A Metamorphic-Enhanced MARS Block Cipher

Ahmed Helmy, Magdy Saeb, A. Baith Mohamed

Arab Academy of Science, Technology and Maritime Transport,
School of Engineering
Computer Engineering Department,
Alexandria, Egypt.

Abstract: MARS is a shared-key (symmetric) block cipher supporting 128-bit blocks and variable key size. MARS is designed to take advantage of the powerful operations supported in today's computers, resulting in a much improved security/performance tradeoff over existing ciphers. In this paper a metamorphic function is added to the MARS cipher that now can be called Metamorphic- Enhanced MARS. This function uses XOR, ROT, INV and NOP logical operation to improve the ciphering process. The objective of this enhancement is to make a high confusion without disturbing the linear and differential characteristics of the MARS cipher.

Keywords: MARS, Metamorphic Cipher, Cryptography, Block Cipher, Two-fish.

Introduction

The Metamorphic-Enhanced Cipher function it is a function that improves the MARS Cipher. In other words, the Metamorphic-Enhanced MARS Cipher is a tied combination between a Stone Metamorphic Cipher, and The Two-fish Block Cipher [1], [2]. It has four low-level operations that are all bit-balanced to encrypt the plaintext bit stream. These bit-balanced operations are: XORing a key bit with a plaintext bit (XOR), inverting a plaintext bit (INV), exchanging one plaintext bit with another one in a given plaintext word using a right rotation operation (ROR), and producing the plaintext without any change (NOP). The aim of this alteration is to provide an improvement to the MARS cipher that introduces high confusion into the enhanced MARS without disturbing its linear and differential diffusion criteria [1].

MARS is a Symmetric-key block ciphers 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 such as pseudorandom number generators, message authentication protocols, stream ciphers, and hash functions. There are many symmetric-key block ciphers which offer different levels of security, flexibility and efficiency. Among the many symmetric-key block ciphers, currently available, are: AES, TwoFish, MARS, RC5, CAST, Blowfish, FEAL, SAFER, and IDEA. These ciphers have received the greatest practical interest [3]. The name of the metamorphic cipher was inspired from the reaction that takes place in a rock when various minerals go from amphibolites facies to some color schist facies. Some of the minerals such as quartz may not take place in this reaction. The process in its essence follows certain rules; however the end result provides a pseudo random distribution of the minerals in the rock or stone. The metamorphic natural process results in thousands or even millions of different shapes of the rock or stone [4]. The sub-keys of The Metamorphic-Enhanced MARS Cipher are generated using a combination of the Meta-MARS encryption function and a one-way hash function where the generated sub-keys stream is used to select the various operations. Moreover, the Meta-MARS encryption function inherits the structure of the MARS block cipher and uses the four bit-balanced operations in the h-function of the MARS to define the function Meta-h. This Meta-h is the heart of Meta-MARS algorithm and is responsible for the key expansion of the algorithm [1].

Receeived July, 6, Reviewed July 16, 2013

In the following sections, we provide an overview of MARS algorithm, MARS structure, key expansion function and finally we provide the structure of Metamorphic-Enhanced MARS cipher.

The MARS Algorithm

MARS is a shared-key block cipher, with a block size of 128 bits and a key size of 128 bits. It was designed to meet and exceed the requirements for a standard for shared-key encryption. It takes four 32-bit words plaintext as input and produces four 32-bit words cipher text as output [3].

The cipher itself is word-oriented, in that all the internal operations are performed on 32-bit words, and hence the internal structure is endian-neutral (i.e., the same code works on both little- endian and big-endian machines). When the input (or output) of the cipher is a byte stream, we use little endian byte ordering to interpret each four bytes as one 32-bit word [5].

