修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　情報理工学研究科　　情報・ネットワーク工学専攻　博士前期課程		
氏　　名	小柳　翔吾	学籍番号	2231045
論 文 題 目	強安全性基準に基づく受動的盗聴者が存在する生体識別システム		

要　旨

生体識別システム（BIS）は，指紋などの情報を利用してユーザを識別するシステムである．パスワード方式や IC カードの識別に比べて記憶忘れや紛失といった問題を回避できるため，その重要性が高まっている．一方で，ユーザに対して固有の生体情報の流出は好ましくないことから，漏洩する情報量を最小限にとどめることが重要である．そこで，情報理論的アプローチを用いて主に 2 種類の BIS モデルが検討されている．生体情報系列から秘密鍵を生成する GS-BIS モデルと外部から秘密鍵を与える CS-BIS モデルである．これらのモデルでは，符号器と復号器の間に共有される符号語が公開データベースに保存されるため，信頼性の高い識別を保ちつつ符号語に含まれる生体情報や秘密鍵に関する情報量をできる限り抑えることが重要である．そのため 2021 年に Yachonga と Yagi によって，2 つのモデルの識別（ユーザ数），符号化，プライバシー漏洩および秘密鍵レートの容量域（それらのレート組の最適なトレードオフの関係性）が明らかにされた．また，2016 年に Kittichokechai と Caire によって盗聴者が存在する GS-BIS が解析された．ただしこれらの文献では，秘密鍵の漏洩を情報系列長に対して線形的に増加することを許容する弱安全性基準で評価している．信頼性の高いシステムを構築するためには，情報系列長に依らない強安全性基準で秘密鍵の漏洩を解析することが重要である．そこで本論文では，強安全性基準に基づく受動的盗聴者が存在する 2 つのモデルにおける容量域を導出する．また，計算例として二元情報源に対する容量域を導出して，各レート組の関係性を明らかにする．その結果，GS-BIS モデルの容量域は CS-BIS モデルの容量域よりも大きく，符号化レートの下限が秘密鍵レートの最大値分だけ差があることが明らかになった．また，強安全性基準と弱安全性基準の数学的な表現が一致し，各レート組にトレードオフの関係があることが判明した．

令和５年度　修士学位論文

強安全性基準に基づく受動的盗聴者が存在する生体識別システム

電気通信大学 大学院 情報理工学研究科
博士前期課程 情報・ネットワーク工学専攻
2231045　小柳 翔吾
指導教員　八木 秀樹 准教授　大濱 靖匡 教授

提出　令和６年１月 28 日

THE UNIVERSITY OF ELECTRO-COMMUNICATIONS
Department of Communication Engineering and Informatics

目 次

第 1 章

はじめに

生体識別システム（Biometric Identification System: BIS）は，指紋や音声などの情報を利用してユーザを識別するものである．パスワードや IC カードの識別に比べて記憶忘れや紛失といった問題を回避できるため，その重要性が高まっている [1]．一方で，生体情報はユーザに対して固有の情報であるため，盗聴者に漏洩する情報量を最小限に留めることが重要である．そこで，情報理論的アプローチを用いて安全性や精度を考慮した BIS の解析が行われている．

2003 年に Willems ら [2] は BIS を解析し，達成可能な最大のユーザ数（識別容量）を明らかにした．文献 [2] の発展として，文献 [3] では符号化レートを導入したシステムが解析された．次に，Ignatenko と Willems [4] は符号化により，生体情報系列から符号語と秘密鍵を生成する **Generated Secret BIS（GS-BIS）**と呼ばれるモデルを検討した．このモデルでは，符号器と復号器の間に共有される符号語が公開データベース上に保存されると想定するため，信頼性の高い識別を保ちつつ符号語に含まれる生体情報系列に関する情報量をできる限り抑えることが重要である．また，BIS は GS-BIS モデルの他に **Chosen Secret BIS（CS-BIS）**と呼ばれるモデルがある．CS-BIS モデルは，秘密鍵が外部から独立して無作為かつ一様に選ばれ，秘密鍵とユーザの生体情報系列を使って符号語を生成するモデルである．ここでは，2 つのモデルにおける識別（ユーザ数），プライバシー漏洩および秘密鍵レートの**容量域** (それらのレート組の最適なトレードオフの関係性) が明らかにされた．文献 [4] の発展として，文献 [5]，[6]，[7] では上述の 2 つのモデルの識別，符号化，プライバシー漏洩および秘密鍵レートの容量域が明らかにされた．なお，ガウス型の連続情報源まで拡張した BIS の容量域は文献 [8]，[9] で議論されている．文献 [10] では，外部から乱数を与えることで秘密鍵の漏洩を一般のレートまで許容するモデルが解析された．文献 [11] では盗聴者が存在する GS-BIS モデルが研究された．ただし，検討されているモデルでは，生体情報系列を登録する際に発生する雑音を考慮していない．現実の世界では，スキャナーなどを用いて生体情報を抽出する過程で雑音が加わる．従って，登録過程において生じる雑音を BIS に取り入れることは重要な意味を持つ．文献 [12] では登録雑音を考慮した受動的盗聴者が存在する 2 つのモデルの容量域が

明らかにされた．しかし，秘密鍵の漏洩に関する制約式が弱安全性基準に基づいている．信頼性の高いシステムを構築するためには，情報系列長によらない強安全性基準の基で，秘密鍵の漏洩を解析することが重要である．文献 [15] では強安全性基準に基づく容量域が導かれているが，シングルユーザのシステムを解析しているためユーザの推定が検討されていなかった．一般的な BIS では，莫大なユーザ数を保持しており，利用するユーザを正しく推定することが求められている．そのため，BIS の性能を解析をする際に識別レートの制約を課すことが自然な流れである．さらに，復号器への通信路は盗聴者への通信路に比べて雑音が少ないという関係に限定されているが，両者の通信路の関係性はあらゆる状況を考えるべきである．

本論文では，強安全性基準に基づく受動的盗聴者が存在する 2 つのモデルにおける容量域の導出を目的とする．ただし文献 [15] とは異なり，マルチユーザのシステムであり，復号器への通信路と盗聴者への通信路の関係を限定しない．主要な結果の順定理の証明は，鍵共有問題の枠組みで提案された情報スペクトル的手法 [13]，[14]，[16] を用いて，補助確率変数の個数を 1 つから 2 つに拡張して解析する．逆定理の証明は弱安全性基準の解析法 [12] と同様であり，得られた容量域の表現は文献 [12] で与えられた表現と一致していることを明らかにする．また，計算例として二元情報源に対する容量域を導出して，各レート組の関係性を明らかにする．

本論文の構成を以下に示す．第 2 章では，本論文で使用する記号とシステムモデルを定義する．第 3 章では，達成可能性を定義し，主要な結果として一般情報源に対する容量域を導出する．また，計算例として二元情報源に対する容量域を導出する．第 4 章では，主要な結果の証明を与える．第 5 章では，まとめと今後の課題を述べる．

第 2 章

記号の定義とシステムモデル

2.1 記号の定義

本論文では基本的に文献 [18] と同じ記号を使用し，対数の底は 2 とする．$\mathcal{A}$ は有限アルファベット，大文字の A は $\mathcal{A}$ に値を取る確率変数，小文字の $a \in \mathcal{A}$ はその実現値を表す．$P_A(a) = \Pr[A = a]$ は $\mathcal{A}$ 上の確率分布を表す．確率変数 A のエントロピーを $H(A)$，確率変数 A と B の結合エントロピーを $H(A, B)$，A と B の間の相互情報量を $I(A; B)$ とする．$H_b(\cdot)$ は二値エントロピー関数を表す．$*$ 演算子は $a * b = a(1-b) + (1-a)b$ と定義する．$a < b$ であるような整数 a と b に対して，$[a : b]$ は集合 $\{a, a+1, \cdots, b\}$ を表し，a 番目から b 番目のシンボルまでの系列 $(c_a, \cdots, c_b)$ を c_a^b と表す．系列 $(c_1, \cdots, c_{a-1}, c_{a+1}, \cdots, c_b)$ を $c^{b\backslash a}$ と表す．$\mathbb{R}_+^n$ を 0 以上の実数を成分とする n 次元ベクトルの集合とする．

2.2 システムモデル

本論文で検討する BIS は 2 つの過程: (I) **登録過程**と (II) **識別/認証過程**によって構成されており，そのシステムを図 2.1 に示す．ただし，GS-BIS モデルでは秘密鍵が符号器から出力され，CS-BIS モデルでは秘密鍵を符号器に入力することを矢印の向きで表している．以下の説明では，$\mathcal{I}_n = [1 : M_I]$，$\mathcal{J}_n = [1 : M_J]$ および $\mathcal{S}_n = [1 : M_S]$ をそれぞれユーザのインデックス，符号語および秘密鍵の集合とし，$\mathcal{X}$，$\tilde{\mathcal{X}}$，$\mathcal{Y}$ および $\mathcal{Z}$ を有限集合とする．

(I) **登録過程**: 任意のユーザ $i \in \mathcal{I}_n$ に対して，n 個のシンボルから成る生体情報系列 $x_i^n = (x_{i1}, \cdots, x_{in}) \in \mathcal{X}^n$ は，無記憶情報源 $P_X(\cdot)$ から独立同一分布 (i.i.d.) に従って生成され，その確率は $P_{X_i^n}(x_i^n) \triangleq \prod_{k=1}^n P_X(x_{ik})$ で与えられる．生体情報系列 $x_i^n \in \mathcal{X}^n$ を入力すると，登録通信路 $P_{\tilde{X}|X}$ を介して登録系列（雑音のある生体情報系列）$\tilde{x}_i^n = (\tilde{x}_{i1}, \cdots, \tilde{x}_{in}) \in \tilde{\mathcal{X}}^n$ が出力される．各生体情報系列が互いに独立に生成され，$P_{\tilde{X}|X}$ を定常無記憶の通信路と

仮定すると，各系列組の同時分布は次のように与えられる．

$$P_{\tilde{X}_1^n \cdots \tilde{X}_{M_I}^n X_1^n \cdots X_{M_I}^n}(\tilde{x}_1^n, \cdots, \tilde{x}_{M_I}^n, x_1^n, \cdots, x_{M_I}^n) \triangleq \prod_{i=1}^{M_I} \prod_{k=1}^{n} P_{\tilde{X}|X}(\tilde{x}_{ik}|x_{ik}) P_X(x_{ik}). \tag{2.1}$$

GS-BIS モデルの場合は，符号器が登録系列 $\tilde{x}_i^n$ $(i \in \mathcal{I}_n)$ を符号語 $j(i) \in \mathcal{J}_n$ と秘密鍵 $s(i) \in \mathcal{S}_n$ に符号化することから，符号化関数 $f(\cdot)$ を用いて $(j(i), s(i)) = f(\tilde{x}_i^n)$ となる．CS-BIS モデルの場合は，秘密鍵 $s(i) \in \mathcal{S}_n$ が他の全ての確率変数から独立に無作為かつ一様に選ばれる．符号器が，生体情報系列 $\tilde{x}_i^n$ $(i \in \mathcal{I}_n)$ と秘密鍵 $s(i) \in \mathcal{S}_n$ を符号語 $j(i) \in \mathcal{J}_n$ に符号化することから，$j(i) = f(\tilde{x}_i^n, s(i))$ となる．符号語は公開されるデータベースの i の位置に保存され，秘密鍵はユーザ i に返される．データベースに格納された全ての符号語を $\boldsymbol{j} \triangleq \{j(1), \cdots, j(M_I)\}$ とし，その確率変数を $\boldsymbol{J}$ と表す．

(II) **識別/認証過程**: システムにアクセスした未知のユーザ $w \in \mathcal{I}_n$ の生体情報系列 $x_w^n \in \mathcal{X}^n$ が入力されると，定常無記憶な識別通信路 $P_{YZ|X}$ を介して観測系列 $y^n = (y_1, \cdots, y_n) \in \mathcal{Y}^n$ と盗聴者の観測系列 $z^n = (z_1, \cdots, z_n) \in \mathcal{Z}^n$ が出力される．なお，$P_{Y|X}$ を復号器への通信路，$P_{Z|X}$ を盗聴者への通信路と呼ぶ．復号器は，観測系列 y^n とデータベース上の符号語 $\boldsymbol{j}$ を使って，識別されるユーザの推定値 $\widehat{w}$ と秘密鍵の推定値 $\widehat{s(w)}$ を復号することから，復号関数 $g(\cdot)$ を用いて $(\widehat{w}, \widehat{s(w)}) = g(y^n, \boldsymbol{j})$ となる．ここで，$(\widehat{w}, \widehat{s(w)}) = (w, s(w))$ ならばユーザの識別と秘密鍵の共有に成功する．

本論文では図 2.1 に示すように，データベース上の符号語 $\boldsymbol{j}$ と観測系列 $z^n = (z_1, \cdots, z_n) \in \mathcal{Z}^n$ を知っている盗聴者が存在する場合の秘密鍵に基づく識別の問題を検討する．ここでは，盗聴者が受動的であり，ユーザの生体情報系列と秘密鍵を推測しようとする場合を考える．

各生体情報系列が互いに独立に生成され，$P_{YZ|X}$ が定常無記憶の通信路であることから，識別されるユーザ w に対する系列組の同時分布は次のように与えられる．

$$P^{(w)}_{Y^n Z^n X_w^n \tilde{X}_w^n}(y^n, z^n, x_w^n, \tilde{x}_w^n) \triangleq \prod_{k=1}^{n} \Big(P_{YZ|X}(y_k, z_k|x_{wk}) P_X(x_{wk}) P_{\tilde{X}|X}(\tilde{x}_{wk}|x_{wk}) \Big). \tag{2.2}$$

ここで，$P^{(w)}$ は w の依存性を示している．本論文では，文献 [11] と同様に識別されるユーザに対応する確率変数 W の分布が未知であると仮定する．そのため，識別されるユーザが $W = w$ だったとき，その条件の下で推定の誤る確率を $\mathbb{P}_w(\cdot)$，相互情報量を $I_w(\cdot;\cdot)$，エントロピーを $H_w(\cdot)$ と表記し，議論を進める．

