■1 群（信号・システム）- 1 編（情報理論）

# 13 章 情報セキュリティ符号化

**【本章の構成】**

本章では，以下について解説する．

■1 群 - 1 編 - 13 章

# 13-1 シャノンの暗号システム

■1 群 - 1 編 - 13 章

# 13-2 認証符号

# 13-3 秘密分散

（執筆者：岩本　貢）[2009 年 12 月 受領]

## 13-3-1 背景と問題設定

1970 年台後半は共通鍵暗号の最初の標準化である DES の策定，公開鍵暗号の概念と RSA 暗号の登場など，現代暗号の基盤ともいうべき暗号方式が登場した時期である．しかし，これらの暗号の信頼性は秘密鍵の秘匿を前提にしており，秘密鍵の管理手法については別に考える必要がある．秘密鍵などの重要な情報を管理する難しさは，情報漏洩や盗難防止のためにコピーを極力作りたくない反面，データの破損や紛失防止のためにはコピーを複数保持したいという，2 つの要求が矛盾する点にある[1, 2]．このような問題に対しても 1970 年代後半に Blakley[1]と Shamir[2]が独立に解決策を示しており，この方法を $(k,n)$ しきい値秘密分散法（$(k,n)$–Threshold Secret Sharing Scheme，以下では単に，$(k,n)$ しきい値法）と呼ぶ．

$(k,n)$ しきい値法では，秘密情報 $S$ を $n$ 個の分散情報（Share）と呼ばれる情報に分散して符号化する．$n$ 個の分散情報のうち，任意の $k\,(\leq n)$ 個以上からは $S$ が完全に復号できるが，任意の $k-1$ 個以下の分散情報からは $S$ に関する情報が一切漏れないようにすることで，$k-1$ 個以下の盗難，$n-k$ 個までの情報の破損に耐性を持たせることができる．

本節では，有限体上の代数演算に基づく秘密分散法（Secret Sharing Scheme）について述べる*．

## 13-3-2 $(k,n)$ しきい値法

### (1) 定　義

秘密情報 $S$ を有限集合 $\mathcal{S}$ 上に値をとる確率変数とし，暗号化に用いられる乱数を有限集合 $\mathcal{E}$ 上に値をとる確率変数 $E$ で表す．ここで，$i$ 番目の分散情報が値をとる有限集合を $\mathcal{P}_i$, $i=1,2,\ldots,n$ と書くと，$(k,n)$ しきい値法の暗号化は決定的写像 $\varphi : \mathcal{S}\times\mathcal{E} \to \mathcal{P}_1\times\mathcal{P}_2\times\cdots\times\mathcal{P}_n$ によって表され，$(S,E,\varphi)$ から $\mathcal{P}_i$ 上に値をとる確率変数 $P_i$ に関する同時分布 $(P_1,P_2,\ldots,P_n)$ が定まる．このような設定のもとで $(k,n)$ しきい値法は次のように定義できる．

定義 1. 秘密情報を表す確率変数 $S$ と任意の分散情報集合 $\boldsymbol{A}\subset\{P_1,P_2,\ldots,P_n\}$ が次を満たすとき，$(S,E,\varphi)$ は $(k,n)$ しきい値法をなすという．

$$H(S|\boldsymbol{A}) = \begin{cases} 0, & \text{if } |\boldsymbol{A}| \geq k \\ H(S), & \text{if } |\boldsymbol{A}| \leq k-1 \end{cases} \tag{13･1}$$

ここで，$H(\cdot)$ はエントロピーである．　□

式 (13･1) における $|\boldsymbol{A}| \leq k-1$ の場合は，秘密情報 $S$ が分散情報集合 $\boldsymbol{A}$ と確率的に独立であることを意味し，いかなる能力を持った攻撃者に対しても $\boldsymbol{A}$ から $S$ に関する情報が一切漏れない．このような攻撃者の能力に依存しない安全性を，計算量的安全性と対比して情報

* 秘密分散法には，それ以外にも視覚情報を用いる視覚復号型秘密分散法，量子状態を用いて量子状態や古典情報を分散する量子秘密分散法など，全く異なる実現手法があるが，本稿では省略する．

理論的安全性†（Information Theoretic Security）という．

**（2）Shamir の $(k,n)$ しきい値法と符号化効率**

まず，最も基本的な Shamir による $(k,n)$ しきい値法の構成法を説明する[2]．

**［暗号化］** ディーラは，有限体 $\mathbb{F}$ 上の値を係数に持つ $k-1$ 以下の多項式を，一様分布に従って選ぶ．選んだ多項式を，

$$f(x) = s + a_1 x^1 + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \tag{13･2}$$

とおく*．ディーラは $i$ 番目の分散情報として $p_i \stackrel{\text{def}}{=} f(i), i = 1,2,\ldots,n$ を計算し，$i$ 番目の参加者に秘密通信路を用いて配布する．配布後は $f(x)$ を消去してよい．

**［復号］** 任意の $(i_u, p_{i_u}) = (i_u, f(i_u)), u = 1,2,\ldots,k$ を用いれば，Lagrange の補間公式から，$k-1$ 次の多項式 $f(x)$ は次のように復元される．

$$f(x) = \sum_{u=1}^{k} p_{i_u} \prod_{\substack{v=1 \\ v\neq u}}^{k} \frac{x - i_v}{i_u - i_v} \tag{13･3}$$

なお，式 (13･2) のように $f(x)$ の定数項を秘密情報にする場合は，次のように $x = 0$ を代入することで，多項式 $f(x)$ そのものを求めることなく $s$ の値が計算できる†．

$$s = f(0) = \sum_{u=1}^{k} p_{i_u} \prod_{\substack{v=1 \\ v\neq u}}^{k} \frac{i_v}{i_v - i_u} \tag{13･4}$$

Shamir の $(k,n)$ しきい値法が式 (13･1) を満足することは，以下のように確認できる．$k$ 個以上の分散情報から秘密情報が復号できることは Vandermonde 行列の正則性から容易に分かる．また，$k-1$ 個以下の分散情報に対する安全性は，$k-1$ 個の分散情報から得られる連立方程式の数が $k-1$ 本であるのに対して，必要とする未知数 $s, a_i$ の数が $k$ 個あることから直感的に理解できるが，厳密な証明は文献[3]などを参照して欲しい．

ここで，Shamir の $(k,n)$ しきい値法の符号化効率について考えてみよう．もし秘密情報 $s$，乱数 $a_i, i = 1,2,\ldots,k-1$ が同じ有限体 $\mathbb{F}$ の上の一様分布に従って独立に選ばれているとすれば，$H(S) = H(P_1) = H(P_2) = \cdots = H(P_n) = \log_2 |\mathbb{F}|$ が成立する．次の定理は，Shamir の $(k,n)$ しきい値法が，分散情報のサイズに関して最適であることを示している．

定理 1 (Karnin-Greene-Hellman[3])．任意の $(k,n)$ しきい値法において，$H(P_i) \geq H(S), i = 1,2,\ldots,n$ が成り立つ．つまり，分散情報のサイズは秘密情報のそれより小さくできない．□

