ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

FPGA Implementations of the Humming Bird Cryptographic Algorithm

Ganam Thirumalesh
M.Tech,(VLSI Design),
Department of ECE,
Siddhartha Institute of Engineering and Technology.

T Krishnarjuna Rao, M.Tech
Associate Professor,
Department of ECE,
Siddhartha Institute of Engineering and Technology.

ABSTRACT:

Humming bird is a new ultra-light weight cryptographic algorithm targeted for resource – constrained devices like RFID tags smartcards and wireless sensor nodes. In this paper, we describe efficient hardware implementations of a stand-alone Hummingbird component in field-programmable gate array (FPGA) devices. We implement an encryption only core and an encryption/decryption core on the low-cost Xilinx FPGA series Spartan-3 and compare our results with other reported lightweight block cipher implementations on the same series. Our experimental results highlight that in the context of low-cost FPGA implementation Hummingbird has favorable efficiency and low area requirements. Hummingbirdisan encryptionand messageauthentication primitivethat has a256-bit secretkey, usesa64-bitnonceand optionally producesa64-bitauthenticatorforthemessage.

RFID systems can be classified according to tag price, with distinction between high-cost and low-cost tags. Our research work focuses mainly on low-cost RFID tags. All the synthesis and simulation results are performed on Xilinx ISE 14.4 using VHDL.

Key words: ***Lightweight cryptographic primitive, resource-constrained devices, FPGA implementations***

INTRODUCTION

Radio Frequency Identification (RFID) is rapidly developing technology enabling automatic object identification. In an RFID system, each object islabeled with a small transponder, calledanRFID tag, whichreceivesandresponds toradio-frequencyqueries fromatransceiver, calledanRFID reader.AnRFID tagiscomposedofatinyintegrated circuit forstoring and processing identificationinformation, aswellasaradio antenna forwirelessdata transmissions. FID tags usually haveconstrainedcapabilities in every aspect ofcomputation, communicationandstorage duet the extremely low production cost. There are various applications for low-cost and low-power tags such as animal identification, point-of-sales, and inventory management and so on.

Despite the lowcostofRFID systems and their convenienceinidentifying anobject withoutphysical contact,theradiocommunicationsbetween RFID tagsandreaders also raiseanumber of security issues.Forexample,today'sRFID systemsdonotconduct the mutualauthenticationbetween RFID readers and tags, soitiseasyforanadversary to impersonateareader oratag to obtain sensitive information,and even launch Denial ofService(DOS) attacks.Moreover, RFID tags automatically emit their unique identify- fiersupon reader interrogationwithoutalerting their users. Consequently, an adversary equipped withcommodity RFID reader's caneffectivelytrace apersoncarrying atagged item bylinking twodifferentsightings ofthe

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

sameRFID tag, whichpotentiallyviolate the owner'sprivacy. Inaddition, many possiblesecurity threatsarise fromunprotected wirelesscommunicationsbetween RFID readers and tags.

To solve the aforementioned security and privacy issues, aprivacy-preservingmutual authenticationprotocolisrequiredforareaderandatagtoa uthenticateeachother. After themutualauthentication, onlyalegitimate readercanaccessthecontents oftagsandthe reader canbeassured thatthetagsareauthenticandhavenotbeencounterfeited atthe sametime. Whilealotofefforthasbeenmadeindesigningauthenticat ionprotocols forRFID systemsoverthepast few years, wefocusonthechallenge-response protocolsusing symmetric keycryptographyinthis paper. Toconduct themutualauthenticationbased onthechallenge-response techniques, RFIDtagsmustbeabletoexecutesecuresymmetric keyprimitives. In[9,10],Feldhoferet.al.proposed alow-powerand compact ASICcore for128-bit-keyAESwith3400gates.Their AESimplementationonlycontains oneS-box implementedas combinatoriallogicand can encrypt a 128-bit data block within 1032 clockcycles.The authorsalsoproposed asymmetric challenge-response authentication protocol whichcanbeintegratedintotheexisting ISO/IEC18000standard.Other workalong the lineoffinding more compact AESimplementations,sayHämalainenet. al.'s workinordesigningnewlightcryptographicschemes, suchasinLeander et.al. Suggested alightweightDESvariantcalledDESL (DESLightweight), inBogdanovet. Al.described anultra-lightweightSP-networkbasedblockcipherPRESENT.Particularly, aerial version of PRESENT can be implemented more compactly. Feldhoferet.al.'salgorithm inforintegratingAESintotheISO/IEC18000standard specificallytargetstheISO18000-3protocols.

