Comparing Cryptographic Algorithms in Scalable Feistel Networks

Khin Yupar Myo
University of Computer Studies, Yangon, Myanmar
nyoei07@gmail.com

Abstract

Scalability of symmetric cipher is still not as natural as for public-key cryptosystems. Most of the current block ciphers do not support freely variable block and key lengths. A generalization of the concepts of Feistel Networks (FN), known as Extended Feistel Network (EFN), that splits the input blocks into n>2 sub-blocks. EFN consists of a series of rounds whereby at least one sub-block is subjected to an F function. The aim of this system compares the performance of scalable Extended Feistel Network by using a variety of file sizes. This is done by compare RC6 that uses EFN-Type II and MARS that uses EFN-Type III encryption algorithms.

1. Introduction

Scalability is a desirable property of cryptographic primitives (block length, key length and number of rounds). Mathematically well-founded scalable cryptographic primitives are useful because they enable us to adjust an encryption configuration according to security and performance requirements for a specific application. An algorithm called scalable, if its basic parameters are alterable by design. For instance, a block cipher is scalable, if its block length *n* and key length *k* can adjust without redefining or extending the cipher.

The first modern block cipher, DES is not scalable at all. Most of the AES candidates are only partially scalable ciphers. Now, the hardware developments are improved and the cryptographic computation can be performed faster. The scalability through primitives will take more memory space to store the cipher code.

In this paper, different files are processed with RC6 that uses EFN-Type II and MARS that uses EFN-Type III. The performance of the encrypted files and the decrypted files are compared with two algorithms.

This paper is organized with six sections. The first section is introduction of the system. Section two explains related work for the system. Section three briefly explains the two Extended Feistel Networks: MARS and RC6 used in this paper. Section four describes System Design and Implementation. Evaluation of the system comparing results is explained in section five. Section six is conclusion of the system.

2. Related Works

Many researchers presented the following using Scalable Feistel Network.

Valer Canda and Tran van Trung analyzed to keep the proposal general and place the emphasis on the scalability and efficiency of the scheme, rather than to design a concrete stand-like cipher, optimal on all platforms [1].

Subariah Ibrahim and Mohd Aizaini Maarof analyzed diffusion method on scalable Fiestel network (FN). They employed in RC6, CAST256 and MARS algorithm. They divided three types of Extended Feistel Network, and analyzed diffusion rate [4].

3. Feistel Network

A Feistel cipher is a special class of iterated block cipher where the cipher text is calculated from the plaintext by repeated application of the same transformation or round function, it is also known as Feistel network (FN). Feistel ciphers are also sometimes called DES like ciphers [5].

In a Feistel cipher, the plaintext being encrypted is split into two halves. The round function *F* is applied to one half using a sub key and the output of *F* is applied to one half using a sub key and the output of *F* is XORed with the other half. The two halves are swapped. Each round follows the same pattern except for the last round where there is no swap [6].

A feature of a Feistel cipher is that encryption and decryption are structurally identical, though the sub keys used during encryption at each round are taken in reverse order during decryption.

3.2. Extended Feistel Network

The Feistel Network (FN) is not very suitable for constructing cipher with block length greater than 64 bits. For that reason, some of the AES candidates introduced the extended Feistel networks (EFN).

These modified structures use four equally-sized sub-blocks and function F. These sub-blocks are mixed through repeated application of keyed, *F*-functions in order to generate a permutation of the input block. The swapping of sub-blocks can be viewed as a circular shift. There are various types of transformations in EFN, such as EFN Type-I, EFN Type-II and EFN Type-III [4].

3.1. Scalable Block Cipher

A block cipher can be characterized by its basic parameters: the block size, b, the key size, k and the number of rounds, r. A cipher security depends on these parameters, the larger size or number, the more secure the cipher is called scalable cipher. A scalable cipher is becoming a trend since a call for Advanced Encryption Standard (AES), which requested for a minimal requirement of 128-bit block size and 128/192/256 bit key sizes. Scalability of key can easily be achieved by using key scheduling algorithm. However, scalability of block size can be achieved through a modification of the size of the basic operations or the modification of the structure of the cipher.

According to their scalability, block ciphers can be classified into the following four categories:

- Strongly scalable-ciphers which by design support any combination of block length n and key length k.
- Fully scalable-ciphers with some minor restrictions regarding the format of n and k (e.g. n must be a power of 2 and k must be a multiple of 32) but without upper limits for these values.
- Partially scalable-ciphers supporting only a small finite set of possible values for n and k.
- Not scalable-ciphers where n and k are fixed by design [1].

