Basic Study of Group Secret Key Agreement Based on Mobile Propagation Characteristics －Part Ⅱ: Problems of the Conventional Method and Suggestion of New Method in Chain Connection－

Hideichi SASAOKA and Hisato IWAI*

(Received October 10, 2019)

Wireless physical layer security attracts attention as a kind of the information security that utilized radio propagation characteristics. A lot of studies of secret key agreement are performed as the main field, but there are relatively few studies of group secret key agreement. This paper shows the summary of the conventional method based on mobile propagation characteristics for chain connection systems and clarified a problem of the technique to notify of difference of the series of RSSI. Then, this paper suggested a method to acquire multiple group secret key using a notice of the EX-OR of the series of two binary RSSI to solve a problem. This paper also suggested a method to acquire multiple group secret key by the key distribution using the notice of the EX-OR with the series of binary RSSI and the binary random number. These suggestion methods show that the update of the secret key becomes easy by utilizing multiple group secret key.

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

キーワード：物理層セキュリティ，秘密鍵共有，グループ秘密鍵，移動伝搬特性

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 —

笹岡　秀一，　岩井　誠人

１．はじめに

第五世代移動通信システムの導入が間近に迫るなど最近の無線通信の普及・発展が目覚しいが，無線通信は開かれた空間を介して電波を送受信するため，盗聴や不正アクセスの危険性がある．この対策として共通鍵暗号や公開鍵暗号など情報セキュリティ技術が従来から用いられている．ここで，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．さらに，複数移動端末に対して同報秘密通信やグループ認証を実施する場合，グループ秘密鍵の管理や配送が重要となる．

これらの情報セキュリティ技術は，計算量的な複雑性を安全性の根拠としているが，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

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

（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，複数端末を対象とした秘密鍵容量の検討 [4]やグループ秘密鍵の生成アルゴリズムの検討 [5]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 [6,7]．これは相関情報に基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 [8]．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 [9]．ここで、マルチパス伝搬が生じる移動通信路においては、様々な電波伝搬特性が秘密鍵生成に用いられている. 例として，マルチトーン信号の位相差 [6,7]，無線伝送路のインパルス応答 [10]，振幅周波数特性の時変化 [11]，受信信号強度の時変化 [12,13]などを用いた秘密鍵生成がある．また，伝搬特性の時変化が少ない室内通信環境を対象として，アレーアンテナの指向性パターン変動を活用した人工フェージングの受信信号強度を用いた秘密鍵生成がある [14,15]．これらの手法は，秘密鍵の取得と更新が無線物理層の処理のみで比較的容易となることが特長である．

これらは，送受一対を対象としており，双方向の電波伝搬特性の測定に基づいて秘密鍵（秘密鍵候補）を生成する．また，秘密鍵候補が不一致の場合，公開通信路を介した情報交換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 [16]．一方，グループ秘密鍵の取得は，一対の秘密鍵共有を複数の無線端末間で実施し，取得した複数の秘密鍵を用いて同一秘密鍵を既存の暗号技術で各無線端末へ配送すればよい．しかし，秘密鍵配送と異なる手法として，全無線端末において相関の高い秘密情報を生成し，鍵生成と鍵一致処理等によりグループ秘密鍵を生成する手法がある [17-19]．

その手法の一つは，受信電界強度表示 (RSSI: Received Signal Strength Indicator) の時系列(RSSI 系列)を測定し，基準端末と対象端末との RSSI 系列の差分値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方式である [17]．この論文では，星型接続と鎖型接続に対してグループ秘密鍵の生成手順と秘密鍵容量を示している． ここで，星型接続におけるグループ秘密鍵の生成に対しては，RSSI 系列の差分値の和を用いた攻撃法が指摘され，その対策としてビットの排他的論理を通知する手法が提案されている [18]．さらに，星型接続における新しいグループ秘密鍵生成が提案されている [19]．

しかし，鎖型接続を対象としたグループ秘密鍵生成の検討はほとんどない．そこで，本論文では，鎖型接続における RSSI 系列の差分値を通知する従来方式の概要を示すとともに，従来方式の課題を明らかにした．また，２値 RSSI 系列の排他的論理和を通知によるグループ秘密鍵生成の鎖型接続への適用の概要を示すとともに，双方向通知を用いた新たな手法を提案した．さらに，個別秘密鍵を用いた秘密鍵配送の鎖型接続への適用の概要を示すとともに，双方向通知を用いた新たな手法を提案した．

２．RSSI 系列の差分値を通知する従来方式

2.1 鎖型接続における従来方式の概要

2.1.1 システム構成とグループ秘密鍵生成

ここでは，無線端末の鎖型接続において，RSSI 系列の差分値の通知を用いた秘密鍵共有 [17]の概要を説明する．はじめに，無線端末の数が３で，中継回数が１の場合を対象に，情報通知による秘密鍵生成の基本手順を Fig. 1 に示す [17]．

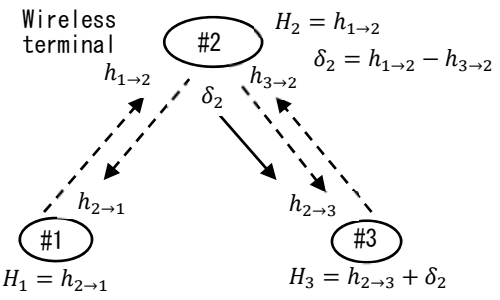


Fig. 1. Principal of secret key generation using one relay terminal.

