# 無線秘密鍵生成共有方式の秘匿性を高める可変指向性アンテナの研究

2013 年 9 月

博士 (工学)

坂 井　尚 貴
豊橋技術科学大学

# 無線秘密鍵生成共有方式の秘匿性を高める
# 可変指向性アンテナの研究

## 論文要旨

本論文は無線秘密鍵生成共有方式の秘匿性を高める 3 素子ダイポールエスパアンテナと USB メモリスティック型エスパアンテナの設計および試作について述べる．無線通信で送受する情報は暗号技術を用いる．暗号技術の 1 つに共通鍵暗号プリミティブがある．共通鍵暗号プリミティブは暗号と復号に共通の鍵を使うことが特徴である．共通鍵を盗聴局に盗まれること無く，安全に正規局で共有することが重要である．これを鍵配送問題という．無線秘密鍵生成共有方式は鍵配送問題を解決する技術である．本方式は電波の空間的ゆらぎと時間的ゆらぎから，鍵の生成と共有を行なう．電波のゆらぎは周辺の伝搬環境の変化，正規局に搭載された可変指向性アンテナの指向性パタンの変化で生成される．しかし，本方式が生成する鍵は周辺環境または可変指向性アンテナの性能次第では，配列が単調になり，一部が盗聴局に推定される．我々は鍵の秘匿性を高めるための手段として可変指向性アンテナの設計および試作する．鍵の秘匿性を高める可変指向性アンテナを設計試作するには，設計指標が必要である．

本論文は，無線秘密鍵生成共有方式で生成する鍵の秘匿性を向上させるアンテナ設計指標を提案，その有効性を明らかにする．アンテナ設計指標を用いて 3 素子エスパアンテナを設計および試作する．エスパアンテナは小型，小電力の特長をもつ可変指向性アンテナである．本方式は計算資源が少ない小型無線通信端末への応用が期待されおり，望まれるアンテナの特長は小型，小電力と，エスパアンテナの持つ特長と一致する．最後に 3 素子エスパアンテナの設計試作の成果を発展させ USB スティック型エスパアンテナを試作，評価する．電波のゆらぎと指向性の関係に着目し 5 つのアンテナ設計指標を提案する．アンテナ指標は，指向性パタンを評価する「指向性の複雑性評価指標」と，指向性パタン群を評価する「指向性の多様性評価指標」の 2 種類ある．複雑性評価指標として，エンドファイア・ブロードサイド比（EBR），軌跡長（LLL），累積ビーム幅（CBW）を提案する．多様性評価指標として，パラメータ領域指向性相関係数（PDC），指向性パタン相関係数（ADC）を提案する．受信信号対雑音電力比 0dB 以上，直接波対反射波電力比 3dB 以下の伝搬環境条件において，提案した指標の中で PDC と鍵の秘匿性指標（正規盗聴局間受信信号履歴相関係数）が最も高い正の相関性を示した．故に PDC の低減は鍵の秘匿性向上に有用である．次に PDC を用いて 3 素子ダイポールエスパアンテナの最適な素子間隔を解析と実験で探究する．結果，最小 PDC が得られる素子間隔は 1/16 波長を示した．前述の結果を基に，USB メモリスティック型エスパアンテナを設計，試作した．素子間隔が 1/4 波長の 3 素子ダイポールエスパアンテナと比較し，試作した USB スティック型エスパアンテナは，鍵の秘匿性指標 Imac が 0.01 向上，サイズが 1/8 小型化を達成した．

# Variable Beamforming Antennas for Wireless Secret Key Agreement Systems

## ABSTRACT

This paper presents a three-element dipole ESPAR antenna and a USB stick ESPAR antenna for variable beamforming in wireless secret key agreement system. Wireless communication exchanges data in safety by cryptography technologies. The modern field of cryptography technologies is divided into two areas of symmetric-key cryptography and public-key cryptography. In the symmetric-key cryptography, a regular terminal needs to exchange a secret key with its party terminal for applying the secret key to encryption and decryption. This exchange must be done in secret from eavesdroppers. However, that is difficult in wireless communication systems. This is because, if the regular terminal transmits the key on a radio wave, it is easily intercepted by eavesdroppers. This is called key distribution problem. As a solution of this problem, a wireless secret key agreement system was proposed. The system generates and shares the key by making full use of wave fluctuations in space and time. The wave fluctuations are generated by changing the radio propagation environment around the terminals or varying the directivity of a variable beamforming antenna. However, the system has a problem. This problem is that a part of the key is estimated to intercept wave fluctuations by eavesdropper under some propagation property or antenna performance conditions. As degree of the key that isn't estimated by eavesdropper, secrecy of the key is defined. As a solution to achieve high secrecy of the key, we design and prototype variable beamforming antennas. This is because, secrecy of the key depends on wave fluctuations, and wave fluctuation is generated directivity fluctuation formed by the antenna. We expect to improve secrecy of the key when the antenna is designed by FoMs to indicate its performance. However, there are no FoMs that correlate with the secrecy of the key. Therefore, there is not a report on an antenna design and prototype for the system.

This paper aims to establish a variable beamforming antenna technology that improves the performance of wireless secret key agreement systems. We propose five FoMs for antenna directivity that correlate with the secrecy of the key to generate. The FoMs are defined from relation between the directivity and the wave fluctuations made by controlling the directivity.

We show the validity of the proposed FoMs by computer simulation. This is done by showing the cross correlation coefficient between secrecy of the key and the FoMs. Based on the FoMs, we design and prototype two kinds of variable beamforming antennas.

First, we define five antenna FoMs. These FoMs are classified into two categories: (1) FoM of directivity complexity and (2) FoM of directivity diversity. The FoM of directivity complexity shows fluctuation quantity of directivity. As the FoM, Endfire to Broadside Ratio (EBR), Locus Line Length (LLL), and Cumulative Beam Width (CBW) are proposed. The FoM of directivity diversity shows directivity fluctuation independence of space and time. As the FoM, Parameter Domain Correlation coefficient (PDC) and Azimuth Domain Correlation coefficient (ADC) are proposed.

Next, we describe about the validity of the five FoMs. We investigate two characteristics by the system simulation. First characteristic is percentage of improving secrecy of the key by the FoMs. Second characteristic is a cross correlation coefficient between secrecy of the key and the FoMs. RS profile correlation coefficient between regular terminals and an eavesdropper is defined as secrecy of the key. RS profile is values before quantizing the key. Simulation model of wave propagation is Transmit-Receive Beamlet Correspondence model. As results, validity of PDC is highest compared with other the FoMs. The cross correlation coefficient between PDC and secrecy of the key shows above 0.77 at RNR over -10 dB and K factor below 3 dB. And, the percentage of improving secrecy of the key gets up to 40%. RNR and K factor are wave propagation properties. RNR is Received signal to Noise Ratio. K factor is Direct wave to Reflection wave Ratio.

Then, we design and prototype variable beamforming antennas based on PDC. The system employs an ESPAR antenna. This is because, features of an ESPAR antenna conforms with feature of a antenna desired by the system. The system is expected to apply mobile communication required very little computational resource. Therefore the system desires antenna features of compact size, low power consumption, and low cost. The ESPAR antenna has the same antenna features as ones. We investigate optimal element space of 3-element ESPAR antenna for the system by PDC in analysis and measurement of directivity. As the result, optimal element space is sixteenth-wavelength.

Finally, we prototype a USB stick ESPAR antenna by utilizing the previous results. The antenna shows downsizing of one-eighth and the slightly better value of PDC in comparison with the 3-element dipole ESPAR antenna having quarter-wavelength element space.

# 目次

# 第 1 章

# 序論

## 1.1　暗号化通信の技術背景

無線通信にとって暗号技術はな不可欠である．無線 LAN やスマートフォンなどの一般向け無線通信端末が爆発的に普及し，ソーシャルネットワークサービスやクラウドサービス等の様々な情報サービスが現れている．これらサービスは，個人情報や企業内部情報等の機密性の高い情報を取り扱うことが多々ある．情報は電波を介して、端末および基地局の間を頻繁に行き来している．電波は誰もが傍受することができるため，無線通信により送られる情報は悪意ある第三者でも簡単に得ることができる．つまり，悪意ある第三者が情報を獲得しても，情報を無価値化するためには，情報の暗号化が重要である．

現在，良く知られる暗号技術の基本構成要素（暗号プリミティブ）は，共通鍵暗号プリミティブと公開鍵暗号プリミティブに大別することができる [1][2]．共通鍵暗号プリミティブとは，正規局が持つ暗号鍵と復号鍵に共通の鍵を使う技術である．代表的な物に，ストリーム暗号，ブロック暗号，等がある．

ストリーム暗号とは，送信側が平文と共通鍵に対して排他的論理和演算を行なう事でデータを暗号化する．そして，受信側は暗号文と共通鍵に対して排他的論理和演算を行なう事で暗号文を復号する．平文サイズより共通鍵サイズが小さい場合，適当な擬似乱数発生器でもって共通鍵を，平文サイズの擬似乱数鍵に拡張する．この場合，擬似乱数鍵が「ランダム」に見えるだけでなく，悪意ある第三者が擬似乱数鍵の数ビットかを手に入れても他のビットを予測できない（一方向性），という事でなければならない．ストリーム暗号は暗号文の誤りを復号時に拡大しない等の特長があり，雑音の影響で情報の誤りが起きやすい無線通信分野で良く利用される．

ブロック暗号とは，平文をブロックと呼ばれる単位毎に分割し，ブロックと同じサイズの共通鍵を用いてそれぞれのブロックの暗号化を行う．このとき，ブロック毎に暗号化のやり方を擬似乱数的に変化させる．利用用途が多岐にわたることが特長であるが，反面，

ストリーム暗号と比べ計算資源が必要な事が問題である．

以上のような共通鍵暗号プリミティブは，暗号／復号に必要な計算資源が少ないことが特長である．特に，平文サイズと共通鍵サイズが等しい場合，無限の計算資源を持ってしても，公開情報から共通鍵を推測することができない．情報理論的に安全であると言える．しかしながら，共通鍵を悪意ある第三者に漏れる事無く，正規局同士で共有しなければならない，鍵配送問題が大きな課題と言われている．

この鍵配送問題を解決し，現在最も広く普及している暗号技術が公開鍵暗号プリミティブである [1][3]．公開鍵暗号プリミティブとは，正規局が持つ暗号鍵と復号鍵が異なる鍵を用いており，暗号化するための鍵を公開し，復号のための鍵を秘密とする．代表的な物に，素因数分解ベース方式と離散対数ベース方式の 2 種類がある．公開鍵暗号プリミティブは，数学的問題を解く事の困難さを暗号セキュリティーに活用しており，暗号鍵を含む公開情報から復号鍵を有限時間内に推測することは，現存する数学的アルゴリズムや計算資源において限りなく困難である．つまり情報理論的に安全であると言える．そして，暗号化および復号化には計算資源を必要とするため，平文そのものを暗号化するより，秘密鍵を暗号化して，秘密鍵の共有に使われることが多い．しかしながら，公開鍵暗号プリミティブは量子コンピュータによる並列計算処理で多項式時間で解ける事が，Pester Shor により証明された [4]．そして，量子コンピュータの実現可能性が叫ばれている事からも，近い将来，公開鍵暗号プリミティブの鍵の安全性は崩壊する恐れがある．つまり，公開鍵暗号プリミティブにかわる新たな鍵配送手段の研究が急務である．

この鍵配送問題を物理現象を用いて解決する技術として，量子鍵配送方式が有名である [5]-[7]．量子鍵配送方式は，量子力学の原理を安全性の担保としているため，無限の計算資源を持ってしても秘密鍵を推定することができない．しかしながら，量子鍵配送方式は，光ファイバーを介した通信のみに適用できる方式であり，無線通信への応用は困難である．

## 1.2 無線秘密鍵生成共有方式の研究背景

無線通信による鍵の配送問題の解決手法として電波ゆらぎを用いた無線秘密鍵生成共有方式が提案，研究されている [8]-[28]．この方式は周辺環境の変化による電波伝搬路の無作為な変化（電波ゆらぎ）を秘密鍵生成に活用する．電波ゆらぎとは，送信アンテナが放射する電波に対して，受信アンテナが受信する信号の時間的変化および空間的変化のことを示しており，この両方を駆使する事で秘密鍵を安全に生成，共有する．本方式は電波伝搬の原理を安全性の担保としており，無限の計算資源を持ってしても秘密鍵を推定する事は困難である．しかし，電波のゆらぎがない，もしくは小さい・緩やかである伝搬環境において，本方式は鍵生成の効率および秘匿性が著しく劣化する問題がある．

電波ゆらぎが小さい伝搬環境において，鍵生成効率および秘匿性を向上させる手法として，可変指向性アンテナを用いた無線秘密鍵生成共有方式が提案，研究されている [29]-[53]．本方式は，正規局に可変指向性アンテナを搭載し，電波のゆらぎを周辺環境の変化と指向性パタンの変化の両方で起こす方式である．そして，周辺環境の変化と指向性パタンの変化の相乗効果により，鍵生成効率および秘匿性向上効果が期待できる．しかしながら，特定の伝搬環境で，かつ周辺環境の変化がない，もしくは緩やかである場合において，鍵の秘匿性が低下することが知られている [53]．

この問題を解決するために，文献 [29][36][43] は本方式の鍵生成に用いる複数の指向性パタンの選別による秘匿性の向上を示唆している．指向性パタンの選別は，可変指向性アンテナが形成可能な指向性パタンの中から行なわれる．故に，可変指向性アンテナは秘匿性向上に貢献できる指向性パタンを形成できることが重要である．可変指向性アンテナが形成可能な指向性パタンは，アンテナの構造に依存する．可変指向性アンテナの設計試作により本方式の秘匿性が飛躍的に向上することが期待できる．しかしながら，1）本方式の秘匿性を高めうるアンテナを設計するためのアンテナ設計指標がない．2）そのため，無線秘密鍵生成共有方式のために設計，試作した可変指向性アンテナは報告されていない．という課題がある．

課題 1) の解決法として，鍵の秘匿性を示す秘匿条件付き相互情報量（Information mutual on anti-tapping condition: Imac）[35][22] や鍵容量 [14] をアンテナ設計指針として用いることが考えられる．鍵容量および Imac をアンテナ設計指針として用いた場合，無線秘密鍵生成共有方式のシステム構築およびシステムの秘匿性評価実験を行なう必要があるため，可変指向性アンテナの評価に多くの時間を消費する．また，鍵容量，Imac は同じアンテナ，同じ伝搬環境条件（受信信号対雑音電力比，直接波対反射波電力比）であっても，正規局や盗聴局の配置，周辺環境などによっては評価結果が変わる．以上より鍵容量および Imac をアンテナの設計指標として用いることは，評価時間，普遍性の点から不適当である．本論文の第一中間目標として，アンテナの指向性を測定するだけで，無線秘密鍵生成共有の秘匿性向上が期待できるアンテナであることを示す，可変指向性アンテナの設計指標を提案する．可変指向性アンテナの設計指標は様々な環境で有用なものを目指す．

## 1.3　可変指向性アンテナの研究背景

1.2 節で述べた課題 2 より，本論文は無線秘密鍵生成共有方式のための可変指向性アンテナの設計，試作を最終目標とする．無線秘密鍵生成共有方式は鍵生成に計算資源を使わないため小型端末への応用が期待されている．そのため，可変指向性アンテナは小型，小電力であることが望ましい．

一般よく用いられる可変指向性アンテナとして，フェーズドアレーや Digital Beam-

forming（DBF）がある [54][56]．フェーズドアレーは複数の放射素子をアレー状に配置し，各素子が受信（送信）する電波の振幅および位相を独立に電子制御するアレーアンテナである．そして各素子の電波を合成して受信回路に出力する．電子制御には移相器や高周波増幅回路等のアナログ回路を用いて行う．そのため，デバイスパラメータのばらつき等により，理想とする指向性形成は苦手である．

フェーズドアレーより優れた指向性形成能力を持つ可変指向性アンテナが DBF である．DBF は複数の放射素子にそれぞれに A/D 変換回路を搭載し，各素子の励振の振幅および位相をデジタル制御するアンテナである．デジタル的に振幅と位相を制御するため，フェーズドアレーで問題となったデバイスパラメータのばらつきの影響を受けず，また正確な演算機能を駆使するため，理想に近い指向性制御を容易に行うことができる．しかし，A/D 変換回路以外にも高周波増幅回路や周波数変換回路等を各素子ごとに必要とするため，フェーズドアレーより高コストになる．

上記２種類の可変指向性アンテナと比べ低コスト，低消費電力を追求した可変指向性アンテナとしてエスパアンテナが研究開発されている [57]-[73]．エスパアンテナは主放射素子の近傍に複数のパラサイト素子を設けて電磁的に結合させる．これにより，八木・宇田アンテナと同様の原理で指向性を形成する．エスパアンテナはパラサイト素子の電気長を可変リアクタンス回路で変えることにより指向性を制御する．可変リアクタンス回路はバラクタと呼ばれる可変容量ダイオードを用いいて作られる．指向性制御回路がバラクタ回路のみであること，受信回路が 1 系統であることから，低コスト，低消費電力を実現している．

本論文は小型，低消費電力，構成要素の簡単さが特徴であるエスパアンテナを基とし，無線秘密鍵生成共有方式用 USB スティック型エスパアンテナを設計・試作する．エスパアンテナは近年の半導体技術の進歩により実現可能となった比較的新しいフェーズドアレーである．空間的電磁界結合を積極的に利用したフェーズドアレーであるため，アンテナの構造と指向性制御の物理的な理解が困難であり，従来のフェーズドアレーの設計プロセスを用いることは難しい．従って，初めにエスパアンテナの基本的な構造と指向性制御に関する基礎知識を習得する．その知識を用いて無線秘密鍵生成共有方式用 USB スティック型エスパアンテナを設計・試作する．

## 1.4　本論文の構成

本論文の構成について述べる．第 2 章では無線秘密鍵生成共有方式の鍵生成共有シミュレーターを構築するための基本知識について述べる．第 3 章は無線秘密鍵生成共有方式の秘匿性を向上が期待できる可変指向性アンテナの設計指標を提案する．鍵生成に重要な電波のゆらぎの物理現象に着目し，「指向性の複雑性」と「指向性の多様性」の 2 つの観点

から指標を提案した．第 4 章は，第 3 章で提案したアンテナ設計指標が，無線秘密鍵生成共有方式の秘匿性を高める可変指向性アンテナを設計に有用であるかを明示する．アンテナ設計指標の有用性検証に用いる無線秘密鍵生成共有方式の鍵生成共有シミュレーターは第 2 章で記述してあるものを用いる．第 5 章は，第 4 章で示した無線秘密鍵生成共有方式のためのアンテナ設計指針を用いて最適設計を行う，エスパアンテナに関する基本知識について述べる．第 6 章は，エスパアンテナの基本構造である 3 素子ダイポールエスパアンテナを用いて，アンテナの構造とアンテナ設計指標の関係について理論および実験で探求する．第 7 章は，第 6 章で得たアンテナの構造とアンテナ設計指標の関係を用いて，USB メモリスティック型エスパアンテナを設計，評価する．最後に第 8 章にて，上記成果をまとめる．

# 第 2 章

# 可変指向性アンテナを用いた無線秘密鍵生成共有方式

本章は，可変指向性アンテナを用いた無線秘密鍵生成共有方式の秘匿性評価シミュレーションを行なうための基本知識を記述する．2.1 節で，可変指向性アンテナを用いた無線秘密鍵生成共有方式の基本原理を記述する．2.2 節では，本方式を用いて実際に行なわれる秘密鍵生成共有の手順について述べる．2.3 節は，鍵の安全性を評価する上で重要な秘密鍵の盗聴手法を説明する．以上の 3 つ節で無線秘密鍵生成共有方式のシステムを構築するための基本知識を習得する．そして，2.4 節は，生成した秘密鍵が盗聴局に傍受されること無く正しく共有できることを示す秘匿性評価指標の説明する．

2.5 節および 2.6 節は，伝搬環境および可変指向性アンテナのシミュレーションモデルについて定義，説明する．定義するシミュレーションモデルは，第 4 章の無線秘密鍵生成共有方式の秘匿性を高める可変指向性アンテナの性能の探究する，鍵生成共有シミュレーションに用いる．

## 2.1　原理

電波のゆらぎを用いた無線秘密鍵生成共有方式の原理について述べる．本方式は電波伝搬の原理を鍵生成，共有および安全性に利用している．

鍵生成および共有の原理について説明する．図 2.1 に示す様に正規局 Alice および Bob は互いに電波の送受信する．このとき，互いの送受信が全て完了する間に正規局周辺の伝搬環境が変化しないかつ，Alice と Bob が互いに同じ信号を送信した場合において，Alice および Bob が得ることができる受信信号（Received Signal: RS）は等しい．この現象を電波伝搬の原理の一つ，「電波伝搬の相反性（可逆性）」という．

次に上記，正規局間で電波の送受信を繰り返し行なう．このとき，正規局周辺が市街地

やオフィス内外などの変化に富んだ環境であるかつ，正規局がそれぞれ得る RS の時間間隔が伝搬環境の変化よりも広い場合において，Alice および Bob が得る RS 履歴は乱数性を持つ．この現象は「マルチパスフェージング」と呼ばれる．

鍵の安全性の担保である電波伝搬の原理を説明する．盗聴局 Eve は秘密鍵を得るために，Alice と Bob がやり取りしている電波を傍受する．このとき，図 2.1 より，正規局と盗聴局の場所が異なるために，正規局間の電波伝搬路と Alice と Eve の間の電波伝搬路は異なる．従って，正規局が得る RS と Eve が得る RS は異なる．つまり，盗聴局は正規局が得る RS 履歴を推定する事が困難である．具体的には正規局と盗聴局の間の距離が 1/4 波長以上離れると盗聴局は正規局の RS 履歴を推定する事が困難である [14]．この現象は「電波伝搬の空間的局所性」と呼ばれる．

以上の 3 つの電波伝搬の原理により，正規局は互いに乱数性を持つ同じ RS 履歴を獲得することができ，さらには盗聴局が RS 履歴を推定する事が困難であるため，安全に RS 履歴を共有できる．しかしながら，本方式は正規局周辺の環境が変化に乏しい環境である場合，鍵生成共有にかかる時間および鍵の秘匿性が劣化する問題がある．

上記課題を解決するために，可変指向性アンテナを利用した無線秘密鍵生成共有方式がある [29][33]．本方式は，正規局が互いに電波を送受する際に，正規局が持つ指向性パタンも連動してランダムに変化させる．これにより，正規局が得る RS 履歴は，フリスの伝搬公式より電波伝搬路の時間変化に，アンテナの指向性パタンの時間変化が含まれる．その際，電波伝搬の相反性，RS 履歴の乱数性，および電波伝搬の空間的局所性は保たれる．つまり，本方式は環境の変化による電波のゆらぎと，指向性パタンの変化による電波ゆらぎの相乗効果によって，鍵の秘匿性および生成効率の向上を狙う．加えて，周辺環境の変化に乏しい環境であっても，指向性パタンの変化により RS 履歴が得られるため，鍵の秘匿性及び生成効率が保たれる．

## 2.2　秘密鍵生成共有手順

本方式を用いるシステムとして，可変指向性アンテナを搭載した基地局と無指向性アンテナを搭載した端末局を想定する．このときの RS 履歴の生成共有手順のイメージを図 2.2 に，鍵生成共有手順ののフローチャートを図 2.3 に示す．図 2.2 の正規局 Alice は可変指向性アンテナ，正規局 Bob および盗聴局 Eve は無指向性アンテナを持つ．図 2.2 下 IQ 軸は各局が受信する信号の実部と虚部を表している．IQ 軸の原点から伸びるベクトル，例えばベクトル A は，指向性パタン A を Alice が形成し Alice と Bob で電波を 1 回送受信したときの，各局が受信した RS の複素ベクトルである．図 2.3 より，鍵生成共有手順は主に 2 つのフェーズで分けられる．第一フェーズで，図 2.2 の手順に従い指向性パタンを変更する毎に電波の送受信を繰り返すことで両正規局（Alice と Bob）は RS 履歴を生

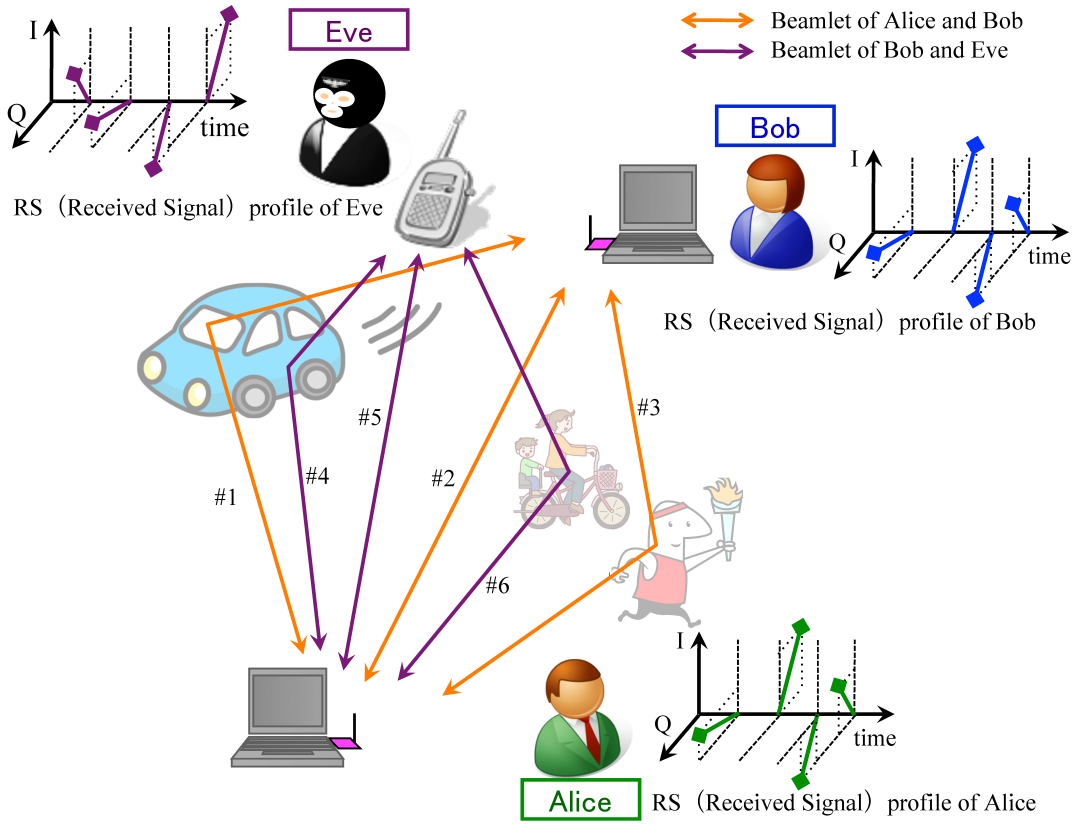



図 2.1　Secret key generation with wave propagation

成・共有する．正規局の送信と受信の時間間隔は，周辺環境の変化が起こるより十分短い周期で行なう．第二フェーズで，両正規局は RS 履歴の量子化，誤り訂正 [33] 等を経て秘密鍵を生成する．従って，この秘密鍵の秘匿性は，第一フェーズの「RS 履歴の生成共有方法」および第二フェーズの「量子化と誤り訂正の方法」の 2 つに左右される．

本論文はアンテナの指向性が鍵の秘匿性に与える影響を調べることが目的である．つまり，第一フェーズの RS 履歴の生成共有に与える影響を調べることと等価である．第二フェーズを含めた秘密鍵の秘匿性とアンテナの指向性の関係を調べることは，量子化や誤り訂正の手段によっては結果が変わる恐れがある．そこで本論文は，アンテナの指向性が第一フェーズの RS 履歴のみに影響を与えることから，より不変性のある RS 履歴の秘匿性を評価する．

## 2.3　秘密鍵盗聴手法

本方式に対する秘密鍵の盗聴手法の手順について述べる．鍵の盗聴法は受動的盗聴法と能動的盗聴法の 2 つが考えられている [38][43][28]．受動的盗聴法とは，盗聴局から正規

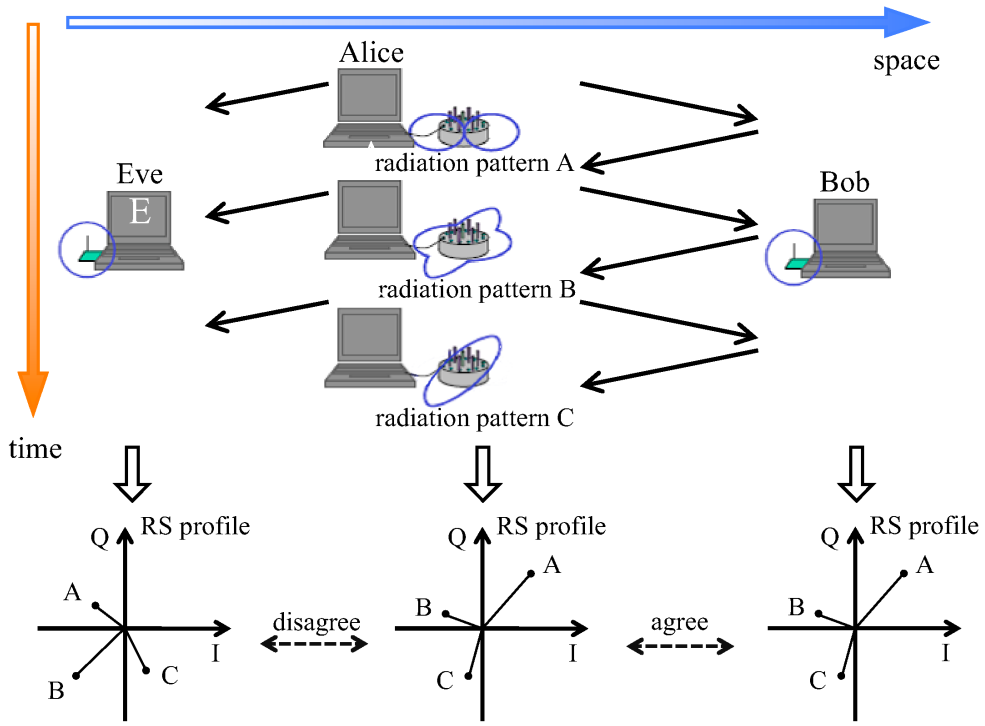



図 2.2　Secret key generation and eavesdropping procedure

局に対し何らかの攻撃を仕掛けることなく，密かに鍵を盗聴する手法である．そのため，正規局に盗聴中である事が気づかれにくい特長を持つ．能動的盗聴法とは，盗聴局から正規局に対し何らかの攻撃を仕掛けることで，鍵を盗聴する手法である．盗聴局から攻撃を仕掛けるため，盗聴性能は受動的盗聴法に比べ高い．その反面，正規局に盗聴中である事を気づかれる恐れがある．以下の小節でそれぞれの盗聴法の具体例について説明する．

