A Study on Secret Key Agreement Scheme with Mutual Information-Maximized Vector Quantization

Tomoyuki HIGASHIDE*, Shinsuke IBI*, Takumi TAKAHASHI** and Hisato IWAI*

(Received July 7, 2021)

Wireless communication is riskier than wired communication due to eavesdrop by unauthorized stations. To deal with this problem, public key cryptosystem and common key cryptosystem are used in general. In contrast, key agreement schemes based on information-theoretically security attract attention. One example is a secret key agreement scheme based on radio wave propagation characteristics. This technique uses channel reciprocity and location dependency of radio wave propagation. Most of the secret key agreement schemes generate keys by scalar quantization. However, secret keys generated by scalar quantization occur key disagreement in higher probability than those by vector quantization. A general quantizer selection scheme selects a quantizer with minimum key disagreement between two authorized stations. An eavesdropper is able to generate keys with this quantizer more easily. This paper assumes correlated multiple-input multiple-output (MIMO) channel, and proposed the quantizer utilizing correlation between authorized stations as key information and the quantizer selection scheme taking key entropies leak to eavesdroppers into consideration. This scheme that reduces information leaks to eavesdropper maintaining key disagreement probability between authorized stations.

Key words: secret key agreement scheme, physical layer security, correlated MIMO, vector quantization

キーワード：秘密鍵共有方式，物理層セキュリティ，有相関 MIMO，ベクトル量子化

相互情報量最大化規範ベクトル量子化を用いた物理層秘密鍵共有方式に関する検討

東出 朋之，衣斐 信介，高橋 拓海，岩井 誠人

1. はじめに

無線通信では空間を介して情報の送受信を行うため，有線通信に比べ第三者による電波傍受が容易である．そのため，盗聴や不正アクセスの脅威に晒されており，セキュリティ面での脆弱性の問題がある．この問題の対策として，公開鍵暗号方式や共通鍵暗号方式などがある [1]．公開鍵暗号方式は受信者のみが秘密鍵を保持しており，受信者が生成した公開鍵により暗号化したメッセージを秘密鍵により復号化する方式である．公開鍵暗号方式では，端末で複雑な演算処理を必要とするため，一般的に共通鍵暗号方式が用いられる．共通鍵暗号方式は暗号化・復号化に同じ秘密鍵を用いる方式である．しかし，共通鍵暗号方式では，あらかじめ秘密鍵を共有するため，安全に鍵配送を行い，共有した秘密鍵を管理する必要がある．また，これらの暗号方式の安全性は計算量的複雑性

* Department of Electronics, Doshisha University, Kyoto
Telephone: +81-774-65-6355, E-mail: sibi@mail.doshisha.ac.jp
** Graduate School of Engineering, Osaka University, Osaka

に基づいており，演算能力の向上などにより安全性が低下する可能性がある．

一方，情報理論的な複雑性に基づく安全性を根拠とした暗号方式に関する理論的な研究もなされている [2]．その一つとして物理層セキュリティが注目されている．物理層セキュリティは無線物理層において情報セキュリティを実現することで安全に情報共有を行うことを可能とし，それを実現する現実的な方法として，通信路特性を用いた秘密情報伝送 [3] や，電波伝搬特性を用いた秘密情報伝送 [4]，秘密鍵共有方式 [5] などがある．

電波伝搬特性に基づいた秘密鍵共有方式では，電波伝搬の可逆性により正規局間で相関が高い電波伝搬特性が得られるため，正規局間で秘密鍵を共有する一方，伝搬環境の場所依存性により盗聴局は正規局間の電波伝搬特性と相関の低い伝搬特性が得られることから，盗聴局からの秘密鍵の盗聴を困難としている．この方式は情報理論的には相関情報に基づいた秘密鍵共有方式に分類される．この方式では，秘密鍵共有プロトコルは (I) advantage distillation [6]，(II) information reconciliation [7]，(III) privacy amplification [8] と呼ばれる 3 フェーズで構成される．(I) では，正規局間で共有する情報量が正規-盗聴局間で共有する情報量よりも大きくなるような乱数を生成する．(II) では正規局同士が公開通信路で情報交換し，不一致の訂正を行い，乱数系列を一致させる．(III) では，盗聴局に盗聴されることなく正規局間で鍵共有を行う．本検討では (I) において，より効率的な秘密鍵を生成することを目的としている．

これら秘密鍵共有の基本的な方式に，フェージングによる不規則変動を用いる方式がある [5]．一方，準静的レイリーフェージング環境においては，鍵生成の過程で伝搬環境の変化がないため，複数アンテナのアンテナ重みを用いて人工的に電波受信強度に時変化を与える方式 [9] や，エスパアンテナの指向性パターンを変化させ受信強度を変化させる方式 [10] などが提案されている．また，これらのシステムに対する盗聴方法の検討もなされている [11, 12]．さらに，MIMO (Multiple-Input Multiple-Output) 通信路を利用したシステム [13, 14] にも物理層セキュリティが展開されている．加えて，エスパアンテナを用いたシステム [15] では実験的な検討もされている．しかし，得られた受信信号に雑音が含まれるため，量子化によって鍵生成を行う際，受信信号が正規局間で異なる量子化セルに入ることで鍵不一致が発生する．また，これら方式の多くは取得された電波伝搬特性から秘密鍵を生成する過程で簡略化のためスカラー量子化を用いている．

