International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Design a High Speed Error Prediction AES Algorithm

[1] DOPPALAPUDI. SRAVYA, [2] NELAM RAJAKUMARI
[1]M.tech-Scholar, Dept of ECE, Malineni Perumallu Educational Society's Group Of Institutions, Guntur, India
[2]Assistant Professor, Dept of ECE, Malineni Perumallu Educational Society's Group Of Institutions, Guntur, India

ABSTRACT: The main intent of this paper is to develop a hard drive security using Advanced Encryption Standard (AES). This method will authenticate and protect the content of hard drive security from legal use. Here the both error correction and encryption methods are handled independently and they are evaluated in binary noise removal in channel type. The proposed method is labelled as disk trust and it consists of two technologies which builds the cost effective solution for small scale applications. At last the hard drive security using AES is evaluated on set of data files with different key sizes and the results are employed using encryption and decryption systems. In this paper we present a high-performance, high throughput, and area efficient architecture for the VLSI implementation of the AES algorithm. The subkeys, required for each round of the AES algorithm, are generated in real-time by the key-scheduler module by expanding the initial secret key, thus reducing the amount of storage for buffering.

Key words: AES, Sub bytes, Shift Rows, Mix Columns, S-box.

I.INTRODUCTION

The internet plays a key role in day-to-day life. The people can transfer important data through the internet such as Email, banking transaction and online purchase. In order to acquire secured transaction, network security is most essential. Network security is mostly achieved through the cryptography. Cryptography refers to the art and science of transforming the message to provide them with secure and immune to attacks. Different algorithms and protocols are utilized to protect the data. In this paper, AES algorithm is implemented. AES is a cryptographic algorithm that is utilized for protecting electronic data or information. AES is a symmetric algorithm which process 128 bit stream in 10 rounds. It uses same key for encryption information. The AES algorithm input is applied, to perform number 10 rounds transformation and finally cipher is generated.

Millions of users interchange their information in different fields, like medical reports and bank services, financial and legal files via Internet. A cryptography technique is especially applicable and plays a major role for secure the data. This implementation will be useful in wireless security such as military communication and mobile telephony where there is a greater emphasis on the speed of communication. AES can be implemented in software or hardware. The hardware implementation is more suitable for high speed applications in real time. From last several years, Data Encryption Standard (DES) had been utilized as a cryptographic algorithm. DES is replaced by the Rijndael algorithm due to its short key length. A standard algorithm in the cryptography domain is Advanced Encryption Standard (AES).

II.EXISTED SYSTEM

AES Advanced Encryption algorithm has excellent cryptographic properties, which employs symmetrical structure to resist all known attacks. The algorithm has fast speed of encryption and decryption and strong anti-attack capability. As the only one non-linear element of high decryption algorithm, the S box determines the encryption strength and decryption speed of the algorithm. In addition to good cryptographic properties, a good S-box also has little hardware resources consumption.

The number of S box used in the block ciphers is more, the nonlinearity of the cryptographic algorithms is higher, and the confusion of the cipher algorithm is stronger. In fact, the bigger S box, which is used in the hardware structure, the calculation, check list and storage are also required more time and space.

In this case, the algorithm becomes very low efficient. So how choose a good S-box, we need to consider the security of algorithm and the work efficiency of implementation. The traditional method generates the S box, which has a good index of cryptography. However, it is difficult to use pure logic hardware implementation consuming a large number of logic units. What's worse, the use of look-up table costs too much memory resource. Ideally, the method needs 16 clock cycles to complete the transformation, which is not conductive to the high-speed implementation of encryption system.

III.PROPOSED SYSTEM

The Advanced Encryption Standard (AES) is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world for sensitive data encryption.

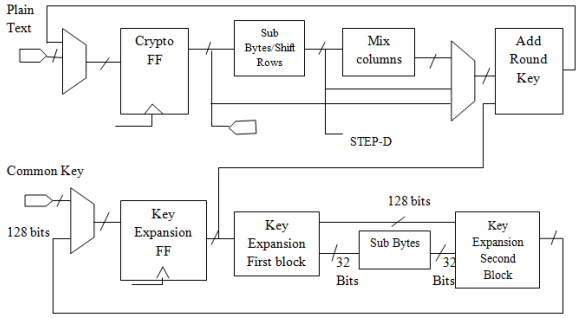

FIG 1. PROPOSED SYSTEM

AES is actually, three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits and 256 bits, respectively. In Advanced encryption standard there are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys

Each round in encryption process further follows some steps to complete each round till n. Each round possess four rounds.