ThesearеHighFrequency (HF) protocols, i.e.13.56MHz, wherelow powerandsmallsizearenotsignificantadvantages.EPCg lobalclass-1generation-2(EPC Gen2inbrief) was approved asISO18000-6CinJuly2006.It iswidelybelievedthatGen2tagswillbethemainstreamfo rRFIDapplicationsbecauseof thelargeeffectivereadingrange.NotethatEPCGen2proto colsare Ultrahigh Frequency (UHF) protocolswhichrequireimplementationsthataresignific antlymorepowerefficient and faster than the minimums required at HF. However, thevery slownature ofAES requires modification totheISO18000-3protocol forth challenge-response to work.

In this paper, wepresentanewultra-lightweightencryption scheme, referred to as Hummingbird, whicharedesigned byEngels, Schultz, Schweitzer and Smith, forlow-cost RFID tags and embedded microchips. Hummingbirdhasahybrid structureofblockcipher and stream cipher and wasdeveloped with aminimal hardware footprintinmind. The hybrid modelcanprovide the designed security with smallblocksizeand isthere-foreexpected tomeet the stringentresponse time and powerconsumptionrequirements describedintheISO18000-6Cprotocolwithoutanymodification of thecurrentstandard.

LITERATURE SURVEY

Cryptography is a technique that makes messages not readable by unauthorized persons, by the use of encoding method for information (messages). Thus the resultant message is non- readable and helps to hide the information. In this way it gives security to maintain confidentiality. Some of the application of cryptography includes the security of ATM cards, computer passwords and electronic commerce. Cryptography is derived from the Greek words krypton (hidden) and graphs (written) respectively. Cryptography involves two processes. These are encryption and decryption. Encryption converts the plain text to cipher text. Decryption converts cipher

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

text to plain text. Cryptography based on key used are classified as private key and public key cryptography. In private key cryptography both encrypt or and decrypt or uses same key, that is shared between them only.example: AES, DES. In public key (asymmetric key cryptography) the encryption key is not hidden i.e. it is public, while another key called private key is used for decryption so two keys used are different it is also called as asymmetric key cryptography. It is more secure than private key cryptography. Examples are RSA and ECC. Key is used in the process of conversion of plaintext to cipher text. Key used is usually larger one and is measured in bits. As the length of key increases the security of cryptographic algorithm also increases. The motivation that tends to study the cryptographic algorithm is the requirement of protecting given information. There are 3 important aspects of security that requires to be consider are confidentiality, integrity & availability.

1. Confidentiality: This property deals about let the information private from unauthorized one and makes it only accessed by the authorized ones.
2. Integrity: It ensures that the message sent by sender is received at the receiver end as it was, without any modification or error.
3. Availability: It ensures that one that has the permission to access information have to get it when needed. In today's modern life, there is evermore care is needed to protect our information. So it is necessary to study the cryptographic algorithm. The various cryptographic methods like AES, DES have been failed to meet the requirements of low level devices especially in control system, this leads to the innovation of ultra lightweight cryptography, and hummingbird cryptography is one of such method. Lightweight cryptography is new research area. These algorithms try to have lower area, lower power, low cost and less processing time. Hummingbird cryptography can be considered as a FSM because of combination of block cipher and stream cipher. It includes continuous updating of internal state register. Thus easy to understand and leads to better security for control system application.

