IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
ISSN: 2319 – 4200, ISBN No. : 2319 – 4197 Volume 1, Issue 5 (Jan. - Feb 2013), PP 44-48
www.iosrjournals.org

A Secure Software Implementation of Nonlinear Advanced Encryption Standard

[1]S.Vinoth John Prakash, [2]A.Arun.ME.,(Ph.D)
[1]PG Scholar Saveetha Engineering College
[2]Associate Professor Saveetha Engineering College

Abstract: *Advanced Encryption Standard algorithm (AES) was introduced to resist classical methods of cryptanalysis (i.e.) from linear or differential attacks. The cryptographic strength of the AES depends strongly depends on the choice of S-box. The result of the new attack methods shows that there may be some lacuna in the design of S-box in AES algorithm. The setback is the weakness of the existing linearity structure in the S-box. After a detail analyze on the AES algorithm and a new performance scheme for rising complication of nonlinear transformation in the structure of S- box is presented. In order to resist from the new attacks and to execute the AES with the protected encryption and decryption by using verilog and to provide a further more protection a Bio-metric scheme has been used in both the encryption and decryption schemes. The result shows that the new nonlinear implementation of the AES S-Box by using Verilog provides enhanced security with good enough speed for encryption and decryption.*
Keywords: *AES, Non-linear S-Box, Bio-metric Image.*

I. Introduction

Network security is becoming more and more important as people spend more time connected. Compromising network security is often much easier than compromising physical or local security, and is much more common. Computer security is a general term that covers a wide area of computing and information processing. Industries that depend on computer systems and networks to conduct daily business transactions and access information regard their data as an important part of their overall assets. It is the process of preventing and detecting unauthorized use of computer. Prevention measures help you to stop unauthorized users from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data. It is expected to become the accepted means of encrypting digital information, including financial, telecommunications, and government data. AES is the successor to the older Data Encryption Standard (DES).

II. Advanced Encryption Standard

AES stands for Advanced Encryption Standard. AES is a symmetric key encryption algorithm which replaces the commonly used Data Encryption Standard (DES). AES provides strong encryption and was selected by NIST as a Federal Information Processing Standard. The AES algorithm uses three key sizes: a 128,192, or 256-bit encryption key. Each Encryption key size causes the algorithm to Behave slightly differently, so the increasing key sizes not only offer a larger number of bits with which you can scramble the data, but also increase the complexity of the cipher algorithm. The AES algorithm has four basic transformations as shown below:

1. Sub Bytes Transformation:
   This operates independently on each byte of the State using a substitution table (Sbox).
2. Shift Rows Transformation:
   Left shift is performed on each row by a certain number of bytes.
3. Mix Columns Transformation:
   Each byte of a column is mapped into a new value that is a function of all four bytes in that column.
4. Add Round Key Transformation:
   The 128 bits of State are bitwise XORed with the 128 bits of the round key

III. Existing System

The security of sensitive Information transmitted via the Internet has been the focus of modem cryptographist's attentions. The Rijndael algorithm was adopted as the Advanced Encryption Standard (AES) by the (NIST). Data Encryption Standard (DES) is the first open encryption algorithm to protect the sensitive

information. However, the shorter length of key, the complementary property and existence of weak and semi weak keys reduce the security of DES; it is to find a stronger encryption algorithm to substitute the DES. The objective in using the AES is to transfer the data so that only the desired receiver with a specific key would be able to retrieve the original data. However, with the existence of malicious injected faults in non secure environments. The existing scheme of the S-box is linear and it is not secure against cryptanalysis. So DES not be secure as proposed system. The key size of the exciting system will not be small which increases the area.

