Drop of the Secret Key Capacity by the Multiple Spot Eavesdropping in Wireless Secret Key Agreement Based on the Complex Channel Coefficient

Hideichi SASAOKA* and Hisato IWAI*

(Received April 4, 2022)

Secret key agreement based on radio propagation characteristics attracts attention as a kind of the wireless physical layer security. However, there are few studies on drop of the secret key capacity by multiple spot eavesdropping. This paper derived the theoretical formula of the secret key capacity in secret key agreement based on the complex channel coefficient. This paper also derived the theoretical formula of the leakage information by multiple spot eavesdropping and showed that leakage information increased with the increase of the eavesdropping spot number. Validity of these theoretical formulas was confirmed by computer simulation. Then, this paper calculated the correlation coefficient of the channel coefficient in the simple propagation environment, and evaluated security of secret key agreement by calculating leakage information for multiple spot eavesdropping.

Key words: wireless secret key agreement, secret key capacity, multiple spot eavesdropping, complex channel coefficient

キーワード：無線秘密鍵共有，秘密鍵容量，複数地点盗聴，複素チャネル係数

複素チャネル係数に基づく無線秘密鍵共有における 複数地点盗聴による秘密鍵容量の低下

笹岡　秀一，　岩井　誠人

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共通鍵暗号方式や公開鍵暗号方式などが一般的である．また，移動通信の場合には処理演算量が簡易な共通鍵暗号方式が用いられる．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となる．さらに，これらの暗号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．

これらの手法と異なり情報量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]．これらの技術には，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（盗聴通信路）を用いた鍵配送[4]，相関情報を

*Department of Electronics, Doshisha University, Kyoto
Telephone: +81-774-65-6267, Fax: +81-774-65-6267, E-mail: iwai@mail.doshisha.ac.jp

用いた秘密鍵共有 [5]などがある．また，より現実的な技術として，移動通信路特性を用いた秘密鍵共有[6,7]と秘密情報伝送が提案されている [8]．ここで，秘密鍵共有は相関に基づく秘密鍵共有の一種であり，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 [9]．すなわち，電波伝搬の可逆性によって正規者間で相関性の高い秘密情報を共有する一方，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 [10].

相関情報に基づく秘密鍵共有においては，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．そして，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で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 [5,11]．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 [5,12].

一方，移動通信における秘密鍵共有では，フェージング変動を受けた受信信号の標本化と量子化（チャネル係数の時系列）が相関情報に相当し，離散的な確率変数となる．この場合に，相関情報をガウス分布するアナログ情報と想定した理論解析により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 [13,14]．また，ガウス分布するアナログ相関情報に対する秘密鍵容量の上限・下限の厳密な理論解析と信号対雑音電力比（SN 比）に対する秘密鍵容量特性の評価には，衛星通信路モデルと移動通信モデルを対象とした理論解析 [15,16]がある．しかし，上記の検討はチャネル係数が実数の場合を取り扱い，複素のチャネル係数（複素相関情報）を対象としていない．なお，複素のガウス性相関情報に対する理論解析が行われているが，グループ秘密鍵共有を対象としたものである [17]．また，秘密鍵容量の導出に当たり盗聴者の複数地点測定を想定していない.

本論文では，はじめに従来の秘密鍵容量の理論式を概説した後，相関情報が複素の場合に理論式を拡張した. また, 盗聴者への漏洩情報量の検討を行い，盗聴地点数に対する漏洩情報量と秘密鍵容量の理論式を示した．次に，単調な電波伝搬環境におけるチャネル係数の空間相関係数を算出し，複数地点盗聴に対する漏洩情報量と秘密鍵容量を評価した.

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概要

2.1.1 相関情報に基づく秘密鍵共有の原理

相関情報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．Fig. 1 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 $(C_1, C_2, \cdots)$ 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．なお，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 [18]．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，鍵レートの理論上の上限を秘密鍵容量と呼ぶ.

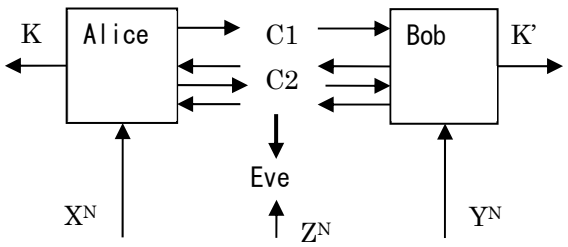

Fig. 1. Secret key agreement from correlated information.

2.1.2 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,

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

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

で与えられる [5]．ここで，式(1)と式(2)は，X, Y, Z が相関のある有限の離散乱数の場合に，その分布に無関係に成り立つ.

式(1)と式(2)において相互情報量 $I(X;Y)$ は,

$$I(X;Y) = H(X) + H(Y) - H(X,Y) \quad (3)$$

と表され， $I(X;Z), I(Y;Z)$ も同様の式で表される.

一方，条件付き相互情報量 $I(X;Y|Z)$ は，

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

と表される．

2.2 ガウス性相関情報に対する秘密鍵容量の理論式

2.2.1 衛星通信路モデルにおける既知の理論式

Fig. 2 に相関情報を取得する衛星通信路モデルを示す．このモデルでは，正規者（アリスとボブ）と盗聴者（イブ）の受信信号 X,Y,Zが，ガウス性の共通信号 Sと受信雑音 N_X, N_Y, N_Zとの和となり，$X = S + N_X, Y = S + N_Y, Z = S + N_Z$ と表される．ここで，S, N_X, N_Y, N_Z は平均0でその電力を P_S, P_X, P_Y, P_Z とする独立なガウス変数とする．

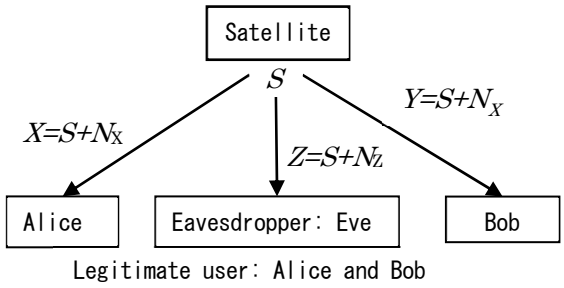

Fig. 2. Channel model of satellite communication to obtain the correlative information.

