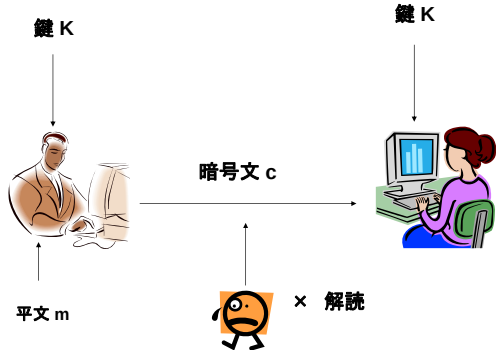
共通鍵暗号について

黒澤　馨
茨城大学　工学部

内容

- 準備
- 暗号化モード
- MAC方式モード
- Authenticated Encryption
- Tweakable ブロック暗号
- CMAC

共通鍵暗号系のモデル



無条件な安全性

- シャノンが定義。
- 敵が無限大の能力を持っていると仮定。

- 暗号系は無条件に安全 if
  Pr(平文=m | 暗号文=c)＝Pr(平文=m)
  for any m and any c.

シャノンの定理

- 無条件に安全な暗号系においては、
  鍵の長さ ≧平文の長さ

シャノンの定理

- 無条件に安全な暗号系においては、
  鍵の長さ ≧平文の長さ

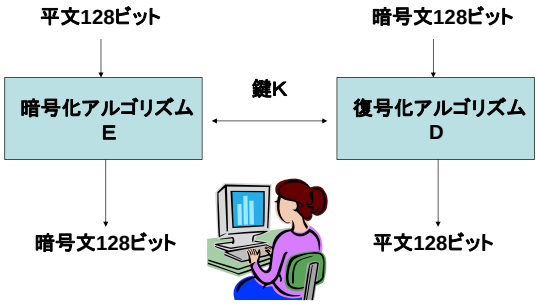
- 対偶:
  鍵の長さ ＜平文の長さ
  だと、敵に何らかの情報が漏れる。

One-Time-Pad

- 暗号文＝平文＋鍵（ランダム）
  鍵の長さ＝平文の長さ。

- 任意の平文の確率分布に対し、
  Pr(平文=m | 暗号文=c)＝Pr(平文=m)
  for any m and any c.
  を証明できる。

ブロック暗号



ブロック暗号

- ブロック暗号は、
  平文Mから暗号文Cへの置換。
  鍵が置換を決定。

AES暗号

- 鍵の長さ：128ビット、192ビット、256ビット

- 鍵長＝128ビットの場合、
  平文>128ビットだと、
  シャノン定理より無条件に安全ではない

- 平文の何らかの情報が敵に漏れている。

計算量的な安全性

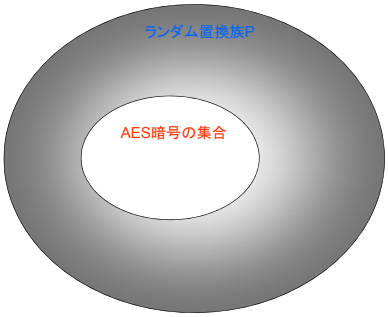
- 敵は、多項式時間アルゴリズム。

- 特に、
  AES暗号は擬似ランダム置換、
  と仮定。

ランダム置換族 P

- 128ビットから128ビットへの置換の
  全ての集合
- 最強のブロック暗号

- 置換の総数＝(2^128)! 個
  鍵長＝log_2 (2^128)! ビット
  ＝ exponentially long !!