### 13-3-3 ランプ型秘密分散法

定理 1 がもう一つ意味することは，もし分散情報のサイズを秘密情報より小さくすると，$k-1$ 個以下の分散情報から秘密情報が漏洩してしまうということである．このような視点か

† または，無条件安全性（Unconditional Security）ともいう．

* ここで，多項式の最高次数の係数は 0 であってもよいことに注意する．

† $(k,n)$ しきい値法を構成するとき，式 (13･2) の任意の係数を秘密情報にすることができるが，定数項を秘密情報にしていることが多いのは，このように $s$ が簡単に計算できるためである．

ら，秘密情報の部分情報が漏洩することを許す代わりに分散情報のサイズを小さくする方法を，ランプ型秘密分散法（Ramp Secret Sharing Scheme）という．ランプ型しきい値秘密分散法である $(k,d,n)$ ランプ型しきい値法は，Blakley-Meadows[4], 山本[5]によって独立に提案された．$(k,d,n)$ ランプ型しきい値法では式 (13･1) の代わりに次を要請する．

$$H(S|\boldsymbol{A}) = \begin{cases} 0, & \text{if } |\boldsymbol{A}| \geq k \\ \ell H(S)/d, & \text{if } |\boldsymbol{A}| = k-\ell \\ H(S), & \text{if } |\boldsymbol{A}| \leq k-d-1 \end{cases} \qquad \text{for } \ell = 1,2,\ldots,d \tag{13･5}$$

ここで，$1 \leq d \leq k$ であり，$d=1$ の場合，式 (13･5) は式 (13･1) に一致する．$(k,d,n)$ ランプ型しきい値法を実現するには，秘密情報を $(s_0,s_1,\ldots,s_{d-1}) \in \mathcal{S}^d$ として式 (13･2) の代わりに $f(x) = s_0 + \cdots + s_{d-1}x^{d-1} + a_d x^d + \cdots + a_{k-1}x^{k-1}$ とすればよい．もし，$s_i, i=0,\ldots,d-1$ 及び $a_i$, $i=d,\ldots,k-1$ が有限体 $\mathbb{F}$ 上の一様分布に従って独立に選ばれているなら，$H(S) = d\log_2|\mathbb{F}|$, $H(P_1) = H(P_2) = \cdots = H(P_n) = \log_2|\mathbb{F}|$ となり，分散情報のサイズが秘密情報のサイズの $1/d$ であることが分かる．定理 1 と同様に，この方式が最適であることが次の定理から分かる．

定理 2 (山本[5]). 任意の $(k,d,n)$ ランプ型秘密分散法において，$H(P_i) \geq H(S)/d, i=1,2,\ldots,n$ が成り立つ．つまり，分散情報のサイズは秘密情報のサイズの $1/d$ より小さくできない．□

### 13-3-4 一般アクセス構造への拡張

$(k,n)$ しきい値法は，分散情報の個数に応じて秘密情報を復号する権限が与えられる方式である．より一般に，任意の分散情報集合に対して秘密情報を復号する権限が与えられるように拡張された秘密分散法を，一般アクセス構造に対する秘密分散法（Secret Sharing Scheme for General Access Structures）という．ここで，秘密情報を復号することが許される集合を有資格集合（Qualifies Set, Authorized Set）と呼び，秘密情報に関する情報が一切得られない集合を禁止集合（Forbidden Set, Unauthorized Set）と呼ぶ．また，有資格集合と禁止集合の族をそれぞれ $\mathcal{A}_{\mathsf{Q}}, \mathcal{A}_{\mathsf{F}}$ と書き，$(\mathcal{A}_{\mathsf{Q}}, \mathcal{A}_{\mathsf{F}})$ をアクセス構造（Access Structure）と呼ぶ．一般に $\mathcal{A}_{\mathsf{Q}} \cap \mathcal{A}_{\mathsf{F}} = \emptyset$ であるが，$\mathcal{A}_{\mathsf{Q}} \cup \mathcal{A}_{\mathsf{F}}$ が分散情報全体の冪集合に一致する必要はない．

一般アクセス構造に対しては，以下の要請が自然に導入される．

定義 2 (単調性). 有資格集合を含む任意の分散情報集合が有資格集合となり，禁止集合の任意の部分集合が禁止集合となるようなアクセス構造は単調性（Monotonicity）を持つという．□

単調性が秘密分散法を構成するうえでの必要条件であることは明らかである．そこで問題になるのは，単調性を持つアクセス構造が適切なサイズの有限体のもとで常に実現可能か，ということである．この問題に対しては次のような肯定的な結果が得られている．

定理 3 (伊藤-斎藤-西関[6]). 単調性を持つ任意のアクセス構造を持つ秘密分散法は，適切なサイズの有限体のもとで必ず構成できる．□

なお，有資格集合に対して異なる複数の秘密情報を割り当てる秘密分散法も提案されている[7]．また，ランプ型秘密分散法で一般のアクセス構造を考えることも可能である．これらについては文献 8) で検討されており，単調性の概念を自然に拡張することで定理 3 と同様の結果が成り立つことが知られている．

### 13-3-5 秘密分散法の機能拡張

秘密分散法は重要なデータの管理だけでなく，マルチパーティー計算などへの応用といった観点から，様々な機能拡張が提案されている．それらについて以下に簡単に述べる．

(a) アクセス構造や分散情報の更新

秘密情報を長期間保管する場合に，アクセス構造を途中で動的に変更したり[9]，アクセス構造はそのままで，分散情報の値だけを更新する手法[10]が提案されている．

(b) 不正者の検出や特定

マルチパーティー計算においては，参加者の不正を防ぐことが不可欠である．単に不正の存在を検出する方式[11]やディーラを含む不正者を特定する方法（可検証秘密分散[12], Verifiable Secret Sharing Scheme）などがある．