スカラー量子化はベクトル量子化に比べ，伝搬係数間の相関や統計に対して，空間充填や量子化セルの形状などの観点から最適な閾値を設定することが困難となる [16]．その結果，スカラー量子化を適用した場合，伝搬係数の観測点間の距離や観測点と閾値の間の距離が近づくことから，正規局間で観測点が異なる量子化セル内に含まれてしまい，鍵が不一致となる確率が高くなる．この問題への対策としては，量子化セル境界付近にガードバンドを設ける方式 (CQG: Channel Quantization with Guard-band) [17] や量子化セル境界が観測点から遠ざかるよう選択的に適応させる方式 (CQA: Channel Quantization Alternating) [18] などがある．CQG はガードバンドをセル境界の付近に設け，そのガードバンドの外側の観測点のみを鍵生成に使用する方式である．この方式を 2 次元ベクトル量子化に適用した方式も提案されている [19]．CQA は正規局 A で得られた観測点が 2 つのスカラー量子化器で量子化を行った際，観測点と閾値との距離がより大きい量子化セルを適用する方式である．これらの方式をベクトル量子化に適用し複数の量子化器の中から選択する方式もある [20]．しかし，一般的にこの方式は正規局間の鍵のビット誤り率 (BER: Bit Error Rate) が小さくなる量子化器選択を行うため，盗聴局 E が得る伝搬係数の情報が量子化器の判定に反映されていない．つまり，各正規局の観測点が同じセル内に入る確率が高い量子化器の中に盗聴局の観測点が同様のセルに入る確率が高くなる量子化器が含まれる可能性がある．

本検討では，秘密鍵共有方式における鍵生成時の量子化セル境界問題に焦点を当てる．有相関 MIMO 通信路行列からベクトル量子化を用いることでスカラー量子化より効率的に秘密鍵生成を行い，加えて，

量子化器選択を適用したベクトル量子化を用いた秘密鍵生成において，盗聴局への漏洩を考慮した制約を設けた量子化器選択方式を提案する．このとき，量子化器選択の評価関数として条件付き相互情報量を用いる．条件付き相互情報量を最大化する評価関数により，盗聴局へ漏洩する鍵情報が最小化されることに加え，正規局間の相互情報量を最大化する量子化器を選択することで，漏洩を考慮した上で鍵不一致率を小さくするように量子化を行う．計算機シミュレーションによる正規局間および正規-盗聴局間の鍵不一致率特性からベクトル量子化による正規局間の鍵不一致率の低減効果と条件付き相互情報量を用いた評価関数による盗聴局への漏洩抑制効果を確認する．

2. MIMO 通信路における物理層秘密鍵共有方式

2.1 秘密鍵共有方式

本検討では，秘密鍵共有方式として有相関 MIMO 通信環境における鍵共有を考える．盗聴局 1 局を想定した場合のシステムモデルを Fig. 1 に示す．正規局 A で M 本のアンテナを，正規局 B および盗聴局 E では N 本のアンテナを具備しているものとする．屋外移動通信では，フェージングによって時変化する RSSI (Received Signal Strength Indicator) を任意の閾値に基づき量子化し鍵候補を生成できる．一方，屋内通信環境などの準静的レイリーフェージング環境では正規局間で固有の単一の値が得られるためランダムな鍵候補を生成することができない．この場合，MIMO 通信路行列から鍵候補を生成することによって正規局間で固有のランダム鍵候補が得られる．秘密鍵は正規局 A と B が相互に長さ K のパイロットシンボル $\boldsymbol{X}_{\mathrm{A}} \in \mathbb{C}^{M\times K}$, $\boldsymbol{X}_{\mathrm{B}} \in \mathbb{C}^{N\times K}$ を送信し，それにより推定した通信路行列の観測値を量子化することで得られる．ここで，$\mathbb{C}^{a\times b}$ はサイズ $a\times b$ の複素数体を表す．

無線通信環境で送信されたパイロットシンボルは盗聴局 E でも受信され，各正規局での受信信号および盗聴局での受信信号 $\boldsymbol{Y}_{\mathrm{A}} \in \mathbb{C}^{M\times K}$, $\boldsymbol{Y}_{\mathrm{B}}, \boldsymbol{Y}_{\mathrm{E}} \in \mathbb{C}^{N\times K}$ は次式で表される．

$$\boldsymbol{Y}_{\mathrm{A}} = \boldsymbol{H}^{\mathrm{T}}\boldsymbol{X}_{\mathrm{B}} + \boldsymbol{Z}_{\mathrm{A}} \tag{1}$$

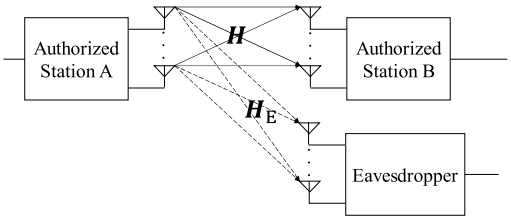

Fig. 1. MIMO-based secret key agreement scheme.

$$\boldsymbol{Y}_{\mathrm{B}} = \boldsymbol{H}\boldsymbol{X}_{\mathrm{A}} + \boldsymbol{Z}_{\mathrm{B}} \tag{2}$$

$$\boldsymbol{Y}_{\mathrm{E}} = \boldsymbol{H}_{\mathrm{E}}\boldsymbol{X}_{\mathrm{A}} + \boldsymbol{Z}_{\mathrm{E}} \tag{3}$$

ここで，$^{\mathrm{T}}$ は行列の転置を表し，$\boldsymbol{H} \in \mathbb{C}^{N\times M}$ は正規局間の通信路行列，$\boldsymbol{H}_{\mathrm{E}} \in \mathbb{C}^{N\times M}$ は正規-盗聴局間の通信路行列，$\boldsymbol{Z}_{\mathrm{A}} \in \mathbb{C}^{M\times K}$ は正規局 A，$\boldsymbol{Z}_{\mathrm{B}}, \boldsymbol{Z}_{\mathrm{E}} \in \mathbb{C}^{N\times K}$ は正規局 B および盗聴局 E における加法性白色雑音 (AWGN: Additive White Gaussian Noise) 行列であり，各要素は平均 0，複素分散 N_0 の複素ガウス分布 $\mathcal{CN}(0, N_0)$ に従う．また，$\mathcal{CN}(a, b)$ は平均 a と分散 b の複素ガウス過程を意味する．

アンテナ間の空間相関を考慮するため，本検討では Kronecker モデルを用いる [21]．このとき通信路行列 $\boldsymbol{H}$ は次式で表現される．

$$\boldsymbol{H} = \boldsymbol{R}_{\mathrm{R}}^{1/2}\boldsymbol{G}\boldsymbol{R}_{\mathrm{T}}^{1/2} \tag{4}$$

