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

Hideichi SASAOKA and Hisato IWAI*

(Received April 16, 2020)

Secret key agreement based on radio propagation characteristics attracts attention as a kind of the wireless physical layer security recently. There are few studies of group secret key agreement in this field, but there is a method to notify of the difference between the series of RSS. 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. 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. Numerical computation also shows that leakage information increases with increase of the number of the terminals. Furthermore, the result of the computer simulation shows validity of theoretical expression.

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１）星型接続の場合 —

笹岡　秀一，　岩井　誠人

1. はじめに

最近の無線通信の普及・発展が目覚しいが，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，その対策として暗号技術が従来から用いられている．移動通信の場合には，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が，鍵管理や鍵配送が必要となる．これらの暗号技術は，計算量的な複雑性を安全性の根拠としている．これら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．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．しかし，これらは理論的研究が多く，実用的なものは少ない．

一方，移動通信などの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

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

づく手法の一種であるが，無線物理層セキュリティにおける秘密鍵共有である [6]．また，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容量の理論的検討も重要である．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，公開通信路を介した情報の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）を用いた手法が提案されている [13]．その手法は，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ことで，グループ秘密鍵を生成するものである [13]．この手法を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を行っている．しかし，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星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の課題

2.1 グループ秘密鍵生成の概要

2.1.1 送受一対の秘密鍵生成と秘密鍵容量

電波伝搬特性の可逆性と場所依存性に基づく秘密鍵生成の構成例を Fig. 1 に示す．Fig. 1 では無線端末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．なお，移動伝搬路の場合にチャネル係数は，複素，絶対値，実部に対して，それぞれ複素ガウス，レイリー，ガウス分布となる．この CC 系列には，可逆性に起因する共通（相関）成分 $\boldsymbol{h}_{A,B}$ と雑音成分 $(\boldsymbol{n}_{A,B}, \boldsymbol{n}_{B,A})$ が含まれている．なお，この部分は，共通（信号）成分と雑音成分の和 $(\boldsymbol{X}_A, \boldsymbol{X}_B)$ の取得（秘密情報抽出）でモデル化される [12]．次に，取得した CC 系列に対して量子化・符号化を行い，多値乱数（秘密鍵候補）$(\boldsymbol{K}_A, \boldsymbol{K}_B)$を生成する．

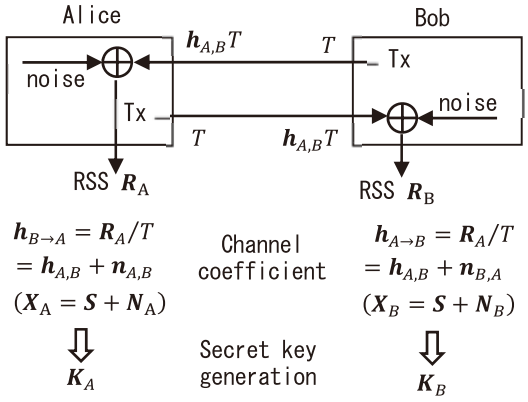

Fig. 1. Secret key generation model based on radio propagation characteristics.

この多値乱数の時系列に対して，正規端末 (Alice, Bob)間で秘密鍵共有(Secret Key Agreement)手順 [9]を実施して，秘密鍵候補と一致を図るとともに盗聴端

末が知りえない正味の秘密鍵を取得する．ここで，正規端末間で取得できた鍵生成の速度（鍵レート）の実現可能な最大値，即ち，理想的な秘密鍵共有が行われた場合の鍵レートの最大値が秘密鍵容量である．一対の正規端末と盗聴端末(Eve)が取得する多値乱数を X,Y,Z とすると，秘密鍵容量 $S(X;Y||Z)$ の上限と下限が，

$$\begin{aligned} S(X;Y||Z) &\le min[I(X;Y),\ I(X;Y|Z)] \\ S(X;Y||Z) &\ge max[I(X;Y)-I(X;Z)\ , \\ &\qquad I(X;Y)-I(Y;Z)] \end{aligned} \tag{1}$$

と表される [2].

2.1.2 グループ秘密情報抽出の原理

Fig. 2 に中継端末(Ryan)と二つの移動端末 (Alice, Bob) からなる秘密情報抽出の基本構成を示す. ここで, Fig. 2 に示す観測値は CC 系列でなくチャネル係数の標本値であり，その標本値は受信雑音を含むため，

$$\begin{aligned} h_{A\to R} &= h_A + n_{R,A} \quad h_{R\to A} = h_A + n_{A,R} \\ h_{B\to R} &= h_B + n_{R,B} \quad h_{R\to B} = h_B + n_{B,R} \end{aligned} \tag{2}$$

と表される．また，アリスとボブの取得する相関情報は，$\delta_{A,B} = h_{A\to R} - h_{B\to R}$ を用いて，

$$\begin{aligned} H_A &= h_{R\to A} = h_{A\to R} + \left(n_{A,R} - n_{R,A}\right) \\ H_B &= h_{R\to B} + \delta_{A,B} = h_{A\to R} + \left(h_{R\to B} - h_{B\to R}\right) \\ &= h_{A\to R} + \left(n_{B,R} - n_{R,B}\right) \end{aligned} \tag{3}$$

となる． 式(3)は，相関（共通）成分 $h_{A\to R}$ と雑音成分 $N_A = \left(n_{A,R} - n_{R,A}\right),\ N_B = \left(n_{B,R} - n_{R,B}\right)$ の和で表される．

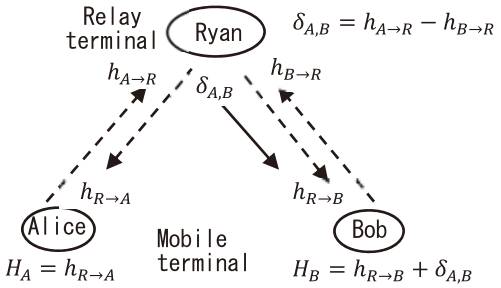

Fig. 2. Principal of secret key generation using relay terminal.

