Enhancing Security of Text using Modified Encryption Algorithm

Shweta Sharma*1, Meghana A. Hasamnis*2
*1 M. Tech. (VLSI Design), Research Scholar
*2 Professor, Department of Electronics Engineering
Shri Ramdeobaba College of Engineering and Management, Nagpur 440013, India

Abstract— Due to growth in the use of internet, cell phones, multimedia technology, data security is the most critical problem. Data can be Text, Image, voice message, video etc. It is vital to provide security to secure confidential data while transmitting to protect information by various attacks like brute force attacks. This security to multimedia is achieved by cryptography. Cryptography is a technique of providing security to data by encryption process.

Advanced Encryption Standard (AES) which is symmetric algorithm is used for encryption and decryption of Text. Performance of Advanced Encryption Standard algorithm is further enhanced by adding a key stream generator RC4 stream cipher. AES characteristics are its security and its resistance against attacks and the major characteristic of RC4 is its speed.

In this paper two above algorithms are combined and various approaches are suggested to provide additional security, as combination of both the ciphers is more secure than the original ciphers.

Platform is generated using single core Microblaze soft core processor and the proposed combination of AES and RC4 algorithm are implemented on the developed platform which enhances the security of the data.

Keywords—Advanced Encryption Standard, RC4 Algorithm, Stream Cipher, Microblaze, Atlys FPGA board.

I. INTRODUCTION

Increasing growth of multimedia, the security problem arises from various attacks like Brute force attack. Cryptography comes into picture to provide security to data, Images, multimedia. Cryptography is a science which provide end to end security consisting of encryption and decryption whether by using public key or private key. Cryptography can be classified as Secret key/symmetric key and Public key/Asymmetric key. Whereas symmetric key is categorised into Stream cipher and Block cipher.

Stream cipher uses data byte by byte whereas block cipher uses complete block and key for complete block remains same. Stream cipher are much faster as compare to stream cipher because it encrypts and decrypt data independently. The RC4 is synchronous stream cipher optimized for efficient hardware implementation at very high data rates.

Microblaze is a 32-bit RISC Harvard architecture softcore processor with a valuable instruction set optimized for embedded applications. Microblaze soft processor has bus support PLB, OPB, FSL, LMB, AXI. And Microblaze is a commercial processor. Microblaze soft core processor is used for implementation [13].

Combination of AES and RC4 stream cipher is used to provide extra security with different approaches. 128-bit input data is given as input to RC4 XORed with Pseudo random key and give ciphered output. The ciphered output of RC4 is taken as key to AES encryption which will be XORed with plain data and generate ciphered text. In decryption the ciphered data is XORed with the same key as used during encryption and generate the 128bits-plain data then this data is decrypted by RC4 decrypt. The complete encryption and decryption process is implemented using Microblaze soft core processor.

II. ALGORITHMS

A. Advanced Encryption Standard

AES generally uses key size of 128, 192, 256 bits. For every different key size rounds(Nr) are different like 10, 12, 14 rounds for 128, 192, 256 bits respectively. Whereas block size (Nb) is same for all key size. AES with 128bits is used in modified proposed AES Algorithm.

Generally, AES operations are AddRoundKey, SubBytes, ShiftRows and MixColumns. Respective inverse operations: InvAddRoundKey, InvSubBytes, InvMixColumns and InvShiftRows are performed in order to decrypt the data [1].

i) SubBytes Operation: - In subBytes operation every byte is replaced by S-Box (Replacement Box) first hexadecimal value is represent in X-co-ordinate whereas in second hexadecimal value corresponds to Y-co-ordinate accordingly reverse in decryption (InvSubByte).

ii) Shift Rows Operation: - In Shift Rows operation every state is shifted towards left
and the result is replaced by row number for example 1\textsuperscript{st} row is shifted towards left by 1, 2\textsuperscript{nd} row is shifted by 2 and so on.

\textbf{iii) MixColumns Operation:} - The state bytes behave like Galois Field algebra (GF) [2]. Every column of state is multiplied by GF polynomial column and replaced by the result.

\textbf{iv) ADDRound Key operation:} - In this operation XORING of state and round key is performed which is generated in every round. ADDRound Key operation is performing in both encryption and decryption.

\textbf{v) Key Expansion:} - It is consisting of three operations, in first operation The key matrix is circularly shifted by 1 and so on. In second operation in input word each word is replaced as per S-Box. In last operation XOR is perform between round constant values of every round. The complete structure of AES Algorithm is shown in Fig.1[8]

![Fig.1. Design flow of AES Algorithm](image)

During Decryption reversible process of Encryption is Performed with the identical key used during encryption.

\textbf{Stream Cipher:} - Cryptography is classified either as Block or Stream ciphers. Block ciphers are basically memoryless algorithms it permutes N blocks of plain text and generated N blocks cipher text using N-keys. Whereas stream cipher is consisting of internal states and typically serially operates generating the stream having pseudorandom key bits or key stream, the generated keystream is XORED with data to be encrypted or decrypted.

\textbf{B. RC4 Stream Cipher}

For RSA Data security, Incorporation Ron Rivest invented a varied key size RC4 in 1987. Varied key size, byte-oriented cipher that is it usually uses 64 bit and 128-bit key sizes.