(c) ゲーム理論を考慮した秘密分散法

近年，マルチパーティ計算において参加者の行動がゲーム理論に基づいて変化する場合が議論されている．このような状況を考慮した秘密分散法が提案されている[13]．

**■参考文献**


1) G.R. Blakley：“Safeguarding cryptographic keys,” AFIPS 1979 National Computer Conference, vol.48, pp.313–317, 1979.
2) A. Shamir：“How to share a secret,” Communications of the ACM, vol.22, no.11, pp.612–613, 1979.
3) E.D. Karnin, J.W. Greene, and M.E. Hellman：“On secret sharing systems,” IEEE Trans. Inform. Theory, vol.29, no.1, pp.35–41, 1983.
4) G.R. Blakley and C. Meadows：“Security of ramp schemes,” Advances in Cryptology-CRYPTO’84, LNCS 196, Springer-Verlag, pp.242–269, 1985.
5) 山本：“$(k, L, n)$ しきい値秘密分散システム,” 電子通信学会論文誌, vol.J68–A, no.9, pp.945–952, 1985. English translation: Electronics and Communications in Japan, Part I, vol. 69, no. 9, pp. 46–54, Scripta Technica, Inc., 1986.
6) M. Itoh, A. Saito, and T. Nishizeki：“Multiple assignment scheme for sharing secret,” Journal of Cryptology, vol.6, pp.15–20, 1993. Preliminary version: IEEE Globecom’87, pp.99–102.
7) C. Blundo, A.D. Santis, and U. Vaccaro：“Efficient sharing of many secrets,” Proc. of STACS’93 LNCS 665, Springer-Verlag, pp.692–703, 1993.
8) K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and T. Tsujii：“Nonperfect secret sharing schemes and matroids,” Advances in Cryptology-EUROCRYPT’93, LNCS 765, Springer-Verlag, pp.126–141, 1993.
9) C. Blundo, A. Cresti, A.D. Santis, and U. Vaccaro：“Fully dynamic secret sharing scheme,” Theoretical Computer Science, no.165, pp.407–440, 1996. Preliminary version: CRYPTO’94, pp.150–163.
10) A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung：“Proactive secret sharing or: how to cope with perpetual leakage,” Advances in Cryptology-CRYPTO’95 LNCS 963, Springer-Verlag, pp.186–208, 1995.
11) M. Tompa and H. Woll：“How to share a secret with cheaters,” Journal of Cryptology, vol.1, no.3, pp.133–138, 1988. Preliminary version: CRYPTO’86, LNCS 263, pp.262–265.
12) T.P. Pedersen：“Non–interactive and information–theoretic secure verifiable secret sharing,” Advances in Cryptology–CRYPTO’91, LNCS 576, Springer-Verlag, pp.221–242, 1991.
13) J. Halpern and V. Teague：“Rational secret sharing and multiparty computation,” Proc. of 36th STOC, pp.623–632, 2004.

■1 群 - 1 編 - 13 章

# 13-4 Information Hiding

■1 群 - 1 編 - 13 章

# 13-5 相関乱数を利用した秘密鍵共有と Secret Key Capacity

（執筆者：村松　純）[2009 年 12 月 受領]

## 13-5-1 相関乱数を利用した秘密鍵共有

二人の正規のユーザーと盗聴者（両者を合わせて「全ユーザー」と呼ぶ）に互いに相関のある乱数系列が事前に配布されている状況のもとで，正規のユーザーが公開通信路上で情報交換を行うことにより，盗聴者が知ることができない秘密鍵を生成することを考える（図 13･1 を参照）．これは相関乱数を利用した秘密鍵共有と呼ばれている．この問題は Maurer [1) 4)] と Ahlswede-Csiszár [3)] によって独立に導入された．

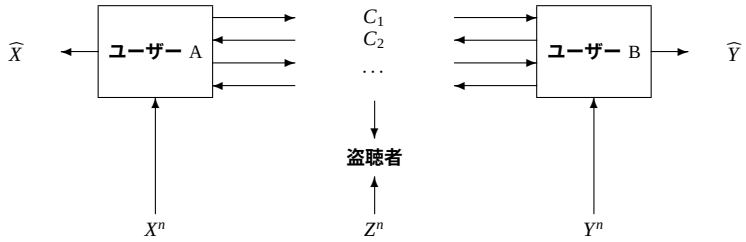


**図 13･1　相関乱数を利用した秘密鍵共有**

相関乱数を利用した秘密鍵共有では，ユーザーに乱数が配布する方法に関して以下の 2 通りの設定が考えられている．

**通信路モデル**　正規のユーザーの一人が乱数を生成して，雑音のある通信路を通して送信する．その出力をもう一人の正規のユーザーと盗聴者が受信した結果を乱数として保持する．結果として，全ユーザーが相関乱数を入手したことになる．

**情報源モデル**　正規のユーザーと盗聴者に乱数系列があらかじめある相関のある情報源の出力として配布されている状況を考える．この状況を説明する一つの (特殊な) 例として，Maurer [4)] の衛星放送を用いたシナリオがある．正規のユーザーにとって信頼のおける衛星が全ユーザーにとって未知の乱数系列を放送し，それぞれのユーザーがそれぞれの持つアンテナを用いて受信した結果を乱数として保持する．このとき，衛星と各アンテナの間に雑音のある通信路を仮定すれば，それぞれの通信路の出力は相関のある情報源とみなすことができる．

以下では，情報源モデルに焦点をあてる（通信路モデルに関しては文献 3) を参照）．正規ユーザーをそれぞれ「ユーザー A」,「ユーザー B」と呼び，盗聴者を「ユーザー E」と呼ぶ．そして，ユーザー A，ユーザー B，ユーザー E に配布された乱数を定常無記憶な確率過程として，それぞれ確率変数 $X, Y, Z$ と記す．

### 13-5-2 秘密鍵容量

#### (1) プロトコル

ユーザー A，ユーザー B に配布された乱数から秘密鍵を共有するために使用するプロトコルの形式的な定義を以下に与える．

**定義**．ユーザー A，ユーザー B，ユーザー E が利用できる情報源の $n$ 回の出力をそれぞれ $X^n, Y^n, Z^n$ とする．ステップ数 $t$ のプロトコル $(C_1^t, \widehat{X}, \widehat{Y})$ は，メッセージ交換を表す確率変数 $C_1^t \equiv (C_1, \ldots, C_t)$ とメッセージ交換後に送信者と受信者が計算する確率変数 $\widehat{X}, \widehat{Y}$ で構成される．ここでは，公開された情報は盗聴者によって改竄されないことを仮定する．

1. ユーザー A は，これまでに公開された情報 $C_1^{i-1}$ と乱数系列 $X^n$ から $C_i$ ($i \geq 1$ は偶数) を非決定的な手続きを用いて計算して公開する．ただし，$i = 1$ のときは公開された情報はないので $C_1^{-1}$ を利用しない．

2. ユーザー B は，これまでに公開された $C_1^{i-1}$ と乱数系列 $Y^n$ から $C_i$ ($i \geq 2$ は偶数) を非決定的な手続きを用いて計算して公開する．

3. 上記の手続き 1, 2 を，$i$ を 1 つずつ増加させながら $i = t$ になるまで繰り返す．

4. ユーザー A は，これまでに公開された $C_1^t$ と $X^n$ から非決定的な手続きを用いて $\widehat{X}$ を計算する．同時に，ユーザー B は，これまでに公開された $C_1^t$ と $Y^n$ から非決定的な手続きを用いて $\widehat{X}$ を計算する．

形式的には，$(C_1^t, \widehat{X}, \widehat{Y})$ は，以下の性質を満たす確率変数である*．

$$Z^n Y^n C_{i+1}^t \leftrightarrow X^n C_1^{i-1} \leftrightarrow C_i, \quad i \geq 1 \text{ が奇数のとき} \tag{13·6}$$

$$Z^n X^n C_{i+1}^t \leftrightarrow Y^n C_1^{i-1} \leftrightarrow C_i, \quad i \geq 2 \text{ が偶数のとき} \tag{13·7}$$

$$Z^n Y^n \leftrightarrow X^n C_1^t \leftrightarrow \widehat{X} \tag{13·8}$$

$$Z^n X^n \leftrightarrow Y^n C_1^t \leftrightarrow \widehat{Y} \tag{13·9}$$

ここで，関係式 $U \leftrightarrow V \leftrightarrow W$ は確率変数 $U, V, W$ がマルコフ連鎖をなしていることを意味する．

