SECURED CRYPTOGRAPHY USING RETINAL IMPLEMENTATION IN VLSI

Yogalakshmi. G
M.Tech VLSI
Sathyabama University
Chennai, India
yogalaksmi2107@gmail.com

Sai Prasanthi. B
M.E. Embedded Systems
Sathyabama University
Chennai, India
prashi.sai17@gmail.com

Shdevi. M
M.E. Embedded Systems
Sathyabama University
Chennai, India
srisai5880@gmail.com

Abstract: In recent days Field-Programmable Gate Arrays (FPGAs) has become a popular tool for the implementations of cryptographic block ciphers, a well-designed FPGA solution can combine some algorithmic flexibility and it is cost efficiency with equivalent software implementation with throughput that can be comparable to custom ASIC designs. In recent days selected Advanced Encryption Standard (AES) is slowly replacing older ciphers as building block of choice for the secure systems and is well suited to an FPGA implementation. Some possible biometric schemes (RETINA) can be used for authentication along with cryptography on networked embedded systems. The Public-key infrastructures are secure, but only to the extent but the private keys of individuals are maintained secret. Usually this involves the securing of the private key(s) using a password, a PIN or a token. The Biometrics themselves cannot provide a higher deal of safety, but its combination will provide a higher degree of security for embedded computing devices. Finally we improve the performance of the proposed system using pipelining technique and the efficiency can be proved through hardware synthesis.

Keywords- Advanced Encryption Standard (AES), fixed hamming-distance-based attack (FHDA), constant based algorithm (CBA), Retina, FPGA, cryptography, private keys

I. INTRODUCTION

In today's digital word, encryption is emerging as a disintegrable part in all communication and information processing systems for protecting and in transition of data. The encryption is transformation of plain data (known as plain text) into unintelligible data (known as cipher text) through this algorithm. There are enormous encryption algorithms that are now commonly used in computation, but the U.S government has declared the advanced encryption standard (AES) to be used by Federal departments and agencies for protecting sensitive information.

Any conventional symmetric cipher such as AES requires a single key for both encryption and decryption, which is independent of the plain text and the cipher itself. It should be impractical to retrieve the plain text depending on the cipher text; the encryption biometrics, in this retinal based advance AES algorithm is proposed key is high importance in symmetric cipher such as AES. In this project we analyse the potential drawbacks of authenticating devices using biometrics, in this retinal based advance AES algorithm is proposed.

These algorithms were subject to further analysis prior to the selection of the best algorithm for the AES. Finally, in October 2000, NIST announced that the Rijndael algorithm won. The Rijndael is specified with key and block sizes with any multiple of 32 bits, and minimum of 128 bits, maximum 256 bits. Therefore, the problem of splitting key becomes more difficult [1]. In cryptography, algorithm AES is also known as Rijndael [2]. AES has a fixed block of size 128 bits and has keys of size 128, 192 or 256 bits.

A. Biometric Authentications

In [3], [4] the general description of biometric system and the types of features used in the security systems. There are systems which are in development today that make use of voice patterns, scanning of iris ,retinal scans, recognition of face, hand geometry pattern, and some dynamic feature biometrics such as gait (i.e., way individual walk) and lip movement when a person speaks a particular

word[5]. Some systems make use of combination of two or more biometrics. Most of the systems use the biometric template for authentication and for identification. To be authenticated a user should first enter a system username, and then submit biometric template to allow the system to compare the new template to that of the stored template. The demanding task is searching a large database to match a template to identify an unknown user. Other key aspect which are common to all biometric systems is access error which are caused due to misreading of the biometric itself. If a biometric information is stolen during transit then the system or the network is subject to attacks.

II. DESCRIPTION OF AES ALGORITHM

The AES algorithm is also called symmetrical block cipher that can perform both encrypt and decrypt information. Encryption converts data to an incomprehensible form called as cipher text. The Decryption of cipher text converts the data back into its original form, which is called as plain-text

A. AES encryption

The AES algorithm operates on 128-bit block of data (text) and are executed in Nr - 1 loop time and the number of iterations of a loop, Nr, can be 10, 12, or 14 depending on the length of key. The key length is 128, 192 or 256 bits in length respectively. The first and the last rounds vary from other rounds and there is an additional Add Round Key transformation in starting of the first round, there is no transformation of mix column is performed in the last round. In this project, we use the length of key as 128 bits as a model for general explanation.

B. The Sub Bytes Transformation

The Sub Bytes transformation is not a linear byte substitution, operating on each of the state of bytes independently. In existing methods the Sub Bytes transformation which are done using a pre- calculated substitution table called as S-box. But here the Sub Byte transformation is computed by using the multiplicative inverse in GF(2^8) followed by an affinitive transformation. For its reverse, the Inverse Sub Byte transformation, the inverse affinitive transformation is applied first prior to computing the multiplicative inverse.

