相関のある情報を用いたMultiple Access Wiretap Channelにおける秘匿通信について

小川 善功[1]　田中 亮大[1]　四方 順司[1,2]

概要：Multiple Access Wiretap Channel(MAC-WT) は，2 入力 1 出力の通信路に盗聴者を考慮した通信路モデルである．ここで，送信者により送られる情報は独立であることが一般的である．MAC-WT モデルでは，盗聴者のレートが受信者のレート以下であると仮定した場合，その差分が秘匿レートとなる．本稿では，2 入力 2 出力の盗聴通信路モデルであり，2 入力情報として共通情報を持つモデルについて考察する．また，このような提案モデルにおいて，盗聴者に対して秘匿性が保たれるレートの領域を導出し，2 入力情報のうち一方に関しては，MAC-WT を単純に適用する場合よりも秘匿レートを増加可能であることを示す．

キーワード：物理層セキュリティ，Wiretap Channel，秘匿レート，Multiple Access Channel

1. はじめに

1.1 背景

現在，私たちの身の回りでは携帯電話や IoT 機器をはじめとした無線通信を利用した機器が広く普及している．無線通信では通信路上で雑音の影響を受けるため，送信する情報に誤り訂正機能を付与することで信頼性を確保している．また，無線通信は公共の空間を通して情報を送信するため，不特定多数の人に受信される可能性があることから通信内容を盗聴させる危険性が高いといえる．そこで，このような通信路において，信頼性だけでなく秘匿性を確保する技術として物理層セキュリティ [1] という技術が提案されている．

物理層セキュリティにおける代表的な通信モデルの 1 つとして，Wiretap Channel(WT) は Wyner[2] によって提案された盗聴通信路モデルである．このモデルは雑音通信路において盗聴者が存在する通信モデルで，送信者 Alice から送られる符号語にのる雑音の量について，正規の受信者 Bob は雑音の量が少なく元の情報を復号することができ，盗聴者 Eve は雑音の量が多く元の情報を復号することができないといった仮定の下で秘匿通信が行えるものとなっている．また，WT では暗号化を用いず通信路の特性を用いて秘匿通信を行うため，鍵を用いた暗号化をする必要がないという利点がある．

また，2 入力 1 出力の通信路 (Multiple Access Channel) において盗聴者を考慮したモデルとして，Multiple Access Wiretap Channel(MAC-WT) というモデルがある [3], [4]. MAC-WT モデルでは 2 人の送信者 Alice と Carol がそれぞれ情報を符号化し，雑音通信路の入力とする．ここで，Alice と Carol により送られる情報は独立である．正規の受信者 Bob と盗聴者 Eve はそれぞれ雑音を含んだ符号語を受信する．このとき，WT モデル同様，Bob の受信する符号語に含まれる雑音の量が Eve の受信する符号語に含まれる雑音の量より少ない仮定の下で秘匿通信が行える．

1.2 本稿の貢献

本稿では，2 入力 2 出力の盗聴通信路モデルにおいて、2 入力情報として共通情報を持つモデルについて考察する．また，提案モデルにおいて，盗聴者に対して秘匿性が保たれるレートの上界及び下界を導出し，一方の入力情報のレートに関しては MAC-WT モデルにおける秘匿性が保たれるレートの上界及び下界よりも増加していることを示す．

2. WT モデルと MAC-WT モデルにおける秘匿レート

本節では準備として WT モデルと MAC-WT モデルについてまとめ，盗聴者を考慮した場合における秘匿レートについて説明する．

[1] 横浜国立大学 大学院環境情報学府/研究院
[2] 横浜国立大学 先端科学高等研究院

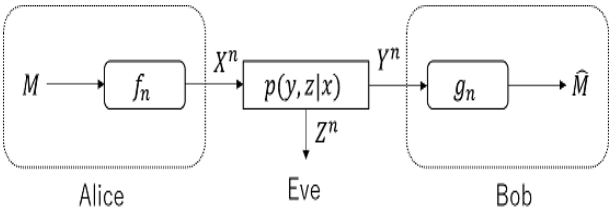

図 1 Wiretap Channel

2.1 WT モデル

WT モデルは，図 1 のように送信者 Alice，正規の受信者 Bob，盗聴者 Eve からなる通信モデルである．このモデルにおける通信路は雑音通信路である．ここで，Eve は盗聴のみを行うものと仮定する．Alice と Bob は通信路の特徴の 1 つである通信路上の雑音を利用することで，秘匿通信を行うことができる．秘匿レートを R_s とする．

記号の表記

- M：平文の確率変数 ($M \in \mathcal{M}, \mathcal{M}$ は平文の集合)
- X^n：Alice より送信される符号語の確率変数 ($X^n \in \mathcal{X}^n, \mathcal{X}^n$ は符号語集合)
- Y^n：Bob が受信する符号語の確率変数 ($Y^n \in \mathcal{Y}^n, \mathcal{Y}^n$ は符号語集合)
- Z^n：Eve が受信する符号語の確率変数 ($Z^n \in \mathcal{Z}^n, \mathcal{Z}^n$ は符号語集合)

雑音通信路において，通信路に入力された符号語 X^n は雑音の影響を受ける．そのため，確率 $p(y,z|x)$ より Bob には符号語 Y^n が，Eve には符号語 Z^n が出力される．Bob と Eve はそれぞれ受信した符号語から元の平文を復号する．

このモデルにおける復号誤り確率は次のように定義される．

定義 1 (復号誤り確率 [2])．復号器より得られた平文 $\hat{m}$ より

$$P_e := \frac{1}{2^{nR_s}} \sum_{m \in \mathcal{M}} Pr\{\hat{m} \neq m\}$$

復号誤り確率が無視できるほど小さいとき，信頼性のある通信といえる．

一方，安全性について，十分大きな n に対して，$\frac{1}{n}H(M|Z^n) \approx \frac{1}{n}H(M) = R_s$ をみたすとき，完全秘匿性をもつという．これより，安全性は次のように定義される．

