128ビットブロック暗号 CLEFIA の小型ハードウェア実装評価

秋下 徹　　樋渡 玄良

ソニー株式会社

CLEFIA

本発表の概要

- 128 ビットブロック暗号 CLEFIA のハードウェア実装の更なる小型化を目指して，8 ビット・シリアルアーキテクチャに基づいた実装を行なった.
- 128 ビット鍵 CLEFIA の実装評価結果
  - 暗号化のみ　　2.9 kGE
  - 暗復号　　3.0 kGE

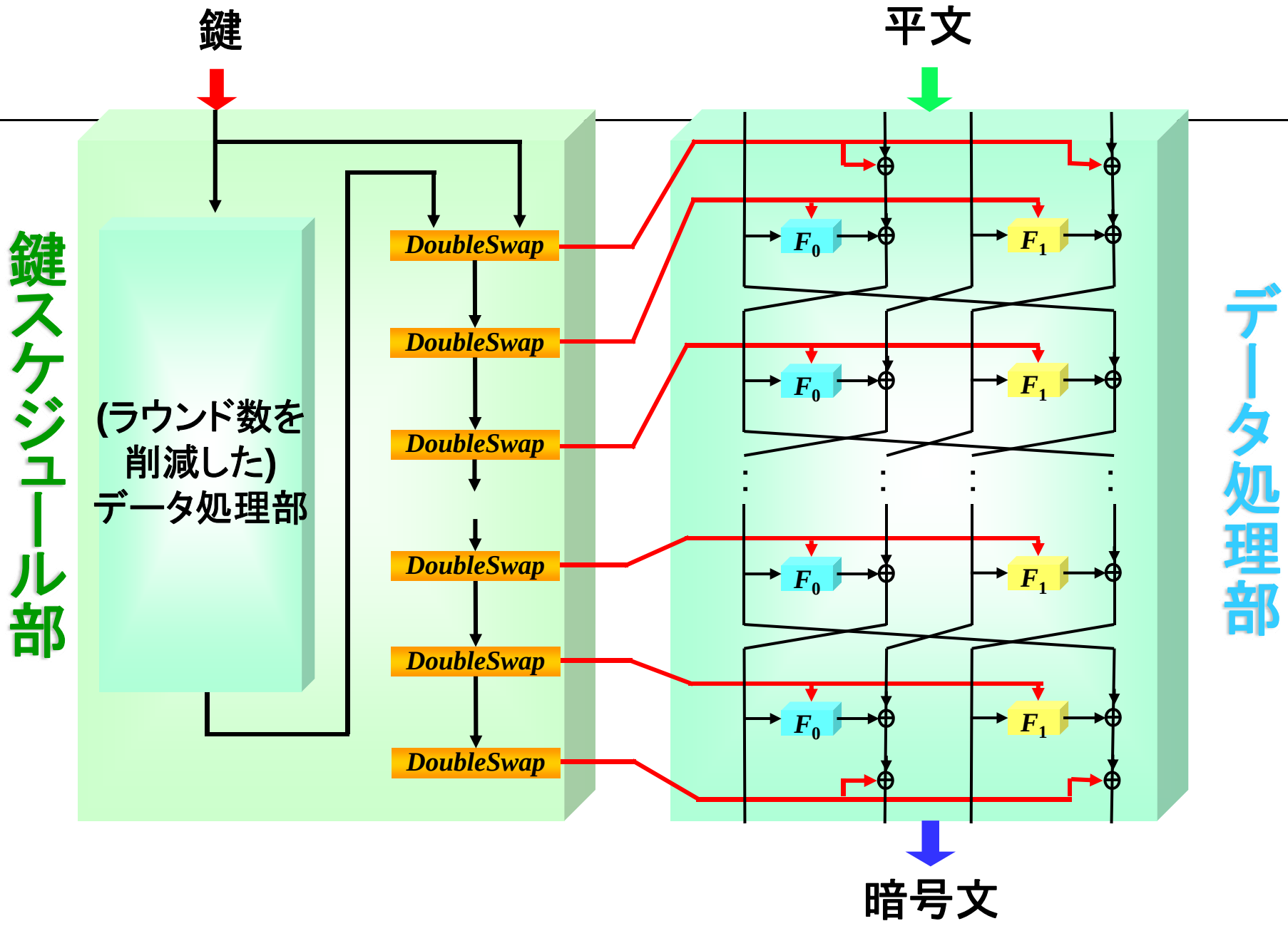
CLEFIA のハードウェア実装における小型実装性能を示す結果が得られた

本発表の流れ

- 128 ビットブロック暗号 CLEFIA
  - 概要
  - 既存のハードウェア実装評価
- 8 ビット・シリアルアーキテクチャによる AES 実装
  - Hamalainen らの AES 実装
- 8 ビット・シリアルアーキテクチャによる CLEFIA 実装
  - CLEFIA 暗号化実装
  - CLEFIA 暗復号実装
- 実装性能評価
- まとめ

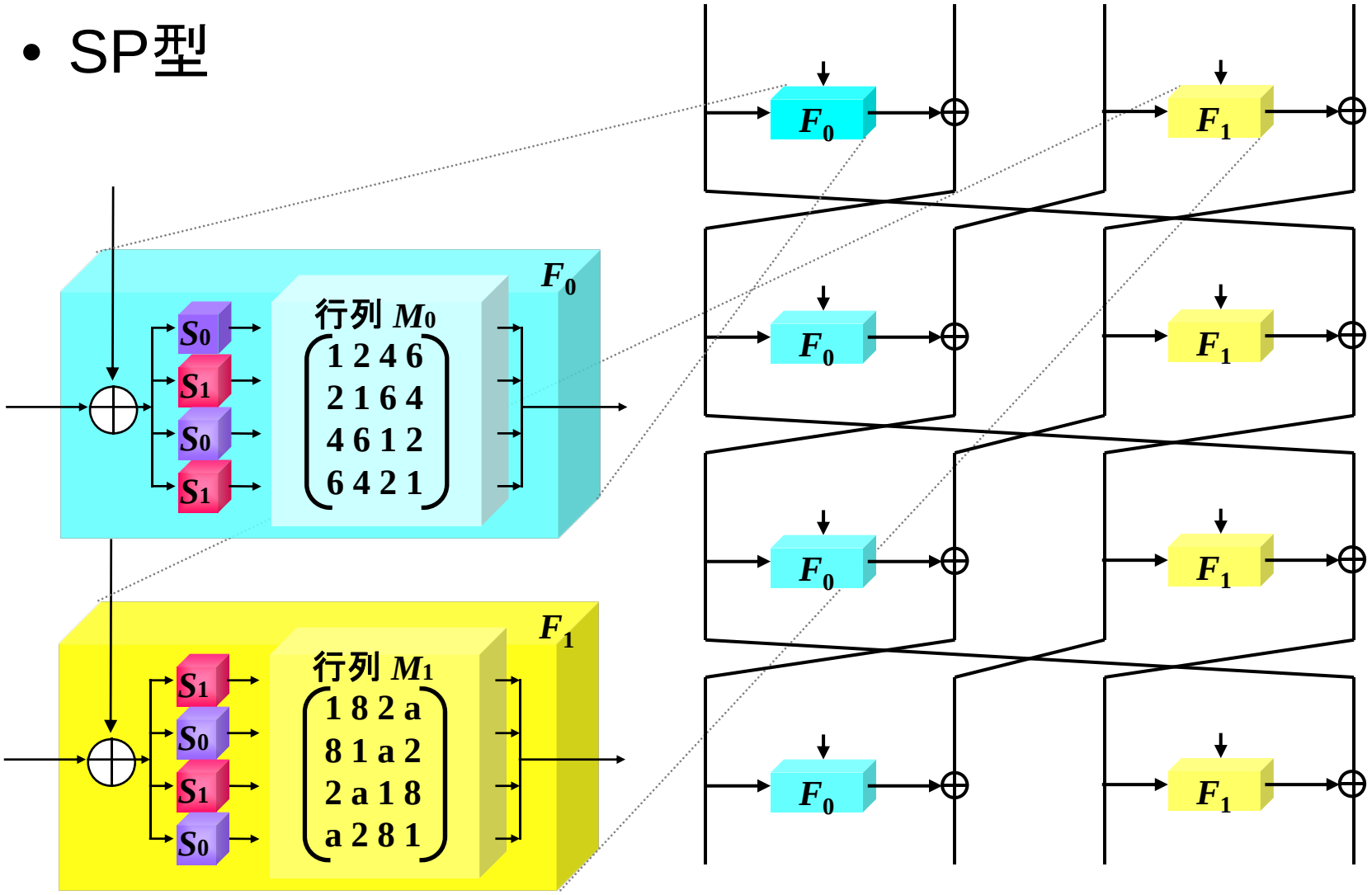
128 ビットブロック暗号 CLEFIA

- 名古屋大学とソニーにより 2007 年に提案された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
- 安全性，速度，実装コストのバランスを追及
- 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)


鍵
平文
鍵スケジュール部
(ラウンド数を
削減した)
データ処理部
DoubleSwap
DoubleSwap
DoubleSwap
DoubleSwap
DoubleSwap
DoubleSwap
F_0
F_1
データ処理部
暗号文

