Wiretap Channel IIにおける能動的攻撃を考慮した暗号通信について

田中 亮大[1]　四方 順司[1,2]

概要：Wiretap Channel II は，通信路上のデータ（符号語）を攻撃者が部分的に盗聴できる通信路モデルである．一方，攻撃者が盗聴した符号シンボルを改ざんできるモデルとして，消失攻撃モデルと反転攻撃モデルの 2 種類が Aggarwal らによって提案されている．本稿では，Wiretap Channel II をベースとして，これらの攻撃をすべて考慮した一般的な攻撃モデルを新たに提案する．また，提案モデルにおける完全秘匿率の上界と下界を導出する．本稿の成果は，Aggarwal らの成果の拡張になっている．

キーワード：Wiretap Channel II，物理層セキュリティ，能動的攻撃者，完全秘匿率

1. はじめに

1.1 背景

Wiretap Channel II は盗聴通信路モデルであり，1984 年に Ozarow と Wyner[5] によって提案され，近年では物理層セキュリティ [2] における代表的な通信路モデルの 1 つになっている．物理層セキュリティとは，ネットワークプロトコルにおける最下層である物理層（通信路）の特性を利用することで情報理論的な安全性を満たす秘匿通信を可能にするものであり，通信路上で雑音などが発生しやすい無線通信に向いている暗号技術として注目されている．Wiretap Channel II では，盗聴者 Eve が通信路上の符号語について部分的に盗聴可能であり，正規の送信者 Alice と受信者 Bob が事前知識としてその盗聴能力を知っていると仮定する．さらに，このモデルにおいて，情報理論的に安全な通信が可能な符号化レート（完全秘匿率）について導出されている．

また，2009 年，Aggarwal ら [6] によって，Wiretap Channel II における能動的攻撃者を考慮した盗聴通信路モデルが提案された．[6] では，能動的攻撃者による符号語への改ざん攻撃モデルとして，反転攻撃モデルと消失攻撃モデルの 2 種類が提案されており，各モデルに対する完全秘匿率が導出されている．ここで，反転攻撃とは通信路上の符号語に対して観測した符号シンボルをそれと異なる符号シンボルに改ざんする攻撃であり，消失攻撃とは観測した符号シンボルを消失させる（消失記号に改ざんする）攻撃である．近年でも，Wang, Safavi-Naini [7] によって，Wiretap Channel II を多元符号による符号構成に拡張し，能動的攻撃者を考慮したモデルとして Adversarial Wiretap Channel が提案されており，反転攻撃モデルと消失攻撃モデルに対する符号構成および完全秘匿率が示されている．

1.2 関連研究

1975 年に Wyner[4] によって，正規の送受信者間の通信路の雑音が送信者と盗聴者間での雑音よりも小さいとき，秘密鍵を用いずに情報理論的に安全性な通信が可能な盗聴通信路モデルとして Wiretap Channel が提案された．次に，Ozarow, Wyner[5] によって，雑音無しの通信路において盗聴者の盗聴能力を制限した盗聴通信路モデルとして Wiretap Channel II が提案され，符号構成法に基づく情報理論的安全性が示された．また，2008 年から Bloch ら [1], [2] が，これら暗号技術を，物理層セキュリティとしてまとめたことで，主に無線通信における安全性の議論に用いられている．以降，様々な盗聴通信路モデル [3] が提案される中で，Wiretap Channel II への能動的攻撃を考慮した盗聴通信路モデルが Aggarwal ら [6] によって提案され，誤り訂正符号を用いて信頼性を向上させた物理層セキュリティに関する研究がおこなわれている．一方で，近年も，能動的攻撃者を想定した攻撃モデルとして，反転攻撃モデル，消失攻撃モデルの 2 種類が主に提案されており，例えば，反転攻撃モデルでは [7]，消失攻撃モデルでは [8] 等が提案されている．

