arXiv:cs/0509036v1 [cs.CR] 13 Sep 2005

Differential Chosen-Plaintext Cryptanalysis of an Improved Fast Encryption Algorithm for Multimedia (FEA-M)

Shujun Li * and Kwok-Tung Lo

Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong SAR, China

Abstract

This paper studies the security of an improved fast encryption algorithm for multimedia (FEA-M). A simple differential chosen-plaintext attack is proposed to completely break the improved FEA-M. The proposed attack is very efficient in complexity and needs only two pairs of chosen plaintext blocks.

Key words: fast encryption algorithm for multimedia, FEA-M, differential chosen-plaintext attack, cryptanalysis

1 Introduction

Multimedia data play important roles in today's digital world. In many multimedia applications, such as pay-TV services, commercial video conferences and

* The corresponding author, personal web site: `http://www.hooklee.com`.
Email addresses: `hooklee@mail.com` (Shujun Li), `enktlo@polyu.edu.hk` (Kwok-Tung Lo).

medical imaging systems, fast and secure encryption methods are required to protect the multimedia contents against malicious attackers. In recent years, many different multimedia encryption schemes have been proposed to fulfill such an increasing demand (Uhl and Pommer, 2005; Furht et al., 2004; Li et al., 2004). In (Yi et al., 2001), Yi et al. proposed a new fast encryption algorithm for multimedia (FEA-M), which bases the security on the complexity of solving nonlinear Boolean equations. Later FEA-M was employed to construct a key agreement protocol by the same authors in (Yi et al., 2002). Since then, some different attacks have been reported (Mihaljević and Kohno, 2002; Mihaljević, 2003; Wu et al., 2003; Youssef and Tavares, 2003), most of which can break the key with a smaller complexity than the simple brute force attack (Mihaljević and Kohno, 2002; Mihaljević, 2003; Wu et al., 2003) and one can even completely break the whole cryptosystem (with only one known and two chosen plaintext blocks) (Youssef and Tavares, 2003). To enhance the security and avoid some other defects, an improved version of FEA-M was proposed by Mihaljević (Mihaljević, 2003). This paper evaluates the security of the improved FEA-M proposed in (Mihaljević, 2003), and points out that it is still insecure against a differential chosen-plaintext attack. The proposed attack is very efficient, since only two pairs of chosen plaintext blocks are needed to completely break the cryptosystem. As a result, the improved FEA-M has to be further enhanced to resist the differential attack; otherwise it cannot be used in the applications where chosen-plaintext attacks are feasible.

2 The Improved FEA-M

The original FEA-M is a block cipher with both plaintext and ciphertext feedback. Previous works have shown that it has the following defects: 1) the key can be easily broken by an adaptive chosen-plaintext attack proposed in (Youssef and Tavares, 2003); 2) an efficient known-plaintext attack can break it with a complexity smaller than the brute force attack (Mihaljević and Kohno, 2002; Mihaljević, 2003; Wu et al., 2003); 3) it is sensitive to packet loss (Mihaljević, 2003) and channel errors due to the use of plaintext feedback. To overcome the above-mentioned defects of the original FEA-M, Mihaljević proposed an improved FEA-M in (Mihaljević, 2003). The improved FEA-M scheme contains two stages: key distribution and working stage. The first stage generates two secret binary matrices, a session key $\boldsymbol{K}$ and an initial matrix $\boldsymbol{V}$, generally from a master key $\boldsymbol{K}_0$, which is known by both the sender and the receiver. The key distribution protocol is actually the one used in (Yi et al., 2002) and can be described as follows.

- The sender randomly computes

$$\boldsymbol{K}^* = \boldsymbol{K}_0 \boldsymbol{K}^{-1} \boldsymbol{K}_0, \tag{1}$$
$$\boldsymbol{V}^* = \boldsymbol{K}_0 \boldsymbol{V} \boldsymbol{K}_0, \tag{2}$$

  and sends $(\boldsymbol{K}^*, \boldsymbol{V}^*)$ to the receiver.

- The receiver recovers $\boldsymbol{K}^{-1}$ and $\boldsymbol{V}$ by computing

$$\boldsymbol{K}^{-1} = \boldsymbol{K}_0^{-1} \boldsymbol{K}^* \boldsymbol{K}_0^{-1}, \tag{3}$$
$$\boldsymbol{V} = \boldsymbol{K}_0 \boldsymbol{V}^* \boldsymbol{K}_0. \tag{4}$$

After the key distribution stage, the sender and the receiver sides can start the encryption/decryption procedure with the session key $\boldsymbol{K}$ and the initial matrix $\boldsymbol{V}$. Denoting the i-th $n \times n$ plain-matrix by $\boldsymbol{P}_i$ and the i-th cipher-matrix by $\boldsymbol{C}_i$, the encryption procedure is as follows:

$$\boldsymbol{C}_i = \boldsymbol{K}\left(\boldsymbol{P}_i + \boldsymbol{K}\boldsymbol{V}\boldsymbol{K}^i\right)\boldsymbol{K}^{n+i} + \boldsymbol{K}\boldsymbol{V}\boldsymbol{K}^i, \tag{5}$$

and the decryption procedure is

$$\boldsymbol{P}_i = \boldsymbol{K}^{-1}\left(\boldsymbol{C}_i + \boldsymbol{K}\boldsymbol{V}\boldsymbol{K}^i\right)\boldsymbol{K}^{-(n+i)} + \boldsymbol{K}\boldsymbol{V}\boldsymbol{K}^i. \tag{6}$$

The above procedure repeats for each plain/cipher-matrix until the plaintext/ciphertext exhausts.