F 関数

- SP型



CLEFIA

CLEFIA のハードウェア実装評価

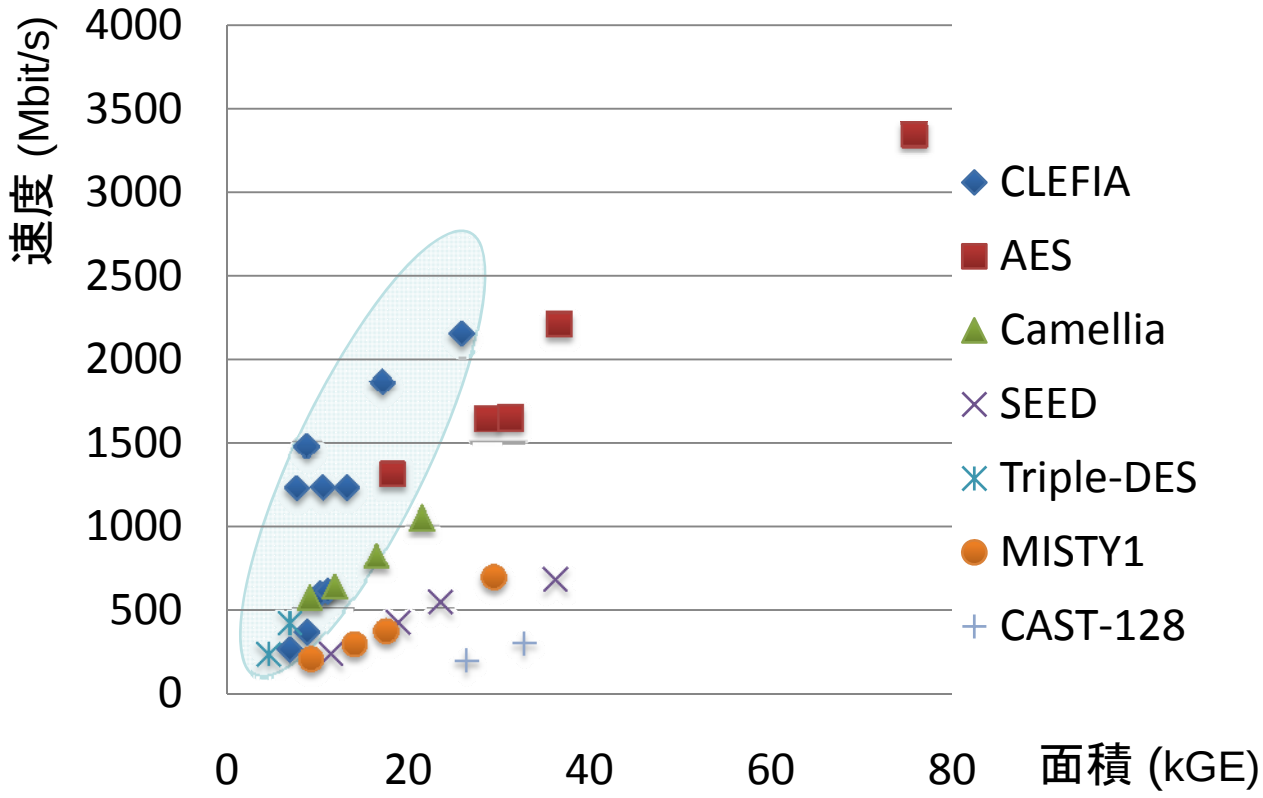
- 設計者評価

実装法	アルゴリズム	暗/復号 (cycle)	ゲート規模 (GE)	速度 (Mbps)	ゲート効率 (Kbps/GE)		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

白井, 渋谷, 秋下, 盛合, 岩田. “128 ビットブロック暗号 CLEFIA のハードウェア実装評価”, ISEC 2007-49

CLEFIA のハードウェア実装評価

- 第三者評価
  - ISO 標準ブロック暗号 (ISO/IEC 18033-3) との比較



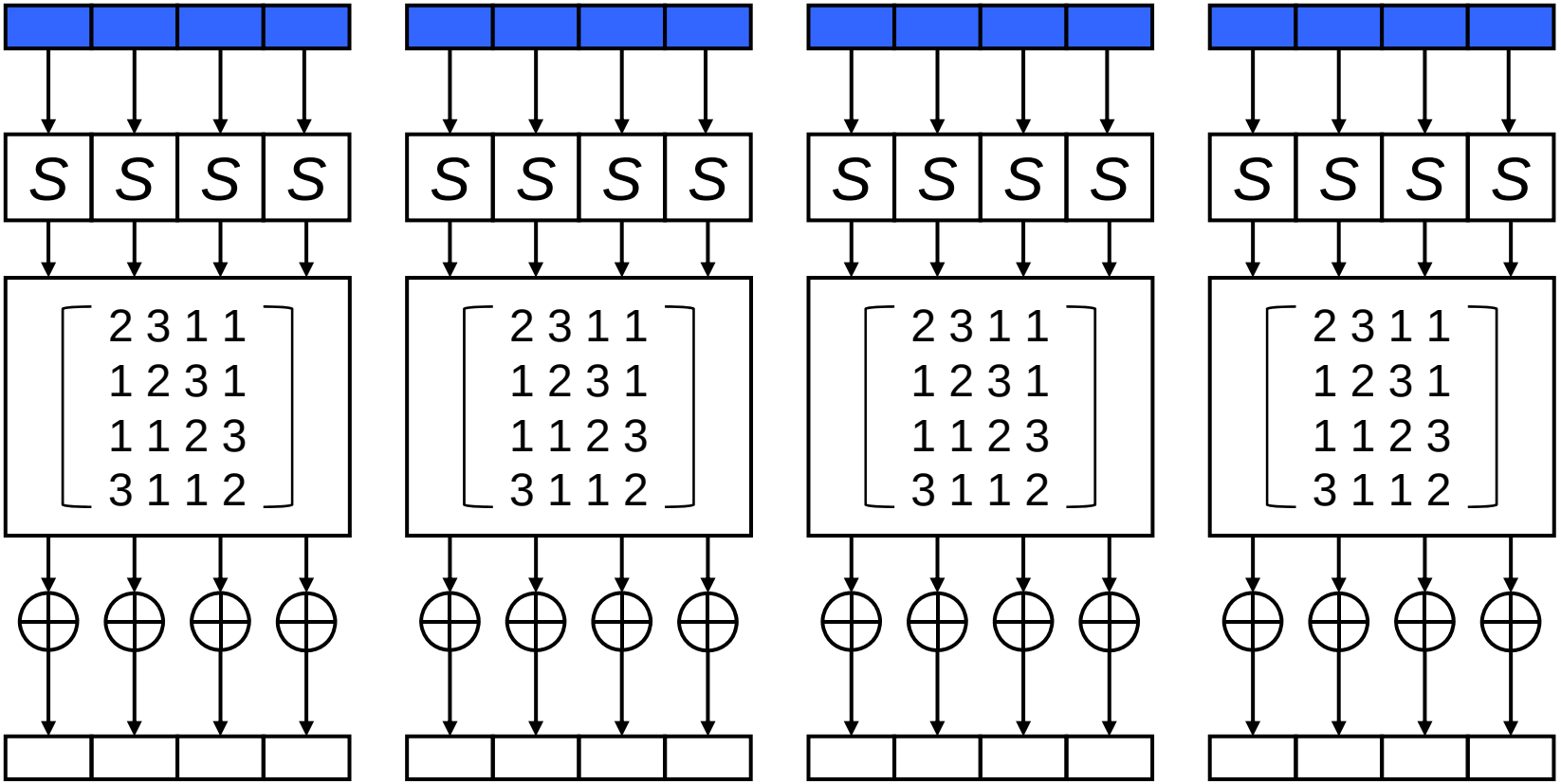
菅原, 本間, 青木, 佐藤. “128 ビットブロック暗号 CLEFIA の ASIC 実装評価”, CSS2007

