CIPHERUNICORN-A
暗号評価の現状報告
（詳細評価）

平成14年1月28日

共通鍵暗号評価小委員会
委員　神田　雅透

CIPHERUNICORN-A

- 2000年にNECより発表
- 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
- CRYPTREC2000からの継続評価対象暗号
- 特徴
  - Feistel構造(16段) + whitening
  - 「本流部」と「一時鍵生成部」という二重構造を有する段関数
  - 暗号強度評価支援システム(NEC独自開発)によって段関数を設計

CRYPTREC2000評価結果

- 安全性について，今のところ問題は見つかっていない
  - 仕様段数が16段であることを総合的に考慮すれば，現在の理論的な解読技術によって解読することはほぼ不可能と期待される
- 複雑な段関数のため，正確な評価が難しく，継続的な評価が必要
  - 差分解読法や線形解読法を始めとする，理論的な解読技術に対する安全性を正確に評価・解析することは困難である
  - (簡略化した) mF関数を実際のラウンド関数に置き換え，より詳細な評価を行うことが必要である
- 処理速度は遅いグループ
  - CRYPTREC2000継続評価対象128ビットブロック暗号の中では最も遅いグループ (Triple DESと同程度)

評価手順

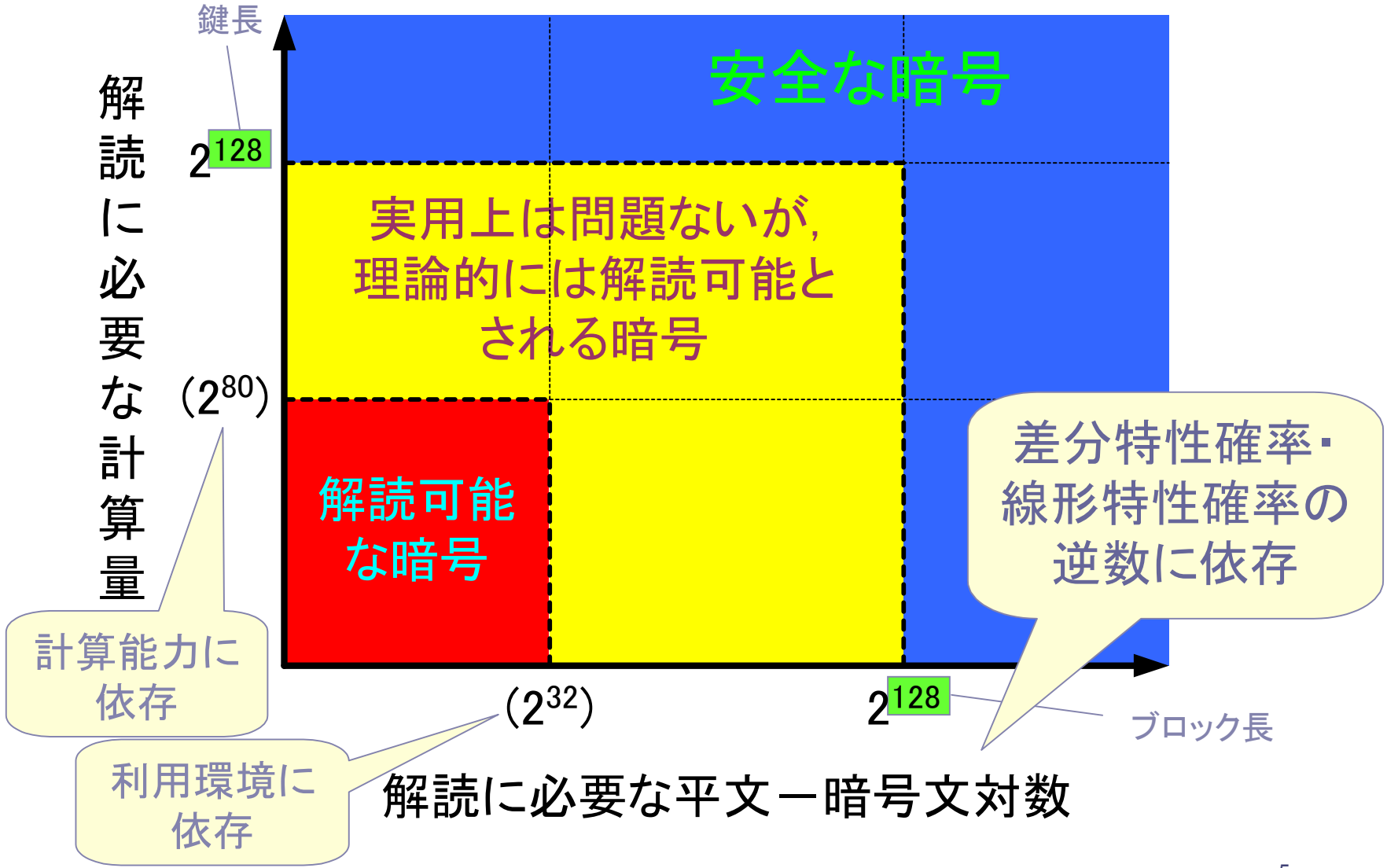
- 詳細評価:

  国内外の4人(チーム)の暗号研究の専門家に以下の観点から評価を依頼

  - mF関数を利用した評価の妥当性
  - 差分特性確率の観点から見た，差分解読法に対する安全性
  - 線形特性確率の観点から見た，線形解読法に対する安全性
  - その他，安全性に関して気がついた点

安全性評価の見方

ブロック長，鍵長
とも128ビット



評価者1のコメント

- 差分解読法，線形解読法に対して安全であると思われる傍証を与える
  - 差分解読法に対する安全性
    - 段関数での特性確率の上界: $\leqq 2^{-21}$
    - 13段での特性確率の上界: $\leqq 2^{-126}$
  - 線形解読法に対する安全性
    - 差分解読法よりは安全であるとは思われる
    - 安全性自己評価が正しいと仮定して，
      - 段関数での特性確率の上界: $\leqq 2^{-13.9}$
      - 13段での特性確率の上界: $\leqq 2^{-83.4}$
    - 安全性自己評価と矛盾する結果が出ている
      - 段関数での線形特性確率の上界が高くなる可能性を否定せず
    - A3関数，定数乗算部，一時鍵生成部の影響をほとんど考慮していない

評価者2のコメント

- 差分解読法，線形解読法に対する安全性に問題があると疑わせるような証拠は見つからなかった
  - 差分解読法に対する安全性
    - A3関数，乗算なし段関数での特性確率の上界: $\leqq 2^{-14.4}$
    - 段関数での特性確率が 2^{-12} を大きく超えるようなものが存在することはありえず，また，A3関数や定数乗算は安全性向上に寄与すると期待される
  - 線形解読法に対する安全性
    - 安全性自己評価の特性確率の上界は誤り
    - mF関数での特性確率の上界: $\leqq 2^{-21.68}$
    - A3関数や定数乗算は安全性向上に寄与すると期待される
- 弱鍵が存在する
  - 32ビット副鍵すべてが秘密鍵の上位32ビットと同一

    { 0x61db99c8, 0x9f3d618, 0x9f3d618, 0x9f3d618, … }

    副鍵の値そのものになる

評価者3のコメント

- 差分解読法に対して安全であると確証するまでには至らなかった
  - 安全性自己評価よりも効率的な差分特性を発見
  - mF関数での特性確率の上界: $\leqq 2^{-7}$
  - 15段での特性確率の上界: $\leqq 2^{-70}$
    (13段での特性確率の上界: $\leqq 2^{-56}$)
  - 上記の結果はバイト単位探索によるものであるため，定数乗算とA3関数の効果を詳細に検討すれば，特性確率（の上界）が変動する可能性がある
- 線形解読法に対して安全であると考えられる
  - 安全性自己評価の特性確率の上界は誤り
  - mF関数での特性確率での上界: $\leqq 2^{-21.37}$
  - 15段での特性確率の上界: $\leqq 2^{-149.58}$
    (13段での特性確率の上界: $\leqq 2^{-128.22}$)

評価者4のコメント

- 差分解読法に対して安全であると思われる傍証を与える
  - 一時鍵生成部の効果を除いたとき（本流部のみ）の段関数での評価
    - 特性確率の上界: $\leqq 2^{-7}$
    - 6段繰り返し表現での特性確率の上界: $\leqq 2^{-56}$
    - 13段での特性確率の上界: $\leqq 2^{-119}$
  - 一時鍵生成部の効果
    - A3関数と逆の特性を有しているため，安全性向上に寄与すると期待される

総評

攻撃法		評価者1	評価者2	評価者3	評価者4
差分解読法	モデル	完全	mF関数	mF関数	本流部 6段繰返
	段関数での 特性確率の上界	$\leqq 2^{-21}$	$\leqq 2^{-14.4}$	$\leqq 2^{-7}$	$\leqq 2^{-7}$
	13段での 特性確率の上界	$\leqq 2^{-126}$	$\leqq 2^{-115}$	$\leqq 2^{-56}$	$\leqq 2^{-119}$
線形解読法	モデル	mF関数	mF関数	mF関数	---
	段関数での 特性確率の上界	$\leqq 2^{-13.9}$ (注釈有)	$\leqq 2^{-21.6}$	$\leqq 2^{-21.3}$	---
	13段での 特性確率の上界	$\leqq 2^{-83.5}$ (注釈有)	$\leqq 2^{-130}$	$\leqq 2^{-128}$	---

注：設計者による評価が正しいと仮定したときの結果

まとめ

- 安全性にする懸念材料が，完全には払拭されるレベルにはない
  - 差分解読法・線形解読法に対して，少なくとも実用上問題が発生する可能性は極めて低い
    - これらの解読法による攻撃はおそらく成功しないだろうという「傍証」が得られている
    - これらの解読法に対して理論的に安全であるという「確証」までは至っていない
  - 非自明と思われる弱鍵の存在が指摘された
    - 全ての副鍵に上位32ビットしか使われないような秘密鍵が少なくとも一つ存在する
    - 安全性へ与える影響度は現時点では不明