World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:1, 2014

Improved MARS Ciphering Using a Metamorphic-Enhanced Function

Moataz M. Naguib, Hatem Khater, A. Baith Mohamed

***Abstract*—**MARS is a shared-key (symmetric) block cipher algorithm supporting 128-bit block size and a variable key size of between 128 and 448 bits. MARS has a several rounds of cryptographic core that is designed to take advantage of the powerful results for improving security/performance tradeoff over existing ciphers. In this work, a new function added to improve the ciphering process it is called, Meta-Morphic function. This function use XOR, Rotating, Inverting and No-Operation logical operations before and after encryption process. The aim of these operations is to improve MARS cipher process and makes a high confusion criterion for the Ciphertext.

***Keywords*—**AES, MARS, Metamorphic, Cryptography, Block Cipher.

I. Introduction

THE principal goal in the design of any encryption algorithm must be security. It is required to achieve the desired security level at minimal cost or expenditure. In block ciphers, the cost can be reduced if the algorithm uses less number of rounds. Therefore, it is required to make a trade-off between the security level and cost of the algorithm [1].

Block ciphers are very important in communication systems as they provide confidentiality through encryption. The popular block ciphers are Advanced Encryption Standard (AES) and MARS algorithms. Each cipher uses several rounds of fixed operations to achieve desired security level. The security level is measured in terms of diffusion and confusion [1].

The Metamorphic function used to improve the MARS ciphering process. In other hand, it has four logic-level operations to encrypt the text before and after ciphering process. These operations such as: XOR, INV, ROR and NOP. XORing (XOR) process applied on the key with a plaintext and producing a new encrypted text. Inverting (INV) process applied on the plaintext bit and deriving a new inverted text. The rotating (ROR) process applied on the plaintext which rotates the text to the right by a given rotating distance. The No-Operation (NOP) process produces the plain text without any change. 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 [2].

Moataz M. Naguib, Hatem Khater, Baith Mohamed are with the Computer Engineering Department, Arab Academy for Science Technology & Maritime Transport, AASTMT, Alexandria, Egypt (e-mail: moataz.alex1@gmail.com; hatem.a.khater@gmail.com; baithmm@hotmail.com).

The name of the metamorphic cipher was inspired from the reaction that takes place in a rock when various minerals go from amphibolite's 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 Meta-Morphicnatural process results in thousands or even millions of different shapes of the rock or stone [3], [4].

II. Description of MARS

MARS has a heterogeneous structure, with cryptographic core rounds that are wrapped by simpler mixing rounds. The cryptographic core rounds provide strong resistance to all known cryptanalytical attacks, while the mixing rounds provide good avalanche and offer very wide security margins to thwart new attacks [5]. It 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.

MARS takes as input four 32-bit plaintext data words A, B, C, D and produces four 32-bit Ciphertext data words A', B', C', D'. The cipher is word-oriented, in that all the internal operations are performed on 32-bit words. MARS is a type-3 Feistel network, divided into three phases: A 16-round "cryptographic core" phase wrapped with two layers of 8-round "forward" and "backwards mixing" as shown in Fig. 1.

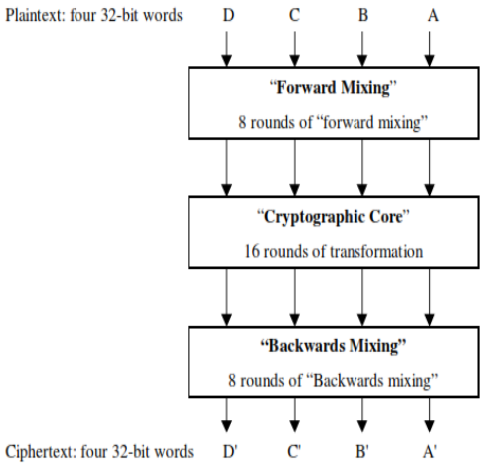

Fig. 1 High-level structure of MARS encryption procedure [5]

The cryptographic core rounds provide strong resistance to all known cryptanalytical attacks, while the mixing rounds

provide good avalanche and offer very wide security margins to thwart new (yet unknown) attacks.