[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

1.3 本稿の貢献

本稿では，Wiretap Channel II において反転攻撃モデルと消失攻撃モデルを同時に扱うことができる一般的な能動的攻撃モデルを提案する．そして，この理論的枠組みの下，安全な通信が可能なレート（完全秘匿率）について解析する．さらに，提案した一般的モデルにおける完全秘匿率の上界および下界を導出する．これらの上界および下界は，Aggarwal ら [6] によって導出された反転攻撃モデル（または消失攻撃モデル）における完全秘匿率の上界および下界の一般化になっていることを示す．

2. Wiretap Channel II と完全秘匿率

本節では準備として Wiretap Channel II と能動的攻撃者による 2 種類の攻撃モデルについてまとめ，各攻撃モデルごとに得られた完全秘匿率について説明する．

2.1 Ozarow-Wyner の盗聴モデル

Wiretap Channel II モデルでは，図 1 のように送信者 Alice が正規の受信者 Bob に符号化した平文を送るとき，盗聴者 Eve がその符号語を盗聴しようとしている状況を想定している．この時，盗聴者 Eve は長さ n の符号語から μ 個の符号シンボルのみをノイズ無く盗聴できるとする．なお，k ビット長の平文 $S^k \in \{0,1\}^k$ と符号語 $X^n \in \mathcal{X}^n \subseteq \{0,1\}^n$ は，それぞれバイナリ列であり，平文は一様分布と仮定する．

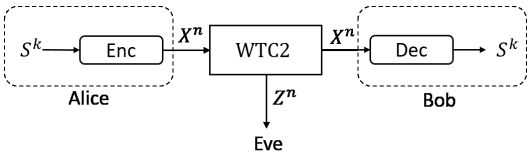

図 1 Wiretap Channel II

盗聴者 Eve の攻撃能力 μ $(0 \le \mu \le n)$ は事前に公開されているものとし，以下のようなフェーズで送受信及び盗聴が行われるものとする．

(1) 送信者 Alice は，暗号化アルゴリズム ENC=$\{f_n\}$（f_n は符号器）を用いて，平文 S^k を符号化し，符号語 X^n を正規の受信者に向けて送信する．

(2) 通信路 WTC2 を通して，盗聴者 Eve は符号語 Z^n を盗聴する．ただし，盗聴可能ビット $\mathcal{L} \subseteq \{1,2,\ldots,n\}$ $(|\mathcal{L}| = \mu)$ により，$Z^n = [z_1,\ldots,z_n]$ は次のように定義される．

$$z_i = \begin{cases} x_i, & \text{if } i \in \mathcal{L}, \\ ?, & \text{otherwise.} \end{cases}$$

ここで記号 “ ? ” は Eve が観測できなかったシンボルを意味する．

(3) 受信者 Bob は符号語 X^n を受信し，復号アルゴリズム DEC=$\{\phi_n\}$（ϕ_n は復号器）を用いて，X^n から平文 S^k を得る．

また，Wiretap Channel II モデルにおいて安全性は次のように定義される．

定義 1 (安全性 [5])．盗聴者 *Eve* の攻撃能力 μ $(0 \le \mu \le n)$ に対して，Δ を以下で定義する：

$$\Delta \triangleq \min_{\mathcal{L}:|\mathcal{L}|=\mu} H(S^k|Z^n)$$

このとき，十分に大きな k に対して $\Delta/k \approx 1$ ならば，安全であると定義する．

以上の盗聴通信路モデルにおいて，$R = k/n$ を完全秘匿率と呼ぶ．このとき，R の限界として以下の不等式が満たされる．

定理 1 (完全秘匿率 [5])．盗聴割合 $\rho = \mu/n$ とする．完全秘匿率 $R = k/n$ は以下の式を満たす．

$$R \le 1 - \rho$$

2.2 Aggarwal らの能動的攻撃モデル

図 2 に Aggarwal ら [6] によって提案されているモデルを示す．このモデルでは，攻撃者は，Wiretap Channel II を介して盗聴した符号語シンボルに対して改ざん攻撃を行えることが想定されている．