### 2.3.1　受動的盗聴法

受動的盗聴法の一つに，正規局が放射する電波を受信し，盗聴局も正規局と同様に RS 履歴を生成，それを鍵とする手法が文献 [38][43] で述べられている．鍵傍受の様子を図 2.1 に，手順を図 2.2 に示す．図 2.1 より，可変指向性アンテナを搭載する Alice からの電波のみを盗聴する．何故ならば，Alice の電波には指向性パタンおよび電波伝搬路の情報が含まれており，盗聴局はその両方の情報を獲得することが重要だからである．見通し内伝搬環境において，盗聴局は両正規局を結ぶ直線上に配置する [47]．これは，見通し内伝搬環境において盗聴局の両正規局の直線上配置は，平均以上の秘密鍵の推定が期待できるからである．今後はこの現象を「直接波問題」と呼ぶ．直接波問題について図 2.1 を用いて具体的に説明する．

可変指向性アンテナを用いた無線秘密鍵生成共有方式において，RS は図 2.1 にも示さ

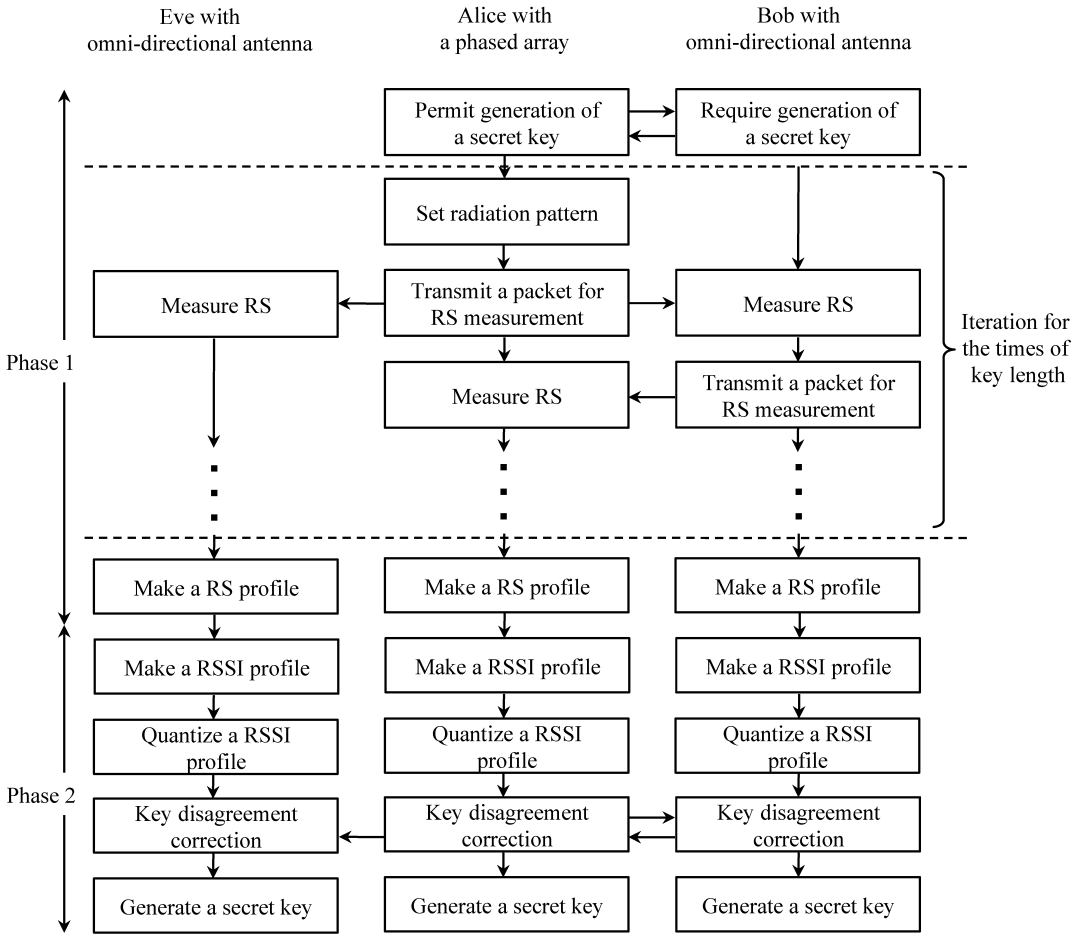



図 2.3　Flowchart of secret key generation and eavesdropping

れているように各素波を足し合わせた物であり，RS 履歴は各素波の時間変化を足し合わせた物であるとも言える．正規局が受信する各素波の中で，フリスの電波伝搬公式から，直接波が最も振幅が大きいと言える．従って，各素波の時間変化を足し合わせて得られる RS 履歴は，振幅の最も大きい直接波に強い影響を受けるといえる，見通し内伝搬環境において，盗聴局 Eve は正規局間の直接波を傍受する事が秘密鍵を推定する上で最も有効な手段の 1 つであると言える．論文 [35]-[38]，[43] において受動的盗聴法が鍵の秘匿性評価に最も用いられているため，本論文では受動的盗聴法を用いて鍵の秘匿性を評価する．

### 2.3.2　能動的盗聴法

能動的盗聴法として，正規局間の素波の一つを増幅させる事で，盗聴性能を高める手法が提案されている [28]．図 2.4 を用いて，能動的盗聴法の原理について述べる．Eve は正規局間で得られる素波の中の一つを増幅する．この増幅された素波を含め RS 履歴は生成

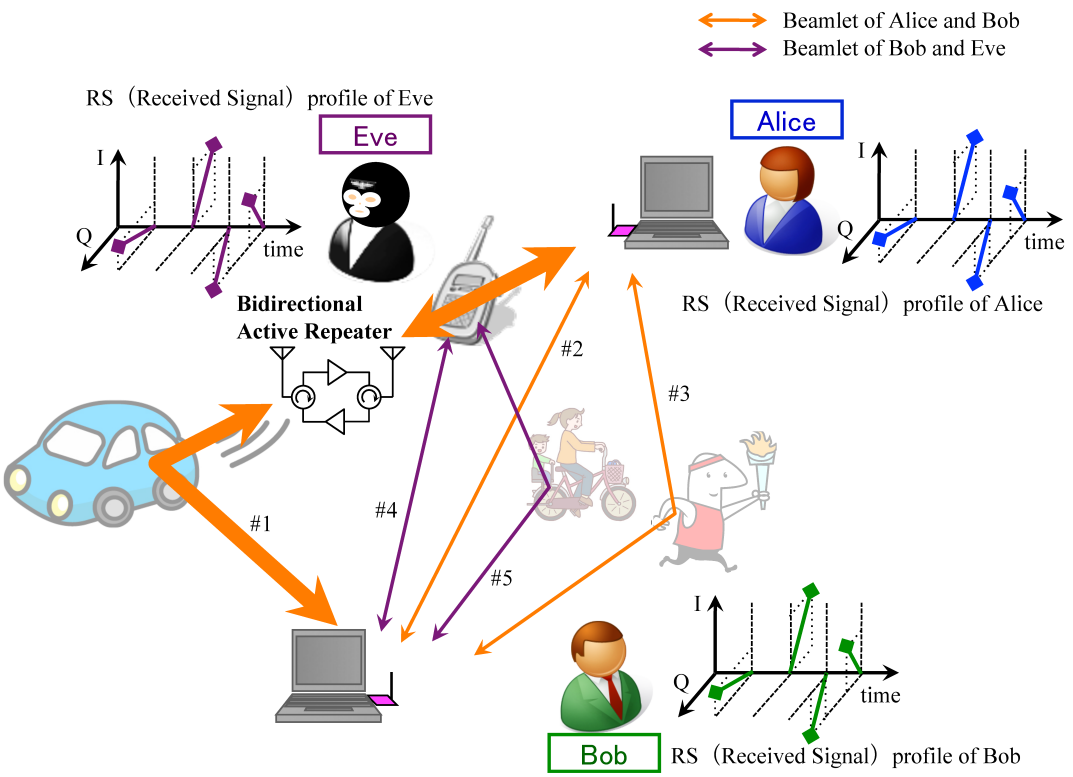



図 2.4　Active eavesdropping scheme by Duplex Amplifier Repeater

される．この時，Eve が増幅した素波が他の素波に比べ振幅が十分大きい場合，正規局が得る RS 履歴は，Eve が増幅する任意の素波の時間変化に支配される．そして，Eve は自身が増幅した任意素波を傍受する事で，鍵推定を行なう．まとめると，この能動的盗聴法は受動的盗聴法でも述べた直接波問題の原理を応用した盗聴法である．能動的盗聴法の特長として，正規局が見通し外の伝搬環境の場合，正規局が直接波除去手法 [20] を用いた場合においても，安定して鍵を推定できる手法である．本論文での鍵の秘匿性評価において，能動的盗聴法を用いた場合，他の論文との鍵の秘匿性の比較が難しいため，本論文では本節での紹介のみとする．

## 2.4　秘密鍵の秘匿性評価指標

本節は無線秘密鍵生成共有方式で生成共有した鍵の秘匿性を評価する指標，秘匿条件付き相互情報量（Imac）と受信信号（RS）履歴相関係数を説明する．Imac は RS 履歴を離散値として秘匿性を評価する指標であり，一般的な鍵の秘匿性評価に用いられる．RS 履歴相関係数は RS 履歴を連続値として，秘匿性を評価する指標であり，鍵の秘匿性評価としてはあまり用いられない．本論文は RS 履歴の連続値で秘匿性を評価するため，RS 履

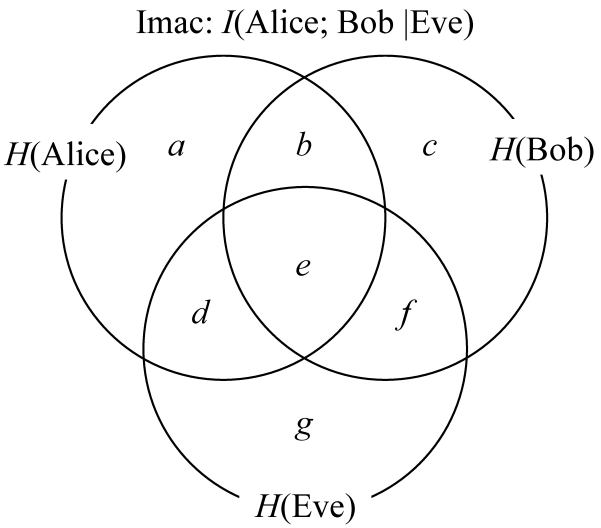



図 2.5　Information mutual on anti-tapping condition (Imac)

歴相関係数を用いる．そのため，Imac と RS 履歴相関係数の関係を明確し，RS 履歴相関係数から直感的に Imac が推定できるようにする．

### 2.4.1　秘匿条件付き相互情報量

無線秘密鍵生成共有方式により得られる秘密鍵の秘匿性評価指標として用いられる指標に，秘匿条件付き相互情報量（Information mutual on anti-tapping condition: Imac）[35] や鍵容量 [38][40] 等がある．どちらも概念は「第三者に盗まれていない正規局間のみで共有できている情報量」である．他の見方として，鍵 1bit あたり何 bit の情報が盗聴局に盗まれずに正規局間で共有できているかを示す指標である．鍵容量は上界と下界があり，Imac より厳密に秘密鍵の秘匿性を評価する．鍵容量の上界・下界が 0.3 以上の場合，上界，下界，Imac はほぼ一致する [22]．そして，鍵容量が 0.3 未満となる環境は鍵の生成効率が低いため非実用的である．すなわち，実用的環境下では鍵容量と Imac は一致するため，簡単化のためには Imac での評価が適当である．

Imac について，正規局 Alice と Bob および盗聴局 Eve が持つ情報量をベン図で示した図 2.19 を用いて説明する．Imac はベン図の領域 b に対応する情報量である．Imac は次式で与えられる．

$$\begin{aligned} \mathrm{Imac} &= I(\mathrm{Alice};\mathrm{Bob}|\mathrm{Eve}) && (2.1)\\ &= b \\ &= (b+a)-a \\ &= H(\mathrm{Alice}|\mathrm{Eve}) - \mathrm{H}(\mathrm{Alice}|\mathrm{Bob},\mathrm{Eve}) && (2.2) \end{aligned}$$

表 2.1　definition of key combination probability

| Alice | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|
| Bob | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| Eve | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |
| probabililty | $p_1$ | $p_2$ | $p_3$ | $p_4$ | $p_5$ | $p_6$ | $p_7$ | $p_8$ |

$I$ は情報量関数，$H$ はエントロピー関数を表す．「;」は AND（$I(x;y)$ 相互情報量），「,」は OR（$H(x,y)$ 結合エントロピー），「|」は条件（$H(x|y)$ 条件付きエントロピー）を表す．エントロピー関数および条件付きエントロピー関数は，

$$H(X) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) \tag{2.3}$$

$$\begin{aligned} H(Y|X) &= -\sum_{i=1}^{n} p(x_i) H(Y|x_i) \\ &= -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j)\log_2 p(y_j|x_i) \end{aligned} \tag{2.4}$$

$$H(Y|x_i) = -\sum_{j=1}^{m} p(y_j|x_i)\log_2 p(y_j|x_i) \tag{2.5}$$

$$p(y_j|x_i) = \frac{p(x_i, y_j)}{p(x_i)} \tag{2.6}$$

と定義する．$X$，$Y$ は確率変数を表しており，$x_i$，$y_j$ は，確率変数 $X$，$Y$ が取りうる値を表す（$i$，$j$ は整数）．n および m は確率変数が取りうる値の数を表す．また，演算の優先順位は，「,」＞「;」＞「|」と一般的に定められている．

上式を用いて $H(\text{Alice}|\text{Eve})$ および $H(\text{Alice}|\text{Bob},\text{Eve})$ を導出する．Alice，Bob および Eve が持つ鍵の組合せは表 2.1 で示す 8 通りである．それら組合せが取りうる確率は表 2.1 に示す $p_1, p_2, ..., p_8$ である．先ず盗聴されていない Alice が持つ情報量 $H(\text{Alice}|\text{Eve})$ を導出する．確率変数 (Alice|Eve) が取りうる値，およびその確率を，表 2.1 を用いて以下の行列 $\mathbf{P}(\text{Alice}|\text{Eve})$ で表す．

$$\begin{aligned} &\mathbf{P}(\text{Alice}|\text{Eve}) \\ &= \begin{bmatrix} p(\text{Alice}=0|\text{Eve}=0) & p(\text{Alice}=0|\text{Eve}=1) \\ p(\text{Alice}=1|\text{Eve}=0) & p(\text{Alice}=1|\text{Eve}=1) \end{bmatrix} \end{aligned} \tag{2.7}$$

$$= \begin{bmatrix} \dfrac{p_1+p_3}{p_1+p_3+p_4+p_7} & \dfrac{p_2+p_5}{p_2+p_5+p_6+p_8} \\ \dfrac{p_4+p_7}{p_1+p_3+p_4+p_7} & \dfrac{p_6+p_8}{p_2+p_5+p_6+p_8} \end{bmatrix} \tag{2.8}$$

これを条件付きエントロピー関数の式 2.5 に代入すると，

$$
\begin{aligned}
&H(\mathrm{Alice}|\mathrm{Eve}) \\
&= -p(\mathrm{Eve}=0)\mathrm{H}(\mathrm{Alice}|\mathrm{Eve}=0) - \mathrm{p}(\mathrm{Eve}=1)\mathrm{H}(\mathrm{Alice}|\mathrm{Eve}=1) \qquad (2.9)\\
&= (p_1+p_3+p_4+p_7)\left(\frac{p_1+p_3}{p_1+p_3+p_4+p_7}\right)\log_2\left(\frac{p_1+p_3}{p_1+p_3+p_4+p_7}\right) \\
&\quad +(p_1+p_3+p_4+p_7)\left(\frac{p_4+p_7}{p_1+p_3+p_4+p_7}\right)\log_2\left(\frac{p_4+p_7}{p_1+p_3+p_4+p_7}\right) \\
&\quad +(p_2+p_5+p_6+p_8)\left(\frac{p_2+p_5}{p_2+p_5+p_6+p_8}\right)\log_2\left(\frac{p_2+p_5}{p_2+p_5+p_6+p_8}\right) \\
&\quad +(p_2+p_5+p_6+p_8)\left(\frac{p_6+p_8}{p_2+p_5+p_6+p_8}\right)\log_2\left(\frac{p_6+p_8}{p_2+p_5+p_6+p_8}\right) \qquad (2.10)
\end{aligned}
$$

が得られる．次に確率変数 (Alice|Bob, Eve) が取りうる値，およびその確率を，行列 $\mathbf{P}(\mathrm{Alice}|\mathrm{Bob},\mathrm{Eve})$ で表すと，

$$
\begin{aligned}
&\mathbf{P}(\mathrm{Alice}|\mathrm{Bob},\mathrm{Eve}) \\
&= \begin{bmatrix} p(0|0,0) & p(0|0,1) & p(0|1,0) & p(0|1,1) \\ p(1|0,0) & p(1|0,1) & p(1|1,0) & p(1|1,1) \end{bmatrix} \qquad (2.11)\\
&= \begin{bmatrix} \dfrac{p_1}{p_1+p_4} & \dfrac{p_2}{p_2+p_6} & \dfrac{p_3}{p_3+p_7} & \dfrac{p_5}{p_5+p_8} \\ \dfrac{p_4}{p_1+p_4} & \dfrac{p_6}{p_2+p_6} & \dfrac{p_7}{p_3+p_7} & \dfrac{p_8}{p_5+p_8} \end{bmatrix} \qquad (2.12)
\end{aligned}
$$

となる．これを条件付きエントロピー関数の式 2.5 に代入すると，

$$
\begin{aligned}
&H(\mathrm{Alice}|\mathrm{Bob},\mathrm{Eve}) \qquad (2.13)\\
&= (p_1+p_4)\left(\frac{p_1}{p_1+p_4}\right)\log_2\left(\frac{p_1}{p_1+p_4}\right) + (p_1+p_4)\left(\frac{p_4}{p_1+p_4}\right)\log_2\left(\frac{p_4}{p_1+p_4}\right) \\
&+ (p_2+p_6)\left(\frac{p_2}{p_2+p_6}\right)\log_2\left(\frac{p_2}{p_2+p_6}\right) + (p_2+p_6)\left(\frac{p_6}{p_2+p_6}\right)\log_2\left(\frac{p_6}{p_2+p_6}\right) \\
&+ (p_3+p_7)\left(\frac{p_3}{p_3+p_7}\right)\log_2\left(\frac{p_3}{p_3+p_7}\right) + (p_3+p_7)\left(\frac{p_7}{p_3+p_7}\right)\log_2\left(\frac{p_7}{p_3+p_7}\right) \\
&+ (p_5+p_8)\left(\frac{p_5}{p_5+p_8}\right)\log_2\left(\frac{p_5}{p_5+p_8}\right) + (p_5+p_8)\left(\frac{p_8}{p_5+p_8}\right)\log_2\left(\frac{p_8}{p_5+p_8}\right)
\end{aligned}
$$

が得られる．そして，式 2.10，2.10 を Imac の式 2.2 に代入する事で Imac を導出することができる．本論文は RS 履歴の秘匿性を評価したい．しかしながら，上記 Imac の導出式より，Imac は離散値である秘密鍵の秘匿性を評価することはできるが，連続量である RS 履歴の秘匿性を評価することは難しい．そこで，連続量である RS 履歴の秘匿性を示すのに受信信号履歴相関係数を用いる．

### 2.4.2　受信信号履歴相関係数

両正規局が共有できる鍵情報を示す指標として正規局間 RS 履歴相関係数 $\rho_{ab}$

$$\begin{aligned}
&\rho_{ab} = \rho(\dot{R}_a, \dot{R}_b) \\
&\rho(x, y) = \\
&\frac{|E[xy^*] - E[x]E[y^*]|}{\sqrt{(E[|x|^2] - |E[x]|^2)(E[|y|^2] - |E[y]|^2)}} \\
&E[\dot{R}] = \frac{1}{m}\sum_{h=1}^{m} R_h
\end{aligned} \tag{2.14}$$

を定義する．$*$ は複素共役である．$R_h$ は第 h 番目の受信信号の値を示しており，その受信信号系列を $\dot{R}$ とする．上記式は Alice と Bob の RS 履歴 $\dot{R}_a$，$\dot{R}_b$ の相互相関係数の絶対値である．これを本論文では単に相互相関係数と呼ぶ．$E[\dot{R}]$ は RS の履歴平均，m は鍵長を示す．

正規局が持つ鍵情報の内，盗聴局が推定できた鍵情報を示す指標として正規盗聴局間 RS 履歴相関係数 $\rho_e$

$$\rho_e = \max(\rho(\dot{R}_a, \dot{R}_e), \rho(\dot{R}_b, \dot{R}_e)) \tag{2.15}$$

を定義する．上記式は Alice と Eve の RS 履歴相関係数 $\rho(\dot{R}_a, \dot{R}_e)$，および Bob と Eve の RS 履歴相関係数 $\rho(\dot{R}_b, \dot{R}_e)$ の内，より多く鍵情報が得られた方，つまり，相関係数が高い方を正規盗聴局間 RS 履歴相関係数とした．

定義した RS 履歴相関係数と Imac の関係について考察する．Imac は鍵 1bit あたり何 bit の情報が盗聴局に盗まれずに正規局間で共有できているかを示す指標である．そして，図 2.19 のベン図より，本節で定義した $\rho_{ab}$ は領域 b+e を，$\rho_e$ は領域 d+e or f+e を定性的に表している．従って，$\rho_{ab}$ と $\rho_e$ を両方同時に考慮する事により，定性的に Imac を表すことができる．具体例として，RS 履歴を中央値で 2 値化処理し秘密鍵を生成した場合における，RS 履歴相関係数と Imac の関係を図 2.6 に示す．図 2.6 より，$\rho_{ab}$ が大きく，$\rho_e$ が小さい場合に Imac が向上する事がわかる．これは，ベン図を用いた RS 履歴相関係数と Imac の定性的な振る舞いと一致する．

## 2.5　伝搬環境モデル

本節は第 4 章の無線秘密鍵生成共方式のシミュレーションで用いる伝搬環境モデルを定義する．使用するモデルは 2.5.1 節の送受素波対応モデルと 2.5.2 のレイトレーシング法を用いた長方形部屋伝搬環境モデルである．送受素波対応モデルは普遍性のある伝搬環境

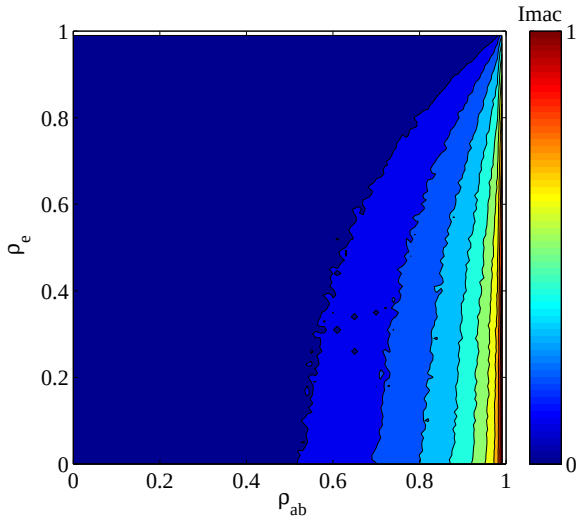



図 2.6　Relationship of Imac and RS profile correlation

モデルであり，第 4 章で得られる結論に普遍性を持たせるために用いる．レイトレーシング法を用いた長方形部屋伝搬環境モデルは，送受素波対応モデルで得られた結果検証のために，より実際の伝搬環境に近いモデルとして扱う．

### 2.5.1　送受素波対応伝搬環境モデル

簡素でかつ普遍的な伝搬環境を表す送受素波対応 (Transmit-Receive Beamlet Correspondence: TRBC) 伝搬環境モデルを提案，説明する．TRBC 伝搬環境モデルは図 2.7 に示す 2 次元伝搬環境を仮定し，Alice が放射する素波と，周囲環境の影響を受け Bob に到来する素波が 1 対 1 の関係にある．Bob への到来波は散乱や反射の影響を受けない直接波と，影響を受ける反射波の 2 種類に分かれる．反射波の伝搬特性は文献 [74]-[77] を参考に，振幅値一定，位相シフト $\phi_i$ 一様乱数とする．$i$ は図 2.7 に示す素波の番号である．以上を踏まえ Alice および Bob の RS を以下の R で表す．

$$
\begin{aligned}
R &= \lambda_d D(\alpha_0) E_{iso}(P_t) l_e \\
&\quad + \sum_{i=1}^{M-1} \frac{\lambda_r \exp(j\phi_i)}{\sqrt{M-1}} D(\alpha_i) E_{iso}(P_t) l_e \\
&\quad + n_I + j n_Q \\
\lambda_d &= \sqrt{\frac{K}{K+1}}, \quad \lambda_r = \sqrt{\frac{1}{K+1}} \\
K &= \frac{P_d}{P_r}
\end{aligned}
\tag{2.16}
$$

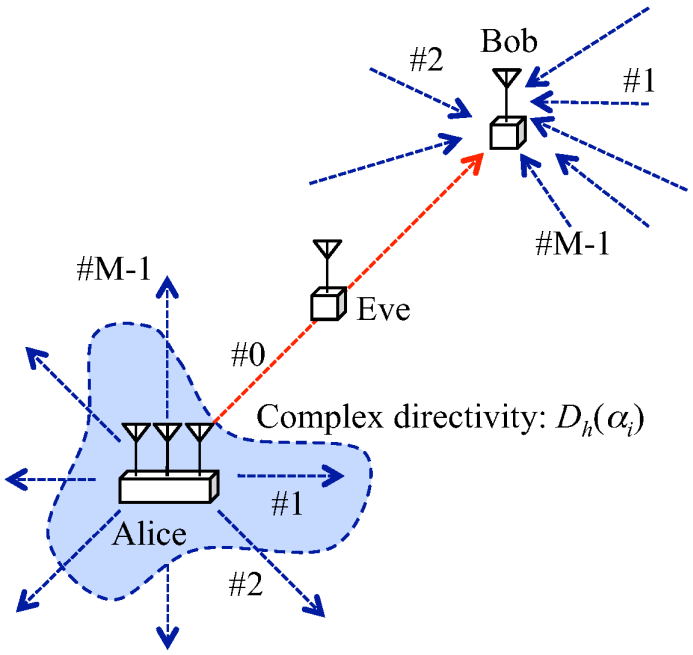
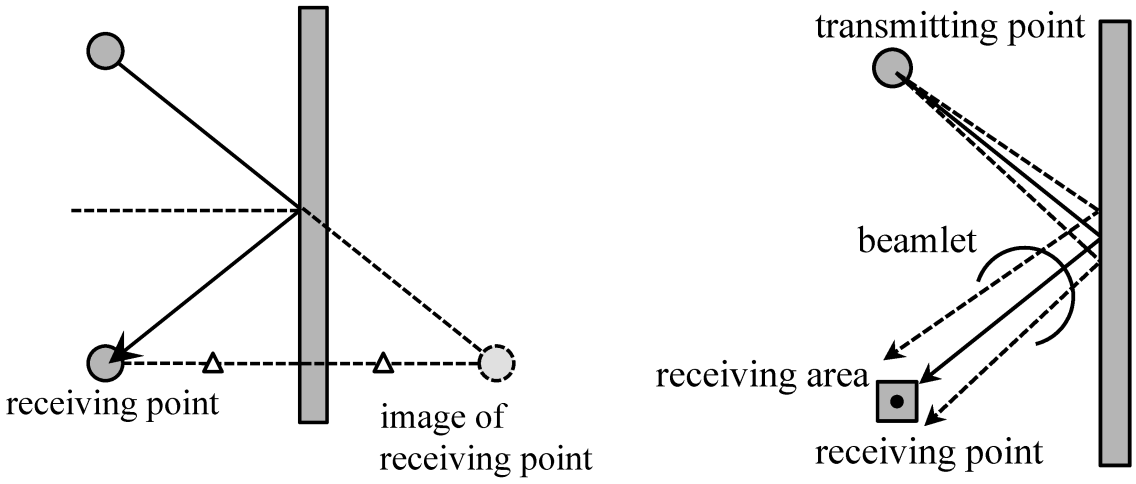



図 2.7　TRBC propagation model

$l_e$ はアンテナ有効長，$D(\alpha_i)$ は $\alpha_i$[rad] 方向のアンテナ指向性（対象のアンテナと等方性アンテナの電界比）を表す．$E_{iso}(P_t)$ は送信電力 $P_t$ を与えたときの等方性アンテナから放射される，受信地点の電界を表している．$\lambda_d$，$\lambda_r$ は直接波と反射波それぞれの伝搬路係数の規格化振幅値を表している．$P_d$ は直接波の平均電力を示しており，$P_r$ は反射波の総和によって形成されるレイリー波の平均電力を示している．そして，$P_d$ と $P_r$ の比 K を K 因子と呼ぶ．式 (2.16) の右辺 1 行目は直接波の受信信号を示している．式 (2.16) の右辺 2 行目は全ての反射波の受信信号の和を示しており，$M$ は素波の数を表す．右辺 3 行目は，受信局の白色ガウス雑音を示しており，$n_I$，$n_Q$ は平均 0，分散 $\sigma_n^2$ の正規乱数である．上式より，伝搬環境の性質を決定するパラメータは K 因子および雑音電力 $\sigma_n^2$ である．