1. Sub bytes

2. Shift rows

3. Mix column

4. Add round key

A. Substitution round: In this step, Sub-Bytes are byte-by-byte substituted during the forward encryption process.

B. Shift Rows: In this step, shifting the rows of the state array during the forward process(S-Box process)

C. Mix Column: Mix Columns for mixing up of the bytes in each column separately during the forward process.

D. Add Round Key: In this step, round key is added to the output of the previous step during the forward process. This step differs from others because of key size difference.

AES is one of the 128-bit symmetric key cryptosystems and composed of the five sub processes called Add Round key, Sub bytes, Shift Rows, Mix columns and Key expansion. Figure 1 shows an AES circuit in which every sub-process corresponds to a circuit module. Note that the Shift Rows module can be merged into the Sub Bytes module and thus we make a single module for them. Key-expansion sub-process is partitioned into the two modules, the Key Expansion (first block) module and Key Expansion (second block) module.

In this AES circuit, for given a plain text, Sub Bytes, Shift Rows, Mix Columns and Add Round Key modules are repeatedly used to generate a cipher text. At that time, a secret key is given by using the Key Expansion and Sub Bytes modules. The AES circuit without inserting Suspicious Timing Error Prediction Circuit (STEPC) generates a cipher text in 14 clock cycles.

Now we insert STEPCs into the AES circuit. Here STEPCs are incorporated into the inter-module connections between the Sub Bytes/ Shift Rows module and Mix Columns module and also between the Sub Bytes module and Key Expansion (second block) module.

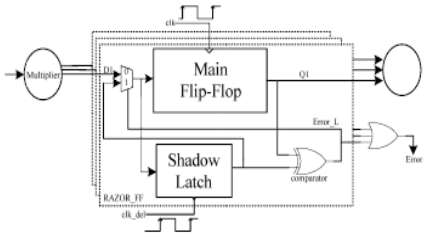

FIG 2. RAZOR FLIP-FLOPS

A 1-bit Razor flip-flop contains a main flip-flop, shadow latch, XOR gate, and mux. The shadow latch catches the execution result using a delayed clock signal, which is slower than the normal clock signal and the main flip-flop catches the execution result for the combination circuit using a normal clock signal. The path delay of the current operation exceeds the cycle period, and the main flip-flop catches an incorrect result if the latched bit of the shadow latch is different from that of the main flip-flop.

To notify the system the Razor flip-flop will set the error signal to 1 to re execute the operation if any errors occur and notify the AHL circuit that an error has occurred. To detect whether an operation that is considered to be a one-cycle pattern can really finish in a cycle we utilize Razor flip-flops. If not the operation is re-executed with two cycles. Although the re-execution may seem costly, because the re-execution frequency is low the overall cost is low.

