128ビットブロック暗号 CLEFIA

白井 太三† 渋谷 香士† 秋下 徹†
盛合 志帆† 岩田 哲††

† ソニー株式会社
†† 名古屋大学

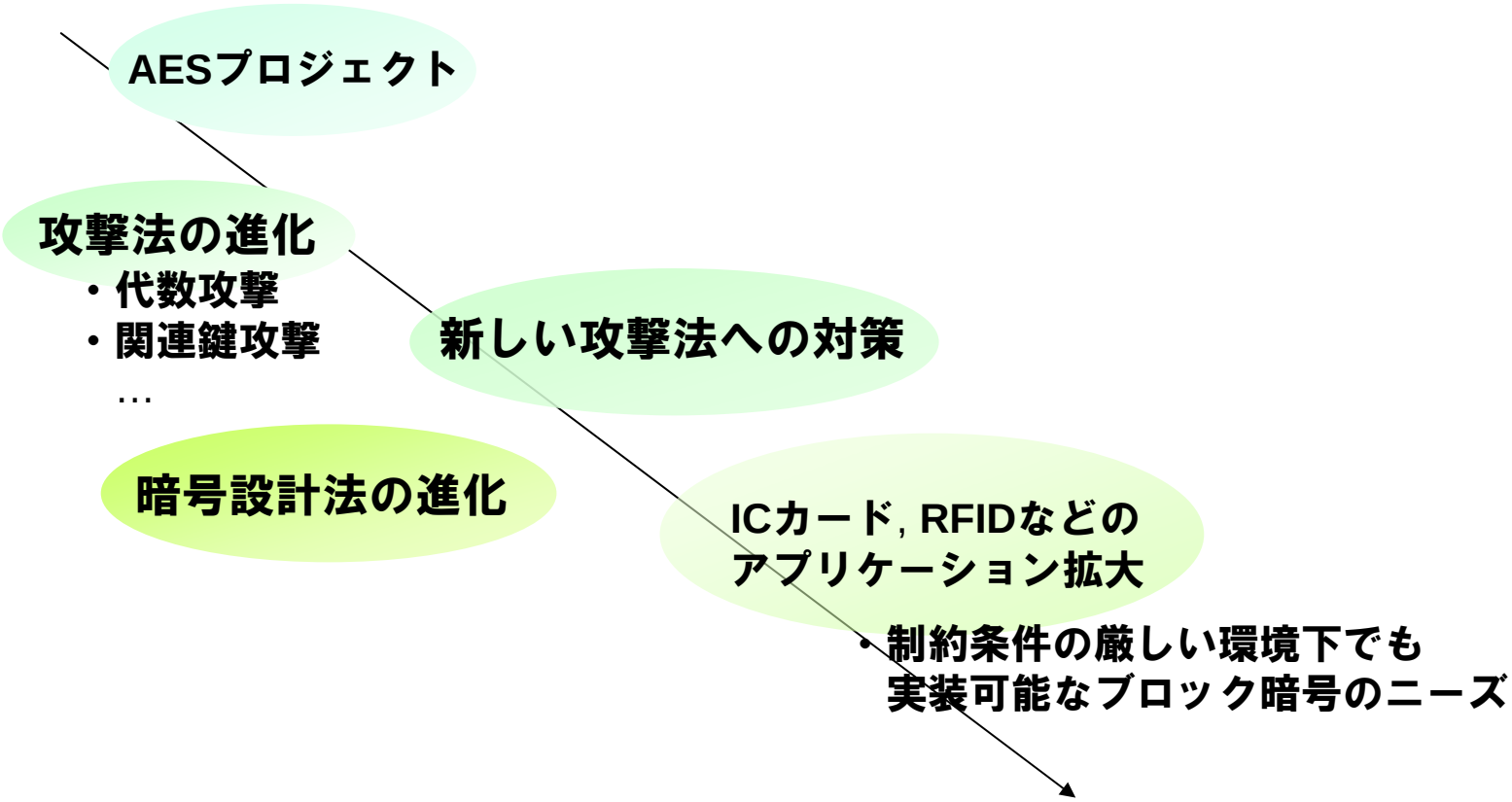
CLEFIA

目次

- 背景
- アルゴリズム仕様
- 設計方針
- 安全性評価
- 実装性能評価
- まとめ

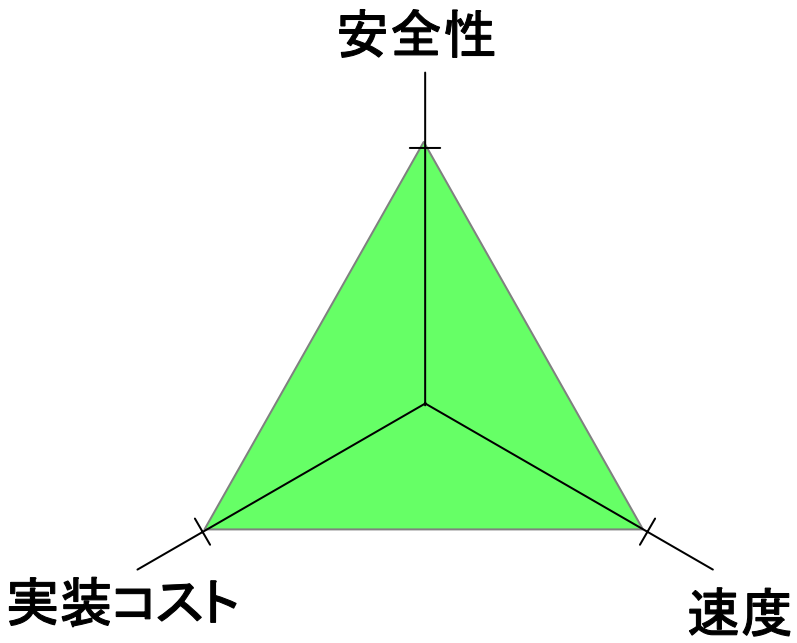
背景

- AESプロジェクト開始(1997～)から10年



設計の動機

- 最新の研究成果，設計手法により どこまで安全かつ小さく、高速な128ビットブロック暗号を設計できるか?

