応募暗号技術の安全性評価について 2
ストリーム暗号
Enocoro-128v2

CRYPTREC
Cryptography Research and Evaluation Committees

公募の目的（公募要項P.4 第5.1節抜粋）

・策定から5年以上が経過し、解析・攻撃技術の高度化及び暗号技術の開発が進展している

・安全性評価のみならず危殆化及び移行対策を含めた適切な暗号選択の支援への要望

・導入コスト、相互運用性、普及度合いなどの評価観点の必要性の指摘

・リストの改訂に必要な技術の追加

CRYPTREC
Cryptography Research and Evaluation Committees

応募暗号に関する留意事項(公募要項P.2 第2.2節抜粋)

・2010年9月までに査読付き国際学会に採択されていること

・第三者が全ての機能を実装可能となる情報が開示されていること

・国内外での評価が可能であること

・評価に際しては、知的財産の利用が無償で行えること

・電子政府リスト策定後3年以内に調達可能なこと

CRYPTREC
Cryptography Research and Evaluation Committees

ストリーム暗号の応募状況及び評価対象

応募暗号技術　2件	
・Enocoro-128v2	株式会社日立製作所
・Kcipher-2	KDDI株式会社
現行リスト掲載　3件	
・MUGI	株式会社日立製作所
・MULTI-S01	株式会社日立製作所
・128-bit RC4	事務局提案 （現行リストの注釈5では、SSL3.0/TLS1.xでの利用に限定している。）

CRYPTREC
Cryptography Research and Evaluation Committees

安全性評価の観点(1/3)　評価項目

（公募要項からの抜粋）

共通鍵暗号については、現リストに掲載されている暗号技術と比較して安全性又は 実装性において優れた暗号技術を公募します。そのため、評価においても現リストに 掲載された暗号に対する優位点の評価を行います。

（1） 安全性評価項目

暗号は守秘目的以外にも利用されるので、いわゆる暗号文単独攻撃以外の既知平文攻撃、(適応的)選択平文・暗号文攻撃、関連鍵攻撃、選択IV攻撃等、攻撃者にとって非常に都合のよい環境での耐性も評価します。

イ. ストリーム暗号に関する評価項目

time/memory/data-tradeoffや分割統治攻撃、相関攻撃、またGroebner基底計算アルゴリズムを元にした代数攻撃等の既知の攻撃法に対する耐性を評価します。また、応募暗号に特化した攻撃法や、ヒューリスティックな安全性の根拠も評価の対象とすることがあります。その他、サイドチャネル攻撃等に対する耐性についても評価します。

安全性評価の観点(2/3)　評価項目

- Time-Memory-Data Tradeoff 攻撃
- 分割統治攻撃
- 相関攻撃
- 代数的攻撃
- 推測決定攻撃
- 識別攻撃
- 関連鍵攻撃
- 統計的性質
- 応募暗号に特化した攻撃

CRYPTREC
Cryptography Research and Evaluation Committees

安全性評価の観点(3/3)　～評価のポイント～

・鍵に対する全数探索よりも効果的な攻撃手法が発見されないこと

2^{128}の計算量を下回る攻撃手法がないこと
現行リストにおいては、2^{100}の計算量で評価

・現行リスト掲載の暗号技術よりも安全性/実装性で優位であること
・応募暗号に特化した攻撃手法及びヒューリスティックな安全性の根拠も加味

CRYPTREC
Cryptography Research and Evaluation Committees

Enocoro-128v2 の概要(1/3)

- Enocoroの初期版(Enocoro-80v1)は、2007年に発表されたストリーム暗号向けの擬似乱数生成器(ストリーム暗号)である。なお、Enocoro-128v2仕様については、ISITA2010で発表されている。

- 128ビットの鍵、64ビットの初期値(IV) を入力として、最大 2^{64} バイトの鍵ストリームを生成する。

- 内部状態は、272ビット(34バイト)あり、PANAMA型と呼ばれる構造を持つ。

CRYPTREC
Cryptography Research and Evaluation Committees

Enocoro-128v2 の概要(2/3)

