128ビットブロック暗号
CLEFIA

3/2-3/3 2010 応募暗号説明会

堅木　雅宣
ソニー株式会社

CLEFIA

はじめに

- CLEFIA
  - 国際会議FSE2007にて発表
  - 共通鍵ブロック暗号
    - ブロック長　128ビット
    - 鍵長128/192/256ビット
    - AESと同じインターフェース
  - 設計者
    - 白井，渋谷，秋下，盛合（ソニー），
    - 岩田（名古屋大）

目次

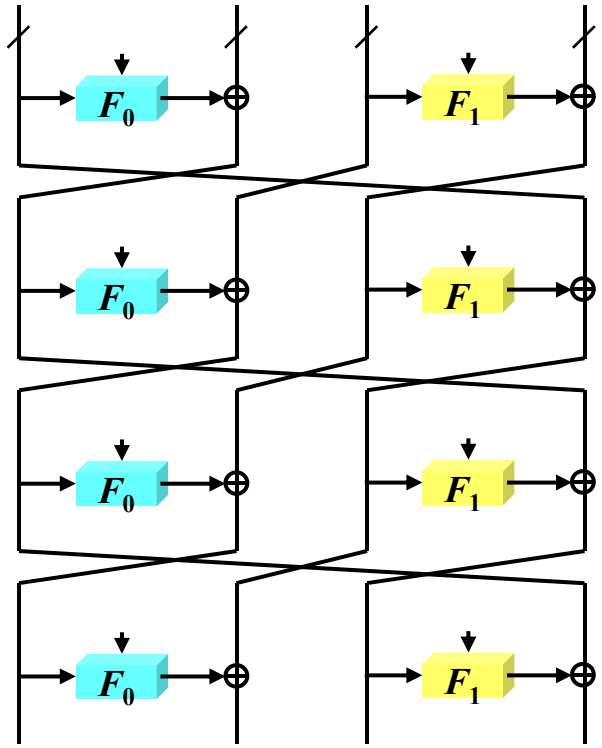
- 技術仕様
  - アルゴリズム概要
  - 設計方針
- 安全性評価
- 実装性能評価
- 公開状況等の情報
- まとめ

