IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 04, Issue 01 (January. 2014), ||V7|| PP 14-20

Encryption Implementation of Rock Cipher Based on FPGA

Murtada Mohamed Abdelwahab , Abdul Rasoul Jabar Alzubaidi
[1-] *Department of Electronic Engineering - Faculty of Engineering & Technology – University of Gezira*
[2-] *Electronic Dept – Engineering Collage -Sudan University for Science and Technology*

Abstrct :- Information security systems must provide high levels of correctness, and reliability. The presented implementation is an application for symmetric encryption algorithm which developed by using two keys to encrypt an input block consist of 128 bit. This implementation is developed for the purpose of producing a powerful encryption data. The operation of encryption and decryption required to insert two keys together in order to access the system correctly. Each key expanded randomly to 128 bit and then it used in each round of encryption. The design is based on Field Programmable Gate Array (FPGA) and used VHDL code to implement the design. The simulation results are considered reliable and completely correct.

Keywords: *FPGA, Encryption, Decryption, Algorithm*

I. INTRODUCTION

The meaning of security is not limited on one concept or a particular algorithm .In fact any algorithm may deserve to describe as a secure algorithm, when it has unpredictable context or if it created with a complex computations. This design is a cryptographic system based on the use of two of the keys to perform encryption and decryption functions. The algorithm is similar to DES algorithm in some configuration steps, instead of using single key in multiple rounds of encryption, this implementation is used two input keys each one is used for a single round. This implementation modified the previous work [9] which offers only an encryption method with the use of two keys, while the proposed implementation offers both algorithms encryption and decryption with the usage of FPGA device .The proposed implementation optimized because all users are needed to use two keys to access the system. FPGAs offer a low-risk, quick time-to-market solution that industrial designers can easily modify when they need to make changes, also they can fix problems in an easy process [1]. The FPGA chip consists of a large number of small logic circuit elements, which can be connected together using the programmable switches .The logic circuit elements are arranged in a regular two dimensional structure. A hardware description language is similar to a typical computer language except that an HDL is used to describe and modeling hardware rather than a program to be executed on a computer [2]. Nowadays, the rapid evolution of communication systems offers, to a very large percentage of population, access to a huge amount of information and a variety of means to use in order to exchange personal data. Therefore, every single transmitted bit of information needs to be processed into an unrecognizable form in order to be secured. This enciphering of the data is necessary to take place in real time and for this procedure cryptography is the main mechanism to secure digital information. Due to the large amount of information data, a multiple forms of encryption algorithms have been developed. Among the different cryptographic algorithms, the most popular example in the field of symmetric ciphers is the Data Encryption Standard (DES) algorithm, which was developed by IBM in the mid-seventies The DES algorithm, is popular and in wide use today because it is still reasonably secure and fast. A much more secure version of DES called Triple-DES (TDES), which is essentially equivalent to using DES three times on plaintext with three different keys. Naturally, it is three times slower than the original form of DES but it provides more security [3]. On 1973, the National Bureau of Standards published seeking for cryptosystems in the Federal Register. The result was the development of the Data Encryption Standard, or DES. Since the first appearance on the scene in March 17, 1975 DES has become the most widely used cryptosystem in the world .After a considerable amount of public discussion, DES was adopted as a standard for "unclassified" applications on January 15, 1977. DES has been reviewed by the National Bureau of Standards (approximately) every five years since its adoption. Its most recent renewal was in January 1994, when it was renewed until 1998. It was expected that it will not remain a standard beyond 1998[4]. Hardware implementations of the Advanced Encryption Standard (AES) Rijndael algorithm have recently been the object of an intensive evaluation. Several papers describe efficient architectures for ASICs (Application Specific Integrated Circuits) and FPGAs (Field Programmable Gate Array). In October 2000, NIST (National Institute of Standards and Technology) selected Rijndael as the new Advanced Encryption Standard (AES), in order to replace the old Data Encryption Standard (DES). The selection process included performance evaluation on both software and hardware platforms and since that many hardware architectures were proposed and published in many journals and conference in all over the world [5].