The MARS Structure

The MARS structure can be considered as six different layers through which a plaintext block must pass to become a cipher text block [6]:

1. **Pre-Whitening Layer**: The plaintext has 128 bits of key material added to its words modulo 2^{32}.
2. **Forward Mixing Layer**: Eight rounds of unkeyed mixing operations making extensive use of the MARS S-box.
3. **Forward Core Layer**: Eight rounds of the keyed unbalanced Feistel cipher, using a combination of S-box lookups, multiplications, data-dependent rotations, additions, and xors to resist cryptanalytic attack.
4. **Backward Core Layer**: Eight rounds of the keyed unbalanced Feistel cipher, using a combination of S-box lookups, multiplications, data-dependent rotations, additions, and xors to resist cryptanalytic attack.
5. **Backward Mixing Layer**: Eight rounds of unkeyed mixing operations making extensive use of the MARS S-box.
6. **Post-Whitening Layer:** The block has 128 bits of key material subtracted from its words modulo 2^{32}.

Fig. 1 shows the high structure of the MARS algorithm and some of notations will be used:

- D [ ] is an array of 4 32-bit data words. Initially D contains the plaintext words, and at the end of the encryption process it contains the cipher text words.
- K [ ] is the expanded key array, consisting of 40 32-bit words.
- S [ ] am an S-box, consisting of 512 32-bit words. Below we also denote the first 256 entries in S by S0 and the last 256 entries by S1.

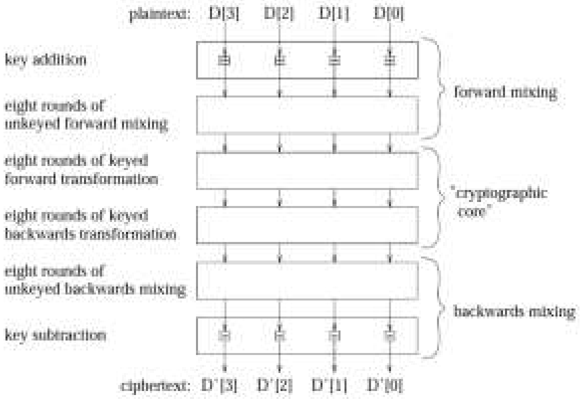
plaintext: D[3] D[2] D[1] D[0]
key addition
eight rounds of unkeyed forward mixing
forward mixing
eight rounds of keyed forward transformation
eight rounds of keyed backwards transformation
"cryptographic core"
eight rounds of unkeyed backwards mixing
key subtraction
backwards mixing
ciphertext: D'[3] D'[2] D'[1] D'[0]

Fig. 1 High-level [structure of the cipher[3]

The first phase provides rapid mixing and key avalanche, to frustrate chosen-plaintext attacks, and to make it harder to "strip out" rounds of the cryptographic core in linear and differential attacks. It consists of addition of key words of the data words, followed by eight rounds of S-box based, un-keyed type-3 Feistel mixing (in "forward mode") [5]. Fig. 2 describes the structure of forward mode.

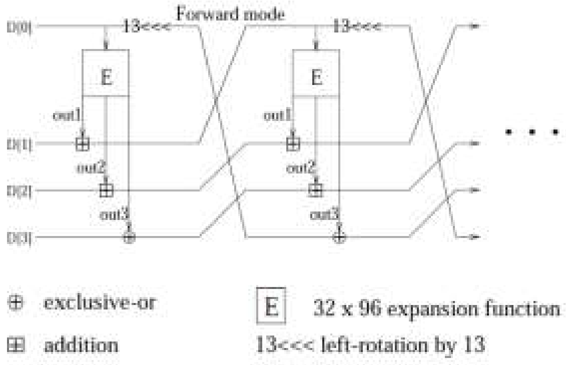

Fig. 2 Forward Mode Structure [3]

The second phase is the "cryptographic core" of the cipher, consisting of sixteen rounds of keyed type-3

Feistel transformation. To ensure that encryption and decryption have the same strength, we perform the first eight rounds in "forward mode" while the last eight rounds are performed in "backwards mode" [5]. Fig. 3 shows the structure of Backward mode.