次に，星型接続におけるグループ秘密情報抽出の構成を Fig. 3 に示す [13,14]. Fig. 3 において，各移動端末で取得される相関情報は，$\delta_i = h_{1\to R} - h_{i\to R}$ を用いると，式(3)と同様に，

$$\begin{aligned} H_i &= h_{R\to 1} + \delta_i = h_{1\to R} + N_i \\ N_i &= n_{i,R} - n_{R,i} \end{aligned} \tag{4}$$

と表される．

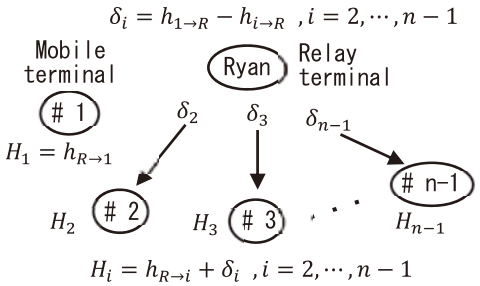

Fig. 3. Configuration of group key generation via star connection.

2.2 従来の秘密鍵容量の理論式とその課題

2.2.1 相互情報量で表すグループ秘密鍵容量

この節では，従来のグループ秘密鍵容量の理論式の導出の概要を説明する．ここで，Fig. 3 に示すチャネル係数と通知情報 $h_{i\to R}, h_{R\to i}, \Delta_n = (\delta_2,\cdots,\delta_{n-1})$ はある時刻の値であるが，長さ M の時系列を太字 $\boldsymbol{h}_{i\to R}, \boldsymbol{h}_{R\to i}, \boldsymbol{\Delta}_n$ で表す．

グループ秘密鍵共有は，中継端末と複数の移動端末間での公開討論 (public discussion) で行われるが，公開討論のあとで全ての移動端末が中継端末と同じ共通情報 $\left[\boldsymbol{h}_{1\to R}, \boldsymbol{h}_{2\to R},\cdots,\boldsymbol{h}_{n-1,R}\right]$ を取得する．このとき，共通情報のエントロピーは，

$$R_{\mathrm{Key}} = \frac{1}{M} H\left(\boldsymbol{h}_{1\to R}, \boldsymbol{h}_{2\to R},\cdots,\boldsymbol{h}_{n-1,R}\right) \tag{5}$$

となる [13].

一方，観測が最悪の移動端末に対して，初期鍵を生成するために中継端末が与えるべき情報量は，$\boldsymbol{\Delta}_n, \boldsymbol{h}_{R\to i}$ を知った条件の下での $\boldsymbol{h}_{1\to R},\cdots,\boldsymbol{h}_{n-1,R}$ のエントロピーであるので，

$$\begin{aligned} R_{\mathrm{bin}} = \max_{1\le i\le n-1} \frac{1}{M} H(&\boldsymbol{h}_{1\to R},\cdots, \\ &\boldsymbol{h}_{n-1,R}|\boldsymbol{\Delta}_n, \boldsymbol{h}_{R\to i}) \end{aligned} \tag{6}$$

となる [13]．この結果，星型接続で共有できる相互情報量は，

$$\begin{aligned} R_{\mathrm{star}} &= R_{\mathrm{key}} - R_{\mathrm{bin}} \\ &= \min_{1\le i\le n-1} \frac{1}{M} I\left(\left[\boldsymbol{h}_{1\to R},\cdots,\boldsymbol{h}_{n-1,R}\right];\left[\boldsymbol{\Delta}_n, h_{R\to i}\right]\right) \end{aligned} \tag{7}$$

と表される[13].

一方, サイド情報から盗聴者に漏洩する情報量は,

$$R_e = \frac{1}{M} I\left(\left[\boldsymbol{h}_{1\to R}, \cdots, \boldsymbol{h}_{n-1,R}\right]; [\boldsymbol{\Delta}_n, \boldsymbol{H}]\right) \tag{8}$$

と表される．ここで，盗聴者が取得する観測値の系列を $\boldsymbol{h}_{\mathrm{i}\to\mathrm{e}}$ とし，$\boldsymbol{H} = [\boldsymbol{h}_{1\to e}, \boldsymbol{h}_{2\to e}, \cdots, \boldsymbol{h}_{n-1\to e}]$ とする．また，秘密鍵容量は,

$$R_{\mathrm{star}}^{\mathrm{sec}} = R_{\mathrm{star}} - R_{\mathrm{e}} \tag{9}$$

で表される[13].

ここで，$R_{\mathrm{star}}^{\mathrm{sec}}$ の算出に当たり，端末１以外の任意の端末（例えば，2）を選択する．また，時系列の取り扱いをやめ，ある時刻の標本値を対象とする．さらに，盗聴者が取得する観測値は，正規端末の観測値と独立（無相関）とする．また，各正規端末の観測値間の観測値も無相関とする．これらの前提の下で数式の簡略化を行うと最終的に,

$$R_{\mathrm{star}}^{\mathrm{sec}} = I(h_{1\to R}; h_{R\to 2}|\Delta_n) \tag{10}$$

が得られる[13].