ここで，式(1)において $min[I(X;Y), I(X;Y|Z)] = I(X;Y|Z)$ であることが示されている [15]．また，X,Y,Z のエントロピー $H(X), H(Y), H(Z)$ と結合エントロピー $H(X,Y), H(X,Z), H(Y,Z), H(X,Y,Z)$ を求めることで，秘密鍵容量の上限 $S(X;Y||Z)_{up}$ は，

$$S(X;Y||Z)_{up} = \frac{1}{2}\log_2\left[1 + \frac{{P_Z}^2{P_S}^2}{(P_S+P_Z)\{P_S(P_XP_Y+P_YP_Z+P_ZP_X)+P_XP_YP_Z\}}\right] \quad (5)$$

と表される [15]．

一方，秘密鍵容量の下限 $S(X;Y||Z)_{low}$ は，

$$S(X;Y||Z)_{low} = max\left[\frac{1}{2}log_2\left\{1 + \frac{{P_S}^2(P_Z-P_X)}{(P_S+P_Z)\{P_S(P_X+P_Y)+P_XP_Y\}}\right\}, \frac{1}{2}log_2\left\{1 + \frac{{P_S}^2(P_Z-P_Y)}{(P_S+P_Z)\{P_S(P_Y+P_Z)+P_YP_Z\}}\right\}\right] \quad (6)$$

と表される [15]．

2.2.2 移動通信路モデルにおける既知の理論式

Fig. 3 に相関情報を取得する移動通信モデルを示す．このモデルでは，正規者（アリスとボブ）が既知信号 T を送信し，フェージング変動を受けるチャネル係数 S に影響された信号 $S \cdot T$ を受信し，観測値 $X = S + N_X$, $Y = S + N_Y$ を得る．また，盗聴者（イブ）は，チャネル係数 S_E に影響された信号を受信し，観測値 $Z = S_E + N_Z$ を得る．ここで，盗聴者と正規者のチャネル係数（S_EとS）の相関係数を ρ とすると，$S_E = \rho S + \sqrt{1-\rho^2}W$ となる．ここで，S, W, N_X, N_Y, N_Z は平均0でその電力を $P_S, P_W = P_S, P_X, P_Y, P_Z$ とする独立なガウス変数とする．なお，S_E の電力は $P_E = P_S$ となる．

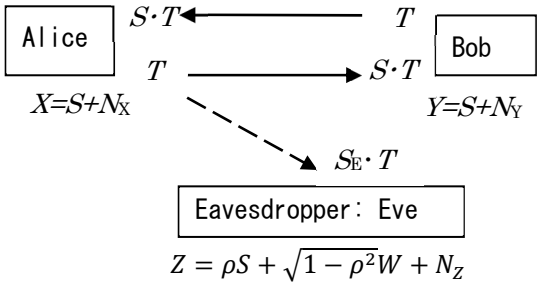

Fig. 3. Channel model of land mobile communication to obtain correlative information.

ここで，X,Y,Z のエントロピーと結合エントロピーを求め，$min[I(X;Y), I(X;Y|Z)] = I(X;Y|Z)$ を示すことで，秘密鍵容量の上限 $S(X;Y||Z)_{up}$ は，

$$S(X;Y||Z)_{up} = \frac{1}{2}\log_2\left[\frac{\{(1-\rho^2){P_S}^2+P_S(P_X+P_Z)+P_XP_Z\}}{(P_S+P_Z)} \cdot \frac{\{(1-\rho^2){P_S}^2+P_S(P_Y+P_Z)+P_YP_Z\}}{\{(1-\rho^2){P_S}^2(P_X+P_Y)+P_S(P_XP_Y+P_YP_Z+P_ZP_X)+P_XP_YP_Z\}}\right] \quad (7)$$

となる [16]．また，秘密鍵容量の下限 $S(X;Y||Z)_{\mathrm{low}}$ は，

$$S(X;Y||Z)_{\mathrm{low}} = max\left[\frac{1}{2}\log_2\frac{\{(1-\rho^2){P_S}^2+(P_X+P_Z)P_S+P_XP_Z\}(P_S+P_Y)}{\{P_S(P_X+P_Y)+P_XP_Y\}(P_S+P_Z)}, \frac{1}{2}\log_2\frac{\{(1-\rho^2){P_S}^2+(P_X+P_Z)P_S+P_XP_Z\}(P_S+P_X)}{\{P_S(P_X+P_Y)+P_XP_Y\}(P_S+P_Z)}\right] \quad (8)$$

となる [16]．

式(7)と式(8)は，P_s, P_x, P_y, P_z, ρ に依存するが，正規者 A と B の電力が等しい（$P_x = P_y$）と仮定し，正規者信号対雑音電力比（SN 比）を $\gamma = P_s/P_x$ で，盗聴者対正規者電力比を $\alpha = P_z/P_x$ で表すと，秘密鍵容量の上限は，

$$S(X;Y||Z)_{up}=\frac{1}{2}\log_2\left[\frac{\{(1-\rho^2)\gamma^2+(\alpha+1)\gamma+\alpha\}^2}{(\gamma+\alpha)\{2(1-\rho^2)\gamma^2+(\alpha+1)\gamma+\alpha\}}\right] \quad (9)$$

$$S(X;Y||Z)_{up}=\frac{1}{2}\log_2\left\{1+\frac{(1-\rho^2)^2\gamma^2}{2(1-\rho^2)\gamma+1}\right\},\alpha=0 \quad (10)$$

となる[16]．また，秘密鍵容量の下限は，

$$S(X;Y||Z)_{\mathrm{low}}=\frac{1}{2}\log_2\left\{1+\frac{(1-\rho^2)(\gamma^3+\gamma^2)+\gamma^2(\alpha-1)}{(\gamma+\alpha)(2\gamma+1)}\right\} \quad (11)$$

$$S(X;Y||Z)_{\mathrm{low}}=\frac{1}{2}\log_2\left\{1+\frac{(1-\rho^2)\gamma^2-\rho^2\gamma}{2\gamma+1}\right\},\alpha=0 \quad (12)$$

となる[16]．

３．複素のガウス性相関情報に対する秘密鍵容量

3.1 衛星通信路モデルにおける理論解析

受信検波信号が同相・直交成分からなる場合，相関情報を取得する衛星通信路モデルは Fig. 2 と異なり，位相回転を受けた送信信号が受信され，観測値が複素となる．このため，

$$\tilde{X}=S_A+\tilde{N}_X,\tilde{Y}=S_B+\tilde{N}_Y,\tilde{Z}=S_E+\tilde{N}_Z \quad S_A=Se^{j\theta_A},S_B=Se^{j\theta_B},S_E=Se^{j\theta_E} \quad (13)$$

と表される．

式(13)で $\tilde{X},S_A,S,\tilde{N}_X$ を実部と虚部で表すと，

$$\begin{aligned}\tilde{X}&=(S_r+jS_i)e^{j\theta_A}+\tilde{N}_X=\tilde{X}_r+j\tilde{X}_i\\ \tilde{X}_r&=S_r\cos\theta_A-S_i\sin\theta_A+\tilde{N}_{Xr}\\ \tilde{X}_i&=S_r\sin\theta_A+S_i\cos\theta_A+\tilde{N}_{Xi}\end{aligned} \quad (14)$$

