International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

DESIGN A HIGH SPEED AND HIGH SECURE CCM BASED AUTHENTICATED ENCRYPTION

[1]MOVVA SIVANAGESWARAO, [2]N VAMSIKRISHNA, [3]A RAGHAVARAJU,
[4]N VIJAYSHANKER

[1]M.Tech Scholar, Department of ECE, Chebrolu Engineering College, Chebrolu, Guntur Dist, Andhra Pradesh Andhra Pradesh, India

[2]Assistant Professor, Department of ECE, Chebrolu Engineering College, Chebrolu, Guntur Dist, Andhra Pradesh Andhra Pradesh, India

[3,4]Associate professor, Department of ECE, Chebrolu Engineering College, Chebrolu, Guntur Dist, Andhra Pradesh Andhra Pradesh, India

ABSTRACT: CCM (Counter with Chaining Mode) is the abbreviation for Counter with Cipher Block essentially combines the counter (CTR) mode of encryption with CBC-MAC authentication scheme. To process each message block, a counter is encrypted with the underlying block cipher and the result is XORed to the message for ciphertext production. In this project, design a high speed and high secure CCM based authenticated encryption is implemented. This project is aimed at providing better security and resource efficiency compared to existing standards. CCM based authenticated encryption system provides both privacy and integrity. Key scheduling algorithm will provide the key according to the schedule. S-Box is used to substitute the bits after pre-processing stage. To save all this 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 project 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**.**

KEYWORDS: CCM (Counter with Chaining Mode), tweakey Encryption, S-Box, Key scheduling algorithm

I. INTRODUCTION

Cryptography is gotten from Greek "kryptós", which means concealed or puzzle and "graphein" implies making. It is the demonstration of puzzle creating used to share mystery information over open frameworks, where substance of specialmessage are changed into inconceivable structure, in order to be recouped particularly by the normal person [1]. Cryptography was being used in obsolete Egypt since 1900 BC, where different emblematic portrayals had been cut for the inspiration driving intriguing and pleasure. Cryptography was first used as a secret strategy for correspondence by Julius Ceaser from 100 BC to 40 BC to mask critical information, and his figure become the building up stone of present day cryptography and is suggested as "Ceaser Cipher", where each character of the Roman letters all together is moved by three circumstances aside. This move makes it trash to the enemies.

A method of changing usual plain text to a form of incomprehensible text is called Cryptography. The fundamental task of the

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

cryptography is to store and send the information in a specific form so, that only particular person in destination can receive and process it [2]. Cryptography provides security against stealing of information along with another feature known as authentication. The Cryptography was emerged from the advancements in the encryption in order to strengthen its role in providing security over communication. During ancient days the encryption and decryption processes of cryptography were purely mathematical and performed using manual methods. The developments in different fields like military, business, government organizations have led to adoption of cryptography techniques to protect their data. At present, the encryption and decryption techniques of cryptography were kept unchanged, but implemented using computers. The implementation of cryptographic techniques using computers makes process much faster and safe [3]. Here, some cryptography techniques are explained. With profound researches in the field of cryptography, different algorithms were proposed. The description of algorithm and their pros and cons are briefly explained here. Some algorithms are easy to interpret, implement and thus, decrypt. In contrast to this some algorithms very complex to understand and implement so, can't be decrypted easily. Some are modest. As the encryption is basically employed to protect the data, the cryptography must provide protection against data theft and unauthorized access. The main objective of cryptography is to safeguard business and personal information and prevent theft of identity [4].

II. LITERATURE SURVEY

Earlier encryption plans were incredibly direct and merge essential numerical errands to change over a plain book to figure text. These procedures were incredibly feeble to repeat ambushes. Since the beginning of World War I, cryptographic building become progressively erratic with the passage of consistently, as they were basically generally used in the transmission of private information. Further, the utilization of PC systems has changed the field of security as current techniques perform encryption and disentangling at quick at that too at bit level. Also, contemporary cryptography relies upon certain logical conditions which are for all intents and purposes hard to understand until some remarkable models is met, these properties make it hard and tenacious for an adversary to think about an attack [5].

Different parts of the model are depicted underneath:

- Plain substance is the arranged information that will be mixed and sent over the framework.
- Cipher text is the mystery information that has been mixed using an encryption computation on the plain substance.
- Encryption count is a blend of complex numerical limits which are used to encode the mystery information [6].
- Decryption count is also a mix of complex numerical limits which are used to unscramble the ordered information. Typically an unscrambling figuring is an inverse of encryption estimation.
- Encryption key is a puzzle regards that the sender utilizes as one of the commitments to the encryption computation identified with plain substance to make a figure text.
- Decryption key is a puzzle regard that the recipient uses as one of the

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

commitments to the translating computation in synchronicity with figure text to get plain substance.

