FPGA Implementation of Folding Architecture in Humming bird Algorithm for Reducing Area and High Throughput

R.Tharani
PG Student (VLSI Design), Dept of ECE, Arasu Engineering College, Kumbakonam, Tamil Nadu, India.

G.Kavitha
Assistant professor, Dept of ECE, Arasu Engineering College, Kumbakonam , Tamil Nadu, India.

Abstract— Hummingbird is a new ultra light weight cryptography algorithm target for resources constrained devices like RFID tag, smart card and wireless sensor. In this project we design the hardware implementation of humming bird cryptography algorithm based on the folding Architecture in Spartan 3 FPGAs. Humming bird is to meet stringent response of area and power requirements which can provide the design security with a small block size. This algorithm resists to the most common attacks like algebraic attack, linear and differential cryptanalysis. We investigate for integrating humming bird into a privacy preserving and authentication protocol. In this technique to reduce the clock cycle to encryption and decryption the message. In this work, an enhanced hardware implementation of the humming bird cryptography algorithm for reduces area and high throughput for low cost Spartan 3E family.

Index Terms— Light weight Cryptography, Mutual Authentication, Protocol security analysis and FPGA.

1. INTRODUCTION

Cryptography is the art or making a secret code of the information content using a key. A low cost smart devices like RFID tags and smart cards are rapidly becoming pervasive in our daily life[3] .A well known application include electronic passport, contact payment , product tracking. However major problems that prevailing now is the lack of information security where the private data can be accessed by unauthorized person in different sighting of the same RFID tag an adversary can easily trace a person carrying a target. Unprotected wireless communication will have many issues between RFID tag and reader[5][7].RFID is rapidly developing technology enabling automatic object identification .RFID tag is composed of a tiny integrated circuit for storing and processing identification information as well as radio antenna for wireless data transmission. The various application for low cost and low power can be implemented tag such as identification, point of sales and inventory management. To solve the security and privacy issues, a privacy-preserving mutual authentication protocol is required for reader and tag to authenticate each other [6].

Humming bird encryption used the principle of classics rotor machine which will perform the substitution and permutation operation. For that a new research area is put forward called ultra light weight cryptography to obtain the trade off among privacy, performance and cost for humming bird has a hybrid structure of block cipher and stream cipher. The hybrid model can provide the design security with small block size and therefore expect to meet to meet the stringent response time and power consumption requirements[4][7]. So the humming bird algorithm is to resists to the most common attacks like structural attacks, birthday attacks, linear and differential cryptanalysis. The encryption and decryption process of the humming bird can be viewed as the continuous running of enigma machine. To design and implement pipelined architecture in humming bird cryptographic algorithm to get reduced area and improved throughput. Recently this humming bird cryptography algorithm is using twitter to improve the privacy [7].

I. HUMMING BIRD CRYPTOGRAPHY ALGORITHM

A new ultra light weight cryptographic algorithm referred to as humming bird for resource constrained devices.[3] The design of humming bird cryptographic algorithm is motivated by the well known Enigma machine taking into account both security and efficiency. The block cipher and stream cipher combines to make hybrid structure of humming bird. It has been shown to be resists to the most common attacks to block cipher and stream cipher including birthday attack, linear and differential cryptanalysis etc.[4] cheap smart devices like RFID tag and smart cards are becoming important ant in our daily life. This algorithm is able to switch key easily and rapidly.[11][15]

A. Humming bird mutual authentication protocol

The humming bird mutual authentication protocol is used to establish the trust relationship between reader and tag based on the highly efficient humming bird cryptographic algorithm. For a secured RFID system, the reader can determine the

correct key that is communicating with tag without exposing the tag identity.[10]

In this private identification protocol, the reader initially sends a QUERY signal with a 16 bit SESSSION ID as input. After receiving the QUERY, the tag will generate four 16 bit random vectors that will be used for initializing the four status registers. After initialization, it will take RS1 ^RS3 message data as input. Encrypt it three times and generate three cipher texts CT0, CT1, CT2 as tag indicators. Then the tag will transmit these three cipher texts together with the initialize vectors to the reader. With the key, the reader can do the encryption and generate three cipher texts and the same will be compared with the three tag indicators. If it matches, then the tag will accept otherwise reject and move for the next tag. [5]. The mutual authentication protocol is shown in Fig 1

