NTT

情報理論の未解決問題

村松純

NTT **コミュニケーション科学基礎研究所**

2022.7.21

おしながき

- なぜ「未解決問題」なのか?
- 準備
- 私が過去に取り組み解決できなかった「未解決問題」

私がお話できそうなもの

- Bounded-Observability (**情報理論的安全性**) [M et al.,ProcIEEE2015]
- CoCoNuTS
  - 10**分で説明する** CoCoNuTS[M-Miyake, **電子情報通信学会解説記事** 2021]
  - CoCoNuTS **へのアイデアの変遷** [M,AEW10]
  - CoCoNuTS **の証明テクニック**
- **ポーラ符号** [M,ITW2019][M,ISIT2021][M,ISIT2022]
- **多端子情報理論** [M,ITW2013][M-Miayke,ISITA2018][M,arXiv2022a][M,arXiv2022b]
- **私が感動した定理**

[補足] 講演時お見せしたスライドの一部を省略しました. 上記の具体的な内容については, また機会があるときにお話させていただければと思います.

おしながき

- なぜ「未解決問題」なのか?
- 準備
- 私が過去に取り組み解決できなかった「未解決問題」

通信路符号

- 符号化では, 送りたいメッセージ $M^{(n)}$ から信号 X^n へ変換して送る.
- 通信路では, 信号が雑音の影響を受けて変化する $(X^n \to Y^n)$.
- 復号化では, 雑音を受けた信号 Y^n から元のメッセージ $M^{(n)}$ を再生する.

通信路符号の Shannon 限界(通信路容量)

[符号の定義]

- 符号化を行う関数 $\Phi^{(n)} : \mathcal{M}^{(n)} \to \mathcal{X}^n$
- 復号化を行う関数 $\Psi^{(n)} : \mathcal{Y}^n \to \mathcal{M}^{(n)}$

[符号化レートの定義] $R \equiv \frac{\log_2 |\mathcal{M}^{(n)}|}{n}$

[通信路容量の定義]

- 以下の条件を満たす C を通信路容量(通信路符号の Shannon 限界)と呼ぶ.
  - ブロック長 n を十分大きくとれば, 復号誤り確率が 0 に近く, かつ伝送速度が C に近い符号が存在する.
  - 十分大きくブロック長 n において, 復号誤り確率が 0 に近く, かつ伝送速度が C より大きい符号は存在しない.

$$C \equiv \sup_{\substack{\{(\Phi^{(n)},\Psi^{(n)})\}_{n=1}^{\infty}: \\ \lim_{n\to\infty} \mathrm{Prob}(M^{(n)} \neq \Psi^{(n)}(Y^n)) = 0}} \frac{\log_2 |\mathcal{M}^{(n)}|}{n}$$

FAQ: Shannon 限界を越えることはできるんですか？

- いいえ．Shannon 限界は「あらゆる実装を考えたときの性能限界」と定義されており，それを越えることは定義と矛盾するため不可能です．
- ただし，Shannon 限界は通信路に応じて異なるため，(例えばアンテナの改良等で通信路の性質が向上することにより) Shannon 限界自体を大きくすることは可能です．
- (教科書に記載されている)数式として与えられた Shannon 限界は，特定の通信路に対して限界を求めた結果(定理/公式)であり，仮にある実装が式の値を越えたとしても，理論とは異なる通信路であることを示唆しているに過ぎません．

定理(順定理)[Shannon,1948]

- 伝送速度 R が

$$R > \max_{P_X} I(X;Y)$$

を満足すれば, 誤り確率が 0 に収束する符号 が存在する.

定理(逆定理)[Shannon,1948]

- 伝送速度 R が上記の条件を満足しなければ,
誤り確率が 0 に収束する符号 は存在しない.

通信路容量 $C = \max_{P_X} I(X;Y)$

1字容量式

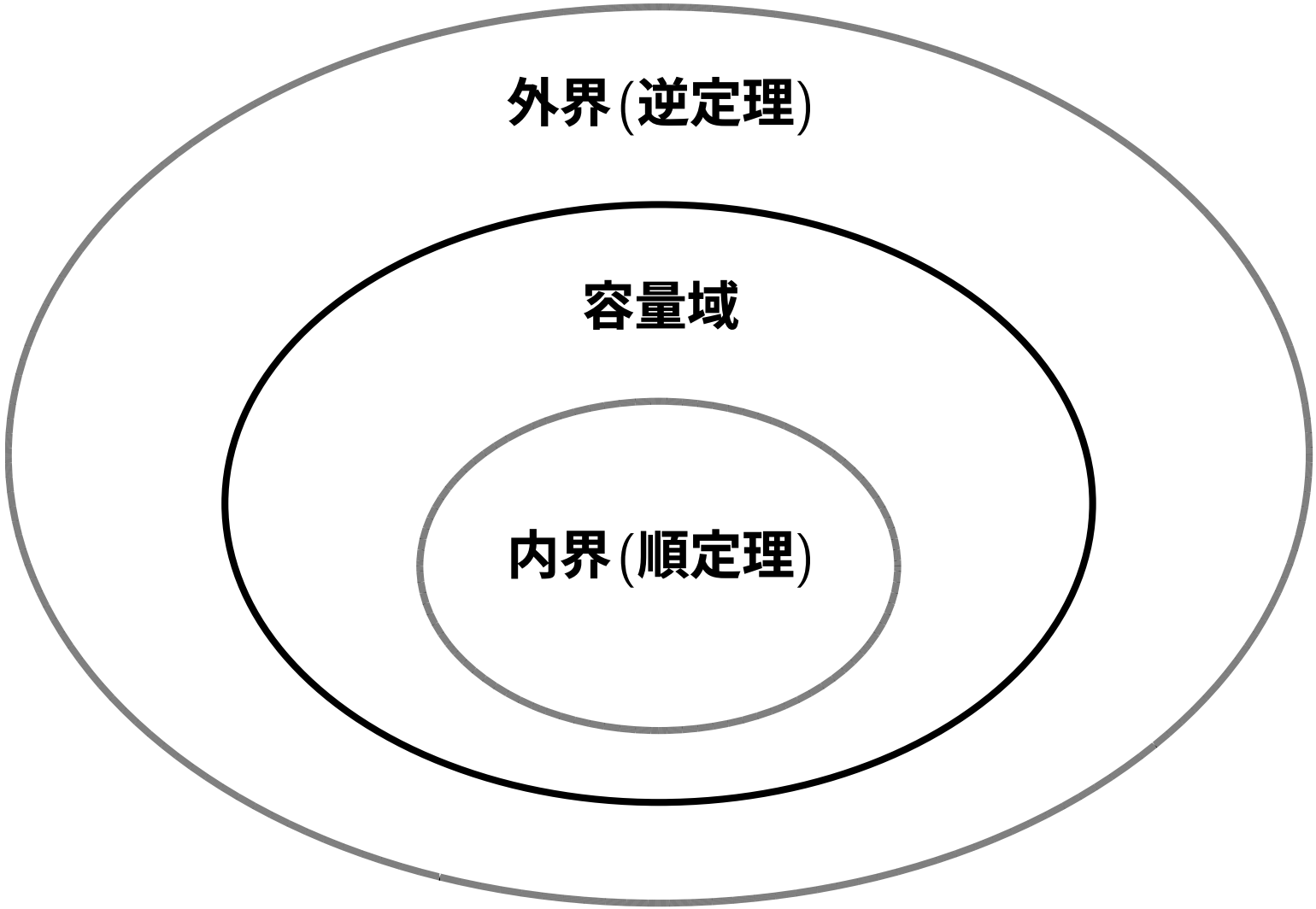
$$\sup_{\{(\Phi^{(n)},\Psi^{(n)})\}_{n=1}^{\infty}:\ \lim_{n\to\infty}\mathrm{Prob}(M^{(n)}\neq\Psi^{(n)}(Y^n))=0}\frac{\log_2|\mathcal{M}^{(n)}|}{n}=\max_{P_X} I(X;Y)$$

- **左辺はnに関する極限を含む最適化(計算困難).**
- **右辺は有限次元($(|\mathcal{X}|-1)$次元)の最適化(計算可能).**
- **要するに, 通信路符号化定理は, 通信路の定常無記憶性を仮定して**, Shannon **限界(通信路容量)の有限次元の最適化問題へ還元する(計算可能な)公式を与えている. (補足: 同時に情報量との関係も表現している)**

多字容量式

- **通信路/情報源の定常無記憶性を仮定せず右辺に$n\to\infty$の極限を許した容量公式を導出するテクニックとして, 情報スペクトル理論がある** [Verdú-Han,1994][M,IEEE-IT2014].

