I240 暗号理論 2019
モード型共通鍵暗号

2019/10/18 講師 藤崎

1 はじめに

理想論でなく実際に使われる共通鍵暗号についてすこし触れる。実際に使われる共通鍵暗号は、固定長の平文 $m \in \{0,1\}^n$ を置換により暗号化するブロック暗号と呼ばれるものを部品とし、モード (mode of operation) と呼ばれる技術により、可変長の平文 $m \in \{0,1\}^*$ を暗号文に変換している。ブロック暗号そのものも共通鍵暗号である。

ブロック暗号は理想としてランダム置換であって欲しいが、現実的にはそのようなものを n の多項式時間のアルゴリズムで作ることは不可能である。しかし、モード型の共通鍵暗号、MAC では便宜上ブロック暗号をランダム置換として考え、安全性を議論することが通例である。

2 ブロック暗号 (Block cipher)

ブロック暗号 $\mathsf{SKE} = (\mathcal{K}, \mathcal{M}, \mathbf{E}, \mathbf{D})$ は、$\mathcal{K} = \{0,1\}^\ell$, $\mathcal{M} = \{0,1\}^n$ として、$\mathbf{E}$, $\mathbf{D}$ が、

$$\mathbf{E} : \{0,1\}^\ell \times \{0,1\}^n \to \{0,1\}^n$$
$$\mathbf{D} : \{0,1\}^\ell \times \{0,1\}^n \to \{0,1\}^n$$

$\mathbf{D}(k, \mathbf{E}(k,m)) = m$ を満たすような (k を固定した時) $\{0,1\}^n$ 上の置換と逆置換になっているようなものである。理想のブロック暗号は、秘密鍵 k をランダムに選んだ時 $E(k,\cdot)$ がランダム置換 (random permutation) になっていることであるが、実際にそれを実現することは効率的なアルゴリズムでは不可能である。しかし、後述のモードで述べるように、モードを使った共通鍵暗号や MAC の安全性を考える時、ブロック暗号をランダム置換と考えて扱う。

AES (Adavanced Encryption Standard) は、NIST 標準の有名なブロック暗号であり、128 ビットの平文を暗号化出来る（すなわち $n = 128$)。一方、鍵は $128, 192, 256$ ビットのサイズを選ぶことができ（すなわち $\ell = 128, 192, 256$)、それぞれ AES-128, AES-192, AES-256 と呼ばれる。

問題 1 $\{0,1\}^n$ 上起こりうる置換 (permutation) $\pi : \{0,1\}^n \to \{0,1\}^n$ の個数を求めよ。

2.1 モード型共通鍵暗号

以下、いくつかのモード型共通鍵暗号を紹介する。モード型共通鍵暗号は、可変長の平文 $m \in \{0,1\}^*$ を暗号化することができる。

■ECB モード暗号 大きな欠点があり秘匿が十分でないので現在はほとんど使われていない。図 1 のように、平文 $m \in \{0,1\}^*$ をブロック暗号の入力サイズ n により t 個に分割 $m = m_1 | \cdots | m_t$ ($m_i \in \{0,1\}^n$) した後、

$$c_1 = \mathbf{E}(k, m_1), \ldots, c_t = \mathbf{E}(k, m_t)$$

を計算し暗号文を $c = c_1|\cdots|c_t$ とする単純な暗号方式である。復号は自明なので省略。

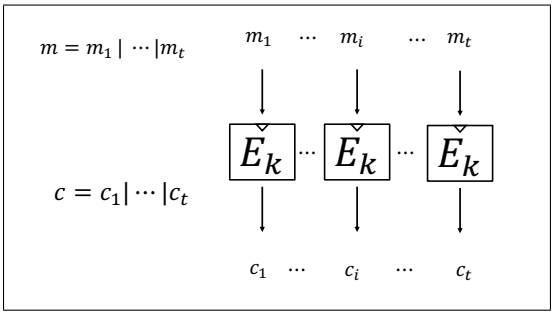

図 1　ECB モード

■CBC モード暗号　現在もよく使われているが、平文の長さを可変長にすると問題があることがすでに 2002 年から知られている [Vau02]. 実際、最新バージョンの TLS (Transport Layer Security) [*1] より前の TLS は CBC モードの共通鍵暗号をサポートしている（例えば、AES-256 と組み合わせて、AES-256-CBC のように使われる）が、多くの TLS の新しい攻撃を生み出す元凶となっている。一方、平文の長さを固定長に限定し、IV を一様ランダムにとり、部品であるブロック暗号がランダム置換であると仮定すると安全性が証明できることが知られている [BDJR97]。

