Secret Key Capacity of Wireless Key Agreement Based on Correlated Gaussian Information Source ー Part II: Mobile Communication Channel Model ー

Hideichi SASAOKA*

(Received January 19, 2016)

Wireless physical layer security schemes such as secret key agreement and secret data transmission have attracted attention in current wireless community. For the secret key agreement from correlated information, a general formula of the secret key capacity is given, but a specific formula of the secret key capacity has not been presented for secret key agreement from correlated information in wireless channels. This paper deals with the theoretical analysis on the secret key capacity for the Gaussian correlated information in mobile communication channel. The analysis result shows that the upper bound of the secret key capacity is given with conditional mutual information and that the formulas of the upper and lower bounds are expressed as functions of the correlation of channel coefficient between eavesdropper and legitimate user, the signal-to-noise power ratio, and the noise power ratio of eavesdropper to legitimate user.

Key Word：key agreement, secret key capacity, correlated information, mobile communication channel

キーワード：鍵共有，秘密鍵容量，相関情報，移動通信路

無線通信におけるガウス性相関情報に基づく秘密鍵共有の秘密鍵容量 ―（その２）移動通信路モデル―

笹岡　秀一

１．はじめに

近年，移動通信など無線通信の普及が目覚ましいが，無線通信は開かれた空間を通して電波の送受を行うため，盗聴や不正アクセスなど情報セキュリティ上の脆弱性が問題となっている．この盗聴対策としては，共通鍵暗号方式や公開鍵暗号方式など用いられることが多い．なお，移動通信の場合，公開鍵暗号方式は端末での処理演算量に問題があるため，共通鍵暗号方式が用いられるのが一般的である．しかし，共通鍵暗号方式は鍵管理や鍵配送が必要であること，端末の紛失・盗難の危険性があることが問題である．また，これらの暗号技術の安全性は，計算量的な複雑性を根拠としており，演算能力の向上や新アルゴリズムの発見により安全性が低下する懸念がある．

これらの従来方式と異なり情報理論的な複雑性を安全性の根拠とする暗号技術も研究されている[1,2]．これらには，使い捨て鍵（ワンタイムパッド）を用いた暗号方式（シャノンの暗号方式）[3]，雑音のある通信路を用いた鍵配送（盗聴通信路を用いた鍵配

*Department of Electronics, Doshisha University, Kyoto
Telephone: +81-774-65-6355, Fax: +81-774-65-6801, E-mail: hsasaoka@mail.doshisha.ac.jp

送）[4]，相関情報を用いた秘密鍵共有[5]などがある．また，量子通信路を用いた鍵配送[6]もこれに属する技術と考えることができる．これらの暗号技術のうちで，通信路雑音を活用した方式は比較的簡易で現実的とも思えるが，現在は存在性を議論する理論的研究が多く，実用性が疑問視されている[2]．一方，より現実的なものとして，移動通信路特性を用いた秘密鍵共有[7,8]と秘密情報伝送が提案されている[9]．この秘密鍵共有は，相関に基づく秘密鍵共有の一種であるが，移動通信における電波伝搬特性を活用して実用的な鍵共有を実現している[10]．すなわち，電波伝搬の可逆性により正規者間で相関性の高い秘密情報を共有する一方で，電波伝搬の場所依存性によって盗聴者の情報推定を阻止している[11]．

相関情報を用いた秘密鍵共有においては，その共有アルゴリズムとともに共有可能な情報量の理論的検討が重要である．これについては，正規者（アリス，ボブ）と盗聴者（イブ）が相関情報（ディジタル情報）を受け取る一方，公開通信路を用いてアリスとボブが情報を送受することにより鍵共有を図るモデルに対して，秘密鍵容量が求められている[5,12]．ここで，相関情報は多値又は２値の相関のある離散乱数（離散的な確率変数）で，その入手法には衛星通信の利用や二元対称通信路での誤り発生などがある[5,13]．一方，移動通信路を用いた秘密鍵共有では，フェージング変動などガウス分布する連続な確率変数を観測して，離散的な量子化された標本値（離散的な確率変数）を相関情報とする場合がある．その場合に，量子化刻みを微小に設定し，相関のあるガウス分布するアナログ情報に対する条件付き相互情報量を求め，正規者が共有可能な情報量の上限を評価している[14,15]．しかし，陸上移動通信路を対象とし，より厳密な秘密鍵容量を用いて鍵共有特性を評価した例は少なく，衛星通信路モデルを対象にした詳しい理論解析が行われているのみである[16]．

そこで，本論文では，無線通信におけるガウス性相関情報に基づく秘密鍵共有の秘密鍵容量を検討した．はじめに，相関情報に基づく秘密鍵共有の原理とその秘密鍵容量の上限と下限を示すとともに，相関のあるガウス性情報の相互情報量の解析法を示す．次に，陸上移動通信路モデルを対象にし，相関のあるガウス性情報を用いた場合の秘密鍵容量の上限と下限について理論解析を行った．

２．相関情報に基づく秘密鍵共有と秘密鍵容量

2.1 相関情報に基づく秘密鍵共有の原理

相関を用いた秘密鍵共有法を一般化すると Fig.1 の構成になる．図は，正規者（アリス，ボブ）が，お互いに相関のある乱数を受け取り，公開通信路を通して情報($C_1,C_2,\cdot\cdot$)を送受することで，イブに知られない秘密鍵を共有する構成を示している．

ここで，秘密鍵共有のプロトコルは，①Advantage distillation，②Information reconciliation，③Privacy amplification の三段階から構成される[17]．ステップ①は，正規ユーザ間の相互情報量が，一方のユーザと盗聴者との相互情報量より小さい場合に，公開通信路による情報交換で改善を行う．ステップ②は，相関のある関数系列からイブに対する秘密を保持しながら，アリスとボブの乱数系列を一致させる．ステップ③は，アリスとボブで一致している乱数系列からイブが知ることができない秘密鍵を生成する．ここで，あるプロトコルを用いてイブに知られないでアリスとボブ間で共有できた鍵生成の速度を鍵レートと呼び，実現可能な鍵レートの上限を秘密鍵容量と呼ぶ．

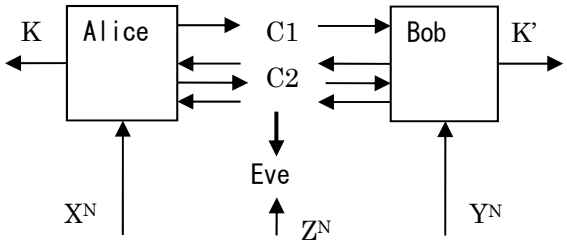

Fig. 1. Secret key agreement from correlated information.

