応募状況説明

CRYPTREC事務局

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

本日の説明対象技術カテゴリ

・共通鍵暗号(ストリーム暗号)

・暗号利用モード(新設)

・メッセージ認証コード(新設)

CRYPTREC
Cryptography Research and Evaluation Committees

ストリーム暗号

・128bit以上の鍵サイズ

・Time/memory/data-trade off、分割統治攻撃、相関攻撃、代数的解法など汎用的、良く知られた攻撃手法に対して安全なこと

・鍵に対する全数探索よりも効果的な攻撃手法が発見されていないこと

・サイドチャネル攻撃に対する安全性も加味(新設)

・現リスト暗号よりも安全性/実装性で優位であること(新設)

CRYPTREC
Cryptography Research and Evaluation Committees

ストリーム暗号応募状況及び評価対象

応募技術　2件

- Enocoro　　株式会社日立製作所
- KCipher-2　　KDDI株式会社

現リスト技術　3件

- MUGI　　株式会社日立製作所
- MULTI-S01　　株式会社日立製作所
- 128bit-RC4　　RSAセキュリティ株式会社

CRYPTREC
Cryptography Research and Evaluation Committees

現リスト暗号 MUGI

・ブロック暗号の評価手法(2000年当時)が適用しやすい安全性評価が容易な構造

・AESのS-boxの採用

・128bit鍵+128bit初期値(公開値)

・ソフトウェア処理は早いグループ(2003年当時)

CRYPTREC
Cryptography Research and Evaluation Committees

現リスト暗号 MULTI-S01

・擬似乱数生成器PANAMAを内部関数に採用

・256bit鍵

・メッセ–ジ秘匿とメッセージ認証を同時に達成

・ソフトウェア処理は早いグループ(2003年当時)

CRYPTREC
Cryptography Research and Evaluation Committees

現リスト暗号 128bit-RC4

・学会等で議論される”alleged RC4”がRC4と等価なアルゴリズムである
ことをRSAセキュリティと確約した上で安全性評価

・初期状態によって安全性が損なわれる指摘がある

・リスト注釈5「SSL3.0/TLS1.0以上に限定」しての利用を推奨

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)

暗号利用モード応募状況及び評価対象

応募技術　なし

事務局選出技術

- CBC (Cipher Block Chaining)
- CFB (Cipher FeedBack)
- CTR (CounTeR)
- OFB (Output FeedBack)

CRYPTREC
Cryptography Research and Evaluation Committees

メッセージ認証コード(新設)

・証明可能安全性、適応選択文書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)

CRYPTREC
Cryptography Research and Evaluation Committees

暗号利用モード応募状況及び評価対象

応募技術　1件

・PC-MAC-AES　日本電気株式会社

事務局選出技術

・CBC-MAC

・OMAC

・HMAC

CRYPTREC
Cryptography Research and Evaluation Committees