AES の小型実装

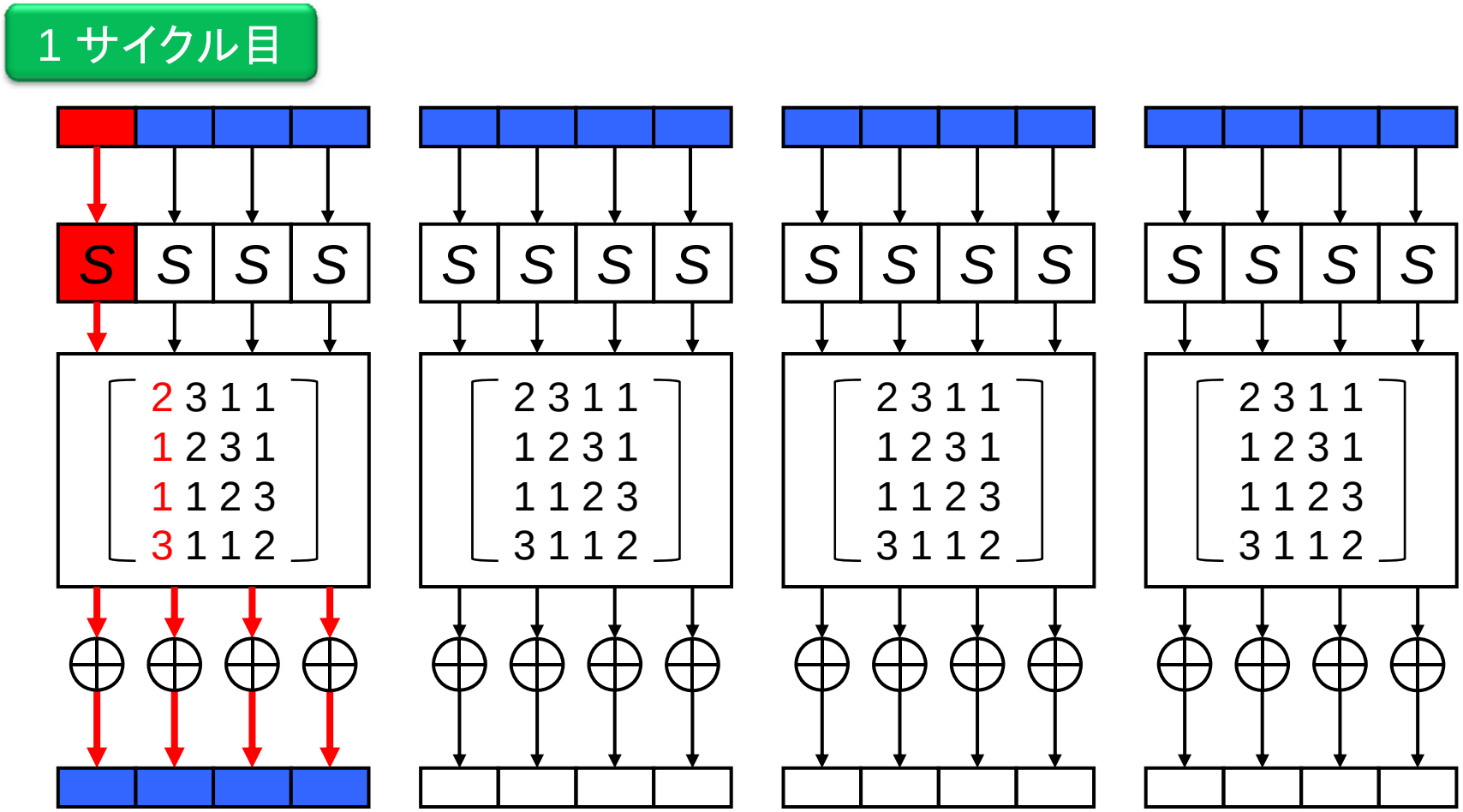
- RFID では暗号プリミティブに使用可能なゲート規模が 250－4,000 GE
- AES-128 の 8 ビット・シリアルアーキテクチャによる実装
  - 規模の大きい S-box 回路を 1 つのみ配置し小型化を図る
  - Feldhofer らによる実装　　3,400 GE
    - RAM を用いたシリアルアーキテクチャ，暗復号に対応
  - Hamalainen らによる実装　　3,100 GE
    - シフトレジスタを用いたシリアルアーキテクチャ，暗号化のみ対応