内界と外界



$$\{R : 0 \leq R \leq 0\} \subset \{R : 0 \leq R \leq \max_X I(X;Y)\} \subset \{R : 0 \leq R \leq \log_2 |\mathcal{X}|\}$$

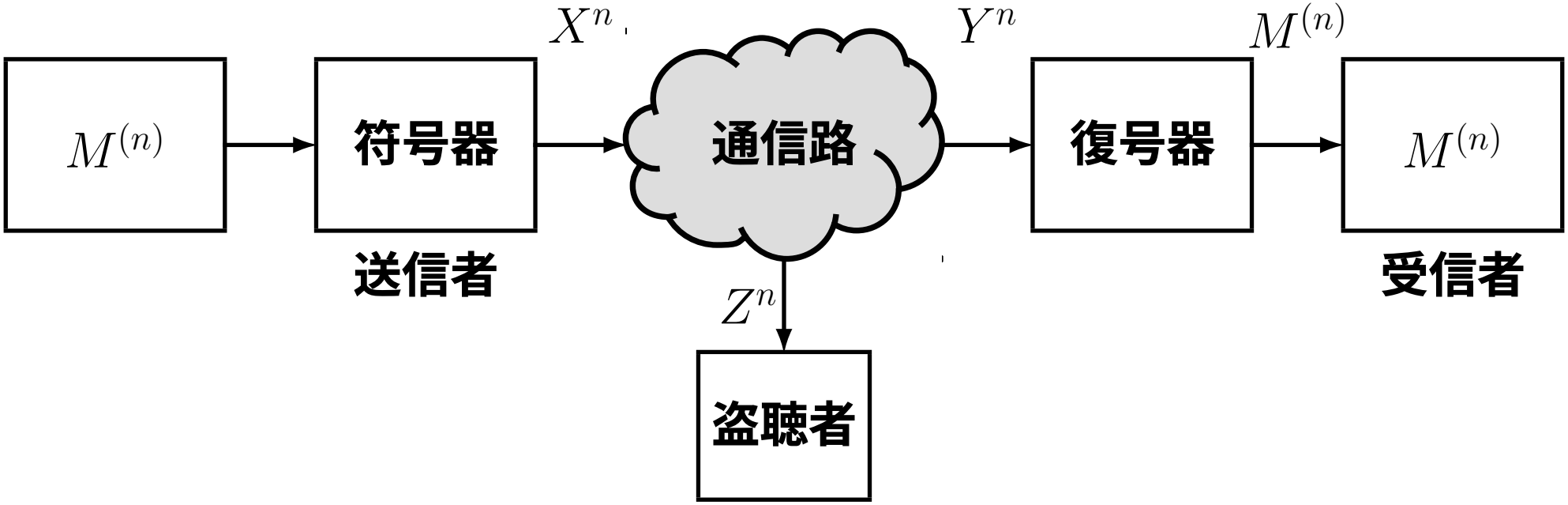
おしながき

- なぜ「未解決問題」なのか?
- 準備
- 私が過去に取り組み解決できなかった「未解決問題」

私が過去に取り組み解決できなかった「未解決問題」

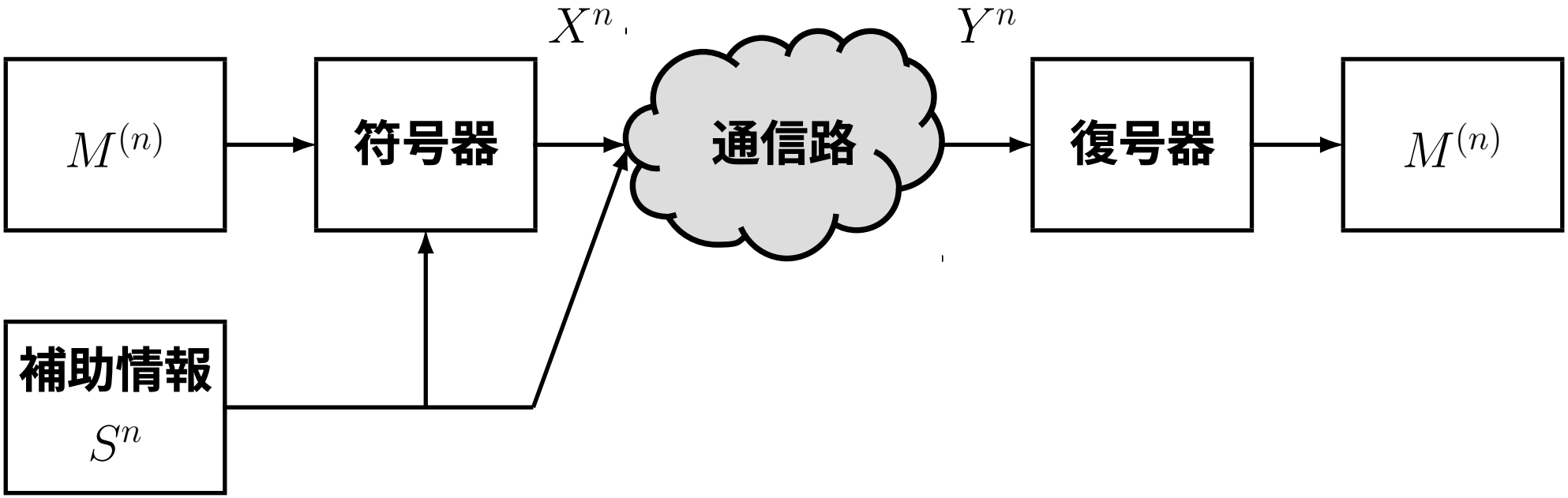
- **補助情報のある盗聴通信路**
  - **多字秘密容量式を導出** [M,ISIT2014].
- **ブロードキャスト通信路**
  - Marton **内界**, Gel'fand-Pinsker **内界**, Liang-Kramer **内界と等価な** 1 **字内界を導出** [M,ITW2013].
  - **多字容量域を導出** [M-Miyake,ISITA2018].
- **干渉通信路**
  - Han-Kobayashi **内界**, Jian-Xin-Gerg **内界と等価な** 1 **字内界を導出** [M,arXiv2022a].
  - **多字容量域を導出** [M,arXiv2022b].
- **分散有歪情報源符号**
- **秘密鍵共有**
  - **多字秘密鍵容量を導出** [M et al.,IEICE-A2006][M-Miyake,Springer2018].

盗聴通信路[Wyner,1975]



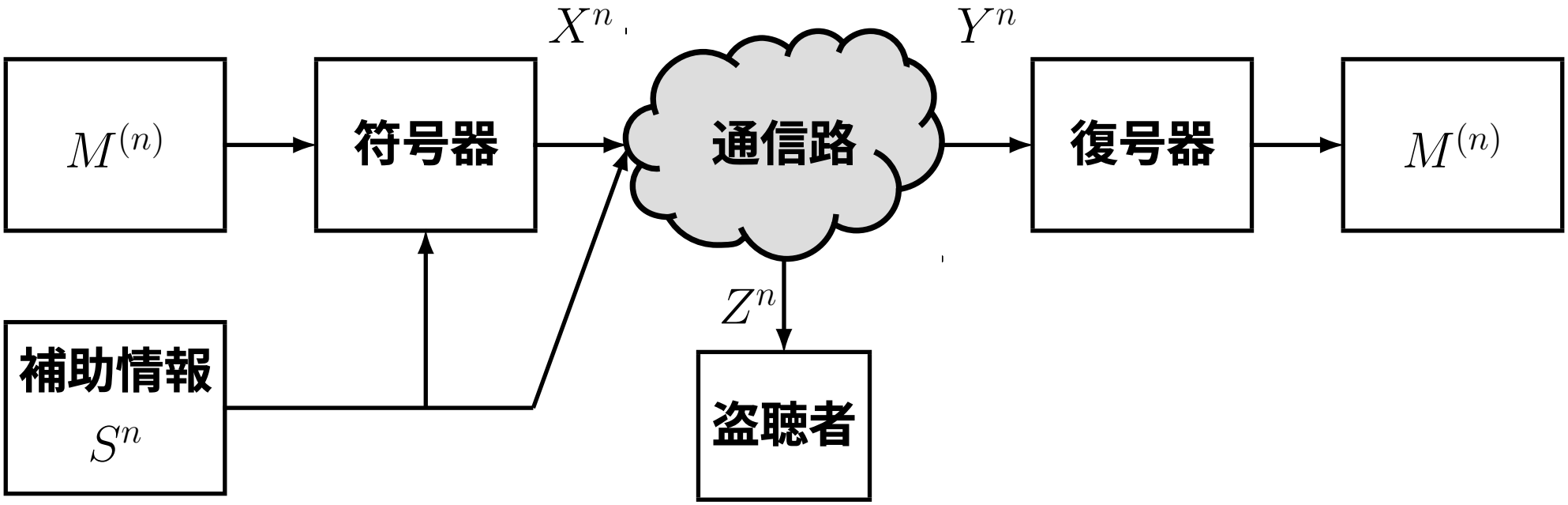
- 符号化では, 送りたいメッセージ $M^{(n)}$ から信号 X^n へ変換して送る.
- 通信路では, 盗聴者が信号 Z^n を傍受する.
- 復号化では, 雑音を受けた信号 Y^n から元のメッセージ $M^{(n)}$ を再生する. このとき, 盗聴者に情報を漏らさないようにする.

