Cryptanalysis of the Parameterized Improved Fast Encryption Algorithm for Multimedia

Rabeah Al-Zaidy, Aleksandar Kircanski, and Amr M. Youssef, *Senior Member, IEEE*

***Abstract*—The Parameterized Improved Fast Encryption Algorithm for Multimedia (PIFEA-M) is a fast cipher recently proposed by Chefranov (IEEE communications letters, Vol. 12, No. 6, June 2008) to resist an implementation dependent differential attack on earlier versions of the cipher. In this paper we show that a similar differential style attack can still break PIFEA-M with a very low data and computational complexity.**

***Index Terms*—Cryptanalysis, multimedia encryption, FEA-M, IFEA-M, PIFEA-M.**

I. Introduction

Confidentiality plays one of the key roles in proper implementation of multimedia applications over the Internet. Due to the widespread existence of eavesdropping and hacking tools, privacy of the content has to be ensured for users exchanging multimedia data such as video or voice. Encryption is one of the basic tools to achieve this privacy. The volume of information exchanged in multimedia applications is high and encryption algorithms designed for this purpose have to be fast. At the same time, the algorithm has to be secure enough.

To address this problem, Yi *et al.* [1] proposed Fast Encryption Algorithm for Multimedia (FEA-M). The design of the cipher utilizes Boolean matrices and does not follow a typical scheme of neither block nor stream cipher design. In [2], a practical adaptive chosen plaintext attack on FEA-M, requiring only 1.5 kilobytes of data, has been presented. Similar attack was also described in [3]. In [4], it is shown that the underlying system of FEA-M nonlinear equations can be solved in a much more efficient way than in general case. In the same paper, IFEA-M cipher has been proposed by modifying FEA-M so that it resists algebraic attacks and to provide tolerance to packet loss errors.

A problem with possible improper implementation of IFEA-M has been pointed out in [5]. Assuming that the attacker is able to force the user to use the same session key twice (for example by controlling the pseudorandom generator through public time service), the attacker would then be able to find the master key using a differential known plaintext attack. To defend against this differential attack, Chefranov [6] proposed PIFEA-M, a parameterized version of IFEA-M, and estimated that its performance is around 25% better than of IFEA-M. As for resistance to previously reported software dependent differential attack, in [6] it is claimed that breaking the cipher requires at least $O(2^{72})$ operations, which is practically infeasible using current technologies.

In this paper we show that, under the same assumptions, PIFEA-M is still suspectable to differential attacks. Let (P_i^j, C_i^j) denote a plaintext-ciphertext pair produced by i-th encryption in session j. Given the pairs (P_1^1, C_1^1), (P_1^2, C_1^2), (P_2^1, C_2^1) and (P_2^2, C_2^2), we show that the attacker can recover all other successive plaintexts P_i, $i \geq 3$ from both sessions with very small computational complexity.

II. PIFEA-M Specification

In this section, we briefly review the specifications of PIFEA-M. For further details, the reader is referred to [6]. PIFEA-M encrypts $n \times n$ Boolean matrices using $n \times n$ key. Master key K_0 is assumed to be shared by the users in advance and the steps to achieve common secret matrix are described in [7]. Session key K, initial matrix V and parameter matrix R are generated by the sender and transmitted to receiver as follows:

$$\begin{array}{rcl} K^* & = & K_0 \cdot K^{-1} \cdot K_0 \\ V^* & = & K_0 \cdot V \cdot K_0 \\ R^* & = & K_0 \cdot R \cdot K_0 \end{array} \qquad (1)$$

The receiver discloses obtained data as follows:

$$\begin{array}{rcl} K^{-1} & = & K_0^{-1} \cdot K^* \cdot K_0^{-1} \\ V & = & K_0^{-1} \cdot V^* \cdot K_0^{-1} \\ R & = & K_0^{-1} \cdot R^* \cdot K_0^{-1} \end{array} \qquad (2)$$

The parameter matrix R contains five n-bit numbers r_k, $k = 1, \ldots 5$ contained by the first five rows of the matrix. All other elements of the matrix are set to zero. Session K and initial matrix V are generated randomly by sender.

The message to be transmitted is padded with zeros if needed and then divided to blocks $P_1, \ldots P_r$ of size n^2. These blocks are then arranged as matrices of dimension $n \times n$ and encrypted and decrypted as follows:

$$\begin{array}{rcl} C_i & = & (P_i \oplus A_{r_1 r_2}) B_{r_3 r_4 r_5, i} \oplus A_{r_1 r_2} \\ P_i & = & (C_i \oplus A_{r_1 r_2}) B^{-1}_{r_3 r_4 r_5, i} \oplus A_{r_1 r_2}, \end{array} \qquad (3)$$

where $A_{r_1 r_2} = V^{r_1} K^{r_2}$, and $B_{r_3 r_4 r_5, i} = V^{r_3} K^{r_4 + i} V^{r_5}$.

III. The Attack

We present a differential style known plaintext attack, provided that the following assumption holds:

Assumption 1: It is assumed that the same session key matrices K and V are used are used in two sessions [6].