2.2.2 エントロピーの算出による理論式の導出

ここでは，式(10)の条件付相互情報量をエントロピーで表すことにより，信号対雑音電力(SN)比の関数で表される秘密鍵容量の理論式を導出する．はじめに，式(10)の条件部分 $\Delta_n = [\delta_2, \delta_3, \cdots, \delta_{n-1}]$ の取り扱いを容易とするため，Δ_n が条件でない形式に変更する. このため, 条件付相互情報量 $I(X;Y|Z)$ が

$$\begin{aligned} I(X;Y|Z) = &-H(Z) + H(Z|X) \\ &+H(Y,Z) - H(Y,Z|X) \end{aligned} \tag{11}$$

と表されることを用いると,

$$\begin{aligned} R_{\mathrm{star}}^{\mathrm{sec}} = &H(\Delta_n|h_{1\to R}) - H(\Delta_n) \\ &-H(h_{R\to 2}, \Delta_n|h_{1\to R}) + H(h_{R\to 2}, \Delta_n) \end{aligned} \tag{12}$$

となる[13]．ここで，式(12)の各項は,

$$H(\Delta_n|h_{1\to R}) = H(-h_{2\to R}, \cdots, -h_{n-1\to R}) \tag{13}$$

$$\begin{aligned} H(\Delta_n) = H(&h_{1\to R} - h_{2\to R}, \cdots, \\ &h_{1\to R} - h_{n-1\to R}) \end{aligned} \tag{14}$$

$$\begin{aligned} H(h_{R\to 2}, \Delta_n|h_{1\to R}) = &H(-h_{2\to R}, h_{R\to 2}) \\ &+H(-h_{3\to R}, \cdots, -h_{n-1\to R}) \end{aligned} \tag{15}$$

$$\begin{aligned} H(h_{R\to 2}, \Delta_n) = H(&h_{1\to R} - h_{2\to R}, \cdots, \\ &h_{1\to R} - h_{n-1\to R}, h_{R\to 2}) \end{aligned} \tag{16}$$

と表される[13].

次に，それぞれのエントロピーは，確率変数の共分散行列を求め，行列を対角化（直交化）した場合の対角要素の積（即ち，行列式）を用いることで求められる．確率変数の配列とその共分散行列の行列式との対応は,

$$\begin{aligned} &[-h_{2\to R}, \cdots, -h_{n-1\to R}] \\ &\quad \Rightarrow \sigma_h^{2(n-2)}(1+\gamma^{-1})^{(n-2)} \end{aligned} \tag{17}$$

$$\begin{aligned} &[h_{1\to R} - h_{2\to R}, \cdots, h_{1\to R} - h_{n-1\to R}] \\ &\quad \Rightarrow \ \sigma_h^{2(n-2)}(1+\gamma^{-1})^{(n-2)}(n-1) \end{aligned} \tag{18}$$

$$\begin{aligned} &[-h_{3\to R}, \cdots, -h_{n-1\to R}] \\ &\quad \Rightarrow \sigma_h^{2(n-3)}(1+\gamma^{-1})^{(n-3)} \end{aligned} \tag{19}$$

$$[-h_{2\to R}, h_{R\to 2}] \ \Rightarrow \ \sigma_h^4[(1+\gamma^{-1})^2 - 1] \tag{20}$$

$$\begin{aligned} &[h_{1\to R} - h_{2\to R}, \cdots, h_{1\to R} - h_{n-1\to R}, h_{R\to 2}] \\ &\quad \Rightarrow \ \sigma_h^{2(n-1)}\left[n - 1 - \frac{n-2}{(1+\gamma^{-1})^2}\right] \end{aligned} \tag{21}$$

となる[13]．ここで，γ は SN 比である．

この結果を用いて,

$$\begin{aligned} R_{star}^{sec} &= \log_2\left(1 + \frac{1/(n-1)}{(1+\gamma^{-1})^2}\right) \\ &= \log_2\left(1 + \frac{\gamma^2}{(n-1)(2\gamma+1)}\right) \end{aligned} \tag{22}$$

となる[13].

2.2.3 従来の秘密鍵容量の理論式の問題点

従来のグループ秘密鍵容量の理論式は，中継端末と単一の移動端末のチャネル係数（$h_{1\to R}$, $h_{R\to 2}$）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，複数の移動端末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,

$$R_{\mathrm{star}}^{\mathrm{sec}} = I(h_{R\to 1}; \cdots; h_{R\to n-1}|\Delta_n) \tag{23}$$

であるべきである．しかし，従来の理論式の導出法では，式(23)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，式(1)に示すように上限と下限で表される．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，式(1)の上限に対応している．しかし，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．

3. グループ秘密鍵容量の新しい理論式

3.1 グループ秘密鍵容量の理論解析の準備

3.1.1 条件付エントロピーの簡易な導出法

ここでは, 式(10)から SN 比の関数で表される理論式を求める新しい導出法を示す．式(10)の条件付相

互情報量は，条件付エントロピーを用いて，

$$R_{\mathrm{star}}^{\mathrm{sec}} = H(h_{1\to R}|\Delta_n) + H(h_{R\to 2}|\Delta_n) - H(h_{1\to R}; h_{R\to 2}|\Delta_n) \quad (24)$$

と表される．ここで，式(24)の条件付エントロピーから条件を除く数式変形を考える．このため，Δ_n の一次結合を $D_{\delta,n} = \sum_{i=2}^{n-1} a_i\delta_i$ とし，$h_{1\to R} - D_{\delta,n}$ と δ_i が無相関（独立）となる a_i を設定する．このとき，

$$H(h_{1\to R}|\Delta_n) = H\left(h_{1\to R} - D_{\delta,n}|\Delta_n\right) = H\left(h_{1\to R} - D_{\delta,n}\right) \quad (25)$$

となる．

このような $D_{\delta,n}$ を求めるため，通知情報 Δ_n を用いた盗聴端末における相関情報の推定値 $H_{e,n}$ が，

$$H_{e,n} = \frac{1}{n-2}\sum_{i=2}^{n-1}\delta_i = h_{1\to R} - \frac{1}{n-2}\sum_{i=2}^{n-1} h_{i\to R} \quad (26)$$

であることを用いる [15]．また，この $H_{e,n}$ に係数を掛けて式(25)を満たすものを求める．その結果，

$$h_{e,n} = \frac{n-2}{n-1}H_{e,n} = \frac{n-2}{n-1}h_{1\to R} - \frac{1}{n-1}\sum_{i=2}^{n-1} h_{i\to R} \quad (27)$$

$$h_{s,n} = h_{1\to R} - h_{e,n} = \frac{1}{n-1}\sum_{i=1}^{n-1} h_{i\to R} \quad (28)$$

