Secret Key Capacity of Group Key Agreement Based on Mobile Propagation Characteristics－Part II: In the Case of Chain Connection

Hideichi SASAOKA and Hisato IWAI*

(Received July 13, 2020)

Secret key agreement based on radio propagation characteristics attracts attention as a kind of the wireless physical layer security recently. As one field, there is a group secret key agreement to notify of the difference between the series of RSS in star connection and chain connection system. However, the conventional method has a problem in derivation of theoretical expression of the secret key capacity. This paper deals with a close numerical formula of upper and lower limit of the secret key capacity to be given in mutual information for chain connection systems. This paper derives new theoretical expression of the secret key capacity that is a function of the SN ratio by new theoretical analysis for the mutual information. As a result, numerical computation shows that the upper limit of the secret key capacity accords with the lower limit in high SN ratio. In addition, the simulation results show validity of theoretical expression because the simulation results accord with theoretical characteristics well.

Key words: physical layer security, group secret key agreement, secret key capacity, mobile propagation characteristics

キーワード：物理層セキュリティ，グループ秘密鍵共有，秘密鍵容量，移動伝搬特性

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２）
― 鎖型接続の場合 ―

笹岡　秀一，　岩井　誠人

1. はじめに

無線通信は電波の傍受が容易で盗聴の危険性があるので，その対策として計算量的な複雑性を安全性の根拠とする暗号技術が用いられている．暗号技術には共通鍵暗号と公開鍵暗号に大別されるが，移動通信においては端末での処理演算量の関係で共通鍵暗号を用いるのが一般的である．しかし，共通鍵暗号においては，鍵管理や鍵配送が必要となる．

これらの一般的な暗号技術と異なり情報理論的な複雑性を安全性の根拠とする手法も研究されている．これらには，雑音のある通信路（盗聴通信路）を用いた鍵配送 [1]，相関情報に基づく鍵抽出（鍵生成）と鍵一致処理等による同一の秘密鍵共有 [2,3]などがある．また，移動通信において電波伝搬路特性を用いた秘密鍵生成が提案されている [4,5]．これは相関情報に基づく秘密鍵共有の手法の一種であるが，無線

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

物理層セキュリティにおける秘密鍵共有である [6]. この方式は電波伝搬の可逆性より正規者間で高性能な秘密鍵を共有する一方, マルチパス伝搬の場所依存性により正規者以外の秘密鍵の盗聴を阻止して効率的に秘密鍵を生成することが特徴である [7,8]. なお，生成された秘密鍵に不一致がある場合には，公開通信路を介した情報交換（公開討論）による鍵不一致解消やプライバシー増幅など秘密鍵共有プロトコルに基づいて正味の秘密鍵が共有される [9].

ここで, 相関情報を用いた秘密鍵共有においては, 秘密鍵共有手順とそれを実施した場合に得られる秘密鍵レートの検討が重要である. また，秘密鍵共有が理想的に実施された場合の秘密鍵レートの最大値，即ち，秘密鍵容量の理論検討も重要である. これに関しては，正規者（アリス，ボブ）と盗聴者（イブ）が相関情報を受け取る一方，公開通信路を介した情報通知を用いて秘密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 [2,10]. ここで，相関情報は多値又は２値の相関のある離散乱数で，その入手手法には衛星通信の利用や２元対称通信路での誤り発生などがある [2,3]. また，衛星通信モデルを対象として, 相関のあるガウス分布する標本値（アナログ情報）に対する秘密鍵容量の検討も行われている [11]. また, 移動通信路を対象としたガウス性相関情報に基づく秘密鍵共有における秘密鍵容量の検討が行われている [7,12].

一方, 電波伝搬特性に基づくグループ秘密鍵の生成の検討は少ないが，受信電界強度(RSS)の時系列（RSS 系列）を測定し，基準端末と対象端末とのRSS 系列の差分を他の無線端末に通知する手法が提案されている [13]. また, 星型接続と鎖型接続に適用した場合のグループ秘密鍵の秘密鍵容量の理論解析が行われている [13]. さらに，星型接続を対象にして, 新しい理論解析とシミュレーションによる妥当性の検証が行われている [14]. しかし，鎖型接続を対象としたシミュレーションによる妥当性の検証が行われていない.

本論文では，はじめに RSS 系列の差分を通知する鎖型接続におけるグループ秘密鍵の生成を対象として, 従来の理論解析の概要を示すとともにその問題点を明らかにした. 次に，相互情報量で表される秘密鍵容量の上限と下限のより正確な理論式を検討した. また，簡易な理論解析法を適用することで，SN 比の関数となる秘密鍵容量の理論式を導出した. さらに，秘密鍵容量のシミュレーション結果に基づいて，新しい理論式の妥当性を確認した.

2.　従来のグループ秘密鍵容量の理論式

2.1 鎖型接続のグループ秘密鍵生成

電波伝搬特性の可逆性と場所依存性に基づく複数無線端末間でのグループ秘密鍵生成は, 送受一対の無線端末間の秘密鍵生成が基本となり, 中継端末を介した拡張により実現される [14]. グループ秘密鍵生成では，はじめに無線端末 A と B 間で双方向の受信信号強度 (RSS: Received Signal Strength) を測定し，標本化により相関の高いチャネル係数 (CC: Channel Coefficient) 系列 $(\boldsymbol{h}_{A\to B}, \boldsymbol{h}_{B\to A})$ を取得する. 次に，中継端末を介して CC 系列の差分を通知することで，無線端末間で相関情報を取得する.

鎖型接続における通知情報の逐次中継を用いたグループ鍵生成の構成を Fig. 1 に示す. ここで，無線端末(Front, 1, 2〜n-2, n-1)で観測するチャネル係数を　$h_{1\to F}$, $(h_{F\to 1}, h_{2\to 1}), (h_{i-1\to i}, h_{i+1\to i}), h_{n-2\to n-1}$ とすると，通知情報 δ_i^C は,

$$\begin{aligned} \delta_1^C &= h_{F\to 1} - h_{2\to 1} \\ \delta_i^C &= h_{i-1\to i} - h_{i+1\to i}\,, i = 2, \cdots, n-1 \end{aligned} \tag{1}$$

と表される. ここで，$\Delta^C = [\delta_1^C, \delta_2^C, \cdots, \delta_{n-2}^C]$ とし，その時系列を $\boldsymbol{\Delta}^C$ とする.

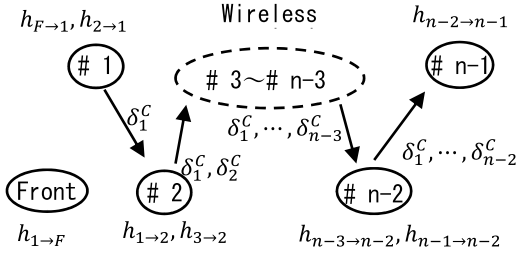

Fig. 1. Configuration of group key generation via chain connection.

