Available online at www.sciencedirect.com
ScienceDirect

ELSEVIER

February 2014, 21(1): 104–108
www.sciencedirect.com/science/journal/10058885

The Journal of China Universities of Posts and Telecommunications

http://jcupt.xsw.bupt.cn

Eight-sided fortress: a lightweight block cipher

LIU Xuan[1], ZHANG Wen-ying[1,2,4] (✉), LIU Xiang-zhong[3], LIU Feng[1]

1. School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China
2. Science and Technology on Information Assume Laboratory, Beijing 100072, China
3. No.2 Middle School Attached to Shnadong Normal University, Jinan 250014, China
4. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract

In this paper, we present a new lightweight block cipher named eight-sided fortress (ESF), which is suitable for resource-constrained environments such as sensor networks and low-cost radio rrequency identification (RFID) tags. Meanwhile, we present the specification, design rationale and evaluation results in terms of the hardware implementation. For realizing both efficiency and security in embedded systems, similar to the other lightweight block ciphers, ESF is 64 bits block length and key size is 80 bits. It is inspired from existing block cipher, PRESENT and LBlock. The encryption algorithm of ESF is based on variant Feistel structure with SPN round function, used Feistel network as an overall structure with the purpose of minimizing computational resources.

Keywords block cipher, lightweight, RFID tags, efficiency, cryptography design

1 Introduction

With the development of low resource devices such as RFID tags, sensor nodes, smart cards, protection of privacy and so on, which are regarded as critical technologies in digital information society based on hardware and Internet. However resource-efficient cryptographic primitives are extremely critical on performance for security and efficiency in wireless communication and embedded systems. Lightweight cryptography has become a hot pot, research on designing and analyzing lightweight block ciphers have attracted a lot of attention. In fact, the applications of these technology have some properties, such as small storage space, weak computation ability, extremely power constraints etc. However, conventional algorithms such as AES although quite secure, are not suitable for extremely constrained environments. The filed of lightweight cryptography deals with designing ciphers for such environments [1]. In lightweight cryptography there is trade-off between security, cost, and performance, but it is highly difficult to optimize all the three, yet at the same time the design of new lightweight block cipher is also carefully considered the trade-off between hardware level and software level optimization, this allows us to make a trade-off and even though we use block cipher design techniques [2].

Recently, the lightweight cryptography for resource-constraint applications has attracted much attention. A series of lightweight block ciphers have been proposed in the literature, such as LBlock [3], PRESENT [1], HIGHT [4], mCrypton [5], DESL [6], KATAN and KTANTAN [7], CGEN [8], MIBS [9], TWIS [10], SEA [11] etc. All of these ciphers are designed and aimed at specifically for low-cost environments. Among them, LBlock [3] employs a variant of Festal structure and the encryption algorithm is four bits oriented which can be implemented efficiently in both hardware and software platform. Hardware implementation requires about 1 320 GE on 0.18 μm technology. PRESENT [1] is an example of an SP-network and consists of 31 rounds, a block size of 64 bits, and a key size of 80 bits or 128 bits. Its structure favors repetition and hence it can be compactly implemented in

Received date: 10-08-2013
Corresponding author: ZHANG Wen-ying, E-mail: wenyingzh@sohu.com
DOI: 10.1016/S1005-8885(14)60275-2

hardware. It requires only 1 570 GE and its hardware requirements are competitive with today's leading stream ciphers. HIGHT [4] uses 64 bits block length and 128 bits key length. It is a hardware oriented cipher, based on 32 rounds iterative structure which is modification of Generalized Feistel structure. HIGHT uses very simple operations such as XOR, addition mod 28, and left bit-wise rotation, and can be implemented with 3 048 GE on 0.25μm technology. mCrypton [5] has a precise hardware assessment and requires 2 949 GE. DESL [6] is based on the classical data encryption standard (DES) [12] design, but unlike DES it uses special case of a single *S*-box repeated eight times and hardware implementation results of DESL requires around 1 848 GE. KATAN and KTANTAN [7] are a family of lightweight block ciphers which contain six variants altogether. To ensure sufficient mixing, 254 rounds of the cipher are executed and the plaintext is loaded into two registers. In each round, several bits are taken from the registers and enter into two nonlinear Boolean functions. The output of the Boolean functions is loaded to the least significant bits of the registers. KATAN and KTANTAN are among the most hardware-efficient, requiring less than 1 000 GE. CGEN [8] is compact algorithm and built closely around the principles underlying the AES [13]. MIBS [9] is based on Feistel structure with SPN round function, used Feistel network as an overall structure with the purpose of minimizing computational resources, and selected the SPN for round function. The hardware implementation of MIBS-64 requires 1 400 GE on 0.18 μm technology. TWIS [10] is inspired from existing block cipher, CLEFIA [14–15], while SEA [11] with parameters requires around 2 280 GE.

In this paper, we propose a new lightweight block cipher called ESF. It is 64 bits block cipher and uses key of size 80 bits. Its consists of two parts: Key scheduling part and Data processing part, which is based on variant Feistel structure with SPN round function, and used Feistel network as an overall structure with the purpose of minimizing computational resources, addition a round subkey in each round function. The encryption algorithm of ESF consists of a 31 rounds intermediate structure. Furthermore, ESF performance is efficiently not only in software platforms but also in resource-contained hardware environments.

The rest of this paper is organized as follows. The specification of ESF is given in Sect. 2. Sect. 3 describes the design rationale. Sect. 4 provide results on hardware implementation. Finally, we conclude in Sect. 5.

2 Specification of ESF

This section provides the specification of ESF. The test vectors of ESF can be found in Appendix A.

2.1 Notations

The following notations are used throughout this paper.

M: 64 bits plaintext
C: 64 bits ciphertext
K: 80 bits master key
F: Round function
K_r: 32 bits round subkey
P: Permutation
<<<7: 7 bits cyclic left shift
S: 4×4 *S*-box
S: Substitution layer consists of eight 4×4 S-box in parallel
||: Two binary strings concatenation
$\oplus$: Bit-wise XOR
$[i]_2$: Binary form of an round_counter i

2.2 Data processing

The data processing part of ESF consists of an encryption part and a decryption part. Encryption and decryption are based on the 2-branch variant Feistel structure with SPN round function. Round functions composed of a key addition, an *S*-box layer and a permutation. The particular of this cipher is that the permutation and the substitution layer are reversible, meaning that the same primitive is used for both encryption and decryption process. Let $M,C\in\{0,1\}^{64}$ be a plaintext and corresponding ciphertext respectively, and let $M=L_0||R_0$ denote a 64 bits plaintext. Despite the design principle of ESF structure is adopted from the design principle of LBlock structure, the permutation layer is different from the LBlock, which applied on bit-wise permutation. The structure of ESF reduces restriction of designing inner auxiliary functions. Compared to SP-like structure, the round function is light. Since encryption process is simply converted into decryption process, implementation of the circuit supporting both encryption and decryption processes does not require much more cost