International Journal of Advanced and Innovative Research (2278-7844) / Volume 7 Issue 3

DESIGN AND IMPLEMENTATION OF HUMMINGBIRD CRYPTOGRAPHY USING ADVANCE DATAFLOW BASED S-BOX

Diksha Mehta, GGITS, Jabalpur
Prof. Utsav Malviya, GGITS, Jabalpur
Prof Sunil Saha, GGITS, Jabalpur

Abstract: Hummingbird is a lightweight calculation which comprises of piece figure of 256-piece key and scrambles a 16-bit information in one activity. In this theory, a square figure for hummingbird calculation is composed and actualized over Vertex FPGA. The encryption and unscrambling unit are composed independently lastly, it is watched that the decoded result flawlessly coordinates with principle information. The proposed engineering is intended to keep minimal with the goal that rest of reconfigurable territories of FPGA can be proficiently utilized for different purposes. As conservativeness is important for frameworks implanted with cryptography part, we expect that the proposed configuration can demonstrate specialized value.

Keywords: Advance encryption System (AES), Secured & fast encryption routine (SAFAR), VHSIC Hardware Description Language (VHDL), Hummingbird cipher(HC)

I-INTRODUCTION

Hummingbird encryption is a 8 round Feistel coordinate with a square size of 64 bits, and a key length of 128 bits. The round capacity comprises of an external capacity FO. This external capacity is thus worked from an inward capacity. HUMMINGBIRD is a square figure utilized as a part of UMTS, GSM, and GPRS portable interchanges frameworks. In UMTS, HUMMINGBIRD is utilized as a part of the classification (f8) and respectability calculations (f9) with names UEA1 and UIA1, individually. In GSM, HUMMINGBIRD is utilized as a part of the A5/3 enter stream generator and in GPRS in the GEA3 key stream generator. Murmuring winged animal is another ultra-light weight cryptographic calculation focused for asset – compelled gadgets like RFID labels smartcards and remote sensor hubs. In this theory, we depict productive equipment executions of a remain solitary Hummingbird segment in field-programmable door cluster (FPGA) gadgets. We actualize an encryption just center and an encryption/unscrambling center on the ease Xilinx FPGA arrangement Vertex-3 and contrast our outcomes and other announced lightweight square figure executions on a similar arrangement. Our test comes about feature that with regards to minimal effort FPGA usage Hummingbird has ideal effectiveness and low zone prerequisites.

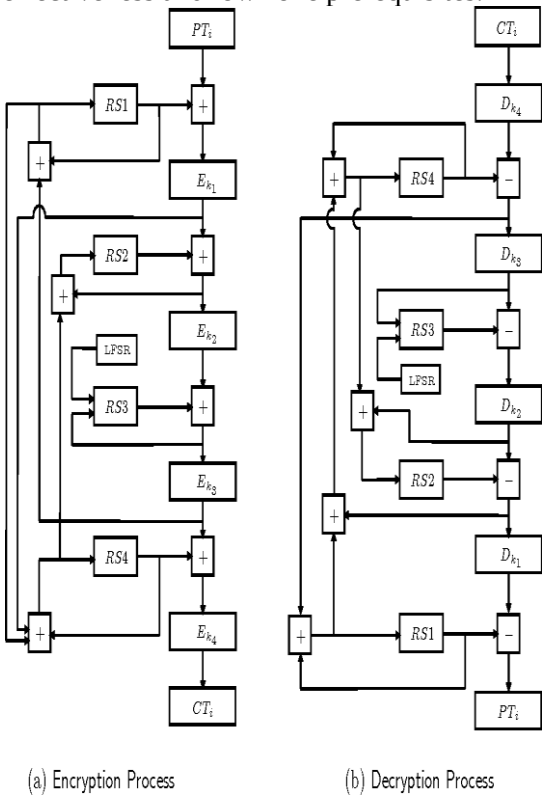


Figure 1.1 Humming Bird Encryption Process

Hummingbird is an encryption and message validation crude that has a 256-piece mystery key, utilizes a 64-bit nonce and alternatively delivers a 64-bit authenticator for the message. RFID frameworks can be arranged by label cost, with unique excellence between high-cost and ease labels. Our examination work centers

©2018 IJAIR. All Rights Reserved

predominantly around minimal effort RFID labels. An underlying examination and investigation of the cutting edge recognizes the requirement for lightweight cryptographic arrangements reasonable for these exceptionally obliged gadgets. From a simply hypothetical perspective, standard cryptographic arrangements might be a right approach. Notwithstanding, standard cryptographic natives (hash capacities, message validation codes, square/stream figures, and so forth.) are very requesting regarding circuit measure, control utilization and memory estimate, so they make exorbitant answers for ease RFID labels. Lightweight cryptography is consequently a squeezing need.