基本手順では，無線端末間で双方向の RSSI 系列を測定する．次に，無線端末(#2)より無線端末(#3)に RSSI 系列の差分値を通知し，移動端末で秘密情報を取得する [17].

Fig. 1 において，測定された双方向の RSSI 系列 $h_{1\to2}, h_{2\to1}, h_{3\to2}, h_{2\to3}$ には，可逆性に起因する共通の RSSI 成分と雑音成分が含まれており，

$$\begin{aligned} h_{1\to2} &= h_{1,2} + n_{2,1} \quad h_{2\to1} = h_{1,2} + n_{1,2} \\ h_{3\to2} &= h_{2,3} + n_{2,3} \quad h_{2\to3} = h_{2,3} + n_{3,2} \end{aligned} \tag{1}$$

と表される．また，RSSI 系列の差分値 δ_2 と移動端末で生成される秘密情報 H_1, H_2, H_3 は，

$$\delta_2 = h_{1,2} - h_{2,3} + n_{2,1} - n_{2,3} \tag{2}$$

$$\begin{aligned} H_1 &= h_{1,2} + n_{1,2} \\ H_2 &= h_{1,2} + n_{2,1} \\ H_3 &= h_{1,2} + n_{3,2} + (n_{2,1} - n_{2,3}) \end{aligned} \tag{3}$$

と表される．ここで，雑音成分が小さければ，十分に相関の高い秘密情報となる．また，この秘密情報から秘密鍵を生成すると，鍵不一致が少ない秘密鍵が生成できる．しかし，秘密鍵が一致しない場合には，公開通信路を介した情報交換による鍵不一致解消と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 [16]．また，秘密鍵共有の処理が理想的に行われた場合の秘密鍵容量の理論式が示されている [2].

次に，この基本手順を無線端末の数が４で，中継回数が２の場合のグループ秘密鍵生成の手順 [17]を Fig. 2 に示す. 図では RSSI 系列の測定の部分の表示を省略し, RSSI 系列の差分値の通知と秘密情報の取得を主に表示している．

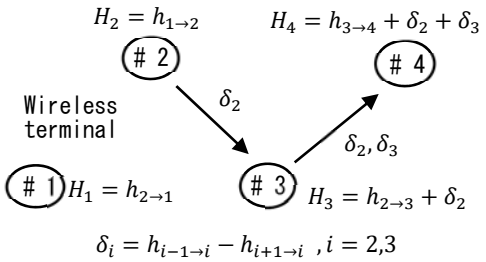


Fig. 2. Principal of secret key generation using two-stage relay.

図に示すように秘密情報 H_4 を得るには, RSSI 系列の差分値 δ_2, δ_3 が必要となる. また, 秘密情報 H_4 は,

$$H_4 = h_{12} + n_{4,3} + (n_{2,1} - n_{2,3}) + (n_{3,2} - n_{3,4}) \tag{4}$$

と表され，中継回数の増加に伴い雑音の影響が増加することが分かる．

さらに，無線端末の数が n で，中継回数が $\mathrm{n}-2$ の多中継端末の場合のグループ秘密鍵生成の手順を Fig. 3 に示す．中継回数の増加に伴って必要な通知情報が増加する．図において，H_i は,

$$H_i = h_{i-1\to i} + \sum_{j=2}^{i-1} \delta_j \ , i \geq 3 \tag{5}$$

と表される．

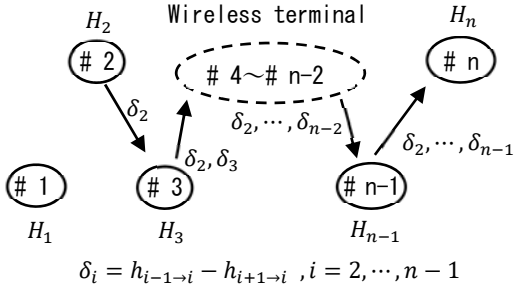


Fig. 3. System configuration of conventional group key generation using multistage relay.

2.1.2 秘密鍵容量の理論検討と特性評価

上記の鎖型接続において各端末で得られた秘密情報に対してグループ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が，この処理が理想的に実施された場合のグループ秘密鍵容量が理論検討されている [17]．その結果によると，グループ秘密鍵容量 S_{chain} は,

$$S_{chain} = \log \left[\frac{\left\{ (1+\gamma_m^{-1}) d_n^{(1)} - d_{n-1}^{(1)} \right\}^2}{d_n^{(1)} \left\{ (1+\gamma_m^{-1}) d_n^{(2)} - d_{n-1}^{(2)} \right\}} \right] \tag{6}$$

と表される [17]．ここで，γ_m は伝送路の信号対雑音電力比である．また， $d_n^{(1)}, d_n^{(2)}$ は漸化式を用い,

$$\begin{aligned} d_1^{(1)} &= 2(1+\gamma_m^{-1}) \\ d_2^{(1)} &= 4(1+\gamma_m^{-1})^2 - 1 \\ d_n^{(1)} &= 2(1+\gamma_m^{-1}) d_{n-1}^{(1)} - d_{n-2}^{(1)} \end{aligned} \tag{7}$$