技術仕様

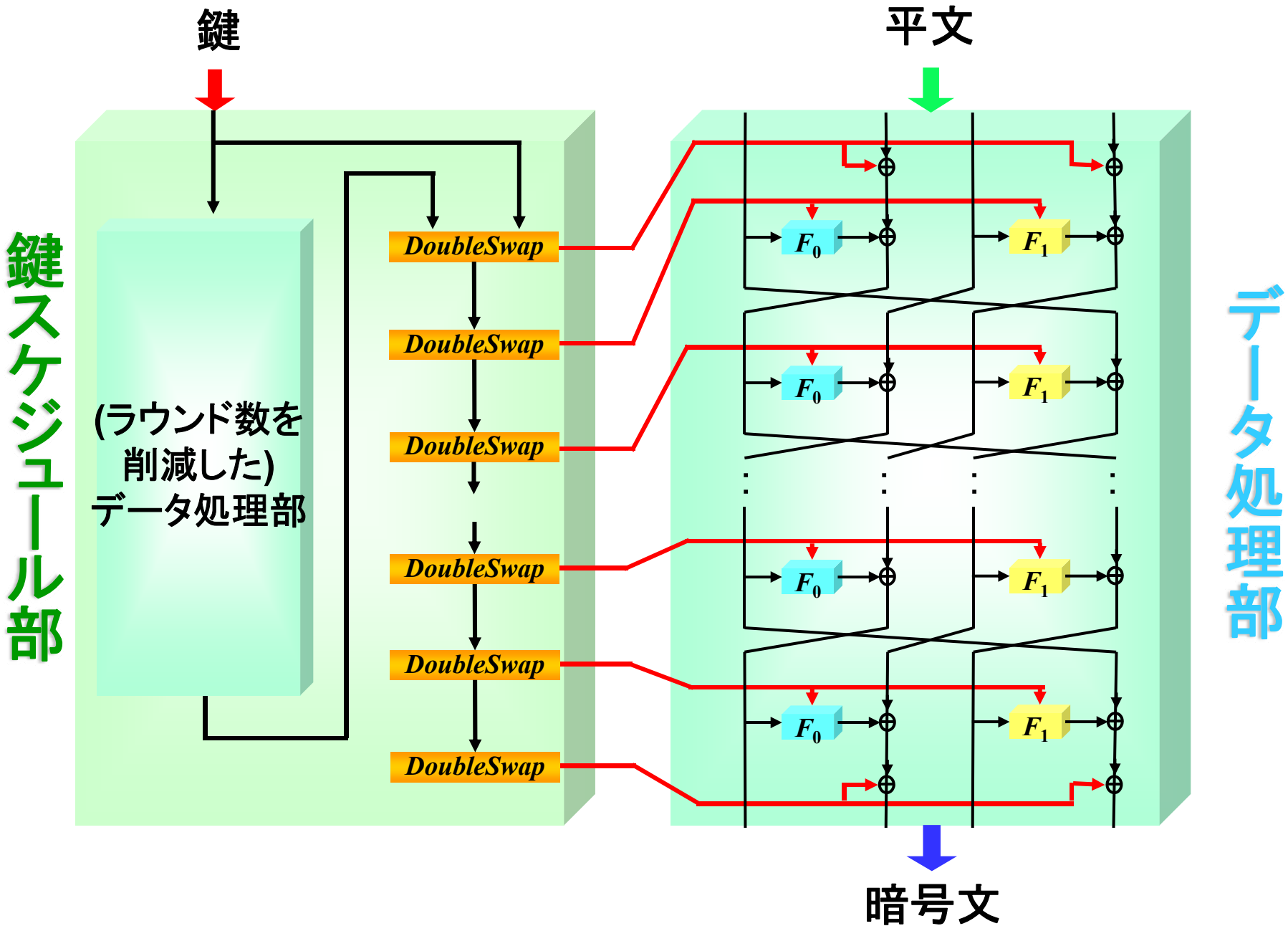
アルゴリズム概要

CLEFIAアルゴリズム概要

- 共通鍵ブロック暗号
  - ブロック長：128ビット
  - 鍵長：128/192/256ビット
- 基本構造
  - Type-2 一般化Feistel構造（GFN）
    - データ処理部，鍵スケジュール部ともに
  - ラウンド数：18 (128ビット鍵)
    22 (192ビット鍵)
    26 (256ビット鍵)