2.2 従来の秘密鍵容量の理論解析

この節では, 鎖型接続の場合の秘密鍵容量の理論

式の導出の概要を説明する．なお，相互情報量で表すグループ秘密鍵容量の理論式の導出は，星型接続の場合の導出と共通する部分が多い[13,14]．鎖型接続における結果のみを示すと，

$$R_{chain}^{sec} = I(h_{1\to F}; h_{n-2\to n-1}|\boldsymbol{\Delta}^C) \tag{2}$$

となる[13]．ここで，式(2)の条件部分 $\boldsymbol{\Delta}^C$ の取り扱いを容易にするため，星型接続の場合と同様の数式変形を用いると，

$$\begin{aligned} R_{chain}^{sec} &= -H(\boldsymbol{\Delta}^C) + H(h_{n-2\to n-1}, \boldsymbol{\Delta}^C) \\ &\quad + H(\boldsymbol{\Delta}^C, h_{1\to F}) - H(h_{n-2\to n-1}, \boldsymbol{\Delta}^C, h_{1\to F}) \end{aligned} \tag{3}$$

となる[13]．

上記のそれぞれの項の確率変数の配列とその共分散行列の行列式との対応は，

$$\boldsymbol{\Delta}^C \implies (\sigma_h^2)^{n-2} d_n^{(1)} \tag{4}$$

$$\boldsymbol{\Delta}^C, h_{1\to F} \implies (\sigma_h^2)^{n-1} d_n^{(2)} \tag{5}$$

$$\boldsymbol{\Delta}^C, h_{n-2\to n-1} \implies (\sigma_h^2)^{n-1} d_n^{(3)}, d_n^{(3)} = d_n^{(2)} \tag{6}$$

$$\begin{aligned} &h_{n-2\to n-1}, \boldsymbol{\Delta}^C, h_{1\to F} \implies (\sigma_h^2)^n d_n^{(4)} \\ &\qquad d_n^{(4)} = (1+\gamma_m^{-1}) d_n^{(2)} - d_{n-1}^{(2)} \end{aligned} \tag{7}$$

となる[13]．

その結果，R_{chain}^{sec} は，

$$R_{chain}^{sec} = \log\left[\frac{\left\{(1+\gamma_m^{-1}) d_n^{(1)} - d_{n-1}^{(1)}\right\}^2}{d_n^{(1)}\left\{(1+\gamma_m^{-1}) d_n^{(2)} - d_{n-1}^{(2)}\right\}}\right] \tag{8}$$

と表される[13]．ここで，$d_n^{(1)}, d_n^{(2)}$ は漸化式を用い，

$$\begin{aligned} d_1^{(1)} &= 2(1+\gamma_m^{-1}) \\ d_2^{(1)} &= 2(1+\gamma_m^{-1}) d_1^{(1)} - 1 \\ d_n^{(1)} &= 2(1+\gamma_m^{-1}) d_{n-1}^{(1)} - d_{n-2}^{(1)} \end{aligned} \tag{9}$$

および，

$$d_n^{(2)} = (1+\gamma_m^{-1}) d_n^{(1)} - d_{n-1}^{(1)} \tag{10}$$

と表される[13]．

2.3 従来の理論式の課題

従来のグループ秘密鍵容量の理論式は，先頭無線端末(Front)と最終無線端末(n-1)の二つのチャネル係数（$h_{1\to F}$, $h_{n-2\to n-1}$）の条件付情報量となっている．しかし，本来のグループ秘密鍵容量は，先頭端末を除く複数端末（1〜n−1）が個々に取得するチャネル係数の条件付相互情報量である．即ち，

$$R_{\text{chain}}^{\text{sec}} = I(h_{1\to 2}; \cdots; h_{n-2\to n-1}|\boldsymbol{\Delta}^C) \tag{11}$$

であるべきである．しかし，従来の理論式の導出法では，式(11)の簡略化が困難と思われる．これが，従来の理論式に対する一つ目の問題である．

一方，秘密鍵容量の理論式は，上限と下限で表される[2]．従来の秘密鍵容量の理論式は，条件付相互情報量に基づいており，秘密鍵容量の上限に対応している．このため，従来の理論式は，下限を与える理論式を対象としていない．これが，従来の理論式に対する二つ目の問題である．

さらに，式(9)、(10)の漸化式の添え字に編集ミスがある．Fig. 1 に示す鎖型接続におけるグループ鍵生成の構成において，n=3 の場合，$\boldsymbol{\Delta}^C = \delta_1^C$ となり，$\Delta^C \implies \sigma_h^2\{2(1+\gamma_m^{-1})\}$ となることを考慮すると，$d_3^{(1)} = 2(1+\gamma_m^{-1})$ と訂正すべきである．このような変更を行うと式(9)は，

$$\begin{aligned} d_1^{(1)} &= 0,\ d_2^{(1)} = 1 \\ d_3^{(1)} &= 2(1+\gamma_m^{-1}) \\ d_4^{(1)} &= 2(1+\gamma_m^{-1}) d_3^{(1)} - d_2^{(1)} \\ d_n^{(1)} &= 2(1+\gamma_m^{-1}) d_{n-1}^{(1)} - d_{n-2}^{(1)} \end{aligned} \tag{12}$$

となる．また，式(10)は，

$$\begin{aligned} d_2^{(2)} &= (1+\gamma_m^{-1}) \\ d_3^{(2)} &= (1+\gamma_m^{-1}) d_3^{(1)} - 1 \\ d_n^{(2)} &= (1+\gamma_m^{-1}) d_n^{(1)} - d_{n-1}^{(1)} \end{aligned} \tag{13}$$

となる．

3. 秘密鍵容量の新しい理論解析法

3.1 通知情報の変更と従来の秘密鍵容量

Fig. 1 に示す鎖型接続におけるグループ鍵生成の構成は，通知情報の数が中継回数の増加に伴い増加することが問題である．この課題は，Fig. 1 の通知情報 δ_i^Cを Fig. 2 の通知情報 δ_i に変更することで解決できる[15]．

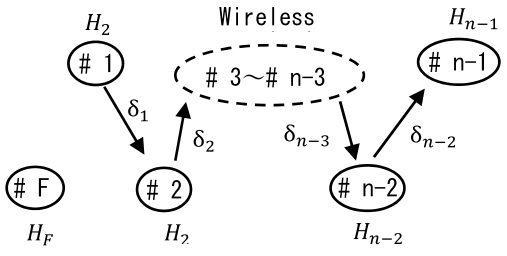

Fig. 2. Modified system configuration of group key generation via chain connection.

ここで，

$$\delta_1 = \delta_1^C,\ \delta_i = \delta_{i-1} + \delta_i^C,\ i = 2,\cdots,n-2 \quad (14)$$

である．また，各端末が取得する相関情報 H_i は，

$$\begin{aligned} &H_F = h_{1\to F},\ H_1 = h_{F\to 1} \\ &H_i = \delta_{i-1} + h_{i-1\to i},\ i = 2,\cdots,n-1 \end{aligned} \quad (15)$$

となる．

ここで，$\Delta = [\delta_1, \delta_2, \cdots, \delta_{n-2}]$ とし，その時系列を $\boldsymbol{\Delta}$ とする．この $\boldsymbol{\Delta}$ は，$\boldsymbol{\Delta}^C$ と互いに変換可能であるので，

$$\begin{aligned} R_{chain}^{sec} &= I(h_{1\to F}; h_{n-2\to n-1}|\boldsymbol{\Delta}^C) \\ &= I(h_{1\to F}; h_{n-2\to n-1}|\boldsymbol{\Delta}) \end{aligned} \quad (16)$$

となる．さらに，式(15)を用いると，

$$R_{chain}^{sec} = I(H_F; H_{n-1}|\boldsymbol{\Delta}) \quad (17)$$

となる．

新しい通知情報 δ_i は，中継回数の増加と共に雑音の影響が増加する[15]．そこで，雑音の影響を明確にするために，

$$\begin{aligned} &\delta_i^F = h_{F\to 1} - h_{i+1\to i} \\ &h_{i\to i+1} - h_{i+1\to i} = n_{i+1,i} - n_{i,i+1} = N_{i,i+1} \\ &N_i = \textstyle\sum_{j=2}^{i} N_{j-1,j} \end{aligned} \quad (18)$$

を用いると，

$$\begin{aligned} &\delta_1 = \delta_1^C = \delta_1^F \\ &\delta_i = \textstyle\sum_{j=1}^{i} \delta_i^C = \delta_i^F + N_i,\ i = 2,\cdots,n-2 \end{aligned} \quad (19)$$

となる．式(19)を用いると式(15)は，

$$\begin{aligned} &H_F = h_{1\to F},\ H_1 = h_{F\to 1} \\ &H_i = h_{F\to 1} + N_i,\ i = 2,\cdots,n-2 \end{aligned} \quad (20)$$