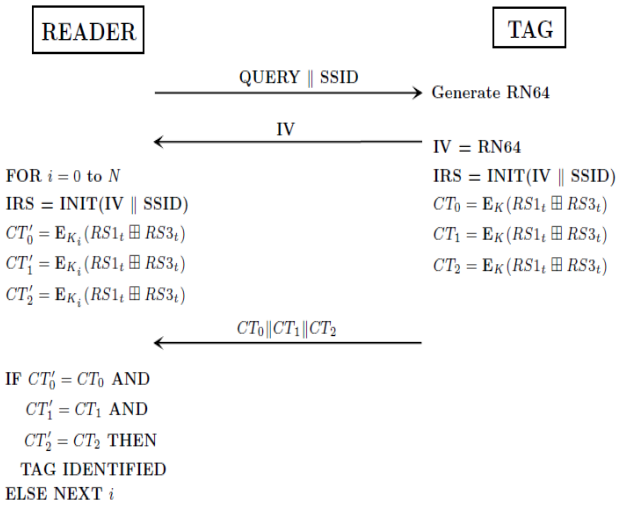

Fig. 1 humming bird mutual authentication protocol

Consider a RFID system with one billion tags, a tag generate three indicators. So for one billion tags it requires too many indictors. It takes much area to store these indicators for reduce the area consumption , This project of folding architecture for simplified and secured mutual authentication with high throughput.[12]

B. security analysis of humming bird algorithm

Humming bird is a hybrid mode of block cipher and stream cipher. In humming bird have several advantages .It is secure for encryption and decryption. It is well suited for resources constrained environment. The state space of the algorithm requires little memory. The message which is to be kept in secret is referred to as plain text. The process of hiding its content is called encryption and the encrypted message is referred as cipher text. The process of receiving the content of the plain text back from cipher text is decryption. There is no cipher text expansion unless a message authentication code is added to the cipher text. It appears to be appropriate for either software and hardware can be implementation. This algorithm able to switch key and rapidly. FPGA implantation humming bird design by using folding architecture for improved security and area is given in Fig 2. Recently this humming bird cryptography algorithm is using in twitter to improve the privacy efficiently.[9]

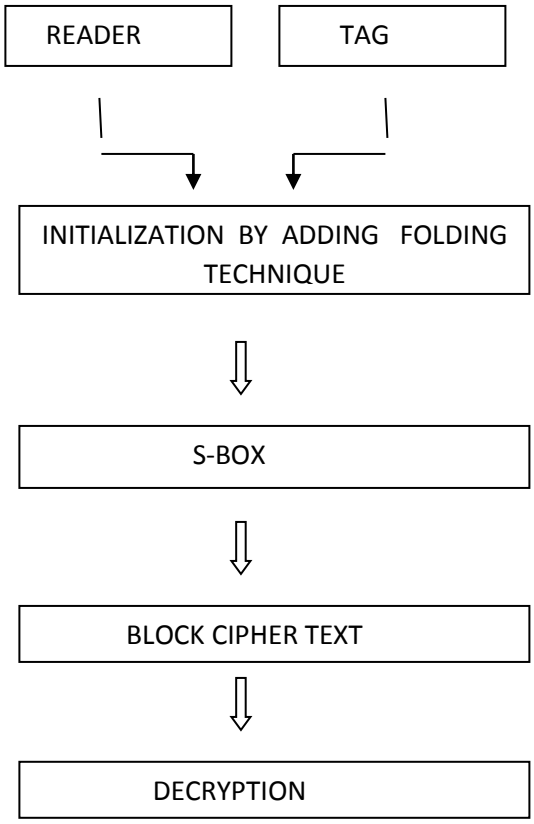

Fig. 2.Flow chart for secured humming bird algorithm

In the above design reader and tag perform using mutual authentication protocol for security purpose. If key matches, the tag will generate random in initialization algorithm by adding pipelining technique with the encrypted data to the reader. After receiving the initialization it will be implemented for S-box, substitution for mapping in different ways. Then it gives block cipher to process 16 bit data in 4 rounds of diffusion and confusion concepts. Finally decrypt the message. In order to improved the security and improved area.[13]

2. IMPLEMENTATION OF FOLDING ARCHITECTURE IN HUMMING BIRD ALGORITHM

Folding is transformation technique using in DSP architecture implementation for minimizing the number of functional blocks in synthesizing DSP architecture. The transformed DSP system produces $y(n)$ in each 2 l where each 2 l increase 1 n, index of y. The resources used in original system are 2

adders, and the resources used in transformed system are 1 adder, 1 register, 3 multiplexer. The functional block, adder, is therefore reduced.