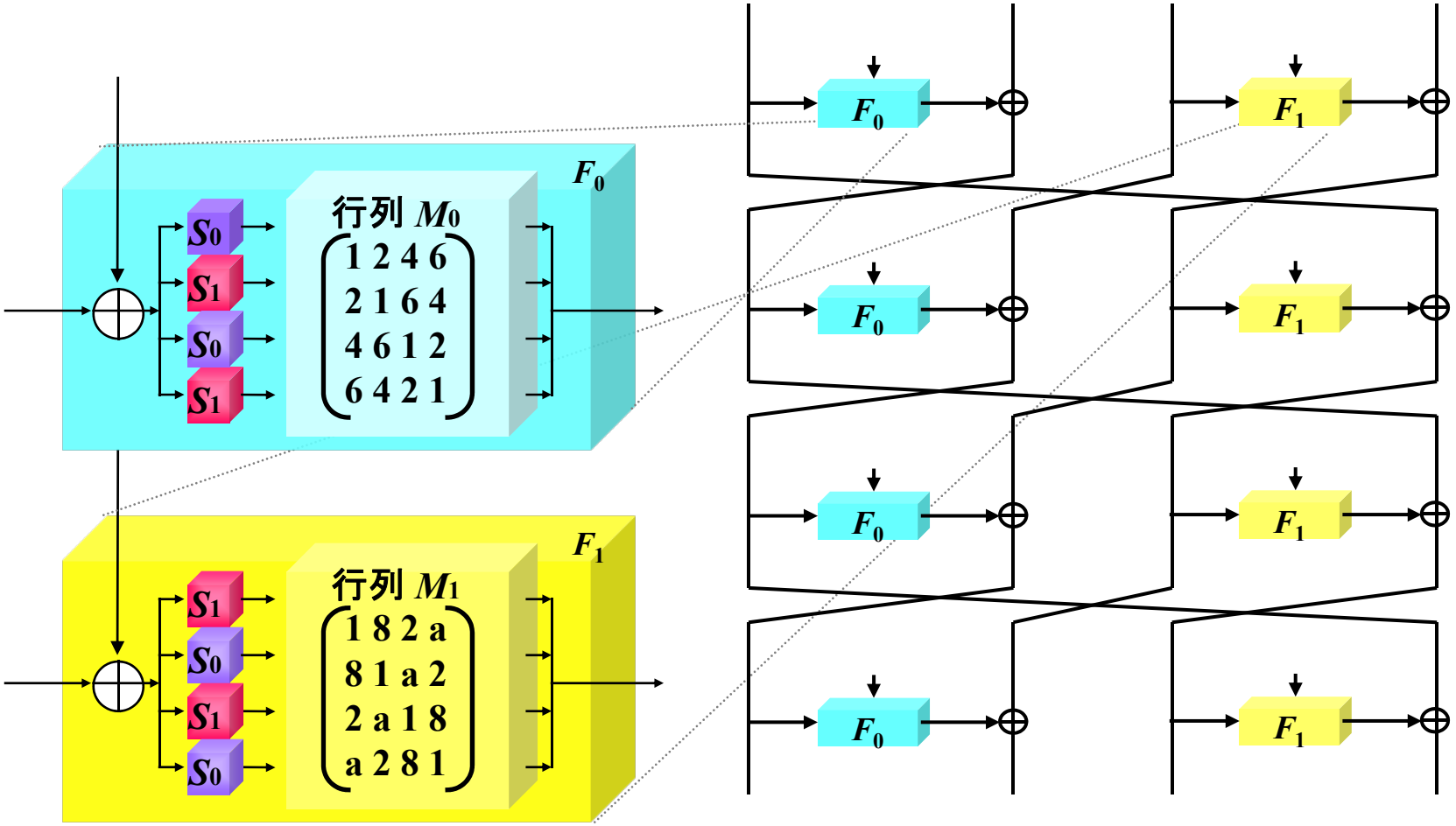


4系列Type-2一般化Feistel構造



F 関数

- Substitution-Permutation (SP)型



技術仕様

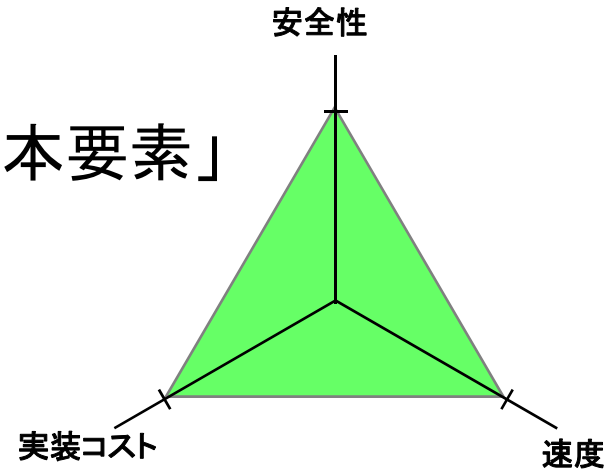
設計方針

設計方針(1/2)

- 背景
  - 現リスト選定以降の暗号解析技術の進歩
  - 実装制約の厳しい環境への実装ニーズ
- 動機

  128ビットブロック暗号の設計:

  最新の設計解析技術をもちいて,
  「実用的な暗号に求められる3つの基本要素」
  のバランスをさらに追究する

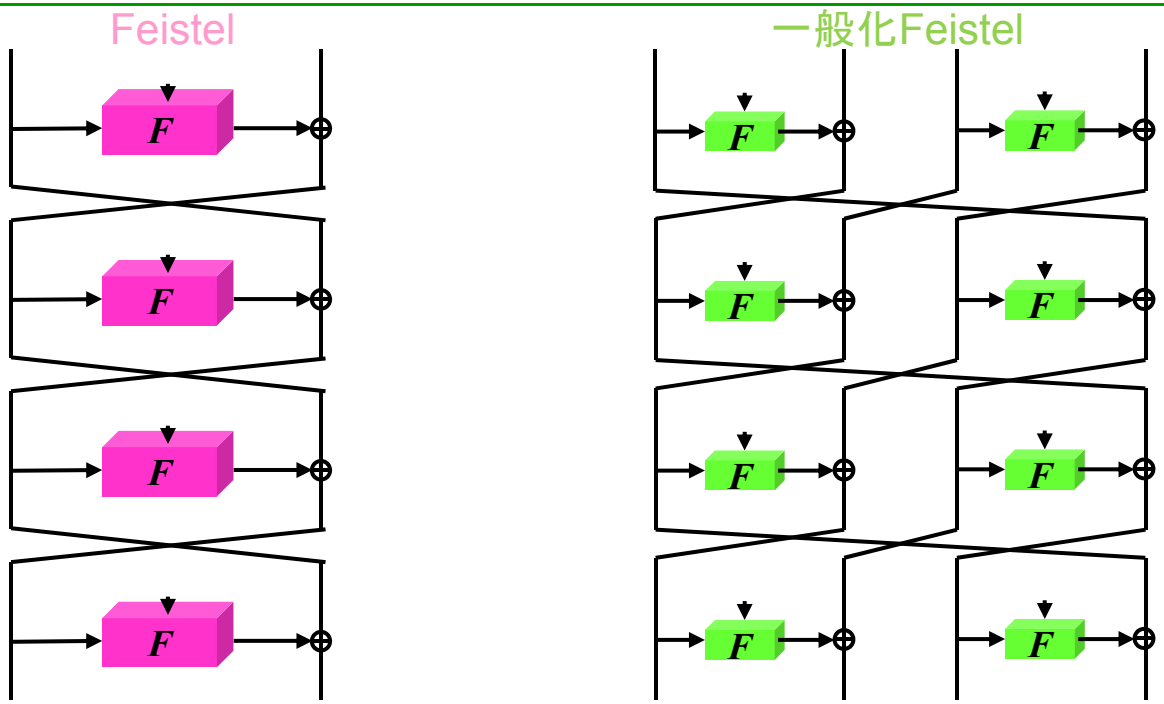


設計方針(2/2)

- 主な特長

1. 全体構造: 一般化Feistel構造
   - コンパクトなF関数の実現
2. F関数: 拡散行列切り替え法(DSM)
   - 差分・線形攻撃への耐性向上
3. 鍵スケジュール部:一般化Feistel構造
   - 関連鍵攻撃への耐性向上
4. 各コンポーネント:効率的な実装が可能
   - 安全性だけでなく実装性も十分考慮