および,

$$d_n^{(2)} = (1+\gamma_m^{-1}) d_n^{(1)} - d_{n-1}^{(1)} \tag{8}$$

と表される．このように，グループ秘密鍵容量は，信号対雑音電力比と無線端末数に依存する．

この理論式に基づいて，信号対雑音電力比に対するグループ秘密鍵容量特性および無線端末数に対するグループ秘密鍵容量特性が評価されている [17]．その結果によると，鎖型接続における特性は，星型接続の特性に比較して大幅に劣化すること，その劣化量が無線端末数の増加に対してより顕著となることが示されている [17]．一方，計算機シミュレーションによる特性評価はなく，一部，鍵不一致率特性等の実験結果が示されているのみである．

2.2 従来方式の課題

2.2.1 通知情報の増加と雑音による特性劣化

鎖型接続における従来方式の課題の一つは，通知情報が無線端末数の増加と共に増えることである．この課題は，Fig. 4 に示すように通知情報に若干の変更を行う簡易化した手法で解決できる．図に示すように通知情報を δ_i から Δ_i に変更する．ここで，

$$\begin{aligned}&\delta_i = h_{i-1\to i} - h_{i+1\to i}\ ,i = 2,\cdots,n-1\\&\Delta_2 = \delta_2,\ \Delta_i = \Delta_{i-1} + \delta_i, i = 3,\cdots,n-1\end{aligned} \tag{9}$$

と表される．この結果，単一の通知情報により全無線端末での秘密情報の取得が可能となる．

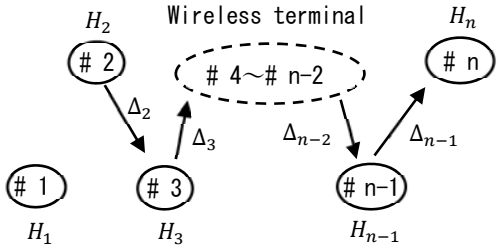


Fig. 4. Modified system configuration of conventional group key generation using multistage relay.

次に，この手法における雑音成分の影響を検討する．式(2)を拡張すると，

$$\delta_i = h_{i-1,i} - h_{i,i+1} + n_{i,i-1} - n_{i,i+1} \tag{10}$$

となる．また，式(5)は，$i \geq 3$ の場合に，

$$H_i = h_{1,2} + n_{i.i-1} + \sum_{j=2}^{i-1}\left(n_{j,j-1} - n_{j,j+1}\right) \tag{11}$$

となる．式(11)において H_i に含まれる雑音項の数が $\{1 + 2(i-2)\}$ となっており，中継回数の増加とともに雑音の影響が増加することが分かる．一方，星型接続において雑音成分の影響は，中継回数 1 回に相当し，移動端末数の増加の影響を受けない．このことは，信号対雑音電力比に対するグループ秘密鍵容量の特性が星型接続の場合と比較して大幅に劣化する原因と考えられる．

このように中継回数の増加に伴い，雑音成分の累積の影響でグループ秘密鍵容量特性が著しく特劣化するので，その対策が重要となる．ここで，雑音成分が相加する現象は，アナログ中継の場合によく発生する．一方，ディジタル中継においては，雑音が中継毎に除かれるため雑音が相加されることはない．このことに着目するとこの対策の一つは，２値化などのディジタル化となる．

2.2.2 通知情報を用いた盗聴の危険性

星型接続において RSSI 系列の差分値を通知するグループ秘密鍵生成において，通知情報に基づく盗聴により秘密鍵容量が大幅に低下することが指摘されている [18]．しかし，鎖型接続においては，通知情報 X_i を用いた盗聴の可能性が未検討であるので，以下で盗聴の危険性を検討する．ここで，$\delta_{2,i} = (h_{1\to 2} - h_{i+1\to i})$ とすると，Δ_2, Δ_3 が，

$$\begin{aligned}\Delta_2 &= \delta_2 = h_{1\to 2} - h_{3\to 2} = \delta_{2,2}\\\Delta_3 &= \delta_2 + \delta_3 = h_{1\to 2} - h_{4\to 3} + h_{2\to 3} - h_{3\to 2}\\&= \delta_{2,3} + \left(n_{3,2} - n_{2,3}\right)\end{aligned} \tag{12}$$

と表される．式(12)を一般化すると，

$$\Delta_i = \sum_{j=2}^{i}\delta_j = \delta_{2,i} + \sum_{j=2}^{i-1}\left(n_{j+1,j} - n_{j,j+1}\right) \tag{13}$$

となる．さらに，$\delta_{2,i} \gg \sum_{j=2}^{i-1}\left(n_{j+1,j} - n_{j,j+1}\right)$ の仮定が一般に妥当であるので，$\Delta_i \cong \delta_{2,i}$ となる．

通知情報の傍受による攻撃方は，はじめに通知情報の和，

$$\begin{aligned}D_\Delta &= \frac{1}{n-2}\sum_{i=2}^{n-1}\Delta_i \cong \frac{1}{n-2}\sum_{i=2}^{n-1}\delta_{2,i}\\&\cong h_{1\to 2} - \frac{1}{n-2}\sum_{i=2}^{n-1}h_{i+1\to i}\end{aligned} \tag{14}$$

を求める．次に，D_Δ とその平均値 $\overline{D_\Delta}$ との偏差を盗聴者が推定する秘密情報 H_E とすると，

$$H_E \cong h_{1\to2} - \overline{h_{1\to2}} + \frac{1}{n-2}\sum_{i=2}^{n-1}\left(h_{i+1\to i} - \overline{h_{\iota+1\to\iota}}\right) \tag{15}$$

