Secret Key Capacity of Wireless Key Agreement Based on Correlated Gaussian Information Source－Part I: Satellite Channel Model－

Hideichi SASAOKA

(Received June 7, 2013)

Information security schemes based on radio propagation property such as secret key agreement and secret data transmission have attracted attention in the current wireless community. For the secret key agreement from common information, a general formula of the secret key capacity is given, but a specific formula of secret key capacity has not present for secret key agreement from Gaussian correlated information, which is typical case in wireless channels.

This paper deals with the theoretical analysis on secret key capacity for the satellite communication channel model. The analysis result shows that the upper band of secret key capacity is given with conditional mutual information and that the formula of upper and lower band is expressed as functions of the signal-to-noise power ratio and the noise power ratio of eavesdropper to legitimate user. The analysis result also shows that secret key capacity can approximately be given by conditional mutual information in the case that noise power ratio of eavesdropper to legitimate user is large.

Key Word：Key agreement, Secret key capacity, Correlated information, Satellite channel

キーワード：鍵共有，秘密容量，相関情報，衛星通信路

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１）衛星通信路モデル—

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]．

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

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，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い．

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，衛星通信路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について検討した．

２．相関情報に基づく秘密鍵共有の原理と秘密容量

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,・・)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 三段階から構成される[16]．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．

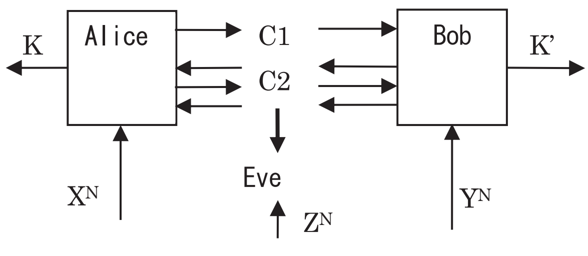

Fig. 1. Secret key agreement from correlated information.

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，

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

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

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,

$$S(X;Y||Z) = I(X;Y|Z) \tag{3}$$

で与えられる [17].

(1)式と(2)式において 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), (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,

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) \tag{4}$$

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

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

と表される．

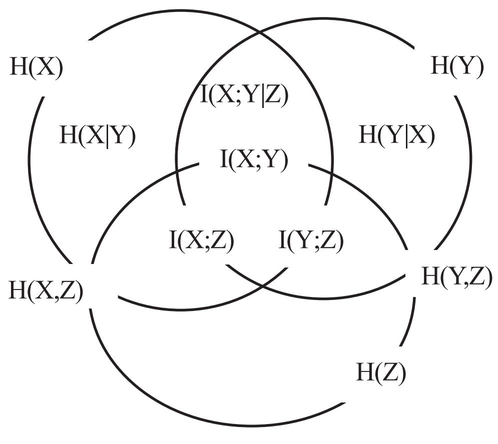

Fig. 2.Relation between entropy and mutual information.

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 [18]．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．

次に，X と Z を平均が 0，分散が $\sigma_x{}^2, \sigma_z{}^2$ 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，相互情報量は I(X;Y)以下のように求められる [18]．はじめに，エントロピーH(X), H(Y)は,

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

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

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

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

となる. なお(7)式は, 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，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) より容易に求められる．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,

$$I(X;Y) = log_2\sqrt{\frac{\sigma_x{}^2+\sigma_z{}^2}{\sigma_z{}^2}} = log_2\sqrt{(1+\frac{\sigma_x{}^2}{\sigma_z{}^2})} \tag{9}$$

となる．

３．ガウス性相関情報に基づく衛星通信路の秘密容量

3.1 衛星通信路モデル

正規者（アリスとボブ）と盗聴者（イブ）が共通の信号 S をそれぞれの受信雑音 N_X，N_Y，N_Z，とともに得るモデル（衛星通信路モデル）を考える．このようなモデルを Fig.3 に示す．Fig.3 において，$X=S+N_x$, $Y=S+N_y$, $Z=S+N_z$ となる．S, N_x, N_y, N_z が平均 0 で，お互いに独立なガウス変数とし，その電力を P_s, P_x, P_y, P_z とする．

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,

$$H(X) = log_2 \sqrt{2\pi e(P_s + P_x)}$$
$$H(Y) = log_2 \sqrt{2\pi e(P_s + P_y)} \qquad (10)$$
$$H(Z) = log_2 \sqrt{2\pi e(P_s + P_z)}$$

と表される．

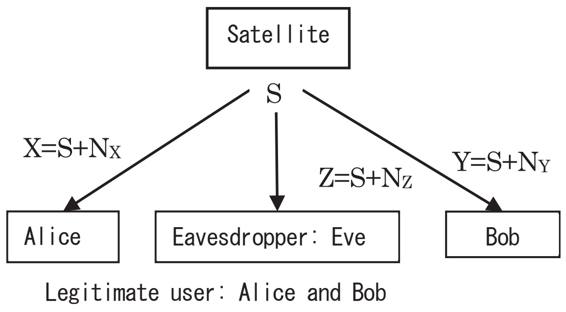

Fig. 3. Satellite communication channel model.