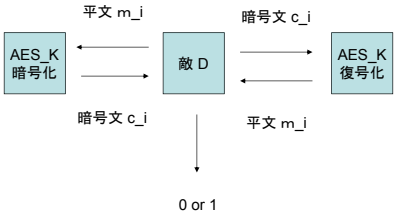
擬似ランダム置換族

- AES暗号の総数＝2^128 個
- AES暗号の集合⊂ランダム置換族P

- 定義：
  AES暗号は擬似ランダム置換族
  if AES暗号とPは indistinguishable。

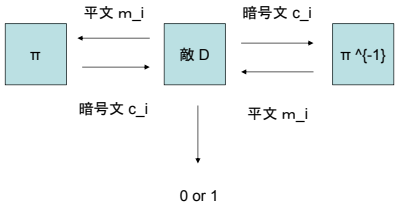
実験 0

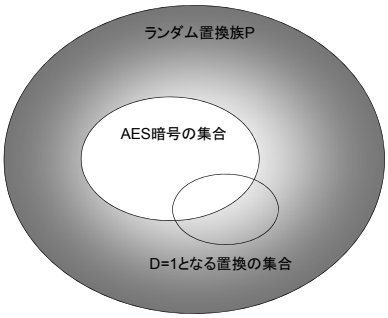
- AES暗号の鍵Kをランダムに選ぶ。

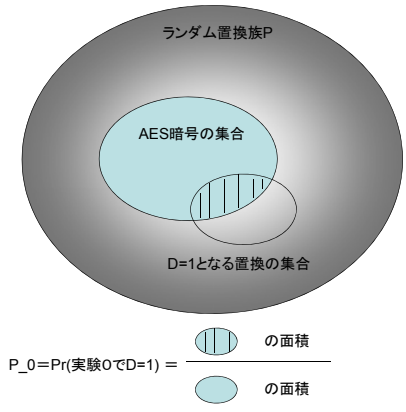


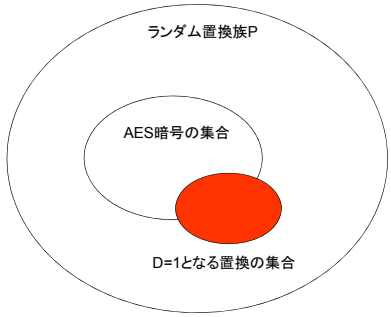
実験 1

- ランダム置換族Pから、
  置換πをランダムに選ぶ









$P\_1 = Pr(\text{実験1でD=1}) = \frac{\text{赤の面積}}{\text{全面積}}$

Indistinguishability

- AES暗号の集合とランダム置換族Pは indistinguishable
  if
  |p_0-p_1| = negligible
  for any 多項式時間のD.

擬似ランダム置換族

- 定義:
  AES暗号は擬似ランダム置換族
  if AES暗号とランダム置換族Pは
  indistinguishable.

我々の仮定

- AES暗号は擬似ランダム置換族。

ランダム関数族 F

- 128ビットから128ビットへの関数の全ての集合 F

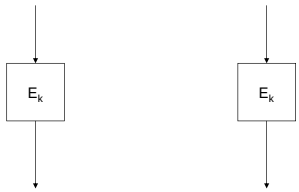
- 定義:
  関数の集合Xは擬似ランダム関数族
  if XとFはindistinguishable.

定理

- ランダム置換族Pは、擬似ランダム関数族
（略証）
- 128ビットの任意のビット列x≠yに対し、
- ランダム置換πにおいては、
  Pr[π(x)=π(y)]=0
- ランダム関数 f においては、
  Pr[f(x)=f(y)] =1 / 2^{128}
- 差分はnegligible

ECBモード

平文 = (m1,・・・・・・・・・・・・・・・・・,mt)

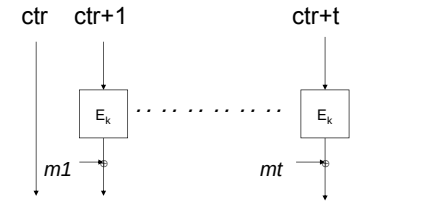


暗号文=(c1,・・・・・・・・・・・・・・・・・,ct)

欠点

- c1=c2の場合、
  m1=m2
  ということが、敵にわかってしまう。

カウンタモード

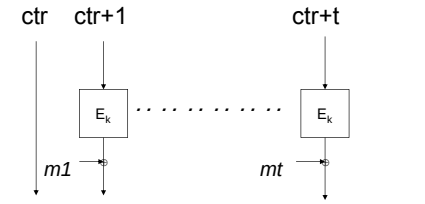


(ctr, c1,・・・・・・・・・・・・・・・・・,ct)＝暗号文

安全性の証明

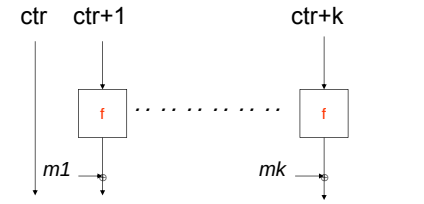
- AES暗号～ランダム置換族 P （仮定）
  ～ランダム関数族 F （定理）
- AES暗号E_Kを、ランダム関数 f
  に置き換えても、敵は区別できない。

