ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 5, May 2015

A New Robust Scan Technique for Secured Advanced Encryption Standards (AES) Against Differential Cryptanalysis Attacks

Sabna.K.V [1], Vanathi.A [2]

PG Student, Department of Electronics and Communication, GKM College of Engineering and Technology, Chennai[1]
Assistant Professor, Department of Electronics and Communication, GKM College of Engineering and Technology, Chennai[2]

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

Keywords: masking, biometric authentication, key extraction.

I. Introduction

Networked and mobile embedded computing devices like personal digital assistants, and handheld computers are the new face of intelligent computing. These have made information retrieval and delivery effortless. The security of information stored or accessed via such networked devices should be an important consideration, given their ubiquitous nature in today' s society. This pervasive computing architecture should be designed so that entities in the network do not get access to unauthorized information. Therefore we need to renew our concern for the security of networked embedded devices, and develop architectures so that security is inherent. In this project we survey potential drawbacks of authenticating devices using biometrics. In this retinal based advance encryption standard algorithm is proposed.

These algorithms were subject to further analysis prior to the selection of the best algorithm for the AES. Finally, on October 2, 2000, NIST announced that the Rijndael algorithm was the winner. Rijndael can be specified with key and block sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits. Therefore, the problem of breaking the key becomes more difficult [1]. In cryptography, the AES is also known as Rijndael [2]. AES has a fixed block size of 12bits and a key size of 128, 192 or 256 bits.

A. *Biometric Authentications*

In [9],[10] general description of biometrics and the types of biometric features used in security systems. There are systems in use or in development today that make use of voice patterns, iris scans, retinal scans, face recognition, hand geometry, and even dynamic feature biometrics such as gait (how a person walks) and lip movement when a person speaks a particular word. Some systems make use of a combination of two or more biometrics. Most systems use the biometric template for authentication as opposed to identification. To be authenticated a user will first enter a system username, and then submit a biometric template to allow the system to compare the new template to the stored template Another key aspect common to all biometric systems is access error caused by misreading of the biometric itself. If a biometric is stolen in transit then the system or the network is subject to replay attacks.

II. Description Of AES Algorithm

The AES algorithm is a symmetric block cipher that can encrypt and decrypt information. Encryption converts data to an unintelligible form called cipher-text. Decryption of the cipher-text converts the data back into its original form, which is called plain-text.

A. AES encryption

The AES algorithm operates on a 128-bit block of data and executed Nr - 1 loop times. A loop is called a round and the number of iterations of a loop, Nr, can be 10, 12, or 14 depending on the key length. The key length is 128, 192 or 256 bits in length respectively. The first and last rounds differ from other rounds in that there is an additional AddRoundKey transformation at the beginning of the first round and no MixCoulmns transformation is performed in the last round. In this paper, we use the key length of 128 bits (AES-128) as a model for general explanation.

B. Sub Bytes Transformation

The Sub Bytes transformation is a non-linear byte substitution, operating on each of the state bytes independently. In existing methods the Sub Bytes transformation is done using a once-pre calculated substitution table called S-box. But here in this project the Sub Byte transformation is computed by taking the multiplicative inverse in $GF(2^8)$ followed by an affine transformation. For its reverse, the Inv Sub Byte transformation, the inverse affine 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 different offsets. Row 0 is not shifted; row 1 is shifted one byte to the left; row 2 is shifted two bytes to the left and row 3 is shifted three bytes to the left.

D. Mix Columns Transformation

In Mix Columns transformation, the 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: $c(x)=\{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$.

E. Add Round Key Transformation

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

III. Retinal Key Extraction

Due to the security and testability requirements as mentioned above, a novel hybrid secured system approach is proposed as a countermeasure against scan-based differential cryptanalysis.

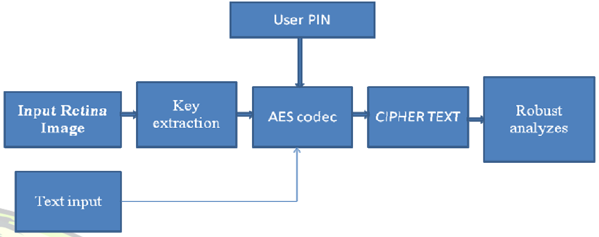


Fig 1. Retinal based cryptography architecture

Each person has a set of unique characteristics that can be used for authentication. Biometrics uses these unique characteristics for authentication. Today's Biometric systems examine retina patterns .When here is no known way to replicate a retina. As far as anyone knows, the pattern of the blood vessels at the back of the eye is unique and stays the same for a lifetime. However, it requires about 15 seconds of careful concentration to take a good scan. Retina scan remains a standard in military and government installations.

A. key extraction

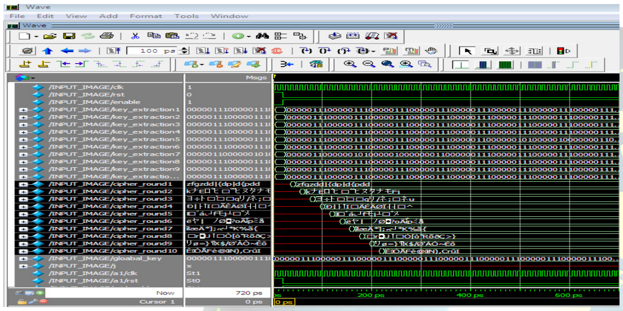
The retinal image is converted into pixels using MATLAB and the values are stored as a text file. The text file is accessed by the Modelsim ALTERA and the corresponding keys are calculated. These values are then fed to the AES transformation module which returns the cipher key.