### 2.5.2　レイトレーシング法

実際の伝搬環境に近いモデルをベースとして，無線秘密鍵生成共有方式のシミュレーション解析を行なうため，電波伝搬解析シミュレータであるレイトレーシング法を導入する [76]-[82]．レイトレーシング法は電波を幾何学的なレイ（光線）としてとらえ，送受信点間にある複数の伝搬経路を，直接波，反射波，回折波等からなるレイとして近似的にモデル化し，その合成として受信信号を求める手法である．レイトレーシング法を用いた受信信号を算出する手順は




(a) imaging method　(b) launching method

図 2.8　Ray tracing model

step 1 幾何学に基づく伝搬経路の推定
step 2 反射点，回折点における反射係数，回折係数の計算
step 3 それら係数およびフリスの伝搬公式により導出した全てのレイの合成による受信信号の算出

となる．以下にそれぞれのステップについて，計算方法について詳細を述べる．その際，本論文で解析対象とする伝搬環境モデルは，2 次元長方形部屋環境を想定しているため，回折現象は計算対象外とする．

送信点から受信点までのレイを幾何学に基づく方法として，イメージング法とローンチング法がある．それぞれの概念を図 2.8 に示す．

イメージング法は送信点，受信点および考慮する全ての反射面，回折面の組合せから，幾何学的に反射点と回折点を求める．具体例として図 2.8(a) より，送信点と受信点を一回反射で結ぶレイの反射点と伝搬距離を導出する．正規の受信点を，反射する壁を挟んで線対称の位置に鏡像の受信点を配置し，正規の送信点と鏡像の受信点を直線で結ぶ．反射する壁と直線が交わる座標点が，反射点となる．また，直線の長さが伝搬距離になる．後述するローンチング法と比べ，伝搬距離や反射点を厳密に求めることができる．しかし，送信点，受信点，全ての反射面，回折面の組合せに対して，レイを探索する必要があるため，複雑な伝搬路モデルにおいては膨大な計算時間がかかる．

ローンチング法は，図 2.8(b) に示すように送信点から一定の角度毎に離散的にレイを発射させ，その軌跡を逐次追跡して受信点に到達するレイを探索する．このとき，離散的な角度でレイを発射するため，受信点ちょうどの座標にレイが到着する事は不可能である．従って，受信点の周辺に受信エリアを定義し，そのエリア内に到達したレイを受信したレ

イと見なす．この方法は複雑な伝搬環境においても高速にレイを探索することができる．しかしながら，伝搬距離や，反射点，回折点等に誤差が含まれる問題がある．前述にもあるように，解析対象とする伝搬環境モデルは 2 次元長方形部屋環境であるため，本論文はイメージング法を用いて，伝搬経路の推定を行なう．

反射係数の計算式を示す．文献 [78] より，媒質 1（$\mu_1, \epsilon_1, \sigma_1$）から媒質 2（$\mu_2, \epsilon_2, \sigma_2$）へ電波が入射する場合の反射係数 $R$ は

$$R = \frac{\mu_2 \sin\theta - \mu_1\sqrt{n_{12}^2 - \cos^2\theta}}{\mu_2 \sin\theta + \mu_1\sqrt{n_{12}^2 - \cos^2\theta}}$$
$$n_{12} = \sqrt{\frac{\mu_2}{\mu_1}}\sqrt{\frac{\epsilon_2 - j\sigma_2/\omega}{\epsilon_1 - j\sigma_1/\omega}}$$

と表せる．$\theta$ は入射角 [rad]，$\omega$ は入射波の角周波数 [rad/sec] である．$n_12$ は媒質 1 に対する媒質 2 の比複素屈折率である．本論文では，2 次元伝搬路を想定しているため，偏波は垂直偏波のみを考慮した反射係数 $R$ の式を記述している．しかし，3 次元空間を想定するためには，偏波の向きを考慮したベクトル計算が必要である．

最後に，反射係数および電波伝搬損失を考慮した各レイの受信信号およびその合成信号を算出する [79]．送信点から放射された電波において，送信点から方位角 $\alpha_t$[rad]，距離 $d$[m] 離れた点における電界 $E_1$[V/m] は，

$$E_1 = \frac{D_t(\alpha_t)E_0(P_t)}{d}e^{-jkd}$$
$$E_0 = \sqrt{30P_t} \tag{2.17}$$

である．k は波数，$D_t$ は送信アンテナの複素指向性であり，送信アンテナが放射する電界を等方性アンテナの放射電界で正規化した物である．$E_0(P_t)$ は送信放射電力 $P_t$[W]，距離 1m 離れた点における，等方性アンテナの放射電界である．送信点から距離 $d$ 離れた受信点に電界 $E_1$ が方位角 $\alpha_r$[rad] から到来したとき，受信アンテナが得ることができる受信信号 $v_r$[V] は

$$v_r = E_1 l_e(\alpha_r)$$
$$l_e = \sqrt{\frac{\lambda^2}{4\pi}}D_r(\alpha_r) \tag{2.18}$$

である．$l_e$[m] はアンテナ有効長，$D_r$ は受信アンテナの複素指向性である．以上の式に反射係数 R を考量することにより，送信電力 $P_t$ における受信信号 $v_r$ は以下の式が導き

だせる．

$$v_r = \sum_{i=1}^{M} E_{1,i}(\alpha_{t,i}) l_e(\alpha_{r,i})$$

$$E_{1,i}(\alpha_{t,i}) = \frac{\sqrt{30P_t} D_t(\alpha_{t,i})}{d_i} \prod_{j=1}^{N_i} R_{i,j} e^{-jkd_i}$$

$$l_e(\alpha_{r,i}) = \sqrt{\frac{\lambda^2}{4\pi}} D_r(\alpha_{r,i})$$

$M$ は素波の数であり，$N$ は各素波の反射面で反射した回数である．

## 2.6 可変指向性アンテナモデル

本節は第 4 章の無線秘密鍵生成共方式のシミュレーションで用いる伝搬環境モデルを定義する．使用するモデルは 2.6.1 節の正規乱数アンテナモデルと 2.6.2 のフェーズドアレーモデルである．正規乱数アンテナモデルは普遍性のある可変指向性アンテナモデルであり，第 4 章で得られる結論に普遍性を持たせるために用いる．フェーズドアレーモデルは，正規乱数アンテナモデルで得られた結果検証のために，実際の可変指向性アンテナモデルとして扱う．

### 2.6.1 正規乱数アンテナモデル

簡素でかつ普遍的な可変指向性アンテナモデルを定義する．通常，アンテナが形成可能な指向性パタンはアンテナの構造に依存してしまう．故に，任意のアンテナを定義し，指向性を算出する手段は，普遍性があるとは言いにくい．従って，形成可能な指向性パタンが構造に依存しない多様な指向性パタンが得られるよう，可変指向性アンテナモデルの指向性の式は

$$D_h(\alpha_i) = x_{h,i} + jy_{h,i} \tag{2.19}$$

と表す．$x_{h,i}$，$y_{h,i}$ は互いに独立な平均 0，分散 1 の正規乱数である．正規乱数を用いることにより，指向性について振幅成分をレイリー確率密度分布と，位相成分を一様乱数と見なすこともできる．h は指向性パタンのインデックスを示す．式 2.19 で得られる指向性パタンセットは等価的にある 1 種の可変指向性アンテナモデルが形成可能な指向性パタンといえる．指向性パタンセットとは鍵を形成するときに用いる，図 2.2 に示す指向性パタン A,B,C の集合を示している．このときの得られる指向性パタンのセットについて，各指向性パタンは放射電力の変動を含む．放射電力の変動は，可変指向性アンテナの指向性切り替えにより生じる給電系との反射係数変動を表す．

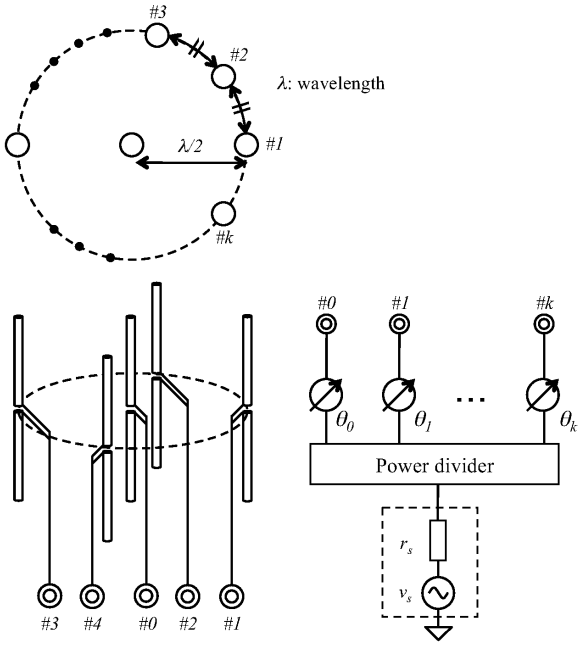



図 2.9　Configuration of Alice's phased array

### 2.6.2　フェーズドアレーモデル

実用性のある可変指向性アンテナとして，本論文はフェーズドアレーを想定する．想定するフェーズドアレーの構造を図 2.9 を用いて説明する．アンテナ構造は半径「半波長」となる円の中心および円周上に半波長ダイポール素子を配置したものである．それら素子の間の電磁界結合は考慮しない．そして，各素子の入力インピーダンスを電源の内部インピーダンス $r_s$ と同じとし，各素子の移相器の変化によらず，常にインピーダンス整合が取れているとする．必要とするアンテナの素子数により円周上のダイポール素子を調整，配置する．

## 2.7　本章の結論

本章は第 4 章で用いる無線秘密鍵生成共有方式の鍵生成共有シミュレーターを構築するための基本知識について記述した．

2.1 節では，可変指向性アンテナを用いた無線秘密鍵生成共有方式の基本原理を記述した．本方式は「電波伝搬の相反性（線形性）」「マルチパスフェージング」「電波伝搬の空間的局所性」の 3 つの電波伝搬の原理を駆使することで，正規局は互いに乱数性を持つ同じ RS 履歴を安全に共有できる．また，電波伝搬の原理と指向性パタンの変化の相乗効果

で鍵の秘匿性および生成効率の向上する．2.2 節では，本方式を用いて実際に行なわれる秘密鍵生成共有の手順について説明した．鍵生成共有の手順は第一フェーズの RS 履歴の生成共有と第二フェーズの信号処理に大きく分けることができ，本論文では第一フェーズの RS 履歴の生成共有までとした．2.3 節は，鍵の安全性を評価する上で重要な秘密鍵の盗聴手法を説明した．盗聴には受動的盗聴法と能動的盗聴法があり，本論文は受動的盗聴法を用いた鍵の安全性評価を採用した．2.4 節は，2.2 節で記述した RS 履歴生成共有に関して，その秘匿性を評価する指標について定義した．2.5 節および 2.6 節は，第 4 章で鍵の秘匿性評価のための無線秘密鍵生成共有方式の鍵生成共有シミュレーションに用いる伝搬環境モデルと可変指向性アンテナモデルについて定義した．

# 第 3 章

# 秘匿性を高める可変指向性アンテナの設計指標の提案

本章では無線秘密鍵生成共有方式の鍵の秘匿性を高めるアンテナを設計する際に，その指針となる指標を提案する．別の見方としては，可変指向性アンテナの性能を評価する指標ともいえる．無線秘密鍵生成共有方式に用いる可変指向性アンテナは，指向性パタンを変化させる事で電波のゆらぎを起こすことを目的として使われる．具体的には指向性の方位角による変動および電気的パラメータによる変動よりに電波のゆらぎは起こる．指向性の方位角による変動は，電波のゆらぎを形成する各素波の空間ゆらぎに影響を与える．指向性の電気的パラメータによる変動は，各素波の時間ゆらぎに影響与える．つまり，可変指向性アンテナは指向性が方位角および電気的パラメータ領域において，多様に変化する事が重要であると言える．

本論文は指向性の変化を示す指標として，大きく 2 種類の評価指標を提案する．3.1 節では，方位角領域，電気パラメータ領域（指向性を切り替える電気的パラメータの事 ex. 移相器，スイッチング素子）において指向性が変化に富んでいることを示す指標を，指向性の複雑性評価指標として提案する．第 3.2 節では，方位角領域，パラメータ領域において指向性が多様（独立）であることを示す指標を，指向性の多様性評価指標として提案する．

## 3.1　指向性の複雑性評価指標

方位角領域および電気パラメータ領域において，指向性が変化に富んでいることを示す指標として，指向性の複雑性評価指標を提案する．方位角領域における複雑性指標は指向性パタンの特徴量を抽出しているとも考えられる．それゆえ指向性パタンを変化させるための，最適な電気パラメータを特徴量から見出すことができる．以上より方位角領域にお

ける複雑性指標は，鍵の秘匿性向上のための評価指標と電気パラメータの最適設計の 2 通りの用途が期待できる．従って本論文では特に方位角領域における指向性の複雑性評価指標を提案する．

### 3.1.1　エンドファイア・ブロードサイド比（EBR）

指向性の方位角分布を簡易的に表す指標として，エンドファイア・ブロードサイド比（Endfire to Broadside Ratio: EBR）を定義する．EBR はエンドファイア方向（方位角 0deg と 180deg の 2 方向を中心に ±45deg の範囲）の放射電力と，ブロードサイド方向（方位角 90deg と 270deg の 2 方向を中心に ±45deg の範囲）の放射電力の比を表した物である．EBR は次式で表される．

$$\mathrm{EBR} = 10\log_{10}\frac{\int_{-\pi/4}^{\pi/4}|\mathrm{D}(\phi)|^2\mathrm{d}\phi + \int_{3\pi/4}^{5\pi/4}|\mathrm{D}(\phi)|^2\mathrm{d}\phi}{\int_{\pi/4}^{3\pi/4}|\mathrm{D}(\phi)|^2\mathrm{d}\phi + \int_{-3\pi/4}^{-\pi/4}|\mathrm{D}(\phi)|^2\mathrm{d}\phi} \quad [\mathrm{dB}]$$
$$(-\infty < \mathrm{EBR} < \infty)$$

$D(\phi)$ は方位角 $\phi$ の複素指向性を表している．EBR $<$ 0dB のとき指向性はブロードサイドグループに属し，EBR $>$ 0dB のときエンドファイアグループに属する．

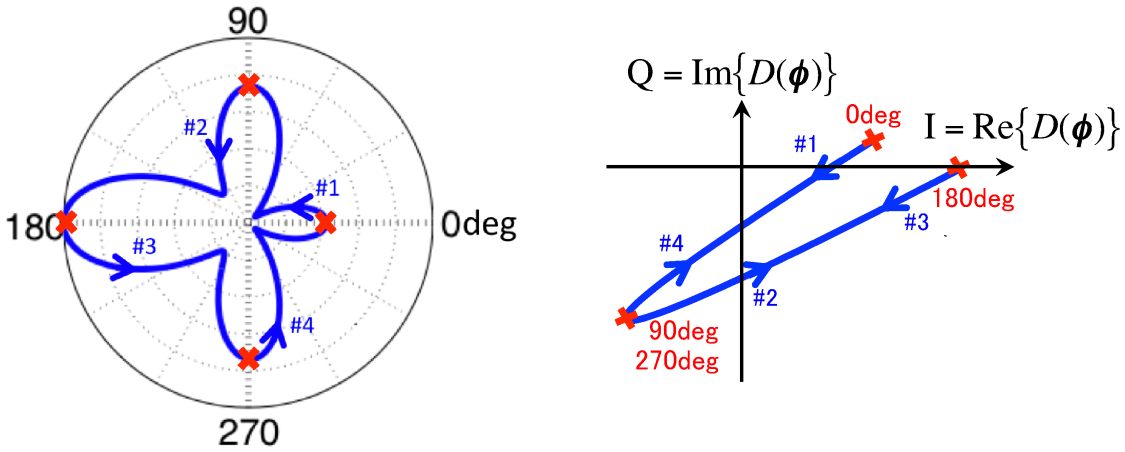
### 3.1.2　軌跡長（LLL）

方位角を 0 から 360 度変化させた水平面内複素指向性の振幅と位相の変化量を示す指標として軌跡長（Locus Line Length: LLL）を定義する．図 3.1 に示す指向性の軌跡を例に LLL を説明する．可変指向性アンテナは図 3.1(a) に示された指向性パタンを形成する．これを図 3.1(b) にある複素指向性の実部を横軸，虚部を縦軸とする I-Q 平面上に，複素指向性を射影する．そして，図 3.1(b) にある指向性軌跡の長さを LLL と定義しする．式を以下に示す．

$$\mathrm{LLL} = \frac{\left\{\int_0^{2\pi}\left|\frac{dD(\phi)}{d\phi}\right|d\phi\right\}^2}{\int_0^{2\pi}|D(\phi)|^2 d\phi} \tag{3.1}$$

LLL は水平面内放射電力で正規化されている．

LLL の値が持つ物理的意味について，LLL が 0 に近いほど指向性パタンはオムニ形状である．大きいほど指向性パタンは複雑な形状である．具体的には，サイドローブ数が大きい指向性パタン，および任意の方向に鋭いビームを向ける指向性パタンの LLL は大きな値になる．




(a) Directivity pattern.　(b) Directivity on I-Q plane.

図 3.1　Directivity locus example.

### 3.1.3　累積ビーム幅（CBW）

方位角を 0 から 360 度変化させた水平面内複素指向性の振幅と位相の分散を示す指標として累積ビーム幅（Cumulative Beam Width: CBW）を定義する．定義する CBW は

$$\begin{aligned} \mathrm{CBW} &= 2\pi \frac{|\langle D(\phi)\rangle|^2}{\langle |D(\phi)|^2\rangle} \\ &= \frac{|\int_0^{2\pi} D(\phi)d\phi|^2}{\int_0^{2\pi} |D(\phi)|^2 d\phi} \quad [\mathrm{rad}] \\ &\quad (0 \le \mathrm{CBW} \le 2\pi) \end{aligned}$$

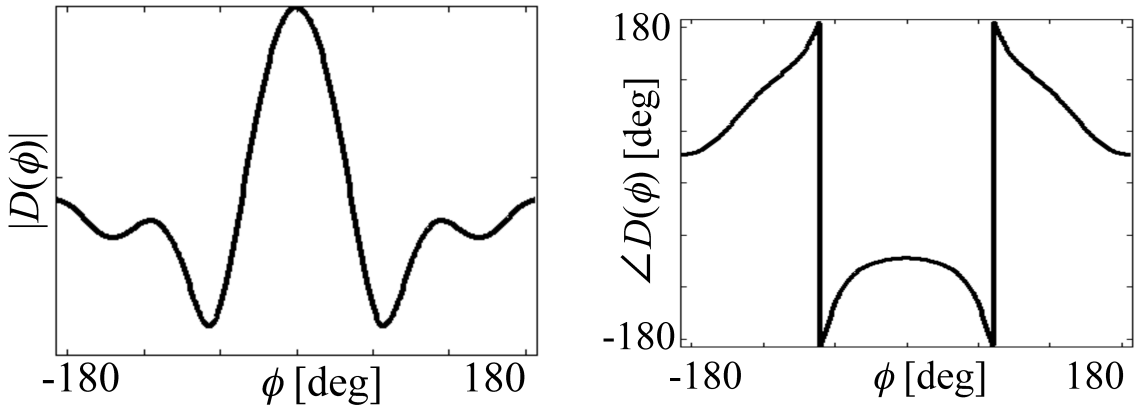
とする．$\langle D(\phi)\rangle$ は平均複素指向性である．分子は複素指向性の分散であり，指向性の放射電力で正規化している．$2\pi$ を乗算することで式を簡単化しており，結果単位を rad とした．

CBW の値が持つ物理的意味について説明する．図 3.2 を用いて説明する．

1)　図 3.2(a) の指向性の振幅値においてその変化が大きい，例えば指向性の半値ビーム幅が狭いアンテナほど CBW の値は 0 rad に近づく．

2)　図 3.2(b) の指向性の位相において，$\phi$ が 0 から $2\pi$ まで変化した時に振幅一定，位相が 0 から $2\pi$ で一様に変化するアンテナでは CBW の値は 0 rad である．

3)　指向性が全方位一定のアンテナでは CBW の値は $2\pi$rad である．




(a) Magnitude of directivity　　(b) Phased of directivity

図 3.2　Directivity magnitude and phased example

## 3.2　指向性の多様性評価指標

指向性が方位角領域および電気パラメータ領域において変化の多様性（独立性）を示す指標，指向性の多様性評価指標を提案する．前節の指向性の複雑性は，指向性の変化の程度について定量的に示す物であった．本節の指向性の多様性は，指向性の変化の質について定量的に示す事が目的である．その理由について，盗聴局は正規局の指向性の変化の一部を得ることができると考えられる．そのため，ただ闇雲に指向性を変化させた場合において，盗聴局に指向性の変化に特徴を見出す可能性がある．結果，指向性の変化の一部から全ての指向性の変化を推定され，最後には電波のゆらぎを推測される恐れがある．故に，指向性の変化の一部から全ての指向性の変化を推定されないよう，各素波の時間的ゆらぎ，空間的ゆらぎが互いに独立となるような指向性の変化を定量的に評価する．

### 3.2.1　制御パラメータ領域指向性相関係数（PDC）

電気パラメータ領域における指向性の多様性（独立性）を示す指標である制御パラメータ領域指向性相関係数（Parameter Domain Correlation: PDC）について説明する．

PDC は秘匿性の要因である各素波のゆらぎに着目する．素波とは，送信局から様々な方向に放射された電波のうち，ある 1 つの伝搬路を通って受信局に到来する電波の事であり，複素ベクトルである．素波のゆらぎとは，Alice の指向性パタンが切り替わることによる素波の変化である．正規局が持つ RS 履歴は，各素波のゆらぎのベクトル和である．一方，盗聴局は，正規局が受信する素波のうち任意の 1 つを分離，傍受することができるような鋭い指向性を有すると仮定する．正規局が受信する，全ての到来方向からの素波のゆらぎが互いに独立（低相関性）である場合，正規局の RS 履歴と各素波のゆらぎは低相

関である．従って，盗聴局は 1 つの素波のゆらぎを傍受しても，正規局の RS 履歴を推定することは困難である．また，盗聴局は正規素波を全て傍受することは困難である．何故ならば電波伝搬の空間的局所性より，全ての素波を 1 台の盗聴局が受信するためには正規局と同じ位置で同時に素波を受信する必要があるが，これは現実的に困難である．または，複数台の盗聴局を正規局の周辺に配置し，それぞれが 1 つの素波を傍受するという案 [83] も考えられるが，これも現実的に困難であるといえる．一方で正規局が受信する各素波のゆらぎの相関性が高い場合，盗聴局は正規素波 1 つを傍受すれば鍵を推定できる．ゆえに指向性パタンが切り替わることによって得られる各素波の時間変動が互いに独立であれば盗聴局は鍵推定が困難となる．

そこで，代表的可変指向性アンテナであるフェーズドアレーおよびスイッチドビームの 2 種類を評価対象とし，各素波のゆらぎの独立性を高めるためのアンテナの指向性多様性指標 PDC を定義する．フェーズドアレーの PDC 評価について，例えば 3 素子フェーズドアレー（移相器が 2 つ）を対象とし，その移相器の性能が位相範囲が 0 から $2\pi$，位相刻みが $\pi/180$ とする．従って，3 素子フェーズドアレーが形成する指向性パタンの数 $N$ は，

$$\begin{aligned} N &= (\text{移相器の位相刻み数})^{(\text{移相器の数})} \\ &= 360^2 \\ &= 129600 \end{aligned}$$

となる．そして，3 素子フェーズドアレーが形成できる指向性を $D_h(h = 1, 2, ..., 129600)$ と定義したとき，任意 2 方位角の複素指向性の相互相関係数を

$$\rho_{pd}(\phi_i, \phi_j) = \frac{|\mathrm{C}(\phi_i, \phi_j)|}{\sqrt{\mathrm{C}(\phi_i, \phi_i)\mathrm{C}(\phi_j, \phi_j)}} \tag{3.2}$$

$$\mathrm{C}(\phi_i, \phi_j) = \frac{1}{N}\left[\sum_{h=1}^{N}\{D_h(\phi_i)D_h(\phi_j)^*\} - \frac{1}{N}\sum_{h=1}^{N}\{D_h(\phi_i)\}\sum_{h=1}^{N}\{D_h(\phi_j)^*\}\right]$$

と定義する．$\phi_i$ は第 i 番目の素波の方位角である．$C(\phi_i, \phi_j)$ は $D_h(\phi_i)$ と $D_h(\phi_j)$ の共分散である．スイッチドビームについて，切り替えができる指向性パタンの数を N 個と定義することにより，式 (3.2) から $\rho_{pd}$ を導出することができる．また，他の種類の可変指向性アンテナにおいても，形成できる指向性パタンを N 個の指向性パタンと離散的に定義することにより，$\rho_{pd}$ で評価できる．

$\rho_{pd}$ は 2 方向を対象とした評価指標である．しかし，各素波のゆらぎの独立性を示すには，アンテナが放射する素波の全方向において，$\rho_{pd}$ を示す必要がある．そこで，対象とする素波の数 $M$ の全ての組み合わせの $\rho_{pd}$ を示す

$$E[\rho_{pd}] = \frac{1}{M^2}\sum_{i=1}^{M}\sum_{j=1}^{M}\rho_{\mathrm{pd}}(\phi_i, \phi_j) \tag{3.3}$$

を定義する．これを PDC とする．$E[\rho_{pd}]$ の値が低いほど，アンテナ指向性は多様であり，無線秘密鍵生成共有方式の秘匿性を高め得ることが期待できる．

### 3.2.2　指向性パタン相関係数（ADC）

アンテナが形成可能な指向性パタンの多様性を示す指標である指向性パタン相関係数（ADC: Azimuth Domain Correlation）について述べる．前節の PDC が任意の 2 方向の方位角における指向性のパラメータ領域における相関性に対して，ADC は任意の 2 つの電気パラメータにおける方位角領域の指向性（指向性パタン）の相関性である．

ADC は鍵生成の要である指向性パタンの変化に着目する．無線秘密鍵生成共有方式は指向性パタンを切り替えることで電波のゆらぎを生み出し，秘密鍵を生成する．切り替える指向性パタンが相関性の高い形状であった場合，電波のゆらぎが小さくなる．そして，電波のゆらぎが小さいことは，指向性の一部から，他の指向性を推測しやすいと考えられる．従って，切り替える指向性パタンは互いに相関性が低い方が望ましい．

そこで，PDC 同様，代表的可変指向性アンテナであるフェーズドアレーおよびスイッチドビームの 2 種類を評価対象とし，指向性パタンの独立性評価指標 ADC の定義式を定義する．任意 2 種類の電気パラメータにおける指向性パタン $D_1$，$D_2$ の相互相関係数は，

$$|\rho_{ad(1,2)}|^2 = \frac{|\int_0^{2\pi} D_1(\phi)D_2^*(\phi)d\phi|^2}{\int_0^{2\pi}|D_1(\phi)|^2d\phi\int_0^{2\pi}|D_2(\phi)|^2d\phi} \tag{3.4}$$

となる．

上記指標は 2 種類 1 組の指向性パタンの独立性を評価する．無線秘密鍵生成共有方式で電波ゆらぎを起こすために，N 個の形成可能な指向性パタンから M 個の指向性パタンを選択する．選択した M 個の指向性パタンが互いに独立であることを示す式は

$$\begin{aligned}
&\min\max[|\rho_{ad}|] \\
&= \min_{\forall i,j}\left[\max\left\{\ |\rho_{ad(i,j)}|\ ;i<j\ \right\}\right] \\
&= \min_{\forall i,j}[\max\{|\rho_{ad(1,2)}|,|\rho_{ad(1,3)}|,...,|\rho_{ad(1,n)}|,|\rho_{ad(2,3)}|,...,|\rho_{ad(2,n)}|,...,|\rho_{ad(n-1,n)}|\}] \\
&\quad (i,j=\text{directivity index})
\end{aligned} \tag{3.5}$$

となる．これを ADC とする．上記式は，M 個の指向性パタンの組合せの中で，最も指向性パタンの相関性が高い指向性パタンペアの $|\rho_{ad}|$ が最小となるように，N 個の指向性パタンの中から M 個の指向性パタンを選択した時の，$\max\left\{\ |\rho_{ad(i,j)}|\ ;i<j\ \right\}$ の値を示す．ADC が低い程，アンテナが形成可能な指向性パタンは多様であると言える．

## 3.3 本章の結論

本章は無線秘密鍵生成共有方式の秘匿性を向上が期待できる可変指向性アンテナの設計指標を提案した．提案したアンテナ設計指標は大きく分けて「指向性の複雑性評価指標」と「指向性の多様性評価指標」の 2 種類とした．

指向性の複雑性評価指標は，方位角領域において指向性が複雑に変化していることを示す指標として，EBR，LLL，CBW の 3 種類を提案した．EBR は指向性の方位角分布を示す指標として定義した．LLL は方位角領域において，複素指向性の振幅と位相の変化量を示す指標として定義した．CBW は方位角領域において，複素指向性の振幅と位相の分散を示す指標として定義した．

指向性の多様性評価指標は方位角領域および電気パラメータ領域において変化が多様（独立）であることを示す指標として，PDC，ADC の 2 種類を提案した．PDC は電気パラメータ領域における指向性の多様性（独立性）を示す指標として定義した．ADC は方位角領域における指向性（指向性パタン）の多様性を示す指標として定義した．