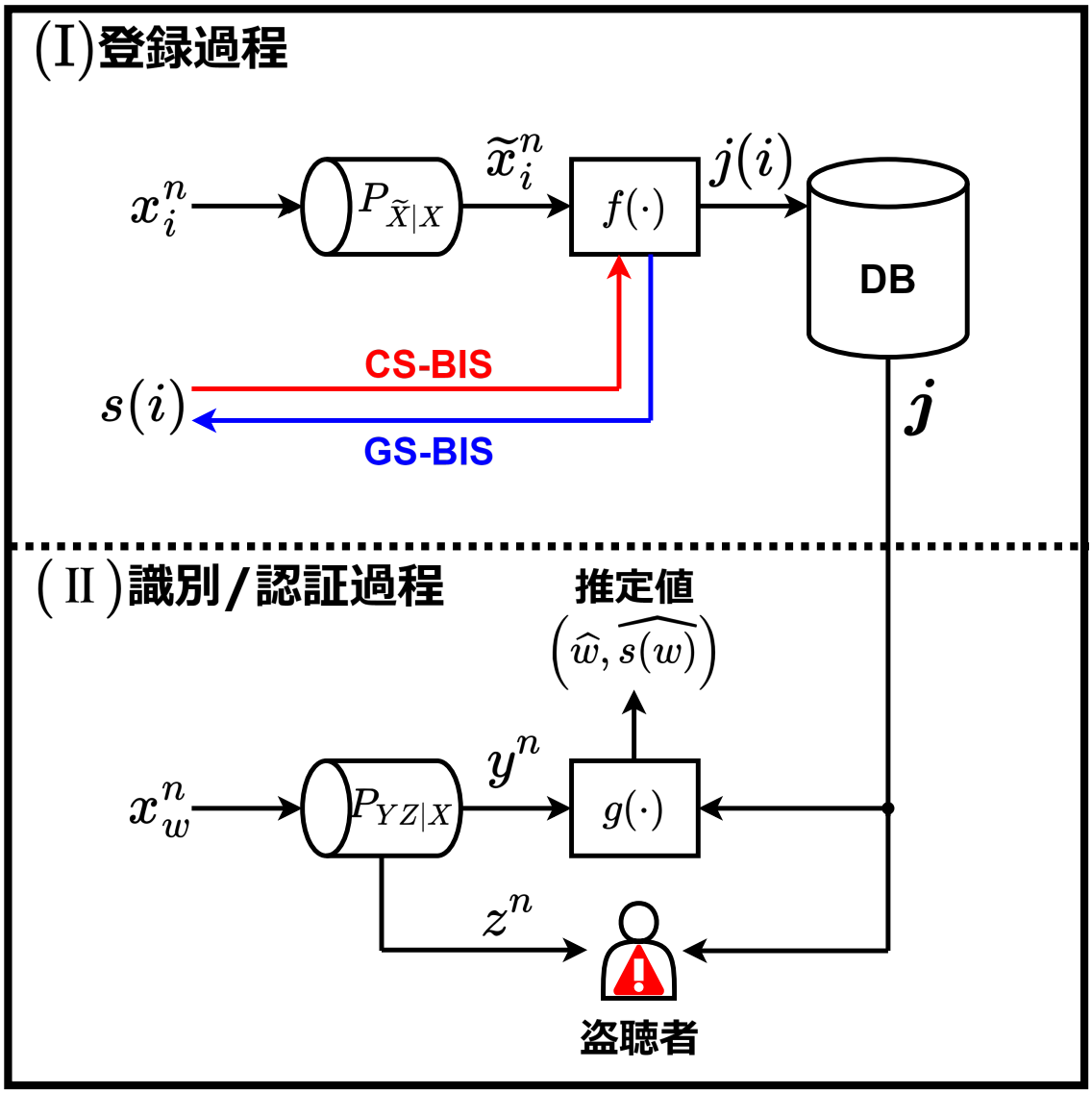

図 2.1: 受動的盗聴者が存在する BIS

第 3 章

達成可能性の定義と主要な結果

本章では，強安全性基準に基づく受動的盗聴者が存在する BIS の達成可能性の定義とその容量域を示す.

3.1 達成可能性の定義

検討するモデルの達成可能性の定義は次のように与えられる.

定義 1. GS-BIS モデルにおける識別，符号化，プライバシー漏洩および秘密鍵レートの組 $(R_I, R_J, R_L, R_S) \in \mathbb{R}_+^4$ が**達成可能**とは，任意の $\delta > 0$ と十分に大きな系列長 n に対して，

$$\max_{w\in\mathcal{I}_n} \mathbb{P}_w[(\widehat{W}, \widehat{S(W)}) \neq (w, S(w))] \leq \delta, \tag{3.1}$$

$$\log M_I \geq n(R_I - \delta), \tag{3.2}$$

$$\log M_J \leq n(R_J + \delta), \tag{3.3}$$

$$\max_{w\in\mathcal{I}_n} I_w(X_w^n; \boldsymbol{J}, Z^n) \leq n(R_L + \delta), \tag{3.4}$$

$$\max_{w\in\mathcal{I}_n} I_w(S(w); \boldsymbol{J}, Z^n) \leq \delta, \tag{3.5}$$

$$\min_{w\in\mathcal{I}_n} H_w(S(w)) \geq n(R_S - \delta) \tag{3.6}$$

を満たすような符号器 f と復号器 g の組が存在することを意味する．また，達成可能な (R_I, R_J, R_L, R_S) の全ての組を GS-BIS モデルにおける**容量域**と呼び，$\mathcal{R}_G$ と表す.

式 (3.5) では，$(\boldsymbol{J}, Z^n)$ を観測したときの $S(w)$ に関する情報漏洩量を $I_w(S(w); \boldsymbol{J}, Z^n)$ によって測り，その量がどの $w \in \mathcal{I}_n$ についても δ 以下になることを要請している．この基準を一般的に**強安全性基準**と呼ぶ．同様に，$S(w)$ に関する情報漏洩量が $n\delta$ 以下になることを**弱安全性基準**と呼ぶ．定義 1 において，式 (3.1) はシステムの信頼性の制約式で，識別されるユーザ w に対する最大の誤り確率が δ 以下になることを示している．式 (3.2) は識別レートに関する制約式で，R_I をできるだけ大きく設定するべきことを表す．式 (3.3) は符号化レートに関する制約式で，R_J をできるだけ小さく設定するべきことを

表す．式 (3.4) はプライバシー漏洩レートに関する制約式で，データベース上の符号語 $\boldsymbol{J}$ と盗聴者の観測系列 Z^n から見たときの生体情報系列 X_w^n の漏洩量を表しており，R_L をできるだけ小さく設定するべきことを表す．式 (3.5) はデータベース上の符号語 $\boldsymbol{J}$ と盗聴者の観測系列 Z^n から見たときの秘密鍵 $S(w)$ の漏洩に関する制約式で，最大の秘密鍵の漏洩量が δ 以下になることを示している．式 (3.6) は秘密鍵レートに関する制約式で，R_S をできるだけ大きく設定するべきことを表す．

定義 2. CS-BIS モデルにおける識別，符号化，プライバシー漏洩および秘密鍵レートの組 $(R_I, R_J, R_L, R_S) \in \mathbb{R}_+^4$ が**達成可能**とは，任意の $\delta > 0$ と十分に大きな系列長 n に対して，式 (3.1)–(3.5) に加えて

$$\log M_S \geq n(R_S - \delta) \tag{3.7}$$

を満たすような符号器 f と復号器 g のペアが存在することを意味する．また，達成可能な (R_I, R_J, R_L, R_S) の全ての組を CS-BIS モデルにおける**容量域**と呼び，$\mathcal{R}_C$ と表す．

CS-BIS モデルでは，秘密鍵の分布が一様であるため式 (3.6) を式 (3.7) に置き換えている．

3.2　主要な結果

主要な結果として一般情報源に対する容量域を導出するために，以下の 2 つの領域を定義する．

定義 3. 識別，符号化，プライバシー漏洩および秘密鍵レートの組 (R_I, R_J, R_L, R_S) の領域は以下のように定義される．

$$\begin{aligned}
\mathcal{A}_G \triangleq \bigcup_{P_{U|\tilde{X}}, P_{V|U}} \{&(R_I, R_J, R_L, R_S) \in \mathbb{R}_+^4 : \\
&R_I \leq I(Y;V), \\
&R_J \geq R_I + I(\tilde{X};U|Y), \\
&R_L \geq I(X;U,Y) - I(X;Y|V) + I(X;Z|V), \\
&R_S \leq I(Y;U|V) - I(Z;U|V)\},
\end{aligned} \tag{3.8}$$

$$\begin{aligned}
\mathcal{A}_C \triangleq \bigcup_{P_{U|\tilde{X}}, P_{V|U}} \{&(R_I, R_J, R_L, R_S) \in \mathbb{R}_+^4 : \\
&R_I \leq I(Y;V), \\
&R_J \geq R_I + I(\tilde{X};U|Y) + I(Y;U|V) - I(Z;U|V), \\
&R_L \geq I(X;U,Y) - I(X;Y|V) + I(X;Z|V), \\
&R_S \leq I(Y;U|V) - I(Z;U|V)\}.
\end{aligned} \tag{3.9}$$

ただし，補助確率 V，U はマルコフ連鎖 $V - U - \tilde{X} - X - (Y, Z)$ を成し，$|\mathcal{V}| \leq |\tilde{\mathcal{X}}| + 5$，$|\mathcal{U}| \leq (|\tilde{\mathcal{X}}| + 5)(|\tilde{\mathcal{X}}| + 3)$ を満たす有限アルファベット $\mathcal{V}$，$\mathcal{U}$ 上に値を取る．

容量域は以下のように与えられる．

定理 1. GS-BIS モデルと CS-BIS モデルの識別，符号化，プライバシー漏洩および秘密鍵レートの容量域はそれぞれ

$$\mathcal{R}_G = \mathcal{A}_G, \quad \mathcal{R}_C = \mathcal{A}_C \tag{3.10}$$

で与えられる．

(証明). 定理 1 の証明は第 4 章に記載する．□

順定理の証明は情報スペクトル的手法 [13] を用いる．逆定理の証明は文献 [12] と同様に評価できる．領域の凸性は [25, Section V-A] と同様の手法で証明できる．$\mathcal{A}_G$ と $\mathcal{A}_C$ の領域は文献 [12] で導出された弱安全性基準の領域と等しい．また，$\mathcal{A}_G$ と $\mathcal{A}_C$ において less noisy channels [15] を仮定し，補助確率変数 V を定数にすると文献 [15, Theorem 3] の結果と一致する．

GS-BIS モデルでは，生体情報系列から秘密鍵と符号語を生成するため符号語には生体情報系列の情報のみを含めている．一方で CS-BIS モデルでは，秘密鍵と生体情報系列から符号語を生成するため，ユーザと秘密鍵の推定を正しく行うためにはデータベース上の符号語に秘密鍵の情報も含めなくてはいけない．そのため，CS-BIS モデルでは R_J の最小値が R_S の最大値分だけ大きくなっており，容量域は $\mathcal{A}_C$ よりも $\mathcal{A}_G$ の方が大きい．

3.3　二元情報源に対する容量域

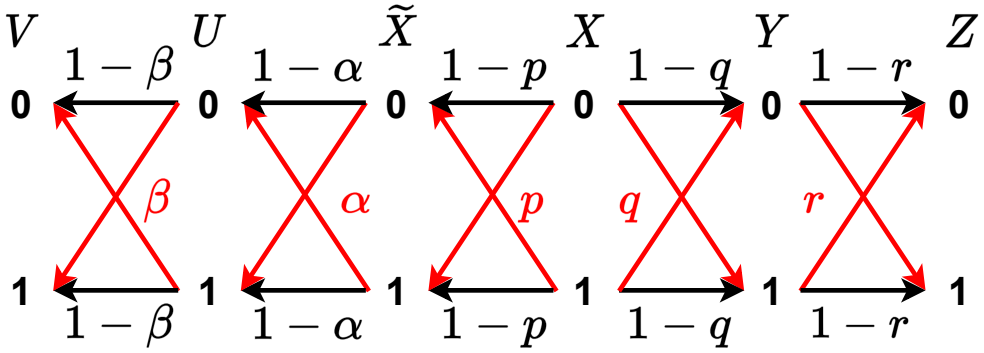

図 3.1: 二元対称通信路の遷移確率

本節では，定理 1 の GS-BIS モデルにおける計算例を導出する．議論を簡単にするために，盗聴者への通信路 $P_{Z|X}$ は復号器への通信路 $P_{Y|X}$ に比べて劣化していると仮定する．つまり，(X, Y, Z) はマルコフ連鎖 $X - Y - Z$ を成す．

情報源と通信路の仮定は図 3.1 のようになる．まず, 情報源の確率変数は $X \sim \mathrm{Bern}(1/2)$ と仮定する．次に，登録通信路 $P_{\tilde{X}|X}$，復号器への通信路 $P_{Y|X}$ および盗聴者への通信路 $P_{Z|Y}$ はいずれも二元対称通信路（BSC）で, それぞれの誤り確率は $(p, q, r) \in [0, 1/2]$ と仮定する．また，テスト通信路 $P_{U|\tilde{X}}$，$P_{V|U}$ は BSC でそれぞれの誤り確率は α，β と仮定する．この設定の最適な領域を以下に示す．

定理 2.