となる．ここで，中継端末数が増加するとともに，

$$H_E \cong h_{1\to2} - \overline{h_{1\to2}} \tag{16}$$

となる．これは，星型接続の場合に示された攻撃法と類似している [18]．相違点は，式(13)に示される雑音成分の影響が，中継端末数の増加とともに増加することである．このため，星型接続の場合と比較して盗聴者への秘密鍵情報の漏洩が減少する．

なお，通知情報の傍受による秘密情報の漏洩の対策として，ディジタル化したビットの排他的論理和の使用が有効であることが指摘されている [18]．

３．２値 RSSI 系列の排他的論理和の通知方式

3.1 一方向通知を用いたグループ秘密鍵の生成

3.1.1 シテム構成とグループ秘密鍵の生成の原理

従来方式の課題の解決のためには，ディジタル化 RSSI 系列の使用が有効であり，提案方式は符号化した多ビットの RSSI 系列とそれらの排他的論理和の通知を想定している．しかし，以下では提案方式の説明と数式表現を簡易にするために，２値化した単一ビットの RSSI 系列を用いた手法を示す．

はじめに，無線端末数が４で，中継端末数が２の場合のグループ秘密鍵生成の基本手順を Fig. 5 に示す．基本手順では，無線端末間で双方向の RSSI 系列を測定し，一対の２値 RSSI 系列 $k_{i\to i+1}, k_{i+1\to i}$ を取得する．また，各中継端末で２値 RSSI 系列の排他的論理和 ε_i を求め，さらに通知情報 X_i を算出する．

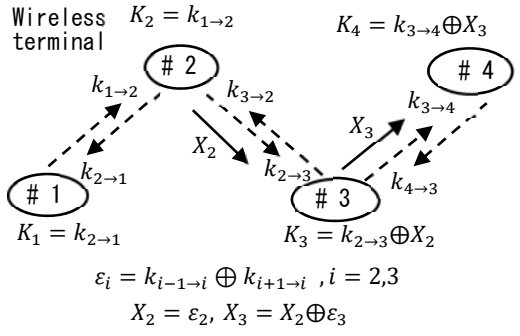


Fig. 5. Principal of new group key generation via chain connection.

ここで，

$$\varepsilon_i = k_{i-1\to i} \oplus k_{i+1\to i} \ , i = 2,3 \tag{17}$$

$$X_2 = \varepsilon_2,\ X_3 = X_2 \oplus \varepsilon_3 \tag{18}$$

と表される．また，各端末で取得する秘密鍵は，

$$\begin{aligned} &K_1 = k_{2\to1},\ K_2 = k_{1\to2} \\ &K_i = k_{i-1\to i} \oplus X_{i-1},\ i = 2,3 \end{aligned} \tag{19}$$

となる．この秘密鍵は，鍵一致処理（鍵共有）を行う前の鍵であり，以下では秘密鍵候補と呼ぶ．

図において，２値 RSSI 系列には，雑音がない理想的な場合に二つの無線端末の対向で取得される同一の秘密鍵（以下，個別秘密鍵と呼ぶ）と雑音に起因する不一致成分が含まれており，

$$\begin{aligned} &k_{1\to2} = k_{1,2} \oplus d_{2,1} \ , \ k_{2\to1} = k_{1,2} \oplus d_{1,2} \\ &k_{2\to3} = k_{2,3} \oplus d_{3,2} \ , \ k_{3\to2} = k_{2,3} \oplus d_{2,3} \\ &k_{3\to4} = k_{3,4} \oplus d_{4,3} \ , \ k_{4\to3} = k_{3,4} \oplus d_{3,4} \end{aligned} \tag{20}$$

と表される．また，

$$\varepsilon_i = k_{i-1,i} \oplus k_{i,i+1} \oplus d_{i,i-1} \oplus d_{i,i+1} \ , i = 2,3 \tag{21}$$

となり，

$$X_3 = k_{1,2} \oplus k_{3,4} \oplus d_{2,1} \oplus d_{2,3} \oplus d_{3,2} \oplus d_{3,4} \tag{22}$$

となる．さらに，各無線端末で生成される秘密鍵候補は，

$$\begin{aligned} &K_1 = k_{1,2} \oplus d_{1,2} \ , \ K_2 = k_{1,2} \oplus d_{2,1} \\ &K_3 = k_{1,2} \oplus d_{3,2} \oplus d_{2,1} \oplus d_{2,3} \\ &K_4 = k_{1,2} \oplus d_{4,3} \oplus d_{2,1} \oplus d_{2,3} \oplus d_{3,2} \oplus d_{3,4} \end{aligned} \tag{23}$$

となる．式(23)から中継段数の増加に伴い秘密鍵候補に対して雑音に起因する不一致成分の影響が増加することが分かる．

ここで，一対の２値 RSSI が個別秘密鍵と一致する場合，即ち，$d_{i,i+1} = d_{i+1,i} = 0, i = 1, \cdots, 3$ となる場合には，

$$K_i = k_{1,2} \ , i = 1, \cdots, 4 \tag{24}$$

となり，１番目と２番目の無線端末間の個別秘密鍵がグループ秘密鍵となる．なお，不一致成分がある場合にも．グループ秘密鍵に対して鍵不一致解消を行うことで，グループ秘密鍵が取得される．