となる．

3.2 条件付エントロピーの簡易な導出法

3.2.1 無線端末数が 3 の場合

ここでは，式(17)に示す秘密鍵容量を与える条件付相互情報量 $R_n = I(H_F; H_{n-1}|\delta_1, \cdots, \delta_{n-2})$ の簡易な導出を示す．このため，

$$\begin{aligned} h_{e,i} &= \tfrac{1}{i+1}\textstyle\sum_{j=1}^{i} \delta_j^F \\ &= \tfrac{i}{i+1} h_{F\to 1} - \tfrac{1}{i+1}\textstyle\sum_{j=1}^{i} h_{j+1\to j} \end{aligned} \quad (21)$$

$$\begin{aligned} h_{s,i} &= h_{F\to 1} - h_{e,1} \\ &= \tfrac{1}{i+1}\left(h_{F\to 1} + \textstyle\sum_{j=1}^{i} h_{j+1\to j}\right) \end{aligned} \quad (22)$$

を用いる．

ここで，$R_3 = I(H_F; H_2|\delta_1)$ の場合，

$$\begin{aligned} R_3 &= I\left(H_F - h_{e,1}; H_2 - h_{e,1}|\delta_1\right) \\ &= I\left(h_{s,1} + N_{F,1}; h_{s,1} + N_2|\delta_1\right) \end{aligned} \quad (23)$$

となる．また，式(23)において，

$$\mathrm{E}\left[h_{s,1}\delta_1\right] = 0,\ \mathrm{E}\left[N_{F,1}\delta_1\right] = \mathrm{E}\left[N_{1,2,}\delta_1\right] = 0 \quad (24)$$

を用いると，

$$\begin{aligned} R_3 &= I\left(h_{s,1} + N_{F,1}; h_{s,1} + N_{1,2}\right) \\ &= H\left(h_{s,1} + N_{F,1}\right) + H\left(h_{s,1} + N_{1,2}\right) \\ &\quad -H\left(h_{s,1} + N_{F,1}, h_{s,1} + N_{1,2}\right) \end{aligned} \quad (25)$$

となる．さらに，式(25)に対して，

$$\begin{aligned} &P_S = \mathrm{E}[h_{F\to 1}^2] = \mathrm{E}[h_{2\to 1}^2],\ \mathrm{E}\left[h_{s,1}^2\right] = \tfrac{1}{2}P_S \\ &P_N = \mathrm{E}\left[n_{F,1}^2\right] = \mathrm{E}\left[n_{1,F}^2\right] = \mathrm{E}\left[n_{1,2}^2\right] = \mathrm{E}\left[n_{2,1}^2\right] \\ &\quad \mathrm{E}\left[N_{F,1}^2\right] = \mathrm{E}\left[N_{1,2}^2\right] = 2P_N \end{aligned} \quad (26)$$

を用いると，

$$\begin{aligned} H\left(h_{s,1} + N_{F,1}\right) &= H\left(h_{s,1} + N_{1,2}\right) \\ &= \log_2\sqrt{2\pi e(P_S/2 + 2P_N)} \end{aligned} \quad (27)$$

$$\begin{aligned} H\left(h_{s,1} + N_{F,1}, h_{s,1} + N_{1,2}\right) \\ = \log_2\sqrt{2\pi e 2P_N(P_S + 2P_N)} \end{aligned} \quad (28)$$

となる[11]．

この結果，式(27)，(28)を用いて，

$$R_3 = \log_2\sqrt{\frac{(P_S+4P_N)^2}{2P_N(P_S+2P_N)}} = \log_2\sqrt{\frac{(1+\gamma/4)^2}{1+\gamma/2}} \quad (29)$$

となる．ここで，SN 比 $\gamma = P_S/P_N$ である．

3.2.2 無線端末数が 4 以上の場合

$n \geq 4$ の場合，$R_n = I(H_F; H_{n-1}|\delta_1, \cdots, \delta_{n-2})$ の複数条件 $\delta_1, \cdots, \delta_{n-2}$ を単一条件 $\delta_1 + \cdots + \delta_{n-2}$ にまとめることを考える．このため，$i \geq 2$ に対して，

$$\hat{h}_{e,i} = \tfrac{1}{i+1}\textstyle\sum_{j=1}^{i} \delta_j = h_{e,i} + \tfrac{1}{i+1}\sum_{j=2}^{i} N_j \quad (30)$$

を用いる．ここで，$R_4 = I\left(H_F; H_3|\hat{h}_{e,2}\right)$ の場合，$\hat{h}_{e,2} = h_{e,2} + \frac{1}{3}N_{1,2}$ となり，

$$\begin{aligned} R_4 &= I\left(H_F - \hat{h}_{e,2}; H_3 - \hat{h}_{e,2}|\hat{h}_{e,2}\right) \\ &= I\left(h_{s,2} + N_{F,1} - \tfrac{1}{3}N_{1,2}; h_{s,2}\right. \\ &\quad \left. +\tfrac{2}{3}N_{1,2} + N_{2,3}|h_{e,2} + \tfrac{1}{3}N_{1,2}\right) \end{aligned} \quad (31)$$

となる．

次に，式(31)の条件付き相互情報量を相互情報量に変換する．このため，$A_{F4} = H_F - \hat{h}_{e,2} - \alpha_{F4}\hat{h}_{e,2}$ と $\hat{h}_{e,2}$ との相関がゼロとなる α_{F4} と A_{F4} を求めると，

$$\alpha_{F4} = \frac{E\left[\left(h_{s,2}+N_{F,1}-\frac{1}{3}N_{1,2}\right)\cdot\hat{h}_{e,2}\right]}{E[\hat{h}_{e,2}\cdot\hat{h}_{e,2}]} = -\frac{P_N}{3P_S+P_N} \quad (32)$$

$$A_{F4}=\frac{(P_S+P_N)h_{F\to1}+P_S(h_{2\to1}+h_{3\to2})}{3P_S+P_N}+\frac{(3P_S+P_N)N_{F,1}-P_SN_{1,2}}{3P_S+P_N} \tag{33}$$

となる．同様に，$A_{E4}=H_3-\hat{h}_{e,2}-\alpha_{E4}\hat{h}_{e,2}$ と $\hat{h}_{e,2}$ との相関がゼロとなる A_{E4} を求めると，

$$A_{E4}=\frac{(P_S-P_N)h_{F\to1}+(P_S+P_N)(h_{2\to1}+h_{3\to2})}{3P_S+P_N}+\frac{2P_SN_{1,2}+(3P_S+P_N)N_{2,3}}{3P_S+P_N} \tag{34}$$

となる．これらの結果をまとめると，

$$R_4=I\left(A_{F4};A_{E4}|\hat{h}_{e,2}\right)=I(A_{F4};A_{E4})=H(A_{F4})+H(A_{E4})-H(A_{F4},A_{E4}) \tag{35}$$

となる．

次に，式(35)を SN 比の関数として表す．このため，A_{F4},A_{E4} の共分散行列の要素を $Pa_{F4}=\mathrm{E}\left[{A_{F4}}^2\right]$, $Pa_{E4}=\mathrm{E}\left[{A_{E4}}^2\right]$, $Pa_{FE4}=\mathrm{E}[A_{F4}A_{E4}]$ とすると，

$$Pa_{F4}=\frac{P_S^2+7P_SP_N+2P_N^2}{(3P_S+P_N)},\ Pa_{FE4}=\frac{P_S^2-P_SP_N}{(3P_S+P_N)},\quad Pa_{E4}=\frac{P_S^2+9P_SP_N+2P_N^2}{(3P_S+P_N)} \tag{36}$$