II-PROPOSED DESIGN

This theory introduced the effective FPGA usage of the ultra-lightweight cryptographic calculation Hummingbird. The proposed speed advanced Hummingbird encryption/decoding centers can scramble or unscramble a 16-bit message obstruct with 4 clock cycles, after an instatement procedure of 20 clock cycles. Contrasted with other lightweight FPGA executions of piece figures XTEA, ICEBERG, SEA and AES, Hummingbird can accomplish bigger throughput with littler zone prerequisite. Therefore, Hummingbird can be considered as a perfect cryptographic crude for asset compelled situations. Figure 1 demonstrates the design of proposed work which mirrors the thought behind the new rationale for engineering as clarify above.

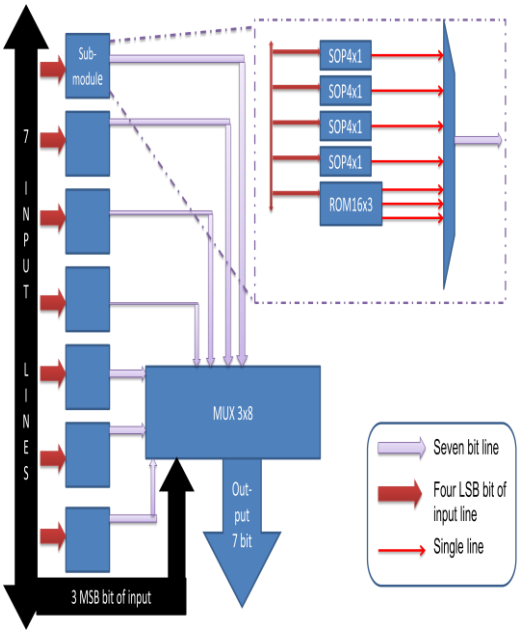


Figure 2: Proposed architecture S7 box

Figure 2 demonstrates the proposed s7 box and s9 confine is additionally been planned comparable path as can be seen that proposed configuration is a criticism pipeline engineering and here two distinctive module (combinational rationale, EPROM) are been utilized aggregate 8 times and at each time it stores the incentive in new cushion after eight cycle we have add up to 8 an incentive in 8 unique cradles at that point by utilizing upper four bits of info we extricate the last yield.

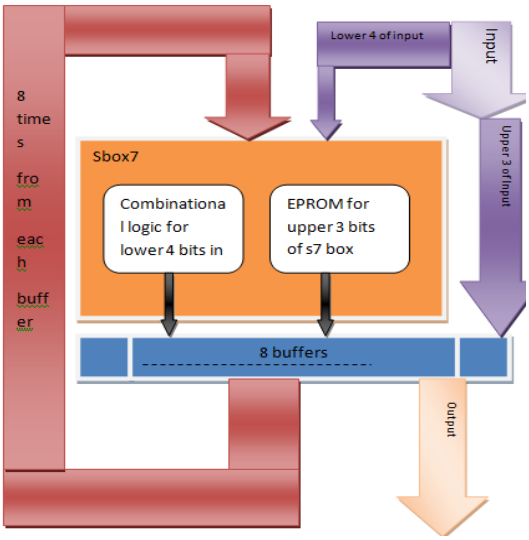


Figure 3 the new pipelined S7-box architecture

Hummingbird-2 has been actualized in equipment and in programming for different microcontroller designs. Capacities were composed in low level computing construct and hand-advanced for all stages. All library capacities are C-callable and numerous improvement conditions are upheld. As Hummingbird-2 calculation takes into account exchange offs between execution speed and size, we have actualized up to three programming usage profiles for some microcontroller stages. Piece figure is fundamental piece of hummingbird calculation which gives aversion from different assaults,

©2018 IJAIR. All Rights Reserved
http://ijairjournal.com

for example, direct assault, differential assault, and insertion assault.