THEORY OF LIGHTWEIGHT CRYPTOGRAPHY

Design new ciphers with the goal of having low hardware implementation costs.Lightweight Cryptography is a modern scientific sub-division and it is positioned at the site of intersection of electrical engineering, cryptography and computer science. It concentrates on efficient implementation and new design options of cryptographic protocols. Due to cost constraint and strong model for attacks like possible physical attacks, there is ever growing obligation for lightweight security solutions.

The lightweight cryptography always copes with the compromise between security, cost and performance. Forblock ciphers the key length itself provides a compromise between security and cost, the number of rounds usedgives the compromise of security and performance and the hardware architecture results tradeoff between costand performance.Usually any two out of the three designing goals like security and low cost, security and performance or lowcost and performance are optimized in an easy way. But it is found that it is very hard to achieve optimization
Of all the three design goals at a given time. For example: the pipelined architecture results a high performanceand good secured implementation but it requires large area, which takes more cost. In the same way secured andlow cost hardware implementation is possible with the disadvantage of low performance. Generally there arethree methodologies for yielding cryptographic primitives for lightweight applications like passive RFID tags. Thethree approaches are mentioned below:

1) Optimized low-cost implementations for standardized and trusted algorithms.
2) Slightly modify a well investigated and trusted cipher.

The main problem that arises due to first approach is due to the fact that most recent block ciphers were designed mainly concentrating on software implementation properties without taking care of hardware friendly properties. It is good approach for

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

algorithms that run in software on PCs and embedded devices. But if the requirement is to achieve low cost security on device where these two assumptions fails, it is found that at this situation many block cipher failed to give good result of performance. The second approach is to use well investigated ciphers. The design of which requires low hardware costs. Example for this type of cipher is data encryption standard (DES). It was designed in the year of 1970s and here the targeted platform was hardware. In the second approach, DES is slightly modified to get DESL. The drawback of DESL is due to the fact of insufficient key length for many of modern application, but here key whitening technique allows the enhancement of security level. Thus DESL results show the optimization potentials. Therefore, further reduction of hardware area requirements is achieved through the third approach and it leads to the design of ultra-lightweight ciphers like PRESENT, hummingbird.

A. Architecture strategies

An implementation of less cost smart devices like positive RFID tags or smart cards takes low area and low power consumption while considering throughput as a secondary interest. Usually, an RFID reader device used to read many devices requires a higher throughput with giving less importance to area and power consumption. With active smart devices like contact smart cards there is no strict power constraints but there is a timing and sometime energy constraints will occurs. Usually the implementation to meet the design goals of interest takes place in one of the three major hardware architecture options: Parallel(loop unrolled), round- wise and serial. A parallel block cipher implementation takes only one clock cycle for several round operation of encryption /decryption process. Usually these type of implementations are pipelined i.e. register are employed in the critical path thus increases the maximum clock frequency. Even though, the parallel implementation gives high throughput rates, it is rarely used for RFID application because it demands higher area and power requirements. These demands makes the parallel implementation of bloc cipher and stream ciphers are rarely suitable for passive RFID applications. In round-wise implementation, each round function of either block or stream cipher takes one clock cycle. It results, decreased area and power consumption with decreased throughput. With low power and low area, round-wise implementation is best suited for stream cipher and used as a reasonable options for block ciphers. In order to achieve low power consumption and area requirements, serial implementation can be used. In this case one clock cycle is required to process a fraction of one round. On the AES are achieved by serialization. But it is always not suitable cancelled by the overheads due to additional control logic. Even though, from the view of low power and low area, it is best suited for RFID like applications with the use of block cipher. The stream ciphers are usually implemented in a bit serial fashion.