とすると，$\mathrm{E}\left[h_{s,n}\cdot\delta_i\right] = 0$ が成立つ．この結果，

$$H(h_{1\to R}|\Delta_n) = H\left(h_{1\to R} - h_{e,n}|\Delta_n\right) = H\left(h_{s,n}|\Delta_n\right) = H\left(h_{s,n}\right) \quad (29)$$

となる．

次に，$h_{R\to 2} + \delta_2 = h_{1\to R} + N_2$ を用いると，

$$H(h_{R\to 2}|\Delta_n) = H(h_{1\to R} + N_2|\Delta_n) = H\left(h_{s,n} + N_2|\Delta_n\right) = H\left(h_{s,n} + N_2\right) \quad (30)$$

となる．また，同様にして，

$$H(h_{1\to R}; h_{R\to 2}|\Delta_n) = H\left(h_{s,n}; h_{s,n} + N_2\right) \quad (31)$$

となる．この結果，

$$R_{\mathrm{star}}^{\mathrm{sec}} = I\left(h_{s,n}; h_{s,n} + N_2\right) \quad (32)$$

となる．さらに，

$$R_{\mathrm{star}}^{\mathrm{sec}} = H\left(h_{s,n} + N_2\right) - H\left(h_{s,n} + N_2|h_{s,n}\right) = H\left(h_{s,n} + N_2\right) - H(N_2) \quad (33)$$

となる．

ここで，$h_{s,n} + N_2$ と N_2 の実部，虚部の電力は，

$$P_r = P_i = \frac{1}{n-1}\sigma_s^2 + 2\sigma_N^2$$
$$P_{N,r} = P_{N,i} = 2\sigma_N^2 \quad (34)$$

となり，各エントロピーは，

$$H\left(h_{s,n} + N_2\right) = \log_2(2\pi e P_r) = \log_2\left(2\pi e\left(\frac{1}{n-1}\sigma_s^2 + 2\sigma_N^2\right)\right) \quad (35)$$
$$H(N_2) = \log_2\left(2\pi e P_{N,r}\right) = \log_2\left(2\pi e(2\sigma_N^2)\right)$$

となる．この結果，秘密鍵容量は SN 比 $\gamma = \sigma_s^2/\sigma_N^2$ を用いて，

$$R_{star}^{sec} = \log_2\left(1 + \frac{\gamma}{2(n-1)}\right) \quad (36)$$

と表される．既存の論文の理論式と若干の相違があるが，非常に類似している．

3.1.2. 簡易な導出法の妥当性の確認

条件付エントロピーの簡易な導出法の妥当性を確認するため，式(36)に示す新規の理論式と式(22)に示す従来の理論式との比較を行った．Fig. 4 に SN 比に対する秘密容量特性を示す．Fig. 4 から両者の理論特性は，低 SN 比において微小な不一致があることを除き非常によく一致していることが分かる．

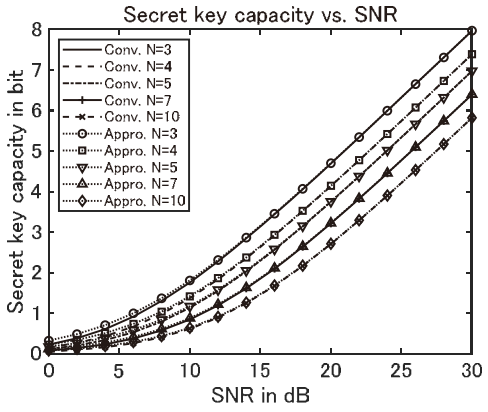

Fig. 4. Secret key capacity as a function of signal to noise power ratio (SN ratio).

3.2 相互情報量で表すグループ秘密鍵容量

3.2.1 一対の秘密鍵容量の多数端末への拡張

一対の秘密鍵容量は式(1)で表されるが，多数の正規端末と盗聴端末が多値変数 $(X_1, \cdots, X_n, Z)$ を取得する場合，グループ秘密鍵容量 $S(X_1; \cdots; X_n||Z)$ の上限と下限は，

$$S(X_1; \cdots; X_n||Z) \le min[I(X_1; \cdots; X_n), I(X_1; \cdots; X_n|Z)] \quad (37)$$

$$S(X_1; \cdots; X_n||Z) \ge max[I(X_1; \cdots; X_n) - I(X_1; Z), \cdots, I(X_1; \cdots; X_n) - I(X_n; Z)] \quad (38)$$

と表されると考えられる．

ここで，$I(X_1; Z), \cdots, I(X_n; Z)$ は盗聴端末への秘密

鍵の漏洩情報量を意味する．また，盗聴端末への漏洩がない場合に，相互情報量 $I(X_1;\cdots;X_n)$ が秘密鍵容量となる．

3.2.2 グループ秘密鍵容量の理論式

Fig. 3 に示されるグループ秘密鍵生成において，各移動端末で取得される相関情報が式(4)で表され，盗聴端末で通知情報が取得される．その結果，式(37)の条件付相互情報量は，$I(H_1;\cdots;H_{n-1}|\Delta_n)$ と表される．ここで，式(4)，式(26)，式(27)を用いると，

$$\begin{aligned} I(H_1;\cdots;H_{n-1}|\Delta_n) &= I\big(h_{1\to R}+N_1-h_{e,n};\\ &\qquad \cdots;h_{1\to R}+N_{n-1}-h_{e,n}|\Delta_n\big)\\ &= I\big(h_{s,n}+N_1;\cdots;h_{s,n}+N_{n-1}|\Delta_n\big)\\ &= I\big(h_{s,n}+N_1;\cdots;h_{s,n}+N_{n-1}\big) \end{aligned} \tag{39}$$