カウンタモード



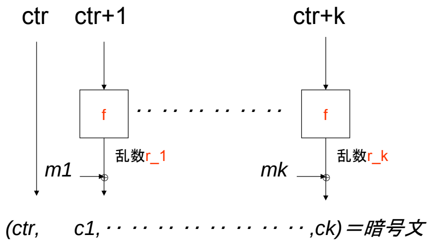
(ctr, c1,・・・・・・・・・・・・・・・・・,ct)＝暗号文

理想化したカウンタモード

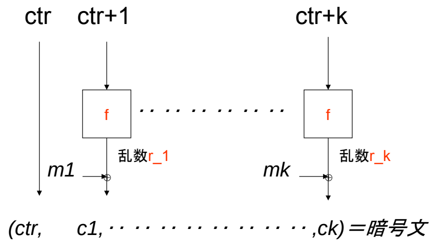


(ctr, c1,・・・・・・・・・・・・・・・・・,ck)＝暗号文

理想化したカウンタモード



One-Time-Pad

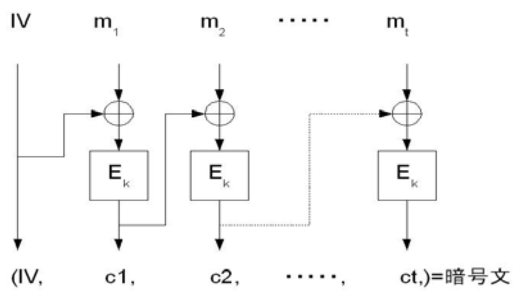


よって、安全

CTRモードの標準化

- DHが1979年に提案
- 米国NIST標準 SP800-38A
  AES暗号制定の際に追加

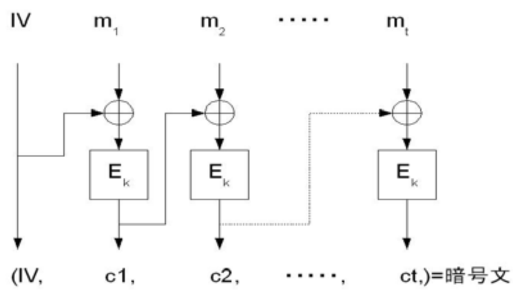
CBCモード



IVについて

- IV=固定、あるいはカウンタの場合
  安全でない。
- IV=乱数なら、
  安全性が証明されている。

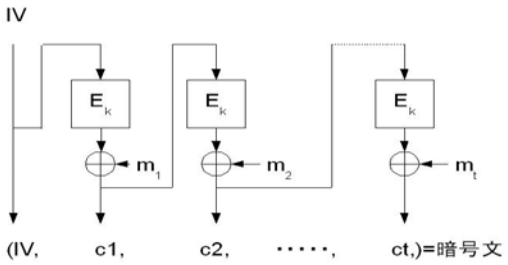
CBCモード



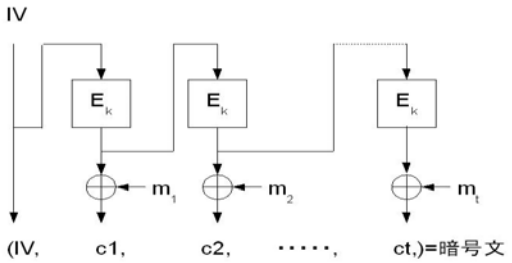
NISTの SP800-38A

- For the CBC and CFB modes,
  the IV for any particular execution of the encryption process must be unpredictable.
- For the OFB mode,
  unique IVs must be used for each execution of the encryption process.

CFBモード



OFBモード



標準化

- CBCモード、CFBモード、OFBモード
- 米国NIST標準
  FIPS81、SP800-38A
- 米国の国内規格
  ANSI X3
- ISO 8372, ISO/IEC 10116

共通鍵暗号系の安全性

- Bellare, Desai, Jokiph, Rogaway,

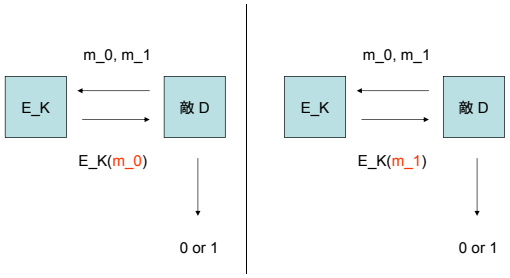
  “A concrete Security Treatment of Symmetric Encryption”

  at FOCS’97

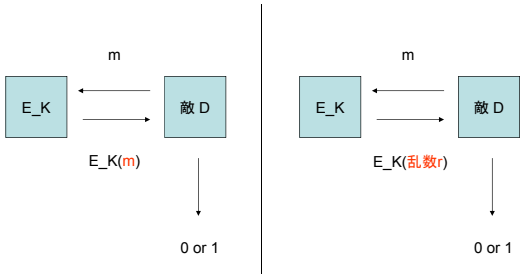
4つの安全性の定義

- LOR (Left or Right) CPA (CCA)
- ROR (Real or Random) CPA (CCA)
- FTG (Find then Guess) CPA (CCA)
- SEM (Semantic Security) CPA (CCA)