となる．式(14)の $S_r,S_i,\tilde{N}_{Xr},\tilde{N}_{Xi}$ は互いに独立であり，$\tilde{X}_r,\tilde{X}_i$ も独立となる．また，$S_r,S_i,\tilde{N}_{Xr},\tilde{N}_{Xi}$ の電力を $P_{Sr}=P_{Si}=P_s,\ P_{Xr}=P_{Xi}=P_x$ とすると $\tilde{X}_r,\tilde{X}_i$ の電力は，$P_{\tilde{X}r}=P_{\tilde{X}i}=P_s+P_x$ となる．この結果，$H(\tilde{X}_r)=H(\tilde{X}_i)$ となり，

$$\begin{aligned}H(\tilde{X})&=H(\tilde{X}_r,\tilde{X}_i)=H(\tilde{X}_r)+H(\tilde{X}_i)\\&=2H(\tilde{X}_r)=2H(\tilde{X}_i)=\log_2\{2\pi e(P_s+P_x)\}\end{aligned} \quad (15)$$

となる．

次に，$\tilde{X}$ の位相回転を補償した X は，

$$\begin{aligned}X&=\tilde{X}e^{-j\theta_A}=S+\tilde{N}_Xe^{-j\theta_A}=X_r+jX_i\\X_r&=S_r+N_{Xr}=S_r+\tilde{N}_{Xr}\cos\theta_A-\tilde{N}_{Xi}\sin\theta_A\\X_i&=S_i+N_{Xi}=S_i-\tilde{N}_{Xr}\sin\theta_A+\tilde{N}_{Xi}\cos\theta_A\end{aligned} \quad (16)$$

となる．式(16)の N_{Xr},N_{Xi} が独立となり，X_r,X_i も独立となる．また，$P_{Xr}=P_{Xi}=P_s+P_x$ を用いると，式(15)と同様，

$$\begin{aligned}H(X)&=H(X_r,X_i)=2H(X_r)=2H(X_i)\\&=\log_2\{2\pi e(P_s+P_x)\}=H(\tilde{X})\end{aligned} \quad (17)$$

となる．この結果は，位相回転を補償してもエントロピーに変化がないことを示している．

次に，位相回転の補償が結合エントロピーに与える影響を検討する．ここで，条件 $\tilde{X}$ が位相回転により X と変化しても，条件付き確率が不変（$H(\tilde{Y}|\tilde{X})=H(\tilde{Y}|X)$）となるので，

$$\begin{aligned}H(\tilde{X},\tilde{Y})&=H(\tilde{X})+H(\tilde{Y}|\tilde{X})\\&=H(X)+H(\tilde{Y}|X)=H(X,\tilde{Y})\end{aligned} \quad (18)$$

となる．また，同様な変形を $\tilde{Y}$ に対して行うと，

$$H(\tilde{X},\tilde{Y})=H(X,Y) \quad (19)$$

となる．この結果は，位相回転を補償しても結合エントロピーに変化がないことを示している．

この結果を活用すると，秘密鍵容量の上限 $S(X;Y||Z)_{up}$ と下限 $S(X;Y||Z)_{low}$ は，式(5)と式(6)の２倍となる．

3.2 移動通信路モデルにおける理論解析

受信検波信号が同相・直交成分からなる場合，相関情報を取得する移動通信モデルは Fig. 3 と異なり，位相回転を受けた送信信号が受信され，チャネル係数とその空間相関係数が複素となる．このため，

$$\begin{aligned}&\tilde{X}=S_A+\tilde{N}_X,\tilde{Y}=S_B+\tilde{N}_Y,\tilde{Z}=S_E+\tilde{N}_Z\\&S_A=Se^{j\theta_A},\ S_B=Se^{j\theta_B}\\&S_E=\rho_E\mathrm{S}+\sqrt{1-|\rho_E|^2}\tilde{W},\rho_E=|\rho_E|e^{j\theta_E}\end{aligned} \quad (20)$$

と表される．

式(20)で，$\tilde{X},\tilde{Y},\tilde{Z}$ に位相回転補償を行うと，

$$\begin{aligned}X&=S+N_X,\ N_X=\tilde{N}_Xe^{-j\theta_A}\\Y&=S+N_Y,N_Y=\tilde{N}_Ye^{-j\theta_B}\end{aligned} \quad (21)$$

$$Z=\rho S+\sqrt{1-\rho^2}W+N_Z,\ \rho=|\rho_E| \quad W=\tilde{W}e^{-j\theta_E},\ N_Z=\tilde{N}_Ze^{-j\theta_E} \quad (22)$$

となる．ここで，S,W,N_X,N_Y,N_Z の実部・虚部は独立で，その電力は$P_{Sr}=P_{Si}=P_{Wr}=P_{Wi}=P_s,\ P_{Xr}=P_{Xi}=P_x,\ P_{Yr}=P_{Yi}=P_y,P_{Zr}=P_{Zi}=P_z$ となる．

次に，複素相関情報 $\tilde{X},\tilde{Y},\tilde{Z}$ のエントロピーと結合エントロピーは，3.1 節の検討と同様に位相回転補償を行っても変化がない．そこで，$\tilde{X},\tilde{Y},\tilde{Z}$ の代わりに X,Y,Z を用いる．

この結果を活用すると，秘密鍵容量の上限と下限 $S(X;Y||Z)_{up},\ S(X;Y||Z)_{low}$ は，それぞれ式(7)と式

(8)の２倍となる．また，$P_x = P_y$ とし，$\alpha = P_z/P_x$ とすると，$S(X;Y||Z)_{up}$ は式(9)の２倍となり，$\alpha = 0$ の場合に式(10)の２倍となる．一方，$S(X;Y||Z)_{low}$ はそれぞれの場合に式(11)と式(12)の２倍となる．

なお，秘密鍵容量に関係する個々の相互情報量も実数の場合の理論式[16]の２倍となっている．それゆえ，相互情報量 $I(X;Y)$，$I(X;Z)$ は，

$$I(X;Y) = \log_2 \frac{(P_s+P_x)(P_s+P_y)}{P_s(P_x+P_y)+P_xP_y} \tag{23}$$

$$I(X;Z) = \log_2 \frac{(P_s+P_x)(P_s+P_z)}{(1-\rho^2){P_s}^2+P_s(P_x+P_z)+P_xP_z} \tag{24}$$

となる．さらに，$P_x = P_y$ とし，$\alpha = P_z/P_x$ を用いて，

$$I(X;Y) = \log_2 \frac{(\gamma+1)^2}{2\gamma+1} = \log_2\left(1+\frac{\gamma^2}{2\gamma+1}\right) \tag{25}$$

$$I(X;Z) = \log_2\left\{1+\frac{\rho^2\gamma^2}{(1-\rho^2)\gamma^2+\gamma(\alpha+1)+\alpha}\right\} \tag{26}$$

$$I(X;Z) = \log_2\left\{1+\frac{\rho^2\gamma}{(1-\rho^2)\gamma+1}\right\},\quad \alpha = 0 \tag{27}$$