2.2 秘密鍵容量の上限と下限

Fig. 1 に示す秘密鍵共有法に対して，秘密鍵容量 $S(X;Y||Z)$ の上限と下限は，

$$S(X;Y||Z) \le min[I(X;Y), I(X;Y|Z)] \qquad (1)$$

$$S(X;Y||Z) \geq max[I(X;Y)-I(X;Z),\ I(X;Y)-I(Y;Z)] \quad (2)$$

で与えられる[5]．ここで，X, Y, Zは相関のある有限の離散乱数を想定しているのみで，その分布に無関係に成り立つ式である．したがって，X,Y,Z に特定の条件がある場合，システムに追加的な条件がある場合には，さらに正確な秘密鍵容量が求められる．特に，アリスとボブの鍵生成を助けるヘルパーが存在し，ヘルパーとイブがともにZの情報を得るとき，秘密鍵容量は，

$$S(X;Y||Z) = I(X;Y|Z) \quad (3)$$

で与えられる[18]．

式(1)と式(2)において X, Y の相互情報量 $I(X;Y), I(X;Z), I(Y;Z)$ や条件付き相互情報量 $I(X;Y|Z)$ と，X, Y, Zのエントロピー $H(X), H(Y), H(Z)$ や結合エントロピー $H(X,Y), H(X,Z), H(Y,Z)$ および条件付きエントロピー $H(X|Y), H(Y|X)$ などは，Fig.2 に示すような関係にある．ここで，相互情報量 $I(X;Y)$ は，

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) \quad (4)$$

と表され，$H(X;Z), H(Y;Z)$ も同様に表される．一方，$I(X;Y|Z)$ は，

$$I(X;Y|Z) = H(X,Z) + H(Y,Z) - H(Z) - H(X,Y,Z) \quad (5)$$

と表される．

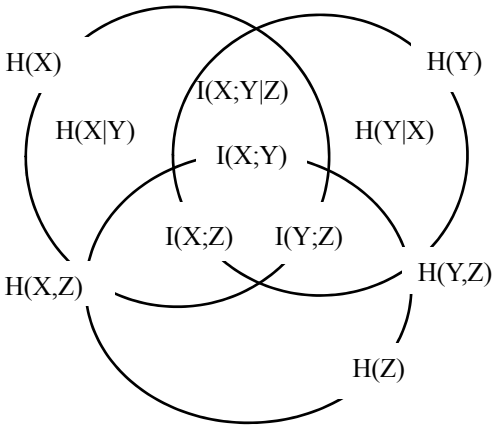

Fig. 2. Relation between entropy and mutual information.

2.3 ガウス変数の相互情報量

ガウス分布する連続な確率変数を離散的に量子化した標本値を相関情報とした場合に，その相互情報量は量子化刻みに依存し，理論解析が煩雑となる．そこで，以下では量子化刻みを微小に設定した極限を想定し，アナログ情報源の相互情報量の解析手法を使用し理論解析を行う．

アナログ情報源のエントロピーは，量子化刻みを無限小にした極限において無限大に発散する．しかし，量子化刻みを共通にした場合の二つのアナログ情報源のエントロピーの差は有限となり，意味をもつ[19]．そして，ディジタル（離散）の場合の確率分布を確率密度関数で置換え，和を積分に置換えれば，アナログ（連続）の場合のエントロピーが定義できる．

文献[18]によれば，X と Z を平均が 0，分散が σ_x^2, σ_z^2 でお互いに独立な確率変数とし $Y = X + Z$ とすると，X と Y は相関のあるガウス変数となり，相互情報量 $I(X;Y)$ は以下のように求められる．はじめに，エントロピー $H(X), H(Y)$ は，

$$H(X) = log_2\sqrt{2\pi e\sigma^2} \quad (6)$$

$$H(Y) = log_2\sqrt{2\pi e(\sigma_x^2 + \sigma_y^2)} \quad (7)$$

となる．なお，X,Y を信号とみなすと，$\sigma_x^2,\ \sigma_y^2 = \sigma_x^2 + \sigma_z^2$ が信号電力に相当する．次に，$H(Y|X)$ は，

$$H(Y|X) = log_2\sqrt{2\pi e\sigma_z^2} \quad (8)$$

となる．なお，式(7)は X を知った条件の下での Y のエントロピーであるので，Y から X を引いて $Z = Y - X$ としてもエントロピーが変化しないことと X と Z が独立であることから，$H(Y|X) = H(Y-X|X) = H(Z|X) = H(Z)$ を用いて容易に求められる．

この結果，相互情報量 $I(X;Y)$ は，$I(X;Y) = H(Y) - H(Y|X)$ を用いて，

$$I(X;Y) = log_2\sqrt{\frac{\sigma_x^2+\sigma_y^2}{\sigma_z^2}} \quad (9)$$

となる．

３．相関情報を用いた移動通信路の秘密鍵容量

3.1 陸上移動通信路モデル

正規者（アリスとボブ）がお互いに既知の信号 T

を送信し，信号 S･T を受信することで，伝搬路特性 S を得るモデル（陸上移動通信路モデル）を考える．また，盗聴者は，S と相関のある S'の伝搬路特性を得るものとする．ここで，S' は，S と相関のある成分と無相関の成分の和で表され，$S' = \rho S + \sqrt{1-\rho^2}W$ と表される．なお，それぞれで得られた伝搬路特性には受信雑音が含まれるものとする．このようなモデルを Fig. 3 に示す.

