応募暗号技術の安全性評価について1
128ビットブロック暗号
CLEFIA

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

128ビットブロック暗号応募状況及び評価対象

応募技術　2件　(第1次評価対象)

- CLEFIA　　ソニー株式会社
- HyRAL　　株式会社ローレルインテリジェントシステムズ

現リスト技術　5件

- AES　　事務局提案
- Camellia　　日本電信電話株式会社
- CIPHERUNICORN-A　日本電気株式会社
- Hierocrypt-3　　株式会社東芝
- SC2000　　富士通株式会社

CRYPTREC
Cryptography Research and Evaluation Committees

安全性評価の観点　評価項目

・差分攻撃/線形攻撃

S-box単位で差分/線形確率を計算。差分/線形パス上に含まれるactive S-box数から特性的確率を見積もる。

→　**不能差分攻撃へ拡大**

・高階差分攻撃(飽和攻撃)

S-box等非線形関数の代数次数を計算。非線形関数部の繰り返し回数から代数次数を見積もる。

→　**補間攻撃/代数的攻撃へ拡大**

・関連鍵攻撃/弱鍵

鍵処理部が生成する拡大鍵の特徴の解析。

CRYPTREC
Cryptography Research and Evaluation Committees

安全性評価の観点　～評価のポイント～

・現電子政府推奨リストは2^{100}の計算量で評価

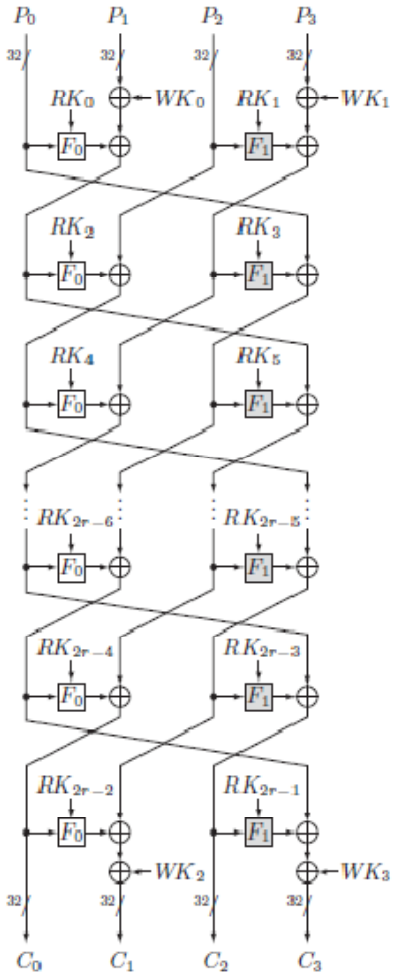
2^{128}の計算量を下回る攻撃手法がないこと

・現電子政府推奨リストよりも安全性/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

CLEFIA　ソニー株式会社



データ処理部
暗号化処理

CLEFIAの特徴

・4系列Type2一般化Feistel構造

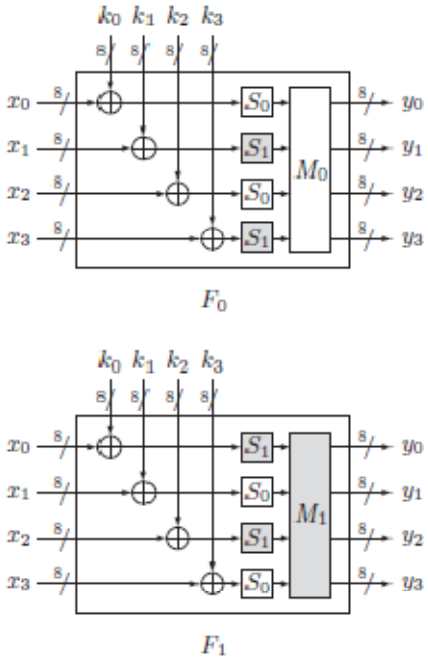
- 128ビット鍵　→　18ラウンド
- 192ビット鍵　→　22ラウンド
- 256ビット鍵　→　26ラウンド

・詳細な自己評価書

・高い小型実装性能(今回の評価対象外)

