CryptoVerif のための MAC の安全性の定式化に関する考察

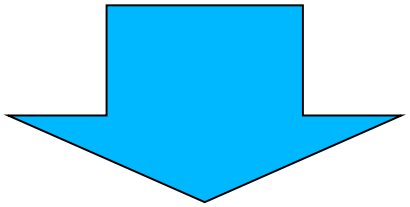
2007/9/15

○*荒井　研一，**岡崎　裕之，**不破　泰

*信州大学大学院総合工学系研究科
**信州大学大学院工学系研究科

CryptoVerif

- CryptoVerif とは
  - Blanchetが作成(自身のサイトで公開)
  - ゲーム列による安全性の検証を自動で行うプログラム



FDH署名の安全性検証を自動化できることが示されている

ゲーム列による安全性証明

- ゲーム列による安全性証明について

V. Shoup, “Sequences of games: a tool for taming complexity in security proofs,”

ゲームとは・・・
攻撃者と挑戦者との間で行われる攻撃ゲーム

セキュリティが破られる ⇔ 攻撃者が勝利

計算量的安全性 ⇔ 攻撃者の勝つ確率が十分に小さい

ゲーム列による安全性証明

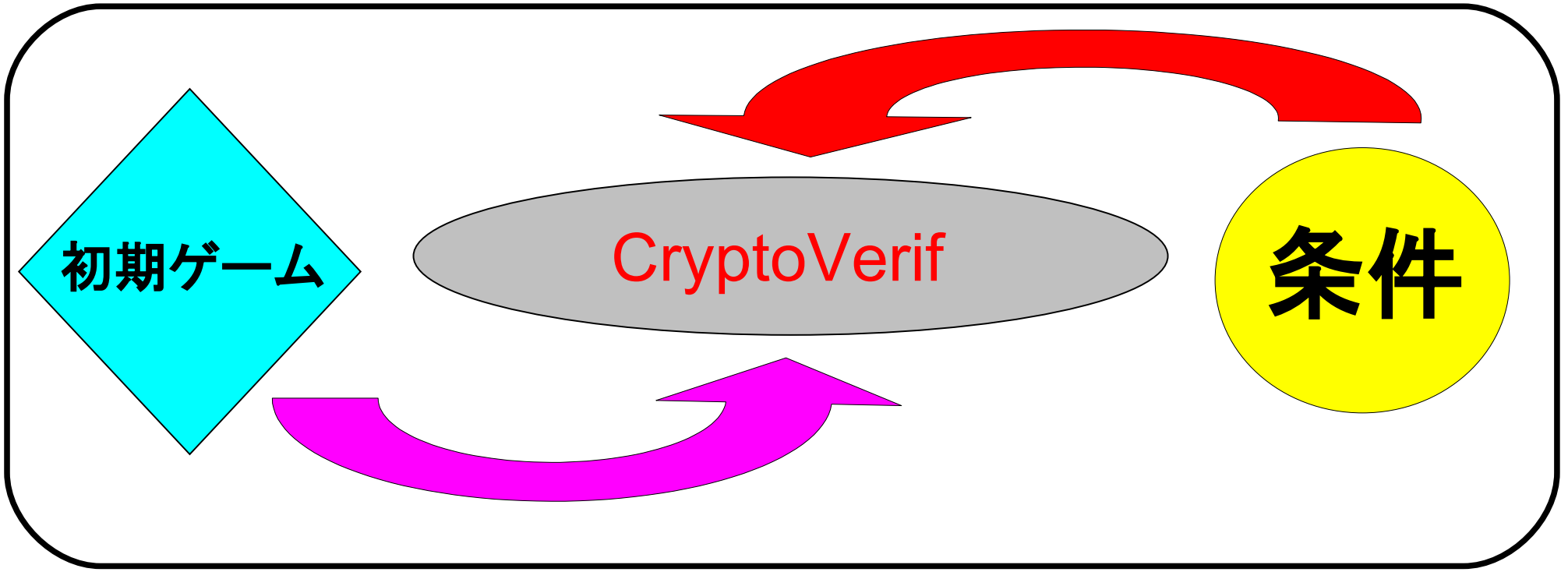
- ゲーム列による安全性証明とは