Fig. 3 に示すように，$X = S + N_x$，$Y = S + N_y$，$Z = S' + N_z$ となる．また，S，W，N_x，N_y，N_z，がお互いに独立なガウス変数とし，それぞれの電力を P_s，P_w=P_s，P_x，P_y，P_z とする．なお，S' の電力は，$P_{S'} = \overline{S'^2} = \rho^2 P_s + (1-\rho^2)P_w = P_s$ となる．X, Y, Zのエントロピー $H(X), H(Y), H(Z)$ は，その分散（電力）を用いて，

$$\begin{aligned} H(X) &= log_2\sqrt{2\pi e(P_s + P_x)} \\ H(Y) &= log_2\sqrt{2\pi e(P_s + P_y)} \\ H(Z) &= log_2\sqrt{2\pi e(P_s + P_z)} \end{aligned} \tag{10}$$

と表される.

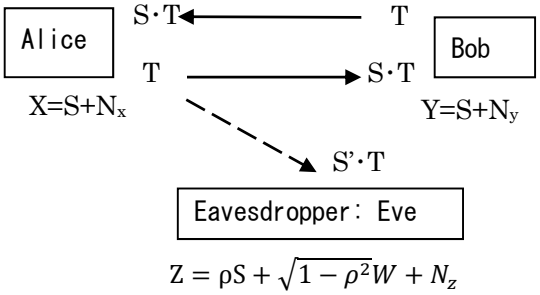

Fig. 3. Land mobile communication channel model.

3.2 ガウス性相関情報の相互情報量

Fig.3 の陸上移動通信路モデルにおいて，X と Y の 2 変数間の相互情報量 $I(X;Y)$ は，衛星通信路モデル [16]の場合と同様に，

$$I(X;Y) = log_2\sqrt{\frac{(P_s+P_x)(P_s+P_y)}{P_s(P_x+P_y)+P_xP_y}} \tag{11-1}$$

となる．また，$I(X;Z), I(Y;Z)$ は，付録 A の式(A-8)と同様な導出により，

$$\begin{aligned} I(X;Z) &= log_2\sqrt{\frac{(P_s+P_x)(P_s+P_z)}{A}} \\ A &= (1-\rho^2){P_s}^2 + P_s(P_x + P_z) + P_xP_z \end{aligned} \tag{11-2}$$

$$\begin{aligned} I(Y;Z) &= log_2\sqrt{\frac{(P_s+P_y)(P_s+P_z)}{B}} \\ B &= (1-\rho^2){P_s}^2 + P_s\left(P_y + P_z\right) + P_yP_z \end{aligned} \tag{11-3}$$

となる.

一方，Xと Yの結合エントロピー $I(X;Y)$ は，衛星通信路モデル [16]の場合と同様に，

$$\begin{aligned} &H(X,Y) \\ &= log_2\sqrt{(2\pi e)^2\{P_s\left(P_x + P_y\right) + P_xP_y\}} \end{aligned} \tag{12-1}$$

となる．また，X, Y と Z の結合エントロピー $H(X,Z)$, $H(Y,Z)$ は，付録 A の式(A-9)と同様な導出により，

$$\begin{aligned} H(X,Z) &= log_2\sqrt{(2\pi e)^2 A} \\ H(Y,Z) &= log_2\sqrt{(2\pi e)^2 B} \end{aligned} \tag{12-2}$$

となる．さらに，X, Y, Z 間の結合エントロピー $H(X,Y,Z)$ は，付録 B の式(B-8)より，

$$\begin{aligned} H(X,Y,Z) &= log_2\sqrt{(2\pi e)^3 C} \\ C &= (1-\rho^2){P_s}^2\left(P_x + P_y\right) \\ &\quad + P_s\left(P_xP_y + P_yP_z + P_zP_x\right) + P_xP_yP_z \end{aligned} \tag{13}$$

となる．これらの結果から条件付き相互情報量 $I(X;Y|Z)$ は，式(10)，式(12-2)，式(13)を式(5)に代入して，

$$I(X;Y|Z) = log_2\sqrt{\frac{AB}{(P_s+P_z)C}} \tag{14}$$

となる.

3.3 秘密鍵容量の上限式の導出

秘密鍵容量の上限 $S(X;Y||Z)_{up}$ は，式(1)に示されるように $I(X;Y)$ と $I(X;Y|Z)$ の最小値となる．そこで，$I(X;Y)$ と$I(X;Y|Z)$ の大小関係を検討する．式(11-1)，式(14)より，

$$\begin{aligned} I(X;Y) - I(X;Y|Z) &= log_2\sqrt{\frac{D}{E}} \\ D &= (P_s + P_x)\left(P_s + P_y\right)(P_s + P_z)C \\ E &= \{P_s\left(P_x + P_y\right) + P_xP_y\}AB \end{aligned} \tag{15}$$

となる．式(15)において D, Eは，$D > 0$, $E > 0$ であるので，$D > E$ の場合に $I(X;Y) - I(X;Y|Z) > 0$ となる.