Square figure scrambles 16 bit information pieces utilizing 64 bit sub key. Piece figure contain four general rounds and a last round. Every customary round contains three stages, for example, key blending step, substitution step and change step. In key blending step information square is blended with round key. Here four 16 bit round key k_0^i,k_1^i,k_2^i,k_3^i is assessed from 64 bit sub enter and utilized as a part of ensuing four rounds. In square figure last cycle two more keys is utilized that are k_4^i,k_5^iwhich are assessed from past four keys

The chose four S-boxes, meant by s_i (x)=F_2^4→ F_2^4,i=0,1,2,3 are Serpent-type S-boxes with extra properties which can guarantee that the 16-bit piece figure is impervious to straight and differential assaults and also insertion assault [11], [1]. The stage layer is actualized by straight change. The fundamental piece graph of figure square is appeared in the Fig 3.3, A notable general encryption calculation for square figure is appeared in [11] which is given underneath.

Algorithm 16-bit Block cipher encryption $E_{ki}(.)$
Input: A 16-bit data block $m = (m_0, m_1, m_2, \ldots\ldots m_{15},)$ and a 64-bit subkey k_i such that subkey $k_i = K_0^{(i)}|K_1^{(i)}|K_2^{(i)}|K_3^{(i)}$
Output: A 16-bit data block $m' = (m'_0, m'_0, \ldots\ldots m'_{15})$
1. for j=1 to 4 do
2. $m <- m \oplus K_j^{(i)}$ [key mixing step]
3. $A = m_0 \mid m_1 \mid m_3 \mid m_3$, $B = m_4 \mid m_5 \mid m_6 \mid m_7$
C $= m_8 \mid m_9 \mid m_{10} \mid m_{11}$, D $= m_{12} \mid m_{13} \mid m_{14} \mid m_{15}$
4. $m <- S_1(A)|S_2(B)|S_3(C)|S_4(D)$ [substitution layer]
5. $m <- m \oplus (m \ll 6) \oplus (m \ll 10)$ [permutation layer]
6. end (for)
7. $m <- m \oplus K_0^{(i)} \oplus K_2^{(i)}$
8. $A = m_0 \mid m_1 \mid m_3 \mid m_3$, $B = m_4 \mid m_5 \mid m_6 \mid m_7$
C $= m_8 \mid m_9 \mid m_{10} \mid m_{11}$, D $= m_{12} \mid m_{13} \mid m_{14} \mid m_{15}$
9. $m <- S_1(A)|S_2(B)|S_3(C)|S_4(D)$ 10. m' m $\oplus$K1
10. $m' <- m \oplus K_0^{(i)} \oplus K_3^{(i)}$
11. return $m' = (m'_0, m'_0, \ldots\ldots m'_{15})$

We plan to work on design and implementation of the algorithm with our proposed S box. The proposed architecture is explained in next section. In this thesis, the cipher block is presented by new expressions. The encryption and decryption block is designed separately. For the S block and the Inverse S block, all the equations against the notation are evaluated using truth table and Karnaugh map. The hexadecimal notation for S_1 (x) is shown in [11]. The Boolean functions for S_2 (x)against the notation showed in Table II and the Boolean functions for inverse S box is shown in Table III. The flow chart of proposed encryption and decryption unit is depicted in Fig. 3.4 and Fig. 3.5. In Fig. 3.4 and Fig. 3.5, it is seen that, there is 64 bit sub key is used with 16 bit round keys. Here, basic structure of the cipher block in hummingbird is maintained. It is clearly seen from both figures, the decryption process is the mirror image of the encryption process. By using these notations equations are evaluated for s box and inverse s box

Bit	Boolean function
S[0]	(x[2]&~x[1]&~x[0])|(~x[3]&~x[2]&x[1])|(x[3]&x[2]&x[1])|(x[2]&x[1]&x[0])|(x[3]&~x[2]&~x[1]&x[0])
S[1]	(x[3]&~x[2]&~x[1])|(x[3]&~x[1]&~x[0])|(x[3]&~x[2]&~x[0])|(~x[3]&~x[2]&x[0])|(~x[3]&x[2]&x[1]&~x[0])|(x[3]&x[2]&x[1]&x[0])
S[2]	(~x[3]&~x[1]&x[0])|(x[3]&~x[1]&~x[0])|(~x[3]&~x[2]&x[1])|(x[3]&x[2]&~x[0])|(~x[2]&x[1]&x[0])
S[3]	(~x[2]&~x[1]&~x[0])|(x[3]&~x[2]&~x[1])|(~x[3]&x[2]&x[0])|(~x[3]&x[1]&x[0])|(x[2]&x[1]&~x[0])

