JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Design and Implementation of a VLSI Architecture using Tweakey Encryption for High-Speed Applications

[1]SHAIK SABIHA, [2] SHAJAHAN PATAN
[1]M. Tech Scholar, Dept of ECE, Narasaraopeta Institute of Technology, Narasaraopet, A.P, India
[2]Assistant Professor, Dept of ECE, Narasaraopeta Institute of Technology, Narasaraopet, A.P, India

Abstract: In this paper the design and implementation of high-speed VLSI architecture of tweakey Encryption is done. This article is aimed at providing better security and resource efficiency compared to existing standards. Tweakey encryption system provides both privacy and integrity. Key scheduling algorithm will provide the key according to the schedule. S-Boxis used to substitute the bits after pre-processing stage. To save all these bits, register is used. Shift rows technique is used to shift the operation in row wise manner. At last, the shifted bits are encrypted using tweakey Encryption. This is implemented using Xilinx 14.7 ISE design tool. From results, RTL schematic, Technology schematic and output waveforms are given in detail manner. At last, compared to existed system, proposed tweakey Encryption gives effective output.

Key Words: **Tweakey Encryption, Shift Rows, S-BOX, and Cryptography.**

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 techniques is Authenticated Encryption system [1].

In AES generally four standard transformation techniques are used. The four transformations are round Key, substitution of bytes, shifting 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 another 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 introduces 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.

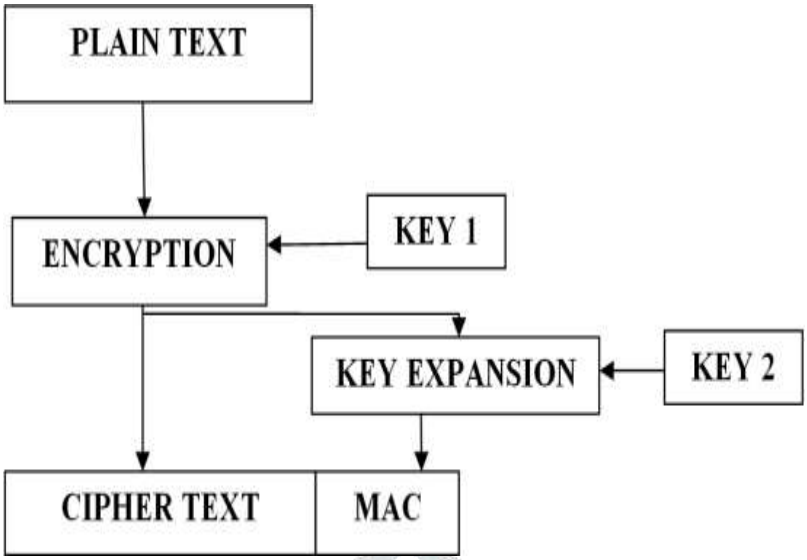

Figure (1): Authenticated Encryption System.

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 input and key are taken as inputs. These inputs are assigned in the form of bits. S-Box is used to substitute the bits. Shift row is the transformation technique which is used to transform the bits in row format. Key scheduling algorithm will provide the key according to the schedule. To save all these bits, register is used. At last, the shifted bits are encrypted using tweakey Encryption.

