128ビットブロック暗号 CLEFIA のハードウェア実装評価

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

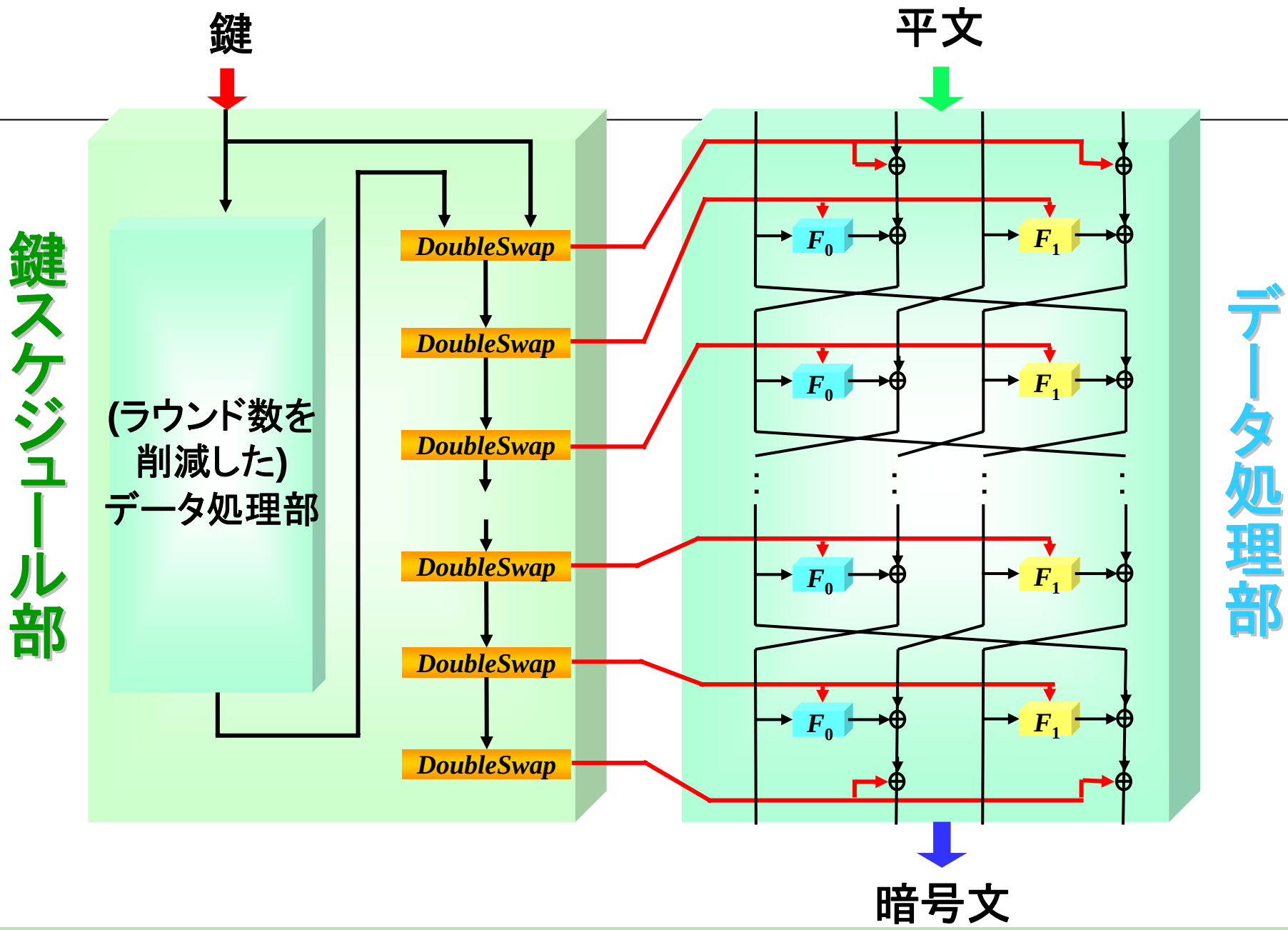
CLEFIA

目次

- 128 ビットブロック暗号 CLEFIA
- *F* 関数の最適化
  - S-box
  - 拡散行列
- 鍵スケジュール部の最適化
  - *DoubleSwap* 関数
  - 部分鍵の等価変形
- 実装性能評価
- まとめ

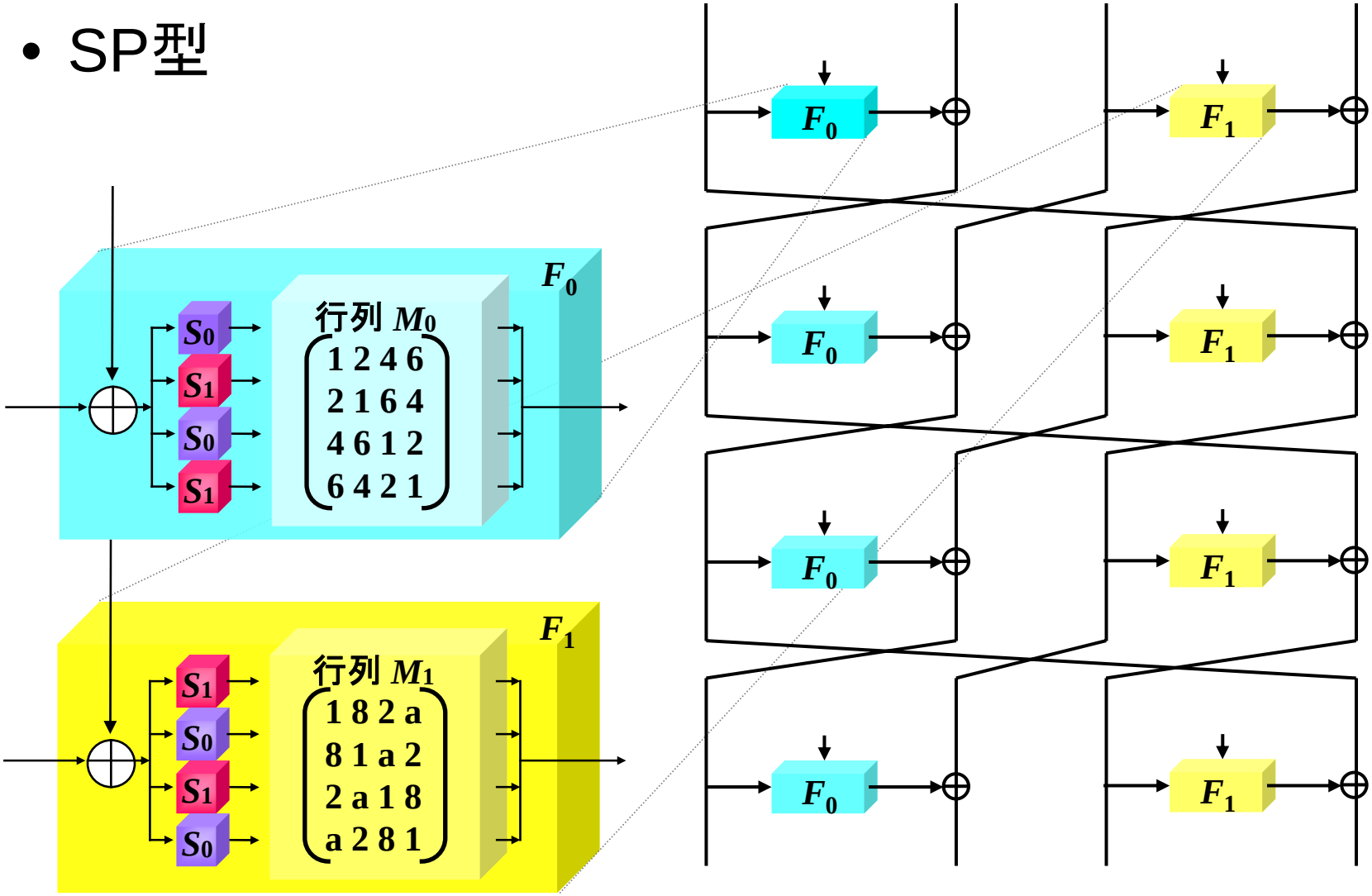
128 ビットブロック暗号 CLEFIA

- 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)