となる．また，行列式 $Da_4=Pa_{F4}Pa_{E4}-{Pa_{FE4}}^2$ は，

$$Da_4=\frac{18P_S^3P_N+66P_S^2P_N^2+32P_SP_N^3+4P_N^4}{(3P_S+P_N)^2} \tag{37}$$

となる．

この結果，

$$R_4=\log_2\sqrt{\frac{Pa_{F4}Pa_{E4}}{Da_4}}=\log_2\sqrt{\frac{(P_S^2+7P_SP_N+2P_N^2)(P_S^2+9P_SP_N+2P_N^2)}{18P_S^3P_N+66P_S^2P_N^2+32P_SP_N^3+4P_N^4}}=\log_2\sqrt{\frac{(1+7\gamma/2+\gamma^2/2)(1+9\gamma/2+\gamma^2/2)}{1+8\gamma+33\gamma^2/2+9\gamma^3/2}} \tag{38}$$

となる．

3.3 従来の秘密鍵容量の新しい近似式

3.3.1 高 SN 比における近似

高 SN 比の場合には，3.2.2 において雑音間の相関の影響が減少し，$n\geq5$ の場合も $\alpha_{Fn}\cong0,\alpha_{En}\cong0$ となるので，

$$\hat{R}_n=H(B_{Fn})+H(B_{En})-H(B_{Fn},B_{En}) \tag{39}$$

となる．ここで，

$$B_{Fn}=h_{s,n-2}+N_{F,1}-\left(\frac{n-3}{n-1}N_{1,2}+\cdots+\frac{1}{n-1}N_{n-3,n-2}\right) \tag{40}$$

$$B_{En}=h_{s,n-2}+\left(\frac{2}{n-1}N_{1,2}+\cdots+\frac{n-1}{n-1}N_{n-2,n-1}\right) \tag{41}$$

である．

次に、式(40)，(41)のB_{Fn},B_{En}の共分散行列の要素 $Pb_{Fn}=E\left[{B_{Fn}}^2\right],Pb_{En}=E\left[{B_{En}}^2\right],Pb_{FEn}=E[B_{Fn}B_{En}]$ を求めると，

$$Pb_{Fn}=\frac{1}{n-1}P_S+\left[1+\frac{\{1^2+\cdots+(n-3)^2\}}{(n-1)^2}\right]2P_N=\frac{1}{n-1}P_S+\left\{2+\frac{(n-3)(n-2)(2n-5)}{3(n-1)^2}\right\}P_N \tag{42}$$

$$Pb_{En}=\frac{1}{n-1}P_S+\left[\frac{\{2^2+\cdots+(n-1)^2\}}{(n-1)^2}\right]2P_N=\frac{1}{n-1}P_S+\left\{\frac{(n-1)n(2n-1)-6}{3(n-1)^2}\right\}P_N \tag{43}$$

$$Pb_{FEn}=\frac{1}{n-1}P_S-\frac{\{(n-3)2+\cdots+1(n-2)\}}{(n-1)^2}2P_N=\frac{1}{n-1}P_S-\frac{(n-3)(n-2)(n+2)}{3(n-1)^2}P_N \tag{44}$$

となる．式(42)，(43)，(44)において，

$$k_{Fn}=2+\frac{(n-3)(n-2)(2n-5)}{3(n-1)^2}=\frac{2n^3-9n^2+25n-24}{3(n-1)^2}$$
$$k_{En}=\frac{(n-1)n(2n-1)-6}{3(n-1)^2}=\frac{2n^3-3n^2+n-6}{3(n-1)^2} \tag{45}$$
$$k_{FEn}=\frac{(n-3)(n-2)(n+2)}{3(n-1)^2}=\frac{n^3-3n^2-4n+12}{3(n-1)^2}$$

とすると，行列式 $Db_n=Pb_{Fn}Pb_{E4}-{Pb_{FEn}}^2$ は，

$$Db_n=\frac{k_{Fn}+k_{En}+2k_{FEn}}{n-1}P_SP_N+\left(k_{Fn}k_{En}-{k_{FEn}}^2\right){P_N}^2 \tag{46}$$

となる．この結果，

$$\hat{R}_n=\log_2\sqrt{\frac{Pb_{Fn}Pb_{En}}{Db_n}}=\log_2\sqrt{\frac{\left(\frac{1}{n-1}P_S+k_{Fn}P_N\right)\left(\frac{1}{n-1}P_S+k_{En}P_N\right)}{\frac{k_{Fn}+k_{En}+2k_{FEn}}{n-1}P_SP_N+\left(k_{Fn}k_{En}-k_{FEn}^2\right)P_N^2}}=\log_2\sqrt{\frac{1+\frac{k_{Fn}+k_{En}}{(n-1)k_{Fn}k_{En}}\gamma+\frac{1}{(n-1)^2k_{Fn}k_{En}}\gamma^2}{K_1+K_2\gamma}} \tag{47}$$

となる．ここで，

$$K_1=\frac{k_{Fn}k_{En}-{k_{FEn}}^2}{k_{Fn}k_{En}},K_2=\frac{k_{Fn}+k_{En}+2k_{FEn}}{(n-1)k_{Fn}k_{En}} \tag{48}$$

とする．

3.3.2 新しい近似式

式(47)は，低 SN 比での近似精度が良好でなく，γ の減少に伴い，一旦ゼロとなった後で正の値をとり，ゼロに漸近しない．そこで，γ の減少に伴いゼロに漸近する簡易な近似を検討する．近似式を

$$Ra_n = \log_2 \sqrt{\frac{1+b_n\gamma+c_n\gamma^2}{1+a_n\gamma}} \tag{49}$$

の形式とする．ここで，a_n, b_n, c_n は n の有理式である．

式(47)において，$\gamma \gg 1$ の場合に γ に比例する支配的な成分の係数 β_n は，

$$\begin{aligned}\beta_n &= \frac{1}{(n-1)k_{Fn}} \cdot \frac{1}{(n-1)k_{En}} \div K_2 \\ &= \frac{1}{(n-1)(k_{Fn}+k_{En}+2k_{FEn})} = \frac{1}{2(n-1)^2}\end{aligned} \tag{50}$$

となる．また，式(47)の√内において，γ 対する分子の 1 次係数，2 次係数と分母の 1 次係数の n に対する次数が，それぞれ $-2, -4, -2$ であることを参考にして，

$$Ra_n = \log_2 \sqrt{\frac{1+\alpha_2\beta_n\gamma+\alpha_1\beta_n^2\gamma^2}{1+\alpha_1\beta_n\gamma}} \tag{51}$$

なる近似を行う．ここで，α_1, α_2 は定数とする．ここで，$n=3$ の場合に，式(29)と一致するように定数をもとめると，$a_1 = a_2 = 4$ となる．この結果，

$$Ra_n = \log_2 \sqrt{\frac{1+\frac{2}{(n-1)^2}\gamma+\frac{1}{(n-1)^4}\gamma^2}{1+\frac{2}{(n-1)^2}\gamma}} \tag{52}$$

となる．

3.4 簡易な理論解析法の妥当性の確認

従来の秘密鍵容量の理論式に対する簡易な導出法の妥当性を確認するため，従来の理論式と新しい理論解析による理論式及び近似式との比較を行った．ここで，従来の理論式は式(8)で表される R_{chain}^{sec} である．なお，$d_n^{(1)}, d_n^{(2)}$ として訂正した式(12)と式(13)を用いている．また，新しい理論式は，式(27)，式(38)で表される R_3, R_4 である．また，近似式は，式(52)で表される Ra_n を示している．Fig. 3 に SN 比に対する秘密容量特性を示す．Fig. 3 において，conv. は従来の理論式，new は新しい理論式，ap. は近似式である．Fig. 3 から両者の理論特性は，一部で微小な不一致があることを除き，非常によく一致することが分かる．

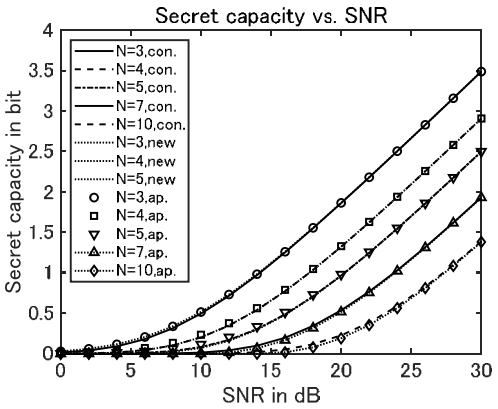

Fig. 3. Secret key capacity as a function of signal to noise power ratio (SN ratio).

