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
HyRAL

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

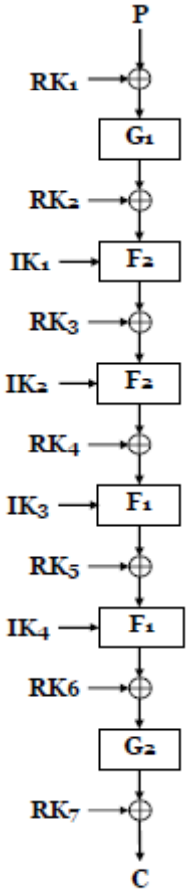
2^{128}の計算量を下回る攻撃手法がないこと

・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

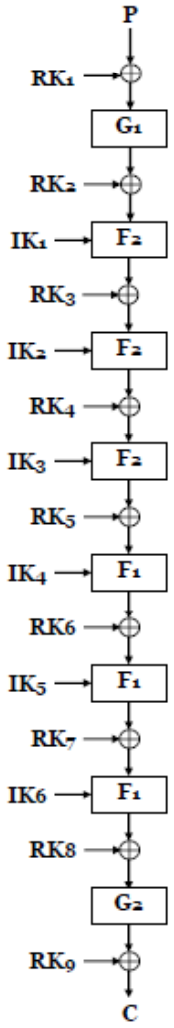
・応募暗号に特化した攻撃手法及びヒューリスティックな安全性の根拠も加味

CRYPTREC
Cryptography Research and Evaluation Committees

HyRAL　株式会社ローレルインテリジェントシステムズ



128ビット鍵



データ処理部
暗号化処理　129ビット鍵以上

HyRALの特徴

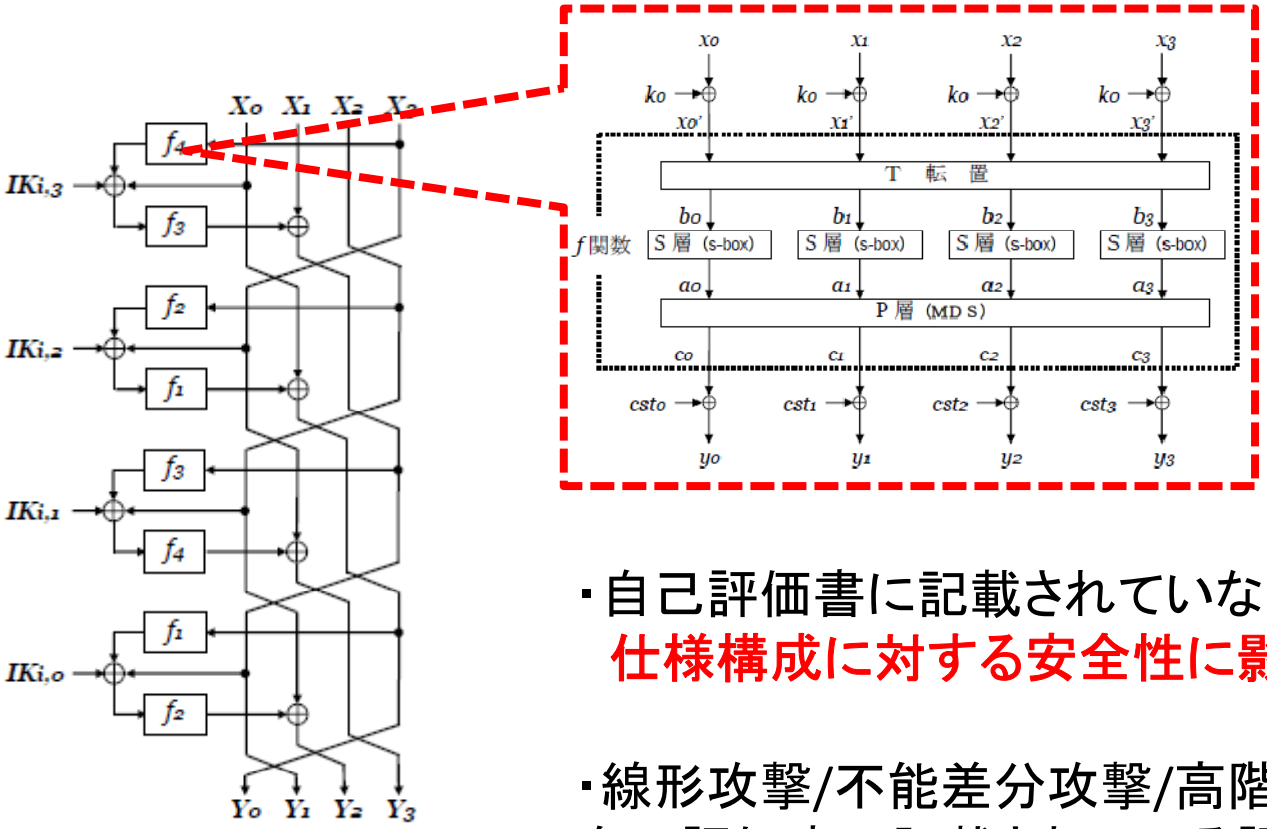
- 鍵長を128～256ビットで設定可能
- 4種類の4ラウンド4系列変形Feistel構造の関数の連結