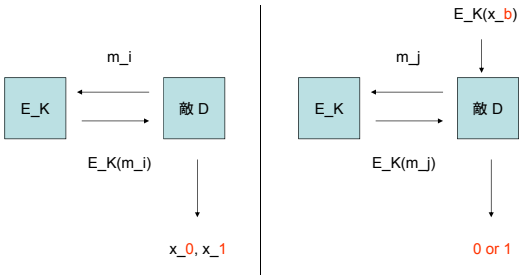
LOR-CPA 安全性



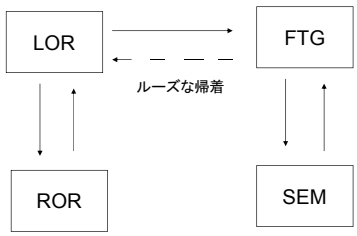
ROR-CPA 安全性



FTG-CPA 安全性



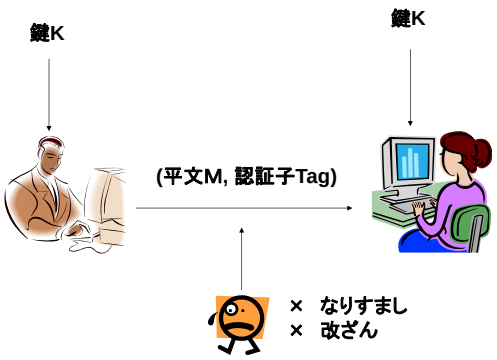
相互関係



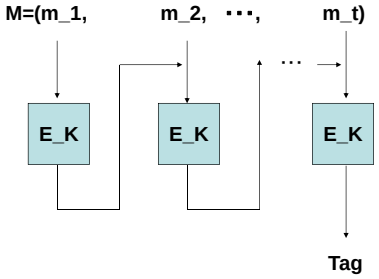
各モードのLOR-CPA安全性

- CTRモード, CBCモード
  BDJR (FOCS 1997)
- CFBモード
  Alkassar, Geraldy, Birgit Pfitzmann, Sadeghi (FSE 2001)
- CTR-OFBモード
  Jaechul Sung, Sangjin Lee, Jongin Lim, Wonil Lee, Okyeon Yi (ICISC 2001)

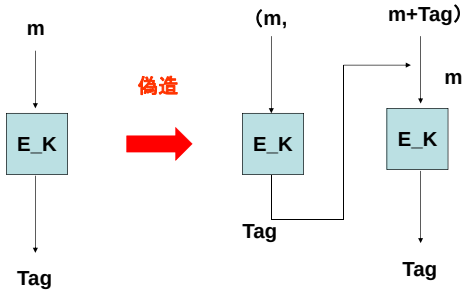
MAC方式のモデル



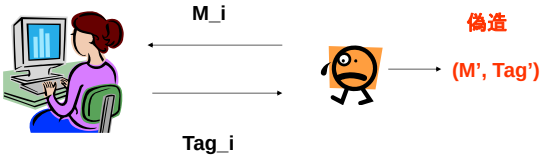
CBC-MAC



CBC-MACの脆弱性



安全性のモデル

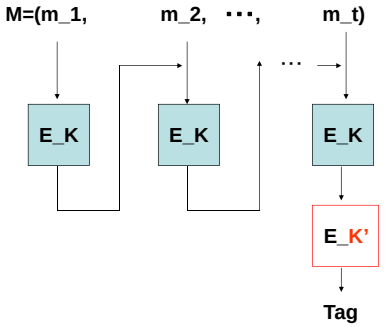


選択メッセージ攻撃

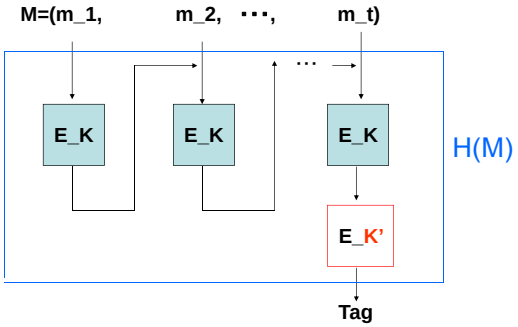
CBC MAC の安全性

- 平文が固定長の場合は安全
- しかし、可変長の平文を許す場合は、偽造可能

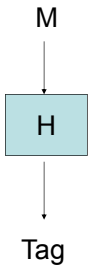
EMAC



EMAC



一般に、



MAC定理

Hが擬似ランダム関数

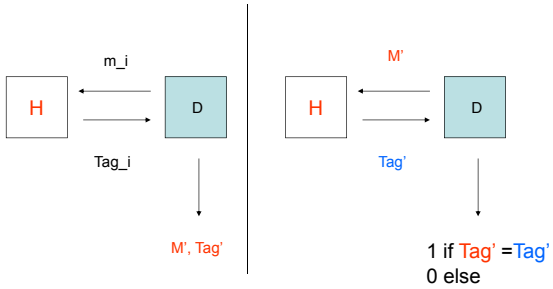
⇓

Hは安全なMAC方式

証明

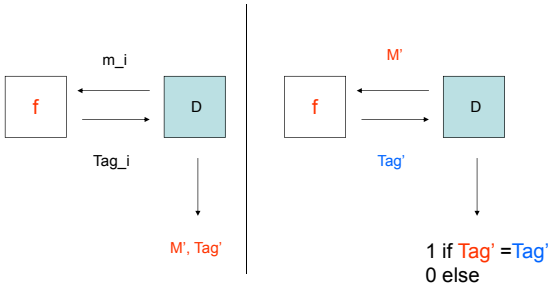
- Hに対し、選択平文攻撃により、確率εで偽造可能と仮定。
- すると、Hと擬似ランダム関数 f ではないことを示す。

