2009年2月18日
CRYPTRECワークショップ

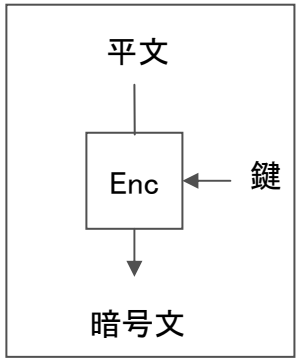
暗号利用モードの最新動向

富士通研究所
下山武司

暗号利用モードの経緯

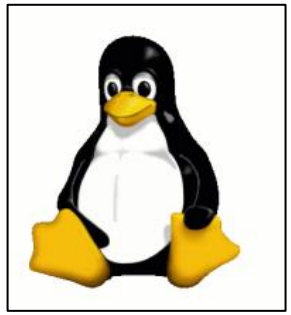
FUJITSU

ブロック暗号(ECBモード)

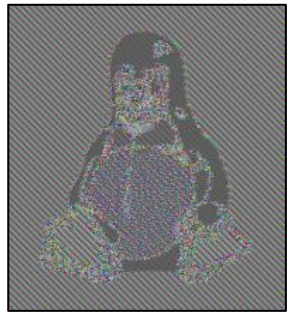


- 同じ平文に対しては同じ暗号文
- 乱数列と識別可能（右に例示）

原画



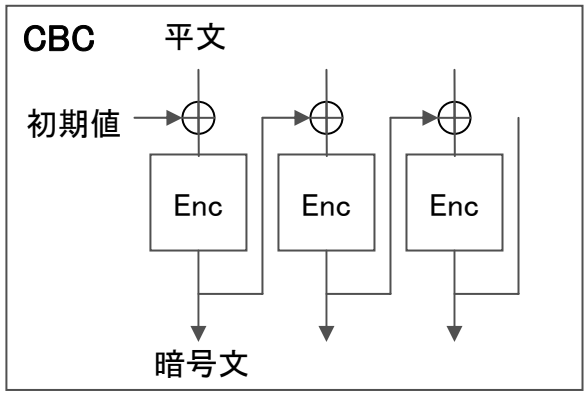
ECBモード暗号化



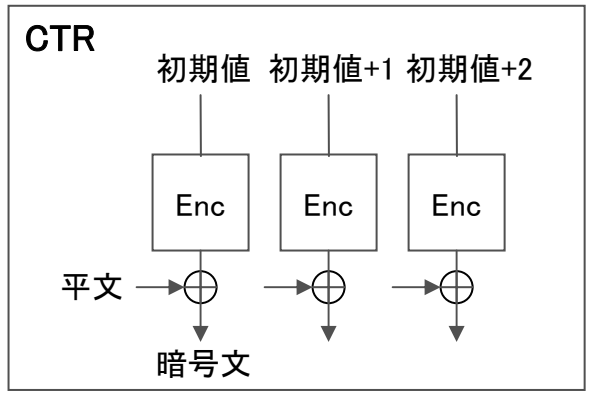
出典　http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

