EPOC-2暗号評価の現状報告（詳細評価）

平成14年1月28日

公開鍵暗号評価小委員会
委員　渡辺 創

EPOC-2暗号 (応募者の主張)

- 暗号種別：守秘
- 安全性の根拠：
  - $n=p^2q$ 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上で最強の安全性
- 特長：
  - 暗号化より復号が高速（RSA-OAEPより高速）
  - RSA仮定より一般的な仮定のもとで安全性を証明
  - 一般の安全性帰着より効率の良い帰着が可能
- その他：
  - 共通鍵暗号と組み合わせたハイブリッド暗号

詳細評価

- 前年度応募の暗号から少し仕様変更（継続評価扱い）
- 次の観点から複数（４名）の評価者に評価を依頼:
  - 暗号プリミィティブに関して
  - 暗号スキームに関して
  - （前年度評価結果と今年度応募暗号の関係について）
  - その他（$n=p^2q$ 型素因数分解問題の困難性等）

評価コメント－ $n=p^2q$ 型素因数分解問題の困難性－

- **特に問題は指摘されていない（n=pq とほぼ同等の安全性）。**
- NFS（数体ふるい法）によって素因数分解される合成数のサイズについての予測を考慮して、用いる素数（からなる合成数）のサイズを決定すべき（試算によると1024ビットは2018年に分解可能）である。
  - 他の暗号の場合も同指摘は考慮すべきである。
- NFS に対する素因数分解問題の困難性を、用いる共通鍵暗号（128ビット）と同等にするためには、より大きな素数（からなる合成数）を使用すべきである（最近の試算結果による）。
  - 他の暗号の場合も同指摘は考慮すべきである。
- 別に素因数分解問題についての評価を行なっており、そこでは n=pq 型よりやや易しいとの指摘があった。

評価コメント　－ 暗号プリミティブ－

プリミティブについての指摘が、スキームの安全性証明に影響を与えている。

- 用いられているプリミティブは、元となった Eurocrypt'98 で発表された関数とパラメータの条件が異なっている。そのため自己評価書のみでは、証明可能安全性が確認できていない（複数の評価者）。
  - パラメータ h_0 の条件、h の位数等
  - 別の条件の付加、帰着の効率が落とせば可能？とも
- 指摘した評価者は、Eurocrypt'98 と同条件にすれば、（効率の良い帰着による）証明可能安全性を持つとも報告している。

評価コメント　－ スキーム －

- 大きな問題は指摘されていない
  （ランダムオラクルモデルにおいて最強の安全性を持つ）。
- 共通鍵暗号としてブロック暗号を用いる場合、その使用法によっては IND-CPA が満たされないことがあるので、注意が必要である。そのため証明可能安全性を持たなくなる。