Avalanche Analysis of Extended Feistel Network

SUBARIAH IBRAHIM[1] MOHD AIZAINI MAAROF[2] NORBIK BASHAH IDRIS[3]

[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

[3]Centre of Advance Software Engineering
Universiti Teknologi Malaysia, CityCampus Jalan Semarak
54100, Kuala Lumpur, Malaysia
Tel: +60-32615–4429, Fax: +60-03–290-4432, E-mail: norbik@utmkl.utm.my

ABSTRACT

In general, block ciphers consist of one top-level structural model into which the round function *F* is plugged into. In order to analyze the security of a cipher, it is also important to study the intrinsic security provided by these top-level structural models. Most research focuses in determining *F* functions that yield secure Feistel Networks (FN). This paper analyses the structural models of a generalized concept of FN known as Extended Feistel Network (EFN). EFN splits the input blocks into $n > 2$ sub-blocks. Like conventional FN, EFN consists of a series of rounds whereby at least one sub-block is subjected to an *F*-function. The work examines the models in terms of its avalanche criterion in order to determine the optimal scheme suitable for the design of a flexible block size cipher. The analysis shows that EFN Type-II is the most optimal structural model for this design.

KEYWORDS

Cryptography, Extended Feistel Network, Avalanche Analysis.

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]. 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 is used in several Advance Encryption Standard (AES) candidates such as CAST-256 [7], MARS [8] and RC6 [9]. The AES candidates use 128-bit block size and 128, 196 and 256 bits key size. The call to AES was made due to the vulnerability of DES. The first drawback is the short key size and another one is its 64-bit block size [10][11]. The small block size is vulnerable to matching cipher-text attacks [12]. As the cryptanalysis techniques become more sophisticated, in future even 128-bit block size may become too small and vulnerable to attacks. Therefore, it is relevant to design a cipher with a flexible block size. Some ciphers with flexible block size are FOX [13] and TST [14]. In fact Rijndael and RC6 were first designed with flexible block sizes. This trend has motivated our work on the analysis of EFN schemes.

There has been considerable research in determining what sorts of *F*-functions yield secure Feistel networks, but little has been

written about the underlying EFN structure [1]. Some work on EFN schemes can be found in [2][15][16][17]. The aim of this paper is to investigate the behavior of EFN structures in terms of the avalanche effect on the cipher-text. Avalanche is an important cryptographic property of a block cipher which states that a cipher satisfies the avalanche criterion if a single plaintext bit is changed, one half of the cipher-text bits will change [18]. This is to determine the optimal scheme that is suitable for the design of a flexible block size cipher.

This paper is organized as follows. In section 2, a formal definition of EFN is given. Section 3 reviews the cryptographic property of avalanche criterion and strict avalanche criterion. The methodology of the avalanche analysis of EFN is given in section 4. Next, the results and discussion are presented in section 5 and finally a conclusion is made in section 6.

2. 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. For the purpose of this paper, we described 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:

$$C_1, C_2, \ldots, C_{n-1}, C_n = P_2 \oplus F(P_1), P_3, \ldots, P_{n-1}, P_n, P_1. \quad (1)$$

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

$$C_1, C_2, \ldots, C_{n-1}, C_n = P_2 \oplus F(P_1), P_3, P_4 \oplus F(P_3), \ldots, P_n \oplus F(P_{n-1}), P_1. \quad (2)$$

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

$$C_1, C_2, \ldots, C_{n-1}, C_n = P_2 \oplus F(P_1), P_3 \oplus F(P_2), \ldots, P_n \oplus F(P_{n-1}), P_1. \quad (3)$$

3. Cryptographic Property – Strict Avalanche Criterion

The corner stone of a block cipher design is to provide confusion and diffusion [19]. Confusion is to complicate the statistical relationship between the cipher-text and the key [20], while diffusion spreads the influence of individual plaintext symbols over as much of the cipher-text as possible, thereby hiding the statistical features of the plaintext [19]. The effect of confusion and diffusion to the cipher-text is known as avalanche effect. A cipher satisfies the avalanche criterion if a single plaintext bit is changed, on average, half of the cipher-text bits change [18][21][22].