ただし，$\boldsymbol{G}$ の各要素は $\mathcal{CN}(0,1)$ に従い，$\boldsymbol{R}_{\mathrm{R}}^{1/2} \in \mathbb{R}^{N\times N}$，$\boldsymbol{R}_{\mathrm{T}}^{1/2} \in \mathbb{R}^{M\times M}$ は送受信の相関行列である．ここで，$\mathbb{R}^{a\times b}$ はサイズ$a\times b$の実数体を表す．指数表現 [22] に基づき，その (i, j) 要素は以下の式で表される．

$$[\boldsymbol{R}_{\mathrm{R}}]_{i,j} = [\boldsymbol{R}_{\mathrm{T}}]_{i,j} = \begin{cases} 1 & (i = j) \\ \rho^{|i-j|} & (i \neq j) \end{cases} \tag{5}$$

ただし，$\rho \in [0, 1]$ は隣り合うアンテナ間の相関係数である．また，正規-盗聴局間の通信路行列の要素 $[\boldsymbol{H}_{\mathrm{E}}]_{i,j}$ は $\mathcal{CN}(0,1)$ に従い，$\boldsymbol{H}$の要素 $[\boldsymbol{H}]_{i,j}$ と独立の変数である．

各局の受信信号から以下の式により通信路行列の推定値 $\widehat{\boldsymbol{H}}$ を得る．

$$\widehat{\boldsymbol{H}}_A^{\mathrm{T}} = \boldsymbol{Y}_{\mathrm{A}}\boldsymbol{X}_{\mathrm{B}}^{\dagger} \tag{6}$$

$$\widehat{\boldsymbol{H}}_{\mathrm{B}} = \boldsymbol{Y}_{\mathrm{B}}\boldsymbol{X}_{\mathrm{A}}^{\dagger} \tag{7}$$

$$\widehat{\boldsymbol{H}}_{\mathrm{E}} = \boldsymbol{Y}_{\mathrm{E}}\boldsymbol{X}_{\mathrm{A}}^{\dagger} \tag{8}$$

ただし，$\cdot^{\dagger}$は疑似逆行列を意味する．得られた通信路行列 $\widehat{\boldsymbol{H}}$ を各局で量子化し秘密鍵を生成する．

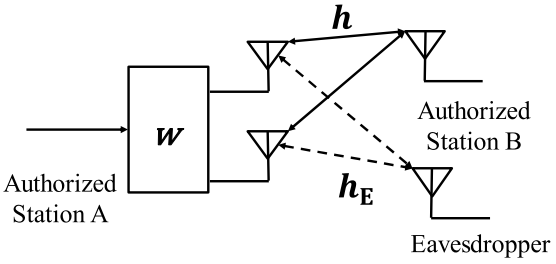

Fig. 2. Secret key agreement scheme by antenna weights of multiple antennas (Conventional scheme).

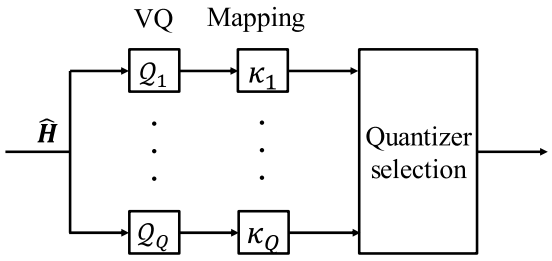

Fig. 3. Secret key generation with vector quantization and quantizer selection.

2.2 MISO 通信環境における秘密鍵共有方式

複数アンテナを用いた秘密鍵共有方式の特殊なケースとして正規局 B および盗聴局で具備されるアンテナ本数が 1 本の場合の MISO (Multiple-Input Single-Output) を想定し，従来方式と位置付ける．このシステムモデルを Fig. 2 に示す．正規局間の通信路行列 $\boldsymbol{h} \in \mathbb{C}^{1\times M}$ の要素を h_i とし，正規局と盗聴局の間の通信路行列 $\boldsymbol{h}_{\mathrm{E}} \in \mathbb{C}^{1\times M}$ の要素 $h_{\mathrm{E}i}$ は $\mathcal{CN}(0,1)$ に従い，h_i と独立の変数であるとする．ここでアンテナの重みベクトル $\boldsymbol{w} \in \mathbb{C}^{M\times 1}$ により伝搬路ベクトルの要素を合成し，等価的に単一アンテナ同士の伝搬路とする．この時の伝搬係数 s は次式となる．

$$s = h_1 w_1 + h_2 w_2 + \cdots + h_M w_M \tag{9}$$

正規局 A では M 本のアンテナで受信後にアンテナ重みにより合成を行っているため雑音がガウス雑音と異なり，各正規局での受信信号 $\boldsymbol{y}_{\mathrm{A}}, \boldsymbol{y}_{\mathrm{B}} \in \mathbb{C}^{1\times K}$ と盗聴局での受信信号 $\boldsymbol{y}_{\mathrm{E}} \in \mathbb{C}^{1\times K}$ を以下の式で表す．

$$\boldsymbol{y}_{\mathrm{A}} = (h_1 w_1 + h_2 w_2 + \cdots + h_M w_M)\boldsymbol{x}_{\mathrm{B}} + \boldsymbol{w}^{\mathrm{T}}\boldsymbol{Z}_{\mathrm{A}} \tag{10}$$

$$\boldsymbol{y}_{\mathrm{B}} = (h_1 w_1 + h_2 w_2 + \cdots + h_M w_M)\boldsymbol{x}_{\mathrm{A}} + \boldsymbol{z}_{\mathrm{B}} \tag{11}$$

$$\boldsymbol{y}_{\mathrm{E}} = (h_1 w_1 + h_2 w_2 + \cdots + h_M w_M)\boldsymbol{x}_{\mathrm{A}} + \boldsymbol{z}_{\mathrm{E}} \tag{12}$$