# 第 4 章

# アンテナ設計指標と秘匿性の関係

本章は第 3 章で提案した秘匿性を高めうる可変指向性アンテナの設計指標が，様々な伝搬環境下において有用であることを明らかにする．

4.1 節では提案した可変指向性アンテナの設計指標の変化が，無線秘密鍵生成共有方式の RS 履歴の秘匿性に与える影響を明らかにする．4.2 節では提案した可変指向性アンテナの設計指標が，RS 履歴の秘匿性を向上させるための可変指向性アンテナの設計指標に有用であるかを検証する．検証には 2 組のアンテナおよび伝搬環境モデルを用い，可変指向性アンテナの設計指針と RS 履歴の秘匿性の相関性を明らかにする．

## 4.1　アンテナ設計指標による鍵の秘匿性向上効果の期待値

本節は可変指向性アンテナが RS 履歴の秘匿性の伝搬環境特性に与える影響を調べる．始めに RS 履歴の秘匿性と伝搬環境特性の関係を TRBC 伝搬環境モデルを用いて示す．伝搬環境パラメータである「直接波対反射波電力比（K 因子）」と「受信信号電力対雑音電力比（Received signal to Noise Ratio: RNR）」が RS 履歴の秘匿性に与える影響を調べる．そして，TRBC 伝搬環境モデルを用いた RS 履歴の秘匿性と伝搬環境パラメータの関係が定性的にも正しいことを確認する．

次に可変指向性アンテナによる RS 履歴の秘匿性向上効果について，RS 履歴秘匿性の伝搬環境特性と可変指向性アンテナの関係から定義する．最後に可変指向性アンテナの性能の違いによる RS 履歴の秘匿性向上効果と伝搬環境特性を示すと共に，第 3 章で定義した各種アンテナ設計指標の秘匿性向上効果について明らかにする．

得られる可変指向性アンテナによる RS 履歴の秘匿性向上効果と伝搬環境特性の関係に普遍性を持たせるため，用いる可変指向性アンテナモデルおよび伝搬環境モデルは普遍性のあるモデルを採用する．アンテナモデルは 2.6.1 節で定義した正規乱数アンテナモデルを用いる．伝搬環境モデルは 2.5.1 節で定義した送受素波対応モデルを用いる．RS 履

歴の秘匿性は正規局間 RS 履歴相関係数および正規盗聴局間 RS 履歴相関係数の両方を用いる．

RS 履歴の生成共有および盗聴は図 2.2 の手順に従う．また盗聴局は図 2.7 に示す正規局間を結ぶ直線上に配置し直接波のみを傍受する．無線秘密鍵生成共有方式の RS 履歴生成共有シミュレーションの流れについて，

Step1)　K 因子および受信信号電力対雑音電力比 RNR を決定する．
Step2)　直接波放射角 $\alpha_0$ と反射波放射角 $\alpha_i (i=1,...,M-1)$ を，$[0, 2\pi\frac{1}{M}, ..., 2\pi\frac{M-1}{M}]$ の中から重ならないように無作為選択する
Step3)　素波の位相シフト $\phi_i$ を一様乱数で決める．
Step4)　500 種類の可変指向性アンテナから 1 つ選ぶ
Step5)　RS 履歴を生成共有する．
Step6)　全種類の可変指向性アンテナの RS 履歴を生成するまで Step4 に戻る．
Step7)　正規局場所の変更回数だけ，Step2 に戻る．

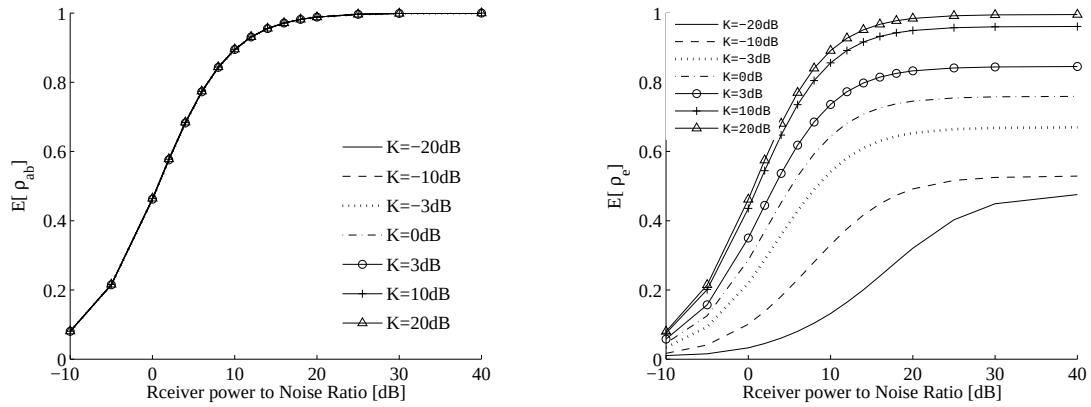
とする．

RS 履歴生成時における受信信号電力とは，Alice の指向性パタン切り替えにより正規局が得る受信信号電力の履歴を平均した値である．表 4.1 のシミュレーション諸元より，想定する可変指向性アンテナは 8 つの形成可能な指向性パタンをもったスイッチドビームアンテナである．形成可能な指向性パタンは正規乱数アンテナモデルにより与えられる．そして，想定する可変指向性アンテナを 500 種類用意する．鍵長，正規局場所変更回数は RS 履歴相互相関係数の値が十分収束する標本数とした．素波の数について，各素波の合成が仲上ライスフェージング伝搬環境を再現するよう素波の数を 18 とする [75]．受信信号対雑音電力比（Signal to Noise Ratio）の略称は一般的に SNR を用いるが，本論文の 4.2 節で送信電力対雑音電力比（Transmited signal to Noise Ratio: TNR）を用いるため，それとの区別するため RNR とする．

RS 履歴の秘匿性と伝搬環境特性の関係を図 4.1 に表す．縦軸の $E[\rho_{ab}]$ および $E[\rho_e]$ は，500 種類ある可変指向性アンテナが取りうる $\rho_{ab}$，$\rho_e$ を平均した値を示す．図 4.1(a) の結果より，$E[\rho_{ab}]$ は RNR が大きい程高い値を示す．これは，RNR が大きくなるにしたがい，雑音の振幅値が正規局の RS 履歴の振幅値より小さくなったためと考えられる．$E[\rho_{ab}]$ は K 因子に依存しないこともわかる．これは，RNR が変化しないならば，K 因子に依らず，RS 履歴の振幅値は変化しないためと説明できる．図 4.1(b) の結果より，$E[\rho_e]$ は RNR が大きい程高い値を示す．これは，RNR が大きくなるにしたがい，雑音の振幅値が RS 履歴の振幅値より小さくなったためと考えられる．$E[\rho_e]$ は K 因子が大きい程高い値を示す．K 因子が大きい程，直接波が RS 履歴の形成に強い影響を与えること，そして盗聴局が直接波を傍受していること，以上が $E[\rho_e]$ の上昇に繋がったと考えられる．以

表 4.1　Simulation parameter of the system in Clarke's model

| パラメータ | 記号 | 値 | 単位 |
|---|---|---|---|
| 素波の数 | | 18 | |
| 受信信号電力対雑音電力比 | RNR | -10 〜 40 | dB |
| 直接波対反射波電力比 | K | -20,-10,-3,0,3,10,20 | dB |
| 指向性パタンの数 | | 8 | |
| 可変指向性アンテナの数 | | 500 | |
| RS 履歴長 | | $8 \times 10^3$ | |
| 正規局場所の変更回数 | | 3000 | |




(a)RNR characteristic of $\rho_{ab}$.　(b)RNR characteristic of $\rho_e$

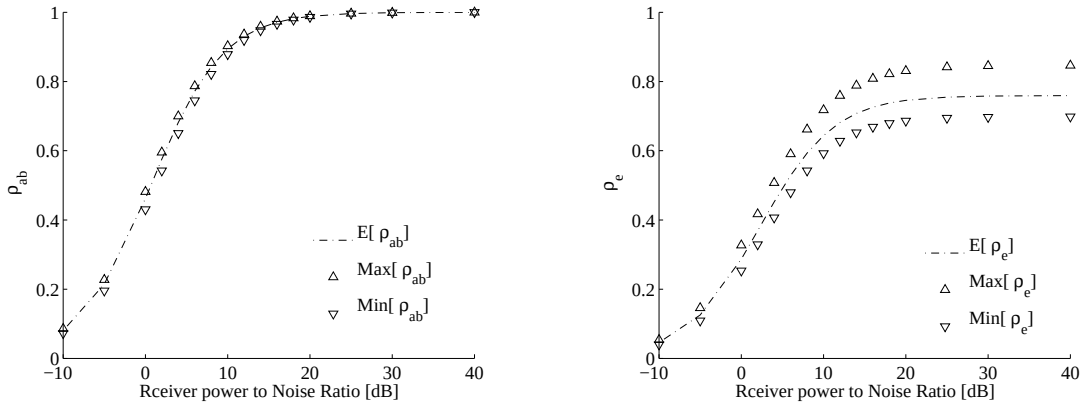
図 4.1　Relation of the system security to propagation properties.

上をまとめると，TRBC 伝搬環境モデルを用いた RS 履歴の秘匿性と伝搬環境特性の関係は，定性的にも正しいといえる．また，伝搬環境のパラメータにより様々な RS 履歴の秘匿性を表現できることからも，TRBC 伝搬環境モデルを用いた無線秘密鍵生成共有シミュレーションは有用であると言える．

次に，秘匿性向上効果について，図 4.2 の K 因子が 0dB の時の可変指向性アンテナの選択による RS 履歴秘匿性の伝搬環境特性から定義する．図 4.2 より，500 種類ある可変指向性アンテナがそれぞれ取りうる $\rho_{ab}$ について，最大を $\max[\rho_{ab}]$，最小を $\min[\rho_{ab}]$ とする．同様に，$\rho_e$ の最大を $\max[\rho_e]$，最小を $\min[\rho_e]$ とする．

図 4.2(a) より，指向性パタンの選択により，$E[\rho_{ab}]$ から $\max[\rho_{ab}]$ への $\rho_{ab}$ の向上がわずかに期待できる．この $\rho_{ab}$ 向上効果を

$$\rho_{ab,p-m} = (\max[\rho_{ab}] - E[\rho_{ab}])/E[\rho_{ab}] \tag{4.1}$$




(a)RNR characteristic of $\rho_{ab}$.　　(b)RNR characteristic of $\rho_e$

図 4.2　Relation of the system security to propagation for selecting a variable directivity antenna.

と定義する．$\rho_{ab,p-m}$ は大きい程，秘匿性の向上効果が大きい．図 4.2(b) より，指向性パタンの選択による $E[\rho_e]$ から $\min[\rho_e]$ への $\rho_e$ の低減は，RNR が大きいほど大きい．この $\rho_e$ 低減効果を

$$\rho_{e,p-m} = \frac{\min[\rho_e] - E[\rho_e]}{E[\rho_e]} \tag{4.2}$$

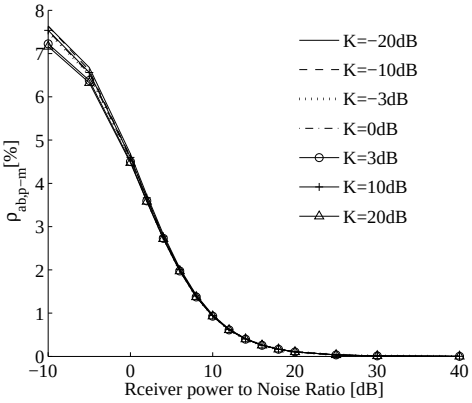
と定義する．$\rho_{e,p-m}$ は小さい程，秘匿性の向上効果が大きい．

### 4.1.1　指向性の複雑性指標による鍵の秘匿性向上効果

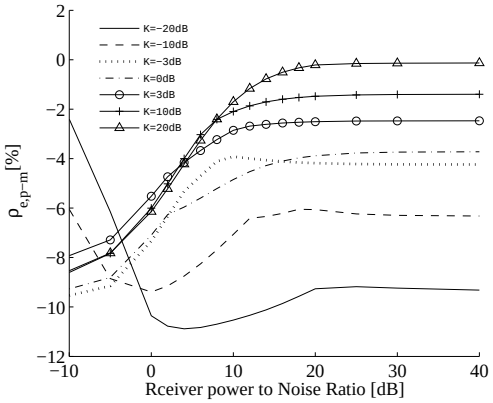
指向性の複雑性指標による RS 履歴の秘匿性向上効果と伝搬環境特性を示す．指向性の複雑性指標は，第 3 章で定義した EBR，LLL，CBW の 3 種類である．シミュレーション諸元およびそのフローチャートは，用意する 500 種類の可変指向性アンテナを除いて，前節と同じ物を用いる．

用意する可変指向性アンテナについて説明する．本節は，可変指向性アンテナのもつ指向性の複雑性指標が RS 履歴の秘匿性向上に効果があることを明らかにすることが目的である．このとき，指向性の複雑性指標の観点から，一様な可変指向性アンテナを 500 種類用意した場合，指向性の複雑性指標による秘匿性向上効果は得られない．従って，指向性の複雑性指標の観点から，多様な可変指向性アンテナを 500 種類用意する．しかし，指向性の複雑性指標をそのまま可変指向性アンテナの評価に用いた場合，1 つ問題がある．

表 4.1 の諸元より，可変指向性アンテナは 8 つの指向性パタンを形成する．そのため可変指向性アンテナを指向性の複雑性で評価する場合，1 つの可変指向性アンテナに対して 8 つの指向性の複雑性指標が算出され，一意に決まらない．そこで，本節は可変指向性アンテナが得られる指向性の複雑性指標の変化幅，ΔEBR，ΔLLL，ΔCBW を定義，用いる．ΔEBR 等は，得られる 8 つの指向性の複雑性指標の最大値と最小値の差を示す指標

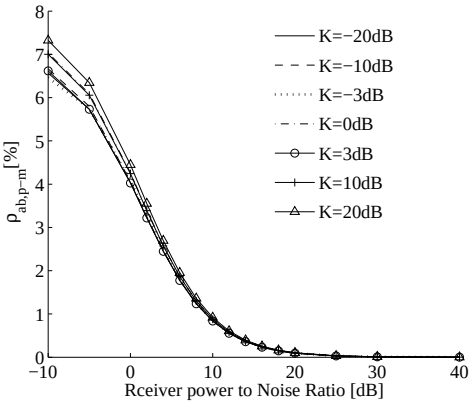



(a)RNR characteristic of improvement to $\rho_{ab}$.

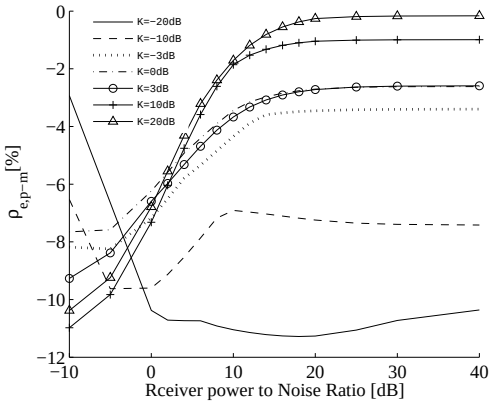



(b)RNR characteristic of improvement to $\rho_e$

図 4.3　Relation of the system security improvement to propagation properties for selecting a variable directivity antenna with ΔEBR.




(a)RNR characteristic of improvement to $\rho_{ab}$.

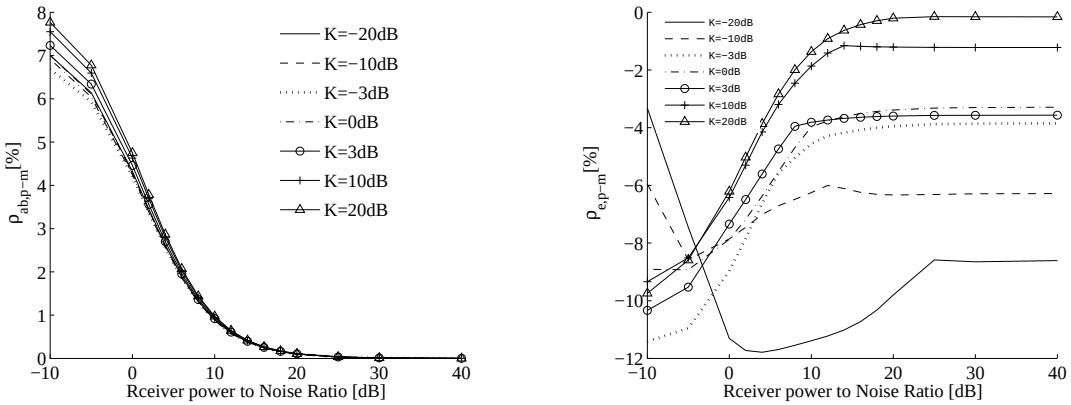



(b)RNR characteristic of improvement to $\rho_e$

図 4.4　Relation of the system security improvement to propagation properties for selecting a variable directivity antenna with ΔLLL.

である．何故ならば，RS 履歴の秘匿性を向上させるには，指向性パタンが変化することが重要である．故に指向性の変化を示す指標として，得られる 8 つの指向性の複雑性指標の変化幅を提案し，これを指向性の複雑性指標の観点から可変指向性アンテナを評価する指標とする．

指向性の複雑性指標 ΔEBR，ΔLLL，ΔCBW よる RS 履歴の秘匿性向上効果と伝搬環境特性を図 4.3，4.4，4.5 に示す．図 4.3(a) より，K 因子に依らず RNR が低い，つまり雑音の多い環境において，ΔEBR による $\rho_{ab}$ の向上が期待できる．しかしながら，RNR の低い 0dB 以下の伝搬環境は，図 4.1 から $\rho_{ab}$ は 0.5 以下と秘密鍵の共有効率が著しく悪い．また，期待できる向上効果を考慮しても，$\rho_{ab}$ はおおよそ 0.5 以下であることから，秘密鍵生成共有方式が利用困難な環境である．従って ΔEBR は $\rho_{ab}$ の向上に有用とは言




(a)RNR characteristic of improvement to $\rho_{ab}$.　(b)RNR characteristic of improvement to $\rho_e$

図 4.5　Relation of the system security improvement to propagation properties for selecting a variable directivity antenna with ΔCBW.

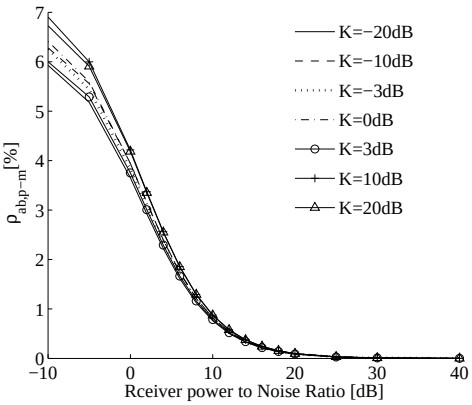
えない．図 4.4(a)，図 4.5(a) より，ΔLLL および ΔCBW による $\rho_{ab}$ の向上効果も ΔEBR と同じである．以上をまとめると，実際の利用を想定した場合において指向性の複雑性指標による $\rho_{ab}$ の向上効果は大きくない．

図 4.3(b) より，RNR が 0dB 以上の伝搬環境において K 因子が小さい程，ΔEBR による $\rho_e$ の低減が期待できる．特に RNR が 10dB 以上において，その効果は安定している．そして，K 因子が-20dB のとき，$\rho_{e,p-m}$ はほぼ 0% と得られる低減効果はない．従って，RNR が 0dB 以上，K 因子が 10dB 以下の伝搬環境において ΔEBR による $\rho_e$ の低減効果は，最大で 11%，最小で 1% 期待できる．図 4.4(b)，図 4.5(b) より，ΔLLL および ΔCBW による $\rho_{ab}$ の向上効果も ΔEBR と同じ傾向である．従って，RNR が 0dB 以上，K 因子が 10dB 以上の伝搬環境において，指向性の複雑性指標による $\rho_e$ の向上効果は，最大で 11%，最小で 1% 期待できる．

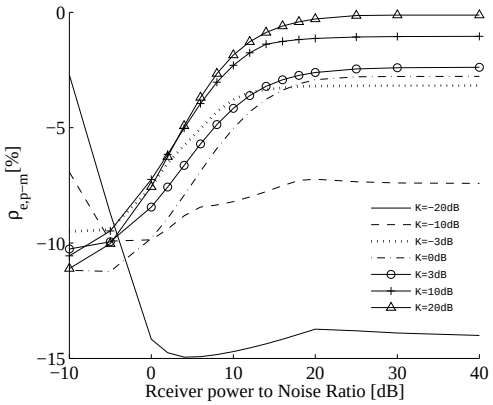
### 4.1.2　指向性の多様性指標による鍵の秘匿性向上効果

指向性の多様性指標による RS 履歴の秘匿性向上効果と伝搬環境特性を示す．指向性の多様性指標は，第 3 章で定義した ADC，PDC の 2 種類である．シミュレーション諸元およびそのフローチャート，および用意する 500 種類の可変指向性アンテナは，4.1.1 節と同じ手段をとる．

指向性の多様性指標 ADC，PDC よる RS 履歴の秘匿性向上効果と伝搬環境特性を図 4.6，4.7 に示す．図 4.6(a) より，K 因子に依らず RNR が低い雑音の多い環境において，ADC による $\rho_{ab}$ の向上が得られた．また，図 4.7(a) より，PDC による $\rho_{ab}$ の向上効果も ADC と同じ傾向が得られており，K 因子に依らず RNR が低い雑音の多い環境において，

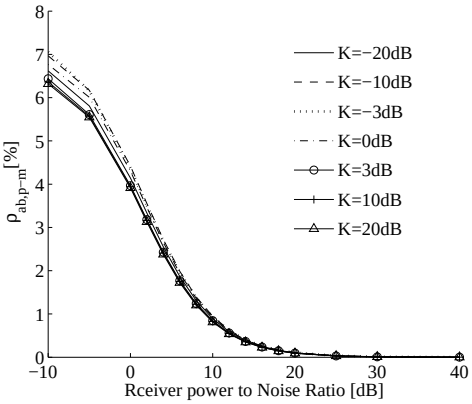



(a)RNR characteristic of improvement to $\rho_{ab}$.

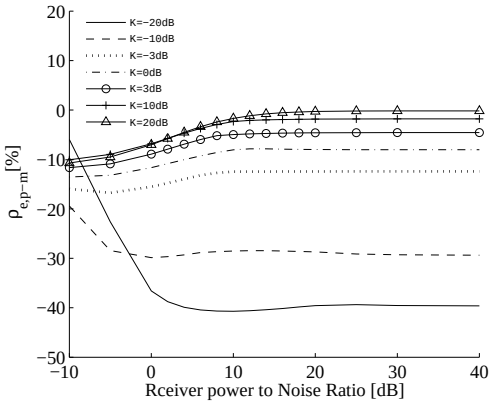



(b)RNR characteristic of improvement to $\rho_e$

図 4.6　Relation of the system security improvement to propagation properties for selecting a directivity set with $\rho_{ad}$.




(a)RNR characteristic of improvement to $\rho_{ab}$.




(b)RNR characteristic of improvement to $\rho_e$

図 4.7　Relation of the system security improvement to propagation properties for selecting a directivity set with $\rho_{pd}$.

PDC による $\rho_{ab}$ の向上が得られた．また，前節の指向性の複雑性指標と ADC，PDC ともに同じ傾向である．従って，実際の利用を想定した場合において指向性の多様性指標による $\rho_{ab}$ の向上効果は期待できない．

図 4.6(b) より，RNR が 0dB 以上の伝搬環境において K 因子が小さい程，ADC による $\rho_e$ の低減が期待できる．特に RNR が 10dB 以上において，その効果は安定している．図 4.1 より K 因子が 20dB 以上の伝搬環境は，$\rho_{e,p-m}$ はほぼ 0% と得られる低減効果はない．従って，実際の利用を想定した RNR が 0dB 以上，K 因子が 10dB 以下の伝搬環境において ADC による $\rho_e$ の低減は最大で 15%，最小で 2% の効果が期待できる．また，指向性の複雑性指標を用いた $\rho_e$ の低減効果と比較し，最大で 4% 大きい低減効果が得られている．

図 4.7(b) より，RNR が 0dB 以上の伝搬環境において K 因子が小さい程，PDC による $\rho_e$ の低減が期待できる．ADC と同様に実際の利用を想定した RNR が 0dB 以上，K 因子が 10dB 未満の伝搬環境において PDC による $\rho_e$ の低減は最大で 40%，最小で 2% の効果が期待できる．さらに，ADC を用いた $\rho_e$ の低減効果と比較し，最大で 25% 程度の大きい低減効果が得られている．

以上をまとめるとアンテナの設計指標による RS 履歴の秘匿性向上効果は，RNR が 0dB 以上，K 因子が 10dB 以下の伝搬環境において $\rho_e$ の低減が期待できる．一方で $\rho_{ab}$ の向上効果はほとんどない．故に，$\rho_e$ の低減に対して $\rho_{ab}$ はほとんど影響しないと言える．従って，アンテナ設計指標による RS 履歴の秘匿性向上効果は期待できる．提案するアンテナ設計指標の中で，PDC による $\rho_e$ の低減効果が最も大きく，最大で 40% の低減効果を得ることができた．

## 4.2　鍵の秘匿性とアンテナ設計指標の相関性

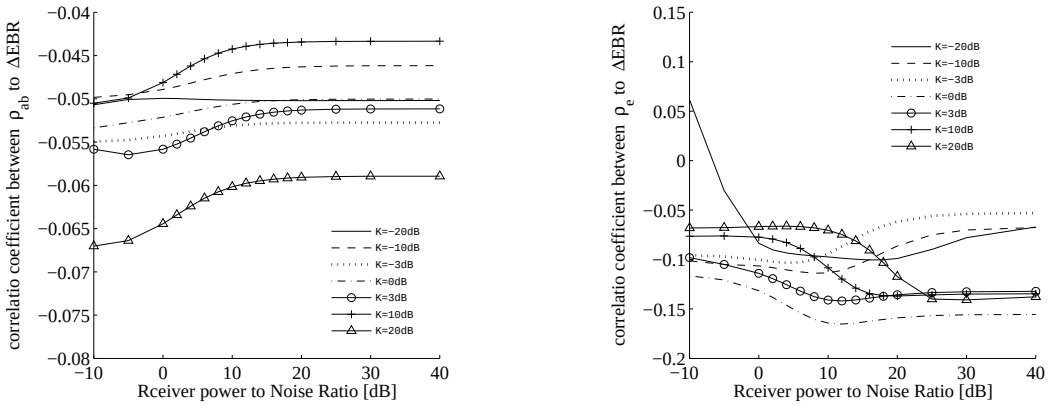
本節は可変指向性アンテナの設計指標によるアンテナの最適設計が RS 履歴の秘匿性向上に有効であることを明確にする．検証は 2 通りのアプローチで行う．検証 1 は，可変指向性アンテナの設計指標により設計した可変指向性アンテナが様々な伝搬環境で秘匿性向上効果が得られるかを明らかにする．具体的には，RS 履歴の秘匿性と可変指向性アンテナの設計指標の相関性を算出する．そのために，対象とする可変指向性アンテナおよび伝搬環境モデルは，4.1 節でも利用した普遍性のあるモデル，「正規乱数アンテナモデル／送受素波対応伝搬環境モデル」を用いる．

検証 2 は，検証 1 で得られた結果を別の観点から検証するため，対象とする可変指向性アンテナおよび伝搬環境モデルをより現実に即したモデルで，アンテナの最適設計が RS 履歴の秘匿性向上に有効であることを示す．具体的には，設計したフェーズドアレーが長方形部屋環境下において RS 履歴の秘匿性が向上することを確認する．

### 4.2.1　検証 1：正規乱数アンテナ／送受素波対応伝搬環境

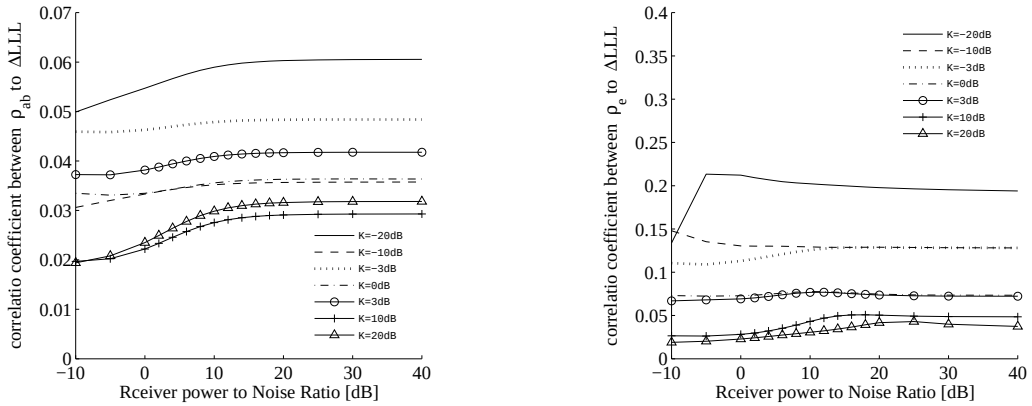
正規乱数アンテナモデルおよび送受素波対応伝搬環境モデルを用いて RS 履歴の秘匿性と可変指向性アンテナの設計指標の相関性を算出する．RS 履歴の秘匿性と可変指向性アンテナの設計指標の相関性について，例えば $\rho_{ab}$ と $\Delta$EBR の相関性算出式は

$$\rho = \frac{\sum_i^N \left(\rho_{ab,i} - E[\rho_{ab}]\right)\left(\Delta\mathrm{EBR_i} - \mathrm{E}[\Delta\mathrm{EBR}]\right)}{\sqrt{\left\{\sum_i^N \left(\rho_{ab,i} - E[\rho_{ab}]\right)^2\right\}\left\{\sum_i^N \left(\Delta\mathrm{EBR_i} - \mathrm{E}[\Delta\mathrm{EBR}]\right)^2\right\}}} \tag{4.3}$$




(a) System security: $\rho_{ab}$　　(b) System security: $\rho_e$

図 4.8　Correlation coefficient between ΔEBR and the system security.