The two basic working principles of the classical ciphers: substitution and transposition are still the most important structure that used in the construction of the modern symmetric encryption algorithms. A combinations of substitution and transposition ciphers founded in two important modern symmetric encryption algorithms: Data Encryption Standard (DES) and Advance Encryption Standard, AES, .Encryption algorithms are divided into [6] :

- Symmetric key algorithms where the same key is used for encryption and decryption. For example DES algorithm.
- Asymmetric key algorithms (Public-key cryptography), where different keys are used for encryption and decryption.

For the purpose of inventing hard cipher two different input keys has been used. The work also aimed to demonstrate how FPGAs can address the need for faster recovery. This encryption algorithm targeted for small embedded applications. It was initially designed for software implementations in controllers, smart cards or processors.

II. MATERIALS AND METHODS

Xilinx –project navigator, ISE 9.2 is the computer aided design tool which used in synthesizing the model design and implementing (i.e Translate Map & Place and Route) VHDL code with FPGA device . The proposed design based on symmetric algorithm .The algorithm was improved by using two keys, both transmitter and receiver are used the same keys. The required operation function of this implementation is described in Fig .1.

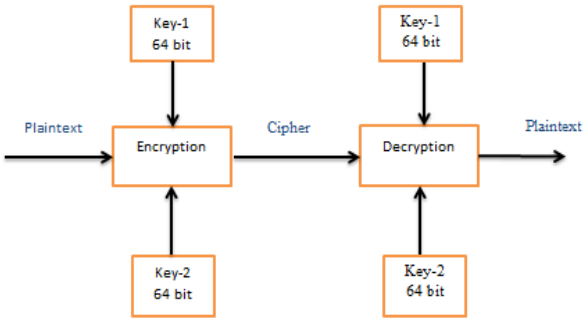

Figure 1. Implementation scheme

Basically the implementation composed of a combination of transposition and substitution techniques. Each input block of data consists of 128 bit and it can be considered as a set of bytes arranged in array, it may called s-box and can be given by:

S box =

$$\begin{pmatrix} B0 & B1 & B2 & B3 \\ B4 & B5 & B6 & B7 \\ B8 & B9 & B10 & B11 \\ B12 & B13 & B14 & B15 \end{pmatrix} \quad (1)$$

2.1 Substitution Technique:

In a substitution cipher, the encryption function $e_k(m)$ represents the substitution function which replaces each $m \epsilon M$ (input data) with a corresponding $c \epsilon C$ (cipher) ,this operation is done by using a special algorithm map with applying some logical operands. The substitution function is parameterized by a secret key k. The decryption algorithm $D_k(c)$ is merely the reverse substitution. In general substitution can be given by [4]: :

$$E : M \rightarrow C \quad (2)$$

And the reverse substitution is just the corresponding inverse mapping which can be written as:

$$D : C \rightarrow M \quad (3)$$

2.2 Transposition Technique

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed. Mathematically an objective function is used on the characters' positions to encrypt and an inverse function to decrypt [7]. Transposition is the process of rearranging data bytes. The used transposition's mechanism is described in Fig 2. Each byte of the incoming data changes position following the illustrated path as shown in the chart below.

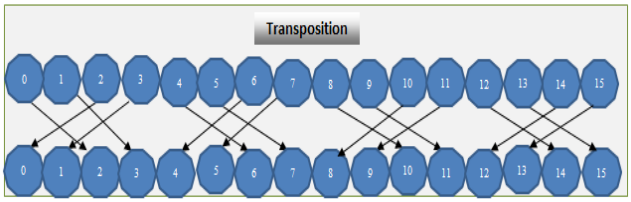

Figure 2. Transposition Mechanism

1.3 Encryption Algorithm

The proposed design accepts 128 bit of data and used two keys each with a length of 64_bit. Basically encryption algorithm is divided into three stages:

- SubBytes: At this stage the input data block is divided into 16 bytes and represented as array .
- .Add key: adding the two keys together in order to encrypt the input block. The receiver and sender must shared the same two secret keys in order to use the system.The key consist of 64 bit which expanded to 128 bit then the two generated keys are randomly added with the input data block.
- The Transposition: The Transposition Cipher (also known as the Permutation Cipher) has been in use for hundreds of years. It is a technique that used to changes the positions of data elements.

These three steps are shown in Fig.3 which describes the basic architecture of encryption algorithm.

