MAES BASE EFFICIENT ARCHITECTURE FOR REAL TIME AUDIO

Neel Khatri [1], Nandlal Dhandhukia [2]

[1] *M.E. Student, VLSI and Embedded System Design, GTU PG School, Ahmedabad, Gujarat, India.*
[2] *Assistant Professor, Head of ECE Department, Laxmi Institute of Technology, Sarigam, Gujarat, India.*

ABSTRACT

During the last decades, information security has become a major issue. Cryptography is playing major role in information and security division. The main aim of the cryptography is to protect the data from unauthorized users or hackers. The concept of cryptography consists of two parts, one is encryption and another decryption. Encryption is a process of converting the plain text to cipher text using some keys. Decryption is a process of converting the cipher text to plain text using the keys. Encrypting and decrypting data have recently been widely investigated and developed because there is a demand for a stronger encryption and decryption which ensures privacy and practically very hard to crack. Cryptography plays major role in fulfilment of these demands. There are several algorithms in cryptography to encode and decode the data based on the key. These algorithms are useful in transmission of messages and data between one user and another. Taking a real time voice as input and it gives to the audio code 97 and the output of this audio codec gives to the FPGA kit. In this kit perform two process encryption and decryption. Here we used MAES algorithm for encryption and the decrypted voice is given to the audio codec 97 and at last we get original voice through output speaker.

Keyword: - *Cryptography, Encryption, Decryption and MAES*

1. INTRODUCTION

In today’s internet world the data transmission should be fast and secured. The secret signal data may get hacked by breaking the password assigns to the system. Thus it is very important designing a robust encrypted method for perfect data security. Many public places such as Banking sectors, Share markets, Educational sectors, IT industries, Government sectors and Medical sectors required secured secret data transmission. There are many software’s developed by the hackers to attack on any weak secret key (password). It means only user ID and password are not enough to protect the secret data. The confidential data must be saved in the encrypted form. There are two types of cryptography algorithm a. symmetric-key cryptography used for the encryption process in which sender and receiver uses the secret key b. Public-key cryptography used where the different keys are used for encryption and decryption [3]. Cryptography is the study of Secret (crypto) -Writing (graphy). It is the science or art of encompassing the principles and methods of transforming an intelligible message into one that is intelligible and then transforming the message back to its original form [1**].**

1.1 Difference between Cryptography and Steganography

Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world.

Table -1: Comparison between Cryptography and Steganography

Topics	Steganography	Cryptography
Techniques	LSB, Spatial Domain	Transposition, Substitution, RSA
Capacity	Differ as different technology Usually low hiding capacity.	Capacity is so high, but as message is long it chances to be decrypt.
Detection	Not easy to detect because to find Steganography image is hard.	Not easy to detect, depend on technology used.
Applicability	Universally	Universally
Robust	Yes	Yes

1.2 Types of Cryptography

1. DES: DES is a block cipher based encryption and decryption process. The key is 56bits in length, which is divided into 16 sub keys for 16 rounds of processing; each one is used for each round. Decryption is same as encryption where cipher text is used as input to DES and sub-keys Ki are used in reverse order i.e. from K16 in fast round to K1 in last round [8].
2. 3DES: TDES (Triple Data Encryption Standard) applies three times the DES encoding and decoding algorithms, with a larger key, of 128 bits and it is more robust than its predecessor [10].
3. AES: Both DES and 3DES are not good candidates for long term security, NIST in 1997issues a call for proposals for a new Advanced Encryption Standard. AES uses block length of 128 bits and a key length that can be 128, 192 or 256 bits [8].
4. Blowfish: It is Block cipher based encryption algorithm provided by Bruce Schneider in 1993. It has variable length key ranging from 32 bits to 448 bits and block size of 64 bits. The algorithm operates with two parts: a key expansion part and a data encryption part. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays to taling 4168 bytes. All operations are EX-ORs and additions on 32-bit words. Blowfish is successor to Twofish. It suffers from week key problems. So some attacks are possible against it [9].
5. RC4: It is a variable key-size stream cipher with byte-oriented operations. Stream ciphers are more efficient for real time processing. It is simple and quite easy to explain. RC4 was kept as a trade secret by RSA Security. But in September 1994, the RC4 algorithm was posted on the Internet on the Cypherpunks anonymous remailers list. The algorithm can be efficiently implemented in both hardware and software [8].
6. Twofish: Twofish is an algorithm from counterpane Internet Security. It is highly suited for large microprocessors and also for smart card microprocessors. Twofish was designed to meet NIST's design criteria for AES. It is based on Feistel network. Specifically, they are a 128-bit symmetric block cipher with key lengths of 128 bits, 192 bits, and 256 bits [8].
7. Threefish: It is defined for three block sizes: 256, 512, and 1024 bits. The key size is equal to the block size while the tweak value is 128 bits regardless of the block size. Instead of S-boxes, Threefish uses XOR and modulus addition to achieve non-linearity and hence good security. It is also suitable for hardware and software implementations especially in 64-bit platforms since it operates on words of 64-bit size [8].