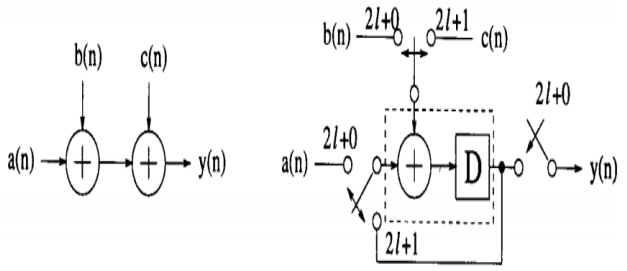

Fig 3 Folding Architecture

A. *Initialization algorithm*

Fig 4 shows the overall structure of humming bird initialization algorithm. When using humming bird in practice, four 16 bit random nonce's NONCE random number bit are first chosen to initialize the four internal state register RS (i=1,2,3,4) and Eki (i=1,2,3,4) are 16 bit block cipher respectively followed by four consecutive encryption on the message RS1 to RS3 by humming bird running in initialization mode final 16 bit cipher text TV is used to initialize LFSR(Linear Feedback Shift Register).[6] Moreover, the 13 th bit of the LFSR is always set to prevent a zero register. The LFSR is also stepped once before it is used to update the internal state register RS3. In this algorithm is used for security and high throughput. In order to implement folding technique for reduced the area efficiently. [3] By using the folding technique it reduce the area and throughput efficiently with improved the result and provide high performance than compared to the existing system. It achieve no memory block. In this method encryption and decryption the message efficiently with high result.

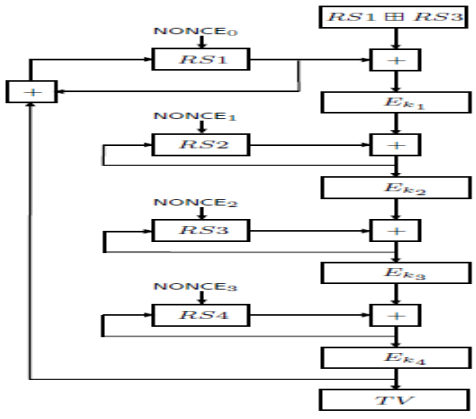

Fig. 4 Block diagram of Initialization algorithm

Nonce Initialization:

$RS1_0 = \text{NONCE}_0$
$RS2_0 = \text{NONCE}_1$
$RS3_0 = \text{NONCE}_2$
$RS4_0 = \text{NONCE}_3$

Four Rounds Encryption:

for $t = 0$ to 3 **do**

$V12_t = E_{k_1}((RS1_t \boxplus RS3_t) \boxplus RS1_t)$
$V23_t = E_{k_2}(V12_t \boxplus RS2_t)$
$V34_t = E_{k_3}(V23_t \boxplus RS3_t)$
$TV_t = E_{k_4}(V34_t \boxplus RS4_t)$
$RS1_{t+1} = RS1_t \boxplus TV_t$
$RS2_{t+1} = RS2_t \boxplus V12_t$
$RS3_{t+1} = RS3_t \boxplus V23_t$
$RS4_{t+1} = RS4_t \boxplus V34_t$

end for

LFSR Initialization:

$\text{LFSR} = TV_3 \mid 0\text{x}1000$

B. *Features of s box*

S- Box used in humming bird for reduce the area and power consumption the four S-boxes can be reduced in single S-box which is repeated four times in the 16 bit block cipher. This algorithm is used to improve the security. [7]

TABLE-I

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S1(x)	8	6	5	F	1	C	A	9	E	B	2	4	7	0	D	3
S2(x)	0	7	E	1	5	B	8	2	3	A	D	6	F	C	4	9
S3(x)	2	E	F	5	C	1	9	A	B	4	6	8	0	7	3	D
S4(x)	0	7	3	4	C	1	8	F	D	E	6	B	2	8	9	5