#### (2) 秘密鍵共有プロトコルと秘密鍵容量（Secret Key Capacity）

ユーザー A と ユーザー B は，前節で定義したプロトコル $(C_1^t, \widehat{X}, \widehat{Y})$ を用いて相関のある乱数から秘密鍵を共有する．プロトコルを用いて生成された新たな乱数 $(\widehat{X}, \widehat{Y})$ を，使い捨て暗号などの秘密鍵とするためには，次の 2 つの条件を満たす必要がある．

- 乱数系列 $\widehat{X}$ と $\widehat{Y}$ は 1 に近い確率で一致していなければならない．
- 盗聴者の入手した乱数 $Z^n$ と公開された情報 $C_1^t$ から秘密鍵 $(\widehat{X}, \widehat{Y})$ に関する情報が洩れ

* 上記のプロトコルの定義では，$C_1^t, \widehat{X}, \widehat{Y}$ を計算する手続きとして非決定的なものを許すと仮定したが，決定的な計算しか許さない場合も考えられている．

ていてはいけない.

それぞれのユーザーが所持している相関のある情報源 $X, Y, Z$ から共有可能な秘密鍵の情報量の上限は秘密鍵容量（Secret Key Capacity）と呼ばれ，形式的には以下のように定義される．

**定義**．ユーザー A，ユーザー B，盗聴者の利用できる情報源をそれぞれ $X, Y, Z$ とする．レート $R \geq 0$ の秘密鍵共有プロトコル $(C_1^t, \widehat{X}, \widehat{Y})$ は，任意の $\varepsilon > 0$ に対して以下の条件を満たすプロトコルである*.

$$\Pr\left(\widehat{X} \neq \widehat{Y}\right) \leq \varepsilon \tag{13･10}$$

$$\frac{I(\widehat{X}; Z^n C_1^t)}{n} \leq \varepsilon \tag{13･11}$$

$$H(\widehat{X}) \geq \log|\widehat{\mathcal{X}}| - \varepsilon \tag{13･12}$$

$$\frac{H(\widehat{X})}{n} \geq R - \varepsilon \tag{13･13}$$

ここで，$|\widehat{\mathcal{X}}|$ は確率変数 $\widehat{X}$ のとりうる値の集合である．秘密鍵共有プロトコル（ブロック長 $n$，ステップ数 $t$ の制限なし）によって達成可能なレートの上限を**秘密鍵容量** と呼び，$S(X; Y\|\|Z)$ と記す.

上記の定義において, 前述の二条件はそれぞれ式 (13･10), 式 (13･11) と対応する．式 (13･12) は秘密鍵 $\widehat{X}$ が等確率分布に近いことを，式 (13･13) は秘密鍵 $\widehat{X}$ の生成レート（乱数 1 文字当たりの情報量）が $R$ であることを意味する．ここで，条件 (13･11) をより強い条件

$$I(\widehat{X}; Z^n C_1^t) \leq \varepsilon$$

に置き換えた場合のプロトコルと鍵生成レートの上限は，それぞれ強秘密鍵共有プロトコル，強秘密鍵容量と呼ばれる．強秘密鍵容量が秘密鍵容量と同一の値となることは Maurer-Wolf [5] によって示されている.

### 13-5-3 秘密鍵共有が可能となる相関情報源の条件

興味のある一つの問題として，与えられた相関乱数源を用いて秘密鍵共有が可能であるかどうかを判定する問題がある．Maurer [6] は，前述の衛星放送シナリオで衛星が 2 値の信号を発信する衛星とユーザーと盗聴者の持つアンテナ間の離散通信路が独立である場合に，秘密共有が可能（すなわち秘密鍵容量が正）となる相関情報源の必要十分条件

$$S(X; Y\|\|Z) > 0 \Leftrightarrow I(X; Y|Z) > 0$$

を導出した.

### 13-5-4 秘密鍵容量の情報理論的表現

秘密鍵容量の情報理論的表現（計算可能な形式）を求める問題は特殊な場合を除いては未

* エントロピー，相互情報量の定義については文献 [3] を参照.

解決の問題として残されている．以下，これまでに知られている主要な結果を列挙する．

**(1) 秘密鍵容量の上界と下界**

Maurer [4] は，以下の秘密鍵容量の上界と下界を導出した．

**定理**．ユーザー A，ユーザー B，盗聴者の利用できる情報源をそれぞれ $X, Y, Z$ とする．このとき，任意の $(X, Y, Z)$ に対して，

$$\max\{I(X;Y) - I(X;Z), I(X;Y) - I(Y;Z)\} \le S(X;Y||Z) \le \min\{I(X;Y), I(X;Y|Z)\}$$

が成り立つ．

よりタイトな上界については Maurer-Wolf [6]，Renner-Maurer [7] で与えられている． 特に，Renner-Maurer [7]では，Maurer-Wolf [6]の上界がタイトでない（同時に $I(X;Y|Z)$ もタイトでない）ことを示す例を挙げている．

**(2) $S(X;Y||Z) = I(X;Y|Z)$ の十分条件**

Ahlswede-Csiszár [3]は，秘密鍵容量に関して以下の結果を与えた．

**定理**．ユーザー A，ユーザー B，盗聴者の利用できる情報源 $X, Y, Z$ がいずれかの順序でマルコフ連鎖となっているとき，

$$S(X;Y||Z) = I(X;Y|Z)$$

が成り立つ．

**(3) 1 ステップの秘密鍵共有**

Ahlswede-Csiszár [3]は，ユーザー A のみが情報を公開する場合（$t = 1$ の場合）に関する秘密鍵容量を導出した．なお，強秘密鍵容量についても同様の結果が得られることは Csiszár [4] で示されている．

**定理**．ユーザー A，ユーザー B，盗聴者の利用できる情報源をそれぞれ $X, Y, Z$ とする．このとき，1 ステップの秘密鍵共有プロトコルで達成可能なレートの上限*$S_{t=1}(X;Y||Z)$ は

$$S_{t=1}(X;Y||Z) = \max_{(U,T):U\leftrightarrow T\leftrightarrow X\leftrightarrow YZ} [I(T;Y|U) - I(T;Z|U)] \tag{13・14}$$