3.3. MARS

MARS is a symmetric block cipher, with a block size of 128 bits and a variable key size, ranging from 128 to over 400 bits. It was designed to meet and exceed the requirements for a standard for symmetric key encryption. Design of MARS uses structure, where the top and bottom rounds are designed differently than the middle ones. MARS works with 32 rounds.

MARS has a block length of 128 bits and word-size of 32 bits, it follows that each block consists of four words. Among the various network-structures which are capable of handling four words in a block, it seems that a type-III Extended Feistel Network. The MARS cipher uses a variety of operations (on 32-bit words). It combines exclusive-or, addition, table look-up, multiplication, fixed rotation and data-dependent rotation. Table look-up operation of MARS uses a single table of 512 32-bit words, called the S-box. Sometimes the S-box is viewed as two tables, each of 256 entries [2].

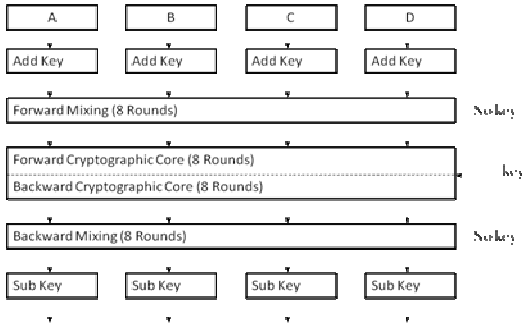

Figure 1. High Level Structure of MARS

A type-III Extended Feistel Network consists of many rounds, where in each round one data word are used to modify all the other data words.

Figure 1 shows the high level structure of MARS. First the data words are added with 4 key words. Then 8 rounds of unkeyed Type-II Feistel mixing are performed. Type-III Feistel mixing means there is always one word that is used to modify the three other words. The modification is done without key information by using S-boxes. The output of the S-boxes is added or xored with the other words. Additional to the S-box mixing several shifts are performed.

Then, the cryptographic core is a Type-III Feistel network. But here the algorithm uses a keyed function instead of the unkeyed S-boxes as in the forward mixing stage. The output of the E-function is also added or xored with the other words. There are total 16 rounds in the core. Eight forward plus eight backward rounds.

The structure of the backward mixing showed in is very similar to the one of the forward mixing. It consists also of 8 rounds of a unkeyed Type-III Feistel network, followed by a key subtraction step.

3.4. RC6

RC6 is a symmetric key block cipher based on the RC5 and designed by Rivest and other researchers at RSA Security. Figure 2 shows the overall structure of RC6. This algorithm depends mainly on the use of four working registers, each of size 32 bits. So, it handles 128 bits input and output blocks. RC6 supports key sizes of 128,192, and 256 bits. RC6 consists of 20 rounds. It has six primitive operations, which are (addition, subtraction, data dependent rotation, fixed rotation, multiplication, XOR). The

use of multiplication greatly increases the diffusion achieved per round. RC6 uses an expanded key table S[0, …, t-1], consisting of key t = 2r + 4 32-bit words. And RC6 uses Extended Feistel Network Type-II. Integer multiplication works by multiplying two 32-bit source values and produces a 64-bit result. RC6 uses of 32-bit variable rotations and integer multiplications [3].

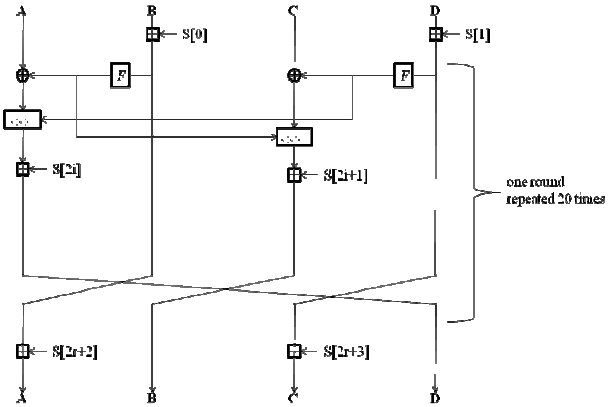

Figure 2. Structure of RC6

4. System Design and Implementation

This paper described the comparison of encryption time and decryption time of various file sizes using MARS that uses Extended Feistel Network Type-III and RC6 that uses Extended Feistel Network Type-II. The inputs of proposed system are either text file or images file. And the system has compared the performance of encryption and decryption as shown in Figure 3.

