Information for each entry item is restricted to the designated pages. However, the applicant may decide how much page space to assign for any individual entry item.

Receipt Number	

Cryptographic Techniques Overview

1. Name of Cryptographic Technique **FEAL-NX**

Categories
1.Asymmetric Cryptographic Schemes
[✓ 2.Symmetric Ciphers]
3.Hush Functions
4.Pseudo-random Number Generators

Security Functions of Asymmetric Cryptographic Schemes
1.confidentiality 2. Authentication 3. signature 4. key- sharing

Subcategories of Symmetric Ciphers
1. stream ciphers [✓ 2.64-bits block ciphers] 3. 128-bits block ciphers

2. Cryptographic Techniques Overview

2.1 Design policy

(1) Main design

(a) Interface and parts

- ◊ Block length 64bits key length 128bits possible
- ◊ S-box based arithmetic operation and logic operation

(b) Function of randomization

- ◊ High data randomizing structure

(c) Making of Extended key

- ◊ S-box based arithmetic operation and logic operation

(2) Security

(a) Round number

- ◊ Select N ≥ 32 to provide sufficient invulnerability to differential, linear, and impossible differential cryptanalysis

(b) F-function

- ◊ High data randomizing structure

(3) Implementation

(a) Software

- ◊ Well supports 8bit CPU
- ◊ Good for use in current smart cards and portable digital assistants

(b) Arithmetic operation

- ◊ Uses 8-bit addition

(c) Using RAM/ROM

- ◊ Possible to implement using 8bit CPU operation code
- ◊ Moderate memory requirements to store data and programs

2.2 Intended applications

FEAL-NX especially suits implementation on with low-end devices. Its uses include cipher communication, entity authentication, and random number generation. Since it requires just a small amount of coding to achieve 8-bit micro processor operation, it is easy to implement on legacy-machines' ROMs. If implemented on smart cards, authentication using symmetric encipherment is possible.

2.3 Basic theory and techniques

(1) Design theory

◊ Evaluation of randomness [1,2]

(2) Security evaluation

◊ Select N to provide sufficient invulnerability to differential, linear, and impossible differential cryptanalysis [3,4,5]

Results of using

- ◊ Smart card
- ◊ Cipher facsimile
- ◊ ISDN digital telephone
- ◊ Cipher board for personal computer
- ◊ Cipher box for personal computer
- ◊ Cipher LSI
- ◊ Cipher device for network use
- ◊ ATM security compatible element (see [9] for specification)

References of submission

[1] 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.

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

[3] 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).

[4] 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).

[5] 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).

[6] Shoji Miyaguchi, Hikaru Morita, and Atsushi Fujioka: “FEAL encipherment and its application”, IEICE , the symposium of security and reliability about communication network for information society, pp.29-34, Aug. 1991. (in Japanese)

[7] 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.

[8] 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.

[9] ATM Forum: Phase I ATM Security Specification.