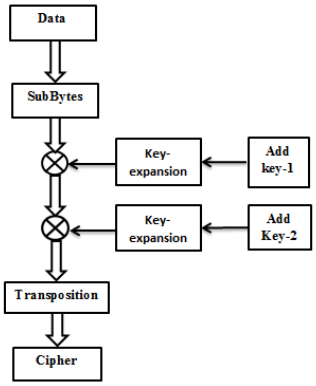

Figure 3: Encryption stage

The example in Fig.4 shows the computation scheme which describes how the output cipher can be created. Three blocks are needed to construct the output cipher with the use of xor operand. The three blocks includes the two generated keys and input data block.

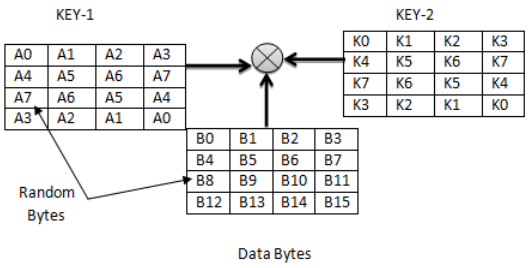

Figure 4: Computations scheme

The composed output cipher of the blocks which descriped in Fig.4 can be written mathmatically as given in equation (4):

$$Bi \otimes Ai \otimes Kj \quad (4)$$

Equation (4) states that each random byte Bi from the input block is added randomly with a random Ai byte from the first key(key-1). Then the result is added (xor) with a random Kj byte from the second key (key-2). Therefore the cipher output C that resulted from adding the two keys and the input block can be written mathmatically by:

$$C= \begin{bmatrix} A0 & A1 & A2 & A3 \\ A4 & A5 & A6 & A7 \\ A7 & A6 & A5 & A4 \\ A3 & A2 & A1 & A0 \end{bmatrix} \otimes \begin{bmatrix} B0 & B1 & B2 & B3 \\ B4 & B5 & B6 & B7 \\ B8 & B9 & B10 & B11 \\ B12 & B13 & B14 & B15 \end{bmatrix} \otimes \begin{bmatrix} K0 & K1 & K2 & K3 \\ K4 & K5 & K6 & K7 \\ K7 & K6 & K5 & K4 \\ K3 & K2 & K1 & K0 \end{bmatrix} \quad (5)$$

As shown in equation(5) each input key expanded to 128 bit in the given arrangment . Therefore the final cipher result is written as :

$$C = \begin{bmatrix} C0 & C1 & C2 & C3 \\ C4 & C5 & C6 & C7 \\ C8 & C9 & C10 & C11 \\ C12 & C13 & C14 & C15 \end{bmatrix} \quad (6)$$

Where C is calculated in the following equations:

$$\begin{aligned} C(0) &= A0 \otimes B0 \otimes K0 \\ C(1) &= A1 \otimes B1 \otimes K1 \\ &\vdots \\ C(14) &= A1 \otimes B14 \otimes K1 \\ C(15) &= A0 \otimes B15 \otimes K0 \end{aligned} \quad (7)$$

The last operation is actually a transposition cipher which only rearranges the positions of the elements without changing their identities. Thus by applying the given transpositions chart with the cipher array, a new arrangement of elements is composed and it can be given by:

$$C = \begin{bmatrix} C2 & C3 & C0 & C1 \\ C6 & C7 & C4 & C5 \\ C10 & C11 & C8 & C9 \\ C14 & C15 & C12 & C13 \end{bmatrix} \quad (8)$$

The algorithm can use multiple forms of elements arrangement instead of that shown in the given example .

1.4 Decryption Algorithm:

Decryption algorithm can be described as shown in Fig. 5. The algorithm context is almost similar to the previous encryption algorithm. But it performs the reverse transposition for the input block.

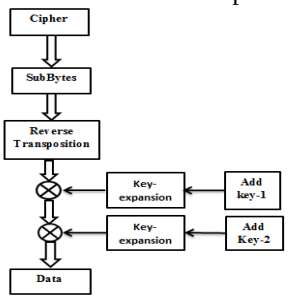

Figure.5. Decryption scheme

The output plaintext can be given by:

$$C_i \otimes A_i \otimes K_i \quad (9)$$

Where C_i is the input block cipher which consists of 128 bit divided into 16 bytes. Basically the algorithm depends on the use of reverse transposition for the cipher block and each key is expanded to 128 bit, then each byte of the input cipher is randomly added (xor) with corresponded byte from the two generated keys.

