Diffusion Analysis of EFN-MDS Structure

SUBARIAH IBRAHIM[1] MOHD AIZAINI MAAROF[2]

[1,2]Department of Communication and Computer System
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia, Skudai 81310, Johore, Malaysia
[1]Tel: +60-07–557-6160 x 32386, Fax: +60-07–556-5044, E-mail: subariah@fsksm.utm.my
[2]Tel: +60-07–557-6160 x 32002, Fax: +60-07–556-5044, E-mail: maarofma@fsksm.utm.my

Abstract

In general, block ciphers consist of one top-level structural model into which the round function *F* is plugged into. The study focuses on Extended-Feistel-Network (EFN) that is a generalization of a Feistel Network (FN). This structure is employed in several ciphers that were developed for Advanced Encryption Standard such as CAST-256, MARS and RC6. The problem with EFN is that it requires many rounds when the number of sub-blocks used in EFN is large. This paper proposed a new structural model that can overcome this problem by incorporating EFN with a linear transformation based on Maximum Distance Separable (MDS) codes. The diffusion analysis shows that EFN-MDS requires at most half the number of rounds to achieve completeness property as compared to EFN structure. Therefore the proposed structure is suitable for designing ciphers with scalable block sizes and ciphers with large block sizes.

Keywords

Cryptography, Extended Feistel Network, Diffusion Analysis, Maximum Distance Separable Code.

1. Introduction

A Feistel Network (FN) is a general method of transforming the input block in a cipher through a repeated application of keyed, non-linear *F*-functions into a permutation [1][2]. It was invented by Horst Feistel [3] and was popularized by Data Encryption Standard (DES) [4]. Since then it has been used in many block cipher designs such as FEAL [5] and Blowfish [6]. An FN structure has been extensively analyzed by the cryptologic community for more than 20 years and appears to be free of basic structural weaknesses [7]. A direct extension of FN splits the input block into n > 2 sub-blocks [2]. This structure is known as Extended Feistel Network [EFN]. EFN consists of a series of rounds whereby at least one sub-block is subjected to an *F*-function. The *F*-function plays a key role in the diffusion process due to its completeness property [2]. A completeness property is an important cryptographic criterion whereby all output bits of a cipher are dependent on all input bits and vice-versa. This property was defined by Kam and Davida [8]. EFN is used in several Advanced Encryption Standard (AES) candidates such as CAST-256 [9], MARS [10] and RC6 [11].

In EFN structure, the rate of diffusion slows down as the number of sub-blocks increases. This means as the number of sub-blocks increases, the threshold number of rounds required to achieve completeness also increases. The increase is almost double the number of sub-blocks for EFN Type I model and one more than the number of sub-blocks for EFN Type II and Type III models. This analysis was shown by Subariah and Aizaini [12]. In this paper we proposed a top level cipher structure that exploits EFN structure and yet improves its diffusion rate. The structure incorporates EFN with a linear transformation that is based on Maximum Distance Separable codes (MDS codes). MDS codes have proved to exhibit optimal diffusion property as shown by SHARK [13], AES [14] and Twofish [15]. Therefore we call our proposed structure EFN-MDS.

This paper is organized as follows. In section 2, a related work is reviewed and some background definitions of EFN and MDS are given. The main contribution of this paper lies in section 3 and 4. Section 3 presented our proposed top level cipher structure for EFN-MDS while section 4 analyses the diffusion effect of our proposed structure. Finally a conclusion is made in section 5.

2. Background and Related Work

In EFN, a round is a transformation that combines the sub-blocks of the plaintext through non-linear, key-dependent *F*-functions followed by a permutation of the sub-blocks. The permutation of the sub-blocks together with the *F*-functions play an important role in the diffusion process in block ciphers [16]. The diffusion process refers to the effect of spreading the influence of an input bit over as much of the output bits as possible, thereby hiding features of the plaintext [17]. A cipher is called complete if each output bit depends on all of its input bits [18][2]. A diffusion analysis on EFN used in several AES candidates was discussed in [2].