4. グループ秘密鍵容量の上限・下限の理論式

4.1 鎖型接続の等価モデル

Fig. 1 に示す鎖型接続におけるグループ鍵生成の修正構成（Fig. 2）は，等価的に Fig. 4 に示す星型接続における構成に変更できる．この構成では，中継端末 Ryan から通知情報 $\delta_1, \cdots, \delta_{n-2}$ が多段中継でなく，同報的に各無線端末に送信され，各無線端末で相関情報 $H_1, \cdots, H_{n-1}$ が取得される．

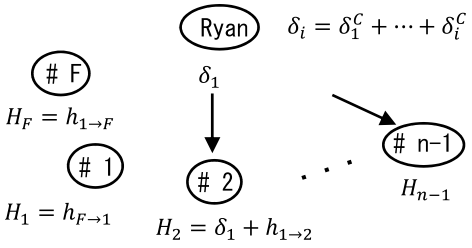

Fig. 4. Modification of system configuration from chain connection to star connection.

この結果，鎖型接続のグループ鍵生成の等価モデルが，Fig, 5 のように表される．このモデルにおいて各無線端末が取得する相関情報 X_i は，$X_i = S + N_i$ となる．ここで，

$$N_1 = 0,\ N_i = \sum_{j=2}^{i} N_{j-1,j},\ i = 2, \cdots, n-1 \tag{53}$$

と表される．また，盗聴者が取得する相関情報 Z

は，$h_{e,1}, n=3$, $\hat{h}_{e,n-2}$, $n \geq 4$ と表される．このモデルを星型接続における等価モデル比較すると，信号成分 S ，雑音成分 N_i ，盗聴成分 Z の値が相違することを除いて同一である [14]．このため，星型接続における理論解析と同様な手法が適用できる．

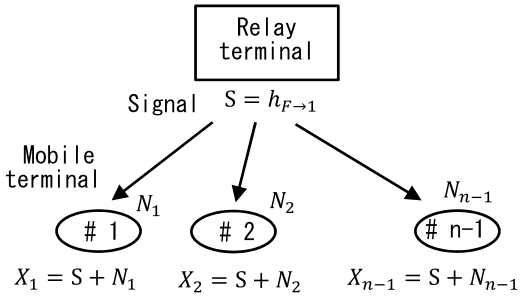

Fig. 5. Equivalent model of group key generation without eavesdropper.

4.2 グループ秘密鍵容量の下限の理論式

4.2.1 相互情報量の理論式

グループ秘密鍵容量の下限は，

$$\begin{aligned} &S(X_1;\cdots;X_{n-1}||Z) \\ &\geq max[I(X_1;\cdots;X_{n-1}) - I(X_1;Z),\cdots \\ &\quad ,I(X_1;\cdots;X_{n-1}) - I(X_{n-1};Z)] \end{aligned} \tag{54}$$

と表される [14]．ここで，$I(X_1;\cdots;X_{n-1})$ は，盗聴のない場合に無線端末が共有する相互情報量であり，$I(X_1;Z),\cdots,I(X_{n-1};Z)$ は，盗聴端末への秘密鍵の漏洩情報量である．

ここでは，相互情報量 $MI_n = I(X_1;\cdots;X_{n-1})$ の理論解析を行う．はじめに，多数の相関情報の相互情報量が，一対の相関情報の相互情報量に帰着できることを示す．$MI_4 = I(X_1;X_2;X_3)$ の場合，

$$\begin{aligned} I(X_1;X_3|X_2) &= H(X_3|X_2) - H(X_3|X_1,X_2) \\ &= H\big(N_{2,3}|X_2\big) - H\big(N_{2,3}|X_1,X_2\big) = 0 \end{aligned} \tag{55}$$

を用いると，

$$MI_4 = I(X_1;X_3) - I(X_1;X_3|X_2) = I(X_1;X_3) \tag{56}$$

となる．また，$MI_5 = I(H_1;H_2;H_3;H_4)$ の場合，式(55)と同様に，

$$\begin{aligned} &I(X_1;X_2;X_4|X_3) \\ &= I(X_1;X_4|X_3) - I(X_1,X_4|X_2,X_3) = 0 \end{aligned} \tag{57}$$

を用い，さらに式(56)と同様な導出を行うと，

$$\begin{aligned} MI_5 &= I(X_1;X_2;X_4) - I(X_1;X_2;X_4|X_3) \\ &= I(X_1;X_4) - I(X_1;X_4|X_2) = I(X_1;X_4) \end{aligned} \tag{58}$$

となる．同様にして，

$$\begin{aligned} MI_n &= I(X_1;X_{n-1}) \\ &= H(X_{n-1}) - H(X_{n-1}|X_1) \end{aligned} \tag{59}$$

となる．さらに，MI_n は，

$$\begin{aligned} MI_n &= H(h_{F\to1} + N_{n-1}) \\ &\quad -H(h_{F\to1} + N_{n-1}|h_{F\to1}) \\ &= H(h_{F\to1} + N_{n-1}) - H(N_{n-1}) \end{aligned} \tag{60}$$

となる．また，N_{n-1} の電力が $P_{N_{n-1}} = 2(n-2)$ となるので，

$$\begin{aligned} MI_n &= \log_2 \sqrt{\frac{P_S + 2(n-2)P_N}{2(n-2)P_N}} \\ &= \log_2 \sqrt{1 + \frac{\gamma}{2(n-2)}} \end{aligned} \tag{61}$$

となる．

4.2.2 漏洩情報量の理論式

漏洩情報量は，$I(X_1;Z),\cdots,I(X_{n-1};Z)$ であるが，雑音がない $X_1 = h_{F\to1}$ の場合に最大となるので，ここでは $LI_n = I(h_{F\to1};Z)$ を考える．はじめに，LI_3 は，

$$\begin{aligned} LI_3 &= H(h_{F\to1}) - H\big(h_{F\to1}|h_{e,1}\big) \\ &= H(h_{F\to1}) - H\big(h_{s,1}\big) \end{aligned} \tag{62}$$

となる．ここで，$\mathrm{E}[(h_{F\to1})^2] = P_S$, $\mathrm{E}\big[{h_{s,1}}^2\big] = \frac{1}{2}P_S$ を用いると，

$$LI_3 = \log_2 \sqrt{\frac{P_S}{P_S/2}} = \log_2 \sqrt{2} \tag{63}$$

となる．

次に，$n \geq 4$ の場合，

$$\begin{aligned} LI_n &= I\big(h_{F\to1};\hat{h}_{e,n-2}\big) \\ &= H(h_{F\to1}) + H\big(\hat{h}_{e,n-2}\big) - H\big(h_{F\to1},\hat{h}_{e,n-2}\big) \end{aligned} \tag{64}$$

ここで，$h_{F\to1}, \hat{h}_{e,n-2}$ の共分散行列の要素は，

$$\begin{aligned} Pl_F &= \mathrm{E}[(h_{F\to1})^2] = P_S \\ Pl_{Fe,n} &= \mathrm{E}\big[h_{F\to1}\hat{h}_{e,n-2}\big] = \frac{n-2}{n-1} \end{aligned} \tag{65}$$

$$\begin{aligned} Pl_{e,n} &= \mathrm{E}\big[\hat{h}_{e,n-2}^2\big] \\ &= \mathrm{E}\big[h_{e,n-2}^2\big] + \mathrm{E}\left[\left(\frac{1}{n-1}\sum_{j=2}^{n-2} N_j\right)^2\right] \end{aligned} \tag{66}$$