補助情報のある通信路符号 [Gel'fand-Pinsker,1980]



- 符号化では, 送りたいメッセージ $M^{(n)}$ から信号 X^n へ変換して送る.
- 通信路では, 信号が雑音の影響を受けて変化する $(X^n \to Y^n)$.
- 復号化では, 雑音を受けた信号 Y^n から元のメッセージ $M^{(n)}$ を再生する.

補助情報を伴う盗聴通信路[Chen-Vinck,2008]



- 符号化では, 送りたいメッセージ $M^{(n)}$ から信号 X^n へ変換して送る.
- 通信路では, 盗聴者が信号 Z^n を傍受する.
- 復号化では, 雑音を受けた信号から元のメッセージ $M^{(n)}$ を再生する. このとき, 盗聴者に情報を漏らさないようにする.

補助情報を伴う盗聴通信路の秘密容量(Shannon 限界)

[符号の定義]

- 符号化を行う関数 $\Phi^{(n)} : \mathcal{M}^{(n)} \times \mathcal{S}^n \to \mathcal{X}^n$
- 復号化を行う関数 $\Psi^{(n)} : \mathcal{Y}^n \to \mathcal{M}^{(n)}$

[符号化レートの定義] $R \equiv \frac{\log_2 |\mathcal{M}^{(n)}|}{n}$

[(強)情報理論的安全性の定義] $\lim_{n\to\infty} I(M^{(n)}; Z^n) = 0$

[秘密容量の定義]

- 以下の条件を満たす C_{WS} を秘密容量(Shannon 限界)と呼ぶ.
  - ブロック長 n を十分大きくとれば, 復号誤り確率が 0 に近く, かつ符号化レートが C_{WS} に近い情報理論的安全性を持つ符号が存在する.
  - 十分大きくブロック長 n において, 復号誤り確率が 0 に近く, かつ符号化レートが C_{WS} より大きい情報理論的安全性を持つ符号は存在しない.

秘密容量の内界と外界[Chen-Vinck, 2008][Liang et al, 2009]

$$C_{WS} \geq \max_{\mu_{\widehat{X}X|S}} \left[I(\widehat{X};Y) - \max\left\{ I(\widehat{X};S), I(\widehat{X};Z) \right\} \right]$$

$$C_{WS} \leq \min \left\{ \max_{\mu_{\widehat{X}X|S}} \left[I(\widehat{X};Y) - I(\widehat{X};S) \right], \max_{\mu_{\widehat{X}X|S}} \left[I(\widehat{X};Y) - I(\widehat{X};Z) \right] \right\}$$

$$= \min\left\{ C_{GP}, C_W \right\},$$

ここで $\mu_{\widehat{X}SXYZ}(\widehat{x},s,x,y,z) = \mu_{YZ|XS}(y,z|x,s)\mu_{\widehat{X}X|S}(\widehat{x},x|s)\mu_S(s)$.

- $S \equiv$ **定数 とすると**, $C_{WS} = C_W$.
- $Z \equiv$ **定数 とすると**, $C_{WS} = C_{GP}$.

秘密容量の内界と外界[Chen-Vinck, 2008][Liang et al, 2009]

$$C_{WS} \geq \max_{\mu_{\widehat{X}X|S}} \left[I(\widehat{X};Y) - \max\left\{ I(\widehat{X};S), I(\widehat{X};Z) \right\} \right]$$

$$C_{WS} \leq \min \left\{ \max_{\mu_{\widehat{X}X|S}} \left[I(\widehat{X};Y) - I(\widehat{X};S) \right], \max_{\mu_{\widehat{X}X|S}} \left[I(\widehat{X};Y) - I(\widehat{X};Z) \right] \right\}$$

$$= \min\left\{ C_{GP}, C_W \right\},$$

ここで $\mu_{\widehat{X}SXYZ}(\widehat{x},s,x,y,z) = \mu_{YZ|XS}(y,z|x,s)\mu_{\widehat{X}X|S}(\widehat{x},x|s)\mu_S(s)$.

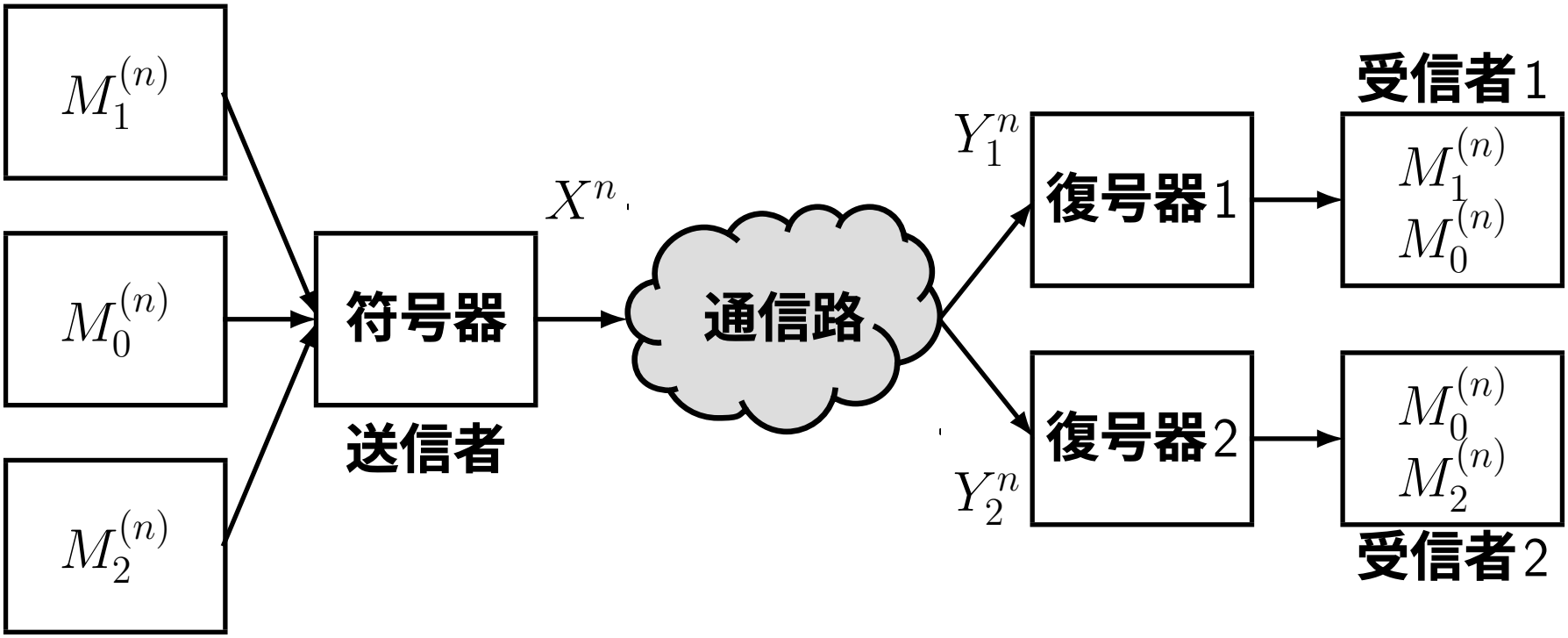
多字秘密容量[M,ISIT2014]

$$C_{WS} = \sup_{\boldsymbol{V}} \left[\min\left\{ \underline{H}(\widehat{\boldsymbol{X}}|\boldsymbol{S}), \underline{H}(\widehat{\boldsymbol{X}}|\boldsymbol{Z}) \right\} - \overline{H}(\widehat{\boldsymbol{X}}|\boldsymbol{Y}) \right],$$

ここで $\sup_{\boldsymbol{V}}$ **はすべての一般通信路** $\{\mu_{\widehat{X}^nX^n|S^n}\}_{n=1}^{\infty}$ **にわたり**,
$(\widehat{X}^n, S^n, X^n, Y^n, Z^n)$ **の同時分布は**

$$\mu_{\widehat{X}^nS^nX^nY^nZ^n}(\widehat{\boldsymbol{x}},\boldsymbol{s},\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}) \equiv \mu_{Y^nZ^n|X^n}(\boldsymbol{y},\boldsymbol{z}|\boldsymbol{x})\mu_{\widehat{X}^nX^n|S^n}(\widehat{\boldsymbol{x}},\boldsymbol{x}|\boldsymbol{s})\mu_{S^n}(\boldsymbol{s}).$$

ブロードキャスト通信路[Cover,1972]



