Self evaluation of FEAL-NX

1 Evaluation of security

1.1. Differential cryptanalysis

In extending differential cryptanalysis, Aoki , Kobayashi, and Moriai[1] greatly reduced the computational amount needed [2]. They determined that differential cryptanalysis could not be applied to FEAL with more than 32 rounds.

Biham et al.[3] proposed a new cyptanalysis of Skipjack[4] using impossible differentials. Although regular differential cryptanalysis utilizes high-probability differential characteristic, the cryptanalysis using impossible differentials utilizes low or zero-probability differential characteristic. Aoki developed a new cryptanalysis approach based on impossible differentials and applied it to FEAL. He showed that the upper limit of FEAL, against impossible differentials, was 9 rounds [5].

[1] Kazumaro Aoki, Kunio Kobayashi, and Shiho Moriai. The best differential characteristic search of FEAL. IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences Japan, Vol. E81-A, No. 1, pp. 98--104, 1998. (Japanese preliminary version was presented at ISEC96-31).

[2] Mitsuru Matsui, On correlation between the order of S-boxes and the strength of DES. In Alfredo De Santis, editor, Advances in Cryptology ---EUROCRYPT'94, volume 950 of Lecture Notes in Computer Science, pp.366--375. Springer-Verlag, Berlin, Heidelberg, New York, 1995.

[3] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In Jacques Stern, editor, Advances in Cryptology ---EUROCRYPT'99, volume 1592 of Lecture Notes in Computer Science, pp. 12--23. Springer-Verlag, Berlin, Heidelberg, New York, 1999 (A preliminary version was presented at CRYPTO'98 rump session).

[4] U.S. Department of Defense. SKIPJACK and KEA Algorithms, 1998 (http://csrc. nist. gov/encryption/skipjack-kea.htm).

[5] Kazumaro Aoki. On cryptanalysis with impossible differentials. In 1999 Symposium on Cryptography and Information Security, number T4-1.3 in SCIS'99, International Conference Center Kobe, Kobe, Japan, 1999. Technical Group on Information Security (IEICE). (in Japanese).

1.2. Linear cryptanalysis

Moriai, Aoki, and Ohta expanded a security-confirming method for linear cryptanalysis[6] and showed that linear cryptanalysis can not be applied to more-than-26-round FEAL[7]. Thus, FEAL becomes one of the cryptographic algorithms whose security limit against linear cryptanalysis is known. Other similar secret-key block cryptographic algorithms, those whose limits are known, are DES, LOKI89, and LOKI91.

[6] Mitsuru Matsui, On correlation between the order of S-boxes and the strength of DES. In Alfredo De Santis, editor, Advances in Cryptology ---EUROCRYPT'94, volume 950 of Lecture Notes in Computer Science, pp.366--375. Springer-Verlag, Berlin, Heidelberg, New York, 1995.

[7] Shiho Moriai, Kazumaro Aoki, and Kazuo Ohta. The best linear expression search of FEAL. IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan), Vol. E79-A, No. 1, pp. 2--11, 1996 (The extended abstract was presented at CRYPTO'95).

1.3. History of cryptanalysis on FEAL

The cryptanalysis history of FEAL cipher is shown in Table 1[8]. In the case of differential cryptanalysis and linear cryptanalysis, which don't rely the key length, Table 1 supports the evidence that FEAL-NX (N≥32) is safe.

Table 1 History of cryptanalysis against FEAL

Published year	Chosen plain-text attack	Known plain-text attack
1988	13.3 (4)	
1989		
1990	13.3 (8), 4.3 (4)	
1991	63 (31), 11.0 (8), 3 (4)	16.6 (4), 7.6 (4), 4.6 (4), 14.3 (6), 10.0 (6)
1992		2.3 (4), 6.6 (6), 14 (7), 15 (8), 28 (8)
1993	7 (8)	0 (4), 0 (5), 0 (6)
1994		25 (8), 24 (8), 62 (20)
1995	3.6 (8)	63.7 (25)

Note: Value x(y): the number of chosen plain-texts or known plain-texts cryptanalyzed is 2^x . y is the round number of FEAL being attacked.