MDS codes are used in several ciphers due to its property that exhibits optimal diffusion. It is used in AES which has an SPN structure [14]. Some examples of ciphers with EFN structure that used MDS are Camellia [19] and Twofish [15]. Their approach is to use MDS matrix within the *F*-function that is after the S-boxes. Our approach is that MDS matrix is used to mix the bits from different sub-blocks after the *F*-function operation.

2.1 Extended Fiestel Network

In a conventional FN, the plaintext block is divided evenly into two sub-blocks. The round function *F* operates on the right sub-block and then combined with the left sub-block via bitwise exclusive or (XOR). The two sub-blocks are then swapped and become the input to the next round. However, an EFN splits the input block into $n > 2$ sub-blocks [2]. These sub-blocks are then mixed through repeated application of keyed, non-linear *F*-functions in order to generate a permutation of the input block [1]. The swapping of sub-blocks can be viewed as a circular shift. There are various types of transformations in EFN. This paper focuses on three types of EFN, namely, EFN Type-I, EFN Type-II and EFN Type-III.

EFN Type-I employs only one *F*-function in its design. The output cipher-text for each round can be described as follows:

$$C_1, \mathrm{C}_2, \ldots, \mathrm{C}_{n\text{-}1}, \mathrm{C}_\mathrm{n} = P_n, P_{1,} P_2, \ldots, P_{n\text{-}1} \oplus F(P_\mathrm{m}). \qquad (1)$$

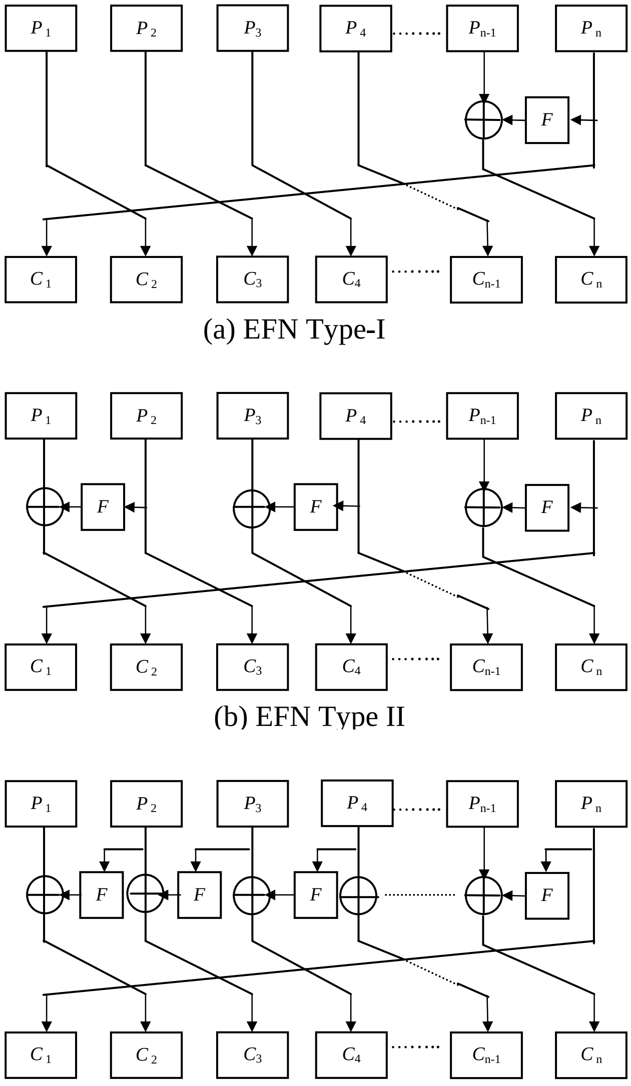
where P_i is the *i*th sub-block. EFN Type-II uses one *F*-function for every two consecutive sub-blocks. Similarly, this type of transformation can be defined by:

$$C_1, \mathrm{C}_2, \ldots, \mathrm{C}_{n\text{-}1}, \mathrm{C}_\mathrm{n} = P_n, P_1 \oplus F(P_2), P_2, P_3 \oplus F(P_4), \ldots, P_{n\text{-}1} \oplus F(P_n). \qquad (2)$$

