Comments on the Security of Fast Encryption Algorithm for Multimedia (FEA-M)

A. M. Youssef, and S. E. Tavares, Member, IEEE

Abstract – *We show that the Fast Encryption Algorithm for Multimedia (FEA-M) proposed by Yi et al is insecure. In particular, we present a simple attack that reduces the complexity of obtaining both the session key and the master key to solving a set of linear equations. The low complexity of the attack combined with its simplicity makes it feasible in many multimedia applications.*

Index Terms – Cryptanalysis, Encryption, FEA-M.

I. INTRODUCTION

THE number of applications accessing multimedia content over the Web has grown immensely in the past few years. Combined with the growing number of end users and the relatively easy access to hacking tools, security has become one of the most significant problems for distributing new multimedia contents. Digital data can easily be copied and multiplied without any information loss [7]. This requires security solutions for such fields as distributed production processes and electronic commerce, since the producers seek to provide access control mechanisms to prevent misuse and theft of the material. Encryption is one of the basic tools that can be used to achieve multimedia security. Efficient and secure multimedia data encryption is a challenging task because multimedia data size is usually very large, and because the data needs to be processed in real time. Direct application of standard encryption algorithms may result in an increase in latency to a degree not acceptable by many multimedia applications. Yi *et al* [5], [6] proposed a Fast Encryption Algorithm for Multimedia (FEA-M). The authors claim that the security of FEA-M is based on the difficulty of solving non-linear Boolean equations and time variable Boolean linear equations. In this correspondence, we show that this scheme is insecure. In particular, we present a simple adaptive chosen plaintext attack that reduces the complexity of obtaining both the session key and the master key to solving a set of linear equations. The data required to carry out the attack is only 1.5K Bytes, which makes it feasible and practical in many multimedia applications.

[1] This work was done while the first author was visiting the cryptography and data security lab at Queen's university, Canada.

A. M. Youssef is with the Electronics and Communications Engineering Department, Faculty of Engineering, Cairo University, Egypt (e-mail: amr_y@eleceng.ee.queensu.ca). S. E. Tavares is with the Electrical and Computer Engineering Department, Queen's University, Kingston, ON., K7M1B6, Canada (e-mail: tavares@ee.queensu.ca).

II. FEA-M DESCRIPTION

FEA-M encrypts 64×64 Boolean plaintext matrices using 64×64 Boolean key matrix. The authors in [5] described the encryption and decryption operations of the original FEA-M algorithm as follows:

The sender and the recipient are assumed to share a common Boolean matrix secret-key K_0 in advance. The steps to achieve this common secret matrix are described in [6]. The steps for generating the session key, K, is detailed in [5]. Besides the session key matrix K, the sender is required to randomly generate an initial Boolean matrix V_0. The matrices K_0 and K are invertible matrices of order $n=64$. By using the master key matrix K_0, the sender can send the session key K and the matrix V_0 to the recipient as follows:

The sender computes

$$K^* = K_0 K^{-1} K_0,$$
$$V^* = K_0 V_0 K_0, \tag{1}$$

then sends (K^*, V^*) to the receiver who recovers K, V_0 as follows:

$$K^{-1} = K_0^{-1} K^* K_0^{-1},$$
$$V_0 = K_0^{-1} V^* K_0^{-1}.$$

Then the encryption process proceeds as follow:

The plaintext message is divided into a series of blocks $P_1, P_2, \cdots, P_r$ with same length n^2. The last block P_r is appended with some 0 's if its length is less than n^2. The n^2 bits of each block are arranged as a square matrix of order n. Each plaintext matrix is encrypted into the ciphertext C_i in the following way:

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

where $\oplus$ denotes the XOR operation.

For the sake of added security, the authors recommended that the session key matrix should be updated regularly during the encryption of multimedia data. In what follows we assume that the session key will remain unchanged for at least 3 blocks of plaintext. This is a very realistic assumption. In

Contributed Paper
Manuscript received January 14, 2003

practice, one expects that the session key update will be done at much longer intervals because more frequent updates will severely degrade the system performance. For further details about the algorithm, the reader is referred to [5], [6].

III. The Attack

Schneier [3] provides a nice introduction to different types of cryptanalytic attacks. A mathematical treatment can be found in [1], [4].

The attack described here is an adaptive chosen plaintext attack, i.e., we assume that the cryptanalyst can observe some of the plaintext and its corresponding ciphertext blocks. Moreover, the cryptanalyst can adaptively (depending on the outcome of some previous encryption operations) choose some plaintext blocks and obtain their corresponding ciphertext blocks. Again, the interested reader is referred to [3] for different scenarios on how to apply this kind of attacks in practice.