初期ゲームを次々に変換しながら

- 攻撃者の勝つ確率は各ステップでほとんど変化しない
- 最終ゲームでは攻撃者が勝つ確率が十分に小さい

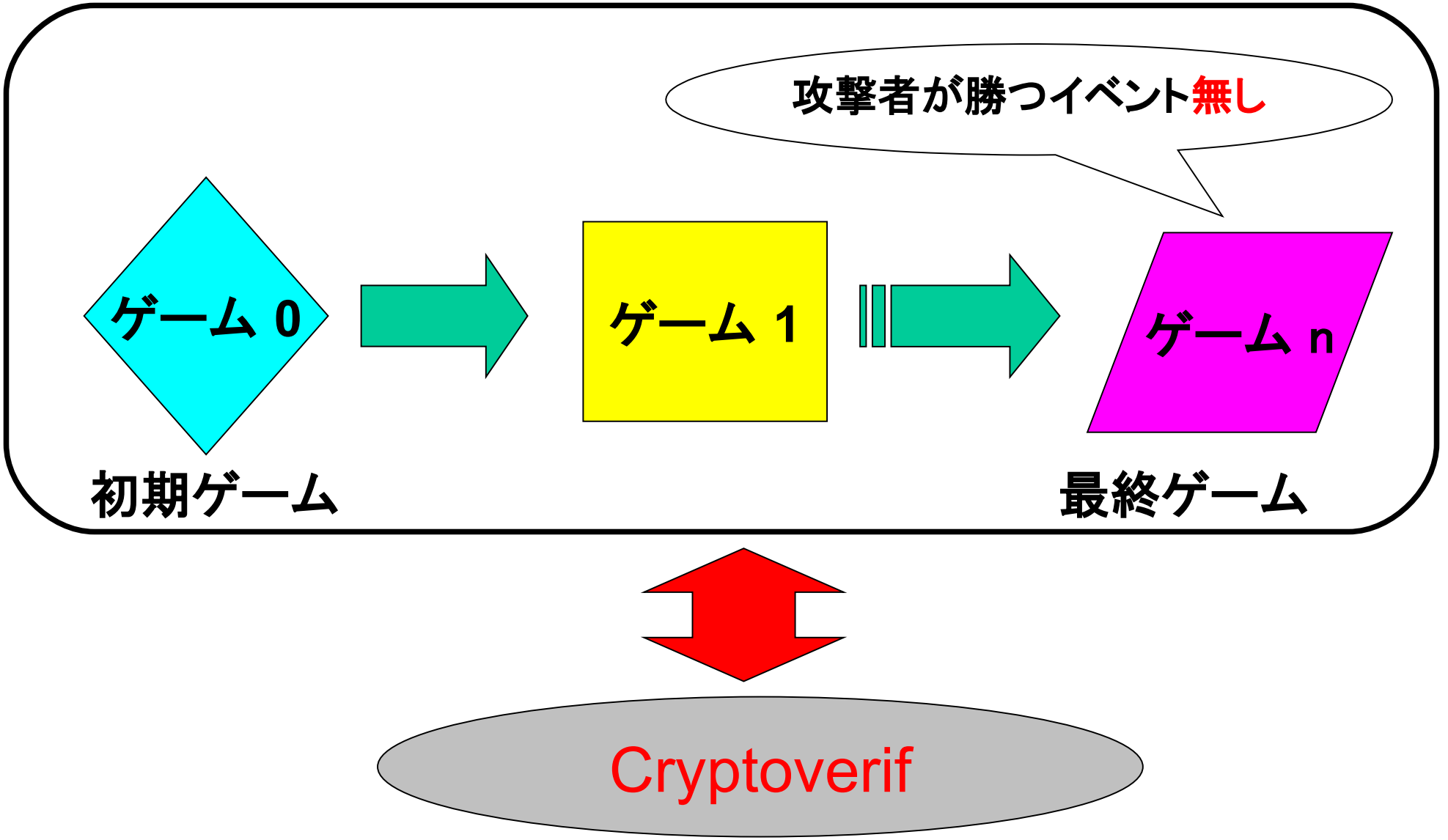
を証明する

ゲーム列による検証の自動化



初期ゲームと条件を与える

ゲーム列による検証の自動化

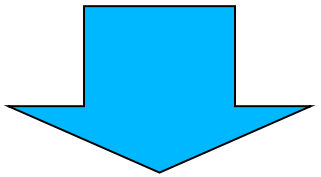


与えられた条件から最終ゲームに到達可能かを判定

CryptoVerifのSampleについて

- 既に与えられている暗号プロトコルについて

•認証プロトコル
•鍵交換プロトコル



Sampleにいくつかあり

•Otway-Rees
•Needham-Schroeder
etc…

CryptoVerifのSampleについて

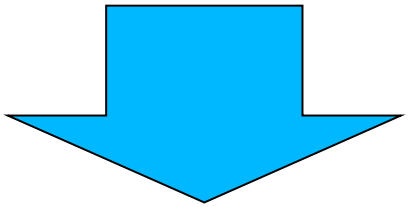
- 既に与えられている暗号プリミティブについて

  - 落とし戸付き一方向性関数
  - 強擬似ランダム置換
  - UF-CMA Signature
  - UF-CMA MAC
  - IND-CCA2 公開鍵暗号