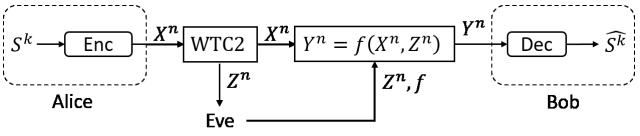

図 2 能動的攻撃者を考慮した Wiretap Channel II

また，改ざん攻撃に関して 2 種類の攻撃モデル（反転攻撃モデル，消失攻撃モデル）が提案されている．それぞれの攻撃モデルについて以下に示す．

(1) 送信者 Alice は，暗号化アルゴリズム ENC=$\{f_n\}$（f_n は符号器）を用いて，一様ランダムな平文 S^k を符号化し，符号語 X^n を正規の受信者に向けて送信する．

(2) 通信路 WTC2 を通して，攻撃者 Eve は符号語 Z^n を盗聴する．また，Eve は Z^n の情報をもとに正規の符号語 X^n に改ざん攻撃を行うことで符号語 $Y^n := f(X^n, Z^n)$ に改ざんする．ここで、f は Eve の戦略アルゴリズムを意味するが，具体的には，以下の 2 種類の攻撃（反転攻撃，消失攻撃）を想定する．以下では，2 種類の攻撃モデルに応じて，$Y^n = [y_1,\ldots,y_n]$ を定義する．

(a) **反転攻撃モデル**: Eve は Z^n の情報をもとに，受信者 Bob に以下の $Y^n = [y_1,\ldots,y_n]$ を受信させることを目的に，X^n の（反転による）改ざんを行う．

$$y_i = \begin{cases} \bar{x_i}, & \text{if } i \in \mathcal{L}, \\ x_i, & \text{otherwise.} \end{cases}$$

図 2 において，反転攻撃モデルを想定した場合は図 3 となる．

(b) **消失攻撃モデル**: Eve は Z^n の情報をもとに，受信者 Bob に以下の $Y^n = [y_1, \ldots, y_n]$ を受信させることを目的に，X^n の（消失による）改ざんを行う．

$$y_i = \begin{cases} \varepsilon, & \text{if } i \in \mathcal{L}, \\ x_i, & \text{otherwise.} \end{cases}$$

ただし，上記において記号 ε は消失記号である．また，図 2 において，消失攻撃モデルを想定した場合は図 4 となる．

(3) 受信者 Bob は符号語 Y^n を受信し，復号アルゴリズム DEC=$\{\phi_n\}$ (ϕ_n は復号器) を用いて，Y^n から平文 $\hat{S^k}$ を得る．

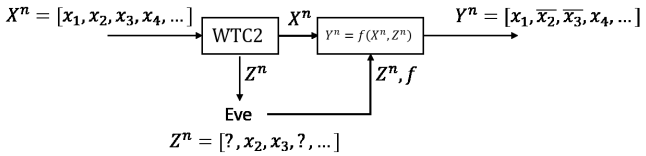

図 3 反転攻撃モデル

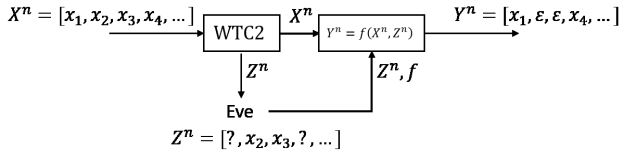

図 4 消失攻撃モデル

また，このモデルでの復号誤り確率 P_e^n は次のように定義される．

定義 2 (復号誤り確率)．復号アルゴリズム（あるいは復号器）DEC=$\{\phi_n\}$ と受信符号語 Y^n より

$$P_e^n := 2^{-k} \sum_{s^k \in \mathcal{S}^k} \Pr\{\phi_n(Y^n) \neq s^k | S^k = s^k\}.$$