定義 2 (安全性 [2])．以下の条件を満たすとき，秘匿レート R_s は達成可能であるという．

$$\lim_{n\to\infty} P_e = 0$$

$$R_s \leq \lim_{n\to\infty} \frac{1}{n} H(M|Z^n)$$

以上より，WT モデルにおける秘匿レートの上界について以下の不等式が導出されている．

命題 1 (WT モデルにおける秘匿レート [2])．$I(X^n;Y^n) \geq I(X^n;Z^n)$ と仮定するとき，秘匿レート R_s は以下の式を満たす．

$$R_s \leq \lim_{n\to\infty} \frac{1}{n}\{I(X^n;Y^n) - I(X^n;Z^n)\}$$

2.2 MAC-WT モデル

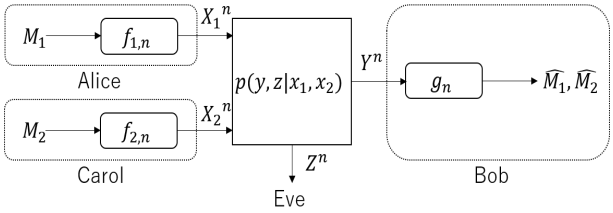

図 2 Multiple Access Wiretap Channel

MAC-WT モデルは，図 2 のように 2 人の送信者 Alice, Carol，正規の受信者 Bob，盗聴者 Eve からなる通信モデルである．このモデルにおける通信路は雑音通信路である．ここで，Eve は盗聴のみを行うものと仮定する．また，Alice の秘匿レートを $R_{1,s}$，Carol の秘匿レートを $R_{2,s}$ とする

記号の表記

- M_1：平文の確率変数 ($M_1 \in \mathcal{M}_1, \mathcal{M}_1$ は平文の集合)
- M_2：平文の確率変数 ($M_2 \in \mathcal{M}_2, \mathcal{M}_2$ は平文の集合)
- ${X_1}^n$：Alice より送信される符号語の確率変数 (${X_1}^n \in \mathcal{X_1}^n, \mathcal{X_1}^n$ は符号語集合)
- ${X_2}^n$：Carol より送信される符号語の確率変数 (${X_2}^n \in \mathcal{X_2}^n, \mathcal{X_2}^n$ は符号語集合)
- Y^n：Bob が受信する符号語の確率変数 ($Y^n \in \mathcal{Y}^n, \mathcal{Y}^n$ は符号語集合)
- Z^n：Eve が受信する符号語の確率変数 ($Z^n \in \mathcal{Z}^n, \mathcal{Z}^n$ は符号語集合)

WT モデル同様，通信路から確率 $p(y,z|x_1,x_2)$ より Bob には符号語 Y^n が，Eve には符号語 Z^n が出力される．Bob と Eve はそれぞれ受信した符号語から元の平文を復号する．MAC-WT モデルでは，受信する符号語について，符号語 ${X_1}^n, {X_2}^n$ は互いに干渉しあう．そこで，平文 M_1 を復号するとき，符号語 Y^n には通信路上の雑音だけでなく符号語 ${X_2}^n$ との干渉による雑音も含まれる．また，先に平文 M_2 が復号されている場合，符号語 X_2 についても受信者は既知となるため，符号語 Y^n から符号語 ${X_2}^n$ との干渉による雑音を取り除くことができると考える．このモデルにおける復号誤り確率および安全性は次のように定義される．

定義 3 (復号誤り確率 [3])．復号器より得られた平文 $\hat{m_1}, \hat{m_2}$ より

$$P_e := \frac{1}{2^{n(R_{1,s}+R_{2,s})}} \sum_{m_1 \in \mathcal{M}_1, m_2 \in \mathcal{M}_2} Pr\{\hat{m}_1 \neq m_1 \ or \ \hat{m}_2 \neq m_2\}$$

定義 4（安全性 [3]）．以下の条件を満たすとき，秘匿レート $R_{1,s}, R_{2,s}$ は達成可能であるという．

$$\lim_{n\to\infty} P_e = 0$$

$$R_{1,s} \leq \lim_{n\to\infty} \frac{1}{n} H(M_1|Z^n)$$

$$R_{2,s} \leq \lim_{n\to\infty} \frac{1}{n} H(M_2|Z^n)$$

$$R_{1,s} + R_{2,s} \leq \lim_{n\to\infty} \frac{1}{n} H(M_1, M_2|Z^n)$$

以上より，MAC-WT モデルにおける秘匿レートの上界ついて以下の不等式が導出されている．

命題 2（MAC-WT モデルにおける秘匿レート [3]）．$I({X_1}^n; Y^n|X_2) \geq I({X_1}^n; Z^n|X_2)$，$I({X_2}^n; Y^n|X_1) \geq I({X_2}^n; Z^n|X_1)$ と仮定するとき，秘匿レート $R_{1,s}, R_{2,s}$ は以下の式を満たす．

$$R_{1,s} \leq \lim_{n\to\infty} \frac{1}{n}\{I({X_1}^n; Y^n|{X_2}^n) - I({X_1}^n; Z^n)\}$$
$$R_{2,s} \leq \lim_{n\to\infty} \frac{1}{n}\{I({X_1}^n; Y^n|{X_1}^n) - I({X_2}^n; Z^n)\}$$
$$R_{1,s} + R_{2,s} \leq \lim_{n\to\infty} \frac{1}{n}\{I({X_1}^n, {X_2}^n; Y^n) - I({X_1}^n, {X_2}^n; Z^n)\}$$

3. 提案モデル

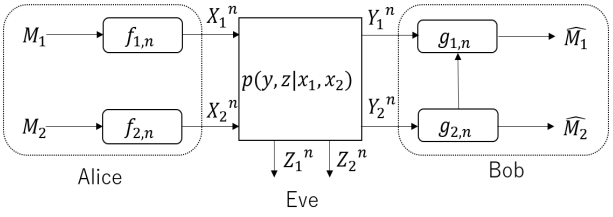

図 3 提案モデル

本節では 2 入力 2 出力の盗聴通信路モデルについて考える．提案モデルは，図 3 のように送信者 Alice，正規の受信者 Bob，盗聴者 Eve からなる通信モデルである．このモデルにおける通信路は雑音通信路で，Alice は共通情報を持つ情報をそれぞれ符号化し通信路に入力とする．ここで，Eve は盗聴のみを行うものと仮定する．秘匿レートを $R_{1,s}, R_{2,s}$ とする．

記号の表記（以下 $i = \{1, 2\}$ とする）

- M_i：平文の確率変数 ($M_i \in \mathcal{M}_i, |\mathcal{M}_i| = 2^{nR_{i,s}}, \mathcal{M}_i$ は平文の集合)
- ${X_i}^n$：Alice より送信される符号語の確率変数 (${X_i}^n \in \mathcal{X_i}^n, \mathcal{X_i}^n$ は符号語集合)
- ${Y_i}^n$：Bob が受信する符号語の確率変数 (${Y_i}^n \in \mathcal{Y_i}^n, \mathcal{Y_i}^n$ は符号語集合)
- ${Z_i}^n$：Eve が受信する符号語の確率変数 (${Z_i}^n \in \mathcal{Z_i}^n, \mathcal{Z_i}^n$ は符号語集合)