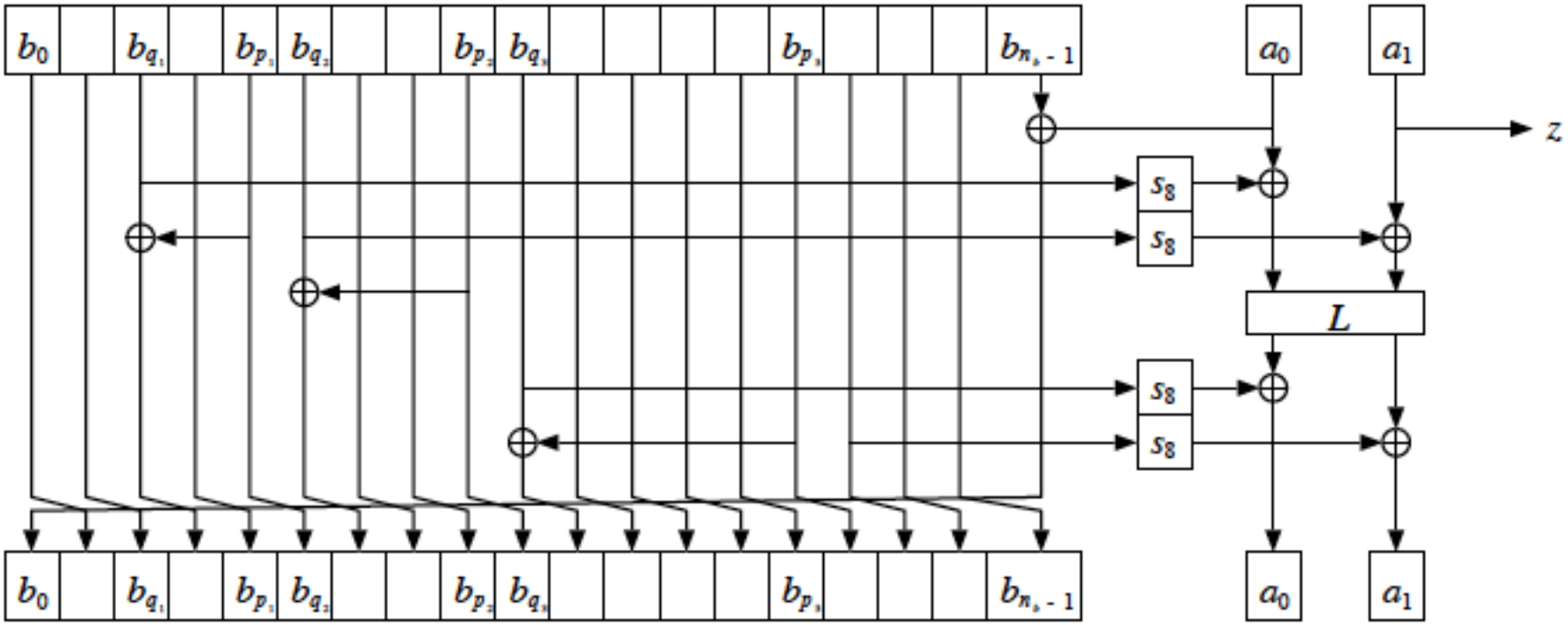

図1:内部状態の更新
(応募書類からの抜粋)

CRYPTREC
Cryptography Research and Evaluation Committees

Enocoro-128v2 の概要(3/3)