Table 1 Proposed Expressions of S-box

For inverse S –box, S box notation is considered as input and x is considered as output

Decryption Bit	Boolean function

©2018 IJAIR. All Rights Reserved

X[3]	(~s[3]&~s[1]&~s[0]) | (~s[3]&~s[2]&s[1]) | (~s[3]&s[1]&s[0])| (~s[2]&s[1]&s[0]) | (s[3]&s[2]&~s[1]&s[0]) | (s[3]&s[2]&s[1]&~s[0]));
X[2]	((~s[3]&~s[2]&~s[1]) | (~s[3]&s[1]&s[0]) | (s[3]&s[2]&~s[1]) | (s[3]&~s[1]&s[0]) | (s[3]&~s[2]&s[1]&~s[0]));
X[1]	((~s[3]&s[2]&~s[1]) | (~s[3]&~s[2]&s[1]) | (~s[2]&s[1]&~s[0]) | (s[3]&s[2]&s[0]) | (s[3]&~s[1]&s[0]));
X[0]	((~s[3]&~s[1]&~s[0]) | (s[2]&~s[1]&~s[0]) | (s[3]&~s[2]&s[0]) | (s[3]&s[1]&s[0]) | (~s[2]&s[1]&s[0]) | (~s[3]&s[2]&~s[0]));

Table 2 Proposed Boolean Functions of Inverse S Box

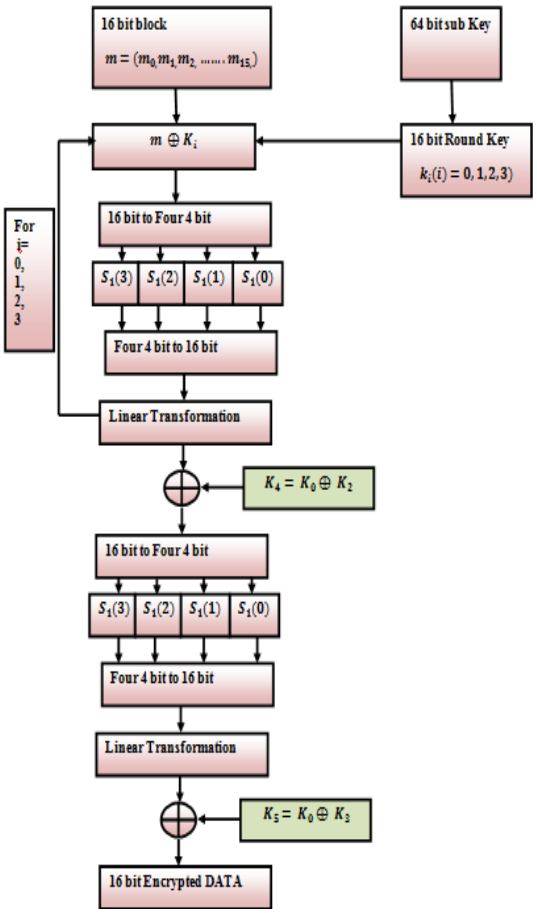


Fig. 3: Flow Graph of Proposed Encryption Unit of Block cipher.

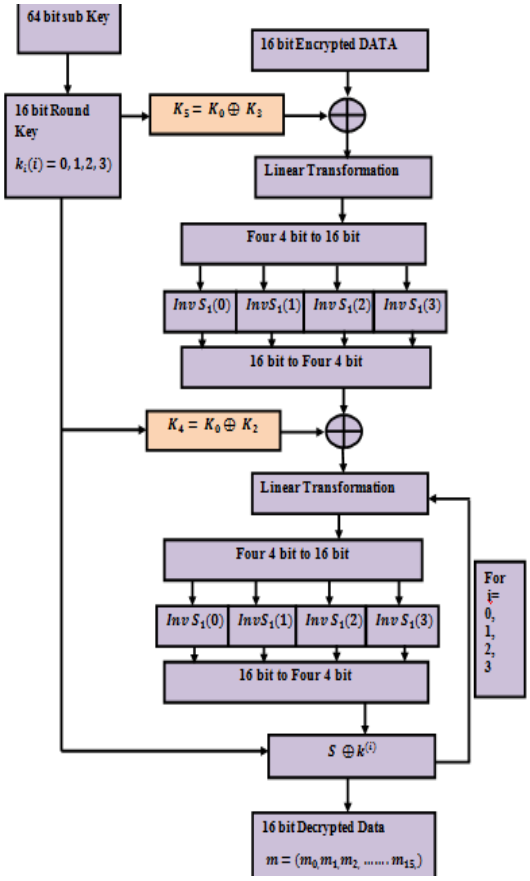


Fig. 4: Flow Graph of Proposed Decryption Unit of Block cipher.

