共通鍵暗号技術評価報告

共通鍵暗号評価小委員会委員長
東京理科大学理工学部電気工学科
金子敏信

@CRYTPRECシンポジウム　H13.4.18

概要

- 暗号技術（共通鍵小委）
  - ブロック暗号、ストリーム暗号、ハッシュ関数、乱数生成
- 評価の観点
  - 安全性、実装性
- 暗号技術の評価結果

暗号技術(共通鍵小委)

- ブロック暗号
  - 64ビットブロック暗号　鍵長128ビット
  - 128ビットブロック暗号 鍵長128,192,256ビット
- ストリーム暗号
- ハッシュ関数
- 乱数生成技術

共通鍵暗号の評価（安全性）

- 安全性
  - 情報理論的安全性
  - 計算量的安全性　←実用暗号
    - 最良の攻撃アルゴリズム、最速の計算機でも計算量的に攻撃不能
- 攻撃方法
  - 全数探索
  - ショートカット法

全数探索

- 数組の平文･暗号文対→鍵の全数探索
  - 計算量$2^{|K|}$
- 安全性指標　|K|　鍵ビット数
    - DES-ChallengeⅢ　|K|=56　22時間
    - 計算機能力の進歩
  - $|K| \leqq 64$　　危険
  - $64 < |K| < 128$　？
  - $|K| \geqq 128$　　安全

ショートカット法
（ブロック暗号）

- 差分／線形攻撃[横、個別]
- 代数的攻撃[横、個別]
  - 高階差分攻撃、補間攻撃、SQUARE攻撃
- アバランシュ性評価[横、個別]
- その他の攻撃[個別]
  - 鍵関連攻撃、mod n攻撃、スライド攻撃他

⇒計算量$2^{|K|}$以下の攻撃有り→学術的に解読可

共通鍵暗号の評価（実装性,他）

- ソフトウエア実装評価（ブロック暗号、ストリーム暗号）
  - 暗号化／復号速度（ランダム化部、ランダム化部＋鍵処理部）
  - ソフトウエアサイズ
  - PC環境、サーバ環境、ハイエンド環境
- ハードウエア実装評価（ブロック暗号）
  - 0.25～0.35μmのASIC、Verilog-HDL、Design Compiler
- 特許等の取り扱い

64ビットブロック暗号

- 対象暗号
  - CIPHERUNICORN-E (NEC1998)　UNI-E
  - FEAL-NX (NTT1990)
  - Hierocrypt-L1 (東芝2000)　Hiero-L1
  - MISTY1 (三菱1996)
  - Triple DES (IBM1979)　T-DES

64ビットブロック暗号:特徴:構造

- Feistel型
  - UNI-E　16段
    - F関数に本流部、一時鍵部
  - FEAL　32段
    - 初期、最終処理
  - MISTY1　8段
    - ２段毎にFL
    - 段関数は再帰型Feistel
- SPN型
  - Hiero-L1　6段
    - 入れ子型SPN
    - XS: 32x32　S-box
- 組み合わせ型
  - T-DES
    - DESを３回
    - DESはFeistel型 16段

64ビットブロック暗号：特徴：構成部品

- S-box
  - UNI-A　8x8 4種類
  - Hiero-L1 8x8 1種類
  - MISTY1 9x9,7x7 2種類
  - T-DES 6x4 8種類
- S関数
  - FEAL 8bit 算術演算、巡回シフト
- S-box構成法
  - ランダム構成or理論的構成
- P層構成法
- 使用演算
- 全体構造の設計思想

64ビットブロック暗号：安全性：差分／線形

- 証明可能安全性（差分／線形）
  - 最大差分確率／最大線形確率が十分小
  - MISTY1　3段　2^{-56}
  - Hiero-L1　2段　2^{-40}
- 実際的安全保障
  - 特性確率の上界＜2^{-64}
  - Heiro-L1　2段線形／差分　2^{-90}
  - UNI-E　12段差分、8段線形<2^{-64}　（簡略化したF関数）

