HIME(R)暗号評価の現状報告 (スクリーニング評価)

平成14年1月28日

公開鍵暗号評価小委員会
委員　有田　正剛

HIME(R)
(応募者の主張)

- **応募暗号種別**: 守秘
- **安全性の根拠**: $N=p^dq$型素因数分解問題の困難性
- **証明可能安全性**: ランダムオラクルモデルのもとで最強の安全
- **方式の特徴**:
  - 非常に高速な暗号化処理
  - 復号化処理はRSA-OAEPの約2.5倍高速
- **SW実装情報**:

  暗号化 0.6 ms, 復号化 37.0 ms (Pentium III 800MHz)

スクリーニング評価

- 3名の評価者に評価を依頼
- 暗号技術仕様書に関して:
  - 記述レベルでの誤りがある。
  - 概ね、問題なし。
- 自己評価書に関して:
  - 安全性の証明に関して、問題点は指摘されていない。

評価者コメント

- 法$N=p^dq$を使用したRabin-OAEP
- 復号方法,すなわち法$N=p^dq$型での平方根演算方法について
  - CRTを用いた方法（CRYPTO'98 高木)と同程度ではないか？
- 証明可能安全性について
  - 従来の他者の結果に特に矛盾しない。
- $N=p^dq$型素因数分解問題
  - 自己評価書での分析が十分でない。
- その他
  - d=2,3以外の場合の記述がない。