IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 16-20

Highly reliable RC5 System Using Biometric Based key generation

Poonkothai.R[1], Priyanka.P[2], BalaVigneshwari.M[3]
[1,2]UG students, [3]Assitatnt professor, Department of ECE
Apollo engineering College, Poonamalle.

Abstract : *In Recent Days Field-Programmable Gate Arrays (Fpgas) Are Becomes 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 Rc5 Standard 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 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- *Mimo, Spatial Modulation, Index Modulation, Bit Error Rate, Ml Detector Etc.*

I. INTRODUCTION

For a long time, the Data Encryption Standard (DES) was considered as a standard for the symmetric key encryption. DES has a key length of 56 bits. However, this key length is currently considered small and can easily be broken. For this reason, the National Institute of Standards and Technology (NIST) opened a formal call for algorithms in September 1997. A group of fifteen AES candidate algorithms were announced in August 1998. Next, all algorithms were subject to assessment process performed by various groups of cryptographic researchers all over the world. In August 2000, NIST selected five algorithms: Mars, RC5, Rijndael, Serpent and Two fish as the final competitors. These algorithms were subject to further analysis prior to the selection of the best algorithm for the RC5. The RC5 cipher [1] was developed by Ron Rivest. The cipher is block-based and symmetric. The advantage of the RC5 cipher over other ciphers as the DES [2] is its simplicity of implementation and its flexibility due to its parameterizable nature. Also simplicity of operations is of paramount importance to improve operation speed.

For secure use of conventional encryption, we have two requirements: a strong encryption algorithm and transmission and reception of secret key in secure fashion. Here we used RC5encryption algorithm which is symmetric block cipher.

1.1 Basic primitives

RC5 has a variable word size, a variable number of rounds and a variable length secret key. RC5 is exactly designated as RC5-w/r/b, where w denotes word size in bits, the standard value is 16,32and 64 bits; r denotes number of rounds and allowable value ranges from 0 to 255; b denotes length of user's secret keyin bytes and the allowable value ranges from 0 to 255. The parameters we have used are RC5-32/12/16. RC5 consists of three components: key expansion, encryption and decryption algorithm

This uses three primitive operations and their inverse.

1. Addition of words "+". This is modulo-2w addition and the inverse operation subtraction of words"-".
2. Bit wise exclusive OR (XOR) of words
3. The rotation of word x left by y bits is denoted x<<<y. The inverse operation is the rotation of word x right by y bits is denoted x>>>y.

II. RC5 ALGORITHM

Cryptographic algorithms can be divided on the basis of key usage as Symmetric and Asymmetric ciphers. In symmetric ciphers a key is used as a parameter to the encryption algorithm which takes the data and converts it into a random sequence of characters which have no relation (ideally) to the original data. This random sequence of characters is known as cipher text.

This cipher text is sent to the receiver over the medium. The receiver then gives the same key as input to the decryption algorithm and converts the cipher text back to the plain text. If the key used for encryption is not the same as the key used for decryption, the cipher is asymmetric. Asymmetric ciphers are mainly used to exchange the keys for exchanging the symmetric keys which are used to establish a secure connection between devices. Asymmetric ciphers are not used extensively because they are inherently slower compared to symmetric ciphers.

Ciphers can also be divided as stream based or block based ciphers based on the size difference between the cipher text and the corresponding plain text. In Block based ciphers the length of plain text is same as the cipher text but in stream based ciphers, the cipher text is usually longer than the plaintext. Though stream ciphers are less complex and easier to implement compared to Block based ciphers, they have security issues arising due to the pseudo random generators used in them.

2.1 Key Expansion

This routine expands the user's secret key K to fill the expanded key array S, S resembles an array of t=2(r+1) random binary words determined by K. It uses two word-sized binary constants Pw and Qw.