64ビットブロック暗号:安全性:差分／線形 cont

- 計算機探索:最大特性確率＜2^{-64}
  - T-DES　DESの2回繰り返し<2^{-64}
    - DES 差分　$2^{-54.1}$　線形　$2^{-44.9}$
  - FEAL-NX　31段差分　2^{-62} 25段線形 $2^{-62.3}$

  ⇒FEAL-32Xは2^{99}の計算量で解読可

  学術的解読（現時点の使用はOK長期使用は？）

64ビットブロック暗号：安全性：代数的攻撃

- 高階差分攻撃(SQUARE攻撃を含む)
  - 評価指標：代数次数
- 補間攻撃（線形和攻撃）耐性
  - 評価指標：未知補間係数個数
- 指標：（入出力変数で変化）全可能性調査不可
  - 形式的代数次数
  - S-box単位8階以下高階差分
  - S-boxの全単射性利用(SQUARE攻撃)、
  - ガロア体GF(2^8)多項式基底表現。線形和攻撃

64ビットブロック暗号：安全性：代数的攻撃

- 全暗号、今回の評価に対し耐性
- 高階差分攻撃が効果的な暗号
  - Hiero-L1： 32階差分（32階SQUARE）平文組2^{37}、計算量2^{117} 3.5段まで
  - MISTY1（FL関数なし）：7階差分、平文組2^{11}、計算量2^{93}、6段まで
  - MISTY1：32階差分、平文組2^{37}、計算量2^{75}で5段まで

64ビットブロック暗号：安全性：その他の攻撃

- 中間一致攻撃
  - T-DES 選択平文2^{56} 計算量$2^{108.2}$ 学術的解読可
- カイ2乗攻撃、不能差分攻撃、ブーメラン攻撃、mod n攻撃、非全単射攻撃
- どの暗号方式も実用的観点では安全性に関する問題点の報告なし
- 実装時に、タイミング攻撃、電力攻撃の配慮要

64ビットブロック暗号：安全性：アバランシュ性評価

- 暗号化処理全体
  - 全てのアルゴリズムが期待値を満足し安全
- 鍵スケジュール部単体
  - FEAL-NX、Hiero-L1、MISTY1で期待値を満たさない部分有り
- ラウンド関数単体
  - FEAL-NX、Hiero-L1、MISTY1で期待値を満たさない部分有り

64ビットブロック暗号：実装評価(SW)

- PC環境： PentiumIII (650MHz)
  暗号化／復号速度[Mbps]
  UNI-E 29.0/29.3
  FEAL-NX 117.8/117.2
  Hiero-L1 209.0/203.9
  MISTY1 195.3/200.0
  T-DES 48.7/48.7
- {UNI-E,T-DES}:遅め
- {Hiero-L1,MISTY1}：速め

- サーバ環境： Ultra SPARC Ⅱi(400MHz)
  暗号化／復号速度[Mbps]
  UNI-E 17.5/17.5
  Hiero-L1 67.7/51.2
- ハイエンド環境：Alpha21264 (463MHz)
  暗号化／復号速度[Mbps]
  UNI-E 18.8/18.9
  Hiero-L1 141.1/141.1
  MISTY1 139.1 /143.8

64ビットブロック暗号：実装評価(HW)

- FEAL-NX,Hiero-L1,MISTY実装評価、T-DESは文献による参考値（数値は資料参照）
- T-DESとの相対比較 (T-DES=1)

ループ・アーキテクチャ無し

	回路規模	処理速度
Hiero-L1：	2.5	2.25
FEAL-NX：	1/2	0.7

ループ・アーキテクチャ

MISTY1:	10～7.6	2.5～1.9

64ビットブロック暗号：安全性余裕と速度

	安全性余裕	速度
UNI-E	16 / −*	0.60
FEAL-NX	32 / 32	2.41
Hiero-L1	6 / 3.5	4.25
MISTY1	8 / 5	4.07
T-DES	48 / 48	1

