応募暗号技術の安全性評価について 1
メッセージ認証コード
PC-MAC-AES

CRYPTREC
Cryptography Research and Evaluation Committees

公募の目的 (公募要項P.4 第5.1節抜粋)

・策定から5年以上が経過し、解析・攻撃技術の高度化及び暗号技術の開発が進展している

・安全性評価のみならず危殆化及び移行対策を含めた適切な暗号選択の支援への要望

・導入コスト、相互運用性、普及度合いなどの評価観点の必要性の指摘

・リストの改訂に必要な技術の追加

CRYPTREC
Cryptography Research and Evaluation Committees

応募暗号に関する留意事項(公募要項P.2 第2.2節抜粋)

・2010年9月までに査読付き国際学会に採択されていること

・第三者が全ての機能を実装可能となる情報が開示されていること

・国内外での評価が可能であること

・評価に際しては、知的財産の利用が無償で行えること

・電子政府リスト策定後3年以内に調達可能なこと

CRYPTREC
Cryptography Research and Evaluation Committees

暗号利用モード(新設)

・証明可能安全性、適応選択平文/暗号文攻撃における識別不能性

・利用するnonceや乱数の有無や安全性における要件の妥当性

・利用するブロック暗号に対する安全性(ideal cipher modelなど)の要件など

・利用状況に特化した攻撃(関連鍵攻撃の実行可能性など)の有無

・実装効率性(並列処理など)

暗号利用モードの評価項目

- 証明可能安全性
  - 適応的選択文書攻撃
  - 検証オラクルを多数回呼び出したときの識別不可能性
  - 弱偽造不可能性
  - 強偽造不可能性
- Nonce、乱数要素の有無
- 利用暗号ブロックに対する仮定の強さ
- 利用ブロック暗号に特定の方式を適用した場合の安全性

CRYPTREC
Cryptography Research and Evaluation Committees

PC-MAC-AESの概要

- 証明可能安全性を確保するために、CMACのモード構成を利用
- ブロック暗号として、full-AESの代わりに4-round AESを用いることで高速化を図っている。（CBC-MACに比べて1.4 - 2.5倍高速）
- 4-round AESへの鍵の設定においては、AESの暗号化関数を用いた鍵スケジュールを利用

CRYPTREC
Cryptography Research and Evaluation Committees

PC-MAC-AESの仕様について

- 応募暗号説明会（2010.3.2 – 2010.3.3）において、国際会議で採録された論文の仕様と、今回応募されているアルゴリズムの仕様に差異があることが報告された。
- 事務局で提案者と仕様の差異に関して確認を行った結果、安全性評価上の差異がないことを確認。
- 暗号方式委員会の審議により、提案仕様で評価を進めることとなった。

CRYPTREC
Cryptography Research and Evaluation Committees

安全性評価結果

- 証明可能安全性について
  - 評価者による攻撃成功確率のupper boundの修正
    - 評価者による安全性証明
      - 限定的な攻撃者（短いメッセージの問い合わせに限定）で攻撃のtime complexityは 2^{56}
      - 一般的な攻撃者の場合で、同じモデルで証明した場合には攻撃のtime complexityは 2^{33}
    - 評価者による新しい証明
      - より一般的な攻撃者による攻撃の成功確率のupper boundは $O(q\sigma^2/2^n)$ 。time complexityは 2^{42}
      - 別の証明手法によると、一般的な攻撃者による攻撃の成功確率のupper boundは $O(\sigma^2/2^n)$ 。time complexityは 2^{56}

CRYPTREC
Cryptography Research and Evaluation Committees

安全性評価結果

PC-MAC-AESの分類

- CBC-MAC
  - MacDES
  - EMAC
    - TMAC
      - CMAC
      - PC-MAC

安全性評価結果

- 新たな攻撃の指摘
  - Subkey Recovery Attack
    - TMAC の Subkey L をリカバリする攻撃が適用可能
    - L がリカバリできると、各ブロックの鍵をリカバ可能
    - リカバのコストは、2^{65} クエリ

    - 4 ラウンド AES を用いた場合の攻撃
      - 各ラウンドの Subkey K1, K2, K3, K4 を求める攻撃手法の提案。4-round AESを用いた CBC-MAC に分類される構造に適用可能
      - 2^{67} のクエリと 2^{40} の計算量でラウンド鍵と中間値を求めることができる。

CRYPTREC
Cryptography Research and Evaluation Committees

安全性評価結果

- 新たな攻撃の指摘
  - Random Permutationからの識別可能性
    - Random Permutationを用いた場合と、4-round AESを用いた場合の識別が可能。必要なコストは2^{65}クエリ

- 指摘された攻撃は、PC-MAC-AESのみに適用可能ではなく、CBC-MAC 系統に適用可能。
  - 攻撃シナリオの実現性に対する検討が必要
- 攻撃に必要なコストは提案者の安全性証明のバウンドより大きい

CRYPTREC
Cryptography Research and Evaluation Committees

まとめ

- 新たな安全性解析結果が報告
  - 評価結果、攻撃シナリオの妥当性については、今後検討が必要
  - CMACとの優位性の比較
    - CMAC に4-round AES を適用した場合の、よりコンパクトな実装の可能性
    - CMAC + 4-round AES の証明可能安全性
  - 別の課題
    - 似た構造の PELICAN や Alpha-MAC にサイドチャネル攻撃が指摘されているため、サイドチャネル攻撃の組み合わせに対する耐性の検討

CRYPTREC
Cryptography Research and Evaluation Committees