暗号利用モード：ブロック暗号の欠点を補うパッチ

CBC, OFB, CFBモード



CTRモード



暗号利用モード一覧

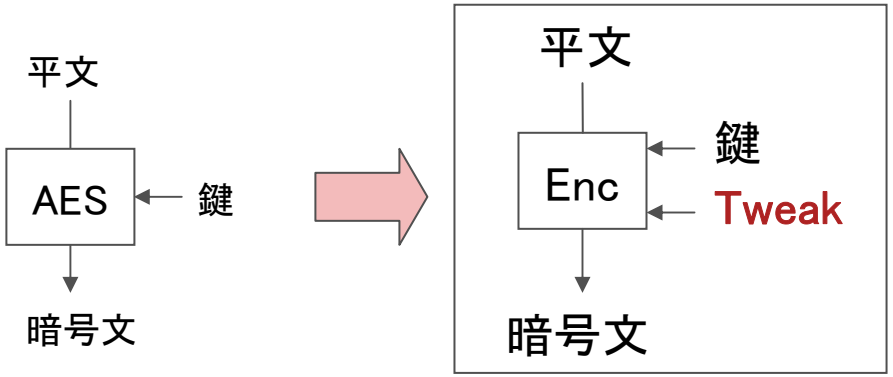
FUJITSU

秘匿	ストリーム暗号	ABC, CBC, CFB, k-CFB, CTS, 2DEM, IGE,
	キーストリーム	OFB, CTR, CENC, F8, KFB,
	ブロック暗号	ABL3, ABL4, Bear, CMC, EMD, EME, EME2, Feistel, HCH, HCTR, Lion, LRW, Mercy, NR, PEP, TET, XEX, XCB, XTS,
認証	MAC	ALRED*, ALPHA-MAC*, CBC-MAC, CMAC, EMAC, F9, FRMAC, GMAC, HMAC*, IPMAC, MMH, MT-MAC, NMAC*, OMAC, PC-MAC, PELICAN*, PMAC, Poly1305-AES, RMAC, Tail-MAC, TMAC, Two-Track-MAC, UMAC, VMAC, XCBC-MAC, XECB-MAC, XOR-MAC,
	ハッシュ	AES-hash, EMD, Merkle-Damgard, MDP, PMD-MMO,
	一方向性関数	Davis-Meyer, abreast-DM, tandem-DM, Hirose-DBL, Matyas-Meyer-Oseas, Miyaguchi-Preneel, MDC-2, MDC-4,
認証付秘匿	CCM, CHM, CS, CWC, EAX, GCM, Key-Wrap-AES, IACBC, IAPM, MULTI-S01*, OCB, PCFB, k-PCFB, SIV, XCBC,	

ブロック暗号からブロック暗号へ

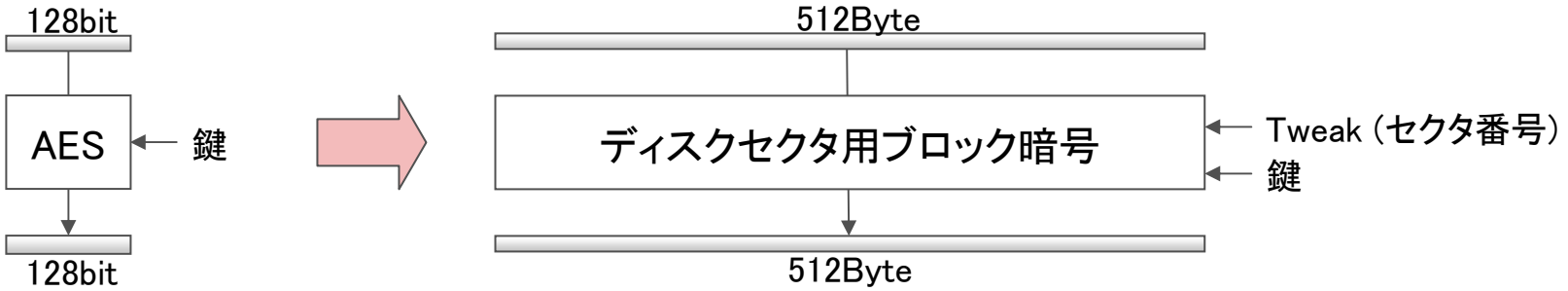
FUJITSU

Tweakable Block Cipher



性質：
- Tweakの値は公開可能
- Tweak更新処理は、鍵更新より軽い
- Tweakの攪拌性能は秘密鍵と同様
  （Tweak毎に異なるランダム置換を生成）

ディスクセクタ暗号化利用モード



- ディスクセクタのブロック単位は512Byte
- この512Byteをブロック長としたTweakable Block Cipher を構成し、より高いセキュリティを確保

暗号利用モードの設計思想

FUJITSU

ブロック暗号の欠点を補うパッチ

↓

安全な暗号プリミティブを手軽に構成する方法

キーワードその１：多様化～さまざまなバリエーションが登場

ブロック暗号	→ ストリーム暗号
	→ キーストリーム生成（擬似乱数生成）
ハッシュ関数	→ ブロック暗号（ワイドブロック暗号）
	→ メッセージ認証子（鍵付ハッシュ関数）
ストリーム暗号	→ ハッシュ関数