3.2 ガウス性相関情報の相互情報量

Fig.3 の衛星通信路モデルにおいて X, Y, Z の２変数間の相互情報量 I(X;Y)，I(X;Z)，I(Y;Z) は，付録 A の(A-6)式と同様な導出により

$$I(X;Y) = log_2 \sqrt{\frac{(P_s+P_x)(P_s+P_y)}{P_s(P_x+P_y)+P_xP_y}}$$
$$I(X;Z) = log_2 \sqrt{\frac{(P_s+P_x)(P_s+P_z)}{P_s(P_x+P_z)+P_xP_z}} \qquad (11)$$
$$I(Y;Z) = log_2 \sqrt{\frac{(P_s+P_y)(P_s+P_z)}{P_s(P_y+P_z)+P_yP_z}}$$

となる．また，X, Y, Z の２変数間の結合エントロピー H(X,Y), H(X,Z), H(Y,Z) は，付録 A の(A-7)式と同様な導出により，

$$H(X,Y) = log_2 \sqrt{(2\pi e)^2\{P_s(P_x+P_y)+P_xP_y\}}$$
$$H(X,Z) = log_2 \sqrt{(2\pi e)^2\{P_s(P_x+P_z)+P_xP_z\}} \qquad (12)$$
$$H(Y,Z) = log_2 \sqrt{(2\pi e)^2\{P_s(P_y+P_z)+P_yP_z\}}$$

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(B-7)式より，

$$H(X,Y,Z) =$$
$$log_2 \sqrt{(2\pi e)^3\{P_s(P_xP_y+P_yP_z+P_zP_x)+P_xP_yP_z\}} \qquad (13)$$

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，(10)，(12)，(13)式を(5)式に代入して，

$$I(X;Y|Z) =$$
$$log_2 \sqrt{\frac{\{P_s(P_x+P_z)+P_xP_z\}\{P_s(P_y+P_z)+P_yP_z\}}{(P_s+P_z)\{P_s(P_xP_y+P_yP_z+P_zP_x)+P_xP_yP_z\}}} \qquad (14)$$

となる．

3.3 秘密鍵容量の上限式の導出

秘密鍵容量の上限は，(1)式に示されるように 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．(11)式，(14)式より，

$$I(X;Y) - I(X;Y|Z) =$$
$$log_2 \sqrt{\frac{(P_s+P_x)(P_s+P_y)(P_s+P_z)\{P_s(P_xP_y+P_yP_z+P_zP_x)+P_xP_yP_z\}}{\{P_s(P_x+P_y)+P_xP_y\}\{P_s(P_x+P_z)+P_xP_z\}\{P_s(P_y+P_z)+P_yP_z\}}} \qquad (15)$$

となる．ここで，(15)式の√￣内の分子を A，分母を B とすると，$A > 0$，$B > 0$ であるので，$A > B$ の場合に $I(X;Y) - I(X;Y|Z) > 0$ となる．

そこで，A を展開して P_s の冪で整理すると，

$$A = a_4P_s^4 + a_3P_s^3 + a_2P_s^2 + a_1P + a_0$$
$$a_4 = P_xP_y + P_yP_z + P_zP_x$$
$$a_3 = (P_x + P_y + P_z)a_4 + P_xP_yP_z$$
$$a_2 = a_4^2 + (P_x + P_y + P_z)P_xP_yP_z \qquad (16)$$
$$a_1 = 2\,a_4\,P_xP_yP_z$$
$$a_0 = P_x^2P_y^2P_z^2$$

と表される．一方，

$$B = b_3P_s^3 + b_2P_s^2 + b_1P_s + b_0$$
$$b_3 = (P_x + P_y + P_z)a_4 - P_xP_yP_z$$
$$b_2 = a_4^2 + (P_x + P_y + P_z)P_xP_yP_z \qquad (17)$$
$$b_1 = 2\,a_4\,P_xP_yP_z$$
$$b_0 = P_x^2P_y^2P_z^2$$