Formally avalanche can be defined as follows [18]:

Definition 2.7:
A cipher is said to satisfy the avalanche criterion if, for each key, on average half of the cipher-text bits change when one plaintext bit is changed. That is,

$$E(w(\Delta C) \mid w(\Delta P) = 1) = N / 2 \quad (4)$$

where,

$\Delta P = P' \oplus P''$,
$\Delta C = C' \oplus C''$,
w - the Hamming weight of the specified vector,
and N – the block size.

An extension to avalanche is Strict Avalanche Criterion (SAC) as specified in the following definition [18]:

Definition 2.8:
A cipher is said to satisfy SAC if, for each key, each cipher-text bit changes with a probability of 0.5 when a single plaintext bit is changed. That is,

$Prob(\Delta C_t = 1 \mid \Delta P_t = e_i) = 0.5$ for $1 \le t \le N$ and $1 \le i \le N$

where,

$e_i = [e_1\ e_2 \ldots e_N]$ with

$$e_i = 1 \text{ and } e_j = 0 \text{ for } j \neq i. \qquad (5)$$

SAC is the avalanche probability that can be used as one measure of the performance of a cipher. The fewer rounds it takes for the avalanche probability to converge to 0.5, the more efficient the cipher construction is said to be because it can reach a certain level of security strength with fewer number of rounds [23]. The satisfaction of the avalanche criterion and SAC is a necessary condition for the randomness of the cipher-text.

4. SAC Analysis Methodology

The objective of the SAC analysis is to determine the structural model for EFN that will allow efficient implementation with the fewest number of rounds necessary to achieve a suitable level of security. For this analysis, an experiment was set up to evaluate the SAC properties of EFN Type-I, EFN Type-II and EFN Type-III structural models. In this analysis, DES *F*-function is employed for all three types of EFN models. Three different block sizes were analyzed, that are 128-bit, 192-bit and 256-bit, whereby the size of each sub-block is 32-bit. In general, the procedure of the experiment is as follows:

i. Perform two encryptions, $E(P1,K2)$ and $E(P2,K2)$ to produce cipher-texts $C1$ and $C2$.
ii. Evaluate $Y = C1 \oplus C2$.
iii. Count the occurrence of each bit in Y and evaluate the SAC probability by averaging the counts of bit occurrences.

The encryptions are repeated for rounds 1 – 16 for each pair of plaintexts. The block diagram for the procedure of the experiment is as depicted in **Figure 1**.

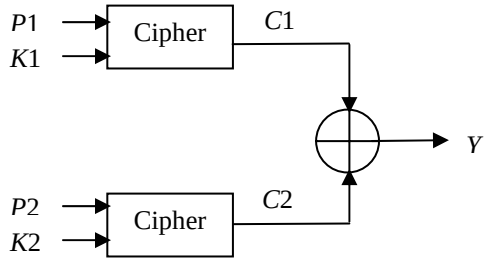

Figure 1: A block diagram for the avalanche effect tests.

The total population of the data is the product of the plaintext space and the key space. Since the total population is very large, therefore it is not possible to test all the data. Therefore a sample of population will be tested. The sample is divided into three data sets as used in [24]. They are grouped as follows:

i. Set $K1 = K2 = \mathbf{0}$, $P1 = \mathbf{0}$ and $P2 = P_i$ where P_i is the plaintext when its ith bit position is set to 1 and all other bits are set to 0 (Note: **0** signifies setting all bit positions to 0).
ii. Set $K1 = K2 = \mathbf{0}$, $P1 = \mathbf{1}$ and $P2 = P_i$ where P_i is the plaintext when its ith bit position is set to 0 and all other bits are set to 1 (Note: **1** signifies setting all bit positions to 1).
iii. Set $K1$ and $K2$ to a random key value with $K1 = K2$. Set $P1$ and $P2$ to the same fixed random value but in every iteration of the test, $P2 = P_i$ where P_i is the plaintext when its ith bit position is changed. This set is repeated for 100 times.