1．全体構造：一般化Feistel構造の採用



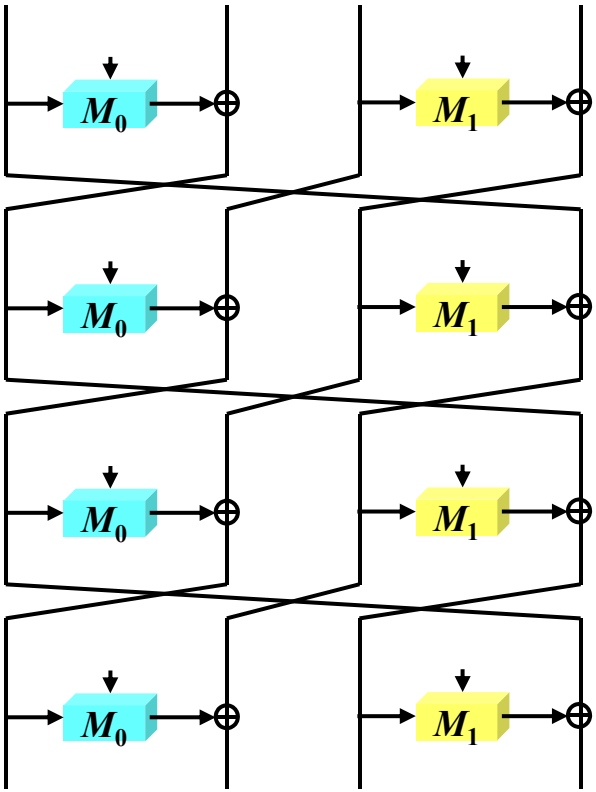
一般化Feistel構造の特徴

- F 関数のサイズが小さい
- 複数のF 関数が同時に実行できる
- 多くのラウンド数が必要

拡散行列切り替え法(DSM)により削減可能

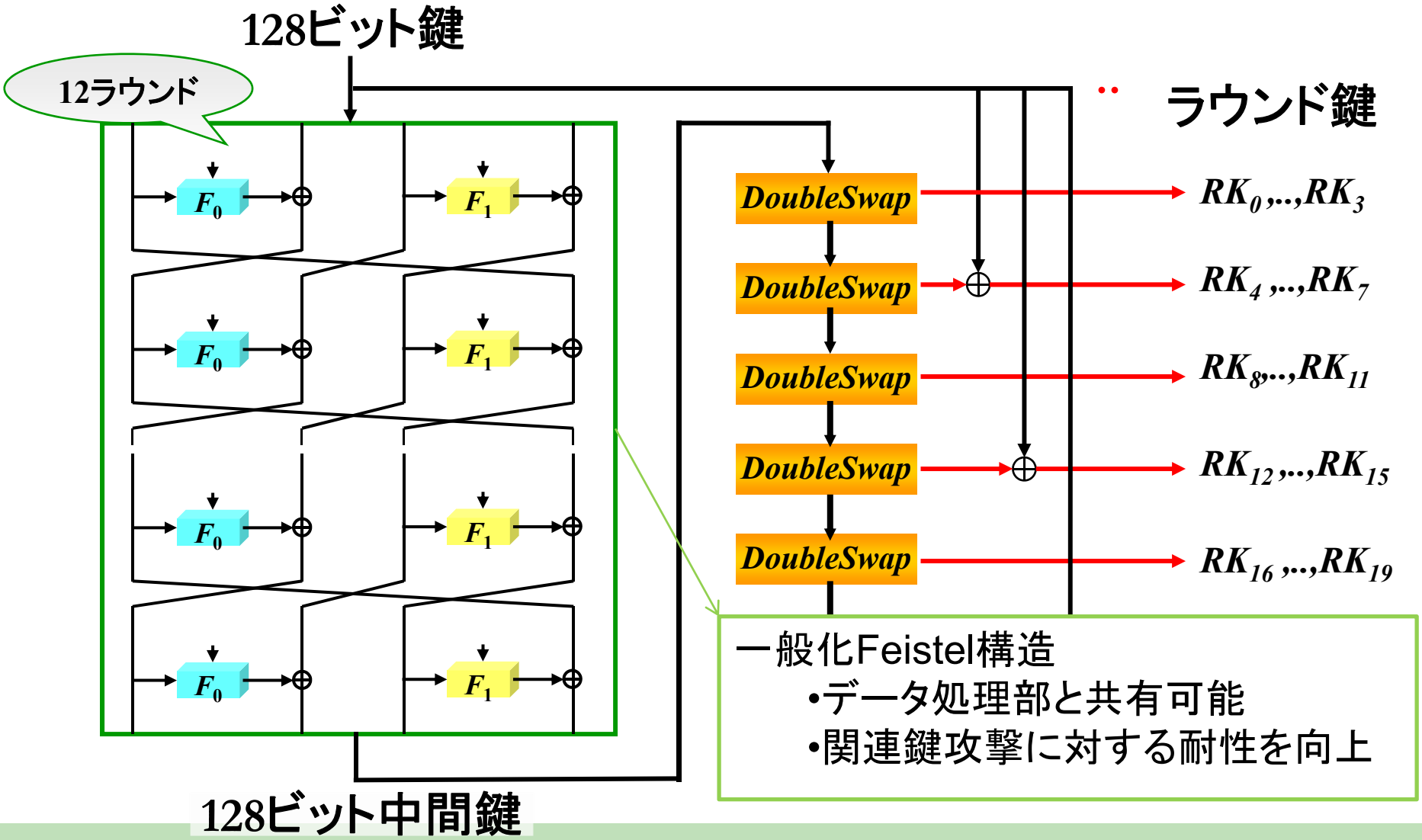
2. F関数：拡散行列切り替え法 (DSM)

- 拡散行列切り替え法の採用
  - DSM：Diffusion Switching Mechanism
  - Feistel typeの構造において,複数の拡散行列を組み合わせることにより差分/線形攻撃への耐性を高める手法
- 必要なラウンド数の削減に成功
  - CLEFIAの場合
    - DSMなし：16ラウンド
    - DSMあり：12ラウンド