となる．ここで，信号成分は式(21)を用いて，

$$\begin{aligned}\mathrm{E}\left[h_{e,n-2}^2\right] &= \frac{(n-2)^2}{(n-1)^2}\mathrm{E}\left[h_{F\to 1}^2\right] + \frac{1}{(n-1)^2} \\ &\quad \cdot E\left[h_{2\to 1}^2 + \cdots + h_{n-1\to n-2}^2\right] \\ &= \left\{\frac{(n-2)^2}{(n-1)^2} + \frac{n-2}{(n-1)^2}\right\} P_S = \frac{n-2}{n-1} P_S\end{aligned} \tag{67}$$

となる．また，雑音の項は式(53)を用いて，

$$\begin{aligned}&\mathrm{E}\left[\left(\frac{1}{n-1}\sum_{j=2}^{n-2} N_j\right)^2\right] \\ &= \mathrm{E}\left[\frac{(n-2)^2}{(n-1)^2} N_{1,2}^2 + \cdots + \frac{1}{(n-1)^2} N_{n-3,n-2}^2\right] \\ &= \frac{(n-3)(n-2)(2n-5)}{3(n-1)^2} P_N\end{aligned} \tag{68}$$

となる．また，共分散行列の行列式 $Dl_n = Pl_F Pl_{en} - Pl_{Fen}{}^2$ を求めると，

$$Dl_n = P_S\left\{\frac{(n-2)P_S}{(n-1)^2} + \frac{(n-3)(n-2)(2n-5)P_N}{3(n-1)^2}\right\} \tag{69}$$

となる．

この結果，式(38)と同様に，

$$\begin{aligned}LI_n &= \log_2 \sqrt{\frac{(n-1)P_S + \frac{1}{3}(n-3)(2n-5)P_N}{P_S + \frac{1}{3}(n-3)(2n-5)P_N}} \\ &= \log_2 \sqrt{\frac{1+\frac{3(n-1)}{(n-3)(2n-5)}\gamma}{1+\frac{3}{(n-3)(2n-5)}\gamma}}\end{aligned} \tag{70}$$

となる．さらに，式(61)，式(70)からグループ秘密鍵容量の下限は，

$$\begin{aligned}SCl_n &= MI_n - LI_n \\ &= \log_2 \sqrt{\frac{\left\{1+\frac{1}{2(n-2)}\gamma\right\}\left\{1+\frac{3}{(n-3)(2n-5)}\gamma\right\}}{1+\frac{3(n-1)}{(n-3)(2n-5)}\gamma}}\end{aligned} \tag{71}$$

となる．

4.3 グループ秘密鍵容量の上限の理論式

4.3.1 グループ秘密鍵容量の上限の一般式

グループ秘密鍵容量の上限は，

$$\begin{aligned}&S(X_1, \cdots, X_{n-1} || Z) \\ &\le min[I(X_1, \cdots, X_{n-1}), I(X_1, \cdots, X_{n-1}|Z)]\end{aligned} \tag{72}$$

と表される[14]．ここでは，秘密鍵容量の上限である条件付き相互情報量 $SCu_n = I(X_1, \cdots, X_{n-1}|Z)$ の理論解析を行う．

はじめに，$SCu_3 = I(X_1; X_2|h_{e,1})$ の場合，

$$\begin{aligned}SCu_3 &= I\left(h_{F\to 1}; h_{F\to 1} + N_{1,2}|h_{e,1}\right) \\ &= I\left(h_{s,1}; h_{s,1} + N_{1,2}\right) \\ &= H\left(h_{s,1} + N_{1,2}\right) - H\left(N_{1,2}\right)\end{aligned} \tag{73}$$

となる．また，

$$\begin{aligned}H\left(h_{s,1} + N_{1,2}\right) &= \log_2 \sqrt{2\pi e(P_S/2 + 2P_N)} \\ H\left(N_{1,2}\right) &= \log_2 \sqrt{2\pi e 2P_N}\end{aligned} \tag{74}$$

となる．その結果，

$$SCu_3 = \log_2 \sqrt{\frac{P_S/2+2P_N}{2P_N}} = \log_2 \sqrt{1 + \frac{1}{4}\gamma} \tag{75}$$

となる．

次に，$SCu_4 = I(X_1; X_2; X_3|\hat{h}_{e,2})$ の場合，

$$SCu_4 = I\left(X_1; X_3|\hat{h}_{e,2}\right) - I\left(X_1; X_3|X_2, \hat{h}_{e,2}\right) \tag{76}$$

となるが，式(55)と同様に，

$$\begin{aligned}&I\left(X_1; X_3|X_2, \hat{h}_{e,2}\right) \\ &= I\left(X_3|X_2, \hat{h}_{e,2}\right) - I\left(X_3|X_1, X_2, \hat{h}_{e,2}\right) \\ &= I\left(N_{2,3}|X_2, \hat{h}_{e,2}\right) - I\left(N_{2,3}|X_1, X_2, \hat{h}_{e,2}\right) = 0\end{aligned} \tag{77}$$

を用いると，

$$\begin{aligned}SCu_4 &= I\left(X_1; X_3|\hat{h}_{e,2}\right) \\ &= I\left(h_{s,1} - \tfrac{1}{3}N_{1,2}; h_{s,1} + \tfrac{2}{3}N_{1,2} + N_{2,3}|\hat{h}_{e,2}\right)\end{aligned} \tag{78}$$

となる．ここで，$C_{F4} = h_{s,1} - \frac{1}{3}N_{1,2} - \mu_{F4}\hat{h}_{e,2}$ と $\hat{h}_{e,2}$ との相関がゼロとなる C_{F4} を求めると，

$$C_{F4} = \frac{(P_S+2P_N)h_{F\to 1} + P_S(h_{2\to 1}+h_{3\to 2}) - P_S N_{1,2}}{3P_S+2P_N} \tag{79}$$

となる．また，$C_{E4} = h_{s,1} + \frac{1}{3}N_{1,2} + N_{2,3} - \mu_{F4}\hat{h}_{e,2}$ と $\hat{h}_{e,2}$ との相関がゼロとなる C_{E4} を求めると，

$$\begin{aligned}C_{E4} &= \frac{(P_S-2P_N)h_{F\to 1} + (P_S+2P_N)(h_{2\to 1}+h_{3\to 2})}{3P_S+2P_N} \\ &\quad + \frac{2P_S N_{1,2} + (3P_S+2P_N)N_{2,3}}{3P_S+2P_N}\end{aligned} \tag{80}$$

となる．

式(79)，(80)の C_{F4}, C_{E4} の共分散行列の要素 $Pc_{F4} = E\left[C_{F4}{}^2\right]$, $Pc_{E4} = E\left[C_{E4}{}^2\right]$, $Pc_{FE4} = E[C_{F4}C_{E4}]$ と共分散行列の行列式 $Dc_4 = Pc_{F4}Pc_{E4} - Pc_{FE4}{}^2$ を求めると，

$$\begin{aligned}Pc_{F4} &= \frac{P_S(3P_S^2+6P_SP_N+4P_N^2)}{(3P_S+2P_N)^2} \\ Pc_{E4} &= \frac{3P_S^3+30P_S^2P_N+36P_SP_N^2+8P_N^3}{(3P_S+2P_N)^2} \\ Pc_{FE4} &= \frac{3P_S^3-4P_SP_N^2}{(3P_S+2P_N)^2}\end{aligned} \tag{81}$$

$$\begin{aligned}Dc_4 &= P_SP_N\left\{\frac{108P_S^4+276P_S^3P_N}{(3P_S+2P_N)^4}\right. \\ &\quad \left. + \frac{360P_S^2P_N^2+208P_SP_N^3+32P_N^4}{(3P_S+2P_N)^4}\right\}\end{aligned} \tag{82}$$

