Implementation of Hummingbird 1s Cryptographic Algorithm for Low Cost RFID Tags using LabVIEW

P.V.G. Raj Pritha
M.E. Communication Systems, E.C.E. Department
Prathyusha Institute of Technology and Management
Tamil Nadu, India.
rajprithame@gmail.com

N.Suresh
Asst. Professor, E.C.E. Department
Prathyusha Institute of Technology and Management
Tamil Nadu, India.
sureshae@gmail.com

Abstract- Hummingbird is a novel Ultra-light weight cryptographic encryption scheme used for RFID applications of privacy-preserving identification and mutual authentication protocols, motivated by the well known enigma machine. Hummingbird has a precise response time and the design of small block size will reduce the power consumption requirements.This algorithm is shown as it prevents from the common attacks like Linear and differential cryptanalysis.The properties of privacy identification and mutual authentication are together investigated in this algorithm.This is implemented using the LABVIEW software.

Keywords: privacy-preserving identification; mutual authentication protocols, lightweight cryptography scheme.

I. INTRODUCTION

Radio frequency identification (RFID) is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by and read at short ranges via magnetic fields, and then act as a passive transponder to emit microwaves or UHF radio waves . Others use a local power source such as a battery, and may operate at hundreds of meters. Unlike a bar code, the tag does not necessarily need to be within line of sight of the reader, and may be embedded in the tracked object.

RFID tags are used in many industries. An RFID tag attached to an automobile during production can be used to track its progress through the assembly line. Pharmaceuticals can be tracked through warehouses. Livestock and pets may have tags injected, allowing positive identification of the animal. On off-shore oil and gas platforms, RFID tags are worn by personnel as a safety measure, allowing them to be located 24 hours a day and to be quickly found in emergencies

II. HUMMINGBIRD ENCRYPTION

In order to overcome this security issues a new algorithm called Hummingbird algorithm have been designed as mutual authentication algorithm which is a combination of both block cipher and stream cipher, this is designed with a small block size and expected to meet stringent response time and power consumption.

This consists of 16-bit block size, 256-bit key size and 80-bit internal state where the key size provides security for various RFID applications.

A. Encryption and Decryption

The structure of the Hummingbird algorithm consists of four 16-bit block ciphersE_{K1},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 k_1,k_2,k_3 and k_4,they can be used in four block ciphers.In the encryption process a 16-bit plaintext PT_i is executed by modulo 2^{16} addition of $PT_i$and the first internal state register RS1.The result of this block is then encrypted by the first block cipher CT_i.