また，通信路について，確率 $p(y_1, y_2, z_1, z_2|x_1, x_2)$ より Bob には符号語 ${Y_1}^n, {Y_2}^n$ が，Eve には符号語 ${Z_1}^n, {Z_2}^n$ が出力される．Bob と Eve はそれぞれ受信した符号語から元の平文を復号する．

次に，提案モデルにおける符号化，復号の手順について説明する．

(1) Alice は，符号化器 $f_{1,n}$ を用いて，一様ランダムな平文 M_1 から共通部分以外の情報（$M_1{}'$ とする）を符号化し，符号語 ${X_1}^n$ を送信する．次に，符号化器 $f_{2,n}$ を用いて，一様ランダムな平文 M_2 を符号化し，符号語 ${X_2}^n$ を送信する．

(2) Bob は，はじめに復号器 $g_{2,n}$ を用いて受信した符号語 ${Y_2}^n$ から平文 $\hat{m_2}$ を復号する．次に，復号器 $g_{1,n}$ を用いて受信した符号語 ${Y_1}^n$ から平文 $\hat{m_1}'$ を復号し，平文 $\hat{m_2}$ より共通情報を得ることで平文 $\hat{m_1}$ を復号する．

(3) Eve も Bob と同様の手順で復号を行う．

提案モデルにおける復号誤り確率および安全性は次のように定義する．

定義 5（復号誤り確率）．復号器より得られた平文 $\hat{m_1}, \hat{m_2}$ より

$$P_e := \frac{1}{2^{n(R_{1,s}+R_{2,s})}} \sum_{m_1\in\mathcal{M}_1, m_2\in\mathcal{M}_2} Pr\{\hat{m}_1 \neq m_1 \ or \ \hat{m}_2 \neq m_2\}$$

定義 6（安全性）．以下の条件を満たすとき，秘匿レート $R_{1,s}, R_{2,s}$ は達成可能であるという．

$$\lim_{n\to\infty} P_e = 0$$

$$R_{1,s} \leq \lim_{n\to\infty} \frac{1}{n} H(M_1|{Z_1}^n)$$

$$R_{2,s} \leq \lim_{n\to\infty} \frac{1}{n} H(M_2|{Z_2}^n)$$

4. 提案モデルにおける秘匿レート

本節では提案モデルにおける秘匿レートの上界と下界について示す．平文 M_1, M_2 について，それぞれの達成可能な秘匿レート $R_{1,s}, R_{2,s}$ の上界と下界を導出する．ここで，平文 M_1, M_2 の共通情報 c について，レートを R_c とし，$|c| = 2^{nR_c}$ とする．

4.1 上界の導出

本稿での提案モデルにおいて、安全性定義より秘匿レート $R_{1,s}, R_{2,s}$ の上界が以下のように求められる．

定理 1（秘匿レートの上界）．提案モデルにおいて，秘匿レート $R_{1,s}, R_{2,s}$ は以下の不等式を満たす．

$$R_{1,s} \leq \lim_{n\to\infty} \frac{1}{n}\{I({X_1}^n; {Y_1}^n|{X_2}^n) + \frac{1}{n}H(c) - \frac{1}{n}I({X_1}^n; {Z_1}^n)\}$$
$$R_{2,s} \leq \lim_{n\to\infty} \frac{1}{n}\{I({X_2}^n; {Y_2}^n) - \frac{1}{n}I({X_2}^n; {Z_2}^n)\}$$

証明．Bob は符号語 ${Y_1}^n$ から平文 $M_1{}'$ を，符号語 ${Y_2}^n$

から平文 M_2 をほぼ誤りなく復号できることから，以下の不等式が成り立つ．

$$H(M_1{}'|{Y_1}^n) \leq \epsilon \tag{1}$$

$$H(M_2|{Y_2}^n) \leq \epsilon \tag{2}$$

また，Bob のそれぞれの受信符号語に含まれる雑音の量は Eve のそれぞれの受信符号語に含まれる雑音の量より少ないという仮定より，以下の不等式が成り立つ．

$$I({X_1}^n;{Y_1}^n|X_2) \geq I({X_1}^n;{Z_1}^n|X_2) \tag{3}$$

$$I({X_2}^n;{Y_2}^n) \geq I({X_2}^n;{Z_2}^n) \tag{4}$$

式 (3)，(4) より，

$$I({X_1}^n;{Y_1}^n|X_2,U) \geq I({X_1}^n;{Z_1}^n|X_2,U) \tag{5}$$

$$I({X_2}^n;{Y_2}^n|U) \geq I({X_2}^n;{Z_2}^n|U) \tag{6}$$

ここで，$p({x_1}^n,{x_2}^n) = p({x_1}^n)p({x_2}^n)$ であり，U は $U \to ({X_1}^n,{X_2}^n) \to ({Y_1}^n,{Y_2}^n,{Z_1}^n,{Z_2}^n)$，${X_1}^n \to U \to {X_2}^n$ となる任意の確率変数である．したがって，次のような結果が得られる．

$$\begin{aligned} I({X_1}^n;{Y_1}^n|X_2,M_1{}') &\geq I({X_1}^n;{Z_1}^n|X_2,M_1{}') \\ &\geq I({X_1}^n;{Z_1}^n|M_1{}') \end{aligned} \tag{7}$$

これは，(5) より U を $M_1{}'$ として，$({X_1}^n,M_1{}')$ と ${X_2}^n$ が独立していることより導出される．また，(6) より

$$I({X_2}^n;{Y_2}^n|M_2) \geq I({X_2}^n;{Z_2}^n|M_2) \tag{8}$$

が導出される．

以上より，安全性の条件から秘匿レートの上界を導出する．

$$\begin{aligned} R_{1,s} &\leq \frac{1}{n}H(M_1|{Z_1}^n) \\ &= \frac{1}{n}H(M_1) - \frac{1}{n}I(M_1;{Z_1}^n) \\ &= \frac{1}{n}H(M_1{}',c) - \frac{1}{n}I(M_1{}',c;{Z_1}^n) \qquad (9) \\ &= \frac{1}{n}H(M_1{}') + \frac{1}{n}H(c) - \frac{1}{n}I(M_1{}';{Z_1}^n) \\ &\leq \frac{1}{n}H(M_1{}') + \frac{1}{n}H(M_1{}'|{Y_1}^n) + \frac{1}{n}H(c) \\ &\quad -\frac{1}{n}I(M_1{}';{Z_1}^n) + \epsilon \qquad (10) \\ &= \frac{1}{n}I(M_1{}';{Y_1}^n) + \frac{1}{n}H(c) - \frac{1}{n}I(M_1{}';{Z_1}^n) + \epsilon \\ &\leq \frac{1}{n}I(M_1{}';{Y_1}^n) + \frac{1}{n}H(c) - \frac{1}{n}I(M_1{}';{Z_1}^n) + \epsilon \\ &\quad +\frac{1}{n}I({X_1}^n;{Y_1}^n|{X_2}^n,M_1{}') \\ &\quad +\frac{1}{n}I({X_1}^n;{Z_1}^n|M_1{}') \qquad (11) \\ &= \frac{1}{n}I(M_1{}',{X_1}^n;{Y_1}^n|{X_2}^n) + \frac{1}{n}H(c) \\ &\quad -\frac{1}{n}I(M_1{}',{X_1}^n;{Z_1}^n) + \epsilon \\ &= \frac{1}{n}I({X_1}^n;{Y_1}^n|{X_2}^n) + \frac{1}{n}H(c) \\ &\quad -\frac{1}{n}I({X_1}^n;{Z_1}^n) + \epsilon \qquad (12) \end{aligned}$$

