ハッシュ関数の動向

CRYPTREC シンポジウム2009

パネル1「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」

2009年2月18日

㈱日立製作所

システム開発研究所

吉田　博隆

Contents

ハッシュ関数とは

- ITシステムにおけるコア技術として幅広く利用
  - 機能要件
    任意長のメッセージから、固定長の出力を計算
  - 基本安全性要件
    - ハッシュ値から圧縮前のデータを復元することは困難(一方向性)
    - あるデータのハッシュ値と同じハッシュ値を持つ、異なるデータを見つけることは困難(第二原像困難性)
    - あるハッシュ値を与える異なる2つのデータを見つけることは困難（衝突困難性）
  - ハッシュ関数に対する攻撃の計算量
    ターゲットの結果が得られるまで，nビットの出力長をもつハッシュ関数に対し、入力を選択して出力の計算を繰返す場合
    - 原像計算：2^n
    - 第二原像計算：2^n
    - 衝突計算：$2^{n/2}$

ハッシュ関数の近年の動向と現状(FIPS)

- 近年の動向
  - 1995年：SHA-1*1を含む標準FIPS*2 180-1をNIST*3が公開
  - 2002年：SHA-256/384/512を含む標準FIPS180-2をNISTが公開
  - 2004年：FIPS 180-2にSHA-224が追加 →SHA-224/256/384/512はSHA-2と総称。
  - 2005年：SHA-1に対する衝突攻撃が発表
    ハッシュ関数の危殆化が進行
  - 2007年：NISTがCryptographic Hash Competitionを開始、公募要領が公開。
    勝者はSHA-3と呼ばれ、2012年に選定される予定
- SHA-xの現状
  - SHA-1:現状最も広範囲に使用。衝突困難性に関する安全性レベルが80ビットから63ビットまで落ちたが、一方向性に関しては脆弱性の報告なし。
  - SHA-2:ファミリー:ブロック暗号標準AESに対応した安全性をもつため新システムへの適用は推奨。基本安全性要件に関する脆弱性の報告なし。

*1 SHA: Secure Hash Algorithm
*2 Federal Information Processing Standards
*3 米国標準技術研究所（NIST：National Institute of Standards and Technology）
*4 http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

Cryptographic Hash Algorithm Competitionの位置づけと公募要綱

位置づけ：ハッシュ関数の解読技術の進展に対応。
現FIPS180-2にSHA-3を追加(augment)する。

最小限の要件

- 224/256/384/512ビットの出力長をサポート
  （⇒SHA-2ファミリーと同じ出力長）
- ロイヤルティーフリー、知財権の制約なし
- 入力の最大長は少なくとも2^{64}-1

実装性能・コスト

- ソフトウェア実装評価
  リファレンス/最適化コードの提出
  - 32/64ビットCPUでの評価
  - 8ビットCPUでの評価

安全性（最重要の評価基準）

- アプリケーションの安全性の保証
  - ディジタル署名(FIPS 186-2),
    HMAC (FIPS 198)等
- Additional security
  - ランダム化ハッシュモードの安全性
  - 衝突計算困難性、(第二)原像計算困難性
  - Length-extension攻撃に対する安全性

NISTリファレンスプラットフォーム
プロセッサ：Intel Core 2 Duo 2.4GHz
メモリ：2GB
OS：Windows Vista Ultimate 32-bit Edition、64-bit Edition

コンパイラ
Microsoft Visual Studio 2005 Professional Edition、ANSI C

Cryptographic Hash Algorithm Competitionの応募状況*1

- 応募総数：64件
- 第1ラウンド候補アルゴリズム：51件

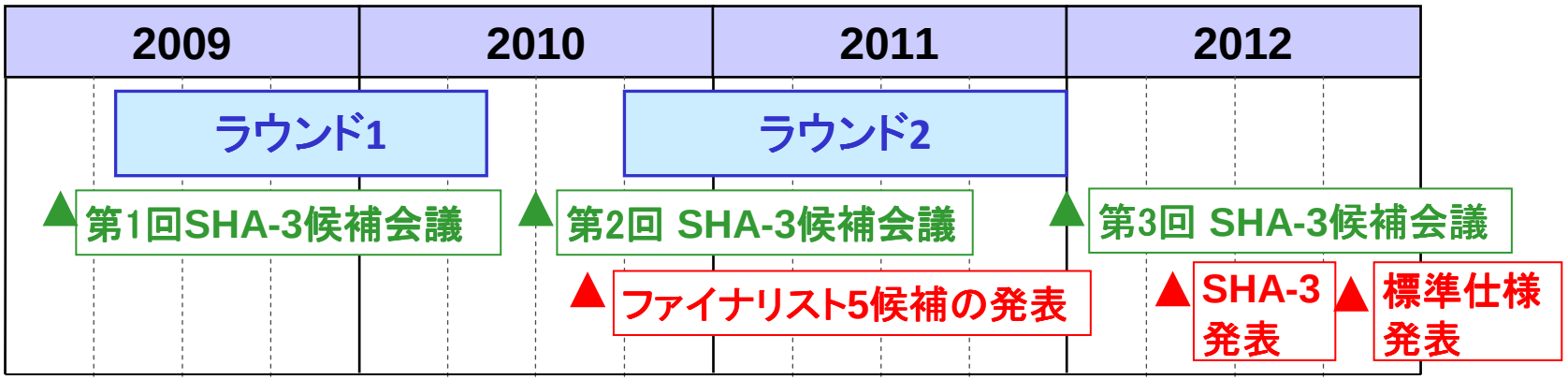
  日本：3件（ AURORA, Lesamnta, Luffa ）
- 2009年2月16日時点での選考対象：42件
  9件は、提案者が解読されたことを認めた
- 設計の傾向
  - 従来型の代表例：ブロック暗号ベース型
  - 新規型の代表例：(変形)スポンジ型

国別応募状況*2（件）

国名	応募件数
アメリカ	13
フランス	7
日本	3
イギリス	2
韓国	2
スイス	2
中国	2
トルコ	2
ドイツ	2
ノルウェー	2
ベルギー	2
ルクセンブルグ	2
その他	10
合計	51

*1 http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions_rnd1.html
*2 Principal Submitterの所属の国籍による分類

Cryptographic Hash Competitionの今後のスケジュール(仮)



ラウンド1 の評価内容

- 暗号強度に関する公開評価のレビュー
- 性能テスト
  - 最適化実装に関する各種性能テスト
  - NISTリファレンスプラットフォームが使用される
- その他テスト
  - その他の特徴に対するテスト

ラウンド2 の評価内容

- 提出物の分析と、分析結果の一般公開
- 性能テスト
  - 最適化実装に関する各種性能テスト
  - ハードウェア実装評価
  - 追加のプラットフォーム上の性能評価
- その他テスト
  - その他の特徴に対するテスト

将来のCRYPTREC公募におけるハッシュ関数の評価について

- 公募対象
  - 主は汎用ハッシュ関数
  - 以下も検討の余地はある？
    - 特殊用途
    - ハッシュ関数関連のモード

- 評価項目(汎用ハッシュ関数)
  - NISTのCryptographic Hash Algorithm Competitionにおける評価項目は基本的によい。
    - 安全性：基本安全性要件と新たに議論されている安全性
    - 性能：提案者にもハードウェア実装評価を課す必要があるのでは