B. Hardware properties of cryptographic building blocks

Rounds and the final internal state itself is considered as the cipher text. Note that regardless of strategy used for implementation, the internal cipher states are saved at each round. RAM and ROM are available in the case of software environment. But in case of low cost tag it is not possible. Most of the RFID tags usually have memory modules, these have minimum storage capacity. Including this, the read and write access with this memory module requires very much power. So it is better to store all variables and intermediate values in registers, instead of using external memory modules. Registers have flip-flops. To store a single bit flip-flops need a gate count ranging from 5:33GE to 12:33GE(gate equivalent). There are variety of flip-flops having complexity between these two extremes. By considering tradeoff between efficiency and supporting logic two flip- flops cells are obtained. These are called as scan flip- flops, which means they also can be used as multiplexers(MUX), which is a good feature to reduce the power consumption. It is found that storage of internal state requires at least 50% of total area and power. So there is need to concentrate on reducing storage required, while

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

implementing cryptographic algorithms for low cost application.

C. Combinatorial elements

The combinational elements includes basic Boolean operations like NOT, NAND, NOR, OR, AND and XOR. In addition to these the combinational elements includes some basic logic functions like multiplexers(MUX). In this case the gate count differs based on the standard cell library used. Note that hardware XOR and MUX are more expensive, with comparison to other Boolean operations.

D. Confusion and diffusion

This section includes overview of sequential and combinational logic elements and the discussion of important cryptographic properties like confusion and diffusion from the point of their hardware properties.

E. Internal state storage

Usually each ciphers have an internal state which is referred as cipher state and key state. If used cipher is block cipher, then cipher state is first initialized with the help of plain text or ciphertext and then modified using key, so it is also called as a key state. But if selected cipher is stream cipher, then the cipher state initialization requires both the initialization value and the key and then this initialized cipher state used to output the key stream. In case of block cipher, there are fixed number of Shannon was the first one who introduced the concept of confusion and diffusion in the cipher design for security.

These two are attractive properties for security purpose. In reality, most of the block ciphers are considered as product ciphers i.e. they are based on subsequent operation of confusion and diffusion. In a block cipher confusion is identified at a substitution layer and diffusion is identified at a permutation or at a mixing layer. In reality it is much difficult to identifying and separating the components that results to confusion and diffusion techniques. Some ciphers incorporate the arithmetic operations as a diffusion and confusion technique, but this increase the power and area requirements significantly. The most commonly used confusion method uses s-boxes. In the s-box a small amount of change in the input variable of s-box results a larger change in the output variable. Then the diffusion layer is employed to spread the resultant output of s-box quickly throughout the entire state. In classical way this can be done by the use of bit permutation. This bit permutation in hardware is realized using only wires without involving any transistors. Thus they become a efficient component. Note that complex diffusion techniques are also possible like mix-column layer employed in AES. But they require large hardware cost.

The use of s- boxes for block cipher or stream cipher results non- linearity. Usually look up table(LUT) approach is used to implement s-boxes in software. But this LUT design in hardware takes larger area because the mixing of combinatorial logic and ROM is not easy with standard design flow of hardware. If combinatorial implementation do not change the s- box internal structure then it leads to higher area requirements with number of input and output bits. If output bits of s-box are more, then it requires more Boolean equation, if input bits are more the Boolean equations are become more complicated. The interaction between cryptography and hardware implementation should be such that, it must be able to withstand the differential and linear cryptanalysis. This can be achieved by incorporating high non- linearity s-boxes, which itself requires high gate count.

