IMPLEMENTATION OF TRIPLE HILL CIPHER ALGORITHM ON RECONFIGURABLE LOGIC

Jayendra Kushwah[1], Nitesh Dodkey[2], Niraj Umale[3]
Dept. of Electronics and Communication Engineering, Surabhi group of institution, India

Abstract: These days security becomes an important feature with the growth of e–communication. Electronic cryptographic techniques have evolved and these days many cryptographic algorithms can be implemented on reconfigurable logic like FPGAs. In this work the triple hill cipher algorithm is implemented, the plain text of 128 bits is encrypted using 256 bits key, the cipher text produced is of 128 bits. Two designs are proposed in this work, first the high speed combinational design and second the low area sequential design. The target device used to implement the design is Virtex 4. 40% decrease in resource used is observed in design 2 sequential design as compared to base paper design [14].

Keywords: FPGA, Triple Hill Cipher, Encryption, Cryptography

I. INTRODUCTION

Cryptography is one of the methods used to protect data from unauthorized access and being stolen [1]. Cryptography is the science and study of secret writing. A cipher is a secret method of writing , whereby plaintext is transformed into cipher text .The process of transforming plaintext into cipher text is called encryption. The reverse process of transforming cipher text into plaintext is called decryption. Both encryption and decryption are controlled by a cryptographic key or keys [2][3]. There are two types of cryptosystem, which are symmetric cryptosystem and asymmetric cryptosystem. In Symmetric cryptosystem, the sender and recipient share the same key. It means the same key is used for encryption and decryption. In Asymmetric cryptosystem, different keys are used. A public key is used by sender to encrypt the message while the recipient used a private key to decrypt it [1][2]. In this paper we focus on hill cipher which is a type of symmetric cryptosystem. The hill cipher was first described in 1929 by its inventor, the mathematician Lester S. Hill, in the journal of the American mathematical monthly (Eisenberg, 1998) [1][3][4]. The hill cipher is a classical symmetric cipher based on matrix transformation. It has several advantages including its resistance to frequency analysis and simplicity due to the fact that it uses matrix multiplication and inversion for encryption and decryption. However, it succumbs to the known plaintext attack [5] and as such there have been efforts to strengthen the cipher through the use of various techniques which have improved the security of the cipher quite significantly [6],[7],[8]. In this paper we present a proposed triple hill cipher algorithm which consists of three stages of hill cipher , each stage is considered a block cipher with a block length of 128 bits and key length of 256 bits. The message to be encrypted is processed by this block cipher in three stages to increase the security. The keys are taken from random number generator each stage consists of eight rounds with different eight keys , in each round three operations are implemented ; key and plaintext matrix multiplication, stir operation and XOR operation.

II. TRIPLE HILL CIPHER

Figure 1 shows the high level block diagram of Triple hill cipher algorithm. The 256 bits key is generated using a random number generator is used to encrypt the input plain text in stage 1 of the operation to produce cipher text 1. The input key is rotated and rotated key is used to encrypt the cipher text 1 which produces cipher text 2. The key is rotated again to produce the third key which is used to encrypt cipher text 2 to produce the final cipher text. The three stages shown in figure are identical.

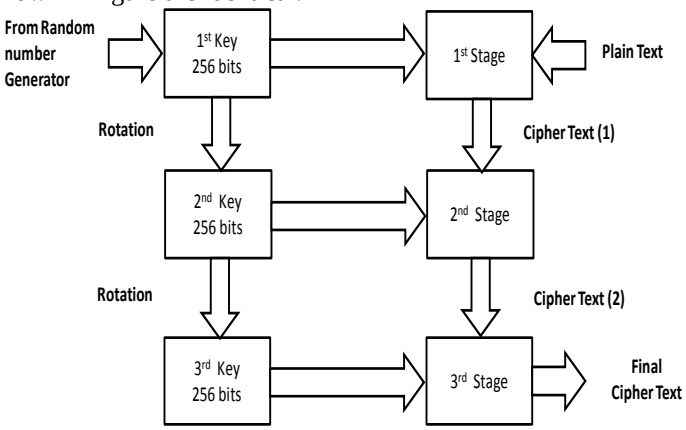

Figure 1: High level block diagram of triple Hill cipher algorithm

Figure 2 shows the diagram of single stage of triple hill cipher algorithm. A total of 8 identical round operations are performed on the plain text to generate the cipher text of that stage, in each round a 128 bit key is required. A key generation module call the sub key generation is used to generate eight internal key using the 256 bit input key. The eight keys are 128 bits long; these sub keys are generated by jumbling the 256 bit input key. The keys are generated using the following equations:

k1 <= key(255 downto 224) & key(191 downto 160) & key(127 downto 96) & key(63 downto 32);
k2 <= key(223 downto 192) & key(159 downto 128) & key(95 downto 64) & key(31 downto 0);
k3 <= key(255 downto 160) & key(31 downto 0);
k4 <= key(127 downto 32) & key(159 downto 128);
k5 <= key(223 downto 96);
k6 <= key(95 downto 0) & key(255 downto 224);
k7 <= key(31 downto 0) & key(255 downto 160);
k8 <= key(159 downto 32);

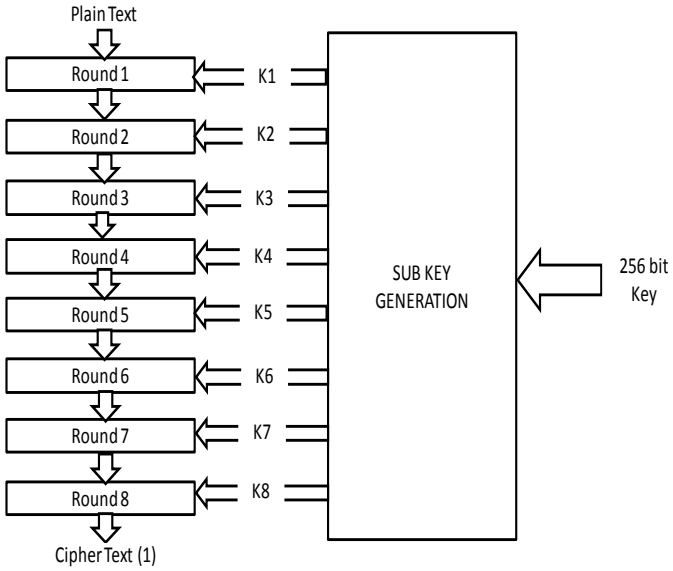

Figure 2: Single stage operation of triple Hill cipher algorithm

Figure 3 shows the internal architecture of single round of triple hill cipher, mainly three operations are performed, the first operation is the matrix multiplication of the plain text matrix with the 128 bit cipher key. The second operation the stir operation where the inputs bits are jumbled and the third operation is the XOR operation of the data obtained from the stir operation to the 128 bits input cipher key. The cipher key for the matrix multiplication process and the xor process is same.

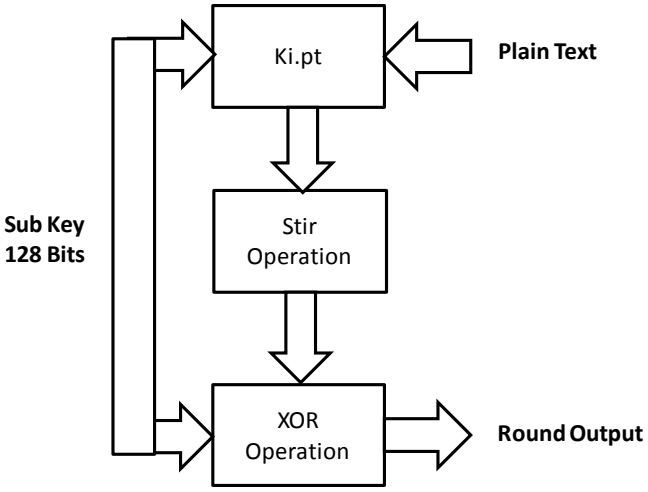

Figure 3: Single round operation of triple Hill cipher algorithm

Figure 4 shows the matrix multiplication operation of triple hill cipher algorithm. The 128 bits key is divided into sixteen parts, each of eight bits represented as k0, k1 …….. k15. The 128 bits plain text is also divided into sixteen pats each of eight bits represented as d0, d1, …… d15. The process used for matrix multiplication is Galois multiplication i.e. the multiplication operation is performed by AND gates to implement ANDing operation and the addition operation is performed by XOR operation. The result is obtained in r matrix, which is of 128 bits divided into sixteen parts of eight bits each.