The SAC analysis for DES with conventional FN is also performed and is used to compare the performance of EFN models.

5. Results and Discussion

The SAC probability for each round for all models with the same block size is plotted in order to compare which model will converge to SAC probability = 0.5 faster. The SAC probability for DES is also plotted on each graph so that we can compare the performance with respect to DES. **Figure 2 – Figure 4** are the SAC probability graphs plotted for block size of 128-bit, 192-bit and 256-bit respectively.

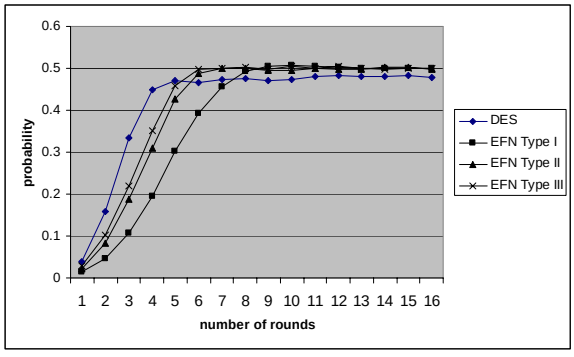

Figure 2: SAC probability comparison for 128 bit block size

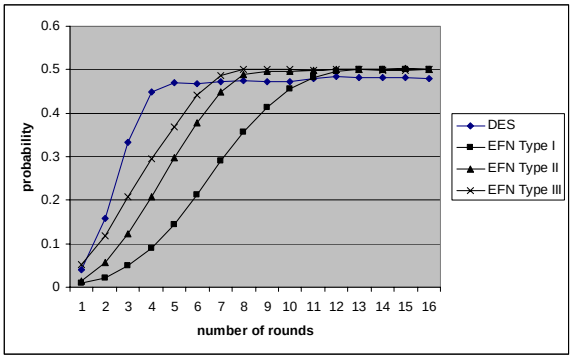

Figure 3: SAC probability comparison for 192-bit block size.

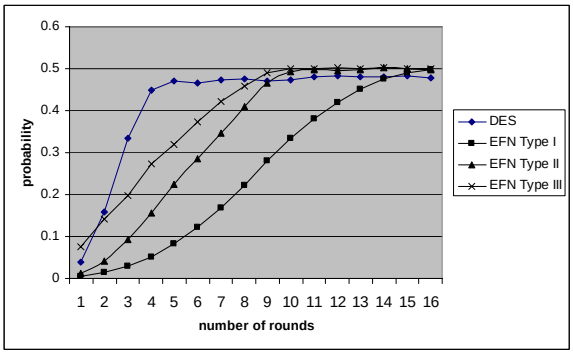

Figure 4: SAC probability comparison for 256-bit block size

From the graphs, it is evident that DES avalanche probability climbs close to 0.5 faster when compared to the three types of EFN for all block sizes of plaintexts. However, DES with conventional FN or 64-bit block size never reach avalanche probability of 0.5 while all three types of EFN managed to achieve 0.5 probability. Among the EFN models, EFN Type-III appears to be the most efficient cipher in terms of avalanche because its probability approaches 0.5 faster than the other two types. Another observation is that more rounds are needed in order to converge to a probability of 0.5 when the block size is increased. In general, EFN Type-II performs almost as well as EFN Type-III and EFN Type-I performs the worst. For EFN Type-II and EFN Type-III models, there is only a small increase in threshold number of rounds to achieve avalanche probability of 0.5 as the block size increases but for EFN Type-I, the increase is almost exponential.