  etc…

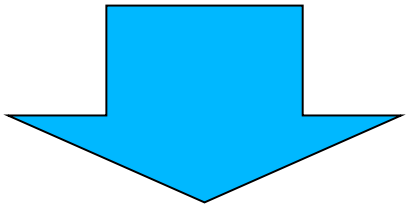
MACの安全性の定式化

暗号プリミティブとしてのUF-CMAなMAC



既に与えられている

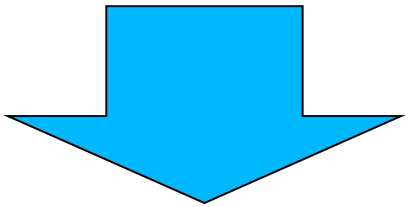
MAC自体の安全性の評価



評価がなされているものはない

MACの安全性の定式化

MAC：共通鍵暗号方式のブロック暗号を利用

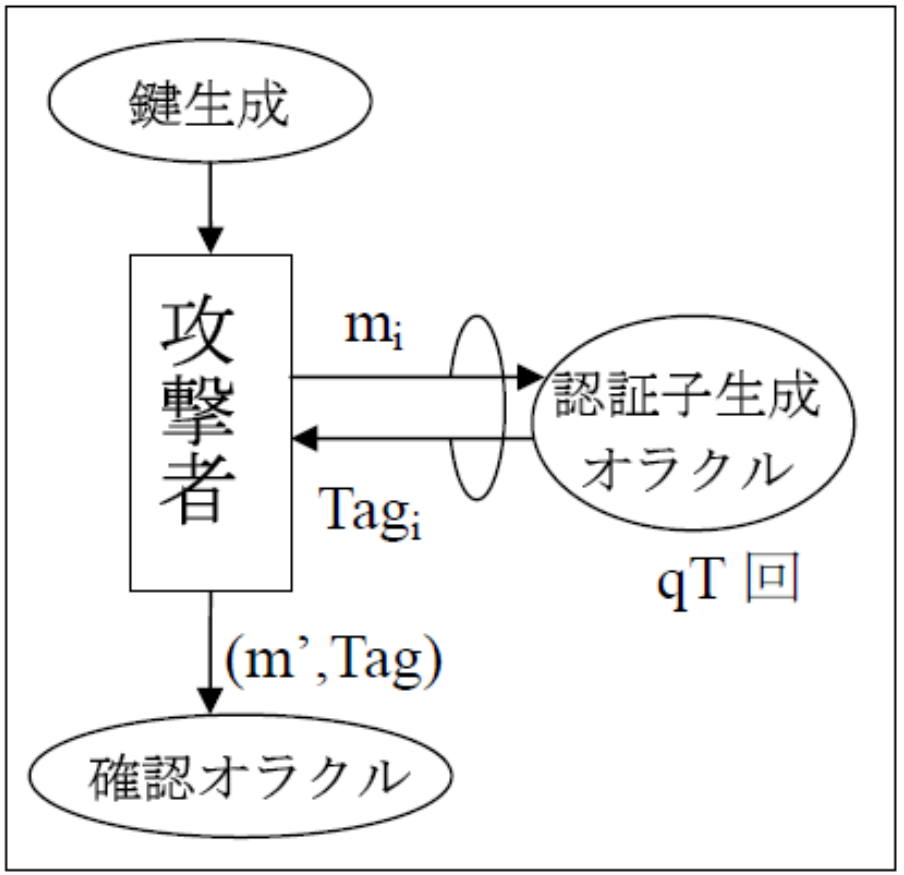


ブロック暗号の安全性

擬似ランダム置換

強擬似ランダム置換

選択メッセージ攻撃のもとでのMACの定式化

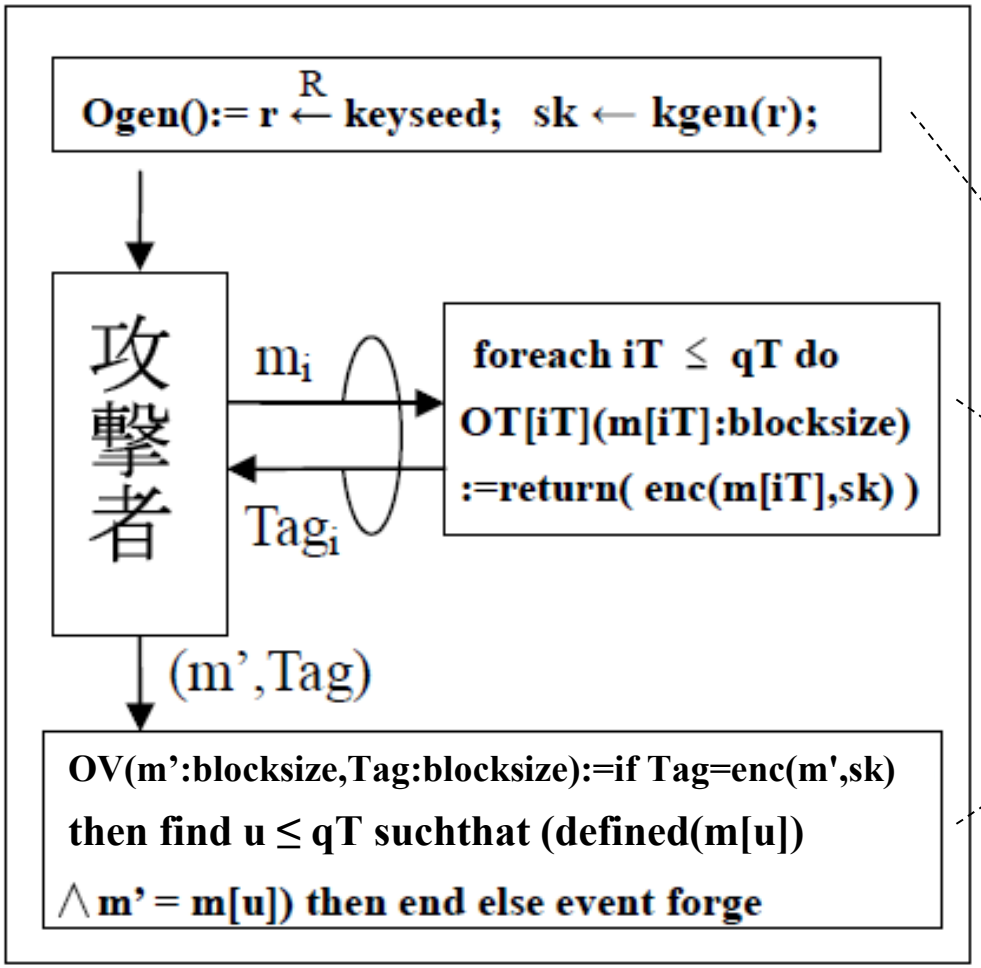