キーワードその２：証明可能安全性

安全なブロック暗号の利用を前提
（強）擬似ランダム置換
理想的ブロック暗号

⇨ 暗号利用モードの安全性を数学的に証明

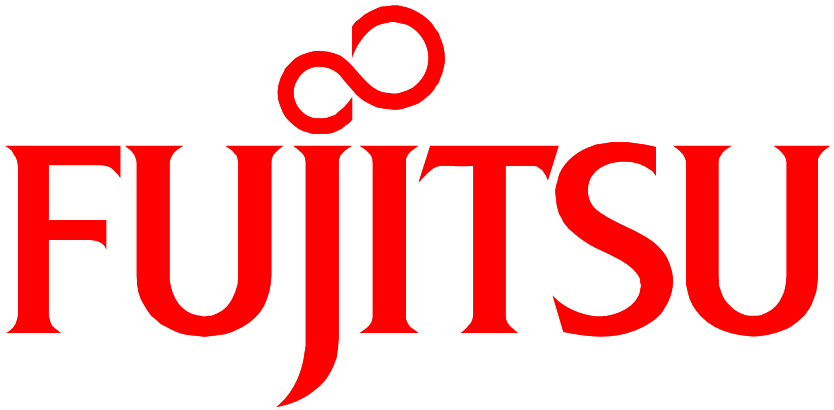
- 乱数列との識別不可能性
- 送（受）信者の否認不可能性
- （強）偽造不可能性

評価方法に対する意見

FUJITSU

- 全般
  - 公募カテゴリについて
    - 用途、鍵長、ブロック長等毎に分類？細分化しすぎるのは問題有。
    - 「モード」と「MAC」は、それぞれ「秘匿用モード」と「認証用モード」と解釈?
    - Hash, 一方向性関数は、安全性評価の統一の観点から「MAC」に分類?
    - 認証付秘匿モードは、「モード」？それとも「MAC」?
- セキュリティ要件
  - 証明可能安全性
    - 前提と、導かれる耐性、その妥当性、現実性
    - 証明の前提が崩れたときの耐性については？

    (例：HMACの鍵回復攻撃、Key Check Value(ANSI X9.24)等)
- パフォーマンス要件
  - 評価指標
    - 並列処理性、
    - 事前計算回数、
    - プリミティブ呼び出し回数/ブロック、
    - 鍵スケジュール呼び出し回数/ブロック、
  - 内部で用いるプリミティブは出来る限り共通化して評価
    - 鍵スケジュールと暗号化の性能比はブロック暗号毎に異なる。
    - ブロック暗号ベース vs ハッシュ関数ベース vs ストリーム暗号ベース　性能比較は？
- 標準化、利用実績
  - 各種標準化をどこまで取り入れるか？
    - ISO/IEC8372, 9797, 18033, NIST-SP800 38A,B,C,D, ANSI X3,X9, RFC2104, FIPS46-2, FIPS81,FIPS113, IEEE P1619.1,2, NESSIE, 3GPP,