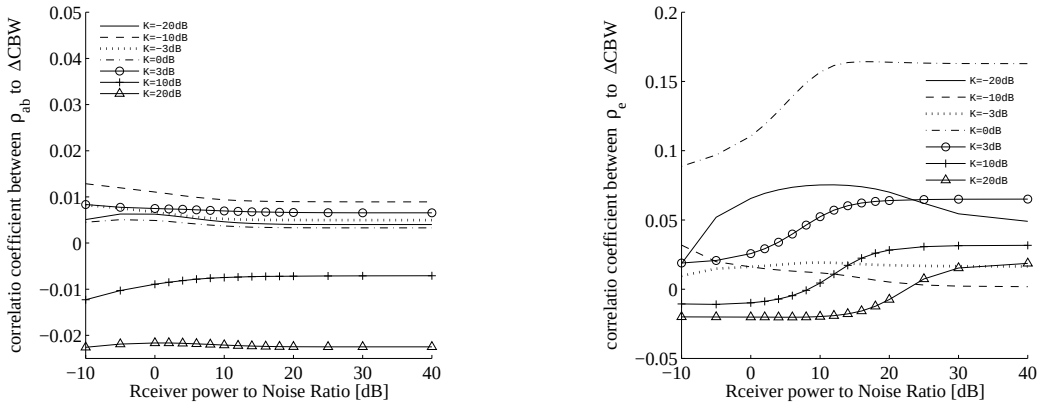

(a) System security: $\rho_{ab}$　　(b) System security: $\rho_e$

図 4.9　Correlation coefficient between ΔLLL and the system security.

$\rho_{ab,i}$ および $\Delta\mathrm{EBR_i}$ は i 番目の可変指向性アンテナを示しており，N は可変指向性アンテナの数を表す．シミュレーション諸元およびそのフローチャート，および用意する 500 種類の可変指向性アンテナは，4.1.1 節と同じ手段をとる．

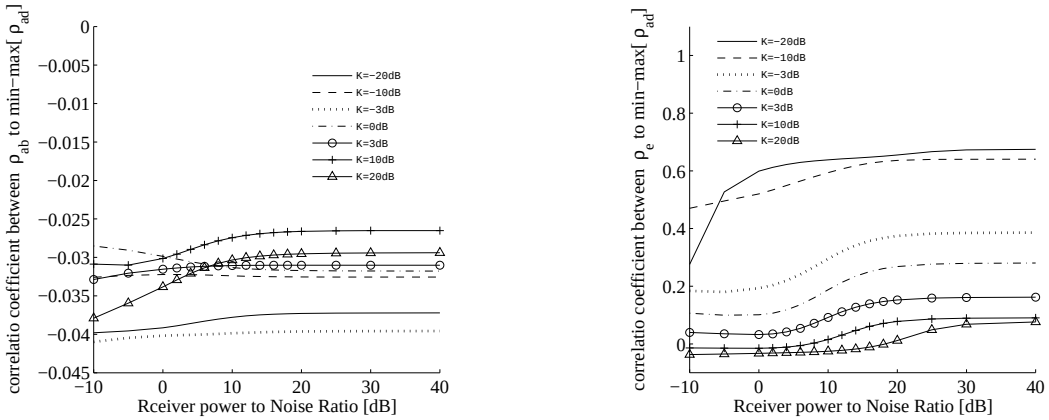
**鍵の秘匿性と指向性の複雑性指標の相関性**

指向性の複雑性指標 ΔEBR，ΔLLL，ΔCBW と RS 履歴の秘匿性の相関性の伝搬環境特性を図 4.8，4.9，4.10 に示す．結果より，全ての伝搬環境において，$\rho_{ab}$ とアンテナ設計指標の相関性は 0.07 以下と相関性が低いことがわかる．また，$\rho_e$ とアンテナ設計指標の相関性も，0.2 以下と相関性が低いことがわかる．しかしながら，ΔEBR，ΔLLL，ΔCBW で $\rho_e$ との相関性を比較すると ΔLLL が最も相関性が高い．以上をまとめると，指向性の複雑性指標は，秘匿性を向上しうる可変指向性アンテナの最適設計のための設計指標に有用とはいえない．一方で指向性複雑性指標の中では ΔLLL が，秘匿性を向上しうる可変




(a) System security: $\rho_{ab}$　　(b) System security: $\rho_e$

図 4.10　Correlation coefficient between ΔCBW and the system security.



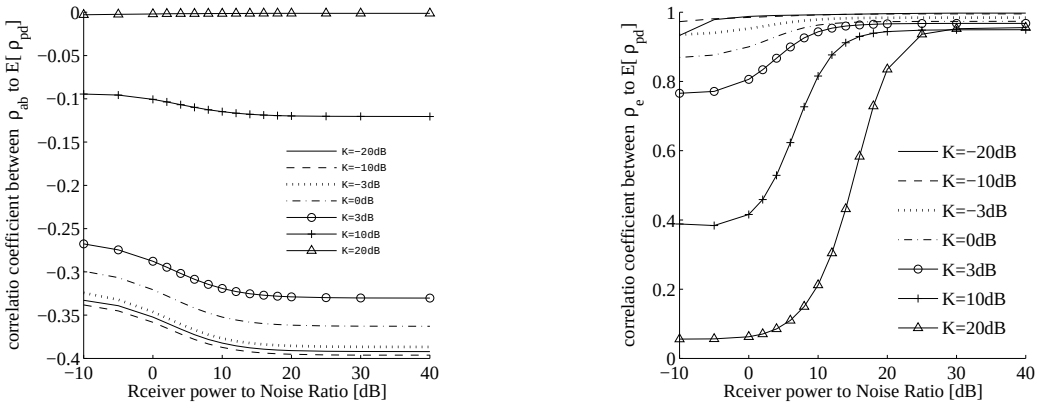

(a) System security: $\rho_{ab}$　　(b) System security: $\rho_e$

図 4.11　Correlation coefficient between $\rho_{ad}$ and the system security.

指向性アンテナの設計に向いていると考えられる．従って，指向性の複雑性指標のもう一つの利用方法である，電子パラメータの最適範囲の設計に LLL が有効ではないかと考えられる．

**鍵の秘匿性と指向性の多様性指標の相関性**

指向性の多様性指標 ADC，PDC と RS 履歴の秘匿性の相関性の伝搬環境特性を図 4.11，4.12 に示す．結果より，全ての伝搬環境において，$\rho_{ab}$ と指向性の多様性指標の相関性は 0.04 以下と相関性が低いことがわかる．図 4.11(b) より，RNR が 0dB 以上かつ K 因子が-10dB 以下の環境において，$\rho_e$ と ADC の相関性は 0.5 以上ある．上記環境において ADC を用いたアンテナ最適設計は RS 履歴の秘匿性向上に有効である．図 4.12(b) より，RNR が-10dB 以上かつ K 因子が 3dB 以下の伝搬環境において，$\rho_e$ と PDC の相関性は 0.77 以上ある．上記環境において PDC を用いたアンテナ最適設計は RS 履歴の秘匿性向




(a) System security: $\rho_{ab}$　　(b) System security: $\rho_e$

図 4.12　Correlation coefficient between $\rho_{pd}$ and the system security.

上に有効である．

以上をまとめると，指向性多様性指標 ADC および PDC は指向性複雑性指標と異なり，秘匿性を向上しうるアンテナの最適設計に設計指標として用いることができる．ADC と PDC を比較すると，アンテナの最適設計した場合において，秘匿性向上効果が期待できる伝搬環境は PDC の方が広範囲である．$\rho_e$ と PDC の相関性は，RNR が-10dB 以上かつ K 因子が 3dB 以下の伝搬環境にて 0.77 以上と ADC よりも高い相関性を示している．4.1.2 節の結論から PDC でアンテナ最適設計をした際の $\rho_e$ の向上効果は ADC より最大 25% 高い効果が期待できる．通信は RNR が 0dB 以上の伝搬環境で行なわれること [75]，見通し内室内環境において，K 因子は 3dB 程度であること [84][85] を考慮すると，一般的な室内環境の通信に用いる無線秘密鍵生成共有システムの秘匿性向上に PDC が有用であると言える．従って，本論文で提案したアンテナ設計指標の中で最も RS 履歴の秘匿性向上に有効な指標は PDC である．

### 4.2.2　評価モデル：フェーズドアレー／長方形部屋伝搬環境

前節で得られた結論，PDC を用いたアンテナ最適設計は RS 履歴の秘匿性向上に最も有効であることを検証するため，長方形部屋環境での $\rho_e$ と PDC の相関性について調べる．用いる可変指向性アンテナは 2.6.2 で定義したフェーズドアレーモデルより 2 から 5 素子のフェーズドアレーとする．長方形部屋環境モデルを図 4.13 に示す．伝搬路特性は 2.5.2 節で記述した 2 次元レイトレース法を用いて導出する．シミュレーションの流れを下記に，諸元を表 4.2 に示す．レイトレース法および RS 履歴算出プログラムの詳細は付録 B，付録 C で述べる．

Step1)　フェーズドアレーの素子数を決める．

表 4.2　Raytracing simulation parameters

| | 記号 | 値 | 単位 |
|---|---|---|---|
| 搬送波周波数 | f | 2.4 | GHz |
| 送信信号電力対受信雑音電力比 | TNR | 0〜80 | dB |
| 指向性パタンセットの数 | | 500 | |
| フェーズドアレーの素子数 | k | 2 〜 5 | |
| RS 履歴長 | | 8 | |
| 正規局場所の試行数 | | 3000 | |

Step2)　指向性パタンセットを指定数だけ用意する．
Step3)　送信電力対受信雑音電力比に従い白色ガウス雑音電力を決定する．
Step4)　正規局の場所を一様乱数で決める．
Step5)　用意された指向性パタンセットの中から 1 つ選ぶ．
Step6)　RS 履歴を生成共有する．
Step7)　全指向性パタンセットの RS 履歴生成が完了するまで Step5 に戻る．
Step7)　正規局場所の試行数だけ Step4 に戻る．
Step8)　全 TNR を網羅するまで Step3 に戻る．
Step9)　全種類のフェーズドアレーを解析するまで Step1 に戻る．

各素子数フェーズドアレーの $\rho_e$ の TNR 特性を図 4.14 に示す．図 4.14 よりフェーズドアレーの素子数増加による $\rho_e$ の低減が確認できる．特に，TNR が 70dB のとき $\rho_e$ の低減効果が大きい．各素子数フェーズドアレーにおける TNR が 70dB での $E[\rho_{pd}]$ と $\rho_e$ の

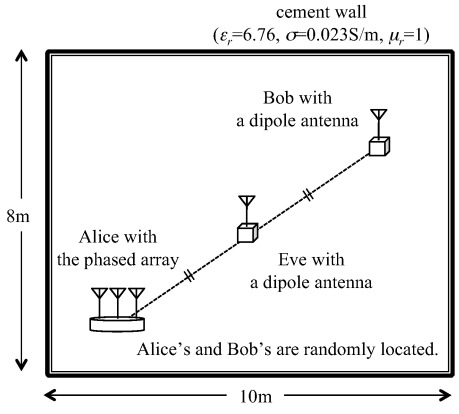



図 4.13　Rectangle room model

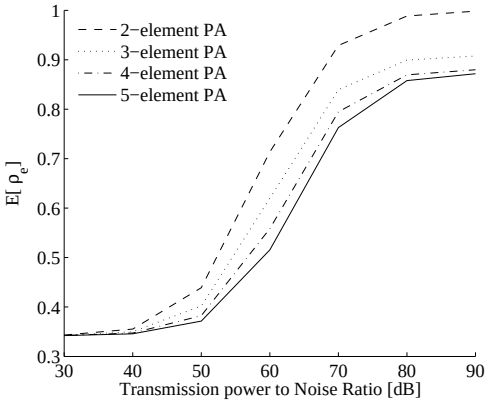



図 4.14　Characteristic of $\rho_e$ on TNR

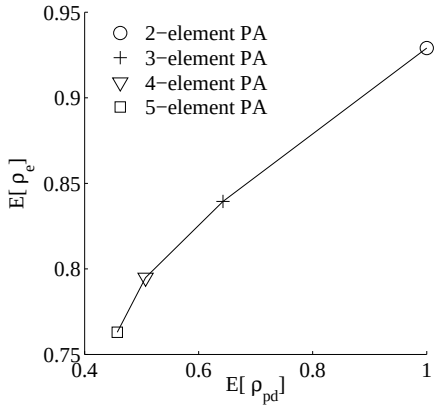



図 4.15　Relation between $E[\rho_{pd}]$ and $\rho_e$ for number of elements of phased array

関係を図 4.15 に示す．図 4.15 のより，フェーズドアレーの素子数が増えるほど，$E[\rho_{pd}]$ は低減している．これは，アンテナの指向性制御パラメータの自由度が増えて，指向性形成能力が向上する物理的な傾向と一致する．$E[\rho_{pd}]$ と $\rho_e$ に正の相関が見られる．ゆえに，PDC によるアンテナの最適設計は $\rho_e$ の低減に有効である．

## 4.3　本章の結論

本章は第 3 章で提案したアンテナ設計指標，EBR，LLL，CBW，PDC，ADC が RS 履歴の秘匿性向上に有用であることを検証した．RS 履歴の秘匿性は正規局間 RS 履歴の相関係数 $\rho_{ab}$ および正規盗聴局間 RS 履歴の相関係数 $\rho_e$ の 2 つを同時に考慮する．

アンテナ設計指標の影響を受けて $\rho_{ab}$ および $\rho_e$ がどの程度変わるか，効果があるかを探究した．全ての伝搬環境において，アンテナ設計指標による $\rho_{ab}$ の向上効果は期待できない結果が得られた．$\rho_e$ は，RNR が 0dB 以上，K 因子が 10dB 以下の伝搬環境において，アンテナの設計指標による値の低減が有効である結果が得られた．そして，$\rho_e$ の低減にしたいして $\rho_{ab}$ はほとんど影響しない，独立であるといえる．従って，アンテナ設計指標による RS 履歴の秘匿性向上は，$\rho_e$ の低減による効果が期待できる．アンテナ設計指標の中で，PDC による $\rho_e$ の低減効果が大きく，最大で 40% の低減効果を示した．

アンテナ設計指標と $\rho_{ab}$ および $\rho_e$ の相関性について調べ，アンテナ設計指標によるアンテナ設計が RS 履歴の秘匿性向上に有効であるかを探究した．指向性の複雑性指標と $\rho_{ab}$ および $\rho_e$ との相関性は全て 0.2 以下と低い結果が得られた．指向性の多様性指標と $\rho_{ab}$ および $\rho_e$ との相関性について，RNR が 0dB 以上かつ K 因子が-10dB 以下の伝搬環境下で $\rho_e$ と ADC の相関性は 0.5 以上得られた．RNR が-10dB 以上かつ K 因子が 3dB 以下の伝搬環境下で $\rho_e$ と PDC の相関性は 0.77 以上得られた．従って，本節は提案した

アンテナ設計指標の中で最も RS 履歴の秘匿性向上に有効な指標は PDC であり，その向上効果が有効である伝搬環境は RNR が 0dB 以上かつ K 因子が 3dB 以下ということを明らかにした．通信は RNR が 0dB 以上の伝搬環境で行なわれ，見通し内室内環境において，K 因子は 3dB 程度であることから，一般的な室内環境の通信に用いる無線秘密鍵生成共有システムの秘匿性向上に PDC が有用であると言える．

# 第 5 章

# エスパアンテナ

本章では可変指向性アンテナの 1 種，エスパアンテナについて詳述する．5.1 でエスパアンテナの動作原理について述べ，5.2 ではエスパアンテナの指向性算出手法について説明する．

## 5.1 原理

エスパアンテナは八木宇多アンテナと同じ空間でビームを形成するフェーズドアレーである．具体的な構造例を図 5.1 に示す．エスパアンテナは中央に放射素子を配置し，その近傍に複数のパラサイト素子を配置する．パラサイト素子は無給電素子とも呼ばれ，送受信回路に直接接続されない．また，放射素子ならびに周辺のパラサイト素子と空間的に電磁結合している．そして，八木宇多アンテナと同じ原理で指向性を形成する．各素子により形成された指向性を制御するため，パラサイト素子の電気長を可変させる．電気長を制御することにより，パラサイト素子は「反射器」や「導波器」の動作をする．各パラサイト素子の電気長を制御するため，直列に可変容量ダイオード（バラクタ）が挿入されており，バラクタには高周波チョークコイルまたは高抵抗を介して直流バイアス電圧を印加する．

エスパアンテナの特徴として，

(1) 給電が 1 系統
(2) 低消費電力，低コスト
(3) 素子間結合が指向性形成の本質

の 3 点ある．高周波信号は中央素子のみに給電する．そのため，総受信回路が 1 系統のみで済む．エスパアンテナは各バラクタに印加する直流バイアス電圧でそのリアクタンス値を制御することにより，水平面内に様々な指向性を形成する．これらバイアス電圧は可変容量ダイオードに対して逆方向であるので電圧駆動制御回路に直流電圧が流れない．つま

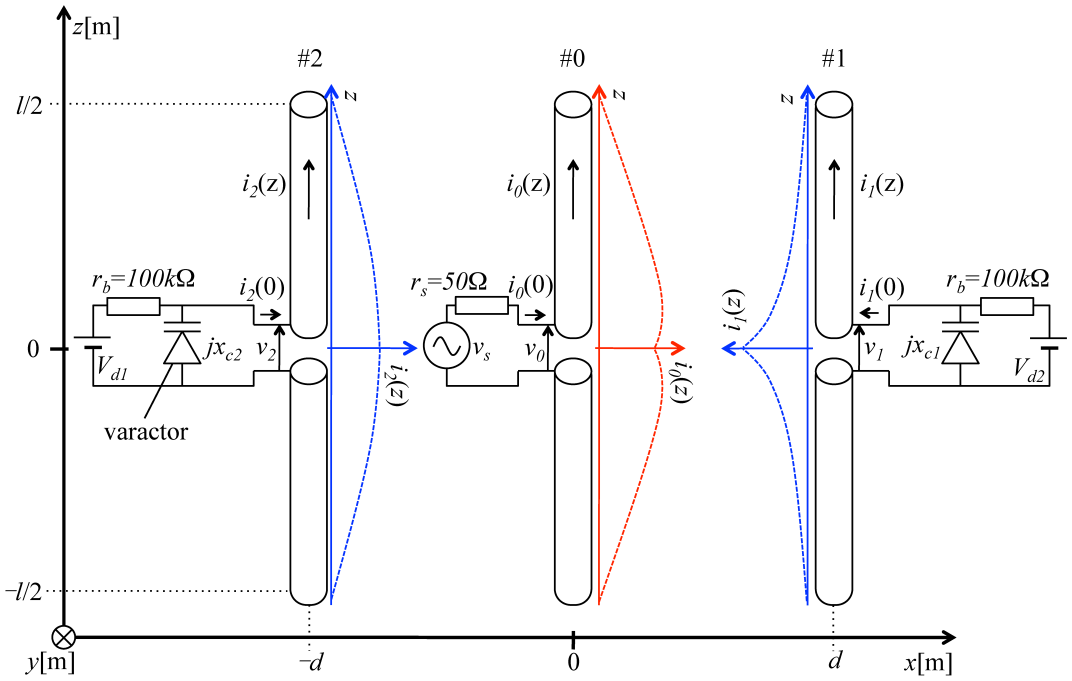



図 5.1　3-element ESPAR antenna configuration

り，パラサイト素子は直流的にも高周波的にもエネルギーを消費しない．放射素子と可変移相回路が別々に設計されていた従来のフェーズドアレーと比べてハードウェアの構成が飛躍的に簡単である．そのため，アンテナの高周波化が容易であり，また低コストな可変指向性アンテナである．

これら利点を有する反面，素子間結合が指向性形成の本質であることと，放射素子とバラクタが一体となっているため動作メカニズムと制御時の指向性の振る舞いが直感的に理解しにくいという問題点がある．つまり，無線秘密鍵生成共有方式のためのエスパアンテナを設計段階において，従来の設計理論がそのまま適用できないという問題点とも言える．そこで本論文は基本的な構造における指向性の振る舞いを，第 6 章にて網羅的に調べる．その成果を用いて無線秘密鍵生成共有方式のためのエスパアンテナの設計，試作を行なう．

## 5.2　指向性算出手法

本節はエスパアンテナの指向性パタンを計算により算出する方法を説明する．何故ならば，エスパアンテナは電子的に指向性を制御するため，指向性を切り替える毎に計算しなければならない．アンテナの指向性は電磁界解析シミュレータを用いて求めることが一般的である．故に，エスパアンテナが形成できる指向性全てを電磁界解析で求めることは計

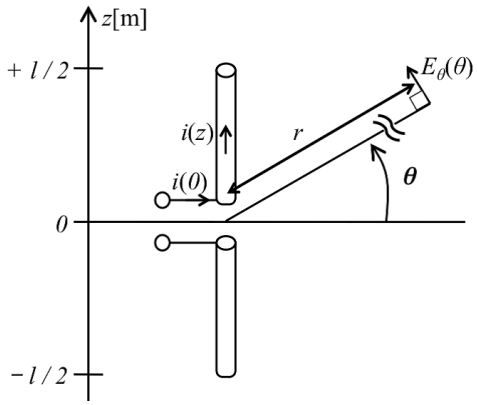



図 5.2 Far-field of dipole antenna

算時間が膨大となり，非現実的である．従って，簡単な計算式でエスパアンテナの指向性を算出することが重要である．本節は，等価ウェイトベクトル法と空間分布イミタンス行列法の 2 種類について説明する．

### 5.2.1 等価ウェイトベクトル法

ステアリングベクトル（各素子の配列位置から水平面内の方位角 $\phi$[rad] 方向の遠方点への放射伝達関数を要素とするベクトル）と指向性ベクトル（各素子の指向性を要素とするベクトル）の内積で，エスパアンテナの指向性を求める等価ウェイトベクトル法が提案されている [63].

各素子（ダイポールアンテナ）の指向性について図 5.2 を用いて説明する．ダイポールアンテナの素子上の微小区間 $dz$ に流れる電流 $i(z)$[A] が遠方界に与える電界を $dE_\theta$[V/m] としたとき，ダイポールアンテナの電界は，

$$E_\theta = \int_{-l/2}^{+l/2} j\eta \frac{ki(z)e^{-jkr}}{4\pi r} \sin\theta e^{+jkz\cos\theta} dz \tag{5.1}$$

で表される．このとき，ダイポールアンテナの素子長が半波長であるとすると，図 5.1 に示す各素子の電流分布 $i(z)$ は $i(z) \approx i(0)\cos\left(\frac{2\pi}{\lambda}z\right)$ の式で近似できる．この近似式を式 (5.1) に代入すると，

$$E_\theta = j\eta \frac{i(0)e^{-jkr}}{2\pi r} \left[\frac{\cos\left(\frac{\pi}{2}\cos\theta\right)}{\sin\theta}\right] \quad [\mathrm{V/m}] \tag{5.2}$$

の式を求めることができる．

式 (5.2) を要素とした指向性ベクトル $\boldsymbol{E}_\theta$（水平面内指向性なので仰角 $\theta = \frac{\pi}{2}$）を用い

て，単位距離（$r = 1\mathrm{m}$）はなれたエスパアンテナの電界は以下の式で表される．

$$
\begin{aligned}
&E_{esp}(\phi) = \boldsymbol{\alpha}(\phi)^T \boldsymbol{E}_\theta, \quad \boldsymbol{\alpha}(\phi) = [1, e^{j\psi}, e^{-j\psi}]^T \\
&\boldsymbol{E}_\theta = j\eta \frac{e^{-jk}}{2\pi} \boldsymbol{i} \\
&\boldsymbol{i} = [i_0(0), i_1(0), i_2(0)]^T = v_s \left(\mathbf{Y}^{-1} + z_s \mathbf{U}_0 + j\mathbf{X}_{var}\right)^{-1} \boldsymbol{u}_0 \\
&\psi = \frac{2\pi d}{\lambda} \cos\phi, \quad \boldsymbol{u_0} = [1, 0, 0]^T, \quad \mathbf{U}_0 = diag[1, 0, 0] \\
&\mathbf{X}_{var} = diag[0, x_1, x_2], \quad \mathbf{Y} = \begin{bmatrix} y_{00} & y_{01} & y_{02} \\ y_{10} & y_{11} & y_{12} \\ y_{20} & y_{21} & y_{22} \end{bmatrix};
\end{aligned}
\tag{5.3}
$$

$\mathbf{Y}$ はアドミタンス行列であり，その要素 $y_{ij}$ はアンテナ素子#$i$，$j$ 間の電気的な結合を示している．よって，アドミタンス行列はアンテナの構造によって一意に決まり，行列の要素は電磁界解析を行うことで求めることができる．つまり，等価ウェイトベクトルは 1 回の電磁界解析を行うだけで，エスパアンテナの電界を簡単な行列計算で求めることができる．

次に得られたエスパアンテナの電界から指向性評価によく用いられる動作利得を求める．動作利得 $G_{abs}$ は，入力電力 $P_{in}$[W] におけるエスパアンテナの放射強度とアイソトロピックアンテナ（全方位無指向性アンテナ）の放射強度の比である．式 (5.3) より，エスパアンテナの放射強度 $U(\phi)[W/sr]$ は，

$$
\begin{aligned}
W_{rad}(\phi) &= \frac{1}{2} \Re[E_{esp}(\phi) \cdot H^*_{esp}(\phi)] \\
&= \frac{1}{2} \frac{|E_{esp}(\phi)|^2}{\eta} \qquad (5.4) \\
U(\phi) &= r^2 W_{rad}(\phi) \qquad (5.5)
\end{aligned}
$$

となる．$W_{rad}(\phi)$ は放射電力密度 $[W/m^2]$ である．エスパアンテナの入力電力 $P_{in}$ と同じ電力を用いたアイソトロピックアンテナの放射電界強度は以下の式で表される．

$$
\begin{aligned}
P_{in} &= \frac{1}{2} \Re[v \cdot i^*] \qquad (5.6) \\
&= \frac{1}{2} \Re[\frac{v_s}{2} \cdot \frac{v_s}{2z_s}^*] \\
&= \frac{1}{8} \frac{|v_s|^2}{z_s} \qquad (5.7) \\
U_{iso} &= \frac{P_{in}}{4\pi} \qquad (5.8)
\end{aligned}
$$

以上より，動作利得 $G_{abs}(\phi)$ は，

$$G_{abs}(\phi) = 10\log\frac{U(\phi)}{U_{iso}(\phi)} \tag{5.9}$$

$$= 10\log\left(4\pi\frac{U(\phi)}{P_{in}}\right) \tag{5.10}$$

と表せる．単位は [dBi] である．

### 5.2.2 空間分布イミタンス行列法

等価ウェイトベクトル法は，エスパアンテナの指向性を高速に算出することができる反面，ダイポール素子上の電流分布に近似式を与えているため，算出する指向性に誤差が生じる．特に，ダイポール素子の間隔 $d$ が狭くなる程，電流分布が近似式からはずれ，指向性の計算誤差が大きくなることが文献 [61] で述べられている．本節では，指向性の算出速度を変えること無く，図 5.1 に示す電流分布 $i(z)$ を厳密に計算することで，指向性の計算誤差をなくす空間分布イミタンス行列法について説明する．

前節より，電流分布の近似を行なわなかった場合のダイポールアンテナの遠方界は，

$$E_\theta = j\eta\frac{ke^{-jkr}}{4\pi r}\sin\theta\int_{-l/2}^{+l/2} i(z)e^{+jkz\cos\theta}dz \tag{5.11}$$

が得られる．得られた指向性ベクトル $\boldsymbol{E}_\theta$（水平面内指向性なので仰角 $\theta = \frac{\pi}{2}$）を用いて，単位距離（$r = 1$m）はなれたエスパアンテナの電界は，

$$E_{esp}(\phi) = \boldsymbol{\alpha}(\phi)^T\boldsymbol{E}_\theta, \quad \boldsymbol{\alpha}(\phi) = [1, e^{j\psi}, e^{-j\psi}]^T \tag{5.12}$$

$$\boldsymbol{E}_\theta = j\eta\frac{e^{-jk}}{2\pi}\boldsymbol{i}_{int}$$

$$\boldsymbol{i}_{int} = \int_{-l/2}^{+l/2}[i_0(z), i_1(z), i_2(z)]^T dz = \int_{-l/2}^{+l/2}\boldsymbol{i}(z)dz$$

$$= v_s\left(\mathbf{Y}_{int}^{-1} + z_s\mathbf{U}_0 + j\mathbf{X}_{var}\right)^{-1}\boldsymbol{u}_0$$

$$\psi = \frac{2\pi d}{\lambda}\cos\phi, \quad \boldsymbol{u_0} = [1,0,0]^T, \quad \mathbf{U}_0 = diag[1,0,0]$$

$$\mathbf{X}_{var} = diag[0, x_1, x_2], \quad \mathbf{Y}_{int} = \int_{-l/2}^{+l/2}\mathbf{Y}(z)dz,$$

$$\mathbf{Y}(z) = \begin{bmatrix} y_{00}(z) & y_{01}(z) & y_{02}(z) \\ y_{10}(z) & y_{11}(z) & y_{12}(z) \\ y_{20}(z) & y_{21}(z) & y_{22}(z) \end{bmatrix};$$

と表すことができる．$\mathbf{Y}(\mathbf{z})$ はイミタンス行列と定義し，イミタンス行列はアンテナの構造により一意に決まる．イミタンス行列の物理的意味について具体的に述べる．図 5.1 に