復号誤り確率が無視できるほど小さいとき，その通信は信頼性があるといえる．一方で，安全性（秘匿性）については，十分大きな n に対して，$n^{-1}H(S^k|Z^n) \approx n^{-1}H(S^k) = k/n$ をみたすとき，完全秘匿性をもつという．以上より，以下の安全性の定義が与えられる．

定義 3 (安全性)．暗号化システム（ENC=$\{f_n\}$, DEC=$\{\phi_n\}$）は次の条件をみたすとき，完全秘匿率 $R = k/n$ を達成可能であるという．ある自然数 n_0 と任意の自然数 $n \geq n_0$，$|\mathcal{L}| \leq l$ $(< n)$ に対して

$$P_e^n \leq \epsilon,$$
$$\frac{H(S^k|Z^n)}{n} \geq R - \epsilon.$$

このとき，完全秘匿率 R の下界および上界が以下のように示される．ただし，$h(p)$ は 2 値エントロピー関数で

$$h(p) := -p \log p - (1-p) \log(1-p)$$

である．また，$x^+ := \max(x, 0)$ とする．

命題 1 (完全秘匿率の下界 [6])．改ざん割合を $\rho = \mu/n$ とする．このとき，2 種類の攻撃モデルにおける完全秘匿率 $R = k/n$ の下界は，それぞれ以下で与えられる．

(a) 反転攻撃モデル:

$$R \geq (1 - \rho - h(2\rho))^+$$

(b) 消失攻撃モデル:

$$R \geq (1 - \rho - h(\rho))^+$$

命題 2 (完全秘匿率の上界 [6])．改ざん割合を $\rho = \mu/n$ とする．このとき，2 種類の攻撃モデルにおける完全秘匿率 $R = k/n$ の上界は，それぞれ以下で与えられる．

(a) 反転攻撃モデル:

$$R \leq (1 - \rho - h(\rho))^+$$

(b) 消失攻撃モデル:

$$R \leq (1 - \rho - h(\rho/2))^+$$

3. 提案モデル

本節では 2 節のモデルを以下のように拡張する．Eve は盗聴した符号語シンボルに対して，反転割合 δ だけ反転改ざん攻撃を，$(1-\delta)$ だけ消失改ざん攻撃を行う．

盗聴者 Eve の攻撃能力 $\mu (0 \leq \mu \leq n)$ および反転割合 $\delta (0 \leq \delta \leq 1)$ は事前に公開されているものとし，以下のようなフェーズで送受信及び盗聴が行われるものとする．

(1) 送信者 Alice は，暗号化アルゴリズム ENC=$\{f_n\}$（f_n は符号器）を用いて，一様ランダムな平文 S^k を符号化し，符号語 X^n を正規の受信者に向けて送信する．

(2) 通信路 WTC2 を通して，盗聴者 Eve は符号語 Z^n を盗聴する．ただし，盗聴可能ビット $\mathcal{L} \subseteq \{1, 2, \ldots, n\}$ $(|\mathcal{L}| = \mu)$ により，$Z^n = [z_1, \ldots, z_n]$ は次のように定義される．

$$z_i = \begin{cases} x_i, & \text{if } i \in \mathcal{L}, \\ ?, & \text{otherwise.} \end{cases}$$

また，Eve は Z^n の情報をもとに正規の符号語 X^n に改ざん攻撃を行うことで符号語 $Y^n := f(X^n, Z^n)$ に改ざんする．ここで、f は Eve の戦略アルゴリズムを意味するが，具体的には，以下のような攻撃を想定する．Eve は Z^n の情報をもとに，受信者 Bob に以下の $Y^n = [y_1, \ldots, y_n]$ を受信させることを目的に，X^n

の（反転と消失による）改ざんを行う．反転攻撃ビット $\mathcal{F} \subseteq \mathcal{L}(|\mathcal{F}| = \mu\delta)$ より，

$$y_i = \begin{cases} \bar{x_i}, & \text{if } i \in \mathcal{F}, \\ \varepsilon, & \text{if } i \in \mathcal{L} \setminus \mathcal{F}, \\ x_i, & \text{otherwise.} \end{cases}$$