Table 1.Four S-box in hexadecimal notation

C. *16 bit block cipher*

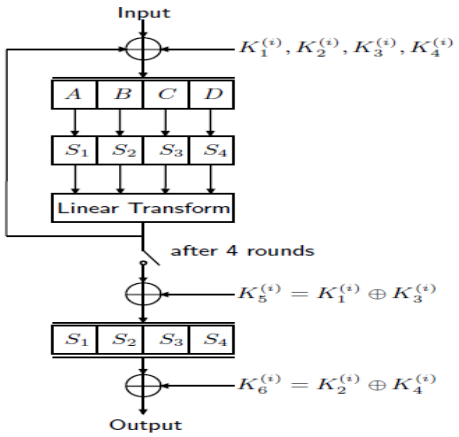

Fig. 5 Block diagram of Block Cipher

Humming bird employs four identical block cipher Eki (i =1, 2, 3, 4) in a consecutive manner. Each of which is a typical

substitution – permutation (SP) network with 16- bit block size and 64-bit key as shown in the following. The block cipher consists of four regular rounds and a final round. The 64 bit sub key Ki is split into four 16 bit round key k(i)5 and k(i)6 directly derived from the four round keys. While each regular round comprises of a key mixing step, a substitution layer and permutation layer, the final round only includes the key mixing and the s-box substitution steps[4]. The key mixing step is implemented using a simple exclusive-OR operation, where as the substitution layer composed of four S-boxes with 4 bit input and 4 bit output. [8]

D. Encryption process

The overall structure of the humming bird encryption algorithm is depicted in figure. Content of the first internal state register RS1.[5][7] The result of the addition is then encrypted by the first block cipher EK1. This procedure is repeated in a similar manner for another three times and the output of EK4 is the corresponding cipher text CTi. Based on their current states, the outputs of the first three block cipher, and the states of the LFSR.[14]

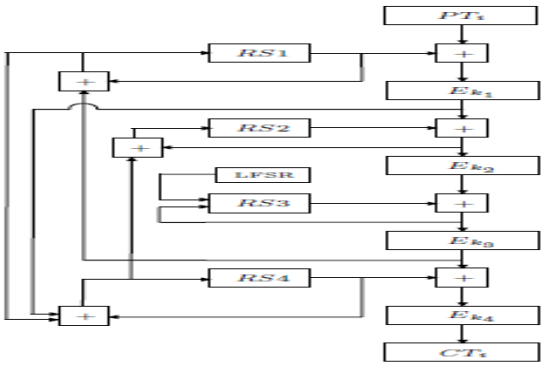

Fig 6 Block diagram of Encryption process

E. FPGA Implementation of humming bird

The improved new ultra light weight cryptographic algorithm has coded by using VHDL.[10] FPGA implementation of a humming bird can be implement an encryption and decryption core on the low cost Xilinx FPGA series of SPARTAN 3 provide enough flexibility for various Application.[5] [9].

In this humming bird algorithm can be implemented in folding architecture. It achieve reduce area and high throughput. It resists attacks and it will be implemented in several applications like smart card, wireless sensor and communication channels for improve the security. The experimental result shows that this algorithm has higher security and throughput with improved area than the existing algorithms.[1] Recently this humming bird cryptographic algorithm is using in twitter to improve the security. It achieves no memory blocks occupation