MARS accepts a variable size user-supplied key ranging from 4 to 14 words (i.e., 128 to 448 bits). MARS uses a key expansion procedure to "expand" the user-supplied key (consisting of n 32-bit words, where n is any number between 4 and 14) into a key array K [ ] of 40 words for the encryption/decryption operation [5].

The MARS cipher uses a variety of operations to provide a combination of high security, high speed, and implementation flexibility. Specifically, it combines exclusive-or (XOR), addition, subtractions, multiplications, and both fixed and data-dependent rotations. MARS also uses a single (S-box) table of 512 32-bit words to provide good resistance against linear and differential attacks, as well as good avalanche of data and key bits. This S-box is also used by the key expansion procedure. Sometimes the S-box is viewed as two tables, each of 256 entries, denoted by S_0andS_1. In the design of the S-box, it generated the entries in a "pseudo-random fashion" and tested that the resulting S-box has good differential and linear properties [5].

III. S-Box Design

In the design of the S-box, we generated a "pseudorandom fashion" and tested that the resulting S-box has good differential and linear properties [6].

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. Within each of the two S-boxes S0; S1, every two entries differ in at least three of the four bytes. (We note that it is very unlikely that a random S-box will have this property, and so we first "fix" the S-box by modifying one of the entries in each pair that violates this condition).
3. S does not contain two entries S[i] S[j] (i≠j)such that Si or S[i]=¬S[j].
4. S has($\binom{512}{2}$) distinct XOR-differences and S *($\binom{512}{2}$) distinct subtraction-differences.
5. Every two entries in S differ by at least four bits.

Linear properties: We try to minimize the following quantities:

6. Parity bias: $|\Pr_x[\text{parity}(S[x]=0]-\frac{1}{2}|$.
7. Single-bit bias:$\forall_j$, $|Pr_x[S[x]_j=0]-\frac{1}{2}|$.
8. We require that the single-bit bias of S be at most 1/30.
9. Two consecutive bits bias: $\forall_j, |\Pr_x[S[x]_j \oplus S[x]_{j+1}-\frac{1}{2}|$.
10. We require that the two-bit bias of S be at most 1/30.
11. Single-bit correlation:$\forall_{i,j}$, $|\Pr_x[S[x]_j = x_i]-\frac{1}{2}|$.
12. We minimize this quantity over all he S-boxes that satisfy the conditions 1-8.

IV. The MARS Structure

The MARS structure can be considered as six different layers through which a plaintext block must pass to become a Ciphertext block [7]:

1. **Pre-Whitening Layer**: The plaintext has 128 bits of key material added toits words modulo 2^{32}.
2. **Forward Mixing Layer**: Eight rounds of un-keyed mixing operations making extensive use of the MARS S-box.
3. **Forward Core Layer**: Eight rounds of 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 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 un-keyed 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. 2 shows the high structure of the MARS algorithmand some of notations will be used [6]:

- D [ ] is an array of 4 32-bit data words. Initially 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 byS1.

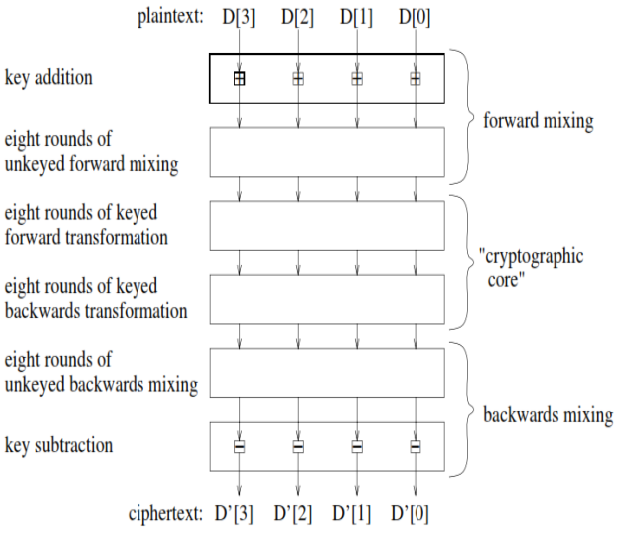

Fig. 2 High-level structure of the cipher [6]

V. MARS Key Expansion

The MARS key expansion procedure expands the user-supplied key ranging from 4 to 14 words into a 40-word key for use in the encryption/decryption operation.