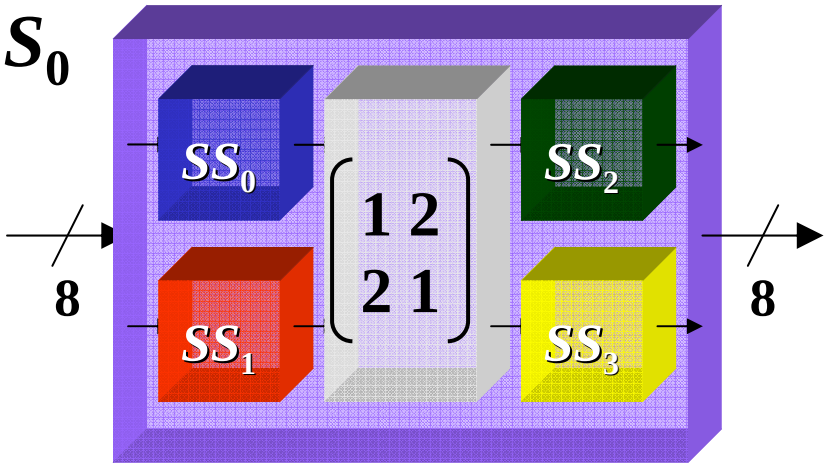


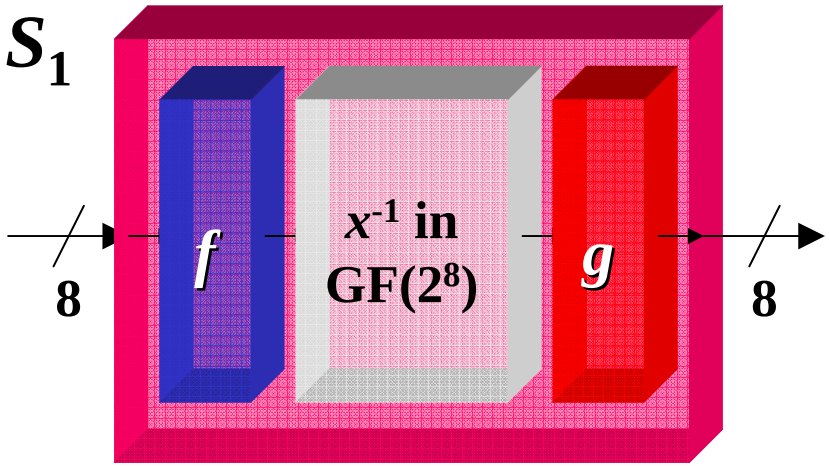
F 関数

- SP型



S-box





f, g: GF(2)上 affine 変換

CLEFIA の特長

- 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

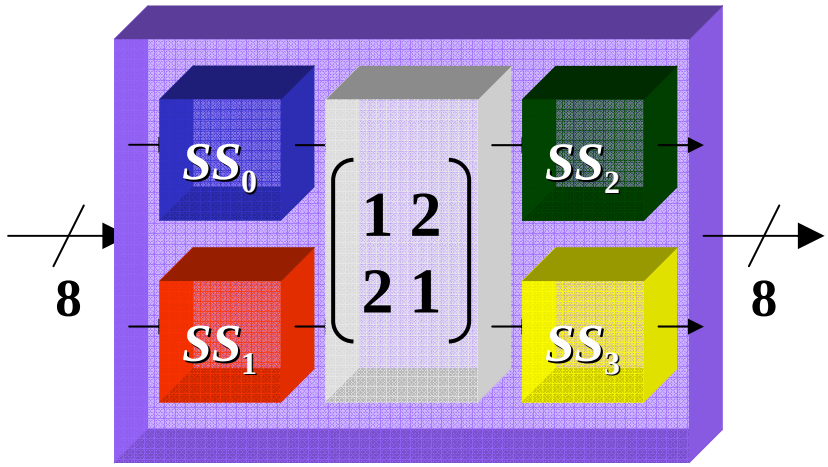
実装環境

記述言語	Verilog-VHDL
シミュレータ	VCS ver.2005.06
論理合成ツール	Design Compiler ver.2006.06
設計ライブラリ	0.09um CMOS 標準セルライブラリ
	1 gate = 2-way NAND, 最悪条件

F 関数の最適化

- 各コンポーネントの最適化
  - S-box S_0, S_1
  - 拡散行列 M_0, M_1

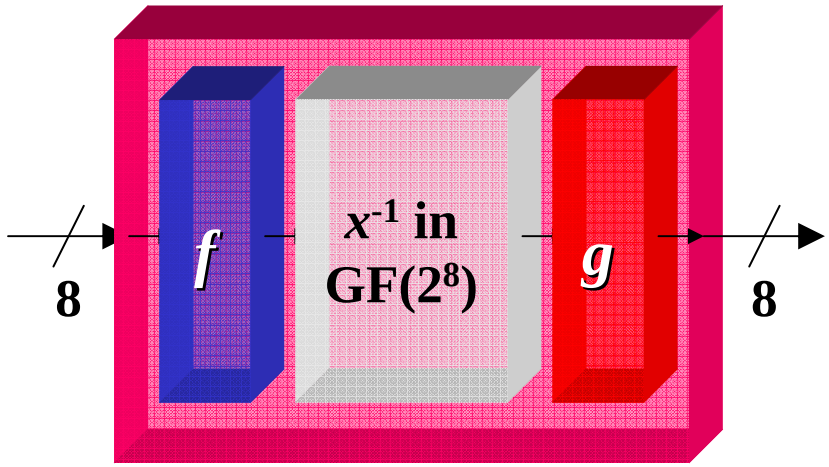
S-box S_0



4bit入出力 S-box SS_0, SS_1, SS_2, SS_3 ⇒ 自動合成
GF(2^4)上の行列演算 ⇒ 10 XOR

144.75 gate, 1.33 ns

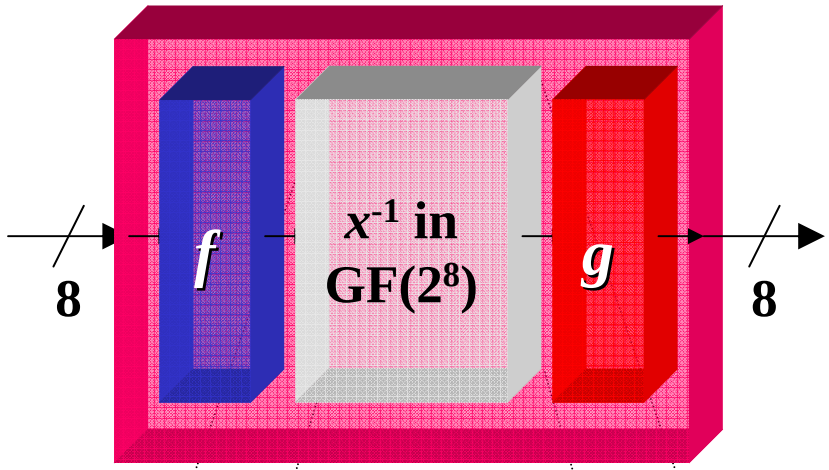
S-box S_1



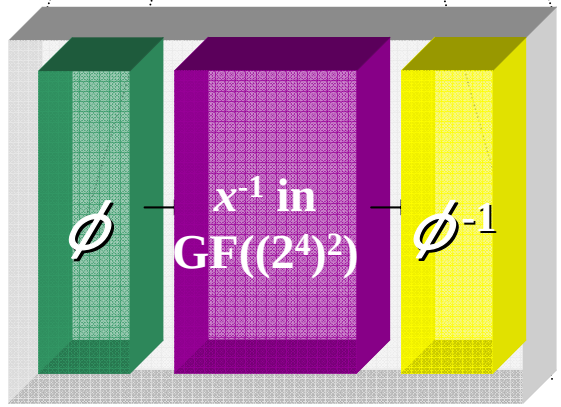
$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 0&0&0&1&1&0&0&0 \\ 0&1&0&1&0&0&0&1 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&1&1&0 \\ 0&1&1&0&0&1&0&1 \\ 0&1&0&1&1&1&0&0 \\ 0&1&1&0&0&0&0&0 \\ 1&0&0&0&0&0&0&1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 0&0&0&0&1&0&1&0 \\ 0&1&0&0&0&0&0&1 \\ 0&1&0&1&1&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&1&1&0&0&0&0 \\ 0&0&0&0&0&0&1&0 \\ 1&0&0&1&0&0&0&0 \\ 0&1&0&0&0&1&0&0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

S-box S_1



$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 0\,0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,1\,1\,0\,1\,0 \\ 0\,1\,1\,0\,0\,1\,0\,0 \\ 1\,1\,1\,1\,0\,1\,0\,0 \\ 1\,0\,1\,0\,1\,1\,0\,0 \\ 1\,0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,0\,0\,1\,0\,1\,0 \\ 1\,1\,1\,0\,1\,1\,1\,1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix}$$