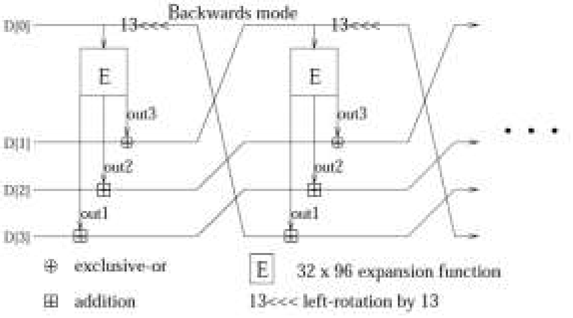

Fig. 3 Backwards mode Structure [3]

The last phase provides rapid mixing and key avalanche, to protect against chosen-ciphertext attacks. This phase is essentially the inverse of the first phase, consisting of eight rounds of the same type-3 Feistel mixing as in the first phase (except in "backwards mode"), followed by subtraction of key words from the data words [5].

Main keyed Transformation

The "cryptographic core" of the MARS cipher is a type-3 Feistel network, consisting of sixteen rounds. In each round we use a keyed E-function (E for expansion) which is based on a novel combination of multiplication, data-dependent rotations, and an S-box lookup. This function takes as input one data word and returns three data words as output Fig. 4 shows the structure of the E - function.

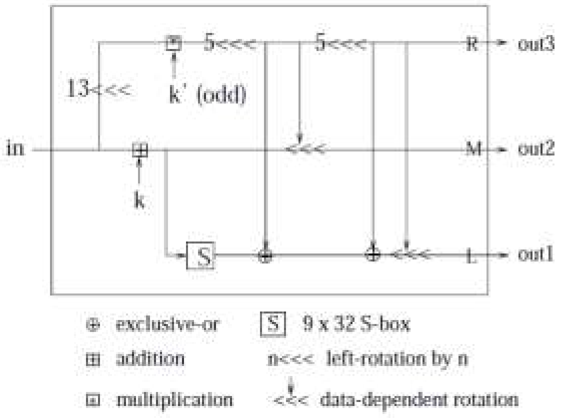

Fig. 4 The E-function of the main keyed transformation [3]

MARS Key Expansion

The key expansion procedure consists of three steps (Figure 4).

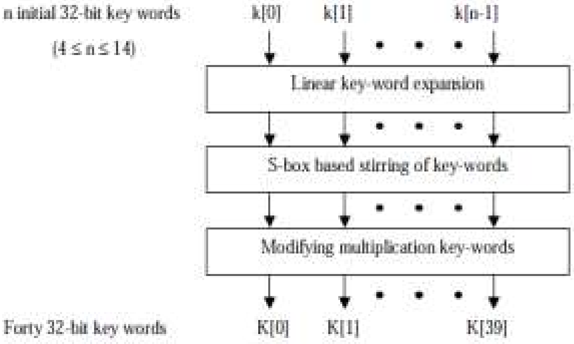
n initial 32-bit key words
(4 ≤ n ≤ 14)
k[0]
k[1]
k[n-1]
Linear key-word expansion
S-box based stirring of key-words
Modifying multiplication key-words
Forty 32-bit key words
K[0]
K[1]
K[39]

Fig. 5 Key expansion procedure of MARS [3]

The first step is "linear expansion" which expands the original user-supplied key to forty 32-bit words using a simple linear transformation. The second step is "S-box based key stirring" which stirs the expanded key using seven rounds of a type-1 Feistel network to destroy linear relations in the key. Then a "multiplication key-word modifying" step examines the key words which are used in the MARS encryption/decryption operation for multiplication and modifies them if needed [3].

The properties of the S-box used in the MARS algorithm [7]:

Differential properties: We require that the S-box has the following properties:

1) The S-box does not contain the all-zero or the all-one word.
2) S does not contain two entries S [I], S [j] (I ≠ j) such that S [I] = S [j], S [I] = ¬ S [j] or S [I] = - S [j].
3) S has 2^{512} distinct xor-differences and 2 * 2^{512} distinct subtraction-differences.
4) Every two entries in S differ by at least four bits.

