応用数学６ 2010 年 10 月 6 日

完全秘匿性

講師: 安永憲司

現代暗号における安全性の定式化は，Shannon が秘密鍵暗号方式に対して行ったものが始まりである．Shannon が定義した安全性は，現在**完全秘匿性**と呼ばれている安全性と等しい．

1 Shannon による安全性の定式化

定義 1 (Shannon 秘匿性) 秘密鍵暗号方式 $(\mathcal{M}, \mathcal{K}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が，$\mathcal{M}$ 上の分布 D に関して **Shannon 秘匿**であるとは，任意の $m \in \mathcal{M}$ と任意の c に対して，

$$\Pr_{\substack{k \leftarrow \mathsf{Gen} \\ m' \leftarrow D \\ \mathsf{Enc}}}[m = m' \mid \mathsf{Enc}_k(m') = c] = \Pr_{m' \leftarrow D}[m = m']$$

暗号方式が **Shannon 秘匿**であるとは，$\mathcal{M}$ 上のすべての分布 D に関して Shannon 秘匿であるときである．

2 完全秘匿性

定義 2 (完全秘匿性) 秘密鍵暗号方式 $(\mathcal{M}, \mathcal{K}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が**完全秘匿**であるとは，任意の $m_1, m_2 \in \mathcal{M}$ と任意の c に対して，

$$\Pr_{\substack{k \leftarrow \mathsf{Gen} \\ \mathsf{Enc}}}[\mathsf{Enc}_k(m_1) = c] = \Pr_{\substack{k \leftarrow \mathsf{Gen} \\ \mathsf{Enc}}}[\mathsf{Enc}_k(m_2) = c]$$

を満たすときである．

定理 3 秘密鍵暗号方式において，Shannon 秘匿性と完全秘匿性は等価である．

証明: 両方向の証明を行う．

完全秘匿性 ⇒ Shannon 秘匿性.

暗号方式 $(\mathcal{M}, \mathcal{K}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が完全秘匿だと仮定する．以下では，$\mathcal{M}$ 上の任意の分布 D，任意の $m \in \mathcal{M}$, 任意の c に対して，

$$\Pr_{k, m', \mathsf{Enc}}[m = m' \mid \mathsf{Enc}_k(m') = c] = \Pr_{m'}[m = m']$$

であることを示す．ここで，$\Pr_{k,m',\mathsf{Enc}}[\cdot]$ は，確率を，$k \leftarrow \mathsf{Gen}, m' \leftarrow D, \mathsf{Enc}$ の乱数の上でとることを表している．条件付き確率の定義より，左辺は以下のように変形できる．

$$\begin{aligned}
\frac{\Pr_{k,m',\mathsf{Enc}}[m = m' \cap \mathsf{Enc}_k(m') = c]}{\Pr_{k,m',\mathsf{Enc}}[\mathsf{Enc}_k(m') = c]} &= \frac{\Pr_{k,m',\mathsf{Enc}}[m = m' \cap \mathsf{Enc}_k(m) = c]}{\Pr_{k,m',\mathsf{Enc}}[\mathsf{Enc}_k(m') = c]} \\
&= \frac{\Pr_{m'}[m = m'] \Pr_{k,\mathsf{Enc}}[\mathsf{Enc}_k(m) = c]}{\Pr_{k,m',\mathsf{Enc}}[\mathsf{Enc}_k(m') = c]}.
\end{aligned}$$

したがって，

$$\Pr_{k,m',\mathsf{Enc}}[\mathsf{Enc}_k(m') = c] = \Pr_{k,\mathsf{Enc}}[\mathsf{Enc}_k(m) = c]$$

を示せば十分である．以下でそれを示す．

$$\begin{aligned}
\Pr_{k,m',\mathsf{Enc}}[\mathsf{Enc}_k(m') = c] &= \sum_{m''\in\mathcal{M}} \Pr_{m'}[m' = m''] \Pr_{k,\mathsf{Enc}}[\mathsf{Enc}_k(m'') = c] \\
&= \sum_{m''\in\mathcal{M}} \Pr_{m'}[m' = m''] \Pr_{k,\mathsf{Enc}}[\mathsf{Enc}_k(m) = c] \\
&= \Pr_{k,\mathsf{Enc}}[\mathsf{Enc}_k(m) = c] \sum_{m''\in\mathcal{M}} \Pr_{m'}[m' = m''] \\
&= \Pr_{k,\mathsf{Enc}}[\mathsf{Enc}_k(m) = c].
\end{aligned}$$

一つ目の等号は，定義通りである．二つ目の等号は，完全秘匿性より成り立つ．三つ目の等号は，m'' と関係のない項を括りだしており，四つ目の等号は，確率の和が 1 になることを利用している．

Shannon 秘匿性 $\Rightarrow$ 完全秘匿性.