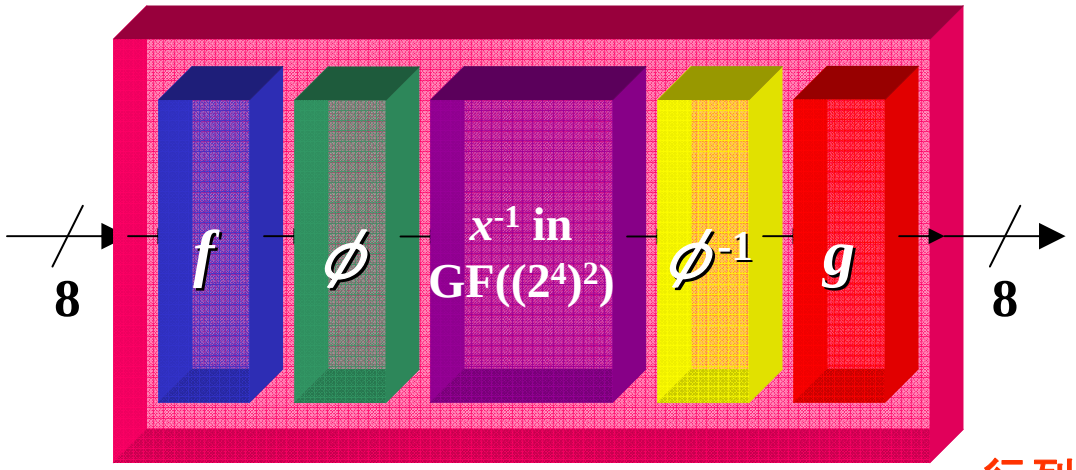


$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 1\,1\,1\,1\,0\,0\,1\,0 \\ 1\,1\,0\,1\,0\,1\,0\,0 \\ 1\,0\,0\,0\,0\,0\,0\,0 \\ 1\,1\,0\,0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,1\,1\,1\,0 \\ 0\,1\,1\,1\,0\,1\,0\,0 \\ 0\,0\,0\,0\,1\,1\,0\,0 \\ 1\,1\,0\,1\,0\,0\,0\,1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix}$$

GF(2^4): $z^4+z+1=0$

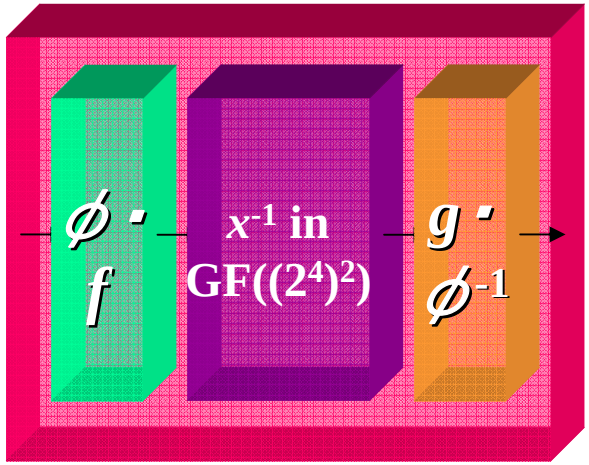
GF((2^4)^2): $z^2+z+\lambda=0$ ($\lambda=\omega^3$)

S-box S_1



行列をマージすると…

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&1&1&0&0 \\ 0&0&0&1&0&0&1&0 \\ 0&0&1&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&1 \\ 1&0&0&1&0&0&0&0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$



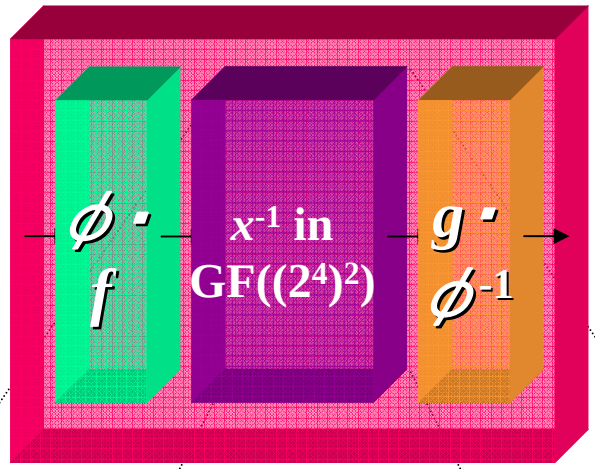
$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0&1 \\ 0&0&0&1&1&0&0&0 \\ 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&1&0 \\ 0&0&0&0&1&1&0&0 \\ 0&0&1&1&0&0&0&0 \\ 1&0&1&0&0&0&0&0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

2 XOR + 2 XNOR + 2 NOT

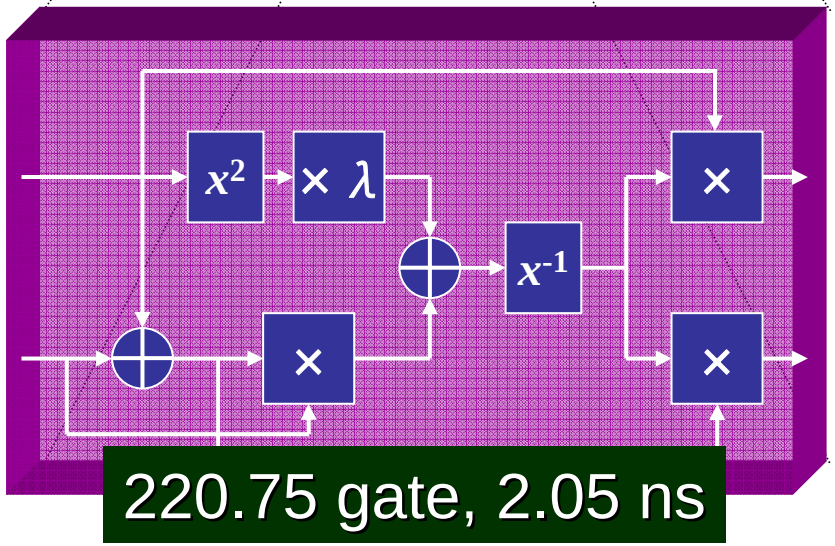
2 XOR + 4 XNOR

S-box S_1

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&1&1&0&0 \\ 0&0&0&1&0&0&1&0 \\ 0&0&1&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&1 \\ 1&0&0&1&0&0&0&0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$



$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0&1 \\ 0&0&0&1&1&0&0&0 \\ 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&1&0 \\ 0&0&0&0&1&1&0&0 \\ 0&0&1&1&0&0&0&0 \\ 1&0&1&0&0&0&0&0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$



AES の S-box との比較

		ゲート規模 (gate)	遅延時間 (ns)
CLEFIA	S_0	144.75	1.33
	S_1	220.25	2.05
AES	*SubByte/SubByte*$^{-1}$	~~252.75~~ 306.25	N/A

S_0, S_1 とも *SubByte/SubByte*$^{-1}$ と比較して小型

AES: D. Canright. “A Very Compact S-box for AES”, CHES 2005

拡散行列 M_0

$$\begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} = \begin{pmatrix} 01 & 02 & 04 & 06 \\ 02 & 01 & 06 & 04 \\ 04 & 06 & 01 & 02 \\ 06 & 04 & 02 & 01 \end{pmatrix} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{pmatrix}$$

X_i, Y_i : GF(2^8)の元

Hardmard行列の特性により共有化が可能

$$= \begin{pmatrix} 01 & 00 & 00 & 00 \\ 00 & 01 & 00 & 00 \\ 00 & 00 & 01 & 00 \\ 00 & 00 & 00 & 01 \end{pmatrix} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{pmatrix} + \begin{pmatrix} 00 & 02 & 00 & 02 \\ 02 & 00 & 02 & 00 \\ 00 & 02 & 00 & 02 \\ 02 & 00 & 02 & 00 \end{pmatrix} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{pmatrix} + \begin{pmatrix} 00 & 00 & 04 & 04 \\ 00 & 00 & 04 & 04 \\ 04 & 04 & 00 & 00 \\ 04 & 04 & 00 & 00 \end{pmatrix} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{pmatrix}$$

$$\begin{aligned} A_0 &= X_0 \oplus X_1 \\ A_1 &= X_2 \oplus X_3 \\ B_0 &= X_0 \oplus X_2 \\ B_1 &= X_1 \oplus X_3 \end{aligned} \qquad \begin{aligned} C_0 &= \{02\} \times B_0 \\ C_1 &= \{02\} \times B_1 \\ D_0 &= \{04\} \times A_0 \\ D_1 &= \{04\} \times A_1 \end{aligned} \qquad \begin{aligned} Y_0 &= C_1 \oplus D_1 \oplus X_0 \\ Y_1 &= C_1 \oplus D_0 \oplus X_1 \\ Y_2 &= C_0 \oplus D_1 \oplus X_2 \\ Y_3 &= C_0 \oplus D_0 \oplus X_3 \end{aligned}$$