$$
\begin{aligned}
\mathcal{R}'_G = \bigcup_{(\alpha,\beta)\in[0,1/2]} \{(R_I, R_J, R_L, R_S) \in \mathbb{R}_+^4 :\ & \\
R_I &\le 1 - H_b(\alpha * \beta * p * q) \\
R_J &\ge R_I + H_b(\alpha * p * q) - H_b(\alpha), \\
R_L &\ge 1 - H_b(q * r) + H_b(\alpha * p * q) - H_b(\alpha * p) \\
&\quad + H_b(\alpha * \beta * p * q * r) - H_b(\alpha * \beta * p * q), \\
R_S &\le H_b(\alpha * p * q * r) - H_b(\alpha * p * q) - H_b(\alpha * \beta * p * q * r) + H_b(\alpha * \beta * p * q)\}.
\end{aligned}
\tag{3.11}
$$

(証明). 定理 2 の証明は付録 A に記載する．　□

以下の議論では，定理 2 に値を代入して各レート組の関係性を解析する．$\mathcal{R}'_G$ において $(p, q, r) = (0.02, 0.05, 0.15)$ と設定する．そして，$R_I = 0.05$ を固定し，R_L をいくつかの値に設定する．この条件下で，横軸を R_J とし，縦軸を R_S の最大値で表したグラフを図 3.2 に示す．

図 3.2 より，R_J がある値より大きくなると R_S の最大値は一定になる．これは，R_J がある値より大きくなると，固定した R_I と R_L 以外の制約がかからなくなるからである．また，R_S の最大値が一定になる値は R_L に起因する．R_L が大きくなると制約が弱くなっていき，$R_L = 0.55$ 付近で R_L の制約がかからなくなる．つまり，今回の条件下では $R_S = 0.34$ 以上は R_S の最大値を大きくすることはできない．一方で，$R_L = 0.35$ よりも R_L が小さくなると $R_S = 0$ となり，有効な鍵を生成できないシステムになってしまう．すなわち，符号化をした時点で $R_L = 0.35$ の漏洩が発生することを意味する．また，R_J を小さくし R_S を大きく設定したいが，R_J を大きくすると R_S も大きくなることから，両者にはトレードオフ関係が存在する．

同様に，$\mathcal{R}'_G$ において $(p, q, r) = (0.15, 0.2, 0.3)$ と設定する．そして，$R_L = 0.41$ を固定し，R_J をいくつかの値に設定する．この条件下で，横軸を R_I とし，R_S の最大値で表したグラフを図 3.3 に示す．

図 3.3 より，グラフの概形は $R_L = 0.41$ と R_J の制約が強い方に依存する．$R_J \leq 0.9$ では R_J の制約が強く，それ以外では R_L の制約が強くなっている．また，R_I と R_S はどちらも大きく設定したいが，R_I を大きくすると R_S も小さくなることから，両者にはトレードオフ関係が存在する．

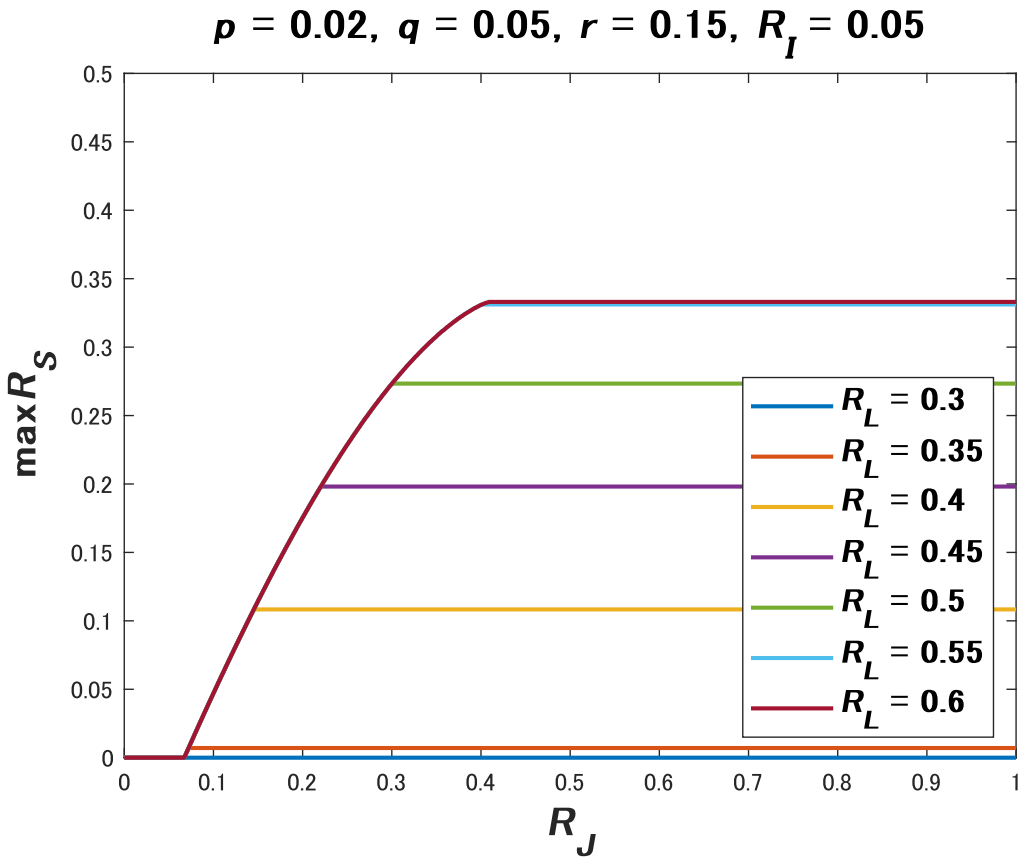

図 3.2: R_J と R_S の関係を表したグラフ

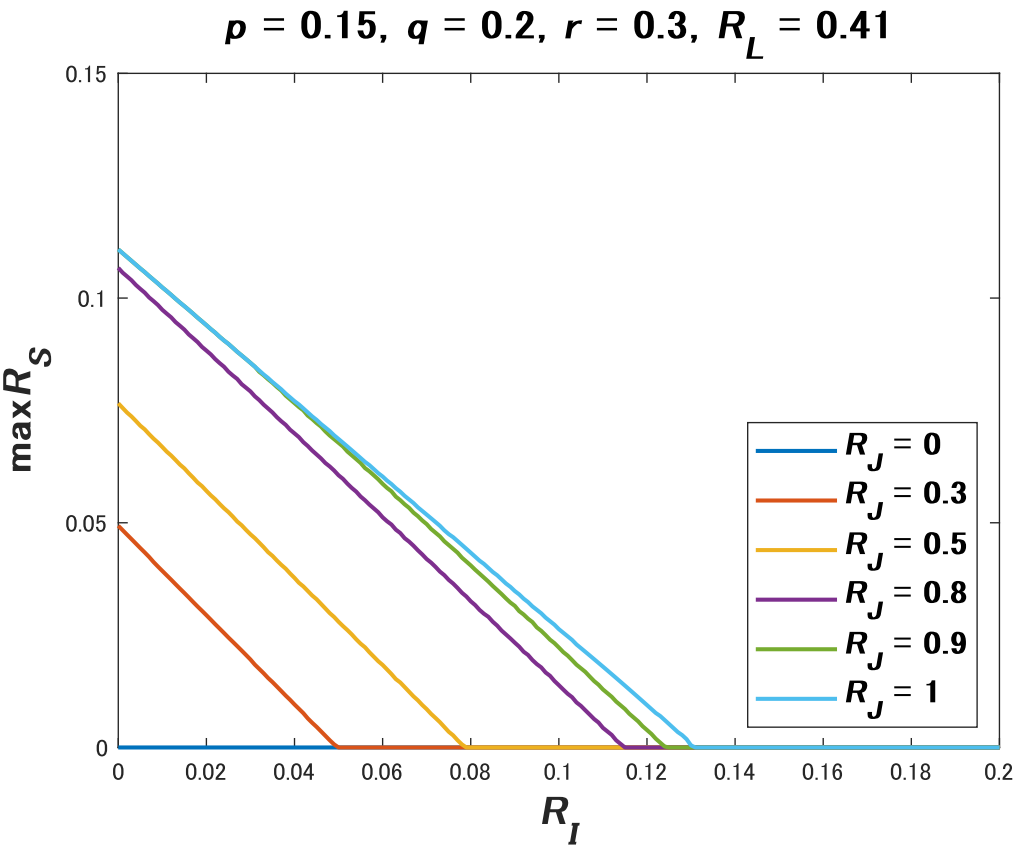

図 3.3: R_I と R_S の関係を表したグラフ

第 4 章

定理1の証明

4.1 順定理の証明

4.1.1 GS-BIS モデル

順定理の証明では，$\mathcal{R}_{\mathcal{G}} \supseteq \mathcal{A}_{\mathcal{G}}$ を示す．本論文では，シングルユーザに対する文献 [15] の順定理の証明をマルチユーザに拡張する．また，文献 [15] では補助確率変数が 1 つであるが，2 つに拡張する．プライバシー漏洩レートの評価は文献 [24] を参照している．

まずは，各パラメータの設定を行う．テスト通信路 $P_{U|\tilde{X}}$，$P_{V|U}$ と系列長 n を固定し，δ を十分に小さな正の実数とする．次に，それぞれのレートを $R_I = I(Y;V) - \delta$，$R_L = I(X;U,Y) - I(X;Y|V) + I(X;Z|V) + 7\delta$，$R_S = I(Y;U|V) - I(Z;U|V) - 6\delta$ および $R_J = R_I + I(\tilde{X};U|Y) + 4\delta$ とし，ユーザの要素数 $M_I = 2^{nR_I}$，符号語の要素数 $M_J = 2^{nR_J}$ および秘密鍵の要素数 $M_S = 2^{nR_S}$ を設定する．また，補助的な符号化レートを $R_v = R_I + I(\tilde{X};V|Y) + 2\delta$，$R_u = I(\tilde{X};U|Y,V) + 2\delta$ とし，集合 $\mathcal{J}_n^{(v)} = [1 : 2^{nR_v}]$，$\mathcal{J}_n^{(u)} = [1 : 2^{nR_u}]$ を設定する．ただし，$R_v + R_u = R_J$ である．ここで，マルコフ連鎖 $V - U - \tilde{X} - X - (Y,Z)$ が成立することに注意されたい．

以降の議論で必要となる集合を以下のように定義する．

$$\mathcal{T}_{v\tilde{x}}^n = \Big\{(v^n, \tilde{x}_w^n) : \frac{1}{n}\log\frac{P_{V^n|\tilde{X}^n}(v^n|\tilde{x}_w^n)}{P_{V^n}(v^n)} \le I(\tilde{X};V) + \delta\Big\},$$

$$\mathcal{T}_{vu\tilde{x}}^n = \Big\{(v^n, u^n, \tilde{x}_w^n) : \frac{1}{n}\log\frac{P_{U^n|V^n\tilde{X}^n}(u^n|v^n,\tilde{x}_w^n)}{P_{U^n|V^n}(u^n|v^n)} \le I(\tilde{X};U|V) + \delta\Big\},$$

$$\mathcal{A}_{vy}^n = \Big\{(v^n, y^n) : \frac{1}{n}\log\frac{P_{V^n|Y^n}(v^n|y^n)}{P_{V^n}(v^n)} \ge I(Y;V) - \delta\Big\},$$

$$\mathcal{A}_{vuy}^n = \Big\{(v^n, u^n, y^n) : \frac{1}{n}\log\frac{P_{U^n|V^nY^n}(u^n|v^n,y^n)}{P_{U^n|V^n}(u^n|v^n)} \ge I(Y;U|V) - \delta\Big\}$$

$$\mathcal{B}_{vuxz}^n = \Big\{(v^n, u^n, x_w^n, z^n) : \frac{1}{n}\log\frac{P_{X^n|U^nZ^n}(x_w^n|u^n,z^n)}{P_{X^n|V^nZ^n}(x_w^n|v^n,z^n)} \ge I(X;U|V,Z) - \delta\Big\}.$$

ここで，$V^n \sim \prod_{t=1}^n P_{V_t}$，$P_{V_t} = P_V$ および $U^n \sim \prod_{t=1}^n P_{U_t|V_t}$，$P_{U_t|V_t} = P_{U|V}$ である．

ランダム符号の生成：　$N_v = 2^{n(I(\tilde{X};V)+\delta)}$ 個の系列 $v^n(m) : m \in [1 : N_v]$ を分布 P_{V^n} に従ってランダムに生成し，これらの系列の集合を $\mathcal{O}_n \subset \mathcal{V}^n$ と表す．N_v 個の系列は，一様に分布した $[1 : N_v]$ 上の置換 π_v によって並び替えられ，関数 $\phi_v : \mathcal{O}_n \to \mathcal{J}_n^{(v)}$ で 2^{nR_v} 個のビンに均等に分割される．$j_v \in [1 : 2^{nR_v}]$ は $v^n(m)$ が属するビンのインデックスを表し，$j_v = \phi_v(\pi_v(v^n(m)))$ とする．

また，各 $v^n(m)$ に対して $N_u = 2^{n(I(\tilde{X};U|V)+\delta)}$ 個の系列 $u^n(m,l) : l \in [1 : N_u]$ を分布 $P_{U^n|V^n=v^n(m)}$ に従って生成し，これらの系列の集合を $\mathcal{Q}_n \subset \mathcal{U}^n$ と表す．N_u 個の系列は，一様に分布した $[1 : N_u]$ 上の置換 π_u によって並び替えられ，関数 $\phi_u : \mathcal{Q}_n \to \mathcal{J}_n^{(u)}$ で 2^{nR_u} 個のビンに均等に分割される．$j_u \in [1 : 2^{nR_u}]$ は $u^n(m,l)$ が属するビンのインデックスを表し，$j_u = \phi_u(\pi_u(u^n(m,l)))$ とする．マルコフ連鎖 $V - U - \tilde{X} - Y$ を用いて，$\log N_u - nR_u = n(I(\tilde{X};U|V)+\delta) - n(I(\tilde{X};U|Y,V)+2\delta) = n(I(Y;U|V)-\delta)$ を計算することにより，各ビンには $2^{n(I(Y;U|V)-\delta)}$ 個の系列が含まれる．ビン内の系列のインデックスを $l' \in [1 : 2^{n(I(Y;U|V)-\delta)}]$ とすると，一般性を損なうことがなく $l = (j_u, l')$ と表現できる．

