Metamorphic Feistel Networks

Magdy Saeb,

Arab Academy of Science, Technology & Maritime Transport, Alexandria, Egypt

Great Wall Information Security, Kuala Lumpur, Malaysia

www.great-wall-security.com

mail@magdysaeb.net

Abstract: In classical Feistel Networks, a one-way function (F) is using the round key as an input parameter to change its output. However, in this work, the round key serves two roles; it changes the structure, or morphs the one-way function rendering it a metamorphic one-way function (MF) and at the same time encrypts the right hand side of the Feistel Network using this function. We discuss this concept and show the resulting generalized modified structures for various Feistel Networks.

Key words: Feistel Network, Metamorphic, Cipher, Encryption

1. Introduction

In the past forty years, the classical Feistel network [1, 2] has been the corner stone of many ciphers. The basic idea behind this structure is to divide the cipher block into two sides; the right hand and the left hand sides. Using a fixed-structure one-way function and the round key on the right hand side, the function output value is varied. Then, this output is used to encrypt the left hand side. Permutation of the block sides then follows. One can readily notice that the round keys serve one purpose, which is just a value parameter that is used to change the one-way function output. To improve the security of Feistel networks, we utilize the round keys to serve two roles; as an instruction that morphs the structure of the one-way function and as a value parameter to encrypt the right hand block of the cipher [3]. This is accomplished by using a metamorphic key-dependent one-way function. We refer to this metamorphic function by the abbreviation MF. Accordingly, the nonlinearity is tremendously increased. In the following sections, we discuss the proposed Metamorphic Feistel structure using MF, the importance of having a rotation operation in this one-way metamorphic function, how to generate the round keys to resist related key attacks and how to convert unbalanced, alternating, type 1, type 2 and type 3 Feistel Nets to Metamorphic Feistel Nets. The security analysis presented is based on standard security analysis previously discussed in the literature. Finally, we give a summary and our conclusions.

2. The Metamorphic One-way Function

A Feistel network is a symmetric structure used in the construction of block ciphers [2]. It was named after the developer Horst Feistel. A large number of block ciphers use this scheme. These well-known Feistel-based

ciphers include: Blowfish, Camellia, CAST-128, DES, FEAL, GOST 28147-89, ICE, KASUMI, LOKI97, Lucifer, MARS, MAGENTA, MISTY1, RC5, Simon, TEA, Triple DES, Twofish, XTEA, CAST-256, CLEFIA, MacGuffin, RC2, RC6, Skipjack, and SMS4. The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule. Therefore, the code density is nearly halved. A Feistel network is an iterated cipher with an internal function called a round function. It is based on the concept of the invertible product cipher. The Feistel Net provides what Claude Shannon referred to as substitution and permutation (S-P) networks. As it is well-known in the literature; the idea is to provide diffusion and confusion operations in the cipher. Diffusion is used to dissipate statistical structure of plaintext over the bulk of cipher text. Confusion makes the relationship between cipher text and the key as complex as possible. There are a large number of security proofs of this Feistel structure. We will discuss one of these security proofs in some detail. There were also a large number of attacks against this structure. As stated before, we will replace a fixed one-way function with a structurally key-dependent metamorphic function. The modified Feistel net is shown in Figure 1. The metamorphic function structure for one-bit and four-bit structures are shown in Figures 2.a, and 2.b. In practice the four-bit net is replaced by n-bit structure where n is the block size. The subscript i refers to the bit location while the subscript j refers to the round iteration number. The four operations NOP, ROR, XOR and INV refer to no operation, rotate right operation, xor operation and invert operation respectively. All operations are on the bit level [3]. The selection is performed using two round key bits from an agreed-upon location. Since the selected bitwise operations are round key-dependent, the nonlinearity is tremendously increased and we have a different one-way function for each round. The rotate operation is an essential component in this structure to avoid a cyclical behavior [4]. All four operations are bit-balanced. The Feistel XOR operation outside the one-way function is a word-size n-bit operation using L_j and the output of the metamorphic function MF as inputs.

