Cryptanalysis of Fast Encryption Algorithm for Multimedia FEA-M

Miodrag J. Mihaljević and Ryuji Kohno, *Member, IEEE*

***Abstract*—Certain weaknesses in the algebraic structure of recently proposed fast encryption algorithm for multimedia FEA-M are pointed out. It is shown that, when the secret key consists of k bits, under realistic chosen and known plaintext attacks, the secret key recovery has complexity proportional to $2k^2$ and k^4, respectively, implying that FEA-M is an insecure algorithm even if the secret keys of 4096 bits are employed.**

***Index Terms*—Boolean matrix, chosen plaintext attack, cryptanalysis, effective secret key size, encryption, known plaintext attack, multimedia.**

I. Introduction

A NUMBER OF results have been reported regarding to employment of matrices over finite fields for construction of public-key cryptosystems (see [1], for example). Recently, a fast encryption algorithm for multimedia, FEA-M, has been proposed in [2] as a symmetric-key encryption technique based on matrices over a finite field. Very recently, an undesirable property of FEA-M that it has the effective secret key size much smaller than the nominal one, as well as the related vulnerability are reported in [3].

This letter shows a complete breakability of FEA-M even if a secret key of 4096 bits is employed. Two methods for cryptanalysis are proposed corresponding to the realistic chosen and known plaintext attacks.

II. Overview of FEA-M

We consider Boolean matrices, i.e., matrices over the finite field $\mathrm{GF}(2) = \{0, 1\}$, and employ the following notation. Addition and multiplication over $\mathrm{GF}(2)$ are denoted by "$\oplus$" and "$\cdot$", respectively. Let $A = [a_{ij}]_{n\times n}$, $B = [b_{ij}]_{n\times n}$ and $C = [c_{ij}]_{n\times n}$ are three arbitrary Boolean matrices. Then, Boolean matrix addition and Boolean matrix multiplication are defined as follows: $A + B = [a_{ij}] + [b_{ij}] = [a_{ij} \oplus b_{ij}]$ and $AC = [a_{ij}][c_{ij}] = [\bigoplus_{1\le k\le n} a_{ik} \cdot c_{kj}]$ where

$$\bigoplus_{1\le k\le n} a_{ik} \cdot c_{kj} = (a_{i1} \cdot c_{1j}) \oplus (a_{i2} \cdot c_{2j}) \oplus \cdots \oplus (a_{in} \cdot c_{nj}).$$

FEA-M belongs to the class of symmetric encryption techniques, and it performs encryption and decryption according to the following.

At first, the plaintext message should be divided into a series of blocks $P_1, P_2, \ldots, P_r$ with same length n^2. If the length of the last block is less than n^2, we need append some 0s in it so that its length is exactly n^2. The n^2 bits of each block are arranged as a square matrix of order n. The encryption and decryption processes involve the session key K and the initial matrix V_0 which are binary square matrices of order n. Generation and distribution of these two matrices will be discussed later on, and at this moment we assume that they are known by the sender and receiver, and that they are unknown to any other third party. Each plaintext matrix P_i is encrypted into ciphertext C_i in the following way:

$$\begin{aligned} C_1 &= K(P_1 + V_0)K + V_0 \qquad (1)\\ C_2 &= K(P_2 + C_1)K^2 + P_1\\ C_i &= K(P_i + C_{i-1})K^i + P_{i-1}. \qquad (2)\end{aligned}$$

Each corresponding ciphertext matrix C_i is decrypted into plaintext P_i in the following way:

$$\begin{aligned} P_1 &= K^{-1}(C_1 + V_0)K^{-1} + V_0 \qquad (3)\\ P_2 &= K^{-1}(C_2 + P_1)K^{-2} + C_1\\ P_i &= K^{-1}(C_i + P_{i-1})K^{-i} + C_{i-1}. \qquad (4)\end{aligned}$$

FEA-M assumes employment of a master secret key in form of an $n \times n$ binary invertible matrix K_0 which has been distributed to the parties in a secure way. Initially, the sender is required to generate session key in form of a binary matrix K. A method for the generation of the matrix K and its inverse K^{-1} is proposed in [2] and will not be discussed here because it is not relevant for our analysis.