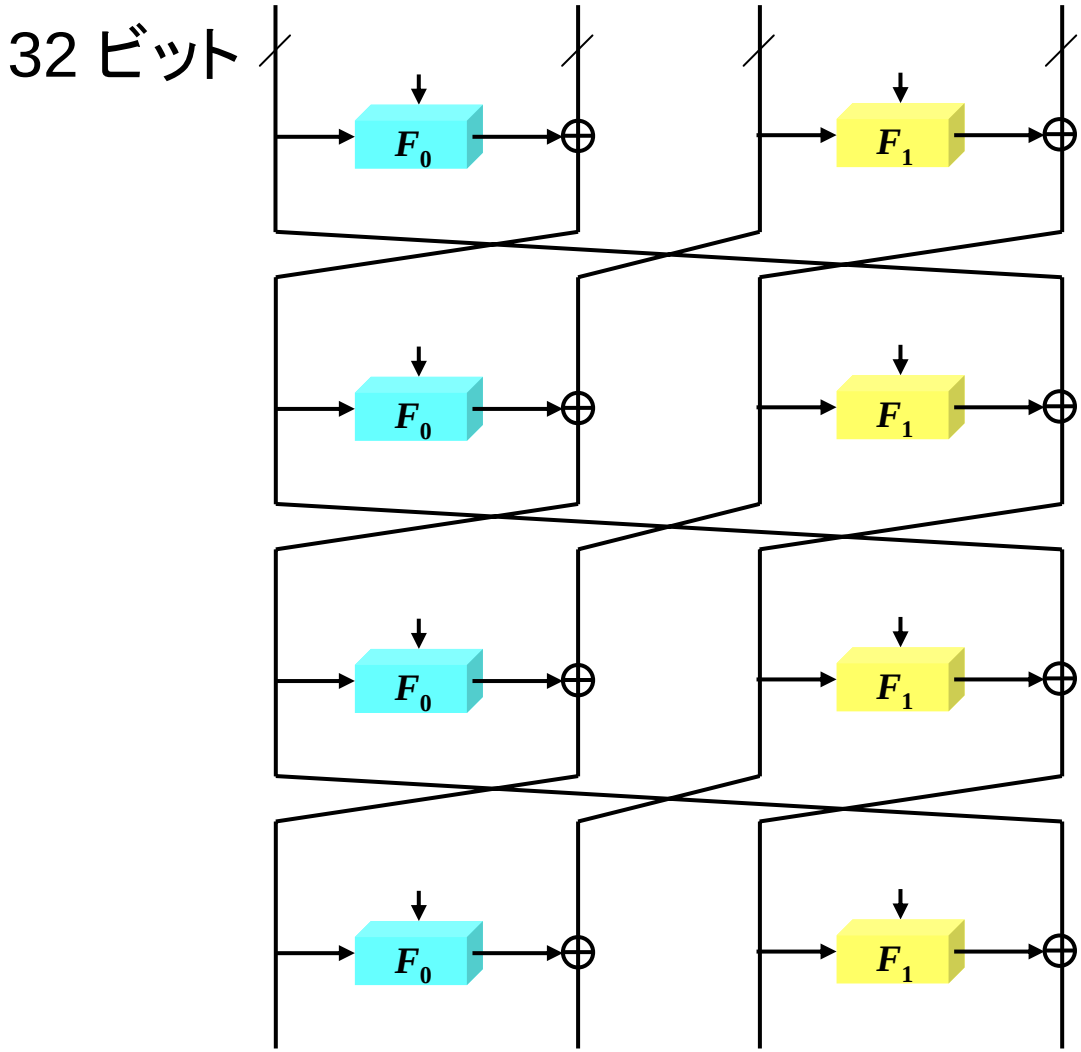


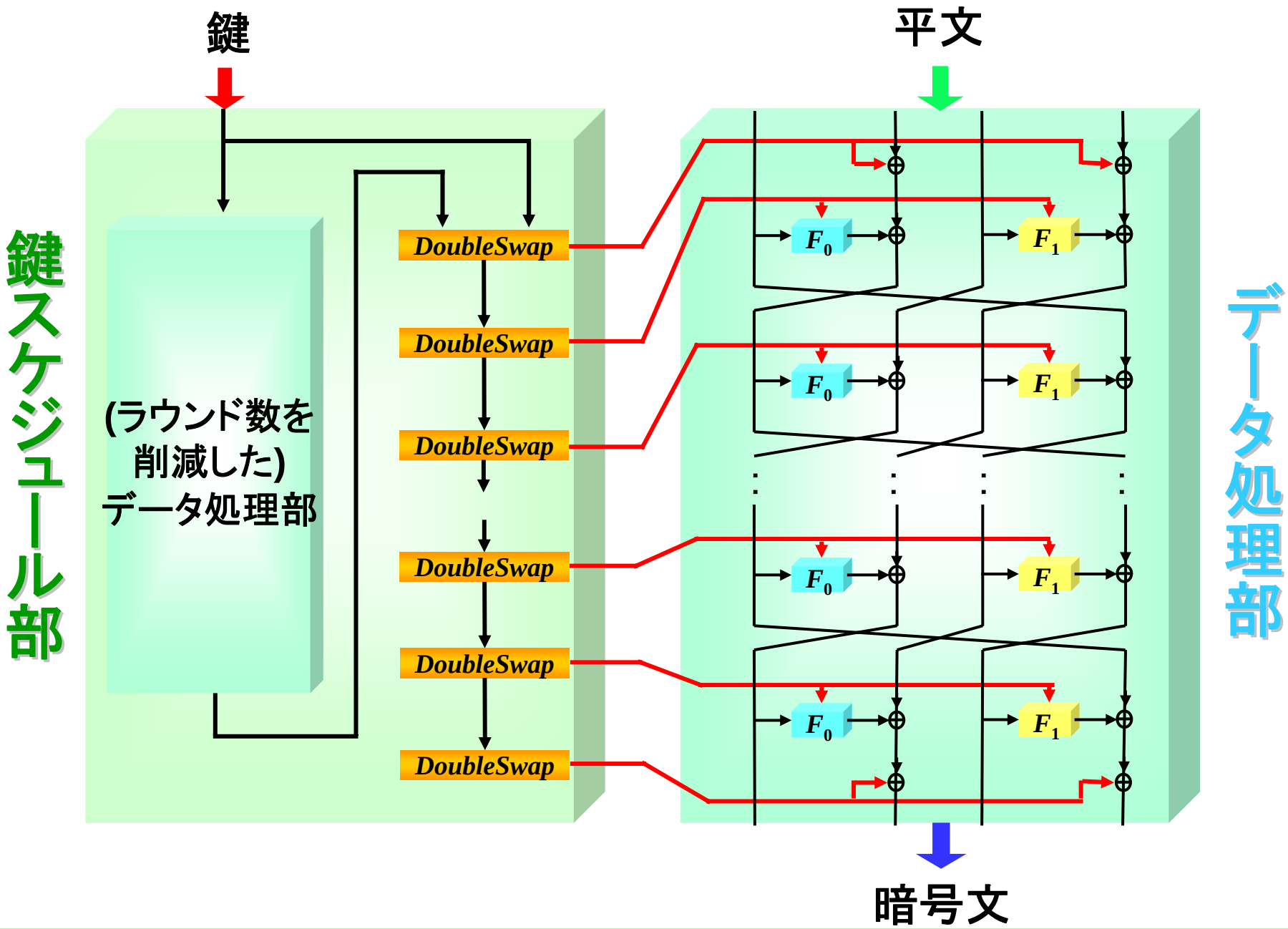
CLEFIAのアルゴリズム仕様

- 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)