ここで，$\boldsymbol{x} \in \mathbb{C}^{1\times K}$ は各局から送信されるパイロットシンボルであり，正規局 A では全アンテナから同じパイロットシンボル $\boldsymbol{x}_{\mathrm{A}}$ を送信する．また，$\boldsymbol{Z}_{\mathrm{A}} \in \mathbb{C}^{M\times K}$ は正規局 A，$\boldsymbol{z}_{\mathrm{B}}, \boldsymbol{z}_{\mathrm{E}} \in \mathbb{C}^{1\times K}$ は正規局 B および盗聴局 E における信号に含まれる加法性白色雑音であり，各要素は複素分散 $N_{\mathrm{A}}, N_{\mathrm{B}}, N_{\mathrm{E}}$ の複素ガウス分布 $\mathcal{CN}(0,N_{\mathrm{A}}), \mathcal{CN}(0,N_{\mathrm{B}}), \mathcal{CN}(0,N_{\mathrm{E}})$ に従う．従来方式では，$\boldsymbol{w}$ により合成した各局の受信信号を用い，$\boldsymbol{w}$ を信号 1 サンプルごとに時変化させて疑似的な SISO (Single-Input Single-Output) 通信環境の受信信号系列を変化させることでランダムな強度変動を実現する．正規局間で双方向に伝送を行い，測定した RSSI 系列から閾値を決定し量子化を行うことで鍵候補を生成する．

2.3 ベクトル量子化と量子化器選択

本節では，MISO 通信環境に限定した従来方式の秘密鍵共有方式ではなく，2.1 節で述べた MIMO 通信環境における秘密鍵共有方式においてベクトル量子化と量子化器選択を適用した秘密鍵生成方法について述べる．ベクトル量子化と量子化器選択を用いた秘密鍵生成モデルを Fig. 3 に示す．通信路行列 $\hat{\boldsymbol{H}}$ を Q 個のベクトル量子化器 $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_Q\}$によって各局で量子化を行う．ここで量子化器 $\mathcal{Q}_q$ は MN 次元空間 $\mathbb{C}^{MN}$ を C 個のセルに量子化する量子化器であり，以下の式で表される．

$$\mathcal{Q}_q : \mathbb{C}^{MN} \to \{1, \ldots, C\} \tag{13}$$

この量子化器 $\mathcal{Q}_q$ の出力から，以下の式で表される写像 κ_q により対応する鍵を鍵セット $\{s_1, \ldots, s_L\}$ から生成する．

$$\kappa_q : \{1, \ldots, C\} \to \{s_1, \ldots, s_L\} \tag{14}$$

ここで，s_l は 1 サンプルの通信路行列要素 $[\hat{\boldsymbol{H}}]_{i,j}$ から生成される長さが $\log_2 L$ [bit/sample]の秘密鍵であり，L は生成され得る秘密鍵の総数である．通信路行列 $\hat{\boldsymbol{H}}$ が N 行 M 列の行列であるから，その要素数は MN であり，量子化により $MN\log_2 L$ [bit]の秘密鍵が生成される．

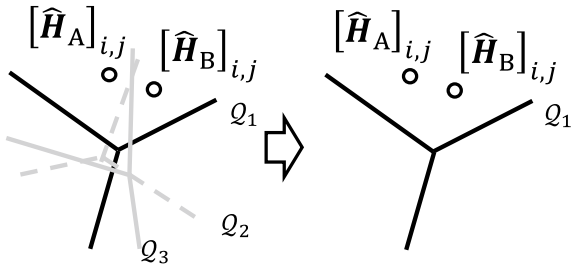

Fig. 4. Model of quantizer selection.

量子化器選択の模式図を Fig. 4 に示す．Q 個の異なる量子化器の中から正規局間の鍵不一致率が最小となる量子化器を選択する．正規局 A で $\hat{\boldsymbol{H}}_{\mathrm{A}}$ が与えられた場合の正規局間の条件付き鍵不一致は以下の式で与えられる．

$$\Pr\left[Q_q(\hat{\boldsymbol{H}}_{\mathrm{A}}) \neq Q_q(\hat{\boldsymbol{H}}_{\mathrm{B}})|\hat{\boldsymbol{H}}_{\mathrm{A}}\right] \tag{15}$$

この鍵不一致率が最小となる量子化器のインデックスは以下の式で表される．

$$q^* = \arg\min_q \Pr\left[Q_q(\hat{\boldsymbol{H}}_{\mathrm{A}}) \neq Q_q(\hat{\boldsymbol{H}}_{\mathrm{B}})|\hat{\boldsymbol{H}}_{\mathrm{A}}\right] \tag{16}$$

正規局 A でインデックス q^* を計算し，正規局 B に送信することで，同様の量子化器で $\hat{\boldsymbol{H}}_{\mathrm{B}}$ を量子化することが可能となる．

また，条件付き鍵不一致率 $\Pr\left(Q_q(\hat{\boldsymbol{H}}_{\mathrm{A}}) \neq Q_q(\hat{\boldsymbol{H}}_{\mathrm{B}})|\hat{\boldsymbol{H}}_{\mathrm{A}}\right)$ は量子化セルの不規則な構造により計算することが困難となるため，以下の式により，トレーニングデータとの鍵不一致率の平均によって近似することで計算する．

$$\begin{aligned}&\Pr\left[Q_q(\hat{\boldsymbol{H}}_{\mathrm{A}}) \neq Q_q(\hat{\boldsymbol{H}}_{\mathrm{B}})|\hat{\boldsymbol{H}}_{\mathrm{A}}\right]\\ &\approx \frac{1}{J}\sum_{j=1}^{J}\Pr\left[Q_q(\hat{\boldsymbol{H}}_{\mathrm{A}}) \neq Q_q(\underline{\hat{\boldsymbol{H}}}_{\mathrm{B}j})\right]\end{aligned} \tag{17}$$

ここで，正規局 B を想定した通信路行列のトレーニングデータ $\{\underline{\hat{\boldsymbol{H}}}_{\mathrm{B}j}\}$ は独立同分布 (i.i.d.: independent and identically distributed) で生成され，J はランダムに生成されたトレーニングデータのセット数である．