XORゲート数 112, XOR遅延段数 4

拡散行列 M_1

$$\begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} = \begin{pmatrix} 01 & 08 & 02 & 0A \\ 08 & 01 & 0A & 02 \\ 02 & 0A & 01 & 08 \\ 0A & 02 & 08 & 01 \end{pmatrix} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{pmatrix}$$

X_i, Y_i : GF(2^8)の元

$$= \begin{pmatrix} 01 & 00 & 00 & 00 \\ 00 & 01 & 00 & 00 \\ 00 & 00 & 01 & 00 \\ 00 & 00 & 00 & 01 \end{pmatrix} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{pmatrix} + \begin{pmatrix} 00 & 00 & 02 & 02 \\ 00 & 00 & 02 & 02 \\ 02 & 02 & 00 & 00 \\ 02 & 02 & 00 & 00 \end{pmatrix} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{pmatrix} + \begin{pmatrix} 00 & 08 & 00 & 08 \\ 08 & 00 & 08 & 00 \\ 00 & 08 & 00 & 08 \\ 08 & 00 & 08 & 00 \end{pmatrix} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{pmatrix}$$

$$A_0 = X_0 \oplus X_1 \qquad C_0 = \{02\} \times A_0 \qquad Y_0 = C_1 \oplus D_1 \oplus X_0$$
$$A_1 = X_2 \oplus X_3 \qquad C_1 = \{02\} \times A_1 \qquad Y_1 = C_1 \oplus D_0 \oplus X_1$$
$$B_0 = X_0 \oplus X_2 \qquad D_0 = \{08\} \times B_0 \qquad Y_2 = C_0 \oplus D_1 \oplus X_2$$
$$B_1 = X_1 \oplus X_3 \qquad D_1 = \{08\} \times B_1 \qquad Y_3 = C_0 \oplus D_0 \oplus X_3$$

XORゲート数 118, XOR遅延段数 4

AES の拡散行列との比較

		XOR ゲート数	XOR 遅延段数
CLEFIA	M_0	112	4
	M_1	118	4
AES	*MixColumn/MixColumn*$^{-1}$	166	7

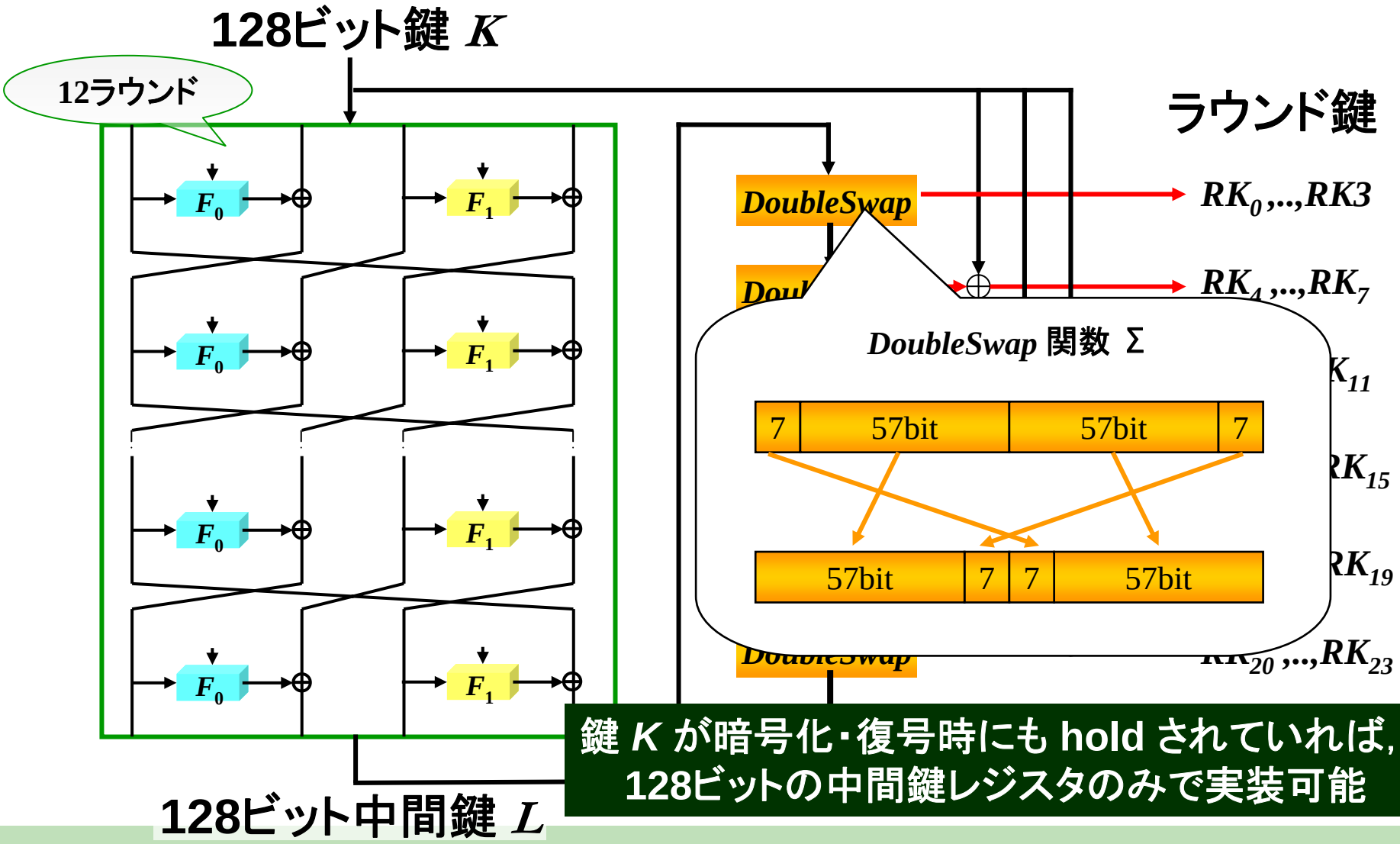
M_0, M_1 とも *MixColumn/MixColumn*$^{-1}$ と比較して小型かつ高速

AES: 清水，佐野，本山，大熊，川村. “SPN型ブロック暗号の実装について”, ISEC 2001-55

鍵スケジュール部の最適化

- *DoubleSwap* 関数の最適化
- 部分鍵の等価変形

鍵スケジュール部 (128ビット鍵)



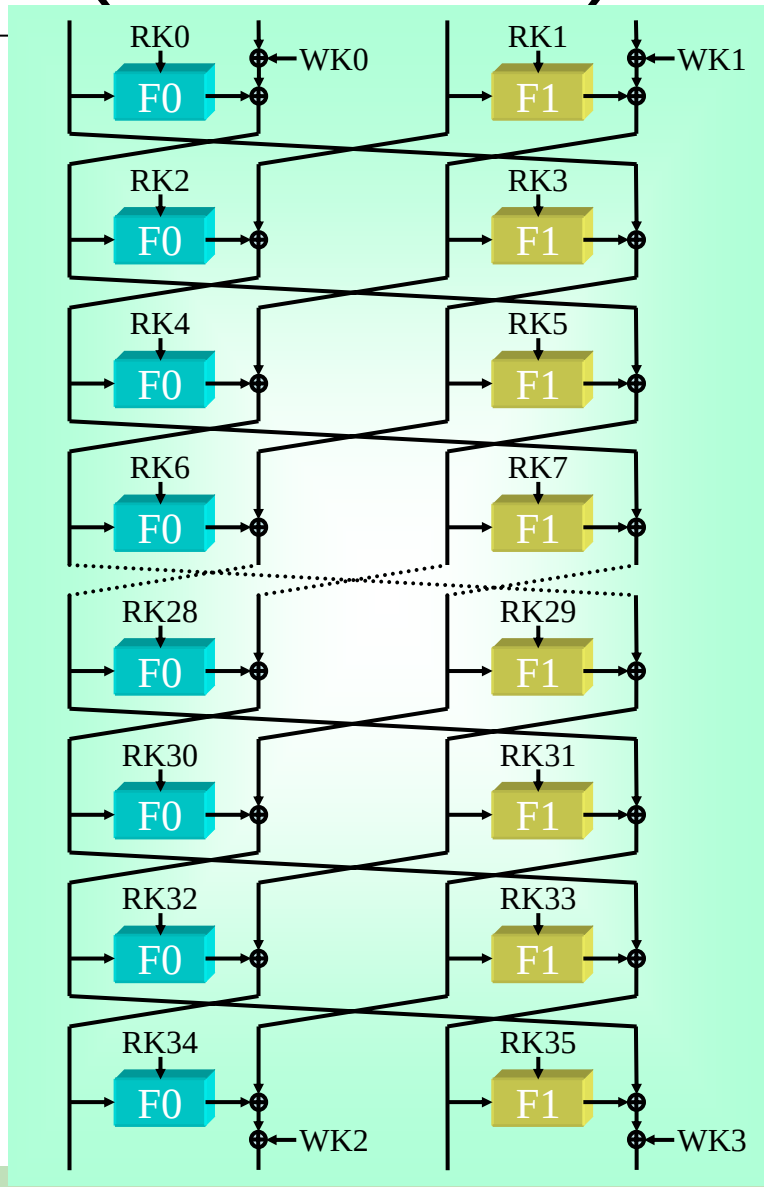
鍵 K が暗号化・復号時にも hold されていれば,
128ビットの中間鍵レジスタのみで実装可能