Linear properties: We try to minimize the following quantities:

5) Parity bias | $\Pr_x$ [Parity (S [X]) = 0] - $\frac{1}{2}$ | We require that the parity bias of S is at most 1/32.

6) Single-bit bias: $\forall j, \mid \Pr_x [S[X]_j = 0] - \frac{1}{2} \mid$ We require that the single-bit bias of S be at most 1/30.
7) Two consecutive bit bias: $\forall j, \mid \Pr_x [S[X]_j \oplus S[]_{j+1} = 0] - \frac{1}{2} \mid$ We require that the two-bit bias of S is at most 1/30;

Metamorphic-Enhanced MARS Cipher

The Metamorphic-Enhanced MARS Cipher is a metamorphic cipher that improves the MARS Cipher. The user key is first encrypted then the encrypted key is used to generate the sub-keys. The Meta-MARS encryption function is built using the four low-level operations in the MARS encryption cipher. All operations are at the bit level composing the basic Crypto Logic Unit (CLU) [1]. Where the operation selection bits can be chosen from any two sub-key consecutive bits and Table1 demonstrates the details of each one of these operations.

Table 1: CLU operations [1]

Mnemonic	*Operation*	*Select Operation code*
XOR	*Ci = Ki ⊕ Pi*	“00”
INV	*Ci =¬ (Pi)*	“01”
ROR	*Pi ← (Pi ,m)*	“10”
NOP	*Ci = Pi*	“11”

The basic crypto logic unit (CLU) is shown in Figure 5. All operations are at the bit level. The unit is to be repeated a number of times depending on the required word or block size.

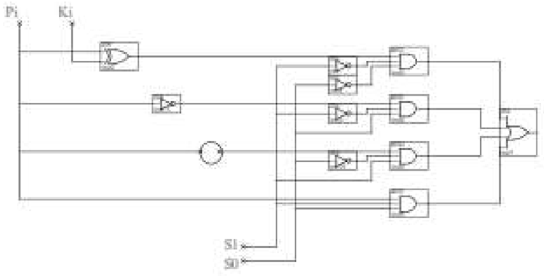

Fig. 5 The crypto logic unit Structure [4]

The rotation operation, referred to by the circular symbol. In the software version the CLU operation can be done by using switch case or if statement. This CLU used in encryption or Decryption process. The operation selection bits (S_1 S_0) can be chosen from any two sub-key consecutive bits; as shown in Figure 6. The same applies for the rotation selection bits (S'_1 S'_0).

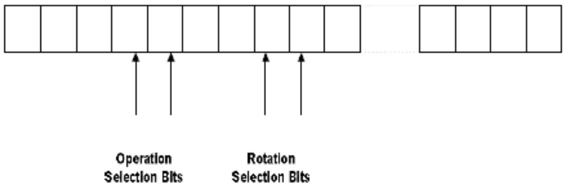

Fig. 6 The proposed key format where the location of the selection bits [4]

The Algorithm

In this section, we provide the formal description of the Metamorphic MARS block cipher algorithm as follows:

Algorithm: METAMORPHIC MARS BLOCK CIPHER

INPUT: Plain text message P, User Key K

OUTPUT: Cipher Text C

Algorithm body:

Encryption Function

Begin

1. Read P message from the user.

2. Read user Key K.

3. Encrypt message plain text by calling the Meta-MARS encryption function.

4. Repeat step 3 till the P_i message encrypted.

End Encryption;

Function Meta-MARS Encryption

Begin

1. Read P_i message.

2. Read next k_i from sub-key;

3. Read selection bits of sub-key;

4. Read rotation selection bits from sub-key;

5. Use selection & rotation bits to select and perform the operation: XOR, INV, ROR, NOP in Meta-h functions in Meta-MARS Algorithm;

```
End Meta-MARS
End Algorithm.
```

