事務局選出暗号の安全性評価について
暗号利用モード

CRYPTREC
Cryptography Research and Evaluation Committees

公募の目的 (公募要項P.4 第5.1節抜粋)

・策定から5年以上が経過し、解析・攻撃技術の高度化及び暗号技術の開発が進展している

・安全性評価のみならず危殆化及び移行対策を含めた適切な暗号選択の支援への要望

・導入コスト、相互運用性、普及度合いなどの評価観点の必要性の指摘

・リストの改訂に必要な技術の追加

CRYPTREC
Cryptography Research and Evaluation Committees

暗号利用モード(新設)

・証明可能安全性、適応選択平文/暗号文攻撃における識別不能性

・利用するnonceや乱数の有無や安全性における要件の妥当性

・利用するブロック暗号に対する安全性(ideal cipher modelなど)の要件など

・利用状況に特化した攻撃(関連鍵攻撃の実行可能性など)の有無

・実装効率性(並列処理など)

暗号利用モードの評価対象

- Confidentiality Mode
  - ECB, CBC, CFB, OFB, CTR, XTR
- Authenticity Mode
  - CMAC, HMAC, GMAC, ISO 9797-1
- Authenticated-Encryption Mode
  - CCM, GCM

CRYPTREC
Cryptography Research and Evaluation Committees

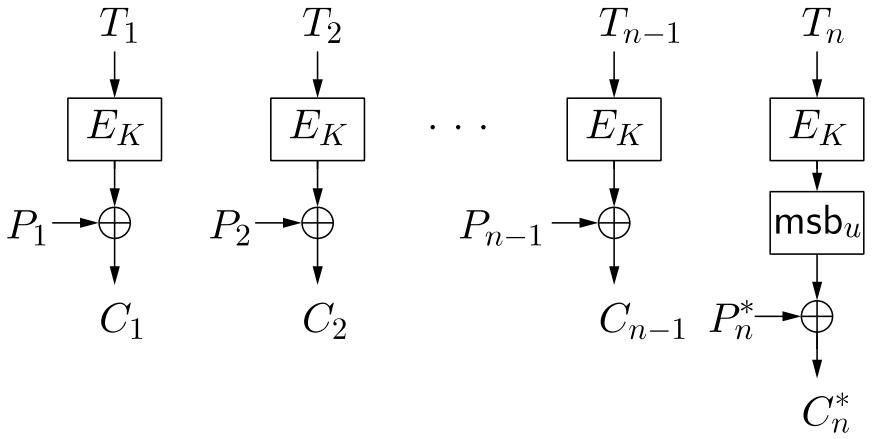
暗号利用モードの評価項目

- 証明可能安全性
  - 適応的選択文書攻撃
  - 検証オラクルを多数回呼び出したときの識別不可能性
  - 弱偽造不可能性
  - 強偽造不可能性
- Nonce、乱数要素の有無
- 利用暗号ブロックに対する仮定の強さ
- 利用ブロック暗号に特定の方式を適用した場合の安全性

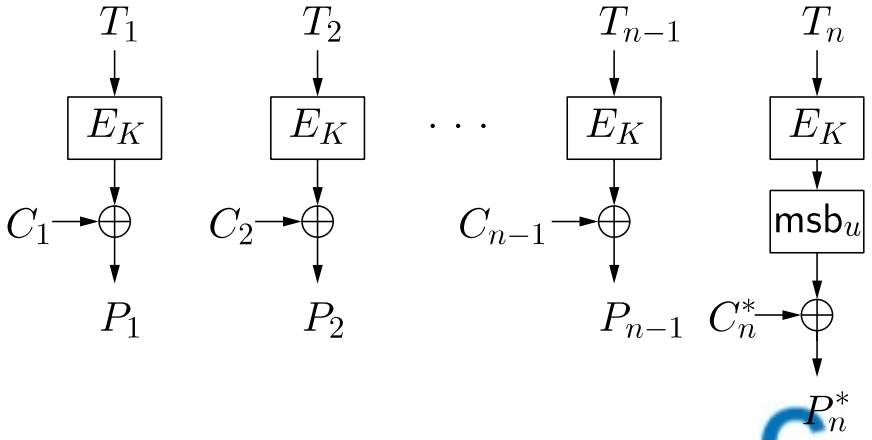
CRYPTREC
Cryptography Research and Evaluation Committees