暗号方式 $(\mathcal{M}, \mathcal{K}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が Shannon 秘匿だと仮定する．任意の $m_1, m_2 \in \mathcal{M}$ と任意の c を考える．分布 D として，$\{m_1, m_2\}$ 上の一様分布を考える．以下では，

$$\Pr_{k,\mathsf{Enc}}[\mathsf{Enc}_k(m_1) = c] = \Pr_{k,\mathsf{Enc}}[\mathsf{Enc}_k(m_2) = c]$$

を示す．分布 D の定義より，$\Pr_m[m = m_1] = \Pr_m[m = m_2] = \frac{1}{2}$ である．このとき，Shannon 秘匿性より，

$$\Pr_{k,m,\mathsf{Enc}}[m = m_1 \mid \mathsf{Enc}_k(m) = c] = \Pr_{k,m}[m = m_2 \mid \mathsf{Enc}_k(m) = c].$$

条件付き確率の定義より，

$$\begin{aligned}
\Pr_{k,m,\mathsf{Enc}}[m = m_1 \mid \mathsf{Enc}_k(m) = c] &= \frac{\Pr_{k,m,\mathsf{Enc}}[m = m_1 \cap \mathsf{Enc}_k(m) = c]}{\Pr_{k,m,\mathsf{Enc}}[\mathsf{Enc}_k(m) = c]} \\
&= \frac{\Pr_m[m = m_1] \Pr_{k,\mathsf{Enc}}[\mathsf{Enc}_k(m_1) = c]}{\Pr_{k,m,\mathsf{Enc}}[\mathsf{Enc}_k(m) = c]} \\
&= \frac{\frac{1}{2} \Pr_{k,\mathsf{Enc}}[\mathsf{Enc}_k(m_1) = c]}{\Pr_{k,m,\mathsf{Enc}}[\mathsf{Enc}_k(m) = c]}.
\end{aligned}$$

同様に，

$$\Pr_{k,m,\mathsf{Enc}}[m = m_2 \mid \mathsf{Enc}_k(m) = c] = \frac{\frac{1}{2} \Pr_{k,\mathsf{Enc}}[\mathsf{Enc}_k(m_2) = c]}{\Pr_{k,m,\mathsf{Enc}}[\mathsf{Enc}_k(m) = c]}.$$

項を整理すると，

$$\Pr_{k,\mathsf{Enc}}[\mathsf{Enc}_k(m_1) = c] = \Pr_{k,\mathsf{Enc}}[\mathsf{Enc}_k(m_2) = c].$$

□

3 使い捨て鍵暗号 (One-Time Pad)

完全秘匿性を達成する暗号化方式として，使い捨て鍵暗号 (One-Time Pad) を紹介する．

定義 4 (使い捨て鍵暗号) 使い捨て鍵暗号は次の $(\mathcal{M}, \mathcal{K}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ で定義される．

$$\begin{aligned}
\mathcal{M} &= \{0,1\}^n \\
\mathcal{K} &= \{0,1\}^n \\
\mathsf{Gen} &= k;\ \text{ただし } k \xleftarrow{R} \{0,1\}^n \\
\mathsf{Enc}_k(m_1 m_2 \dots m_n) &= c_1 c_2 \dots c_n;\ \text{ただし } c_i = m_i \oplus k_i \\
\mathsf{Dec}_k(c_1 c_2 \dots c_n) &= m_1 m_2 \dots m_n;\ \text{ただし } m_i = c_i \oplus k_i
\end{aligned}$$