あるアレー素子は半導体を含まない 3 端子対線形回路網と見なすことができる．つまり，素子上の電流分布 $\boldsymbol{i}(z) = [i_0(z), i_1(z), i_2(z)]^T$ もポートの入力電圧 $\boldsymbol{v} = [v_0, v_1, v_2]^T$ に対して線形性が成り立つため，電流分布 $\boldsymbol{i}(z)$ と入力電圧 $\boldsymbol{v} = [v_0, v_1, v_2]^T$ の関係を表す行列としてイミタンス行列 $\mathbf{Y}(\mathbf{z})$ を定義しており，

$$\boldsymbol{i}(z) = \mathbf{Y}(z)\boldsymbol{v} \tag{5.13}$$

と表すことができる．イミタンス行列を構成する要素 $y_{00}(z)$，$y_{10}(z)$，$y_{20}(z)$ はポート 0 に 1V, 他のポートはショートした場合のアンテナ素子上電流分布であり，$y_{00}(z) = i_0(z)$, $y_{10}(z) = i_1(z)$，$y_{20}(z) = i_2(z)$ と表せる．他の要素についても同様の物理的性質を持つ．空間分布イミタンス行列法を用いたエスパアンテナの指向性算出プログラムの詳細は付録 A に載せる．

## 5.3　本章の結論

本章は無線秘密鍵生成共有方式のための可変指向性アンテナの設計試作の基となる，エスパアンテナについて記述した．

5.1 節では，エスパアンテナの動作原理およびその特徴について詳述した．具体的には，エスパアンテナは八木宇多アンテナの原理である空間的電磁界結合を積極的に利用して指向性パタンを形成する可変指向性アンテナであること，そして，パラサイト素子の電気長を制御することで素子の動作を「反射器」や「導波器」に切り替える仕組みであることを記述した．エスパアンテナは従来の設計理論がそのまま適用できない問題点があるため，本論文では，無線秘密鍵生成共有方式のためのエスパアンテナを設計する上で，基本的なエスパアンテナ構造と指向性制御の関係を調べた後，アンテナの設計，試作を行なうこととした．

5.2 節では，エスパアンテナの指向性算出手法について説明した．算出法には等価ウェイトベクトル法と空間分布イミタンス行列法の 2 種類あり，本論文は，より指向性を厳密に算出することができる空間分布イミタンス行列法を採用した．

# 第 6 章

# 3 素子ダイポールエスパアンテナの設計，試作および評価

本章は無線秘密鍵生成共有方式のためのエスパアンテナを設計，試作するための前準備として，エスパアンテナの基本構造である，3 素子ダイポールエスパアンテナのアンテナ構造とアンテナ設計指標の関係について探究する．本章で着目するアンテナ構造はアンテナ素子間隔とする．何故ならば，エスパアンテナの指向性形成に素子間の電磁界結合が深く関わっており，アンテナの素子間隔はその空間的電磁界結合に強い影響を与えるアンテナ構造だからである．また，第 4 章より，対象とするアンテナ設計指標は，指向性の多様性を示す PDC である．エスパアンテナの指向性の多様性を追求するために，1）アンテナの指向性が多様となるリアクタンス範囲の探究，2）エスパアンテナの指向性が多様となるアンテナ構造の探究，の 2 つの課題に取り組む．

課題 1 は，あるアンテナ素子間隔における最も複雑な形状の指向性パタンとオムニ形状の指向性パタンを得るためのリアクタンス範囲を明らかにする．加えて，リアクタンスの変動が指向性パタンの変動に大きくな影響を与えるリアクタンス範囲を明らかにする．課題 2 では，課題 1 で得られるリアクタンス範囲内において形成可能な指向性が多様となるアンテナ素子間隔を追求する．

## 6.1 指向性の複雑性評価指標のリアクタンスおよび素子間隔依存性

本節はエスパアンテナが形成可能な指向性が多様となるリアクタンス範囲を探究する．何故ならば，エスパアンテナが形成可能な指向性を最大化するには，リアクタンス範囲を無限しなければならいが，現実的には困難である．加えて，リアクタンスの絶対値が極端に大きい場合，パラサイト素子に流れる電流が非常に小さくなり，そのためリアクタンス

表 6.1　Parameter of directivity analysis

| | 値 | 単位 |
|---|---|---|
| 信号源内部抵抗 | 50 | Ω |
| 素子長: h | $1/2$ | $\lambda$ |
| 素子半径 | $1/100$ | $\lambda$ |
| 素子間隔: $d$ | $1/32, 1/16, 1/8, 1/4, 1/2$ | $\lambda$ |
| 方位角: $\phi$ | 0〜360 | deg |

$\lambda$ は自由空間波長

の変化による指向性の変化はほとんど起きない．従って，指向性パタンを効果的に変化させるリアクタンス範囲を定めることが重要である．

そこで，3.1 節で定義した指向性の複雑性評価指標を用いて指向性のリアクタンス特性を明らかにし，その結果を用いてリアクタンス範囲を定める．本節では 4.2 で得られた結論から，無線秘密鍵生成共有方式の秘匿性向上に最も効果があると考えられる指向性の複雑性評価指標として，LLL を採用する．リアクタンス範囲を明らかにする上で，以下の 2 つの観点から LLL のリアクタンス特性を示す．1）最も複雑な形状の指向性パタンとオムニ形状の指向性パタンを得るためのリアクタンス範囲を明らかにするため，LLL のリアクタンス平面特性を示す．2）リアクタンスによる指向性パタンの制御が効果的であるリアクタンス範囲を明らかにするため，リアクタンス平面上の LLL の傾きのリアクタンス平面特性を示す．リアクタンス平面上の LLL の傾きは

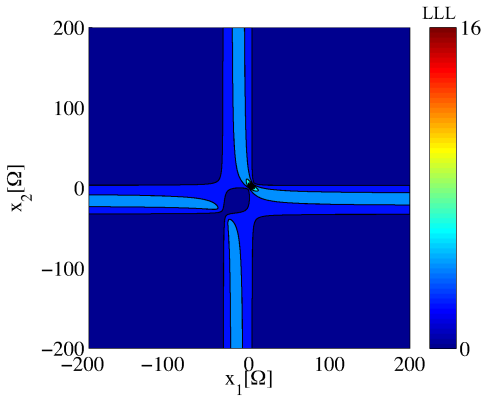
$$\mathrm{grad}[\mathrm{LLL}(x_1, x_2)] = \min\left\{\frac{d\mathrm{LLL}(x_1, x_2)}{dx_1}, \frac{d\mathrm{LLL}(x_1, x_2)}{dx_2}\right\} \tag{6.1}$$

と定義する．

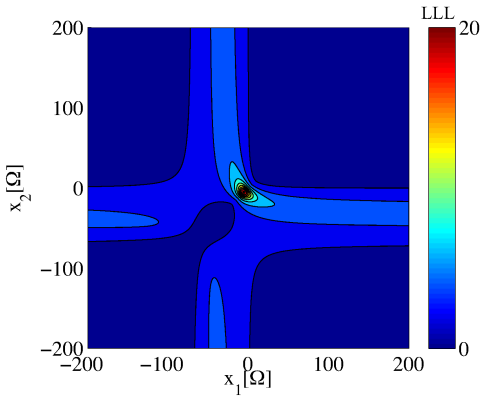
指向性解析諸元を表 6.1 に示す．指向性算出は 5.2 節に記述した空間分布イミタンス行列法を用いる．空間分布イミタンス行列法で用いるイミタンス行列はモーメント法をベースとした電磁界解析ソフト NEC2[86] で算出する．

LLL リアクタンス特性マップを図 6.1 に，grad[LLL] リアクタンス特性マップを図 6.2 に示す．図 6.1 より，リアクタンス値が-200Ω から 200Ω の範囲において，全ての素子間隔でリアクタンス値（200，200）のとき LLL は最小値になる．指向性と電流分布の関係から，リアクタンスが大きいほど指向性はオムニになると考えられ，ゆえに LLL はリアクタンス値が大きいほど最小になると考えられる．

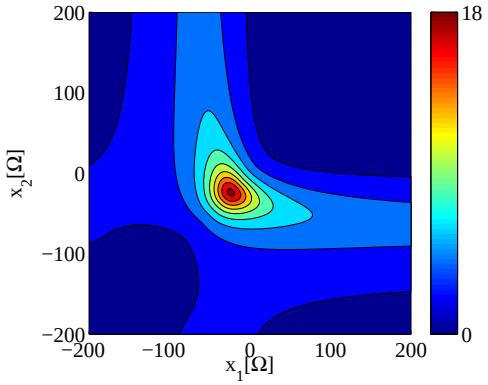
LLL の最小値および最大値が得られるリアクタンス範囲について，最小値となるリアクタンス値は最大値の 0.1 倍の LLL が得られる値と定義する．従って LLL の最小値および最大値が得られるリアクタンス範囲は，素子間隔 $\lambda/32$ で 2〜7Ω，$\lambda/16$ で-10〜10Ω，$\lambda/8$



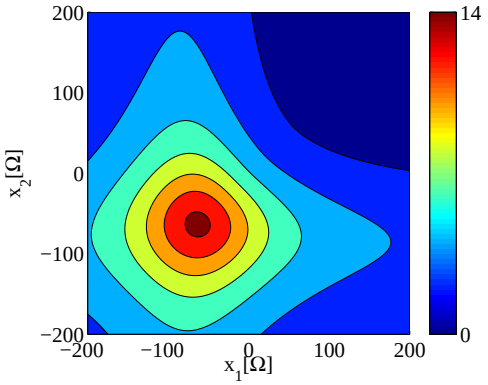

(a) Space between elements: $\lambda/32$



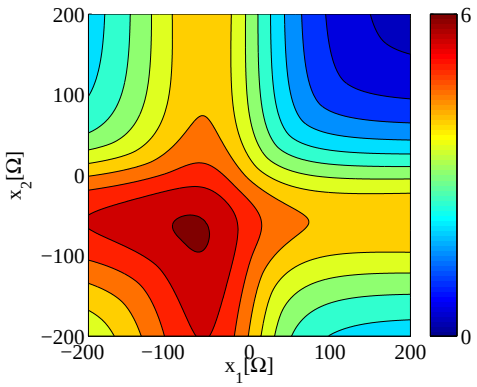

(b) Space between elements: $\lambda/16$




(c) Space between elements: $\lambda/8$

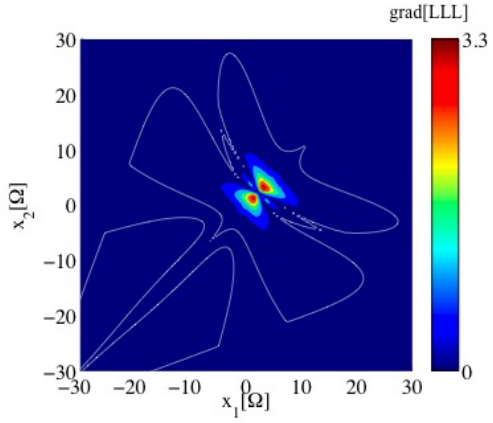



(d) Space between elements: $\lambda/4$

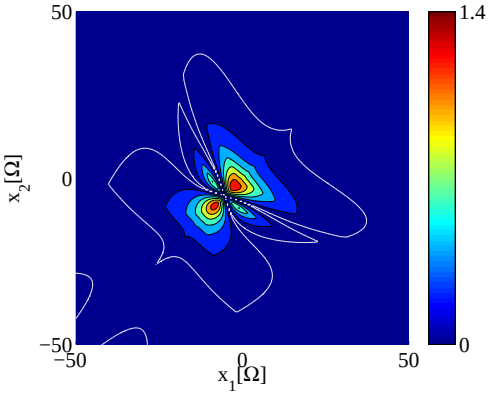



(e) Space between elements: $\lambda/2$

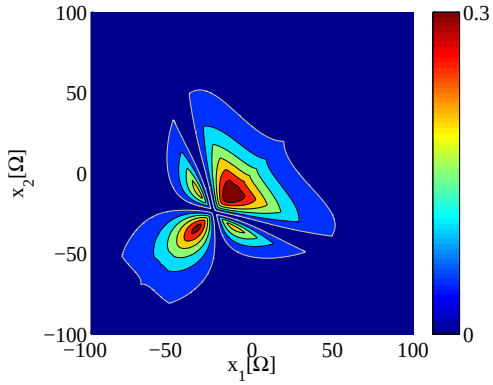
図 6.1　LLL map on reactancec plane



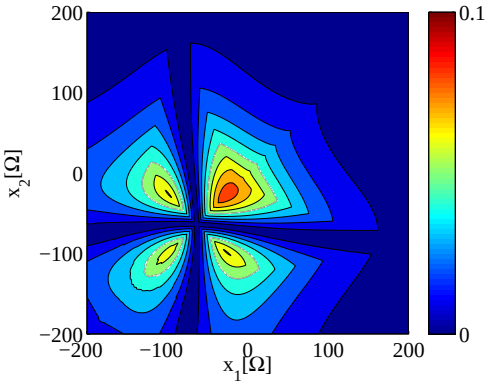

(a) Space between elements: $\lambda/32$



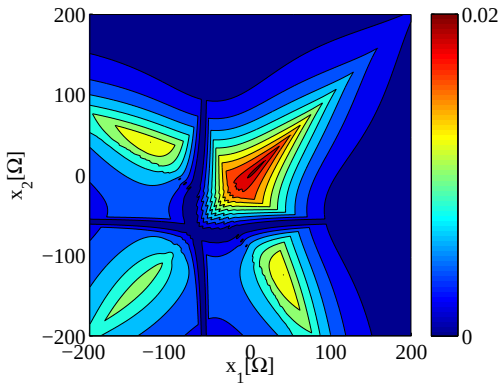

(b) Space between elements: $\lambda/16$




(c) Space between elements: $\lambda/8$




(d) Space between elements: $\lambda/4$




(e) Space between elements: $\lambda/2$

図 6.2　grad[LLL] map on reactancec plane ( white line: grad[LLL]=0.05 )

で-25〜25Ω，$\lambda/4$ で-65〜75Ω，$\lambda/2$ で-70〜150Ω が得られる．

図 6.2 より，grad[LLL] が大きい程，指向性パタンがリアクタンス値の変化に敏感に応答する．つまりは全ての素子間隔においてリアクタンス値が 0 近辺は指向性パタンがリアクタンス値に多感に応答するリアクタンス範囲であると言える．例えば，指向性パタンがリアクタンスの変化に鈍感であると判断する境界線を grad[LLL]=0.05（グラフ中の白のライン）とすると，リアクタンスによる指向性パタンの制御が効果的であるリアクタンス範囲は，素子間隔 $\lambda/32$ で-23〜28Ω，$\lambda/16$ で-40〜40Ω，$\lambda/8$ で-80〜50Ω，$\lambda/4$ で-130〜30Ω が得られる．$\lambda/2$ は解が無いと言える．

以上の結果をまとめると，素子間隔が狭くなる程，リアクタンス範囲は狭くなる傾向が得られる．各アンテナ素子間隔における最適なリアクタンス範囲は，$\lambda/32$ で-23〜28Ω，$\lambda/16$ で-40〜40Ω，$\lambda/8$ で-80〜50Ω，$\lambda/4$ で-130〜30Ω $\lambda/2$ で-70〜150Ω である．これは，素子間隔が狭くなるに従い素子間の電磁界結合が強くなり，その結果リアクタンスが電流分布に与える影響が大きくなったためと考えられる．

## 6.2　指向性の多様性評価指標の素子間隔依存性

本節は指向性の多様性評価指標と素子間隔の関係を明らかにする．指向性多様性評価指標は 4.2 節の結論から，無線秘密鍵生成共有方式の秘匿性向上効果が最も期待できる指向性の多様性評価指標 PDC を用いてエスパアンテナの素子間隔依存性を探究する．

#### リアクタンス領域指向性相関係数 (RDC)

PDC は指向性を可変させるパラメータの領域における指向性の多様性（独立性）を示す指標であるが，評価対象にエスパアンテナを想定していない．そこで PDC を応用し，リアクタンス領域において指向性多様性を示す指標として，リアクタンス領域指向性相関係数（Reactance Domain Correlation coefficient: RDC）を定義する．

対象とする 3 素子ダイポールエスパアンテナについて，リアクタンス $x_1$，$x_2$ の変動による任意 2 方位角 $\phi_1$，$\phi_2$ の複素指向性の変動の多様性（独立性）を

$$\rho_{rd}(\phi_1, \phi_2) = \rho(D(\phi_1), D(\phi_2)) \tag{6.2}$$

$$\rho(x, y) = \frac{|E[xy^*] - E[x]E[y^*]|}{\sqrt{(E[|x|^2] - |E[x]|^2)(E[|y|^2] - |E[y]|^2)}} \tag{6.3}$$

$$E[D(\phi)] = \frac{\int\int D(\phi, x_1, x_2) dx_1 dx_2}{\int\int dx_1 dx_2}$$

と定義する．$\rho(x, y)$ は相互相関係数の絶対値である．そして，全方位の複素指向性の多

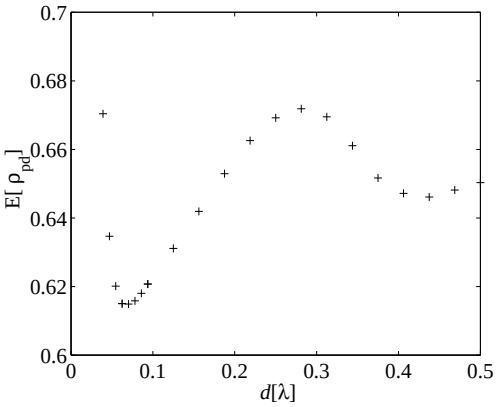



図 6.3　Charactaristic of RDC on the elements space

様性を

$$E[\rho_{rd}] = \frac{1}{4\pi^2} \int_{\phi_1} \int_{\phi_2} \rho_{rd}(\phi_i, \phi_j) d\phi_2 d\phi_1 \tag{6.4}$$

と定義する．これを RDC とする．$E[\rho_{rd}]$ が低いほど，可変指向性は多様であり，無線秘密鍵生成共有方式の秘匿性を高める．

#### RDC の素子間隔特性

RDC の素子間隔特性を解析する．素子間隔は λ/32 から λ/2 まで可変させる．リアクタンスの範囲は 6.1 節の結果より，全ての素子間隔のリアクタンス範囲を包括する-200〜200Ω とする．他の解析諸元は 6.1 節と同じとする．

図 6.3 の RDC の素子間隔特性より，可変する指向性が多様となる素子間隔は，$E[\rho_{rd}]$ が最も低くなる素子間隔 λ/16 である．この結果は LLL の解析結果が素子間隔 λ/16 の時，最大値を示すことと一致する．

節および節をまとめると，RS 履歴の秘匿性を高める 3 素子エスパアンテナの設計パラメータは，RDC の結果より指向性が多様となる素子間隔 λ/16 とする．その時のリアクタンス範囲は-40〜40Ω とする．

## 6.3　アンテナの試作および性能検証

本節は 6.1 節および 6.2 節で得られた解析結果の実証実験を行なう．実証実験を行なうにあたり素子間隔が可変する 3 素子ダイポールエスパアンテナを試作した．

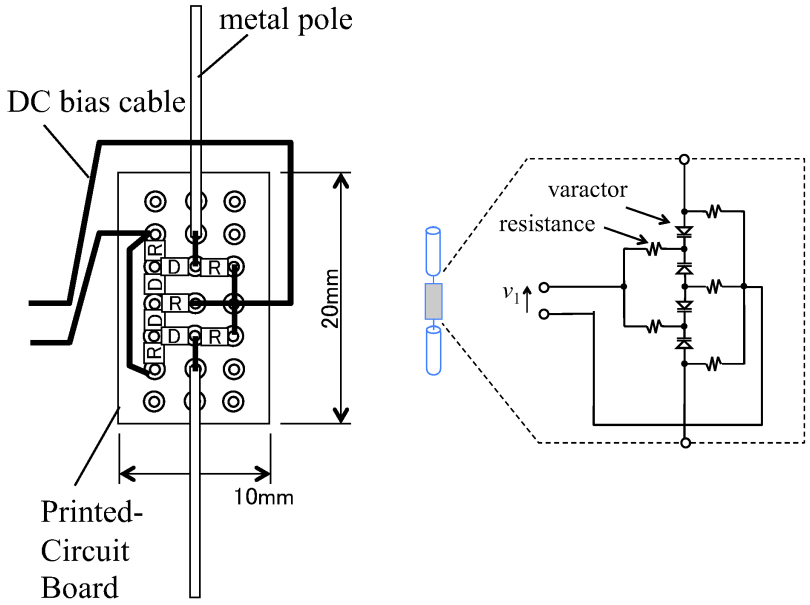



図 6.4　Prototyped variable reactance circuit configuration

### 6.3.1　試作した 3 素子エスパアンテナ

試作した 3 素子ダイポールエスパアンテナの構成回路図を図 6.4 に，写真を図 6.5 に示す．給電素子には 50Ω 同軸ケーブルを，無給電素子にはリアクタンス回路が装荷されている．設計周波数は 2.4GHz とする．リアクタンス回路は文献 [59] に書かれた高調波抑制可変リアクタンス回路を参考に試作する．バラクタは HVD368B を用いる．試作したリアクタンス回路の可変範囲は-68〜70Ω である [67]．これは前節で用いたリアクタンス範囲より狭い．しかしながら，回路サイズの増加の観点からバラクタの数を 4 個とした．バラクタの制御はデジタル/アナログ変換回路（DAC）で行っており，その性能は出力電圧 0〜5V，分解能 8bit である．

試作アンテナの素子間隔を容易に変更するため，アクリル板で給電素子と無給電素子を挟み込み，素子を固定している．素子間隔可動範囲は $\lambda/12$ から $\lambda/4$ の範囲である．

### 6.3.2　指向性および反射係数測定およびアンテナ性能評価

アンテナの測定系を図 6.6 に示す．3 素子エスパアンテナの各ダイポール素子とダイポールアンテナが一直線上に並ぶ様に配置し，これを方位角 0deg とする．ダイポールアンテナ側の無給電素子を#1，反対側を#2 とする．偏波面は地面に対し垂直となる様にする．同軸ケーブルと DC バイアスケーブルは方位角 270deg 方向へ引き出す．

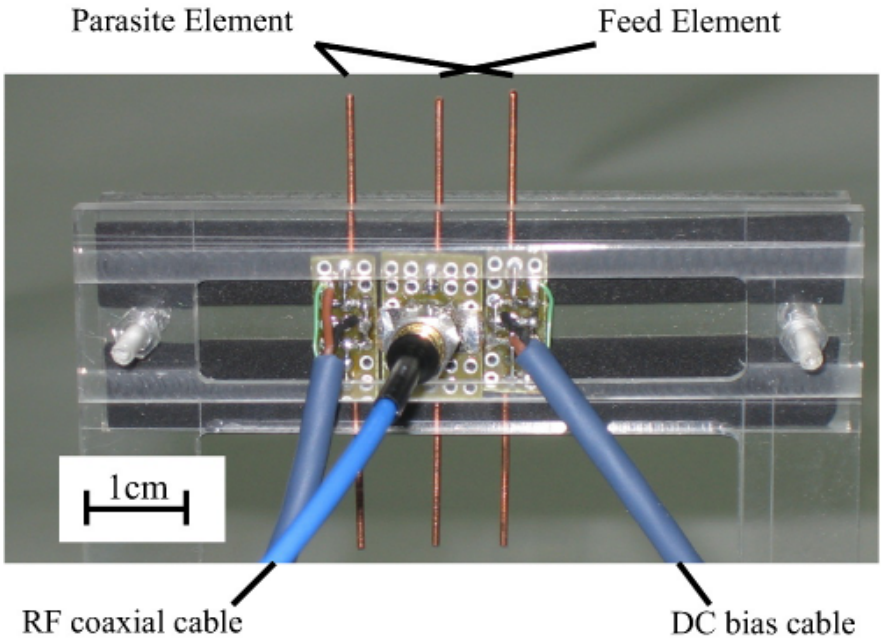



図 6.5　Prototyped 3-element dipole ESPAR antenna

表 6.2　3-element dipole ESPAR antenna maximum gain on a horizontal plane [dBi]

| | 3-element dipole | | | USB |
|---|---|---|---|---|
| varactor voltage | $d=\lambda/4$ | $d=\lambda/8$ | $d=\lambda/12$ | |
| $v_1=0$V,$v_2=2.25$V | -0.69 | -0.75 | 0.65 | -2.26 |
| $v_1=2.94$V,$v_2=4.02$V | -0.93 | -3.90 | -6.85 | -13.1 |
| $v_1=3.73$V,$v_2=4.02$V | -0.72 | -3.31 | -3.79 | -8.25 |

素子間隔 $\lambda/4$，$\lambda/8$，$\lambda/12$ における 3 素子ダイポールエスパアンテナの指向性測定および LLL，RDC を評価する．任意の 3 種類のバラクタ電圧についての利得 (放射効率や不整合損を含む) を表 6.2 に示す．LLL のバラクタ電圧平面マップを図 6.7 に，各素子間隔の RDC を表 6.3 に示す．

図 6.7 より，LLL の極値の位置および素子間隔変化による極値の推移がシミュレーション解析と一致する．表 6.3 より，$E[\rho_{rd}]$ は素子間隔 $\lambda/4$ のとき最大となり解析と一致する．しかし，素子間隔 $\lambda/8$ のとき最小と解析と異なる．その原因について，素子間隔 $\lambda/16$ と $\lambda/8$ の RDC 解析および測定結果は，その差が 0.01 と近い値を示していることから設計誤差であると考えられる．

以上より，3 素子ダイポールエスパアンテナの LLL および RDC の解析と測定結果はよ

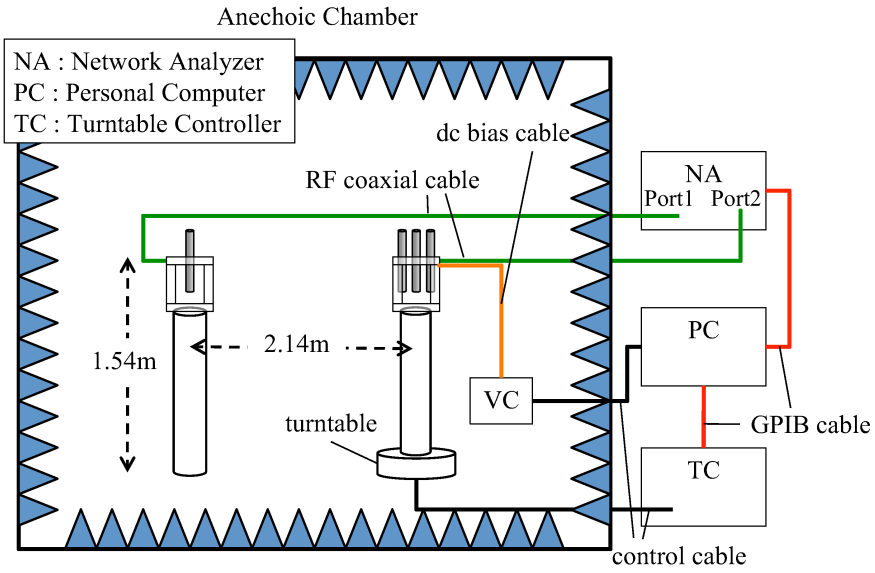



図 6.6　Measurement system of ESPAR antenna directivity

表 6.3　Relation between measured RDC and space between elements

| アンテナ | 3-element dipole | | | USB |
|---|---|---|---|---|
| 素子間隔 | $d=\lambda/12$ | $d=\lambda/8$ | $d=\lambda/4$ | $d=\lambda/16$ |
| $E[\rho_{rd}]$ | 0.626 | 0.611 | 0.674 | 0.670 |
| 理論値 | 0.617 | 0.630 | 0.669 | - |

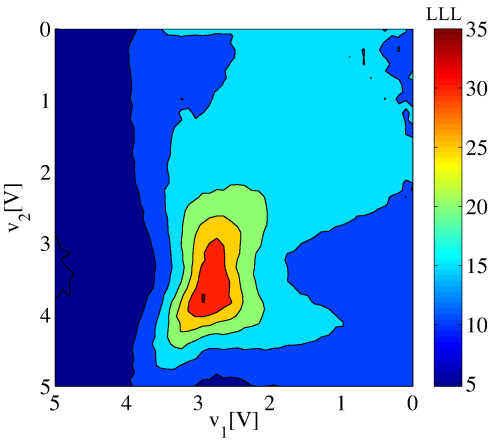
く一致している．

## 6.4　本章の結論

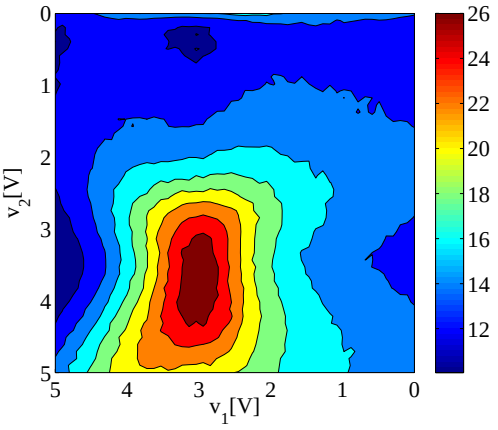
本章は 3 素子ダイポールエスパアンテナのアンテナ構造とアンテナ設計指標の関係について探究した．具体的には，指向性が多様に変化するリアクタンス範囲の追求，およびその時の指向性の多様性指標 RDC が最小となる，アンテナの素子間隔を示した．

6.1 節では，指向性の複雑性評価指標 LLL を用いて，各アンテナ素子間隔における最適なリアクタンス範囲を示した．結果，素子間隔が狭くなる程，最適なリアクタンス範囲は狭くなる傾向が得られた．その時の各アンテナ素子間隔における最適なリアクタンス範囲は，$\lambda/32$ で-23〜28Ω，$\lambda/16$ で-40〜40Ω，$\lambda/8$ で-80〜50Ω，$\lambda/4$ で-130〜30Ω $\lambda/2$ で-70〜150Ω を示した．

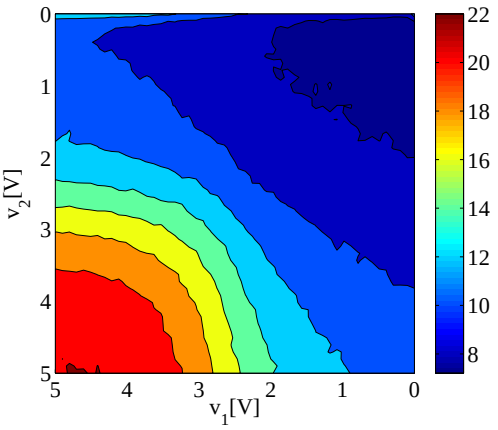
6.2 節では，指向性の多様性評価指標 RDC を用いて，RDC が最小となるアンテナ素子




