CIPHERUNICORN-E
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　時田　俊雄

CIPHERUNICORN-E

- １９９８年に日本電気株式会社（NEC）が発表
- 共通鍵ブロック暗号
  （ブロック長: ６４ビット, 鍵長: 128ビット）
- ISO９９７９に登録（1998年）
- CRYPTREC2000からの継続評価対象暗号
- 特徴
  - Feistel構造(16段) + 補助関数（２段毎に挿入）
  - 「本流部」と「一時鍵生成部」という二重構造を有するラウンド関数
  - 暗号強度評価支援システム(NEC独自開発)によってラウンド関数を設計

CRYPTREC2000評価結果

- 現在のところ安全性の面で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不可能と考えられる
- 処理速度は64ビットブロック暗号では遅いグループ
  - CRYPTREC2000継続評価対象64ビットブロック暗号の中では遅いグループ (PC環境においてTriple DESの約3/5の速度)に属する。

ーーーーーーーーーーーーーーー

- 複雑なラウンド関数のため正確な評価が難しく，継続評価が必要と判断
  - 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

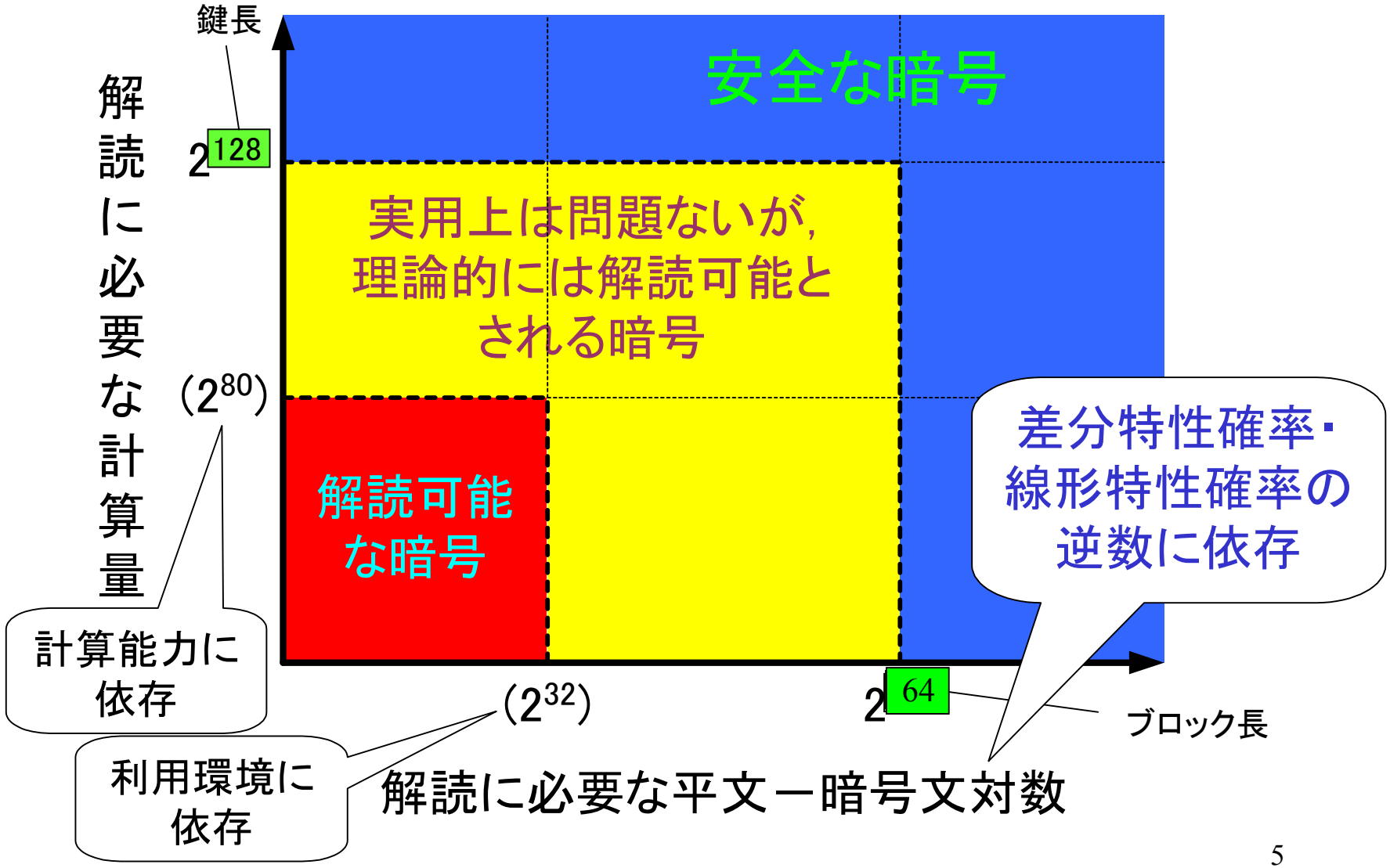
評価手順

- 今年度継続評価:
  - 国内外の4名(チーム)の暗号研究の専門家に
    以下の観点から『安全性評価』を依頼した。

    - 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
    - mF関数を利用した評価の妥当性
    - 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：64ビット
鍵長：128ビット



評価者１のコメント

- 差分解読法及び線形解読法に対して16段のCIPHERUNICRON-Eが攻撃可能であるとは考え難い。
  - 差分解読法に対する安全性
    - ラウンド関数の最大特性確率の上界: $\leqq 2^{-21}$
      (13段の最大特性特性確率の上界: $\leqq 2^{-126}$)
    - １６段仕様のCIPHERUNICORN-Eは差分解読法では解読不可能と結論
  - 線形解読法に対する安全性
    - 差分解読法に対してよりも安全であると思われる
    - ラウンド関数での特性確率の上界: $\leqq 2^{-24.64}$
      (13段の最大特性特性確率の上界: $\leqq 2^{-147.84}$)