1字容量域の導出は50年間未解決

ブロードキャスト通信路符号の容量域

[符号の定義]

- 符号化を行う関数 $\Phi^{(n)} : \mathcal{M}_0^{(n)} \times \mathcal{M}_1^{(n)} \times \mathcal{M}_2^{(n)} \to \mathcal{X}^n$
- 復号化を行う関数 $\Psi_i^{(n)} : \mathcal{Y}^n \to \mathcal{M}_0^{(n)} \times \mathcal{M}_i^{(n)}, i \in \{1, 2\}$

[符号化レートの定義]

- $R_i \equiv \frac{\log_2 |\mathcal{M}_i^{(n)}|}{n}, i \in \{0, 1, 2\}$

[容量域の定義]

- 以下の条件を満たす (R_0, R_1, R_2) の集合 $\mathcal{R}$ を，ブロードキャスト通信路の容量域，その境界線をShannon 限界と呼ぶ.
  - $(R_0, R_1, R_2) \in \mathcal{R}$ のとき，ブロック長 n を十分大きくとれば，復号誤り確率が 0 に近く，かつ符号化レートが (R_0, R_1, R_2) に近い符号が存在する.
  - $(R_0, R_1, R_2) \notin \mathcal{R}$ のとき，十分大きくブロック長 n において，復号誤り確率が 0 に近く，かつ符号化レートが (R_0, R_1, R_2) に近い符号は存在しない.

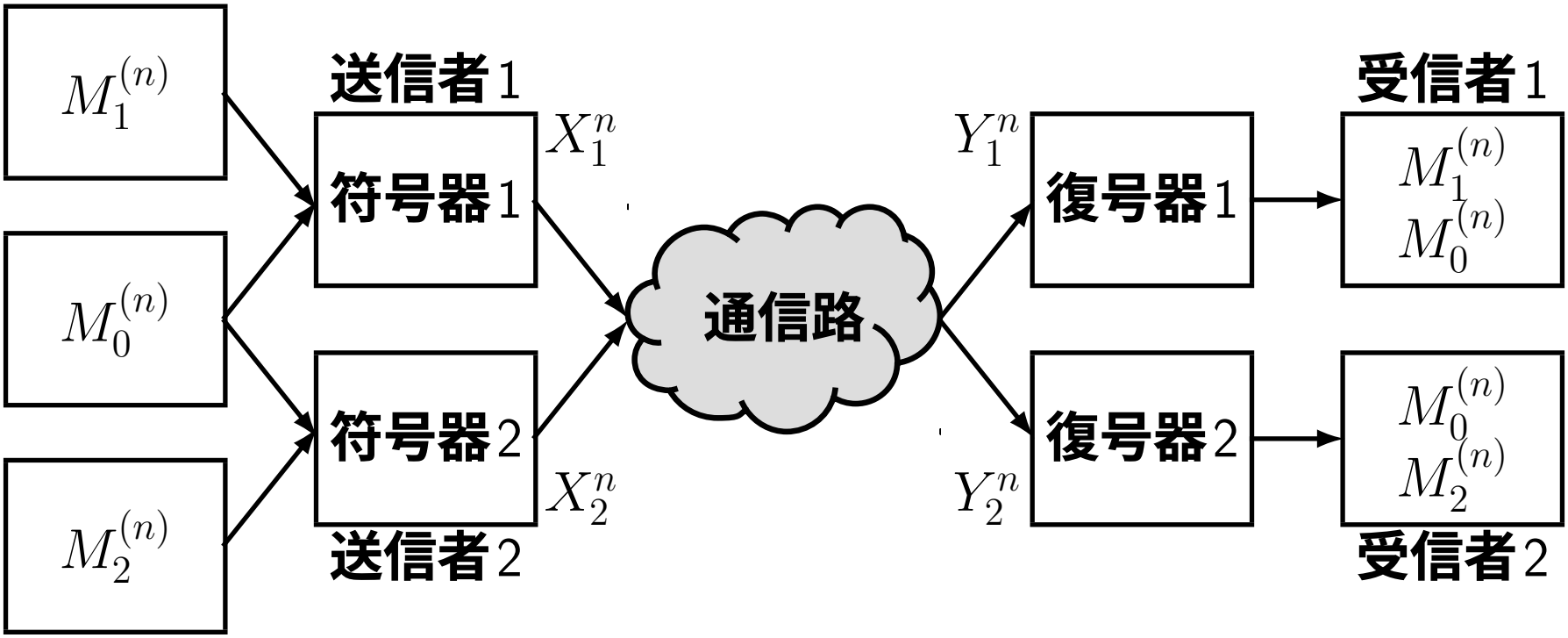
ブロードキャスト通信路の1字内界

- **共通情報** $M_0^{(n)}$ **がない場合**$(R_0 = 0)$
  - Marton **内界**[Marton,1979]
- **共通情報** $M_0^{(n)}$ **がある場合**
  - Marton **内界**?[Csiszár-Körner,1981]
  - Liang-Kramer **内界**[Liang et al.,2011]
  - CoCoNuTS**内界**[M-Miyake,ISITA2018][M,ITW2013]

一般ブロードキャスト通信路の多字容量域

- CoCoNuTS**容量域**[M-Miyake,ISITA2018]
- Somekh-Baruch & Verdú **容量域**[Somekh-Baruch & Verdú,2006]

干渉通信路[Ahlswede,1974][Jiang et al,2008]



1字容量域の導出は50年近く未解決

干渉通信路の容量域

[符号の定義]

- 符号化を行う関数 $\Phi_i^{(n)} : \mathcal{M}_0^{(n)} \times \mathcal{M}_i^{(n)} \to \mathcal{X}_i^n,\ i \in \{1,2\}$
- 復号化を行う関数 $\Psi_j^{(n)} : \mathcal{Y}_j^n \to \mathcal{M}_0^{(n)} \times \mathcal{M}_j^{(n)},\ j \in \{1,2\}$

[符号化レートの定義]

- $R_i \equiv \frac{\log_2 |\mathcal{M}_i^{(n)}|}{n},\ i \in \{0,1,2\}$

[容量域の定義]

- 以下の条件を満たす (R_0, R_1, R_2) の集合 $\mathcal{R}$ を，干渉通信路の容量域，その境界線をShannon 限界と呼ぶ．
  - $(R_0, R_1, R_2) \in \mathcal{R}$ のとき，ブロック長 n を十分大きくとれば，復号誤り確率が 0 に近く，かつ符号化レートが (R_0, R_1, R_2) に近い符号が存在する．
  - $(R_0, R_1, R_2) \notin \mathcal{R}$ のとき，十分大きくブロック長 n において，復号誤り確率が 0 に近く，かつ符号化レートが (R_0, R_1, R_2) に近い符号は存在しない．

干渉通信路符号の1字内界

- **共通情報 $M_0^{(n)}$ がない場合**$(R_0 = 0)$
  - Han-Kobayashi **内界**[Han-Kobayashi,1981].
  - Chong-Motani-Garg **内界**[Chong et al.,2008].
  - CoCoNuTS**内界**[M,arXiv2022a].
  - **容量域は真に大きい**[Nair et al,2015].
- **共通情報 $M_0^{(n)}$ がある場合**
  - Jiang-Xia-Garg **内界**[Jiang et al.,2008].
  - CoCoNuTS**内界**[M,arXiv2022a].

一般干渉通信路の多字容量域

- Somekh-Baruch & Verdú **容量域**[Somekh-Baruch & Verdú,2006].
- CoCoNuTS**容量域**[M-Miyake,ISITA2018][M,arXiv2022b].

有歪情報源符号

- 符号化では, 送信(記録)したいメッセージ(情報)から信号(この例ではディスクの凹凸)へ変換して送る.
- 通信路では, 信号が雑音の影響を受けない理想的な状況を考える.
- 復号化では, 信号から元のメッセージ(情報)を
  一定の品質を保証したうえで再生する.