3.1.2 多数無線端末への拡張

鎖型接続におけるグループ秘密鍵生成を多数無線端末に拡張したシステムを Fig. 6 に示す．図において，２値 RSSI 系列の表示を省略し，通知情報を主に表示している．ここで，２値 RSSI 系列を個別秘密鍵

と不一致成分の排他的論理和で表すと，

$$k_{i\to i+1} = k_{i,i+1}\oplus d_{i+1,i} \\ k_{i+1\to i} = k_{i,i+1}\oplus d_{i,i+1} \quad ,i = 1,\cdots,n-1 \qquad (25)$$

と表される．また，通知情報 X_i，$i \geq 2$ は，

$$X_i = k_{1,2}\oplus k_{i,i+1}\oplus \sum_{j=2}^{i}\left(d_{j,j-1}\oplus d_{j,j+1}\right) \qquad (26)$$

と表される．さらに，秘密鍵候補 K_i，$i \geq 3$ は，

$$K_i = k_{1,2}\oplus d_{i,i-1}\oplus \sum_{j=2}^{i-1}\left(d_{j,j-1}\oplus d_{j,j+1}\right) \qquad (27)$$

と表される．式(27) において K_i に含まれる不一致成分の項の数が $\{1+2(i-2)\}$ となっており，中継回数の増加とともに不一致成分の影響が増加することが分かる．

ここで，一対の２値 RSSI が個別秘密鍵と一致する場合，即ち，$d_{i,i+1} = d_{i+1,i} = 0, i = 1,\cdots,n-1$ となる場合には，$K_i = k_{1,2}$ ，$i = 1,\cdots,n-1$ がグループ秘密鍵となる．なお，既に述べたように，不一致成分がある場合には，グループ秘密鍵に対して鍵不一致解消を行うことで，グループ秘密鍵が取得されるが，以下では同一記述の繰り返しをさけるため，上記の「なお，・・・」の補足説明を省略する．

一方，不一致成分がある場合には，式(27)に示すように中継回数の増加とともに，その影響が増加するため，信号対雑音電力比に対するグループ秘密鍵容量特性が劣化することが予想される．

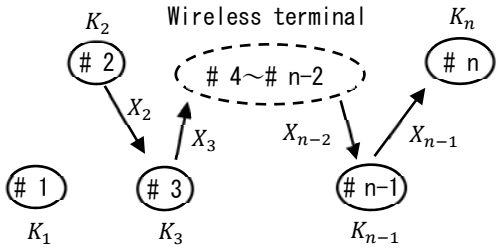


Fig. 6. System configuration of new group key generation via chain connection.

3.2 双方向通知を用いたグループ秘密鍵の生成

3.2.1 一方向通知を両側に適用した方式

上記の 3.1 節において，一方向通知を用いたグループ秘密鍵生成の手法を示した．この手法では，２番目の無線端末からｎ番目の終端無線端末に向けて通知情報を順次中継している．一方，$(n-1)$番目の無線端末から１番目の無線端末に逆方向の通知情報を順次中継することで，別の秘密鍵の取得が可能となる．システムの構成を Fig. 7 に示す．システムの構成は，Fig. 6 とほぼ同様であり，通知情報と生成される秘密鍵の式も同様となる．なお，通知情報 X_i は，無線端末番号の増加方向への通知に対応し，Y_i は逆方向の通知に対応する．

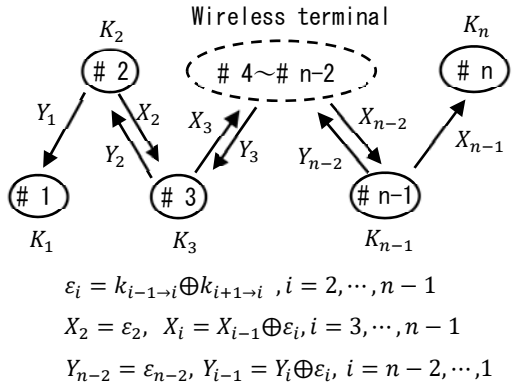


Fig. 7. System configuration of new group key generation via chain connection using two-way notice.

ここで，一対の２値 RSSI が個別秘密鍵と一致する場合，即ち，$d_{i,i+1} = d_{i+1,i} = 0, i = 1,\cdots,n-1$ となる場合には，

$$K_i = \left(k_{1,2}, k_{n,-1,n}\right) \text{ , } i = 1,\cdots,n \qquad (28)$$

となり，１番目と２番目の無線端末間および $n-1$ 番目と n 番目の無線端末間の個別秘密鍵がグループ秘密鍵となる．

3.2.2 中間の無線端末からの両方向通知

はじめに，鎖型接続において中間の無線端末からの両方向通知によりグループ秘密鍵を生成する手法の原理を Fig. 8 に示す．図は無線端末５，中継端末３で構成され，２番目と３番目の２値 RSSI 系列を基準として，その系列に対応する個別秘密鍵をグループ秘密鍵とする構成である．図において２値 RSSI 系列の排他的論理和と通知情報は，

$$\varepsilon_i = k_{i-1\to i}\oplus k_{i+1\to i} \quad ,i = 2,\cdots,4 \\ X_3 = \varepsilon_3,\ X_4 = X_3\oplus\varepsilon_4,\ Y_2 = \varepsilon_2 \qquad (29)$$