- An assailant is a substance who reliably endeavors to check out the correspondence channel to catches the figure text and further endeavors to change over the figure text to plain substance.

Cryptanalysis deals with the assessment and examination of cryptographic computations in a sensible way to grasp their working and find the vulnerabilities to part them. Cryptanalysis is utilized by military and some surveillance exercises financed by tremendous affiliations in order to test security essential systems. What's more, software engineers also use cryptanalysis to mishandle vulnerabilities in different structures and destinations. The route toward performing cryptanalysis isn't exorbitantly fundamental, it requires dominance in the field of math and start to finish understanding Introduction about the genuine working of encryption estimations. In the old-fashioned events, cryptanalysis was simply expected to enlighten the key in order to unscramble a message yet contemporary cryptography uses number-crunching and quick PCs to break encryption estimation [7]. Four fundamental steps in average cryptanalytic attack are

- Obtain the language obeing utilized
- Obtain the system obeing utilized
- Reconstruct the framework
- Reconstruction of the plain content

To discover defenselessness in a cryptographic calculation, it is critical to know the kind of language (for example English, German, French) utilized as plain content and figure text [8]. Deciding the framework can be a period taking stage. This procedure includes checking character frequency, scanning for repeated patterns and performing statistical tests. While remaking of framework happens with the way toward discovering mystery key that has been utilized with the end goal of encryption and it runs corresponding with the reproduction of plain content [9]. Cryptographic assaults rely upon the sort of encryption calculation and sort of data accessible [10].

III. PROPOSED SYSTEM

The below figure (1) shows the block diagram of attribute based authenticated encryption algorithm. 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 this bits, register is used. At last the shifted bits are encrypted using tweakey Encryption.

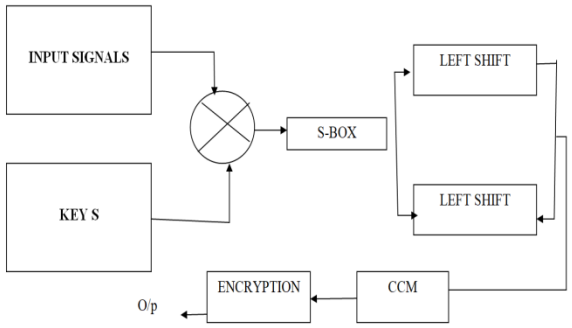

Fig. 1: PROPOSED SYSTEM

3.1 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

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

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 obtained 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.

3.2 SHIFT RIOWS

This transformation is done at encryption site. First row don't have any shift, second row has 1 Byte circular shift to the left, third row has double Byte circular shift to the left and fourth row has three Bytes circular shift to the left. Circular shift is performed to the right in decryption. Since data is stored in a column in the state matrix, this step will do a permutation between columns.

3.3 ENCRYPTION

Encryption algorithm is a combination of complex mathematical functions which are used to encrypt the confidential information. Encryption key is a secret values 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 (2) & (3) shows the RTL schematic and technology schematic of Proposed system. RTL schematic is the combination of inputs and outputs.

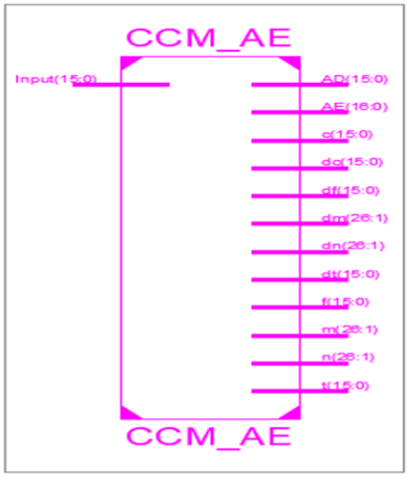

Fig. 2: RTL SCHEMATIC OF PROPOSED SYSTEM

The below figure (2) shows the RTL schematic od proposed system. Register-transfer logic deliberation is utilized in equipment portrayal dialects (HDLs) like Verilog and VHDL to make elevated level portrayals of a circuit, from which lower-level portrayals and at last genuine wiring can be determined. Structure at the RTL level is run of the mill practice in present day advanced plan.