THE POSSIBILITIES ARE INFINITE

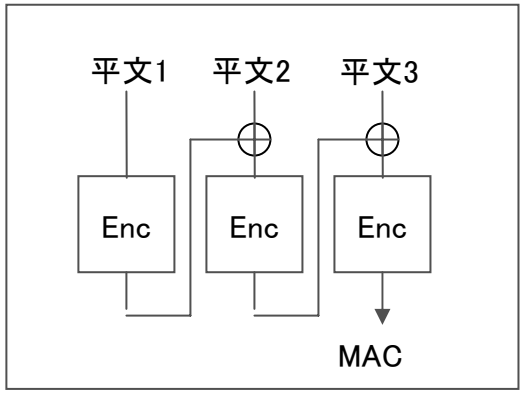
2009年2月18日
CRYPTRECワークショップ

メッセージ認証コード （MAC）

富士通研究所
下山武司

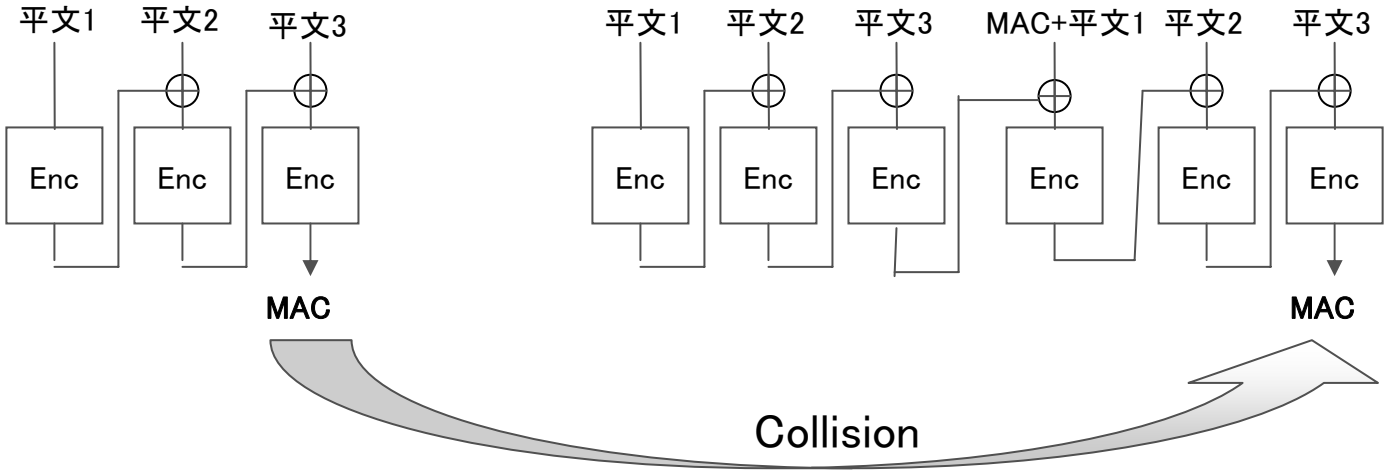
MAC

CBC-MAC



•広く使われているが、自明な欠点あり

Length Extension Attack



暗号利用モード一覧

FUJITSU

秘匿	ストリーム暗号	ABC, CBC, CFB, k-CFB, CTS, 2DEM, IGE,
	キーストリーム	OFB, CTR, CENC, F8, KFB,
	ブロック暗号	ABL3, ABL4, Bear, CMC, EMD, EME, EME2, Feistel, HCH, HCTR, Lion, LRW, Mercy, NR, PEP, TET, XEX, XCB, XTS,
認証	MAC	ALRED*, ALPHA-MAC*, CBC-MAC, CMAC, EMAC, F9, FRMAC, GMAC, HMAC*, IPMAC, MMH, MT-MAC, NMAC*, OMAC, PC-MAC, PELICAN*, PMAC, Poly1305-AES, RMAC, Tail-MAC, TMAC, Two-Track-MAC, UMAC, VMAC, XCBC-MAC, XECB-MAC, XOR-MAC,
	ハッシュ	AES-hash, EMD, Merkle-Damgard, MDP, PMD-MMO,
	一方向性関数	Davis-Meyer, abreast-DM, tandem-DM, Hirose-DBL, Matyas-Meyer-Oseas, Miyaguchi-Preneel, MDC-2, MDC-4,
認証付秘匿	CCM, CHM, CS, CWC, EAX, GCM, Key-Wrap-AES, IACBC, IAPM, MULTI-S01*, OCB, PCFB, k-PCFB, SIV, XCBC,	