となる．また，各無線端末が取得する秘密鍵候補は，

$$K_1 = k_{3\to2} \oplus k_{1\to2} \oplus k_{2\to1},\ K_2 = k_{3\to2}$$
$$K_3 = k_{2\to3},\ K_4 = k_{2\to3} \oplus k_{4\to3} \oplus k_{3\to4}$$
$$K_5 = k_{2\to3} \oplus k_{4\to3} \oplus k_{3\to4} \oplus k_{5\to4} \oplus k_{4\to5} \quad (30)$$

と表される．ここで，式(25)に示すように，２値 RSSI 系列を個別秘密鍵と不一致成分の排他的論理和で表すと，秘密鍵候補は，

$$K_1 = k_{2,3} \oplus d_{2,3} \oplus d_{1,2} \oplus d_{2,1},\ K_2 = k_{2,3} \oplus d_{2,3}$$
$$K_3 = k_{2,3} \oplus d_{3,2},\ K_4 = k_{2,3} \oplus d_{3,2} \oplus d_{3,4} \oplus d_{4,3}$$
$$K_5 = k_{2,3} \oplus d_{3,2} \oplus d_{3,4} \oplus d_{4,3} \oplus d_{4,5} \oplus d_{5,4} \quad (31)$$

となる．ここで，一対の２値 RSSI 系列が個別秘密鍵と一致する場合には，$K_i = k_{2,3}\ , i = 1, \cdots, 5$ となり，２番目と３番目の無線端末間の個別秘密鍵がグループ秘密鍵となる．

以上は，中間の無線端末からの両方向通知を用いたグループ秘密鍵生成の原理を示したが，多数無線端末への拡張も容易に実現できる．また，複数の２値 RSSI 系列を基準としてグループ秘密鍵の取得を繰り返すことで，複数のグループ秘密鍵が取得できる．なお，中間の無線端末を使用することで，不一致成分の増加の影響を若干軽減する効果が期待できる．

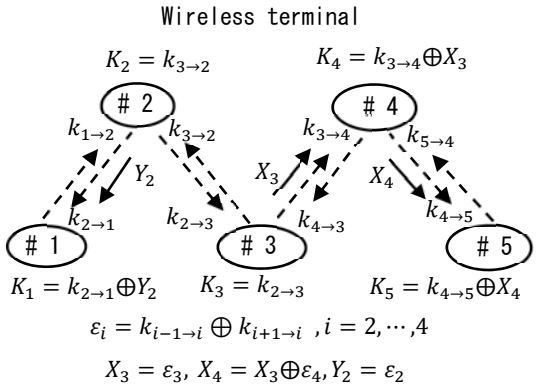


Fig. 8. System configuration of new group key generation via chain connection using two-way notice.

3.2.3 複数のグループ秘密鍵の取得とその応用

２値 RSSI 系列の排他的論理和を通知してグループ秘密鍵を取得する手法は，星型接続において既に提案されている [19]．この従来方式では，一連の処理で複数のグループ秘密鍵を同時に取得できるため，グループ秘密鍵の使い捨て使用が容易となる [19]．また，サブグループ化や新規の無線端末の追加や既存の無線端末の削除などグループ秘密鍵の更新にも便利であることが指摘されている [19]．

鎖型接続の場合は，任意の２値 RSSI 系列を基準とした一連の処理で単一のグループ秘密鍵しか取得できないが，２値 RSSI 系列の複数の基準を変更して一連の処理を行うことで複数のグループ秘密鍵の取得が可能となる．この場合に，２値 RSSI 系列の再測定は必ずしも必要でないので，グループ秘密鍵の使い捨て使用が比較的容易となる．

一方，サブグループ化については，基準とする２値 RSSI 系列の選択および２値 RSSI 系列の排他的論理和を通知する範囲の選択により，複数のサブグループの選択が可能となる．また，新規の無線端末の追加については，鎖型接続の一部に追加して新たな２値 RSSI 系列の取得を行い，２値 RSSI 系列の排他的論理和を新たに通知することで可能となる．さらに，既存の無線端末の削除については，既存の無線端末を除いた鎖型接続を設定するとともに，新たな２値 RSSI 系列の基準に基づく通知を行うことで実現できる．

４．秘密鍵配送を用いたグループ秘密鍵共有

上記の３章では，２値 RSSI 系列の排他的論理和の通知により各無線端末で秘密鍵候補を生成し，その後にグループ秘密鍵共有を行う方式を検討した．しかし，中継回数の増加に伴って信号対雑音電力比に対するグループ秘密鍵容量特性の劣化が避けられない．そこで，雑音の影響を受け難く，雑音の影響をほぼ考慮の対象外とできるシステムを対象として検討を行う．このため，はじめに２値 RSSI 系列から隣接の無線端末間で秘密鍵共有を行い，次に，得られた個別秘密鍵を用いて２値乱数（秘密鍵）を配送することでグループ秘密鍵共有を行うシステムを想定する．

4.1 個別秘密鍵を用いた秘密鍵配送の概要

4.1.1 システム構成と秘密鍵配送の原理

個別秘密鍵を用いた２値乱数の配送によるグルー

プ秘密鍵共有の基本手順を Fig. 9 に示す．基本手順では，図に示すように２値乱数（秘密鍵）を発生させた後で，２値乱数と個別秘密鍵の排他的論理和から通知情報を算出，または，隣接する個別秘密鍵の間の排他的論理和と通知情報との排他的論理和から新たな通知情報を算出して通知することで，各無線端末にグループ秘密鍵が配送される．

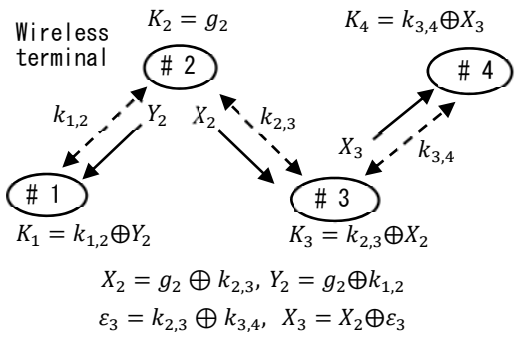


Fig. 9. Principal of group key generation using the secret key distribution.

