiver at the ends of communication channel use dissimilar keys for ciphering and deciphering. It is mainly used for the purpose of authentication and key exchange. Many encryption techniques have been developed from the long time. AE can use different length keys such as 64, 128, 196 bit keys. It is based on symmetric key encryption technique. Unlike the block ciphers, which use two-paired keys at encryption and decryption side, AE uses solitary key for encryption processes. Generally, no particular encryption algorithm is fast in software point of view. But, we can modify hardware structure of encryption algorithm to increase speed and reduce the power and required. Therefore, we present here an optimized hardware structure substituting customary modules of AE algorithm.

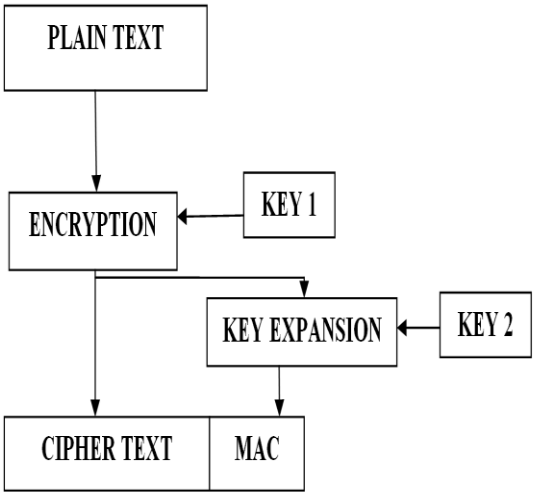


Fig. 1: AUTHENTICATED ENCRYPTION SYSTEM

The three essential blocks of AES are encryption, MAC and key expansion. The algorithm starts with input data block and key. The encryption stats with the data block and key. Before start of encryption process three control signals clock, reset and go are given. The process of ciphering and deciphering depends on these three control signals. The scrambled text is given as input to the deciphering block, which is converted into plain text.

III. TWEAKEY ENCRYPTION

The below figure (2) shows the block diagram of proposed system. In this inputs are taken as A and B. These inputs are assigned in the form of bits. 16 Byte state RF is performed. S-Box LUT is used to substitute the bits. All these are saved in working register. EmLD is used to encrypt and decrypt the data for better security. SPRP will perform the operation randomly for high speed. At last output is obtained. The description of each block is given in detail manner.

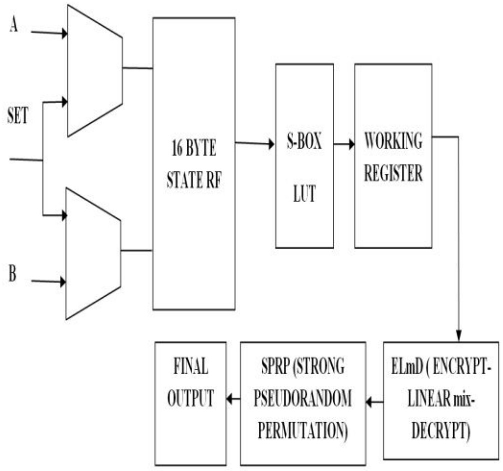

A
SET
B
16 BYTE STATE RF
S-BOX LUT
WORKING REGISTER
ELmD (ENCRYPT-LINEAR mix-DECRYPT)
SPRP (STRONG PSEUDORANDOM PERMUTATION)
FINAL OUTPUT

Fig. 2: PROPOSED SYSTEM

A. SUBSTITUTION BYTE

The first transformation used at the encryption site is Sub Bytes. We interpret the byte as two hexadecimal digits whose left digit gives the row and right digit gives the column of the substitution table. The contents of each byte in a state change but the arrangement of the bytes remains the same. It is an intra-byte transformation.

In this step, the matrix elements use the table that named S-Box. S-Box is a nonlinear function. It is implemented using a 16*16 sate table. This conversion table is built based on values in Galois field that shown by GF (28) and it is resistant against the known attacks. This shows that row and column determines input and output values that are stored in these values table. Having an element of the state matrix, we can obtain the other elements. This means that "four left bits" of elements denote the row and four right bits of elements denote the column of sate table, which is used to reverse S-Box table to decrypt.

The s-Box replaces each Byte of state matrix values based on a substitution of fixed table with the new values. FHED has 32 Bytes in the substitution of elements that have been organized in a 16 × 16 matrix. To replace Bytes with the equivalent, four least significant bits in Bytes as the number of rows and four most significant bits as the number of columns are applied in this state table. It is corresponding element, which is used instead of original value.