$\mathbf{E}, \mathbf{D}$ をそれぞれブロック暗号の暗号化アルゴリズム、復号アルゴリズムとする。平文 $m \in \{0,1\}^*$ をブロック暗号の入力サイズ n により t 個に分割 $m = m_1|\cdots|m_t$ $(m_i \in \{0,1\}^n)$ した後、図 2 のように暗号化、復号を行う。

CBC-Enc $\mathbf{E}^{\mathrm{CBC}}(k, m)$	CBC-DEC $\mathbf{D}^{\mathrm{CBC}}(k, c)$:
$iv \leftarrow \{0,1\}^n$; $c_0 := iv$;	Parse as $c = c_0\|c_1\|\cdots\|c_t$;
for $i = 1, \ldots, t$ do	for $i = 1, \ldots, t$ do
$c_i := \mathbf{E}(k, c_{i-1} \oplus m_i)$;	$x_i := D(k, c_i) \oplus c_{i-1}$
return $c := iv\|c_1\|\cdots\|c_t$.	return $m := x_1\|\cdots\|x_t$.

図 2　CBC-Encryption

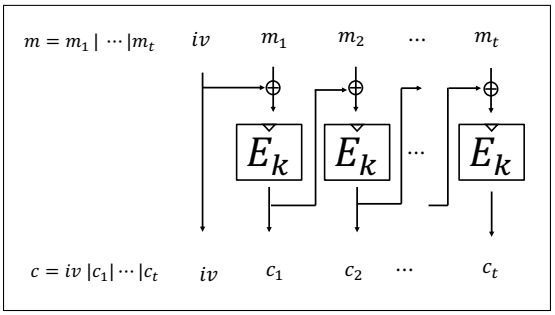

図 3　CBC モード

[*1] 2019 年 1 0 月現在の最新バージョンは TLS 1.3.

■CTR モード暗号　安全性が証明されているステートがある (stateful) 共通鍵暗号。暗号化アルゴリズムはカウンター ctr を持っている。暗号化は、図 4 のように平文 $m \in \{0,1\}^*$ をブロック暗号の入力サイズ n により t 個に分割 $m = m_1|\cdots|m_t$ $(m_i \in \{0,1\}^n)$ した後、

$$c_1 = m_1 \oplus \mathbf{E}(k, ctr), \ldots, c_t = m_t \oplus \mathbf{E}(k, ctr + t)$$

とし、暗号文を $c := ctr|c_1|\cdots|c_t$ とする。最後に暗号化アルゴリズムはカウンターを $ctr := ctr + t$ と更新する。

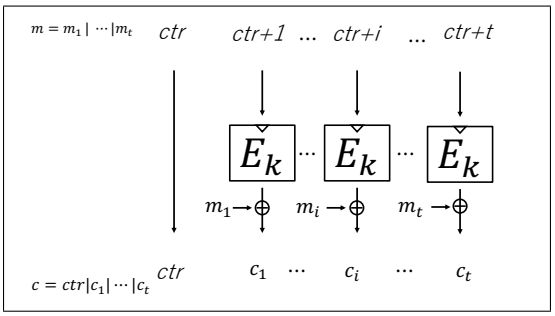

図 4　CTR モード

一方復号は、暗号文 $c := ctr|c_1|\cdots|c_t$ を受け取った後、

$$m_1 = c_1 \oplus \mathbf{E}(k, ctr), \ldots, m_t = c_t \oplus \mathbf{E}(k, ctr + t)$$

を計算し、$m := m_1|\cdots|m_t$ を出力する。

2.2　モード型共通鍵暗号の安全性モデル

モード型共通鍵暗号の安全性モデルを定義しておく [BDJR97]。

■CPA かつ CCA 攻撃ゲーム　敵 (adversary) A とチャレンジャー C の間で行われるモード型共通鍵暗号 $\mathsf{SKE} = (\mathcal{K}, \mathcal{M}, \mathbf{E}, \mathbf{D})$ の安全性を試すゲームである。ここで、SKE はモード型暗号のため、$\mathcal{M} = \{0,1\}^*$ とし、$\mathbf{E}, \mathbf{D}$ はモード型暗号の暗号化アルゴリズム、復号アルゴリズムである（ブロック暗号の暗号化アルゴリズム、復号アルゴリズムでは無いので注意)。今、$\mathcal{K} = \{0,1\}^\kappa$ としておく。