M_0,M_1:拡散行列

3. 鍵スケジュール部 :一般化Feistel構造



一般化Feistel構造
- データ処理部と共有可能
- 関連鍵攻撃に対する耐性を向上

CLEFIA

4. 各コンポーネント

- 効率的な実装を考慮したコンポーネント

GFN	· 小さな F 関数 (32 ビット入出力) · F 関数の逆関数は不要
SP 型 F 関数	· 効率的なテーブル実装が可能 (ソフトウェア実装時)
DSM	· ラウンド数の削減が可能
S-box	· コンパクト実装に適した S_0, S_1 (特にハードウェア実装時)
行列	· 要素のハミングウェイトが小さい
鍵スケジュール部	· データ処理部と共有可能 · 128 ビット鍵の場合，必要なレジスタは 128 ビットレジスタ 1 つのみ · コンパクトな $DoubleSwap$ 関数

安全性評価

自己評価

既知の攻撃について網羅的に安全性評価を実施

- 差分攻撃
- 線形攻撃
- 差分線形攻撃
- Boomerang攻撃
- Amplified Boomerang攻撃
- Rectangle 攻撃
- Truncated 差分攻撃
- Truncated 線形攻撃
- 不能差分攻撃
- 飽和攻撃
- Gilbert-Minier Collision攻撃
- 高階差分攻撃
- 補間攻撃
- XSL/代数攻撃
- χ^2/Statistical攻撃
- スライド攻撃
- 関連暗号攻撃
- 関連鍵攻撃
- 関連鍵Boomerang攻撃
- 関連鍵Rectangle攻撃

外部評価

- 第三者評価（CLEFIA設計時）
  - 下記研究者に安全性評価を依頼．問題ないことを確認
    - Prof. Alex Biryukov
    - Prof. Vincent Rijmen
    - Prof. Serge Vaudenay
    - ABT(Prof. Lars R. Knudsen and Prof. Bart Preneel)

- 攻撃論文（CLEFIA発表後）
  - 不能差分攻撃（段数を減らしたCLEFIAに対して）
  - 現時点でフルラウンドCLEFIAに対する安全性上の懸念点は指摘されていない

実装性能評価

ソフトウェア実装性能

- 12.9cycles/byte, 1.48Gbpsを達成

実装法	鍵長 [bit]	暗号化 [cycles/byte]	復号 [cycles/byte]	鍵セットアップ (暗号化) [cycles]	鍵セットアップ (復号) [cycles]
単一ブロック	128	12.9	13.3	217	229
	192	15.8	16.2	272	293
	256	18.3	18.4	328	357
2 ブロック並列実装	128	11.1	11.1	217	229
	192	13.3	13.3	272	293
	256	15.6	15.6	328	357

* CPU:AMD Athlon 64 processor 4000+ (2.4GHz)
Windows XP 64-bit Edition上で動作. コードはアセンブラ実装.