Hamalainen らの AES 実装

データ処理回路を S-box 回路 1 つのみで構成，1 ラウンドを 16 サイクルで実行



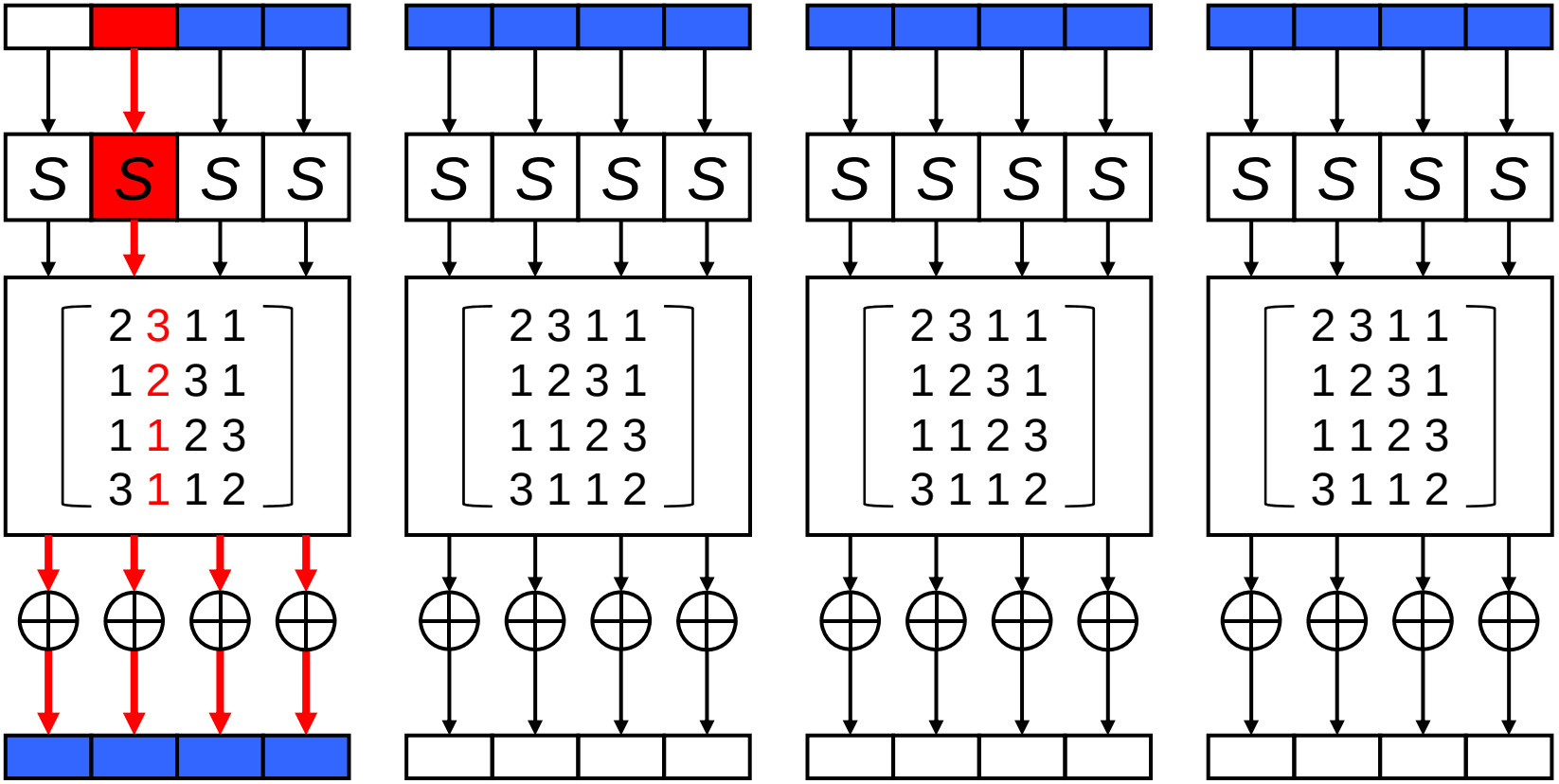
Hamalainen らの AES 実装



CLEFIA

Hamalainen らの AES 実装

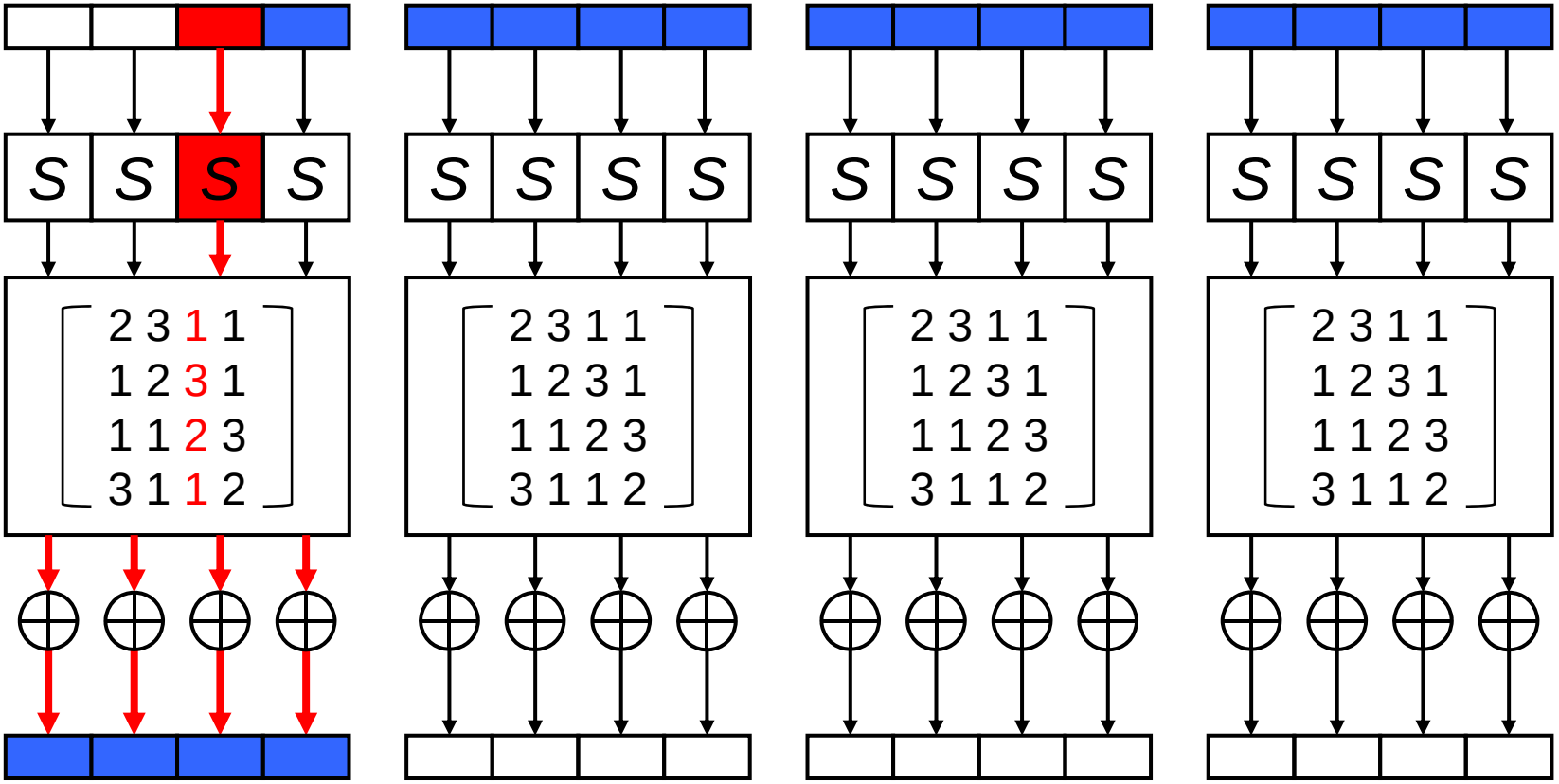
2 サイクル目



CLEFIA

Hamalainen らの AES 実装

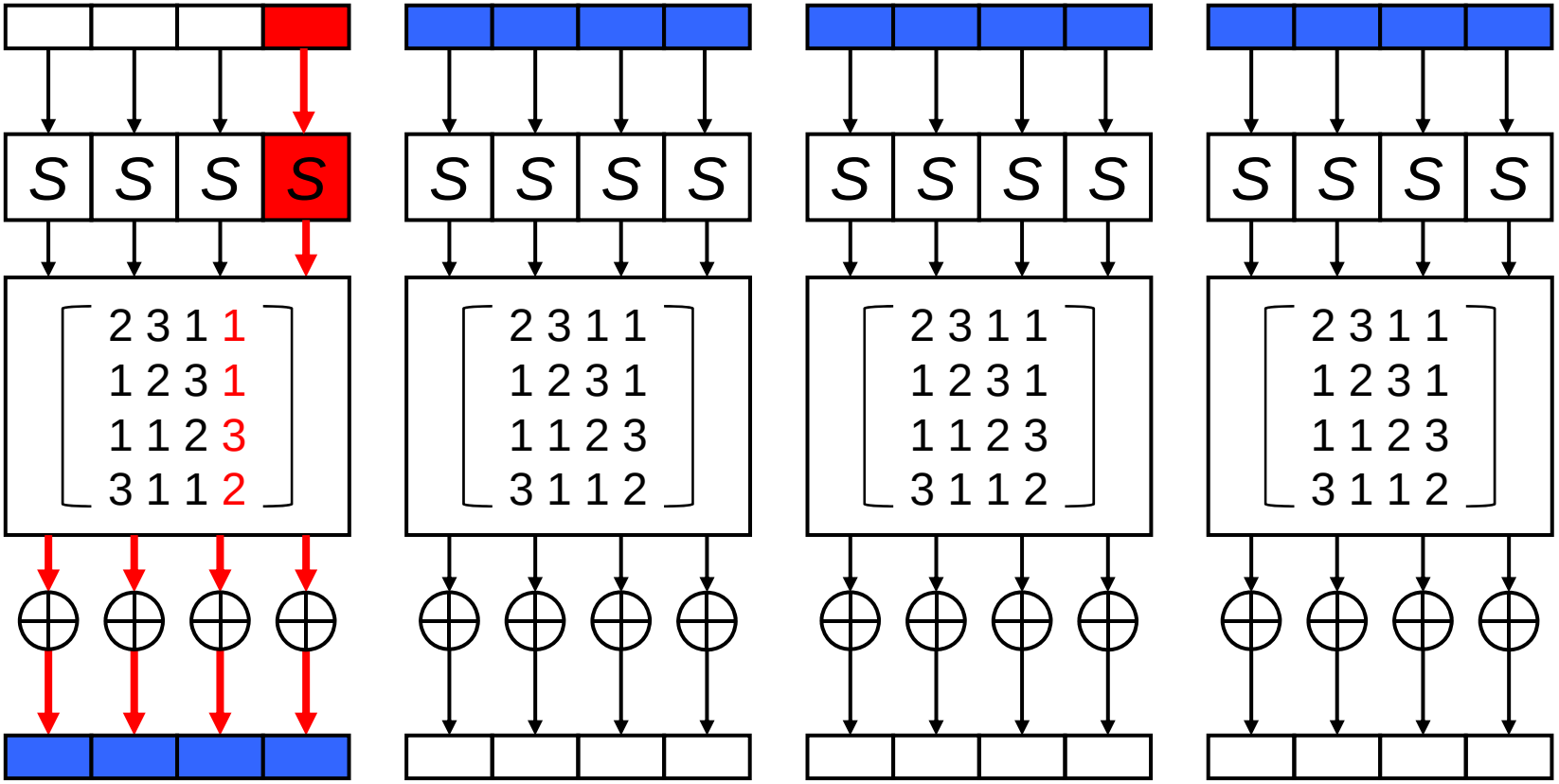
3 サイクル目



CLEFIA

Hamalainen らの AES 実装

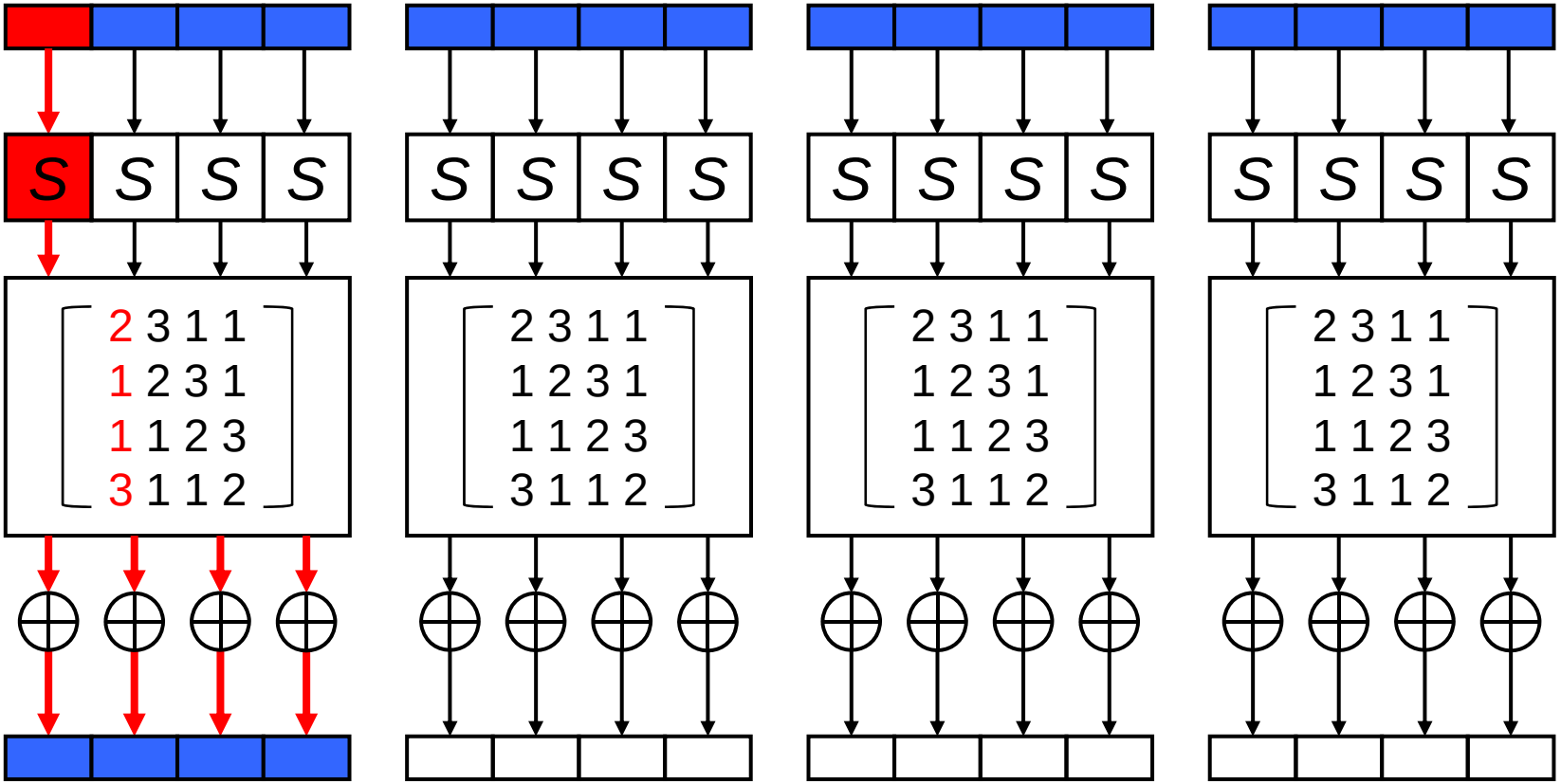
4 サイクル目



CLEFIA

Hamalainen らの AES 実装