Type-2 一般化Feistel構造

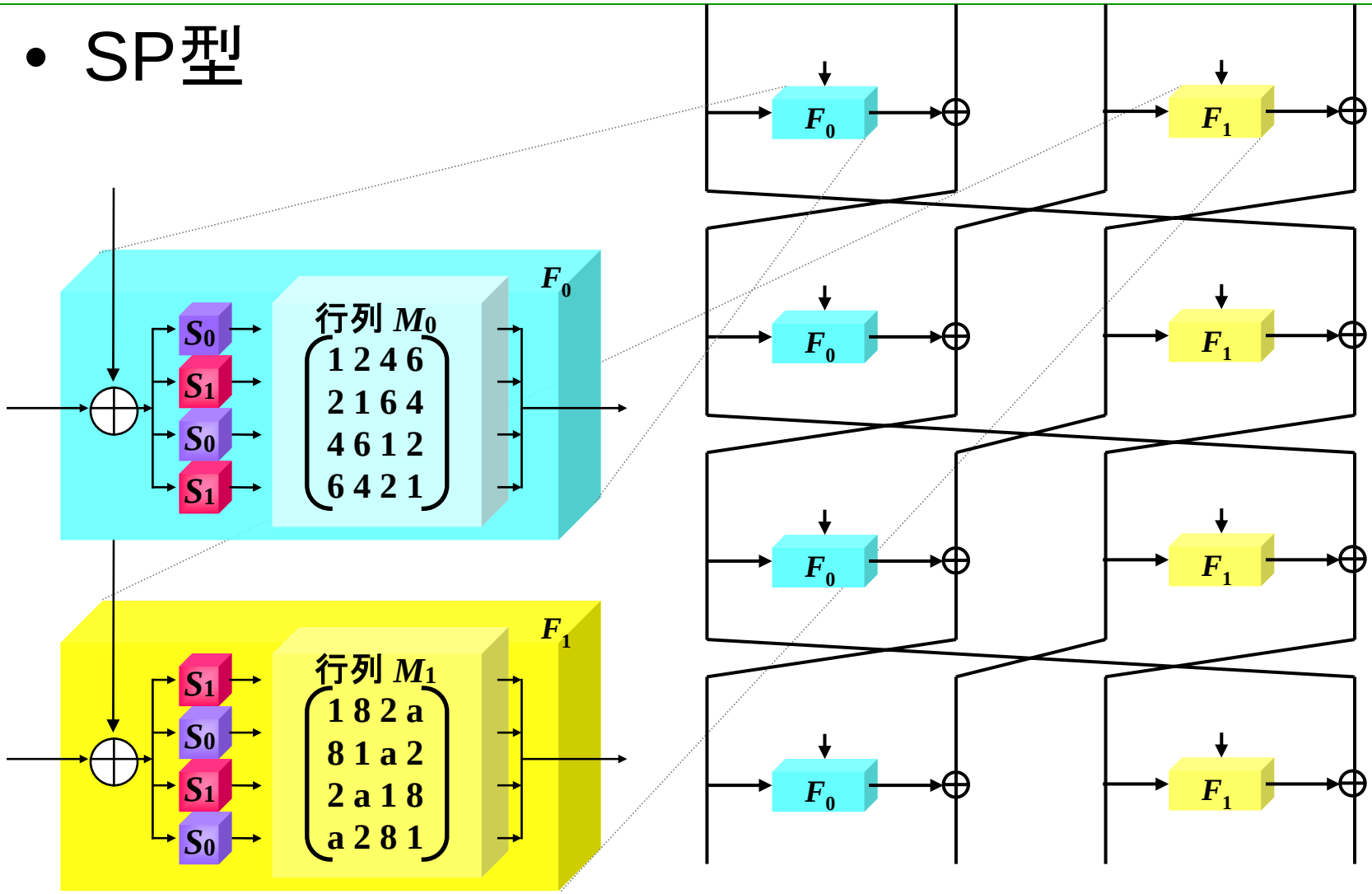
4系列





F 関数

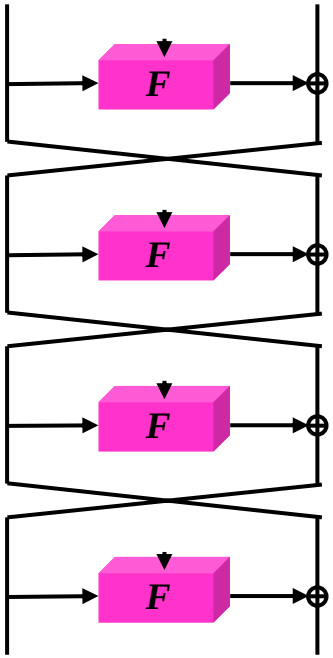
- SP型

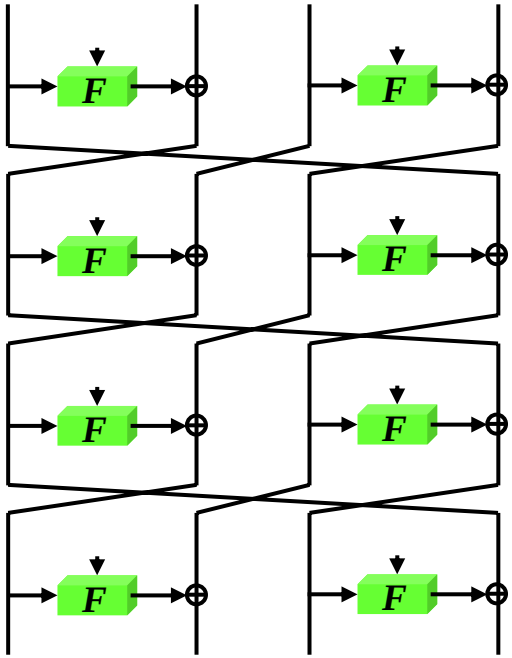


設計方針

- 全体構造
  - 一般化Feistel構造
- 拡散行列
  - DSM: Diffusion Switching Mechanism の利用
- S-box
  - 異なる代数構造に基づくコンパクトなS-box
- 鍵スケジュール部
  - 安全性とコンパクト実装が両立可能

Feistel vs. 一般化Feistel





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

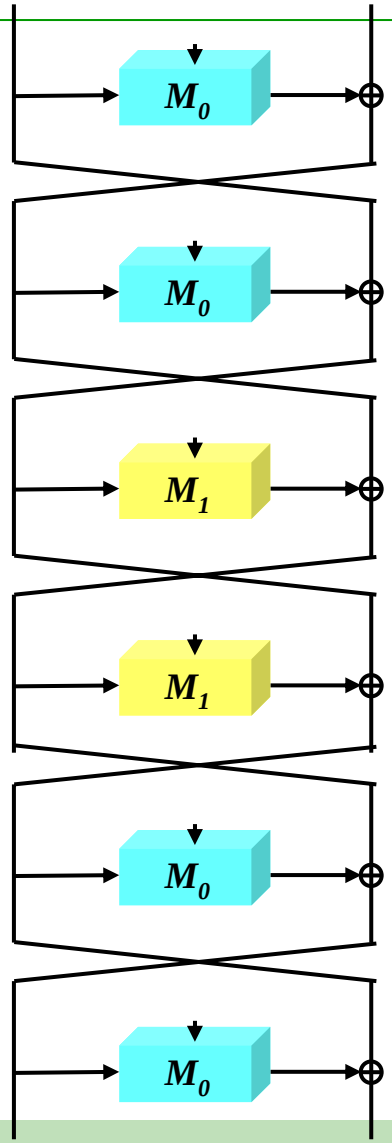
拡散行列切り替え法 (DSM)