安全性余裕＝段数／(学術的)攻撃可能段数

速度(データランダム化部)T-DES基準

64ビットブロック暗号:総合評価

- 安全性について、今のところ問題は見つかっていない。複雑なF関数の為、暗号系全体の正確な評価が難しく、継続的評価が必要。速度は遅いグループである。(UNI-E)
- FEAL-32Xは学術的に解読可能であり、長期の使用を考えた場合、推薦できない。8 bit CPUのSW実装に適する。(FEAL-NX)
- 安全性について、今のところ問題は見つかっていない。処理速度は速いグループである。(Hiero-L1,MISTY1)
- 安全性について、FIPS等で保証されている間は、問題ないと考える。(T-DES)

128ビットブロック暗号

- 対象暗号

  Camellia (NTT,三菱,2000)

  CIPHERUNICORN-A(NEC,2000)

  Hierocrypt-3 (東芝,2000)

  MARS (IBM,1998)

  SC2000 (富士通,2000)

  RC6 (RSAセキュリティ,1998)

  Rijndael (J.Daemen and V.Rijmen,1998)

- 64ビット暗号と同様に安全性、実装性の評価を行う（省略：CRYPTREC報告書参照）

128ビットブロック暗号:構造(表5.1.3)

- Feistel型
  - Came 18段(128),24段
    - 6段毎にFL/FL^{-1}
  - UNI-A 16段
    - Fは本流部と一時鍵部
- SPN型
  - Hiero-3 6段(128),7,8段
    - 入れ子型 1段=2層
  - Rijndael 10段(128), 12,14
    - SQUARE型
- 変形Feistel
  - RC6 20段
    - 32bit F関数(各段2ヶ)
  - MARS
    - 前方混合＋コア＋後方混合
    - コアは16段 32x96 F関数
- 混合型
  - SC2000 SPNとFeistel
    - 19段(128), 22段

128ビットブロック暗号:安全性：差分/線形

- 実際的安全保障(特性確率の上界$<2^{-128}$)
- 活性S-box数
  - Came　12段　線形／差分$<2^{-132}$
  - Hiero-3　2段　線形／差分$<2^{-150}$
  - Rijndael　4段　線形／差分$<2^{-150}$

128ビットブロック暗号:安全性：差分/線形

- Trancated Vector探索
  - UNI-A　15段　線形／差分<2^{-140} (簡略化F)
  - SC2000　15段　差分<2^{-134} 線形<2^{-142}
- 構造上の特徴＋計算機探索併用
  - MARS コア　差分<2^{-156} 線形<2^{-120}（近似）
  - RC6 14段 差分<2^{-140} 18段 線形<2^{-155} （近似）

128ビットブロック暗号:安全性：代数的攻撃

- 全暗号、今回の評価に対し耐性
- 高階差分攻撃が効果的な暗号
  - Rijndael: 32階差分（SQUARE攻撃）
    - 128 bit鍵　7/10, 192 bit鍵　8/12、256 bit鍵 8/14
  - Hiero-3: 32階差分
    - 128 bit鍵　3/6, 192 bit鍵　3.5/7、256 bit鍵 3.5/8

128ビットブロック暗号：安全性：その他の攻撃

- カイ2乗攻撃
  - RC6 128bit鍵 12/20 192bit鍵 14/20 256bit鍵 15/20
- 関連鍵攻撃
  - Rijndael 256bit鍵 9/14
- 不能差分攻撃、ブーメラン攻撃、mod n攻撃、非全単射攻撃
- どの暗号方式も実用的観点では安全性に関する問題点の報告なし
- 実装時に、タイミング攻撃、電力攻撃の配慮要

128ビットブロック暗号：実装評価(SW)

- PC環境

  暗/復[Mbps]

  - Came 255/255
  - UNI-A 53/53
  - Hiero-3 206/195
  - RC6 323/318
  - SC2K 214/204
  - T-DES 49/49

- サーバ環境
  - Came 144/144
  - UNI-A 23/22
  - Hiero-3 109/84
  - RC6 25/25
  - SC2K 186/182
- ハイエンド環境
  - Came 210/210
  - UNI-A 32/34
  - Hiero-3 149/154
  - SC2K 226/216