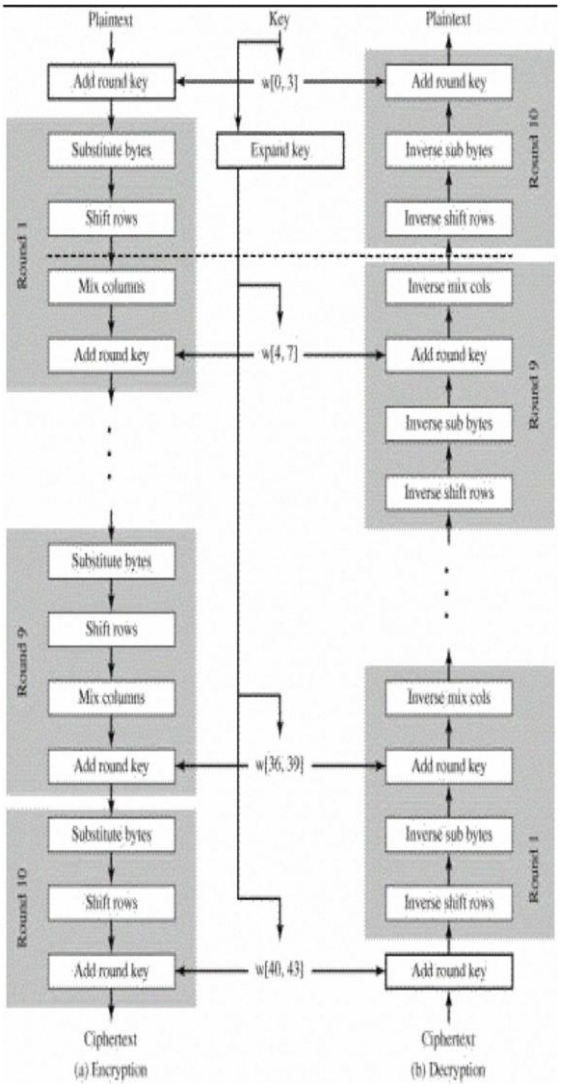

Fig.1.Block diagram of AES Algorithm

IV. Proposed System

Through the research of Rijndael algorithm, we can see that a non-linear layer of S-box transformation is a key to make the entire algorithm strong. It is well known that the cryptographic strength of the AES depends on the choice of the S-box. Many cryptographists have discovered that there is some weakness in the design of the existing S-box. To improve complexity of S-box structure our approach is combining a dynamic nonlinear transformation method and linear function. A good S-box can be very well resist differential cryptanalysis, linear cryptanalysis attacks and so on. The Advanced Encryption Standard (AES) has S-boxes in its Substitution Bytes and Inverse Substitution bytes. To enhance the complexity of the S-Box's structure, the nonlinear and the linear transformations models need to be reconsidered in the design of the S-box.

4.1 Non-Linearity:

In AES, the function of non linearity is achieved by means of the Substitute Bytes step. In the Sub Bytes step, each byte in the array is updated using an 8-bit substitution box, the RijndaeI S-box. S-boxes substitute or transform input bit into output bit. A good S-box will have the property that changing one input bit

will change about half of the output bit. It will also have the property that each of the output bit will depend on every input bit. Here we will design a dynamic S-box that is highly secure to all known attacks. Since nonlinearity is applied to the S-box, the key is also protected. The key could not be known to the attackers due to the dynamic formulation of the s-box. Thus it will provide an enhanced security.

4.2 Biometrics:

Biometrics is slightly different each time they are measured. Therefore they cannot be stored in untreated form as passwords because the unprocessed form of the original biometric and the untreated form of a later measurement of the same biometric would not match. For biometrics to be broadly accepted, it is needed a way to store biometrics in a secure form that cannot be used by an attacker to impersonate a valid user. The nonlinear structure of S-Box provides high security in the encryption and decryption process but to improve authentication we go for biometrics. AES Encryption and then the Decryption takes place for the fingerprint to improve the complexity. To make this as a complete application AES cryptography algorithm is combined with biometric authentication scheme.

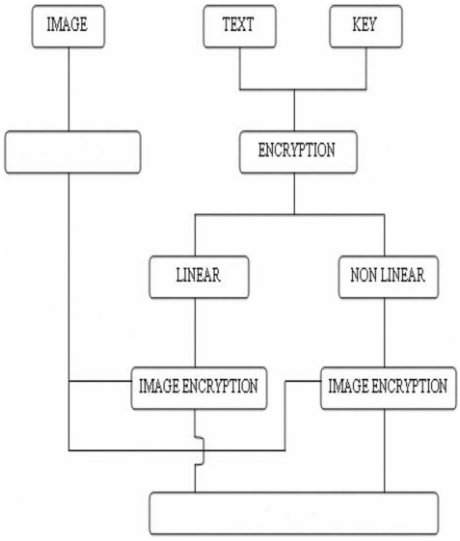

Fig.2. Proposed encryption architecture

V. IMPLEMENTATION

The entire construction is made tough by converting the existing linear structure of the S-box into a nonlinear structure. The nonlinear structure can be achieved by substituting a random hexadecimal number to the actual S-box value. When the real S-box value is called it is mapped to a random hexadecimal number which is generated during the run time of the encryption process by the proposed structure. In the nonlinear implementation three S-Boxes is being used. During encryption, the input value is first mapped to Default S-Box (Pre-defined S-Box), which is the original AES S-Box and this value undergo a XOR process with the new derived S-Box which is the l's complement of the actual S-Box to generate the virtual S-Box. Thus for each different input value the virtual S-Box will be dynamically generated. Similarly for the decryption, the reverse process will take place using the inverse virtual S-Box. During this encryption, the input value will be mapped to the virtually created S-Box then this value will map to the default S Box to produce the encrypted result. During decryption, the input value will be mapped to the default S-Box and then this value will map to the virtually created S-Box to produce the decrypted original result.