Finally EFN Type-III has one *F*-function for every sub-block and is defined as follows:

$$C_1, \mathrm{C}_2, \ldots, \mathrm{C}_{n\text{-}1}, \mathrm{C}_\mathrm{n} = P_1 \oplus F(P_2), P_2 \oplus F(P_3), \ldots, P_{n\text{-}1} \oplus F(P_n), P_1. \qquad (3)$$

The structures for the three EFN transformations are depicted in Figure 1. EFN is used to extend the block size of a cipher. However if the block size is very large, the number of rounds needed to reach completeness is also large.



(a) EFN Type-I

(b) EFN Type II

(c) EFN Type III

Figure 1: EFN transformation structure

2.2 Maximum Distance Separable Matrix

An MDS code over a field is a linear mapping from m field elements to n field elements, with a property that the minimum Hamming distance between any two distinct vectors is at least n+1 [15]. The Hamming distance between two vectors is equal to the Hamming weight of the difference of the two vectors with Hamming weight is defined as the number of nonzero components of a vector. An MDS code can be represented by an MDS matrix, M consisting of $m \times n$ elements. By using matrix M, the relation between output bits, C and input bits, P can be described as follows:

$$C = MP \qquad (4)$$

$$\Rightarrow \begin{pmatrix} C_1 \\ C_2 \\ \mathrm{M} \\ C_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12}\Lambda & a_{1n} \\ a_{21} & a_{22}\Lambda & a_{2n} \\ \mathrm{M} & \mathrm{MO} & \mathrm{M} \\ a_{m1} & a_{m2}\Lambda & a_{mn} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ \mathrm{M} \\ P_n \end{pmatrix} \qquad (5)$$

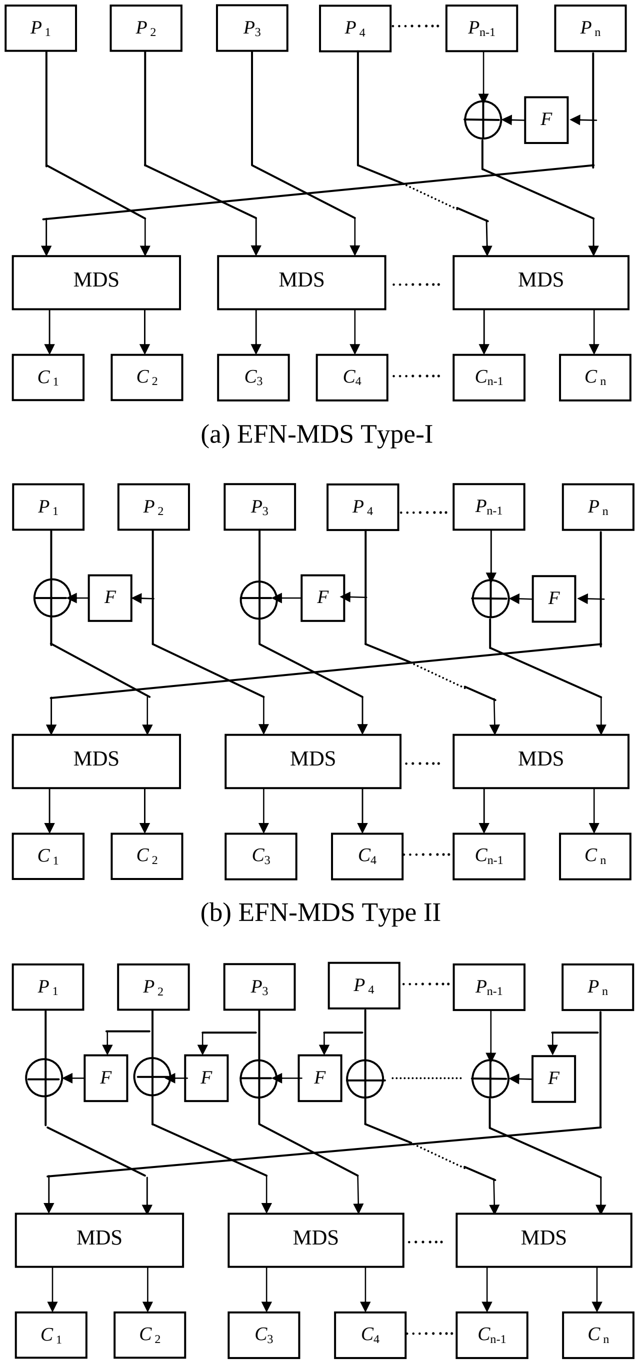
In our proposed cipher structure, P_i and C_i refer to an input sub-block and output sub-block respectively. A well known MDS code can be obtained from Reed-Solomon error-correcting code. A necessary and sufficient condition for a matrix M to be MDS is that every square sub-matrix of M is non-singular [4].