CRYPTREC
Cryptography Research and Evaluation Committees

データ処理部の安全性評価



F関数の構成
(S_0, S_1の2種類のS-box)

・差分/線形攻撃に対する**自己評価のupdate**

- 2種類のS-boxの特性を加味
- Viterbi法によるパスの探索

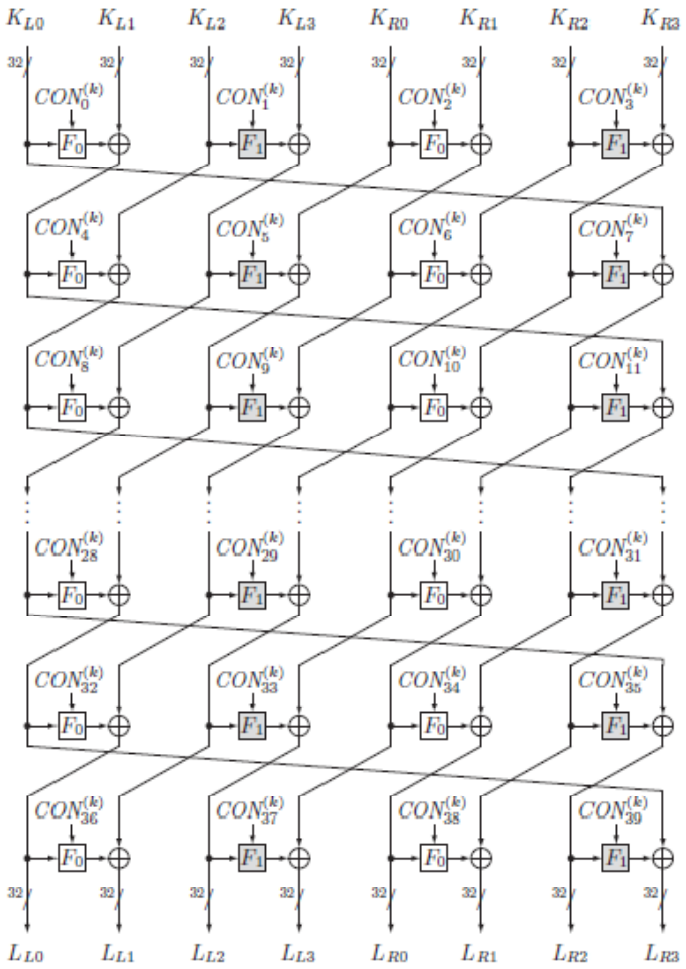
	差分特性確率	線形特性確率
128	$2^{-205.48} \rightarrow \mathbf{2^{-227.42}}$	$2^{-201.48} \rightarrow \mathbf{2^{-222.54}}$
192	$2^{-256.85} \rightarrow \mathbf{2^{-282.78}}$	$2^{-240.90} \rightarrow \mathbf{2^{-277.38}}$
256	$2^{-303.55} \rightarrow \mathbf{2^{-338.46}}$	$2^{-289.08} \rightarrow \mathbf{2^{-331.38}}$

・バランス特性を用いた高階差分特性

10段が攻撃可能(自己評価書)
→より少ない選択平文組数/計算量で攻撃可能
仕様構成に対する安全性に影響なし

CRYPTREC
Cryptography Research and Evaluation Committees

鍵処理部の安全性評価



鍵処理部(192/256ビット鍵の場合)

鍵処理部の特徴

- 128ビット鍵 → 4系列12段構成
- 192/256ビット鍵 → 8系列10段構成

・データ処理部と同様の構造
(評価の容易さ)

攻撃に結びついていない特性の発見

192/256ビット鍵の場合フルラウンドに対する32階差分特性の発見

中間鍵Lの逆算により拡大鍵差分を特定できる弱鍵組の存在

CRYPTREC
Cryptography Research and Evaluation Committees

評価のまとめ(事務局案)

自己評価書、国際的な学会発表を含め安全性評価が充実

2^{128}の計算量を下回る攻撃手法が発見されていない

今後の取り扱い → **評価の継続**

CRYPTREC
Cryptography Research and Evaluation Committees