In EFN, the *F*-function is the most computationally expensive operation in a round. EFN Type-II employs half the number of *F*-functions as EFN Type-III as defined in section 2. Since EFN Type-II performs almost as well as EFN Type-III in achieving the avalanche probability of 0.5 and requires less *F*-functions as compared to EFN Type-III, then EFN Type-II is a better choice for designing a cipher with a flexible block size. Furthermore, EFN Type-II can take advantage over parallel architecture, but not the other two types of EFN structural models. For EFN Type-I model, although it requires only one *F*-function for all block sizes, the number of rounds needed to achieve avalanche probability of 0.5 increases almost exponentially.

6. Conclusion

An empirical avalanche analysis was performed on three EFN structural models with DES *F*-function. The avalanche probability can be used as a measure on the performance of a cipher whereby the smaller the threshold number of rounds needed to converge to the avalanche probability of 0.5, implies that a cipher construction is more efficient [23]. The experiment shows that as block size increases, the threshold number of rounds to achieve the avalanche probability of 0.5 also increases.

The *F*-function plays a significant role in achieving the avalanche effect as revealed by the analysis. The empirical analysis shows that as more functions are used for each round the smaller the threshold number of rounds needed by the model to achieve avalanche probability of 0.5. However it is important to note that in EFN the *F*-function is the most computationally expensive operation in a round. Since the performance of EFN Type-II is not that far behind the performance of EFN Type-III and EFN Type-II requires half the number of *F*-functions as EFN Type-III, then EFN Type-II structural model is the optimal scheme for the design of a flexible block size cipher.

7. Acknowledgements

The authors would like to thank UTM and MOSTE for their financial support in this work. Special acknowledgement to Mohd Reza for his assistance in programming 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. InD. 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] 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.

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

[9] 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.

[10] Handshuh, H. and Vaudenay, S. A Universal Encryption Standard. *SAC'99, LNCS 1758*, Springer-Verlag, 2000. Pp. 1-12.

[11] 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.

[12] Lucks, S. On the Security of the 128-Bit Block Cipher DEAL. *FSE'99, LNCS 1636*, Springer-Verlag, 1999. Pp. 60-70.

[13] Junod, P. and Vaudenay, S. FOX: A New Family of Block Ciphers. *SAC 2004, LNCS 3357*, Springer-Verlag, 2005. Pp. 114-129.

[14] Canda, V. and Trung, T. Scalable Block Ciphers Based on Feistel-Like Structure). *Proceedings of Tatracrypt 2001, Tatra Mountains, Mathematica Pub*. 25, 2002. Pp. 39-57.

[15] Vaudenay, S. On Provable Security for Conventional Cryptography. *ICISC'99, Seoul, Korea, LNCS 1787*, Springer-Verlag, 1999. Pp. 1-16

[16] Moriai, S. and Vaudenay, S. On the Pseudorandomness of Top-Level Schemes of Block Ciphers. *ASIACRYPT '00, Kyoto, Japan, LNCS 1976*, Springer-Verlag, 2000. Pp. 289-302.

[17] Zheng, Y., Matsumoto, T. and Imai, H. On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypothesis. *CRYPTO '89, LNCS 435*, Springer-Verlag, 1989. Pp. 461-480.

[18] Heys, H.M. and Tavares, S.E. Avalanche Characteristics of Substitution-Permutation Encryption Networks. *IEEE Transaction on Computers*. 1995. 44(9). Pp. 1131- 1139.

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

[20] Stallings, W. *Cryptography and Network Security: Principles and Practices*, 3rd Edition. Prentice Hall. 2003.

[21] Heys, H.M. Modelling Avalanche in DES-Like Ciphers. *Proceedings of SAC 1996*. August. Queens's University, Kingston, Ontario. 1996.

[22] Vergili, I. And Yucel, M.D. Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen $n \times n$ S-Boxes. *Turk Journal of Electrical Engineering*, Vol. 9, No. 2, 2001.

[23] Heys, H.M. Modelling Avalanche in DES-Like Ciphers. *Proceedings of SAC 96*, Kingston, Ontario, August 1996.

[24] Tuan Sabri bin Tuan Mat. *Design of New Block and Stream Cipher Encryption Algorithms for Data Security*. Universiti Teknologi Malaysia: PHD Dissertation, 2000.