Journal of ELECTRICAL ENGINEERING, VOL. 51, NO. 12/s, 2000, 87–91

ON THE CLASSIFICATION OF BLOCK CIPHERS AND NEW ENCRYPTION STANDARD

Marta Šimovcová *

This paper describes the design principles for block ciphers introduced by Lai [4]. We summarize Lai's classification based on types of the round function and analyze two AES-algorithms with regard to Lai's classification of the round function.

Keywords:

2000 *Mathematics Subject Classification*:

1 INTRODUCTION

Most of the symmetric key block ciphers are based on a "Feistel network" and a round function. Feistel ciphers involve dividing the plaintext into two halves and repeatedly applying a round function to the data for some number of rounds. In each round there are used the round function and key. The left half is transformed based on the right half, and then the right half is transformed based on the modified left half.

The round function provides a basic encryption mechanism by composing several simple linear and nonlinear operations such as exclusive-or, substitution, permutation, rotation, and modular arithmetics. Different round functions provide different levels of security, efficiency and flexibility.

The purpose of this paper is to analyze two AES candidates namely MARS [3], [5] and Serpent [2], [5], relative to the Lai's classification of the round functions. The aim was to decide if the Lai's classification is enough for classification of the round functions of MARS and Serpent.

The result is that Serpent can be viewed as a generalization of the Type II (see Section 2), and MARS provides a new type with respect Lai's classification.

This article consists of six sections. In the second section we summarize the design of block ciphers introduced by Lai [4]. Section 3 deals with a short description of two AES candidates, MARS and Serpent. In section four we analyze round functions of the algorithms MARS and Serpent. The fifth section deals with differences in the design between these two algorithms and its classification similar to Lai [4].

2 CLASSIFICATION OF BLOCK CIPHERS BY LAI

Let F_2^m denote the vector space of binary m-tuples. Let $X \in F_2^m$ denote the plaintext and $Y \in F_2^m$ denote the ciphertext. The key Z takes values in a subset K of the vector space F_2^k. A secret key block cipher is a mapping $E\colon F_2^m \times K \to F_2^m$ such that for each $z \in K$, $E(\cdot, z)$ is an invertible mapping from F_2^m to F_2^m.

Lai in his work [4] concerned with E/D similar (encryption decryption similar) ciphers. He studied ciphers based on the following types of transformations:

Involution cipher. A function $In(\cdot,\cdot)\colon F_2^m \times F_2^k \to F_2^m$ is *an involution cipher* if for every $z \in F_2^k$, $In(In(x,z),z) = x$ for all $x \in F_2^m$.

Group cipher. A cipher is called *a group cipher* if the ciphertext Y is computed from a plaintext X and key Z as $Y = X \otimes Z$ where $\otimes$ is a group operation. Note that for a group cipher $k = m$ must hold.

Involutory permutation. An *involutory permutation* is an involution $P_I(.)$ of the set F_2^m, i.e. $P_I(P_I(x)) = x$ for all $x \in F_2^m$.

Based on the above mentioned transformations Lai divided iterated block secret-key ciphers into four groups:

I Using an involution cipher only

The round function is an involution cipher only, i.e.

$$f(X,Z) = In(X,Z)\,.$$

The involution cipher has a disadvantage that for an even number of rounds the choice $Z^{2i} = Z^{2i-1}$ for all i causes the resulting encryption function to be identity.

II Using an involution cipher and an involutory permutation

The round function f is an involution cipher followed by a key independent involutory permutation

$$f(X,Z) = P_I(In(X,Z))\,.$$

Note that the additional permutation inserted after the last round just undoes the permutation of the last round. The decryption is done by using subkeys in a reverse order. The block cipher DES is of this type.

* Department of Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology, Ilkovičova 3, 812 19 Bratislava, Slovakia, E-mail: adamyova@kmat.elf.stuba.sk

Research supported by VEGA-grant 1/7611/20.

ISSN 1335-3632 © 2000 FEI STU

Fig. 1. Illustration of an encryption and decryption process for an iterated cipher of the Type I.

Fig. 3. Illustration of an encryption and decryption process for an iterated cipher of the Type III.

III Using a group cipher and an involution

The round function f is a group cipher followed by an involution cipher

$$f(X,Z) = In(X \otimes Z_A, Z_B)\,.$$

An extra group cipher is put at the end of the last round of encryption process. It is easy to see from Fig.3 that this cipher is E/D similar when the decryption subkeys are group inverses of encryption subkeys in the reverse order.

IV Using a group cipher, an involution cipher and an involutory permutation

For this type the round function has a form

$$f(X,Z) = P_I(In(X \otimes Z_A, Z_B)\,,$$

where $X \otimes Z_A$ is a group cipher which is followed by an involution cipher $In(X, Z_B)$. The involutory permutation P_I is an automorphism of the group $(F_2^m, \otimes)$. An additional involutory permutation and a group cipher are put at the end of the encryption process. The IDEA [4] cipher is of this type.

