公募対象カテゴリを中心とした暗号技術の動向について

－ ブロック暗号 －

ソニー株式会社　　盛合 志帆

ブロック暗号技術の最新動向

- 最近の設計思想
- 攻撃法と安全性評価の動向
- 実装に関する傾向
- 注目すべき暗号

最近の設計思想

- 2005年以降に提案された新ブロック暗号
  (IACR Conference/Workshop: CRYPTO, FSE, CHES, etcでの発表)
  - Hong et al., "**HIGHT**: A New Block Cipher Suitable for Low-Resource Device" (CHES 2006)
  - Shirai et al., "The 128-bit Blockcipher **CLEFIA**" (FSE2007)
  - Leander et al., "New Lightweight DES Variants Suited for RFID Applications" (FSE2007)
  - Bogdanov et al., "**PRESENT**: An Ultra-Lightweight Block Cipher" (CHES 2007)
- キーワード: **Lightweight, 省リソース, 省電力**

最近の設計思想

- **その他, 近年提案されたブロック暗号**
  (その他の会議での発表)
  - Nakahara et al., “The **MESH** Block Ciphers” (WISA 2003)
  - Junod et al., “**FOX**: a new family of block ciphers” (SAC 2004)
  - Lim et al., “**mCrypton** - A Lightweight Block Cipher for Security of Low-cost RFID Tags and Sensors” (WISA 2005)
  - Standaert et al., “**SEA**: A Scalable Encryption Algorithm for Small Embedded Applications” (CARDIS 2006)

攻撃法と安全性評価の動向

- 代数的解析手法の進展
  - Cube Attackなどの新しいアイデア
  - SAT/SMT solverなど解析ツールの進化
- 関連鍵攻撃
  - AESへの攻撃など, 鍵スケジュールを積極的に利用
- 不能差分攻撃
- 線形攻撃の一般化

実装に関する傾向

- より広い範囲の製品・サービスに
  - より安いコスト(消費電力 etc.)が求められる
- より安全に
  - 進化する実装攻撃への防衛が必要
  - サイドチャネル攻撃 (DPA, DFA, Cache Attacks)
  - これらに対する攻撃耐性はアルゴリズムレベルではなく実装方法による差が大きい。

注目すべき暗号

- HIGHT (2006)
  - ブロック長: 64 bit, 鍵長: 128 bit
  - ハードウェア性能に優れ, 約3Kgateで実装可能.
- CLEFIA (2007)
  - ブロック長: 128 bit, 鍵長: 128/192/256 bit
  - ソフト・ハードともにバランスよく, 優位な性能.
- PRESENT (2007)
  - ブロック長: 64 bit, 鍵長: 80/128 bit
  - 速度は遅いが 2Kgate以下(暗号化回路のみ)の実装も可能.

電子政府推奨のブロック暗号に求められる要件に関する意見

- ユーザの要望は用途によって多種多様
  - 安全性, 信頼性, 規格, 各種認証
  - コスト
  - ソフトウェア，ハードウェア実装性能
  - AES vs AES以外

ユーザがリスト等を見て, 各アルゴリズムの特徴が分かり, 用途に合ったものが選べると便利. AESとの差別化ポイントも明記しては.

今回の公募におけるブロック暗号の評価方法に関する意見

- 安全性評価：評価者は攻撃論文の内容の正当性, 現実性も吟味するように努めてほしい.
- 実装評価：サイドチャネル攻撃に対する耐性はどのように評価・比較するのか.
  - 想定される攻撃や実装方法, 実装プラットフォームに強く依存する. (事務局立会いでDPA測定を行う??)
  - そもそもアルゴリズム毎の差より実装方法の差の方が大きいと思われる. (会場からも意見下さい)
- 電子政府推奨暗号リストへ登録されるための製品化・利用実績をどのように評価するのか現時点の考え方をお聞かせ頂きたい.