2. MODIFIED AES

Modified-AES algorithm is a fast lightweight encryption algorithm for security of multimedia data. To overcome the problem of high calculation and computational overhead, we analyze the Advanced Encryption Standard (AES) and modify it, to reduce the calculation of algorithm and for improving the encryption performance. So we develop and implement a modified AES based Algorithm for all kind of data. The basic aim to modify AES is to provide less computation and better security for data. The modify AES algorithm adjusts to provide better encryption speed. In Modified-AES the block length and the key length are specified according to AES.

The four different stages that we use for Modified-AES Algorithm are

1. Substitution bytes
2. ShiftRows
3. Permutation
4. AddRoundKey

Substitution Bytes, ShiftRows and AddRoundKey remain unaffected as it is in the AES. Here the important function is Permutation which is used instead of Mixcolumn. These rounds are managed by the IP table. Permutation is widely used in cryptographic algorithms. Permutation operations are interesting and important from both cryptographic and architectural points of view. The DES algorithm will provide us permutation tables. The inputs to the IP table consist of 128 bits. Modified-AES algorithm takes 128 bits as input. The functions Substitution Bytes and ShiftRows are also interpreted as 128 bits whereas the Permutation function also takes 128 bits [7].

3. BLOCK DIAGRAM

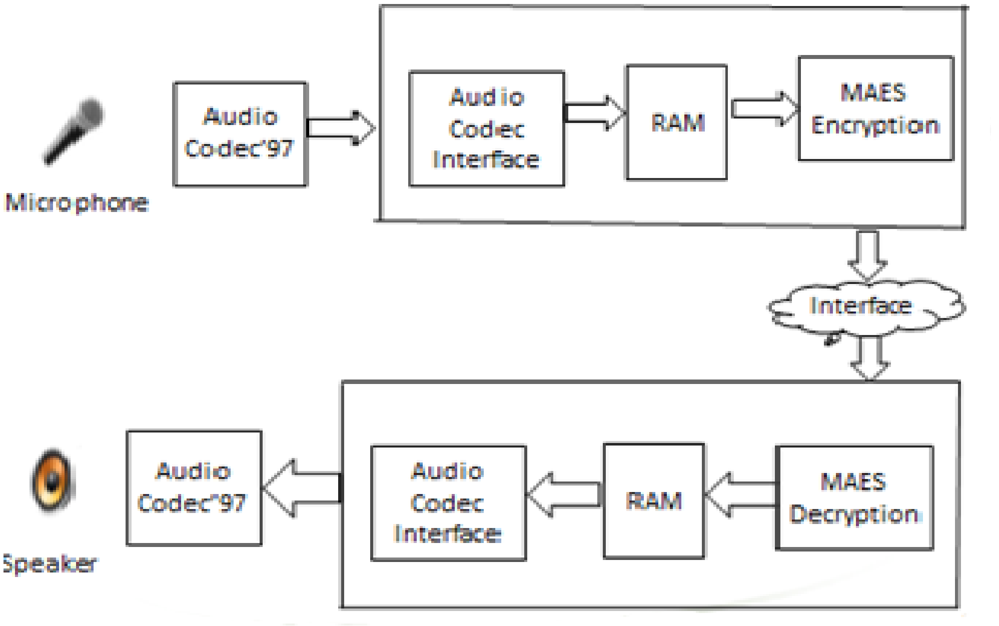
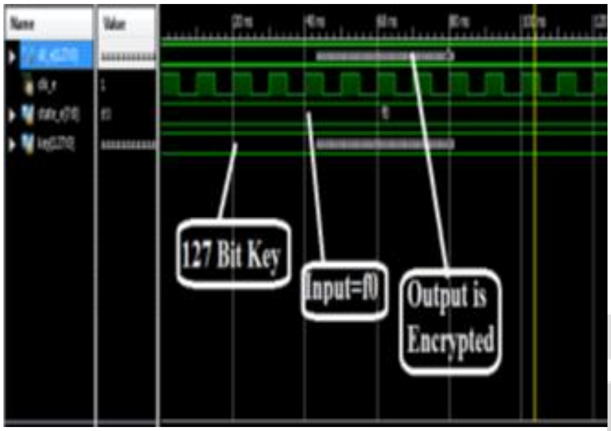


