The FEAL-8 Cryptosystem and a Call for Attack

Shoji Miyaguchi

NTT Communications and Information Processing Laboratories
Y-509A, 1-2356, Take, Yokosuka-shi, 238-03, Japan

1 Introduction

With the aim of providing a highly programming efficient cipher system, NTT has developed the open cipher algorithm, FEAL-8 (Fast Data Encipherment Algorithm) [1][2][3], which is a type of secret key cryptosystem.

In general, the cryptanalysis of a secret key cipher can be classified as:

(1) Only ciphertext attack

(2) Known plaintext attack (Not chosen plaintexts are used.)

(3) Chosen plaintext attack

Dr. Shamir demonstrated an attack method for FEAL-8 (eight round FEAL) and eight round DES at Securicom '89, this past March. Some technical Journals have reported that the attack method he demonstrated was type (1), but we feel that the attack was actually type (3). It appears to us that Shamir's method estimates the key using only the ciphertexts that are obtained by enciphering the chosen plaintexts, where the plaintexts are generated by modifying ordinary messages according

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 624-627, 1990.

to Shamir's special rules (In this case, the ordinary messages are used as a source of pseudo-random numbers). For FEAL−8, the possibility of finding the chosen plaintexts from among the ordinary plaintexts is less than 2^{-64} for this attack method, because pairs of special plaintexts are necessary (We hosted him in June 1988, discussed a possible attack to FEAL−8, and got some information through correspondences). Therefore, we can state that his attack will only pose a threat to the practical use of FEAL−8, only if the following three requirements are simultaneously satisfied:

(a) An attacker provides special plaintexts or a program that generates special plaintexts.

(b) Mode of operation is ECB.

(c) The key remains unchanged after the encipherment process, i.e., the same key is used all the time.

As any one of these requirements can be easily avoided, we think that Shamir's attack will not pose a threat to the practical use of FEAL−8. In order to evaluate the security of FEAL−8 in practical usage, we would like to call throughout the world for possible methods to attack FEAL−8. This call will also contribute to further research in cryptology, especially regarding cryptanalysis of secret key cipher algorithms.

2 Outline of the call

2.1 General

2.1.1 Two confirmation stages

Confirmation is divided into two stages: preliminary and final confirmation. Only candidates who pass the preliminary can advance to the final confirmation stage.

2.1.2 Reward

The first attacker who successfully passes the final confirmation stage will be paid the equivalent of one million yen in his or her country's currency.

2.1.3 Effective application period

The call starts from 20th of August 1989, and ends on the 31st of August 1991.

2.1.4 Expenses

All applicants must personally pay all costs.

2.2 Problem of preliminary confirmation

8192 bytes of plaintexts and 8192 bytes of ciphertexts are given. The ciphertexts were made by the FEAL−8 encipherment procedure using a secret fixed key in the ECB mode. The problem is to determine the secret key. Applicant is not required to explain his attack method.

2.3 Final confirmation

2.3.1 Qualification for the final confirmation

Each candidate, who passes the preliminary confirmation and expresses his will to continue, can advance to the final confirmation stage.

2.3.2 The final confirmation problems

The applicant selects one of the two options below.

Option−1: This includes five problems of the following type.
Problem: The secretariat of this call decides 8192 bytes of plaintexts, and enciphers them in the ECB mode using a secret key. The applicant can use both plaintexts and ciphertexts to determine the key used. Note that different keys will be used for each problem.

Option−2: This includes five problems of the following type.
Problem: The applicant decides 8192 bytes of plaintexts, and the secretariat enciphers them in the CBC mode using a secret key. The applicant can use

both plaintexts and ciphertexts to determine the key used. Note that different keys will be used for each problem.

2.3.3 Time limits

Each candidate is permitted a processing time of five hundred hours to solve all five problems which includes the time requested for computer handling etc. Another two weeks are added for mailing.

3 Reference

(1) Application details are being published. One document will be an international call in English, other is the call in Japanese. However, the document entitled "The FEAL-8 Cryptosystem and a Call for Attack" delivered by Miyaguchi at CRYPTO '89 is effective, i.e., not cancelled.

(2) Because no successful attack is anticipated, NTT will continue to use FEAL-8 as we have in the past.

(3) FEAL-8 specifications have been expanded to FEAL-N (N round FEAL), where N is the number of main internal processings. N is even and equal to or larger than 4, but recommended values of N are 4, 8, 16, 32, ... When N=8 or N=4, FEAL-N is the same as FEAL-8 or FEAL-4 which are already published. Users of FEAL-N may select the number N by their own choice. For example, N=4 is suitable for generating Message Authentication Code, MAC, because of high program efficiency (i.e., 1,000 kbps using a 80286 (10MHz) assembler program (450 bytes)).

Reference

[1] S. Miyaguchi, A. Shiraishi, A. Shimizu, "Fast Data Encipherment Algorithm FEAL-8", *Review of the ECL*, Vol. 36, No. 4, 1988.

[2] A. Shimizu, S. Miyaguchi, "Fast Data Encipherment Algorithm FEAL", *Proceedings of EUROCRYPT 87*, April 1987.

[3] A. Shimizu and S. Miyaguchi, "FEAL — Fast Data Encipherment Algorithm", pp. 20-34 and pp. 104-106, *Systems and Computers in Japan*, Vol. 19., No. 7., 1988, SCRIPTA TECHNICA INC, A Wiley Company.