Fig. 2. Illustration of an encryption and decryption process for an iterated cipher of the Type II.

3 THE AES FINALIST CANDIDATE ALGORITHMS

For many applications, the Data Encryption Standard is nearing the end of its useful life. Its 56-bit key is too small. For these reasons, the US National Institute of Standards and Technology has issued a call for a successor algorithm, to be called Advanced Encryption Standard [5]. The essential requirement is that AES should be both faster and more secure than triple-DES; specifically, it should have a 128 bit block length and key length of 128, 192, and 256 bits.

The Second AES Candidate Conference [6] was held in March 1999 to discuss the results of the analysis conducted by the global cryptographic community on the candidate algorithms. Using the analyses and comments received, NIST selected five algorithms: MARS, RC6, Twofish (United States), Rijndael (Belgium) and Serpent (United Kingdom, Israel, Norway). Recently it was announced that the winner is Rijndael [1].

In this contribution we deal with two of AES algorithms: MARS and Serpent.

3.1 MARS

In MARS, IBM designers used the well-established Feistel network and the reasonable idea that an algorithm in which is the top and bottom rounds different from the middle ones is better resistant to differential and linear cryptanalysis.

MARS takes as input four 32-bit plaintext words and produces four 32-bit ciphertext words. Ciphering with MARS is divided into three phases: a 16-round "cryptographic core" phase wrapped with two layers of 8-round "forward" and "backwards mixing". The forward and backward mixing are essentially inverse of each other.

The forward mixing begins whit the addition of key-words in the data-words followed by 8 rounds of S-box based unkeyed mixing.

The core layer consists of several rounds of keyed transformations which involves a combination of S-box lookups, multiplications and data-dependent rotations to get good resistance to cryptanalytical attack. MARS uses

Fig. 4. Illustration of an encryption and decryption process for an iterated cipher of the Type IV.

Fig. 5. Illustration of an encryption and decryption process for Serpent.

single S-box. Sometimes the S-box is viewed as two tables, each of 256 entries denoted by S_0 and S_1.

The backward mixing has 8 rounds of the inverse mixing rounds followed by key-subtraction. In both forward and backward mixing the four words are rotated after each round, so that the current first target word becomes the next last word, the current second word becomes the next first target word, the current third word becomes the next second target word and the current last word becomes the next third target word.

The decryption operation of MARS is inverse of the encryption operation and the code for decryption is similar to the code for encryption.

3.2 SERPENT

It is a substitution linear-transformation network. It has 32 rounds under the control of 33 128-bit subkeys plus initial and final permutation. The initial permutation is applied to the plaintext. Next follows the key mixing operation, a pass trough S-boxes and a linear transformation except the last round. In the last round linear transformation is replaced by an additional key mixing operation. Each round uses 32 copies of single S-box in which it is used 32 times in parallel. Thus 32 rounds use 32 different S-boxes each of which maps 4 inputs bits to 4 outputs bits. The 32 S-boxes are chosen as the 32 separate lines of the eight DES S-boxes.

Let $\hat{X}_i$ denote the input to the i-th round, $\hat{S}_i$ is the application of the S-box S_i 32 times in parallel, and L is the linear transformation. Thus the cipher may be formally described by the following equations:

$$\hat{X}_0 = IP(X)$$

$$\hat{X}_{i+1} = R_i(\hat{X}_i)$$

$$Y = IP^{-1}(\hat{X}_{32})$$

where

$$R_i(X) = L(\hat{S}_i(X \oplus Z_i)), \quad i = 0, \cdots, 30$$

$$R_i(X) = \hat{S}_i(X \oplus Z_i) \oplus Z_{32}, \quad i = 31.$$

Decryption is different from encryption in that the inverse of S-boxes must be used, as well as the inverse linear transformation and the reverse order of the subkeys.

4 STRUCTURE OF THE ROUND FUNCTION OF MARS AND SERPENT

By analyzing the round function of Serpent from the Lai's point of view we obtain the following scheme of the

Fig. 6. Illustration of an encryption process for algorithm MARS. Forward mixing, Backward mixing and Cryptographic Core.

algorithm: It is easily seen that the structure of Serpent's round function is similar to Type II. Function In is replaced by a function S and permutation is replaced by a linear function L. We can observe a little difference between the algorithm of Type II and Serpent. Functions L and S are not involutory in the sense of Lai's classification. In decryption process there are used inverse functions L^{-1} and S^{-1}, respectively.

Hence, Serpent can be classified as an E/D similar cipher from a more general point of view, because in decryption process are used functions and operation based on function and operation from encryption process (function and its inverse).

Conclusion 1. Serpent can be viewed as a generalization of the Type II.

Because of the algorithm, MARS consists of three different phases (the cryptographic core, forward mixing, backward mixing) we had to analyze each phase separately.