    - １６段仕様のCIPHERUNICORN-Eは線形解読法では解読不可能と結論

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
    - 自己評価書の評価結果と異なる結果を導出
      （mF関数での特性確率の上界: $\leqq 2^{-72.0}$）
    - しかし、現状では差分解読法で攻撃不可能と思われる。
  - 線形解読法に対する安全性
    - 自己評価書の評価結果と異なる結果を導出
      （mF関数での特性確率の上界: $\leqq 2^{-62.0}$）
    - しかし、現状では線形解読法で攻撃不可能と思われる。

評価者3のコメント

- 差分解読法:　自己評価書と異なる評価結果を得たが、安全性の面では問題なしと判断する
  - 差分特性確率において自己評価書と異なる上界値を得た。
  - mF関数での最大特性確率の上界: $\leqq 2^{-14}$
  - 15段での特性確率の上界: $\leqq 2^{-98}$
  - CIPHERUNICORN-Eの段数が16段であることを考慮すれば、差分解読法に対して安全であると考えられる。
- 線形解読法:　自己評価書と異なる評価結果を得たが、安全性の面では問題なしと判断する
  - 線形特性確率において自己評価書と異なる上界値を得た。
  - mF関数での最大特性確率の上界: $\leqq 2^{-27.309}$
  - 15段での最大特性確率の上界: $\leqq 2^{-191.163}$
  - CIPHERUNICORN-Eの段数が16段であることを考慮すれば、線形解読法に対して安全であると考えられる。

評価者４のコメント

- １６段のCIPHERUNICORN-Eが差分解読法及び線形解読法で攻撃可能であるかどうかを評価
  - 差分解読法：　１６段は攻撃不可能と判断
    - ラウンド関数の特性確率の上界: $\leqq 2^{-16}$
    - 上界値での評価という点で自己評価書の結果と矛盾なし
    - １０段以上あれば有効な差分特性はないと判断
  - 線形解読法：　１６段は攻撃不可能と判断
    - ラウンド関数の特性確率の上界: $\leqq 2^{-16}$
    - 自己評価書におけるラウンド関数の上界値（$2^{-63.90}$）は不適切と判断するが、16段が攻撃不可能という結論は変わらず
    - １０段以上あれば有効な線形特性はないと判断

まとめ

- 今年度継続評価の結果、現在までに仕様段数である16段の**CIPHERUNICORN-E**に対して“安全性”の面で問題は見つかっていない。
  - ラウンド関数の差分/線形特性確率の評価、等で自己評価書の評価結果と異なる評価結果（いずれも上界値）が得られたが、いずれの場合も仕様段数（16段）の攻撃可能性を示すものではない。