3 The Differential Chosen-Plaintext Attack

In this section, we propose a simple differential chosen-plaintext attack to break the improved FEA-M. Given two plain-matrices, $\boldsymbol{P}_i^{(1)}$ and $\boldsymbol{P}_i^{(2)}$, and their corresponding cipher-matrices, $\boldsymbol{C}_i^{(1)}$ and $\boldsymbol{C}_i^{(2)}$, we can get Eq. (7).

$$\begin{aligned}\boldsymbol{C}_i^{(1)} - \boldsymbol{C}_i^{(2)} &= \left(\boldsymbol{K}\left(\boldsymbol{P}_i^{(1)} + \boldsymbol{K}\boldsymbol{V}\boldsymbol{K}^i\right)\boldsymbol{K}^{n+i} + \boldsymbol{K}\boldsymbol{V}\boldsymbol{K}^i\right) \\ &\quad - \left(\boldsymbol{K}\left(\boldsymbol{P}_i^{(2)} + \boldsymbol{K}\boldsymbol{V}\boldsymbol{K}^i\right)\boldsymbol{K}^{n+i} + \boldsymbol{K}\boldsymbol{V}\boldsymbol{K}^i\right) \\ &= \boldsymbol{K}\left(\boldsymbol{P}_i^{(1)} + \boldsymbol{K}\boldsymbol{V}\boldsymbol{K}^i\right)\boldsymbol{K}^{n+i} - \boldsymbol{K}\left(\boldsymbol{P}_i^{(2)} + \boldsymbol{K}\boldsymbol{V}\boldsymbol{K}^i\right)\boldsymbol{K}^{n+i} \\ &= \boldsymbol{K}\left(\boldsymbol{P}_i^{(1)} - \boldsymbol{P}_i^{(2)}\right)\boldsymbol{K}^{n+i}\end{aligned} \tag{7}$$

Apparently, Eq. (7) means a simple relation between $\Delta\boldsymbol{C}_i = \boldsymbol{C}_i^{(1)} - \boldsymbol{C}_i^{(2)}$ and $\Delta\boldsymbol{P}_i = \boldsymbol{P}_i^{(1)} - \boldsymbol{P}_i^{(2)}$, i.e., the plaintext and the ciphertext differentials:

$$\Delta\boldsymbol{C}_i = \boldsymbol{K}\left(\Delta\boldsymbol{P}_i\right)\boldsymbol{K}^{n+i} \tag{8}$$

As a result, for two consecutive plaintext-matrices, if we choose $\Delta\boldsymbol{P}_{i+1} = \Delta\boldsymbol{P}_i$, we can immediately deduce:

$$
\begin{aligned}
\Delta \boldsymbol{C}_{i+1} &= \boldsymbol{K}\left(\Delta \boldsymbol{P}_{i+1}\right)\boldsymbol{K}^{n+i} \\
&= \boldsymbol{K}\left(\Delta \boldsymbol{P}_{i}\right)\boldsymbol{K}^{n+i} \\
&= \Delta \boldsymbol{C}_i \boldsymbol{K}
\end{aligned} \tag{9}
$$

Thus, if $\Delta \boldsymbol{C}_i$ is invertible, the session key can be derived easily as follows:

$$
\boldsymbol{K} = \left(\Delta \boldsymbol{C}_i\right)^{-1} \Delta \boldsymbol{C}_{i+1} \tag{10}
$$

To make $\Delta \boldsymbol{C}_i$ invertible, one should choose $\Delta \boldsymbol{P}_i$ to be an invertible matrix (note that $\boldsymbol{K}$ is always invertible as suggested in (Yi et al., 2001, 2002; Mihaljević, 2003)).

After $\boldsymbol{K}$ is broken, one can substitute it into Eq. 1 to get a linear equation with n^2 unknown variables, i.e., the n^2 elements of the initial matrix $\boldsymbol{V}$. By solving this linear equation, it is easy to recover $\boldsymbol{V}$. Once $\boldsymbol{K}$ and $\boldsymbol{V}$ are both known, one can use the method proposed in (Youssef and Tavares, 2003) to recover the master key $\boldsymbol{K}_0$.