C. Shift Rows Transformation

In Shift Rows transformation, the rows of the state are cyclically left shifted over the different offsets. Row 0 is not being shifted; row 1 is being shifted one byte to the left; row 2 is being shifted two bytes to the left and row 3 is being shifted three bytes to the left.

D. Mix Columns Transformation

In the Mix Columns transformation, columns of the state are considered as polynomials over GF (28) and multiplied by modulo x4 + 1 with a fixed polynomial c(x), given by: $c(x)=\{3\}x^3 + \{1\}x^2 + \{1\}x + \{2\}$.

E. Add Round Key Transformation

In Add Round Key method of transformation, a Round Key is added to the State which is resulted from the operation of the Mix Columns transformation by a simple bitwise XOR operation.

III. THE RETINAL KEY EXTRACTION

The security and testing requirements as mentioned above, a hybrid secured systematic approach is proposed as a counter measure against scan-based differential cryptanalysis.

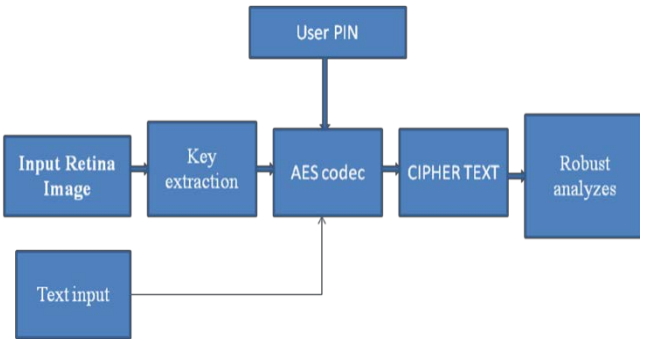


Fig 1. Retinal cryptography architecture

Each and every person has a peculiar set of characteristics that can be used for authentication. Biometrics uses this peculiar method for authentication. Today's Biometric systems examine the retina patterns, Where there is no known way to replicate a retina. The pattern of the blood vessels at the back of eye is unique and stays the same for a lifetime for each person. However, it requires about 15 seconds for careful concentration and to take a good scan. Retina scan remains a standard in military as well as all government installations.

A. Key extraction

The Retinal image is then converted to pixels using MATLAB and their values are stored as text file. The text file is processed by the Models in ALTERA and the respective keys are then calculated. These values are fed to the AES module for transformation which returns the cipher key.

IV. THE SECURITY AND IMPLEMENTATION ANALYSIS

In this section, the security analysis and implementation are discussed to understand the advantages of the proposed secure checking technique over existing methods.

A. Security Analysis

Due to the avalanche effect in cryptographic algorithms, there prevail two kinds of scan-based differential cryptanalysis, called as constant based analysis (CBA) and fixed hamming-distance-based attack (FHDA). Here let us use AES as example for cryptographic algorithm to explain these two kinds of attacks. CBA takes the advantages of the fact are that, in the process of encryption, the contents in some special registers are independent on input applied plaintext. For example, the round registers in AES, without special protection, for each normal input, in the first cycle they would be 0001, then 0010, 1010. By using many different plaintext inputs and scanning out the content at different times of the cryptographic operation, these registors can be easily identified. Then by setting the registers as 1010 (i.e., to indicate that the round cycle 10, and the last round is 128-bit AES), which is because in AES the mix-column operation uses bypass method in last round, it became easier to discover the secret keys. Such attack is called constant based attack. FHDA is another kind of scan- based attack by counting the number of changes in bit on relevant plaintext so as to discover the secret key, and refer [2] for more details on FHDA.

