AN EFFICIENT AND SECURED HB2 ALG WITH LOW LATENCY

1. D.SRUTHI, 2.R.UPENDARRAO

1. PG Scholar, sruthi.dasari4@gmail.com, NRI institute of Technology, Agiripalli, Krishna Dist, AP, INDIA

2. Assistant Professor, upenddar@gmail.com,NRI institute of Technology, Agiripalli, Krishna Dist, AP, INDIA

ABSTRACT: The main objective of this project is to design a new tool for securing the information in Android Platform. This project based on light weight encryption scheme based on humming bird2. This used to secure the data by making use of password based authentication. The cryptographic key is derived from password based key generation method. Further this project can be extended to latency optimized processor for multipurpose applications. Along with time reduction, security also can be increased by using hybrid approaches in key generation processing. This light weight, latency optimization, more security is the vital key features of this designed crypto device.

INDEX TERMS: HUMMING BIRD2, CRYPTO CORE, LATENCY, HUBRID APPROACH, AUTHENTICATION, KEY GENERATION.

INTRODUCTION: Authenticated encryption algorithms provide confidentiality and integrity protection for messages using a single processing step. In general, this process is resistant to all previously known Cryptanalytic attacks. This low cost systems for object identification without any physical contact, Tx and Rx communication also have a number of security problems. It's easy for an adversary to obtain sensitive information, since there is no mutual authentication in today's systems. By linking two different sightings of the same Tx and Rx, an adversary can easily trace a person carrying a tagged item. Hummingbird-2 is an authenticating encryption primitive that has been designed particularly for resource-constrained devices such as RFID tags, wireless sensors, smart meters and industrial controllers. Hummingbird-2 can b implemented with very small hardware or software footprint and is therefore suitable for providing security in low-cost ubiquitous devices. The design described in this paper is an evolutionary step from Hummingbird-1 [8, 10, 11] and was developed in part as a response to the cryptanalysis of the cipher presented in [20]. Hummingbird-2 is resistant to all previously known cryptanalytic attacks

Literature Survey: ESTREAM initiative [2] was launched as an effort to identify new stream ciphers that might be considered for widespread adoption. Since most known (old) stream ciphers have been the target of (more or less realistic) cryptanalytic attacks, a most important objective of the project was the design of a secure cipher and the derivation of sound (easily checkable) security criteria. Modern cryptography originates in the works of Feistel at IBM during the late 1960‘s and ear ly 1970‘s [1]. DES was adopted by the NIST, for encrypting unclassified information in 1977. DES is now replaced by the Advanced Encryption Standard (AES), which is a new standard adopted. Another milestone happened during 1978, marked by the publication of RSA [2]. The RSA is the first full-fledged public-key algorithm. This discovery by and large solved the key exchange problem of cryptography. RSA also proposed the world wide acceptable standard techniques like authentication and electronic signatures in modern cryptography. In the 1980s, elliptic curve cryptography (ECC) [6] became popular due to its superior strength per bit compared to existing public key algorithms such as RSA. ECC is able to produce higher security using a key of small size. This superiority of ECC over RSA resulted into effective usage of bandwidth and quick implementation [8].

PROPOSED SYSTEM:

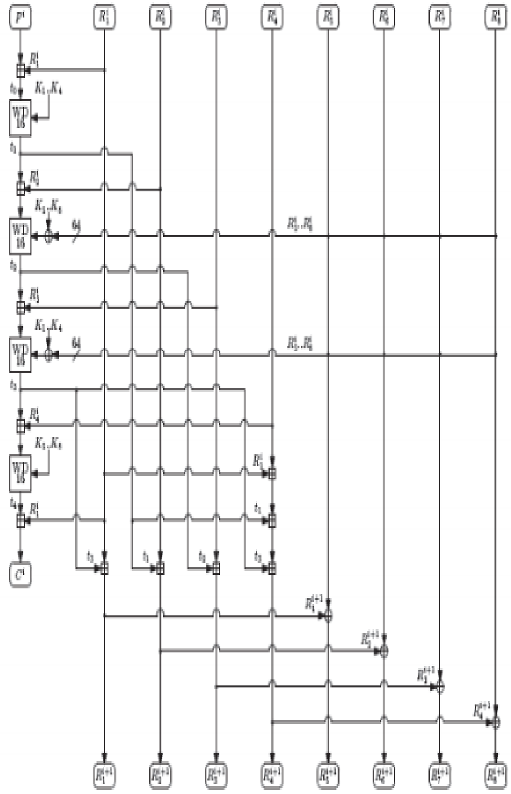


Fig: Encryption architecture

The structure of the Hummingbird algorithm consistsof four 16-bit block ciphers Ek1 ,E k2 ,E k3 and E k4 ,four 16-bit internal state registers RS1,RS2,RS3 and RS4,and a 16-stage LFSR.The secret key is 256-bit which is divided into four 64-bit subkeys ,k1 and k2 ,they can be used in four block ciphers. In the encryption process a 16-bit plaintext PT is executed by modulo 2 addition of PT and the first internal state register RS1.The result of this block is then encrypted by the first block cipher CT .