となる．ここで，$I(X;Z)$ は正規者と盗聴者が共有する情報量であるが，正規者から盗聴者に漏洩する情報量（漏洩情報量）でもある．

3.3 シミュレーションによる相互情報量の検証

上記の理論解析の結果，複素のチャネル係数の場合に結合エントロピーや相互情報量が実部の場合の２倍となること，位相回転に対して不変であることが分かった．この妥当性を検証するため計算機シミュレーションで複素のチャネル係数を発生させ，多値量子化値の発生確率と結合発生確率からエントロピーと結合エントロピーを算出し，相互情報量を算出する[19]．

Fig. 4 に複素と実部のチャネル係数に対する相互情報量 $I(X;Y)$，漏洩情報量 $I(X;Z)$ の理論値とシミュレーション結果を示す．ここで，相関係数 $\rho = 0.5$ で，量子化ビット数 $M_b = 5$ である．Fig. 4 の理論値とシミュレーション結果は，漏洩情報量でほぼ一致しているが，相互情報量では SN 比の増加に伴い不一致が拡大する．この不一致は，量子化の多値数が 32 値と十分に大きくないためである[19]．また，複素の結果は，実部の場合の結果の２倍となっている．

Fig. 5 に空間相関係数と位相回転を変えた場合の漏洩情報量のシミュレーション結果と理論値を示す．ここで，量子化ビット数 $M_b = 4$ である．理論値とシミュレーション結果がほぼ一致している．

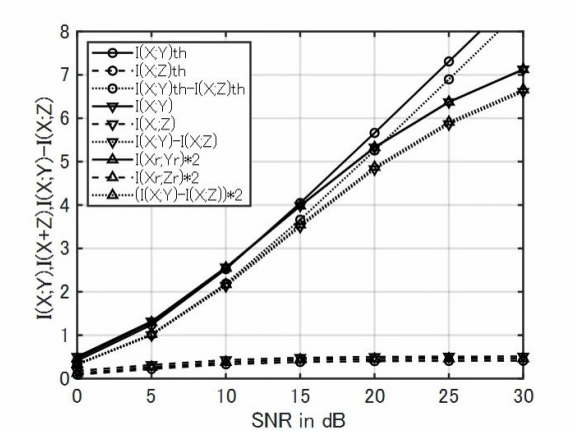

Fig. 4. Simulation results and theoretical value of mutual information as a function of signal to noise power ratio.

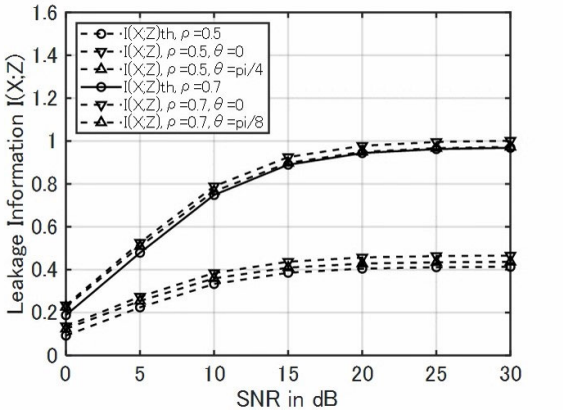

Fig. 5. Simulation results and theoretical value of leakage information as a function of signal to noise power ratio for various correlation coefficient and phase rotation.

４．複数地点観測に対する漏洩情報量の理論解析

4.1 複数地点観測に対する秘密鍵容量と漏洩情報量

秘密鍵容量の上限と下限は，式(1)と式(2)で表されるが，盗聴者の n 地点測定に拡張すると，

$$S(X;Y||Z_1,\cdots,Z_n)_{up} = min[I(X;Y), I(X;Y|Z_1,\cdots,Z_n)] \tag{28}$$

$$S(X;Y||Z_1,\cdots,Z_n)_{low} = max\,[I(X;Y)-I(X;Z_1,\cdots,Z_n),\ I(X;Y)-I(Y;Z_1,\cdots,Z_n)] \tag{29}$$

と表される．ここで，$I(X;Y)$ の部分は式(1)と式(2)

と同様であるが，正規者から盗聴者への漏洩情報量 $I(X;Z_1,\cdots,Z_n)$ が異なっている. 以下では, 移動通信路モデルを対象とし，理論解析を簡易にするため漏洩情報量の導出を行う． なお, 以下では数式の導出を容易にするため, 盗聴者の雑音電力がゼロ（ $P_{Zk}=0,\alpha_k=0$ ）を仮定する.

4.2 盗聴者の２地点観測に対する漏洩情報量

4.2.1 漏洩情報量の理論解析

盗聴者の 2 地点測定に対する漏洩情報量 $I(X;Z_1,Z_2)$ は, $I(X;Z_1,Z_2)=H(X)-H(X|Z_1,Z_2)$ と表されるので，文献[16]の付録 B を参考にして，$H(X|Z_1,Z_2)$ を導出する．このため，$U_2=X-\beta Z_1-\delta Z_2$ とし，U_2と Z_1, U_2 と Z_2 がお互いに独立（直交）となる β と δ を設定すると, $H(X|Z_1,Z_2)=H(U_2)$ となる.

ここで， $X=S+N_X$, $Z_i=S_i=\rho_i S+\sqrt{1-\rho_i{}^2}W_i$, $i=1,2$ とし, X と Z_1,Z_2 相関係数を ρ_1,ρ_2， Z_1,Z_2 の相関係数を ρ_{12}とする．また，$\overline{U_2Z_1{}^*}=\overline{XZ_1{}^*}-\beta\overline{Z_1Z_1{}^*}-\delta\overline{Z_2Z_1{}^*}=0$ と $\overline{U_2Z_2{}^*}=\overline{XZ_2{}^*}-\beta\overline{Z_1Z_2{}^*}-\delta\overline{Z_2Z_2{}^*}=0$ から β,δ を求めると,

$$\beta=\frac{\rho_1-\rho_2\rho_{12}}{1-|\rho_{12}|^2},\ \delta=\frac{\rho_2-\rho_1\rho_{12}{}^*}{1-|\rho_{12}|^2} \tag{30}$$

となり，$U_2=S+N_X-\beta S_1-\delta S_2$ となる.