ただし，上記において記号 ε は消失記号である．また，$0 < \delta < 1$ のとき，提案攻撃モデルを想定した例として図 5 が考えられる．一方で，$\delta = 1$ のとき，反転攻撃モデルとなり，$\delta = 0$ のとき，消失攻撃モデルとなるため，上記の攻撃モデルは [6] の攻撃モデルを拡張したモデルであると言える．

(3) 受信者 Bob は符号語 Y^n を受信し，復号アルゴリズム DEC=$\{\phi_n\}$ (ϕ_n は復号器) を用いて，Y^n から平文 $\hat{S^k}$ を得る．

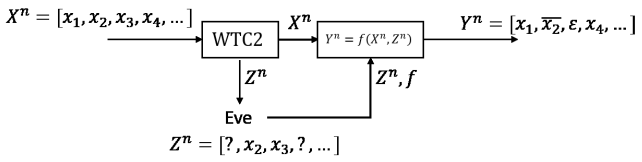

図 5 提案モデル

また，提案モデルでの復号誤り確率および安全性定義は定義 2，定義 3 と同じとする．

4. 提案モデルにおける完全秘匿率

本節では提案モデルにおける完全秘匿率の限界について示す．達成可能な完全秘匿率 R は，一般に，攻撃者の攻撃能力 (μ, δ) に依存する．したがって，R の上界，下界を ρ, $\delta(\rho = \mu/n)$ を使って導出する．

4.1 下界の導出

ENC の構成として Varshamov-Gilbert 限界（VG 限界）を満たす線形符号を利用する．これにより，符号の完全秘匿率 R の下界を以下のように示す．

定理 2 (完全秘匿率の下界)**.** 提案モデルにおいて，完全秘匿率 $R = k/n$ は以下の不等式を満たす．

$$\rho = \mu/n,$$
$$R \geq (1 - \rho - h(\rho\delta + \rho))^+.$$

証明. 命題 1 の証明法の類似により示す．まず符号構成について示す．符号構成は，VG 限界を満たし，$m \times n$ の生成行列 G によって符号語が生成されるものとする．なお，$m \geq k$ で $\mathcal{X}^m$ は全ての m-bit のバイナリ文字列の集合とし，以下を満たすとする．

符号構成

1) $m/n \geq 1 - h(\rho\delta + \rho) - \epsilon$,
2) $\forall x^m \in \mathcal{X}^m,\ wt(x^m G) \geq 2\mu\delta + \mu(1 - \delta)$,
3) G の l 列からなる任意の部分行列 G_l について，以下の l_2 に対して $rank\{G_l\} \geq l_2$ が満たされる:

$$l_2 := l - \frac{1}{m - l + 1} \log_2 \left(\frac{2\binom{n}{l}}{\prod_{i=1}^{\infty}(1 - \frac{1}{2^i})} \right).$$

1) は符号語 X^n に対して，$\mu\delta$ 個のビット誤りと $\mu(1 - \delta)$ 個のビット消失が起きる場合の VG 限界である [9]．また，2),3) では生成行列 G が混合攻撃に対して誤り訂正能力を持っていることを表している．また，生成行列 G の存在については，[6] の Lemma1 より，n が十分に大きいときに保証されることが証明されている．これによって生成される長さ n の 2^m 個の符号語の集合を符号語集合 C とする．この符号語集合 C を $A_i (1 \geq i \geq 2^k)$ に分割する．ただし，各 A_i は元の位数が等しいとする．したがって，A_i はそれぞれ 2^{m-k} 個の符号語の集合である．このとき各 A_i が各平文と対応している．$\{A_i\}$ は以下のような条件を満たすとする．