3. Proposed Top-Level Cipher Structure

The aim of our proposed cipher structure is to improve the diffusion of EFN structure. The EFN structure is enhanced by adding a linear transformation after the sub-blocks are rotated. The purpose is to mix the bits from one sub-block with another sub-block. Since MDS matrix is known to exhibit optimal diffusion [20], we proposed that a linear transformation is based on the MDS matrix.

In our proposed structure, the linear transformation based on MDS matrix combines every two neighbouring sub-blocks. This ensures that the input bits from a sub-block are mixed with at least one other sub-block after the first round. In EFN structure at least one sub-block is left unmixed after the first round. Two sub-blocks combination allows only one MDS matrix needs to be defined even though the cipher block size is scalable, hence the cipher is code efficient. Since MDS operates on two sub-blocks, the sub-block rotation is still needed to permute the sub-blocks. Without the rotation, MDS will operate on the same sub-blocks in every round.

The structures for the EFN-MDS transformations are depicted in Figure 2.



(a) EFN-MDS Type-I

(b) EFN-MDS Type II

(c) EFN-MDS Type III

Figure 2: EFN-MDS Structure

4. Diffusion Analysis of EFN-MDS Structure

Diffusion is a spread of the influence of input bits to output bits [17]. An important cryptographic criterion of a cipher with regard to diffusion is completeness property whereby all output bits of a cipher are dependent on all input bits and vice versa. In this section we will discuss the analysis on the completeness property of EFN-MDS Type I, EFN-MDS Type II and EFN-MDS Type III structure models. In this analysis, it is assumed that the round function, *F*, is complete.

4.1 Methodology

In this work, we employ the diffusion analysis used in [21] whereby the output sub-block for each round is determined. The sub-block is represented by P_i, for example, a cipher with 4 sub-blocks is represented by P_1, P_2, P_3, and P_4. For the output sub-block for each round, the letter in front the bracket represents the block affected by the round function or the MDS transformation and the bracketed letters represent the blocks which influence the affected block (i.e. the blocks which influence input bits). For an illustration of the methodology used for the diffusion analysis, a well known cipher that is DES is used. The dependencies for DES at the output of each round are shown in Table 1. The table indicates that in DES, after one round, the bits corresponding to the plaintext sub-block P_1 are now affected by the bits of plaintext sub-block P_2. After round two, the sub-block P_2 is influenced by all the bits of all sub-blocks. Then after the third round, a complete dependency of the output bits on the input bits has been achieved since both sub-blocks are influenced by all bits of the plaintext. Therefore, we can say that DES achieves complete dependency after 3 rounds.