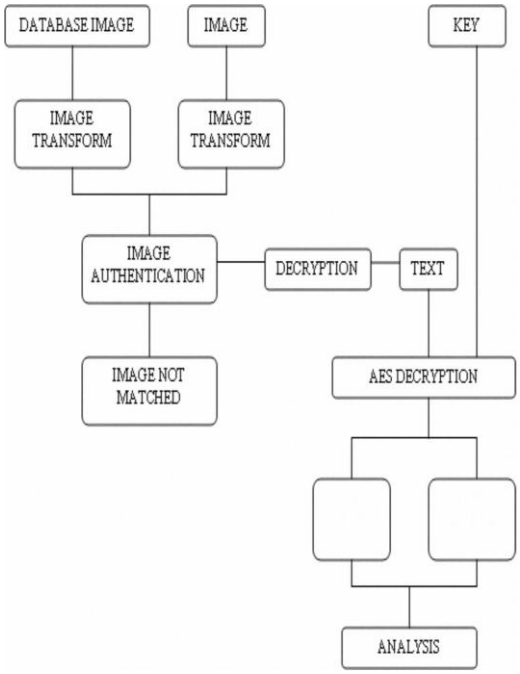

Fig.3.Proposed decryption architecture

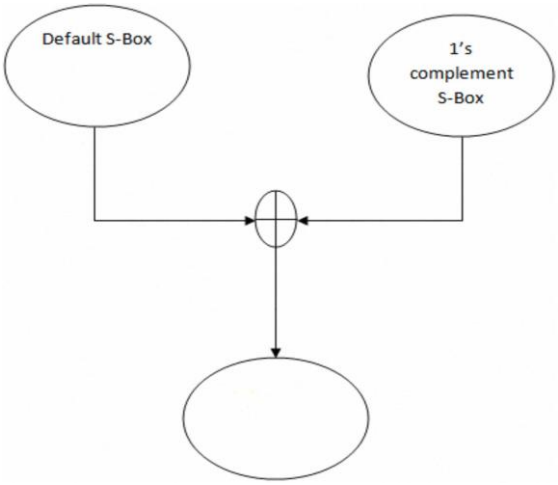

Fig.4.Creation of dynamic S-Box

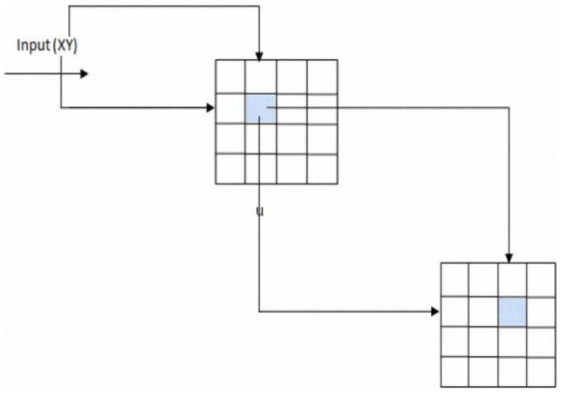

Fig.5.Decryption using Virtual S-Box

In the encryption side, for a given input image, the image transform is done by using the fuzzy vault method in which the rows and columns are interchanged successive times to generate the encrypted image.

In the decryption side, when the user provides the input to the system, it is compared to the finger print image already stored in the database. If both of them match, then authentication is provided and so enters the decryption process.

VI. CONCLUSION

The methods of new attacks well show that the design of S-box has some weaknesses. The principal weakness is the problem of linearity in the S-box and key schedule. It is necessary to improve nonlinear transformations in the design of S-box and key schedule in order to protect from new attacks. Some measures against new attacks were adopted by improving the complexity of nonlinear transformation of S-box in our implementation scheme. This implementation scheme does not affect the originality of the AES algorithm but makes it more non linear and dynamic, thus making it unbreakable. The scheme of Verilog implementation is feasible in the networking environment, and has an acceptable speed of data encryption and decryption. This implementation presents a New nonlinear transformation for AES S-box to enhance the complexity of the S-box structure. The enhanced S-box structure provides a strong and expanded security. The alignment of the biometrics scheme with AES algorithm provides an additional protection in authentication system.

References

[1] National Institute of Standards and Technology (NIST), "Recommendation for Block cipher modes of operation," Dec.2001.
[2] "A New Mutable Nonlinear Transformation Algorithm for S-box" Atsushi WATANABE, Hiroshi HARUKI,Shun SH1MOTOMAI, Takeshi SAITO, Tomoyuki NAGASE
[3] "A Research and Improvement based On Rijndael Algorithm" Van chun, Yanxia GUO
[4] NIST, "Advanced Encryption Standard," FIPS PUB 197, pp. I-51, November 2001
[5] "AES Proposal: Rijndael", Joan Daemen, Vincent Rijmen, Springer- Verlag, Berlin Heidelberg, 2002.
[6] Claude Carlet "Lower bounds on the higher order nonlinearities of Boolean functions and their applications to the inverse function"
[7] Concurrent Structure-Independent Fault Detection Schemes for the Advanced Encryption Standard Mehran Mozaffari- Kermani, and Arash Reyhani-Masoleh.
[8] "Efficient method for simplifYing and approximating the S-boxes based on power functions" by A. F arhadian and M.R. Aref in the year 2009.
[9] "A High speed FGPA implementation of the rinjdael algorithm" by Refik Sever A., Neslin Ismailoglu, Yusuf C.Tekmen, Murat Askar anc Burak Okcan.2004
[10] "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" by Md. Nazrul.