Besides the session key matrix, the sender is required to randomly generate an initial binary matrix V_0. Each element of V_0 is randomly chosen from $\mathrm{GF}(2)$ so that the distribution of 0 and 1 in V_0 obeys the uniform distribution. By using the master secret key matrix K_0, the inverse of the session key matrix K and the initial matrix V_0 can be distributed from the sender to the receiver in the following way. The sender side computes

$$\begin{aligned} K_* &= K_0K^{-1}K_0 \qquad (5)\\ V_* &= K_0V_0K_0 \qquad (6)\end{aligned}$$

and sends (K_*, V_*) to the receiver. The receiver side recovers K^{-1} and V_0 by computing $K^{-1} = K_0^{-1}K_*K_0^{-1}$, and $V_0 = K_0^{-1}V_*K_0^{-1}$.

Manuscript received April 15, 2002. The associate editor coordinating the review of this lettser and approving it for publication was Dr. L. Chen.

M. J. Mihaljević is with the SONY Computer Science Laboratories, Inc., Shinagawa-ku, Tokyo, 141-0022 Japan, and also with the Mathematical Institute, Serbian Academy of Sciences and Arts, Kneza Mihaila 35, Belgrade, Yugoslavia (e-mail: miodragm@turing.mi.sanu.ac.yu).

R. Kohno is with the Yokohama National University, Yokohama, 240-8501 Japan (e-mail: kohno@kohnolab.dnj.ynu.ac.jp).

Publisher Item Identifier 10.1109/LCOMM.2002.803486.

III. Chosen Plaintext Attack

Assumption 1: A collection of the ciphertext blocks $C_1^{(j)}$ is known which corresponds to different pairs $(K_*^{(j)}, V_*^{(j)})$ when $P_1^{(j)}$ is the all zero matrix and $K_*^{(j)}$ is an invertible matrix, $j = 1, 2, \ldots, 2n^4$.

Note that Assumption 1 specifies conditions for a realistic chosen plaintext attack particularly because it requires that only the first block of a plaintext should consists of all zeros, and it does not enforce any constraint on all other plaintext blocks, i.e., they can be arbitrary.

Theorem 1: Complexity of recovering FEA-M master secret key, of n^2 bits in the form of an $n \times n$ binary matrix K_0, is proportional to $2n^4$ providing that Assumption 1 holds.

Proof: Under Assumption 1, for each $j = 1, 2, \ldots, 2n^4$, (3) implies the following one

$$V_0^{(j)} = (K^{(j)})^{-1}(C_1^{(j)} + V_0^{(j)})(K^{(j)})^{-1} \tag{7}$$

where

$$(K^{(j)})^{-1} = K_0^{-1} K_*^{(j)} K_0^{-1}, \tag{8}$$

$$V_0^{(j)} = K_0^{-1} V_*^{(j)} K_0^{-1}. \tag{9}$$

Substituting (8) and (9) into (7) yields

$$K_0^{-1} V_*^{(j)} K_0^{-1} = K_0^{-1} K_*^{(j)} K_0^{-1} (C_1^{(j)} + V_0^{(j)}) K_0^{-1} K_*^{(j)} K_0^{-1},$$

and after certain manipulations we obtain

$$K_0((K_*^{(j)})^{-1} V_*^{(j)} (K_*^{(j)})^{-1}) K_0 = C_1^{(j)} + K_0^{-1} V_*^{(j)} K_0^{-1} \tag{10}$$

for $j = 1, 2, \ldots, 2n^4$, where only K_0 is an unknown variable. Note that, recovering of the master secret key is equivalent to solving the previous system of equations where unknown variables are elements of the master secret key matrix K_0. For each $j = 1, 2, \ldots, 2n^4$, let square $n \times n$ binary matrices $A^{(j)} = [a_{ik}^{(j)}]$, $B^{(j)} = [b_{ik}^{(j)}]$, $C^{(j)} = [c_{ik}^{(j)}]$, $X = [x_{ik}]$ and $Y = [y_{ik}]$, are defined as the following: $A^{(j)} = (K_*^{(j)})^{-1} V_*^{(j)} (K_*^{(j)})^{-1}$; $B^{(j)} = V_*^{(j)}$; $C^{(j)} = C_1^{(j)}$; $X = K_0$; $Y = K_0^{-1}$. Accordingly, the system of (10) can be put into the following form:

$$XA^{(j)}X = C^{(j)} + YB^{(j)}Y, \; j = 1, 2, \ldots, 2n^4 \tag{11}$$

where for each $j = 1, 2, \ldots, 2n^4$, the matrices $A^{(j)}$, $B^{(j)}$ and $C^{(j)}$ are known, and the matrices X and Y are the unknown variables. Note that the fact that Y is the inverse of X does not have any impact on the following approach for recovering the solutions of (11).

For each $i, k = 1, 2, \ldots, n$, the matrix system of equations (11) directly yields the following one:

$$\bigoplus_{m=1}^{n} \bigoplus_{\ell=1}^{n} a_{\ell m}^{(j)} x_{i\ell} x_{mk} = c_{ik}^{(j)} \oplus \left(\bigoplus_{m=1}^{n} \bigoplus_{\ell=1}^{n} b_{\ell m}^{(j)} y_{i\ell} y_{mk} \right), \quad j = 1, 2, \ldots, 2n^4. \tag{12}$$

Note that for each i, k the system of equations (12) contains the following $4n$ unknown binary variables: $[x_{i\ell}]_{\ell=1}^{n}$, $[x_{mk}]_{m=1}^{n}$, $[y_{i\ell}]_{\ell=1}^{n}$ and $[y_{mk}]_{m=1}^{n}$.

Let us introduce $2n^4$ new variables as $x_{i\ell} x_{mk}$ and $y_{i\ell} y_{mk}$, $i, \ell, m, k = 1, 2, \ldots, n$. Then, the system of nonlinear equations is transformed into a system of $2n^4$ linear equations. Accordingly, the complexity of recovering the master secret key is proportional to solving a system of $2n^4$ linear equations which yields the theorem statement.

IV. Known Plaintext Attack

A. Recovering of Session Secret Key

Assumption 2: A sequence of ciphertext blocks C_i obtained from a sequence of known plaintext blocks P_i employing a session key K is available and for each i the matrix $C_i - P_{i-1}$ is an invertible one, $i = 2, 3, \ldots, n^4 + n^2 + 2$.

Theorem 2: Complexity of recovering FEA-M session secret key, of n^2 bits in the form of an $n \times n$ binary matrix K, is proportional to $n^4 + n^2$ providing that Assumption 2 holds.

Proof: Introducing $A_i = C_i - P_{i-1}$ and $B_i = P_i + C_{i-1}$, (2) can be transformed into the following:

$$A_i = KB_iK^i, \qquad i = 2, 3, \ldots, n^4 + n^2 + 2 \tag{13}$$

implying that

$$K^{-i} = KA_{i+1}^{-1}KB_{i+1}, \qquad i = 2, 3, \ldots, n^4 + n^2 + 1. \tag{14}$$

So, we obtain the following system of equations:

$$A_iKA_{i+1}^{-1}KB_{i+1} = KB_i, \qquad i = 2, 3, \ldots, n^4 + n^2 + 1 \tag{15}$$

which can be rewritten as

$$XB_i = A_iYB_{i+1}, \qquad i = 2, 3, \ldots, n^4 + n^2 + 1 \tag{16}$$

where $X = [x_{k\ell}] = K$ and $Y = [y_{k\ell}] = KA_{i+1}^{-1}K$. Note that each $y_{k\ell}$ is a linear combination of certain $x_{rs}x_{uv}$ products. Also recall that Assumption 2 implies that the matrices A_i, A_{i+1}, B_i and B_{i+1} are known. Accordingly, the system of equations (16) is, under Assumption 2, a quadratic one in the unknown entries $x_{k\ell}$ of X, but it becomes a linear one if, beside the n^2 original entries, the n^4 new variables $x_{rs}x_{uv}$ are introduced. The previous directly imply that the complexity of recovering the session key K is proportional to solving a system of $n^4 + n^2$ linear equations.