1. C は鍵空間 $\mathcal{K}$ から一様ランダムに鍵 k を選ぶ。$k \leftarrow \mathcal{K}$.
2. C は一様ランダムにビット $b^* \leftarrow \{0,1\}$ を選ぶ。
3. (チャレンジ) A は、自分の戦略に従って二つの平文の組 (m_0, m_1) を暗号化オラクル $\mathbf{E}^{b^*}(k, \cdot)$ に送り、暗号化オラクルから暗号文 $c^* = \mathbf{E}(k, m_{b^*})$ を受け取る。A は d 回までこの質問を暗号化オラクルにすることができる。ただし $d = O(\kappa)$ である。
4. (選択平文攻撃 (chosen-plaintext attack (CPA))) A は平文 m を暗号化オラクルに送り、暗号文 $c = E(k, m)$ を答えとしてもらう。平文 m の選び方は A の戦略による。A は合計 q_e 回まで質問 (query) を送ることができる。記述を簡単にするため、暗号化オラクルをチャレンジの暗号化オラクル $\mathbf{E}^{b^*}(k, \cdot)$ で代用することとする。選択平文攻撃をしたいときは、A は、同じ平文の組 (m, m) を暗号化オラクルに質問すれば良い。よって、$q_e < d$ となる。A の $\mathbf{E}^{b^*}(k, \cdot)$ オラクルへのアクセス履歴を $L = \{(m_0^1, m_1^1, c_1^*), \ldots, (m_0^d, m_1^d, c_d^*)\}$ とし、特に $L(c) = \{c_1^*, \ldots, c_d^*\}$ と書くことにする。

5. (選択暗号文攻撃 (chosen-ciphertext attack (CCA))) A は暗号文 c を復号オラクル $\mathbf{D}(k,\cdot)$ に送り、$m = \mathbf{D}(k,c)$ をもらうことができる。ただし、すでに $L(c)$ に入っている暗号文は復号オラクルに質問できない。暗号文 c の選び方は A の戦略による。A は合計 $q = O(\kappa)$ 回まで質問 (query) を送ることができる。
6. A は、ビット b を出力する。
7. もし、$b = b^*$ であれば、A の勝ちと定義する。

$d, q = O(\kappa)$ であれば、回数はあらかじめ決まっていなくて良い。A が、SKE に対する CPA&CCA ゲームに勝つ確率の 1/2 からの差を正規化したものを、A の C に対するアドバンテージと呼び、

$$\mathsf{Adv}^{\mathsf{cpa,cca}}_{A,\mathsf{SKE}}(\kappa) := 2\Pr[k \leftarrow \{0,1\}^\kappa;\, b^* \leftarrow \{0,1\} : A^{\mathbf{E}^{b^*}(k,\cdot),\mathbf{D}(k,\cdot)} = b^*] - 1.$$

と定義する。

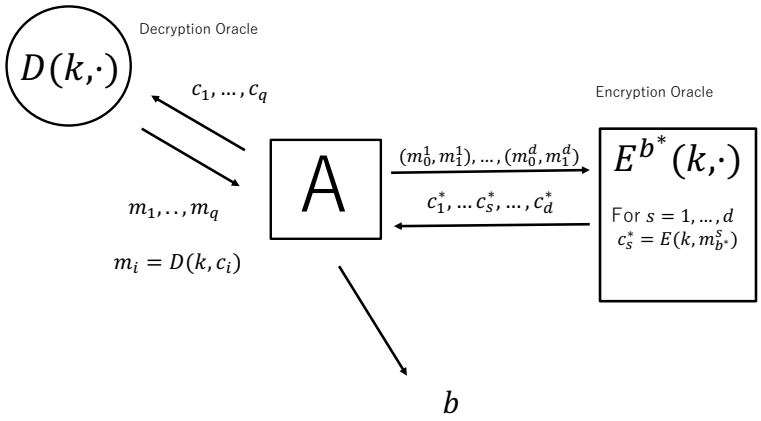

図 5　共通鍵暗号の攻撃モデル

定義 2（モード型共通鍵暗号の安全性） 任意の敵 A に対して、$\mathsf{Adv}^{\mathsf{cpa,cca}}_{A,\mathsf{SKE}}(\kappa) = \mathsf{negl}(\kappa)$ であるとき、モード型暗号 SKE は CPA かつ CCA 安全と呼ぶ。$\mathsf{negl}(\kappa) := \kappa^{-\omega(1)}$ である。

注釈 3　CTR モード暗号のようなステートがある暗号の場合、A は暗号化オラクルが暗号化に利用した ctr の値が含まれる暗号文を復号オラクルに質問として送ることはできないと定義する。

参考文献

[BDJR97] Mihir Bellare, Anand Desai, Eric Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *38th FOCS*, pages 394–403. IEEE Computer Society Press, October 1997.

[Vau02] Serge Vaudenay. Security flaws induced by CBC padding - applications to SSL, IPSEC, WTLS... In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 534–546. Springer, Heidelberg, April / May 2002.