ここで，$U_2=U_{r2}+jU_{i2}$ とすると，U_{r2},U_{i2} は独立となり, $H(U_2)=H(U_{r2})+H(U_{i2})$ となる. さらに, その電力 $P_{U2}=\overline{U_{r2}{}^2}=\overline{U_{i2}{}^2}$ が,

$$P_{U2}=\frac{(1-|\rho_{12}|^2)^2(P_s+P_x)-\{\rho_1{}^2-\rho_1\rho_2(\rho_{12}+\rho_{12}{}^*)-\rho_2{}^2\}P_s}{(1-|\rho_{12}|^2)^2} \tag{31}$$

となることを用いると,

$$H(X|Z_1,Z_2)=\log_2(2\pi eP_{U2}) \tag{32}$$

となる．さらに，漏洩情報量は,

$$\begin{aligned}I(X;Z_1,Z_2)&=H(X)-H(X|Z_1,Z_2)\\&=\log_2\frac{(1-|\rho_{12}|^2)^2(P_s+P_x)}{(1-|\rho_{12}|^2)^2(P_s+P_x)-\{\rho_1{}^2-\rho_1\rho_2(\rho_{12}+\rho_{12}{}^*)+\rho_2{}^2\}P_s}\end{aligned} \tag{33}$$

となる．さらに，SN 比 γ を用いると,

$$I(X;Z_1,Z_2)=\log_2[1+\frac{(\rho_1{}^2-\rho_1\rho_2(\rho_{12}+\rho_{12}{}^*)+\rho_2{}^2)\gamma}{\{1-|\rho_{12}|^2-\rho_1{}^2+\rho_1\rho_2(\rho_{12}+\rho_{12}{}^*)-\rho_2{}^2\}\gamma+1-|\rho_{12}|^2}] \tag{34}$$

となる.

4.2.2 チャネル係数の相関係数と漏洩情報量

式(34)に示される漏洩情報量は，相関係数 ρ_1,ρ_2 の他に相関係数 ρ_{12} に依存する．ここで，ρ_1,ρ_2 と ρ_{12} の関係は， $Z_i=S_i=\rho_i S+\sqrt{1-\rho_i{}^2}W_i$, $i=1,2$ において W_1,W_2 が独立な場合に, $\rho_{12}=\rho_1\rho_2$ となる. また, W_1,W_2 の相関係数が $(-1,1)$ の範囲の全ての値をとる可能性を想定すると， Z_1, Z_2 が無相関となる可能性も皆無でない．さらに，全ての相関係数が同程度（$\rho_{12}\approx\rho_1,\rho_2$）となることも想定される. 以下では, 理論式の導出を容易とするため，$\rho_1=\rho_2=\rho$ とし，$\rho_{12}=\rho^2,\rho,0$ の３種の場合について漏洩情報量を求める.

はじめに，$\rho_{12}=\rho^2$ の場合には，式(34)に代入して数式の整理を行うと,

$$I(X;Z_1,Z_2)\cong\log_2\left\{1+\frac{2\rho^2\gamma}{(1-\rho^2)\gamma+1+\rho^2}\right\} \tag{35}$$

となる．次に，$\rho_{12}=\rho$ の場合にも同様にして,

$$I(X;Z_1,Z_2)\cong\log_2\left\{1+\frac{2\rho^2\gamma}{(1-\rho)(1+2\rho)\gamma+1+\rho}\right\} \tag{36}$$

また，$\rho_{12}=0$ の場合にも同様にして,

$$I(X;Z_1,Z_2)\cong\log_2\left\{1+\frac{2\rho^2\gamma}{(1-2\rho^2)\gamma+1}\right\} \tag{37}$$

となる.

4.3 盗聴者の３地点以上の測定に対する漏洩情報量

4.3.1 ３地点測定に対する漏洩情報量の理論解析

ここでも上記と同様に $\rho_1=\rho_2=\rho_3=\rho$ とし，３地点観測に対する漏洩情報量 $I(X;Z_1,Z_2,Z_3)$ を導出する．ここで，$U_3=X-\beta Z_1-\delta Z_2-\mu Z_3$ と Z_1, Z_2, Z_3 が独立(直交)となる β, δ, μ を設定すると，$H(X|Z_1,Z_2,Z_3)=H(U_3)$ となる.

はじめに，Z_1, Z_2, Z_3 間の相関係数については，$\rho_{12}=\rho_{13}=\rho_{23}=\rho^2$ とする．このとき，$\overline{U_3Z_1{}^*}=0$, $\overline{U_3Z_2{}^*}=0$, $\overline{U_3Z_3{}^*}=0$ から β, δ, μ を求めると,

$$\beta=\delta=\mu=\frac{\rho}{1-2\rho^2} \tag{38}$$

となり, $U_3=S+N_X-\beta(S_1+S_2+S_3)$ となる. ここで，$U_3=U_{r3}+jU_{i3}$ とすると，U_{r3},U_{i3} は独立となり, $H(U_3)=H(U_{r3})+H(U_{i3})$ となる. さらに, その電力 $P_{U3}=\overline{U_{r3}{}^2}=\overline{U_{i3}{}^2}$ が,

$$\begin{aligned}P_{U3}&=P_s+P_x+\{-6\beta\rho+3\beta^2(1+2\rho^2)\}P_s\\&=P_s+P_x-\frac{3\rho^2}{1-2\rho^2}P_s\end{aligned} \tag{39}$$

となることを用いると,

$$I(X;Z_1,Z_2,Z_3)=\log_2(2\pi eP_{U3}) \tag{40}$$

となる．さらに，漏洩情報量は，

$$I(X;Z_1,Z_2,Z_3) = H(X) - H(X|Z_1,Z_2,Z_3) = \log_2\left\{\frac{(P_s+P_x)(1+2\rho^2)}{(P_s+P_x)(1+2\rho^2)-3\rho^2P_s}\right\} \quad (41)$$

となる．さらに，SN 比 γ を用いると，

$$I(X;Z_1,Z_2,Z_3) = \log_2\left\{1+\frac{3\rho^2\gamma}{(1-\rho^2)\gamma+1+2\rho^2}\right\} \quad (42)$$

となる．

次に，$\rho_{12}=\rho_{13}=\rho_{23}=\rho$ とする．このとき，上記と同様に $\beta,\ \delta,\ \mu$ を求めると，

$$\beta=\delta=\mu=\frac{\rho}{1+2\rho} \quad (43)$$

となる．また，上記と同様に U_3 の実部・虚部の電力を求めると，

$$P_{U3}=P_s+P_x-\frac{3\rho^2}{1+2\rho}P_s \quad (44)$$

となる．また，上記と同様に SN 比に対する漏洩情報量の式を求めると，

$$I(X;Z_1,Z_2,Z_3) = \log_2\left\{1+\frac{3\rho^2\gamma}{(1-\rho)(1+3\rho)\gamma+1+2\rho}\right\} \quad (45)$$

となる．

次に，$\rho_{12}=\rho_{13}=\rho_{23}=0$ とする．このとき，上記と同様に $\beta,\ \delta,\ \mu$ を求めると，

$$\beta=\delta=\mu=\rho \quad (46)$$

となる．また，上記と同様に U_3 の実部・虚部の電力を求めると，

$$P_{U3}=P_s+P_x-3\rho^2P_s \quad (47)$$

となる．また，上記と同様に SN 比に対する漏洩情報量の式を求めると，

$$I(X;Z_1,Z_2,Z_3) = \log_2\left\{1+\frac{3\rho^2\gamma}{(1-3\rho^2)\gamma+1}\right\} \quad (48)$$