CLEFIA

鍵スケジューリング (128ビット鍵)

128 ビット鍵 K, 128 ビット中間鍵 L

WK_0	WK_1	WK_2	WK_3	K
RK_0	RK_1	RK_2	RK_3	L
RK_4	RK_5	RK_6	RK_7	$\Sigma(L) + K$
RK_8	RK_9	RK_{10}	RK_{11}	$\Sigma^2(L)$
RK_{12}	RK_{13}	RK_{14}	RK_{15}	$\Sigma^3(L) + K$
RK_{16}	RK_{17}	RK_{18}	RK_{19}	$\Sigma^4(L)$
RK_{20}	RK_{21}	RK_{22}	RK_{23}	$\Sigma^5(L) + K$
RK_{24}	RK_{25}	RK_{26}	RK_{27}	$\Sigma^6(L)$
RK_{28}	RK_{29}	RK_{30}	RK_{31}	$\Sigma^7(L) + K$
RK_{32}	RK_{33}	RK_{34}	RK_{35}	$\Sigma^8(L)$



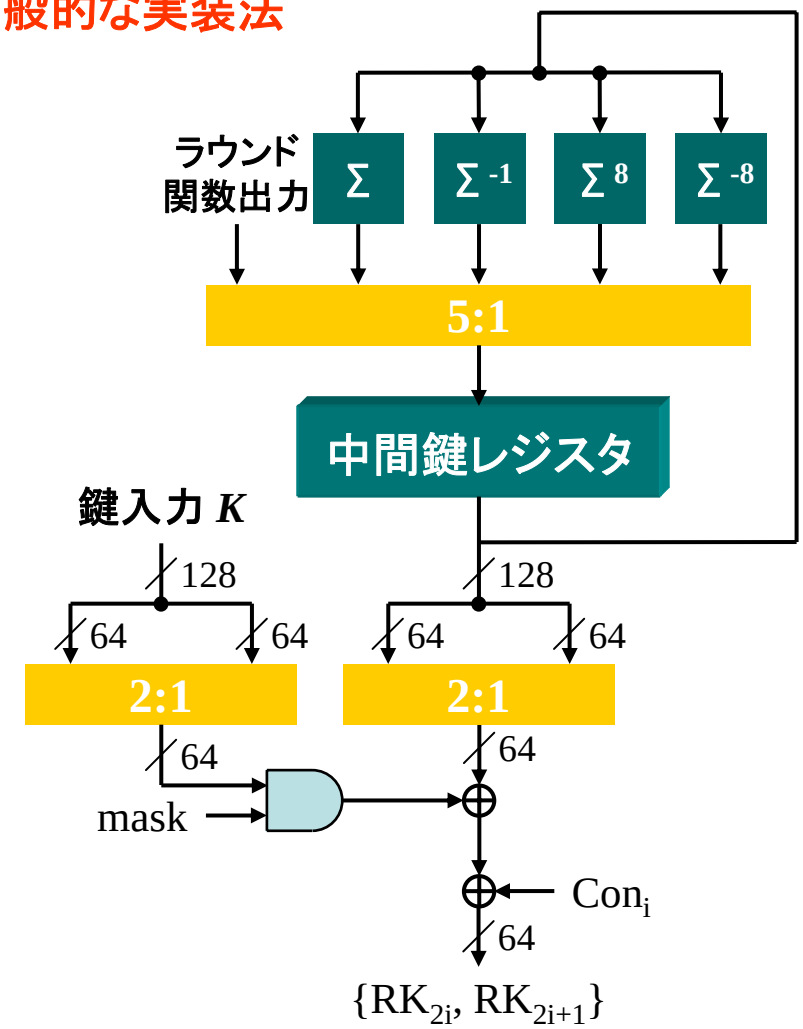
CLEFIA

鍵スケジューリング (128ビット鍵)

128 ビット鍵 K, 128 ビット中間鍵 L

WK_0	WK_1	WK_2	WK_3	K
RK_0	RK_1	RK_2	RK_3	L
RK_4	RK_5	RK_6	RK_7	$\Sigma(L) + K$
RK_8	RK_9	RK_{10}	RK_{11}	$\Sigma^2(L)$
RK_{12}	RK_{13}	RK_{14}	RK_{15}	$\Sigma^3(L) + K$
RK_{16}	RK_{17}	RK_{18}	RK_{19}	$\Sigma^4(L)$
RK_{20}	RK_{21}	RK_{22}	RK_{23}	$\Sigma^5(L) + K$
RK_{24}	RK_{25}	RK_{26}	RK_{27}	$\Sigma^6(L)$
RK_{28}	RK_{29}	RK_{30}	RK_{31}	$\Sigma^7(L) + K$
RK_{32}	RK_{33}	RK_{34}	RK_{35}	$\Sigma^8(L)$