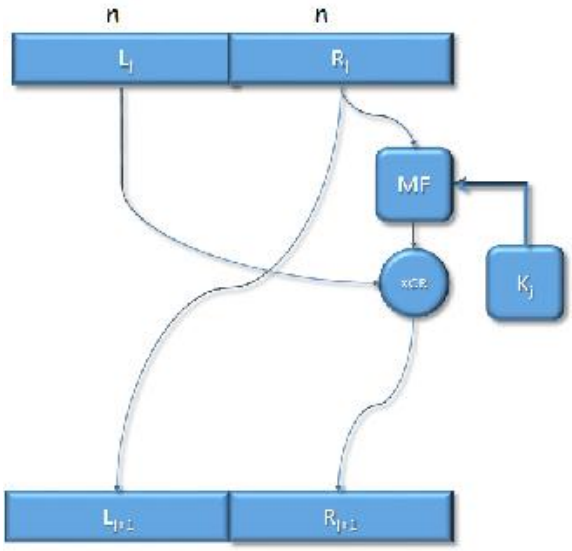

Figure 1: The proposed metamorphic Feistel Net

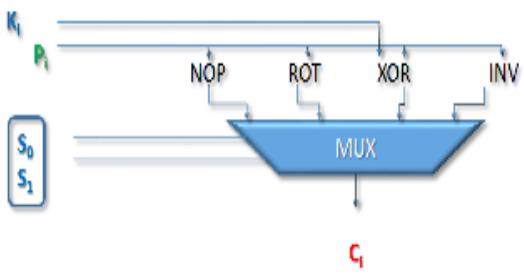

Figure 2.a: The one-bit metamorphic one-way function structure [3]

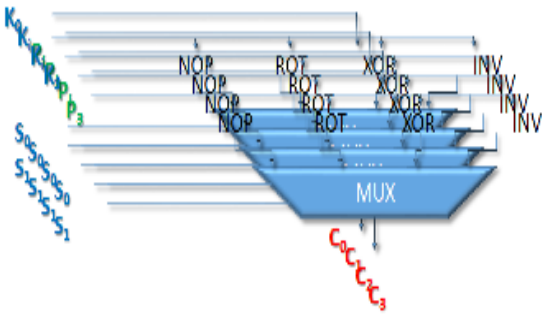

Figure 2.b: A four-bit metamorphic one-way function structure.

To avoid related key attacks, the round keys are generated using two hash functions h_0, h_1. These hash functions are selected pseudo randomly as follows:

Let a random bit string, selected from an agreed-upon location in the round key K_j, is, say, 10110010, then

$K_{j+1} = h_1 (h_0 (h_1 (h_1 (h_0 (h_0 (h_1 (h0 (K_j)))))))))$

3. Generalized Feistel Nets

As mentioned before, there are generalization of the Standard Feistel Net [1] such as; unbalanced Feistel, Alternating Feistel, Type 1, 2 and 3 Feistel Nets. These Feistel Nets, and using the metamorphic one-way function MF, are shown in Figure 3.a, 3.b, 3.c, 3.d, and 3.e.