実験0



Pr(D=1)=ε

実験1



Pr(D=1)=1/2^{128}

証明（続き）

- オラクルがHの場合、
  Pr(D=1)=ε
- オラクルがランダム関数 f の場合、
  Pr(D=1)=1/2^{128}

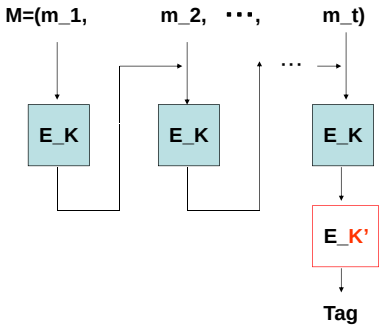
証明（続き）

- オラクルがMAC方式H_Kの場合、
  Pr(D=1)=ε
- オラクルがランダム関数 f の場合、
  Pr(D=1)=1/2^{128}
- Hは擬似ランダム関数ではない。

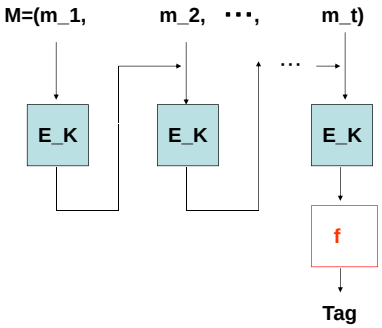
証明（続き）

- オラクルがMAC方式H_Kの場合、
  Pr(D=1)=ε
- オラクルがランダム関数 f の場合、
  Pr(D=1)=1/2^{128}
- H_Kは擬似ランダム関数ではない。
- 対偶：
  Hが擬似ランダム関数なら、
  Hは偽造不可能。

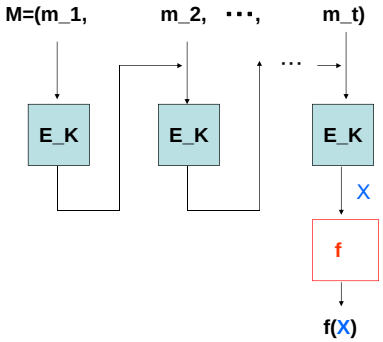
EMAC=擬似ランダム関数を証明

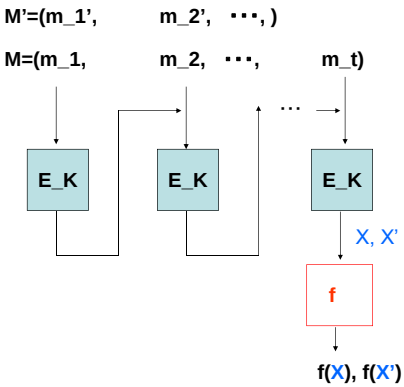


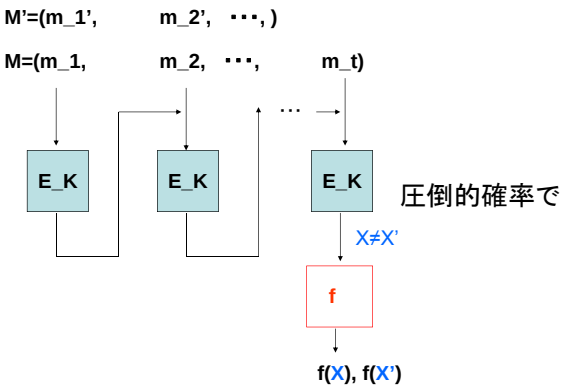
E_K'=擬似ランダム関数fより

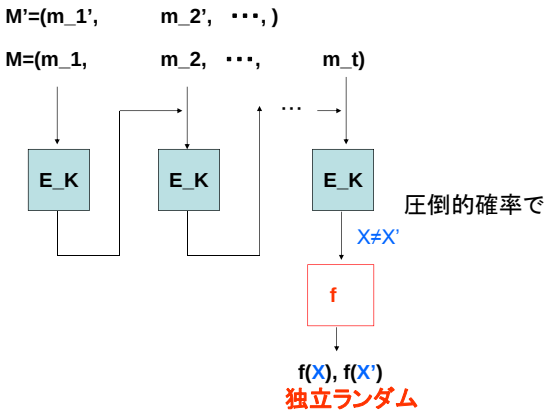


X=CBC(M)とおく

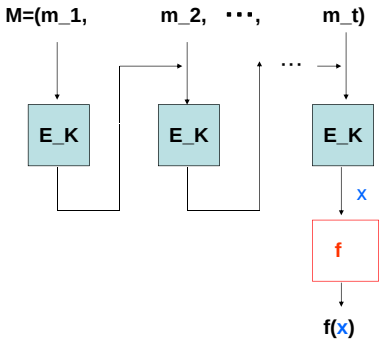








EMACは擬似ランダム関数



EMACの安全性証明

- EMACは擬似ランダム関数を証明した。
- よって、MAC定理より、EMACは安全。

EMAC の標準化

- ISO9797-1 (1995)