HMMING BIRD CRYPTOGRAPHY ALGORITHM

Hummingbird cryptography takes into account both security and efficiency. Hummingbird cryptography starts with initialization process to initialize internal state registers, after that encryption process follows iteratively. Figure 1 describes the initialization and encryption process. This algorithm uses 256-bit key, 16-bit block of data and 4 internal state register each with 16-bit wide. The aim of initialization process is to get the initial value of LFSR.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

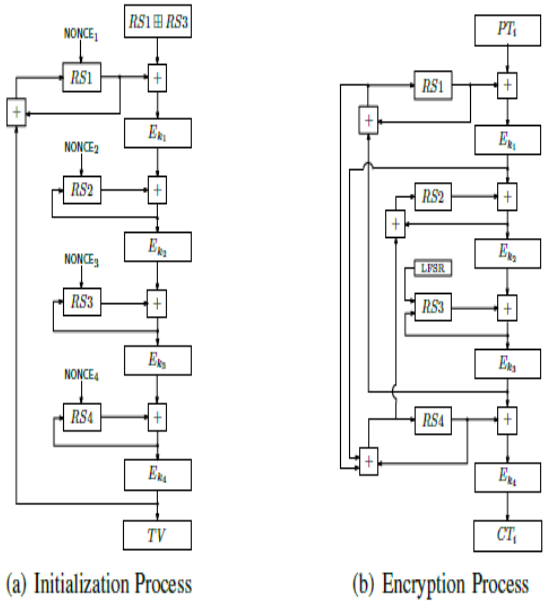

Figure1: (a) initialization process (b) encryption process.

Figure 2 shows the structure of block cipher used. Each block cipher uses 64-bit subkey, obtained from 256-bit
wide key. These subkeys are used by dividing them as 4 16-bit wide round keys for each round.

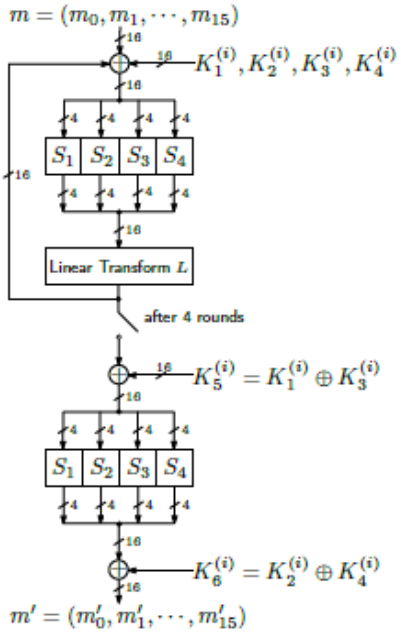

Figure2: structure of block cipher

In the paper[1] hummingbird cryptographic algorithm is developed on zero power 4-bit MARC4 microcontroller from Atmel and they compared the results with another lightweight algorithm PRESENT. The results shows that hummingbird has 58% faster throughput than PRESENT ATAM893-D microcontroller at 16khg, 500khg and 2Mhg.hummingbird can allow one block of data within 12ms with typical low power configuration of about 1.8v supply voltage. It shows that 4-bit microcontroller is one of the important for various security solution. In this, there is a need of further work for checking the hummingbird protocol for RFID tag and reader.

In the paper [2] they developed an encryption only core and an encryption/decryption core on low cost XILINX FPGA series sparton-3 and compared with other lightweight block cipher XTEG, ICEBERG on the same. It is found that hummingbird has favourable area and efficiency. The results shows that there is 4 clock cycles needed to decrypt 16-bit message block in addition to 20 clock cycles for initialization. In this paper[3] they implemented hummingbird cryptography on SMIC0.13m technology. It is ASIC implementation, they mainly concentrated on reducing power. The results shows that it has area of 2,225s equivalent and encrypt 16 bit data with 16 clock cycles plus 69 clock cycles for initialization. It consumes 1.08w for 1.2v power supply at 100KHg. In the paper[4] they implemented hummingbird cryptographic algorithm by coprocessor approach and serialized data processing principles. The work mainly reduces area, thus hardware implementation is provided by this work. In paper[5] they implemented lightweight remedial solution to saainen'n attack. This scheme is found efficient both in hardware and software due to the use of only 2 cyclic shifts, with maintaining compact design of hummingbird.