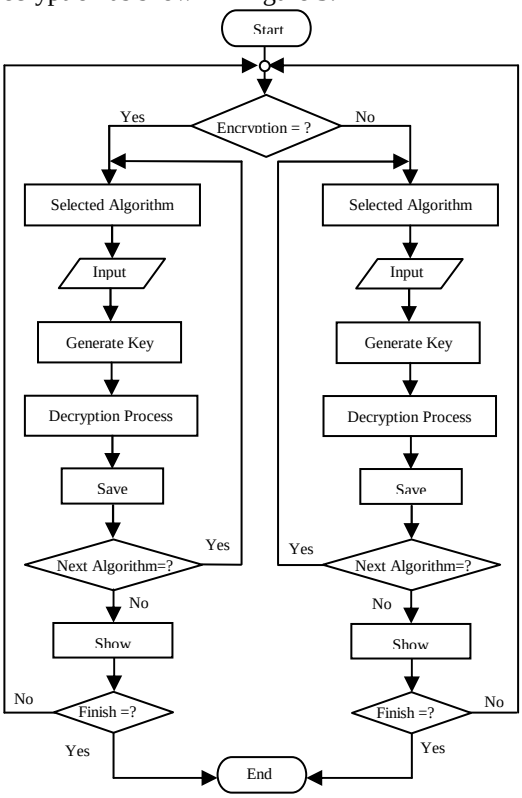

Figure 3. System Design

5. Evaluation of the system comparing results

In this system, same key must be used for both algorithms. The system results compare on various files using MARS and RC6 algorithms. This system is implemented over the single processor version for text file processing at the Table 1 and for image file processing at the Table 2. Performance of MARS is greater than RC6.

Table 1: Encryption and Decryption Time Comparison for Text

File size (KB)	MARS Encrypt/Decrypt (Millisecond)		RC6 Encrypt/Decrypt (Millisecond)	
28.57	4.435	3.2945	4.661	4.841
98.72	14.447	8.764	16.439	16.659
197.44	24.862	17.085	32.878	32.84

Table 2: Encryption and Decryption Time Comparison for Image

File size (KB)	MARS Encrypt/Decrypt (Millisecond)		RC6 Encrypt/Decrypt (Millisecond)	
28.52	2.818	2.7188	4.739	4.911
102.5	10.22	13.6485	16.854	17.131
214.37	22.88	24.492	35.577	35.864

Table 3: Plaintext Estimates for Cryptanalytic Attacks in RC6

	number of rounds				
attack	8	12	16	20	24
differential cryptanalysis	2^{56}	2^{117}	2^{190}	2^{238}	2^{299}
linear cryptanalysis	2^{47}	2^{83}	2^{119}	2^{155}	2^{191}

Table 4: Plaintext Estimates for Cryptanalytic Attacks in MARS

	number of rounds		
attack	8 (Forward)	16 Cryptographic core	8 (Backward)
differential cryptanalysis	2^{20}	2^{240}	2^{20}
linear cryptanalysis		$>2^{128}$	

Table 3 and Table 4 show Plaintext Estimates for Cryptanalytic Attacks in RC6 and MARS. To against attack, the number of known plaintexts must be greater than or equal 2^{128}.

6. Conclusion

This paper has investigated the comparison between Extended Feistel Networks (EFN). This paper described the performance of Scalable Feistel Networks using RC6 that is EFN type-II and MARS that is EFN type-III. After making several testing and comparing two techniques by variety of file sizes, encryption time and decryption time. It can be used for jpeg files and text files format. According to the comparison, MARS is greater performance than RC6 by a variety of file sizes. And then, RC6 is more secure algorithm than MARS in differential attack and linear attack.

It can be extended for bitmap, video and audio file formats.

7. References

[1] Canda, V. and Trung, T. "Scalable Block Ciphers Based on Feistel-Like Structure", 2002.

[2] Carolynn Burwick, Don Coppersmith, Edward D'Avignon, Rosario Genmaro, Halevi, S., Jutla, C., Matyas, S.M., O'Connor, L., Peyravian, M., Safford, D. and Zunic, N. " MARS - A Candidate Cipher for AES",1999.

[3] R. Rivest, M. Robshaw, R. Sidney, and Y. Yin, "The RC6 Block Cipher", NIST AES Proposal,(1998a).

[4] Subariah Ibrahim and Mohd Aizaini Maarof, "Diffusion Analysis of a Scalable Fiestel Network".

[5] http://www.en.wikipedia.org/wiki/feistel_cipher.html.

[6] http://www.x5.net/faqs/crypto/q56.html.