ハードウェア向けストリーム暗号 *Enocoro*-128v2

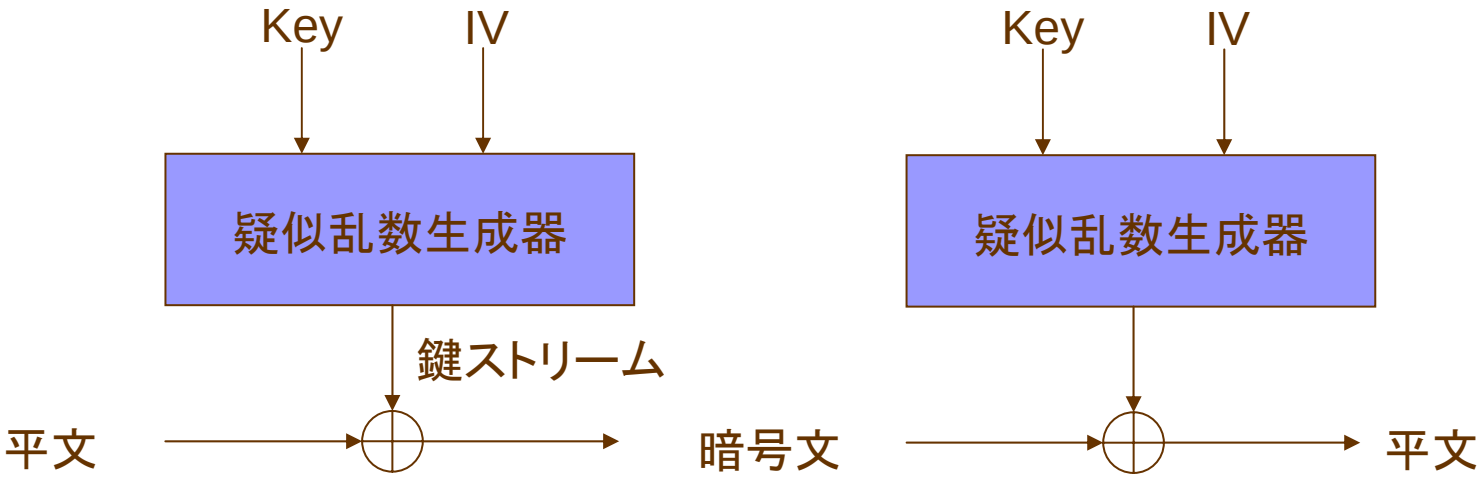
（株）日立製作所
システム開発研究所

概要

- ストリーム暗号とは
- *Enocoro*-128v2の仕様
- 安全性と実装に関する結果
- まとめ

ストリーム暗号

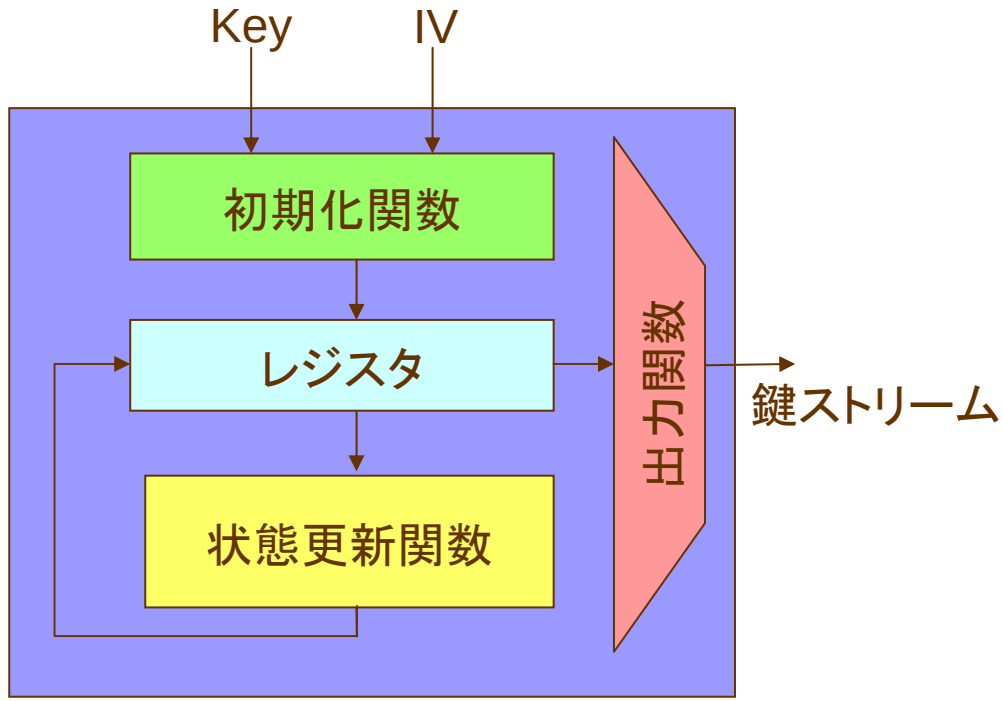
ストリーム暗号とは



- バーナム暗号に端を発する暗号化方式
  - 平文と鍵ストリームを排他的論理和することで暗号化／復号
  - 鍵ストリームは疑似乱数生成器と呼ばれる決定性アルゴリズムで生成
  - ストリーム暗号の安全性＝疑似乱数生成器の安全性

疑似乱数生成器

- 入力
  - 秘密鍵
  - 初期ベクトル(IV):
    公開値
- 出力
  - 長いビット列
  - 高い乱数性を満たす
  - 鍵情報を漏らさない



ストリーム暗号の安全性要件

- ストリーム暗号の安全性
  - 疑似乱数生成器の安全性に帰着
- 鍵復元の困難性
  - 疑似乱数生成器は秘密鍵に関する情報を漏らしてはならない
  - 攻撃者モデル
    - 出力列の(非)乱数性のみを利用する攻撃
    - 初期化の脆弱性を利用する攻撃
- 出力列の乱数性
  - 攻撃＝さまざまな方法で乱数性テストを実施
  - 攻撃者は秘密鍵を復元する必要なし

タイムメモリデータトレードオフ攻撃

- ストリーム暗号に対する汎用的な攻撃
  - BabbageとGolićが提案
    - ブロック暗号に対するTMTOと同じく事前計算が必要
  - 攻撃コストのトレードオフ
    - メモリ (事前計算結果の保存用)
    - 時間 (オンライン処理に必要な時間)
    - データ (攻撃時に入手可能なデータ量)
  - ストリーム暗号に特有の結論
    - 内部状態のサイズが鍵長の2倍未満であれば、ストリーム暗号はTMDTOに対して十分な安全性を達成できない