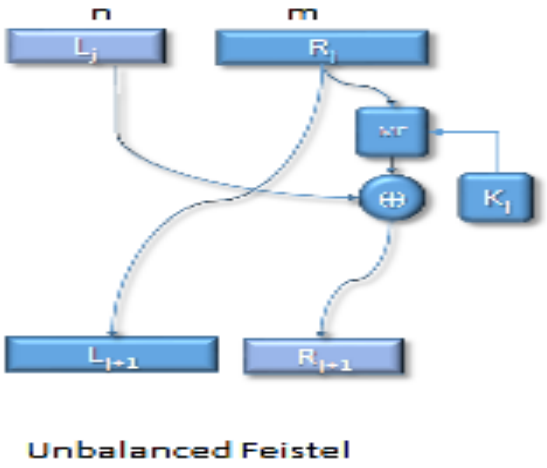

Figure 3.a: Unbalanced Feistel Net with MF

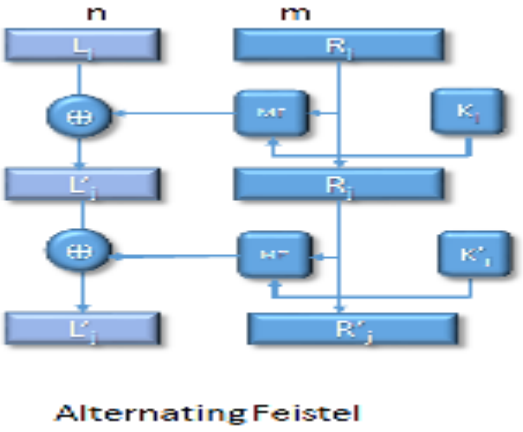

Figure 3.b: Alternating Feistel with MF

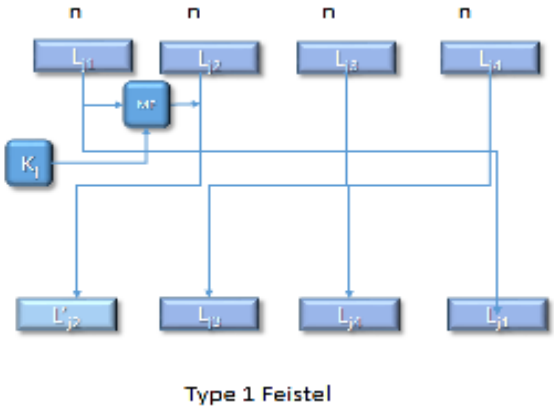

Figure 3.c: Type 1 Feistel

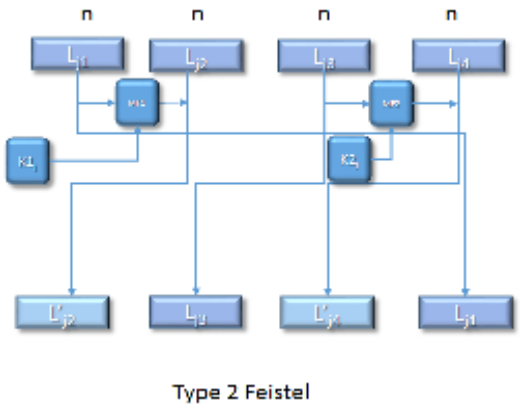

Figure 3.d: Type 2 Feistel

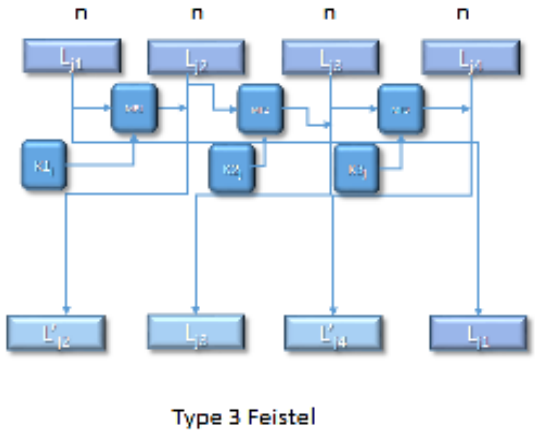

Figure 3.e: Type 3 Feistel

4. Duality Between Hash Functions and Block Ciphers

Examining the structure of the shown hash function (MDP-192), [4], on the left hand side, and ignoring the modulo-2 addition of the final and the initial values, we can readily notice that the applied function is invertible. To explain this in detail, we refer to the Figure 4. Starting from the C_i (Step1) and reversing the number of rotations (step 2), we arrive at the previous value of A_{i-1}. Then using C_i XOR D_i, (step 3) and reversing the number of rotations (step 4), we get the previous value of Bi-1. The same process is repeated to obtain Ci-1and Di-1. The value of Ei-1 is directly obtained from Bi by reversing the number of rotations. Now, we can find the previous values of the nonlinear functions ϕ1i-1 and ϕ 2i-1 by performing the required additions of Ai-1, Bi-1, Ci-1 and Ci- 1, Di-1, Ei-1 respectively. To get the value of Fi-1, we subtract the values of $\phi 1_{i-1}$, $\phi 2_{i-1}$, Ai-1, Ki-1, Wi-1 and Ci from Ai. Therefore, if we substitute the message with a 1024-bit key and the initial values (IV) with a 192-bit plaintext block, one obtains a new block cipher. This block cipher can be called Message Digest Procedure Cipher (MDPC). As stated above, this cipher accepts plaintext blocks of 192-bit length and a key size of up to 1024 bits. This key size can be reduced to 128 bits by padding it with zeroes. This cipher has some features that belong to the Feistel net class of ciphers. We can also notice that the functions ϕ1 and ϕ2 can be converted into two Metamorphic functions.

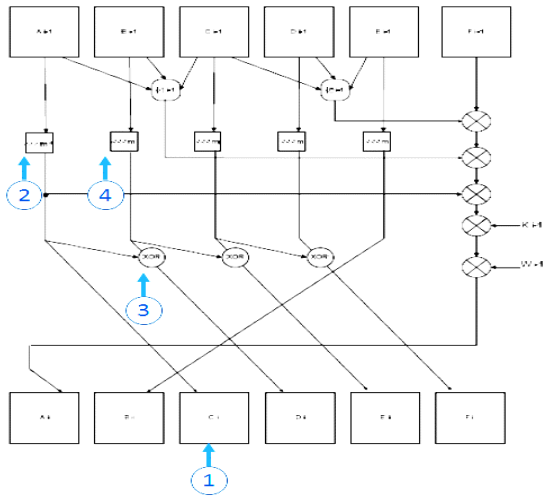

Figure 4: Duality between Hash Functions and Block Ciphers [4]

The importance of having a rotation operation is well explained in this reference [4].

5. Security Proof

A classical product cipher E is given by:

$E: \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$

Where $K \in \{0,1\}^k$, $M \in \{0,1\}^n$, $C \in \{0,1\}^n$ are the key, Message and Cipher respectively. For a metamorphic cipher, there are, in theory, 2^K encryption algorithms since the cipher is key-dependent. Then we get:

$\Xi_K(K): \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$

Where $\Xi_K \in \Xi(K)$ depending on the key K.