[8] Aoki, Ohta, and Moriai: Security evaluation of FEAL , pp. 734-739, NTT R&D Vol. 48, No. 10, Oct. 1999. (in Japanese)

1.4. Cryptanalysis using closure tests

If a cryptographic algorithm includes a closure structure, it can be analyzed easily by the Kaliski et al. developed MCT method (meet-in-the-middle closure test) which detects the closure structure[9]. Morita, and Ohta enhanced the MCT method and developed the SCT method (switching closure test)[10] and applied it to FEAL[11]. They found that FEAL-8 doesn't have a closure structure (with high probability). Although these methods rely on the key length, these results support the evidence that 128-bit-key-length FEAL-NX can not be attacked (computer complexity is about 2^{64}) by using the closure structure.

[9] Burton S. Kaliski Jr., Ronald L. Rivest, and Alan T. Sherman. Is the data encryption standard a group? (results of cycling experiments on DES). Journal of Cryptology, Vol. 1, No. 1, pp. 3--36, 1988.

[10] Hikaru Morita and Kazuo Ohta. New proposal and comparison of closure tests ---more efficient than the Crypto'92 test for DES---. IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan), Vol. E77-A, No. 1, pp. 15--19, 1994 (A preliminary version was presented at CRYPTO'91).

[11] Hikaru Morita, Kazuo Ohta, and Shoji Miyaguchi. Results of switching-closure-test on FEAL. In Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors, Advances in Cryptology --- ASIACRYPT'91, volume 739 of Lecture Notes in Computer Science, pp. 247--252. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

1.5. Statistical evaluation

By defining original indices for data randomness and using theoretical values based on binomial probability, DES to FEAL were shown to offer good data randomness. [12][13]

[12] Akihiro Shimizu and Shoji Miyaguchi: “Fast Data Encipherment Algorithm FEAL,” In David Chaum and Wyn L. Price, editors, Advances in Cryptology --- EUROCRYPT'87, volume 304 of Lecture Notes in Computer Science, pp. 267-278. Springer-Verlag, Berlin, Heidelberg, New York, 1988.

[13] Akihiro Shimizu and Shoji Miyaguchi: “Fast encipherment algorithm FEAL,” IEICE papers, Vol. J70-D, No. 7, pp. 1413-1423, July 1987. (in Japanese)

2. Software implementation

2.1. 8-bit micro processor

The results in Table 2 show that FEAL is very efficient running on the 8-bit micro processors used in the most smart cards.

Table 2 FEAL-NX efficiency

(a) Encryption/Decryption speed

Round number N	Encryption/Decryption speed Kbits/s
32	18.2
64	9.4

Note: Z80H（8bitCPU）, clock 8 MHz, assembler program (278 bytes), not optimized ,work area is 14 bytes.

(b) Key scheduling time

Round number N	Key scheduling time ms
32	4.48
64	8.95

Note: Z80H（8bitCPU）, clock 8 MHz, assembler program (225 bytes), not optimized ,work area is 35 bytes. (excluding storage of expanded keys (key scheduled values))

2.2. 16-bit micro processor

16-bit micro processors will be used soon is in smart cards and portable communication devices. The results of running FEAL on 16-bit micro processors are shown in Table 3 [14]. The results were for 64-bit-key-length FEAL-N (not FEAL-NX). Since the data randomization part of FEAL-NX is identical to that of FEAL-N, the encryption speed of FEAL-NX is the same as that of FEAL-N

Table 3　FEAL-NX efficiency of data randomization part

Round number　N	Encryption/Decryption speed　　Kbits/s
32	220
64	120

Note:　i80286（16bitCPU）, clock 10MHz, assembler program (450 bytes)

[14] Shoji Miyaguchi, Sadami Kurihara, Kazuo Ohta and Hikaru Morita: “Expantion of FEAL Chpher,” NTT R&D, Vol. 39, No. 10, pp. 1439-1450, Oct. 1990.(In Japanese).
Shoji Miyaguchi, Sadami Kurihara, Kazuo Ohta and Hikaru Morita: "Expansion of FEAL Cipher," NTT Review, Vol. 2, No. 6, pp. 117-123, Nov. 1990.