In the above attack, the attacker only needs to choose two plaintexts with four chosen plaintext matrices, $\boldsymbol{P}_i^{(1)}$, $\boldsymbol{P}_{i+1}^{(1)}$, $\boldsymbol{P}_i^{(2)}$ and $\boldsymbol{P}_{i+1}^{(2)}$, which satisfy $\boldsymbol{P}_{i+1}^{(1)} - \boldsymbol{P}_{i+1}^{(2)} = \boldsymbol{P}_i^{(1)} - \boldsymbol{P}_i^{(2)} = \Delta \boldsymbol{P}$ and $\Delta \boldsymbol{P}$ is an invertible matrix. Considering each matrix is a $n \times n$ binary matrix, $4n^2$ chosen plain-bits are required in total. When $n = 64$ (as suggested in (Yi et al., 2001, 2002)), only 2048 plain-bytes are needed. In addition, the complexity of the proposed attack is very small (in the same order as the one proposed in (Youssef and Tavares, 2003)).

Note that a successful attack requires two encryption sessions with the same session key $\boldsymbol{K}$ and the same initial matrix $\boldsymbol{V}$, one for encrypting the first plaintext $\left\{\cdots, \boldsymbol{P}_i^{(1)}, \boldsymbol{P}_{i+1}^{(1)}\right\}$ and the other for encrypting the second plaintext $\left\{\cdots, \boldsymbol{P}_i^{(2)}, \boldsymbol{P}_{i+1}^{(2)}\right\}$. However, in each encryption session, $\boldsymbol{K}$ and $\boldsymbol{V}$ have to be reset at the sender side and distributed to the receiver side via the key distribution protocol. As a result, in almost all cases it is true that two different sessions have different values of $\boldsymbol{K}$ and $\boldsymbol{V}$. Fortunately, generally the random generation process of $\boldsymbol{K}$ and $\boldsymbol{V}$ is controlled by the system clock [1]. In chosen-plaintext attacks, the attacker has a temporary access to the encryption machine, so he can intentionally alert the system clock before running each session to get the same $\boldsymbol{K}$ and $\boldsymbol{V}$ for two separate sessions. In addition, if FEA-M is implemented in such an insecure way that the second stage of FEA-M can restart without running the key distribution stage, the attack becomes straightforward.

4 Conclusions

This paper introduces a differential chosen-plaintext attack to break an improved fast encryption algorithm for multimedia (FEA-M) proposed in (Mihaljević, 2003). The attack works if four plaintext blocks ($4n^2$ plain-bits) can be chosen and two separate encryption sessions can be run with the same session key and the initial matrix. The proposed attack shows for another time that the security against differential cryptanalysis must be carefully checked when designing a cryptosystem.

[1] In (Yi et al., 2001, 2002; Mihaljević, 2003), it is not mentioned how to realize the random process for each encryption session. In real implementations, using the current time stamp to initialize the seed of the pseudo-random number generator is a normal (if not the only) way to realize a (pseudo-)random process.

5 Acknowledgements

This research was supported by The Hong Kong Polytechnic University's Postdoctoral Fellowships Scheme under grant no. G-YX63.

References

Furht, B., Socek, D., Eskicioglu, A. M., December 2004. Fundamentals of multimedia encryption techniques. In: Furht, B., Kirovski, D. (Eds.), Multimedia Security Handbook. CRC Press, LLC, Ch. 3, pp. 93–131.

Li, S., Chen, G., Zheng, X., December 2004. Chaos-based encryption for digital images and videos. In: Furht, B., Kirovski, D. (Eds.), Multimedia Security Handbook. CRC Press, LLC, Ch. 4, pp. 133–167.

Mihaljević, M. J., 2003. On vulnerabilities and improvements of fast encryption algorithm for multimedia FEA-M. IEEE Trans. Consumer Eletronics 49 (4), 1199–1207.

Mihaljević, M. J., Kohno, R., 2002. Cryptanalysis of fast encryption algorithm for multimedia FEA-M. IEEE Trans. Communications Letters 6 (9), 382–384.

Uhl, A., Pommer, A., 2005. Image and Video Encryption: From Digital Rights Management to Secured Personal Communication. Vol. 15 of Advances in Information Security. Springer Science + Business Media, Inc., Boston, USA.

Wu, H., Bao, F., Deng, R. H., 2003. An efficient known plaintext attack on FEA-M. In: Qing, S., Gollmann, D., Zhou, J. (Eds.), Information and Communications Security: 5th International Conference, ICICS 2003, Huhehaote, China, October 10-13, 2003, Proceedings. Vol. 2836 of Lecture Notes in Computer Science. Springer-Verlag, Berlin Heidelberg, pp. 84–87.

Yi, X., Tan, C. H., Siew, C. K., Syed, M. R., 2001. Fast encryption for multimedia. IEEE Trans. Consumer Eletronics 47 (1), 101–107.

Yi, X., Tan, C. H., Siew, C. K., Syed, M. R., 2002. ID-based key agreement for multimedia encryption. IEEE Trans. Consumer Eletronics 48 (2), 298–302.

Youssef, A. M., Tavares, S. E., 2003. Comments on the security of fast encryption algorithm for multimedia (FEA-M). IEEE Trans. Consumer Eletronics 49 (1), 168–170.