で与えられる．特に，$X \leftrightarrow Y \leftrightarrow Z$ が成立している場合は，

$$S_{t=1}(X;Y||Z) = S(X;Y||Z) = I(X;Y) - I(X;Z)$$

となる．すなわち，ユーザー A が情報を公開するだけで秘密鍵容量を達成可能である．

特に，ユーザー A とユーザー B の相関を相互情報量 $I(X;Y)$ とユーザー A と盗聴者ユーザー B の相関を相互情報量 $I(X;Z)$ に関して

$$I(X;Y) - I(X;Z) > 0 \tag{13・15}$$

* 文献 [3]では Forward Key Capacity と呼んでいる．

が成立している状況では，情報整合と秘密増幅（13-6 節を参照）を同時に行うプロトコルを用いて左辺を鍵生成レートとする 1 ステップの秘密鍵共有が可能である．情報整合と秘密増幅を同時に行うプロトコルについては Cachin-Maurer [2)]で提案されており，Ahlswede-Csiszár [3)]，Csiszár [4)]，Muramatsu [10)]は，式 (13･15) を満たせばこの左辺と同じ鍵生成レートを持つ 1 ステップの秘密鍵共有プロトコル（情報整合・秘密増幅）が設計できることを示している．1 ステップの秘密鍵共有プロトコルで達成可能なレートの上限 (13･14) は，$X$ から適切な通信路を用いて右辺に現れる $U,T$ を生成して新たな相関情報源 $((T,U),(Y,U),(Z,U))$ を考えることにより，

$$I(T;Y|U) - I(T;Z|U) = I(T,U;Y,U) - I(T,U;Z,U)$$

をレートとする情報整合と秘密増幅を同時に行うプロトコルを用いることによって達成可能である．

**（4）優位性抽出容量と秘密鍵容量**

秘密鍵共有プロトコルは通常，1. 優位性抽出，2. 情報整合，3. 秘密増幅の 3 段階に分けて構成される（13-6 節を参照）．このうち優位性抽出は，ユーザー A とユーザー B の相関を相互情報量 $I(X;Y)$ とユーザー A と盗聴者ユーザー B の相関を相互情報量 $I(X;Z)$ に関して $I(X;Y) \le I(X;Z)$ が成立している状況で，$I(\widehat{X};\widehat{Y}) \ge I(\widehat{X};Z^n,C_1^t)$ を満たすように設計されたプロトコル $(C_1^t,\widehat{X},\widehat{Y})$ を指す．Muramatsu-Yoshimura-Davis [11)]は，優位性抽出容量を以下のように定義した．

**定義**．ユーザー A，ユーザー B，盗聴者の利用できる情報源をそれぞれ $X, Y, Z$ とする．このとき，相関乱数 $(X,Y,Z)$ の優位性抽出容量 $D(X;Y\|Z)$ を，プロトコルの実行によって達成可能な相互情報量の差の上限として定義する．すなわち，

$$D(X;Y\|Z) \equiv \sup_{n,t,(C_1^t,\widehat{X},\widehat{Y})} \frac{1}{n}\left[I(\widehat{X};\widehat{Y}) - I(\widehat{X};Z^nC_1^t)\right]. \tag{13･16}$$

ここで，sup では条件 (13･6)〜(13･9) を満たすすべての確率変数 $(C_1^t,\widehat{X},\widehat{Y})$ にわたる．

これに基づき，Muramatsu-Yoshimura-Davis [11)]は以下の定理を与えた．

**定理**．ユーザー A，ユーザー B，盗聴者の利用できる情報源をそれぞれ $X, Y, Z$ とする．任意の $(X,Y,Z)$ に対して

$$D(X;Y\|Z) = S(X;Y\|Z) \tag{13･17}$$

が成り立つ．

この定理と前述の式 (13･15) の左辺を達成する情報整合・秘密増幅を構成できることから，秘密鍵共有プロトコルを優位性抽出，情報整合，秘密増幅の 3 段階に分けて構成しても，秘密鍵容量が達成可能であることが分かる．式 (13･16)，式 (13･17) より得られる式

$$S(X;Y\|Z) \equiv \sup_{n,t,(C_1^t,\widehat{X},\widehat{Y})} \frac{1}{n}\left[I(\widehat{X};\widehat{Y}) - I(\widehat{X};Z^nC_1^t)\right]$$

は秘密鍵容量の情報理論的な表現であると解釈することもできるが，$n, t$ や $C_1^t, \widehat{X}, \widehat{Y}$ のアルファベットサイズが制限されていないため，厳密な意味での情報理論的な表現ではないことを注意しておく．

**■参考文献**


1) U.M. Maurer：“Perfect cryptographic security from partially independent channels,” Proc. 23rd ACM Symp. Theory of Computing, New Orleans, LA, May 6–8, pp.561–572, 1991.
2) U.M. Maurer：“Secret key agreement by public discussion from common information,” IEEE Trans. Inform. Theory, vol.IT-39, pp.733–742, May 1993.
3) R. Ahlswede and I. Csiszár：“Common randomness in information theory and cryptography – Part I: Secret sharing,” IEEE Trans. Inform. Theory, vol.IT-39, pp.1121–1132, Jul. 1993.
4) T.M. Cover and J.A. Thomas：Elements of Information Theory 2nd. Ed., John Wiley & Sons, Inc., 2006.
5) U.M. Maurer and S. Wolf：“Information-theoretic key agreement: from weak to strong secrecy for free,” Lecture Notes in Computer Science, vol.1807, pp.351–368, 2000.
6) U.M. Maurer and S. Wolf：“Unconditionally secure key agreement and the intrinsic conditional information,” IEEE Trans. Inform. Theory, vol.45, pp.499–514, Mar. 1999.
7) R. Renner and S. Wolf：“New bounds in secret-key agreement: The gap between formation and secrecy extraction,” Lecture Notes in Computer Science, vol.2656, pp.562–577, 2003.
8) I. Csiszár：“Almost independence and secrecy capacity,” Problems of Information Transmission, vol.32, no.1, pp.40–47, 1996.
9) C. Cachin and U.M. Maurer：“Linking information reconciliation and privacy amplification,” J. Criptology, vol.10, pp.97–110, 1997.
10) J. Muramatsu：“Secret key agreement from correlated source outputs using low density parity check matrices,” IEICE Trans. Fundamentals, vol.E89-A, no.7, pp.2036–2046, Jul. 2006.
11) J. Muramatsu, K. Yoshimura, and P. Davis：“Secret key capacity and advantage distillation capacity,” IEICE Trans. Fundamentals, vol.E89-A, no.10, pp.2589–2596, Oct. 2006.

■1 群 - 1 編 - 13 章

# 13-6 Privacy Amplification

（執筆者：村松　純）[2009 年 12 月 受領]

## 13-6-1 秘密鍵共有の 3 段階

相関乱数からの秘密鍵共有（13-5 節参照）に関して，秘密鍵共有プロトコルを以下の 3 段階に分けて構成するというアプローチがある．この 3 段階は Bennett-Brassard-Crepeau-Maurer [1)]，Cachin-Maurer [2)]で導入され，これらの 3 段階に分けて秘密鍵共有プロトコルを設計しても秘密鍵容量を達成することができる（13-5 節参照）．正規のユーザー A，ユーザー B と盗聴者の入手する乱数系列を表す確率変数をそれぞれ $X, Y, Z$ とする．また，プロトコル $(C_1^t, \widehat{X}, \widehat{Y})$ は 13-5-2 項で与えられた定義に従う*.