また，式(38)において漏洩情報量が $I(H_i;\Delta_n)$ と表されるが，観測値 H_i に SN 比の差がないことから，$I(H_i;\Delta_n)=I(H_1;\Delta_n)$ となる．ここで，式(4)，式(26)，式(27)を用いると，

$$\begin{aligned} I(H_1;\Delta_n) &= H(H_1)-H(H_1|\Delta_n)\\ &= H(H_1)-H\big(h_{s,n}+N_1\big) \end{aligned} \tag{40}$$

となる．

式(39)と式(40)において，$\Delta_n=(\delta_2,\cdots,\delta_{n-1})$ を $h_{e,n}$ に変更しても，$\mathrm{E}\big[h_{s,n}\cdot h_{e,n}\big]=0$ が成立つので，

$$\begin{aligned} &I\big(H_1;\cdots;H_{n-1}|h_{e,n}\big)\\ &\quad= I\big(h_{s,n}+N_1;\cdots;h_{s,n}+N_{n-1}\big) \end{aligned} \tag{41}$$

$$I\big(H_1;h_{e,n}\big)=H(H_1)-H\big(h_{s,n}+N_1\big) \tag{42}$$

と表される．

3.2.3 グループ秘密鍵生成の等価モデル

ここでは，Fig. 3 に示されるグループ秘密鍵生成に基づいて，盗聴を考慮しない場合の等価モデルを Fig. 5 に示す．式(4)より共通（信号）成分は $S=h_{1\to R}$ となり，雑音成分は $N_i=\big(n_{i,R}-n_{R,i}\big)$ となる．また，これらは平均値 0 の独立なガウス変数であり，信号電力 P_S は，$P_s=\overline{h_{i\to R}^2}$ を用いると，$P_S=P_s$ となり雑音電力 P_{N_i} は $P_n=\overline{n_{i,R}^2}=\overline{n_{R,i}^2}$ を用いると $P_{N_i}=\overline{n_{i,R}^2}+\overline{n_{R,i}^2}=2P_n$ となる．また，この場合に得られる相互情報量は，$I(X_1;\cdots,X_{n-1})$ となる．

次に，通知情報の傍受による盗聴を考慮したグループ鍵生成の等価モデルは，式(26)，式(27)の場合に式(41)となることから，Fig. 5 のモデルの $S=h_{1\to R}$ を $S=h_{1\to R}-h_{e,n}=h_{s,n}$ に変更したものになる．

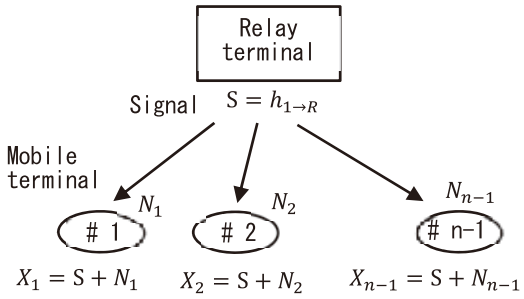

Fig. 5. Equivalent model of group secret key generation without eavesdropper.

3.3. ガウス変数の相互情報量の算出

3.3.1 結合エントロピーで表す相互情報量

はじめに，２変数の相互情報量は，１変数と２変数のエントロピーを用いて，

$$I(X_1,X_2)=H(X_1)+H(X_2)-H(X_1,X_2) \tag{43}$$

と表される．また，３変数の相互情報量は，

$$\begin{aligned} I(X_1;X_2;X_3) &= H(X_1)+H(X_2)+H(X_3)\\ &\quad -H(X_1,X_2)-H(X_2,X_3)\\ &\quad -H(X_3,X_1)+H(X_1,X_2,X_3) \end{aligned} \tag{44}$$

となる[16]．また，４変数の相互情報量は，

$$\begin{aligned} &I(X_1;X_2;X_3;X_4)\\ &\quad=\textstyle\sum_{i=1}^{4}H(X_i)-\sum_{1\le i<j\le 4}H\big(X_i,X_j\big)\\ &\qquad+\textstyle\sum_{1\le i<j<k\le 4}H\big(X_i,X_j,X_k\big)\\ &\qquad-H(X_1,X_2,X_3,X_4) \end{aligned} \tag{45}$$

となる．さらに，５以上の変数の相互情報量も同様に求められる．

3.3.2 ガウス変数の相互情報量の一般式

ここではガウス変数の多変数の相互情報量を導出する．なお，導出に当たっては，２変数の相互情報量の算出手法[11]を参考にしている．

無線端末($i=1,,n-1$)に対して，ガウス変数 X_i のエントロピーは，共通（信号）成分 S と雑音電力 N_i の電力を P_S，P_{Ni} とすると，

$$H(X_i)=\log_2\sqrt{2\pi e(P_S+P_{Ni})} \tag{46}$$

となる[11,12]．また，２変数の結合エントロピーは，

$$\begin{aligned} H\big(X_i,X_j\big) &= \tfrac{1}{2}\log_2\big[(2\pi e)^2F\big(X_i,X_j\big)\big]\\ F\big(X_i,X_j\big) &= P_S\big(P_{Ni}+P_{Nj}\big)+P_{Ni}P_{Nj} \end{aligned} \tag{47}$$

となる[11,12]．また，３変数の結合エントロピーは，

$$H(X_i,X_j,X_k)=\frac{1}{2}\log_2\left[(2\pi e)^3F(X_i,X_j,X_k)\right]$$
$$F(X_i,X_j,X_k)=P_S(P_{Ni}P_{Nj}+P_{Ni}P_{Nk}+P_{Nj}P_{Nk})+P_{Ni}P_{Nj}P_{Nk} \quad (48)$$

