各ページ内での各項目の記入スペースの配分は応募者の任意とする	受付番号	

暗号技術概要説明書

１．暗号名： Camellia （カメリア）

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128-bit、鍵長128/192/256-bitが利用可能
- s-boxと論理演算のみで構成し、算術演算は使用しないこと

(ｲ) ラウンド関数の設計：
- 線形変換(P関数)設計において、E2のP関数設計指針を踏襲
- s-box設計において、GF(2^8)上の逆数関数を利用
- アフィン変換を4種類用意することによって4つのs-boxを構成

(ｳ) 補助関数FL/FL^{-1}関数の設計：
- MISTYのFL関数設計指針を踏襲

(ｴ) 拡大鍵生成関数の設計：
- on-the-fly鍵生成が可能なように設計
- 拡大鍵生成時間を1ブロック暗号化時間より短くすること
- 128-bit鍵による拡大鍵生成は、192/256-bit鍵による拡大鍵生成の一部として構成

(2) 安全性：

(ｱ) 差分攻撃、線形攻撃、丸め差分攻撃(Truncated Differential attack)に対して十分な耐性を有するように設計

(ｲ) 高階差分攻撃、補間攻撃、関連鍵攻撃、不能差分利用攻撃(Impossible differential attack)、スライド攻撃などに対して十分な耐性を有することを検証

(ｳ) 等価鍵が発生しないこと

(3) 実装：

(ｱ) 実装環境に応じたラウンド関数の柔軟な実装が可能になるようにすること
- 64-bit CPU、32-bit CPU、ハイエンドスマートカード、ローエンドスマートカード
- 小型ハードウェア実装、高速ハードウェア実装

(ｲ) ソフトウェア実装においてAES finalistsと同程度以上の高速性が実現可能となるようにすること

(ｳ) ソフトウェア実装においてRAM/ROMの使用量を少なくすること

(ｴ) 小型ハードウェア実装において、世界最小クラスのハードウェア規模で暗号化回路が実現可能になるようにすること

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領域に適用可能。なかでも、暗号通信、認証に非常に適している。

さらに、32/64-bit CPU、ハイエンド／ローエンドスマートカード、ハードウェアいずれについてもそれぞれの環境特性に応じた実装を行うことが可能である。

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、技術は、E2(文献[5])またはMISTY(文献[6])の設計で利用されている実績がある

- P関数の設計
  P関数をXORのみで構成したときに差分攻撃と線形攻撃に対して最良の安全性を有するようにP関数を設計する理論（文献[4]）。E2の設計に利用。
- FL関数の設計
  処理速度に大きな影響を与えることなく、差分攻撃と線形攻撃に対する耐性を強化するように設計する技術 (文献[6])。MISTYの設計に利用。

(2) 安全性評価

- 差分攻撃・線形攻撃に対する安全性を最大差分特性確率・最大線形特性確率の上界値によって理論的に示す手法 (文献[3])
- 丸め差分攻撃に対する安全性を評価するための探索アルゴリズム (文献[8][9])

(3) 実装

- GF(2^8)上の逆数関数を部分体GF(2^4)上を利用して実現する技術 (文献[7])
- 実装環境に応じたラウンド関数の柔軟な実装を可能にする技術 (文献[2])

利用実績・参考文献等：

利用実績：なし

主要な参考文献：

[1] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita, “Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms,” SAC2000, LNCS to appear.
[2] K. Aoki, H. Ueda, “Optimized Software Implementations of E2", IEICE Trans., Vol.E83-A, No.1, 2000.
[3] M. Kanda, “Practical Security Evaluation against Differential and Linear Attacks for Feistel ciphers with SPN Round Function,” SAC2000, LNCS to appear.
[4] M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki, K. Ohta, “A Strategy for Constructing Fast Round Functions with Practical Security Against Differential and Linear Cryptanalysis,” SAC’98, LNCS 1556.
[5] NTT corporation, “E2: Efficient Encryption algorithm,” http://info.isl.ntt.co.jp/e2, (Summary version appears in IEICE Trans., Vol.E83-A, No.1, 2000)
[6] M. Matsui, “New Block Encryption Algorithm MISTY,” FSE’97, LNCS 1267.
[7] M. Matsui, T. Inoue, A. Yamagishi, H. Yoshida, “A note on calculation circuits over GF(2^{2n}),” Technical Report IT88-14, (in Japanese)
[8] M. Matsui, T. Tokita, “Cryptanalysis of a Reduced Version of the Block Cipher E2,” FSE’99, LNCS 1636.
[9] S. Moriai, M. Sugita, K. Aoki, M. Kanda, “Security of E2 against Truncated Differential Cryptanalysis,” SAC’99, LNCS 1758.

IEICE Trans.: IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science
FSE: Fast Software Encryption – Annual International Workshop
LNCS: Springer ― Lecture Notes in Computer Science series
SAC: Annual Workshop on Selected Areas in Cryptography