(a) Space between elements: $\lambda/12$




(b) Space between elements: $\lambda/8$




(c) Space between elements: $\lambda/4$

図 6.7　LLL map on varactor voltage plane

間隔を明らかにした．結果，素子間隔 $\lambda$/16 のとき RDC が最も低くなることを示した．

従って，3 素子ダイポールエスパアンテナにおいて，無線秘密鍵生成共有方式のためのアンテナ構造は，素子間隔 $\lambda$/16，リアクタンス範囲-40〜40Ω，が適当であることを示した．

# 第 7 章

# USB スティック型エスパアンテナの試作および評価

本章は第 6 章で得た，無線秘密鍵生成共有方式に適した 3 素子エスパアンテナのリアクタンス範囲，素子間隔を基に，USB スティック型エスパアンテナを試作，評価する．試作する USB スティック型エスパアンテナは，無線秘密鍵生成共有システムをプラグアンドプレイできるよう試作する．

## 7.1 試作した USB スティック型エスパアンテナの構造

第 6 章で得られた 3 素子エスパアンテナが形成可能な指向性が多様となるリアクタンス範囲，素子間隔を基に，USB スティック型エスパアンテナを試作する．外観を図 7.1 に示す．試作する USB スティック型エスパアンテナは 1 枚プリント基板上にアンテナ，RF 信号源回路，バラクタ制御回路，USB コネクタを実装する．そして，パソコンにプラグインするだけで，無線秘密鍵生成共有方式が利用可能なアンテナとする．アンテナの構造は素子はモノポールとする．そして，第 6 章の結果より，素子間隔は $\lambda/16$ とする．可変リアクタンス回路は 3 素子ダイポールエスパアンテナと同様の回路を用いており，そのリアクタンス範囲は-68〜70Ω である．この範囲は，第 6 章で得られたリアクタンス範囲-40〜40Ω を十分に満たす．可変リアクタンス回路を制御する DAC は USB コネクタケーブルに接続されたパソコンにより制御する．

## 7.2 指向性パタンの測定およびアンテナ性能評価

USB スティック型エスパアンテナの指向性測定およびアンテナ性能評価を行う．試作したアンテナの測定系を図 6.6 で示す．ネットワークアナライザのポート 2 は，USB ス

ティック型エスパアンテナの給電素子に装荷された SMT コネクタに接続する．

測定した指向性の中で特徴的な形状を示す指向性パタン 3 種類を図 7.2 に示す．その指向性の利得 (放射効率や不整合損を含む) を表 6.2 に示す．FBR および LLL のバラクタ電圧平面マップを図 7.3 に，RDC の測定値を表 6.3 に示す．

図 7.2 より，試作したアンテナが多様な指向性パタンを形成できていることが見られる．しかし，表 6.2 から利得がバラクタの値よっては-13.1dBi と低い．これは，本来 RF 信号回路から給電される信号を，測定時では SMT コネクタを用いた給電に切り替えたことによる反射損失，指向性切り替えにともなう入力インピーダンス変動による反射損失，基板の誘電体損失，導体損失，およびバラクタの内部抵抗損が原因と考えられる．

図 7.3 より，素子間隔 $\lambda$/12 の時の 3 素子ダイポールエスパアンテナの LLL 測定結果と同じ形状のマップが得られている．LLL のダイナミックレンジは 3 素子ダイポールエスパアンテナの測定値よりも約 3 倍大きい．表 6.3 より，$E[\rho_{rd}]$ は 0.67 と，素子間隔 $\lambda$/4 の 3 素子ダイポールエスパアンテナと同じ値を示す．これら 3 素子ダイポールと異なる結果の原因はアンテナ形状が非対称性であること，材質が違うこと等が考えられる．

最後に，試作したアンテナについてアンテナ設計指標とアンテナの秘匿性の関係を示す．文献 [43] 文献 [44] 文献 [51] で用いられている従来の 3 素子ダイポールエスパアンテナ，RDC 最小となる最適素子間隔（$\lambda$/16）3 素子エスパアンテナ，USB スティック型エスパアンテナ，それぞれを用いた場合に無線秘密鍵生成共有システムが得られる Imac の一例を図 7.4 に示す．図 7.4 の右のグラフは，TRBC 伝搬モデルにおいて RNR が 20dB 以上のときのアンテナ設計指標 PDC と正規盗聴局間 RS 履歴相関係数 $\rho_e$ の関係を表す．左グラフは，RS 履歴を中央 2 値化処理で鍵生成した場合の，正規盗聴局間 RS 履歴相関係数 $\rho_e$ と鍵の秘匿性 Imac の関係を表す．図 7.4 より，従来の 3 素子ダイポールエスパアンテナと比較し，最適素子間隔 3 素子エスパアンテナは Imac が 0.04 ポイント向上，USB スティック型エスパアンテナは Imac が 0.01 ポイント向上する．

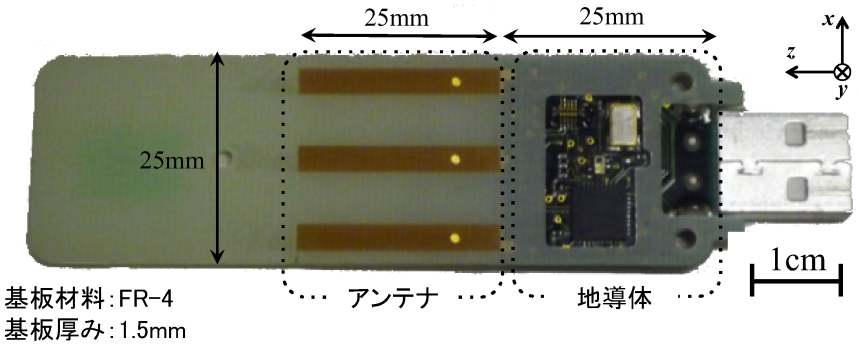
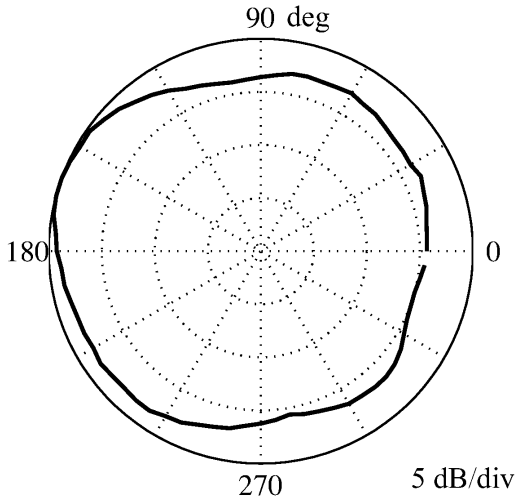
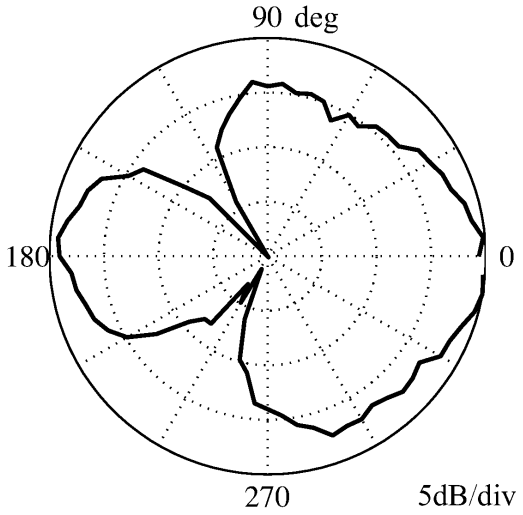


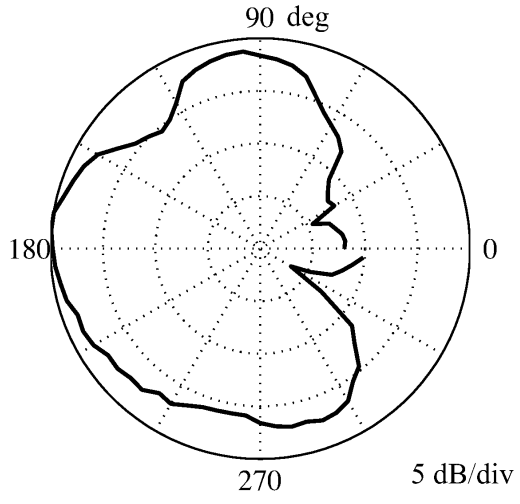

図 7.1　USB stick ESPAR antenna prototype




(a)$v_1 = 0V,\ \ v_2 = 2.25V$




(b)$v_1 = 2.94V,\ \ v_2 = 4.02V$




(c)$v_1 = 3.73V,\ \ v_2 = 4.02V$

図 7.2　USB stick ESPAR antenna directivity pattern examples (normalized)

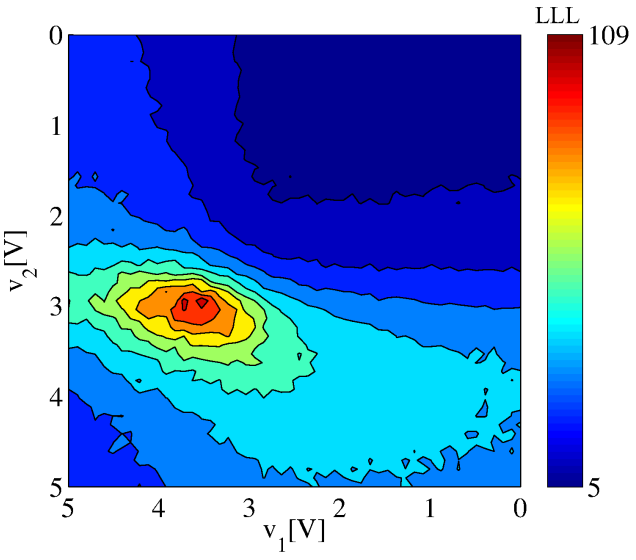



図 7.3　USB stick ESPAR antenna LLL map on varactor voltage plane

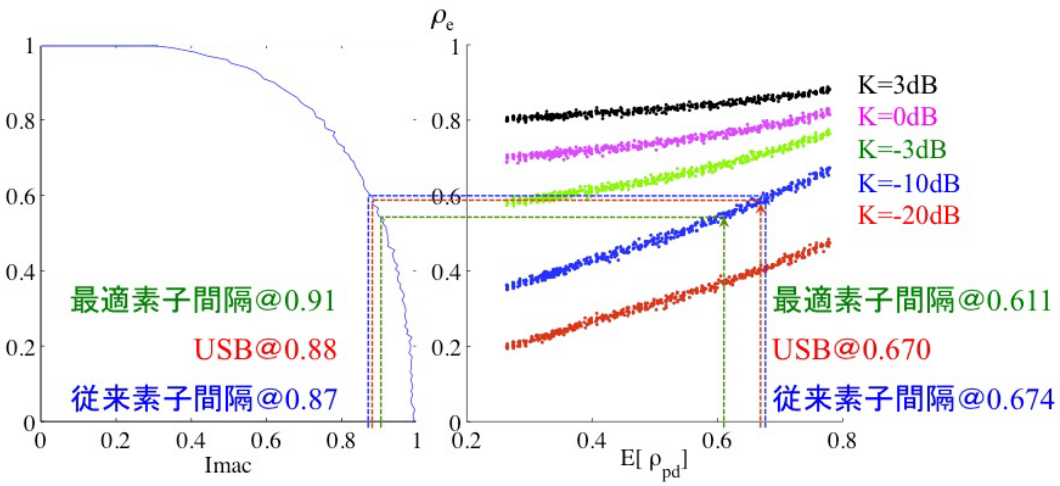



図 7.4　Imac of the wireless secret key agreement system with USB stick ESPAR antenna (TRBC propagation model, RNR=0dB)

まとめると，USB スティック型エスパアンテナは，従来の素子間隔 λ/4 の 3 素子ダイポールエスパアンテナより 1/8 小型化したにも関わらず，RDC は素子間隔 λ/4 の 3 素子ダイポールエスパアンテナに非常に近い値（有効 2 桁）が得られた．TRBC 伝搬路モデル（RNR=0dB，K 因子=-10dB）の伝搬環境において Imac は 0.01 ポイント向上する可能性を示した．しかし，指向性切り替えにともなう反射損失も大きいことから，今後は自動インピーダンス整合回路などの実装が重要である．

## 7.3 本章の結論

本章は USB スティック型エスパアンテナを試作し，評価した．試作した USB スティック型エスパアンテナは 1 枚プリント基板上にアンテナ，RF 信号源回路，バラクタ制御回路，USB コネクタを実装しており，パソコンにプラグインするだけで，無線秘密鍵生成共有方式が利用可能なアンテナとした．

試作した USB スティック型エスパアンテナは，素子間隔 $\lambda/4$ の 3 素子ダイポールエスパアンテナより 1/8 小型化したにも関わらず，RDC は素子間隔 $\lambda/4$ の 3 素子ダイポールエスパアンテナに非常に近い値（有効 2 桁）が得られた．TRBC 伝搬路モデル（RNR=0dB，K 因子=-10dB）の伝搬環境において Imac は 0.01 ポイント向上する可能性を示した．

# 第 8 章

# 結論

本論文は暗号技術の課題である鍵配送問題を解決する無線秘密鍵生成共有方式の秘匿性を高める可変指向性アンテナを設計および試作した．無線通信にとって暗号技術は不可欠である．一般に用いられる暗号技術の一つに共通鍵暗号プリミティブがある．共通鍵暗号プリミティブは，平文の暗号および復号に共通の秘密鍵を用いる．しかしながら，共通鍵を悪意ある第三者に漏れる事無く，正規局同士で共有しなければならない，鍵配送問題が大きな課題と言われている．鍵の配送問題の解決手法として可変指向性アンテナを用いた無線秘密鍵生成共有方式が提案されている．本方式は，正規局に可変指向性アンテナを搭載し，周辺環境の変化と指向性パタンの変化の両方を駆使して電波のゆらぎを起こし，この電波のゆらぎから鍵を生成共有する方式である．この無線秘密鍵生成共有方式に対し，文献 [29][43] は鍵生成に用いる複数の指向性パタンを選別することにより，鍵の秘匿性が向上することを示唆している．つまり，指向性パタン形成の本質であるアンテナの種類の選択および構造設計により，更なる鍵の秘匿性向上が期待できる．しかしながら，1）本方式の秘匿性を高めうるアンテナを見出すための指針，アンテナ設計指標は報告されていない．2）無線秘密鍵生成共有方式のための可変指向性アンテナを設計および試作した報告はない．という 2 つの課題がある．課題 1 に対して，本論文は無線秘密鍵生成共有方式の要である電波ゆらぎに着目し，指向性と電波ゆらぎの関係から，鍵の秘匿性を高めるアンテナ設計指標の提案を目指した．（第 2 章-第 4 章）課題 2 に対して，本論文は無線秘密鍵生成共有方式が計算資源を用いない小型無線通信端末への応用が期待されていることに着目し，可変指向性アンテナの 1 種であるエスパアンテナを基に，USB メモリスティック型エスパアンテナを設計試作を目指した．（第 5 章-第 7 章）以下に研究の成果を述べる．

第 2 章は第 4 章で用いる無線秘密鍵生成共有方式の鍵生成共有シミュレーターを構築するための基本知識について記述した．始めに可変指向性アンテナを用いた無線秘密鍵生成共有方式の基本原理を記述した．そして，本方式を用いて実際に行なわれる秘密鍵生成共有の手順について説明した．鍵生成共有の手順は第一フェーズの RS 履歴の生成共有と

第二フェーズの信号処理に大きく分けることができ，本論文では第一フェーズの RS 履歴の生成共有までとした．次に，鍵の安全性を評価する上で重要な秘密鍵の盗聴手法を説明した．盗聴には受動的盗聴法と能動的盗聴法があり，本論文は受動的盗聴法を用いた鍵の安全性評価を採用した．RS 履歴の生成共有に関して，その秘匿性を評価する指標，正規局間 RS 履歴の相関係数 $\rho_{ab}$ および正規盗聴局間 RS 履歴の相関係数 $\rho_e$ の 2 つを定義した．最後に鍵の秘匿性評価のための無線秘密鍵生成共有方式の鍵生成共有シミュレーションに用いる伝搬環境モデルとして，送受素波対応（TRBC）伝搬環境モデル，レイトレース法を定義，また可変指向性アンテナモデルとして，正規乱数アンテナモデル，フェーズドアレーモデルを定義した．

第 3 章は無線秘密鍵生成共有方式の秘匿性を向上が期待できる可変指向性アンテナの設計指標を提案した．提案したアンテナ設計指標は大きく分けて「指向性の複雑性評価指標」と「指向性の多様性評価指標」の 2 種類とした．指向性の複雑性評価指標は，方位角領域において指向性が複雑に変化していることを示す指標として，エンドファイア・ブロードサイド比（EBR），軌跡長（LLL），累積ビーム幅（CBW）の 3 種類を提案した．指向性の多様性評価指標は方位角領域および電気パラメータ領域において変化が多様（独立）であることを示す指標として，パラメータ領域指向性相関係数（PDC），指向性パタン相関係数（ADC）の 2 種類を提案した．

第 4 章は第 3 章で提案したアンテナ設計指標，EBR，LLL，CBW，PDC，ADC が RS 履歴の秘匿性向上に有用であることを検証した．RS 履歴の秘匿性評価は $\rho_{ab}$ および $\rho_e$ の 2 つを同時に考慮した．結果，TRBC 伝搬環境において，アンテナ設計指標による $\rho_{ab}$ の向上効果は期待できない結果が得られた．$\rho_e$ は，受信信号電力対雑音電力比（RNR）が 0dB 以上，直接波対反射波電力比（K 因子）が 10dB 以下の TRBC 伝搬環境において，アンテナの設計指標による値の低減が有効である結果が得られた．特に PDC による $\rho_e$ の低減効果が大きく，最大で 40% の低減効果を示した．また，RNR が-10dB 以上かつ K 因子が 3dB 以下の伝搬環境下で $\rho_e$ と PDC の相関性は 0.77 以上得られた．従って，本節は提案したアンテナ設計指標の中で最も RS 履歴の秘匿性向上に有効な指標は PDC であり，その向上効果が有効である伝搬環境は RNR が 0dB 以上かつ K 因子が 3dB 以下ということを明らかにした．通信は RNR が 0dB 以上の伝搬環境で行なわれ，見通し内室内環境において，K 因子は 3dB 程度であることから，一般的な室内環境の通信に用いる無線秘密鍵生成共有システムの秘匿性向上に PDC が有用であると言える．

第 5 章は無線秘密鍵生成共有方式のための可変指向性アンテナとして基となるエスパアンテナについて記述した．始めにエスパアンテナの動作原理およびその特徴について詳述した．次にエスパアンテナの指向性算出手法について説明した．算出法には等価ウェイトベクトル法と空間分布イミタンス行列法の 2 種類あり，本論文は，より指向性を厳密に算出することができる空間分布イミタンス行列法を採用した．

第 6 章は 3 素子ダイポールエスパアンテナのアンテナ構造と指向性の制御特性およびアンテナ設計指標の関係について探究した．無線秘密鍵生成共有方式のための 3 素子ダイポールエスパアンテナは素子間隔が RDC が最も低くなる波長/16 であること，リアクタンス範囲が-40〜40Ω，が適当であることを示した．

第 7 章は USB スティック型エスパアンテナを試作し，評価した．試作した USB スティック型エスパアンテナはパソコンにプラグインするだけで，無線秘密鍵生成共有方式が利用可能なアンテナとした．アンテナの構造は 3 素子モノポールとし，素子間隔は第 6 章得られた RDC が最も低くなる波長/16 とした．素子間隔が波長/4 の 3 素子ダイポールエスパアンテナと比較し，試作した USB スティック型エスパアンテナは，サイズは 1/8 小型化し，RDC は非常に近い値（有効 2 桁）を達成した．TRBC 伝搬環境モデル（RNR=0dB，K 因子=-10dB）の伝搬環境において Imac は 0.01 ポイント向上する可能性を示した．

以上をより，本論文は無線秘密鍵生成共有方式の秘匿性を高めるアンテナ設計指標 PDC を世の中で初めて提案，その有効性を示した．PDC を用いて無線秘密鍵生成共有方式のための USB メモリスティック型エスパアンテナを設計，試作した．今後の研究課題は，指向性切り替えによる入力インピーダンスの変動が原因による反射損失の低減，アンテナ設計指標の有効性の実機実験による検証，アンテナの更なる小型化，もしくは秘匿性向上設計，等が考えられる．

# 参考文献


[1] Ross Anderson（著），トップスタジオ（訳），情報セキュリティ技術大全 -信頼できる分散システム構築のために-，pp.73-113，日経 BP 社，東京，2002.

[2] 宮地充子，菊池浩明，情報セキュリティ，オーム社，東京，2003.

[3] 辻井重男，趙晋輝，“楕円暗号へのガイダンス，” 信学論（A），vol.J82-A, no.8, pp.1200-1211, Aug. 1999.

[4] P.W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” Society for Industrial and Applied Mathematics Journal on Computing, vol.26, no.5, pp.1484-1509, Oct. 1997.

[5] 西野哲朗，量子コンピュータと量子暗号，岩波書店，東京，2002.

[6] 広田修, “光通信ネットワークと量子暗号, ” 信学論（B）, vol.J87-B, no.4, pp.478-486, Apr. 2004.

[7] 小柴健史, “量子公開鍵暗号の安全性概念, ” 信学論（A）, vol.J90-A, no.5, pp.367-375, May 2007.

[8] J.E. Hershey, A.A. Hassan, and R. Yarlagadda, “Unconventional Cryptographic Keying Variable Management,” IEEE Trans. Communications, vol.43, no.1, pp.3-6, Jan. 1995.

[9] H. Koorapaty, A.A. Hassan, and S. Chennakeshu, “Secure Information Transmission for Mobile Radio,” IEEE Communications Letters, vol.4, no.2, pp.52-55, Feb. 2000.

[10] A.O. Here, “Secure Space-Time Communication,” IEEE Trans. Information Theory, vol.49, no.12, pp.3235-3249, Dec. 2003.

[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），vol.J87-A, no.10, pp.1320-1328, Oct. 2004.

[12] Z. Li, W. Xu, R. Miller, and W. Trappe, “Securing Wireless Systems via Lower Layer Enforcements,” ACM Workshop on Wireless Security, WiSe2006, California, USA, Sep. 2006.

[13] R. Wilson, D. Tse, and R.A. Scholtz, “Channel Identification: Secret Sharing Using Reciprocity in Ultrawideband Channels,” IEEE Trans. Inform. Forensics and Security,

vol.2, no.3, pp.364-375, Sep. 2007.

[14] 岩井誠人，笹岡秀一，“電波伝搬特性を活用した秘密鍵の伝送・共有技術，” 信学論（B）, vol.J90-B, no.9, pp.770-783, Sep. 2007.

[15] J. Wallace, “Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits,” IEEE International Conference on Communications 2009, pp.1-5, Dresden, Germany, Jun. 2009.

[16] 安川真平，岩井誠人，笹岡秀一，“OFDM の伝送路特性に基づく秘密鍵共有方式における冗長性除去及び雑音低減法，” 信学論（B）, vol.J92-B, no.10, pp.1708-1711, Oct. 2009.

[17] N. Patwari, J. Croft, S. Jana, and S.K. Kasera, “High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements,” IEEE Trans. Mobile Computing, vol.9, no.1, pp.17-30, Jan. 2010.

[18] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N.B. Mandayam, “Information-Theoretically Secret Key Generation for Fading Wireless Channels,” IEEE Trans. Inform. Forensic and Security, vol.5, no.2, pp.240-254, Jun. 2010.

[19] C.C. Chang, H.C. Tsai, “An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks,” IEEE Trans. Wireless Communications, vol.9, no.11, pp.3346-3353, Nov. 2010.

[20] T. Shimizu, H. Iwai, H. Sasaoka, and A. Paulraj, “Secret Key Agreement Based on Radio Propagation Characteristics in Two-Way Relaying Systems,” IEEE Global Communications Conference 2010, GLOBECOM 2010, pp.1-6, Florida, USA, Dec. 2010.

[21] C. Chen, and M.A. Jensen, “Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients,” IEEE Trans. Mobile Computing, vol.10, no.2, pp.205-215, Feb. 2011.

[22] Q. Wang, H. Su, K. Ren, and K. Kim, “Fast and Scalable Secret Key Generation Exploiting Channel Phase Randomness in Wireless Networks,” IEEE International Conference on Computer Communications 2011, INFOCOM2011, pp.1422-1430, Shanghai, China, Apr. 2011.

[23] K. Ren, H. Su, and Q. Wang, “Secret Key Generation Exploiting Channel Characteristics in Wireless Communications,” IEEE Wireless Communications, vol.18, no.4, pp.6-12, Aug. 2011.

[24] A. Agrawal, Z. Rezki, A.J. Khisti, and M. Alouini, “Noncoherent Capacity of Secret-Key Agreement with Public Discussion,” IEEE Trans. Inform. Forensic and Security, vol.6, no.3, pp.565-574, Sep. 2011.

[25] T. Shimizu, H. Iwai, and H. Sasaoka, “Physical-Layer Secret Key Agreement in Two-

Way Wireless Relaying Systems," IEEE Trans. Inform. Forensic and Security, vol.6, no.3, pp.650-660, Sep. 2011.

[26] A. Khisti, S.N. Diggavi, and G.W. Wornell, "Secret-Key Agreement with Channel State Information at the Transmitter," IEEE Trans. Inform. Forensic and Security, vol.6, no.3, pp.672-681, Sep. 2011.

[27] Y.E.H. Shehadeh, O. Alfandi, and D. Hogrefe, "Towards Robust Key Extraction from Multipath Wireless Channels," Journal of Communications and Networks, vol.14, no.4, pp.385-395, Aug. 2012.

[28] T. Shimizu, H. Iwai, and H. Sasaoka, "Group Secret Key Agreement Based on Radio Propagation Characteristics in Wireless Relaying Systems," IEICE Trans. Communications, vol.E95-B, no.7, Jul. 2012.

[29] 森浩樹，笹岡秀一，大平孝，"受信信号強度の空間相関に基づく秘密鍵生成に適したアンテナパターンの検討，" 信学技報, AP2003-188, pp.47-52, Nov. 2003.

[30] 樋口啓介，青野智之，大平孝，笹岡秀一，"エスパアンテナを用いた無線秘密鍵共有方式における共有秘密鍵の空間相関特性シミュレーション，" 信学技報, AP2004-42, pp.7-12, Jul. 2004.

[31] 青野智之，樋口啓介，大平孝，小宮山牧兒，笹岡秀一，"エスパアンテナを用いたIEEE802.15.4 無線秘密鍵共有システム，" 信学論（B）, vol.J88-B, no.9, pp.1801-1812, Sep. 2005.

[32] 小川佳彦，笹岡秀一，今井友裕，湯田泰明，三好憲一，本間光一，"送受両側で位相制御を行った MIMO-OFDM システムにおけるチャネル行列の固有値変動に基づく秘密鍵共有方式の検討，" 信学論（B）, vol.J88-B, no.9, pp.1789-1800, Sep. 2005.

[33] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, H. Sasaoka, "Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channels," IEEE Trans. Antenna and Propagation, vol.53, no.11, pp.3776-3784, Nov. 2005.

[34] 北浦明人，岩井誠人，笹岡秀一，"陸上移動通信におけるアンテナ切換による受信信号強度変化を利用した秘密鍵共有方式，" 信学論（B）, vol.J90-B, no.3, pp.315-317, Mar. 2007.

[35] 長谷川拓，成田譲二，上原秀幸，大平孝，"両端末に 3 素子エスパアンテナを用いた秘密鍵共有システムにおける秘匿条件付き相互情報量，" 信学技報, RCS2008-3, pp.13-18, May. 2008.

[36] 長谷川拓，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共有システムにおいて秘匿条件付相互情報量 Imac を高めるための指向性セット選択法，" 信学技報, SIP2008-151, pp.161-166, Jan. 2009.

[37] 大西将弘，北野隆康，岩井誠人，笹岡秀一，"エスパアンテナを用いた無線秘密鍵

共有方式における干渉信号送信に基づく盗聴耐性向上法，” 信学技報, AP2009-54, pp.59-64, Jul. 2009.

[38] 清水崇之，岩井誠人，笹岡秀一，“エスパアンテナを用いた秘密鍵共有方式における盗聴耐性の高い鍵生成法，” 信学論（B）, vol.J92-B, no.9, pp.1348-1361, Sep. 2009.

[39] K. Zeng, D. Wu, An Chan, and P. Mohapatra, “Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks,” IEEE International Conference on Computer Communications 2010, INFOCOM2010, pp.1-9, California, USA, Mar. 2010.

[40] J.W. Wallace, R.K. Sharma, “Automatic Secret Keys From Reciprocal MIMO Wireless Channels: Measurement and Analysis,” IEEE Trans. Information Forensics and Security, vol.5, no.3, pp.381-392, Sep. 2010.

[41] T. Saito, K. Uematsu, T. Hasegawa, H. Uehara, and T. Ohira, “A New Scheme for Anti-Tapping Tolerance Enhancement in Wireless Secret Key Generator Utilizing Horizontally-Polarized ESPAR Antennas,” 2010 Asia-Pasific Radio Science Conference, AP-RASC2010, 1 page, Toyama, Japan, Sep. 2010.

[42] V. Korzhik, V. Yakovlev, G. Morales-Luna, D. Ovechkin, and Y. Kovajkin, “Wireless Secret Key Sharing Based on the Use of a Variable-Directional Antenna Over Multipath Channels,” International Symposium ELMAR 2010, pp.277-279, Zadar, Croatia, Sep. 2010.