Tweakable ブロック暗号

- Listov, Rivest and Wagner (Crypto 2002)
- 一つの秘密鍵 Kのみから、
  多くの独立な擬似ランダム置換を得る方法。

C_1= [E]_K(公開情報 T_1, 平文)
C_2= [E]_K(公開情報 T_2, 平文)
…

実は、

- 黒澤も、似たようなことを考えていた。
- 悔しいので、ePrintに掲載。
- 最近、Louis Granboulanからメールあり。
  (Crypto, Eurocrypt, FSE等で、
  多くの論文を書いている人。)

Louis Granboulan

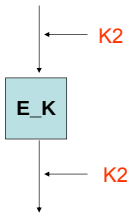
- I am wondering
  why this paper has not been published.
- In my opinion,
  it contains new and interesting results.

(2008年1月12日)

おかげで、IEEEに掲載

Kaoru Kurosawa,
"Power of a Public Random Permutation and
Its Application to AuthenticatedEncryption"
IEEE Transaction on Information Theory,
56, 10, 5366-5374, 2010/10

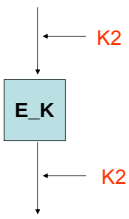
DESX (鍵2つ:KとK2)



Rivestが提案
DESの安全性強化が目的。

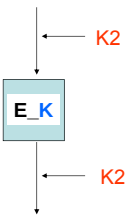
Kilian and Rogaway

実質鍵長が、本当に長くなっていることを証明。



Even and Mansour

Kを公開しても、安全であることを証明。

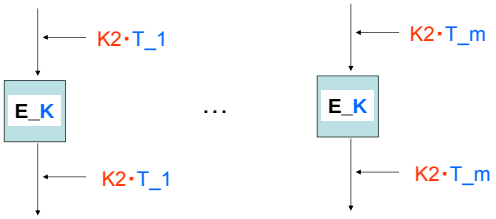


黒澤 (ePrint 2002)

- 秘密鍵K2のみから、
  多くの擬似ランダム置換 P_1, …, P_m
  を構成できることを示した。
  (Even and Mansourは、m=1の場合。)
- Authenticated Encryptionに応用。

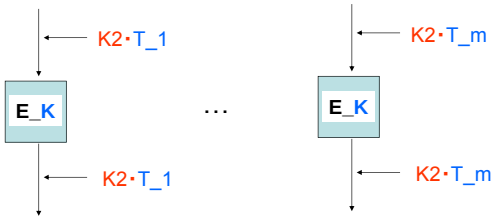
提案方式

K2のみ秘密。
T_1, …, T_mは、任意の公開情報。



定理

以下は、m個の独立な擬似ランダム置換。
また、
K2・Tの部分は、任意のAXU hash関数でよい。

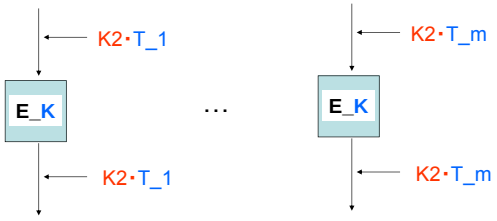


AXU-ハッシュ関数族

- 以下のような H={hash 関数 h}.
  h ∈H をランダムに選んだとき、
  for any T and T',
  h(T)+h(T')= almost ランダム

Listovらの構成

K2、Kの両方が秘密。
T_1, …, T_mは公開情報。



Listovらとの関係

- AES暗号の鍵Kを秘密にすると、
  Listovらの構成に一致する。
- 言い換えると、提案方式は、
  ブロック暗号の鍵Kを公開可能な
  Tweakableブロック暗号の構成を与えている。

Authenticated Encryption

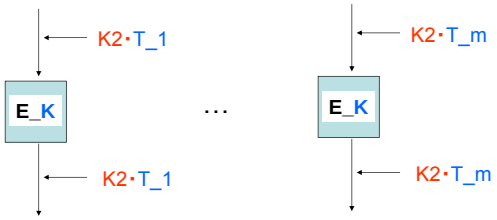
- Counter mode（暗号化）＋MAC（認証）と同じ機能を、少ない計算量で実現する方式
- IAPM (Jutla, 2001)
- OCB mode (Rogaway, et.al. 2001)
  平文の長さ≠128ビットの整数倍でもいいようにIAPMを改良。