事務局選出暗号利用モードの例

- CTR (Confidentiality Mode)



(a) 暗号化

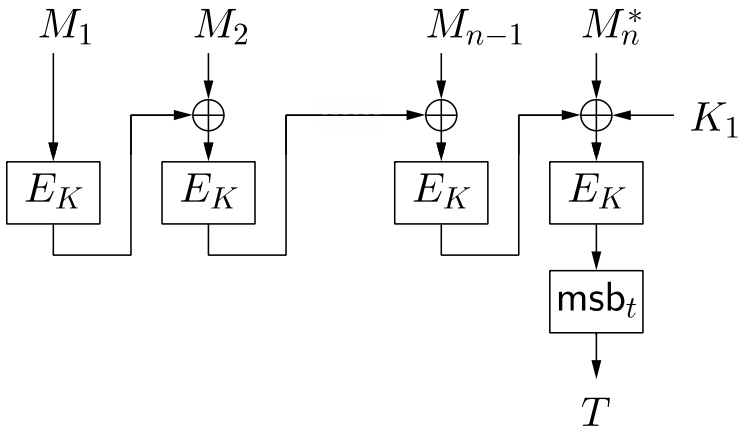


(b) 復号

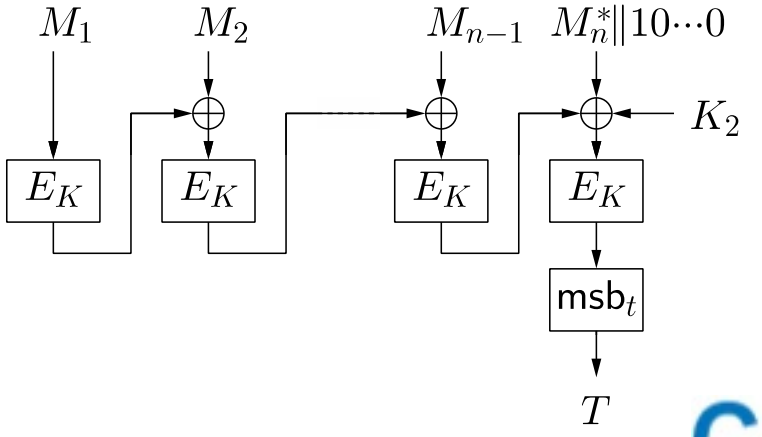
CRYPTREC
Cryptography Research and Evaluation Committees

事務局選出暗号利用モードの例

- CMAC (Authenticity Mode)