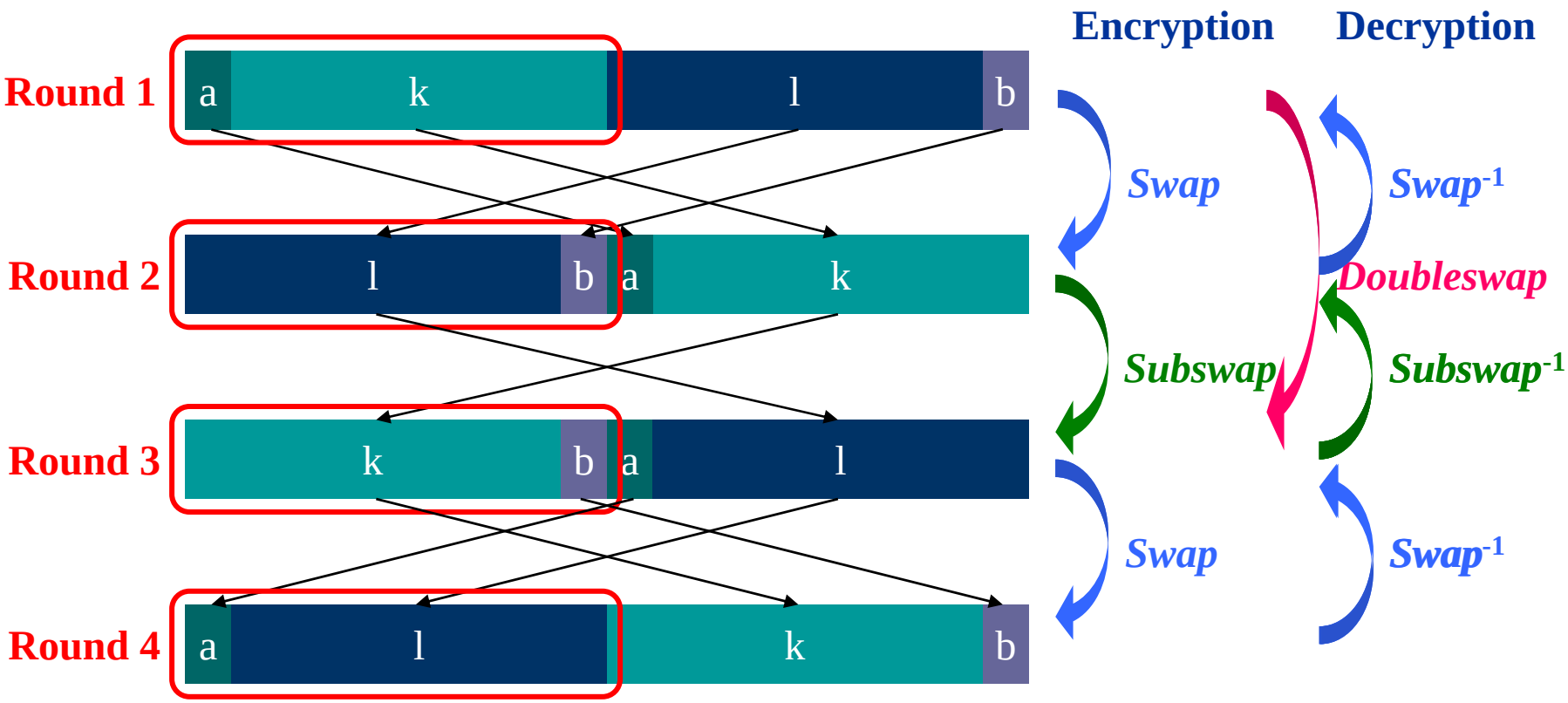
一般的な実装法



CLEFIA

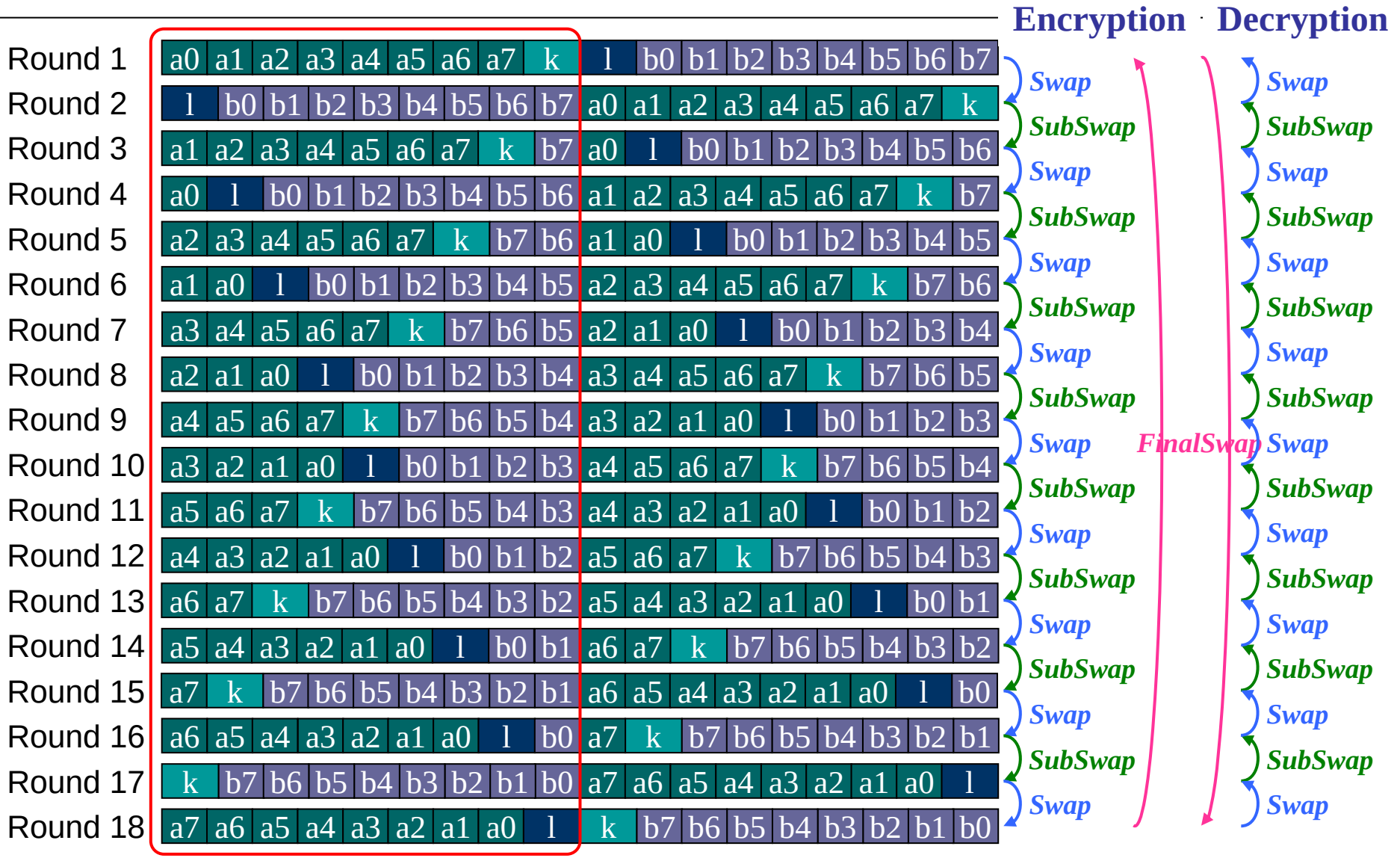
DoubleSwap 関数の最適化

- 中間鍵レジスタの上位と下位をswapさせていくと…



EncryptionとDecryptionでbit permutationが共有可能

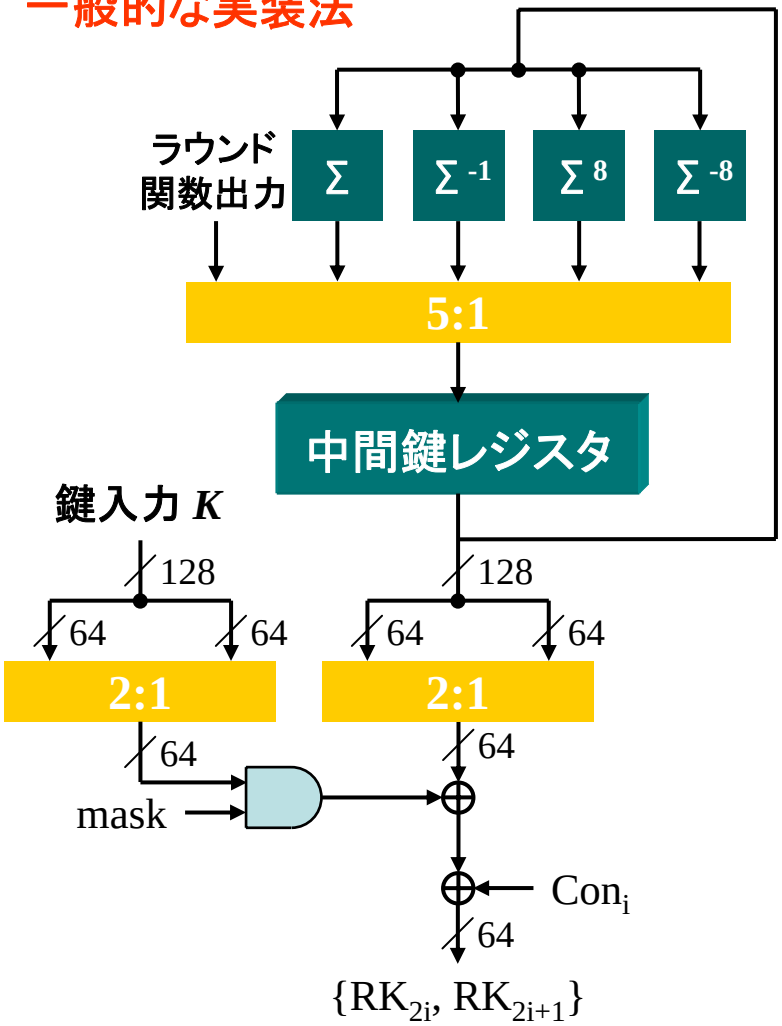
DoubleSwap 関数の最適化



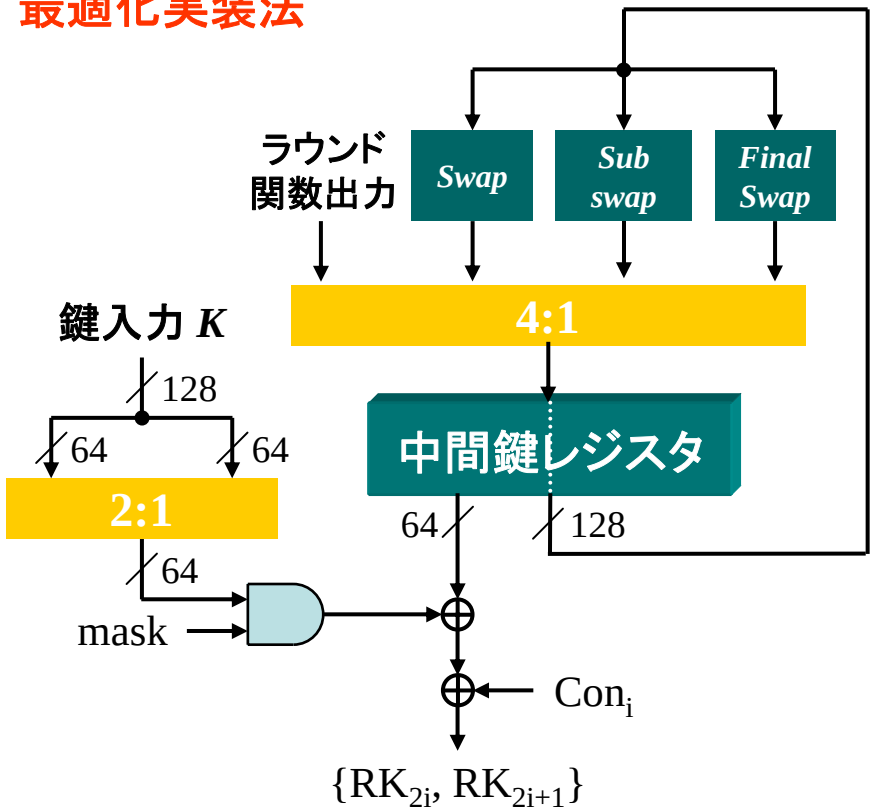
CLEFIA

DoubleSwap 関数の最適化

一般的な実装法



最適化実装法

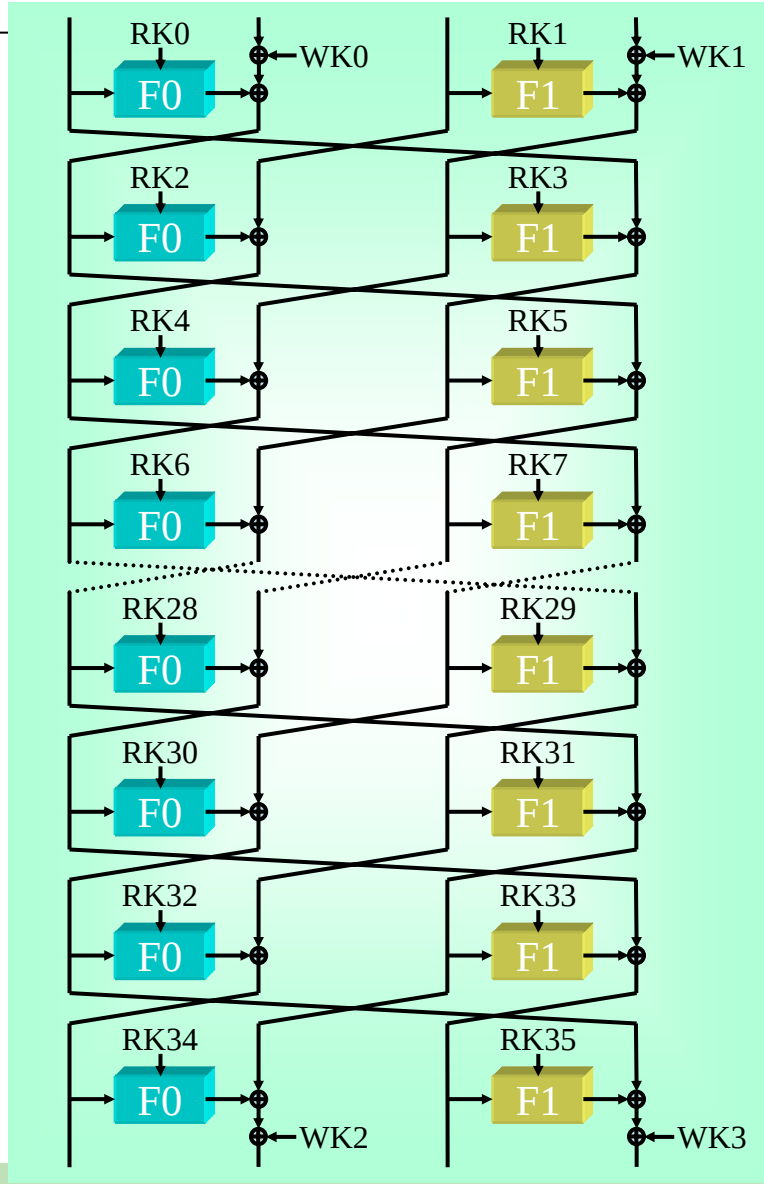


セレクタの削減が可能

部分鍵の等価変形

128ビット鍵 K, 中間鍵 L