3. 相互情報量を用いたベクトル量子化器選択

3.1 秘密鍵共有方式における相互情報量

ここでは，ベクトル量子化と量子化器選択を用いた秘密鍵共有方式において鍵不一致率が最小となる量子化器を選択する方式ではなく，盗聴局に漏れ出す情報量を考慮した量子化器選択方式を提案する．

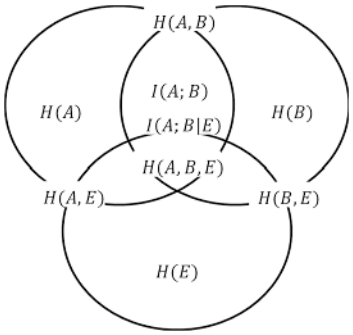

Fig. 5. Relation between entropy and mutual information.

二つの正規局がもつ情報のランダム変数を A，B，盗聴局がもつ情報のランダム変数を E とする．このとき，エントロピーと相互情報量の関係は Fig. 5 に示される．正規局間で共有できる情報量 $I(A;B)$ の中でエントロピー $H(E)$ と重複する領域が盗聴局に漏れる情報量となるため，その情報量を除いた条件付き相互情報量 $I(A;B|E)$ が盗聴局に知られずに正規局間で共有できる情報量となる．確率変数 A，B，E が取り得る値が T，T'，T'' 値とするとその集合は $A=\{a_1,\dots,a_T\}$，$B=\{b_1,\dots,b_{T'}\}$，$E=\{e_1,\dots,e_{T''}\}$ となる．E が e_t となる確率 $P_E[e_{t''}]$ を用いてエントロピー $H(E)$ は次式で表される．

$$H(E) = -\sum_{t''=1}^{T''} P_E[e_{t''}]\log_2 P_E[e_{t''}] \tag{18}$$

また，A と E の結合確率を $P_{A,E}[a_t,e_{t''}]$，B と E の結合確率を $P_{B,E}[b_{t'},e_{t''}]$，A と B と E の結合確率を $P_{A,B,E}[a_t,b_{t'},e_{t''}]$ とすると，その結合エントロピーは以下の式で表される．

$$H(A,E) = -\sum_{t=1}^{T}\sum_{t''=1}^{T''} P_{A,E}[a_t,e_{t''}]\log_2 P_{A,E}[a_t,e_{t''}] \tag{19}$$

$$H(A,E) = -\sum_{t'=1}^{T'}\sum_{t''=1}^{T''} P_{B,E}[b_{t'},e_{t''}]\log_2 P_{B,E}[b_{t'},e_{t''}] \tag{20}$$

$$H(A,B,E) = -\sum_{t=1}^{T}\sum_{t'=1}^{T'}\sum_{t''=1}^{T''} P_{A,B,E}[a_t,b_{t'},e_{t''}] \cdot \log_2 P_{A,B,E}[a_t,b_{t'},e_{t''}] \tag{21}$$

式 (19) から式 (21) を用いて条件付き相互情報量

$I(A;B|E)$ は次式で表される．

$$I(A;B|E) = H(A,E) + H(B,E) - H(E) - H(A,B,E) \quad (22)$$

3.2 相互情報量を用いた量子化器選択

式 (22) の条件付き相互情報量 $I(A;B|E)$ を最大化する量子化器インデックスは以下の式で表される．

$$q^* = \arg\max_q I(A;B|E) \quad (23)$$

また，条件付き相互情報量 $I(A;B|E)$ も条件付き鍵不一致率 $\Pr\left(Q_q(\widehat{\boldsymbol{H}}_\mathrm{A}) \neq Q_q(\widehat{\boldsymbol{H}}_\mathrm{B})|\widehat{\boldsymbol{H}}_\mathrm{A}\right)$ と同様に不規則な量子化セル構造により計算が困難であるため，以下の式により，トレーニングデータにより計算された平均値により近似する．

$$I(A;B|E) \approx \frac{1}{J}\sum_{j=1}^{J} I\left(Q_q(\widehat{\boldsymbol{H}}_\mathrm{A}); Q_q(\underline{\widehat{\boldsymbol{H}}}_{\mathrm{B}j})|Q_q(\underline{\widehat{\boldsymbol{H}}}_{\mathrm{E}j})\right) \quad (24)$$

ここで，$\{\underline{\widehat{\boldsymbol{H}}}_{\mathrm{E}j}\}$ は正規局 B と同様に i.i.d.で生成した盗聴局 E を想定した通信路行列のトレーニングデータである．$I(A;B|E)$ を最大化することで盗聴局 E が得る情報量が最小化されるとともに正規局間の相互情報量が最大化される．その結果，盗聴局に漏れ出す情報量を最小化する条件下で正規局間の鍵不一致率が最小化される量子化器が選択される．

4. 相互情報量を用いた量子化器選択の特性評価

4.1 シミュレーション諸元

提案方式の諸特性を計算機シミュレーションにより評価を行った．シミュレーションの諸元を Table 1 に示す．準静的レイリーフェージング環境を想定し，鍵生成を行う間は通信路行列が変化しないものとする．アンテナ構成は $M = 4$, $N = 4$, アンテナ間の空間相関 $\rho = 0, 0.4$, 秘密鍵は通信路行列要素 1 サンプル当たり $\log_2 L = 1$ [bit/sample] の量子化により生成した．量子化器はランダムなコードブックで数は $Q = 100$ とし，トレーニングデータのセット数は $J = 1000$ で量子化器選択を行った．

Table 1. Simulation parameters.