$$\begin{bmatrix} k0 & k1 & k2 & k3 \\ k4 & k5 & k6 & k7 \\ k8 & k9 & k10 & k11 \\ k12 & k13 & k14 & k15 \end{bmatrix} \cdot \begin{bmatrix} d0 & d1 & d2 & d3 \\ d4 & d5 & d6 & d7 \\ d8 & d9 & d10 & d11 \\ d12 & d13 & d14 & d15 \end{bmatrix} = \begin{bmatrix} r0 & r1 & r2 & r3 \\ r4 & r5 & r6 & r7 \\ r8 & r9 & r10 & r11 \\ r12 & r13 & r14 & r15 \end{bmatrix}$$

Figure 4: Matrix Multiplication operation of triple Hill cipher algorithm

Figure 5 shows the Stir operation. Matrix A of figure 5 is he input matrix which jumbled to produce the matrix B. The process is as follows:

- The 1st and 2nd bits from each byte in a row of A are combined to form the first byte of B in that row
- The 3rd and 4th bits from each byte in a row of A are combined to form next byte of B in that row
- The 5th and 6th bits from each byte in a row of A are combined to form next byte of B in that row
- The 7th and 8th bits from each byte in a row of A are combined to form the last byte of B in that row
- This stir operation is reversible, i.e. Stir(Stir(A))=A

$$A = \begin{bmatrix} 11001100 & 00101010 & 11100110 & 11001100 \\ 11011110 & 10101010 & 00100100 & 01010111 \\ 00011001 & 11101111 & 01111000 & 11000111 \\ 11111100 & 11011011 & 11011100 & 10011001 \end{bmatrix}$$

$$B = \begin{bmatrix} 11001111 & 00101000 & 11100111 & 00101000 \\ 11100001 & 01101001 & 11100101 & 10100011 \\ 00110111 & 01101100 & 10111001 & 01110011 \\ 11111110 & 11010101 & 11101110 & 00110001 \end{bmatrix}$$

$$C = \begin{bmatrix} 11001100 & 00101010 & 11100110 & 11001100 \\ 11011110 & 10101010 & 00100100 & 01010111 \\ 00011001 & 11101111 & 01111000 & 11000111 \\ 11111100 & 11011011 & 11011100 & 10011001 \end{bmatrix}$$

Figure 5: Stir operation of triple Hill cipher algorithm

Figure 6 shows the XOR operation, in this operation bitwise XORing is used, output from the Stir operation is xored with the 128 bits cipher key, the cipher key used in matrix multiplication is reused here.

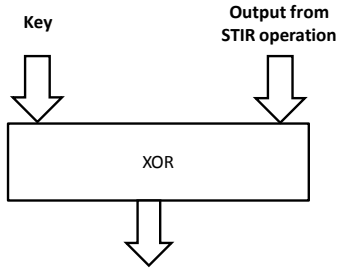

Figure 6: XOR operation of triple Hill cipher algorithm

Eight identical rounds are used to generate the output the one stage called the cipher text. The final cipher text is generated by performing the same operation thrice.

III. COMBINATIONAL ARCHITECTURE

Figure 7 shows the combinational implementation of the triple hill cipher algorithm. The three stages are implemented independently and connected directly in combinational fashion. The advantage of this design architecture is low latency and delay, but it requires huge area i.e. large FPGA resources.

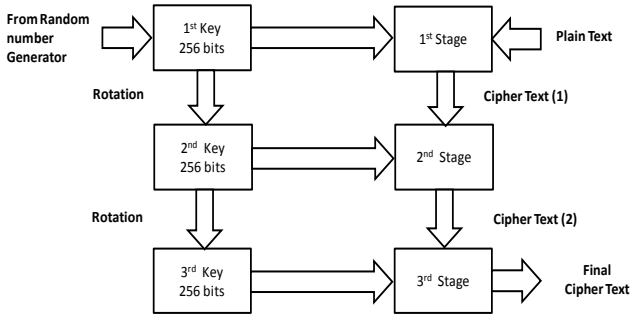

Figure 7: Combinational architecture of triple Hill cipher algorithm

IV. SEQUENTIAL ARCHITECTURE

Figure 8 shows the sequential architecture of the triple hill cipher algorithm. In this design two multiplexers are used, the left multiplexer is used to assign the plain text and the right multiplexer is used to assign the 255 bits key. In the first state of operation the input data 128 bits long is assigned to the single stage along with the 256 bits of key, using the state machine controller. The output of this operation is cipher text 1, which is stored in local register. In the second state of operation cipher text 1 is assigned again to the single stage along with the rotated cipher key and the output generated is called cipher text 2, which is stored in the local register. In the third state of operation the cipher text 2 is assigned to the single stage along with the rotated key to produce the final cipher text. In sequential design only one stage is used to implement the complete triple hill cipher algorithm. The main advantage of this sequential design architecture is low area (less FPGA resources are required). But this will increase latency.