- DSM：Diffusion Switching Mechanism [SS04,SP04,SS06]
- Feistel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

M_0: MDS行列, M_1: MDS行列 でかつ

$M_0 | M_1$: MDS行列となるように設計

*MDS: Maximum Distance Separable



DSMの効果

- 差分/線形攻撃に対する耐性の向上
  - 隣接するラウンド関数間の difference cancellation / linear mask cancellation を防止
  - 同じラウンド数の差分/線形特性に含まれるActive S-boxの最少個数が多くなることを保証できる
  - 必要な総ラウンド数を削減可能
    - CLEFIAのケースでは25%ラウンド数が削減

DSMの効果(最小active S-box数の比較)

従来技術

DSM適用時, D:差分, L:線形

ラウンド数

	$GFN_{4,r}$		
r	D & L w/o DSM	D DSM	L DSM
1	0	0	0
2	1	1	1
3	2	2	5
4	6	6	6
5	8	8	10
6	12	12	15
7	12	14	16
8	13	18	18
9	14	20	20
10	18	22	23
11	20	24	26
12	24	28	30
13	24	30	32

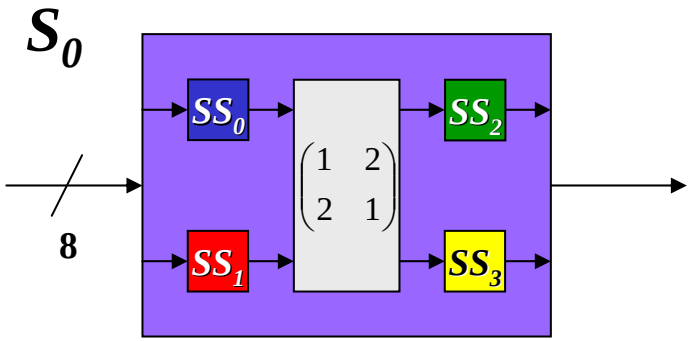
	$GFN_{4,r}$		
r	D & L w/o DSM	D DSM	L DSM
14	25	34	34
15	26	36	36
16	30	38	39
17	32	40	42
18	36	44	46
19	36	46	48
20	37	50	50
21	38	52	52
22	42	55	55
23	44	56	58
24	48	59	62
25	48	62	64
26	49	65	66

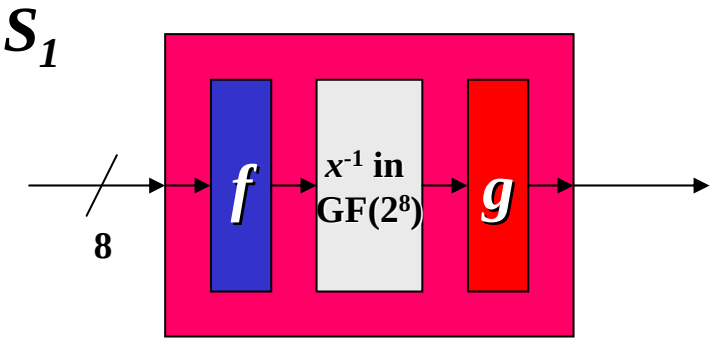
CLEFIAの場合、
28個以上active
s-boxが必要.

従来技術では最低
16ラウンド必要だった.

DSMを用いることで
12ラウンドで達成.