ここで，通知情報は，

$$X_2 = g_2 \oplus k_{2,3}\ ,\ Y_2 = g_2 \oplus k_{1,2}$$
$$X_3 = X_2 \oplus \left(k_{2.3} \oplus k_{3,4}\right) = g_2 \oplus k_{3,4} \tag{32}$$

となる．また，各無線端末に配送される秘密鍵は，

$$K_1 = k_{1,2} \oplus \left(g_2 \oplus k_{1,2}\right) = g_2,\ K_2 = g_2$$
$$K_3 = k_{2,3} \oplus \left(g_2 \oplus k_{2,3}\right) = g_2 \tag{33}$$
$$K_4 = k_{3,4} \oplus \left(g_2 \oplus k_{3,4}\right) = g_2$$

となり，グループ秘密鍵が配送される．

4.1.2 多数無線端末への拡張と応用

個別秘密鍵を用いた２値乱数の配送によるグループ秘密鍵の配送を多数無線端末に拡張したシステムを Fig. 10 に示す．図においては，m番目の無線端末で２値乱数（秘密鍵）を発生させた後で，２値乱数と個別秘密鍵の排他的論理和から通知情報を算出，または，隣接する個別秘密鍵の間の排他的論理和と通知情報との排他的論理和から新たな通知情報を算出して通知することで各無線端末にグループ秘密鍵を配送する．

ここで，通知情報は，

$$X_m = g_m \oplus k_{m,m+1},\ Y_m = g_m \oplus k_{m-1,m}$$
$$X_i = X_{i-1} \oplus \varepsilon_i = g_m \oplus k_{i,i+1}, i = m+1, \cdots, n-1$$
$$Y_i = Y_{i+1} \oplus \varepsilon_i = g_m \oplus k_{i-1,i}\ , i = m-1, \cdots, 2 \tag{34}$$

と表される．また，各無線端末に配送される秘密鍵は，

$$K_i = k_{i,i+1} \oplus Y_{i+1} = g_m\ , i = 1, \cdots, m-1$$
$$K_i = k_{i-1,i} \oplus X_{i-1} = g_m\ , i = m+1, \cdots, n-1 \tag{35}$$

となる．式(35)はグループ秘密鍵が配送されることを示している．

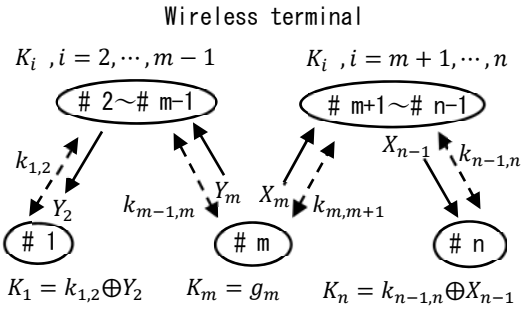


Fig. 10. System configuration of group key generation using the secret key distribution.

4.2 個別秘密鍵を用いた秘密鍵配送の応用

4.2.1 複数のグループ秘密鍵の取得とその応用

２値乱数の配送によりグループ秘密鍵を取得する手法は，星型接続において既に提案されている [19]．この手法では，複数のグループ秘密鍵の取得，サブグループ化，新規無線端末の追加と既存無線端末の削除に便利であることが示されている [19]．

鎖型接続の場合は，複数の２値乱数を発生させることで複数のグループ秘密鍵の取得が可能となる．この場合に，個別秘密鍵の更新の必要がないので，グループ秘密鍵の使い捨て使用が比較的容易となる．

複数のグループ秘密鍵の取得の応用として，２値乱数を発生させる無線端末の選択および鎖型接続の一部の連接した無線端末に通知の範囲を限定するこ

とより，複数のサブグループの構成が可能となる．しかし，星型接続の場合のようにサブグループ化する無線端末を自由に選択することができない．

4.2.2 終端無線端末間の秘密鍵共有への応用

上記の４章では，鎖型接続における鍵配送の手法によるグループ秘密鍵の取得を対象としていたが，鎖型接続の終端無線端末のみで秘密鍵を共有する需要も存在する．しかし，上記のグループ秘密鍵の配送では，グループ外の無線端末に対して秘密が保持されるが，グループ内の無線端末に対して秘密鍵が共有される．このため，終端無線端末のみで秘密鍵を共有するには，公開通信路における秘密鍵配送の手法が必要となる．