ここで，(9) は平文 M_1 が平文 $M_1{}'$ と共通情報 c に分けられることから成り立つ．また，$M_1{}'$ と c は独立である．(10) は (1) を用いて，(11) は (7) を用いることで成り立つ．(12) は ${X_1}^n$ が与えられたとき $M_1{}'$ が ${Y_1}^n,{Z_1}^n$ と独立であることから成り立つ．

$$\begin{aligned} R_{2,s} &\leq \frac{1}{n}H(M_2|{Z_2}^n) \\ &= \frac{1}{n}H(M_2) - \frac{1}{n}I(M_2;{Z_2}^n) \\ &\leq \frac{1}{n}H(M_2) + \frac{1}{n}H(M_2|{Y_2}^n) \\ &\quad -\frac{1}{n}I(M_2;{Z_2}^n) + \epsilon \qquad (13) \\ &= \frac{1}{n}I(M_2;{Y_2}^n) - \frac{1}{n}I(M_2;{Z_2}^n) + \epsilon \\ &\leq \frac{1}{n}I(M_2;{Y_2}^n) - \frac{1}{n}I(M_2;{Z_2}^n) + \epsilon \\ &\quad +\frac{1}{n}I({X_2}^n;{Y_2}^n|M_2) + \frac{1}{n}I({X_2}^n;{Z_2}^n|M_2) \qquad (14) \\ &= \frac{1}{n}I(M_2,{X_2}^n;{Y_2}^n) - \frac{1}{n}I(M_2,{X_2}^n;{Z_2}^n) + \epsilon \\ &= \frac{1}{n}I({X_2}^n;{Y_2}^n) - \frac{1}{n}I({X_2}^n;{Z_2}^n) + \epsilon \qquad (15) \end{aligned}$$

ここで，(13) は (2) を用いて，(14) は (8) を用いることで成り立つ．(15) は ${X_2}^n$ が与えられたとき M_2 が ${Y_2}^n,{Z_2}^n$ と独立であることから成り立つ．

4.2 下界の導出

本稿での提案モデルにおいて、安全性定義より秘匿レート $R_{1,s},R_{2,s}$ の下界が以下のように求められる．

定理 2 (秘匿レートの下界)．提案モデルにおいて，秘匿レート $R_{1,s},R_{2,s}$ は以下の不等式を満たす．

$$\begin{aligned} R_{1,s}+R_{1,d} &\geq \lim_{n\to\infty}\frac{1}{n}\{I({X_1}^n;{Y_1}^n|{X_2}^n)+H(c)\} \\ R_{2,s}+R_{2,d} &\geq \lim_{n\to\infty}\frac{1}{n}I({X_2}^n;{Y_2}^n) \\ R_{1,d} &\geq \lim_{n\to\infty}\frac{1}{n}I({X_1}^n;{Z_1}^n) \\ R_{2,d} &\geq \lim_{n\to\infty}\frac{1}{n}I({X_2}^n;{Z_2}^n) \end{aligned}$$

証明．まず、提案モデルにおける符号構成について示す．符号構成はランダム符号を用いる．

(1) **符号生成**：確率 $p(x_1)$ に従い符号語 ${x_1}^n$ を $2^{nR_1'}$ 個生成する．次に，符号語 ${x_1}^n$ を $2^{nR_{1,s}'}$ 個の集合に分割する．ここで，集合 $i(1 \leq i \leq 2^{nR_{1,s}'})$ 内の $j(1 \leq j \leq 2^{nR_{1,d}})$ 番目の符号語を ${x_1}^n(i,j)$ とする．$R_{1,d}$ を乱数レート，共通情報 c のレートを $R_c = \frac{1}{n}H(c)$ とし，$R_{1,s} = R_{1,s}' + R_c, R_1' = R_{1,s}' + R_{1,d}$ となる．ま

た，符号語を ${x_1}^n(i,j)$ から成る符号を $C_{1,n}$ とし，Alice, Bob, Eve に共有されているものとする．同様にして，確率 $p(x_2)$ に従い符号語 ${x_2}^n$ を 2^{nR_2} 個生成する．次に，符号語 ${x_2}^n$ を $2^{nR_{2,s}}$ 個の集合に分割する．ここで，集合 $k(1 \leq k \leq 2^{nR_{2,s}})$ 内の $l(1 \leq l \leq 2^{nR_{2,d}})$ 番目の符号語を ${x_2}^n(k,l)$ とする．$R_{2,d}$ を乱数レートとし，$R_2 = R_{2,s} + R_{2,d}$ となる．また，符号語を ${x_2}^n(k,l)$ から成る符号を $C_{2,n}$ とし，Alice，Bob，Eve に共有されているものとする．

(2) **符号化**：はじめに，Alice は平文 M_1 より共通情報を取り除いた平文 $M_1{}'$ から対応する符号語 ${x_1}^n$ の集合 i を選択する．次に，乱数 r_1 により j をランダムに選択し，(i,j) の組とする．同様にして，平文 M_2 から対応する符号語 ${x_2}^n$ の集合 k を選択する．次に，乱数 r_2 により l をランダムに選択し，(k,l) の組とする．ここで，平文 $m_1 \in M_1, m_1{}' \in M_1{}', m_2 \in M_2$ は一様分布とする．また，選ばれた平文 m_1, m_2 は共通情報 c を持つものとする．以上より，Alice は符号語 x_1, x_2 を通信路に送信する．