Again, we stress the fact that the cipher designer in [6] explicitly specified that the cipher is secure under the above assumption. In fact, resisting such attacks was the main design goal of PIFEA-M.

Manuscript received August 22, 2008. The associate editor coordinating the review of this letter and approving it for publication was C.-K. Wu.

The authors are with the the Concordia Institute for Information Systems Engineering (CIISE), Concordia University, Montreal, Quebec, Canada (e-mail: {r_alzaid, a_kircan, youssef}@ciise.concordia.ca).

Digital Object Identifier 10.1109/LCOMM.2008.081335

Given the four plaintext-ciphertext pairs (P_i^1, C_i^1), (P_i^2, C_i^2), (P_{i+1}^1, C_{i+1}^1), (P_{i+1}^2, C_{i+1}^2), our proposed attack proceeds as follows:

1. Considering the difference between C_i^1 and C_i^2 yields:

$$\begin{aligned} \Delta C_i &= ((P_i^1 \oplus A_{r_1,r_2}) \cdot B_{r_3,r_4,r_5,i} \oplus A_{r_1,r_2}) \\ &\oplus((P_i^2 \oplus A_{r_1,r_2}) \cdot B_{r_3,r_4,r_5,i} \oplus A_{r_1,r_2}) \\ &= \Delta P_i \cdot B_{r_3r_4r_5,i} \end{aligned} \tag{4}$$

   Substituting $i = 1$ and $i = 2$ in (4) and using the four plaintext-ciphertext pairs, the values of $B_{r_3r_4r_5,1}$ and $B_{r_3r_4r_5,2}$ can be obtained.

2. From the cipher specification, we have:

$$\begin{aligned} B_{r_3r_4r_5,1} &= V^{r_3} \cdot K^{r_4+1} \cdot V^{r_5} \\ B_{r_3r_4r_5,2} &= V^{r_3} \cdot K^{r_4+2} \cdot V^{r_5} \end{aligned} \tag{5}$$

   Inverting both sides of the first equation and then multiplying the equations gives

$$B_{r_3r_4r_5,2} B_{r_3r_4r_5,1}^{-1} = V^{r_3} K V^{-r_3} \tag{6}$$

   By noting that

$$\begin{aligned} B_{r_3r_4r_5,i+1} B_{r_3r_4r_5,i}^{-1} &= \\ V^{r_3} K^{r_4+i+1} V^{r_5} (V^{r_3} K^{r_4+i} V^{r_5})^{-1} &= \\ V^{r_3} K V^{-r_3}, \end{aligned} \tag{7}$$

   then, from (6), we get:

$$B_{r_3r_4r_5,i+1} = B_{r_3r_4r_5,2} \cdot B_{r_3r_4r_5,1}^{-1} \cdot B_{r_3r_4r_5,i} \tag{8}$$

   Thus $B_{r_3r_4r_5,i}$ for $i \geq 3$ can be calculated recursively.

3. As for $A_{r_1r_2}$, it can be easily derived by solving the linear matrix equation (for $i = 1$ or $i = 2$):

$$A_{r_1r_2} = (C_i \oplus P_i B_{r_3r_4r_5,i})(B_{r_3r_4r_5,i} \oplus I)^{-1}, \tag{9}$$

   where I denotes the identity matrix.

Finally, the knowledge of $B_{r_3r_4r_5,i}$ and $A_{r_1r_2}$ enables the attacker to decrypt the plaintext corresponding to any ciphertext C_i, $i \geq 3$ in the assumed two sessions.

IV. Conclusion

The PIFEA-M algorithm is still vulnerable to a the differential style attack that it was supposedly designed to resist. Using only four plaintext ciphertext pairs, and by solving a set of linear equations over $GF(2)$, all successive ciphertext can be deciphered even without explicitly recovering the secret key. On the other hand, one should note that, while the given attack scenario is based on an explicit assumption from the PIFEA-M algorithm specifications, this scenario is not a usual one.

References

[1] 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.

[2] A. M. Youssef and S. E. Tavares, "Comments on the security of fast encryption algorithm for multimedia (FEA-M)," *IEEE Trans. Consumer Electronics*, vol. 49, no. 1, Feb 2003.

[3] M. J. Mihaljevic and R. Kohno, "Cryptanalysis of fast encryption algorithm for multimedia FEA-M," *IEEE Commun. Lett.*, vol 6, no. 9, pp. 382-384, 2002

[4] M. J. Mihaljevic, "On vulnerabilities and improvements of fast encryption algorithm for multimedia FEA-M," *IEEE Trans. Consumer Electronics*, vol. 49, no. 4, Nov. 2003.

[5] S. Li and K. T. Lo, "Security problems with improper implementations of improved FEA-M," *J. Systems & Software*, vol. 80, no. 5, pp. 791-794, 2007.

[6] A. G. Chefranov, "Parametrized improved fast encryption algorithm for multimedia PIFEA-M," *IEEE Commun. Lett.*, vol. 12, no. 6, pp. 404-406, June 2008.

[7] 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