Antennas	Authorized station A	4 antennas
	Authorized station B	4 antennas
	Eavesdropper	4 antennas
Channel	Channel model	Quasi-static Rayleigh fading
	Correlation model	Kronecker model
	Correlation coefficient	0, 0.4
Quantizer Selection	Bits/sample	1
	The number of quantizers	100
	The number of training datasets	1000

4.2 鍵不一致率特性

提案方式により生成した鍵の正規局間および正規-盗聴局間での平均信号対雑音電力比 (SNR: Signal-to-Noise power Ratio) に対する鍵不一致率特性により提案方式の有効性の評価を行う．正規局間の鍵不一致率特性を Fig. 6 に，正規-盗聴局間の鍵不一致率特性を Fig. 7 に示す．両図には，通信路行列の構成要素の絶対値からスカラー量子化により生成した秘密鍵（SQ），ベクトル量子化を用いた場合の従来方式（Traditional VQ）として最小鍵不一致率となる量子化器選択による秘密鍵，提案方式として条件付き相互情報量が最大となる量子化器選択による秘密鍵（Proposed VQ）の鍵不一致率を示している．

Fig. 6 よりベクトル量子化により生成した秘密鍵は従来のスカラー量子化による鍵生成方式に比べ低い鍵不一致率となることがわかる．また，評価関数に条件付き相互情報量を用いた提案方式は必ずしも鍵不一致率が最小となる量子化器を選択しているとは限らず，その鍵不一致率は従来の正規局間の鍵不一致率を最小化する量子化器選択モデルより高くなる．一方，アンテナ間の空間相関 ρ が 0.4 の場合，通信路行列要素間の相関が高くなり，要素間の距離が小さくなることから鍵不一致率が高くなる．

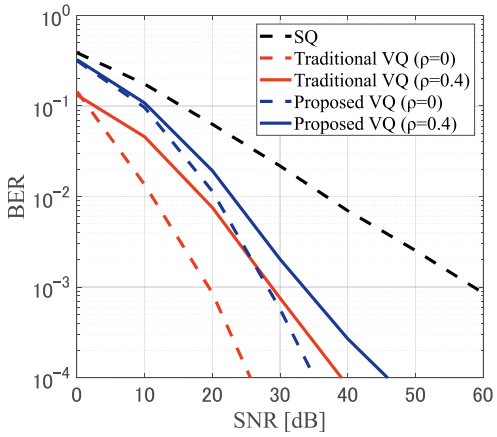

Fig. 6. Key bit error rate between authorized stations.

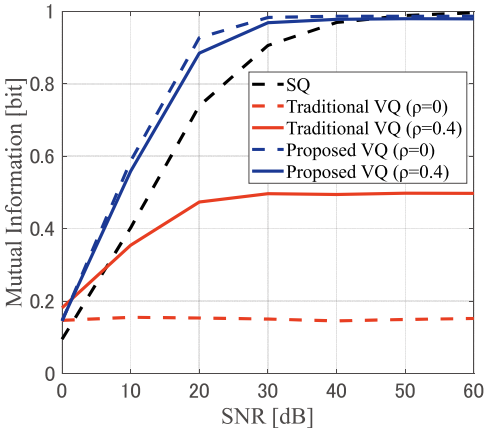

Fig. 8. Mutual information between authorized stations.

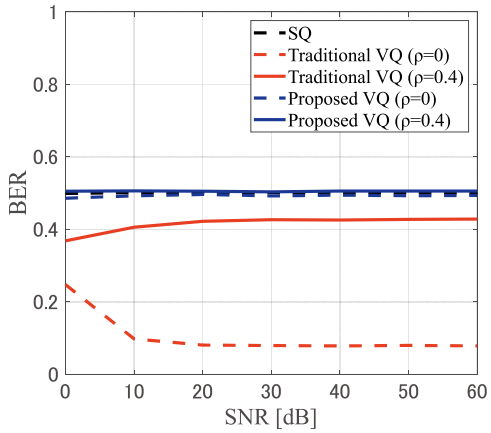

Fig. 7. Key bit error rate between authorized and unauthorized stations.

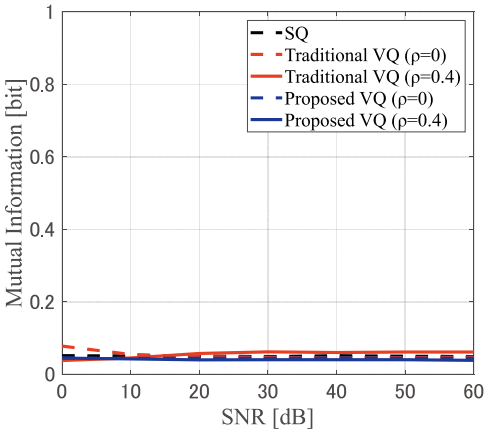

Fig. 9. Mutual information between authorized and unauthorized stations.

一方，Fig. 7 より，ベクトル量子化を用いた場合，正規局間の通信路行列要素が同じ量子化セル内により多く入るよう量子化セルの数を少なく設定しているため，盗聴局でも同様の鍵が得られる確率が高くなる．しかし，盗聴局に対しての漏れを考慮した提案方式による秘密鍵は正規-盗聴局間の鍵不一致率が 0.5 に維持され，鍵情報の漏洩が制限されていることがわかる．空間相関 ρ が 0.4 の場合，両方式において，無相関に比べて盗聴局への漏洩が抑制されていることがわかるものの，ベクトル量子化と条件付き相互情報量による量子化器選択により，盗聴局への鍵情報を増加させることなくスカラー量子化よりも低い鍵不一致率が実現できていることが確認できる．

4.3 相互情報量特性

次に平均 SNR 対相互情報量特性により提案方式の評価を行う．正規局間の相互情報量特性を Fig. 8 に，正規-盗聴局間の相互情報量を Fig. 9 に示す．Fig. 8 に着目すると，従来の正規局間の鍵不一致率が最小となる量子化器選択方式によって生成された秘密鍵の相互情報量は，スカラー量子化によって生成された秘密鍵の相互情報量に比べて低くなっている．一方，提案方式では，雑音の影響が大きい SNR が 40 dB 以下の場合において，スカラー量子化を用いた方式よりも高い相互情報量を実現していることがわかる．また Fig. 9 より，提案方式により生成した秘密鍵は，雑音電力によらず盗聴局へ漏洩する情報量を抑制していることが確認できる．

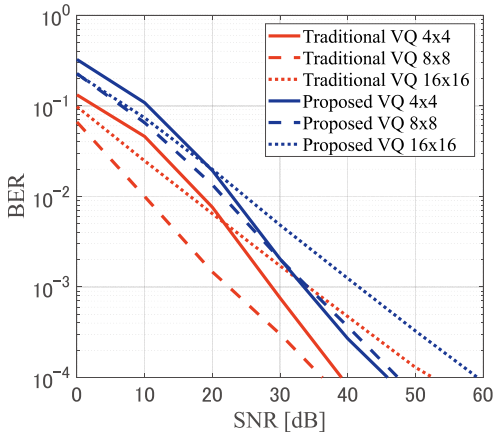

Fig. 10. Key bit error rate between authorized stations with different number of antennas.