The structure of each phase of algorithm MARS is in principle similar to the structure of the Type II but MARS cannot be definitely classified to this Type. The structure is more complex, and several components are different. The permutation used in MARS is of higher order than a permutation expected in Lai's classification. An easy computation shows that the order is 4.

The structure of functions Fm, Bm (Forward an Backward mixing) and Ex (expand function which takes as input one word and returns three data words) is more complex than the structure of the involution function in Lai's work. In decryption process there is used a similar function in the case of forward and backward mixing or inverse function in the case of expand function.

Similarly as in the previous case, MARS can be viewed as a generalized E/D similar cipher.

Conclusion 2. MARS provides a new Type with respect of Lai's classification.

5 NEW DESIGN COMPONENTS

Lai in his classification used three basic items: involutory cipher, involutory permutation and group operation. Software and hardware development, the fact that all modern processors support multiplication of 32-number, bring some new more or less different components. Increasing of the speed of processor allowed using more complex functions and group operation (multiplication, data-dependent rotation).

Involutory cipher is replaced by a cipher that uses one function for encryption, and inverse function for decryption. It causes better resistance of the cipher algorithms to differential attack as well as to linear cryptanalysis and makes analysis more difficult in a restricted time.

Increasing of the order of a permutation caused better bit mixing and avalanche effect, too.

We summarize differences in the following scheme:

Involution cipher	$\longleftrightarrow$	function and its inverse
Group cipher	$\longleftrightarrow$	new group operation: rotation $<<<$
Involutory Permutation	$\longleftrightarrow$	permutation of a higher order

Based on previous analysis we can define new Types from Lai's classification point of view.

Denote GIn generalization of the involutory cipher (function and its inverse), GI the unkeyed generalization of the involutory cipher (i.e. $GI(\cdot)\colon F_2^m \to F_2^m$) and P a permutation of the higher order (the generalization of P_I).

V Generalization of the Type II

The round function f is a general involution cipher followed be an unkeyed general involution cipher

$$f(X,Z) = GI(GIn(X,Z)).$$

In the last round there is an unkeyed involutory cipher GI replaced by a group operation

$$f(X,Z) = GIn(X,Z_A) \otimes Z_B.$$

The decryption is done by using inverses of GIn and GI respectively, and a reverse order of the subkeys.

VI Using different types of round function

Encryption and decryption process has three phases. In each phase the round function has different forms according to the functionality of the phase.

The round function of the first and third phases is an unkeyed general involution cipher (different in each phase) followed by permutation of higher order.

$$f_1(X) = GI_1(P(X)), \quad f_3(X) = GI_2(P(X)).$$

An extra group cipher is put at the beginning of the first phase, and at the end of the third phase instead of addition of a key.

The round function of the second phase is Type II, where the involution cipher is replaced by a general involution cipher. Involutory permutation is replaced by permutation of the higher order

$$f_2(X,Z) = P(GIn(X,Z)).$$

Decryption process is similar to the encryption process, except of the second phase, where an inverse function is used.

6 CONCLUSIONS

Symmetric-key block ciphers have long been used as a fundamental cryptographic element for providing information security. Although they are primarily designed for providing data confidentiality, their versatility allows them to serve as a main component in the construction of many cryptographic systems. The design of cryptosystems depends on current technical possibilities and needs of users.

Based on an analysis from the Lai's classification point of view we conclude that algorithm Serpent brings a generalization of Type II, and MARS brings a new type of the round function.

Acknowledgement

The author gratefully acknowledges many helpful suggestions of Professor Otokar Grošek during preparation of the paper.

References

[1] AES Finalist Information, http://csrc.nist.gov/encryption/aes.

[2] BIHAM, E.—ANDERSON, R.—KNUDSEN, L.: Serpent: A New Block Cipher Proposal, Fast Software Encryption, Lecture Notes in Computer Science 1372, Springer Verlag, 1998, pp. 222–238.

[3] BURWICK, C.—COOPERSMITH, D.—D'AVIGNON, E.—GENNARO, R.—HALEVI, S.—JUTLA, Ch.—MATYAS, S.M.–O'CONNOR, L.—PEYRAVAIN, M.—SAFFORD, D.—ZUNIC, N.: The MARS Encryption Algorithm, http://csrc.nist.gov/encryption/aes.

[4] LAI, X.: On the Design and Security of Block Ciphers, Hartung-Gorre Verlag Konstanz, Zürich, 1992.

[5] LANDAU, S.: Notices of the AMS 47 No. 4 (2000), Communications Security for the Twenty-first Century: The Advanced Encryption Standard.

[6] The Second AES Candidate Conference, http://csrc.nist.gov/encryption/aes/round2/round2.htm.

Received 4 July 2000

Marta Šimovcová (Mgr) is a lecturer at the Faculty of Electrical Engineering and Information Technology of the Slovak University of Technology. Her PhD-thesis supervisor (in applied informatics) is Professor Otokar Grošek.