III. THE RTL DESIGN

The input/output scheme as shown in Fig. 6 demonstrates the inputs and outputs of implementation .It consist of six inputs and two outputs. The outputs can be either a cipher output (encryption mode) or a plaintext type (decryption mode).

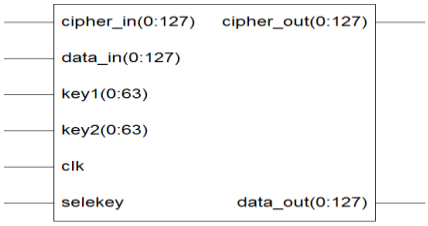

Figure 6. Inputs-outputs Scheme

The purpose of using the selection input is to enable the required operation mode (selekey=1 for encryption and selekey =0 for decryption mode).The clock is used to organize the operation of inputs and outputs . The technology scheme of the components inside the FPGA chip is shown in Fig.7. It also shows the interconnections of components.

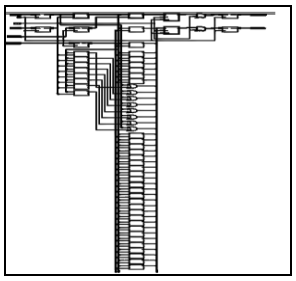

Figure 7. Components on FPGA.

IV. RESULTS AND DISCUSSION

The simulation was done by using the ISE VHDL simulator .The main purpose of simulation is to ensure that the output results has a high level of correctness and reliability in both operation modes. The results of encryption and decryption are shown in the following: discussions.

4.1 Encryption Results

The example in Fig. 8 shows the inputs parameters that used in the simulation process by applying the encryption mode. The purpose of this test is to ensure that the implementation provides a high level of assurance and correctness. The test was performed by setting the input of the selection mode to the following form:

selekey=1

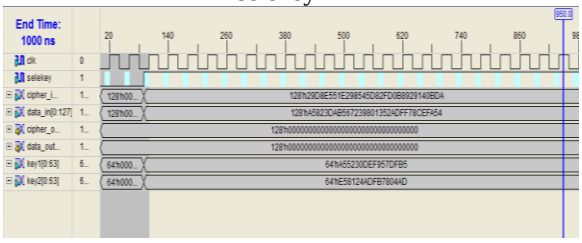

Figure 8 : Simulation inputs (Encryption).

The obtained output results of encryption are shown in Fig. 9. The results were completely correct and compatible with the applied algorithm.

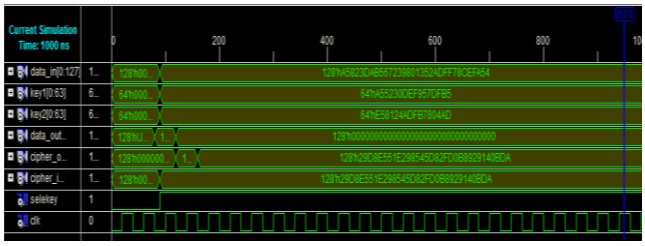

Figure 9: Encryption Results.

4.2 Decryption results:

In order to ensure the accuracy and reliability of the decryption process, this algorithm is tested using inputs as shown in Fig.10. Decryption mode can be selected by changing the status on the selection input as shown in the given form:

selekey=0

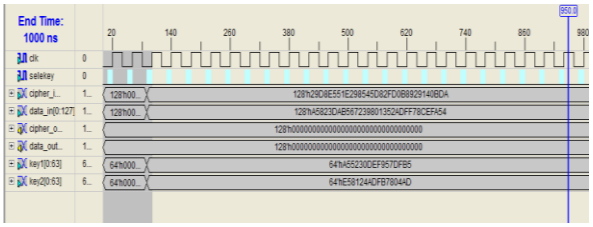

Figure 10 : Decryption Mode.

For the purpose of verifying the results, the same output cipher of the previous experiment has been used as input cipher, so it was expected to obtain the original data. The results of decryption test are shown in Fig.11.