さらに，$\mathcal{H}_n$ を $\mathcal{Q}_n$ から $\mathcal{S}_n$ へのユニバーサルハッシュ関数 [20] の集合とする．関数 $h_n : \mathcal{Q}_n \to \mathcal{S}_n$ は，$\mathcal{H}_n$ から一様に選ばれ，任意の異なる系列 $u^n(m,l) \in \mathcal{Q}_n$ と $u^n(\tilde{m},\tilde{l}) \in \mathcal{Q}_n$ に対して，$P_{H_n}\big(h_n \in \mathcal{H}_n : h_n(u^n(m,l)) = h_n(u^n(\tilde{m},\tilde{l}))\big) \le \frac{1}{|\mathcal{S}_n|}$ を満たす．ここで，P_{H_n} は $\mathcal{H}_n$ 上の一様分布である．

符号化：　符号器は各ユーザ $i \in \mathcal{I}_n$ に対して $\tilde{x}_i^n$ を観測したとき，$(v^n(m(i)), \tilde{x}_i^n) \in \mathcal{T}_{v\tilde{x}}^n$ を満たす $m(i)$ を探す．このような $m(i)$ が見つかった場合，$(v^n(m(i)), u^n(m(i),l(i)), \tilde{x}_i^n) \in \mathcal{T}_{vu\tilde{x}}^n$ を満たす $l(i)$ を探す．$(m(i),l(i))$ の組が複数見つかった場合，1 つの組をランダムに選び，ビンのインデックス $j(i) = \Big(\phi_v(\pi_v(v^n(m(i)))), \phi_u(\pi_u(u^n(m(i),l(i))))\Big)$ と秘密鍵 $s(i) = f_n(u^n(m(i),l(i)))$ を生成する．$j(i)$ はデータベース上の i の位置に保存され，$s(i)$ はユーザ i に返される．$(m(i),l(i))$ の組が見つからなかった場合，$(m(i),l(i)) = (1,1)$ を選び，$j(i) = (1,1)$，$s(i) = 1$ とする．符号化の議論において，$\tilde{x}_i^n$ を観測したときの $(v^n(m(i)), u^n(m(i),l(i)))$ の選び方を関数 $f_n : \tilde{\mathcal{X}}^n \to \mathcal{O}_n \times \mathcal{Q}_n \subset \mathcal{V}^n \times \mathcal{U}^n$ と表す．特に，片方の系列 $v^n(m(i))$，$u^n(m(i),l(i))$ に注目するとき，f_n の制限写像を $f_n^{(v)} : \tilde{\mathcal{X}}^n \to \mathcal{O}_n \subset \mathcal{V}^n$，$f_n^{(u)} : \tilde{\mathcal{X}}^n \to \mathcal{Q}_n \subset \mathcal{U}^n$ と表す．

復号化：　識別されるユーザ $w \in \mathcal{I}_n$ の観測系列 y^n とデータベース上の符号語 $\boldsymbol{j} \in \{j(1), \cdots, j(M_I)\}$ を受け取った復号器は，各 $i \in \mathcal{I}_n$ に対して

$$\begin{aligned} j(i) = \Big(\phi_v(\pi_v(v^n(m(i)))), \phi_u(\pi_u(u^n(m(i),l(i))))\Big), \\ \Big(v^n(m(i)), y^n\Big) \in \mathcal{A}_{vy}^n, \\ \Big(v^n(m(i)), u^n(m(i),l(i)), y^n\Big) \in \mathcal{A}_{vuy}^n \end{aligned} \tag{4.1}$$

を満たすユニークな $(m(i),l(i))$ の組を探す．ユニークな $(m(i),l(i))$ の組が見つかった場合，復号器はユーザと秘密鍵の推定値の組 $(\widehat{w}, \widehat{s(w)}) = \Big(i, f_n(u^n(m(i),l(i)))\Big)$ を出力す

る．ユニークな $(m(i), l(i))$ の組が見つからなかった場合，$(m(i), l(i)) = (1, 1)$ を選び，$(\widehat{w}, \widehat{s(w)}) = (1, 1)$ を出力する．復号化の議論において，y^n と $\boldsymbol{j}$ を観測したときのユニークな $(v^n(m(i)), u^n(m(i), l(i)))$ の組の選び方を関数 $g_n : \mathcal{Y}^n \times \mathcal{J}_n \to \mathcal{O}_n \times \mathcal{Q}_n \subset \mathcal{V}^n \times \mathcal{U}^n$ で表す．

実際の符号化・復号化では，集合 $\mathcal{O}_n$，$\mathcal{Q}_n$ とランダム関数 π_v，π_u，ϕ_v, ϕ_u，h_n，f_n，g_n は固定する．ランダム符号 C_n は

$$\Big\{V^n(m(i)), U^n(m(i), l(i)), \pi_v, \pi_u, \phi_v, \phi_u, h_n, f_n, g_n : \\ m(i) \in [1 : 2^{n(I(X;V)+\delta)}], l(i) \in [1 : 2^{n(I(X;U|V)+\delta)}], i \in \mathcal{I}_n\Big\} \quad (4.2)$$

の集合として定義する．

性能の評価：　ランダム符号 C_n に対して式 (3.1)–(3.6) を平均的に評価する．この解析で必要となる補題を述べる．

補題 1. (Iwata and Muramatsu)[21, Lemma 1]

$$\mathbb{E}_{C_n}[\mathbb{P}_w\{(f_n(\tilde{X}_w^n), Y^n) \notin \mathcal{A}_{vuy}^n \text{ or } (f_n(\tilde{X}_w^n), X_w^n, Z^n) \notin \mathcal{B}_{vuxz}^n\}] \\ \le 2\sqrt{\epsilon_n} + \mathbb{P}_w\{(V^n, U^n, \tilde{X}_w^n) \notin \mathcal{T}_{vu\tilde{x}}^n\} + \exp\{-2^{n\delta}\}. \quad (4.3)$$

ここで，$\epsilon_n = \mathbb{P}_w\{(V^n, U^n, Y^n) \notin \mathcal{A}_{vuy}^n \text{ or } (V^n, U^n, X_w^n, Z^n) \notin \mathcal{B}_{vuxz}^n\}$ であり，$\mathbb{E}_{C_n}$ はランダム符号 C_n を条件とした期待値である．

(証明). 証明は文献 [21] に記載されている．　□

$\mathcal{A}_{vuy}^n$，$\mathcal{B}_{vuxz}^n$，$\mathcal{T}_{vu\tilde{x}}^n$ の定義より，式 (4.3) の右辺の第 1 項目と第 2 項目は指数関数的に 0 に収束する．

補題 2. (Iwata and Muramatsu)[21] ランダム符号 C_n が与えられたときの符号器と復号器の平均的な誤り確率は

$$\mathbb{E}_{C_n}[\mathbb{P}_w\{f_n(\tilde{X}_w^n) \neq g_n(\phi_v(\pi_v(f_n^{(v)}(\tilde{X}_w^n))), \phi_u(\pi_u(f_n^{(u)}(\tilde{X}_w^n))), Y^n)\}] \\ \le 2^{-\delta n} + \mathbb{E}_{C_n}[\mathbb{P}_w(f_n(\tilde{X}_w^n), Y^n) \notin \mathcal{A}_{vuy}^n] \quad (4.4)$$

となる．

(証明). 証明は文献 [21] に記載されている．　□

補題 1 を用いると，式 (4.4) の右辺は指数関数的に 0 に収束する．

次に，秘密鍵の安全性を図る尺度として μ_n を定義する．

$$\mu_n = \sum_{z^n \in \mathcal{Z}^n} \mathbb{P}_w(Z^n = z^n) \| \mathbb{P}_w(S(w), J(w) | Z^n = z^n, C_n) - \mathbb{P}_w(\bar{S}(w)) \mathbb{P}_w(J(w) | Z^n = z^n, C_n) \|. \quad (4.5)$$

ここで，$\|P_A - P_B\|$ は P_A と P_B の変動距離を表し，$\mathbb{P}_w(\bar{S}(w))$ は $\mathcal{S}_n$ 上の一様分布を表す．また，$\mathbb{P}_w(S(w), J(w)|Z^n = z^n, C_n)$ は図 2.1 の GS-BIS モデルにおける分布を表し，$\mathbb{P}_w(\bar{S}(w))\mathbb{P}_w(J(w)|Z^n = z^n, C_n)$ は秘密鍵が一様であるシステムの分布を表す．μ_n が指数関数的に 0 に収束すれば秘密鍵の一様性と独立性が保証され，秘密鍵レートと秘密鍵漏洩の評価が可能である．

補題 3. (Watanabe and Oohama)[14, Lemma 12]

$$\mathbb{E}_{C_n}[\mu_n] \leq 2^{-n\delta} + 2\mathbb{E}_{C_n}[\mathbb{P}_w\{(f_n(\tilde{X}_w^n), X_w^n, Z^n) \notin \mathcal{B}_{vuxz}^n\}]. \tag{4.6}$$

(証明). 証明は文献 [14] に記載されている． □

補題 1 を用いると，式 (4.6) の右辺の第 2 項目は指数関数的に 0 に収束する．

補題 4. (Naito et al.)[22, Lemma 3] 条件付きエントロピー

$$H_w(S(w)|J(w), Z^n, C_n) \geq (1 - \mathbb{E}_{C_n}[\mu_n]) \log M_S + \mathbb{E}_{C_n}[\mu_n] \log \mathbb{E}_{C_n}[\mu_n] \tag{4.7}$$

が成立する．

(証明). 証明は文献 [22] に記載されている． □

補題 3 を用いると，式 (4.7) の右辺は，$\log M_S$ と限りなく近い値になる．つまり，秘密鍵はほぼ一様であり，符号語と盗聴者の観測系列とはほぼ統計的に独立になる．第 2 項目の評価では $\lim_{x\to 0} x \log x = 0$ を用いている．

補題 5. (Yachongka and Yagi) [15, Lemma 6]

$$H_w(\tilde{X}_w^n | X_w^n, f_n(\tilde{X}_w^n), C_n) \leq n(H(\tilde{X}|X, U) + 2\delta + r_n). \tag{4.8}$$

ここで，$r_n = \frac{1}{n}(1 - \log(1-\delta)) + \delta \log|\tilde{\mathcal{X}}|$ であり，$n \to \infty$ と $\delta \downarrow 0$ の下で r_n は 0 に収束する．

(証明). 証明は文献 [15] に記載されている． □

補題 6.

$$H_w(Z^n | V^n(M(w)), C_n) \leq n(H(Z|V) + 2\delta + \epsilon_n). \tag{4.9}$$

ここで，$\epsilon_n = \frac{1}{n}(1 - \log(1-\delta)) + \delta \log|\mathcal{Z}|$ であり，$n \to \infty$ と $\delta \downarrow 0$ の下で ϵ_n は 0 に収束する．

(証明). 証明は付録 B.1 に記載する． □

誤り確率の評価：誤り確率は，補題 2 より評価することができる．文献 [21] で議論されている符号化・復号化の平均的な誤り確率の評価を本論文でも用いている．誤り確率は

$$\begin{aligned}
&\mathbb{P}_w[(\widehat{W}, \widehat{S(W)}) \neq (w, S(w))] \\
&\quad \leq \mathbb{E}_{C_n}[\mathbb{P}_w\{f_n(\tilde{X}_w^n) \neq g_n(\phi_v(\pi_v(f_n^{(v)}(\tilde{X}_w^n))), \phi_u(\pi_u(f_n^{(u)}(\tilde{X}_w^n))), Y^n)\}] \\
&\quad \leq 2^{-\delta n} + \mathbb{E}_{C_n}[\mathbb{P}_w(f_n(\tilde{X}_w^n), Y^n) \notin \mathcal{A}_{vuy}^n] \qquad (4.10)
\end{aligned}$$

となる．ここで，式 (4.10) の第 2 項目は補題 1 より指数関数的に 0 に収束し，第 1 項目も指数関数的に 0 に収束することが明らかである．従って，十分に大きな n に対して

$$\mathbb{P}_w[(\widehat{W}, \widehat{S(W)}) \neq (w, S(w))] \leq \delta \qquad (4.11)$$