2種類のS-box





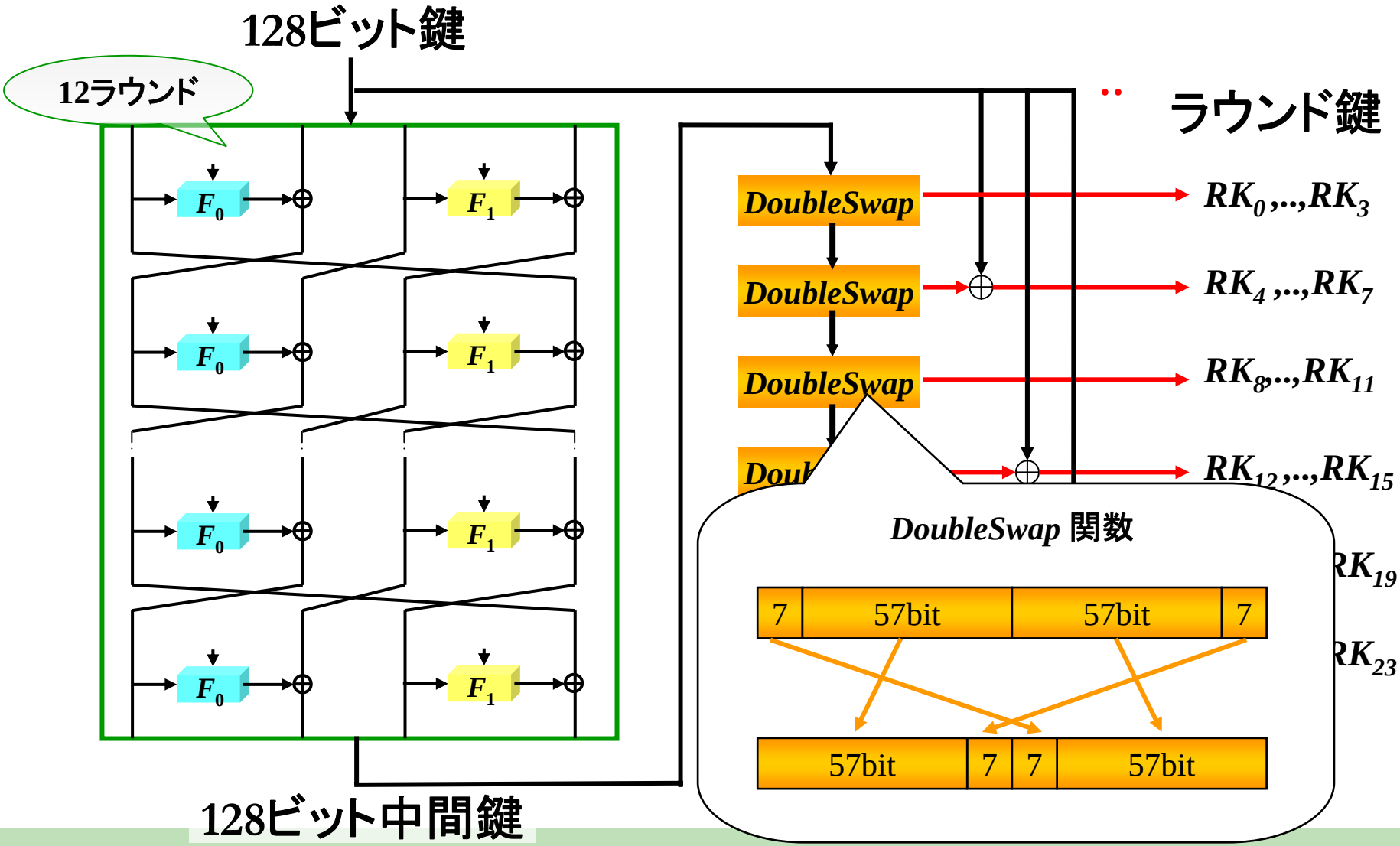
f, g: GF(2)上 affine 変換

・4ビットS-boxベース
使用例：Whirlpool, FOX

・GF(2^8)上逆元関数ベース
使用例：AES, Camellia

- 異なる代数構造
  - 代数攻撃系への耐性向上
- 2種類のS-boxの利用（配置も考慮）
  - 飽和攻撃(Saturation Attack)等への耐性向上

鍵スケジュール部 (128ビット鍵)



CLEFIA

鍵スケジュール部

- 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
- *DoubleSwap*関数
  - シンプルなビット置換演算ながら攪拌効果大
  - 暗号化時も復号時も同じ処理でラウンド鍵生成
  - 最終ラウンドから第1ラウンドへ”戻る”のも容易

安全性評価

- **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**

差分攻撃　線形攻撃

4ビットS-box
ベース

GF(2^8)上
逆元関数ベース

S-box	最大差分確率	最大線形確率
S_0	$2^{-4.678}$	$2^{-4.385}$
S_1	2^{-6}	2^{-6}

- 差分特性: 12ラウンド中に28個のactive S-box
  - 最大差分特性確率 $\leq 2^{-4.678 \times 28} = 2^{-130.984}$
- 線形特性: 12ラウンド中に30個のactive S-box
  - 最大線形特性確率 $\leq 2^{-4.385 \times 30} = 2^{-131.55}$
- 12ラウンドCLEFIA をランダム置換と識別するために有効な差分/線形特性は存在しない

DSMの効果(最小active S-box数の比較)

従来技術

DSM適用時, D:差分, L:線形

ラウンド数

	$GFN_{4,r}$		
r	D & L w/o DSM	D DSM	L DSM
1	0	0	0
2	1	1	1
3	2	2	5
4	6	6	6
5	8	8	10
6	12	12	15
7	12	14	16
8	13	18	18
9	14	20	20
10	18	22	23
11	20	24	26
12	24	28	30
13	24	30	32

	$GFN_{4,r}$		
r	D & L w/o DSM	D DSM	L DSM
14	25	34	34
15	26	36	36
16	30	38	39
17	32	40	42
18	36	44	46
19	36	46	48
20	37	50	50
21	38	52	52
22	42	55	55
23	44	56	58
24	48	59	62
25	48	62	64
26	49	65	66