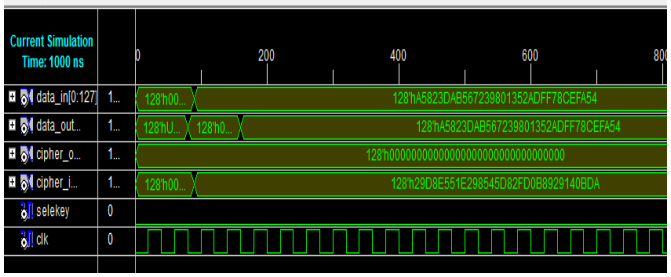

Figure 11. Decryption Results

After verification of the results, there was no doubt that the system gives a results with high-reliability and completely correct. Therefore it can be used in areal applications.

4.3 Synthesis results

Synthesis is carried out by using ISE9.2 and the target device is Xilinx FPGA Vertex5. TABLE I provides the obtained results. The main purpose of synthesis is to determine the implementation area on the chip by checking and determining the amount of logical resources that used by the electronic model of the implementation inside the FPGA chip.

TABLE I. Synthesis Results

Virtex5(target device xc5vlx110t package FF11738 speed-3)			
Logic utilization	**used**	**available**	**utilization**
Number of slices Registers	256	69120	0%
Number of slice LUTs	513	69120	0%
Number of fully used bit slices	256	513	50%
Number of bonded IOBs	642	680	94%
Number of BUFG/ BUFGCTRL$_S$	2	32	6%

The results of Delay is Summarized in the following Report:

The average connection delay for this design is: 2.034 nsec

The maximum PIN delay is: 7.217 nsec

The average connection delay on the 10 worst nets is: 4.647 nsec

Table II shows the comparison results with other related designs in terms of using the internal resources of the FPGA chip.

TABLE II. Comparison of deferent algorithms

Design	**Device**	**Area**
DES [3]	Xc5vlx110T	527 (number of slice LUT_s)
Wong et [8]	Xcv4020E	438 (slices)
Our	Xc5vlx110T	513 (Number of slice LUT_s)
	Xcv1000E	368(slices)

The comparison results show that the proposed implementation has a less consumption resources than DES[3] on virtex5 and wong [8] on virtex E.

V. CONCLUSION

The need to secure data transmission is increased every day therefore it requires secure data encryption devices to preserve data privacy and authentication in critical applications. This paper describes the most popular encryption standards. The presented implementation is a type of symmetric encryption algorithm which depends on a dual key each of 64 bit size. The using of dual keys comes to improve the encryption efficiency. The presented results of the implementation provide a high level of assurance and correctness.

REFERENCES

[1] Dimitrios.M and Ioannis.P," Power consumption estimations vs measurements for FPGA-based security cores", in proceeding of *International Conference on Reconfigurable Computing and FPGAs*, pp 433-437,Cancun ,Mexico,2008.

[2] Stephen.B and Zvonko.V,"Fundamental of Digital logic with VHDL Design",McGrow Hil,(2005).

[3] Prasun. G and Malabika.B," A Compact FPGA Implementation of Triple DES Encryption System with IP Core Generation and On-Chip Verification" , in Proceedings of *International Conference on Industrial Engineering and Operations Management*, Dhaka, Bangladesh, ,2010.

[4] Douglas.S,"Cryptography: Theory and Practice " ,CRC Press,1995.

[5] Gael.R, Francois.X.S, Jean.J. and Jean.D, "Compact and Efficient Encryption/Decryption Module for FPGA Implementation of AES", in Proceeding of *International Conference on Information Technology: Coding and Computing*, pp.339- 345, USA,2004.

[6] http://en.wikipedia.org/wiki/Transposition_cipher.

[7] Wenbo. M, "Modern Cryptography Theory and Practice", Packard Company, (Prentice Hall PTR, 2003).

[8] Wong.K and Wark,E.Dawson," A single- chip FPGA implementation of the Data Encryption Standard (DES) algorithm'' IEEE globecom communication,pp.827-832,vol2,(Sydney ,Australia,1998).

[9] Murtada.A,Abdelrasoul.A," Encryption design based on FPGA using VHDL ,*International Journal of Computer Science and Network Security*,pp.96-100, 12(12) ,December,2012.