となる．(16)式，(17)式より，

$$A - B = (P_xP_y + P_yP_z + P_zP_x)P_s^4 + 2P_xP_yP_zP_s^3 > 0 \qquad (18)$$

が常に成り立つ．

この結果，(1)式の右辺が $min[I(X;Y), I(X;Y|Z)] = I(X;Y|Z)$ となるので，秘密鍵容量の上限は，

$$S(X;Y||Z) \leq I(X;Y|Z) \qquad (19)$$

で与えられる．(19)式は，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，(14)式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 の大小関係により

どのようになるかを検討する．(14)式の√内の分子 C と分母 D を展開して Ps の冪で整理すると，

$$C = (P_x + P_z)(P_y + P_z)P_s^2 + (2P_xP_y + P_yP_z + P_zP_x)P_zP_s + P_xP_yP_z^2 \quad (20\text{-}1)$$

$$D = (P_xP_y + P_yP_z + P_zP_x)P_s^2 + (2P_xP_y + P_yP_z + P_zP_x)P_zP_s + P_xP_yP_z^2 \quad (20\text{-}2)$$

となる．(20)式を用いて(14)式を変形すると，

$$I(X;Y|Z) = log_2\sqrt{1 + \frac{P_z^2P_s^2}{D}} \quad (21)$$

となる．

ここで､簡単のため正規者 A と B の雑音電力を等しいと仮定し、正規者の信号対雑音電力比（SN 比）を γ 、盗聴者対正規者雑音電力比を α で表す. このとき、$P_x = P_y$, $\gamma = P_s/P_x$, $\alpha = P_z/P_x$ である． α を 0.5, 1, 1.5, 2 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，① γ が小（例えば，－4dB 以下）で α によらずほぼ一定，② γ の増加に伴い増加， α が大で増加も大，③ γ が大（例えば，16dB）で一定値に漸近，となることが分かる．

この結果が示すように，衛星通信路モデルにおいて正規者と盗聴者の受信雑音電力に大差がない状態を想定すると，秘密鍵容量の上限が SN 比が十分に大きくても 0.2 程度と比較的小さい．また，盗聴者が高性能な受信装置を用いる場合（受信雑音電力が小の場合）には，その上限が更に小さくなり秘密鍵の生成が効率的に行えない．

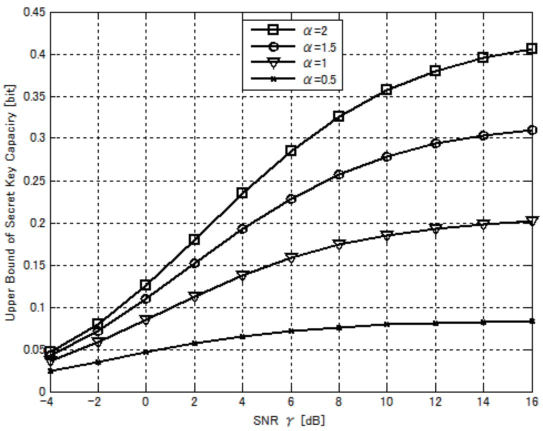

Fig. 4. Upper bound of secret key capacity vs. SNR.

3.5 秘密鍵容量の下限の検討

秘密鍵容量の下限は，(2)式に示すように $I(X;Y) - I(X;Z)$ と $I(X;Y) - I(Y;Z)$ の最大値となる．(11)式を用いてこれらを求めると，

$$I(X;Y) - I(X;Z) = log_2\sqrt{\frac{(P_s+P_y)\{P_s(P_x+P_z)+P_xP_z\}}{(P_s+P_z)\{P_s(P_x+P_y)+P_xP_y\}}}$$

$$= log_2\sqrt{1 + \frac{P_s^2(P_z-P_x)}{(P_s+P_z)\{P_s(P_x+P_y)+P_xP_y\}}} \quad (22)$$

となる．同様に，

$$I(X;Y) - I(Y;Z) = log_2\sqrt{1 + \frac{P_s^2(P_z-P_y)}{(P_s+P_z)\{P_s(P_x+P_y)+P_xP_y\}}} \quad (23)$$

となる．(2)式，(22)式，(23)式より $P_z > P_x$ or $P_z > P_y$ の場合に秘密鍵容量の下限が 0 以上となる. なお, (22)式と(23)式のどちらかが負となる場合には，秘密鍵共有のプロトコルとして，Advantage distillation が必須となる．