Fig -1: Project Block Diagram

4. SIMULATION RESULT

Simulation results of some of the important modules are given below.

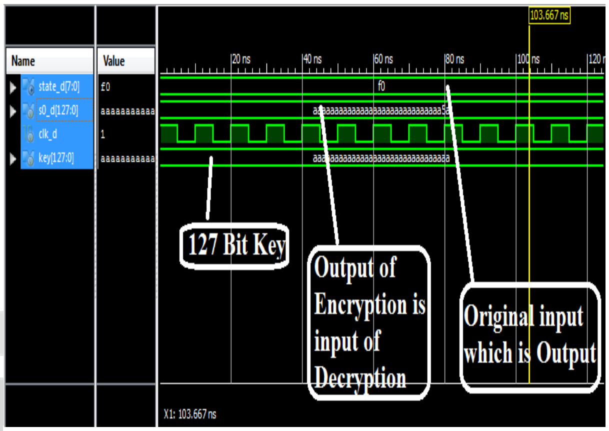


127 Bit Key

Input=f0

Output is Encrypted

Fig -2: MAES Encryption Waveform

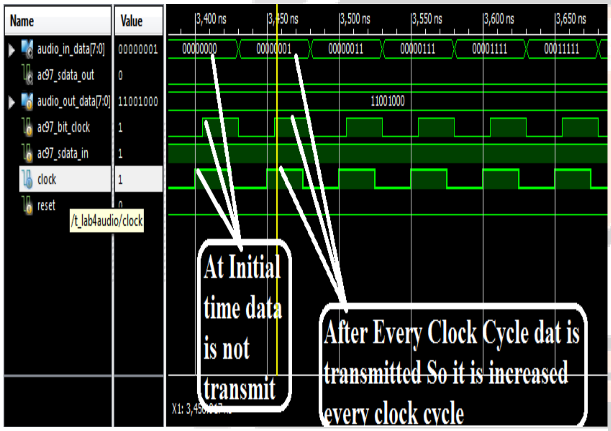


127 Bit Key

Output of Encryption is input of Decryption

Original input which is Output

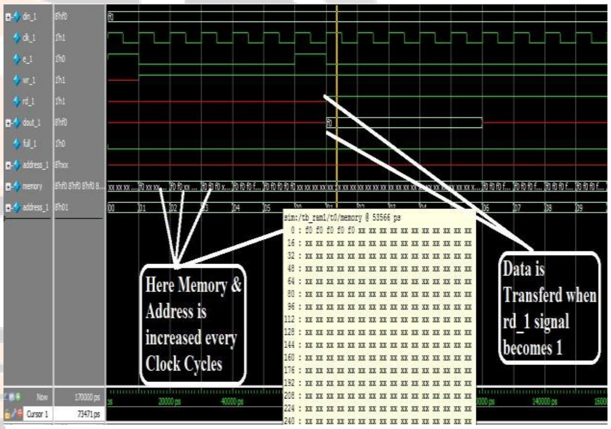
Fig -3: MAES Decryption Waveform



At Initial time data is not transmit

After Every Clock Cycle dat is transmitted So it is increased every clock cycle

Fig -4: Waveform of AC'97



Here Memory & Address is increased every Clock Cycles

Data is Transferd when rd_1 signal becomes 1

Fig -5: RAM Waveform

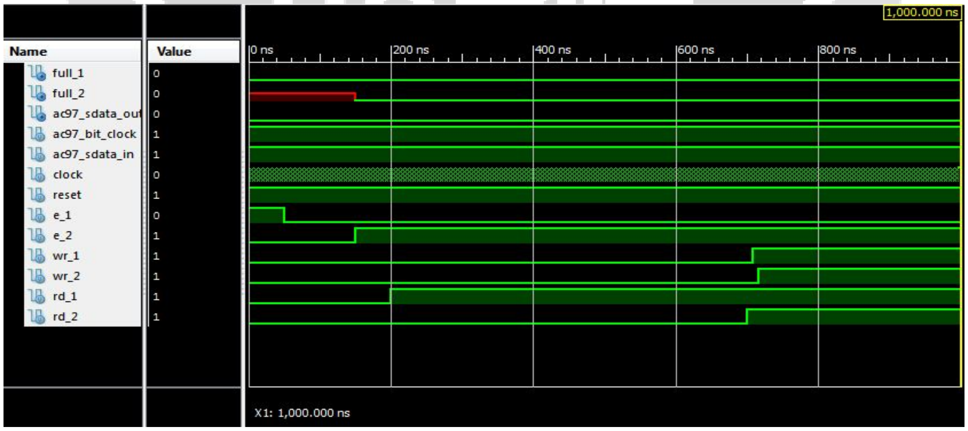


Fig -6: Top Module Waveform

4. CONCLUSIONS

Usually Encyption Algorithm are very useful for multimedia application.I achieved through research a fast effective encryption and decryption algorithm for secure audio signal. Using MAES get more secure output compare to AES. MAES for Audio use in many real time application in commercial and digital multimedia world.

5. REFERENCES

[1]. Anju, Babita, Reena and Ayushi Aggarwal "An Approach to Improve the Data Security usingEncryption and Decryption Technique International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 3, Number 3 (2013), pp. 125-130.
[2]. Dr. Mohammad V. Malakooti, Mojtaba Raeisi Nejad Dobuneh "A Lossless Digital EncryptionSystem for Multimedia Using Orthogonal Transforms" Graduate Student of Department ofComputer Engineering, IAU, Dubai, UAE, 2012 IEEE.