Table 1: Dependencies for DES

Round	Dependencies	
	P_1	P_2
1	P_2	$P_1(P_2)$
2	$P_1(P_2)$	$P_2(P_1,P_2)$
3	$P_2(P_1,P_2)$	$P_1(P_1,P_2)$

4.2 Results and Discussion

In this work, we analyzed diffusion rates for 2, 4, 6, 8 and 10 sub-blocks for all types of EFN-MDS models. Table 2 illustrates the comparison of the threshold number of rounds needed to achieve complete dependency for these three models. The analyses show that all types of EFN-MDS require the same number of rounds for similar number of sub-blocks that is all types of models achieve complete dependency after 2, 3, 3, 4 and 5 numbers of rounds for 2, 4, 6, 8 and 10 sub-blocks respectively. From these analyses, we can conclude that for *n* sub-blocks, all types of EFN-MDS require only *n*/2 number of rounds for n > 4 sub-blocks to achieve completeness. This means that EFN-MDS only requires about half the number of rounds required by EFN Type II and Type III, and need about a quarter number of rounds required by EFN Type I. The summary of threshold number of rounds needed to achieve completeness for EFN-MDS is compared with EFN structure in Table 3 and is illustrated further for clarity using a graph in Figure 3.

Table 2: Diffusion Analysis of EFN-MDS Models

Number of Sub-blocks	Threshold Number of Rounds To Achieve Completeness		
	EFN-MDS Type I	EFN-MDS Type II	EFN-MDS Type III
2	2	2	2
4	3	3	3
6	3	3	3
8	4	4	4
10	5	5	5

Table 3: Comparison of Diffusion Analysis for EFN and EFN-MDS Structures

EFN Type	Threshold No. of Rounds to Achieve Completeness
EFN-Type I	2*n* – 1
EFN-Type II	*n* + 1
EFN-Type III	*n* + 1
All types of EFN-MDS	*n*/2 for *n* > 4

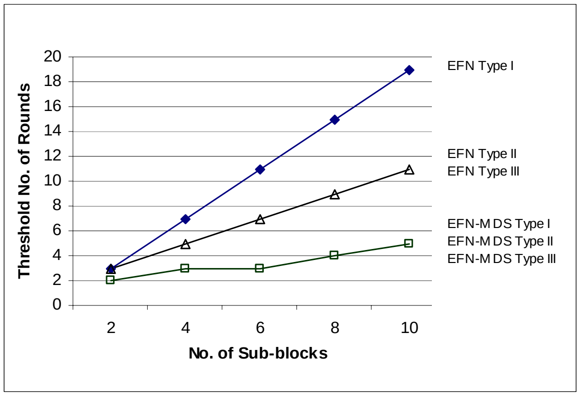


Figure 3: Comparison of EFN and EFN-MDS to Achieve Completeness

5. Conclusion

In this paper we proposed a top level structure for a block cipher that we called EFN-MDS and analysed its completeness property. From our analyses, it was found that the structure only requires at most half the number of rounds required by EFN structures. Due to this property, therefore the structure is suitable for large block size cipher as well as ciphers that support scalable block sizes.

It is important to note that completeness property is only a necessary condition for a block cipher in order to be secure, but it is not a sufficient condition. Therefore further work is to analyse the immunity of the structure against linear and differential cryptanalysis. Another open problem is how to construct a suitable MDS matrix that can ensure a cipher can resist cryptanalytic attack.

6. Acknowledgement

The authors would like to thank UTM for its financial support and facilities in conducting this work.

References

[1] Schneier, B. and Kelsey, J. Unbalanced Feistel Networks and Block Cipher Design. *In Proceedings of Fast Software Encryption 1996*. Springer-Verlag, 1996, pp. 121-144.

[2] Nakahara, J., Vanderwalle, J. and Preneel, B. Diffusion Analysis of Feistel Networks. *Proceedings of 20th Symposium on Information Theory in the Benelux*, Hasrode, Belgium. May 27-28, 1999. Pp. 101-108.