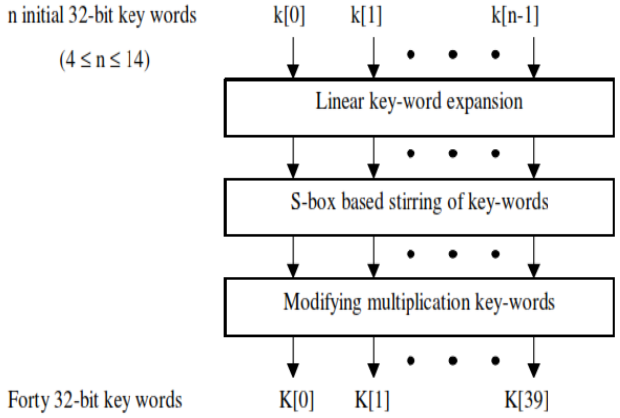

Fig. 3 Key expansion procedure of MARS [5]

The key expansion procedure consists of three steps (as shown in Fig. 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 [5].

VI. Metamorphic Function

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). Table I demonstrates the details of each one of these operations [2].

TABLE I
CLU Operations [2]

Mnemonic	*Operation*	*Select Operation code*
XOR	$Ci = Ki \oplus Pi$	"00"
INV	$Ci = \neg (Pi)$	"01"
ROR	$Pi \leftarrow (Pi, m)$	"10"
NOP	$Ci = Pi$	"11"

The Meta-MARS function used before and after cipher process to improve ciphering, the plaintext is used to be an input to the Meta-MARS function. Then the output of the Meta-MARS function used to be input to the Encryption function. Finally the output of the ciphering process is used to be an input of the Meta-MARS function the following figure describes the ciphering process.

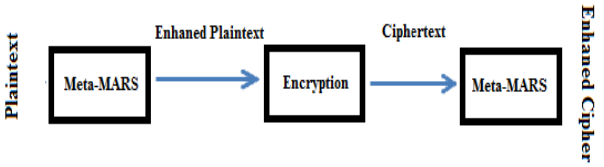

Fig. 4 Cipher Processing Cycle

Fig. 4 shows, the encryption process cycle. The Meta-MARS function used 2 times at the encryption process for encrypt the plaintext and the Cipher text. The objective of this enhancement is to make a high confusion without disturbing the linear and differential characteristics of the MARS cipher then applied on the plaintext and produce a new enhanced text.

VII. Meta-Function Pseudo Code

In this section, the simple pseudo code shows the processing steps of the Cipher Processing Cycle:

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 user.
2. Read user Key K.
3. Encrypt message plain text by calling theMeta-MARS function and produce the Enhanced text.
4. Encrypt enhanced text by using the EncryptionMARS function and produce cipher text.
5. Encrypt Ciphertext by calling the Meta-MARSfunction and produce the enhanced cipher text.

End Encryption;

Function Meta-MARS Encryption
Begin
1. Read Pi message.
2. Read next k_i from sub-key;
3. Read selection bits from sub-key;
4. Case 00:
   XOR: Pi with Ki.
   Case 01:
   INV: Pi.
   Case 10:
   ROR: Rotate Pi.
   Case 11:
   NOP: No Change Pi.

End Meta-MARS
End Algorithm.