B. Recovering of Master Secret Key

Assumption 3: A collection of the session secret keys $K^{(j)}$, $j = 1, 2, \ldots, n^4$, has been recovered which corresponds to the same master secret key K_0.

Theorem 3: Complexity of recovering FEA-M master secret key, of n^2 bits in the form of an $n \times n$ binary matrix K_0, is proportional to n^4 providing that Assumption 3 holds.

Proof: Assumption 3 and (5) imply existence of the following system of equations:

$$K_*^{(j)} = K_0(K^{(j)})^{-1}K_0, \qquad j = 1, 2, \ldots, n^4. \tag{17}$$

This system of equations is a quadratic one in the unknown entries $x_{k\ell}$ of K_0, but it becomes a linear one if the n^4 new variables $x_{k\ell}x_{rs}$ are introduced. The previous directly imply that the complexity of recovering the master secret key K_0 is proportional to solving a system of n^4 linear equations when Assumption 3 holds.

Finally, note the following: (i) according to Assumptions 2 and 3, the recovering of the master secret key based on the known plaintext attack require a sample of the overall dimension of $n^4(n^4+n^2+1) \sim n^8$; (ii) according to Theorems 2 and 3, the overall complexity of the master key recovering is proportional to $n^4(n^4+n^2) \sim n^8$.

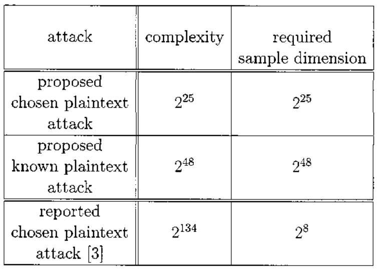
V. Discussion

A set of algebraic techniques has been developed for cryptanalysis of FEA-M. The developed cryptanalytic approaches employ known and chosen plaintext attacks and use the collected samples obtained via the re-synchronization process. It is shown that the real uncertainty about the secret key of FEA-M is undesirable smaller than it is expected based on the nominal secret key length, implying the related methods for cryptanalysis, as well.

Although it is claimed in [2] that the security of FEA-M is based on difficulty of solving the underlying nonlinear equations, Theorems 1–3 show that the underlying system of FEA-M nonlinear equations can be solved in a much more efficient manner than in a general case.

Accordingly, we can say that FEA-M has serious cryptographic weaknesses in its algebraic structure. Note that the scenarios for cryptanalysis which assume a known plaintext attack, or a particular chosen plaintext attack (where in a number of the data streams the first $n \times n$ block consists of all zeros), are at least the possible ones and should be taken into account for the overall security evaluation. Also, it is always interesting and important to know, as precise as possible, the security margins of any enciphering scheme.

TABLE I
Complexity and Required Sample for Recovering a 4096-bit FEA-M Master Secret Key Employing the Proposed Attacks and the Attack Reported in [3]



attack	complexity	required sample dimension
proposed chosen plaintext attack	2^{25}	2^{25}
proposed known plaintext attack	2^{48}	2^{48}
reported chosen plaintext attack [3]	2^{134}	2^{8}

Following Theorems 1–3 and Assumptions 1–3, in Table I, the complexities and required samples of the developed chosen and known plaintext attacks are summarized and compared with the attack reported in [3], assuming a standard FEA-M with 4096-bit master secret key (parameter $n = 64$).

Particularly, in comparison with the attack reported in [3], the attacks proposed in this letter yield a suitable trade-off between the complexity, required sample and the nature (chosen/known plaintext attack), implying substantially more powerful cryptanalysis.

References

[1] H. Sun, “Cryptanalysis of a public-key cryptosystem based on generalized inverses matrices,” *IEEE Commun.Lett.*, vol. 5, pp. 61–63, Feb. 2001.

[2] X. Yi, C. H. Tan, C. K. Siew, and M. R. Syed, “Fast encryption for multimedia,” *IEEE Trans. Consumer Electron.*, vol. 47, pp. 101–107, Feb. 2001.

[3] M. J. Mihaljević and R. Kohno, “On wirelss communications privacy and security evaluation of encryption techniques,” in *IEEE Wireless Communications and Networking Conf. — WCNC2002*, Orlando, FL, Mar. 2002, pp. 865–868.