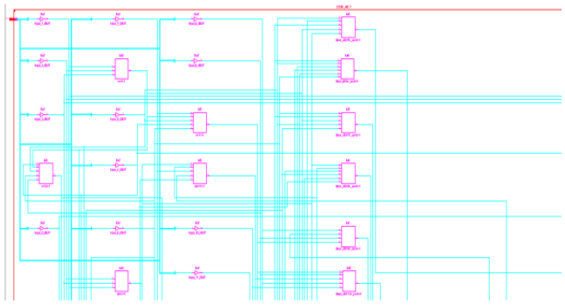

Fig. 3: TECHNOLOGY SCHEMATIC OF PROPOSED SYSTEM

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Technology schematic is the combination of Look up tables, Truth Tables, K-Map and equations. The figure (3) shows the Technology schematic of proposed system. This schematic is generated after the optimization and technology targeting phase of the synthesis process. It shows a representation of the design in terms of logic elements optimized to the target Xilinx device or "technology"; for example, in terms of of LUTs, carry logic, I/O buffers, and other technology-specific components.

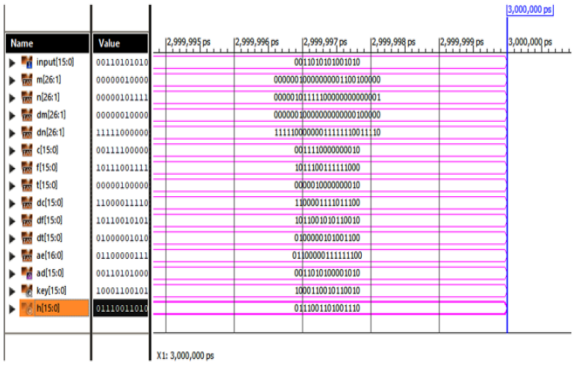

Fig. 4: OUTPUT WAVEFORM OF PROPOSED SYSTEM

The figure (4) shows the output waveform of proposed system. The entire project is implemented using 64 bits.

```
    ----------------------------------------
    Total                     3.806ns (0.301ns logic, 3.505ns route)
                                      (7.9% logic, 92.1% route)

=========================================================================

Cross Clock Domains Report:
--------------------------

=========================================================================


Total REAL time to Xst completion: 21.00 secs
Total CPU time to Xst completion: 21.03 secs

-->

Total memory usage is 4653324 kilobytes

Number of errors   :    0 (   0 filtered)
Number of warnings :    0 (   0 filtered)
Number of infos    :    0 (   0 filtered)
```

Fig. 5: SYNTHESIS REPORT OF PROPOSED SYSTEM

V. CONCLUSION

Hence design a high speed and high secure CCM based authenticated encryption was implemented. For the proposed design input signal were key are used as applying inputs to the system that are assigned in the form of bits. By using the S-box such bits were substituted then the bits were transformed in to the row bit format by using the shift row transformation technique. After that, key was provided based on the schedule with the use of Key scheduling algorithm and then register was used to save the total bits in it. Finally encryption was performed on such shifted bits by using tweakey Encryption. The main intent is to provide privacy and integrity using tweakey 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] X. Feng and S. Li, "Design of an area-effcient million-bit integer multiplier using double modulus NTT," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 25, no. 9, pp. 2658–2662, Sep. 2017.

[4] 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.

[5] X. Cao, C. Moore, M. O'Neill, E. O'Sullivan, and N. Hanley, "Optimised multiplication architectures for accelerating fully homomorphic encryption," IEEE

Trans. Comput., vol. 65, no. 9, pp. 2794–2806, Sep. 2016.
[6] Y. Doröz, E. Öztürk, and B. Sunar, "Accelerating fully homomorphic encryption in hardware," IEEE Trans. Comput., vol. 64, no. 6, pp. 1509–1521, Jun. 2015.
[7] H.-F. Luo, Y.-J. Liu, and M.-D. Shieh, "Efficient memory-addressing algorithms for FFT processor design," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 23, no. 10, pp. 2162–2172, Oct. 2015.
[8] Y. Doröz, E. Öztürk, and B. Sunar, "A million-bit multiplier architecture for fully homomorphic encryption," J. Microprocessors Microsyst., vol. 38, no. 8, pp. 766–775, Nov. 2014.
[9] W. Wang, X. Huang, N. Emmart, and C. Weems, "VLSI design of a large-number multiplier for fully homomorphic encryption," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 22, no. 9, pp. 1879–1887, Sep. 2014.
[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