

IMPLEMENTATION OF HUMMINGBIRD CRYPTOGRAPHIC ALGORITHM FOR LOW COST RFID TAGS USING LABVIEW

Suresh.N¹, Arun prasad.J², Raj pritha.P.V.G³

^{1,2}Assistant professor, ³M.E, Prathyusha institute of technology and management, Thiruvallur, Tamil Nadu, India
suresh.aeme@gmail.com, Jarunprasad06@gmail.com, rajprithame@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 is expected to meet the stringent response time and power consumption requirements which can provide the designed security with a small block size. This algorithm is shown as it is resistant to the most common attacks like linear and differential cryptanalysis. Some properties for integrating this algorithm into a privacy identification and mutual authentication protocol is investigated. This is implemented using the LABVIEW software.

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

-----***-----

1. INTRODUCTION

Automatic object identification is now possible by a technology called Radio Frequency Identification (RFID). RFID tag is a small transponder in a RFID system, used to label each object. Radio frequency queries can be received and responded using transceiver, called RFID reader. RFID is a tiny integrated circuit which is used for storing, processing informations for identification and also radio antenna for wireless data transmissions. Animal identification, Point-of-sales, inventory management are the applications for low-cost and low-power tags.

This lowcost RFID systems for object identification without any physical contact, RFID tags and RFID reader communication also have a number of security problems. Its easy for an adversary to obtain sensitive information, since there is no mutual authentication in today's RFID systems. By linking two different sightings of the same RFID tag an adversary can easily trace a person carrying a tagged item. Unprotected wireless communication will have many issues between FRID tags and readers.

2. 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.

2.1. Encryption and Decryption

The structure of the Hummingbird algorithm consists of four 16-bit block ciphers $E_{K_1}, E_{K_2}, E_{K_3}$ and E_{K_4} , 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 .