と表される．また，４変数の結合エントロピーは，

$$H(X_i,X_j,X_k,X_l)=\frac{1}{2}\log_2\left[(2\pi e)^4F(X_i,X_j,X_k,X_l)\right]$$
$$F(X_i,X_j,X_k,X_l)=P_{Ni}P_{Nj}P_{Nk}P_{Nl}\cdot\left\{P_S\left(\frac{1}{P_{Ni}}+\frac{1}{P_{Nj}}+\frac{1}{P_{Nk}}+\frac{1}{P_{Nl}}\right)+1\right\} \quad (49)$$

となる．ここで，$P_{Ni},P_{Nj},P_{Nk},P_{Nl}\neq 0$ とする．さらに，５以上の変数の結合エントロピーも同様に求められる．

次に，２変数の相互情報量は，式(46)と式(47)を式(43)に代入して，

$$I(X_1,X_2)=\log_2\sqrt{\frac{(P_S+P_{N1})(P_S+P_{N2})}{P_S(P_{N1}+P_{N2})+P_{N1}P_{N2}}} \quad (50)$$

と表される．また，３変数の相互情報量は，式(46)から式(48)を式(44)に代入して，

$$I(X_1;X_2;X_3)=\frac{1}{2}\log_2\left[\frac{(P_S+P_{N1})(P_S+P_{N2})(P_S+P_{N3})}{\{P_S(P_{N1}+P_{N2})+P_{N1}P_{N2}\}}\cdot\frac{\{P_S(P_{N1}P_{N2}+P_{N2}P_{N3}+P_{N3}P_{N1})+P_{N1}P_{N2}P_{N3}\}}{\{P_S(P_{N2}+P_{N3})+P_{N2}P_{N3}\}\{P_S(P_{N3}+P_{N1})+P_{N3}P_{N1}\}}\right] \quad (51)$$

となる．また，４変数の相互情報量は，同様にして，

$$I(X_1;X_2;X_3;X_4)=\frac{1}{2}\log_2\left[\frac{\prod_{i=1}^{4}F(X_i)\cdot\prod_{1\le i<j<k\le 4}F(X_i,X_j,X_k)}{\prod_{1\le i<j\le 4}F(X_i,X_j)\cdot F(X_1,X_2,X_3,X_4)}\right] \quad (52)$$

となる．さらに，５以上の変数の相互情報量も同様に求められる．

3.4 グループ秘密鍵容量の理論式の導出

3.4.1 SN 比の関数で表す相互情報量

上記のガウス変数に対する相互情報量において，信号電力が $P_S=P_s$ で，雑音電力が $P_{Ni}=2P_n$ と同一の場合には，

$$I(X_1,X_2)=\log_2\sqrt{\frac{(P_s+2P_n)^2}{(2P_n+2P_n)P_n}} \quad (53)$$

$$I(X_1;X_2;X_3)=\log_2\sqrt{\frac{(P_s+2P_n)^3(3P_s+2P_n)}{(2P_s+2P_n)^3 2P_n}} \quad (54)$$

$$I(X_1;X_2;X_3;X_4)=\log_2\sqrt{\frac{(P_s+2P_n)^4(3P_s+2P_n)^4}{(2P_s+2P_n)^6(4P_s+2P_n)P_n}} \quad (55)$$

となる．

次に，SN 比を $\gamma=P_s/P_n$ とすると，

$$I(X_1,X_2)=\log_2\sqrt{\frac{(1+\gamma/2)^2}{(1+\gamma)}} \quad (56)$$

$$I(X_1;X_2;X_3)=\log_2\sqrt{\frac{(1+\gamma/2)^3(1+3\gamma/2)}{(1+\gamma)^3}} \quad (57)$$

$$I(X_1;X_2;X_3;X_4)=\log_2\sqrt{\frac{(1+\gamma/2)^4(1+3\gamma/2)^4}{(1+\gamma)^6(1+2\gamma)}} \quad (58)$$

となる．さらに，拡張すると

$$I(X_1;\cdots;X_5)=\log_2\sqrt{\frac{(1+\gamma/2)^5(1+3\gamma/2)^{10}(1+5\gamma/2)}{(1+\gamma)^{10}(1+2\gamma)^5}} \quad (59)$$

$$I(X_1;\cdots;X_6)=\log_2\sqrt{\frac{(1+\gamma/2)^6(1+3\gamma/2)^{20}(1+5\gamma/2)^6}{(1+\gamma)^{15}(1+2\gamma)^{15}(1+3\gamma)}} \quad (60)$$

$$I(X_1;\cdots;X_7)=\log_2\sqrt{\frac{(1+\gamma/2)^7(1+3\gamma/2)^{35}(1+5\gamma/2)^{21}(1+7\gamma/2)}{(1+\gamma)^{21}(1+2\gamma)^{35}(1+3\gamma)^7}} \quad (61)$$

$$I(X_1;\cdots;X_8)=\log_2\sqrt{\frac{(1+\gamma/2)^8(1+3\gamma/2)^{56}(1+5\gamma/2)^{56}(1+7\gamma/2)^8}{(1+\gamma)^{28}(1+2\gamma)^{70}(1+3\gamma)^{28}(1+4\gamma)}} \quad (62)$$

となる．

3.4.2 グループ秘密鍵容量の上限と下限の理論式

グループ秘密鍵容量の上限は，条件付相互情報量 $I(H_1;\cdots;H_{n-1}|\Delta_n)$ で与えられるが，式(41)に示すように相互情報量 $I(h_{s,n}+N_1;\cdots;h_{s,n}+N_{n-1})$ でも表される．ここで，$S=h_{s,n}$ であり，その電力 P_S は，

$$P_S=\overline{h_{s,n}^2}=\overline{\left(\frac{1}{n-1}\sum_{i=1}^{n-1}h_{i\to R}\right)^2}=\frac{1}{(n-1)^2}\sum_{i=1}^{n-1}\overline{h_{i\to R}^2}=\frac{1}{n-1}P_s \quad (63)$$