B. ENCRYPT-LINEAR mix-DECRYPT

It is an efficient, nonce-misuse resistant, fully pipelined implementable online authenticated encryption scheme ELmD, which can also be used in lowend devices, ELmD verified decryption is the algorithm that takes a nonce N, an associated data D and a tagged-ciphertext C and returns a message M or ⊥, depending on the verification. The Decryption function is a three step process : First IV is generated using N and D, which is identical to the initial value generation during the authenticated encryption. Then the decryption is performed using the tagged ciphertext and then the verification is performed and if verified, corresponding message is returned.

The main goal of the cipher is to be efficient, provide high performance and able to perform well in low end devices. For efficiency, we want our cipher to be one pass, nonce misuse resistant. To obtain high performance, we want our cipher efficient as well as fully pipeline implementable. To perform well in low end devices, we require that our cipher to be secure against block wise adaptive adversaries.

We know that, Encrypt Mix Encrypt is a block-cipher mode of operation, that turns a block cipher into a tweakable enciphering scheme.

C. STRONG PSEUDORANDOM PERMUTATION

In cryptography, a strong pseudorandom permutation (PRP) is a function that cannot be distinguished from a random permutation (that is, a permutation selected at random with uniform probability, from the family of all permutations on the function's domain) with practical effort.

An adversary for an unpredictable permutation is defined to be an algorithm that is given access to an oracle for both forward and inverse permutation operations. The adversary is given a challenge input *k* and is asked to predict the value of F_k. It is allowed to make a series of queries to the oracle to help it make this prediction, but is not allowed to query the value of *k* itself.

A randomized algorithm for generating permutations generates an unpredictable permutation if its outputs are permutations on a set of items (described by length-*n* binary strings) that cannot be predicted with accuracy significantly better than random by an adversary that makes a polynomial (in *n*) number of queries to the oracle prior to the challenge round, whose running time is polynomial in *n*, and whose error probability is less than 1/2 for all instances. That is, it cannot be predicted in the complexity class PP, relativized by the oracle for the permutation

IV. RESULTS

The below figure (3) shows the RTL schematic of proposed system.

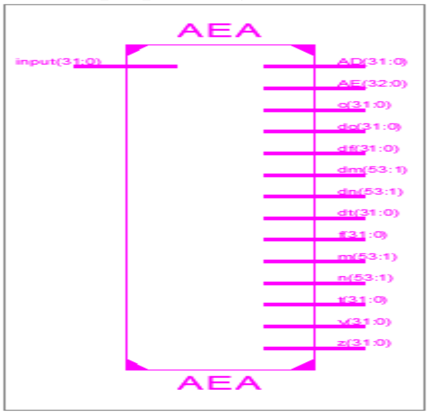


Fig. 3: RTL SCHEMATIC

The below figure (4) shows the Technology schematic of proposed system.

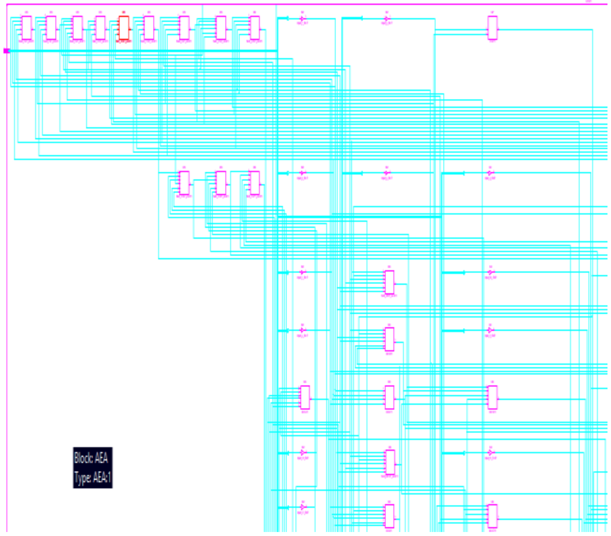
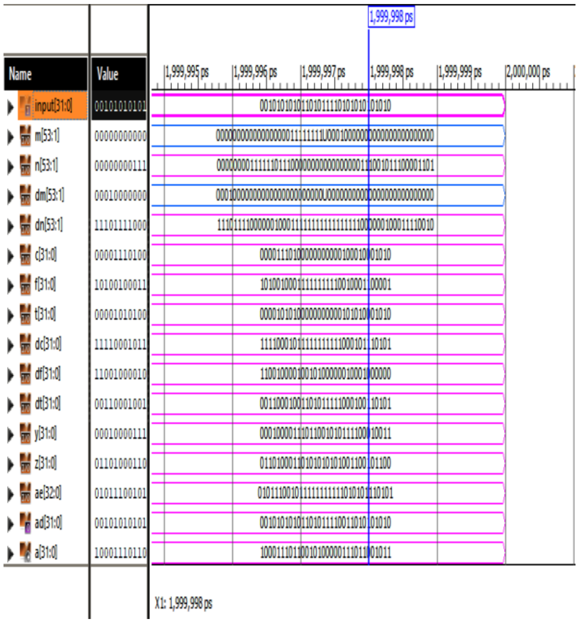