VIII. Summary and Conclusion

The proposed Meta-Morphic function improves MARS cipher process. In this work, we have discussed the following:

- Description of MARS Encryption Algorithm.
- The structure of MARS Cipher.
- The design criteria of S-Box.
- The MARS Key expansion.
  - The Metamorphic enhanced function used before and after cipher process to improve ciphering, the plaintext is used to be an input to the Meta-MARS function. Then the output of the Meta-MARS function used to be input to the Encryption function. Finally the output of the ciphering process is used to be an input of the Meta-MARS function.
  - Metamorphic function has four logic-level operations to encrypt the text before and after ciphering process. These operations such as: XOR, INV, ROR and NOP.

The objective of this enhancement is to make a high confusion without disturbing the linear and differential characteristics of the MARS cipher. Appendix A shows the results of ciphering process.

Appendix A

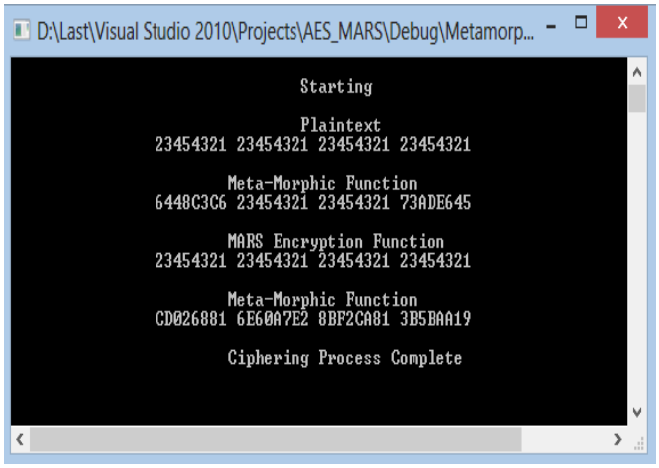

Fig. 5 The results of Meta-Morphic function before and after Encryption process

Acknowledgements

The authors would like to acknowledge Eng. Abdelkader Magdy for his patience and helpful guidance.

References

[1] 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.
[2] Rabie A. Mahmoud, Magdy Saeb, "A Metamorphic-Enhanced Two fish Block Cipher and Associated FPGA Implementation," International Journal of Computer and Network Security (IJCNS), Volume 2, January 2012.
[3] Ahmed Helmy, Magdy Saeb and A. Baith Mohamed, "A Metamorphic-Enhanced MARS Block Cipher," The International Journal of Computer Science and Communication Security (IJCSCS), July, 2013.
[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] 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.
[6] 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 candidate cipher for AES," IBM Corporation, September, 1999.
[7] John Kelsey and Bruce Schneier, "MARS Attacks! Preliminary Cryptanalysis of Reduced-Round MARS Variants".

Moataz M. Naguib received the BSc. In Computer Engineering from Arab Academy for Science in 2006.He is a Master degree student in Computer Engineering at Arab Academy for Science.

Hatem A. Khater received BSc. in Electrical Engineering, MSc. in Electronic and Communication Engineering and Ph.D. in Computer Engineering, Kent University, United Kingdom, in 2008. He is Dr. at the Arab Academy for Science and Technology (AASTMT), Computer Engineering Department, Electronic Communication Engineering Department, College of Engineering and Technology, College of Computing & Information Technology, Walls University, Electronics and Computer Engineering Department Kent University. In addition, he holds the position of Chief of Naval Research and Development Department. His research interests include Software Engineering, cryptograph, Image Feature Detection, Matching Technique,, Geometric Transformation, Image Registration, Pattern Recognition, Computer Graphics, Web Programming, Automatic Controls, Modern Electronics communication, Acoustics, Voice Identifications, GIS, International and European Business, Economics & Management information Systems, Member and Reviewer at IET, also Member of Image and Information Engineering Research Group, University of Kent, U.K.

A. Baith Mohamed received the BSc in Computer Science, Vienna University, MSc and PhD 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 (2010). He is also get the position of Director of Arab Academy for Science, Technology and Maritime Transport, Latakia, SYRIA branch (2013). His research interests include computer and Network Security, Bioinformatics, Steganography, cryptography, and Genetic Algorithms. He was also a member of an International projects teams in Europe, for design and implementation and maintenance of subsystems in the environment of peripheral processor controls as part of a large 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 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.