次に、盗聴者対正規者雑音電力比 α を 1.5, 2 とした場合の SN 比 γ に対する秘密鍵容量の下限をその上限とともに Fig.5 に示す．秘密鍵容量の下限の γ の増減と α の増減に対する特性は，その上限と同様な傾向にあることが分かる．また，図より秘密鍵容量の上限と下限とはかなりの隔たりがあることが分かる．

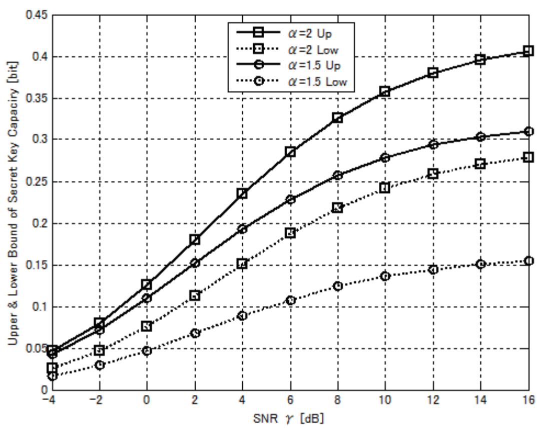

Fig. 5. Upper and lower band of secret key capacity vs. SNR.

４．電波干渉を活用した秘密鍵共有と秘密鍵容量

4.1 干渉波の存在する衛星通信路モデル

上記の秘密鍵容量の上限と下限の検討によると，正規者の雑音に比べ盗聴者の雑音が十分に大きい状態を

想定しないと，衛星通信路モデルにおいて効率的な秘密鍵の生成ができない．しかし，そのような設定は，実環境で容易に実現できるとは限らない．この課題に対して，安全性の向上のための電波干渉の活用が検討されている[15]．

Fig.6 に干渉波の存在する衛星通信路モデルを示す．Fig.6 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，Fig.6 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り立つ．

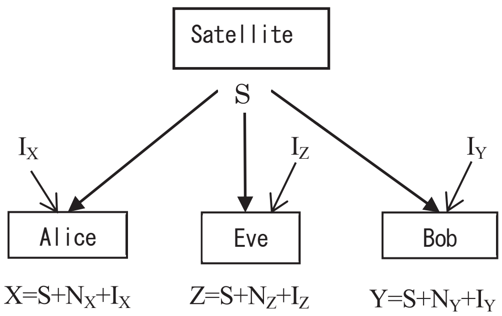

Fig. 6. Satellite communication channel model under radio interference.

4.2 秘密鍵容量の上限と下限の検討

Fig.6 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効果がある．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，盗聴者対正規者雑音電力比 α を 5, 10 とした場合の SN 比 γ に対する秘密鍵容量の下限をその上限とともに Fig.7 に示す．Fig.7 から γ の増加とともに秘密鍵容量の上限と下限が増加することが分かる．また，上限と下限の差が比較的小さく，α の増加とともにより縮小する傾向があることが分かる．このような設定においては，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．

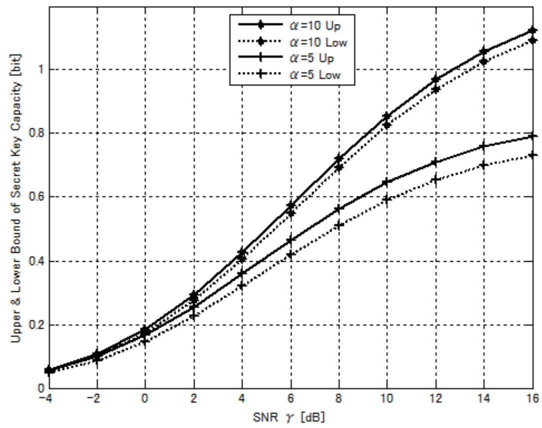

Fig. 7. Upper and lower band of secret key capacity vs. SNR.

5．まとめ

衛星通信路モデルを対象に，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．秘密鍵容量に上限については，一般式をより限定した式を導出し，条件付き相互情報量で表されることを明らかにした．また，相関係数 ρ、SN 比 γ、盗聴者対正規者雑音電力比 α に対する秘密鍵容量の上限の特性を明らかにした．一方，秘密鍵容量の下限については，下限が負とならないために正規者の雑音が盗聴者の雑音に比べて小さいことが必要なことを示した．また，SN 比や α に対する秘密鍵容量の下限の特性を求めた．

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，正規者の対する盗聴者の雑音を大きく設定することで，秘密鍵容量の増加が期待できることを示した．また，そのときの秘密鍵容量の上限と下限の特性を求めた．その結果，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．