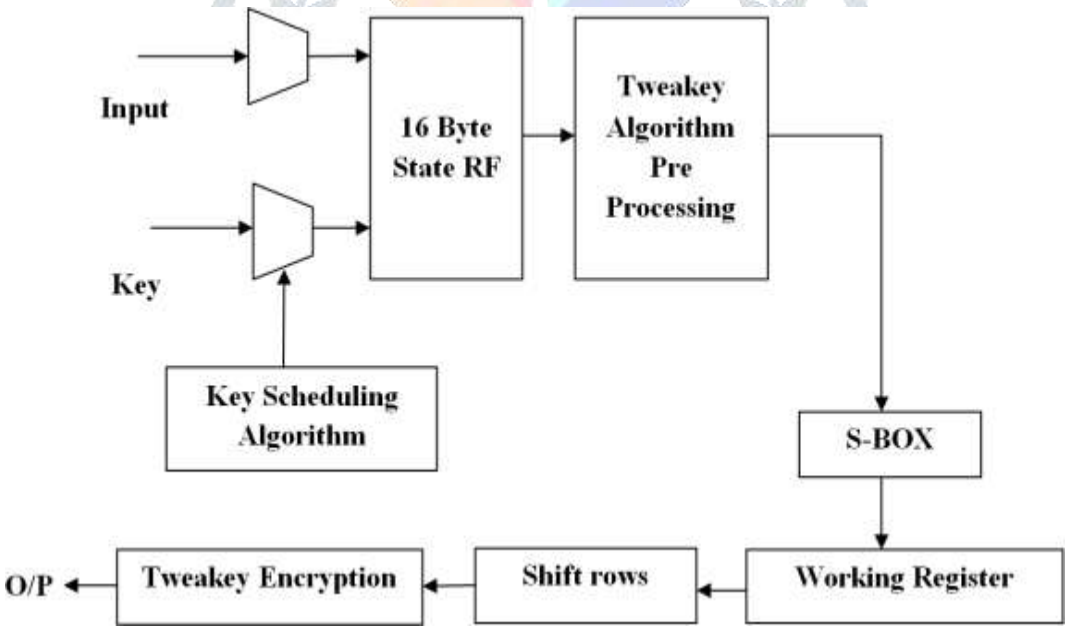

Figure (2): Proposed System.

Substitute Bytes Transformation (S-BOX) is the modified structure of AED starts with changes in the Sub bytes step. The function of this step is to substituted at present in the S-box memory unit within the state by diverse data present in other memory unit. The dispersion of data in memory units creates confusion. The main purpose of this Shannon's contents for scientific restraint arrangement is to stimulate security. The basic purpose of substitution of bytes is to secure information.

Shift row transformation is followed by substitution of bytes step. This step works on shifting of bytes present in each row. Commonly the shifting done either to left side or right side. The shifting employed in the row transformation is circular shift. In this step first row is moved one byte to the left side as it is circular shifting the left most byte comes right side of the row. In the same way the second row is moved two-byte positions left and third row shifts three positions left. Consequently, the size of the output state matrix of this step does not change but, the byte positions will change.

Tweakey Encryption algorithm is a combination of complex mathematical functions which are used to encrypt the confidential information. Encryption key is a secret value that the sender utilizes as one of the inputs to the encryption algorithm in conjunction with plain text to generate a cipher text.

IV. RESULTS

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

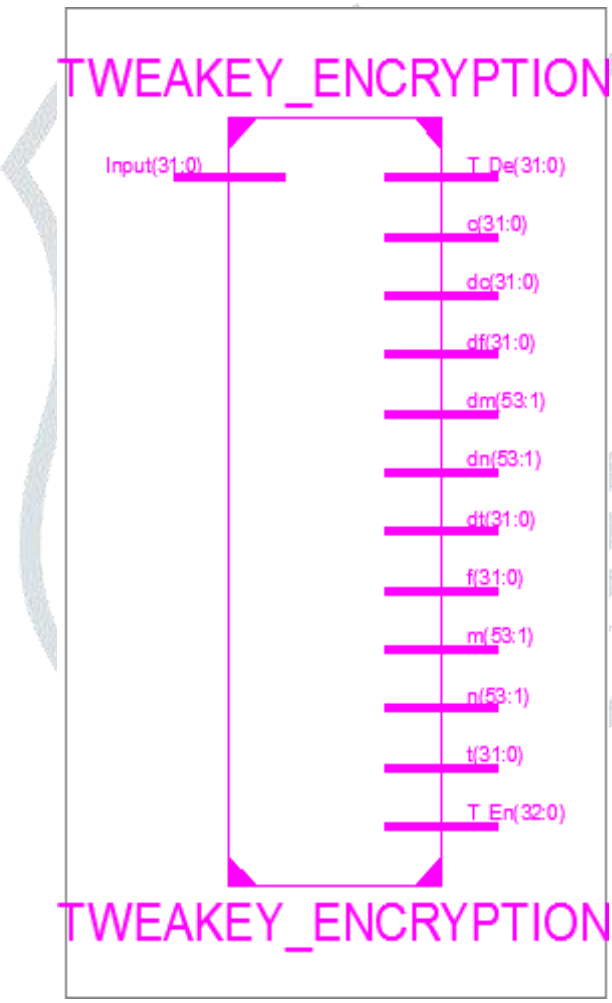

Figure (3): RTL Schematic.