1 サイクル目



16 + 3 バイト分のレジスタが必要

CLEFIA

Hamalainen らの AES 実装

- データパス

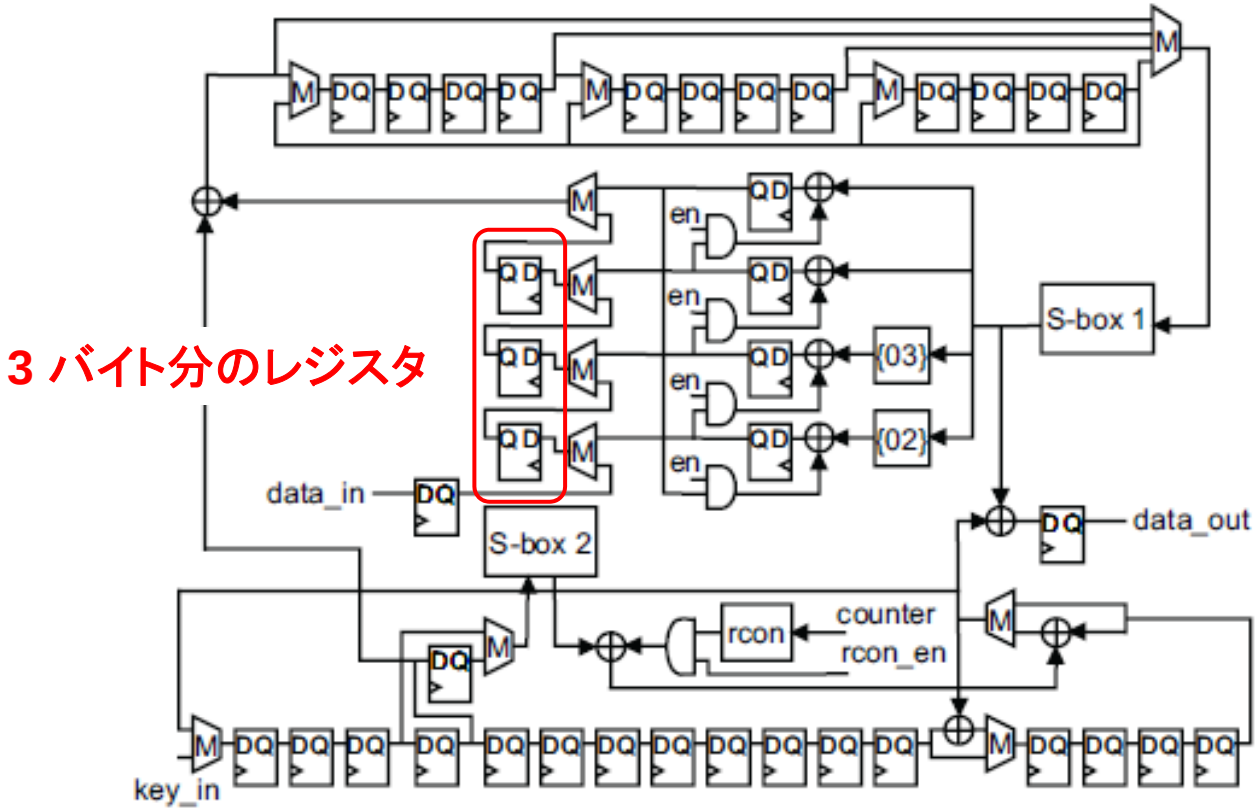


Figure 6. Data path of the AES encryption core.

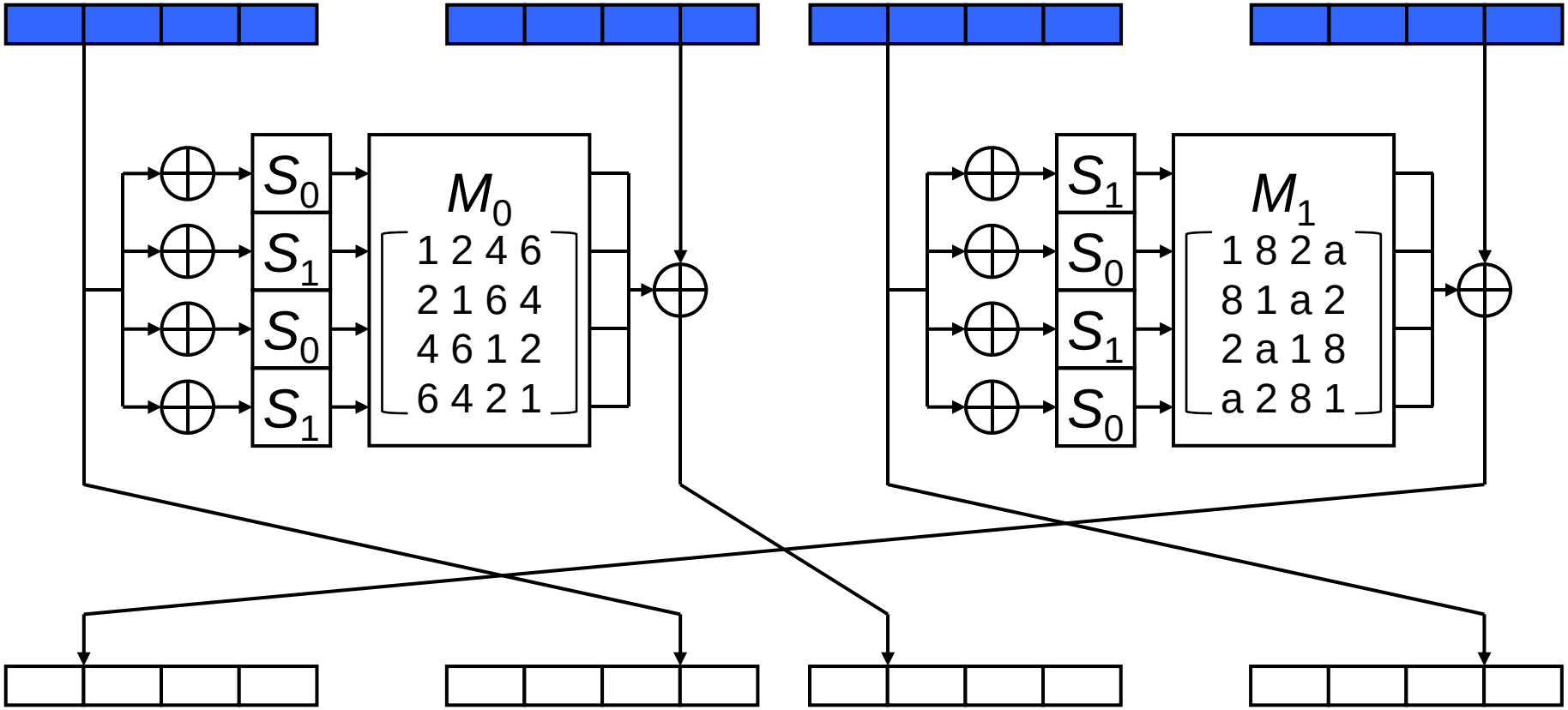
CLEFIA

CLEFIA の小型実装

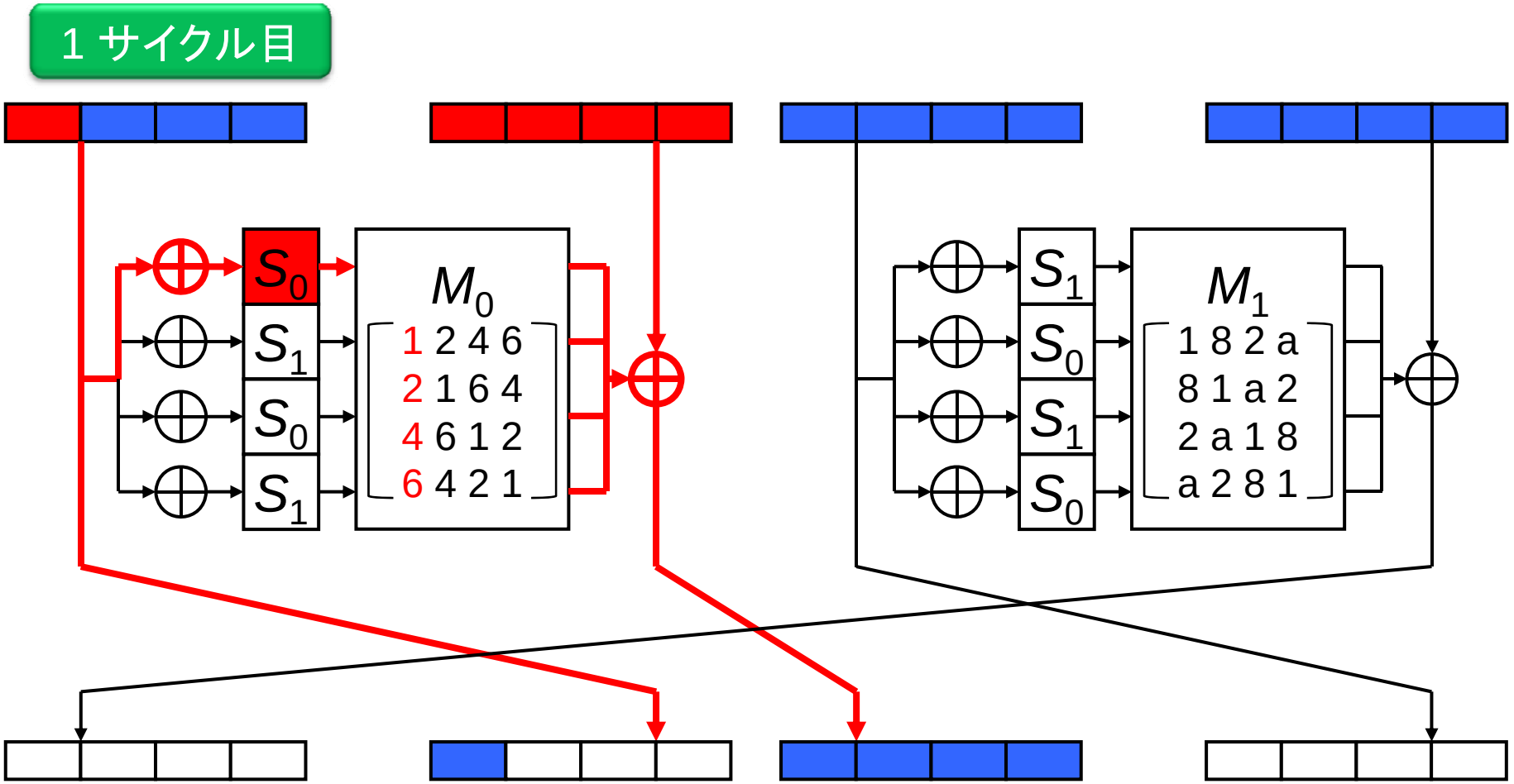
- 従来の実装評価結果では 4,950 GE が最小
  - F 関数を 1 サイクルで実行する 32 ビット・アーキテクチャ
- シフトレジスタを用いた 8 ビット・シリアルアーキテクチャにより小型化を図る
  - 鍵スケジュールにビット演算を含む CLEFIA は RAM を用いた実装には不向き