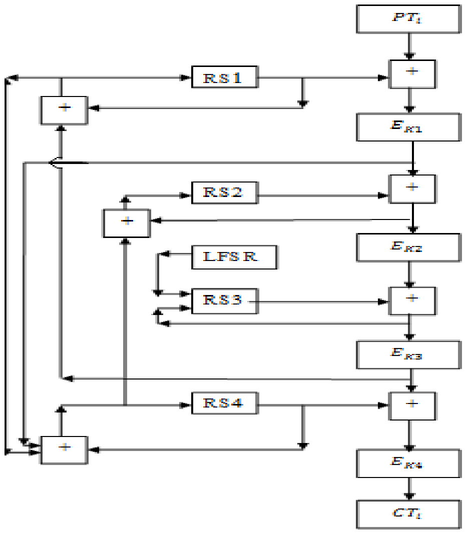


Fig 1. Encryption Process

ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE

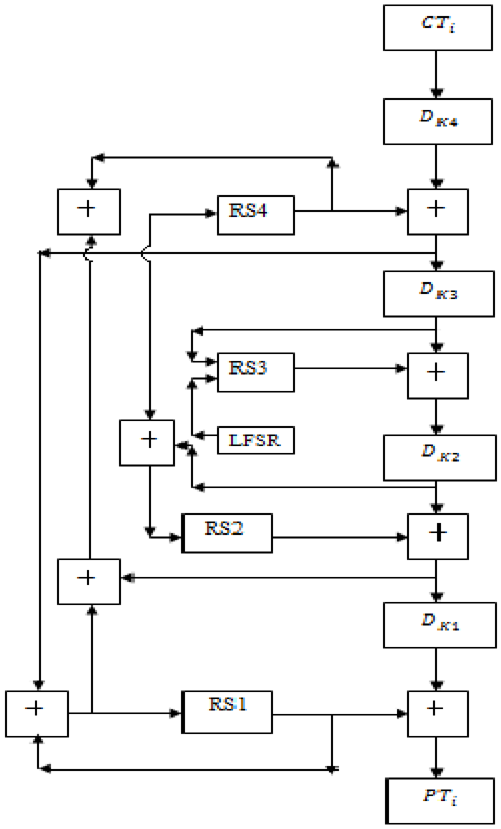


Fig 2. Decryption Process

TABLE I. INTERNAL STATE UPDATING OF HUMMINGBIRD

ENCRYPTION PROCESS	DECRYPTION PROCESS
$V12_t = E_{k1}(PT_S \oplus RS1_t)$	$V34_t = D_{k4}(CT_i) \oplus RS4_t$
$V23_t = E_{k2}(V12_t \oplus RS2_t)$	$V23_t = D_{k3}(V12_t) \oplus RS3_t$
$V34_t = E_{k3}(V23_t \oplus RS3_t)$	$V12_t = D_{k2}(V23_t) \oplus RS2_t$
$CT_i = E_{k4}(V34_t \oplus RS4_t)$	$PT_i = D_{k1}(V34_t) \oplus RS1_t$
Internal State Updating Process	
$LFSR_{t+1} \leftarrow LFSR_t$	
$RS1_{t+1} = RS1_t \oplus V34_t$	
$RS3_{t+1} = RS1_t \oplus V23_t \oplus LFSR_{t+1}$	
$V12_t = RS4_t \oplus V12_t \oplus RS1_{t+1}$	
$SPT_i = RS2_t \oplus V12_t \oplus RS4_{t+1}$	

This procedure is repeated for three times and the output of E_{K4} is the ciphertext CT_i.LFSR is used for updating the internal state registers.The reverse process is done in the Decryption block.

B. 16 bit Block Cipher

Four 16-bit block ciphers are used in a consecutive manner. Substituition and Permutation(SP) network forms the 16-bit block cipher, with 16-bit block size and 64-bit key size. SP consists of three steps, first key mixing where 16-bit block ciphers uses exclusive or operation for implementation in hardware and software, second a substituition layer with 4-inputs and 4-ouputs of serpent type s-boxes and third a permutation layer.the linear form of 16-bit block cipher is given by,$L: \{0,1\}^{16} \rightarrow \{0,1\}^{16}$ defined as,

$$L(m)=m \oplus (m \lll 6) \oplus (m \lll 10),$$

where m=$m_{0,} m_1 \ldots, m_{15,}$is a 16-bit block data.

C. Features of S-Boxes

Inorder to reduce the area and power consumption the four s-boxes are reduced into a single s-box and where it is repeated four times in a 16-bit block cipher.

Four s-boxes in hexadecimal notation

TABLE II. S-BOXES IN HEXADECIMAL

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$s_1(x)$	8	6	5	F	1	A	9	E	B	2	4	4	7	0	D	3
$s_2(x)$	0	7	E	1	5	8	2	3	A	D	6	6	F	C	4	9
$s_3(x)$	2	E	F	5	C	9	A	B	4	6	8	8	0	7	3	D
$s_4(x)$	0	7	3	4	C	A	F	D	E	6	B	B	2	8	9	5

III. SECURITY ANALYSIS OF HUMMINGBIRD

Hummingbird is considered as a finite state machine because it's a hybrid mode of block and stream cipher where the value of LFSR does not depend on the internal states. Hummingbird algorithm is resistant to the following attacks they are Birthday attacks, Differential cryptanalysis, Linear cryptanalysis, Structural attacks, Algebraic attack and cube attacks.