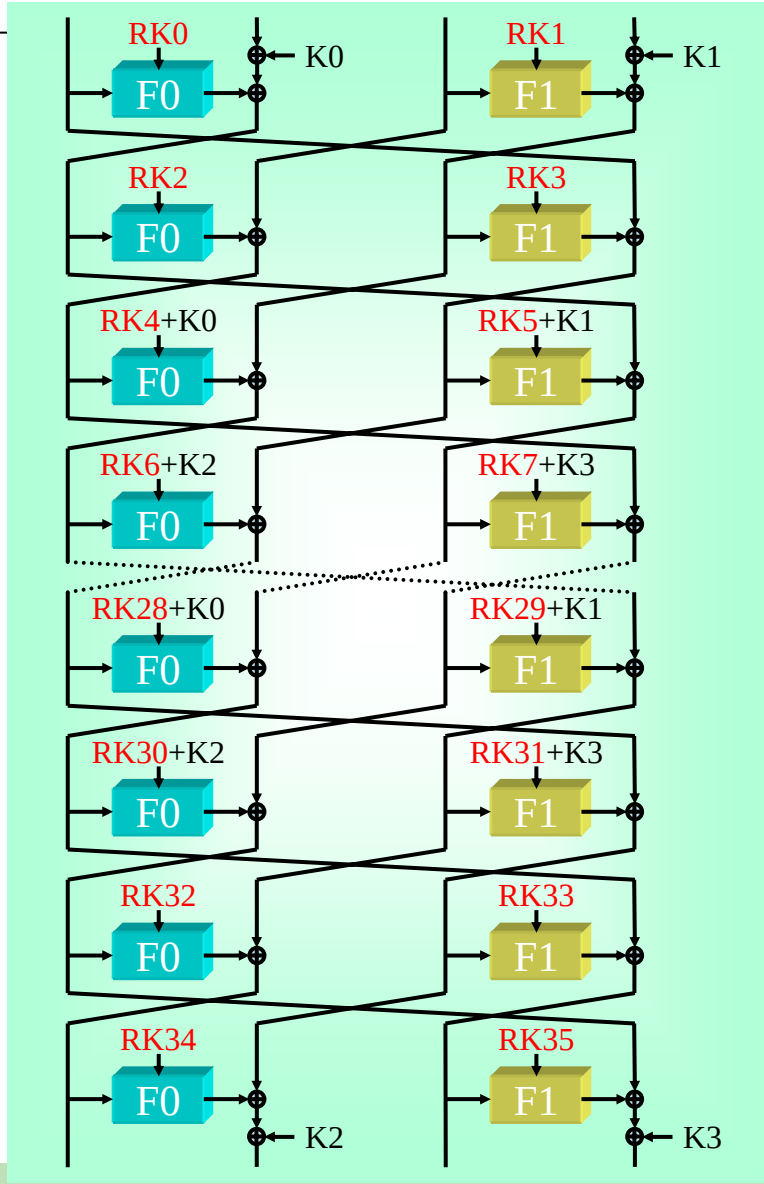
WK_0	WK_1	WK_2	WK_3	K
RK_0	RK_1	RK_2	RK_3	L
RK_4	RK_5	RK_6	RK_7	$\Sigma(L) + K$
RK_8	RK_9	RK_{10}	RK_{11}	$\Sigma^2(L)$
RK_{12}	RK_{13}	RK_{14}	RK_{15}	$\Sigma^3(L) + K$
RK_{16}	RK_{17}	RK_{18}	RK_{19}	$\Sigma^4(L)$
RK_{20}	RK_{21}	RK_{22}	RK_{23}	$\Sigma^5(L) + K$
RK_{24}	RK_{25}	RK_{26}	RK_{27}	$\Sigma^6(L)$
RK_{28}	RK_{29}	RK_{30}	RK_{31}	$\Sigma^7(L) + K$
RK_{32}	RK_{33}	RK_{34}	RK_{35}	$\Sigma^8(L)$