CLEFIA 暗号化実装

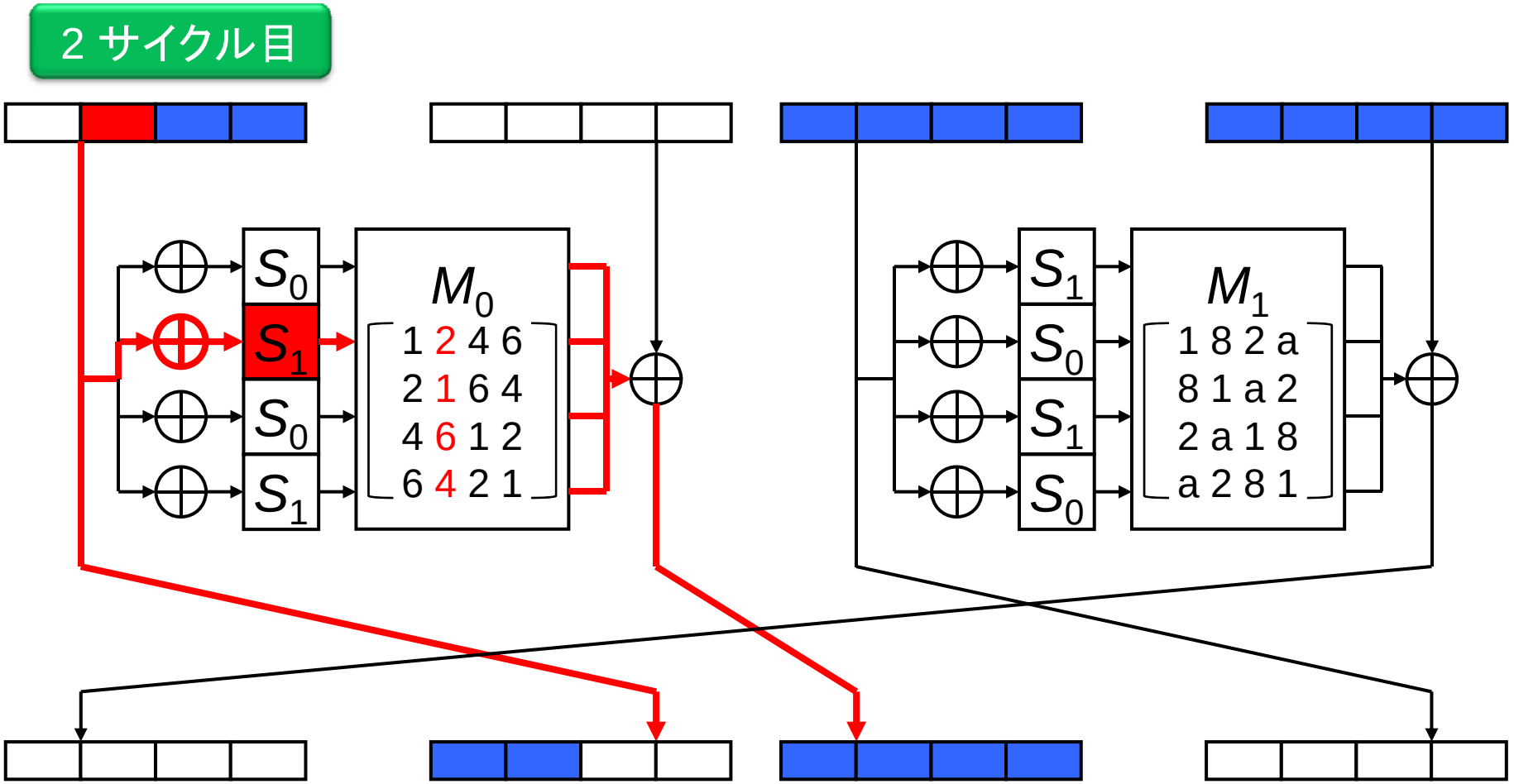
1 ラウンドを 8 サイクルで実行



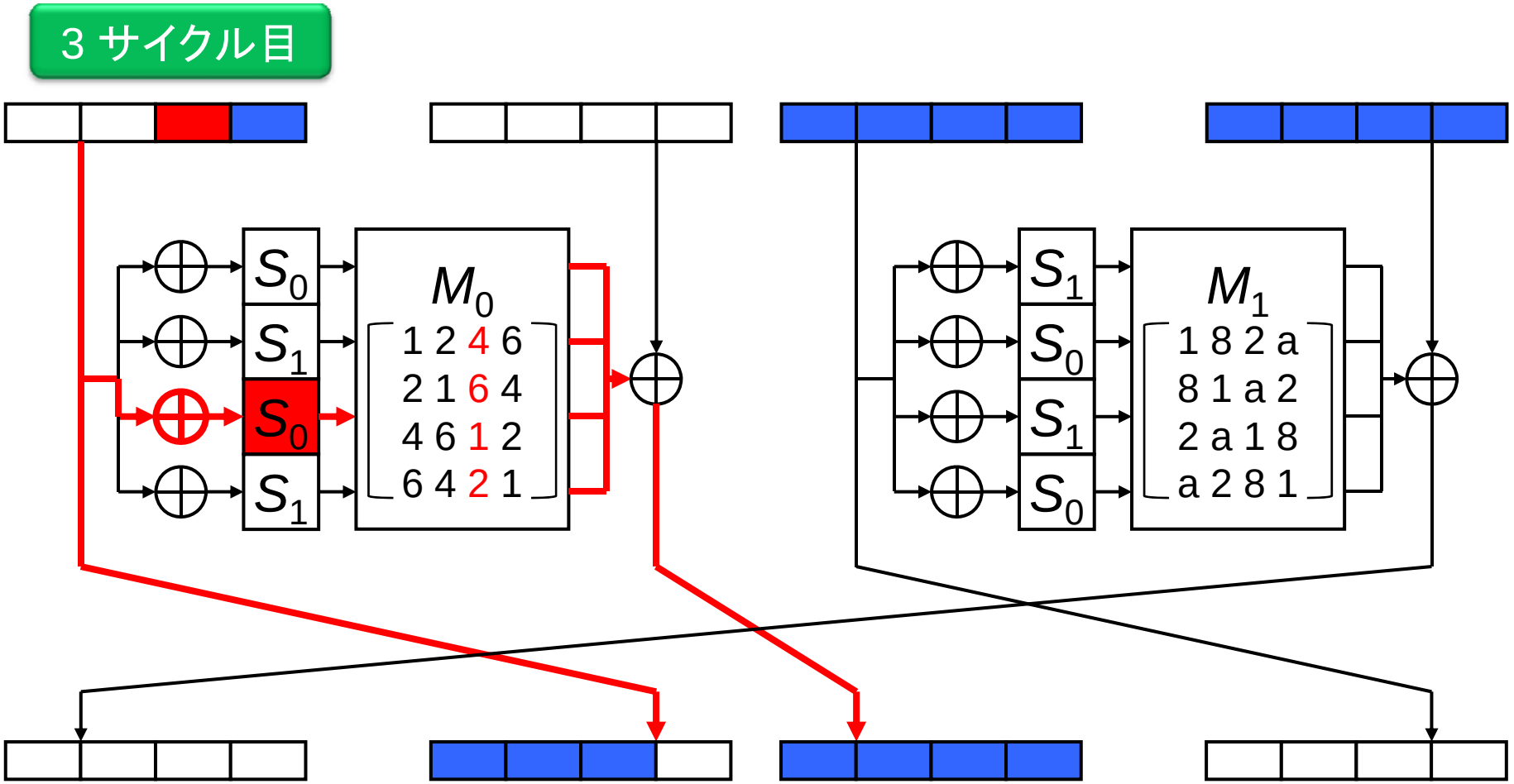
CLEFIA 暗号化実装



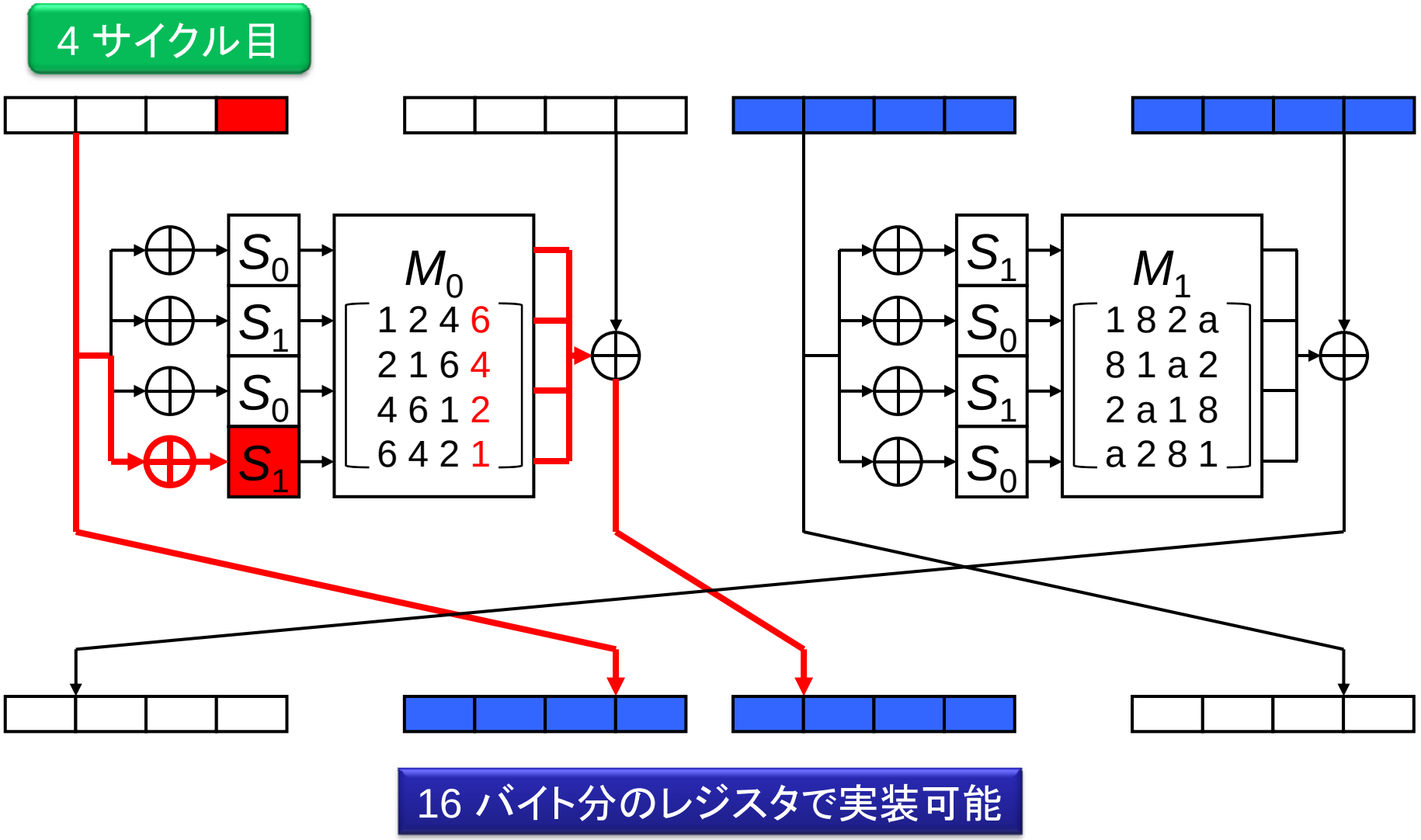
CLEFIA 暗号化実装



CLEFIA 暗号化実装

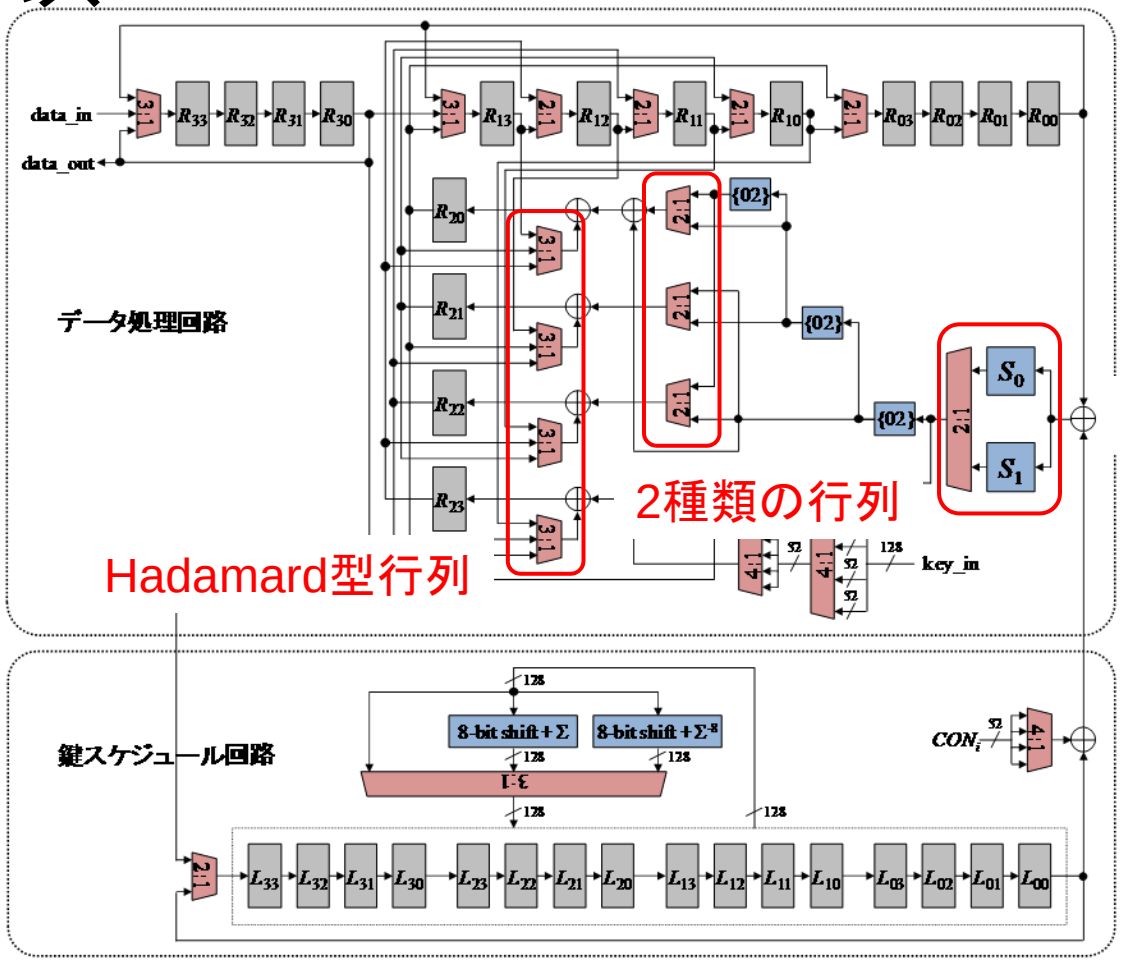


CLEFIA 暗号化実装

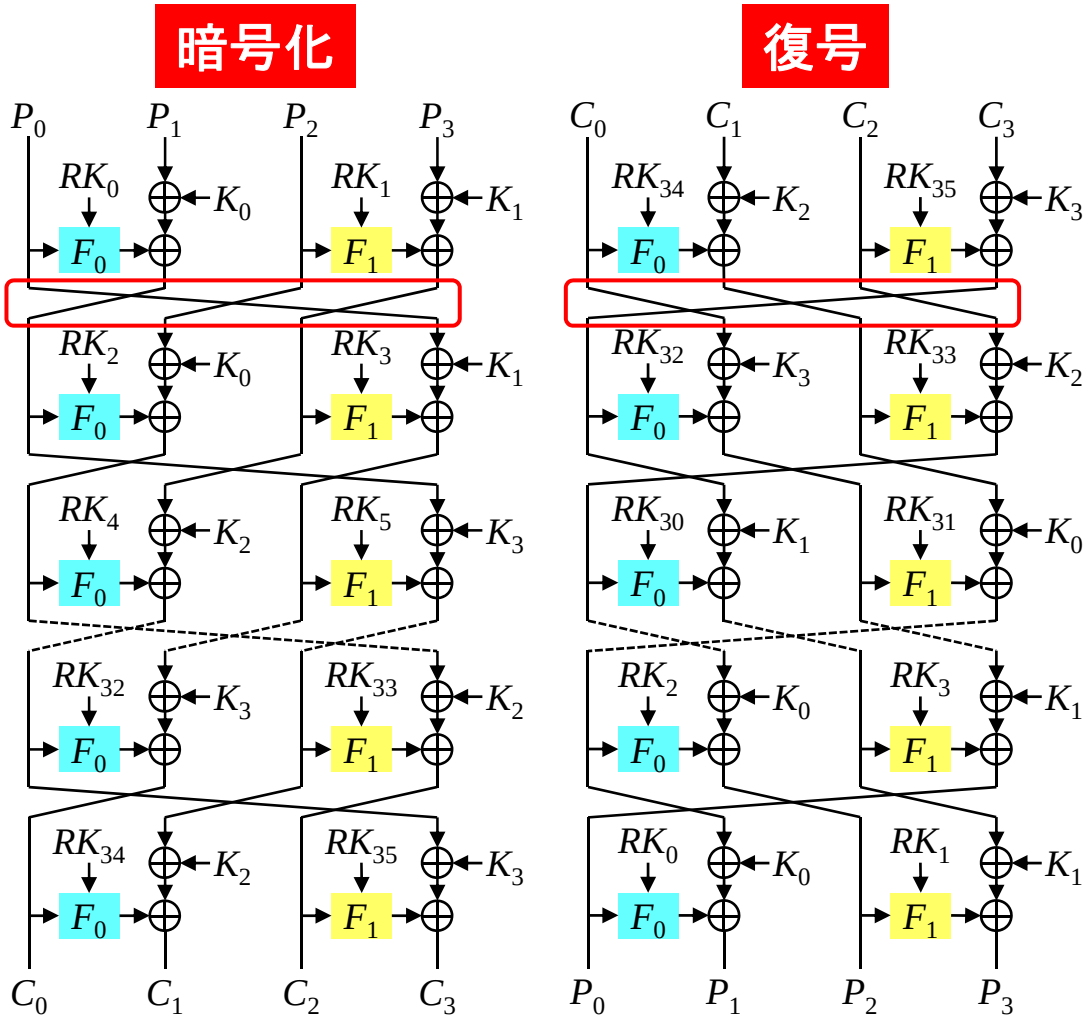


CLEFIA シリアル暗号化実装

- データパス



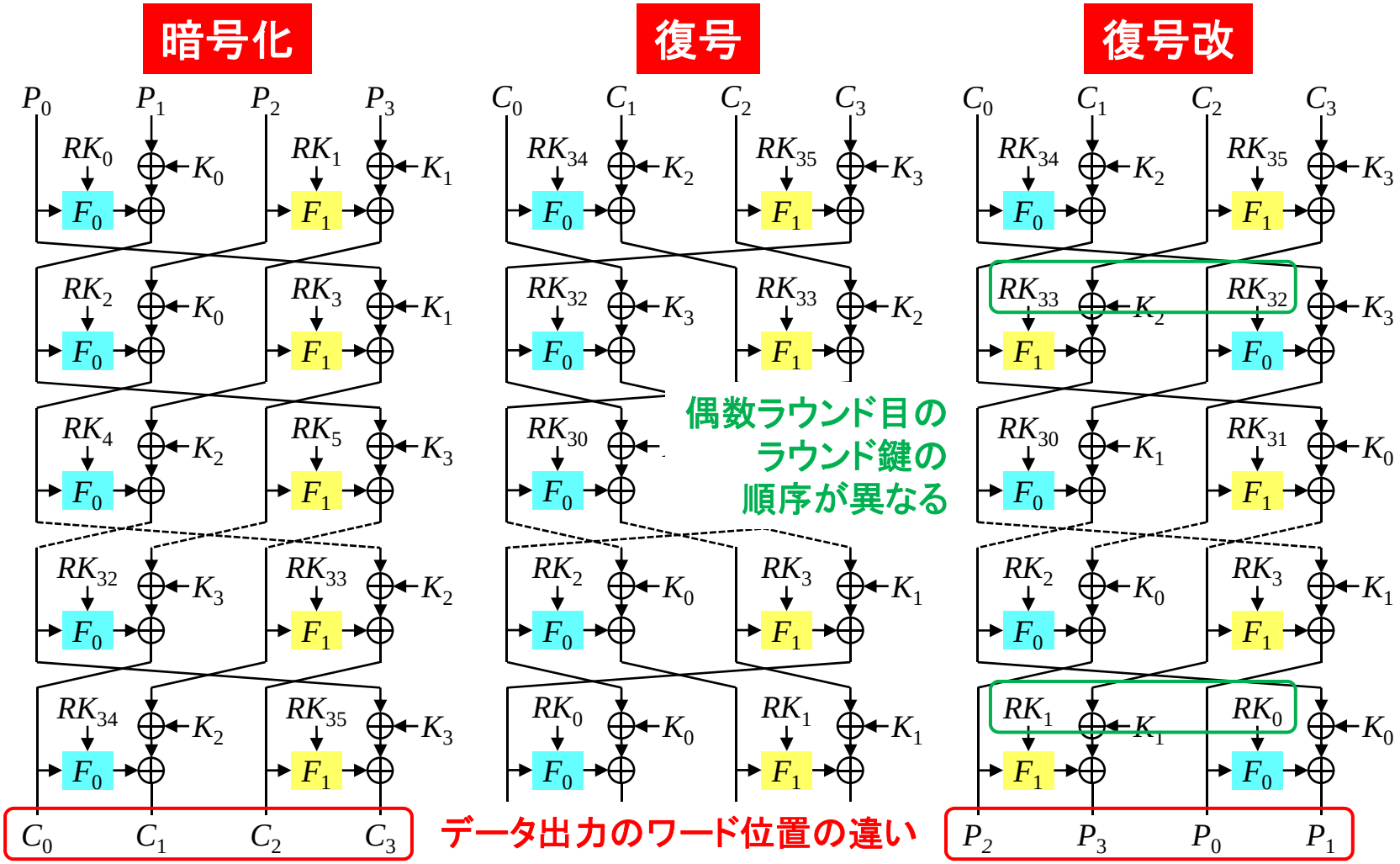
CLEFIA シリアル暗復号実装



ワード巡回方向が異なるため
セレクタの増加が見込まれる

復号の偶数ラウンド目の