条件: Eve は $x^n \in C$ から $z^n \in \{0, 1, ?\}^n$ を得る．このとき，x^n の符号シンボルを部分的に消失シンボルに変更することで z^n が得られる場合，x^n と z^n は consistent であるといい，各 A_i は次の条件を満たすようにする．ただし，L は $L \geq 1$ となる整数とする．

$$|\{x^n \in A_i | z^n \text{ is consistent with } x^n\}| < L.$$

次に，ENC と DEC の構成について示す．ENC では，平文に対応する A_i 内から一様ランダムに符号語を選び出し，受信者に向けて送信する．DEC では，$\mu\delta$ 個の誤りと $\mu(1 - \delta)$ 個の消失が発生している n-bit の符号語を受け取り，誤り訂正をおこなって元の符号語を得た後，その符号語が含まれる A_i とそれに対応する平文を得る．したがって，DEC での復号誤り確率は $P_e = 0$ となる．

以上より，Eve が符号語 Z^n を受け取ったうえでの平文 S^k の曖昧さが漸近的に平文 S^k の曖昧さと同じになり，完全秘匿率の下界が与えられることを示す．

$$\begin{aligned} \Delta &= H(S^k|Z^n) \\ &= H(S^k, Z^n) - H(Z^n) \\ &= H(S^k|X^n, Z^n) + H(X^n|Z^n) - H(X^n|S^k, Z^n) \\ &\geq H(X^n|Z^n) - H(X^n|S^k, Z^n) \end{aligned}$$

また，$H(X^n|Z^n) \geq H(X^n) - H(Z^n) \geq m - \mu$ であるため，

$$\Delta \geq m - \mu - H(X^n|S^k, Z^n)$$

となる．また，$\{A_i\}$ の条件から

$$\Delta \geq m - \mu - \log L$$

よって n が十分に大きいとき，論文 [6] での議論と同様に

$$\Delta/n \geq 1 - h(\rho\delta + \rho) - \rho - \epsilon$$

となり，定義 3 から

$$R \geq (1 - \rho - h(\rho\delta + \rho))^+$$

□

4.2 上界の導出

本稿での提案モデルにおいて，Eve の攻撃能力 μ，反転割合 δ から，安全性定義を達成する完全秘匿率 R の上界が以下のように求められる．

定理 3 (完全秘匿率の上界)．提案モデルにおいて，完全秘匿率 $R = k/n$ は以下の不等式をみたす．

$$R \leq (1 - \rho - h((\rho\delta + \rho)/2))^+$$

ただし，$\rho = \mu/n$.

証明． 完全秘匿率は [4] より，Alice-Bob 間の通信路容量 C_{AB} と Alice-Eve 間の通信路容量 C_{AE} および通信路への符号語の完全秘匿率 R から，$C_{AB} - C_{AE} \geq R$ を満たす．まず，通信路容量 C_{AE} は，Eve が符号長 n の符号語から μ 個のみノイズ無しで受信でき，それ以外については記号 “？” を得るということから，盗聴割合 $\rho = \mu/n$ より，$C_{AE} = \rho$ である．

次に通信路容量 C_{AB} について求める．Alice-Bob 間の通信路上では，符号語 X^n に対して $\mu\delta$ 個の誤りと $\mu(1-\delta)$ 個の消失が発生する．こういった通信路において，Hamming 限界を用いることで誤り訂正可能な伝送レート R の上界を求めることができる [9]．したがって，符号長 n の任意の符号に対して，最小重み $wt(x^m G) \geq 2\mu\delta + \mu(1-\delta)$ から，漸近的に