⇐ **128-bit key**

⇐ **192-bit key**

⇐ **256-bit key**

不能差分攻撃

- 現在、CLEFIA に対して最も有効な攻撃
- Kimらによる探索アルゴリズムを用いて
  2つの9ラウンド不能差分パスを発見

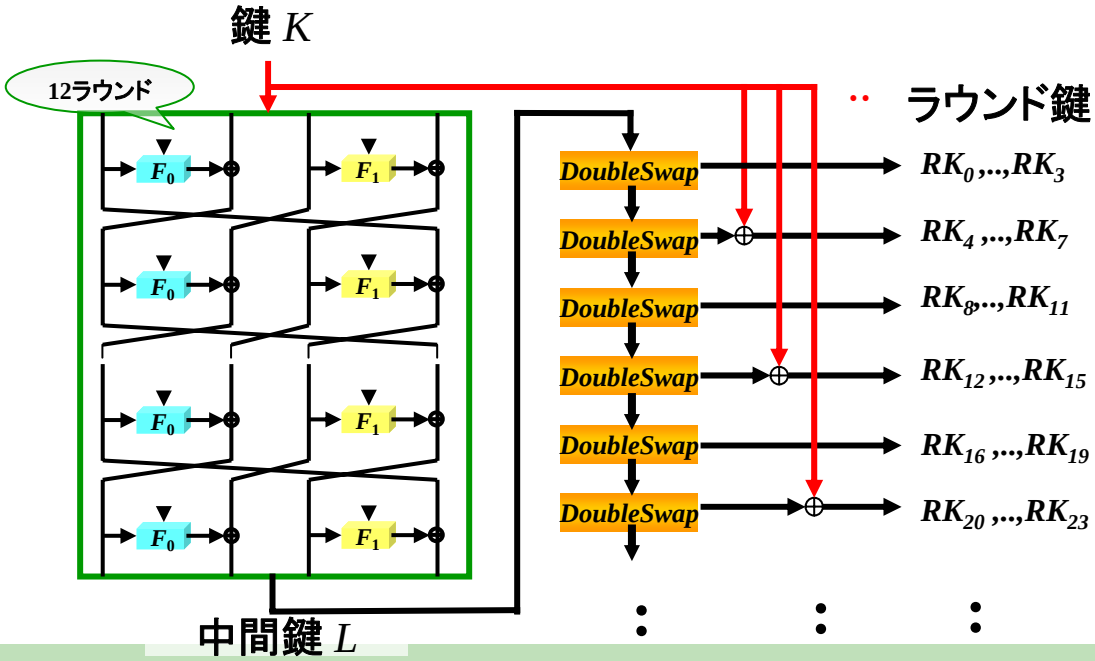
$(0, \alpha, 0, 0) \overset{9r}{\nrightarrow} (0, \alpha, 0, 0)$ と $(0, 0, 0, \alpha) \overset{9r}{\nrightarrow} (0, 0, 0, \alpha)$

但し $\alpha \in \{0, 1\}^{32}$ はあらゆる非ゼロの差分値

ラウンド数	鍵長	ホワイトニング鍵	選択平文数	計算量