In the paper[6] they developed authentication protocol for RFID systems using hummingbird-2cryptographic algorithm, on battery less MSP430 based wisp-tag. The results shows effective and efficientsecurity to low

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

cost passive RFID tags. In the paper[7] they considered fault attack on hummingbirdcryptographic algorithm. The round key of 64bit found with 256 bit secret key and 80 bit internal states. Theyfound the cipher can be broken after around 50 faults. The results shows that to recover the key, 248 values canbe guessed with three 16-bit internal state register, this further increases the complicates attack to 266.In paper[8] they developed two approaches for cloak the RFID tags using hummingbird cryptography. Inpaper[9] the hummingbird cryptography is used in smart devices incorporating zig-bee standard. In paper[10] theypresented security analysis of hummingbird cryptographic algorithm by the application of shortcut attack on theinternal 16- bit block length and 64-bit key block cipher. The results shows that hummingbird-1 has not givethe required security. In paper[11] they developed hummingbird cryptography on sparton-2 FPGA. In this theencryption and decryption units are implemented separately. Among the two approaches to develop block cipher,i.e look up table and Boolean function approach, Boolean function approach was used, it takes more slicesbut gives more security than look up table approach. The results shows high performance with low complexity. Inpaper[12], they developed hummingbird cryptography using LABVIEV software.In all of the above papers some of them tries to improve area, some of them to reduce power and some of them to increase the overall performance. In some paper they try to reduce the tradeoff between area, power, costrequirements and check the hummingbird cryptography security performance. In our design we try to furtherenhancing the performance of hummingbird cryptography. All the synthesis and simulation results are performed on Xilinx ISE 14.4 using Verilog HDL.

SIMULATION RESULTE

All the synthesis and simulation results are performed using Verilog HDL. The synthesis and simulation are performed on Xilinx ISE 14.4. The simulation results are shown below figures.

The corresponding schematics of the Hamming bird encryption after synthesis are shown below.