ここで，$\oplus$ は排他的論理和演算である．

命題 5 使い捨て鍵暗号方式は，完全秘匿性をもつ秘密鍵暗号方式である．

証明: 完全秘匿であることを示す．任意の $m, c \in \{0,1\}^n$ に対して，$\mathsf{Enc}_k(m) = m \oplus k = c$ を満たす k は一つしか存在しない．したがって，任意の $m, c \in \{0,1\}^n$ に対して，

$$\Pr_{k \xleftarrow{R} \{0,1\}^n}[\mathsf{Enc}_k(m) = c] = 2^{-n}.$$

また，c は $\{0,1\}^n$ 上の値しか取らないため，任意の $m_1, m_2 \in \{0,1\}^n$ と任意の c に対して，

$$\Pr_{k \xleftarrow{R} \{0,1\}^n}[\mathsf{Enc}_k(m_1) = c] = \Pr_{k \xleftarrow{R} \{0,1\}^n}[\mathsf{Enc}_k(m_2) = c].$$

□

4 Shannon の定理

完全秘匿性は，安全性としては非常に高いが，それを満たす秘密鍵暗号方式には，ある限界があることが知られている．以下で示す Shannon の定理は，完全秘匿性をもつ秘密鍵暗号方式では，メッセージが n ビットであれば，秘密鍵として共有する鍵も n ビット以上でなければならないことを示唆している．

定理 6 (Shannon の定理) 秘密鍵暗号方式 $(\mathcal{M}, \mathcal{K}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が完全秘匿であるならば，$|\mathcal{K}| \geq |\mathcal{M}|$.

証明: 完全秘匿性をもち，$|\mathcal{K}| < |\mathcal{M}|$ であるような秘密鍵暗号方式 $(\mathcal{M}, \mathcal{K}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ が存在したと仮定する．任意に $m_1 \in \mathcal{M}, k \in \mathcal{K}$ を選び，$c \leftarrow \mathsf{Enc}_k(m_1)$ とする．集合 $S(c)$ を，暗号文 c から復元可能なメッセージの集合を表すものとする．すなわち，$S(c) = \{m \mid \exists k \in \mathcal{K}, m = \mathsf{Dec}_k(c)\}$．$\mathsf{Dec}$ は決定性であるため，この集合のサイズは $|\mathcal{K}|$ 以下である．しかし，仮定より $|\mathcal{K}| < |\mathcal{M}|$ であるため，あるメッセージ $m_2 \in \mathcal{M}$ は，$S(c)$ に含まれない．つまり，

$$\Pr_{k \leftarrow \mathsf{Gen}}[\mathsf{Enc}_k(m_2) = c] = 0$$

である．しかし，

$$\Pr_{k \leftarrow \mathsf{Gen}}[\mathsf{Enc}_k(m_1) = c] > 0$$

であるため，

$$\Pr_{k \leftarrow \mathsf{Gen}}[\mathsf{Enc}_k(m_1) = c] \neq \Pr_{k \leftarrow \mathsf{Gen}}[\mathsf{Enc}_k(m_2) = c]$$

であることがわかる．これは，完全秘匿性に矛盾する． □

上記の証明では，$|\mathcal{K}| < |\mathcal{M}|$ であるような秘密鍵暗号方式に対する，具体的な攻撃方法を示していると言える．つまり，そのような暗号方式に対しては，任意のメッセージ $m_1 \in \mathcal{M}$ に対して，

$$\Pr[m_1 \in S(c) \mid k \leftarrow \mathsf{Gen}, \mathsf{Enc}_k(m_1) = c] = 1$$

であるが，このとき，あるメッセージ $m_2 \in \mathcal{M}$ と定数 $\epsilon > 0$ が存在して，

$$\Pr[m_2 \in S(c) \mid k \leftarrow \mathsf{Gen}, \mathsf{Enc}_k(m_1) = c] \leq 1 - \epsilon$$

である．例えば，Alice が $\{m_1, m_2\}$ から確率 $\frac{1}{2}$ ずつでメッセージを選び，それを暗号化して Bob に送ることを考える．このとき，Eve は，その暗号文が m_1 と m_2 のいずれかであるかを，$\frac{1}{2}$ より大きな確率で当て