Enocoro-128v2の仕様

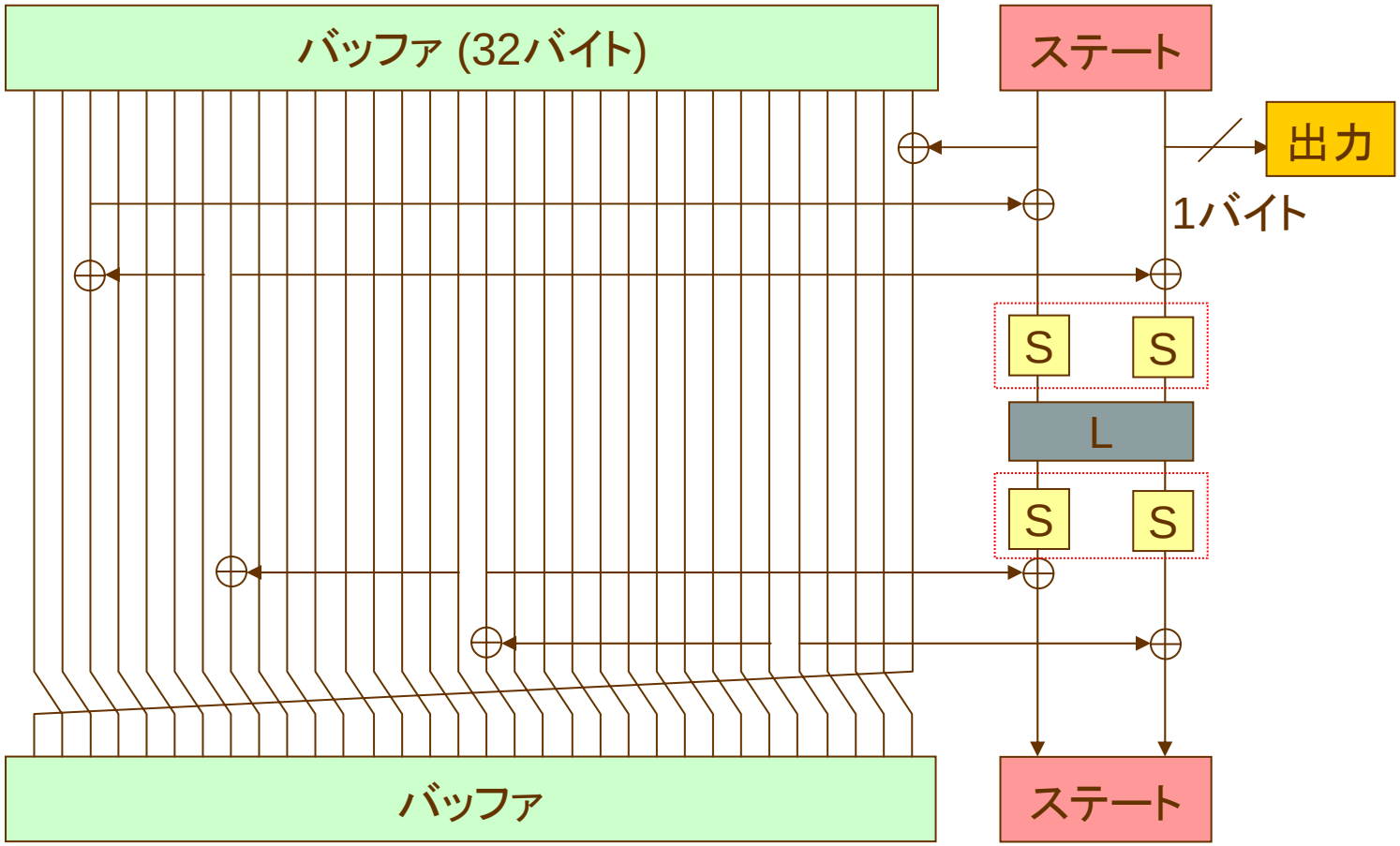
light-weight暗号の開発方針

- eSTREAM Profile-2
  - ハードウェア向け軽量暗号（鍵長80ビット）
  - 最終リスト(portfolio)に掲載されたアルゴリズムはビット単位の演算を採用
- バイト単位処理演算の利点
  - MUGIの開発での実績
    - ソフトウェア／ハードウェアいずれのプラットフォームでも高速
    - AESなど最新のブロック暗号に対する安全性評価技術を比較的容易に適用可能