128ビット鍵	→	24ラウンド
192/256ビット鍵	→	32ラウンド

- 高い安全性の到達を目指す

CRYPTREC
Cryptography Research and Evaluation Committees

データ処理部の安全性評価



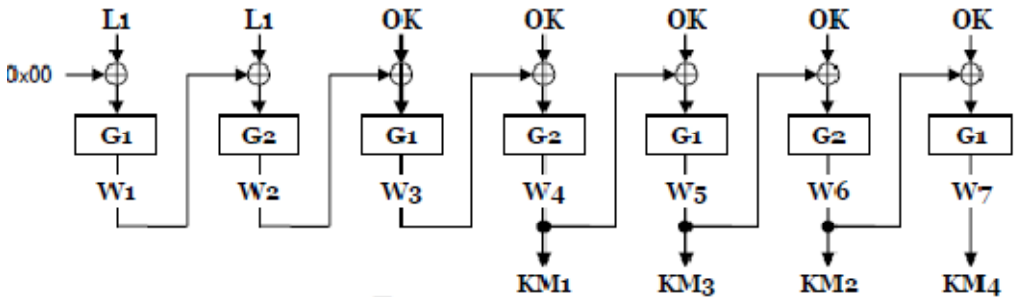
F1関数

・自己評価書に記載されていない差分パスの発見
仕様構成に対する安全性に影響なし

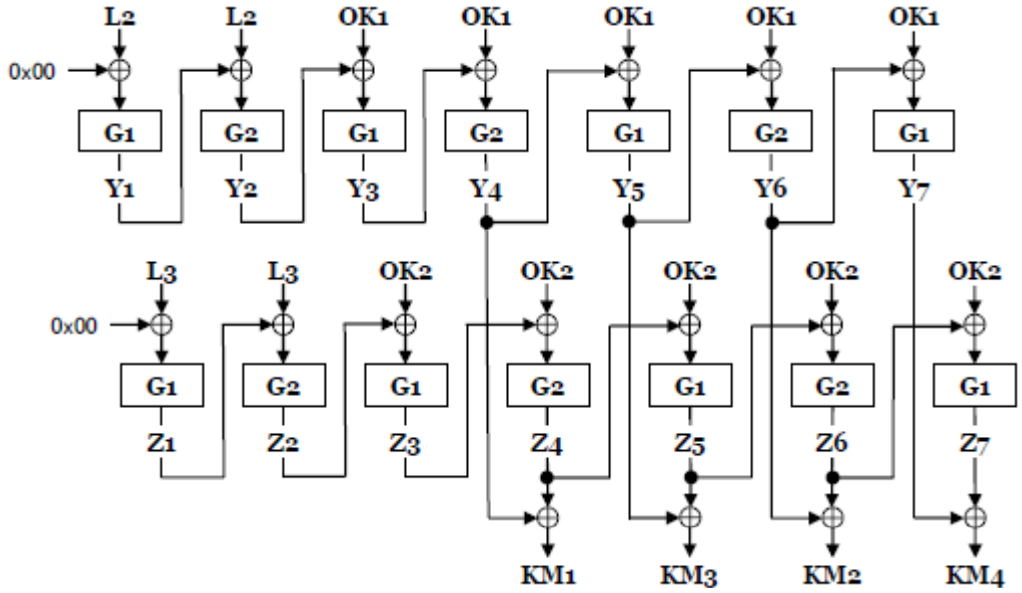
・線形攻撃/不能差分攻撃/高階差分攻撃など、
自己評価書に記載されている評価結果の確認

CRYPTREC
Cryptography Research and Evaluation Committees

鍵処理部の安全性評価



Single key mode
(128ビット鍵)



Double key mode
(129ビット以上の鍵)

CRYPTREC
Cryptography Research and Evaluation Committees

鍵処理部の安全性評価

Double key modeについて

- 差分特性確率が2^{-103}なる差分パスが存在
- 拡大鍵が同じとなる別の鍵　＝　等価鍵
- 差分特性確率を用いると256ビット鍵の場合のみ、2^{50}組の等価鍵が存在
- 等価鍵導出に必要な計算量　＝　$2^{48.8}$

注意

- 128～255ビット鍵に対しては問題が無い
- 2^{256}の鍵空間に対して2^{50}のみの極小数　→　$2^{259.999999\cdots\cdots}$の鍵空間へ縮小

CRYPTREC
Cryptography Research and Evaluation Committees

評価のまとめ(事務局案)

- 128～255ビット鍵に対しては2^{128}の計算量を下回る攻撃手法が発見されていない
- 256ビット鍵に対しては等価鍵が発見

現リスト暗号には発見されていない問題
等価鍵導出が現在の計算機環境で実行可能

今後の取り扱い → **評価の終了**

CRYPTREC
Cryptography Research and Evaluation Committees


CRYPTREC
Cryptography Research and Evaluation Committees