有歪情報源符号の限界域

[符号の定義]

- 符号化を行う関数 $\Phi^{(n)} : \mathcal{X}^n \to \mathcal{C}^{(n)}$
- 復号化を行う関数 $\Psi^{(n)} : \mathcal{C}^{(n)} \to \mathcal{Y}^n$

[符号化レートの定義] $R \equiv \frac{\log_2 |\mathcal{C}^{(n)}|}{n}$

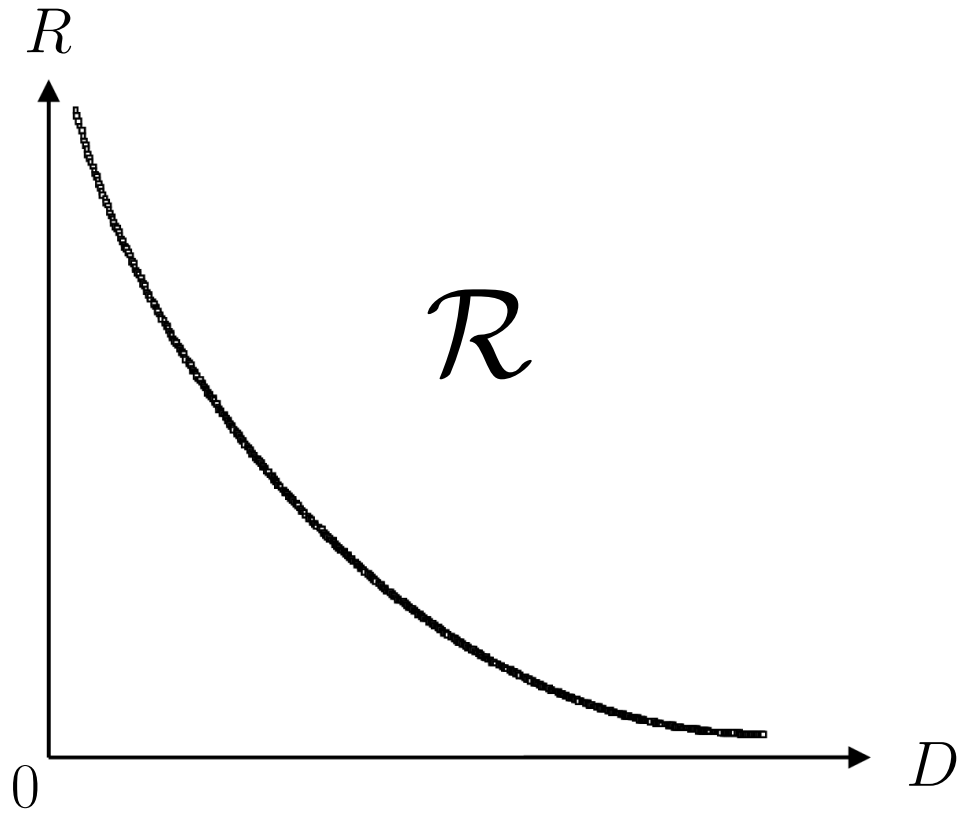
[誤り確率の定義] $\mathrm{Error}(\Phi^n, \Psi^{(n)}) \equiv \mathrm{Prob}\left(d^{(n)}(X^n, \Psi^{(n)}(\Phi^{(n)}(X^n))) > D\right)$

[限界域の定義]

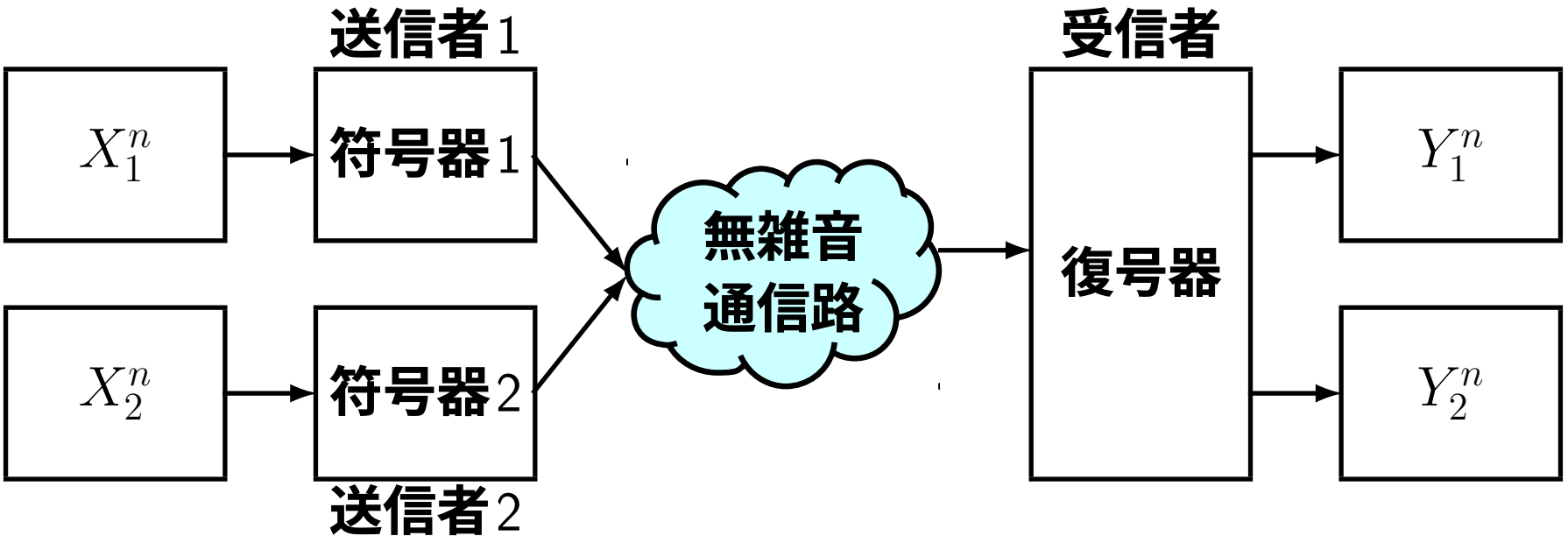
- 以下の条件を満たす (R, D) の集合 $\mathcal{R}$ を有歪情報源符号の限界域と呼ぶ. その境界はレート歪関数(歪レート関数)となる.
  - $(R, D) \in \mathcal{R}$ のとき, ブロック長 n を十分大きくとれば, 復号誤り確率が 0 に近く, かつ符号化レートが R に近い符号が存在する.
  - $(R, D) \notin \mathcal{R}$ のとき, 十分大きくブロック長 n において, 復号誤り確率が 0 に近く, かつ符号化レートが R より小さい符号は存在しない.

有歪符号化の1字限界域

$$\mathcal{R} = \bigcup_{P_{Y|X}} \left\{ (R, D) : \begin{array}{l} I(X;Y) \leq R \\ E[d(X,Y)] \leq D \end{array} \right\}$$



分散有歪情報源符号 [Berger,1978][Tung,1978]



- 符号化では，送信(記録)したいメッセージ(情報)から信号へ変換して送る．
- 通信路では，信号が雑音の影響を受けない理想的な状況を考える．
- 復号化では，2つの信号から元のメッセージ(情報)を一定の品質を保証したうえで再生する．

分散有歪情報源符号の限界域

[符号の定義]

- 符号化を行う関数 $\Phi_i^{(n)} : \mathcal{X}_i^n \to \mathcal{C}_i^{(n)},\ i \in \{1,2\}$
- 復号化を行う関数 $\Psi^{(n)} : \mathcal{C}_1^{(n)} \times \mathcal{C}_2^{(n)} \to \mathcal{Y}_1^n \times \mathcal{Y}_2^n$

[符号化レートの定義] $R_i \equiv \frac{\log_2 |\mathcal{C}^{(n)}|}{n},\ i \in \{1,2\}$

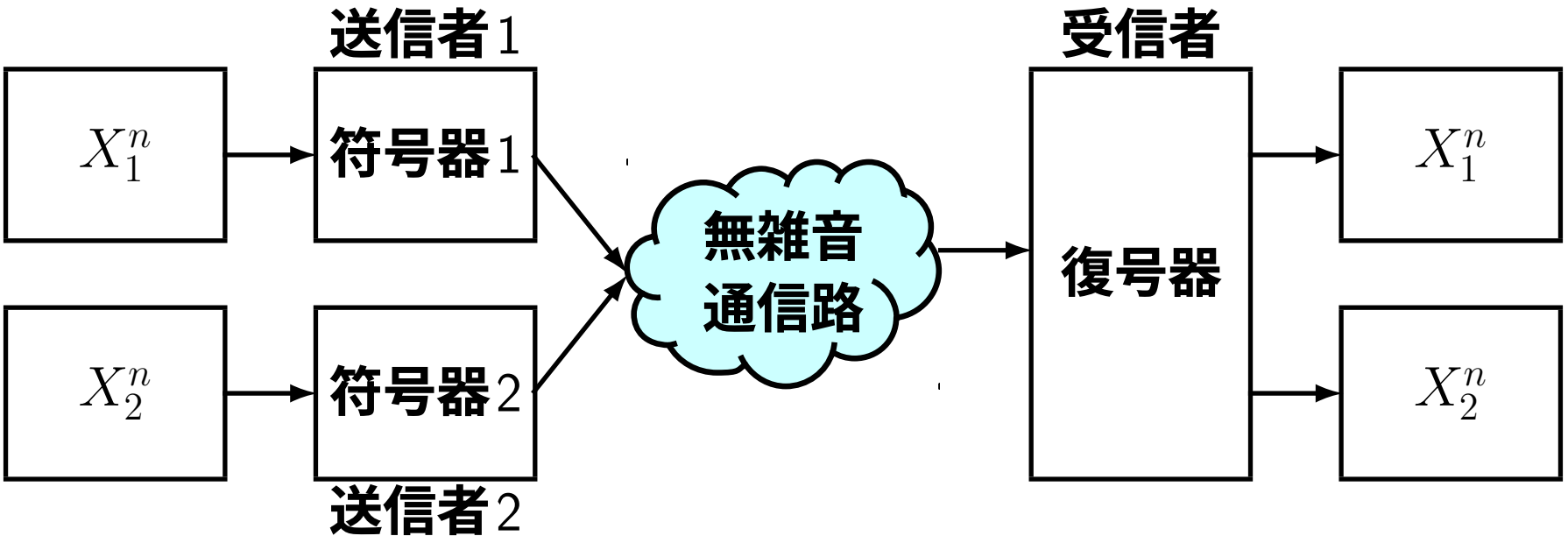
[誤り確率の定義]

$$\mathrm{Error}(\Phi_1^{(n)}, \Phi_2^{(n)}, \Psi^{(n)}) \equiv \mathrm{Prob}\left(\begin{array}{l} d_i^{(n)}(X_i^n, \Psi_i^{(n)}(\Phi_1^{(n)}(X_1^n), \Phi_2^{(n)}(X_2^n))) > D_i \\ \text{を満たす } i \in \{1,2\} \text{ が存在} \end{array} \right)$$