$$1 - h(\frac{2\mu\delta + \mu(1-\delta)}{2n}) \geq R$$

が示され，通信路容量 C_{AB} について以下のように与えられる．

$$C_{AB} = 1 - h((\rho\delta + \rho)/2)$$

したがって，完全秘匿率の上界は，

$$(1 - \rho - h((\rho\delta + \rho)/2)) \geq R$$

□

5. 既存研究との比較

本節では既存研究で提案された 2 種類の攻撃モデルと本稿で提案した提案モデルの完全秘匿率について比較を行う．

ここで, δ $(0 \leq \delta \leq 1)$ は提案モデルにおける反転割合を表す．まず，$\delta = 1$ のとき，提案モデルは反転攻撃モデルと同じであり，このとき，提案モデルにおいて導出した完全秘匿率の上界及び下界は，従来の反転攻撃における完全秘匿率の上界及び下界にそれぞれ一致する。次に，$\delta = 0$ のとき，提案モデルは消失攻撃モデルと同じであり，このとき，提案モデルにおいて導出した完全秘匿率の上界及び下界は，従来の消失攻撃における完全秘匿率の上界及び下界にそれぞれ一致する。以上より，従来の反転攻撃や消失攻撃は，提案モデルの特別なケース（$\delta = 1$ or 0) に相当し，従来の攻撃モデルにおける完全秘匿率の上界及び下界も，本論文で導出した完全秘匿率の上界及び下界の特別なケースに相当する．さらに，提案モデルは，従来は扱えていなかった反転攻撃と消失攻撃の混合攻撃を記述可能であり，また本論文ではそのような複雑な攻撃モデルにおける完全秘匿率の上界及び下界を新たに導出できている．以上より，本論文では既存研究の能動的攻撃モデルを統合的に一般化したモデルを提案し，そのモデルにおける一般的な秘匿率の上界及び下界を導出できたと言える．

攻撃モデル	完全秘匿率の下界	完全秘匿率の上界
反転攻撃モデル [6]	$R \geq (1 - \rho - h(2\rho))^+$	$R \leq (1 - \rho - h(\rho))^+$
消失攻撃モデル [6]	$R \geq (1 - \rho - h(\rho))^+$	$R \leq (1 - \rho - h(\frac{\rho}{2}))^+$
提案モデル	$R \geq (1 - \rho - h(\rho\delta + \rho))^+$	$R \leq (1 - \rho - h(\frac{(\rho\delta+\rho)}{2}))^+$

6. まとめ

本稿では，能動的攻撃を考慮した Wiretap Channel II において，反転および消失による改ざん攻撃が同時に行える能動的攻撃モデルを提案し，完全秘匿率の下界および上界を示した．また，提案モデルは既存研究 [6] で与えられている 2 種類の攻撃モデル (反転攻撃モデルと消失攻撃モデル) を反転割合 δ の設定によって表現可能であるため，既存研究 [6] を拡張したモデルであると言える．以上より，本論文では既存研究の能動的攻撃モデルを統合的に一般化したモデルを提案し，そのモデルにおける一般的な秘匿率の上界及び下界を導出した．

謝辞 本研究は JSPS 科研費 15H02710 の助成および文部科学省国立大学改革強化推進事業の支援を受けたものです。

参考文献

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,”IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security, vol. 54, pp. 2515–2534, June. 2008.

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

[3] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,”IEEE Commun. Surveys

Tuts., vol. 16, no. 3, pp. 1550–1573, Mar. 2014.
[4] A. D. Wyner, "The Wire-Tap Channel," Bell System Technical Journal, vol. 54, pp. 1355–1387, Oct. 1975.
[5] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," Bell System Technical Journal, vol. 63, pp. 2135–2157, Dec. 1984.
[6] V. Aggarwal, L. Lai, A. R. Calderbank and H. V. Poor, "Wiretap channel type II with an active eavesdropper," IEEE International Symposium on Information Theory, pp. 1944–1948, Jul. 2009.
[7] P. Wang and R. Safavi-Naini, "A model for adversarial wiretap channels," IEEE Transactions on Information Theory, vol. 62, no. 2, pp. 970–983, Feb. 2016.
[8] P. Wang, R. Safavi-Naini and F. Lin, "Erasure Adversarial Wiretap Channels," 53rd Annual Allerton Conference on Communication, Control, and Computing, pp. 1061–1068, Sept. 2015.
[9] R. Pellikaan, X. Wu, S. Bulygin and R. Jurrius, "Error-correcting codes," 2015, `http://www.win.tue.nl/~ruudp/courses/2WC11/2WC11-book.pdf`