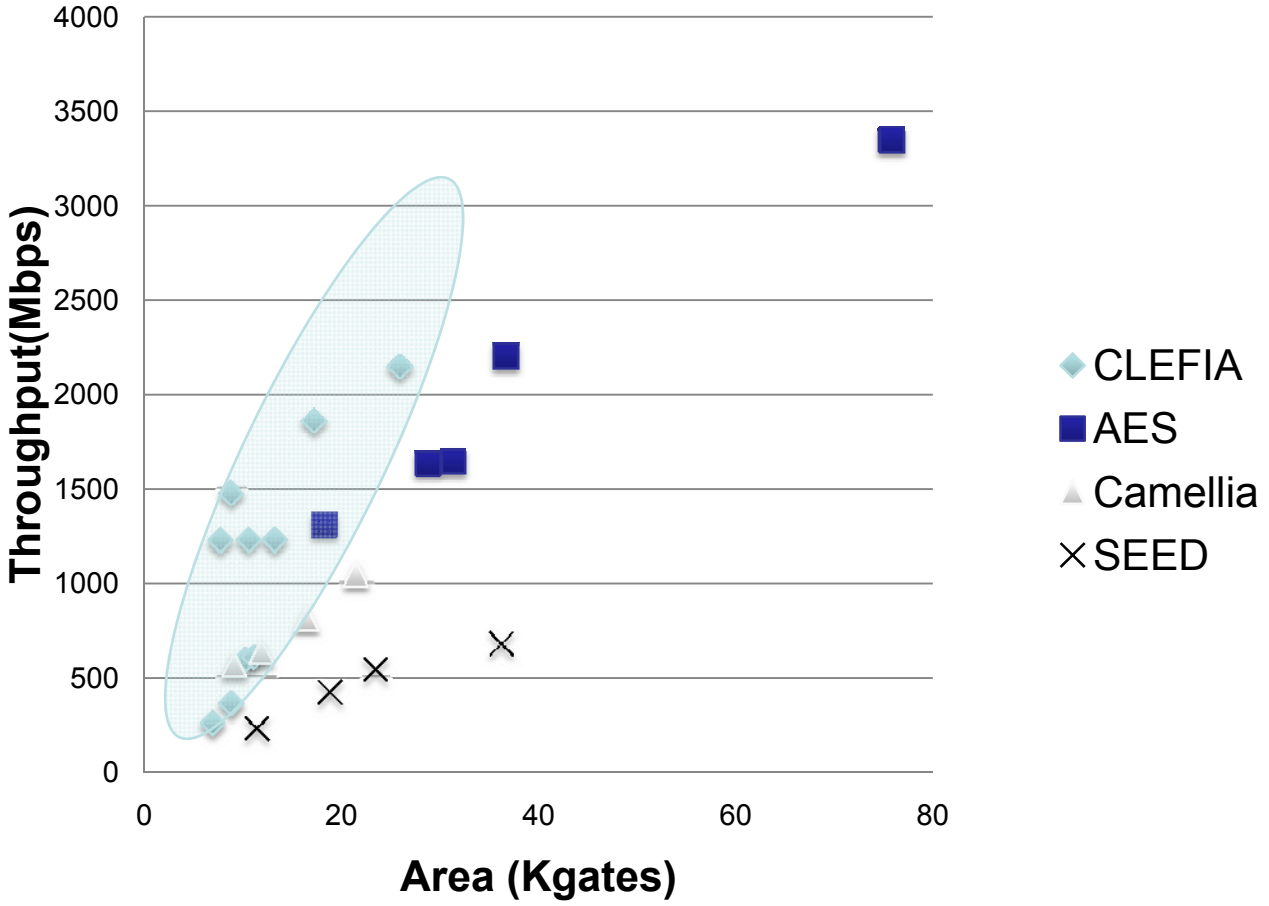
ハードウェア実装性能

- ASICで5Kgate以下で実装可能
- ゲート当たりの速度で高い性能

	鍵長 [bits]	暗復号 [cycles]	鍵セットアップ [cycles]	ゲート規模 [gates]	周波数 [MHz]	速度 [Mbps]	速度/ゲート規模 [Kbps/gate]
CLEFIA (0.09μm)	128	18	12	5,979	225.83	1,605.94	268.63
				12,009	422.29	3,003.00	250.06
		36	24	4,950	201.28	715.69	144.59
				9,377	389.55	1,385.10	147.71
	192	22	20	8,536	206.56	1,201.85	140.81
				15,718	391.08	2,275.39	144.76
	256	26	20	8,482	206.56	1,016.95	119.89
				15,542	391.08	1,925.33	123.88

ハードウェア実装性能（参考）

18033-3 128ビットブロック暗号とのハードウェア実装比較 (ASIC,180nm)