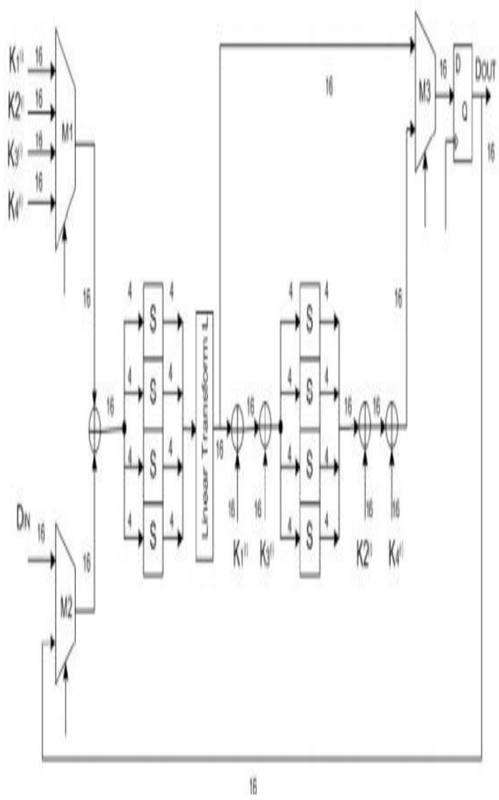


Fig: 2 Round based Architecture

The round-based architecture is Used to further reduce the chip area and power consumption. This architecture repeatedly uses only one round function block as shown in Figure 2 and also consists of four regular rounds which shares the common hardware resources of one substitution and permutation layer and the final round is composed of another substitution layer and four XORs. Therefore, there are totally 5 XORs, 8 S - boxes, and one permutation layer for the data path. Furthermore, three 16-bit multiplexers are introduced for different purposes.

IMPLEMENTATION:

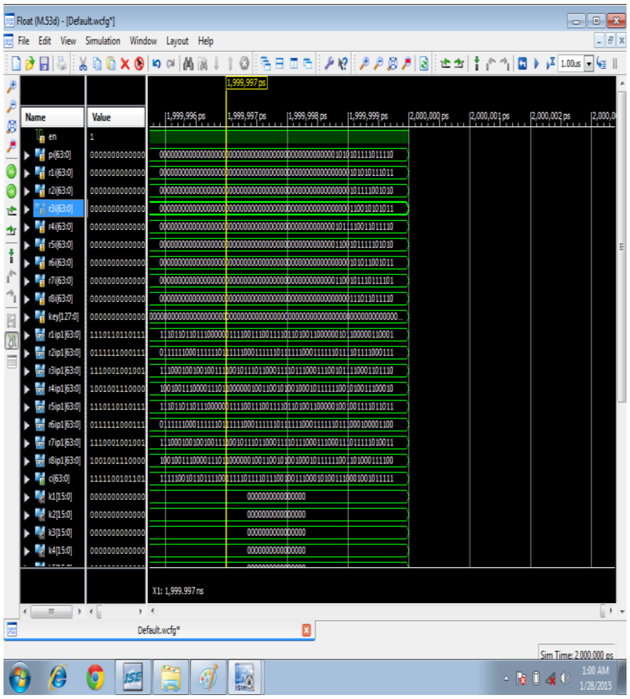
XILINX:

Xilinx, Inc. (NASDAQ: XLNX) is the world's largest supplier of programmable logic devices, the inventor of the field programmable gate array (FPGA) and the first semiconductor company with a fabless manufacturing model

IN the Xilinx software we can do simulation and synthesis .The entire processor will be implemented using the Xilinx FPGAs so you won't have to spend time wiring up that part of the circuit. You will, however, have to wire the switches and lights that are used to control the processor, and have to wire the Xilinx part itself to the switches and lights, but this shouldn't be too bad. You will also use the backplane bus in your lab kit so that the Triscuit will be built on two boards: one for the Xilinx chip, and one for the switches and lights.

The HDL Editor feature provides extensive edit and search capabilities with language-specific color coding of keywords, as well as integrated on-line syntax checking to scan verilog code for errors. The Language Assistant feature speeds design entry by providing a lookup list of typical language constructs and commonly used synthesis modules like counters, accumulators, and adders.