と表される．また，雑音電力は，$P_{Ni}=2P_n$ と同一である．この結果，移動端末数の増加に伴って，SN 比が $1/(n-1)$ となる．一例を示すと，

$$I(H_1,H_2|\Delta_3)=\log_2\sqrt{\frac{(1+\gamma/4)^2}{(1+\gamma/2)}} \quad (64)$$

$$I(H_1;H_2;H_3|\Delta_4)=\log_2\sqrt{\frac{(1+\gamma/6)^3(1+\gamma/2)}{(1+\gamma/3)^3}} \quad (65)$$

$$I(H_1;\cdots;H_4|\Delta_5)=\log_2\sqrt{\frac{(1+\gamma/8)^4(1+3\gamma/8)^4}{(1+\gamma/4)^6(1+\gamma/2)}} \quad (66)$$

となる．

一方，グループ秘密鍵容量の下限を与える理論式は, 相互情報量の差 $I(H_1;\cdots;H_{n-1})-I(H_i;\Delta_n)$ で表される．ここで，$I(H_1;\cdots;H_{n-1})$ は，3.3.3 の式(56)から式(62)などで表される．また，漏洩情報量は，式(42)を用いると，$I(H_1;\Delta_n)=H(H_1)-H(h_{s,n}+N_1)$ となる．ここで，

$$H(H_1)=H(h_{1\to R}+N_1)=\log_2\sqrt{2\pi e(P_s+2P_n)} \quad (67)$$

$$H(h_{s,n}+N_1)=\log_2\sqrt{2\pi e(P_s/(n-1)+2P_n)} \quad (68)$$

となることを用いると，

$$I(H_1;\Delta_n)=\log_2\sqrt{\frac{P_s+2P_n}{P_s/(n-1)+2P_n}}=\log_2\sqrt{\frac{1+\gamma/2}{1+(\gamma/2)/(n-1)}} \quad (69)$$

となる．これらの結果をまとめると，

$$I(H_1;H_2)-I(H_1,\Delta_3)=\log_2\sqrt{\frac{(1+\gamma/2)(1+\gamma/4)}{1+\gamma}} \quad (70)$$

$$I(H_1;H_2;H_3)-I(H_1,\Delta_4)=\log_2\sqrt{\frac{(1+\gamma/2)^2(1+3\gamma/2)(1+\gamma/6)}{(1+\gamma)^3}} \quad (71)$$

となる．同様に n=5～10 の場合，式(59)から式(62)と式(69)を用いて求められる．

4. 数値計算とシミュレーションによる検証

4.1 グループ秘密容量特性の計算結果

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, 端末数の増加に減少するが，SN 比が高くなるほぼ一致している．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理論特性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 MIg で示される相互情報量は，端末数の増加に伴う減少が比較的少ないことが分かる．また，MIe で示される漏洩情報量は，端末数の増加に伴う増加が比較的大きいことが分かる．

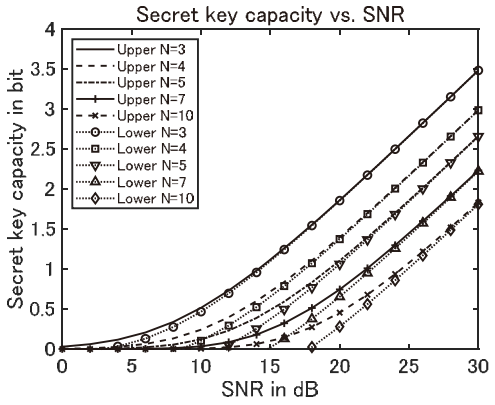

Fig. 6. Upper and lower bound of group secret key capacity as a function of SN ratio.

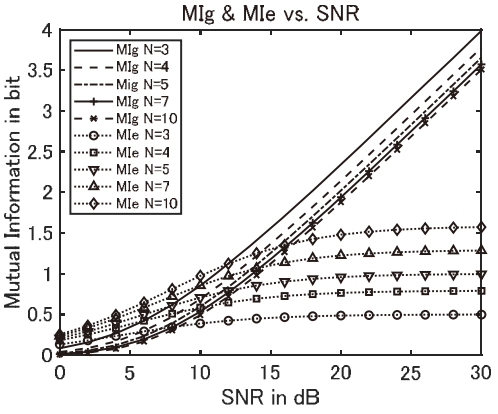

Fig. 7. Group mutual information and leakage information as a function of SN ratio.

4.2 シミュレーションによる検証

4.2.1 秘密鍵容量の算出法

秘密鍵容量は，多変数の相互情報量や条件付相互情報量で表される．また，それらの相互情報量は，エントロピーと結合エントロピーで表される．さらに, 多値乱数のエントロピーと結合エントロピーは, 多値乱数の発生確率から算出される．それゆえ，シミュレーションによる秘密鍵容量の算出は，シミュレーションで求めた多値乱数の発生確率に基づいて行われる．しかし，結合エントロピーの次数が大きくなると（例えば，４以上となると）算出精度が低下するので，以下では，次数が小さい場合に対して検証を行う．

秘密鍵容量の上限を与える条件付相互情報量をエ

エントロピーと結合エントロピーで表すと，

$$I(H_1;H_2|\delta_2) = H(H_1,\delta_2) + H(H_2,\delta_2) - H(\delta_2) - H(H_1,H_2,\delta_2) \quad (72)$$

となる [11]．また，秘密鍵容量の下限に関係する正規端末間の相互情報量 $I(H_1;\cdots;H_{n-1})$ は，式(43)から式(45)において $X_i \to H_i$ の変更を行えばよい．また，漏洩情報量 $I(H_1;\Delta_3)$，$I(H_1;\Delta_4)$ は，

$$I(H_1;\delta_2) = H(H_1) + H(\delta_2) - H(H_1,\delta_2) \quad (73)$$

$$I(H_1;\delta_2,\delta_3) = H(H_1) + H(\delta_2,\delta_3) - H(H_1,\delta_2,\delta_3) \quad (74)$$