ることができる．Eve は，暗号文 c を受け取ったとき，$m_2 \in S(c)$ であるかを調べる．もし $m_2 \notin S(c)$ であれば，m_1 であると推測する，$m_2 \in S(c)$ であれば，m_1 と m_2 を確率 $\frac{1}{2}$ ずつでランダムに推測する．このとき，Eve が正しく推測する確率を見積もる．もし Alice が m_2 を送っていた場合，必ず $m_2 \in S(c)$ であるので，正しく推測する確率は $\frac{1}{2}$ である．Alice が m_1 を送っていた場合，確率 ϵ 以上で $m_2 \notin S(c)$ であり，Eve は正しい推測が出来る．また，確率 $1-\epsilon$ では，$m_2 \in S(c)$ であるため，正しい推測は確率 $\frac{1}{2}$ で行われる．したがって，Eve が正しく推測する確率は，

$$\frac{1}{2}\cdot\frac{1}{2}+\frac{1}{2}\big(\epsilon\cdot 1+(1-\epsilon)\cdot\frac{1}{2}\big)=\frac{1}{2}+\frac{\epsilon}{4}.$$

ただし，上記の方法の場合，ϵ が非常に小さい可能性があり（たとえば，$\epsilon = 2^{-100}$），攻撃としては十分でないかもしれない．しかし，以下では，$\mathcal{M}=\{0,1\}^n, \mathcal{K}=\{0,1\}^{n-1}$ として，長さが 1 ビットだけ短い場合に，$\epsilon=\frac{1}{2}$ を達成できることを示す．

命題 7 秘密鍵暗号方式 $(\mathcal{M},\mathcal{K},\mathsf{Gen},\mathsf{Enc},\mathsf{Dec}), \mathcal{M}=\{0,1\}^n, \mathcal{K}=\{0,1\}^{n-1}$ を考える．このとき，$m_1, m_2 \in \mathcal{M}$ が存在し，

$$\Pr[m_2 \in S(c) \mid k \leftarrow \mathsf{Gen}, \mathsf{Enc}_k(m_1)=c] \le \frac{1}{2}.$$

証明: ある $k \in \mathcal{K}$ と $m \in \mathcal{M}$ に対し，$c \leftarrow \mathsf{Enc}_k(m)$ であったとして，$S(c)$ を考える．Dec が決定性であるため，$|S(c)| \le |\mathcal{K}| = 2^{n-1}$ である．したがって，任意の $m_1 \in \mathcal{M}, k \in \mathcal{K}$ に対して，

$$\Pr[m' \in S(c) \mid m' \xleftarrow{R} \mathcal{M}, \mathsf{Enc}_k(m_1)=c] \le \frac{2^{n-1}}{2^n} \le \frac{1}{2}.$$

任意の $k \in \mathcal{K}$ に対して成り立つため，$k \leftarrow \mathsf{Gen}$ であっても成り立ち，

$$\Pr[m' \in S(c) \mid m' \xleftarrow{R} \mathcal{M}, k \leftarrow \mathsf{Gen}, \mathsf{Enc}_k(m_1)=c] \le \frac{1}{2}.$$

上の不等式は，ランダムに選んだメッセージに対して成り立っているので，この確率を最小にするメッセージ $m_1 \in \mathcal{M}$ が存在して，

$$\Pr[m_2 \in S(c) \mid k \leftarrow \mathsf{Gen}, \mathsf{Enc}_k(m_1)=c] \le \frac{1}{2}.$$

□

上記命題を利用すれば，鍵長がメッセージ長より 1 ビット短いような暗号方式に対して，あるメッセージ m_1, m_2 が存在して，Eve は，その二つのどちらが暗号化されているかを，確率 $\frac{1}{2}+\frac{1}{8}=\frac{5}{8}$ で当てることができる．この確率は，暗号を利用する立場として，受け入れられるものではない．では，ある程度安全な秘密鍵暗号を実現するには，メッセージ長と同じ長さの鍵を共有するしか方法はないのだろうか．

上記の Eve の攻撃法には問題点もある．攻撃としては単純だが，その実行時間は非常に大きいからである．$m_2 \in S(c)$ かどうかを調べるとき，すべての鍵 $k \in \mathcal{K}$ に対して，c を復号して m_2 になるかどうかを調べると，$\mathcal{K}=\{0,1\}^n$ なので，2^n 通りの鍵を調べることになる．これは，入力長 n に対して，指数的に大きな数であり，効率的にできるとは考えられない．この事実から，**計算能力が制限された敵**を考えれば，Shannon の定理による不可能性を克服できるかもしれない．