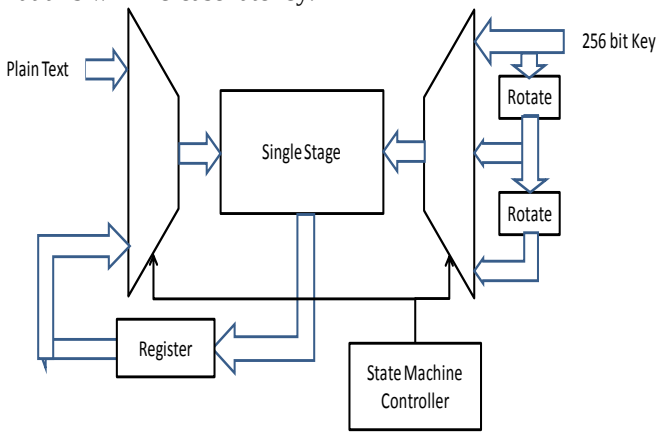

Figure 8: Sequential architecture of triple Hill cipher algorithm

V. RESULTS

Figure 9 shows the simulation of the combinational design. The 128 bits of input data is assigned to the "pt" of the machine and the 256 bits of key is assigned to the "key" input of the machine, clock is assigned to the "clk" input of the machine and the "reset" is assigned to '0'. The output is obtained at the "ct" output, output is obtained immediately after the combinational delay.

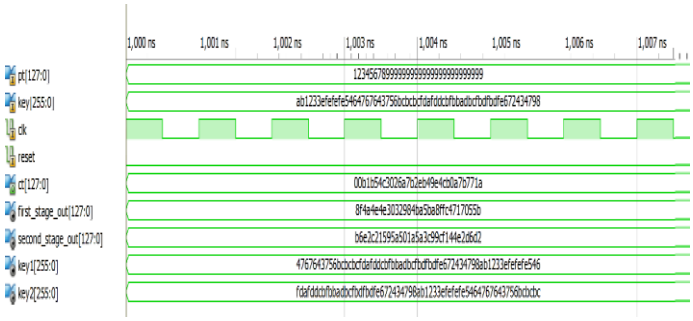

Figure 9: Simulation of combinational architecture of triple Hill cipher algorithm

Figure 10 shows the simulation of the sequential design. The 128 bits of input data is assigned to the "pt" of the machine and the 256 bits of key is assigned to the "key" input of the machine, clock is assigned to the "clk" input of the machine and the "reset" is assigned to '0'. The output is obtained at the "ct" output port, output is obtained after 4 clock cycles of the assignment of input data.

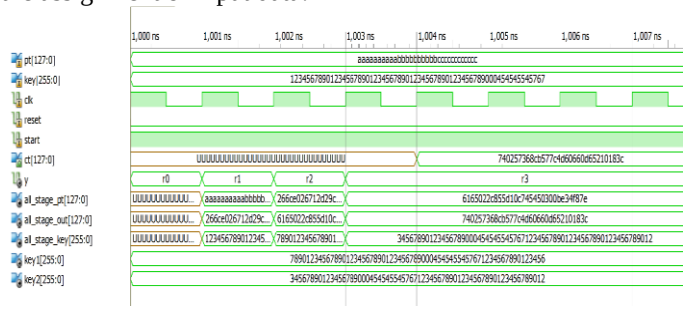

Figure 10: Simulation of sequential architecture of triple Hill cipher algorithm

Device Utilization summary is shown in table 1 and figure 11. The design – 1 combinational design used approximately the same resources as used by base paper design [14]. The design – II sequential design uses 41% less LUTs as compared to base paper design, 40% less Slices compared to base paper design and one extra pin (IOB).