となる．

4.3.2 盗聴者の３地点以上の測定への理論式の拡張

相関係数を $\rho_{ij}=\rho^2$ とする場合に，盗聴者の１，２，３地点観測の結果（式(27)，式(35)，式(42)）を盗聴者の n 地点測定に拡張すると，

$$I(X;Z_1,\cdots,Z_n) \cong \log_2\left\{1+\frac{n\rho^2\gamma}{(1-\rho^2)\gamma+1+(n-1)\rho^2}\right\} \quad (49)$$

となる．また，相関係数を $\rho_{ij}=\rho$ とする場合には，数式(27)，数式(36)，数式(45) を盗聴者の n 地点測定に拡張すると，

$$I(X;Z_1,\cdots,Z_n) \cong \log_2\left\{1+\frac{n\rho^2\gamma}{(1-\rho)(1+n\rho)\gamma+1+(n-1)\rho}\right\} \quad (50)$$

となる．また，相関係数を $\rho_{ij}=0$ とする場合には，数式(27)，数式(37)，数式(48) を盗聴者の n 地点測定に拡張すると，

$$I(X;Z_1,\cdots,Z_n) \cong \log_2\left\{1+\frac{n\rho^2\gamma}{(1-n\rho^2)\gamma+1}\right\} \quad (51)$$

となる．

式(49)，式(50)，式(51)において，観測地点の増加に伴う漏洩情報量の増加を実効的相関係数 ${\rho_{ef,n}}^2$ の増加と見なすと，

$$I(X;Z_1,\cdots,Z_n) \cong \log_2\left\{1+\frac{{\rho_{ef,n}}^2\gamma}{(1-{\rho_{ef,n}}^2)\gamma+1}\right\} \quad (52)$$

$$\rho_{ef,n}^2=\begin{cases}\dfrac{n\rho^2}{(1-\rho^2)+n\rho^2}\\ \dfrac{n\rho^2}{1+(n-\rho)}\\ n\rho^2\end{cases} \quad (53)$$

となる．

4.3.3 実効相関係数と秘密鍵容量

各種の実効相関係数に対する漏洩情報量と秘密鍵容量の下限を Fig. 6 に示す．Fig. 6 に示すように実効相関係数が 1 に近づくと，漏洩情報量が増加する．また，実効相関係数が 0.99 と 1 に接近しても，SN 比が 20dB 以上あれば秘密鍵容量が確保できる．

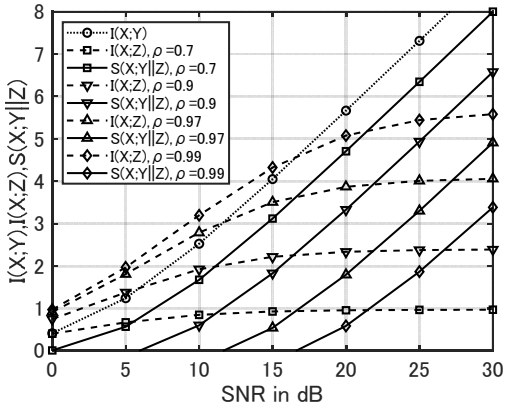

Fig. 6. Theoretical value of secret key capacity and leakage information as a function of signal to noise ratio for various effective correlation coefficient.

次に，数式を用いて検討すると，秘密鍵容量の下限は，式(25)と式(52)を用いると，

$$S(X;Y||Z_1,\cdots,Z_n)_{low} = \log_2\left[\frac{(\gamma+1)\{(1-\rho_{ef,n}^2)\gamma+1\}}{2\gamma+1}\right] = \log_2\left\{1+\frac{\gamma^2-\gamma(\gamma+1)\rho_{ef,n}^2}{2\gamma+1}\right\} \quad (54)$$

となる．ここで，式(54)がゼロ以下となるのは，$-(2\gamma+1) < \gamma^2 - \gamma(\gamma+1)\rho_{ef,n}^2 < 0$ の場合である．そこで，その条件を満たす γ の範囲を求めると，

$$S(X;Y||Z_1,\cdots,Z_n)_{low} \le 0\,,\ 0 < \gamma < \frac{\rho_{ef,n}^2}{1-\rho_{ef,n}^2} \quad (55)$$

となる．

4.4 シミュレーションによる漏洩情報量の検証

4.4.1 シミュレーションの方法

ここでは，上記の理論解析の妥当性をシミュレーションにより検証する．はじめに，盗聴者の１，２，３地点測定に対する漏洩情報量は，

$$I(X;Z_1) = H(X) + H(Z_1) - H(X,Z_1) \quad (56)$$

$$I(X;Z_1,Z_2) = H(X) + H(Z_1,Z_2) - H(X,Z_1,Z_2) \quad (57)$$

$$I(X;Z_1,Z_2,Z_3) = H(X) + H(Z_1,Z_2,Z_3) - H(X,Z_1,Z_2,Z_3) \quad (58)$$

と結合エントロピーを用いて表される．

次に，確率変数 (Z_1,Z_2,Z_3) の発生法は，相関係数の設定に対応して以下の２種類をとした．はじめに，$\rho_{12}=\rho_{13}=\rho_{23}=\rho^2$ の場合には，お互いに独立なガウス変数 (S,W_1,W_2,W_3) を発生させて，

$$Z_i = \rho S + \sqrt{1-\rho^2}W_i,\ i = 1,2,3 \quad (59)$$

とする．一方，$\rho_{12}=\rho_{13}=\rho_{23}=0$ の場合には，お互いに独立なガウス変数 $(W_1,W_2,W_3,W_4,W_5,W_6)$ を発生させて，

$$\begin{aligned} Z_1 &= \rho(S+W_1-W_3)+\sqrt{1-3\rho^2}W_4 \\ Z_2 &= \rho(S+W_2-W_1)+\sqrt{1-3\rho^2}W_5 \\ Z_3 &= \rho(S+W_3-W_2)+\sqrt{1-3\rho^2}W_6 \end{aligned} \quad (60)$$

とする．

なお，上記の確率変数の発生は，複素で実施すべきであるが，結合エントロピーの次元数が大きくなりシミュレーションが大変となる．そこで，複素の代わりに実部で実施し，結果の２倍を表示する．

4.4.2 シミュレーション結果

はじめに，Fig. 7 に $\rho_{12}=\rho_{13}=\rho_{23}=\rho^2$ の場合の１，２，３地点測定に対する漏洩情報量のシミュレーション結果と理論値を示す．ここで，相関関数 $\rho=0.7$ で，量子化ビット数 $M_b=4$ である．Fig. 7 に示すように測定地点数の増加に伴い漏洩情報量が増加している．また，シミュレーション結果と理論値がよく一致している．

