受付番号	

暗号技術概要説明書

１．暗号名：　FEAL-NX

分類：　１．公開鍵暗号　　②．共通鍵暗号　　３．ハッシュ関数　　４．疑似乱数生成

詳細分類		
	公開鍵暗号	１．守秘　　２．認証　　３．署名　　４．鍵共有
	共通鍵暗号	１．ストリーム暗号　②．６４ｂｉｔブロック暗号　３．１２８ｂｉｔブロック暗号

２．暗号の概要

２．１　設計方針：

(1) 主要な設計指針

(ア)インターフェースと構成要素

・ブロック長64-bit、鍵長128-bitが利用可能。

・算術演算からなるs-boxと論理演算からなる。

(イ)ラウンド関数の設計

・データ撹拌性の高い構造を持つ。

(ウ) 拡大鍵生成関数の設計

・算術演算からなるs-boxと論理演算からなる。

(2) 安全性：

(ア)差分攻撃、線形攻撃、不能差分攻撃に対して十分な耐性を有することを検証して、回転数（ラウンド数N）を選択（N≧32）．

(イ) 統計的にデータ撹拌効果の高い構造をf関数として採用

(3) 実装：

(ア) ソフトは８ビットμプロセッサ命令コード構築可能。現状では、ICカードと小形携帯機器の用途に適する。

(イ) 算術演算部分には，８ビット加算を採用．

(ウ) 殆ど既存８ビットμプロセッサ命令体系で実現できるとし，データ蓄積／プログラム実装に必要なRAM/ROMの使用量が少なくする。

２．２　想定するアプリケーション：

共通鍵ブロック暗号が利用できるあらゆる局面に利用可能であるが、特に、小形プロセッサ、小容量メモリなどリソースが限定される領域に適する。用途としては、暗号通信、エンティティ認証，乱数生成が想定される。８ビットμプロセッサ命令コードで僅かなプログラムの付加で構築可能であるので，既存機器のプログラム用ROMに導入することによりコントローラに内蔵されるプロセッサ処理として容易に導入可能である．又、ICカードに内蔵することにより，主に，秘密鍵ベースの認証などに利用可能である．

受付番号	

２．３　ベースとして用いる理論、技術：

(1) 設計に用いている理論

・ランダム性評価[1, 2]

(2) 安全性評価

ラウンド数の選択の為に，差分解読法，不能差分利用攻撃，線形解読法に対する評価結果[3, 4, 5]に基づいて決定した．

利用実績（文献[6,7,8]より）：

- **ICカード**
- **暗号FAX**
- **ISDNディジタル電話**
- **パソコン用暗号ボード**
- **パソコン用暗号ボックス**
- **暗号LSI**
- **回線暗号装置**
- **ATMセキュリティ準拠の物品(規格は[9]参照)**

参考文献等：

[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] 清水明宏，宮口庄司：“高速データ暗号アルゴリズムFEAL,” 電子情報通信学会論文誌，Vol. J70-D, No. 7, pp. 1413-1423, July 1987.

[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] 宮口庄司，森田光，藤岡淳：" FEAL暗号とそのアプリケーション," 電子情報通信学会、情報社会における通信網の安全・信頼性シンポジウム, pp.29-34, Aug. 1991.

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

[8] 森田光，宮口庄司: "FEAL-LSIとその応用," NTT R&D, Vol. 40, No. 10, pp. 1371-1380, Oct. 1 991. [英語版] Hikaru Morita and Shoji Miyaguchi: "FEAL-LSI and its Application," NTT Revie w, Vol. 3, No. 6, pp. 57-63, Nov. 1991.

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