そこで，Dを展開して P_sの冪で整理すると，

$$\begin{aligned}D &= a_5{P_s}^5 + a_4{P_s}^4 + a_3{P_s}^3 + a_2{P_s}^2 + a_1P_s + a_0\\ a_5 &= (1-\rho^2)\left(P_x + P_y\right)\\ a_4 &= (1-\rho^2)\left(P_x + P_y\right)P_1 + P_2\\ a_3 &= (1-\rho^2)\left(P_x + P_y\right)P_2 + P_1P_2 + P_3\\ a_2 &= (1-\rho^2)\left(P_x + P_y\right)P_3 + {P_2}^2 + P_1P_3\\ a_1 &= 2P_2P_3\\ a_0 &= {P_3}^2\end{aligned} \tag{16}$$

と表される．ここで，　$P_1 = P_x + P_y + P_z$　，$P_2 = P_xP_y + P_yP_z + P_zP_z$　，　$P_3 = P_xP_yP_z$　とする．

一方，

$$\begin{aligned}E &= b_5{P_s}^5 + b_4{P_s}^4 + b_3{P_s}^3 + b_2{P_s}^2 + b_1P_s + b_0\\ b_5 &= (1-\rho^2)^2\left(P_x + P_y\right)\\ b_4 &= (1-\rho^2)\left(P_x + P_y\right)(P_1 + P_z) + (1-\rho^2)^2P_xP_y\\ b_3 &= (1-\rho^2)\left\{\left(P_x + P_y\right)P_2 + 2P_3\right\} + P_1P_2 - P_3\\ b_2 &= (1-\rho^2)\left(P_x + P_y\right)P_3 + {P_2}^2 + P_1P_3\\ b_1 &= 2P_2P_3\\ a_0 &= {P_3}^2\end{aligned} \tag{17}$$

となる．式(16)，式(17)より，

$$\begin{aligned}a_5 - b_5 &= \rho^2(1-\rho^2)\left(P_x + P_y\right) \geq 0\\ a_4 - b_4 &= \rho^2P + (1-\rho^2)P_xP_y\} \geq 0\\ a_3 - b_3 &= 2\rho^2P_3 \geq 0\end{aligned} \tag{18-1}$$

であることから，常に

$$\begin{aligned}D - E = (a_5 - b_5){P_s}^5 + (a_4 - b_4){P_s}^4\\ +(a_3 - b_3){P_s}^3 \geq 0\end{aligned} \tag{18-2}$$

が成り立つ．この結果，式(15)が常に正となることから秘密鍵容量の上限は，

$$\begin{aligned}S(X;Y||Z)_{\mathrm{up}} &= min[I(X;Y), I(X;Y|Z)]\\ &= I(X;Y|Z)\end{aligned} \tag{19}$$

となる．式(19)は，陸上移動通信路モデルにおけるガウス性の相関情報の場合に常に成り立つ．

3.4 秘密鍵容量の上限の検討

ここでは，式(14)で与えられる条件付き相互情報量が，信号と雑音の電力 P_s, P_x, P_y, P_z の大小関係，および伝搬路特性の相関係数 ρ によりどのようになるかを検討する．式(14)の√内の分子 Fと分母 Gを展開して P_sの冪で整理すると，

$$\begin{aligned}F &= (1-\rho^2)^2{P_s}^4 + (1-\rho^2)(P_1 + P_z){P_s}^3\\ &+\{(1-\rho^2)\left(P_x + P_y\right)P_z + \left(P_2 + {P_z}^2\right)\}{P_s}^2\\ &+\left(P_xP_y + P_2\right)P_zP_s + P_3P_z\end{aligned} \tag{20-1}$$

$$\begin{aligned}G &= (1-\rho^2)\left(P_x + P_y\right){P_s}^3\\ &+\{(1-\rho^2)\left(P_x + P_y\right)P_z + P_2\}{P_s}^2\\ &+\left(P_xP_y + P_2\right)P_zP_s + P_3P_z\end{aligned} \tag{20-2}$$

となる．式(20)を用いて式(14)を変形すると，

$$\begin{aligned}S(X;Y||Z)_{\mathrm{up}} &= I(X;Y|Z)\\ &= \log_2\sqrt{1 + \frac{(1-\rho^2)^2{P_s}^4 + 2(1-\rho^2)P_z{P_s}^3 + {P_z}^2{P_s}^2}{G}}\end{aligned} \tag{21}$$

となる．

式(21)は，　P_s, P_x, P_y, P_z, ρ に依存するが，正規者 A と B の雑音電力を等しい $(P_x = P_y)$ と仮定し，正規局の信号対雑音電力比（SN 比）を $\gamma = P_s/P_x$ ，盗聴者対正規者電力比を $\alpha = P_z/P_x$ で表すと，

$$S(X;Y||Z)_{\mathrm{up}} = \log_2\sqrt{\frac{\{(1-\rho^2)\gamma^2 + \gamma(\alpha+1) + \alpha\}^2}{(\gamma+\alpha)\{2(1-\rho^2)\gamma^2 + \gamma(\alpha+1) + \alpha\}}} \tag{22}$$

と数式の簡略化が可能となる．

式(22)において相関 $\rho = 0$ の場合，

$$S(X;Y||Z)_{\mathrm{up}} = \log_2\sqrt{1 + \frac{\gamma^2}{(\gamma+1)}} \tag{23}$$

となり，α に依存しない．一方，盗聴者が非常に有利な条件である盗聴者の受信雑音が無し$(\alpha = 0)$の場合，

$$S(X;Y||Z)_{\mathrm{up}} = \log_2\sqrt{1 + \frac{(1-\rho^2)^2\gamma^2}{2(1-\rho^2)\gamma+1}} \tag{24}$$

となる．

相関ρ を 0.0, 0.7, 0.9 とし，α を 0 と 1 とした場合の γ に対する秘密鍵容量の上限を Fig.4 に示す．図から秘密鍵容量の上限は，①γ が減少するとゼロに漸近するが，その傾向は相関 ρ が 1 に近づくほど顕著であること，②γ が増加すると γ の対数に比例して増加すること，③相関 ρ が 1 に近づいても γ が増加すると比較的大きくなること，が分かる．また，α が 0 と 1 の差は，相関が 1 に近づく ρ=0.9 場合，γ が比較的小さい範囲（例えば，0～15dB）で顕著となる．

次に，式(22)において相関 $\rho \cong 1$ 場合に α への依存性が顕著となるが，γ が増加し $\gamma \gg 1$, $\alpha/(1-\rho^2)$ となると，

$$S(X;Y||Z)_{\mathrm{up}} \cong \log_2\sqrt{1+\frac{(1-\rho^2)\gamma}{2}} \qquad (25)$$