We define the vantage that an adversary obtain trying to distinguish Ξ_K from a random permutation (Π) using algorithm A as:

$V(\Xi_K, A) =$

$|Pr\{b \leftarrow A^{\Pi}: b = 1\} - Pr\{K \leftarrow \{0, 1\}^k ; b \leftarrow A^{\Xi K} : b = 1\}|$

The magnitude |.| is taken since $Pr\{b \leftarrow A^{\Pi}: b = 1\}$ could be less than $Pr\{K \leftarrow \{0, 1\}^k ; b \leftarrow A^{\Xi K} : b = 1\}$ for "poorly-designed oracle algorithm" A^{Π}. For the Metamorphic-modified Feistel Network, we define:

$V(\Xi_K, A) = |Pr\{b \leftarrow A^{\Pi}{}_K, \Pi\text{-}1_K: b = 1\} - Pr\{K \leftarrow \{0, 1\} k; b \leftarrow A\Xi_K k, D\Xi_K k: b = 1\}|$

Where, $\Xi_K(K, M) = MF(K) \oplus M_L$

The proof is adapted and summarized based on a proof given by Bellare and Kohono [5, 6]. They have shown that if an adversary A aiming to distinguish a CBC oracle from a random oracle, an adversary $A^{'}$ can be constructed that aims to distinguish a block cipher from a random permutation, such that

$$V(\Xi_K, A) \leq V(E, A^{'}) + (4q^2/2^{n-1}),$$

Where q is the number of queries made by A. In addition, $A^{'}$ makes 2q queries. The time required to make these double queries are not considered in this respect. In their seminal paper, they showed that taking time into account; it will change the difference part into $16q^2/2^{n+1}$ which is the same as: $2^2 .4q^2/ 2^{n-1}. 2^2$.

Obviously, converting the standard Feistel one-way function to a metamorphic key-dependent one-way function will not reduce the security but on the contrary, it will increase the security level.

Summary and Conclusions

We have discussed the different generalizations of Feistel Net. We revisited the security proofs regarding this type of ciphers. Replacing the one-way function in standard Feistel net by another one that is structurally key-dependent metamorphic one-way function will not reduce its security. On the contrary, it generates possible 2^k different structures that the adversary has to figure out before launching an attack. The adversary, therefore, has the sole option of attacking the key. To avoid related key attacks, the round keys were pseudo-randomly generated using two hash functions. We conjecture that the proposed Metamorphic Feistel Cipher is secure for most of today's applications.

References:

1. Bruce Schneier and John Kelsey, "Unbalanced Feistel Networks and Block-Cipher Design," *Fast Software Encryption, Third International Workshop Proceedings* (February 1996), pp. 121-144, Springer-Verlag, 1996.

2. Menezes, Alfred J.; Oorschot, Paul C. van; Vanstone, Scott A.

(2001). *Handbook of Applied Cryptography* (Fifth edition). p. 251. ISBN 0849385237.

3. Magdy Saeb, "The Stone Cipher-192 (SC-192): A Metamorphic Cipher," (IJCNS) International Journal of Computer and Network Security, Vol. 1, No. 2, November 2009.

4. Magdy Saeb, "Design & Implementation of the Message Digest Procedures MDP-192 and MDP-384," ICCCIS2009 International Conference on Cryptography, Coding and Information Security, Paris June24-26, 2009.

5. M. Bellare, T. Kohno, "A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs and applications," in Advances in Cryptology—EUROCRYPT 2003, ed. by E. Biham. Lecture Notes in Computer Science Springer, Berlin, pp. 491–506, 2003.

6. Moses Liskov, Ronald L. Rivest, David Wagner, "Tweakable Block Ciphers," Journal of Cryptology, 24: 588–613, DOI: 10.1007/s00145-010-9073-y, 2011.

Magdy Saeb received the BSEE. School of Engineering, Cairo University, in 1974, the MSEE, and Ph.D. Degrees in Electrical & Computer Engineering, University of California, Irvine, in 1981 and 1985, respectively. He was with Kaiser Aerospace and Electronics, Irvine California, and The Atomic Energy Establishment, Anshas, Egypt. He is a professor emeritus in the Department of Computer Engineering, Arab Academy of Science, Technology & Maritime Transport, Alexandria, Egypt; He was on leave working as a principal researcher in the Malaysian Institute of Microelectronic Systems (MIMOS). Now he is the CTO of Great Wall Information Security, Kuala Lumpur, Malaysia. His current research interests include Cryptography, FPGA Implementations of Cryptography and Steganography Data Security Techniques, Encryption Processors, Mobile Agent Security.

www.magdysaeb.net