IV. HUMMINGBIRD MUTUAL AUTHENTICATION PROTOCOL

The hummingbird mutual authentication protocol is mainly for establishing the trust relationship between the RFID tags and the reader,consider RFID system consists of a reader and N RFID tags,where a unique 256-bit key with each tag is shared by the reader.The following three phases are included in the hummingbird mutual authentication protocol.

ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE

(i)Phase 1: Privacy preserving tag identification:

In this phase the reader will determine the correct key shared with a tag it is communicating with without exposing the tag's identity to the adversaries by performing a private identification procedure[12].

(ii)Phase 2: Mutual authentication between a reader and a tag:

In this phase the reader and the tag authenticate with each other.

(iii) Phase 3: Command execution:

In this phase the command issued and authenticated by the reader is received and executed only by the encryption RFID tag.

A. *Output*

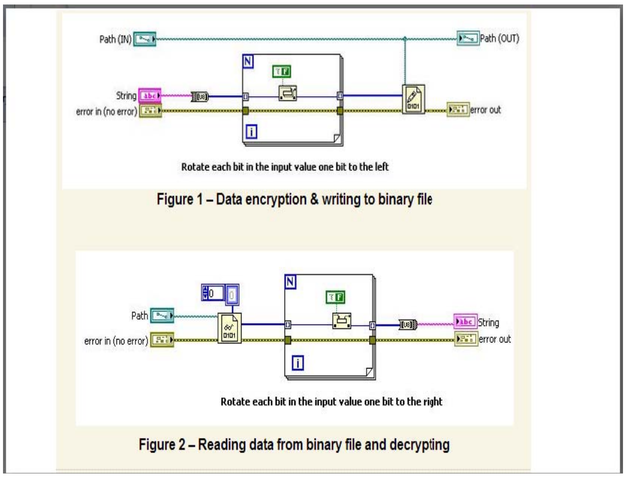
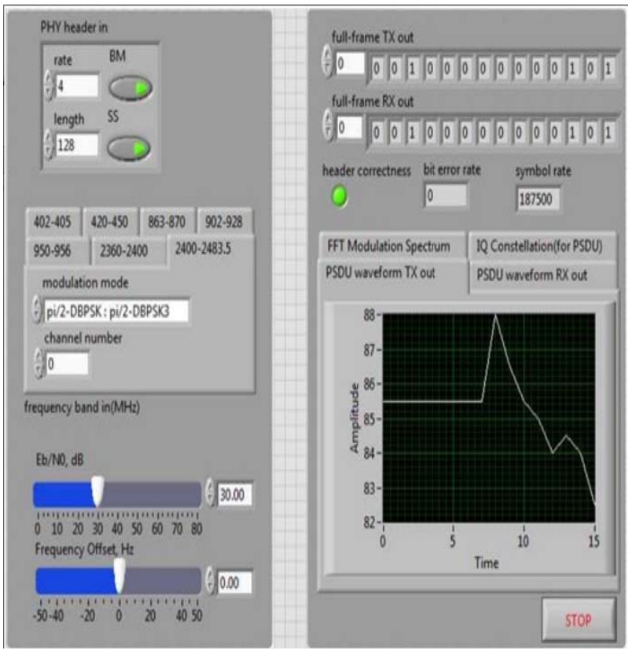

Path (IN)
Path (OUT)
String
error in (no error)
error out
N
i
Rotate each bit in the input value one bit to the left
Path
error in (no error)
String
error out
Rotate each bit in the input value one bit to the right

Figure 1 – Data encryption & writing to binary file

Figure 2 – Reading data from binary file and decrypting

Fig.3. Binary data read and write block.