Table 1: Device Utilization Summary

Device Utilization Summary			
Logic Utilization	Base Paper Design [14]	Design I – Combinational Design	Design II – Sequential Design
Number of 4 input LUTs	9222	9,216	5367
Number of occupied Slices	4636	4,622	2754
Number of bonded IOBs	514	512	515

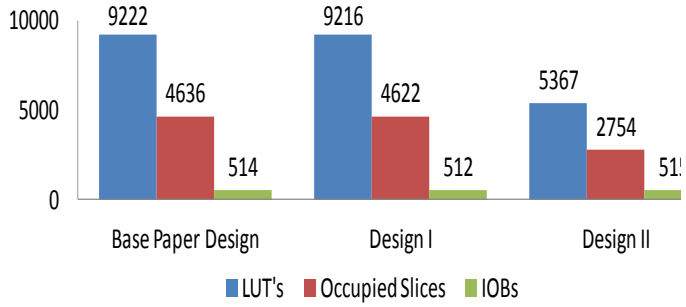

Figure 11: Bar graph showing the device utilization summary

VI. CONCLUSION

In this Hill Cipher algorithm is implemented on FPGA in Triple Hill mode, i.e. the process is repeated three times
Two design architectures are proposed in this work:
Design 1 – Combination Design: In this design all the three stages are implemented using three separate units, hence require large area, but small delay
Design II – Sequential Design: In this design all the three stages are implemented using single unit, hence small area requirement, as depicted device utilization summary

REFERENCES

[1] A.F.A. Abidin, O.Y. Chuan and M.R.K. Ariffin ''A Novel Enhancement Technique of the Hill Cipher for Effective Cryptographic Purposes" Journal of Computer Science 7 (5): 785-789, 2011.

[2] William Stallings ,''Cryptography and Network Security Principles and Practices", Fourth Edition, Prentice Hall, November 16, 2005.

[3] Jasdeep Singh Bhalla,'' A Database Encryption Technique to Enhance Security Using Hill Cipher Algorithm", International Journal of Engineering and Advanced Technology (IJEAT), Vol. 2, No. 4, April 2013.

[4] M. Nordin A. Rahman, A. F. A. Abidin, Mohd Kamir Yusof, N. S. M. Usop,'' Cryptography: A New Approach of Classical Hill Cipher", International Journal of Security and Its Applications,Vol. 7, No. 2, March, 2013.

[5] D.R. Stinson, "Cryptography Theory and Practice",Third Edition, Chapman and Hall/CRC, Pp.13-37, 2006.

[6] [6] V. U. K. Sastry, D. S. R. Murthy, S. Durga Bhavani, "A Block Cipher Involving a Key Applied on Both the Sides of the Plain Text," International Journal of Computer and Network Security (IJCNS), Vol. 1, No. 1, Pp. 27 -30, Oct. 2009.

[7] V. U. K. Sastry, V. Janaki, "A Modified Hill Cipher with Multiple Keys", International Journal of Computational Science, Vol. 2, No. 6, 815-826, Dec. 2008.

[8] Bhibhudendra Acharya, Girija Sankar Rath, and Sarat Kumar Patra, "Novel Modified Hill Cipher Algorithm,",Proceedings of ICTAETS, Pp. 126-130, 2008.

[9] Gandharba Swain,and Saroj Kumar Lenka,''A Technique for Secret Communication Using a New Block Cipher with Dynamic Steganography'', International Journal of Security and Its Applications,Vol. 6, No. 2, April, 2012.

[10] Ahmed Desoky, Anju Panicker Madhusoodhanan,'' Bitwise Hill Crypto System'', DOI: 10.1109/ISSPIT.2011.6151539

[11] Ali Muhammad Ali Rushdi and Fares Ahmad Muhammad Ghaleb,''On Self-Inverse Binary Matrices Over the Binary Galois Field'', Journal of Mathematics and Statistics 9 (3): 238-248, 2013.

[12] D. Coppersmith, D. B. Johnson and S. M. Matyas, ''A proposed mode for triple-DES encryption", IBM J. RES, DEVELOP. VOL. 40 NO, 2 MARCH 1996.

[13] D. Mcllroy Editor, ''On the Security of Multiple Encryption", Communications July 1981 of Volume 24 the ACM Number 7.

[14] Ashraf A.M. KHALAF, Hesham F. A. Hamed "Proposed Triple Hill Cipher Algorithm for Increasing the Security Level of Encrypted Binary Data and its Implementation Using FPGA" July 1-3, 2015 ICACT2015.