となる．

識別レートの評価：パラメータ設定より明らかである．

符号化レートの評価：

$$\frac{1}{n} \log |\mathcal{J}_n| = R_v + R_u = R_J. \qquad (4.12)$$

プライバシー漏洩レートの評価：十分に大きな n について

$$\begin{aligned}
I_w(X_w^n; \boldsymbol{J}, Z^n | C_n) &\overset{\text{(a)}}{\leq} I_w(X_w^n; M(w), J_u(w), Z^n | C_n) \\
&= H_w(X_w^n | C_n) - H_w(X_w^n, M(w), J_u(w), Z^n | C_n) \\
&\quad + H_w(M(w), J_u(w) | C_n) + H_w(Z^n | M(w), J_u(w), C_n) \\
&\overset{\text{(b)}}{=} -H_w(Z^n | X_w^n) - H_w(M(w), J(w) | X_w^n, Z^n, C_n) \\
&\quad + H_w(M(w), J_u(w) | C_n) + H_w(Z^n | M(w), J_u(w), C_n) \\
&= -H_w(Z^n | X_w^n) - H_w(M(w), J(w), f_n(\tilde{X}_w^n) | X_w^n, Z^n, C_n) \\
&\quad + H_w(f_n(\tilde{X}_w^n) | X_w^n, Z^n, M(w), J(w), C_n) \\
&\quad + H_w(M(w), J_u(w) | C_n) + H_w(Z^n | M(w), J_u(w), C_n) \\
&\overset{\text{(c)}}{\leq} -H_w(Z^n | X_w^n) - H_w(f_n(\tilde{X}_w^n) | X_w^n, Z^n, C_n) \\
&\quad + H_w(M(w), J_u(w) | C_n) + H_w(Z^n | M(w), J_u(w), C_n) + n\delta_n \\
&\overset{\text{(d)}}{\leq} -H_w(Z^n | X_w^n) - H_w(f_n(\tilde{X}_w^n) | X_w^n, C_n) \\
&\quad + H_w(M(w) | C_n) + H_w(J_u(w) | C_n) + H_w(Z^n | V^n(M(w)), C_n) + n\delta_n \\
&\overset{\text{(e)}}{\leq} -H_w(Z^n | X_w^n) - n(H(U|X) - H(U|\tilde{X}) - 2\delta - r_n) \\
&\quad + H_w(M(w) | C_n) + H_w(J_u(w) | C_n) + n(H(Z|V) + \epsilon_n + 2\delta) + n\delta_n
\end{aligned}$$

$$
\begin{aligned}
&\overset{(f)}{\leq} n(-H(Z|X) + H(U|\tilde{X}) - H(U|X) + I(\tilde{X};V) \\
&\quad + I(\tilde{X};U|V,Y) + H(Z|V) + r_n + \delta_n + \epsilon_n + 7\delta) \\
&\overset{(g)}{\leq} n(-H(Z|X) + H(U|\tilde{X}) - H(U|X) + I(\tilde{X};V) \\
&\quad + I(\tilde{X};U|V) - I(Y;U|V) + H(Z|V) + 8\delta) \\
&\overset{(h)}{=} n(I(\tilde{X};U) + H(U|\tilde{X}) - H(U|X) - I(Y;U|V) + I(X;Z|V) + 8\delta) \\
&= n(I(X;U) - I(Y;U|V) + I(X;Z|V) + 8\delta) \\
&\overset{(i)}{=} n(I(X;U,Y) - I(X;Y|V) + I(X;Z|V) + 8\delta) \\
&= n(R_L + \delta)
\end{aligned} \tag{4.13}
$$

が成立する．(a) は生成した系列とビンの関係より成立する．(b) は (Z^n, X_w^n) と C_n が独立であるため成立する．(c) はある $\delta_n \downarrow 0$ $(n \to \infty)$ を用いたファノの不等式

$$
\begin{aligned}
H_w(f_n(\tilde{X}_w^n)|X_w^n, Z^n, M(w), J(w), C_n) &\leq H_w(f_n(\tilde{X}_w^n)|X_w^n, J(w), Y^n, C_n) \\
&\leq n\delta_n
\end{aligned} \tag{4.14}
$$

より成立する．ただし，マルコフ連鎖 $f_n(\tilde{X}_w^n) - (X_w^n, J(w), C_n) - Y^n$ を用いている．(d) はマルコフ連鎖 $f_n(\tilde{X}_w^n) - (X^n, C_n) - Z^n$ に加えて，$V^n(M(w))$ は $M(w)$ の関数であるため成立する．(e) は補題 6 と

$$
\begin{aligned}
H_w(f_n(\tilde{X}_w^n)|X_w^n, C_n) &\geq I_w(f_n(\tilde{X}_w^n); \tilde{X}_w^n|X_w^n, C_n) \\
&\geq H_w(\tilde{X}_w^n|X_w^n) - H_w(\tilde{X}_w^n|X_w^n, f_n(\tilde{X}_w^n), C_n) \\
&\overset{(j)}{\geq} n(H(\tilde{X}|X) - H(\tilde{X}|X,U) - 2\delta - r_n) \\
&\overset{(k)}{=} n(H(U|X) - H(U|\tilde{X}) - 2\delta - r_n)
\end{aligned} \tag{4.15}
$$

より成立する．(f) は $M(w) \in [1 : 2^{n(I(\tilde{X};V)+\delta)}]$ と $J_u(w) \in [1 : 2^{n(I(\tilde{X};U|Y,V)+2\delta)}]$ より成立する．(g) はマルコフ連鎖 $V - U - \tilde{X} - Y$ より成立する．(h) はマルコフ連鎖 $V - U - \tilde{X} - X - Z$ より成立する．(i) はマルコフ連鎖 $V - U - X - Y$ より成立する．(j) は補題 5 より成立する．(k) はマルコフ連鎖 $U - \tilde{X} - X$ より成立する．

秘密鍵漏洩の評価：十分に大きな n について

$$
\begin{aligned}
I_w(S(w); \boldsymbol{J}, Z^n|C_n) &= H_w(S(w)|C_n) - H_w(S(w)|J(w), Z^n, C_n) \\
&\leq \log M_S - H_w(S(w)|J(w), Z^n, C_n) \\
&\overset{(a)}{\leq} \log M_S - (1 - \mathbb{E}_{C_n}[\mu_n]) \log M_S + \mathbb{E}_{C_n}[\mu_n] \log \mathbb{E}_{C_n}[\mu_n] \\
&= \mathbb{E}_{C_n}[\mu_n](\log M_S - \log \mathbb{E}_{C_n}[\mu_n]) \\
&\overset{(b)}{\leq} \delta
\end{aligned} \tag{4.16}
$$

が成立する．(a) は補題 4 より成立する．(b) は補題 3 より成立する．

秘密鍵レートの評価：十分に大きな n について

$$\begin{aligned} H_w(S(w)|C_n) &\geq H_w(S(w)|J(w), Z^n, C_n) \\ &\overset{\text{(a)}}{\geq} (1 - \mathbb{E}_{C_n}[\mu_n]) \log M_S + \mathbb{E}_{C_n}[\mu_n] \log \mathbb{E}_{C_n}[\mu_n] \\ &= nR_S(1 - \mathbb{E}_{C_n}[\mu_n]) + \mathbb{E}_{C_n}[\mu_n] \log \mathbb{E}_{C_n}[\mu_n] \\ &= n(R_S - \mathbb{E}_{C_n}[\mu_n](R_S - \frac{1}{n} \log \mathbb{E}_{C_n}[\mu_n])) \\ &\overset{\text{(b)}}{\geq} n(R_S - \delta) \end{aligned} \tag{4.17}$$

が成立する．(a) は補題 4 より成立する．(b) は補題 3 より成立する．

最後に，selection lemma [23, Lemma 2.2] より，定義 1 の全ての条件を満たす良い符号が少なくとも 1 つ存在する．□

4.1.2　CS-BIS モデル

CS-BIS モデルの順定理の証明では，$\mathcal{R}_{\mathcal{C}} \supseteq \mathcal{A}_{\mathcal{C}}$ を示す．このモデルの証明は，GS-BIS モデルの順定理の証明とほとんど同様であるが，符号器・復号器の設定が異なる．one-time pad 操作で秘密鍵を隠して安全に伝送する動作を追加している．ここでは，図 4.1 のように CS-BIS モデルの符号器・復号器の内部に GS-BIS モデルの符号器・復号器をコンポーネントとして組み込んで議論する．(j_G, s_G) と (j_C, s_C) をそれぞれ GS-BIS モデルと CS-BIS モデルの符号語と秘密鍵の組を表す．また，$\oplus$ と $\ominus$ をそれぞれ $|\mathcal{S}_n|$ の加算と減算モジュールを表す．

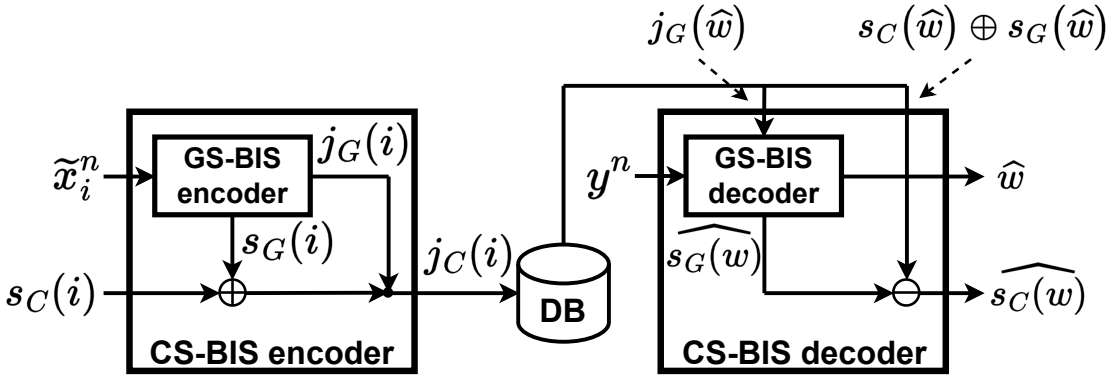

図 4.1: CS-BIS モデルの符号器・復号器

符号化：CS-BIS モデルの符号器は，各ユーザ $i \in \mathcal{I}_n$ に対して $\tilde{x}_i^n$ と $s_C(i)$ を観測したとき，コンポーネントから共有された $s_G(i)$ を用いて $s_C(i) \oplus s_G(i)$ として $s_C(i)$ を隠す．この情報は $j_G(i)$ と統合され，$j_C(i) = (j_G(i), s_C(i) \oplus s_G(i))$ が生成される．$j_C(i)$ はデータベースの i の位置に保存される．

復号化：GS-BIS モデルの復号器はデータベース上の全ての符号語 $\{j_C(1), \cdots, j_C(M_I)\}$ にアクセスできる (CS-BIS モデルの復号器も同様に行える)．なお，$j_C(w) = (j_G(w), s_C(w) \oplus s_G(w))$ の前半部分はコンポーネントで GS-BIS モデルの推定値を出力し，後半部分は減算して CS-BIS モデルの秘密鍵の推定値を出力する用途で使われる．識別されるユーザ $w \in \mathcal{I}_n$ の観測系列 y^n とデータベース上の全ての符号語 $\{j_C(1), \cdots, j_C(M_I)\}$ を受け取った CS-BIS モデルの復号器は，コンポーネントから $\widehat{w}$ と $\widehat{s_G(w)}$ の組を出力する．次に，この情報を用いて $\widehat{w}$ と

$$\widehat{s_C(w)} = s_C(\widehat{w}) \oplus s_G(\widehat{w}) \ominus \widehat{s_G(w)} \tag{4.18}$$

の組を出力する．

性能の評価：

誤り確率の評価：CS-BIS モデルの誤り事象は以下の 2 つの事象の和集合に一致する．

$$\begin{aligned} &\text{(i) } A_w : \widehat{W} \neq w, \\ &\text{(ii) } B_w : \widehat{W} = w,\ \widehat{S_C(w)} \neq S_C(w). \end{aligned} \tag{4.19}$$

これらの事象を用いて式 (3.1) を評価すると以下のようになる．

$$\begin{aligned} \mathbb{P}_w[(\widehat{W}, \widehat{S_C(w)}) \neq (w, s_C(w))] &= \mathbb{P}_w[A_w \cup B_w] \\ &= \mathbb{P}_w[A_w] + \mathbb{P}_w[A_w^C \cap B_w]. \end{aligned} \tag{4.20}$$

式 (4.20) の第 1 項目は GS-BIS モデルと同様に評価できる．第 2 項目は

$$\mathbb{P}_w[A_w^C \cap B_w] = \mathbb{P}_w[\widehat{W} = w,\ \widehat{S_C(w)} \neq S_C(w)] \tag{4.21}$$

と表せる．ここで $\widehat{W} = w$ とすると，式 (4.18) は

$$\widehat{s_C(w)} = s_C(w) \oplus s_G(w) \ominus \widehat{s_G(w)} \tag{4.22}$$

となる．従って，

$$\widehat{s_C(w)} = s_C(w) \quad \Leftrightarrow \quad \widehat{s_G(w)} = s_G(w) \tag{4.23}$$

となり，式 (4.20) の第 2 項目も GS-BIS モデルと同様に評価できる．ここまでの議論より

$$\mathbb{P}_w[(\widehat{W}, \widehat{S_C(w)}) \neq (w, s_C(w))] = \mathbb{P}_w[(\widehat{W}, \widehat{S_G(w)}) \neq (w, s_G(w))] \tag{4.24}$$

となる．従って，GS-BIS モデルと同様に，CS-BIS モデルの誤り確率も補題 2 を用いて評価できる．

識別レート，秘密鍵レートの評価：CS-BIS モデルでは，秘密鍵の分布が一様であるためパラメータ設定より明らかである．

符号化レートの評価：

$$\begin{aligned} R_J &\leq \frac{1}{n}\log M_J + \frac{1}{n}\log M_S \\ &= R_I + I(\tilde{X};U|Y) + I(Y;U|V) - I(Z;U|V) + 2\delta. \end{aligned} \tag{4.25}$$

プライバシー漏洩レートの評価：文献 [15] より，十分に大きな n に対して

$$I_w(X_w^n; J_C(w), Z^n|C_n) \leq I_w(X_w^n; J_G(w), Z^n|C_n) \tag{4.26}$$

が成立する．従って，式 (4.13) と (4.26) より

$$I_w(X_w^n; J_C(w), Z^n|C_n) \leq n(R_L + \delta) \tag{4.27}$$

が成立する．

秘密鍵漏洩の評価：文献 [15] より，十分に大きな n に対して

$$I_w(S_C(w); J_C(w), Z^n|C_n) \leq \log M_S - H_w(S_G(w)|C_n) + I_w(S_G(w); J_G(w), Z^n|C_n) \tag{4.28}$$