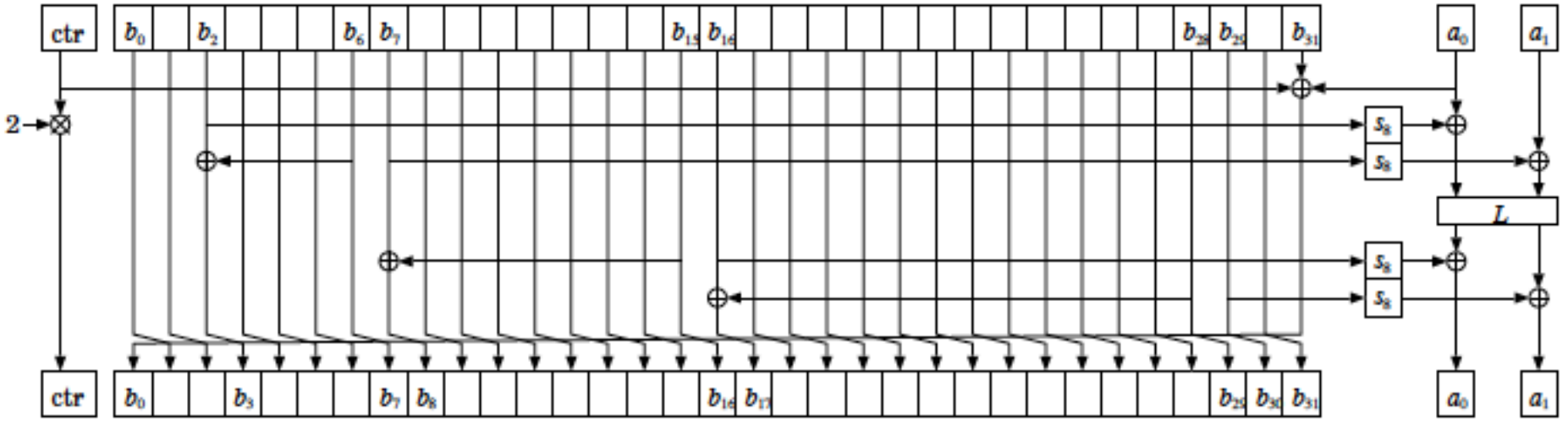

図2：初期化における内部状態の更新(96ラウンド)
（応募書類からの抜粋）

CRYPTREC
Cryptography Research and Evaluation Committees

Enocoro-128v2の安全性評価について(1/5)

- 自己評価書における安全性評価の記載事項
  - Time-Memory-Trade-Off攻撃
  - 推測決定攻撃
  - 分割統治攻撃
  - 代数的な攻撃
  - 出力列の線形相関を利用した乱数識別攻撃
  - 初期化の安全性(乱数との識別、秘密鍵の復元)
    - 差分攻撃
    - 線形攻撃
  - 関連鍵攻撃モデルにおける弱鍵の探索

Enocoro-128v2の安全性評価について(2/5)

- タイム-メモリ-データ-トレード-オフ攻撃(TMDTO 攻撃)
  - Enocoroは内部状態272 ビット、鍵サイズ128 ビットある。TMDTO攻撃に関しては、Babbage-Golić及びBiryukov-Shamirにより改良版が提案されているが、現時点において、特に問題点は認められなかった。

- 推測決定攻撃
  - 計算量が2^{152} を下回るものは見つからなかったので、現時点においては、特に問題点は認められない。

CRYPTREC
Cryptography Research and Evaluation Committees

Enocoro-128v2の安全性評価について(3/5)

- 分割統治攻撃
  - Enocoroの内部状態は、ステート a(t) とバッファー b(t) からなる。状態更新関数は、それぞれ ρ と λ という2つの関数からなる。どちらの関数にも、a(t) と b(t)の両方が入力されるので、分割統治攻撃を適用することは困難であると考えられる。

- 識別攻撃
  - 乱数との識別性については、偏差が2^{-180} が上回るものは見つからなかったので、現時点においては、特に問題点は認められない。

CRYPTREC
Cryptography Research and Evaluation Committees

Enocoro-128v2の安全性評価について(4/5)

- 線形攻撃
  - s_8の最大線形確率$p = 2^{-4}$なので、active S-Box の最小数が32以上になると攻撃に対して安全と考えられる。条件付きで探索した結果、最大差分特性確率が2^{-128}を上回るものは得られなかったので、 現時点においては、特に問題点は認められない。

- 差分攻撃
  - s_8の最大差分確率$p = 2^{-4.678}$なので、active S-Box の最小数が28以上になると攻撃に対して安全と考えられる。条件付きで探索した結果、最大差分特性確率が2^{-128}を上回るものは得られなかったので、現時点においては、特に問題点は認められない。
    - 選択IV攻撃については、現時点においては、特に問題点は認められない。
    - 関連鍵攻撃については、現時点においては、特に問題点は認められない。

CRYPTREC
Cryptography Research and Evaluation Committees

Enocoro-128v2の安全性評価について(5/5)

- その他
  - Maximum Degree Monimial Test については、現時点においては、特に問題点は認められない。
  - 統計的性質については、現時点においては、特に問題点は認められない。

評価のまとめ(事務局案)

現時点において、特に安全性に問題点は
認められなかった。

今後の取り扱い ⇒ **評価の継続**

CRYPTREC
Cryptography Research and Evaluation Committees