[限界域の定義]

- 以下の条件を満たす (R_1, D_1, R_2, D_2) の集合 $\mathcal{R}$ を有歪情報源符号の限界域と呼ぶ．その境界はレート歪関数(歪レート関数)となる．
  - $(R_1, D_1, R_2, D_2) \in \mathcal{R}$ のとき，ブロック長 n を十分大きくとれば，復号誤り確率が 0 に近く，かつ符号化レートが (R_1, R_2) に近い符号が存在する．
  - $(R_1, D_1, R_2, D_2) \notin \mathcal{R}$ のとき，十分大きくブロック長 n において，復号誤り確率が 0 に近く，かつ符号化レートが (R_1, R_2) になる符号は存在しない．

分散無歪情報源符号[Slepian-Wolf,1973]($D_1 = D_2 = 0$)



限界域[Slepian-Wolf,1973]

$$\mathcal{R} = \left\{ (R_1, R_2) : \begin{array}{r} R_1 \geq H(X_1|X_2) \\ R_2 \geq H(X_2|X_1) \\ R_1 + R_2 \geq H(X_1, X_2) \end{array} \right\}$$

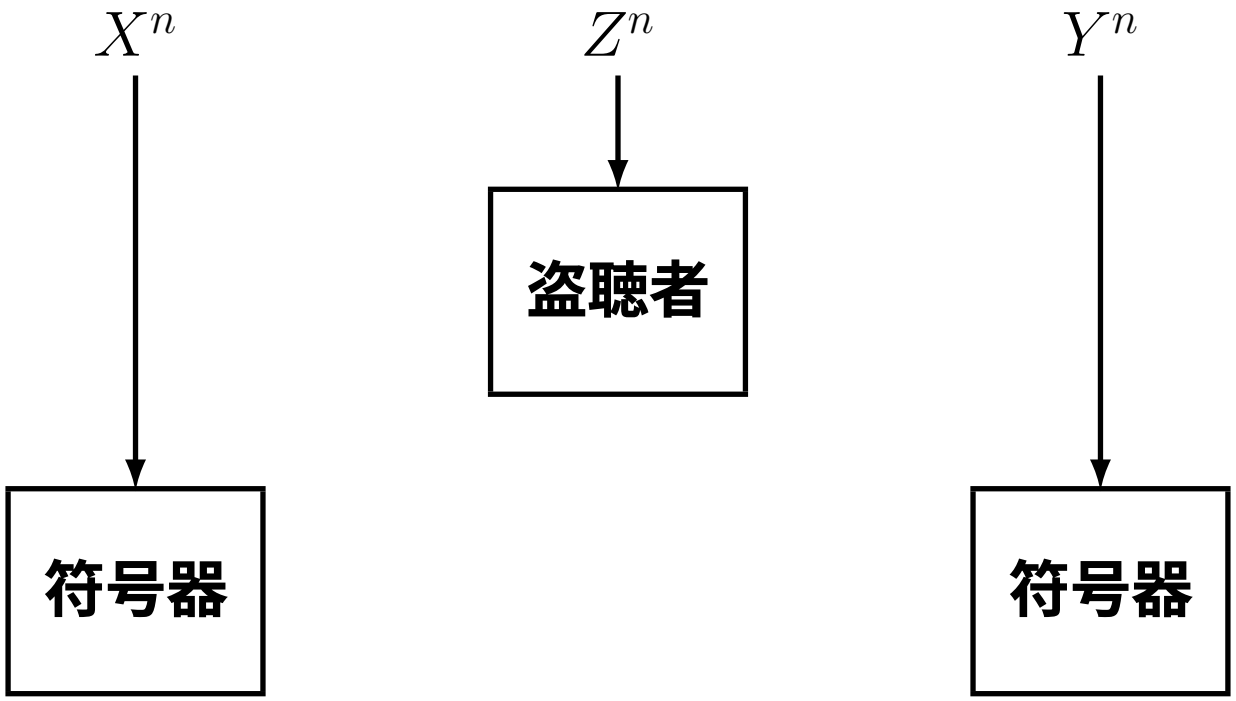
限界域の1字内界と1字外界

- Burger-Tang **内界・外界** [Berger,1978][Tang,1978].
- (X_1, X_2) **に共通情報がある場合**, Burger-Tang **内界よりも真に大きな内界が存在する** [Wagner et al.,2011].
- **予稿集で紹介すべきだった論文**
  - **内界**
    - F. Shirani and S. S. Pradhan,
      IEEE Trans. Inform. Thoery, vol. 67, no. 7 pp. 4485–4503, Jul. 2021.
  - **外界**
    - A. B. Wagner and V. Anantharam,
      IEEE Trans. Inform. Theory, vol. 54, no. 5, pp. 1919–1937, May 2008.
    - W. Kang and S. Ulkus,
      IEEE Trans. Inform. Theory, vol. 57, no. 1, pp. 56–69, Jan. 2011.

多字限界域

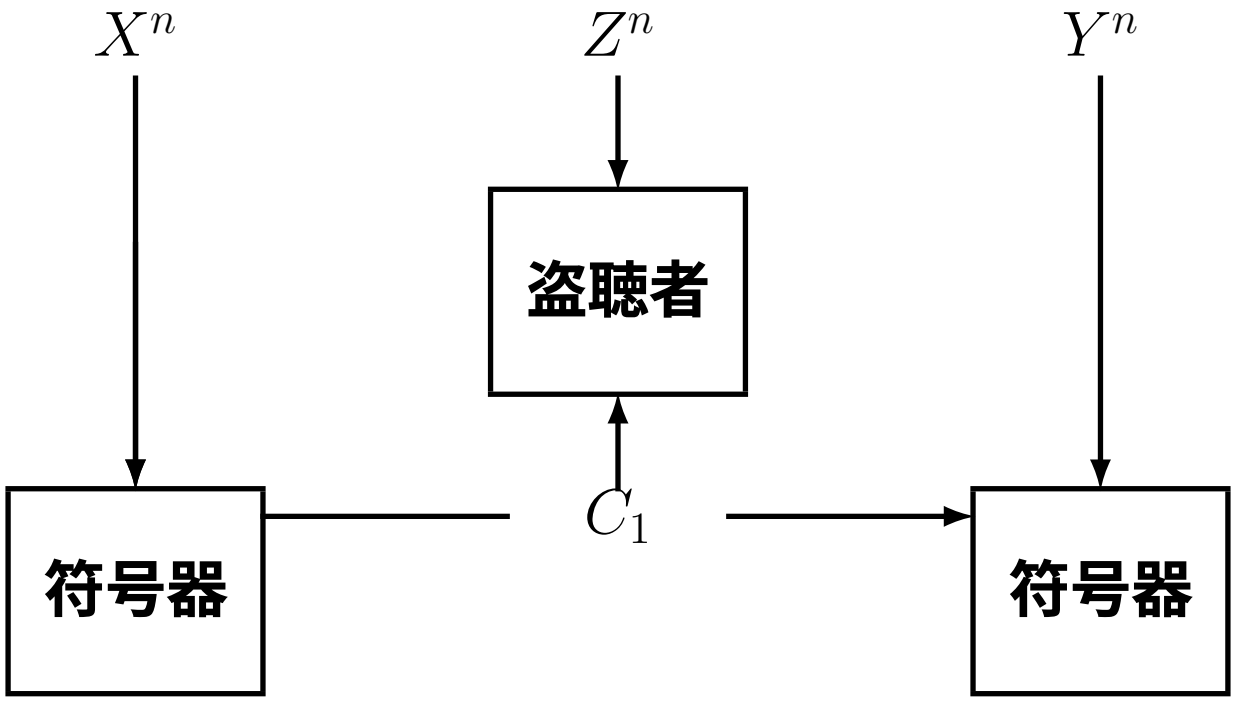
- Yang-Qiu **限界域**[Yang-Qiu,2006]
  - **(補足) この論文は**2006**年に**IEEE-IT**に投稿されたようであるが, その後掲載された形跡がない. また論文の正しさも確認していないので, 引用の際には注意すること.**