となる．相関ρを0.95とし，αを0, 0.5, 1, 2, 4とした場合のγに対する秘密鍵容量の上限をFig. 5とに示す．図からγがある範囲（例えば，0～17.5dBの範囲）においてα依存性が顕著となり，αの増加とともに秘密鍵容量の上限が増加することが分かる．

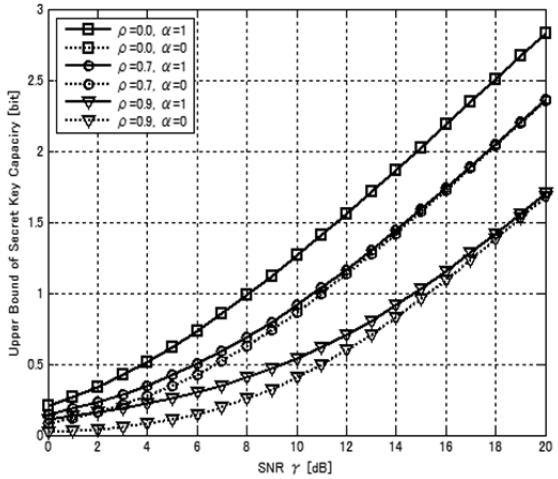

Fig. 4. Upper bound of secret key capacity vs. SNR.

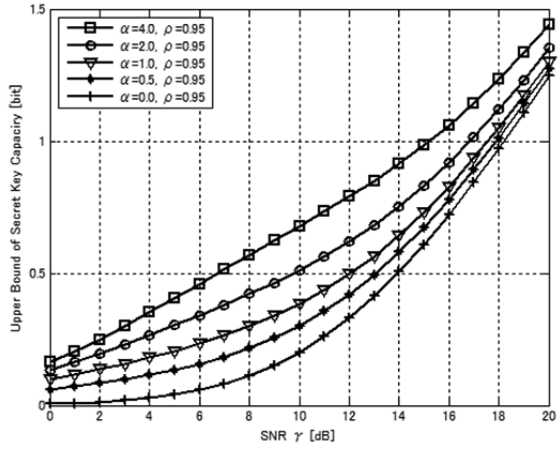

Fig. 5. Upper bound of secret key capacity vs. SNR.

3.5 秘密鍵容量の下限の検討

秘密鍵容量の下限 $S(X;Y||Z)_{\mathrm{low}}$ は，式(2)に示すように，$I(X;Y)-I(X;Z)$ と $I(X;Y)-I(Y;Z)$ の最大値となる．式(11)を用いてこれらを求めると，

$$I(X;Y)-I(X;Z)$$
$$=\log_2\sqrt{\frac{\{(1-\rho^2){P_s}^2+(P_x+P_z)P_s+P_xP_z\}(P_s+P_y)}{\{P_s(P_x+P_y)+P_xP_y\}(P_s+P_z)}}$$
$$=\log_2\sqrt{1+\frac{(1-\rho^2){P_s}^3+(1-\rho^2)P_y{P_s}^2+(P_z-P_y){P_s}^2}{\{P_s(P_x+P_y)+P_xP_y\}(P_s+P_z)}} \qquad (26)$$

となる．同様に

$$I(X;Y)-I(Y;Z)$$
$$=\log_2\sqrt{\frac{\{(1-\rho^2){P_s}^2+(P_x+P_z)P_s+P_xP_z\}(P_s+P_x)}{\{P_s(P_x+P_y)+P_xP_y\}(P_s+P_z)}}$$
$$=\log_2\sqrt{1+\frac{(1-\rho^2){P_s}^3+(1-\rho^2)P_x{P_s}^2+(P_z-P_x){P_s}^2}{\{P_s(P_x+P_y)+P_xP_y\}(P_s+P_z)}} \qquad (27)$$

となる．式(26)と式(27)において，相関無し（ρ=0）とすると，$I(X;Y)-I(X;Z)=I(X;Y)-I(Y;Z)$ となるので，秘密鍵容量の下限は，

$$S(X;Y||Z)_{\mathrm{low}}=\log_2\sqrt{1+\frac{{P_s}^2}{(P_x+P_y)P_s+P_xP_y}} \qquad (28)$$

となり，P_zに依存しない．なお，P_z=0 と ρ=0 の場合に秘密鍵容量の上限は式(22)より，

$$S(X;Y||Z)_{\mathrm{up}}=\log_2\sqrt{1+\frac{{P_s}^2}{(P_x+P_y)P_s+P_xP_y}} \qquad (29)$$

となる．この場合には，秘密鍵容量の上限と下限が一致する．

また，式(26)と式(27)は，$P_x=P_y$ を仮定すると，$I(X;Y)-I(X;Z)=I(X;Y)-I(Y;Z)$ となる．この結果，秘密鍵容量の下限は，$\gamma=P_s/P_x$，$\alpha=P_z/P_x$ を用いて，

$$S(X;Y||Z)_{\mathrm{low}}=\log_2\sqrt{1+\frac{(1-\rho^2)(\gamma^3+\gamma^2)+\gamma^2(\alpha-1)}{(\gamma+\alpha)(2\gamma+1)}} \qquad (30)$$

と表される．

式(30)から $\alpha>1$ の場合に $S(X;Y||Z)_{\mathrm{low}}>0$ となる事が分かる．また，$\rho=0$ の場合，

$$S(X;Y||Z)_{\mathrm{low}}=\log_2\sqrt{1+\frac{\gamma^2}{2\gamma+1}} \qquad (31)$$

となり，αに依存しない．また，$\alpha=0$ の場合，

$$S(X;Y||Z)_{\mathrm{low}}=\log_2\sqrt{1+\frac{(1-\rho^2)\gamma^2-\rho^2\gamma}{2\gamma+1}} \qquad (32)$$