2.3.　32-bit micro processor

Most PCs and WSs use 32-bit micro processors. Results of FEAL on 32-bit micro processors are shown in Table 4.

Table 4　FEAL-NX efficiency

(a) Encryption/Decryption speed

Round number　N	Encryption/Decryption speed　　Mbits/s
32	124
64	64

Note:　Pentium III (32bitMPU), clock 1 GHz, assembler program (N=32　2434 bytes, N=64　4609bytes), optimized , work area is 2044 bytes.

(b) Key scheduling time

Round number　N	Key scheduling time　　μs
32	1.375
64	3.232

Note:　Pentium III (32bitMPU), clock 1 GHz, assembler program (388 bytes), not optimized, work area is 116 bytes. (excluding storage of expanded keys (key scheduled values))

3. Hardware implementation

Two hardware devices have been specially implementation for FEAL. The first was realized as a 1.5 μm CMOS gate array. The results of implementing FEAL-NX on this device are expected to duplicate the FEAL-8 implementation results given in [15]. Since the key scheduling part and data randomizing part are separated, the encryption/decryption speeds shown Table 5 should be accurate. Fixing the number of gates in the data randomization part (encryption part) yields, Table 5.

Table 5 FEAL-NX efficiency (estimated）

Round number N	Encryption/Decryption speed Mbits/s
32	24
64	12

Note: 1.5 μm CMOS gate array, clock 12MHz、the gate amount of randomization part：3.9 KGate

In the second case, we estimated FEAL-NX implementation results from the results of a 0.8 μm gate array FEAL-32 implementation [16]. Here the estimated values are expected to be accurate. These implementation results were developed using different design tools. Since these tools follow the design policy (clock synchronization), the results for FEAL-NX (N=32) are expected to be extremely accurate.

Table 6 FEAL-NX efficiency

Round number N	Encryption/Decryption speed Mbits/s
32	23
64	11.5（estimated）

Note: 0.8μm CMOS gate array, clock 12.5MHz

[15] Hikaru Morita and Shoji Miyaguchi: “FEAL-LSI and its Application,” NTT R&D, Vol. 40, No. 10, pp. 1371-1380, Oct 1991.(In Japanese).
Hikaru Morita and Shoji Miyaguchi: "FEAL-LSI and its Application," NTT Review, Vol. 3, No. 6, pp. 57-63, Nov. 1991.

[16] Masao Aoyama, Hikaru Morita and Tatsuhiro Naganawa: “Cipher and Authentication LSI

for Communication Terminals," NTT R&D, Vol. 44, No. 10, pp. 923-930, Oct. 1995.(In Japanese).
Masao Aoyama, Hikaru Morita and Tatsuhiro Naganawa: "Cipher and Authentication LSI for Communication Terminals," ITU, 7th World Telecommunication Forum, Vol. 1, 2.2B, pp. 251-255, Oct. 1995.

4. Third-party estimation

Australian researchers developed a cryptanalysis software package for DES-type block ciphers[17]. A statistical evaluation of FEAL was reported together with DES and Madryga cipher.

The statistical evaluation in [17] included χ^2 test, serial test, and run test and sequence complexity; binary derivatives were also estimated. Furthermore, avalanche effect, correlation between plain-text and cipher-text, and the correlation between key and cipher-text were estimated. The reported results say that FEAL-N and DES have good characteristics for all indexes and independence between plain and cipher-texts.

The published results are only for 64-bit-key-length FEAL-N. Since the data randomization part of FEAL-NX is identical to that of FEAL-N, their statistical characteristics are the same if the key is fixed. Furthermore, since the key scheduling part of FEAL-NX is a simple expansion of the key scheduling part of FEAL-N, the report supports the evidence that FEAL-NX will show good statistical characteristics for a wide range of key lengths (64~128).

[17] Helen Gustafson, Ed Dawson, Bill Caelli, Comparison of Block Ciphers In Jennifer Seberry and Josef Pieprzyk , editors, Advances in Cryptology --- AUSCRYPT'90, volume 453 of Lecture Notes in Computer Science, pp. 208--220. Springer-Verlag, Berlin, Heidelberg, New York, 1990.