1. **優位性抽出**（Advantage Distillation）　ユーザー A の乱数 $X$ とユーザー B の乱数 $Y$ の相関よりもユーザー A の乱数 $X$ と盗聴者の乱数 $Y$ の相関のほうが大きいとき，この関係を逆転させるために設計されたプロトコルを優位性抽出プロトコルと呼ぶ．形式的には，ユーザー A とユーザー B の相関を相互情報量 $I(X;Y)$ とユーザー A と盗聴者ユーザー B の相関を相互情報量 $I(X;Z)$ に関して $I(X;Y) \le I(X;Z)$ が成立しているときに，優位性抽出プロトコル $(C_1^t, \widehat{X}, \widehat{Y})$ は $I(\widehat{X};\widehat{Y}) \le I(\widehat{X};Z^n, C_1^t)$ を満たすように設計される．盗聴通信路（本章 5-7 節参照）の場合，送信者（正規ユーザー A）が通信路に入力した情報 $X$ に対して，受信者（正規ユーザー B）の受信 $Y$ によって得た入力に関する情報量 $I(X;Y)$ が盗聴者の受信 $Z$ によって得た入力に関する情報量 $I(X;Z)$ よりも大きいときにのみ，秘密通信が可能であった．これに対して Maurer [4)] は，ユーザー B と盗聴者の立場が逆 (すなわち盗聴者がユーザー B よりも $X$ に関する情報量が大きい) の場合でも，優位性抽出プロトコル†によって秘密鍵共有が可能である例を示した‡.

2. **情報整合**（Information Reconciliation）　ユーザー A，ユーザー B，盗聴者の利用できる情報源 $X, Y, Z$ は，(必要に応じて) 優位性抽出プロトコルを実行した結果，

$$I(X;Y) - I(X;Z) > 0$$

を満たしていることを仮定する．ここで，ユーザー A とユーザー B が一致系列を得るために設計されたプロトコルを情報整合プロトコルと呼ぶ．形式的には，情報整合プロトコル $(C_1^t, \widehat{X}, \widehat{Y})$ は，十分小さい $\varepsilon > 0$ に対して

$$\mathrm{Prob}(\widehat{X} \neq \widehat{Y}) \le \varepsilon$$

を満たすように設計される．このプロトコルでは通常，ユーザー A のみが情報公開を行う（すなわち $t = 1$）．そのためにはユーザー A は情報源 $X$ を符号化した結果を公開し，ユーザー B は取得した情報源 $Y$ を $X$ の補助情報として利用して情報源 $X$ を再生する§こと

* エントロピー，相互情報量の定義については文献 [3)]を参照.

† ユーザー A とユーザー B が互いに情報を公開することから公開議論（Public Discussion）と呼ばれている

‡ 盗聴通信路にフィードバックがある場合に同様のことが起こることは文献 [5)]で与えられている.

§ Slepian-Wolf 符号化において，復号器が補助情報をが直接観測できる特殊な場合である.

より一致系列を得る．このプロトコルに関しては Bennett-Bessette-Brassard-Salvail [6]，Brassard-Salvail [7]で議論されている．

3. **秘密増幅**（Privacy Amplification）　ユーザー A，ユーザー B，盗聴者の利用できる情報源 $X, Y, Z$ は，(必要に応じて) 情報整合プロトコルを実行した結果，

$$X = Y$$

を満たしていることを仮定する．ここで，ユーザー A とユーザー B が盗聴者が知ることができない (一致した) 秘密鍵系列を得るために設計されたプロトコルを秘密増幅プロトコルと呼ぶ．形式的には，秘密増幅プロトコル $(C_1^t, \widehat{X}, \widehat{Y})$ は十分小さい $\varepsilon > 0$ に対して

$$\widehat{X} = \widehat{Y}$$
$$I(\widehat{X}; Z^n, C_1^t) \leq \varepsilon$$

を満たすように設計される．このプロトコルに関しては，Bennett-Brassard-Robert [8] や Bennett-Brassard-Crepeau-Maurer [1]で議論されている．また，Cachin-Maurer [2]は前述の情報整合と秘密増幅を同時に行う場合を考察している．

本節では，最後の秘密増幅について解説する．以下では，ユーザー A とユーザー B の持つ情報源を $X$，盗聴者の持つ情報源を $Z$ と記す．

### 13-6-2 ユニバーサルハッシュ関数族を用いた秘密増幅

ユニバーサルハッシュ関数族を用いた秘密増幅は Bennett-Brassard-Robert [8]によって初めて導入された．ここでは，ユニバーサルハッシュ関数族を用いた秘密増幅について述べる．

#### (1) ユニバーサルハッシュ関数族

ユニバーサルハッシュ関数族は Carter-Wegman [9]によって導入された．以下にユニバーサルハッシュ関数族の定義を与える．

**定義**．定義域を $\mathcal{X}$，値域を $\mathcal{K}$ とする関数の集合 $\mathcal{F}$ が，任意の異なる要素 $x, x' \in \mathcal{X}$ に対して

$$\mathrm{Prob}(F(x) = F(x')) \leq \frac{1}{|\mathcal{K}|}$$

を満たすとき，$\mathcal{F}$ をユニバーサルハッシュ関数族*と呼ぶ．ここで，Prob は関数 $F \in \mathcal{F}$ を一様分布に従って選択したときの確率を表す．

以下に，ユニバーサルハッシュ関数族の例を与える．

(a) $\mathcal{X}$ から $\mathcal{M}$ への関数全体の集合

定義域を $\mathcal{X}$，値域を $\mathcal{K}$ とする関数の全体から成る集合を $\mathcal{F}$ としたとき，$\mathcal{F}$ はユニバーサルハッシュ関数族となる．これは，Cover [10]によって導入された Bin Coding と呼ばれるもの

* 汎用ハッシュ関数族とも呼ばれる．

と同じである．

(b) **有限体上の線形関数全体の集合**

$q$ 元の有限体を GF($q$) として，定義域を GF($q$)$^n$，値域を GF($q$)$^m$ とする線形関数の全体からなる集合を $\mathcal{F}$ とする．このとき，$\mathcal{F}$ はユニバーサルハッシュ関数族となる．

(c) **GF(2)$^n$ の積と $m$ ビットへの射影によって定義される関数全体の集合**

定義域を GF(2)$^n$ とし，$[\cdot]_m$ を GF(2)$^n$ の元の下位 $m$ ビット ($1 \le m \le n$) を与える写像とする．このとき，GF(2)$^n$ から $\{0,1\}^m$ への関数の集合 $\mathcal{F}$ を

$$\mathcal{F} \equiv \{f : f(x) \equiv [ax]_m, a \in \mathrm{GF}(2)^n\}$$

と定義すると，$\mathcal{F}$ はユニバーサルハッシュ関数族となる．

**(2) ユニバーサルハッシュ関数族を用いた秘密増幅**

ユーザー A とユーザー B は以下の手続きで秘密増幅を行う．ユーザー A とユーザー B の持つ乱数を $X$ として，利用する乱数のアルファベット $\mathcal{X}$ を定義域として $\{0,1\}^m$ を値域とするユニバーサルハッシュ関数族を $\mathcal{F}$ とする．

1. ユーザー A は $\mathcal{F}$ から一様分布で関数 $F$ を 1 つ選択し，$F$ を公開する．
2. ユーザー A とユーザー B は共に $F(X)$ を計算してこれを秘密鍵とする．