となる．この結果，

$$SCu_4 = \log_2 \sqrt{\frac{Pc_{F4}Pc_{E4}}{Dc_4}} = \log_2 \sqrt{\frac{(1+3\gamma/2+4\gamma^2/3)(1+9\gamma/2+15\gamma^2/4+3\gamma^3/8)}{1+13\gamma/2+45\gamma^2/4+69\gamma^3/8+27\gamma^4/8}} \quad (83)$$

となる．

4.3.2 高 SN 比における近似

グループ秘密鍵容量の上限 SCu_n は，$n \geq 4$ の場合，4.2.1 と同様の導出により，

$$\begin{aligned} SCu_n &= I\left(X_1; X_{n-1}|\hat{h}_{e,n-2}\right) \\ &= I\left(H_1 - \hat{h}_{e,n-2}; H_{n-1} - \hat{h}_{e,n-2}|\hat{h}_{e,n-2}\right) \end{aligned} \quad (84)$$

となる．ここで，3.2.3 と同様に高 SN 比の場合に，$G_{Fn} = H_1 - \hat{h}_{e,n-2}$ および，$G_{En} = H_{n-1} - \hat{h}_{e,n-2}$ と $\hat{h}_{e,n-2}$ の相関がほぼゼロとすると，近似式

$$\begin{aligned} \widehat{SCu}_n &= I(G_{Fn}; G_{En}) \\ &= H(G_{Fn}) + H(G_{En}) - H(G_{Fn}, G_{En}) \end{aligned} \quad (85)$$

となる．ここで，

$$G_{Fn} = h_{s,n-2} - \left(\frac{n-3}{n-1}N_{1,2} + \cdots + \frac{1}{n-1}N_{n-3,n-2}\right) \quad (86)$$

$$G_{En} = B_{En} = h_{s,n-2} + \left(\frac{2}{n-1}N_{1,2} + \cdots + \frac{n-1}{n-1}N_{n-2,n-1}\right) \quad (87)$$

である．また，G_{Fn}, G_{En} の共分散行列の要素 $Pg_{Fn} = E\left[{G_{Fn}}^2\right]$, $Pg_{En} = E\left[{G_{En}}^2\right]$, $Pg_{FEn} = E[G_{Fn}G_{En}]$ を求めると，

$$\begin{aligned} Pg_{Fn} &= \frac{1}{n-1}P_S + \frac{\{1^2+\cdots+(n-3)^2\}}{(n-1)^2}2P_N \\ &= \frac{1}{n-1}P_S + \frac{(n-3)(n-2)(2n-5)}{3(n-1)^2}P_N \end{aligned} \quad (88)$$

$$Pg_{En} = Pb_{En},\ Pg_{FEn} = Pb_{FEn} \quad (89)$$

となる．ここで，

$$\hat{k}_{Fn} = \frac{(n-3)(n-2)(2n-5)}{3(n-1)^2} \quad (90)$$

とすると，行列式 $Dg_n = Pg_{Fn}Pg_{E4} - {Pg_{FEn}}^2$ は，

$$Db_n = \frac{\hat{k}_{Fn}+k_{En}+2k_{FEn}}{n-1}P_S P_N + \left(\hat{k}_{Fn}k_{En} - {k_{FEn}}^2\right){P_N}^2 \quad (91)$$

となる．この結果，

$$\widehat{SCu}_n = \log_2 \sqrt{\frac{1+\frac{\hat{k}_{Fn}+k_{En}}{(n-1)\hat{k}_{Fn}k_{En}}\gamma + \frac{1}{(n-1)^2\hat{k}_{Fn}k_{En}}\gamma^2}{\hat{K}_1+\hat{K}_2\gamma}} \quad (92)$$

$$\hat{K}_1 = \frac{\hat{k}_{Fn}k_{En} - k_{FEn}^2}{\hat{k}_{Fn}k_{En}},\ \hat{K}_2 = \frac{\hat{k}_{Fn}+k_{En}+2k_{FEn}}{(n-1)\hat{k}_{Fn}k_{En}}$$

となる．

4.3.3 新しい近似式

式(92)は，式(47)と同様に低 SN 比での近似精度が良好でない．そこで，3.2.4 と同様に簡易な近似を検討する．式(92)において，$\gamma \gg 1$ の場合に γ に比例する支配的な成分の係数 $\hat{\beta}_n$ は，

$$\begin{aligned} \hat{\beta}_n &= \frac{1}{(n-1)^2\hat{k}_{Fn}k_{En}} \div \hat{K}_2 \\ &= \frac{1}{(n-1)\left(\hat{k}_{Fn}+k_{En}+2k_{FEn}\right)} = \frac{1}{2(n-1)(n-2)} \end{aligned} \quad (93)$$

となる．また，3.2.4 と同様の考察により，式(51)に対応して新しい近似式 Sa_n を定数 $\hat{\alpha}_1, \hat{\alpha}_2$ を用いて，

$$Sa_n = \log_2 \sqrt{\frac{1+\hat{\alpha}_2\hat{\beta}_n\gamma + \hat{\alpha}_1\hat{\beta}_n^2\gamma^2}{1+\hat{\alpha}_1\hat{\beta}_n\gamma}} \quad (94)$$

とする．

式(94)において，Sa_n の√内の有理式 $g_n(\gamma)$ は，

$$g_n(\gamma) = 1 + \frac{(\hat{\alpha}_2-\hat{\alpha}_1)\hat{\beta}_n\gamma + \hat{\alpha}_1\hat{\beta}_n^2\gamma^2}{1+\hat{\alpha}_1\hat{\beta}_n\gamma} \quad (95)$$

と変形される．一方，式(83)に示される SCu_4 の√内の有理式 $f_4(\gamma)$ は，

$$\begin{aligned} f_4(\gamma) &= \frac{1+6\gamma+\frac{45}{4}\gamma^2+\frac{75}{8}\gamma^3+\frac{27}{8}\gamma^4+\frac{9}{32}\gamma^5}{1+\frac{13}{2}\gamma+\frac{45}{4}\gamma^2+\frac{69}{8}\gamma^3+\frac{27}{8}\gamma^4} \\ &= 1 + \frac{-\frac{4}{69}\gamma^{-2}+\frac{2}{23}+0\gamma+\frac{9}{32}\gamma^2}{\frac{8}{69}\gamma^{-3}+\frac{52}{69}\gamma^{-2}+\frac{90}{69}\gamma^{-1}+1+\frac{9}{23}\gamma} \end{aligned} \quad (96)$$

と変形される．この結果，$n = 4$ の場合の式(95)と式(96)を比較し，$\gamma \gg 1$ の場合によく一致するように係数を決めると，$\hat{\alpha}_1 = \hat{\alpha}_2 = 4.7$ となる．この結果，

$$Sa_n = \log_2 \sqrt{\frac{1+\frac{4.7}{2(n-1)(n-2)}\gamma + \frac{4.7}{4(n-1)^2(n-2)^2}\gamma^2}{1+\frac{4.7}{2(n-1)(n-2)}\gamma}} \quad (97)$$

となる．

4.4 数値計算とシミュレーションの結果

4.4.1 数値計算結果

Fig. 6 にグループ秘密鍵容量の上限と下限を与える理論特性を示す．上限と下限を与える理論特性は，SN 比の増加に伴い増加し，端末数の増加に伴い減少するが，SN 比が高くなるとほぼ一致している．また，下限を与える理論特性は，SN 比が低下するとゼロ以下となっている．

次に，秘密鍵容量の下限の内訳を明らかにするた

め，Fig. 7 に移動端末間の相互情報量の理論特性と漏洩情報量の理論特性を示す．Fig. 7 において相互情報量 MI は，端末数の増加に伴う減少が比較的大きく，星型接続の場合の特性と異なっている [14]．また，漏洩情報量 LI は，星型接続の場合の特性とほぼ同様となっている [14]．

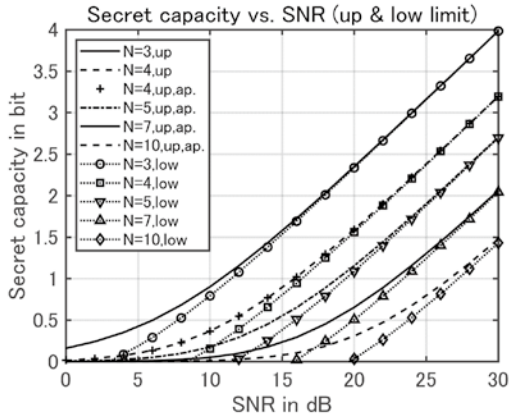

Fig. 6. Upper and lower bound of group secret key capacity as a function of SN ratio.