相関乱数を用いた秘密鍵共有 [Maurer,1993][Ahlswede-Csiszár,1993]



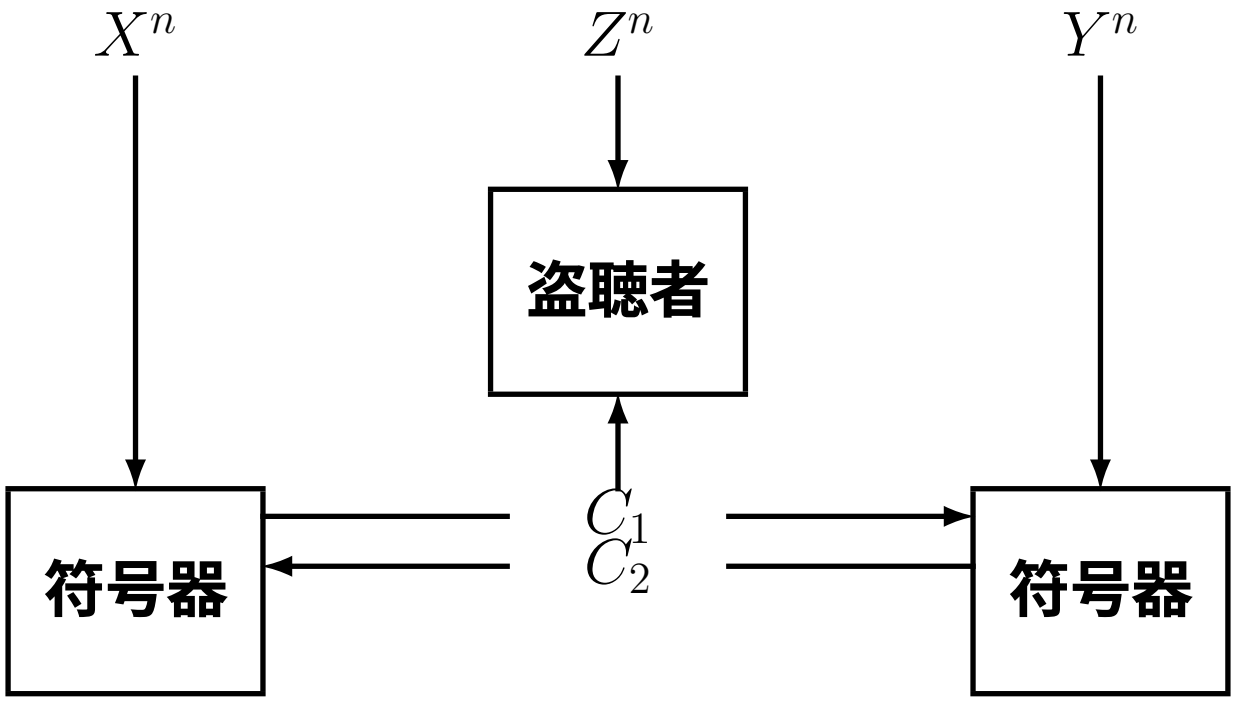
- 相関乱数をそのまま鍵にすることができない. なぜなら
  - X^n と Y^n が同一でない(エラーが生じる).
  - Eve の持つ乱数 Z^n から X^n, Y^n を推測できる(情報の一部が洩れている).
- Alice と Bob はこの状況から Eve が推測することが困難な同一の鍵を共有したい.

相関乱数を用いた秘密鍵共有 [Maurer,1993][Ahlswede-Csiszár,1993]



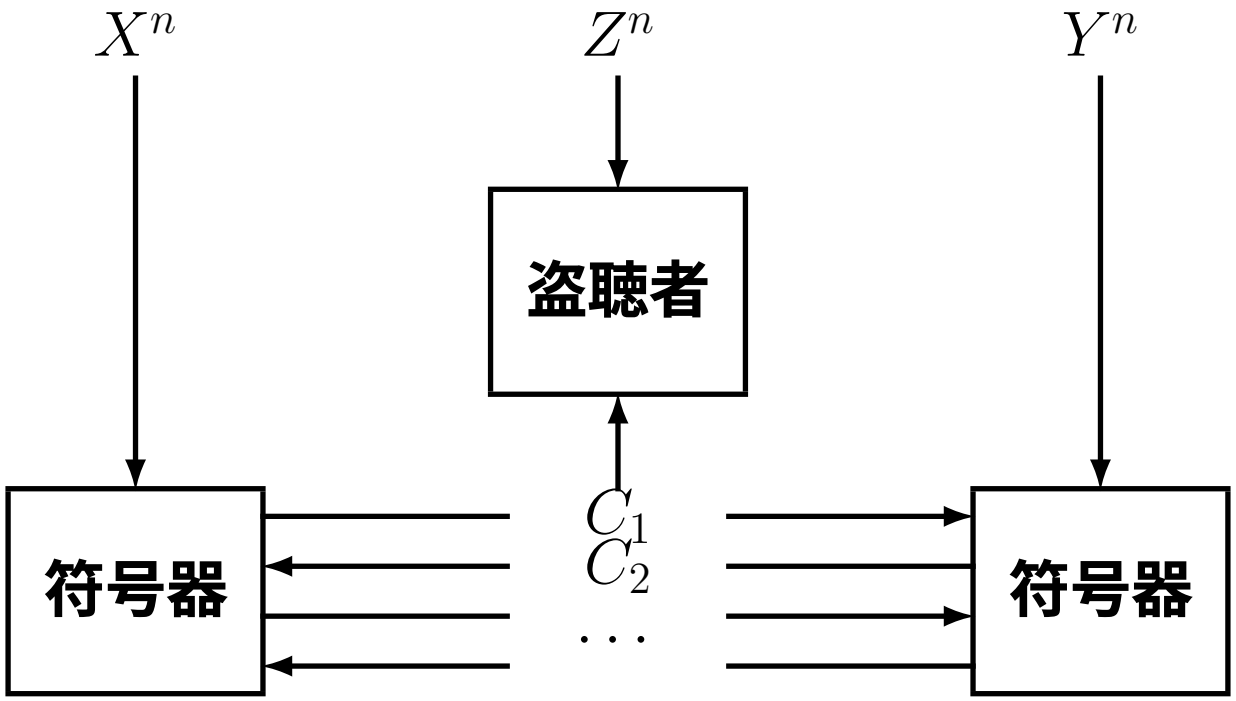
- Alice は X^n から C_1 を計算して(認証された)公開通信路を用いてBobへ送信する.

相関乱数を用いた秘密鍵共有 [Maurer,1993][Ahlswede-Csiszár,1993]