(3) **復号**：はじめに，Bob は受信する符号語 ${y_2}^n$ について復号を考える．

$$({x_2}^n, {y_2}^n) \in {\mathcal{T}^n}_{[X_2Y_2]}$$

となる符号 C_2 における符号語 ${x_2}^n$ がただ一つ存在するとき，Bob は (k,l) の組をただ一つ決定できるため元の平文を復号することができる．ここで，${\mathcal{T}^n}_{[X_2Y_2]}$ は典型系列であり確率 $p(x_2,y_2)$ より得られる．次に，Bob は受信する符号語 ${y_1}^n$ について復号を考える．

$$({x_1}^n, {x_2}^n, {y_1}^n) \in {\mathcal{T}^n}_{[X_1X_2Y_1]}$$

となる符号の組 (C_1, C_2) における符号語の組 $({x_1}^n, {x_2}^n)$ がただ一つ存在するとき，Bob は $(i,j),(k,l)$ の組をただ一つ決定できるため元の平文を復号することができる．ここで，${\mathcal{T}^n}_{[X_1X_2Y_1]}$ は典型系列であり確率 $p(x_1,x_2,y_1)$ より得られる．

以上の符号構成，符号化，復号から秘匿レートの下界について導出する．

安全性の定義より，

$$\begin{aligned} R_{2,s} &\leq \frac{1}{n}H(M_2|{Z_2}^n) \\ H({X_2}^n) &\leq \frac{1}{n}H(M_2|{Z_2}^n) + R_{2,d} \\ &\leq \frac{1}{n}H({X_2}^n|{Z_2}^n) + R_{2,d} \qquad (16) \\ \frac{1}{n}I({X_2}^n;{Z_2}^n) &\leq R_{2,d} \qquad (17) \end{aligned}$$

ここで，(16) は $H(M_2|{Z_2}^n) \leq H(M_2,r_2|{Z_2}^n) = H({X_2}^n|{Z_2}^n)$ を用いる．

次に，安全性の定義より，Eve が受信する符号語 ${Z_2}^n$ における平文 M_2 のエントロピー量と平文 M_2 のエントロピー量が漸近的に等しくなるとき，秘匿レートの下界は次のように導出される．

$$\begin{aligned} R_{2,s} &= \frac{1}{n}H(M_2|{Z_2}^n) \\ &= \frac{1}{n}H(M_2) - \frac{1}{n}I(M_2;{Z_2}^n) \\ &= \frac{1}{n}H(M_2) - \frac{1}{n}I(M_2,r_2;{Z_2}^n) + \frac{1}{n}I(r_2;{Z_2}^n|M_2) \\ &= \frac{1}{n}H(M_2) - \frac{1}{n}I({X_2}^n;{Z_2}^n) + \frac{1}{n}H(r_2|M_2) \\ &\quad -\frac{1}{n}H(r_2|M_2,{Z_2}^n) \\ &= \frac{1}{n}H(M_2) - \frac{1}{n}I({X_2}^n;{Z_2}^n) + \frac{1}{n}H(r_2) - \frac{1}{n}H(r_2|M_2,{Z_2}^n) \\ &= \frac{1}{n}H({X_2}^n) - \frac{1}{n}I({X_2}^n;{Z_2}^n) - \frac{1}{n}H(r_2|M_2,{Z_2}^n) \\ &\geq \frac{1}{n}I({X_2}^n;{Y_2}^n) - \frac{1}{n}I({X_2}^n;{Z_2}^n) - \frac{1}{n}H(r_2|M_2,{Z_2}^n) \qquad (18) \\ &\geq \frac{1}{n}I({X_2}^n;{Y_2}^n) - R_{2,d} - \frac{1}{n}H(r_2|M_2,{Z_2}^n) \qquad (19) \end{aligned}$$

ここで，(18) は $H({X_2}^n) \geq I({X_2}^n;{Y_2}^n)$ を用いて，(19) は (17) を用いる．また，n が十分大きいとき $\lim_{n\to\infty}\frac{1}{n}H(r_2|M_2,{Z_2}^n) = 0$ である．

安全性の定義より，

$$\begin{aligned} R_{1,s} &\leq \frac{1}{n}H(M_1|{Z_1}^n) \\ H({X_1}^n) &\leq \frac{1}{n}H(M_1|{Z_1}^n) - R_c + R_{1,d} \\ &\leq \frac{1}{n}H({X_1}^n|{Z_1}^n) + R_{1,d} \qquad (20) \\ \frac{1}{n}I({X_1}^n;{Z_1}^n) &\leq R_{1,d} \qquad (21) \end{aligned}$$

ここで，(20) は $H(M_1|{Z_1}^n) \leq H(M_1{}',c,r_1|{Z_1}^n) = H({X_1}^n|{Z_1}^n) + H(c)$ を用いる．

次に，安全性の定義より，Eve が受信する符号語 ${Z_1}^n$ における平文 M_1 のエントロピー量と平文 M_1 のエントロピー量が漸近的に等しくなるとき，秘匿レートの下界は次のように導出される．

$$\begin{aligned} R_{1,s} &= \frac{1}{n}H(M_1|{Z_1}^n) \\ &= \frac{1}{n}H(M_1) - \frac{1}{n}I(M_1;{Z_1}^n) \\ &= \frac{1}{n}H(M_1{}') + \frac{1}{n}H(c) - \frac{1}{n}I(M_1{}';{Z_1}^n) - \frac{1}{n}I(c;{Z_1}^n) \\ &= \frac{1}{n}H(M_1{}') + \frac{1}{n}H(c) - \frac{1}{n}I({X_1}^n;{Z_1}^n) + \frac{1}{n}H(r_1) \\ &\quad -\frac{1}{n}H(r_1|M_1{}',{Z_1}^n) - \frac{1}{n}I(c;{Z_1}^n) \\ &= \frac{1}{n}H({X_1}^n) + \frac{1}{n}H(c) - \frac{1}{n}I({X_1}^n;{Z_1}^n) \\ &\quad -\frac{1}{n}H(r_1|M_1{}',{Z_1}^n) - \frac{1}{n}I(c;{Z_1}^n) \\ &\geq \frac{1}{n}H({X_1}^n|{X_2}^n) + \frac{1}{n}H(c) - \frac{1}{n}I({X_1}^n;{Z_1}^n) \\ &\quad -\frac{1}{n}H(r_1|M_1{}',{Z_1}^n) - \frac{1}{n}I(c;{Z_1}^n) \\ &\geq \frac{1}{n}I({X_1}^n;{Y_1}^n|{X_2}^n) + \frac{1}{n}H(c) - \frac{1}{n}I({X_1}^n;{Z_1}^n) \end{aligned}$$

$$-\frac{1}{n}H(r_1|M_1{}',{Z_1}^n)-\frac{1}{n}I(c;{Z_1}^n) \quad (22)$$

$$\geq \frac{1}{n}I({X_1}^n;{Y_1}^n|{X_2}^n)+\frac{1}{n}H(c)$$
$$-R_{1,d}-\frac{1}{n}H(r_1|M_1{}',{Z_1}^n)-\frac{1}{n}I(c;{Z_1}^n) \quad (23)$$