次に, Fig. 8 に $\rho_{12}=\rho_{13}=\rho_{23}=0$ の場合の盗聴者の１，２，３地点測定に対する漏洩情報量のシミュレーション結果と理論値を示す．ここで，量子化ビット数 $M_b=4$ である．Fig. 8 に示すように $|1-3\rho^2| \ll 1$ の場合に漏洩情報量が大幅に増加している．また，シミュレーション結果と理論値がほぼ一致している．

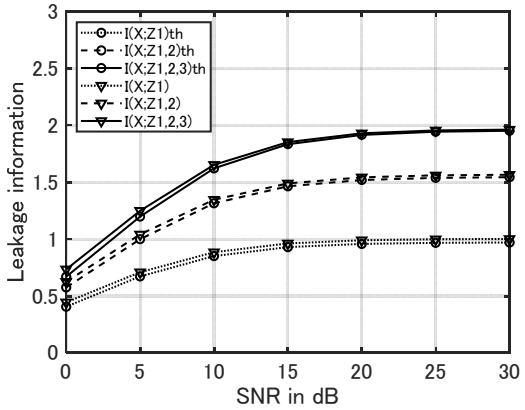

Fig. 7. Leakage information as a function of signal to noise power ratio for $\rho=0.7,\ \rho_{ij}=\rho^2$.

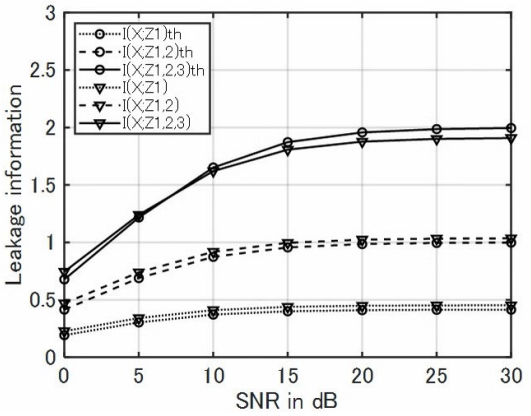

Fig. 8. Leakage information as a function of signal to noise power ratio for $\rho=0.5,\ \rho_{ij}=0$.

５．単調な伝搬環境と複数地点測定での安全性

5.1 チャネル係数の相関係数の分布と実効値

移動通信におけるマルチパス伝搬は，到来方向が

一様な多数波で構成される Jakes モデルで模擬されることが多い．このモデルでは，受信信号強度の空間分布が複雑となるとともに，半波長ほど距離が離れると空間相関係数が急速に低下する．しかし，実際の電波伝搬では，到来波数が少ないなど伝搬環境が単調となり，受信信号強度の空間分布が単調となることも想定される．なお，送信信号が既知の場合に受信信号からチャネル係数が求められる．

そこで，単調な伝搬環境の一例として，到来電波が少数のクラスター方向に限定される場合を対象として，チャネル係数の空間相関係数について検討する．Fig. 9 に正規受信者と盗聴者での受信信号が複数クラスターからの到来波で構成されるクラスター伝搬モデルを示す．図においてチャネル係数は，

$$X = \frac{1}{\sqrt{m}}(V_1 + \cdots + V_m)$$
$$Z = \frac{1}{\sqrt{m}}\left(\tilde{V}_1 + \cdots + \tilde{V}_m\right),\ \tilde{V}_i = V_i e^{j\theta_i} \tag{61}$$

と表される．ここで，チャネル係数の電力は正規化されており，$\overline{XX^*} = \overline{ZZ^*} = \overline{V_i V_i^*} = P_s$ である．

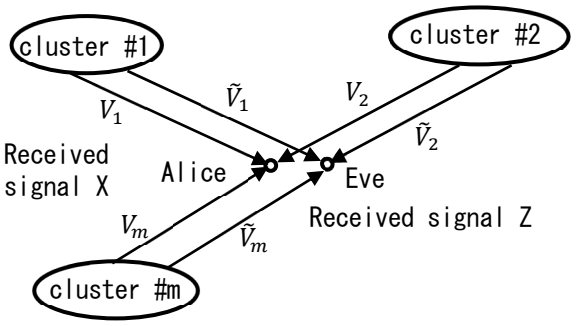

Fig. 9. Propagation model of cluster arrival waves.

正規者と盗聴者のチャネル係数の空間相関係数は，

$$\rho_{XZ} = \frac{\overline{XZ^*}}{\sqrt{\overline{XX^*}\cdot\overline{ZZ^*}}} = \frac{1}{m}\left(e^{-j\theta_1} + \cdots + e^{-j\theta_m}\right) \tag{62}$$

となる．さらに，相関係数の絶対値の 2 乗は，

$$|\rho_{XZ}|^2 = \frac{1}{m^2}\left\{m + \sum_{i\neq k, i,k=1,\cdots,m} e^{j(\theta_k - \theta_i)}\right\} \tag{63}$$

となる．ここで，正規・盗聴者間の距離が離れている（例えば，数波長離れている）場合，$\theta_i, i = 1,\cdots,m$ の値に制約がなく，ほぼランダムな値をとる．この場合に，式(45)の Σ 内の総和の平均がゼロに近づく．ここで，$|\rho_{XZ}|^2$ の平均と ρ_{XZ} の実効値（RMS 値）は，

$$\overline{|\rho_{XZ}|^2} = \frac{1}{m},\ \rho_{rms} = \sqrt{\overline{|\rho_{XZ}|^2}} = \frac{1}{\sqrt{m}} \tag{64}$$

となる．式(64)は，距離がある程度離れるとチャネル係数の空間相関係数の実効値が一定となることを示している．

次に，盗聴者の 2 地点測定によるチャネル係数を

$$Z_1 = \frac{1}{\sqrt{m}}\left(V_1 e^{j\theta_1} + \cdots + V_m e^{j\theta_m}\right)$$
$$Z_2 = \frac{1}{\sqrt{m}}(V_1 e^{j\varphi_1} + \cdots + V_m e^{j\varphi_m}) \tag{65}$$

とすると，(Z_1, Z_2) の相関係数は

$$\rho_{Z_1 Z_2} = \frac{1}{m}\left(e^{j\psi_1} + \cdots + e^{j\psi_m}\right),\ \psi_i = \theta_i - \varphi_i \tag{66}$$

となる．さらに，相関係数の絶対値の 2 乗は，

$$\left|\rho_{Z_1 Z_2}\right|^2 = \frac{1}{m^2}\left\{m + \sum_{i\neq k, i,k=1,\cdots,m} e^{j(\psi_k - \psi_i)}\right\} \tag{67}$$