主要な結果を述べるために，オーダー 2 の (条件付き) Rényi エントロピーを以下のように定義する．

$$R(X) \equiv -\log_2\left(\sum_{x\in\mathcal{X}} P_X(x)^2\right)$$
$$R(X|Z=z) \equiv -\log_2\left(\sum_{x\in\mathcal{X}} P_{X|Z}(x|z)^2\right)$$
$$R(X|Z) \equiv \sum_{z\in\mathcal{Z}} P_Z(z) R(X|Z=z)$$

ここで，$P_X, P_Z$ はそれぞれ $X, Z$ の確率分布，$P_{X|Z}$ は $Z$ を与えたときの $X$ の条件付き確率分布である．一般に

$$R(X) \le H(X)$$
$$R(X|Z) \le H(X|Z)$$

が成立する．

このとき，Bennett-Brassard-Crepeau-Maurer [1)]は次の定理を示した．

**定理**．ユーザー A とユーザー B の持つ乱数を $X$ として，上記の秘密増幅プロトコルで生成した鍵を $F(X)$ とする．盗聴者が $X$ と相関のある乱数系列を持たないとき，

$$H(F(X)|F) \ge R(F(X)|F) \ge m - \log_2(1+2^{m-R(X)}) \ge m - \frac{2^{m-R(X)}}{\ln 2} \qquad (13\cdot18)$$

が成り立つ.

盗聴者が $X$ と相関のある乱数系列 $Z$ を持つとき，$R(X|Z=z) \geq r$ であれば,

$$H(F(X)|F, Z=z) \geq m - \log_2(1+2^{m-r}) \geq m - \frac{2^{m-r}}{\ln 2}$$

が成り立つ．更に，$Z$ が

$$P_Z(\{z : R(X|Z=z) \geq r\}) \geq 1-\delta \tag{13･19}$$

を満たしているとき,

$$I(F(X); F, Z) \leq \delta m + (1-\delta)\log_2(1+2^{m-r}) \leq \delta m + \frac{2^{m-r}}{\ln 2} \tag{13･20}$$

が成り立つ.

式 (13･18) より

$$m \geq H(F(X)) \geq H(F(X)|F) \geq m - \frac{2^{m-R(X)}}{\ln 2}$$

が成り立つことから，式 (13･18) は盗聴者が $X$ と相関のある乱数系列を持たないときに $m$ を $R(X)$ よりも十分小さくとれば，秘密増幅プロトコルによって盗聴者にとっての鍵 $F(X)$ の曖昧さ $H(F(X)|F)$ を $H(F(X))$ に近づけることができる，すなわち盗聴者の持つ鍵に関する情報量 $I(F(X); F)$ を小さくできることを意味している．式 (13･20) は，盗聴者が $X$ と相関のある乱数系列 $Z$ を持ち，十分小さい $\delta$ に対して式 (13･20) を満たすような $r$ が存在すれば，$m$ を $r$ より小さくとることにより秘密増幅プロトコルによって盗聴者にとっての鍵 $F(X)$ に関する情報量 $I(F(X); F, Z)$ を小さくできることを意味している.

**■参考文献**


1) C.H. Bennett, G. Brassard, C. Crepeau, and U. Maurer：“Generalized privacy amplification,” IEEE Trans. Inform. Theory, vol.IT-41, pp.1915–1923, Nov. 1995.
2) C. Cachin and U.M. Maurer：“Linking information reconciliation and privacy amplification,” J. Criptology, vol.10, pp.97–110, 1997.
3) T.M. Cover and J.A. Thomas：“Elements of Information Theory 2nd. Ed.,” John Wiley & Sons, Inc., 2006.
4) U.M. Maurer：“Secret key agreement by public discussion from common information,” IEEE Trans. Inform. Theory, vol.IT-39, pp.733–742, May 1993.
5) S.K. Leung-Yan-Cheong：“Multi-user And Wiretap Channels Including Feedback,” Ph.D. Dissseratation, Stanforrd University, 1976.
6) C.H. Bennett, F. Bessette, G. Brassard, and L. Salvail：“Experimental Quantum Cryptography,” J. Criptology, vol.5, pp.3–28, 1992.
7) G. Brassard and L. Salvail：“Secret-key reconciliation by public discussion,” Lecture Notes in Computer Science, vol.765, pp.410–423, Splinger-Verlag, 1994.
8) C. H. Bennett, G. Brassard, and J. Robert：“Privacy amplification by public discussion,” SIAM J. Comput., vol.17, pp.210-229, 1988.
9) J. L. Carter and M. N. Wegman：“Universal classes of hash functions,” J. Comput. Syst. Sci., vol.18, pp.143–154, 1979.
10) T. M. Cover：“A proof of the data compression theorem of Slepian and Wolf for ergodic sources,” IEEE Trans. Inform Theory, vol.IT-21, pp.226–228, Mar. 1975.

■1 群 - 1 編 - 13 章

# 13-7 盗聴通信路と Secrecy Capacity

（執筆者：村松　純）[2009 年 12 月 受領]

## 13-7-1 盗聴通信路

盗聴通信路は，**図 13･2** で示されるような，送信者が利用する 1 つの入力端子と，正規の受信者と盗聴者が利用する 2 つの出力端子を持つブロードキャスト通信路である．歴史的には，Wyner [1)]が盗聴通信路を**図 13･3** で示されるような退化通信路として初めて導入し，後に Csiszár-Körner [2)]によってブロードキャスト通信路に一般化された．

以下では，盗聴通信路を条件付き確率分布 $W_{YZ|X}$ を持つ定常無記憶ブロードキャスト通信路として扱い，退化通信路の場合はそのことを明示する．

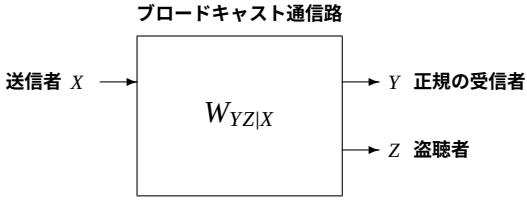


**図 13･2　盗聴通信路（ブロードキャスト型）**

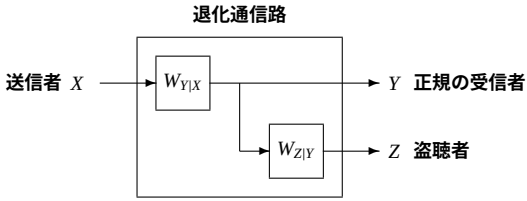


**図 13･3　盗聴通信路（退化型）**

## 13-7-2 盗聴通信路容量（Secrecy Capacity）

**盗聴通信路符号**の構成を**図 13･4** を用いて説明する．まず最初に送信者は，確率的 (非決定的) な符号器 $\Phi_n$ を用いてメッセージ $M$ を符号化して通信路入力 $X^n$ を求め，これを送信する．ここで，確率的な符号器を

$$\text{任意の } m \in \mathcal{M} \text{ に対して} \quad \sum_{x^n \in \mathcal{X}^n} \Phi_{X^n|M}(x^n|m) = 1$$