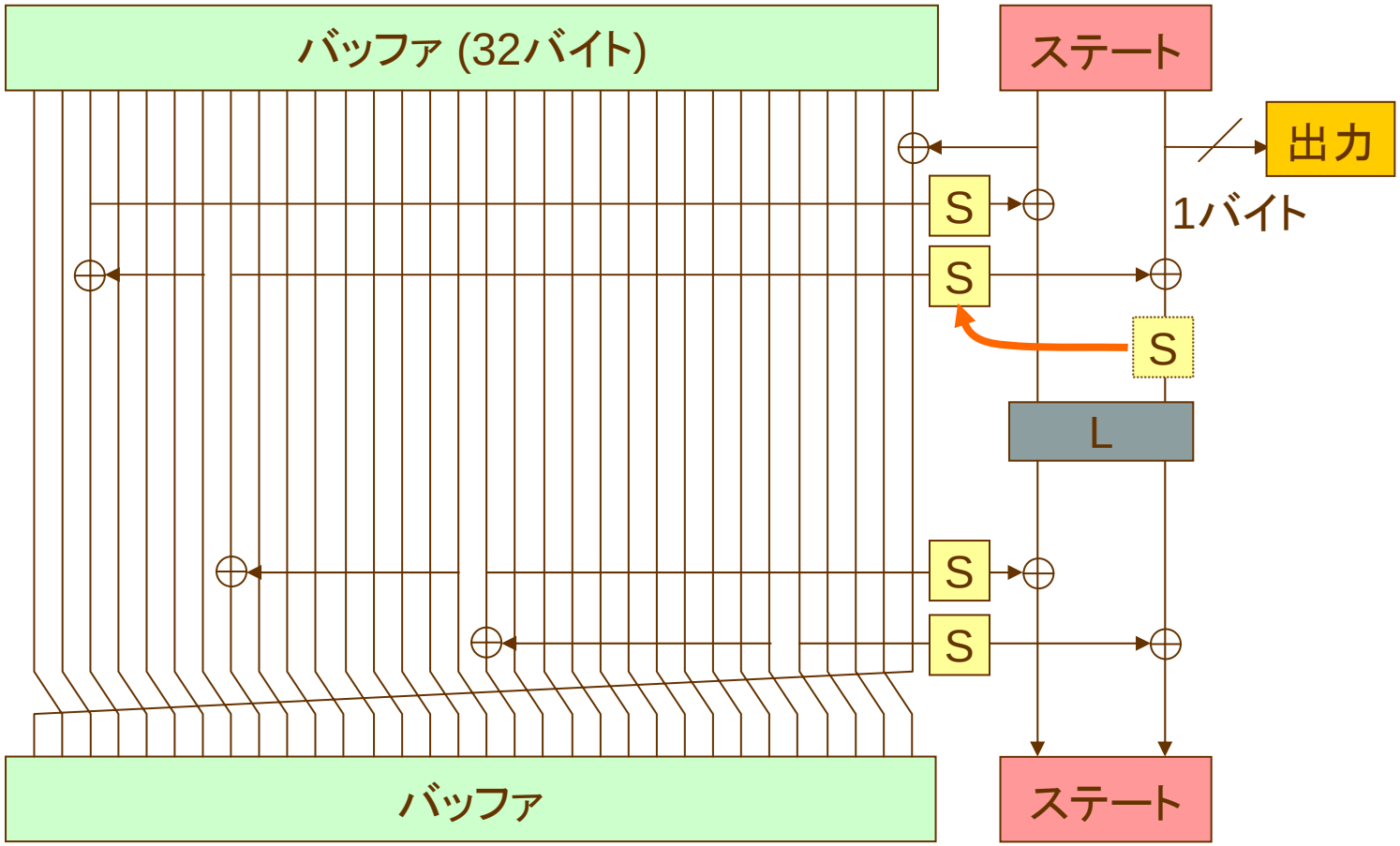
Enocoro-128v2の特徴

- 入出力
  - 鍵長: 128ビット
  - IV長: 64ビット
  - 出力
    - 1バイト／ラウンド
    - （鍵、IV）の組毎に2^{64}バイト以下
- 処理構造
  - 内部状態：272ビット
    - CRYPTREC推奨暗号のMUGI, Panama (MULTI-S01の疑似乱数生成エンジン)に比べて小型
  - バイト単位処理の演算で構成