Fig. 4: TECHNOLOGY SCHEMATIC



1,999,998 ps

Name	Value	1,999,995 ps … 2,000,000 ps
input[31:0]	00101010101	00101010101101011110101010101010
m[53:1]	00000000000	0000000000000000001111111U00010000000000000000000000
n[53:1]	00000000111	0000000011111101110000000000000000011100101110001101
dm[53:1]	00010000000	00010000000000000000000000U0000000000000000000000000
dn[53:1]	11101111000	11101111000000100011111111111111111000001000111110010
c[31:0]	00001110100	00001110100000000000100010001010
f[31:0]	10100100011	10100100011111111110010001100001
t[31:0]	00001010100	00001010100000000000101010001010
dc[31:0]	11110001011	11110001011111111111000101110101
df[31:0]	11001000010	11001000010010100000010001000000
dt[31:0]	00110001001	00110001001101011111000100110101
y[31:0]	00010000111	00010000111011001010111100010011
z[31:0]	01101000110	01101000110101010101001100101100
ae[32:0]	01011100101	010111001011111111111010101110101
ad[31:0]	00101010101	00101010101101011110011010101010
a[31:0]	10001110110	10001110110010100000111011001011

X1: 1,999,998 ps

Fig. 5: OUTPUT WAVEFORM

V. CONCLUSION

Hence design and implementation of high speed VLSI architecture of GCM for authenticated Encryption was implemented. The main intent is to provide privacy and integrity using authenticated encryption algorithm. This will increase the speed of operation in effective way.

VI.REFERENCES

[1] Sandhya Koteshwara , Amitabh Das, Keshab K. Parhi , "Architecture Optimization and Performance Comparison of Nonce-Misuse-Resistant Authenticated Encryption Algorithms", 1063-8210 © 2019 IEEE.

[2] S. Koteshwara and A. Das, "Comparative study of authenticated encryption targeting lightweight IoT applications," IEEE Design Test, vol. 34, no. 4, pp. 26–33, Aug. 2017.

[3] C. Dobraunig, M. Eichlseder, S. Mangard, F. Mendel, and T. Unterluggauer, "ISAP–towards side-channel secure authenticated encryption," IACR Trans. Symmetric Cryptol., vol. 2017, no. 1, pp. 80–105, 2017.

[4] H. Böck, A. Zauner, S. Devlin, J. Somorovsky, and P. Jovanovic, "Nonce-disrespecting adversaries: Practical forgery attacks on GCM in TLS," in Proc. USENIX WOOT, 2016, pp. 1–11.

[5] P. G. Lopez et al., "Edge-centric computing: Vision and challenges," ACM SIGCOMM Comput. Commun. Rev., vol. 45, no. 5, pp. 37–42, Oct. 2015

[6] F. Abed, C. Forler, and S. Lucks, "General overview of the firstround CAESAR candidates for authenticated encryption," IACR Cryptol. ePrint, Tech. Rep. 2014/792, 2014

[7] D. McGrew and D. Bailey, AES-CCM Cipher Suites for Transport Layer Security (TLS), document RFC 6655, 2012.

[8] H. Handschuh and B. Preneel, "Key-recovery attacks on universal hash function based MAC algorithms," in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, 2008, pp. 144–161.

[9] M. Bellare, P. Rogaway, and D. Wagner, "The EAX mode of operation," in Proc. Int. Workshop Fast Softw. Encryption. Berlin, Germany: Springer, 2004, pp. 389–407.

[10] P. Rogaway, M. Bellare, and J. Black, "OCB: A block-cipher mode of operation for efficient authenticated encryption," ACM Trans. Inf. Syst. Secur., vol. 6, no. 3, pp. 365–403, Aug. 2003.

[1]THAMALAPAKULA RAMYA
Completed B.Tech from Hindu college of engineering & Technology and pursuing M.Tech from Mallineni Lakshmaiah women's engineering college. Her M.Tech specialization is Very large scale integration (VLSI).

[2]**Y.BHASKARA RAO** Completed B.Tech from Bapatla engineering college and M.Tech from Bapatla engineering college. At present he is working as associate professor in Mallineni Lakshmaiah women's engineering college.