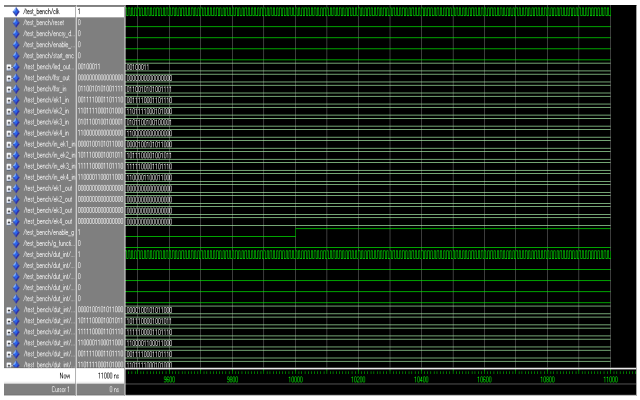

Fig.7 The simulation result of packaging

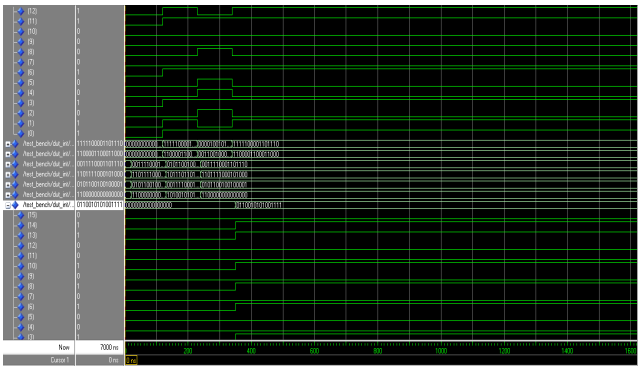

Fig. 8 The simulation result of initialization algorithm

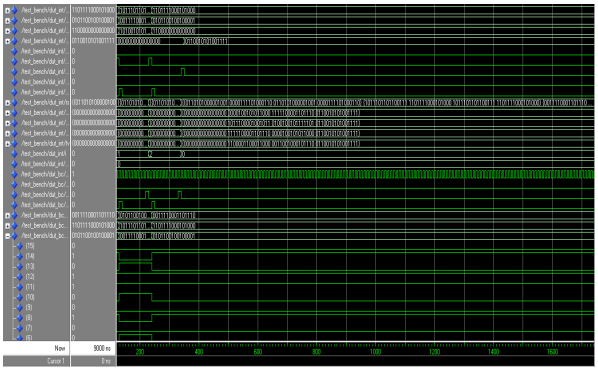

Fig. 9 The simulation result of block cipher

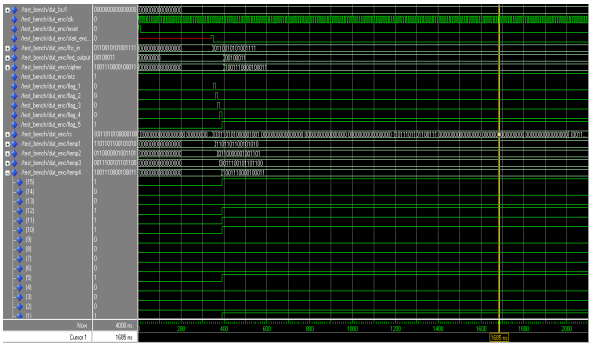

Fig. 10The simulation result of encryption process

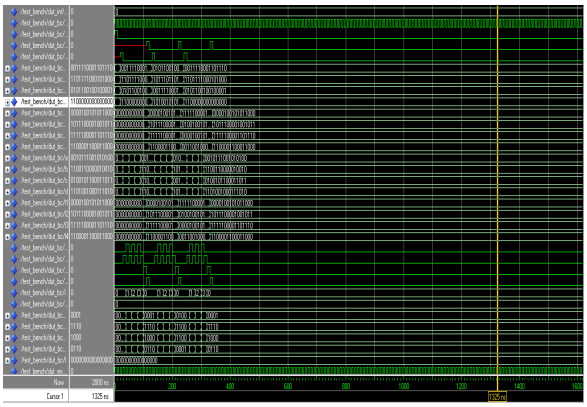

Fig. 11 The simulation result of humming bird algorithm

TABLE-II

RESULT OF HUMMING BIRD ALGORITHM DESIGN			
AREA (NUMBER OF SLICES)	**MEMORY (BLOCKS)**	**FREQUENCY (MHZ)**	**THROUGHPUT (MBPS)**
34	**0**	**222.64**	**84.68**

Table II. Result of Humming bird algorithm

3. CONCLUSIONS

This work presents the most efficient FPGA implementation of the new ultra light weight humming bird cryptographic algorithm can be implemented in folding architecture. High throughput can be obtained and it will reduce the area. It achieved a stringent response time and power requirements which can provide the design security with a small block size. It achieves no memory blocks occupation and overall the performance will be increased.

For the future research, we intend to conduct further using embedded co processor of cryptanalysis humming bird algorithm to achieve high speed are interact in future.