なお，盗聴者にのみ選択的に干渉波妨害を与える現実的な手法については今後の課題である．

付録 A. 衛星通信路モデルにおけるガウス性相関情報の相互情報量と結合エントロピー

Fig.3 のシステムにおいて X と Y の相互情報量 I(X;Y)と結合エントロピーH(X,Y)を求める．

はじめに，H(Y|X)を求めるため，定数βを用いて$U=Y-\beta X$とし, UとXが独立となるようにβを設定すると， $H(Y|X)=H(Y-\beta X|X)=H(U|X)=H(U)$となる．ここで，Uも平均値0のガウス分布に従うため，独立と相関0は等価となる．ここで，UとXの相関が0となる条件

$$\overline{UX}=\overline{YX}-\beta\overline{X^2}=P_s-\beta(P_s+P_x)=0 \quad \text{(A-1)}$$

から，βの値が容易に求められ，

$$\beta=\frac{P_s}{P_s+P_x} \quad \text{(A-2)}$$

となる．次に，Uの分散（電力）P_uは、

$U=Y-\beta X=(1-\beta)S+N_y-\beta N_x$ を用いて，

$$P_u=\overline{U^2}=P_s+P_y-2\beta P_s+\beta^2(P_s+P_x) \quad \text{(A-3)}$$

となる．ここで，(A-2)式を代入して，

$$P_u=\frac{P_s(P_x+P_y)+P_xP_y}{P_s+P_x} \quad \text{(A-4)}$$

となる．

これより，$H(Y|X)=H(U)$ は，

$$H(Y|X)=log_2\sqrt{\frac{2\pi e\{P_s(P_x+P_y)+P_xP_y\}}{P_s+P_x}} \quad \text{(A-5)}$$

となる．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，

$$I(X;Y)=log_2\sqrt{\frac{(P_s+P_x)(P_s+P_y)}{P_s(P_x+P_y)+P_xP_y}} \quad \text{(A-6)}$$

となる．

一方，X と Y の結合エントロピーH(X,Y)は，$H(X,Y)=H(Y|X)+H(X)$ を用いて，

$$H(X,Y)=log_2\sqrt{(2\pi e)^2\{P_s(P_x+P_y)+P_xP_y\}} \quad \text{(A-7)}$$

となる．

付録B. 衛星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，

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

となる．βとδは,

$$\overline{UX}=P_s-\beta(P_s+P_x)-\delta P_s=0$$
$$\overline{UY}=P_s-\beta P_s-\delta(P_s+P_y)=0 \quad \text{(B-2)}$$

の連立方程式を解いて，

$$\beta=\frac{P_sP_y}{P_s(P_x+P_y)+P_xP_y},\quad \delta=\frac{P_sP_x}{P_s(P_x+P_y)+P_xP_y} \quad \text{(B-3)}$$

となる．Uの分散（電力）P_uは，$U=(1-\beta-\delta)S+N_z-\beta N_x-\delta N_y$ を用いて，

$$P_u=P_s+P_z-2(\beta+\delta)P_s+(\beta+\delta)^2P_s$$
$$+\beta^2P_x+\delta^2P_y \quad \text{(B-4)}$$

となる．さらに，(B-2)式を代入して(B-4)式を整理すると，

$$P_u=\frac{P_s(P_xP_y+P_yP_z+P_zP_x)+P_xP_yP_z}{P_s(P_x+P_y)+P_xP_y} \quad \text{(B-5)}$$

となる．その結果,

$$H(Z|X,Y)=log_2\sqrt{2\pi e\frac{P_s(P_xP_y+P_yP_z+P_zP_x)+P_xP_yP_z}{P_s(P_x+P_y)+P_xP_y}} \quad \text{(B-6)}$$

となる．さらに，

$$H(X,Y,Z)=$$
$$log_2\sqrt{(2\pi e)^3\{P_s(P_xP_y+P_yP_z+P_zP_x)+P_xP_yP_z\}} \quad \text{(B-7)}$$

となる．

参考文献

1) H. Yamamoto, “Information theory of cryptology,” IEICE Trans., E74(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, 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. Communi., 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," 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，IT2008-15，9-44，(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) C. H. Bennett, G. Brassard, C. Crepeau, and U.M. Maurer, "Generalized Privacy Amplification," IEEE Trans. Inform. Theory, 41(6), 1915-1923, (1995).

17) I. Csiszar, and P. Narayan, "Common randomness and secret key generation with a helper," IEEE Trans. Inf. Theory, 46(2), 344-366, (2002).

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