ここで，(22) は $H({X_1}^n|{X_2}^n) \geq I({X_1}^n;{Y_1}^n|{X_2}^n)$ を用いて，(23) は (21) を用いる．また，n が十分大きいとき $\lim_{n\to\infty}\frac{1}{n}H(r_1|M_1{}',{Z_1}^n)=0, \lim_{n\to\infty}\frac{1}{n}I(c;{Z_1}^n)=0$ である．

5. 既存研究との比較

本節では既存研究の MAC-WT モデルと提案モデルにおける秘匿レートについて比較を行う．

5.1 MAC-WT の特殊ケースにおける秘匿レート

命題 2 における MAC-WT の秘匿レートについて，平文の復号順序が決まっていない場合の秘匿レートの上界である．そこで，提案モデルと比較するために MAC-WT において，はじめに平文 M_2，次に平文 M_1 について復号する場合における秘匿レートの上界と下界について導出する．

定理 3　(秘匿レートの上界)．MAC-WT の特殊ケースにおいて，秘匿レート $R_{1,s}, R_{2,s}$ は以下の不等式を満たす．

$$R_{1,s} \leq \lim_{n\to\infty}\frac{1}{n}\{I({X_1}^n;{Y}^n|{X_2}^n)-\frac{1}{n}I({X_1}^n;{Z}^n)\}$$
$$R_{2,s} \leq \lim_{n\to\infty}\frac{1}{n}\{I({X_2}^n;{Y}^n)-\frac{1}{n}I({X_2}^n;{Z}^n)\}$$

証明．Bob は符号語 Y^n から平文 M_1，平文 M_2 をほぼ誤りなく復号できることから，以下の不等式が成り立つ．

$$H(M_1|Y^n) \leq \epsilon \quad (24)$$
$$H(M_2|Y^n) \leq \epsilon \quad (25)$$

また，Bob のそれぞれの受信符号語に含まれる雑音の量は Eve のそれぞれの受信符号語に含まれる雑音の量より少ないという仮定より，以下の不等式が成り立つ．

$$I({X_1}^n;{Y}^n|{X_2}) \geq I({X_1}^n;{Z}^n|{X_2}) \quad (26)$$
$$I({X_2}^n;{Y}^n) \geq I({X_2}^n;{Z}^n) \quad (27)$$

式 (18)，(19) より，

$$I({X_1}^n;{Y}^n|{X_2},U) \geq I({X_1}^n;{Z}^n|{X_2},U) \quad (28)$$
$$I({X_2}^n;{Y}^n|U) \geq I({X_2}^n;{Z}^n|U) \quad (29)$$

ここで，$p({x_1}^n,{x_2}^n)=p({x_1}^n)p({x_2}^n)$ であり，U は $U \to ({X_1}^n,{X_2}^n) \to ({Y}^n,{Z}^n)$，${X_1}^n \to U \to {X_2}^n$ となる任意の確率変数である．したがって，次のような結果が得られる．

$$I({X_1}^n;{Y}^n|{X_2},M_1) \geq I({X_1}^n;{Z}^n|{X_2},M_1)$$
$$\geq I({X_1}^n;{Z}^n|M_1) \quad (30)$$

これは，(29) より U を M_1 として，$({X_1}^n,M_1)$ と ${X_2}^n$ が独立していることより導出される．また，(29) より

$$I({X_2}^n;{Y}^n|M_2) \geq I({X_2}^n;{Z}^n|M_2) \quad (31)$$

が導出される．

以上より，安全性の条件から秘匿レートの上界を導出する．

$$\begin{aligned}
R_{1,s} &\leq \frac{1}{n}H(M_1|Z^n) \\
&= \frac{1}{n}H(M_1)-\frac{1}{n}I(M_1;Z^n) \\
&\leq \frac{1}{n}H(M_1)+\frac{1}{n}H(M_1|Y^n) \\
&\quad -\frac{1}{n}I(M_1;Z^n)+\epsilon \quad (32)\\
&= \frac{1}{n}I(M_1;Y^n)-\frac{1}{n}I(M_1;Z^n)+\epsilon \\
&\leq \frac{1}{n}I(M_1;Y^n)-\frac{1}{n}I(M_1;Z^n)+\epsilon \\
&\quad +\frac{1}{n}I({X_1}^n;Y^n|{X_2}^n,M_1) \\
&\quad +\frac{1}{n}I({X_1}^n;Z^n|M_1) \quad (33)\\
&= \frac{1}{n}I(M_1,{X_1}^n;Y^n|{X_2}^n)-\frac{1}{n}I(M_1,{X_1}^n;Z^n)+\epsilon \\
&= \frac{1}{n}I({X_1}^n;Y^n|{X_2}^n)-\frac{1}{n}I({X_1}^n;Z^n)+\epsilon \quad (34)
\end{aligned}$$

(32) は (24) を用いて，(33) は (30) を用いることで成り立つ．(34) は ${X_1}^n$ が与えられたとき M_1 が Y^n, Z^n と独立であることから成り立つ．

$$\begin{aligned}
R_{2,s} &\leq \frac{1}{n}H(M_2|Z^n) \\
&= \frac{1}{n}H(M_2)-\frac{1}{n}I(M_2;Z^n) \\
&\leq \frac{1}{n}H(M_2)+\frac{1}{n}H(M_2|Y^n) \\
&\quad -\frac{1}{n}I(M_2;Z^n)+\epsilon \quad (35)\\
&= \frac{1}{n}I(M_2;Y^n)-\frac{1}{n}I(M_2;Z^n)+\epsilon \\
&\leq \frac{1}{n}I(M_2;Y^n)-\frac{1}{n}I(M_2;Z^n)+\epsilon \\
&\quad +\frac{1}{n}I({X_2}^n;Y^n|M_2)+\frac{1}{n}I({X_2}^n;Z^n|M_2) \quad (36)\\
&= \frac{1}{n}I(M_2,{X_2}^n;Y^n)-\frac{1}{n}I(M_2,{X_2}^n;Z^n)+\epsilon \\
&= \frac{1}{n}I({X_2}^n;Y^n)-\frac{1}{n}I({X_2}^n;Z^n)+\epsilon \quad (37)
\end{aligned}$$

ここで，(35) は (25) を用いて，(36) は (31) を用いることで成り立つ．(37) は ${X_2}^n$ が与えられたとき M_2 が Y^n, Z^n と独立であることから成り立つ．