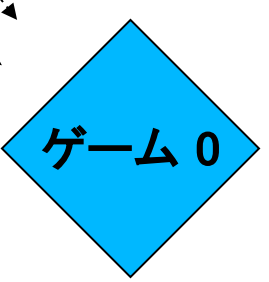
攻撃者は認証子生成オラクルを与えられて未知の認証子を生成しようとする

$(m' \notin \{m_1,\ldots,m_i\})$

生成できたら攻撃者の勝ち

MACの定式化におけるCryptoVerifのコード





初期ゲーム

強擬似ランダムであるブロック暗号を
安全性の根拠として評価

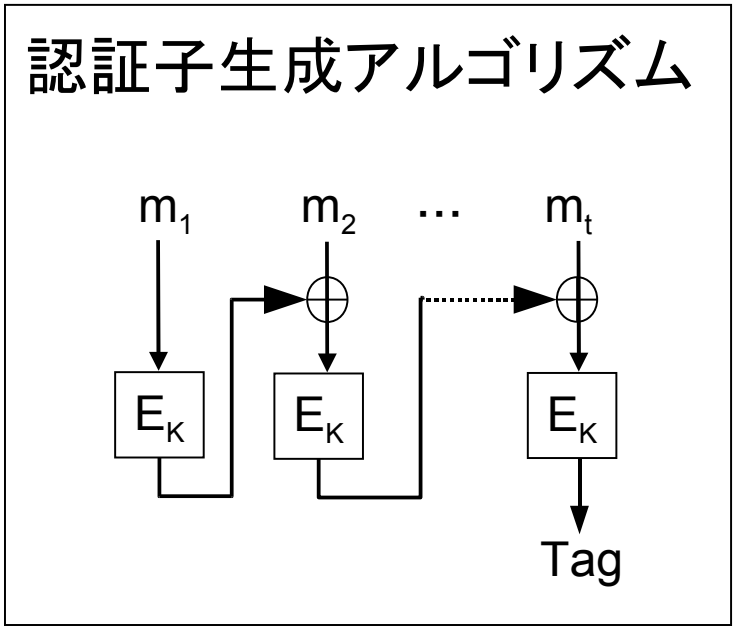
CBC-MACの安全性の定式化

- CBCモードによるMAC

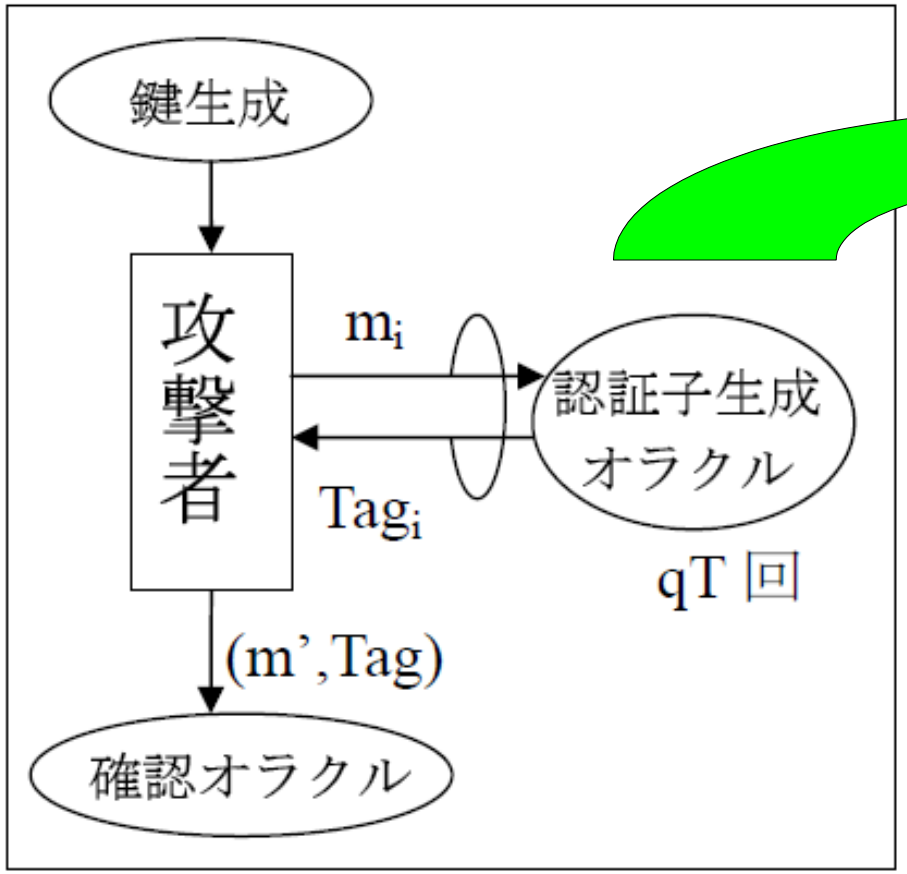
認証子生成アルゴリズム

メッセージ $M = (m_1, \ldots, m_t)$,