PHY header in

rate 4

BM

length 128

SS

402-405 | 420-450 | 863-870 | 902-928 | 950-956 | 2360-2400 | 2400-2483.5

modulation mode pi/2-DBPSK : pi/2-DBPSK3

channel number 0

frequency band in(MHz)

Eb/N0, dB 30.00

Frequency Offset, Hz 0.00

full-frame TX out 0 0 0 1 0 0 0 0 0 0 0 0 0 1 0 1

full-frame RX out 0 0 0 1 0 0 0 0 0 0 0 0 0 1 0 1

header correctness

bit error rate 0

symbol rate 187500

Fig.4. Front panel

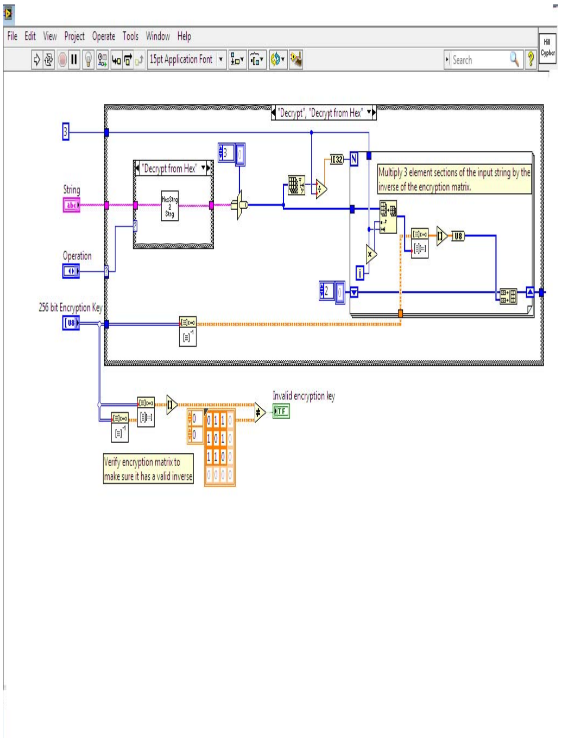

File Edit View Project Operate Tools Window Help
15pt Application Font
Search
"Decrypt", "Decrypt from Hex"
"Decrypt from Hex"
String
Operation
256 bit Encryption Key
Multiply 3 element sections of the input string by the inverse of the encryption matrix.
I32
N
i
U8
Invalid encryption key
Verify encryption matrix to make sure it has a valid inverse

Fig.5(a). Block diagram of encryption and decryption

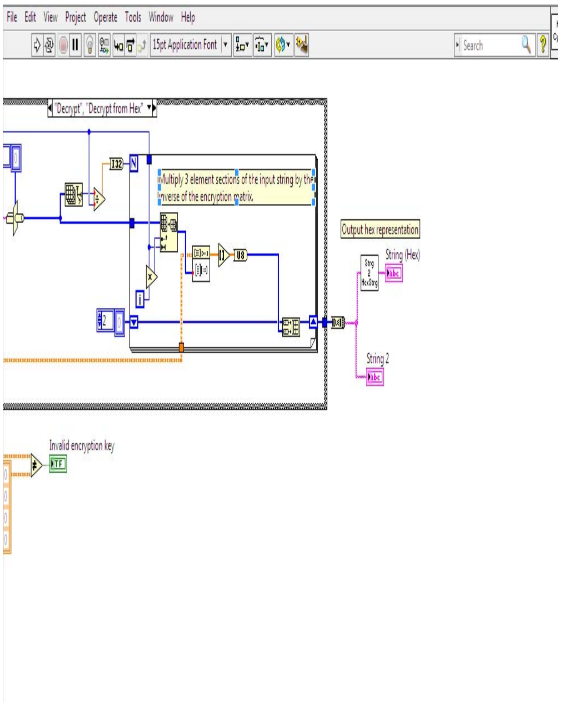
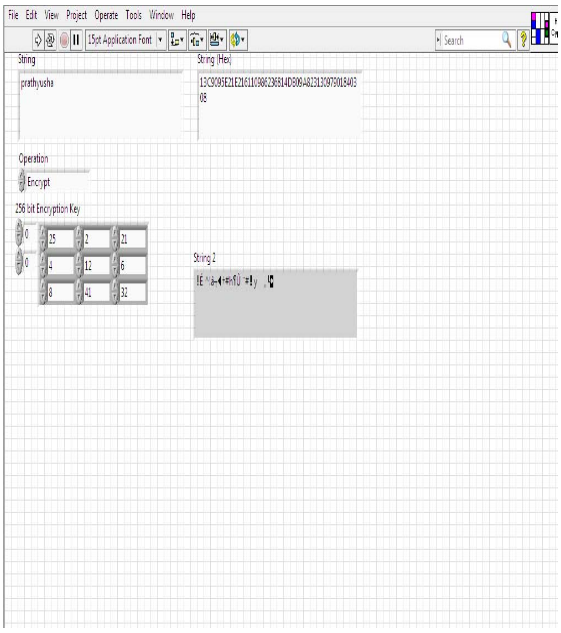