Summary and Conclusion

The Metamorphic-Enhanced MARS Cipher is an improvement of the MARS cipher by introducing high confusion without disturbing its linear and differential diffusion criteria. In this work we have discussed the following:

- The Structure of MARS Algorithm.
- MARS key Expansion function.
- The Metamorphic-Enhanced MARS function used to improve MARS cipher.
- The Metamorphic function uses four bit-balanced operations that are pseudo randomly selected
- These bit-balanced operations are: XOR, INV, ROR and NOP. An XOR operationn is XORing a key bit with a plaintext bit. The INV operation is inverting a plaintext bits. The ROR operation is rotating plaintext word to the right. The NOP operation is producing the plaintext without any change.

The proposed enhancement may improve, and surely will not reduce, the security of the MARS cipher.

Reference

[1] Rabie A. Mahmoud, Magdy Saeb, "A Metamorphic-Enhanced Twofish Block Cipher And Associated FPGA Implementation," International Journal of Computer and Network Security (IJCNS), Volume 2, January 2012.

[2] P. Chodowiec, K. Gaj, “Implementation of the Twofish Cipher Using FPGA Devices,” Electrical and Computer Engineering, George Mason University, 1999.

[3] Carolynn Burwick, Don Coppersmith, Edward D’Avignon, Rosario Gennaro, Shai Halevi, Charanjit Jutla, Stephen M. Matyas, Luke O’Connor, Mohammad Peyravian, David Safford, Nevenko Zunic, "The MARS Encryption Algorithm," IBM, August 27, 1999.

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

[5] Mohan H. S and A Raji Reddy, "Performance Analysis of AES and MARS Encryption Algorithms," International Journal of Computer Science (IJCSI), Vol. 8, Issue 4, No 1, July 2011.

[6] John Kelsey and Bruce Schneier, "MARS Attacks! Preliminary Cryptanalysis of Reduced-Round MARS Variants," www.schneier.com/paper-mars-attacks, accessed, Jan. 2013.

[7] C. Burwick, Don Coppersmith, E. D’Avignon, R. Gennaro, S. Halevi, C. Jutla, S. M. Matyas, L. O’Connor, M. Peyravian, D. Safford, N. Zunic, "MARS a candidate cipher for AES," IBM Corporation, September, 1999.

Acknowledgement

We would like to acknowledge the pogramming efforts in this project performed by Eng. Abdelkader Magdy.

Biography

Ahmed Hamdy Helmy received the BSc. In Computer Engineering, Military Technical College (MTC), in 2002. He is a Master degree student in Computer Engineering at Arab Academy for Science.

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. Currently, he is a professor and head of the Department of Computer Engineering, Arab Academy for Science, Technology & Maritime Transport, Alexandria, Egypt; He was on-leave working as a principal researcher in the Malaysian Institute of Microelectronic Systems (MIMOS). He holds five International Patents in Cryptography. His current research interests include Cryptography, FPGA Implementations of Cryptography and Steganography Data Security Techniques, Encryption Processors, Mobile Agent Security.www.magdysaeb.net.

A. Baith MOHAMED, received the BSc. In Computer Science, Vienna University, MSc. And Ph.D. in Computer Science Vienna University, in 1992. He is a Professor at the Arab Academy for Science and Technology (AASTMT), Computer Engineering Department. In addition, he holds the position of Vice Dean for Training and Community Services, College of Engineering and Technology. His research interests include computer and Network Security, Bioinformatics, Steganography, cryptography, and Genetic Algorithms. He was also a member of an International project team in Europe, for design and implementation and maintenance of subsystems in the environment of peripheral processor controls as part of a larger Public Switched Systems (EWSD) in SIEMENS, AG. Austria. Also, he was a scientific researcher in the department of Information Engineering, Seibersdorf Research Institute (Atomic Energy Agency) in Austria, for the design and implementation of security software system in the domain of railway automation project (VAX/VMS, DEC systems). He was also a member of software testing for distribution points in an international project in AEG, Vienna, Austria.

He is a senior member of IEEE Computer Society, USA since 2001.