が成立する．従って，式 (4.16)，(4.17) および (4.28) より

$$I_w(S_C(w); J_C(w), Z^n|C_n) \leq 2\delta \tag{4.29}$$

が成立する．

最後に，selection lemma [23, Lemma 2.2] より，定義 2 の全ての条件を満たす良い符号が少なくとも 1 つ存在する．　□

4.2　逆定理の証明

4.2.1　GS-BIS モデル

GS-BIS モデルの逆定理の証明では，$\mathcal{R}_{\mathcal{G}} \subseteq \mathcal{A}_{\mathcal{G}}$ を示す．まずは，識別されるユーザの確率変数 W が $\mathcal{I}_n = [1 : M_I]$ 上に一様に分布すると仮定する．また，式 (3.1)，(3.4)–(3.6) の左辺を平均化して得られる式 (4.30)–(4.33) に置き換える．

$$\Pr[(\widehat{W}, \widehat{S(W)}) \neq (W, S(W))] \leq \delta, \tag{4.30}$$

$$I(X_W^n; \boldsymbol{J}, Z^n|W) \leq n(R_L + \delta), \tag{4.31}$$

$$I(S(W); \boldsymbol{J}, Z^n|W) \leq \delta, \tag{4.32}$$

$$H(S(W)|W) \geq n(R_S - \delta). \tag{4.33}$$

ここで，任意の $\delta > 0$ と十分に大きな系列長 n に対して，定義 1 の式 (3.2)，(3.3) に加えて，式 (4.30)–(4.33) を満たす符号器 f と復号器 g のペアが存在し，GS-BIS モデルにおける (R_I, R_J, R_L, R_S) のレート組が達成可能であるとする．これは，定義 1 の制約式を緩和したものであり，容量域 $\mathcal{R}_G$ よりも大きくなる．逆定理の証明では，従来の容量域 $\mathcal{R}_G$ と緩和された容量域の外界は一致することを示す．

次に，$t \in [1 : n]$ に対して，2 つの補助確率変数 $V_t = (J(W), Y_{t+1}^n, Z^{t-1})$ と $U_t = (J(W), S(W), Y_{t+1}^n, Z^{t-1})$ を定義する．また，新しい表記 $X_W^n = (X_1(W), \cdots, X_n(W))$，$\tilde{X}_W^n = (\tilde{X}_1(W), \cdots, \tilde{X}_n(W))$，$\boldsymbol{J}^{\setminus W} = (J(1), \cdots, J(W-1), J(W+1), \cdots, J(M_I))$ を定義する．この設定では，マルコフ連鎖 $U_t - V_t - \tilde{X}_t(W) - X_t(W) - (Y_t, Z_t)$ を満たすことは簡単に確認できる．

逆定理の証明では，以下の補題を使用する．

補題 7. ファノの不等式

$$H(W, S(W)|\boldsymbol{J}, Y^n) \leq n\gamma_n \tag{4.34}$$

が成立する．ただし，$\{\gamma_n > 0\}_{n=1}^{\infty}$ は十分に大きな n に対して 0 に収束するある数列とする．

(証明). 証明は [17] に記載されている． □

識別レートの評価： 式 (3.2) より

$$\begin{aligned}
n(R_I - \delta) &\leq \log M_I = H(W) \\
&= H(W|\boldsymbol{J}, Y^n) + I(W; \boldsymbol{J}, Y^n) \\
&\leq H(S(W), W|\boldsymbol{J}, Y^n) + I(W; \boldsymbol{J}, Y^n) \\
&\overset{\text{(a)}}{\leq} n\gamma_n + I(W; Y^n|\boldsymbol{J}) \\
&\leq H(Y^n) - H(Y^n|W, \boldsymbol{J}) + n\gamma_n \\
&\overset{\text{(b)}}{=} H(Y^n) - H(Y^n|J(W)) + n\gamma_n \qquad (4.35) \\
&= \sum_{t=1}^{n} \{H(Y_t) - H(Y_t|J(W), Y_{t+1}^n)\} + n\gamma_n \\
&\leq \sum_{t=1}^{n} \{H(Y_t) - H(Y_t|J(W), Y_{t+1}^n, Z^{t-1})\} + n\gamma_n \\
&= \sum_{t=1}^{n} I(Y_t; V_t) + n\gamma_n \qquad (4.36)
\end{aligned}$$

が成立する．(a) は補題 7 に加えて，W と $\boldsymbol{J}$ が独立であるため成立する．(b) は Y^n と $\boldsymbol{J}^{\setminus W}$ が独立であるため成立する．

符号化レートの評価：式 (3.2) と (3.3) より

$$
\begin{aligned}
n(R_J - R_I + 2\delta) \geq & \log M_J - \log M_I \geq H(J(W)) - H(W) \\
\overset{\text{(a)}}{\geq} & H(J(W)) - I(Y^n; J(W)) - n\gamma_n \\
= & - H(J(W)|\tilde{X}_W^n) + H(J(W)|Y^n) + H(J(W)|\tilde{X}_W^n) - n\gamma_n \\
\overset{\text{(b)}}{=} & - H(J(W)|\tilde{X}_W^n, Y^n, Z^n, \boldsymbol{J}^{\setminus W}) \\
& + H(J(W)|W, \boldsymbol{J}^{\setminus W}, Y^n) + H(J(W)|\tilde{X}_W^n) - n\gamma_n \\
= & - H(J(W), S(W)|\tilde{X}_W^n, Y^n, Z^n, \boldsymbol{J}^{\setminus W}) + H(S(W)|\tilde{X}_W^n, Y^n, Z^n, \boldsymbol{J}) \\
& + H(J(W), S(W)|W, \boldsymbol{J}^{\setminus W}, Y^n) - H(S(W)|W, \boldsymbol{J}, Y^n) \\
& + H(J(W)|\tilde{X}_W^n) - n\gamma_n \\
= & - H(J(W), S(W)|\tilde{X}_W^n, Y^n, Z^n, \boldsymbol{J}^{\setminus W}) + H(S(W)|\tilde{X}_W^n, Y^n, Z^n, \boldsymbol{J}) \\
& + H(J(W), S(W)|\boldsymbol{J}^{\setminus W}, Y^n) - H(S(W)|W, \boldsymbol{J}, Y^n) \\
& + H(J(W)|\tilde{X}_W^n) - n\gamma_n \\
= & I(J(W), S(W); \tilde{X}_W^n, Z^n|\boldsymbol{J}^{\setminus W}, Y^n) + H(S(W)|\tilde{X}_W^n, Y^n, Z^n, \boldsymbol{J}) \\
& - H(S(W)|W, \boldsymbol{J}, Y^n) + H(J(W)|\tilde{X}_W^n) - n\gamma_n
\end{aligned} \tag{4.37}
$$

が成立する．(a) は式 (4.35) より成立する．(b) はマルコフ連鎖 $J(W) - \tilde{X}_W^n - (Y^n, Z^n, \boldsymbol{J}^{\setminus W})$ と $J(W) - Y^n - (W, \boldsymbol{J}^{\setminus W})$ より成立する．さらに，式 (4.37) の第 1 項目について

$$
\begin{aligned}
& I(J(W), S(W); \tilde{X}_W^n, Z^n|\boldsymbol{J}^{\setminus W}, Y^n) \\
& = H(\tilde{X}_W^n, Z^n|\boldsymbol{J}^{\setminus W}, Y^n) - H(\tilde{X}_W^n, Z^n|J(W), S(W), \boldsymbol{J}^{\setminus W}, Y^n) \\
& \overset{\text{(c)}}{=} H(\tilde{X}_W^n, Z^n|Y^n) - H(\tilde{X}_W^n, Z^n|J(W), S(W), \boldsymbol{J}^{\setminus W}, Y^n) \\
& = H(\tilde{X}_W^n) + H(Y^n, Z^n|\tilde{X}_W^n) - H(Y^n) - H(\tilde{X}_W^n, Z^n|J(W), S(W), \boldsymbol{J}^{\setminus W}, Y^n) \\
& \geq \sum_{t=1}^{n} \{H(\tilde{X}_t(W)) + H(Y_t, Z_t|\tilde{X}_t(W)) - H(Y_t) \\
& \quad - H(\tilde{X}_t(W), Z_t|J(W), S(W), Y_{t+1}^n, Z^{t-1}, Y_t)\} \\
& = \sum_{t=1}^{n} I(\tilde{X}_t(W), Z_t; J(W), S(W), Y_{t+1}^n, Z^{t-1}|Y_t) \\
& = \sum_{t=1}^{n} I(\tilde{X}_t(W); U_t|Y_t)
\end{aligned} \tag{4.38}
$$

が成立する．(c) はマルコフ連鎖 $(\tilde{X}_W^n, Z^n) - Y^n - \boldsymbol{J}^{\setminus W}$ より成立する．式 (4.37) の第 3 項目に補題 7 を用いると

$$
H(S(W)|W, \boldsymbol{J}, Y^n) \leq H(W, S(W)|\boldsymbol{J}, Y^n) \leq n\gamma_n \tag{4.39}
$$

が成立する．従って，式 (4.37)–(4.39) より

$$n(R_J - R_I + 2\delta) \geq \sum_{t=1}^{n} I(\tilde{X}_t(W); U_t|Y_t) - 2n\gamma_n \tag{4.40}$$

が成立する．

プライバシー漏洩レートの評価：式 (4.31) より

$$\begin{aligned}
n(R_L+\delta) \geq & I(X_W^n; \boldsymbol{J}, Z^n|W) \\
\overset{(a)}{=} & I(X_W^n; W, \boldsymbol{J}, Z^n) \\
= & I(X_W^n; W, \boldsymbol{J}, S(W), Y^n) - I(X_W^n; S(W)|W, \boldsymbol{J}, Y^n) \\
& - I(X_W^n; Y^n|W, \boldsymbol{J}) + I(X_W^n; Z^n|W, \boldsymbol{J}) \\
= & I(X_W^n; W, \boldsymbol{J}, S(W), Y^n) - H(S(W)|W, \boldsymbol{J}, Y^n) + H(S(W)|W, \boldsymbol{J}, Y^n, X_W^n) \\
& - I(X_W^n; Y^n|W, \boldsymbol{J}) + I(X_W^n; Z^n|W, \boldsymbol{J}) \\
\overset{(b)}{\geq} & I(X_W^n; W, \boldsymbol{J}, S(W), Y^n) - n\gamma_n - I(X_W^n; Y^n|W, \boldsymbol{J}) + I(X_W^n; Z^n|W, \boldsymbol{J}) \\
= & I(X_W^n; W, J(W), S(W), Y^n) - H(Y^n|J(W)) + H(Y^n|X_W^n, J(W)) \\
& + H(Z^n|J(W)) - H(Z^n|X_W^n, J(W)) - n\gamma_n \\
\overset{(c)}{=} & I(X_W^n; W, J(W), S(W), Y^n) - H(Y^n|J(W)) + H(Y^n|X_W^n) \\
& + H(Z^n|J(W)) - H(Z^n|X_W^n) - n\gamma_n \\
= & H(X_W^n) - H(X_W^n|W, J(W), S(W), Y^n) - I(X_W^n; Y^n) + I(Y^n; J(W)) \\
& + I(X_W^n; Z^n) - I(Z^n; J(W)) - n\gamma_n \\
\overset{(d)}{\geq} & \sum_{t=1}^{n} \{H(X_t(W)) - H(X_t(W)|W, J(W), S(W), X_W^{t-1}, Y^n, Z^{t-1}) \\
& - I(X_t(W); Y_t) + I(Y_t; J(W), Y_{t+1}^n) \\
& + I(X_t(W); Z_t) - I(Z_t; J(W), Z^{t-1})\} - n\gamma_n \\
\overset{(e)}{\geq} & \sum_{t=1}^{n} \{I(X_t(W); J(W), S(W), Y_t^n, Z^{t-1}) - I(X_t(W); Y_t) + I(X_t(W); Z_t) \\
& + I(Y_t; J(W), Z^{t-1}, Y_{t+1}^n) - I(Z_t; J(W), Z^{t-1}, Y_{t+1}^n)\} - n\gamma_n \\
\overset{(f)}{=} & \sum_{t=1}^{n} \{I(X_t(W); U_t, Y_t) - I(X_t(W); Y_t|V_t) + I(X_t(W); Z_t|V_t)\} - n\gamma_n
\end{aligned} \tag{4.41}$$

が成立する．(a) は W と他の確率変数が独立であるため成立する．(b) は式 (4.39) より成立する．(c) はマルコフ連鎖 $(Y^n, Z^n) - X_W^n - J(W)$ より成立する．(d) はマルコフ連鎖 $Z^{t-1} - (J(W), S(W), X_W^{t-1}, Y^n) - X_t(W)$ より成立する．(e) は Csiszár's sum identify [18]

より $\sum_{t=1}^{n} I(Y_t; Z^{t-1}|J(W), Y_{t+1}^n) = \sum_{t=1}^{n} I(Z_t; Y_{t+1}^n|J(W), Z^{t-1})$ となるので成立する．(f) は，マルコフ連鎖 $V_t - X_t(W) - (Y_t, Z_t)$ より成立する．

秘密鍵レートの評価：式 (4.33) より

$$
\begin{aligned}
n(R_S - \delta) \leq & H(S(W)|W) \\
= & H(S(W)|W, \boldsymbol{J}, Z^n) + I(S(W); \boldsymbol{J}, Z^n|W) \\
\overset{\text{(a)}}{\leq} & H(S(W)|W, \boldsymbol{J}, Z^n) + \delta \\
\overset{\text{(b)}}{\leq} & H(S(W)|W, \boldsymbol{J}, Z^n) - H(S(W)|W, \boldsymbol{J}, Y^n) + \delta + n\gamma_n \\
= & H(S(W)|J(W), Z^n) - H(S(W)|J(W), Y^n) + \delta + n\gamma_n \\
= & I(S(W); Y^n|J(W)) - I(S(W); Z^n|J(W)) + \delta + n\gamma_n \\
= & \sum_{t=1}^{n} \{I(S(W); Y_t|J(W), Y_{t+1}^n) - I(S(W); Z_t|J(W), Z^{t-1})\} + \delta + n\gamma_n \\
\overset{\text{(c)}}{=} & \sum_{t=1}^{n} \{I(S(W); Y_t|J(W), Y_{t+1}^n, Z^{t-1}) - I(S(W); Z_t|J(W), Y_{t+1}^n, Z^{t-1})\} \\
& + \delta + n\gamma_n \qquad (4.42) \\
= & \sum_{t=1}^{n} \{I(U_t; Y_t|V_t) - I(U_t; Z_t|V_t)\} + \delta + n\gamma_n \qquad (4.43)
\end{aligned}
$$