となり，$\gamma > \rho^2/(1-\rho^2)$ の場合に正となる．

相関ρを 0.0, 0.7, 0.9 とし，αを 0 と 1 とした場合のγに対する秘密鍵容量の下限を Fig. 6 に示す．α=1 の場合には，Fig. 4 に示す秘密鍵容量の上限との差が比較的小さく，秘密鍵容量の上限と同様な傾向が見られる．一方，α=0（盗聴者の雑音が零）の場合には, 相関ρが 1 に近い(ρ=0.7, 0.9)の場合に，γ が小さい部分で秘密鍵容量が負となることが分かる．

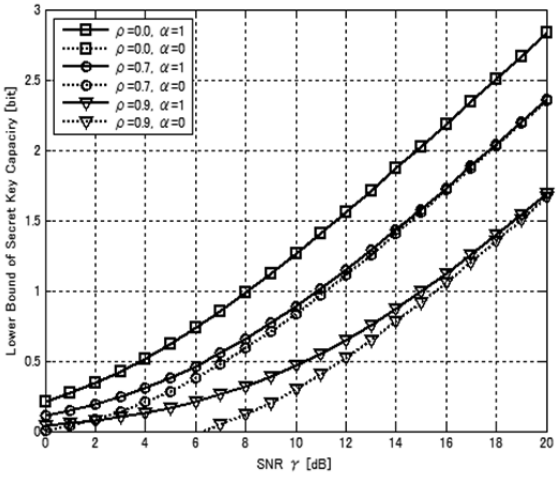

Fig. 6. Lower bound of secret key capacity vs. SNR.

次に, 式(30)において相関が $\rho \cong 1$ の場合にαへの依存性が顕著となるが，γ が増加し $\gamma \gg 1$, $\alpha/(1-\rho^2)$ となると，式(25)と同様に

$$S(X;Y||Z)_{\mathrm{low}} \cong \log_2 \sqrt{1+\frac{(1-\rho^2)\gamma}{2}} \qquad (33)$$

となる．

相関ρを 0.95 とし，αを 0, 0.5, 1, 2, 4 とした場合のγに対する秘密鍵容量の下限を Fig. 7 とに示す．図からγがある範囲（例えば，0～17.5dB の範囲）においてα依存性が顕著となり，αの増加とともに秘密鍵容量の下限が増加することが分かる．また，α=0 と α= 0.5 の場合に，γが小さくなると秘密鍵容量が正とならない場合があることが分かる．

次に, α=0.5 で ρ=0.7, 0.9, 0.95 の場合の秘密鍵容量の上限と下限を Fig. 8 に示す．図から，ρ=0.7 の場合には，上限と下限がほとんど一致していることが分かる．また，相関が ρ=0.9, 0.95 の場合には，SN 比の減少にともない上限と下限の差が増加することが分かる．

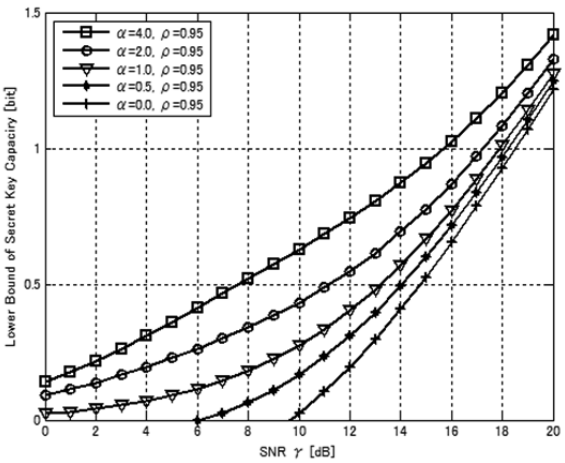

Fig. 7. Lower bound of secret key capacity vs. SNR.

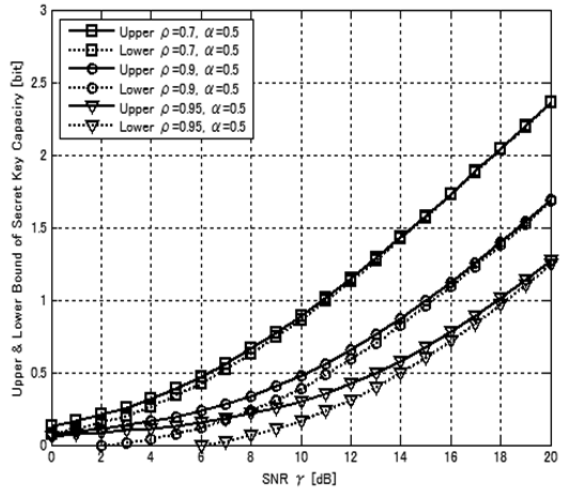

Fig. 8. Upper and lower band of secret key capacity vs. SNR.

４．電波干渉を活用した秘密鍵共有と秘密鍵容量

4.1 干渉波の存在する陸上移動通信路モデル

上記の秘密鍵容量の上限と下限の検討によると，相関ρが 1 に近く，且つ，γが比較的小さい場合，正規者の雑音に比べて盗聴者の雑音が同等かそれ以上でないと秘密鍵容量が低下する．このため，陸上移動通信路モデルにおいても効率的な鍵生成ができ

ない．このような設定を実環境で容易に実現する工夫として，安全性向上のための電波干渉の活用が検討されている．

Fig. 9 に干渉波の存在する陸上移動通信路モデルを示す．図において干渉波 I_x, I_y, I_z はガウス分布に従うものとすると，この図は Fig. 3 のモデルにおいて N_x を N_x+I_x で，N_y を N_y+I_y で，N_z を N_z+I_z で，置換えたものになっている．ここで，それらの和の電力を P_x, P_y, P_z とすると，Fig. 3 のモデルから導出された式がそのまま成立つ．

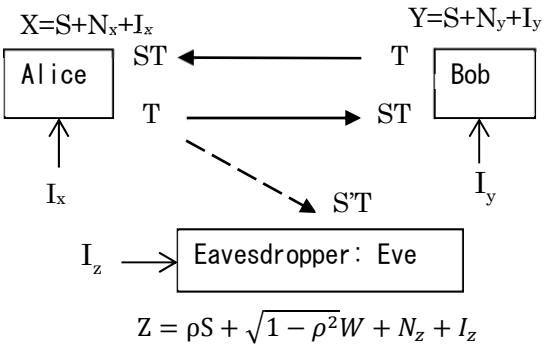

Fig. 9. Land mobile communication channel model under radio interference.