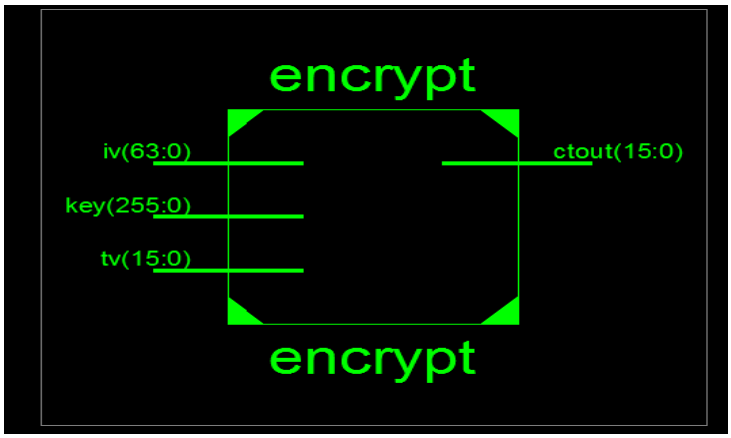

Figure 3: RTL schematic of Top-level Hamming Bird Encryption

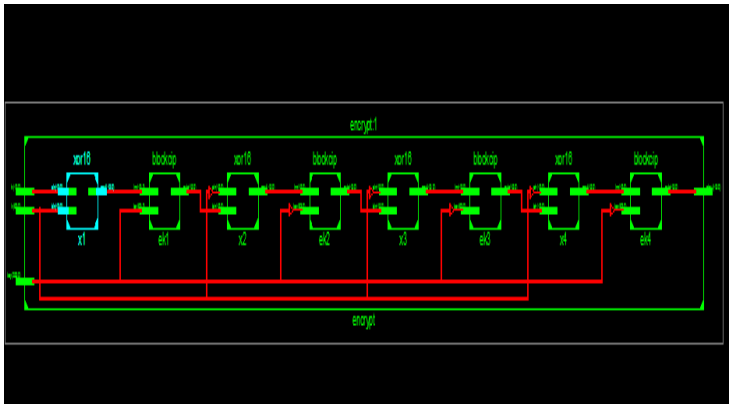

Figure 4: RTL schematic of Internal Hamming Bird Encryption

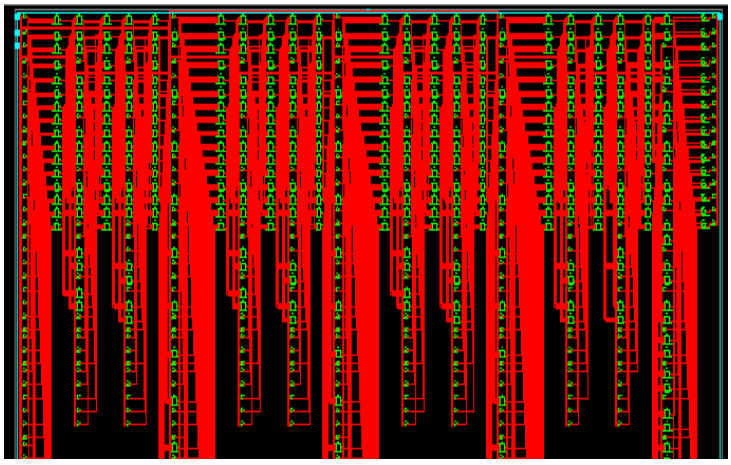

Figure 5: Technology schematic of Internal block Hamming Bird Encryption

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

encrypt Project Status (10/14/2016 - 00:25:06)			
Project File:	hamming.xise	Parser Errors:	No Errors
Module Name:	encrypt	Implementation State:	Synthesized
Target Device:	xc3s200-4tq144	• Errors:	
Product Version:	ISE 14.4	• Warnings:	
Design Goal:	Balanced	• Routing Results:	
Design Strategy:	Xilinx Default (unlocked)	• Timing Constraints:	
Environment:	System Settings	• Final Timing Score:	

Device Utilization Summary (estimated values)			[-]
Logic Utilization	Used	Available	Utilization
Number of Slices	258	14752	1%
Number of Slice Flip Flops	51	29504	0%
Number of 4 input LUTs	500	29504	1%
Number of bonded IOBs	321	376	85%
Number of GCLKs	1	24	4%

Detailed Reports					[-]
Report Name	Status	Generated	Errors	Warnings	Infos
Synthesis Report	Current	Fri Oct 14 00:38:44 2016			

Figure 6: Design summary of Hamming Bird Encryption

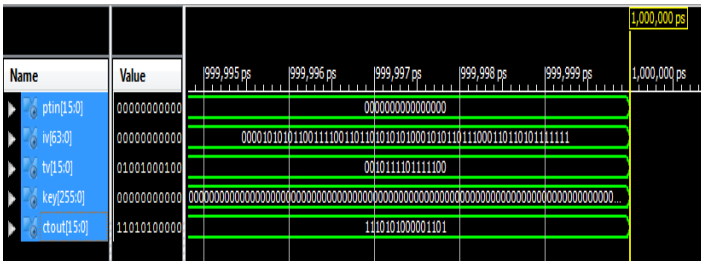

Figure 7: Simulated output for Hamming Bird Encryption

APPLICATIONS:

- ATM machines
- Wireless communication
- Mobile Phones
- Image processing and Network security

CONCLUSION

There are various papers discussed about hummingbird cryptographic algorithm on different sparton-3 FPGA, etc. In all of these, there is a enhanced research on reducing area, power requirement, & increasing speed with aim of giving better security to resource constrained devices like RFID The low power and High speed FPGA implementation is very precisely achieved by the proposed algorithm due to its prominent internal structure. Hence this high performance ultra-lightweight hybrid model will meet the power consumption requirements with constricted response time for diverse embedded applications and can be widely suitable for hardware environment. The design can be implemented on every electronic system which is the part of mobile adhoc network to prevent the security breach.