となる．ここで，2 地点間の距離が離れている場合，上記の議論と同様にして，$\left|\rho_{Z_1 Z_2}\right|^2$ の平均と $\rho_{Z_1 Z_2}$ の実効値（RMS 値）は，

$$\overline{\left|\rho_{Z_1 Z_2}\right|^2} = \frac{1}{m},\ \rho_{rms} = \sqrt{\overline{\left|\rho_{Z_1 Z_2}\right|^2}} = \frac{1}{\sqrt{m}} \tag{68}$$

となる．

Fig. 10 に式(62)や式(66)で表される相関係数の絶対値の確率密度分布を示す．クラスター数の増加に伴って確率密度のピークが相関係数の小さい方に移動することが分かる．また，相関係数がほぼゼロとなる確率は，$m = 2$ の場合を除くとほとんどゼロである．

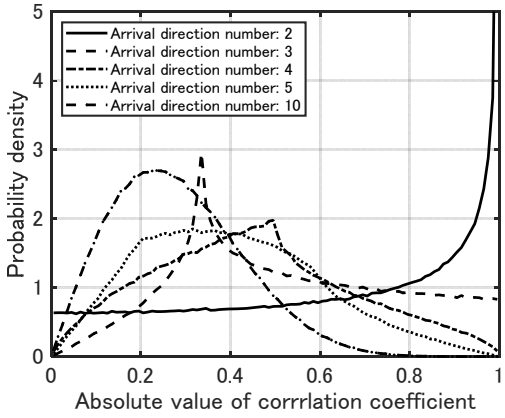

Fig. 10. Distribution of absolute value of correlation coefficient for various number of arrival direction.

5.2 複数地点観測に対する秘密鍵共有の安全性

ここでは，式(53)に示される n 地点測定における実効相関係数，並びに式(63)に示されるクラスター数 m に対する正規者と盗聴者のチャネル係数の空間相関係数の実効値を用いて，大まかな評価を行う．

はじめに，$m=2$ の場合を除くと発生確率がほぼゼロであるが，相関係数を仮に $\rho_{ij}=0$ とする場合には，

$$\rho_{ef,n}^2 \approx n\rho_{rms}^2 \approx \frac{n}{m} \tag{69}$$

となる．ここで，$n \approx m$ となると平均的に $\rho_{ef,n}^2 \approx 1$ となり，漏洩情報量が大幅に増加することになる．しかし，この可能性は，$m=2$ の場合を除くと皆無である．

次に，相関係数を $\rho_{ij}=\rho^2$ とする場合には，

$$\rho_{ef,n}^2 \approx \frac{n\rho_{rms}^2}{1+(n-1)\rho_{rms}^2} = \frac{n}{n+m-1} \tag{70}$$

となる．ここで，$n \gg m$（例えば，$n=9m, 19m$）の場合に $\rho_{ef,n}^2 \cong 0.9, 0.95$ となり，$\rho_{ef,n} \approx 1$ となる．測定地点数に対する実効相関係数のクラスター数依存性を示す．Fig. 11 に示すように，m が小さいと n の増加に伴って実効相関係数が 1 に近づく．

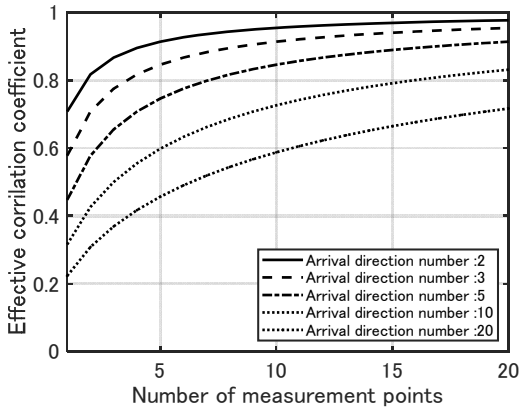

Fig. 11. Effective correlation coefficient vs. number of observation points.

以上の結果，単調な伝搬環境（到来波数 m が小）において測定地点数（n）が多い場合（$n \gg m$）に漏洩情報量が増加する．また，$m=2$ の場合，($n \approx m$) においても漏洩情報量が増加する可能性がある．このように，単調な電波伝搬環境においては，盗聴者の複数地点測定に対する秘密鍵容量が大幅に低下する理論的な危険性がある．このため，電波伝搬環境の複雑性が秘密鍵共有の安全性の確保のために重要である．

しかし，上記の結果は相互情報量に基づく理論上のものであり，現実的な安全性の評価においては，以下のことに注意する必要がある．はじめに，上記は正規者にとって最悪ケース（到来波数が小，盗聴者の受信雑音がゼロ）における理論的な評価である．また，盗聴が理想的に行われた場合の理論上の限界であり，盗聴の具体的な実現法が不明であるとともに，理想的な位相回転補償を前提としている．

6．まとめ

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の理論解析において，複素相関情報への拡張，複数地点盗聴への拡張を検討した．また，単調な電波伝搬環境における複数地点盗聴に対する安全性の評価を行った．

その結果，ガウス性相関情報が複素の場合に，相互情報量や秘密鍵容量の理論式が実の場合の２倍となることが分かった．また，複数地点盗聴における漏洩情報量の理論式を導出し，盗聴地点数と共に漏洩情報量が増加することを示した．また，これらの理論式の妥当性をシミュレーションで確認した．

一方，単調な伝搬環境としてクラスター伝搬モデルを設定した場合に，到来波数が小さいとチャネル係数の空間相関係数が比較的大きいことを示した．また，到来波数に対して盗聴地点数が十分大きくなると，漏洩情報量が大きくなる危険性を明らかにした．

今後の課題として，電波伝搬モデルに基づく理論的な評価のみでなく，シミュレーションによる現実に近い電波伝搬環境を想定したチャネル係数の算出と漏洩情報量と秘密鍵容量の評価がある．

参考文献

1) H. Yamamoto, “Information Theory in 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**, 656-715 (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) J. E. Hershey, A. A. Hassan, and R. Yarlagadda, “Unconventional Cryptographic Keying Variable Management”, *IEEE Trans. Commni*., **43**[1], 3-6 (1995)

7) 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)

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

9) 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)

10) 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)

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

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

13) 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)

14) 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)

15) 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)

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２）移動通信路モデル―”，同志社大学ハリス理化学研究報告，**57**[1], 47-56 (2013)

17) H. Liu. J. Yang, Y. Wang, Y. Chen, and C. E. Koksal, “Group Secret Key Generation via Received Signal Strength: Protocols, Achievable Rates, and Implementation”, *IEEE Trans. Mobile Computing*, **13**[12], 2820-2835 (2014).

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

19) 笹岡秀一, 岩井誠人, “移動伝搬特性に基づくグループ鍵共有の秘密鍵容量－（その１）星型接続の場合－”, 同志社大学ハリス理化学研究報告，**61**[2]，69-78(2020)