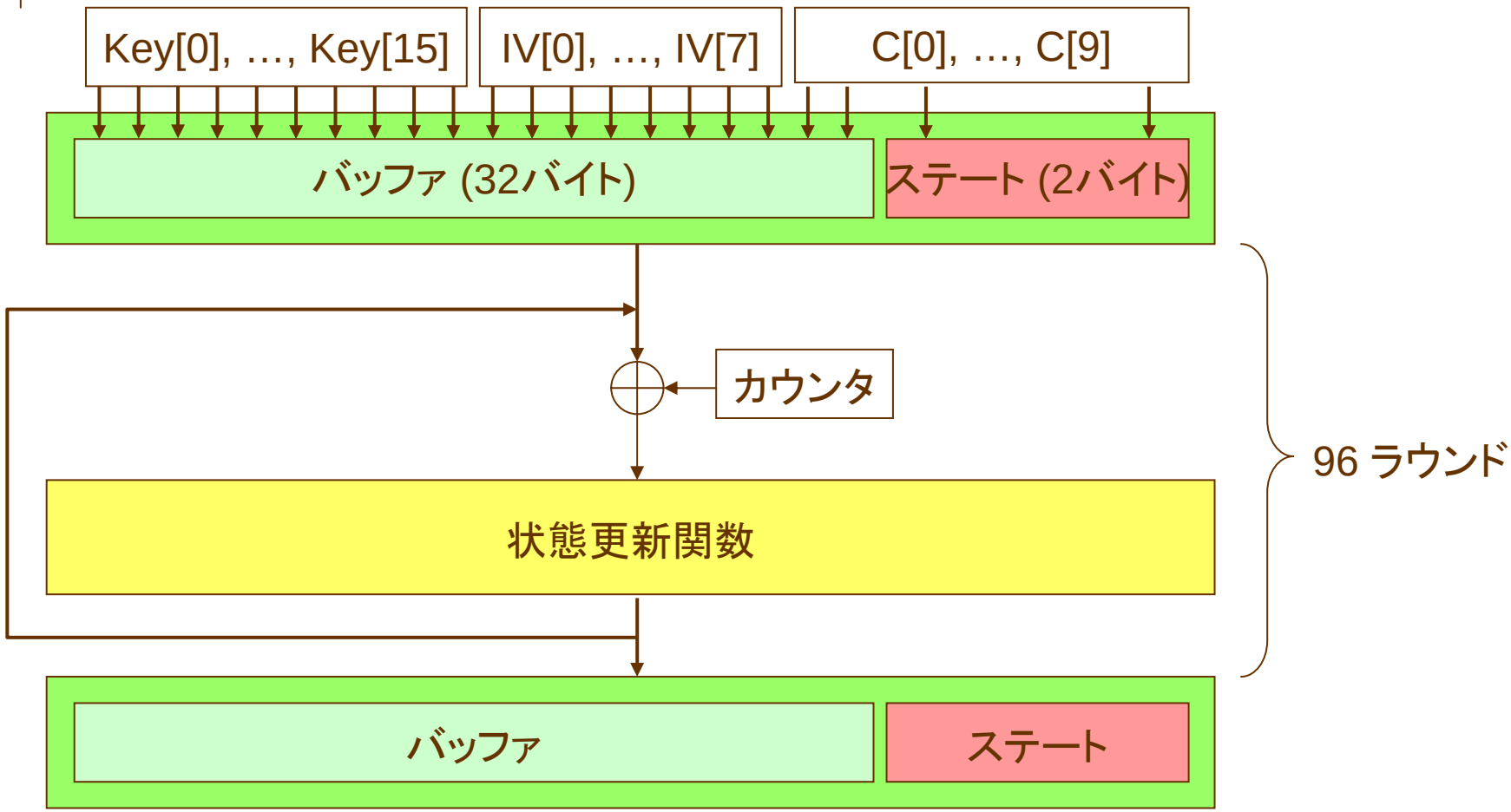
状態更新関数: 基本的なアイデア



状態更新関数: 並列化手法



初期化関数



要素関数

- 8ビットSbox S_8 (非線形置換)
  - 4つの4ビットSbox S_4とGF(2^4)上の2x2行列からSPS構成で合成
  - MDP=$2^{-4.678}$, MLP=2^{-4}, Alg. deg.=6
- 線形変換 *L*
  - GF(2^8)上の2x2行列
  - 分岐数=3

安全性と実装に関する結果

安全性評価に関する結果の一覧

Brute force	鍵の総当り	2^{128}
	TMDTO攻撃	2^{136}
	推測決定攻撃	2^{144}
乱数識別攻撃	線形相関	$\geq 2^{144}$
再同期攻撃	差分攻撃	$\geq 2^{140.3}$
	線形攻撃	$\geq 2^{177.8}$

- いずれの攻撃に対しても、128ビットのセキュリティレベルを達成

ハードウェア実装

アルゴリズム	最大動作 周波数 (MHz)	スループット (Mbps)	回路規模 (K gate)	プロセス (μm)
Grain-128	925.9	926	1.9	0.13
	581.4	4,651	2.5	
Mickey 2.0	413.2	413	5.0	
Enocoro-128v2	**440.0**	**3,520**	**4.1**	**0.09**
MUGI	51.1	1,600	22.7	0.18
	186.2	11,900	46.0	0.18
AES	131.2	311	5.4	0.11
	80.0	10	3.4	0.35

Enocoro-128v2以外の実装結果は以下の文献から引用。
T.Good and M.Benaissa, ``Hardware performance of eStream phase-III stream cipher candidates,'' in SASC 2008 Proceedings, February 13-14, 2008.

ソフトウェア実装

アルゴリズム	スループット (cycles/byte)	初期化 (cycles)
Grain-128	31.2	1137.5
Mickey-128 2.0	1231.4	56592.1
Enocoro-128v2	**46.3**	**4869.5**
AES-CTR	17.8	469.6
SNOW 2.0	5.0	1086.0

Enocoro-128v2以外の結果は以下のサイトから引用。
http://www.ecrypt.eu.org/stream/phase3perf/2007a/pentium-4-a/
(revision 206).

まとめ

- 新しいストリーム暗号*Enocoro*-128v2を提案
  - バイト単位処理演算で構成
  - 高い安全性
  - ハードウェア実装における高いパフォーマンス
  - ソフトウェア実装でも実用レベルの処理速度を達成