File Edit View Project Operate Tools Window Help
15pt Application Font
Search
"Decrypt", "Decrypt from Hex"
I32
N
Multiply 3 element sections of the input string by the inverse of the encryption matrix.
Output hex representation
String (Hex)
String 2
U8
Invalid encryption key

Fig.5(b). Blockdiagram of encryption and decryption



String: prathyusha

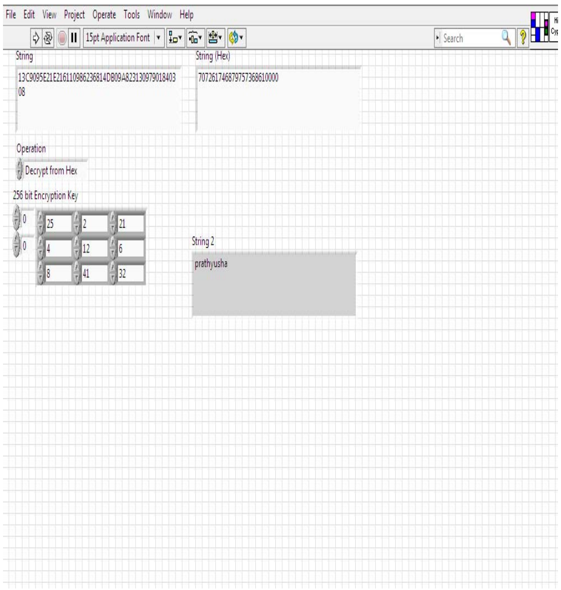
String (Hex): 13C9095E21E216110986236814DB09A82313097901840308

Operation: Encrypt

256 bit Encryption Key: 0, 0; 25, 2, 21; 4, 12, 6; 8, 41, 32

String 2: ‼É ^!â┬◄+#h¶Û ¨#‼y ˛◘

Fig.6. Front panel of encryption block



String: 13C9095E21E216110986236814DB09A82313097901840308

String (Hex): 7072617468797573686100000

Operation: Decrypt from Hex

256 bit Encryption Key: 0, 0; 25, 2, 21; 4, 12, 6; 8, 41, 32

String 2: prathyusha

Fig.7.Front panel of decryption block

V. CONCLUSION

This Hummingbird cryptographic algorithm is implemented using the LABVIEW software, where the encryption and decryption blocks are also designed and the output is generated. The hummingbird 2 algorithm is compared in the future.

REFERENCES

[1] R. Anderson, E. Biham, and L. Knudsen, “Serpent: A Proposal for the Advanced Encryption Standard", available at http://www.cl.cam.ac.uk/rja14/Papers/ serpent .pdf.

[2] E. Biham, “Cryptanalysis of Multiple Modes of Operation", J. Cryptology 11(1), pp. 45-58, 1998.

[3] E. Biham, “Cryptanalysis of Triple Modes of Operation", J. Cryptology 12(3), pp. 161-184, 1999.

[4] E. Biham and L. R. Knudsen, “Cryptanalysis of the ANSI X9.52 CBCM Mode", J. Cryptology 15(1),pp. 47-59, 2002.