提案方式の応用

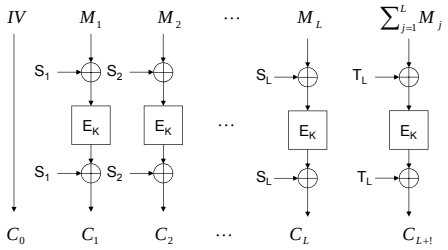
- AES暗号の鍵公開の、IAPM
- AES暗号の鍵公開の、OCB モード
  安全性証明も非常に簡単

提案方式

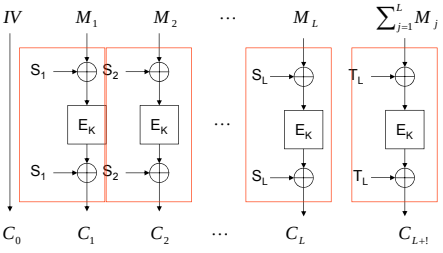
K2のみ秘密。
T_1, …, T_mは、任意の公開情報。



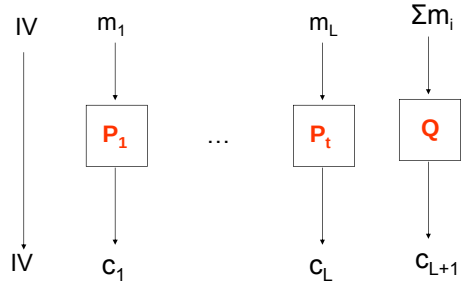
提案するIAPM



提案するIAPM



理想化したIAPM



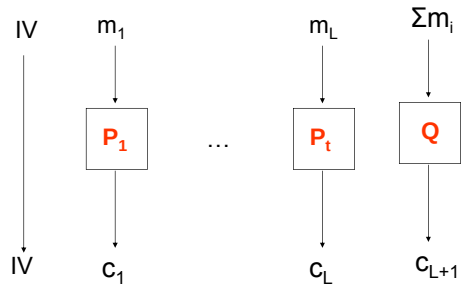
P_i, Qは、IV毎に独立なランダム置換

安全性

敵は、選択平文攻撃をしても、

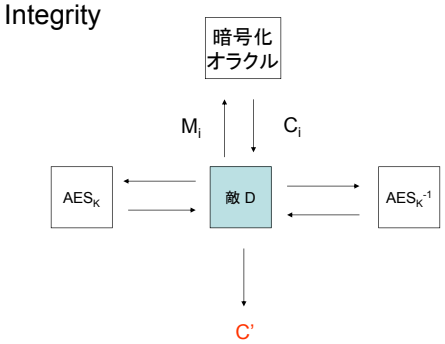
- (Privacy)
  暗号文を解読できない。
- (Integrity)
  正当な暗号文を偽造できない。

Privacy



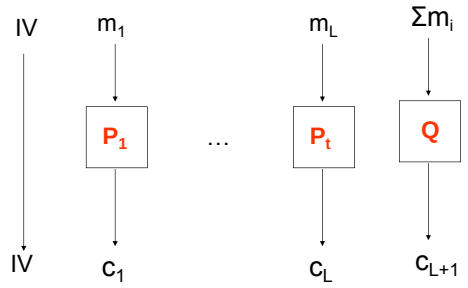
P_i, Qは、IV毎に独立なランダム置換

Integrity



敵は成功 if
C'は正当な暗号文で、かつC'の平文M'≠M_i

Integrity



P_i, Qは、IV毎に独立なランダム置換

計算量

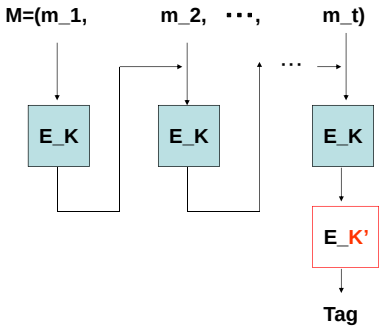
- Counter mode（暗号化）＋MAC（認証）の半分

比較

	オリジナルのIAPM	提案方式
AES暗号の鍵K	秘密	公開
S_i, T_L	AES暗号を使って生成	AXU-hash関数を使って生成
証明	複雑	簡単

OCBモードに対しても、同様な結果。

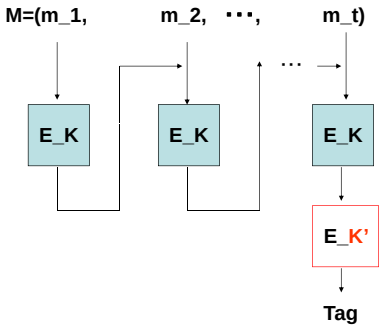
EMACは、鍵が2つ必要



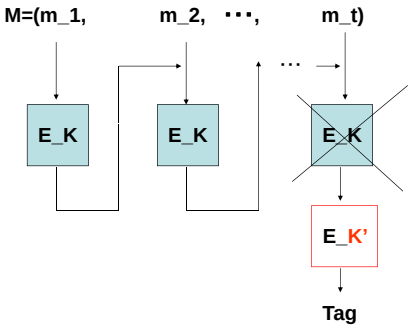
EMACの改良

- XCBC: Black and Rogaway (2000. 6)
  ブロック暗号の鍵1つ＋他の鍵2つ
- TMAC: 黒澤・岩田 (2002. 7)
  ブロック暗号の鍵1つ＋他の鍵1つ
- OMAC: 岩田・黒澤 (2002.12) → CMAC
  ブロック暗号の鍵1つのみ。