[3] Fiestel, H. Cryptography and Computer Privacy. *Scientific American*. 1973. 228(5). Pp. 15-20.

[4] FIPS 46-3. *Data Encryption Standard*. Federal Information Processing Standard (FIPS), Publication 46-3, National Institute of Standards and Technology, U.S. Department of Commerce, Washington D.C., October, 1999.

[5] A. Shimizu and S. Miyaguchi. Fast data encipherment algorithm FEAL. In D. Chaum and W.L. Price, editors, *Advances in Cryptology — Eurocrypt '87*, Springer-Verlag, Berlin, 1988. Pp. 267–280.

[6] Schneier, B. Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). *Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), LNCS 809*. Springer-Verlag, 1994. Pp. 191-204.

[7] Adams, C.M., Constructing Symmetric Ciphers Using the CAST Design Procedure, *Design, Codes and Cryptography*, Vol. 12, pp. 283-316, Kluwer Academic Publishers, Boston, 1997.

[8] Kam, J.B. and Davida G.I. Structured Design of Substitution-Permutation Encryption Networks. *IEEE Transactions on Computers*, Vol. C-28, No. 10, pp. 747-753, 1979.

[9] Adam, C., Heys, H.M., Tavares, E. and Wiener, M. An Analysis of the CAST-256 Cipher. *Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering*, 1999.

[10] Burwick *et al*. MARS - A Candidate Cipher for AES, 1999. www.research.ibm.com/ security/mars.pdf.

[11] Rivest, R.L., Robshaw, M.J.B., Sidney, R. and Yin, Y.L. The RC6 Block Cipher, 1998. *NIST AES Proposal*, http://csrc.nist.gov/ ecryption/ aes.

[12] Subariah Ibrahim and Mohd Aizaini Maarof, Diffusion Analysis of A Scalable Feistel Network, *Proceedings in 3rd World Enformatika Conference*, Istanbul, Turkey, Vol. 5, pp. 98-101, April 27-29, 2005

[13] Rijmen, V., Daemen, J., Preneel, J., Bosselaers, A., De Win, E., The Cipher SHARK, *Fast Software Encryption*, Gollmann, D., (Ed), *LNCS 1039*, Springer-Verlag, Berlin, pp. 99-111, 1996.

[14 Daemen, J. and Rijmen, V., *The Design of Rijndael: AES – The Advanced Encryption Standard*, Springer-Verlag, Berlin, 2001.

[15] Schneier, B., Kelsey, J., Whiting, D. Wagner, D. and Hall, C. Twofish: A 128-bit Block Cipher. *SAC 98*, Springer-Verlag, 1998. Pp. 27-42.

[16] Shannon, C.E., Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4): 656–715. 1948.

[17] Robshaw, M.J.B. Block Ciphers. *RSA Laboratories Technical Report TR-601*, Version 2, August, 2, 1995.

[18] Menezes, A.J., van Oorschot, P.C. and Vanstone, S.A., *Handbook of Applied Cryptography*, CRC Press, 1997.

[19] Shirai, T., Kanamaru, S. and Abe, G., Improved Upper Bounds of Differential and Linear Characteristic Probability for Camellia, Daemen, J. and Rijmen, V. (Eds), *FSE 2002, LNCS 2365*, pp. 128-142, Springer-Verlag, Berlin, 2002.

[20] Daemen, J., Knudsen, L.R. and Rijmen, V., Linear Framework for Block Ciphers, *Design, Codes and Cryptography*, 22, 65-87, Kluwer Academic Publisher, Boston, 2001.

[21] Adams, C., Heys, H.M., Tavares, S.E. and Wiener, M. (1999). An Analysis of the CAST-256 Cipher. Available: http://www.engr.mun. ca/ ~howard/PAPERS/cast256.ps.