定理 4　(秘匿レートの下界)．MAC-WT の特殊ケースにおいて，秘匿レート $R_{1,s}, R_{2,s}$ は以下の不等式を満たす．

$$R_{1,s}+R_{1,d} \geq \lim_{n\to\infty}\frac{1}{n}I({X_1}^n;{Y}^n|{X_2}^n)$$

$$R_{2,s}+R_{2,d} \geq \lim_{n\to\infty}\frac{1}{n}I(X_2{}^n;Y^n)$$
$$R_{1,d} \geq \lim_{n\to\infty}\frac{1}{n}I(X_1{}^n;Z^n)$$
$$R_{2,d} \geq \lim_{n\to\infty}\frac{1}{n}I(X_2{}^n;Z^n)$$

証明．まず、MAC-WT モデルにおける符号構成について示す．符号構成はランダム符号を用いる．

(1) **符号生成**：確率 $p(x_1)$ に従い符号語 ${x_1}^n$ を 2^{nR_1} 個生成する．次に，符号語 ${x_1}^n$ を $2^{nR_{1,s}}$ 個の集合に分割する．ここで，集合 $i(1\leq i\leq 2^{nR_{1,s}})$ 内の $j(1\leq j\leq 2^{nR_{1,d}})$ 番目の符号語を ${x_1}^n(i,j)$ とする．$R_{1,d}$ を乱数レートとし，$R_1=R_{1,s}+R_{1,d}$ となる．また，符号語を ${x_1}^n(i,j)$ から成る符号を $C_{1,n}$ とし，Alice，Bob，Carol，Eve に共有されているものとする．同様にして，確率 $p(x_2)$ に従い符号語 ${x_2}^n$ を 2^{nR_2} 個生成する．次に，符号語 ${x_2}^n$ を $2^{nR_{2,s}}$ 個の集合に分割する．ここで，集合 $k(1\leq k\leq 2^{nR_{2,s}})$ 内の $l(1\leq l\leq 2^{nR_{2,d}})$ 番目の符号語を ${x_2}^n(k,l)$ とする．$R_{2,d}$ を乱数レートとし，$R_2=R_{2,s}+R_{2,d}$ となる．また，符号語を ${x_2}^n(k,l)$ から成る符号を $C_{2,n}$ とし，Alice，Bob，Carol，Eve に共有されているものとする．

(2) **符号化**：はじめに，Alice は平文 M_1 から対応する符号語 ${x_1}^n$ の集合 i を選択する．次に，乱数 r_1 により j をランダムに選択し，(i,j) の組とする．同様にして，Carol は平文 M_2 から対応する符号語 ${x_2}^n$ の集合 k を選択する．次に，乱数 r_2 により l をランダムに選択し，(k,l) の組とする．ここで，平文 $m_1\in M_1, m_2\in M_2$ は一様分布とする．以上より，Alice と Carol は符号語 x_1,x_2 を通信路に送信する．

(3) **復号**：はじめに，Bob は符号語 ${x_2}^n$ に関する復号を考える．

$$({x_2}^n,y^n)\in {\mathcal{T}^n}_{[X_2Y]}$$

となる符号 C_2 における符号語 ${x_2}^n$ がただ一つ存在するとき，Bob は (k,l) の組をただ一つ決定できるため元の平文を復号することができる．ここで，${\mathcal{T}^n}_{[X_2Y]}$ は典型系列であり確率 $p(x_2,y)$ より得られる．次に，Bob は符号語 ${x_1}^n$ に関する復号を考える．

$$({x_1}^n,{x_2}^n,y^n)\in {\mathcal{T}^n}_{[X_1X_2Y]}$$

となる符号の組 (C_1,C_2) における符号語の組 $({x_1}^n,{x_2}^n)$ がただ一つ存在するとき，Bob は $(i,j),(k,l)$ の組をただ一つ決定できるため元の平文を復号することができる．ここで，${\mathcal{T}^n}_{[X_1X_2Y]}$ は典型系列であり確率 $p(x_1,x_2,y)$ より得られる．

以上の符号構成，符号化，復号から秘匿レートの下界について導出する．

安全性の定義より，

$$R_{2,s} \leq \frac{1}{n}H(M_2|Z^n)$$
$$H(X_2{}^n) \leq \frac{1}{n}H(M_2|Z^n)+R_{2,d}$$
$$\leq \frac{1}{n}H(X_2{}^n|Z^n)+R_{2,d} \quad (38)$$
$$\frac{1}{n}I(X_2{}^n;Z^n) \leq R_{2,d} \quad (39)$$

ここで，(38) は $H(M_2|Z^n)\leq H(M_2,r_2|Z^n)=H(X_2{}^n|Z^n)$ を用いる．

次に，安全性の定義より，Eve が受信する符号語 Z^n における平文 M_2 のエントロピー量と平文 M_2 のエントロピー量が漸近的に等しくなるとき，秘匿レートの下界は次のように導出される．

$$\begin{aligned}R_{2,s} &= \frac{1}{n}H(M_2|Z^n)\\ &= \frac{1}{n}H(M_2)-\frac{1}{n}I(M_2;Z^n)\\ &= \frac{1}{n}H(M_2)-\frac{1}{n}I(X_2{}^n;Z^n)+\frac{1}{n}H(r_2)-\frac{1}{n}H(r_2|M_2,Z^n)\\ &= \frac{1}{n}H(X_2{}^n)-\frac{1}{n}I(X_2{}^n;Z^n)-\frac{1}{n}H(r_2|M_2,Z^n)\\ &\geq \frac{1}{n}I(X_2{}^n;Y^n)-\frac{1}{n}I(X_2{}^n;Z^n)-\frac{1}{n}H(r_2|M_2,Z^n) \quad (40)\\ &\geq \frac{1}{n}I(X_2{}^n;Y^n)-R_{2,d}-\frac{1}{n}H(r_2|M_2,Z^n) \quad (41)\end{aligned}$$

ここで，(40) は $H(X_2{}^n)\geq I(X_2{}^n;Y^n)$ を用いて，(41) は (39) を用いる．また，n が十分大きいとき $\lim_{n\to\infty}\frac{1}{n}H(r_2|M_2,Z^n)=0$ である．

安全性の定義より，

$$R_{1,s} \leq \frac{1}{n}H(M_1|Z^n)$$
$$H(X_1{}^n) \leq \frac{1}{n}H(M_1|Z^n)+R_{1,d}$$
$$\leq \frac{1}{n}H(X_1{}^n|Z^n)+R_{1,d} \quad (42)$$
$$\frac{1}{n}I(X_1{}^n;Z^n) \leq R_{1,d} \quad (43)$$