IV. RESULTS

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

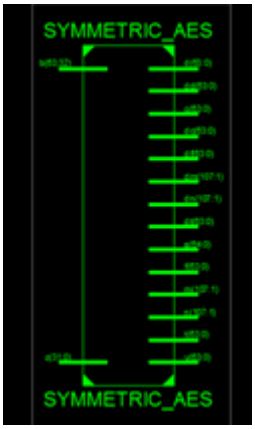

FIG 3. RTL SCHEMATIC

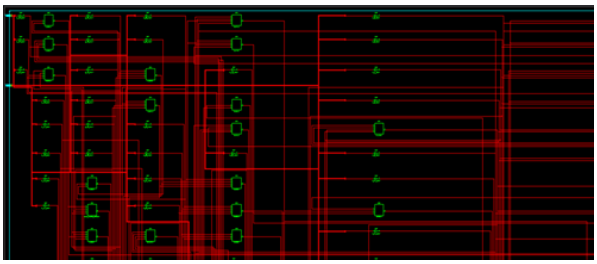

FIG 4. TECHNOLOGY SCHEMATIC

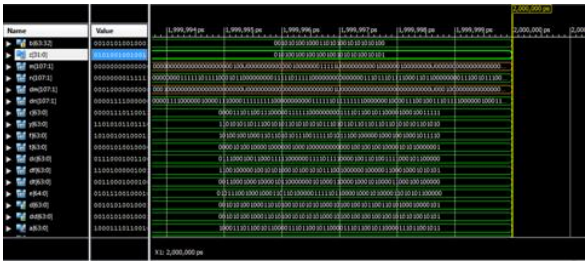

FIG 5. OUTPUT

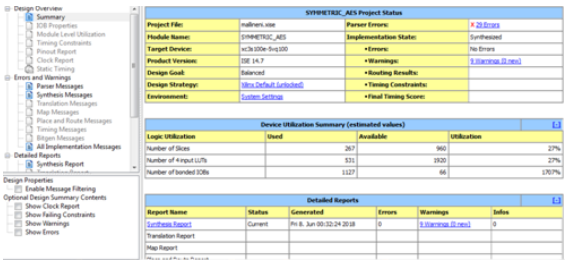

FIG 6. REPORT

V. CONCLUSION

Firstly, understanding the concept of cryptology and flow of AES algorithm is done. Successful implementation of AES algorithm, make to know one of the encryption and decryption standard available in market and it helps to explore the path to implement such an algorithm using VHDL. Mainly, the concept of instantiation and arrays plays a major part in implementation. This is a 128-bit Key dependent algorithm which has control over the 128-bit input data or plaintext. The original message is taken to 10 round operations which produces the ciphertext. So, we provide the high security using aes in communication.

VI. REFERENCES

[1] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, “A DCT Domain Visible Watermarking Technique for Images,” in Proc of the IEEE International Conf on Multimedia and Expo, 2000, pp. 1029–1032.

[2] M. S. Kankanhalli and T. T. Guan, “Compressed-Domain Scrambler Descrambler for Digital Video,” IEEE Transactions on Consumer Electronics, vol. 48, no. 2, pp. 356–365, May 2002.

[3] B. M. Macq and J. J. Quisquater, “Cryptography for Digital TV Broadcasting,” Proceedings of the IEEE, vol. 83, no. 6, pp. 944–957, Jun 1995.

[4] H. Kuo and I. Verbauwhede, “Architectural Optimization for a 1.82 Gbits/sec VLSI Implementation of the AES Rijndael Algorithm,” in Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, 2001, vol. 2162, pp. 51–64.

[5] M. McLoone and J. V. McCanny, “Rijndael FPGA Implementation Utilizing Look-up Tables,” in Proceedings of the IEEE

Workshop on Signal Processing Systems, 2001, pp. 349–360.
[6] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A Compact Rijndael Hardware Architecture with S-Box Optimization," in Proceedings of Advances in Cryptology - ASIACRYPT 2001, 2001, pp. 171–184.
[7] S. Mangard, M. Aigner, and S. Dominikus, "A Highly Regular and Scalable AES Hardware Architecture," IEEE Transactions on Computers, vol. 52, no. 4, pp. 483–491, April 2003.
[8] T. Sodon O. J. Hernandez and M. Adel, "Low-Cost Advanced Encryption Standard (AES) VLSI Architecture: A Minimalist Bit-Serial Approach," in Proc of IEEE Southeast Conference, 2005, pp. 121–125.

DOPPALAPUDI. SRAVYA completed her B.Tech in NRI Institute of Technology, Guntur and pursuing M.Tech in Malineni Perumallu Educational Society's Group of Institutions, Guntur. Her specialization is in VLSI Design.

NELAM RAJAKUMARI completed her B.Tech in Sri Chundi Ranganayakulu Engineering College, chilakaluripeta, Guntur. She completed her M.Tech in QIS College of Engineering, Ongole. At present she is working as assistant professor in Malineni Perumallu Educational Society's Group Of Institutions, Guntur. She has 3 years of teaching experience.