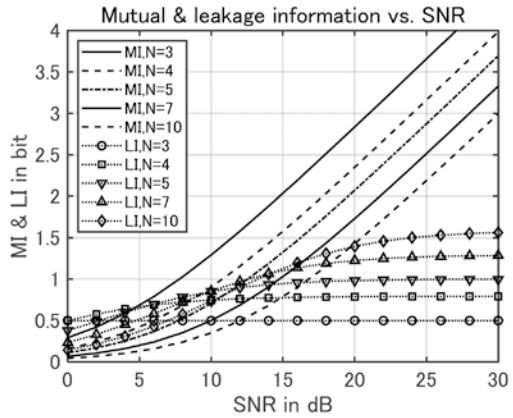

Fig. 7. Mutual information and leakage information as a function of SN ratio.

4.4.2　シミュレーション結果

シミュレーションによる秘密鍵容量の算出法は，標本値の量子化により得られた多値乱数の結合発生確率を求め，次に結合エントロピーを求め，最終的に相互情報量や条件付き相互情報量を求める方法であり，星型接続の場合と同様である [14]．また，多値乱数の量子化レベル数は 64 に設定すればほぼ十分である [14]．

無線端末数 3，4 の場合の秘密鍵容量の上限のシミュレーション結果を Fig. 8 に示す．Fig. 8 からシミュレーション結果が，理論特性とよく一致している．なお，SN が高い場合の不一致は，量子化レベル数の設定のためである．

また，無線端末数 3,4 の場合の相互情報量のシミュレーション結果を Fig. 9 に示す．Fig. 9 からシミュレーション結果が，低 SN 比での若干の不一致を除くと式(61)の理論特性がよく一致することが分かる．

さらに，漏洩情報量のシミュレーション結果を Fig. 10 に示す．シミュレーション結果は，理論特性とよく一致している．

以上の結果，理論式の妥当性が確認できた．

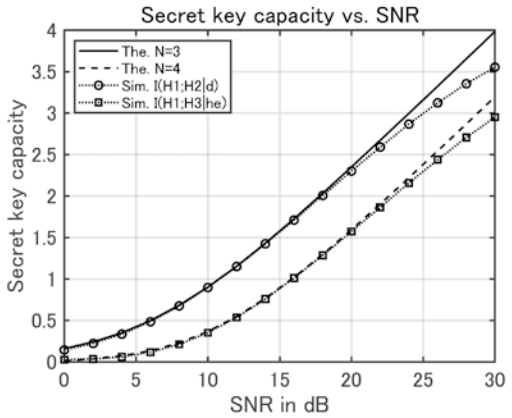

Fig. 8. Upper bound of group secret key capacity as a function of SN ratio.

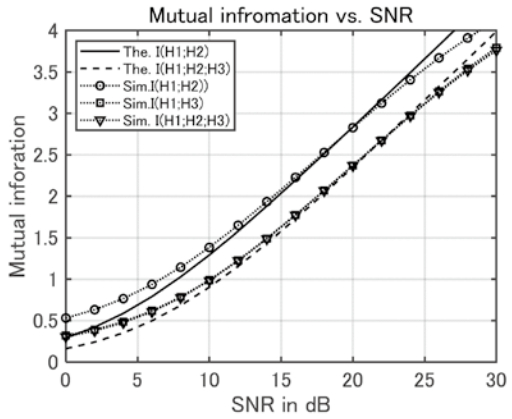

Fig. 9. Mutual information as a function of SN ratio.

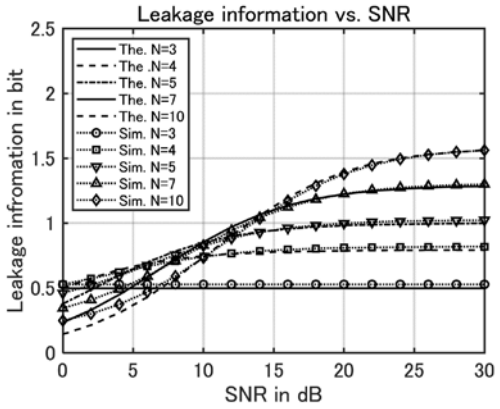

Fig. 10. Leakage information as a function of SN ratio.

5. まとめ

本論文では，鎖型接続の場合を対象として，従来のグループ秘密鍵容量の理論式の問題を解決するため，相互情報量で表される秘密鍵容量の上限と下限をより正確に求めた．また，簡易な理論解析法を用いて，SN 比の関数で表される秘密鍵容量の理論式を導出した．また，数値計算の結果，秘密鍵容量の上限と下限が高 SN 比においてよく一致することが分かった．さらに，シミュレーション結果と理論特性がよく一致したことから，理論式の妥当性が確かめられた．

参考文献

1) A. D. Wyner, “The Wire-Tap Channel”, *Bell Sys. Tech. J.*, **54**[8], 1355-1387 (1975).
2) U. M. Maurer, “Secret Key Agreement by Public Discussion from Common Information”, *IEEE Trans. Inform. Theory*, **39**[3], 733-742 (1993).
3) U. M. Maurer, and S. Wolf, “Unconditional Secure Key Agreement and the Intrinsic Conditional Information”, *IEEE Trans. Inform. Theory*, **45**[2], 499-514 (1999).
4) J. E. Hershy, A. A. Hassan, and R. Yarlagadda, “Unconditional Cryptographic Keying Variable Management”, *IEEE Trans. Communi.*, **43**[1],3-6 (1995).
5) A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, “Cryptographic Key Agreement for Mobile Radio”, *Digital Signal Processing*, **6**[4], 207-212 (1996).
6) K. Zeng, “Physical layer Key Generation in Wireless Networks: Challenges and Opportunities”, *IEEE Comm. Magazine,* **53**[6],33-39 (2015).
7) 岩井誠人，笹岡秀一，“電波伝搬特性を活用した秘密情報の伝送・共有技術”，信学論(B)，**90**[9]，770-783 (2007).
8) T. Aono, K. Higuchi, T. Ohira, T. Komiyama, and H. Sasaoka, “Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channel”, *IEEE Trans. Antenna Propag.*, **53**[11], 3776-3784 (2005).
9) C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, “Generalized Privacy Amplification”, *IEEE Trans. Inform. Theory*, **41**[6], 1915-1923 (1995).
10) 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).
11) 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).
12) 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 (2016).
13) H. L. 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).
14) 笹岡秀一，岩井誠人，“移動伝搬特性に基づくグループ秘密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).
15) 笹岡秀一，岩井誠人，“移動伝搬特性に基づくグループ秘密鍵共有の初期検討（その 2）鎖型接続における従来方式の課題と新方式の提案”, 同志社大学ハリス理化学研究報告，**60**[4]，204-213(2020).