128ビットブロック暗号：実装評価(HW)

- ループ・アーキテクチャ無し(T-DES比)

	回路規模	速度
– Hiero-3	4.8	>4
– Rijndael	4.1	>4
– RC6	>10	<1
– MARS	>10	<1

- ループ・アーキテクチャ(T-DES比）

– Came	4~6	2.5~3

128ビットブロック暗号：安全性余裕

- 256bit鍵段数/学術的解読可能段数
  - Came　24/7　FL/FL-1無し
  - Hiero-3　8/3.5
  - MARS　16/11　コア部のみ
  - RC6　20/15
  - SC2K　22/13
- Cameは24/10に変更予定(by Kaneko 2001.5)
  - 128bit暗号の安全性余裕は、未定着

128ビットブロック暗号 : 総合評価(1)

- 安全性について、今のところ問題は見つかっていない。処理速度は速いグループである。(Camellia,Hierocrypt-3,SC2000)
- 安全性について、今のところ問題は見つかっていない。複雑なF関数の為、暗号系全体の正確な評価が難しく継続的評価が必要。速度は遅いグループである。(CIPHERUNICORN-A)

128ビットブロック暗号 : 総合評価(2)

- 安全性について、今のところ問題は見つかっていない。製品化の予定無との事で、ソフトウェア処理速度評価せず。(MARS)
- 安全性について、今のところ問題は見つかっていない。Pentium III上の暗号化で最速であるが、ソフトウェア処理速度はプラットフォームに大きく依存。(RC6)
- AES暗号であり信頼がおけると考えられる。電子政府としては、FIPS版の再評価後の使用を推薦する。(Rijndael)

ストリーム暗号

- 対象暗号
  - MULTI-S01(日立,2000)
    - 疑似乱数生成器PANAMA使用
    - メッセージ認証も可
  - TOYOCRYPT-HS1(東洋通信,2000)
    - 同期型鍵ストリーム暗号
    - LFSR＋非線形回路
    - HW指向

ストリーム暗号

- 安全性
  - TOYO-HS1
    - 実効鍵長128→96の攻撃
    - 対応策有り
- 実装性(SW)PC環境
  - MULT-S01 238Mbps
  - TOYO-HS1　3
- 実装性(HW)
  - 両者とも1Gbps程度可
  - TOYO-HS1の方がHW規模小

ストリーム暗号 : 総合評価

安全性及び実装性を評価（詳細は報告書）

- ストリーム暗号としての安全性については、今のところ問題は見つかっていない。現時点では学会等で厳密な評価が得られておらず、継続的な評価が必要。SWにおける処理速度は速いグループ（MULTI-S01)
- 提案アルゴリズムになにがしかの改善を行ってから、実システムには採用すべき。HW実装向き。(TOYOCRYPT-HS1)

ハッシュ関数

- 対象暗号技術

  MD5(R.Rivest,1991)

  128bit ハッシュ

  ハッシュ値サイズが小さい(birthday attack)

  RIPEMD-160(H.Dobbertin, A.Bosselaers, B.Preneel 、1996)

  160bit ハッシュ

  SHA-1(NIST)

  160bit ハッシュ

疑似乱数生成

- 対象暗号技術

  TOYOCRYPT-HR1(東洋通信機,2000)

  128段LFSR+非線形関数

  TOYOCRYPT-HS1と同様な欠点あり

  Pseudo-Random Number Generator based on SHA-1（FIPS186-1:DIGITAL SIGNATURE STANDARD APPENDIX C）(NIST,1995)

  長期使用には次世代SHA？

終わりに

- 共通鍵暗号を中心に評価
  - ブロック暗号　　12(10)
  - ストリーム暗号　2(2)
  - ハッシュ関数　　3(0)
  - 乱数生成　　2(1)
- 今回は限られた期間で実施した2000年度版評価。継続的評価が必要
  - 128ビットブロック暗号、一部64ビットブロック暗号、、
  - ストリーム暗号、ハッシュ関数、乱数生成
  - 実装に関わる強度評価