A Graduate Course in Applied Cryptography (Chap. 2.1)

Kosuke Toda (@SeeKT)

2. Encryption

この章では，以下の状況を想定する．

- Alice と Bob が秘密の鍵 k を共有している．
- 盗聴者が存在する状況下で，メッセージ m の秘匿性を維持したままネットワークを介して送信したい．

Remark

- この章で紹介する技術が "secure communication" に関連する課題を全て解決するわけではない．

2.1 Shannon ciphers and perfect security

2.1.1 Definition of a Shannon cipher

ここでは，**Shanon cipher** と呼ばれる，暗号化の基本的なメカニズムを紹介する .

Notation

- $\mathcal{K}$: 鍵空間 (key space)
- $\mathcal{M}$: 平文空間 (message space)
- $\mathcal{C}$: 暗号文空間 (cipertext space)

Shannon cipher

Shannon cipher は，$(\mathcal{K}, \mathcal{M}, \mathcal{C})$ 上で定義される組

$$\mathcal{E} = (E, D)$$

である．ただし，

- $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ は暗号化関数 (encryption function).
  - $c = E(k, m)$ は，k の下での m の暗号化．
- $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$ は復号化関数 (decryption function).
  - $m = D(k, c)$ は，k の下での c の復号化．

ここで，cipher は，次の **correctness property** を満たす必要がある．

$$\forall k \in \mathcal{K}, \forall m \in \mathcal{M}, D(k, E(k, m)) = m.$$

これは，任意の鍵に対して，任意の平文を暗号化して復号したものがもとの平文に一致するということである．

ここで，Alice が Bob に $c = E(k, m) \in \mathcal{C}$ を送ったとする．Bob が c を復号化したときに，$D(k, c) = m$ となるためには，c が Alice と Bob の通信の間に改ざんされていないことが求められる．

以下，$\mathcal{K}, \mathcal{M}, \mathcal{C}$ は有限集合とする．

Ex. 2.1 A one-time pad

- Shannon cipher $\mathcal{E} = (E, D)$ で，鍵，メッセージ，暗号文の長さが全て等しいものである．
  - $\mathcal{E}$ は $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ 上で定義され，fixed parameter L に対して

$$\mathcal{K} := \mathcal{M} := \mathcal{C} := \{0,1\}^L.$$

- 暗号化関数，復号化関数は以下で定義．

$$E(k, m) := k \oplus m$$
$$D(k, m) := k \oplus c$$

  - $\oplus$ は bit-wise explusive-OR.

$\forall x, y, z \in \{0,1\}^L$ に対して以下が成立.

$$x \oplus y = y \oplus x,\ x \oplus (y \oplus z) = (x \oplus y) \oplus z,$$
$$x \oplus 0^L = x,\ x \oplus x = 0^L.$$

$\rightsquigarrow \mathcal{E}$ に対して correctness property が成立.

$$D(k, E(k, m)) = D(k, k \oplus m) = k \oplus (k \oplus m)$$
$$= (k \oplus k) \oplus m = 0^L \oplus m = m,\ \ \forall k, m \in \{0,1\}^L.$$

Ex. 2.2 A variable length one-time pad

- Shannon cipher $\mathcal{E} = (E, D)$ で，鍵長が L で，メッセージと暗号文の長さが高々 L であるもの．

$\rightsquigarrow \mathcal{E}$ は $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ 上で定義され，あるパラメータ L に対して

$$\mathcal{K} := \{0,1\}^L, \quad \mathcal{M} := \mathcal{C} := \{0,1\}^{\leq L}$$

となるもの．

- $\{0,1\}^{\leq L}$: 長さが L 以下のすべてのビット列 (空列も含む)．

- 暗号化関数
  $\forall k \in \{0,1\}^L, \forall m \in \{0,1\}^\ell \subset \{0,1\}^{\leq L},$

$$E(k, m) := k[0, \ldots, \ell - 1] \oplus m.$$

- 復号化関数
  $\forall k \in \{0,1\}^L, \forall c \in \{0,1\}^\ell \subset \{0,1\}^{\leq L},$

$$D(k, c) := k[0, \ldots, \ell - 1] \oplus m.$$

- $k[0, \ldots, \ell - 1]$: k の先頭 ℓ ビット.

$\rightsquigarrow$ correctness property を満たす (one-time pad と同様).

2.1.2 Perfect security

ここでは，"secure" な cipher を数学的に定義する．
⇝ **perfect security** が "gold standard" for security.