2.2 Specifications

The algorithm uses series data dependent rotations heavily to randomize the data during encryption. The decryption stage performs the inverse of the operations performed in the encryption stage to obtain the original data or plain text. Both the encryption and decryption stages use the expanded version of the key called as S array for their operations. The flexibility of the algorithm is due to the fact that the word length (W), key size(b) and the number of rounds(R), are variable. Their values can be adjusted depending on the requirements. The word length specifies the number of bits in each word which the algorithm takes as input. Increasing the word length increases the throughput. But in software implementations, it is necessary to consider the register size of the CPU. Any length greater than the size of the CPU registers degrades performance. The key size is the length of the key (in bytes). Increasing the key size improves security by reducing vulnerability to rainbow or brute force attacks. The number of rounds specifies the number of iterations in the encryption and decryption procedures. Apart from randomizing the data even further, it increases the encryption and decryption times which is a trade-off for security, because it makes brute force attacks difficult or even infeasible.

2.3 Encryption and decryption

We assume that the input block is given in two w-bit registers A and B. We also assume that key expansion has already been performed, so that the arrays(0, t-1) has been computed. Here is the encryption algorithm in following figure 1.Here in this diagram illustrates the Fiestal structure which is basic principle of the symmetric data security process. Basic operation of RC5 encryption algorithm was discussed in chapter 1.

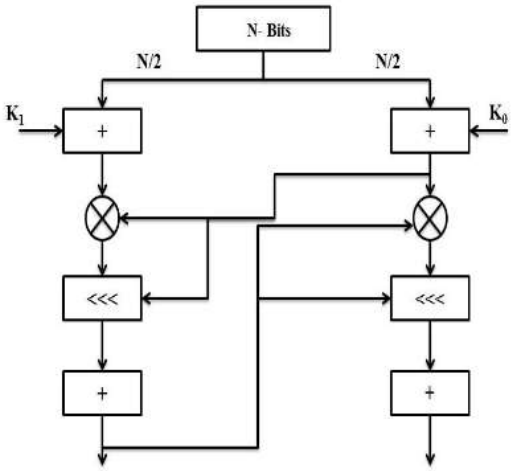

Fig. 1: Encryption modules

2.4 Mixing in the secret key

The third process is to mix in the user's secret key in the array S and L array.

i=j=0;

A=B=0;

Do 3*max(t,c) times;
A=S[i]=(S[i]+A+B)<<< 3;
B=L[i]=(L[i]+A+B)<<< (A+B);
i= (i+1)mod (t);
j= (j+1)mod (c);

2.5 Initializing the array S

The second process is to initialize arrayS to a pseudo random bit pattern using arithmetic progression by constant values Pw and Qw
.S[0]=Pw;
For i=1 to t-1 do
S[i]=S[i-1]+Qw

2.6 Biometric Authentications

In [3],[4] 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[5]. 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. The demanding task of searching a large database to match a template to identify an unknown user. 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.

III. BIO CRYPTO SYSTEM IMPLEMENTATION

To verify the characteristics and the quality of proposed method variety of simulations are carried out. For better timing performance, we adopt the pipelined architecture to produce an output at every clock cycle.

3.1 Security Levels

- The way PIXEL locations are selected (based on secret random generator)
- The way selected pixels are combined and its overlapping depth is secret.
- The KEY origination is secret. (among 10 keys generated).

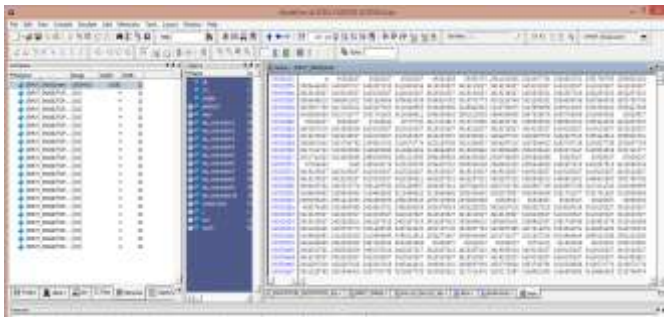

Fig. 2. Bio key generation simulated output.