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

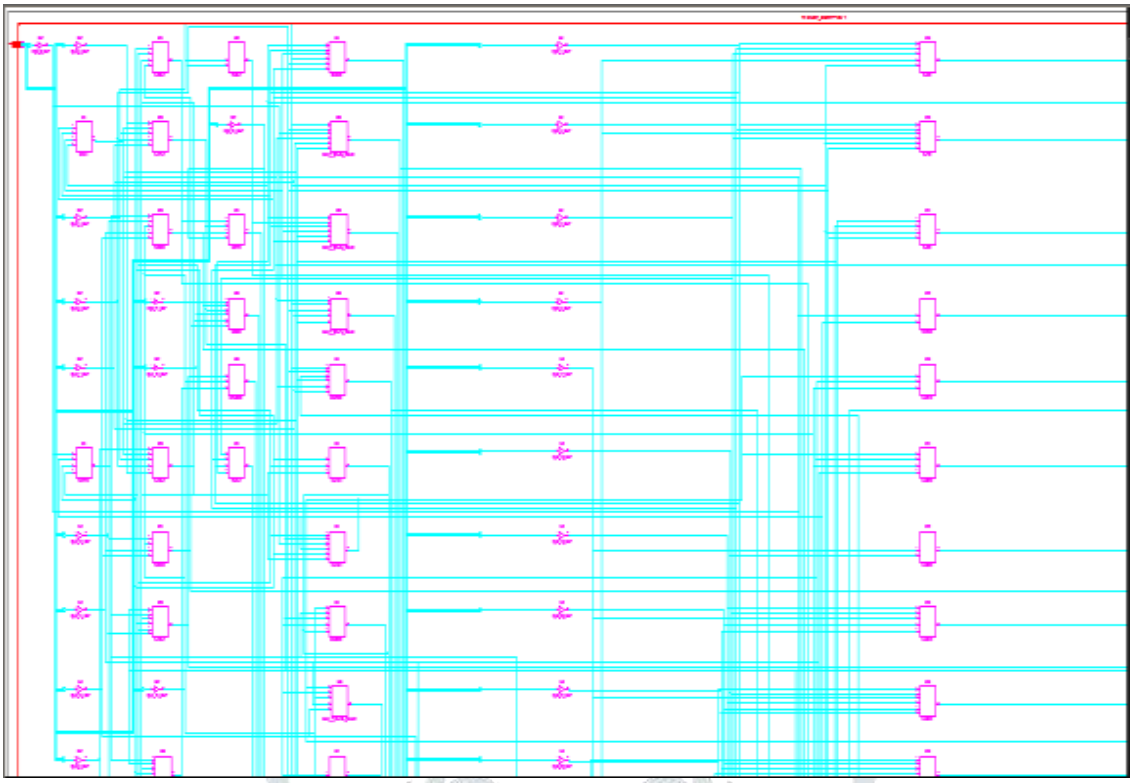

Figure (4): Technology Schematic.