IV. Security And Implementation Analysis

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

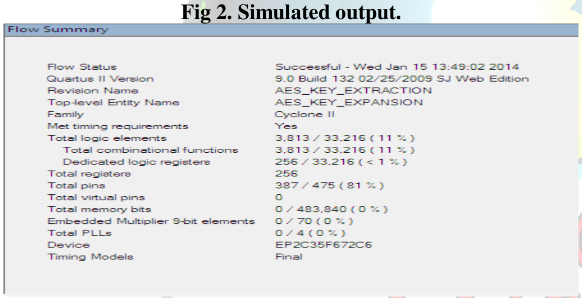
A. Security Analysis

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



```
/INPUT_IMAGE/clk                   1
/INPUT_IMAGE/rst                   0
/INPUT_IMAGE/enable                1
/INPUT_IMAGE/key_extraction1       00000111000000111
/INPUT_IMAGE/key_extraction2       00000111000000111
/INPUT_IMAGE/key_extraction3       00000111000000111
/INPUT_IMAGE/key_extraction4       00000111000000111
/INPUT_IMAGE/key_extraction5       00000111000000111
/INPUT_IMAGE/key_extraction6       00000111000000111
/INPUT_IMAGE/key_extraction7       00000110000001010
/INPUT_IMAGE/key_extraction8       00000111000000111
/INPUT_IMAGE/key_extraction9       00000111000000111
/INPUT_IMAGE/key_extractio...      00000111000000111
/INPUT_IMAGE/cipher_round1         zfgzdd|{dp|d{pdd
/INPUT_IMAGE/cipher_round2         [illegible]
/INPUT_IMAGE/cipher_round3         [illegible]
/INPUT_IMAGE/cipher_round4         [illegible]
/INPUT_IMAGE/cipher_round5         [illegible]
/INPUT_IMAGE/cipher_round6         [illegible]
/INPUT_IMAGE/cipher_round7         ïlæÄ*];[illegible]*K%ã{
/INPUT_IMAGE/cipher_round8         [illegible]
/INPUT_IMAGE/cipher_round9         [illegible]
/INPUT_IMAGE/cipher_round10        [illegible]),CrûI
/INPUT_IMAGE/gloabal_key           00000111000000111
/INPUT_IMAGE/j                     x
/INPUT_IMAGE/a1/clk                St1
/INPUT_IMAGE/a1/rst                St0
Now                                720 ps
Cursor 1                           0 ps
```

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

Here in this we carried out implementation of AES cryptographic algorithms with scan based testing futures. It has been previously demonstrated that scan chains introduced for hardware testability open a back door to potential attacks. Here, we propose a level based masking and RSFF based flip flop masking as a scan-protection scheme that provides testing facilities both at production time and over the course of the circuit's life. Compared to regular scan tests, this technique has no impact on the quality of the test or the model-based fault diagnosis. Here we proved that RSFF based AES will give better hardware complexity & power optimization with considerable delay enhancement. An accurate SFF-based analysis approach was 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.

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 Embedded Systems (CHES2001*), Paris, France, pp. 315-325, May 2001.

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

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

[4]. G. Bertoni, L. Breveglieri, I. Koren, and P. Maistri, "An e□cient hardwarebased fault diagnosis scheme for AES: performances and cost," In Proc. of the IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT2004), Cannes, France, pp. 130-138, Oct. 2004.

[5]. 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.

[6]. L. Breveglieri, I. Koren, and P. Maistri, "Incorporating Error Detection and Online Reconfiguration into a Regular Architecture for the Advanced Encryption Standard," In Proc. of the IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT2005), Monterey, CA, USA, pp. 72-80, Oct. 2005.

[7]. D. Canright, "A Very Compact Rijndael S-box," Naval Postgraduate School Technical Report: NPS-MA-05-001, May 2005.

[8]. G. C. Cardarilli, M. Ottavi, S. Pontarelli, M. Re, and A. Salsano, "Fault localization, error correction, and graceful degradation in radix 2 signed digit-based adders," IEEE Trans. on Computers, vol. 55, no. 5, May 2006.

[9]. M.Fons,F.Fons,E.Canto."biometric based consumer applications driven by reconfigurable hardware architectures."Development of embedded systems research Group, Department of Electronic, Electrical and Automatic Control Engineering, Universitat Rovira i Virgili, Tarragona 43007, Spain.

[10]. Rajiv Mahajan, Teenum Gupta, Sakshi Mahajan, and Navneet Bawa. "Retina as Authentication Tool for CovertChannel Problem". World Academy of Science, Engineering and Technology 56 2009.

[11]. Yi Wang, Member,IEEE,and Yajun Ha, Senior Member, IEEE "A Performance and Area Efficient ASIP for Higher-Order DPA-Resistant AES". IEEE journal on emerging and selected topics in circuits and systems, vol. 4, no. 2, June 2014.