3.2 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.

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 RC5 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

RC5), 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.

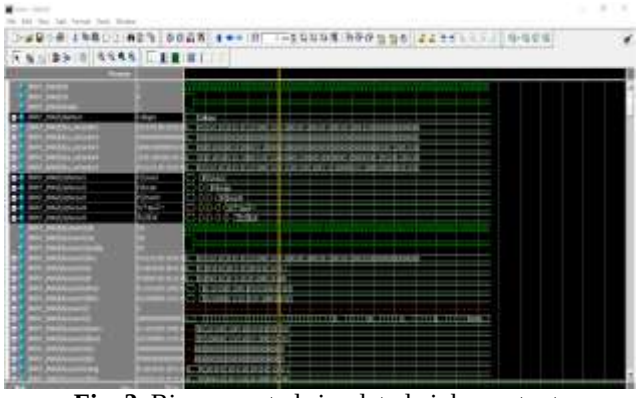

Fig. 3. Bio encrypted simulated cipher output.

Flow Status	Successful - Tue Mar 20 09:23:49 2018
Quartus II Version	9.0 Build 132 02/25/2009 SJ Web Edition
Revision Name	TOP
Top-level Entity Name	encrypt_decrypt_top
Family	Cyclone III
Met timing requirements	N/A
Total logic elements	386 / 5,136 (8 %)
Total combinational functions	386 / 5,136 (8 %)
Dedicated logic registers	384 / 5,136 (7 %)
Total registers	384
Total pins	131 / 183 (72 %)
Total virtual pins	0
Total memory bits	0 / 423,936 (0 %)
Embedded Multiplier 9-bit elements	0 / 46 (0 %)
Total PLLs	0 / 2 (0 %)
Device	EP3C5F256C6
Timing Models	Final

Fig. 4: Area Summary

IV. SYNTHESIS RESULTS

Here we compare the performance of the proposed RC5 model to explore the performance metrics as shown in table 1 with the inner stage pipelining schemes. We extended this analyzes to prove the feasible hardware implementation of RC5core. To prove the performance of the aforementioned designs, here we accomplished the highest achievable complexity reduction and frequency.

Table 1. Comparative performance analyzes of inner stage pipelining enabled RC5 core.

RC5 module	AREA	Fmax report
Without pipelining	450	564.65 MHz
With inner stage pipelining	386	738.01MHz

V. CONCLUSION

Analyzing In this paper, a new bio key generation technique is introduced as an effective countermeasure against hardware based differential cryptanalysis. It could be fully compatible with the state-of-the-art design flow and all the advantages and simplicity of traditional hardware detection are preserved, therefore it is desirable in modern crypto designs as a secure bio enabled key extraction solution with ignorable design/test overhead.

REFERENCES

[1]. B. Yang, K.Wu, and R. Karri, "Scan based side channel attack on dedicated hardware implementation of data encryption standard," in Proc.Int. Test Conf., 2004, pp. 339–344.

[2]. B. Yang, K.Wu, and R. Karri, "Secure scan: A design-for-test architecture for crypto chips," IEEE Trans. Comput.-AidedDes. Integr. Circuits Syst., vol. 25, no. 10, pp. 2287–2293, Oct. 2006.

[3]. R. Nara, N. Togawa, M. Yanagisawa, and T. Ohtsuki, "Scan-based attack against elliptic curve cryptosystems," in Proc. IEEE ASP-DAC2010, pp. 407–412.

[4]. G. Sengar, D.Mukhopadhyay, and D. R. Chowdhury, "Secured flipped scan-chainmodel for crypto-architecture," IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst., vol. 26, no. 11, pp. 2080–2084, Nov. 2007.

[5]. M. Agrawal, S. Karmakar, D. Saha, and D. Mukhopadhyay, "Scan based side channel attacks on stream ciphers and their counter-measures," in Proc. Int. Conf. Cryptology India (INDOCRYPT), 2008, pp. 226–238.