となる．なお，式(74)を簡略化すると，

$$I(H_1;h_{e,n}) = H(H_1) + H(h_{e,n}) - H(H_1,h_{e,n}) \quad (75)$$

と表される．

一方，M 値の乱数のエントロピーと結合エントロピーは，発生確率と結合発生確率を用いて，

$$\begin{aligned} H(X_l) &= -\sum_{i=1}^{M} p_{Xl}(i)\log_2 p_{Xl}(i) \\ H(X_l,X_m) &= -\sum_{i=1}^{M}\sum_{j=1}^{M} p_{Xl,Xm}(i,j) \cdot \log_2 p_{Xl,Xm}(i,j) \\ H(X_l,X_m,X_n) &= -\sum_{i=1}^{M}\sum_{j=1}^{M}\sum_{k}^{M} p_{Xl,Xm,Xn}(i,j,k) \cdot \log_2 p_{Xl,Xm,Xn}(i,j,k) \end{aligned} \quad (76)$$

と表される．

4.2.2 シミュレーション結果と評価

はじめに，相関のある二つのガウス変数（アナログ）を多値量子化（量子化レベル数を可変）した乱数の相互情報量をシミュレーションにより評価した．その結果をアナログの標本値（量子化レベル数無限大に相当）の場合の理論特性とともに Fig. 8 に示す．Fig. 8 から量子化レベル数 ML を 64 に設定すると理論特性に近い結果が得られることが分かる．そこで，以下では ML=64 に設定する．

シミュレーションで取得した端末数 3 の場合の秘密鍵容量の上限の特性を Fig. 9 に示す．Fig. 9 から式(64)の理論特性と式(72)に基づくシミュレーション結果がよく一致することが分かる．なお，SN にが高い場合の不一致は，Fig. 8 に示すように量子化レベル数の設定のためである．

シミュレーションで取得した端末数 3,4 の場合の相互情報量の特性を Fig. 10 に示す．Fig. 10 からシミュレーション結果と理論特性がよく一致することが分かる．

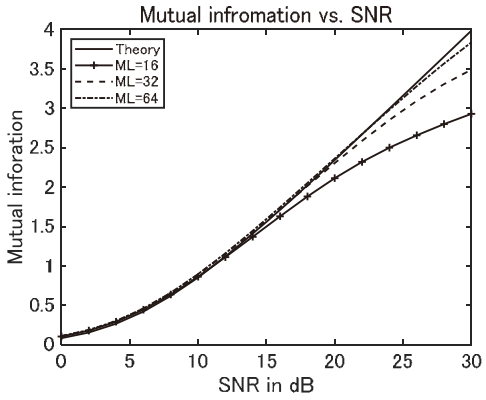

Fig. 8. Mutual information of multi-level random variable as a function of SN ratio.

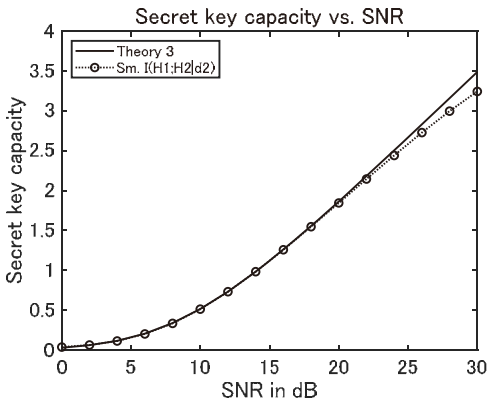

Fig. 9. Upper bound of group secret key capacity as a function of SN ratio.

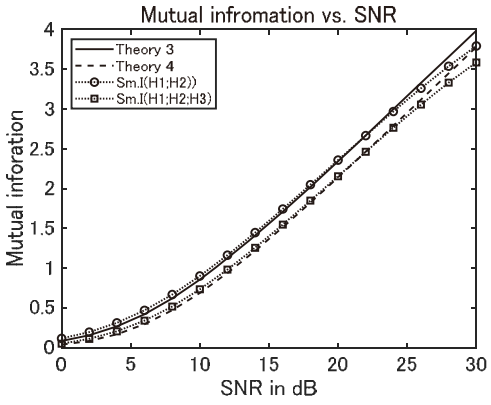

Fig. 10. Mutual information as a function of SN ratio.

シミュレーションで取得した漏洩情報量の特性を

Fig. 11 に示す．Fig. 11 には，式(75)，式(76)および式(78)に基づくシミュレーション結果を示している．これらの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．

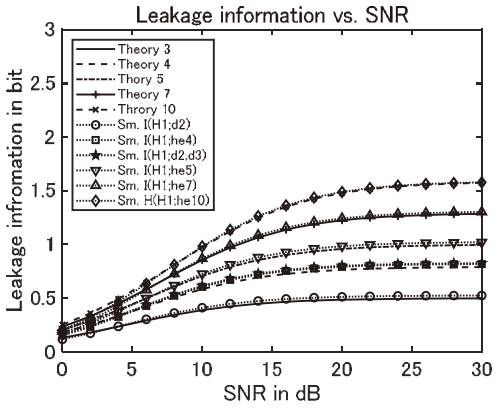

Fig. 11. Leakage information as a function of SN ratio.

5. まとめ

本論文では，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，漏洩情報量が端末数の増加に伴い増加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．

今回，対象外とした鎖型接続の場合のグループ秘密鍵容量の検討は今後の課題である．

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**, 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－”，同志社大学理工学研究報告，**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初期検討 —（その１）星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]，194-203(2019).
15) 黒柳啓太，笹岡秀一，岩井誠人，“RSSI 差分情報の通知によるグループ秘密鍵共有における盗聴により漏洩する情報量の評価”，信学論(B)，**102**[11]，782-790(2019).
16) ノーマン・アブラムソン（宮川洋　訳），情報理論入門，（好学社，東京，1983），pp.152-154.