F_0 と F_1 の配置を入れ替えると

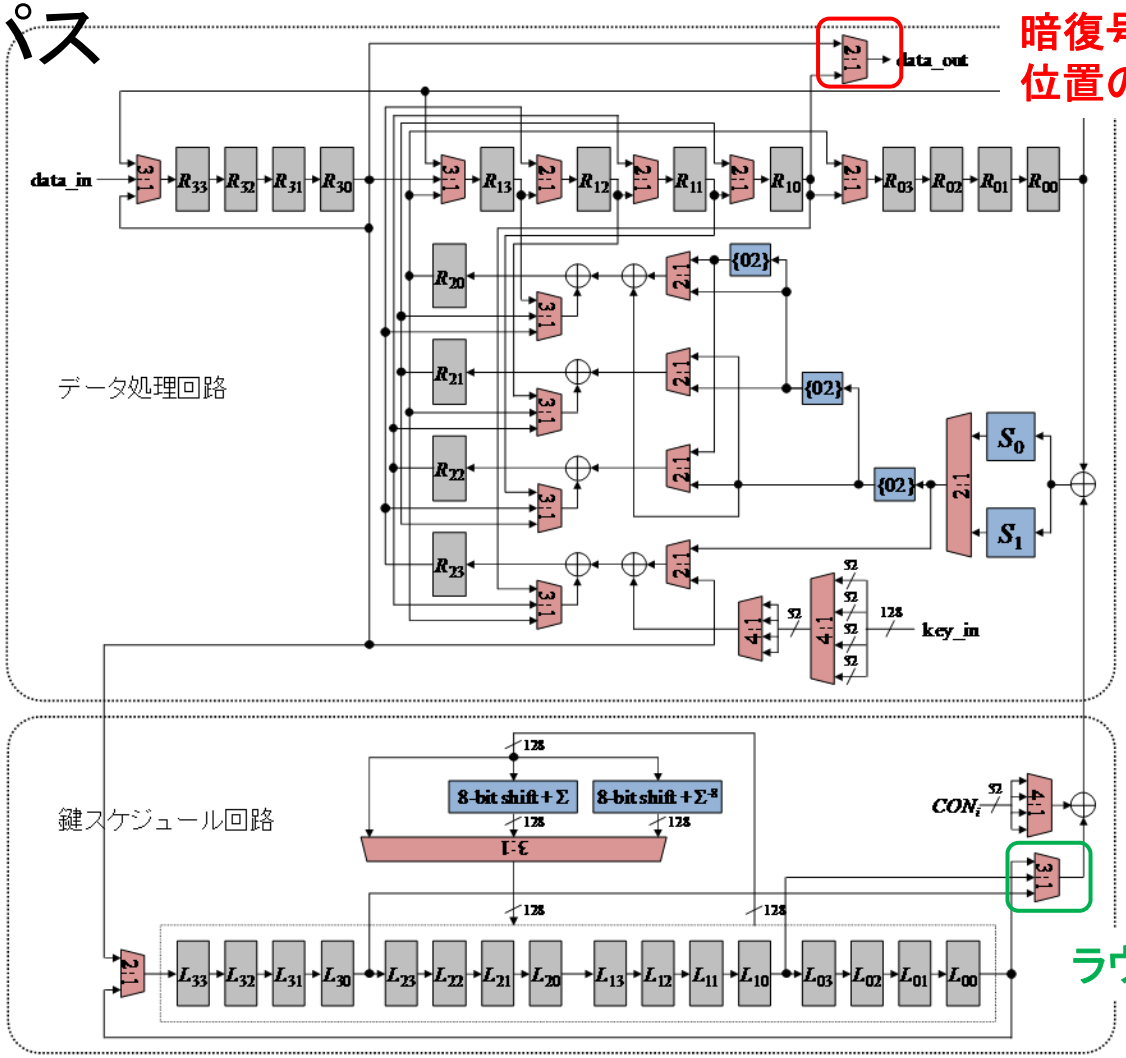
CLEFIA シリアル暗復号実装



ワード巡回方向が同じ方向となり，データパスに大きな変更の必要なし

CLEFIA シリアル暗復号実装

- データパス



実装環境

記述言語	Verilog-VHDL
シミュレータ	VCS ver.2006.06
論理合成ツール	Design Compiler ver.2007.03-SP3
設計ライブラリ	0.13um CMOS 標準セルライブラリ
	1 GE = 2-way NAND, 最悪条件

実装性能評価

アルゴリズム	モード	アーキテクチャ	サイクル	ゲート (GE)	周波数 (MHz)	速度 (Mbps)	プロセス (um)
CLEFIA	enc	8 ビット シフトレジスタ	176	2,893	67	49	0.13
	enc/dec	8 ビット シフトレジスタ	176	2,996	61	44	0.13
CLEFIA	enc/dec	32 ビット	38	4,950	201	677	0.09
AES	enc	8 ビット シフトレジスタ	177	3,100	152	110	0.13
AES	enc/dec	8 ビット RAM	1,032	3,400	90	10	0.35

※ サイクルは入出力に必要なサイクル数を含む

まとめ

- 128 ビットブロック暗号 CLEFIA のハードウェア実装の更なる小型化を目指して，8 ビット・シリアルアーキテクチャに基づいた実装を行なった
- 128 ビット鍵 CLEFIA の実装評価結果
  - 暗号化のみ　　2,893 GE
  - 暗復号　　2,996 GE
    - 既存の CLEFIA の最小値に対して 39% の小型化を実現
    - AES より小さなゲート規模を実現

CLEFIA のハードウェア実装における小型実装性能を示す結果が得られた

ご清聴ありがとうございました

CLEFIA