10	128, 192, 256	あり	$2^{101.7}$	2^{102}
11	192, 256	あり	$2^{103.5}$	2^{188}
12	256	なし	$2^{103.8}$	2^{252}

各種関連鍵攻撃

- 鍵スケジュール部を強固にすることで防御
  - Step.1 一般化Feistel構造により中間鍵 L を生成
  - Step.2 中間鍵を*DoubleSwap*関数で攪拌させながら
    もとの鍵 K とラウンド定数をマスクしてラウンド鍵を生成



各種関連鍵攻撃

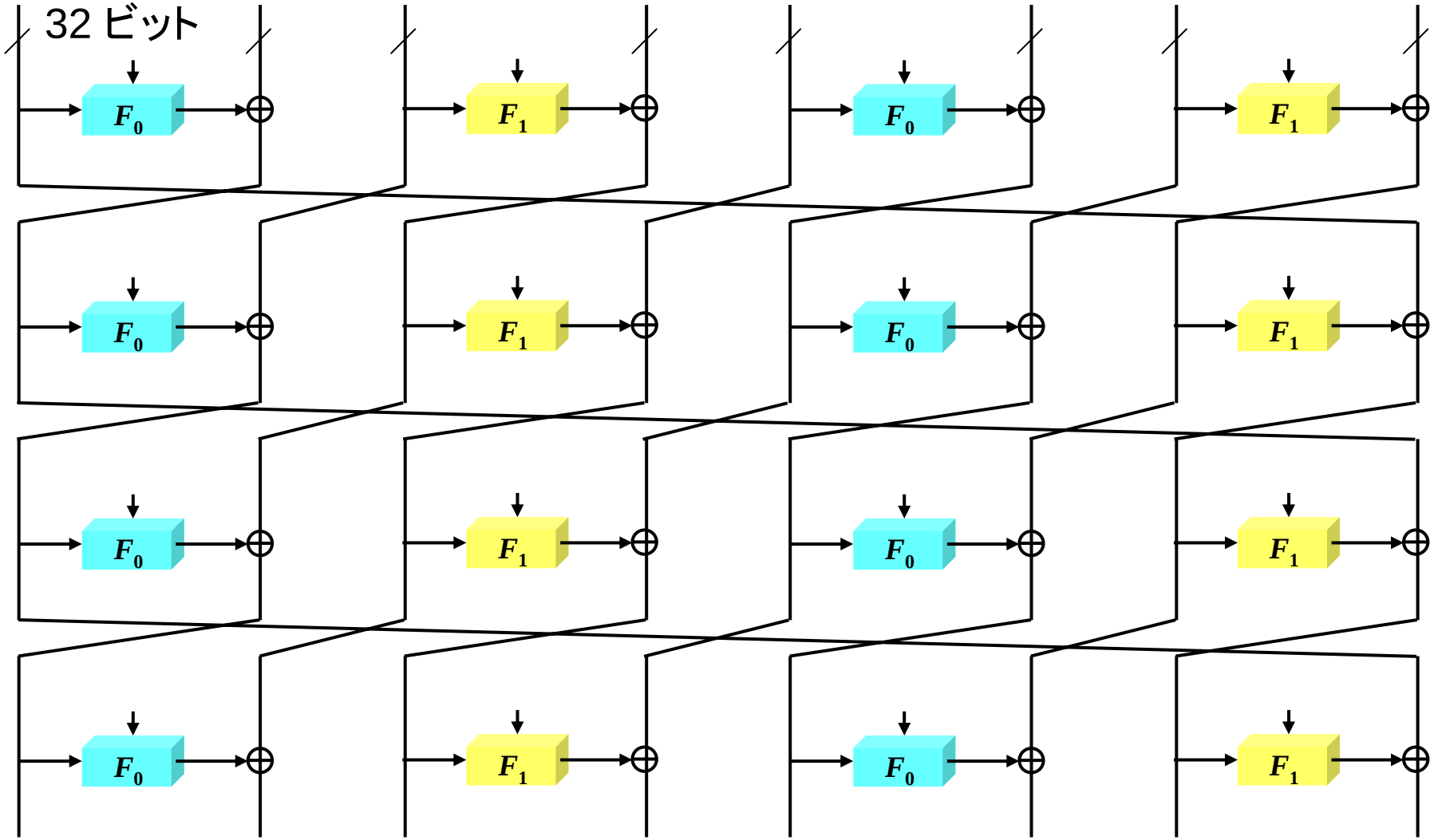
- 一般化Feistel構造 (GFN)
  - 128ビット鍵: 12ラウンド4系列GFN
  - 192/256ビット鍵: 10ラウンド8系列GFN