4.2 秘密鍵容量の上限と下限の検討

Fig. 9 のモデルにおいて，干渉波は正規者間の相互情報量を減少させるとともに，正規者と盗聴者間の相互情報量を減少させる．このため，前者より後者の効果が大きければ，秘密鍵容量が増加する可能性がある．また，正規者に加わる干渉波を何らかの手段で軽減可能，又は，盗聴者への干渉波を増加可能とすると，秘密鍵容量の増加が期待できる．

そこで，秘密鍵容量が小さくなるように相関を ρ=0.98 に設定し，盗聴者対正規者雑音電力比を α=0.5, 2, 8 とした場合の SN 比 γ に対する秘密鍵容量の上限と下限を Fig. 10 に示す．図から γ が増加すると，秘密鍵容量の上限と下限が増加するとともに, 上限と下限の差も縮小することが分かる. また, α が増加すると秘密鍵容量の上限と下限の差が縮小するとともに, 秘密鍵容量が増加することが分かる. α=8 のような設定では，秘密鍵容量が条件付き相互情報量で近似できることが分かる．

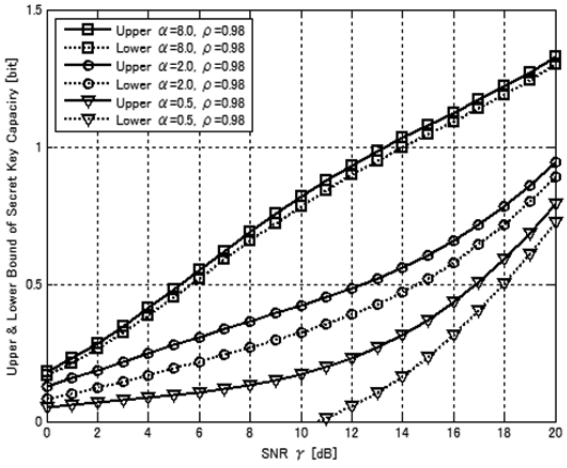

Fig. 10. Upper and lower band of secret key capacity vs. SNR.

5．まとめ

陸上移動通信モデルを対象に，相関のあるガウス性情報を用いた場合の秘密鍵容量の上限と下限の数式を導出した．秘密鍵容量の上限については，一般式をより限定した式を導出し，それが条件付き相互情報量で表されることを明らかとした．相関 ρ と盗聴者対正規者雑音電力比 α をパラメータとする SN 比に対する秘密鍵容量の上限の特性を明らかとした．一方，秘密鍵容量の下限については，正規者の雑音が盗聴者の雑音に比べて小さい場合（α＜1）でも，相関 ρ が小さければ秘密鍵容量が正となることを示した．また，相関 ρ と盗聴者対正規者雑音電力比 α をパラメータとする SN 比に対する秘密鍵容量の下限の特性を明らかとした．

さらに，干渉波を用いて実効的な雑音増加を盗聴者に対してのみ行い，正規者に対する盗聴者の雑音を大きく（α≫1）設定することで，秘密鍵容量の増加が期待できることを示した．また，そのような場合に秘密鍵容量の上限と下限を求めた．その結果，α≫1 の場合に秘密鍵容量が条件付き相互情報量で近似できることが明らかとなった．

参考文献

1) H. Yamamoto, “Information Theory of Cryptology,” *IEICE*

Trans., E**74**[9], 2456-2464 (1991)

2) 今井秀樹，花岡悟一郎，“情報量的安全性に基づく暗号技術”，信学論(A)，**87**[6]，721-733 (2004)

3) C. E. Shannon, “Communication Theory of Secrecy System,” *Bell Syst. Tech. J.* **28**, 565-715 (1949)

4) A. D. Wyner, “The Wire-tap Channel,” *Bell Sys. Tech. J*., **54**, 1355-1387 (1975)

5) U. M. Maurer, “Secret Key Agreement by Public Discussion from Common Information,” *IEEE Trans. Inform. Theory*, IT-**39**[3], 733-742 (1993)

6) C.H. Bennet, and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” *Proc. of IEEE Int. Conf. on Comp. Sys. and Signal Proc.*, 175-179 (1984)

7) J. E. Hershey, A. A. Hassan, and R. Yarlagadda, “Unconventional Cryptographic Keying Variable Management,” *IEEE Trans. Commni*., **43**[1], 3-6 (1995)

8) A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, “Cryptographic Key Agreement for Mobile Radio,” *Digital Signal Processing*, **6**, 207-212 (1996)

9) H. Koorapaty, A. A. Hassan, and S. Chennakeshu, “Secure Information Transmission for Mobile Radio,” *IEEE Communication Letters*, **4**[2], 52-55 (2000)

10)青野智之，樋口啓介，大平孝，小宮山牧兒，笹岡秀一，“エスパアンテナを用いた IEEE802.15.4 無線秘密鍵共有システム”，信学論(B)，**88**[9], 1801-1812 (2005)

11)笹岡秀一，“電波伝搬を活用した無線通信セキュリティ”，信学技報，IT2008-**15**，39-44，(2008)

12) R. Ahlawede, and I. Csiszar, “Common Randomness in Information Theory and Cryptography －Part I: Secret Sharing,” *IEEE Trans. Inform. Theory*, **39**[4], 1121-1132 (1993)

13) U. M. Maurer, and S. Wolf, “Unconditionally Secure Key Agreement and the Intrinsic Conditional Information,” *IEEE Trans. Inform. Theory*, **45**[2], 499-514 (1999)

14) 岩井誠人，笹岡秀一，“電波伝搬特性を活用した秘密情報量の伝送・共有技術”，信学論(B)，**90**[9], 770-783 (2007)