To break FEA-M, we assume that the cryptanalyst can observe (P_1, C_1). Furthermore, we assume that the cryptanalyst can choose P_2, P_3 and obtain their corresponding ciphertext C_2, C_3 respectively. To recover the session key, K, the attack proceeds as follows:

1. The attacker observes C_1 then chooses $P_2 = C_1 \oplus I$, where I is the identity matrix of order n. By noting that $X \oplus X = 0$ for any Boolean matrix X, the attacker can calculate K^3 as follows:

$$C_2 \oplus P_1 = K(P_2 \oplus C_1)K^2 \oplus P_1 \oplus P_1 = KIK^2 = K^3.$$

2. Again, the attacker chooses $P_3 = C_2 \oplus I$. Then the attacker can calculate K^4 as follows:

$$C_3 \oplus P_2 = K(P_2 \oplus C_2)K^2 \oplus P_2 \oplus P_2 = KIK^3 = K^4.$$

3. The attacker can thus recover the session key K by calculating

$$(C_3 \oplus P_2)(C_2 \oplus P_1)^{-1} = K^4 K^{-3} = K.$$

Then the attacker can solve the linear equation

$$C_1 = K(P_1 \oplus V_0)K \oplus V_0$$

to obtain V_0.

Now after recovering the session key K and V_0, we show how we can also recover the master key K_0. At the first glance at (1), it may seem that the attacker needs to solve quadratic Boolean equations to obtain the master key K_0, which is an NP-complete problem [2]. However, because the equations are structured in a very special way, a simple trick will allow us to recover K_0 by solving a set of Boolean linear equations.

Assume that V^* is an invertible matrix (an assumption that will hold with high probability for this choice of $n = 64$), then we can easily calculate a matrix L such that:

$$K^* = V^* L.$$

Using (1) we have

$$K_0 K^{-1} K_0 = K_0 V_0 K_0 L \Rightarrow K^{-1} K_0 = V_0 K_0 L$$

which is a linear equation that the attacker can easily solve to get K_0. If $n = 64$ (as suggested in [5], [6]) then the data complexity of this attack is only 1.5K Bytes which makes it a very realistic attack in many multimedia applications.

In [6], the encryption operation was slightly modified such that

$$C_i = K^i (P_i \oplus C_{i-1}) K^{i+1} \oplus P_{i-1},$$

where $i = 0,1,\cdots$ and $P_0 = C_0 = V_0$.

An almost identical attack can be carried out against this version of the algorithm. Using the same approach as above, the cryptanalyst calculates $C_2 \oplus P_1$ to get K^3. Then the cryptanalyst calculates $C_3 \oplus P_2$ to get K^5 (note that in the basic version of the algorithm we obtained K^4). The cryptanalyst can now easily recover the session key K by calculating

$$(C_2 \oplus P_1)^2 (C_3 \oplus P_2)^{-1} = (K^3)^2 K^{-5} = K,$$

and the rest of the attack proceeds exactly as before.

IV. Conclusion

The encryption algorithm proposed in [5] and its enhanced version in [6] are insecure. Both the session and the master keys can be recovered by a very low complexity adaptive chosen plaintext attack. Basing the encryption algorithm on matrix operations only is risky. After all, linearity has been, and remains, the curse of cryptographers.

References

[1] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, 1996.

[2] N. Courtois, A. Shamir, J. Patarin and A. Klimov, "Efficient algorithms for solving overdefined systems of multivariate polynomial equations," Proc. of Eurocrypt 2000, LNCS 1807, Springer-Verlag, pp. 392-407, 2000.

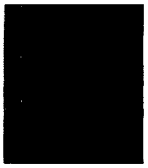
[3] B. Schneier, *Applied cryptography*, Second edition, John Wiley and Sons Inc., 1996.

[4] D. R. Stinson, *Cryptography: Theory and practice*, Second edition, CRC Press Inc., 2002.

[5] X. Yi, C. K. Tan, C.K. Siew and M. R. Syed, "Fast encryption for multimedia," *IEEE Trans. Consumer Electronics*, vol. 47, no. 1, pp. 101-107, Feb. 2001.

[6] X. Yi, C. K. Tan, C. K. Siew and M. R. Syed, "ID-based key agreement for multimedia encryption," *IEEE Trans. Consumer Electronics*, vol. 48, no. 2, pp. 298-303, May 2002.

[7] H. H. Yu, D. Kundur, L. Ching-Yung, "Spies, thieves, and lies: the battle for multimedia in the digital era," *IEEE Multimedia*, vol.8, no. 3, pp. 8-12, July-Sept. 2001.



A. M. Youssef received the B.Sc. and M.Sc. degrees from Cairo University, Cairo, Egypt, in 1990 and 1993 respectively, and the Ph.D. degree from Queen's University, Kingston, ON., Canada, in 1997. After receiving the Ph.D., he worked for the Nortel Networks until mid 1999, and then he joined the Center for Applied Cryptographic Research at the university of Waterloo, Canada, until the end of 2001. He is currently an assistant professor with the Department of Electronics and Communications Engineering, Cairo University. His main research interests are in the area of cryptology and data security.

S. E. Tavares obtained a B.Eng. degree at McGill University in Montreal, an MS degree from Caltech in Pasadena, and a Ph.D. from McGill University, all in electrical engineering. Dr. Tavares is a professor of electrical and computer engineering at Queen's University at Kingston, ON., Canada. He has worked at the National Research Council of Canada in Ottawa and spent portions of sabbaticals at Stanford University and Bell Northern Research in Ottawa. His current research interests include cryptology and communications protocols.