$|m_j| = n,\ j = 1, \ldots, t$

$C_1 = E_K(m_1)$
$C_2 = E_K(C_1 \oplus m_2)$
$\vdots$
$C_t = E_K(C_{t-1} \oplus m_t)$
$Tag = C_t$



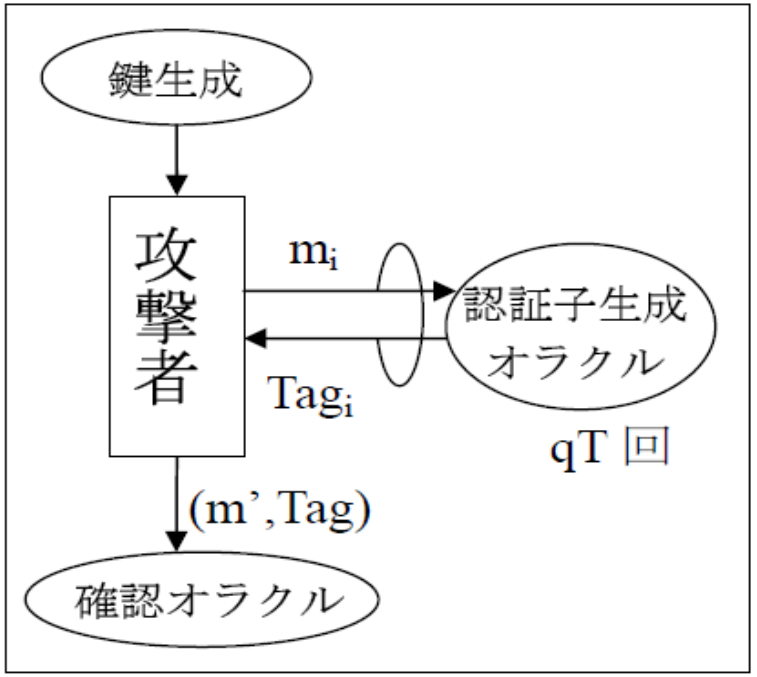
CBC-MACの安全性の定式化



Concat(A,B) ⇒ A||B

Xor(A,B) ⇒ $A \oplus B$

CBC-MACの安全性の定式化



認証子生成アルゴリズム

メッセージ$M = (m_1, ..., m_t)$,
$|m_j| = n,\ j = 1, ..., t$

$C_1 = E_K(m_1)$
$C_2 = E_K(C_1 \oplus m_2)$
⋮
$C_t = E_K(C_{t-1} \oplus m_t)$
$Tag = C_t$

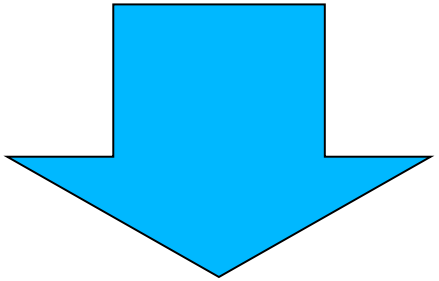
記述する際に，メッセージMのtブロック目という指定ができない

CBC-MACの安全性の定式化

M = (m_1 , m_2)

M = (m_1 , m_2, m_3)

M = (m_1 , m_2, m_3, m_4)



M.Bellare, J.Kilian, and P.rogaway. “The security of the cipher block chaining message authentication code,”