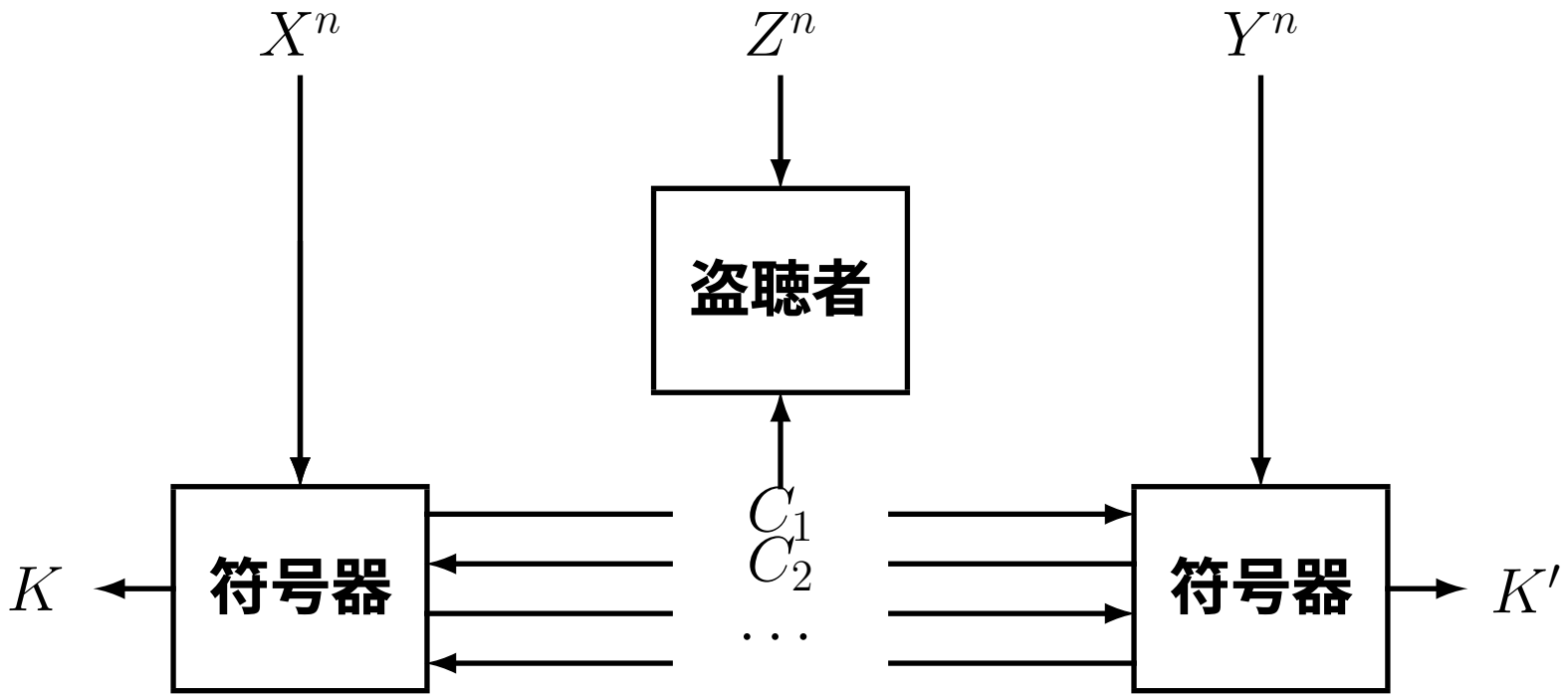
- Alice は X^n から C_1 を計算して(認証された)公開通信路を用いて Bob へ送信する.
- Bob は C_1 と Y^n から C_2 を計算して(認証された)公開通信路を用いて Alice へ送信する.

相関乱数を用いた秘密鍵共有 [Maurer,1993][Ahlswede-Csiszár,1993]



- Alice は X^n から C_1 を計算して(認証された)公開通信路を用いてBobへ送信する.
- Bob は C_1 と Y^n から C_2 を計算して(認証された)公開通信路を用いてAliceへ送信する.
- Alice と Bob は必要に応じて情報交換を行う.

相関乱数を用いた秘密鍵共有 [Maurer,1993][Ahlswede-Csiszár,1993]



- Alice と Bob は情報交換 $C_1, C_2, \ldots, C_t$ を行う.
- Alice と Bob は情報交換の後にそれぞれ鍵 K, K' を計算する.

鍵に要求される性質

$$\mathrm{Prob}\,(K \neq K') \leq \varepsilon \qquad \text{(信頼性)}$$

$$I(K; Z^n, C_1, C_2, \ldots, C_t) \leq \varepsilon \qquad \text{(安全性)}$$

秘密鍵容量(secret key capacity) [Maurer,1993][Ahlswede-Csiszár,1993]

- 情報交換 $C_1^t \equiv (C_1, \ldots, C^t)$ と鍵の計算 K,K' が, 任意の $\varepsilon > 0$ と十分大きな任意の n で以下の式を全て満たすとき, (C_1^t, K, K') を (X, Y, Z) に対するレート $R \geq 0$ の秘密鍵共有プロトコルと呼ぶ.

$$\left| \frac{H(K)}{n} - R \right| \leq \varepsilon$$

$$\mathrm{Prob}(K \neq K') \leq \varepsilon \qquad \text{(信頼性)}$$

$$I(K; Z^n, C_1^t) \leq \varepsilon. \qquad \text{(安全性)}$$

- 可能な秘密鍵共有プロトコルのレート R の上限 $\mathrm{S}(X;Y\|Z)$ を秘密鍵容量と呼ぶ.

秘密鍵容量の一次上界/下界

- [Maurer,1993]

$$\mathrm{S}(X;Y\|Z) \geq \max\{I(X;Y)-I(X;Z), I(Y,X)-I(Y;Z), 0\}$$
$$\mathrm{S}(X;Y\|Z) \leq \min\{I(X;Y|Z), I(X;Y)\}$$

- [Maurer-Wolf,1999]

$$\mathrm{S}(X;Y\|Z) \leq \inf_{\hat{Z}\leftrightarrow Z\leftrightarrow XY} I(X;Y|\hat{Z})$$

- [Renner-Wolf,2003]

$$\mathrm{S}(X;Y\|Z) \leq \inf_{U}\left[\inf_{\hat{Z}\leftrightarrow ZU\leftrightarrow XY} I(X;Y|\hat{Z})+H(U)\right]$$

秘密鍵共有の 3 段階[Bennett et al., 1995]

1. **優位性抽出**(advantage distillation):

   $I(X^n;Y^n) \leq I(X^n;Z^n)$ and $I(X^n;Y^n) \leq I(Y^n;Z^n)$

   $\Rightarrow \quad I(\widehat{X};\widehat{Y}) > I(\widehat{X};Z^n,C_1^t)$ or $I(\widehat{X};\widehat{Y}) > I(\widehat{Y};Z^n,C_1^t)$

2. **情報整合**(information reconciliation):

   正規ユーザは $(\widehat{X},\widehat{Y})$ **から同一の乱数系列** $\widehat{\widehat{X}} = \widehat{\widehat{Y}}$ **を得る**.

3. **秘密増幅**(privacy amplification):

   正規ユーザは同一の乱数系列から盗聴者には推測できない秘密鍵系列を得る.

優位性抽出容量(advantage distillation capacity)

[M et al.,IEICE-A2006]

- (X, Y, Z) に対するプロトコル $(C_1^t, \widehat{X}, \widehat{Y})$ について

$$R = \frac{1}{n}\left[I(\widehat{X}; \widehat{Y}) - I(\widehat{X}; Z^n, C_1^t)\right]$$

を優位性抽出レートと呼ぶ.

- 可能な優位性抽出プロトコルのレート R の上限$\mathcal{D}(X; Y\|Z)$ を優位性抽出容量と呼ぶ. すなわち,

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

ここで, sup では全ての n, t と可能な t ステップのプロトコル$(C_1^t, \widehat{X}, \widehat{Y})$ をとる.

注意: 条件 $\mathrm{Prob}(\widehat{X} \neq \widehat{Y}) \leq \varepsilon$, $I(\widehat{X}; Z^n, C_1^t) \leq \varepsilon$ は優位性抽出プロトコルでは要求しない.

多字秘密鍵容量[M et al., IEICE-A2006]

任意の相関情報源 (X,Y,Z) **に対して**

$$\mathrm{S}(X;Y\|Z)=\mathcal{D}(X;Y\|Z)=\sup_{n,t,C_1^t,\widehat{X},\widehat{Y}}\frac{1}{n}\left[I(\widehat{X};\widehat{Y})-I(\widehat{X};Z^n,C_1^t)\right].$$

補足

- **もしも** $[I(\widehat{X},\widehat{Y})-I(\widehat{Y};Z^nC_1^t)]/n$ **が正ならば, この値をレートに持つ疎行列(**LDPC**符号)を用いた情報整合と秘密増幅プロトコルが存在する**. [M, IEICE-A2006][M-Miyake, IEEE-IT2012][M-Miyake,ITW2012][M-Miyake, Springer2018].
- **一般情報源に対する同様の結果がある** [M-Miyake, Springer2018].

秘密鍵共有に関する部分問題

- $t < \infty$ で常に秘密鍵容量を達成できるか?
- $t = 2$ (1往復)のプロトコルで常に秘密鍵容量を達成できるか?
  - t の増大に伴い情報を盗聴者へ公開することになるので, t を不必要に大きくすることが正規ユーザーにとって良い戦略とは思えない.
- $t = 2$ の場合, C_2 を C_1 に依存させない(お互いが自分の乱数だけを見て情報公開する)ようにしても常に秘密鍵容量を達成できるか?
  - そのようなことが可能な例がある [M et al.,IEICE-A2006].

最後に

- 紹介した問題にまともに挑戦することはおすすめしません.
  - 数多くの研究者が挑戦してできなかったこと.
    - (研究者として) できることを継続することが大切.
    - 新しいテクニックができたときに, ひょっとしたら解けるかもしれない程度に考えておく.
  - 問題の意義がそれほど明確でない.
    - 数学の問題としては成立していると思うが...
    - 問題を解決した先に何があるのかをちゃんと説明できなければいけない.
      - 問題設定は現実的で重要なのか？
- そもそもの疑問
  - 1字表現は可能なのか?
    - 容量域は有限個の補助変数の導入で記述可能なのか?
  - 1字表現は必要なのか?
    - 容量域の境界 (Shannon 限界) に近づく反復アルゴリズムは存在するか?

ご清聴ありがとうございました.