CRYPTREC2001
共通鍵技術評価現状報告

2002年1月28日

共通鍵暗号評価小委員会委員長
東京理科大学教授　金子　敏信

評価対象暗号

- 応募形態の分類
  - 2000年度応募暗号
  - その他評価が必要な暗号

  } 第Ⅰ部
  - 2001年度新規応募暗号 → 第Ⅱ部
- 暗号技術の分類
  - 共通鍵暗号 （64,128ビットブロック暗号）
  - 共通鍵暗号 （ストリーム暗号）
  - ハッシュ関数
  - 擬似乱数生成系

共通鍵暗号評価小委員会

荒木　純道（東京工業大学）
金子　敏信（東京理科大学）
川村　信一（株式会社東芝）
神田　雅透（日本電信電話株式会社）
香田　　徹（九州大学大学院）
古原　和邦（東京大学）
櫻井　幸一（九州大学）

下山　武司（株式会社富士通研究所）
宝木　和夫（株式会社日立製作所）
館林　　誠（松下電器産業株式会社）
角尾　幸保（日本電気株式会社）
時田　俊雄（三菱電機株式会社）
森井　昌克（徳島大学）

Ⅰ．本年度評価

- 2000年度応募暗号　（応2000）
  - CRYPTREC2000レポートによる判断
  - 暗号提案者の継続応募の意志確認

  →監視対象暗号：
    - CRYPTREC2000で詳細評価終了
    - 電子政府暗号候補
    - 主体的な評価を、今年度は行わないが、学会等の評価情報を継続的に収集

  →詳細評価対象暗号：
    - 電子政府暗号候補
    - 昨年度の詳細評価に引き続くさらなる評価が必要
    - 国内外の専門家に観点を絞り詳細評価委託

Ｉ．本年度評価 （2）

- その他評価が必要な暗号
  - デファクトスタンダード等、評価が必要と委員会が判断した暗号（他2000),(他2001）
    - 2002年度までに詳細評価
    - 国内外の専門家による詳細評価
  - 外部組織からのコメント要請に対する評価

→特定評価：（特）

- 要請された暗号の観点を絞った評価

Ｉ．共通鍵暗号（６４ビット）

- 監視対象
  - Hierocrypt-L1　（応2000）
  - MISTY1　（応2000）
  - T-DES　（他2000、特）
- 詳細評価
  - CIPHERUNICORN-E　（応2000）→時田委員
  - RC2　（特）

Ⅰ．共通鍵暗号（１２８ビット）

- 監視対象
  - Camellia　（応2000）（特）
  - Hierocrypt-3　（応2000）（特）
  - RC6　（応2000）
  - SC2000　（応2000）（特）
- 詳細評価
  - AES(Rijndael)　（他2000、他2001）
  - CIPHERUNICORN-A　（応2000）→神田委員
  - SEED　（他2001、特）

Ｉ．ストリーム、ハッシュ、擬似乱数

- ストリーム暗号　詳細評価
  - MULTI-S01　(応2000)→下山委員
  - RC4　(特)
- ハッシュ関数　監視対象
  - RIPEMD-160　(他2000)
  - SHA-1　(他2000)
- ハッシュ関数　詳細評価
  - Draft SHA-{256 | 384 | 512}（他2001）
- 擬似乱数生成系　監視対象
  - PRNG based on SHA-1　(他2000)

Ⅱ．2001年度新規公募暗号

- 応募暗号評価手順
  - 応募締め切り　　2001.9.27
  - 書類審査
    - 応募書類の確認。外部評価委託可能性。
  - 応募暗号説明会　 2001.10.9-10 ヤマハホール
  - スクリーニング評価(外部) 2001.10～2000.12
    - 外部評価者に、昨年に準じた書式で評価依頼
    - 各暗号4名
  - CRYPTRECワークショップ　2002.1.28
  - 来年度の詳細評価の必要性を検討

Ⅱ．新規応募暗号技術

- ストリーム暗号
  - C4−1　（フォーカスシステムズ）
    - 第三者実装が可能なアルゴリズム情報の記載無し
    - 参照プログラムには応募暗号本体の記述無し
  - FSAngo （富士ソフトABC）
    - 参照プログラム、テストベクタ生成プログラムのソース無し
  - MUGI　（日立）
    - スクリーニング評価（外部）実施→櫻井委員

- 擬似乱数生成系
  - Creation of intrinsic random numbers with Clutter Box （エイチ・エム・アイ）
    - 特殊なハードウェアが必要
    - 乱数生成のアルゴリズムに関する十分な情報の記載無し
  - FSRansu　（富士ソフトABC）
    - 参照プログラム、テストベクタ生成プログラムのソース無し
  - High security ultra mini random number generator （SICシステム工学）
    - 特殊なハードウェアが必要
    - 参照プログラムは乱数系列を観測するプログラムであり、乱数生成アルゴリズムの評価不能
  - TAO TIME Cognition Algorithm （JCN）
    - スクリーニング評価（外部）実施→宝木委員

Ⅲ．今年度―来年度の課題

- 今年度特定評価のとりまとめ
  - RC4、RC2、SEED、AES、T－DES
    - 外部評価委託中
- HW実装性能の評価
- 新規応募暗号（応2001）の詳細評価
- 継続的な監視体制
- 電子政府推奨暗号リスト作成