III-RESULTS

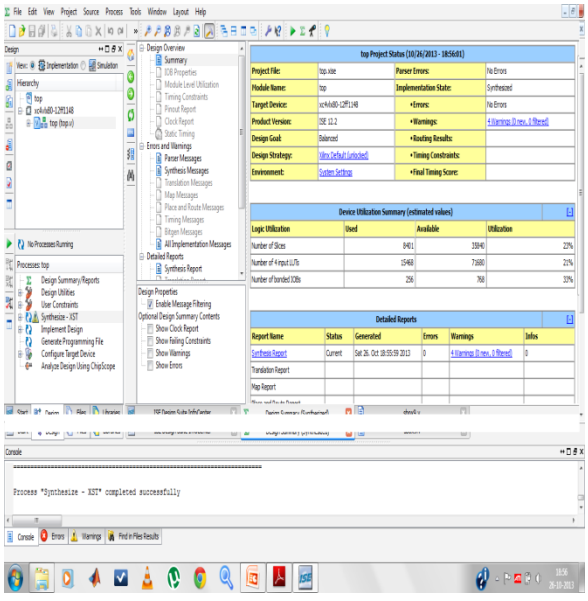


Figure 5 Synthesis Hummingbird Cipher

©2018 IJAIR. All Rights Reserved

FI	**19.855ns (13.045ns logic, 6.810ns route (65.7% logic, 34.3% route)**
FO	25.592ns (11.216ns logic, 14.376ns route) (43.8% logic, 56.2% route)
FL	5.532ns (4.303ns logic, 1.229ns route) (77.8% logic, 22.2% route)
S7box	7.654ns (6.067ns logic, 1.587ns route) (79.3% logic, 20.7% route)
S9box	10.143ns (7.279ns logic, 2.864ns route) (71.8% logic, 28.2% route)
Proposed Overall HUMMINGBIRD	98.916ns (33.643ns logic, 65.273ns route)(34.0% logic, 66.0% route)

Table 3 Timing summary of each module

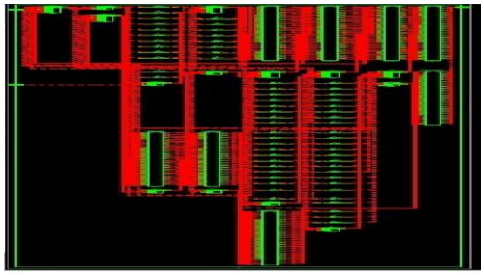
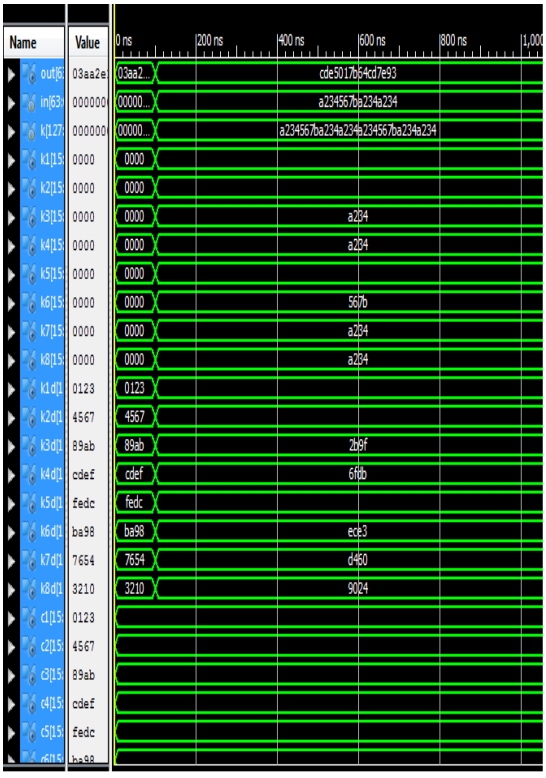