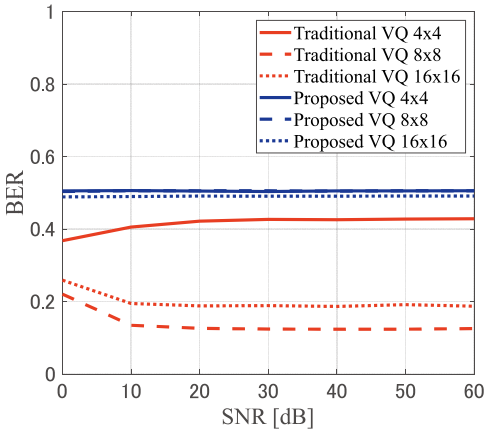

Fig. 11. Key bit error rate between authorized and unauthorized station with different number of antennas.

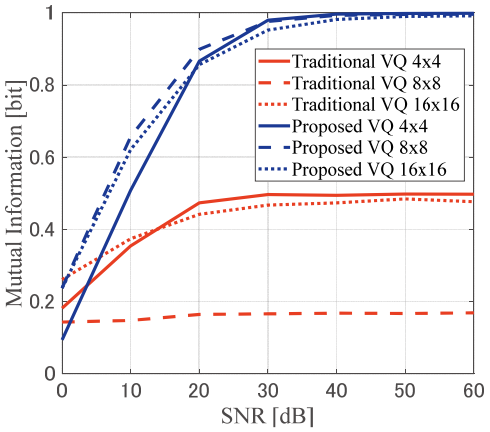

Fig. 12. Mutual information between authorized stations with different number of antennas.

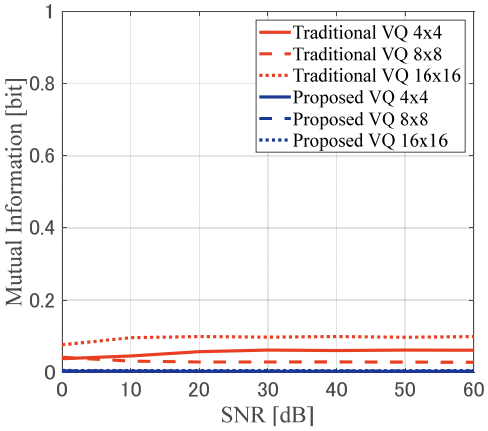

Fig. 13. Mutual information between authorized and unauthorized stations with different number of antennas.

4.4　アンテナ数に対する鍵不一致率特性

Fig. 10 および Fig. 11 に従来の量子化器選択と盗聴局への漏洩を考慮した量子化器選択を用いた場合において，アンテナの本数を変化させたときの正規局間の鍵不一致率特性を示す．Fig. 10 より従来の最小鍵不一致率の量子化器選択により生成された秘密鍵は，アンテナ数を増加させて $M = 8$，$N = 8$ とした場合に正規局間の鍵不一致率が低下している．一方，条件付き相互情報量を最大化する量子化器選択による秘密鍵は，アンテナ数を $M = 8$，$N = 8$ とした場合に SNR が 30 dB 以下では正規局間の鍵不一致率が低下していることが確認できる．両方式ともアンテナ数を，$M = 16$，$N = 16$ とした場合は正規局間の鍵不一致率が増加している．

Fig. 11 より，従来のベクトル量子化と量子化器選択による秘密鍵は正規-盗聴局間の鍵不一致率も正規局間の鍵不一致率と同様にアンテナ数が，$M = 8$，$N = 8$ となる場合に低下しており，盗聴局での鍵生成が容易になっていることが確認できる．一方，提案方式による秘密鍵の鍵不一致率は SNR によらず一定の値で横這いとなり，約 0.5 となっている．以上より，$M = 8$, $N = 8$ とした場合に両方式ともに鍵不一致率の低下が確認できたが，有相関 MIMO 通信環境を想定した場合，アンテナ本数を $M = 16$，$N = 16$ まで増加すると，アンテナ間の空間相関の影響により正規局間の鍵不一致率が高まることがわかった．

4.5 アンテナ数に対する相互情報量特性

ここでは，アンテナ数を変化させた場合の相互情報量特性により評価を行う．正規局間の相互情報量特性を Fig. 12 に，正規-盗聴局間の相互情報量特性を Fig. 13 に示す．Fig. 12 より正規局間の鍵不一致率が最小となる量子化器を選択した場合に比べ，$M=4$, $N=4$ の場合，$M=8$，$N=8$ の場合，$M=16$，$N=16$ の場合の全てにおいて，正規局間で高い相互情報量を実現していることが確認できる．また，$M=4$, $N=4$ の場合に比べて低い鍵不一致率となる $M=8, N=8$ の場合では従来の方式では相互情報量が低くなっているが，提案方式では高くなっている．また Fig. 13 より，従来方式を用いた場合，アンテナの本数を増加させることで盗聴局へ漏洩する情報量が増加していることが確認できるが，条件付き相互情報量によって量子化器を選択することでその情報量が約 0 [bit]となることが確認できる．このことから，条件付き相互情報量を評価関数と用いることで盗聴局への漏洩を低下させると同時に正規局間の相互情報量を増加させることが可能であることがわかる．