RESULTS:



Name	Value
en	1
pi[63:0]	000000000000
r1i[63:0]	000000000000
r2i[63:0]	000000000000
r3i[63:0]	000000000000
r4i[63:0]	000000000000
r5i[63:0]	000000000000
r6i[63:0]	000000000000
r7i[63:0]	000000000000
r8i[63:0]	000000000000
key[127:0]	000000000000
r1ip1[63:0]	1110110110111
r2ip1[63:0]	0111111000111
r3ip1[63:0]	1110001001001
r4ip1[63:0]	1001001110000
r5ip1[63:0]	1110110110111
r6ip1[63:0]	0111111000111
r7ip1[63:0]	1110001001001
r8ip1[63:0]	1001001110000
ci[63:0]	1111100101101
k1[15:0]	000000000000
k2[15:0]	000000000000
k3[15:0]	000000000000
k4[15:0]	000000000000

X1: 1,999.997 ns

Sim Time: 2,000,000 ps

CONCLUSION:

Finally, this project present a novel cryptanalytic technique called round based humming bird2 algorithm which is especially effective if the differential sequence reflecting parts of a cipher associated with parts of the key can be obtained. The proposed Hummingbird encryption and decryption cores can encrypt and decrypt a 256-bit message block with less number of clock cycles. As compared to other light weight block cipher AES, Hummingbird can encrypt and decrypt in less number of clock cycles.

FEATURE WORK:

As the future research, we intend to conduct further cryptanalysis and security evaluations for

Hummingbird cipher as well as propose low power ASIC implementations for low-cost crypto devices.

REFERENCES:

1. R. ANDERSON, E. BIHAM AND L. KNUDSEN. "Serpent: A Proposal for the Advanced Encryption Standard." http://www.cl.cam.ac.uk/~rja14/Papers/serpent. pdf (1999)

2. A. BIRYUKOV, C. DE CANNIÈRE AND M. QUISQUATER. "On Multiple Linear Approximations." CRYPTO 2004, LNCS 3152, pp. 1-22. Springer (2004)

3. E. BIHAM AND A. SHAMIR. "Differential Cryptanalysis of DES-like cryptosystems." In A. Menezes and S.A. Vanstone (Eds.): CRYPTO 1990. LNCS 537, pp. 2–21. Springer (1990)

4. E. BIHAM AND A. SHAMIR. "Differential Cryptanalysis of the Data Encryption Standard." Springer (1993)

5. C. DE CANNIÈRE, O. DUNKELMAN AND M. KNEŽEVI´C . "KATAN & KTANTAN – A Family of Small and Efficient Hardware-Oriented Block Ciphers." CHES 2009, LNCS 5747, pp. 272–288. Springer (2009) 6. I. DINUR AND A. SHAMIR. "Cube Attacks on Tweakable Black Box Polynomials." EUROCRYPT2009, LNCS 5479, pp. 278–299. Springer (2009)

7. M. DWORKIN. "Recommendation for Block Cipher Modes of Operation: Galois/CounterMode (GCM) and GMAC." NIST Special Publication 800-38D (2007)

8. X. FAN, H. HU, G. GONG, E. M. SMITH AND D. ENGELS. "Lightweight Implementationof Hummingbird Cryptographic Algorithm on 4-Bit Microcontroller." The 1st InternationalWorkshop on RFID Security and Cryptography 2009 (RISC'09), pp. 838–84. Springer (2009)

9. N. FERGUSON, D. WHITING, B. SCHNEIER, J. KELSEY, S. LUCKS, AND T. KOHNO "Helix: Fast Encryption and Authentication in a Single Cryptographic Primitive." FSE 2003,LNCS 2887, pp. 330–346. Springer (2003)

10. D. ENGELS, X. FAN, G. GONG, H. HU AND E. M. SMITH. "Ultra-Lightweight Cryptography for Low-Cost RFID Tags: Hummingbird Algorithm and Protocol." Centre for Applied Cryptographic Research (CACR) Technical Reports, CACR-2009-29.http://www.cacr.math.uwaterloo.ca/techreports/2009/cacr2009-29.pdf (2009)

11. D. ENGELS, X. FAN, G. GONG, H. HU AND E. M. SMITH. "Hummingbird: Ultra- Lightweight Cryptography for Resource-Constrained Devices." 1st International Workshop on Lightweight Cryptography for Resource-Constrained Devices (WLC'2010). Tenerife, Canary Islands, Spain, January. (2010)

Miss. D.Sruthi completed her B.tech and pursuing M.tech from NRI institute of Technology,. Her best part is that she galvanizes into the subject.

Mr.R.UPENDARRAO, currently working as Assistant Professor at NRI institute of Technology. His research and his enthusing interests include high performance development at his college applications.