ACKNOWLEDGMENTS

I would like to thank our chairman Mr.R.Thirunavukarasu, Managing Director Mr.T.Senthilkumar,advisor Mr. S. Kodhandapani , principal Dr .B. Gopi for encouraging and providing necessary facilities towards the growth carrying this work. The authors knowledge with the help of Mrs. G. Kavitha.M.E., Arasu Engineering College Tamilnadu in assisting me towards implemented the project work.

REFERENCES

[1] Eisebarth.T, Kumar.S, Paar.C, Poscmann.C, and Uhsadel.L "A Survey of Lightweight Cryptography Implementations", IEEE Design computer Vol 24.No.6.

[2] Harikrishnan T and C.Babu" Cryptanalysis of Hummingbird Algorithm with Improved Security and Throughput" 2015 International Conference on VLSI Systems, Architecture, Technology and Applications (VLSI-SA TA)

[3] Nikita Arora and Yogita Gigras, "FPGA Implementation of Low Power and High Speed Hummingbird Cryptographic Algorithm", International Journal Computer Applications(0975-8887) Volume 92-No.16,April 2014,42

[4] Reena Bhatia, "Study of Hummingbird Cryptographic Algorithm based on FPGA Implementation", 2014 IJCSIT International Journal of ComputerScience and Information Technologies, Vol.5 (3),2014, 4426-4430

[5] Rabban.M and Ramprakash.R, "Design of Hummingbird Algorithm forAdvanced Crypto Systems", 2014 IJEDR, Volume 2,Issue 1,ISSN:2321 9939,385-387.

[6] Revini S. Shende, Mrs. Anagha Y. Deshpande, "VLSI Design of Secure Cryptographic Algorithm", International Journal of Engineering Research and Applications(IJERA) ISSN:2248-9622 Vol. 3,Issue 2,Marchpp.742-746.

[7] Xinxin Fan, Guang Gong, Lauffenburger, Hicks, "FPGA implementationof the Hummingbird cryptographic algorithm", 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp.48

[8] P. Chodowiec and K. Gaj, "Very Compact FPGA Implementationof the AES Algorithm," in Cryptographic Hardware and Embedded Systems - CHES 2003. vol. 2779, C. Walter, c,:. Koy,and C. Paar, Eds., ed: Springer Berlin Heidelberg, 2003, pp. 319-333.

[9] R. Raja Raja and D. Pavithra, "Implementation of hardware efficient light weight encryption method," in Communications and Signal Processing (lCCSP), 20i3 International Conference on, 2013, pp. 191-195.

[10] T. San and N. At, "Compact Hardware Architecture for Hummingbird Cryptographic Algorithm," in Field Programmable Logic and Applications (FPL), 201i International Conference on, 2011, pp. 376-381.

[11] X. F. Daniel Engels, Guang Gong, Honggang Hu, Eric M. Smith, "Ultra-Lightweight Cryptography for Low-Cost RFlD Tags: Hummingbird Algorithm and Protocol," FC'IO Proceedings of the 14th international conference on Financial cryptography and data security,Springer-Verlag Berlin, Heidelberg ©20JO,vol. ISBN:3-642-14991-X 978-3-642-14991-7, pp. 3-18 2010.

[12] M. Biao, R. C. C. Cheung, and H. Yan, "FPGA-based high throughput and area-efficient architectures of the Hummingbird cryptography," in IECON 2011 - 37th Annual Conference on IEEE industrial Electronics Society, 20 II, pp. 3998-4002.

[13] D. Engels, X. Fan, G. Gong, H. Hu, and E. Smith, "Hummingbird: Ultra-light weight Cryptography for Resource Constrained Devices," in Financial Cryptography and Data Security. vol. 6054, R. Sion, R. Curtmola, S. Dietrich, A. Kiayias,J. Miret, K. Sako, et al., Eds., ed: Springer Berlin Heidelberg,2010, pp. 3-18.

[14] Y. E. Salehani and A. Youssef, "Differential fault analysis of Hummingbird," in Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on, 2011, pp. 357-361.

[15] X. Mengqin, S. Xiang, W. Junyu, and J. Crop, "Design of a UHF RFID tag baseband with the hummingbird cryptographic engine," In ASIC (ASiCON), 2011 IEEE 9th internationasl Conference on,2011, pp. 800-803.