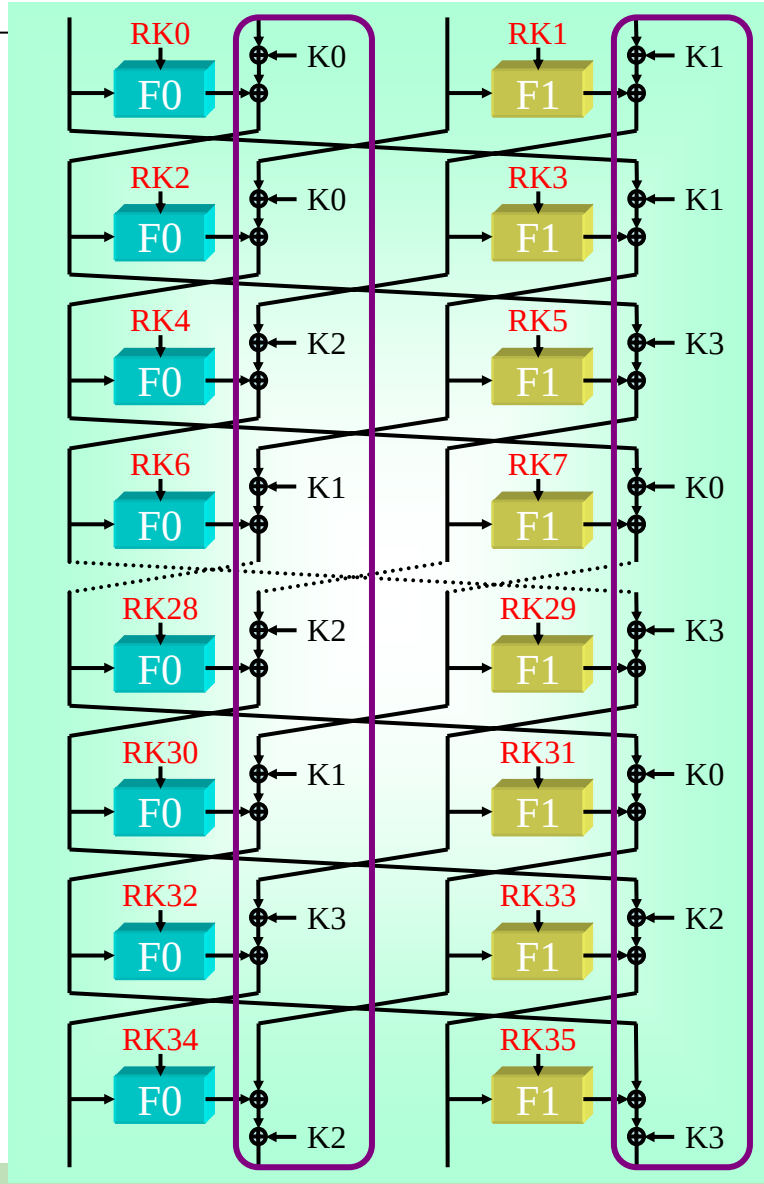


$K = K_0|K_1|K_2|K_3$ として，ラウンド鍵 $RK_{2r}|RK_{2r+1}$ のうち，Lに関する部分を $RK_{2r}|RK_{2r+1}$ とすると…

部分鍵の等価変形

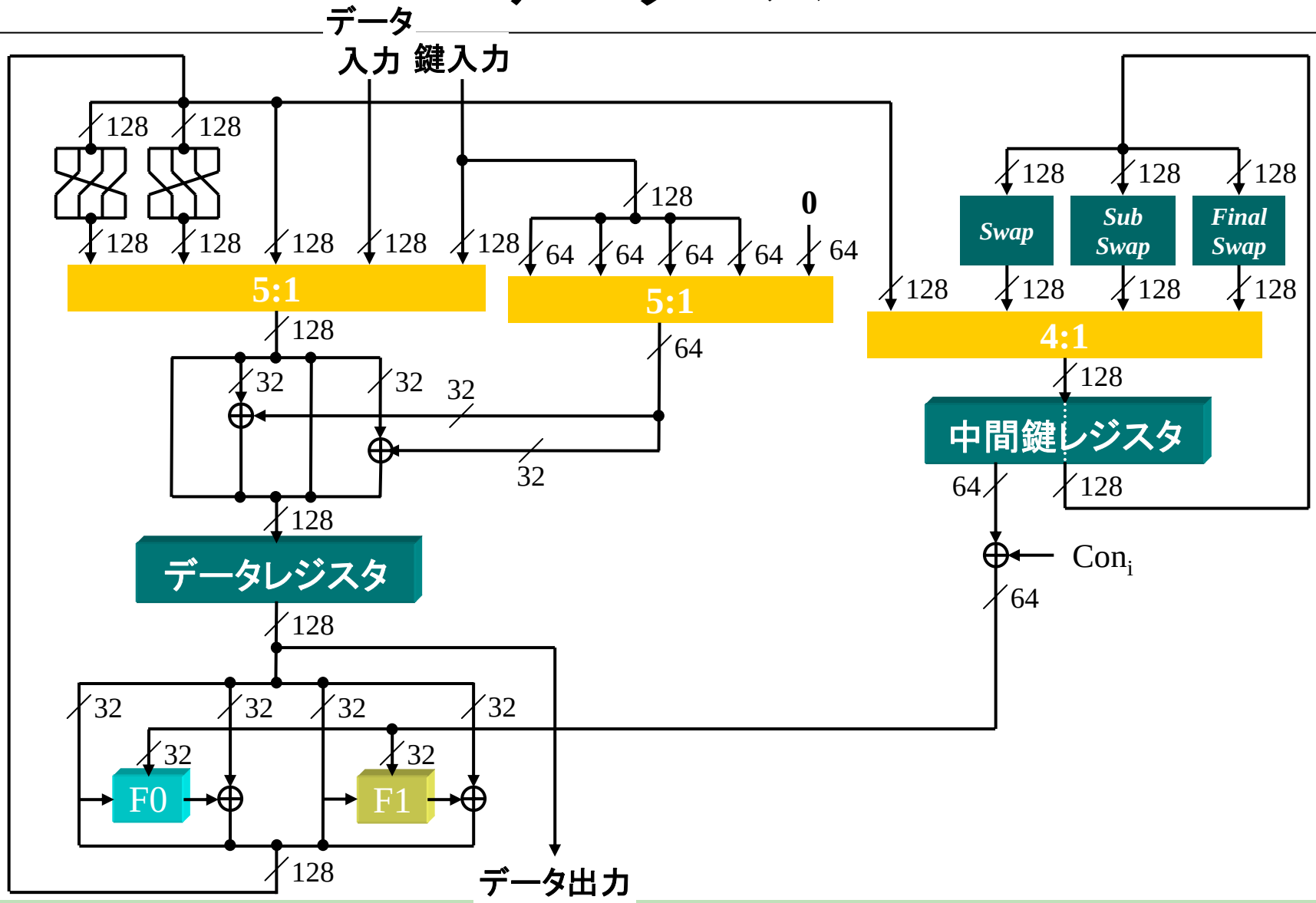
Key whiteningと同じ場所に





CLEFIA

データパス



CLEFIA

実装性能評価

実装法	アルゴリズム	暗/復号 (cycle)	ゲート規模 (gate)	速度 (Mbps)	ゲート効率 (Kbps/gate)		プロセス (um)
高速版	CLEFIA	18	5,979	1,605.94	268.63	1.98	0.09
	AES	11	12,454	1,691.35	135.81	1	0.13
	Camellia	22	10,993	971.29	88.36	0.65	0.13
小型版	CLEFIA	36	4,950	715.69	144.59	2.51	0.09
	AES	54	5,398	311.09	57.63	1	0.13
	Camellia	44	6,511	325.76	50.03	0.87	0.13

CLEFIAの高いハードウェア実装性能を示している

AES, Camellia: A. Sato, S. Morioka, “Hardware-Focused Performance Comparisons for the Standard Block Ciphers AES, Camellia, and Triple-DES”, ISC’03

まとめ

- 128ビットブロック暗号 CLEFIAに関する
  - ハードウェア実装における最適化手法の検討
  - 評価結果の報告

  を行なった
- 非常にシンプルかつ効率的にハードウェア実装可能な構成
- 高いハードウェア実装性能を保持

さいごに

CLEFIA HP
http://www.sony.co.jp/clefia/

- 仕様書 (ver 1.0)
- 設計方針（ver 1.0)
- 自己評価書 (ver 1.0)
- リファレンスコード(ver 1.0.0)

などがダウンロード可能です

発表資料等順次更新する予定です