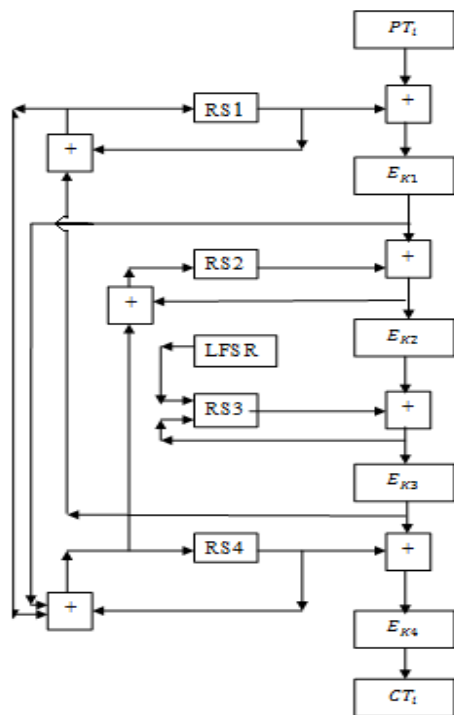


Fig 1. Encryption Process

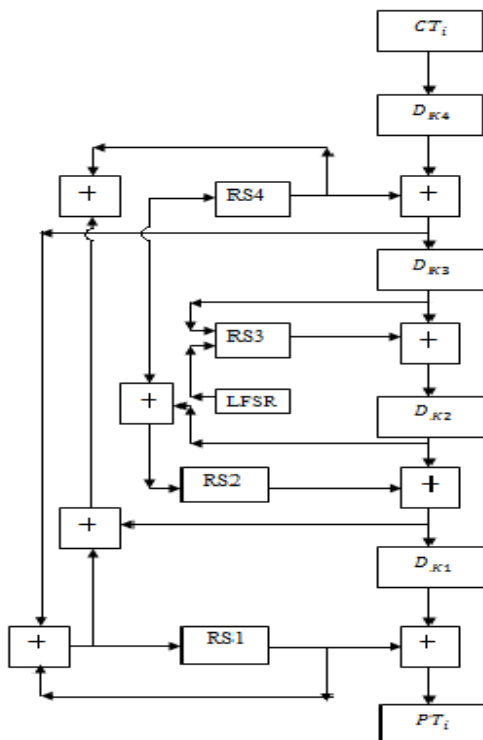


Fig 2. Decryption Process

| ENCRYPTION PROCESS | DECRYPTION PROCESS |
|--|--------------------------------------|
| $V12_t = E_{K1}(PT_t \oplus RS1_t)$ | $V34_t = D_{K4}(CT_t) \oplus RS4_t$ |
| $V23_t = E_{K2}(V12_t \oplus RS2_t)$ | $V23_t = D_{K3}(V12_t) \oplus RS3_t$ |
| $V34_t = E_{K3}(V23_t \oplus RS3_t)$ | $V12_t = D_{K2}(V23_t) \oplus RS2_t$ |
| $CT_t = E_{K4}(V34_t \oplus RS4_t)$ | $PT_t = D_{K1}(V34_t) \oplus RS1_t$ |
| Internal State Updating Process | |
| $LFSR_{t+1} \leftarrow LFSR_t$ | |
| $RS1_{t+1} = RS1_t \oplus V34_t$ | |
| $RS3_{t+1} = RS1_t \oplus V23_t \oplus LFSR_{t+1}$ | |
| $V12_t = RS4_t \oplus V12_t \oplus RS1_{t+1}$ | |
| $SPT_t = RS2_t \oplus V12_t \oplus RS4_{t+1}$ | |

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.

2.2. 16 bit Block Cipher

Four 16-bit block ciphers are used in a consecutive manner. Substitution 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 substitution layer with 4-inputs and 4-outputs 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,

$$L(m) = m \oplus (m \ll 6) \square (m \ll 10),$$

where $m = m_0, m_1, \dots, m_{15}$, is a 16-bit block data.

2.3. Features of S-Boxes

In order 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:

| 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 |

3. 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.

4. HUMMINGBIRD MUTUAL AUTHENTICATION PROTOCOL

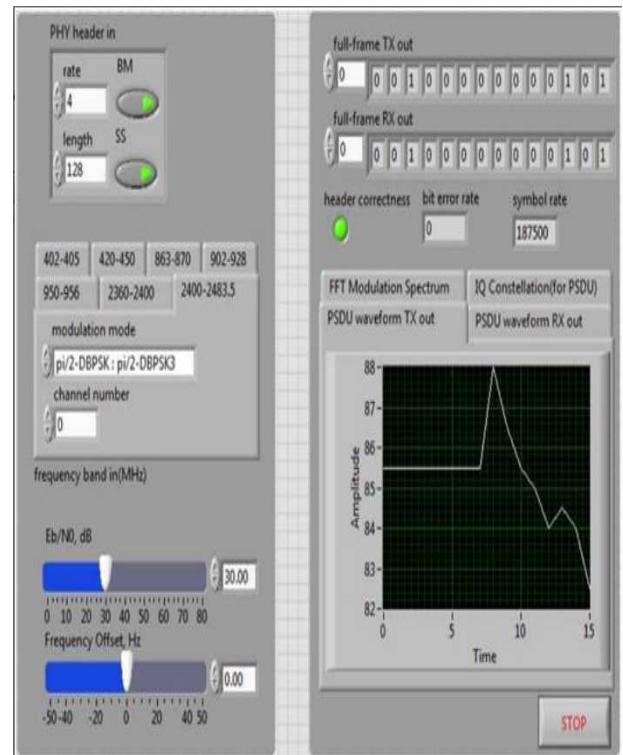
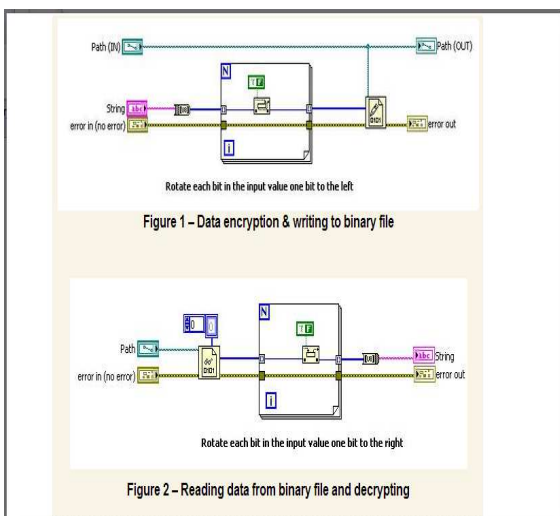
The hummingbird mutual authentication protocol is mainly for establishing the trust relationship between the RFID tags and the reader, consider RFID system consists of a reader and N RFID tags, where a unique 256-bit key with each tag is shared by the reader. The following three phases are included in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

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.

4.1. Output



CONCLUSIONS

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 Workshop 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 the AES 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", IEE Proceedings Information Security, vol. 15, no. 1, pp. 13-20, 2005.

[11]. P. Hämäläinen, T. Alho, M. Hännikäinen, and T. D. Hämäläinen, "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 Techniques, 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 60th 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 Workshop 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