REFERENCES

[1]. Xinxin Fan1, Honggang Hu1, Guang Gong1, Eric M. Smith2, and Daniel Engels2 "Lightweight Implementation of Hummingbird Cryptographic Algorithm on 4-Bit Microcontrollers" Institute of Electrical and Electronics Engineers, Inc. 2009.

[2]. Xinxin Fan and Guang Gong, Ken Lauffenburger, Troy Hicks "FPGA Implementations of the Hummingbird
Cryptographic Algorithm "IEEE International Symposium on Hardware- Oriented Security and Trust (HOST) 2010

[3]. Meng-Qin Xiao, Xiang Shen, Yu-Qing Yang, Jun-Yu Wang "Low Power Implementation of Hummingbird
Cryptographic Algorithm for RFID tag" 2010.

[4]. İsmail San, NurayAt "Compact Hardware Architecture for Hummingbird Cryptographic Algorithm" 21st International Conference on Field Programmable Logic and Applications 2011.

[5]. Xinxin Fan and Guang Gong, Honggang Hu " Remedying the Hummingbird Cryptographic Algorithm " International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11 2011.

[6]. Xinxin Fan and Guang Gong, Daniel W. Engels and Eric M. Smith "A Lightweight Privacy-Preserving Mutual
Authentication Protocol for RFID Systems" Joint Workshop of SCPA 2011 and SaCoNAS2011.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[7]. YaserEsmaeiliSalehani and Amr Youssef " differential fault analysis of hummingbird "

[8]. "Cloaking RFID Tags"2011.

[9]. SaiSeshabhattar, PriyankaYenigalla, Paul Krier‡, Daniel Engels "Hummingbird Key Establishment Protocol For Low-Power ZigBee" The 8th Annual IEEE Consumer Communications and Networking Conference - Security and Content Protection 2011.

[10]. Xunjun Chen, Yuelong Zhu, Zheng Gong, YiyuanLuo "Cryptanalysis of the Lightweight Block Cipher Hummingbird-1"Fourth International Conference on Emerging Intelligent Data and Web Technologies 2013.

[11]. "Design and Implementation of Block Cipher in Hummingbird Algorithm over FPGA" 2014.

[12]. P.V.G. Raj Pritha, N.Suresh

Author Details

Ganam Thirumal, He is pursuing M.Tech in VLSI Design from Siddhartha College of Engineering and Technology, Hyderabad, J.N.T.U.H Affiliated College.

T.Krishnarjuna Rao is an Associate Professor at Siddhartha Institute of Engineering and Technology, Ibrahimpatnam, Hyderabad in ECE Department. He received his B.Tech degree in Electronics and Communication Engineering from ADAM's Engg college, Khammam and M.Tech degree in VLSI System Design from AnuragEnggCollege, Hyderabad. He attended many workshops and conferences related to VLSI and Low power VLSI.He published six papers in various international journals. His research interest is VLSI Technology and design.

Dr. D Subba Rao, is a proficient Ph.D person in the research area of ImageProcessing from Vel-Tech University, Chennai along with initial degrees ofBachelor of Technology in Electronics and Communication Engineering (ECE)from Dr. S G I E T, Markapur and Master of Technology in Embedded Systemsfrom SRM University, Chennai. He has 13 years of teaching experience and haspublished 12 Papers in International Journals, 2 Papers in National Journals andhas been noted under 4 International Conferences. He has a fellowship of TheInstitution of Electronics and Telecommunication Engineers (IETE) along with aLife time membership of Indian Society for Technical Education (ISTE). He iscurrently bounded as an Associate Professor and is being chaired as Head of theDepartment for Electronics and Communication Engineering discipline atSiddhartha Institute of Engineering and Technology, Ibrahimpatnam, Hyderabad.
Email –Id: subbu.dasari@gmail.com
Contact: 09966779182
07893744445