ここで，(42) は $H(M_1|Z^n)\leq H(M_1,r_1|Z^n)=H(X_1{}^n|Z^n)$ を用いる．

次に，安全性の定義より，Eve が受信する符号語 ${Z_1}^n$ における平文 M_1 のエントロピー量と平文 M_1 のエントロピー量が漸近的に等しくなるとき，秘匿レートの下界は次のように導出される．

$$\begin{aligned}R_{1,s} &= \frac{1}{n}H(M_1|Z^n)\\ &= \frac{1}{n}H(M_1)-\frac{1}{n}I(M_1;Z^n)\\ &= \frac{1}{n}H(M_1)-\frac{1}{n}I(X_1{}^n;Z^n)+\frac{1}{n}H(r_1)-\frac{1}{n}H(r_1|M_1,Z^n)\\ &= \frac{1}{n}H(X_1{}^n)-\frac{1}{n}I(X_1{}^n;Z^n)-\frac{1}{n}H(r_1|M_1,Z^n)\\ &\geq \frac{1}{n}H(X_1{}^n|X_2{}^n)-\frac{1}{n}I(X_1{}^n;Z^n)-\frac{1}{n}H(r_1|M_1,Z^n)\\ &\geq \frac{1}{n}I(X_1{}^n;Y^n|X_2{}^n)-\frac{1}{n}I(X_1{}^n;Z^n)\\ &\quad -\frac{1}{n}H(r_1|M_1,Z^n) \quad (44)\end{aligned}$$

$$\geq \frac{1}{n} I({X_1}^n; Y^n | {X_2}^n) - R_{1,d} - \frac{1}{n} H(r_1 | M_1, Z^n) \quad (45)$$

ここで，(44) は $H({X_1}^n|{X_2}^n) \geq I({X_1}^n; Y^n|{X_2}^n)$ を用いて，(45) は (43) を用いる．また，n が十分大きいとき $\lim_{n\to\infty} \frac{1}{n} H(r_1|M_1, Z^n) = 0$ である．

5.2 MAC-WT モデルと提案モデルの比較

	平文M_1の秘匿レート$R_{1,s}$の上界	平文M_2の秘匿レート$R_{2,s}$の上界
MAC-WT	$R_{1,s} \leq \lim_{n\to\infty} \frac{1}{n}\{I(X_1^n; Y^n \mid X_2^n) - I(X_1^n; Z^n)\}$	$R_{2,s} \leq \lim_{n\to\infty} \frac{1}{n}\{I(X_2^n; Y^n) - I(X_2^n; Z^n)\}$
提案モデル	$R_{1,s} \leq \lim_{n\to\infty} \frac{1}{n}\{I(X_1^n; Y_1^n \mid X_2^n) + H(c) - I(X_1^n; Z_1^n)\}$	$R_{2,s} \leq \lim_{n\to\infty} \frac{1}{n}\{I(X_2^n; Y_2^n) - I(X_2^n; Z_2^n)\}$

	平文M_1の秘匿レート$R_{1,s}$の下界	平文M_2の秘匿レート$R_{2,s}$の下界
MAC-WT	$R_{1,s} + R_{1,d} \geq \lim_{n\to\infty} \frac{1}{n} I(X_1^n; Y^n)$ $R_{1,d} \geq \lim_{n\to\infty} \frac{1}{n} I(X_1^n; Z^n)$	$R_{2,s} + R_{2,d} \geq \lim_{n\to\infty} \frac{1}{n} I(X_2^n; Y^n)$ $R_{2,d} \geq \lim_{n\to\infty} \frac{1}{n} I(X_2^n; Z^n)$
提案モデル	$R_{1,d} + R_{1,s} \geq \lim_{n\to\infty} \frac{1}{n}\{I(X_1^n; Y_1^n \mid X_2^n) + H(c)\}$ $R_{1,d} \geq \lim_{n\to\infty} \frac{1}{n} I(X_1^n; Z_1^n)$	$R_{2,s} + R_{2,d} \geq \lim_{n\to\infty} \frac{1}{n} I(X_2^n; Y_2^n)$ $R_{2,d} \geq \lim_{n\to\infty} \frac{1}{n} I(X_2^n; Z_2^n)$

MAC-WT モデルの特殊ケースにおける秘匿レートと提案モデルにおける秘匿レートの上界及び下界について比較する．はじめに，秘匿レートの上界について比較する．秘匿レート $R_{1,s}$ に関しては，提案モデルでは秘匿レートの上界が MAC-WT モデルより共通情報のエントロピー量だけ増加し，秘匿レート $R_{2,s}$ に関しては，秘匿レートの上界に変化はない．次に，秘匿レートの下界について比較する．秘匿レートの下界では，安全性の定義から乱数レートを定理 4，定理 6 のように適当に定めることで，秘匿レートの下界が定まる．ここで，比較のために，両モデルにおける乱数レートは等しいものとする．これより，秘匿レート $R_{2,s}$ に関しては，提案モデルでは秘匿レートの下界が MAC-WT モデルより共通情報のエントロピー量だけ増加し，秘匿レート $R_{2,s}$ に関しては，秘匿レートの下界に変化はない．秘匿レートの上界及び下界における比較から，提案モデルにおける秘匿レートの上界及び下界については，MAC-WT モデルの特殊ケースにおける秘匿レートの上界及び下界と比較して，一方の秘匿レートに関して，上界及び下界がそれぞれ共通情報のエントロピー量だけ増加する．以上より，本論文では 2 入力 2 出力の盗聴通信路モデルにおいて，2 入力情報が共通情報を持つモデルを提案し，一方の入力情報の秘匿レートに関して MAC-WT モデルについのて特殊ケースと比較し，共通情報のエントロピー量だけ増加した秘匿レートの上界及び下界を導出したと言える．

6. まとめ

本稿では，2 入力 2 出力の盗聴通信路モデルを提案し，2 入力情報として共通情報を持つモデルについて考察することで，それぞれの入力情報における秘匿レートの上界及び下界を示した．また，提案モデルと MAC-WT モデルの特殊ケースを比較することで，一方の入力情報における秘匿レートの上界及び下界について，提案モデルでは MAC-WT モデルより共通情報のエントロピー量だけ増加することを示した．これより，2 入力情報について共通情報を持つ場合，一方の入力情報を共通情報を取り除いた情報にすることで，秘匿レートの上界及び下界が MAC-WT モデルと比較して増加することを示した．

謝辞 本研究は JSPS 科研費 18H03238 の助成を受けたものです．

参考文献

[1] M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Cambridge University Press, 2011.

[2] A. D. Wyner,“ The wire-tap channel, ”Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[3] E. Tekin and A. Yener, “ The Gaussian multiple access wire-tap channel, ” IEEE Trans. Information. Theory, vol. 54, no. 12, pp. 5747-5755, May. 2008

[4] E. Ekrem and S. Ulukus, “ On the Secrecy of Multiple Access Wiretap Channel, ” 46th Annual Allerton Conference on Communication, Control, and Computing, pp. 1014-1021, Sept. 2008