The RC4 works in two Phase-

\textbf{I. Key Setup and}

\textbf{II. Key Generator}

For every new key both phase is performed [4]

![Fig.2. Flow chart of RC4[2]](image)

To engender an encryption variable Key Setup for n bit the encryption using two arrays (State), the Key array n-number of mixing operations uses an n-bit Key setup. There are two 256 byte arrays in S-Box and K-Box. S-box is linearly filled like S0=0, S1=1, S2=2 and so on…, whereas K-box composed of key which is filled by order of occurrences in array. RC4 uses two counters- i and j, which are initialized to zero.

RC4 is usually consists of 2 parts:

\textbf{i) Key Scheduling Algorithm (KSA)}

\textbf{ii) Pseudo-Random Generation Algorithm (PRGA) Generate keystream and Xor keystream with the data to generated encrypted stream.}

During Decryption RC4 cipher uses the same secret key as during the encryption phase. It Engender keystream by running the KSA and PRGA. XOR operation of keystream with the encrypted text to engender the plain text. Its logic is simple

\[(A \text{ xor } B) \text{ xor } B = A\]
A = Plain Text or Data
B = Key Stream

RC4 cipher claimed secure against known attacks. Since RC4 is a stream cipher, must never reuse a key. So it’s provide an additional security by providing pseudo generated key.

III. PROPOSED WORK
To provide additional security combination of RC4 cipher and AES Algorithm is proposed. As RC4 cipher is stream cipher it generates pseudo random key which will provide extra security. 128 bit RC4 algorithm generated ciphered output is given as input to AES algorithm where output of RC4 is given as key to AES which will XORed with plaintext and generate encrypted data.

**Fig.3 Block Diagram of Proposed modified AES Encryption Algorithm**

Different approaches of modified AES algorithm
RC4 combined with AES is expected to create a secure algorithm. RC4 can be combined with AES in various ways.

a) **The output of RC4 is used as plaintext in AES**

RC4 output is given to AES as an input. Thus the generated cipher text by RC4 will be plaintext for AES. In decrypt the cipher text reverse procedure is perform it uses AES decryption 1st and generated output to RC4 and generate the initial plaintext. advantage of this is if AES is wrecked, the plaintext cannot be recovered as there is another layer of security to RC4.

b) **RC4 output is given to AES as a key to AES**

RC4 produces a random looking ciphertext as its output which becomes a key in AES operations. Here, the plaintext is what is given as a plaintext in AES and the ciphertext is AES output. For decryption reverse the process. Use AES decryption with the RC4 output as the key. The output generated will be the initial plaintext.

The advantage here is that even if AES is broken, the key remains unknown as the pseudo key (the output of RC4) is attacked and the actual key remains safe.

c) **The output of AES is used as plaintext in RC4**

The output of AES is used as plaintext in RC4 in a similar way as done in RC4 and AES.

d) **AES output is given to RC4 as a key to RC4**

Output of AES is given here as a key to RC4 cipher which will be XORed with plain text of RC4.

IV. IMPLEMENTATION AND RESULTS
The system is generated using Microblaze soft core processor using Xilinx system [1]. The system generated is compiled in Atlys FPGA board Spartan-6-XC6SLX45[14]. The single core system works on 50MHz frequency.

a) **Output of RC4 is used as plaintext in AES**

RC4 output is taken as a plain text to AES with AES key it generates the cipher text.

b) **RC4 output is given to AES as a key to AES**

Output of RC4 that is cipher text of 128 bits is treated as key and xorred with plain text and generate cipher text.
c) AES output is used as a plain text in RC4

AES output 128 bits cipher text is given as key to RC4 and generate cipher text of 128 bits.

d) AES output is given to RC4 as a key to RC4

AES output that is 128 bits’ cipher text is serve as key to RC4 stream cipher and generate the cipher text of 128 bits.

AES Algorithm is implemented in Microblaze platform and CPU Clock Cycles of encryption and decryption is found to be 22623 cycles for encryption and decryption. RC4 is implemented on the same platform and for encryption it takes 709 Cycles and for decryption it takes 714 Cycles. Various approaches which are described above are implemented in same platform with 22657 cycles. From this it can clearly conclude that RC4 is much quicker than AES Algorithm. The CPU Clock Cycle

Graph below shows CPU Clock Cycle of RC4, AES, combination of RC4 and AES.

Fig.4 CPU Clock Cycle of Cipher

The Key stream generator RC4 is designed using C language and verified as plain text of encryption is identical to ciphered text of decryption. It is then included in the encryption code of AES to further enhance the encryption performance. Implementation done without the RC4 cipher was found to have some noise. So in order to add additional security AES encryption algorithm is implemented with the RC4 cipher.

C. CONCLUSION

Proposed AES encryption and decryption algorithm is designed and implemented on the single core Microblaze system on Atlys FPGA board. Proposed AES algorithm offers high security, and high speed. The key stream generator RC4 has an important influence on the encryption performance. The
features of both AES and RC4 ciphers are studied and a new cipher uniting the characteristics of both the ciphers is generated which is more secure than the original ciphers. AES characteristics are its security and its resistance against attacks and the major characteristic of RC4 is its speed. Text obtained after decryption using RC4 possess better security and highly enhanced throughput.

REFERENCES