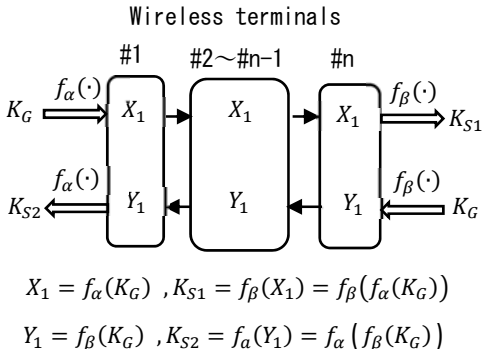
公開通信路を介した鍵配送については，各種の手法が知られているが，ここでは簡易な一実現法を Fig. 11 に示す．図において K_G はグループ秘密鍵で，$f_\alpha(\cdot), f_\beta(\cdot)$ は２値系列の一方向性変換である．また，配送情報 X_1, Y_1, K_{S1}, K_{Sn} は，

$$X_1 = f_\alpha(K_G),\ K_{S1} = f_\beta(X_1) = f_\beta(f_\alpha(K_G))$$
$$Y_1 = f_\beta(K_G),\ K_{Sn} = f_\alpha(Y_1) = f_\alpha\left(f_\beta(K_G)\right) \quad (36)$$

と表される．ここで，一方向性変換に対して，

$$f_\alpha(f_\beta(\cdot)) = f_\beta(f_\alpha(\cdot)) \quad (37)$$

が成り立つとすると，無線端末１と n で取得する秘密鍵 K_{S1}, K_{Sn} は，$K_{S1} = K_{Sn}$ となり，終端無線端末間で秘密鍵が共有される．



$$X_1 = f_\alpha(K_G)\ , K_{S1} = f_\beta(X_1) = f_\beta\left(f_\alpha(K_G)\right)$$
$$Y_1 = f_\beta(K_G)\ , K_{S2} = f_\alpha(Y_1) = f_\alpha\left\{f_\beta(K_G)\right\}$$

Fig. 11. System configuration of secret key agreement between both end of wireless terminal using the secret key distribution.

上記の終端無線端末間での秘密鍵共有の安全性の評価には，グループ内の無線端末による秘密鍵の推定方法とその難易度が重要である．この手法の安全性の根拠は，一方向性変換 $f_\alpha(\cdot), f_\beta(\cdot)$ がそれぞれの終端無線端末でランダムに選択され，途中の無線端末で推測されないことである．途中の無線端末は，K_G, X_1, Y_1 が既知であるので，想定される一方向性変換について総当りで探索すれば，秘密鍵の取得が可能となる．そのため，秘密鍵推定の難易度は，総当り探索に要する計算量と無線端末の演算速度の制約との兼ね合いで決まる．ここで，無線端末の演算速度があまり高くないことを考慮すると，ある程度の安全性が確保できると思われる．なお，具体的な評価は，一方向性変換の規模と演算速度を設定して行う必要があるが，ここでは，これ以上詳しく取り扱わない．

５．まとめ

本論文では，鎖型接続における RSSI 系列の差分値を通知する従来方式は，中継数の増加に伴い雑音の影響が相加されるため，秘密鍵容量特性が大幅に劣化する問題を明らかにした．また，その対策として２値 RSSI 系列の排他的論理和の通知によるグループ秘密鍵生成の有効性を示すとともに，双方向通知を用いて複数のグループ秘密鍵を取得できる新たな手法を提案した．さらに，個別秘密鍵を用いた秘密鍵配送の鎖型接続への適用法を示すとともに，双方向通知を用いて複数のグループ秘密鍵の取得ができる新たな手法を提案した．また，サブグループ化やグループ秘密鍵更新の手法を示すとともに，両終端の無線端末の間の秘密鍵の共有法の検討を行った．

今回，検討の対象外としたグループ秘密鍵共有における鍵不一致解消の手順の検討は今後の課題である．

参考文献

1) A. D. Wyner, “The Wired-tap Channel”, *Bell Sys. Tech. J.*, **54**, 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) I. Csiszar, and P. Narayan, “Secret Capacities for Multiple Terminals”, *IEEE Trans. Inform. Theory*, **50**[12], 3047-3061 (2004).
5) C. Ye, and A. Reznik, “Group Secret Key Generation Algorithms”, *Proc. IEEE Int’l Symp. Inform. Theory* (*ISIT*), 2596-2600 (2007).
6) J. E. Hershy, A. A. Hassan, and R. Yarlagadda, “Unconditional Cryptographic Keying Variable Management”, *IEEE Trans. Communi.*, **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 (2000).
8) K. Zeng, “Physical Layer Key Generation in Wireless Networks: Challenges and Opportunities”, *IEEE Comm. Magazine,* **53**[6],33-39 (2015).
9) 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).
10) S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel”, *Proc. ACM MobiCom*, 128-139 (2008).
11) 北浦明人，笹岡秀一，“陸上移動通信における OFDM の伝送路特性に基づく秘密鍵共有方式”，信学論(A)，**87**[10]，1320-1328 (2004).
12) B. Azimi-sadjadi, A. Kiayias, A. Mercado, and B. Yener, “Robust Key Generation from Signal Envelopes in Wireless Networks”, *Proc. ACM conf. Computer and Comm. Security* (*CCS*), 401-410 (2007).
13) S. Jana, S. Premnath, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy, “On Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environment”, *Proc. ACM MobiCom*, 321-332 (2009).
14) 青野智之, 樋口啓介, 大平孝, 小宮山牧児, 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).
15) 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).
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) 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).
18) 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], 1-9(2019).
19) 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]，(2019).