5. まとめ

本検討では，物理層秘密鍵共有方式において，電波伝搬特性から量子化によって鍵生成を行う際，雑音による信号の分散により受信信号が異なる量子化セルに入ることで鍵不一致が発生する問題点に焦点を当てた．この問題の対策として，有相関 MIMO の秘密鍵共有モデルにおいて，スカラー量子化に比べ空間充填効率の高いベクトル量子化を用いることで鍵不一致率を低下させるとともに，量子化器選択の過程で正規局間の鍵不一致率を低下させる量子化器を選択することで盗聴局においても鍵生成が容易となる可能性を考慮し，量子化器選択の評価関数として条件付き相互情報量を用いた方式を提案した．

有相関 MIMO の秘密鍵共有モデルにおいて，ベクトル量子化を用いることでスカラー量子化による鍵生成に比べて低鍵不一致率となることに加えて，量子化器選択の評価関数として条件付き相互情報量を用いることで盗聴局への漏洩を低減できることを示した．また無相関の通信路行列を基に生成した秘密鍵の鍵不一致率に比べて，相関を考慮した量子化器選択を行うことで正規-盗聴局間の鍵不一致率が増加し，盗聴局へ漏洩する情報量が低下することを示した．しかし，空間相関を考慮することで，アンテナ数を増加させた場合に通信路行列要素間の距離が小さくなる観測点が増加し，その結果，鍵不一致率が増加することが確認された．以上の結果から，ベクトル量子化と量子化器選択を用いる秘密鍵生成において，盗聴局への漏洩を考慮した評価関数を用いた場合においても，スカラー量子化を用いた場合に比べて低鍵不一致率を実現できることが可能であることを示した．

参考文献

1) 岡本龍明，山本博資，現代暗号，(産業図書，東京，1997).
2) C.E. Shannon, “Communication Theory of Secrecy Systems”, *The Bell System Technical Journal*, **28**[4], 656 - 715 (1949).
3) I. Csiszar and J. Korner, “Broadcast Channels with Confidential Messages”, *IEEE Trans. Inf. Theory*, **24**[3], 339 - 348 (1978).
4) H. Koorapaty, A.A. Hassan and S. Chennakeshu, “Secure Information Transmission for Mobile Radio”, *IEEE Commun. Lett.*, **4**[2], 52 - 55 (2000).
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) U.M. Maurer, “Secret Key Agreement by Public Discussion from Common Information”, *IEEE Trans. Inf. Theory*, **39**[3], 733 – 742 (1993).
7) C.H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, “Experimental Quantum Cryptography”, *Journal of Cryptology*, **5**, 3 - 28 (1992).
8) C.H. Bennett, G. Brassard, C. Crepeau and U.M. Maurer, “Generalized Privacy Amplification”, *IEEE Trans. Inf. Theory*, **41**[6], 1915 - 1923 (1995).
9) 西野太志，笹岡秀一，岩井誠人，“複数アンテナ送受信システムにおける電波伝搬特性に基づく秘密鍵共有方式”，信学技報，**108**[445], 373 – 378, (2009).
10) 長谷川拓，斎藤隆史，植松和正，成田譲二，上原秀幸，大平孝，“エスパアンテナを用いた秘密鍵生成共有方式の雑音耐性と盗聴耐性を高める指向性選択”，信学

論(B), **J94-B**[2], 214 - 255 (2011).
11) K. Zeng, “Physical Layer Key Generation in Wireless Networks: Challenges and Opportunities”, *IEEE Commun. Mag.*, **53**[6], 33 - 39 (2015).
12) 大野修一，戒田博和，小谷考弘，“複数アンテナを用いた秘密通信方式の安全性について-ブラインド等化による盗聴可能性の検討-”，信学論(B), **J95-B**[6], 751 - 759 (2012).
13) J.W. Wallace and R.K. Sharma, “Automatic Secret Keys from Reciprocal MIMO Wireless Channels: Measurement and Analysis”, *IEEE Trans. Inf. Forensics Security*, **5**[3], 381 - 392 (2010).
14) E.A. Jorswieck, A. Wolf and S. Engelmann, “Secret Key Generation from Reciprocal Spatially Correlated MIMO Channels”, *IEEE Globecom Workshops*, 1245 - 1250 (2013).
15) T. Aono, K. Higuchi, T. Ohira, B. Komiyama and H. Sasaoka, “Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channels”, *IEEE Trans. Antennas Propagation*, **53**[11], 3776 - 3784 (2005).
16) T. D. Lookabaugh and R. M. Gray. “High-Resolution Quantization Theory and the Vector Quantizer Advantage”, *IEEE Trans. Inf. Theory*, **35**[5], 1020 - 1033 (1989).
17) J.W. Wallace and R.K. Sharma, “Automatic Secret Keys from Reciprocal MIMO Wireless Channels: Measurement and Analysis”, *IEEE Trans. Inf. Forensics Security*, **5**[3], 381 - 392 (2010).
18) C. Chen and M.A. Jensen, “Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients”, *IEEE Trans. Mobile Computing*, **10**[2], 205 – 215 (2011).
19) A. Filip, R. Mehmood, J. Wallace and W. Henkel, “Variable Guard Band Construction to Support Key Reconciliation”, *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 8173 - 8177 (2014).
20) Y.-W. Peter Hong, Lin-Ming Huang and Hou-Tung Li, “Vector Quantization and Clustered Key Mapping for Channel-Based Secret Key Generation”, *IEEE Trans. Inf. Forensics Security*, **12**[5], 1170 - 1181 (2017).
21) J.P. Kermal, L. Schumacher, K.I. Pedersen, P.E. Mongensen and F. Fredriksen, “A Stochastic MIMO Radio Channel Model with Experimental Validation”, *IEEE J. Sel. Areas Commun.*, **20**[6], 1211 - 1226 (2002).
22) A. Chockalingam and B.S. Rajan, Large MIMO Systems, (Cambridge University Press, New York, 2014).