が成立する．(a) は式 (4.32) より成立する．(b) は式 (4.39) より成立する．(c) は Csiszár's sum identify [18] より成立する．証明は付録 B.2 に記載する．

集合 $\mathcal{V}$，$\mathcal{U}$ の cardinality bounds は support lemma [18, Appendix C] を使うことにより $|\mathcal{V}| \leq |\mathcal{X}| + 5$，$|\mathcal{U}| \leq (|\mathcal{X}| + 5)(|\mathcal{X}| + 3)$ を証明できる．

最後に，式 (4.36)，(4.40)，(4.41) および (4.43) に対して time-sharing の議論 [17] を適用し，$n \to \infty$ と $\delta \to 0$ に漸近させることにより式 (3.8) が示される．　□

4.2.2　CS-BIS モデル

CS-BIS モデルの逆定理の証明では，$\mathcal{R}_{\mathcal{C}} \subseteq \mathcal{A}_{\mathcal{C}}$ を示す．ただし，大まかな流れは GS-BIS モデルと同様である．本項では，符号化レートの評価のみ記載する．

符号化レートの評価：式 (4.37) の第 2–4 項目について

$$
\begin{aligned}
& H(S(W)|\tilde{X}_W^n, Y^n, Z^n, \boldsymbol{J}) - H(S(W)|W, \boldsymbol{J}, Y^n) + H(J(W)|\tilde{X}_W^n) \\
& \quad \overset{\text{(a)}}{=} H(S(W)|\tilde{X}_W^n, J(W)) - H(S(W)|W, \boldsymbol{J}, Y^n) \\
& \qquad + I(S(W); J(W)|\tilde{X}_W^n) + H(J(W)|S(W), \tilde{X}_W^n)
\end{aligned}
$$

$$
\begin{aligned}
&\overset{\text{(b)}}{=} H(S(W)|\tilde{X}_W^n, J(W)) - H(S(W)|W, \boldsymbol{J}, Y^n) \\
&\quad + H(S(W)) - H(S(W)|\tilde{X}_W^n, J(W)) \\
&= - H(S(W)|W, \boldsymbol{J}, Y^n) + H(S(W)) \\
&= H(S(W)) - H(S(W)|J(W), Y^n) \\
&\geq H(S(W)|J(W), Z^n) - H(S(W)|J(W), Y^n) \\
&= I(S(W); Y^n|J(W)) - I(S(W); Z^n|J(W)) \\
&= \sum_{t=1}^{n} \{I(S(W); Y_t|J(W), Y_{t+1}^n) - I(S(W); Z_t|J(W), Z^{t-1})\} \\
&\overset{\text{(c)}}{=} \sum_{t=1}^{n} \{I(S(W); Y_t|J(W), Y_{t+1}^n, Z^{t-1}) - I(S(W); Z_t|J(W), Y_{t+1}^n, Z^{t-1})\} \\
&= \sum_{t=1}^{n} \{I(U_t; Y_t|V_t) - I(U_t; Z_t|V_t)\} \qquad (4.44)
\end{aligned}
$$

が成立する．(a) はマルコフ連鎖 $S(W) - (J(W), \tilde{X}_W^n) - (Y^n, Z^n)$ より成立する．(b) は $S(W)$ と $\tilde{X}_W^n$ が独立であることに加えて，$J(W)$ と $(S(W), \tilde{X}_W^n)$ が関数の関係であるため成立する．(c) は式 (4.42) より成立する．式 (4.37)，(4.38) および (4.44) より

$$
n(R_J - R_I + 2\delta) \geq \sum_{t=1}^{n} \{I(\tilde{X}_t(W); U_t|Y_t) + I(U_t; Y_t|V_t) - I(U_t; Z_t|V_t)\} - n\gamma_n \qquad (4.45)
$$

が成立する．

最後に，式 (4.36)，(4.45)，(4.41) および (4.43) に対して time-sharing の議論 [17] を適用し，$n \to \infty$ と $\delta \to 0$ に漸近させることにより式 (3.9) が示される．　□

第 5 章

まとめと今後の課題

本論文では，強安全性基準に基づく受動的盗聴者が存在する BIS の容量域を明らかにした．その結果，GS-BIS モデルの容量域が CS-BIS モデルの容量域よりも大きく，符号化レート R_J の下限が秘密鍵レート R_S の最大値分だけ差があるということが分かった．また，強安全性基準と弱安全性基準の数学的な表現が一致することが分かった．計算例からは各レート組にトレードオフ関係があることが分かった．

本論文で解析した強安全性基準に基づくシステムは，従来の研究（弱安全性基準）に比べて秘密鍵の漏洩が系列長に対して線形的に増加しないことから，高い安全性を保障するため有用である．しかし，生体情報系列の漏洩は系列長に依存するという問題がある．今後の課題として，文献 [26] の考え方を取り入れたプライバシー漏洩の強安全性が挙げられる．この文献ではシステムに対して秘密鍵の他にプライベート鍵が導入されている．プライベート鍵は符号器・復号器に事前に共有するため，符号化・復号化の際に補助的な役割をするものである．そのため，従来のプライバシー漏洩レートは $n\delta$ 以下になるという制約式に置き換わり，新たにプライベート鍵レートが加わっている．この考え方に基づいて，図 2.1 のシステムに対してプライベート鍵を導入し，プライバシー漏洩を δ 以下に抑えることが今後の課題である．また，ガウス情報源に対する容量域の解析も今後の課題の一つである．

参考文献

[1] A. K. Jain, P. Flynn, and A. Ross, *Handbook of Biometrics*, New York, Springer-Verlag, 2009.

[2] F. M. J. Willems, T. Kalker, S. Baggen, and J. P. Linnartz, "On the capacity of a biometrical identification system," *in Proc. IEEE Int. Symp. Inf. Theory*, Yokohama, Japan, p. 82, Jun./Jul. 2003.

[3] E. Tuncel, "Capacity/storage tradeoff in high-dimensional identification systems," *IEEE Trans. Inf. Theory*, vol. 55, no. 5, pp. 2097–2106, May 2009.

[4] T. Ignatenko and F. M. J. Willems, "Fundamental limits for privacy-preserving biometric identification systems that support authentication," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5583–5594, Oct. 2015.

[5] V. Yachongka and H. Yagi, "Identification, secrecy, template, and privacy-leakage of biometric identification system under noisy enrollment," *arXiv: 1902.01663*, Feb. 2019.

[6] V. Yachongka and H. Yagi, "A new characterization of the capacity region of identification systems under noisy enrollment," *in Proc. 54th Annu. Conf. Inf. Sci. Syst.*, Princeton, NJ, Mar. 2020.

[7] V. Yachongka and H. Yagi, "Fundamental limits of biometric identification system under noisy enrollment," *IEICE Trans. Fundamentals*, vol. E104-A(1), no. 1, pp. 283–294, Jan. 2021.

[8] V. Yachongka, H. Yagi and Y. Oohama, "Biometric identification systems with noisy enrollment for Gaussian source," *in Proc. IEEE Inf. Theory Workshop*, Riva del Garda, Italy, 2021, pp. 1–5.

[9] V. Yachongka, H. Yagi and Y. Oohama, "Biometric identification systems with noisy enrollment for Gaussian sources and channels," *Entropy*, vol. 23, no. 1049, Aug. 2021.

[10] M. Koide and H. Yamamoto, "Coding theorems for biometric systems," *in Proc. IEEE Int. Symp. Inf. Theory*, Texas, USA, pp. 2647–2651, Jun. 2010.

[11] K. Kittichokechai and G. Caire, "Secret key-based identification and authentication with a privacy constraint," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6189–6203, Nov. 2016.

[12] 小柳 翔吾, ヤチョンカ ワムア, 八木 秀樹, "登録雑音と受動的盗聴者が存在する生体識別システム," 第 45 回情報理論とその応用シンポジウム（SITA2022）予稿集, Dec. 2022.

[13] T.S. Han, *Information-Spectrum Methods in Information Theory,* Springer, 2003.

[14] S. Watanabe and Y. Oohama, "Secret key agreement from correlated Gaussian sources by rate limited public communication," *IEICE Trans. Fundamentals*, vol. E93-A, no. 11, Nov. 2010.

[15] V. Yachongka, H. Yagi, and H. Ochiai, “Secret-key agreement using physical identifiers for degraded and less noisy authentication channels,” *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 5316–5331, Aug. 2022.

[16] V. Yachongka, H. Yagi and Y. Oohama, “Secret key-based authentication with passive eavesdropper for scalar Gaussian sources,” *in Proc. IEEE Int. Symp. Inf. Theory*, Espoo, Finland, 2022, pp. 2666-2671.

[17] T. M. Cover and J. A. Thomas, *Elements of Information Theory, 2nd ed.*, John Wiley & Sons, New Jersy, 2006.

[18] A. El Gamal and Y.-H. Kim, *Network Information Theory*, Cambridge, U.K.: Cambridge Univ. Press, 2011.

[19] A. Wyner and J. Ziv, “A theorem on the entropy of certain binary sequences and applications-I,” *IEEE Trans. Inf. Theory*, vol. 19, no. 6, pp. 769–772, Nov. 1973.

[20] J.L. Carter and M.N. Wegman, “Universal classes of hash functions,” *J. Comput. Syst. Sci.*, vol. 18, pp. 143-154, 1979.

[21] I. Iwata and J. Muramatsu, “An information-spectrum approach to rate-distortion function with side information,” *IEICE Trans. Fundamentals,* vol. E85-A, no. 6, pp. 1387-1395, Jun. 2002.

[22] M. Naito, S. Watanabe, R. Matsumoto, and T. Uyematsu, “Secret key agreement by soft-decision of signals in Gaussian Maurer’s model,” *IEICE Trans. Fundamentals*, vol. E92-A, no. 2, pp. 525-534, Feb. 2008.

[23] M. Bloch and J. Barros, *Phisical-Layer Security*, Cambridge, U.K.: Cambridge Univ. Press, 2011.

[24] O. Günlü, K. Kittichokechai, R. F. Schaefer, and G. Caire, “Controllable identifier measurements for private authentication with secret keys,” *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 8, pp. 1945-1959, Aug. 2018.

[25] T. Ignatenko and F. M. J. Willems, “Biometric systems: privacy and secrecy aspects,” *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 4, pp. 956-973, Dec. 2009.

[26] L. Zhou, M. T. Vu, T. J. Oechtering and M. Skoglund, ”Privacy-preserving identification systems with noisy enrollment,” *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 3510-3523, 2021.

発表実績

1. 小柳 翔吾, ヤチョンカ ワムア, 八木 秀樹, “登録雑音と受動的盗聴者が存在する生体識別システム,” 第 45 回情報理論とその応用シンポジウム（SITA2022）予稿集, Dec. 2022.
2. 小柳 翔吾, ヤチョンカ ワムア, 八木 秀樹, “強安全性基準に基づく受動的盗聴者が存在する生体識別システム,” 第 46 回情報理論とその応用シンポジウム（SITA2023）予稿集, Nov. 2023.

謝辞

最後に本研究を行うにあたり，お忙しい中ご指導頂いた八木秀樹准教授に心より感謝申し上げます．また，ゼミなどでお世話になりました大濱靖匡教授，Santoso Bagus 准教授，そして研究室の皆様にも心より感謝いたします．

付 録A

定理2の証明

A.1 順定理の証明

順定理の証明では，マルコフ連鎖$V-U-\tilde{X}-X-Y-Z$と$H(X)=H(Y)=H(Z)=1$の関係を用いると，式 (3.8) における (R_I, R_J, R_L, R_S) の組の制約式は以下のように展開できる．

$$
\begin{aligned}
R_I &\le I(Y;V) = 1 - H(Y|V) && \text{(A.1)}\\
&\overset{\text{(a)}}{=} 1 - H_b(\alpha * \beta * p * q),\\
R_J &\ge R_I + I(\tilde{X};U|Y) = R_I + I(\tilde{X};U) - I(Y;U)\\
&= R_I + H(Y|U) - H(\tilde{X}|U) && \text{(A.2)}\\
&\overset{\text{(b)}}{=} R_I + H_b(\alpha * p * q) - H_b(\alpha),\\
R_L &\ge I(X;U,Y) - I(X;Y|V) + I(X;Z|V)\\
&= I(X;U,Y) - (I(X;Y) - I(Y;V)) + I(X;Z) - I(Z;V)\\
&= I(X;U|Y) + I(X;Z) + I(Y;V) - I(Z;V)\\
&= I(X;U) - I(Y;U) + 1 - H(X|Z) + H(Z|V) - H(Y|V)\\
&= H(Y|U) - H(X|U) + 1 - H_b(q * r) + H(Z|V) - H(Y|V) && \text{(A.3)}\\
&\overset{\text{(c)}}{=} 1 - H_b(q * r) + H_b(\alpha * p * q) - H_b(\alpha * p)\\
&\qquad + H_b(\alpha * \beta * p * q * r) - H_b(\alpha * \beta * p * q),\\
R_S &\le I(Y;U|V) - I(Z;U|V)\\
&= I(Y;U) - I(Y;V) - (I(Z;U) - I(Z;V))\\
&= I(Y;U) - I(Z;U) - I(Y;V) + I(Z;V)\\
&= H(Z|U) - H(Y|U) - H(Z|V) + H(Y|V) && \text{(A.4)}\\
&\overset{\text{(d)}}{=} H_b(\alpha * p * q * r) - H_b(\alpha * p * q) - H_b(\alpha * \beta * p * q * r) + H_b(\alpha * \beta * p * q). && \text{(A.5)}
\end{aligned}
$$

(a)–(d) は，テスト通信路 $P_{U|\tilde{X}}$ と $P_{V|U}$ をそれぞれ誤り確率 α と β の BSC とすることで達成される．従って，順定理は証明された． □