を満たす条件付き確率分布 $\Phi_{X^n|M}$ で表す．続いて，通信路出力 $Y^n$ を受信した正規の受信者は，復号器 $\psi_n : \mathcal{Y}^n \to \mathcal{M}$ を用いてメッセージの復元を試みる．ここで，通信路出力 $Y^n$ を受信と同時に，盗聴者はもう一方の出力 $Z^n$ を受信するが，この出力からメッセージ $M$ に関する曖昧さ（エントロピー）がある基準以上になるように構成する．

Csiszár-Körner [2)]では，秘匿したいメッセージの伝達に加えて正規の受信者と盗聴者の両者へ共通の情報を伝達する問題へ拡張しているが，以下では，正規の受信者と盗聴者の両者へ伝達する共通の情報はないことを仮定する．

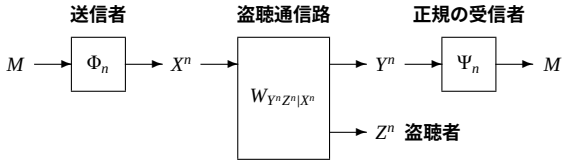


**図 13･4　盗聴通信路符号**

条件付き確率 $W_{Y^nZ^n|X^n}$ に対して，盗聴通信路容量（Secrecy Capacity）を次のように定義する．通信路入力アルファベットを $\mathcal{X}$，正規の受信者への出力アルファベットを $\mathcal{Y}$，正規の受信者への出力アルファベットを $\mathcal{Z}$ とする*.

**定義**．メッセージの集合を $\mathcal{M}$ とする．以下の性質を満たす，符号器と復号器の組 $(\Phi_{X^n|M}, \psi_n)$ を，ブロック長 $n$，信頼性基準 $\varepsilon > 0$，安全性基準 $R_{\mathrm{S}} > 0$，レート $R_{\mathrm{M}} > 0$ の盗聴通信路符号と呼ぶ．

$$\frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}}\sum_{x^n\in\mathcal{X}^n} W_{Y^n|X^n}\left(\{y^n \in \mathcal{Y}^n : \psi(y^n) \neq m\}\,|x^n)\right)\Phi_{X^n|M}(x^n|m) \leq \varepsilon \tag{13･21}$$

$$\frac{H(M|Z^n)}{n} \geq R_{\mathrm{S}} - \varepsilon \tag{13･22}$$

$$R_{\mathrm{M}} = \frac{\log|\mathcal{M}|}{n} \tag{13･23}$$

ここで，

$$W_{Y^n|X^n}(y^n|x^n) \equiv \sum_{z^n\in\mathcal{Z}^n} W_{Y^nZ^n|X^n}(y^n, z^n|x^n), \quad x^n \in \mathcal{X}^n, y^n \in \mathcal{Y}^n$$

とした．

任意の $\varepsilon > 0$ に対して十分大きな $n$ をとることによりブロック長 $n$，信頼性基準 $\varepsilon$，安全性基準 $R_{\mathrm{S}}$，レート $R_{\mathrm{M}}$ の盗聴通信路符号を構成できるとき，$R_{\mathrm{M}}$ を安全性基準 $R_{\mathrm{S}}$ の盗聴通信路符号の達成可能レートと呼ぶ．

特に $R_{\mathrm{S}} = R_{\mathrm{M}}$ を満たしている場合，レート $R_{\mathrm{M}}$ を完全秘匿な盗聴通信路符号の達成可能

* エントロピー，相互情報量の定義については文献 [3)]を参照．

レートと呼ぶ．そして，完全秘匿な盗聴通信路符号の達成可能レートの上限 $C(W_{YZ|X})$ を盗聴通信路容量と呼ぶ．すなわち，

$$C(W_{YZ|X}) \equiv \sup\left\{ R_{\mathrm{M}} : \begin{array}{l} \text{信頼性基準 } \varepsilon,\ \text{安全性基準 } R_{\mathrm{M}},\ \text{レート } R_{\mathrm{M}} \text{ の} \\ \text{盗聴通信路符号が存在} \end{array} \right\}$$

上記の式 (13･21) は受信者の平均復号誤り確率が $\varepsilon$ 以下であることを，式 (13･22) は盗聴者にとってのメッセージに関する曖昧さ (エントロピー) が $R_{\mathrm{S}} - \varepsilon$ 以上であることを意味しており，完全秘匿 ($R_{\mathrm{S}} = R_{\mathrm{M}}$) の場合は

$$\frac{I(M; Z^n)}{n} \leq \varepsilon \tag{13･24}$$

と同値である．式 (13･24) は盗聴者へ伝わるメッセージに関する情報量が $\varepsilon$ 以下であることを意味している．なお，$R_{\mathrm{S}} = R_{\mathrm{M}}$ のとき，更に (13･24) よりも強い条件

$$I(M; Z^n) \leq \varepsilon$$

が成立する符号は強完全秘匿な盗聴通信路符号と呼ばれる．

### 13-7-3 盗聴通信路の符号化定理

盗聴通信路容量の情報理論的表現に関して，以下の結果が知られている．

**定理**．有限集合を入出力アルファベットとする定常無記憶な盗聴通信路 $W_{YZ|X}$ に対して

$$C(W_{YZ|X}) = \max_{X,V: V \leftrightarrow X \leftrightarrow YZ} [I(V; Y) - I(V; Z)] \tag{13･25}$$

が成り立つ．ここで $V \leftrightarrow X \leftrightarrow YZ$ は確率変数が (この順で) マルコフ連鎖をなしていることを意味する．

特に，通信路入力 $X$ の分布を任意に与えたときの通信路出力 $Y, Z$ に関して

$$I(X; Y) \geq I(X; Z) \tag{13･26}$$

を満たしているときは

$$C(W_{YZ|X}) = \max_{X} [I(X; Y) - I(X; Z)] \tag{13･27}$$

が成り立つ．

通信路入力 $X$ の分布を任意に与えたときの通信路出力 $Y, Z$ に関して式 (13･26) を満たす場合は，$X$ と $Y$ の通信路は $X$ と $Z$ よりも容量が大きい（More Capable）と呼ばれている（文献[2)]参照）．退化通信路はこの条件を満たしており，Wyner [1)]は退化通信路の場合に式 (13･27) を導出した．$X$ と $Y$ の通信路は $X$ と $Z$ よりも容量が大きい場合の式 (13･27) と，一般のブロードキャスト通信路に対する式 (13･25) は，Csiszár-Körner [2)]によって導出された．Csiszár [4)]は強完全秘匿の場合についても同じ通信路容量を達成することを示した．

**■参考文献**

1) A.D. Wyner：“The wire-tap channel,” Bell Syst. Tech. J., vol.54, no.8, pp.1355–1387, 1975.
2) I. Csiszár and J. Körner：“Broadcast channels with confidential messages,” IEEE Trans. Inform. Theory, vol.IT-24, pp.339–348, May 1978.
3) T.M. Cover and J.A. Thomas：“Elements of Information Theory 2nd. Ed.,” John Wiley & Sons, Inc., 2006.
4) I. Csiszár：“Almost independence and secrecy capacity,” Problems of Information Transmission, vol.32, no.1, pp.40–47, 1996.