[5] E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag,New York, 1993.

[6] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin,and C. Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher", The 9th International Work-shop on Cryptographic Hardware and Embedded Systems - CHES 2007, LNCS 4727, P. Paillier and I.Verbauwhede (eds.), Berlin, Germany: Springer-Verlag, pp. 450-466, 2007.

[7] I. Dinur and A. Shamir, “Cube Attacks on Tweakable Black Box Polynomials", Advances in Cryptology- EUROCRYPT 2009, LNCS 5479,A. Joux (ed.), Berlin, Germany: Springer-Verlag, pp. 278-299, 2009.

[8] EPCglobal, Inc., http://www.epcglobalinc.org/, 2005.

[9] M. Feldhofer, S. Dominikus, and J.Wolkerstorfer, “Strong Authentication for RFID Systems Using theAES Algorithm", The 6th International Workshop on Cryptographic Hardware and Embedded Systems-CHES 2004, LNCS 3156, M. Joye and J.-J. Quisquater (eds.), Berlin, Germany: Springer-Verlag, pp.357-370, 2004.

[10] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, “AES Implementation on a Grain of Sand", IEEE Proceedings Information Security, vol. 15, no. 1, pp. 13-20, 2005.

[11] P. HÄamÄalÄainen, T. Alho, M. HÄannikÄainen, and T. D. HÄamÄalÄainen,”Design and Implementation of Low-Area and Low-Power AES Encryption Hardware Core", The 9th EUROMICRO Conference on Digital System Design: Architectures, Methods and Tools - DSD 2006, pp. 577-583, IEEE Computer Society, 2006.

[12] International Organization for Standardization, ISO/IEC 9782-2: Information Technology { Security Techniques { Entity Authentication Mechanisms Part 2: Entity Authentication using Symmetric Tech-
niques, 1993.

[13] T. Jakobsen and L. Knudsen, “The Interpolation Attack on Block Ciphers", The 4th Annual Fast Software Encryption Workshop - FSE 1997, LNCS 1267, E. Biham (ed.), Berlin, Germany: Springer- Verlag, pp. 28-40, 1997.

[14] X. Lai, “Higher Order Derivatives and Differential Cryptanalysis", Proceedings of Symposium on Communication, Coding and Cryptography, in honor of James L. Massey on the occasion of his 60'th birthday, 1994.

[15] G. Leander, C. Paar, A. Poschmann, and K. Schramm, “New Lightweight DES Variants", The 14th Annual Fast Software Encryption Workshop - FSE 2007, LNCS 4593, A. Biryukov (ed.), Berlin, Germany: Springer-Verlag, pp. 196-210, 2007.

[16] G. Leander and A. Poschmann, “On the Classification of 4 Bit S-Boxes", The 1st International Work-shop on the Arithmetic of Finite Fields - WAIFI 2007, LNCS 4547, C. Carlet and B. Sunar (eds.),
Berlin, Germany: Springer-Verlag, pp. 159-176, 2007.

[17] M. Matsui, “Linear Cryptanalysis Method for DES Cipher", Advances in Cryptology - EURO-CRYPT'93, LNCS 765, T. Helleseth (ed.), Berlin, Germany: Springer-Verlag, pp. 386-397, 1993.

[18] C. Rolfes, A. Poschmann, G. Leander, and C. Paar, “Ultra-Lightweight Implementations for Smart Devices-Security for 1000 Gate Equivalents", The 8th Smart Card Research and Advanced Application IFIP Conference - CARDIS 2008, LNCS 5189, G. Grimaud and F.-X. Standaert (eds.), Berlin,Germany: Springer-Verlag, pp. 89-103, 2008.

[19] D.Wagner, “Cryptanalysis of Some Recently-Proposed Multiple Modes of Operation", The 5th Annual Fast Software Encryption Workshop - FSE 1998, LNCS 1372, S. Vaudenay (ed.), Berlin, Germany.