A.2　逆定理の証明

逆定理の証明では，式 (3.8) の右辺に含まれるレート組 (R_I, R_J, R_L, R_S) と，それぞれのレートの制約式を満たす $P_{U|\tilde{X}}$ と $P_{V|U}$ を任意に固定する．以下の議論では，式 (A.1)–(A.4) の外界を求めるために，$H(X|U)$ と $H(X|V)$ を固定する．そして，$H(\tilde{X}|U)$，$H(Z|U)$ および $H(Y|V)$ の上界，$H(Y|U)$，$H(Z|V)$ および $H(Y|V)$ の下界を求める．

まずは，定数 $(\alpha, \beta) \in [0, 1/2]$ に対して $P_{U|\tilde{X}}$ と $P_{V|U}$ を

$$H(X|U) = H_b(\alpha * p), \quad H(X|V) = H_b(\alpha * \beta * p) \tag{A.6}$$

が成り立つように固定する．式 (A.6) の設定は $H_b(p) = H(X|\tilde{X}) \leq H(X|U) \leq H(X|V) \leq H(X) = 1$ から得られる．

$H(\tilde{X}|U)$ の上界を求める．$\tilde{X}$ から X の方向において Mrs. Gerber's Lemma (MGL) [19] を用いると，

$$H(X|U) \geq H_b(p * H_b^{-1}(H(\tilde{X}|U))) \tag{A.7}$$

が成立する．ただし，情報源の一様性を適用すると，通信路 $P_{\tilde{X}|X}$ と逆の通信路 $P_{X|\tilde{X}}$ は同じ誤り確率 p を持つ性質を用いている．以降の議論もこの性質を使用する．式 (A.7) は

$$\alpha * p \geq p * H_b^{-1}(H(\tilde{X}|U)) \tag{A.8}$$

に変形できる．ここで，$p \in [0, 1/2]$ なので

$$H_b^{-1}(H(\tilde{X}|U)) \leq \alpha \quad \Rightarrow \quad H(\tilde{X}|U) \leq H_b(\alpha) \tag{A.9}$$

が成立する．

$H(Z|U)$ の上界を求める．Z から X の方向において MGL [19] を用いると，

$$H(X|U) \geq H_b(\nu * H_b^{-1}(H(Z|U))). \tag{A.10}$$

が成立する．ただし，式展開を簡単にするために $\nu = q * r$ と置いている．式 (A.10) は

$$\alpha * p \geq \nu * H_b^{-1}(H(Z|U)) = H_b^{-1}(H(Z|U))(1 - 2\nu) + \nu \tag{A.11}$$

に変形できる．さらに，式 (A.11) は

$$H(Z|U) \leq H_b\left(\frac{\alpha * p - \nu}{1 - 2\nu}\right) \overset{\text{(a)}}{\leq} H_b(\alpha * p * \nu) = H_b(\alpha * p * q * r) \tag{A.12}$$

に変形できる．ここで，(a) は [15, Lemma 7] と二値エントロピー関数が区間 $[0, 1/2]$ で単調増加するため成立する．

$H(Y|V)$ の上界を求める．Y から X の方向において MGL [19] を用いると，

$$H(X|V) \geq H_b(q * H_b^{-1}(H(Y|V))) \tag{A.13}$$

が成立する．式 (A.13) は

$$\alpha * \beta * p \geq H_b^{-1}(H(Y|V)) * q = H_b^{-1}(H(Y|V))(1-2q) + q \tag{A.14}$$

に変形できる．さらに，式 (A.14) は

$$H(Y|V) \leq H_b\left(\frac{\alpha * \beta * p - q}{1-2q}\right) \overset{\text{(a)}}{\leq} H_b(\alpha * \beta * p * q) \tag{A.15}$$

に変形できる．ここで，(a) は [15, Lemma 7] と二値エントロピー関数が区間 $[0, 1/2]$ で単調増加するため成立する．

$H(Y|U)$ の下界を求める．X から Y の方向において MGL [19] を用いると，

$$H(Y|U) \geq H_b(H_b^{-1}(H(X|U)) * q) = H_b(\alpha * p * q) \tag{A.16}$$

が成立する．

$H(Z|V)$ の下界を求める．X から Z の方向において MGL [19] を用いると，

$$H(Z|V) \geq H_b(H_b^{-1}(H(X|V)) * \nu) = H_b(\alpha * \beta * p * \nu) = H_b(\alpha * \beta * p * q * r) \tag{A.17}$$

が成立する．

$H(Y|V)$ の下界を求める．X から Y の方向において MGL [19] を用いると，

$$H(Y|V) \geq H_b(H_b^{-1}(H(X|V)) * q) = H_b(\alpha * \beta * p * q) \tag{A.18}$$

が成立する．

得られた上界の式 (A.9)，(A.12) および (A.15) と下界の式 (A.16)–(A.18) を，式 (A.1)–(A.4) に代入し，α と β を区間 $[0, 1/2]$ で動かして和集合を取ることにより，式 (3.11) の右辺を得る．従って，逆定理は証明された．　□

付 録B

B.1 補題6の証明

まず初めに，集合

$$\mathcal{C}_{vz}^n = \left\{(v^n, z^n) : \frac{1}{n}\log\frac{P_{Z^n|V^n}(z^n|v^n)}{P_{Z^n}(z^n)} \geq I(V;Z) - \delta\right\}$$

を定義する．ここで，$V^n \sim \prod_{t=1}^n P_{V_t}$ と $P_{V_t} = P_V$ であることに注意されたい．また，バイナリ確率変数

$$T = \begin{cases} 1 & \text{if } (V^n(M(w)), Z^n) \in \mathcal{C}_{vz}^n \\ 0 & \text{otherwise} \end{cases} \tag{B.1}$$

を定義する．$v^n(m(w))$ を $2^{n(I(\tilde{X};V)+\delta)}$ 個以上生成したため補題1より $\mathbb{P}_w((V^n(M(w)), \tilde{X}_w^n) \notin \mathcal{T}_{v\tilde{x}}^n) \leq \delta$ が成立する．同様に，マルコフ連鎖 $V - \tilde{X} - Z$ の関係から $\mathbb{P}_w(T=0) \leq \delta$ が成立する．式 (4.9) の左辺について

$$\begin{aligned} H_w(Z^n|V^n(M(w)), C_n) &\leq H_w(Z^n, T|V^n(M(w)), C_n) \\ &\leq H_w(T|C_n) + n\delta H_w(Z) \\ &\quad + \sum_{c^n} \mathbb{P}_w(T=1, C_n = c_n) \cdot H_w(Z^n|V^n(M(w)), T=1, C_n = c_n) \\ &\leq 1 + n\delta \log|\mathcal{Z}| \\ &\quad + \sum_{c^n} \mathbb{P}_w(T=1, C_n = c_n) \cdot H_w(Z^n|V^n(M(w)), T=1, C_n = c_n) \end{aligned} \tag{B.2}$$

が成立する．議論を簡単にするために，$A^n = (V^n(M(w)), Z^n)$ と $a^n = (v^n(m(w)), z^n)$ を用いて，式 (B.2) の第3項目の右側を展開すると，

$$\begin{aligned} &H_w(Z^n|V^n(M(w)), T=1, C_n = c_n) \leq H_w(Z^n|V^n(M(w)), T=1) \\ &= \sum_{a^n \in \mathcal{C}_{vz}^n} \mathbb{P}_w(A^n = a^n, T=1) \times \log\frac{1}{\mathbb{P}_w(Z^n = z^n|V^n(M(w)) = v^n(m(w)), T=1)} \end{aligned}$$

$$= \sum_{a^n \in \mathcal{C}_{vz}^n} \mathbb{P}_w(A^n = a^n, T = 1) \times \left(\log \frac{\mathbb{P}_w(Z^n = z^n | V^n = v^n(m(w)))}{\mathbb{P}_w(Z^n = z^n | V^n(M(w)) = v^n(m(w)), T = 1)} \right.$$
$$\left. + \log \frac{\mathbb{P}_w(Z^n = z^n)}{\mathbb{P}_w(Z^n = z^n | V^n = v^n(m(w)))} + \log \frac{1}{\mathbb{P}_w(Z^n = z^n)} \right)$$
$$\overset{\text{(a)}}{\leq} \sum_{a^n \in \mathcal{C}_{vz}^n} \mathbb{P}_w(A^n = a^n, T = 1)$$
$$\times \left(\log \frac{\mathbb{P}_w(Z^n = z^n | V^n = v^n(m(w)))}{\mathbb{P}_w(Z^n = z^n | V^n(M(w)) = v^n(m(w)), T = 1)} - n(I(Z;V) - \delta) + n(H(Z) + \delta) \right) \tag{B.3}$$

となる．ここで，(a) は $\mathcal{C}_{vz}^n$ の定義の条件と大数の法則より成立する．次に，式 (B.3) の第 1 項目を展開すると，

$$\sum_{a^n \in \mathcal{C}_{vz}^n} \mathbb{P}_w(A^n = a^n, T = 1) \log \frac{\mathbb{P}_w(Z^n = z^n | V^n = v^n(m(w)))}{\mathbb{P}_w(Z^n = z^n | V^n(M(w)) = v^n(m(w)), T = 1)}$$
$$\leq \sum_{a^n \in \mathcal{C}_{vz}^n} \mathbb{P}_w(A^n = a^n | T = 1) \times \log \frac{\mathbb{P}_w(Z^n = z^n | V^n = v^n(m(w)))}{\mathbb{P}_w(Z^n = z^n | V^n(M(w)) = v^n(m(w)), T = 1)}$$
$$\overset{\text{(b)}}{\leq} \log \left(\sum_{a^n \in \mathcal{C}_{vz}^n} \frac{\mathbb{P}_w(A^n = a^n | T = 1) \mathbb{P}_w(Z^n = z^n | V^n = v^n(m(w)))}{\mathbb{P}_w(Z^n = z^n | V^n(M(w)) = v^n(m(w)), T = 1)} \right)$$
$$\overset{\text{(c)}}{\leq} \log \left(\sum_{a^n \in \mathcal{C}_{vz}^n} \frac{\mathbb{P}_w(A^n = a^n) \mathbb{P}_w(Z^n = z^n | V^n = v^n(m(w)))}{\mathbb{P}_w(T = 1) \mathbb{P}_w(Z^n = z^n | V^n(M(w)) = v^n(m(w)))} \right)$$
$$\leq \log \left(\sum_{a^n \in \mathcal{O}^n \times \mathcal{Z}^n} \frac{\mathbb{P}_w(V^n(M(w)) = v^n(m(w)))}{\mathbb{P}_w(T = 1)} \mathbb{P}_w(Z^n = z^n | V^n = v^n(m(w))) \right)$$
$$= -\log \mathbb{P}_w(T = 1) \leq -\log(1 - \delta). \tag{B.4}$$

となる．(b) はイェンセンの不等式より成立する．(c) は

$$\mathbb{P}_w(A^n = a^n | T = 1) = \begin{cases} \frac{\mathbb{P}_w(A^n = a^n)}{\mathbb{P}_w(T=1)} & \text{if } a^n \in \mathcal{C}_{vz}^n \\ 0 & \text{otherwise} \end{cases} \tag{B.5}$$

の関係から $a^n \in \mathcal{C}_{vz}^n$ であれば

$$\mathbb{P}_w(Z^n = z^n | V^n(M(w)) = v^n(m(w)), T = 1) \geq \mathbb{P}_w(Z^n = z^n | V^n(M(w)) = v^n(m(w))) \tag{B.6}$$

となるので成立する．式 (B.2)–(B.4) より

$$H_w(Z^n | V^n(M(w)), \mathcal{C}_n) \leq 1 + n\delta \log |\mathcal{Z}| - \log(1 - \delta) + n(H(Z|V) + 2\delta)$$
$$\leq n(H(Z|V) + \epsilon_n + 2\delta) \tag{B.7}$$

となる. □

B.2 式 (4.42) の証明

Csiszár's sum identify [18] より以下の式が成立する.

$$\sum_{t=1}^{n} I(Y_t; Z^{t-1}|J(W), Y_{t+1}^n) = \sum_{t=1}^{n} I(Y_{t+1}^n; Z_t|J(W), Z^{t-1}), \tag{B.8}$$

$$\sum_{t=1}^{n} I(Y_t; Z^{t-1}|J(W), S(W), Y_{t+1}^n) = \sum_{t=1}^{n} I(Y_{t+1}^n; Z_t|J(W), S(W), Z^{t-1}). \tag{B.9}$$

式 (B.8) と (B.9) を用いると

$$\begin{aligned}
&\sum_{t=1}^{n}\{I(S(W); Y_t|J(W), Y_{t+1}^n) - I(S(W); Z_t|J(W), Z^{t-1})\} \\
&= \sum_{t=1}^{n}\{I(S(W); Y_t|J(W), Y_{t+1}^n) - I(S(W); Z_t|J(W), Z^{t-1})\} \\
&\quad + \underbrace{\sum_{t=1}^{n}\{I(Y_t; Z^{t-1}|J(W), S(W), Y_{t+1}^n) - I(Y_{t+1}^n; Z_t|J(W), S(W), Z^{t-1})\}}_{=0} \\
&= \sum_{t=1}^{n}\{I(Z^{t-1}, S(W); Y_t|J(W), Y_{t+1}^n) - I(Y_{t+1}^n, S(W); Z_t|J(W), Z^{t-1})\} \\
&= \underbrace{\sum_{t=1}^{n}\{I(Y_t; Z^{t-1}|J(W), Y_{t+1}^n) - I(Y_{t+1}^n; Z_t|J(W), Z^{t-1})\}}_{=0} \\
&\quad + \sum_{t=1}^{n}\{I(S(W); Y_t|J(W), Y_{t+1}^n, Z^{t-1}) - I(S(W); Z_t|J(W), Y_{t+1}^n, Z^{t-1})\} \\
&= \sum_{t=1}^{n}\{I(S(W); Y_t|J(W), Y_{t+1}^n, Z^{t-1}) - I(S(W); Z_t|J(W), Y_{t+1}^n, Z^{t-1})\}
\end{aligned} \tag{B.10}$$

が成立する. 従って, 式 (4.42) は証明された. □