15) 笹岡秀一，“電波伝搬・電磁環境を活用した無線通信セキュリティ”，信学技報，EMCJ2007-**52**, 53-58 (2007)

16) 笹岡秀一，“無線通信におけるガウス性相関情報に基づく秘密鍵共有の秘密鍵容量—（その１）衛星通信路モデル—”, 同志社大学理工学研究報告, **54**[3], 185-192 (2013)

17) C. H. Bennett, G. Brassard, C. Crepeau, and U.M. Maurer, “Generalized Privacy Amplification,” *IEEE Trans. Inform. Theory*, **41**[6], 1915-1923 (1995)

18) I. Csiszar, and P. Narayan, “Common Randomness and Secret Key Generation with a Helper,” *IEEE Trans. Inf. Theory*, **46**[2], 344-366 (2002)

19)今井秀樹, 情報理論, (昭晃堂, 東京, 1984), pp.197-205.

付録

A. 陸上移動通信路モデルにおける相互情報量と結合エントロピー

Fig. 3 の陸上移動通信路モデルにおいて，X と Z の相互情報量 $I(X;Z)$ と結合エントロピー H(X, Z) を求める．なお，この導出法は文献[16]の付録 A の導出法と類似である．

条件付きエントロピー H(Z|X) は，$U = Z - \beta X$ とし，U が X と独立となるように β を求めると，

$$H(Z|X) = H(Z - \beta X|X) = H(U|X) = H(U) \quad \text{(A-1)}$$

となる．ここで，β は，

$$\overline{UX} = \overline{ZX} - \beta\overline{X^2} = \rho P_s - \beta(P_s + P_x) = 0 \quad \text{(A-2)}$$

より，

$$\beta = \frac{\rho P_s}{P_s + P_x} \quad \text{(A-3)}$$

となる．この結果，Uが，

$$U = \rho S + \sqrt{1-\rho^2}W + N_z - \beta S - \beta N_x \quad \text{(A-4)}$$

となることから，Uの分散（電力）P_uは，

$$P_u = (\rho - \beta)^2 P_s + (1-\rho^2)P_s + P_z + \beta^2 P_x = P_s + P_z - 2\rho\beta P_s + \beta^2(P_s + P_x) \quad \text{(A-5)}$$

となる．ここで，(A-3)式を代入すると

$$P_U = \frac{(P_s+P_z)(P_s+P_x) - \rho^2 {P_s}^2}{P_s+P_x} = \frac{A}{P_s+P_x} \quad \text{(A-6)}$$

$$\mathrm{A} = (1-\rho^2){P_s}^2 + P_s(P_x + P_z) + P_x P_z$$

となる．

これより，$H(Z|X)$ は，

$$H(Z|X) = log_2\sqrt{2\pi e \frac{A}{P_s+P_x}} \quad \text{(A-7)}$$

となる．この結果，相互情報量が $I(X;Z) = H(Z) - H(Z|X)$ を用いて，

$$I(X;Z) = log_2\sqrt{\frac{(P_s+P_x)(P_s+P_z)}{A}} \quad \text{(A-8)}$$

となる，一方，結合エントロピーは $H(X,Z)=H(X)+H(Z|X)$ を用いて，

$$H(X,Z)=log_2\sqrt{(2\pi e)^2A} \quad \text{(A-9)}$$

となる．

B. 陸上移動通信路モデルにおける結合エントロピーH(X, Y, Z)の導出

結合エントロピー $H(X,Y,Z)$ は，その定義から $H(X,Y,Z)=H(X,Y)+H(Z|X,Y)$ となるが，$H(X,Y)$ は(A-7)式で求められているので，$H(Z|X,Y)$ を導出する．付録 A と同様な手法で，$U=Z-\beta X-\delta Y$ とし，Uと X, Uと Yが独立（無相関）となるようにβとδを設定すると，

$$\begin{aligned} H(Z|X,Y)&=H(Z-\beta X-\delta Y|X,Y)\\ &=H(U|X,Y)=H(U) \end{aligned} \quad \text{(B-1)}$$

となる．αとβは，

$$\begin{aligned} \overline{UX}&=\rho P_s-\beta(P_s+P_x)-\delta P_s=0\\ \overline{UY}&=\rho P_s-\beta P_s-\delta\left(P_s+P_y\right)=0 \end{aligned} \quad \text{(B-2)}$$

の連立方程式を解いて，

$$\begin{aligned} \beta&=\frac{\rho P_sP_y}{P_s(P_x+P_y)+P_xP_y}\\ \delta&=\frac{\rho P_sP_x}{P_s(P_x+P_y)+P_xP_y} \end{aligned} \quad \text{(B-3)}$$

となる．Uの分散（電力）P_uは，

$$\begin{aligned} U&=(\rho-\beta-\delta)S+\sqrt{1-\rho^2}W\\ &\quad +N_z-\beta N_x-\delta N_y \end{aligned} \quad \text{(B-4)}$$

を用いて，

$$\begin{aligned} P_u&=P_s+P_z-2\rho(\beta+\delta)P_s\\ &\quad +(\beta+\delta)^2P_s+\beta^2P_x+\delta^2P_y \end{aligned} \quad \text{(B-5)}$$

となる．さらに，式(B-2)を代入して式(B-5)を整理すると，

$$\begin{aligned} P_u&=\frac{C}{P_s(P_x+P_y)+P_xP_y}\\ \mathrm{C}&=(1-\rho^2){P_s}^2\left(P_x+P_y\right)\\ &\quad +P_s\left(P_xP_y+P_yP_z+P_zP_x\right)+P_xP_yP_z \end{aligned} \quad \text{(B-6)}$$

となる．その結果，

$$H(Z|X,Y)=log_2\sqrt{2\pi e\frac{C}{P_s(P_x+P_y)+P_xP_y}} \quad \text{(B-7)}$$

となる．さらに，

$$H(X,Y,Z)=log_2\sqrt{(2\pi e)^3C} \quad \text{(B-8)}$$

となる．