- one-time pad は perfect security を満たす．
  - key が message と同じ長さで，実用的ではない．
- 任意の perfect secure cipher は，message space と同じサイズの key space を持たなければならない．

⇝ security の定義を弱めたい

Perfect security は，「暗号文の知識がもとのメッセージを推測する可能性を高めるか？」という観点で定義されている．

Def. 2.1 (Perfect security)

$\mathcal{E} = (E, D)$ を，$(\mathcal{K}, \mathcal{M}, \mathcal{C})$ 上で定義された Shannon cipher とする．確率変数 $\boldsymbol{k}$ が，$\mathcal{K}$ 上で一様に分布するような試行を考える．

$\mathcal{E}$ が **perfectly secure** Shannon cipher

$$\overset{\text{def}}{\iff} \forall m_0, m_1 \in \mathcal{M}, \forall c \in \mathcal{C},$$

$$\Pr[E(\boldsymbol{k}, m_0) = c] = \Pr[E(\boldsymbol{k}, m_1)] = c.$$

上で定義した perfect security と同値な条件を示す．

Th. 2.1

$\mathcal{E} = (E, D)$ を $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ 上で定義された Shannon cipher とする．
以下は同値．

1. $\mathcal{E}$ は perfectly secure
2. $\forall c \in \mathcal{C}, \exists N_c$ s.t. $\forall m \in \mathcal{M}$,

$$\left|\{k \in \mathcal{K} : E(k, m) = c\}\right| = N_c.$$

3. 確率変数 $\boldsymbol{k}$ が $\mathcal{K}$ 上に一様に分布するならば，各 m に対して確率変数 $E(\boldsymbol{k}, m)$ は同分布である．

Th. 2.2

One-time pad は，perfectly secure Shannon cipher である．

Proof

$(\mathcal{K}, \mathcal{M}, \mathcal{C})$ 上で定義された Shannon cipher $\mathcal{E} = (E, D)$ が one-time pad であるとする．ただし，$\mathcal{K} := \mathcal{M} := \mathcal{C} := \{0,1\}^L$ とする．このとき，

$$\forall m \in \{0,1\}^L, \forall c \in \{0,1\}^L, \exists k \in \{0,1\}^L \text{ s.t. } k \oplus m = c,$$

つまり，$k := m \oplus c$ である．つまり，$\mathcal{E}$ は Th. 2.1 の条件2を満たす ($N_c = 1 \; \forall c \in \mathcal{C}$)．

Ex. 2.5

variable length one-time pad (Ex. 2.2) は，perfect security を満たさない．

m_0を長さ1の任意の列とし，m_1を長さ2の任意の列とする．また，cを長さ1の列とし，$\boldsymbol{k}$を鍵空間の一様分布からの確率変数とする．このとき，Def 2.1の反例を得る．

$$\Pr[E(\boldsymbol{k}, m_0), c] = \frac{1}{2}, \quad \Pr[E(\boldsymbol{k}, m_1) = c] = 0.$$

直感的には，暗号文が平文の長さを漏らしているため．

盗聴者が暗号文に対して predicate ϕ を適用している状況を考える．
ただし，$\phi : \mathcal{C} \to \{0,1\}$ は，$\mathcal{C}$ 上の boolean-valued function.
$\rightsquigarrow$ Perfect security は，暗号文に対する predicate がメッセージの何の情報も漏らさないことを保証する．

Th. 2.3

$\mathcal{E} = (E, D)$ を $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ 上で定義された Shannon cipher とする．
確率変数 $\boldsymbol{k}$ が，$\mathcal{K}$ 上で一様に分布するような試行を考える．このとき，$\mathcal{E}$ が perfectly secure であることの必要十分条件は以下．
$\forall \phi : \text{predicate on } \mathcal{C}, \forall m_0, m_1 \in \mathcal{M},$

$$\Pr[\phi(E(\boldsymbol{k}, m_0))] = \Pr[\phi(E(\boldsymbol{k}, m_1))].$$

また，perfect security は，暗号文を見た後でも平文に対する情報が増えないということを保証する．

Th. 2.4

$\mathcal{E} = (E, D)$ を $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ 上で定義された Shannon cipher とする．
確率変数 $\boldsymbol{k}, \boldsymbol{m}$ に対する以下の試行を考える．

- $\boldsymbol{k}$ は $\mathcal{K}$ 上で一様に分布する．
- $\boldsymbol{m}$ は $\mathcal{M}$ 上の分布．
- $\boldsymbol{k}$ と $\boldsymbol{m}$ は独立．

確率変数 $\boldsymbol{c} := E(\boldsymbol{k}, \boldsymbol{m})$ を定義する．このとき，以下が成り立つ．

- $\mathcal{E}$ が perfectly secure ならば，$\boldsymbol{c}$ と $\boldsymbol{m}$ は独立である．
- 逆に，$\boldsymbol{c}$ と $\boldsymbol{m}$ が独立で，各メッセージ $m \in \mathcal{M}$ が非ゼロの確率で生じるならば，$\mathcal{E}$ は perfectly secure である．

ここで，「$\boldsymbol{m}$ と $\boldsymbol{k}$ が独立な確率変数である」という仮定は理にかなっている．

2.1.3 The bad news

One-time pad は perfectly secure な Shanon cipher で最も鍵の長さが短い.

Th. 2.5

$\mathcal{E} = (E, D)$ を $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ 上で定義された Shannon cipher とする.
$\mathcal{E}$ が perfectly secure ならば, $|\mathcal{K}| \geq |\mathcal{M}|$ である.