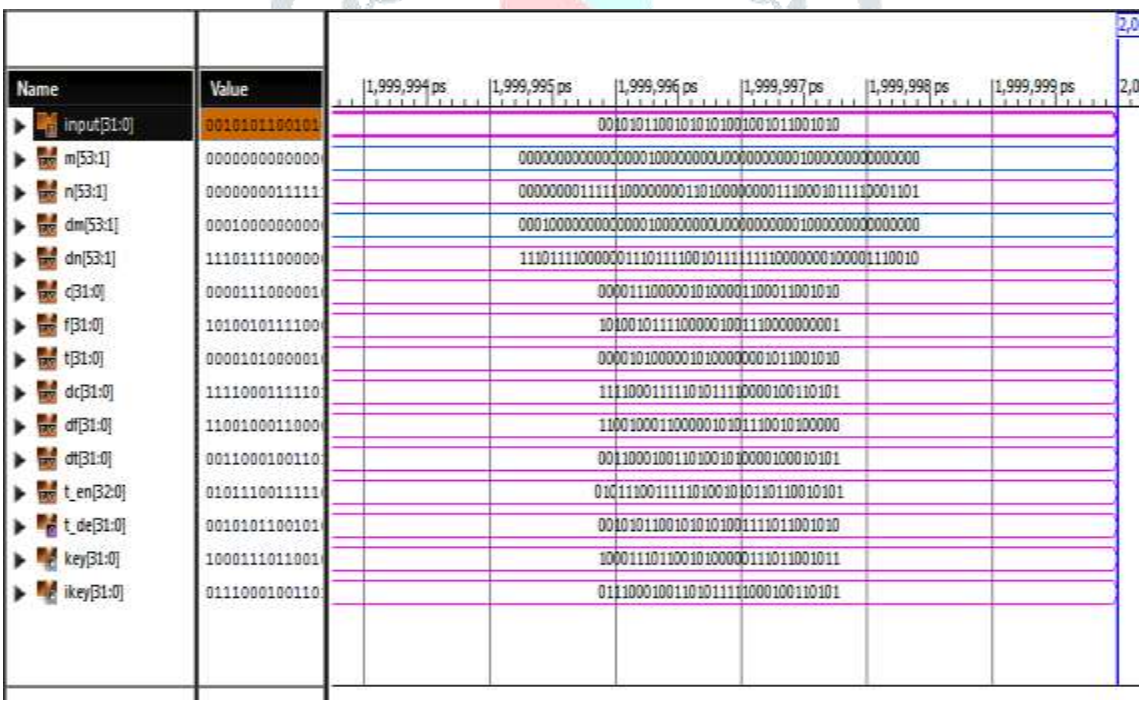

Figure (5): Output Waveform.

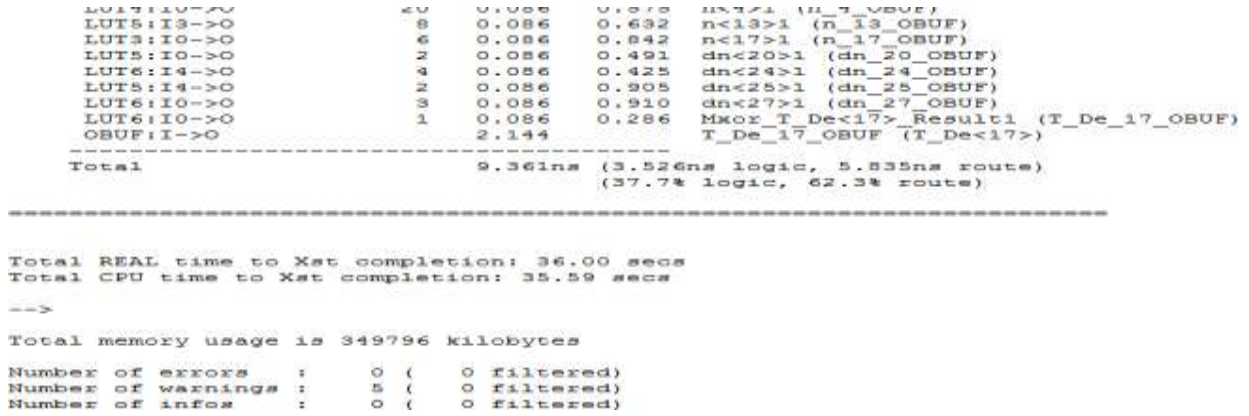

Figure (6): Synthesis Report.

V. CONCLUSION

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

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," IACRCryptol.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] Sandhya Koteshwara, Amitabh Das, Keshab K. Parhi, "Architecture Optimization and Performance Comparison of Nonce-Misuse-Resistant Authenticated Encryption Algorithms", 1063-8210 © 2019 IEEE.
[11] 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.
[12] 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.
[13] 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.
[14] 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
[15] F. Abed, C. Forler, and S. Lucks, "General overview of the first round CAESAR candidates for authenticated encryption,"IACR Cryptol.ePrint,Tech. Rep.2014/792, 2014
[16] D. McGrew and D. Bailey, AES-CCM Cipher Suites for Transport Layer Security (TLS), document RFC 6655, 2012.
[17] 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.
[18] 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.