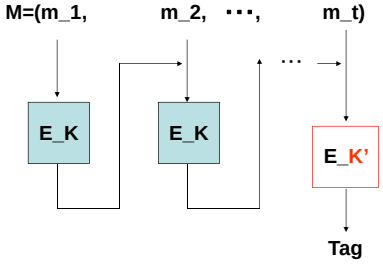
EMACの改良



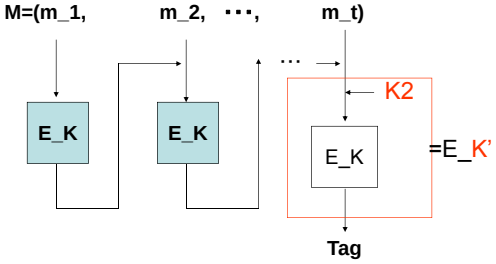
EMAC



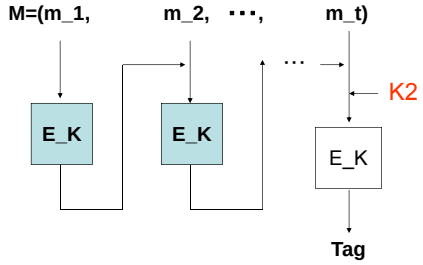
EMACの変形



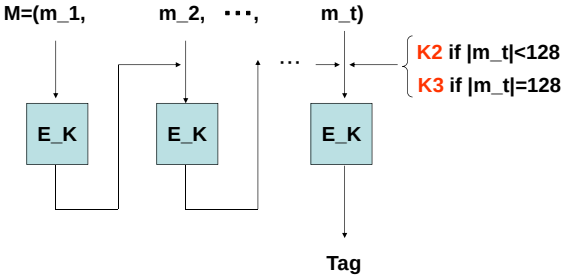
EMACの変形



EMACの変形

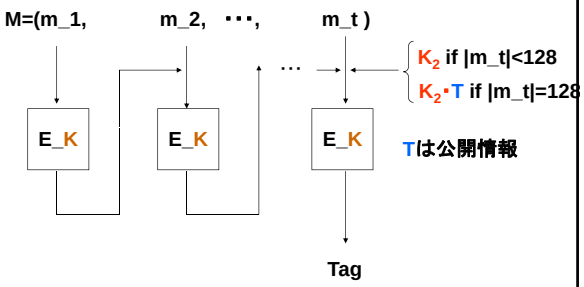


XCBC (Black & Rogaway)



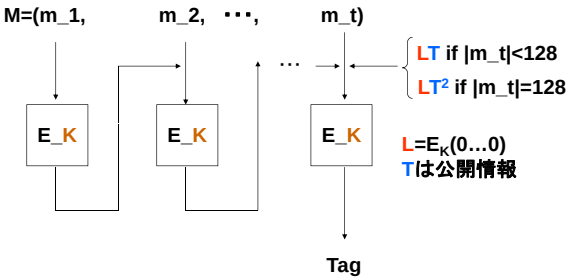
鍵＝(K, K2, K3)

TMAC (黒澤、岩田)



鍵＝(K, K_2)： 2つで済む

OMAC (岩田、黒澤)



鍵＝K： 1つで済む

EMACの改良

- XCBC: Black and Rogaway (2000. 6)
  ブロック暗号の鍵1つ＋他の鍵2つ
- TMAC: 黒澤・岩田 (2002. 7)
  ブロック暗号の鍵1つ＋他の鍵1つ
- OMAC: 岩田・黒澤 (2002.12) → CMAC
  ブロック暗号の鍵1つのみ。

CMAC の標準化動向 (1)

- NIST 推奨方式
  (セキュリティ技術では日本初)
- CSE（カナダ国防省通信安全局）標準方式
- ISO での国際規格化に向け検討されている。
- Windows XP (SP2) で使用されている。
- IBM, Intel, Microsoft, 松下, ソニー, 東芝, ディズニー, ワーナーが開発しているAACSという著作権保護技術で使用されている。

CMACの標準化動向 (2)

- IETFのRFC4493,4494,4615にも採用。
- 無線LANより広いエリアをカバーする規格であるIEEE 802.16eでも採用。