Figure 6 the HUMMINGBIRD cipher RTL



schematics

Figure 7 The HUMMINGBIRD cipher Simulation

From the simulation as shown in above slides
Key :a234567ba234a234a234567ba234a234
Result:-1
Output: cde5017b64cd7e93
Input: A234567ba234a234
Output^Input: 6fd15700c6f9dca7
Avalanche: 41 bit change/64 bit
Result:-2
Output: df5ab6daed24e9c5
Input: A234a234567ba234
Output^Input: 7d6e14eebb5f4bf1
Avalanche: 45 bit change/64 bit

Parameters	Design of FI	Design of FO	Design of FL	Design of Sbox-7	Design of Sbox-9	Complete Hummingbird module
No. of slice	429	1379	18	26	157	8401
No. of LUT's	782	2541	32	52	289	15468
No. of IOB's Logical Time delay	13.04 ns	11.216 ns	4.303 ns	6.067 ns	7.279 ns	33.64 ns

Table 4: Results for each module

Table 4above demonstrates the blend aftereffects of murmuring fowl cryptography strategy saw in the wake of composing RTL content of the outline on Xilinx. The amalgamation comes about are of every module of Humming winged creature encryption and full outline the LUT and number of cuts are the region resport and Time delay is the speed report of the proposed plan.

Table demonstrates the outcomes saw at the different reflection levels as the proposed configuration is an outline with basic displaying thus it has numerous diverse squares which are been composed and incorporate contrastingly and after that join as definite plan, table demonstrates the individual

©2018 IJAIR. All Rights Reserved
http://ijairjournal.com

plan and coordinated outline watched integrate comes about.

Relative RESULTS: Table 5 beneath is the similar aftereffects of proposed outline and the accessible work it looks at the outcomes as far as zone, speed and power.

	Parameters	Stavroula Mammou et al [1]		Xinxin Fan et al [2]		Proposed work	
S-box design		S-box 7 (S7)	S-box 9 (S9)	S-box 7 (S7)	S-box 9 (S9)	S-box 7 (S7)	S-box 9 (S9)
	No. of slice	34	169	-	-	26	157
	Logical Time delay (ns)	-	-	-	-	6.067	7.279
Overall Hummingbird encryption design	No. of slice	8784		8770		8401	
	Logical Time delay (ns)	34.01		-		33.64	

Table 5: Comparative Results for each module

Reproduction is been taken for different conceivable information input and been checked with various key's and watched revise encryption the aggregate torrential slide (change in figure from the information and number of bit change for one piece change in input information) saw in the middle of 43-48 for 64 bit information which is right around 80-85% change in figure and it is superior to anything accessible strategies like AES,[21],[23], DES[22], , HUMMINGBIRD and TEA[18],[19],[2].

IV-CONCLUSION

We have introduced Hummingbird-2, a lightweight confirmed encryption calculation that we accept to be impervious to every single standard assault to piece figures and stream figures, for example, differential and straight cryptanalysis, structure assaults and different mathematical assaults. Hummingbird-2 additionally has the further preferred standpoint of being impervious to picked IV assaults. We have likewise exhibited consequences of programming and equipment executions of Hummingbird-2. Hummingbird-2 can be executed with minimal in excess of 2000 door counterparts, influencing it to appropriate for universal gadgets, for example, RFID labels and sensors. Hummingbird-2 has the extra preferred standpoint over other lightweight encryption natives that it delivers a message confirmation code.

REFERENCES

[1] Stavroula Mammou, Dimitrios Balobas and Nikos Konofaos, A VHDL execution of the Hummingbird cryptographic algorithm,2017 Panhellenic Conference on Electronics and Communication (PACET), This work was bolstered by the Research Projects for Excellence IKY/SIEMENS., 978-1-5386-2287-2/17/IEEE

[2] Xinxin Fan and Guang Gong, Ken Lauffenburger, Troy HicksFPGA Implementations of the Hummingbird Cryptographic Algorithm, Thesis exhibited at seventh global meeting on RFID Security and Privacy (RFIDSec), USA, 26-28 June 2017.

[3] Revini S. Shende, Mrs. Anagha Y. Deshpande, VLSI Design Of Secure Cryptographic Algorithm, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 2, March - April 2013, pp.742-746 742

[4] Reena Bhatia, Study of Hummingbird Cryptographic Algorithms in light of FPGA Implementation,/(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4426-4430

[5] Ismail San, Nuray At, Enhanced FPGA Implementation of the Hummingbird Cryptographic Algorithm, to show up in the procedures of the fourteenth International Conference on Financial Cryptography and Data Security - FC 2015, 2015.

©2018 IJAIR. All Rights Reserved