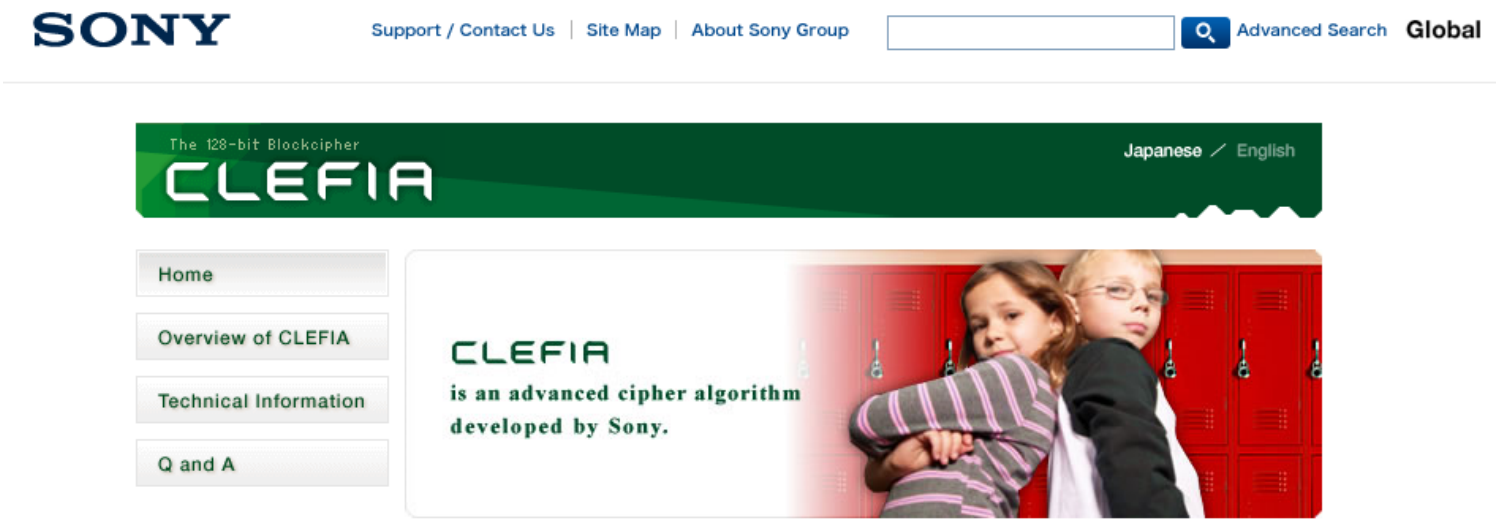


T. Sugawara, N. Homma, T. Aoki, and A. Satoh, “ASIC Implementations of the 128-bit Block Cipher CLEFIA." in Proceedings of Computer Security Symposium 2007 (CSS2007), pp. 175-180, 2007. (in Japanese)

公開状況等の情報

公開情報等(1/3)

- CLEFIA website
  - www.sony.co.jp/clefia
  - CLEFIAに関する技術情報(公開資料，関連論文リスト)等を公開



公開情報等(2/3)

- 国際会議
  - Fast Software Encryption 2007
    - T. Shirai, K. Shibutani, T. Akishita, S. Moriai, T. Iwata, “The 128-bit Blockcipher CLEFIA.” FSE 2007, LNCS 4593, pp. 181-195, Springer-Verlag, 2007.

- 標準化
  - ISO/IEC JTC 1/SC27　下記に提案中
    - ISO/IEC 29192 – Information technology –Security techniques – Lightweight cryptography – Part 2: Block ciphers
  - IETF Internet draftとして提出
    - M. Katagi, S. Moriai, “The 128-bit Blockcipher CLEFIA”, October19, 2009. http://tools.ietf.org/html/draft-katagi-clefia-00

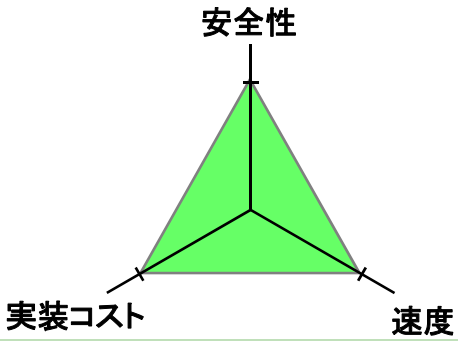
公開情報等(3/3)

- バージョン情報
  - CLEFIA のアルゴリズム仕様はこの暗号技術仕様書の記載で一意に定められ，他のバージョンは存在しない.
  - CLEFIA は，同一の名称，かつ同一の仕様で発表および応募を行っている.

- ライセンス条件
  - CLEFIA技術に必須な登録特許又は特許出願について，CLEFIA技術を実施する者(政府機関を含む)に対し，妥当かつ非差別的な条件で許諾します.

まとめ

- 128ビットブロック暗号CLEFIA
  - 安全性
    - 既存の攻撃法に対して十分な安全性を確認
  - 実装性能
    - 高速かつコンパクトな実装が可能
    - 特に，ハードウェア実装性能では既存暗号に対する優位性が十分期待できる.



CLEFIA