[3]. Sheetal A. Kulkarni , Shubhangi B. Patil "A Robust Encryption Method for Speech Data Hiding in Digital Images for Optimized Security", International Conference on Pervasive Computing (ICPC), IEEE.
[4]. Raja Sree. Avirneni, K. Padma Vasavi"A High Speed VLSI Architecture For Digital Speech Watermarking With Compression", International Journal of Electrical and Electronics Engineering (IJEEE),Vol-2, Iss-2,3,4,2012.
[5]. Eashwar Thiagarajan and Madhuri Gourishetty "Study of AES and its Efficient SoftwareImplementation", Department of Electrical Engineering & Computer Science,Oregon StateUniversity, Corvallis, Oregon 97331 -USA.
[6]. Obaida Mohammad Awad Al-Hazaimeh "A New Approach for Complex Encrypting And Decrypting Data International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013.
[7]. Pravin Kawle, Avinash Hiwase, Gautam Bagde, Ekant Tekam, Rahul Kalbande "Modified Advanced Encryption Standard", International Journal of Soft Computing and Engineering (IJSCE), Volume-4, Issue-1, March 2014.
[8]. Rashmi A. Gandhi , Atul M. Gosai "A Study on Current Scenario of Audio Encryption", International Journal of Computer Applications Volume 116 – No. 7, April 2015.
[9]. Mansi,Mrs Raman Chawla "An Audio Multiple Shuffle Encryption Algorithm" International Journal Of Engineering And Computer Science, Volume 4 Issue 9 Sep 2015.
[10]. Luminiţa SCRIPCARIU and Mircea-Daniel Modified Advanced Encryption Standard" 11th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS, Suceava, Romania, May 17-19, 2012.