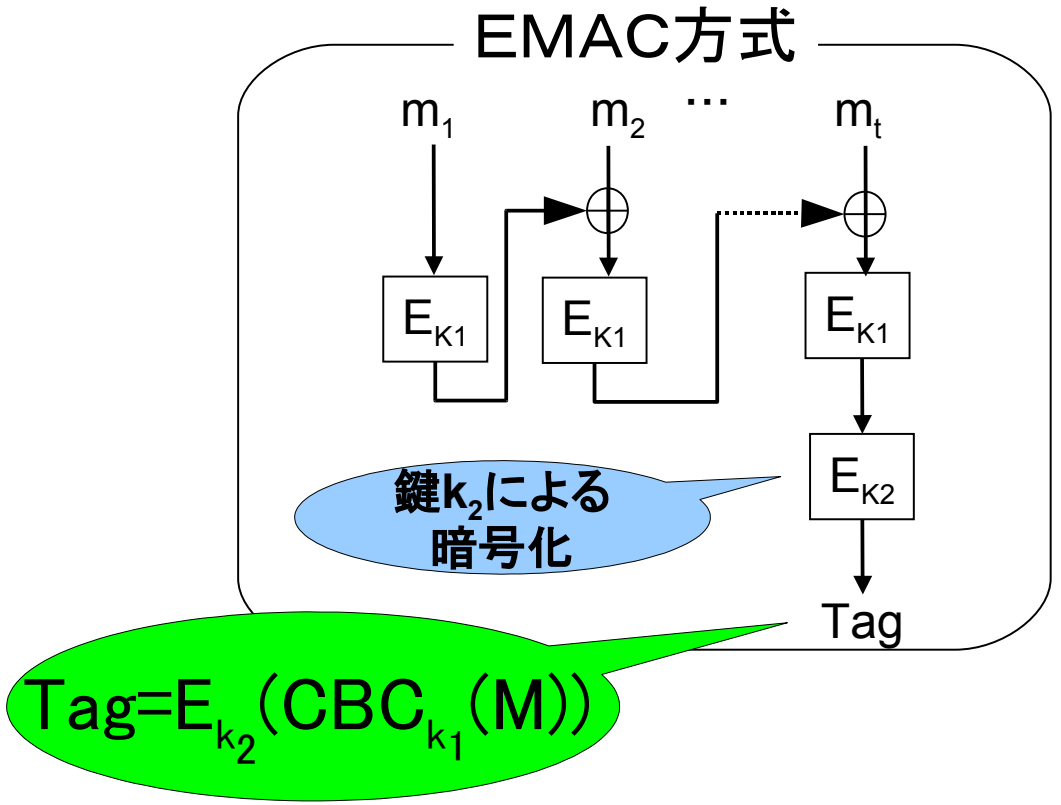
$$\mathbf{Adv}^{\mathrm{mac}}_{\mathrm{CBC}^m\text{-}F}(q,t) \leq \mathbf{Adv}^{\mathrm{prp}}_{F}(q',t') + \frac{2q^2m^2+1}{2^l}$$

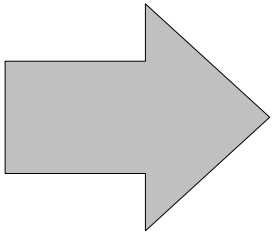
EMACの安全性の定式化

- EMAC(Encrypted MAC)

  新しい鍵であるk_2を使って、CBC-MACの認証子である

  $CBC_{k_1}(M)$を暗号化して認証子を作成



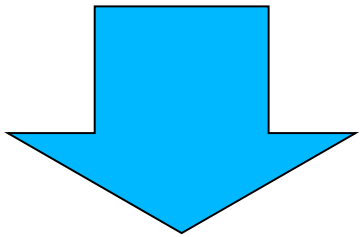


評価　×

その他の安全性の定式化

- その他の安全性の定式化

ハッシュ関数の衝突計算困難性
(Collision Resistance)



$x = x'$ かつ $h(x) = h(x')$ を満たす入力の組である x, x' を計算するのは困難

まとめ

- Cryptoverifについて
- MACの安全性の定式化について
- その他の安全性の定式化について