最近の研究動向

FUJITSU

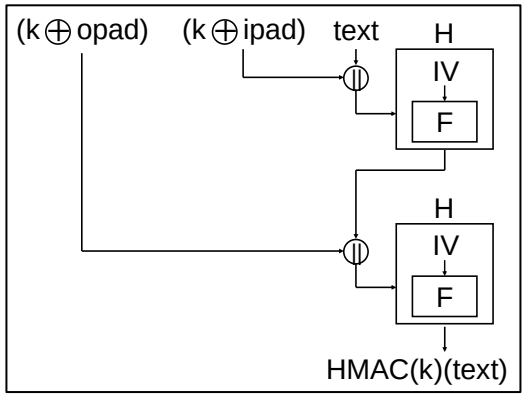
CMAC(OMAC) のNIST SP800-38B公開(2005/3)

- 岩田先生(名古屋大)と黒澤先生(茨城大)が開発(2003/2)
- 偽造困難性を1個のKeyで実現した証明可能安全なMAC

※ Key Check Value (ANSI 9.24)への対策が必要？

Hash関数をベースとするMACへの攻撃

HMAC



- TLS, SSH, IPsecにて利用
- 証明可能安全なMAC (安全なハッシュ関数を仮定)

しかし

- 脆弱なハッシュ関数を用いた場合は、鍵回復攻撃が可能

段数を削減したブロック暗号を利用したMACの登場 (MT-MAC, PELICAN等)

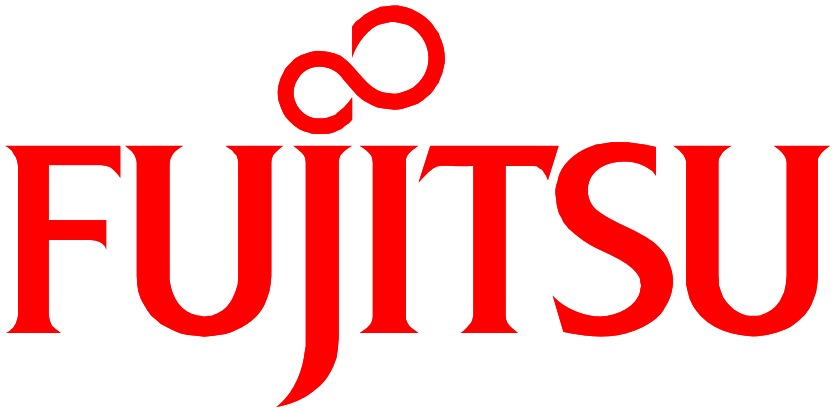
- 処理内部で4段のAESを利用し処理速度を向上(※128bit AESは10段)
- 証明可能安全ではあるが、攻撃論文も散見されるため、詳細な調査が必要。

評価方法に対する意見

FUJITSU

- 全般
  - 公募カテゴリについて
    - 用途、鍵長、ブロック長等毎に分類？細分化しすぎるのは問題有。
    - 「モード」と「MAC」は、それぞれ「秘匿用モード」と「認証用モード」と解釈?
    - Hash, 一方向性関数は、安全性評価の統一の観点から「MAC」に分類?
    - 認証付秘匿モードは、「モード」？それとも「MAC」?
- セキュリティ要件
  - 証明可能安全性
    - 前提と、導かれる耐性、その妥当性、現実性
    - 証明の前提が崩れたときの耐性については？

    (例：HMACの鍵回復攻撃、Key Check Value(ANSI X9.24)等)
- パフォーマンス要件
  - 評価指標
    - 並列処理性、
    - 事前計算回数、
    - プリミティブ呼び出し回数/ブロック、
    - 鍵スケジュール呼び出し回数/ブロック、
  - 内部で用いるプリミティブは出来る限り共通化して評価
    - 鍵スケジュールと暗号化の性能比はブロック暗号毎に異なる。
    - ブロック暗号ベース vs ハッシュ関数ベース vs ストリーム暗号ベース　性能比較は？
- 標準化、利用実績
  - 各種標準化をどこまで取り入れるか？
    - ISO/IEC8372, 9797, 18033, NIST-SP800 38A,B,C,D, ANSI X3,X9, RFC2104, FIPS46-2, FIPS81,FIPS113, IEEE P1619.1,2, NESSIE, 3GPP,



THE POSSIBILITIES ARE INFINITE