あらゆるΔKからΔLへの遷移確率が十分小さくなるようにラウンド数を決定

- ラウンド定数
  - 鍵長によって異なるラウンド定数のセットを用いることで、スライド攻撃や関連暗号攻撃を防御

Type-2 一般化Feistel構造

8系列



ハードウェア実装性能

- ASICで5Kgate以下で実装可能*
- 面積当たり速度でAESを上回る最高性能**

	鍵長 (bits)	暗/復号 (cycles)	鍵セットアップ (cycles)	最適化オプション	面積 (gates)	クロック周波数 (MHz)	速度 (Mbps)	速度/面積 (Kbps/gate)
CLEFIA (0.09 μm)	128	18	12	面積優先	5,979	225.83	1,605.94	268.63
				速度優先	12,009	422.29	3,003.00	250.06
		36	24	面積優先	4,950	201.28	715.69	144.59
				速度優先	9,377	389.55	1,385.10	147.71
	192	22	20	面積優先	8,536	206.56	1,201.85	140.81
	256	26	20	面積優先	8,482	206.56	1,016.95	119.89
AES [21] (0.13 μm)	128	11	N/A	面積優先	12,454	145.35	1,691.35	135.81
		54	N/A	面積優先	5,398	131.24	311.09	57.63

* 0.09μmCMOS標準セルライブラリ使用

** 使用ASICライブラリの差(0.09μm, 0.13μm)を考慮した公平な比較のためにCLEFIAの性能を1.5で割っても.

高速・コンパクトH/W実装への寄与点

- 一般化Feistel構造
  - 小さな F 関数
  - 逆関数が不要
- DSMによりラウンド数を削減
- データ処理部と鍵スケジュールが共有可能
- 各パーツが非常にコンパクト
  - 拡散行列(遅延も小さい)
  - S-box
  - *DoubleSwap*関数

ソフトウェア実装性能

- Athlon64上で12.9cycles/byte, 1.48Gbpsを達成

	実装タイプ	鍵長 (bits)	暗号化関数 (cycles/byte)	復号関数 (cycles/byte)	鍵セットアップ (cycles)	テーブルサイズ (KB)
CLEFIA	1 ブロック	128	12.9	13.3	217	8
		192	15.8	16.2	272	
		256	18.3	18.4	328	
	2 ブロック並列	128	11.1	11.1	217	16
		192	13.3	13.3	272	
		256	15.6	15.6	328	
AES [18]	1 ブロック	128	10.6	N/A	N/A	8

* AMD Athlon 64プロセッサ 4000+ (2.4GHz)を使用し,
Windows XP 64-bit Edition上で動作. コードはアセンブラ実装.

ソフトウェア実装性能

- S-box参照回数はAESより少ないものの，データ依存性が高い．
  - AES: 160回, CLEFIA: 144回
- 2ブロック並列実装では依存性は低減．

	実装タイプ	鍵長 (bits)	暗号化関数 (cycles/byte)	復号関数 (cycles/byte)	鍵セットアップ (cycles)	テーブルサイズ (KB)
CLEFIA	1 ブロック	128	12.9	13.3	217	8
		192	15.8	16.2	272	
		256	18.3	18.4	328	
	2 ブロック並列	128	11.1	11.1	217	16
		192	13.3	13.3	272	
		256	15.6	15.6	328	
AES [18]	1 ブロック	128	10.6	N/A	N/A	8

* AMD Athlon 64プロセッサ 4000+ (2.4GHz)を使用し，
Windows XP 64-bit Edition上で動作. コードはアセンブラ実装.

まとめ

- 128ビットブロック暗号 CLEFIA を提案
- 高速かつコンパクトな実装が可能
  - ハードウェア実装：単位ゲートあたりの速度において最高記録を達成
  - ソフトウェア実装：128ビットブロック暗号において最も高速なグループ
- 既知の暗号解読法に対する安全性を確認