(a) $\mathsf{len}(M_n^*) = b$ のとき

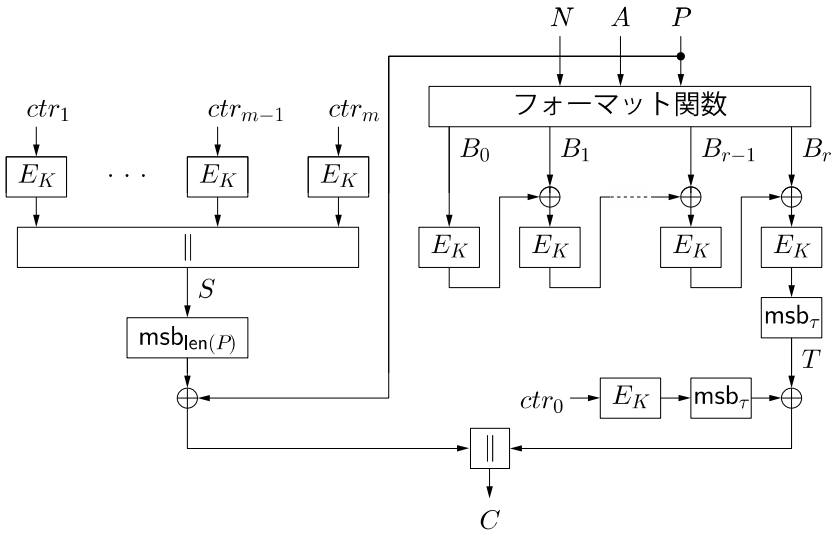


(b) $\mathsf{len}(M_n^*) < b$ のとき

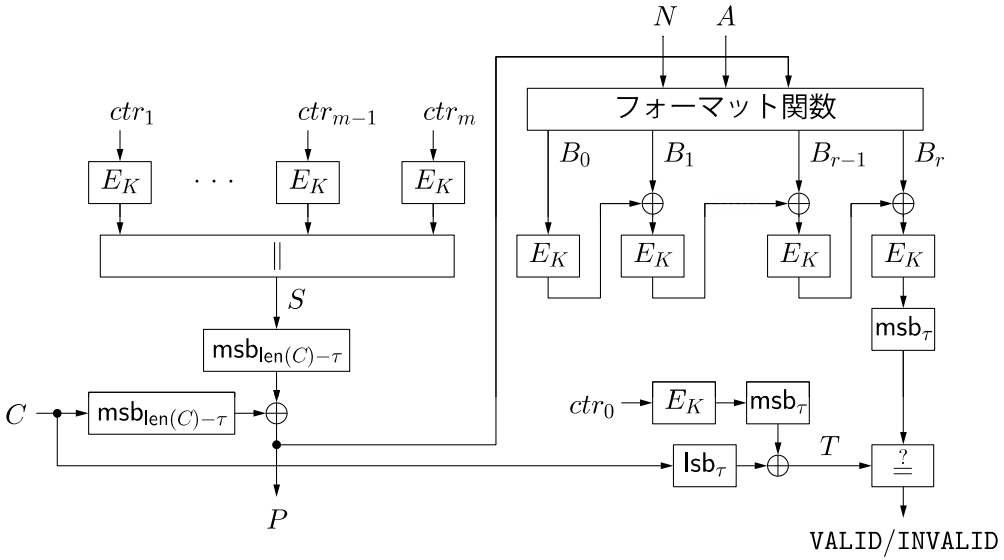
CRYPTREC
Cryptography Research and Evaluation Committees

事務局選出暗号利用モードの例

- CCM (Authenticated-Encryption Mode)



Generation-Encryption



Decryption-Verification

CRYPTREC
Cryptography Research and Evaluation Committees

安全性評価結果

- Confidentiality Mode
  - CBC、CFB、OFBについては、適応的選択平文攻撃に対する証明可能安全性を有する。
  - ECBについては用途が限定される。
  - CBC、CFB、OFB、ECBのいずれにも、適応的選択暗号文攻撃が存在する。 → 使い方に関する注釈が必要
  - CBCについては、以下のケースに選択平文攻撃が存在。
    - 平文ブロックごとに暗号文が存在する場合
    - Nonceを平文と同じ鍵で暗号化して初期ベクトルを生成する場合
  - CTRは問題はない。
  - ディスクの暗号化を意図したXTRは、繰り返し回数はリークするが、ブロック位置はリークしない。

CRYPTREC
Cryptography Research and Evaluation Committees

安全性評価結果

- Authenticity Mode
  - ISO/IEC 9797-1に掲載されている21種類のMACのバリエーションのうち、CBC-MAC系統について仕様が不明確
    - Key Separation
  - HMACについては、SHA-1を使用した場合の問題点の報告があるが、実用上は問題がない。
  - CMACについては、Birthday-bound Attackが指摘されているものの、脆弱性の指摘されていないブロック暗号を用いる限り証明可能安全性を有する。
  - GMACについては、タグの利用方法によっては安全性のマージンが小さくなるため、利用方法の限定が必要。

安全性評価結果

- Authenticated-Encryption Mode
  - CCM、GCMともに、適応的選択平文攻撃に対する証明可能安全性を有する。
    - 脆弱性の問題が指摘されていないブロック暗号を用いる場合には、問題がない
  - GCMについては、短いタグを用いたときに注意が必要。

CRYPTREC
Cryptography Research and Evaluation Committees

まとめ

- Confidentiality Mode
  - 適応的選択平文攻撃への対応、CBCにおける利用方法に注意が必要
- Authenticity Mode
  - CBC-MAC系のKey Separationの仕様の不明確さに起因する使い方の問題
  - GMACにおけるタグの長さへの注意
- Authenticated encryption
  - GCMにおけるタグの長さへの注意

- 今後、注意すべき利用方法について検討を行い、利用方法の注釈等について検討を行う。

CRYPTREC
Cryptography Research and Evaluation Committees