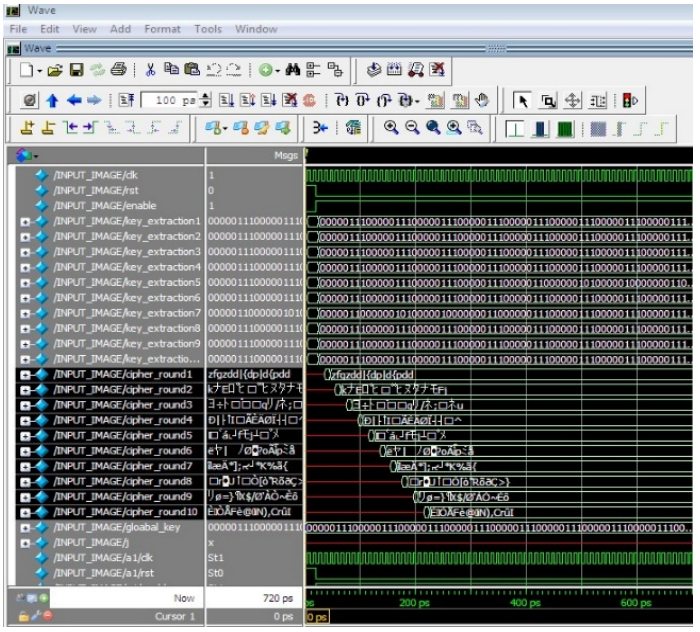
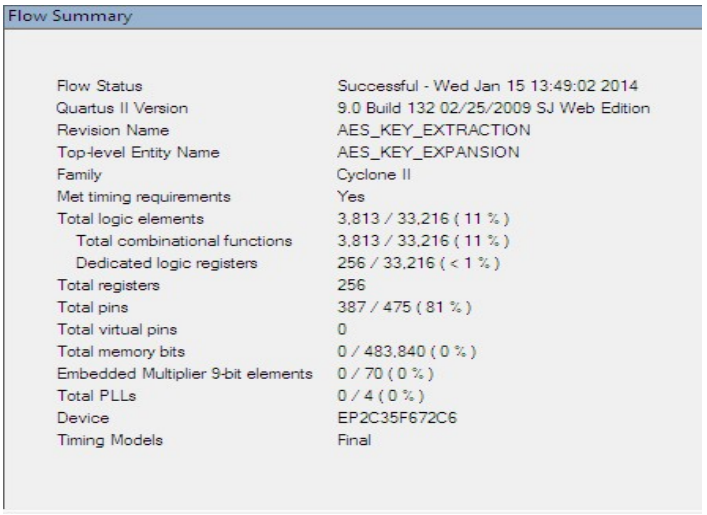


Fig 2. Simulated output.


Flow Summary

Flow Status	Successful - Wed Jan 15 13:49:02 2014
Quartus II Version	9.0 Build 132 02/25/2009 SJ Web Edition
Revision Name	AES_KEY_EXTRACTION
Top-level Entity Name	AES_KEY_EXPANSION
Family	Cyclone II
Met timing requirements	Yes
Total logic elements	3,813 / 33,216 (11 %)
Total combinational functions	3,813 / 33,216 (11 %)
Dedicated logic registers	256 / 33,216 (< 1 %)
Total registers	256
Total pins	387 / 475 (81 %)
Total virtual pins	0
Total memory bits	0 / 483,840 (0 %)
Embedded Multiplier 9-bit elements	0 / 70 (0 %)
Total PLLs	0 / 4 (0 %)
Device	EP2C35F672C6
Timing Models	Final

Fig 3 Area Summary

V. CONCLUSION

In this we have carried out the implementation of AES cryptographic algorithms with scan based testing futures. It has previously demonstrated that the scan chains introduced for the hardware testability opens a back door to the potential attacks. Here, we are proposing a level based masking and RSFF based flip flop masking as a scan-protection scheme that provides the facilities for testability both at production time and over the course of the circuit's life. Compared to regular scan tests, this technique has no effect on the quality of the test or the model based fault diagnosis. Here we prove that RSFF based AES gives better hardware complexity & optimal power with considerable delay enhancement. An accurate SFF-based analytical approach has introduced for AES core with single and multi FF characterizations. The proposed approach was derived from the SFF method. The method avoids the use of a large number of masking parameters to minimize the required resources for area and power efficient built-in testing applications. ModelSim based pre simulation results of an AES implementation showed the feasibility of the approach. For a QUARTUS- II based hardware synthesis report proved the efficiency of proposed method.

FUTURE WORK

Public-key structure are secure, but only to the extent that private keys of individuals are maintained secret. Here are going to describe retinal based cryptogrphy which involves the private key(s) security using a password, a PIN or a token. Biometrics alone cannot provide a great deal of safety, but a combination of biometrics , passwords or PINs and tokens provide a higher degree of security for many computing devices, than passwords or tokens alone. Further, with various level of rounds and random memory location selection based key extraction from biometrics can secure keys with greater confidence and with a higher level of security will be compared to other security mechanisms.

REFERENCES

[1] M.Akkar and C. Giraud, "An Implementation of DES and AES, Secure against Some Attacks," In Proc. of the Workshop on Cryptographic Hardware and on Embedded Systems (CHES2001), Paris, France, pp. 315-325, May 2001.

[2]http://www.altera.com/products/software/products/quartus2/qts-index.html

[3] R. Anderson, E. Biham, and L. Knudsen, "Serpent: A Proposal for the Advanced Encryption Standard," AES algorithm submission, June 1998.

[4] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "Error Analysis and Detection Procedures for Hardware Implementation of Advanced Encryption Standard," IEEE Trans. on Computers, vol. 52, no. 4, pp. 492-505, April 2003.

[5] G. Bertoni, L. Breveglieri, I. Koren, and P. Maistri,"An efficient hardware based fault diagnosis scheme forAES performance and cost "In proc of IEEE international symposium on Defect and fault tolerance in VLSI system(DFT 2004),Cannes,France,pp 130-138,oct 2004

[6] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the Importance of Eliminating Errors in Cryptographic Computations," Journal of Cryptology, vol. 14, no. 2, pp.101-119, 2001.