[43] 長谷川拓，斉藤隆史，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）, vol.J94-B, no.2, pp.214-225, Feb. 2011.

[44] 植松和正，斎藤隆史，上原秀幸，大平孝，“エスパアンテナを用いた無線秘密鍵生成システムの実証実験，” 信学技報, AP2010-186, pp.77-82, Mar. 2011.

[45] 北野隆康，岩井誠人，笹岡秀一，“MIMO 固有ビーム空間分割多重伝送における秘密情報伝送，” 信学論（B）, vol.J94-B, no.2, pp.85-93, Jun. 2011.

[46] 西田陽，清水崇之，岩井誠人，笹岡秀一，“FDTD 法によるアレーアンテナを用いた無線秘密鍵共有方式の盗聴耐性評価，” 信学技報, AP2011-35, pp.47-50, Jul. 2011.

[47] T. Yoshida, T. Saito, K. Fujiki, K. Uematsu, H. Uehara, and T. Ohira, “Impact of Direct-Path Wave on Imac in Secret Key Agreement System Using ESPAR Antennas,” URSI General Assembly, URSI-GA 2011, 4 pages, Istanbul, Turkey, Aug. 2011.

[48] 前田正彦，岩井通，窄口優人，相河聡，“アレーアンテナを用いた秘密鍵生成における鍵生成高速化技術の安全性評価，” 信学論（B）. vol.J94-B, no.11, pp.1494-1497, Nov. 2011.

[49] 藤木雄大，吉田斉史，斎藤隆史，坂井尚貴，上原秀幸，大平 孝，“無線秘密鍵共有シス

テムに対する能動的盗聴法の提案と実証，” 信学技報, MW2012-207, pp.43-48, Mar. 2012.

[50] M.G. Madiseh, W. Neville, and M.L. McGuire, “Applying Beamforming to Address Temporal Correlation in Wireless Channel Characterization Based Secret Key Generation,” IEEE Trans. Information Forensics and Security, vol.7, no.4, pp.1278-1287, Aug. 2012.

[51] 大森陽介，吉田斉史，坂井尚貴，上原秀幸，大平孝，“無線秘密鍵共有方式において両端末ともにエスパアンテナを用いることによる盗聴耐性向上，” 信学技報, MW2012-103, pp.125-128, Oct. 2012.

[52] 坂井尚貴，小田康明，ウリントヤ，上原秀幸，大平孝，“無線秘密鍵生成共有方式の秘匿性を高める可変指向性アンテナ指向性多様性指標の提案，” 信学技報, AP2012-125, pp.19-24, Jan. 2013.

[53] T. Yoshida, Y. Omori, N. Sakai, T. Ohira, “Imac Enhancement Exploiting the Eigenvalue of RadioWave Fluctuation in Secret Key Agreement System,” 2013 Asia-Pacific Radio Science Conference AP-RASC2013, 1 page, Taipei, Taiwan, Sep. 2013.

[54] C.A. Balanis, Antenna Theory -Analysis and Design- Third Edition, John Wiley and Sons, Inc., New Jersey, 2005.

[55] 後藤尚久，図解・アンテナ，電子情報通信学会，東京，1995.

[56] 後藤尚久，アンテナがわかる本 なるほどナットク!，オーム社，東京，2005.

[57] R. Harrington, “Reactively Controlled Directive Arrays,” IEEE Trans. Antenna and Propagation, vol.26, no.3, pp.390-395, May. 1978.

[58] T. Ohira and K. Gyoda, “Electronically Steerable Passive Array Radiator Antennas for Low-Cost Analog Adaptive Beamforming,” IEEE International Conference on Phased Array Systems and Technology 2000, pp.101-104, California, USA, May 2000.

[59] Q. Han, K. Inagaki, K. Iigusa, R. Schlub, T. Ohira, and M. Akaike, “Harmonic Distortion Suppression Technique for Varactor-Loaded Parasitic Radiator Antennas,” IEICE Trans. Electronics, vol.E85-C, no.12, pp.2015-2021, Dec. 2002.

[60] 秋山章，行田弘一，大平孝，安藤真，“エスパアンテナのビーム及びヌル形成能力に関する数値シミュレーション，” 信学論（B）, vol.J85-B, no.12, pp.2234-2244, Dec. 2002.

[61] 飯草恭一，“エスパアンテナの構造パラメータを遠方界より計算する方法，” 信学技報, AP2003-35, pp.53-60, May 2003.

[62] R. Schlub, J. Lu, and T. Ohira, “Seven-Element Ground Skirt Monopole ESPAR Antenna Design from a Genetic Algorithm and the Finite Element Method,” IEEE Trans. Antenna and Propagation, vol.51, no.11, pp.3033-3039, Nov. 2003.

[63] 大平孝，飯草恭一，“電子走査導波器アレーアンテナ，” 信学論（C）, vol.J87-C, no.1, pp.12-31, Jan. 2004.

[64] J. Lu, D. Ireland, and R. Schlub, “Development of ESPAR Antenna Array Using Numerical Modeling Techniques,” International Conference on Computational Electromagnetics and Its Applications 2004, ICCEA 2004, pp.182-185, Beijing, China, Nov. 2004.

[65] H. Kawakami and T. Ohira, “Electrically Steerable Passive Array Radiator (ESPAR) Antennas,” IEEE Antennas Propagation Magazine, vol.47, no.2, pp.43-50, Apr. 2005.

[66] J. Lu, D. Ireland and R. Schlub, “Dielectric Embedded ESPAR (DE-ESPAR) Antenna Array for Wireless Communications,” IEEE Trans. Antenna and Propagation, vol.53, no.8, pp.2437-2443, Aug. 2005.

[67] 坂井尚貴，上原秀幸，大平孝，“3 素子エスパアンテナの試作と性能評価実験，” 信学技報, AP2008-66, pp.165-170, Jul. 2008.

[68] S.A. Mitilineos, K.S. Mougiakos, and S.C.A. Thomopoulos, “Design and Optimization of ESPAR Antennas via Impedance Measurements and a Genetic Algorithm,” IEEE Antennas and Propagation Magazine, vol.51, no.2, pp.118-123, Apr. 2009.

[69] B. Alshami, H. Aboulnour, and M. Did, “Design of a Broadband ESPAR Antenna,” Mediterranean Microwave Symposium 2009, MMS 2009, pp.1-6, Tangiers, Morocco, Nov. 2009.

[70] N. Sakai, H. Uehara, and T. Ohira, “Variable Beamforming Characterization of a 3-Element Dipole ESPAR Antenna from a Complexity-of-Directivity Viewpoint,” Asia-Pacific Microwave Conference 2009 APMC2009, 4 pages, Suntec City, Singapore, Dec. 2009.

[71] T. Hassan, A. Kausar, H. Umair, and M.A. Anis, “Gain Optimization of a Seven Element ESPAR Antenna Using Quasi-Newton Method,” IEEE International Conference on Microwave Technology and Computational Electromagnetics 2011, ICMTCE2011, pp.293-296, Beijing, China, May 2011.

[72] H.T. Liu, S. Gao, and T.H. Loh, “Electrically Small and Low Cost Smart Antenna for Wireless Communication,” IEEE Trans. Antenna and Propagation, vol.60, no.3, pp.1540-1549, Mar. 2012.

[73] J.J. Luther, S. Ebadi, and X. Gong, “A Microstrip Patch Electronically Steerable Parasitic Array Radiator (ESPAR) Antenna with Reactance-Tuned Coupling and Maintained Resonance,” IEEE Trans. Antenna and Propagation, vol.60, no.4, pp.1803-1813, Apr. 2012.

[74] R.H. Clarke, “A Statistical Theory of Mobile-Radio Reception,” Bell Syst. Tech. Journal, vol.47, pp.957-1000, 1968.

[75] 高畑文雄，ディジタル無線通信入門, pp.143-174, 培風館, 東京, 2002.

[76] T.K. Sarkar, Z. Ji, K. Kim, A. Medouri, and M.S.-Palma, “A Survey of Various Propagation Models for Mobile Communication,” IEEE Antennas and Propagation Magazine, vol.45, no.3, pp.51-82, Jun. 2003.

[77] H. Hashemi, “The Indoor Radio Propagation Channel,” Proceedings of the IEEE, vol.81, no.7, pp.943-968, Jul. 1993.

[78] 岩井誠人，移動通信における電波伝搬 -無線通信シミュレーションのための基礎知識-, pp.132-142, コロナ社, 東京, 2012.

[79] J.W. McKown and R.L. Hamilton, “Ray Tracing as a Design Tool for Radio Networks,” IEEE Network Magazine, vol.5, no.6, pp.27-30, Nov. 1991.

[80] 今井哲朗，“レイトレーシング法による移動伝搬シミュレーション，” 信学論（B），vol.J92-B, no.9, pp.1333-1347, Sep. 2009.

[81] 高田潤一，朱厚涛，“移動体およびワイヤレス通信における多重は伝搬シミュレーションマイクロセル環境におけるレイトレース法の適用，” 信学技報，マイクロ波シミュレータ研究会, 7 pages, Mar. 2003.

[82] Z. Blazevic, I. Zanchi, and I. Marinovic, “Scaled Measurements and Ray-Tracing Simulations of Multipath Propagation Radio Channels,” International Conference on Applied Electromagnetics and Communications 2005, ICECom 2005, pp.1-5, Dubrovnik, Croatia, Oct. 2005.

[83] 井上恵輔，丹後俊宏，岩井誠人，笹岡秀一，“他地点観測信号に基づく伝搬路特性推定法の特性解析，” 信学技報, AP2007-74, pp.1-6, Aug. 2007.

[84] Y. Lustmann and D. Porrat, “Indoor Channel Spectral Statistics, K-Factor and Reverberation Distance,” IEEE Trans. Antenna and Propagation, vol.58, no.11, pp.3685-3692, Nov. 2010.

[85] V. Nikolopoulos, M. Fiacco, S. Stavrou, and S.R. Saunders, “Narrowband Fading Analysis of Indoor Distributed Antenna Systems,” IEEE Antenna and Wireless Propagation Letters, vol.2, no.1, pp.89-92, Feb. 2003.

[86] D. Fedorov, “NEC-2 for MMANA by UA3AVR,” http://www.qsl.net/ua3avr/, Jul. 2013.

# 謝辞

本博士論文をまとめるにあたり，多くの方のご指導とご協力を賜り，完成することができました．研究指導に加えて，書類の書き方など研究者として生きていく術を多忙な中教えて頂きました，豊橋技術科学大学電気・電子情報工学系 大平孝教授，上原秀幸教授，久留米工業高等専門学校 ウリントヤ准教授に心から感謝いたします．研究を進めるにあたり，情報・知能工学系 梅村恭司教授，本学電気・電子情報工学系 宮路祐一助教に貴重なご意見を賜りました．ここに感謝いたします．毎年，三研究室合同ゼミで研究のご指導ご鞭撻を頂きました，同志社大学理工学部電子工学科 笹岡秀一教授，岩井誠人教授，兵庫県立大学工学研究科電気系工学専攻 相河聡教授に深く感謝申し上げます．エスパアンテナの設計試作をするにあたり，通菱テクニカ株式会社生産技術推進センター 木崎一廣様には一方ならぬお世話になりました．深く感謝いたします．本研究の遂行にあたり文部科学省グローバル COE プログラムより多大なる支援を受けました．研究室生活で日常生活から研究に至るまで，波動工学研究室，ワイヤレス通信研究室の諸先輩方，同輩，後輩一同に数多くの助言を頂きました．ありがとうございます．あらゆる面で苦楽を共にし，心の支えとなってくれた，友人一同には感謝の念に堪えません．最後に，大学生活を経済的，精神的に支えてくれた家族に，深く感謝の意を表します．

# 研究業績目録

## 学術論文（査読あり）

(A1) 坂井尚貴，小田康明，ウリントヤ，上原秀幸，大平孝，“無線秘密鍵生成共有方式の盗聴耐性を高める可変指向性アンテナ指向性多様性指標，” 信学論（B）, vol.J96-B, no.9, pp.936-944, Sep. 2013.

(A2) 坂井尚貴，小田康明，ウリントヤ，上原秀幸，大平孝，“無線秘密鍵生成共有方式用USB スティック型エスパアンテナ，” 信学論（B）, vol.J96-B, no.9, pp.1057-1066, Sep. 2013.

## 国際学会発表（査読あり）

(A3) T. Yoshida, Y. Omori, N. Sakai, and T. Ohira, “Imac Enhancement Exploiting the Eigenvalue of RadioWave Fluctuation in Secret Key Agreement System,” 2013 Asia-Pacific Radio Science Conference, AP-RASC2013, 1 page, Taipei, Taiwan, Sep. 2013.

(A4) Y. Suzuki, T. Sugiura, N. Sakai, M.Hanazawa, and T. Ohira, “Dielectric Coupling from Electrified Roadway to Steel-Belt Tires Characterized for Miniature Model Car Running Demonstration,” IEEE MTT-S International MicrowaveWorkshop Series on Innovative Wireless Power Transmission, IMWS-IWPT2012, pp.35-38, Kyoto, Japan, May 2012.

(A5) M. Hanazawa, N. Sakai, and T. Ohira, “SUPRA: Supply Underground Power to Running Automobiles,” IEEE International Electric Vehicle Conference, IEVC2012, pp.1-4, Greenville, SC, Mar. 2012.

(A6) N. Sakai, H. Uehara, and T. Ohira, “Variable Beamforming Characterization of a 3-Element Dipole ESPAR Antenna from a Complexity-of-Directivity Viewpoint,” Asia-Pacific Microwave Conference 2009, APMC2009, pp.751-754, Suntec City, Singapore, Dec. 2009.

## 国際学会発表（査読なし）

(A7) Naoki Sakai, “Performance Estimation of Secret Key Agreement System Using ESPAR Antennas,” IEEE AP/MTT-S Midland Student Express 2012 Autumn, Kanazawa, Japan, Nov. 2012.

(A8) Naoki Sakai, “Power Feed to Running Electric Vehicles via Road-to-Tire Capacitive Coupling,” IEEE AP/MTT-S Midland Student Express 2011 Autumn, S2-2, Kanazawa, Japan, Nov. 2011.

(A9) Naoki Sakai, “Antenna Design Criteria to Enhance Privacy for Wireless Secret Key Schemes,” IEEE AP/MTT-S Midland Student Express 2011 Spring, S1-6, Nagoya, Japan, Nov. 2011.

## 国内学会発表

(A10) 佐藤 翔一，水谷豊，坂井 尚貴，大平 孝，“リアルタイム負荷追従インピーダンス自動整合回路の提案，” 信学技報, MW2013-92, pp.23-28, Sep. 2013.

(A11) 鈴木良輝，鳥井俊宏，坂井尚貴，大平孝，“電化道路電気自動車 EVER の実証実験，” ワイヤレス・テクノロジ・パーク アカデミアプログラム, 横浜, May 2013.

(A12) 佐藤翔一，小田康明，坂井尚貴，上原秀幸，大平孝，“平板型 3 素子エスパアンテナの指向性可変性能の素子形状依存性，” 信学総大, B-1-124, page 124, Mar. 2013.

(A13) 坂井尚貴，小田康明，ウリントヤ，上原秀幸，大平孝，“無線秘密鍵生成共有方式の秘匿性を高める可変指向性アンテナ指向性多様性指標の提案，” 信学技報, AP2012-125, pp.19-24, Jan. 2013.

(A14) 杉浦貴光，鈴木良輝，坂井尚貴，ウリントヤ，大平孝，“電化道路電動カート EVER 用高効率整流回路，” 信学技報, WPT, pp.7-12, Dec. 2012.

(A15) 大森陽介，吉田斉史，坂井尚貴，上原秀幸，大平孝，“無線秘密鍵共有方式において両端末ともにエスパアンテナを用いることによる盗聴耐性向上，” 信学技報, MW2012-103, pp.125-128, Oct. 2012.

(A16) 鈴木良輝，鳥井俊宏，水谷豊，杉浦貴光，坂井尚貴，上原秀幸，大平 孝，“車両タイヤによるゼロギャップ無線電力伝送，” ワイヤレス・テクノロジ・パーク アカデミアプログラム, 横浜, July 2012.

(A17) ウリントヤ，南昂孝，崎原孫周，坂井尚貴，大平孝，“伝送線路帰還型 FET 発振回路における最大有能 Q ファクタ MAQ 理論，” 信学技報, MW2012-18, pp.1-4, Jun. 2012.

(A18) 藤木雄大，吉田斉史，斎藤隆史，坂井尚貴，上原秀幸，大平孝，“無線秘密鍵共有システムに対する能動的盗聴法の提案と実証，” 信学技報, MW2012-207, pp.43-48,

Mar. 2012.

(A19) 高谷侑希，小田康明，菊池祐樹，森 翔太，坂井尚貴，上原秀幸，大平孝，“前後方向指向性切り替え H 形エスパアンテナ，” 信学技報, MW2012-207, pp.49-54, Mar. 2012.

(A20) 小田康明，菊池祐樹，高谷侑希，森翔太，タンソパンナー，坂井尚貴，上原秀幸，大平孝，“3 素子エスパアンテナの素子上電流分布の数式モデル構築，” 信学総大, B-1-133, 1 page, Mar. 2011.

(A21) 森翔太，菊池祐樹，高谷侑希，タンソパンナー，坂井尚貴，上原秀幸，大平孝，“2 素子エスパアンテナの指向性可変性能の素子長・素子間隔依存性，” 信学技報, AP2010-111, pp.113-118, Dec. 2010.

(A22) 森翔太，菊池祐樹，タンソパンナー，坂井尚貴，上原秀幸，大平孝，“平行平板エスパアンテナの指向性可変特性，” 信学技報, MW2010-26, pp.1-6, Jun. 2010.

(A23) 菊池祐樹，森翔太，タンソパンナー，坂井尚貴，上原秀幸，大平孝，“エスパアンテナの放射指向性を高速かつ厳密に計算する空間分布イミタンス行列法，” 信学総大, B-1-126, 1 page, Mar. 2010.

(A24) 小林真純，坂井尚貴，ウリントヤ，上原秀幸，大平孝，“ゲートとソースにスタブを装荷した FET 発振回路の基本設計，” 信学技報, MW2009-29, pp.57-62, Jun. 2009.

(A25) 坂井尚貴，三谷友彦，上原秀幸，大平孝，“3 素子エスパアンテナの水平面内指向性の測定およびモーメント法解析，” 信学技報, SPS2008-23, pp.25-30, Mar. 2009.

(A26) 坂井尚貴，上原秀幸，大平孝，“3 素子エスパアンテナの試作と性能評価実験，” 信学技報, AP2008-66, pp.165-170, Jul. 2008.

(A27) 坂井尚貴，上原秀幸，大平孝，“平面エスパアンテナが張ることができる複素指向性空間の次元数，” 信学技報, AP2008-33, pp.23-28, Jun. 2008.

(A28) 坂井尚貴，上原秀幸，大平孝，“3 素子エスパアンテナが形成し得る直交指向性の個数，” 信学総大, B-1-90, 1 page, Mar. 2008.

(A29) 坂井尚貴，上原秀幸，大平孝，“3 素子エスパアンテナの指向性のリアクタンスと素子間隔依存性，” 信学技報, AP2007-120, pp.29-34, Dec. 2007.

## 特許

(A30) 大平 孝，坂井尚貴，藤木雄大，斎藤隆史，吉田斉史，「管理局、無線秘密鍵管理システム及びその方法」, 特許出願 2011-203862, 2011.9.16.

(A31) 大平 孝，ウリントヤ，坂井尚貴，鈴木良輝，水谷豊，「電力伝送路」, 特許出願 2013-107987, 2013.5.22.

## 受賞

(A32) 次世代イノベーションキーテクノロジ部門 準ブランプリ，CEATEC2012，2012 年 10 月.

(A33) 大学展示優秀発表賞，Microwave Workshop and Exhibition 2011，2011 年 12 月.

(A34) センシングアーキテクト優秀活動賞，豊橋技術科学大学，2011 年 3 月.

(A35) Excellent Student Award, IEEE Nagoya section, 2010 年 3 月.

(A36) 学生奨励賞，アンテナ・伝播研究専門委員会，2008 年 12 月.

(A37) 学生研究奨励賞，社団法人電子情報通信学会東海支部，2008 年 6 月.

## その他

(A38) 坂井尚貴，“「1G:石炭 2G：石油 3G：電池」に続く第 4 世代自動車，”NE ジャパン ワイヤレス・テクノロジー・アワード 2013 記念講演，東京国際展示場，東京都，2013 年 5 月.

(A39) 豊橋技術科学大学グローバル COE　ポスターコンペティション研究費獲得，2011 年.

(A40) 電子情報通信学会東海支部　豊橋技術科学大学　学生ブランチ代表，2011 年.

(A41) 豊橋技術科学大学グローバル COE　研究デモ機・展示物等の製作助成費獲得，2010 年.

(A42) 豊橋技術科学大学グローバル COE　センシング・アーキテクトシンポジウム実行委員，2010 年.

# 付録

## 付録 A　エスパアンテナプログラム

数値計算言語 Matlab を用いてエスパアンテナの指向性を算出する．パラサイト素子のリアクタンス値 [Ω] のベクトル「Pvec」を引数，指向性ベクトル「direc」を返り値とする．

```
-------------------------------------------------------------------------
function direc=DirectivityOfPAA(Pvec)

%Calculate input voltage
global vs;% エスパアンテナの電源電圧
global rs;% エスパアンテナの電源抵抗
global Im;% 虚数 i
global umat;% 単位行列
global Ymat;% アレーアンテナの多ポート回路網のアドミタンス行列
global intYmat;% アレーアンテナの単位電流分布を積分して求めたアドミタンス行列.
global ita;% 特性インピーダンス
global waveNum;% 波数
global alpha;% アレーファクタ


expPvec=[1;exp(Im*Pvec)];

% 入力電圧ベクトルの計算
Vvec=vs*inv(rs*inv(Ymat)+umat)*expPvec;

% 電流分布の積分値ベクトルの計算
Ivec=invYmat*Vvec;
% 各素子の遠方界 [V/m] の計算
Eele = ita*Im*waveNum*exp(-Im*waveNum).*(Ivec./(4*pi));
% 指向性の計算
direc = alpha*Eele;%[V/m]

end
-------------------------------------------------------------------------
```

# 付録 B　レイトレース法による伝搬路特性計算プログラム

数値計算言語 Matlab を用いて 2 次元レイトレース法による長方形部屋の伝搬路特性を算出する．正規送信局の位置座標「terminalT」，正規受信局の位置座標「terminalR」を引数，各伝搬路の距離「direc」，各素波の放射角度「phiT」，各素波の入射角度「phiR」，各素波の壁による反射損失「sumRefCoef」，素波の数「numPath」を返り値とする．

```
------------------------------------------------------------------------
function [ distance, phiT, phiR, sumRefCoef, numPath ]=RayTrace( terminalT, terminalR )

global Im; % 虚数 i
global omega; % 各周波数 [rad]
global roomSize; % 部屋のサイズベクトル [縦 横] [m]
global numRef; % 壁反射回数
global numRoom; % 部屋の鏡像をナンバリングした結果を記録した行列
global mu0; % 真空の透磁率
global eps0; % 真空の誘電率
global sigma0; % 真空の導電率

% コンクリートの電気パラメータ
mu1=mu0;
eps1 = 6.76*eps0;
sigma1 = 0.023;

% 各パラメータの初期化
numPath = numRef*(numRef+1)*2+1;
distance = zeros(numPath,2);
phiT = zeros( numPath, 1);
phiR = zeros( numPath, 1);
sumRefCoef = zeros( numPath, 1);

%% レイトレース法による各伝搬路の距離の計算
%x 軸方向の距離
distance(:,1) = (numRoom(:,1)==0).*( terminalR(1)-terminalT(1) )+...
                (numRoom(:,1)>0).*( (roomSize(1)-terminalT(1))+...
                                    (mod(numRoom(:,1),2)*(roomSize(1)-terminalR(1)) +...
                                    (~mod(numRoom(:,1),2))*terminalR(1))+...
                                    ((abs(numRoom(:,1))-1)*roomSize(1)) )-...
                (numRoom(:,1)<0).*( (terminalT(1)) +...
                                    ((~mod(numRoom(:,1),2))*(roomSize(1)-terminalR(1)) +...
                                    (mod(numRoom(:,1),2))*terminalR(1))+...
                                    ((abs(numRoom(:,1))-1)*roomSize(1)));
%y 軸方向の距離
distance(:,2) = (numRoom(:,2)==0).*( terminalR(2)-terminalT(2) )+...
                (numRoom(:,2)>0).*( (roomSize(2)-terminalT(2))+...
                                    (mod(numRoom(:,2),2)*(roomSize(2)-terminalR(2)) +...
                                    (~mod(numRoom(:,2),2))*terminalR(2))+...
                                    ((abs(numRoom(:,2))-1)*roomSize(2)) )-...
                (numRoom(:,2)<0).*( (terminalT(2)) +...
                                    ((~mod(numRoom(:,2),2))*(roomSize(2)-terminalR(2)) +...
                                    (mod(numRoom(:,2),2))*terminalR(2))+...
                                    ((abs(numRoom(:,2))-1)*roomSize(2)));

%% 送信局の放射角の計算
phiT = atan2(distance(:,2),distance(:,1));

%% 受信局の入射角の計算
phiR = (numRoom(:,3)==1).*(phiT-pi)+...
       (numRoom(:,3)==2).*(-phiT)+...
       (numRoom(:,3)==3).*(phiT)+...
       (numRoom(:,3)==4).*(pi-phiT);

phiR = phiR + ((phiR>pi)*(-2*pi)) + ((phiR<-pi)*(2*pi));

%% 壁の反射損失計算
% 壁の入射角
phiRefX=((phiT>=(-pi/2)).*(phiT<=(pi/2))).*abs(phiT) +...
 ~((phiT>=(-pi/2)).*(phiT<=(pi/2))).*(pi-abs(phiT));
```

```
phiRefY=(-1).^(~((phiT>=(-pi/2)).*(phiT<=(pi/2)))).*(pi/2-abs(phiT));

% 壁の反射損失計算
gammaSpace=Im*omega*sqrt(eps0*mu0*(1-Im*sigma0/(omega*eps0)));
gammaWall=Im*omega*sqrt(eps1*mu1*(1-Im*sigma1/(omega*eps1)));

gammaX=((mu1/gammaWall).*cos(phiRefX) -...
(mu0/gammaSpace).*sqrt(1-(imag(gammaSpace)/...
imag(gammaWall))^2.*sin(phiRefX).^2))./((mu1/gammaWall).*cos(phiRefX) +...
(mu0/gammaSpace).*sqrt(1-(imag(gammaSpace)/...
imag(gammaWall))^2.*sin(phiRefX).^2));

gammaY=((mu1/gammaWall).*cos(phiRefY) -...
(mu0/gammaSpace).*sqrt(1-(imag(gammaSpace)/...
imag(gammaWall))^2.*sin(phiRefY).^2))./((mu1/gammaWall).*cos(phiRefY) +...
(mu0/gammaSpace).*sqrt(1-(imag(gammaSpace)/...
imag(gammaWall))^2.*sin(phiRefY).^2));

sumRefCoef = gammaX.^abs(numRoom(:,1)).*gammaY.^abs(numRoom(:,2));
------------------------------------------------------------------------
```

# 付録Ｃ　受信信号強度計算プログラム

数値計算言語 Matlab を用いて受信局が受信する電波の受信信号強度履歴を算出する．エスパアンテナ指向性を算出するためのリアクタンス値ベクトルのセット「setPvec」，各伝搬路の距離「distance」，送信局の放射角「phi」，壁の反射損失「sumRefCoef」を引数，受信信号履歴「rssi」，直接波強度履歴「directPathRSSI」，反射波強度履歴「refPathRSSI」を返り値とする．

```
------------------------------------------------------------------------
function [rssi directPathRSSI refPathRSSI] = calculateRSSI( setPvec, distance, phi, sumRefCoef )

global Pt;% 送信側電源電力
global vs;% 送信側電源電圧
global rs;% 送信側電源内部抵抗
global Im;% 虚数 i
global umat;% 単位行列
global Ymat;% アレーアンテナの多ポート回路網のアドミタンス行列
global ita;% 特性インピーダンス
global waveNum;% 波数
global Eiso;% 等方性アンテナの遠方界
global keyLength;% 鍵長
global lambda;% 波長
global elementSpace;% ダイポール素子間隔
global numElements;% ダイポール素子数
global theta;% 天頂角
global numDirectpath;% 直接波のインデックス

% アンテナのアレーファクタを計算
dis=elementSpace*lambda;
alpha = ones(length(phi),numElements);
for i = 1:1:(numElements-1)
alpha(:,i+1) = exp(Im*waveNum*dis*cos(theta)*cos(phi + 2*(i-1)*pi/(numElements-1)));
end

% ダイポールアンテナの指向性計算
DirecDipole=1.28;

%RSSI 履歴計算プログラム
for p=1:keyLength
    Pvec=[1;exp(Im*setPvec(:,p))];

    % アレーアンテナの入力電圧計算
    Vvec=vs*inv(rs*inv(Ymat)+umat)*Pvec;
    % 入力電力計算
    Ivec=2*Ymat*Vvec;
    % 各素子の遠方界計算
    Eele = ita*Im*waveNum*exp(-Im*waveNum).*(Ivec./(4*pi));
    % 等方性アンテナの遠方界計算
    Eiso = mean(abs(DirectivityOfPAA(setPvec(:,p))));
    % 電界次元の指向性を計算
    direc = alpha*Eele/Eiso;

    %RSSI の計算
    rssi(p)=(lambda/(4*pi)*...
     sum((DirecDipole*direc.*exp(Im*waveNum*distance)./distance).*sumRefCoef))*sqrt(Pt);

    directPathRSSI(p)=(lambda/(4*pi)*sum((DirecDipole*direc(numDirectpath).*...
     exp(Im*waveNum*distance(numDirectpath))./distance(numDirectpath)).*...
sumRefCoef(numDirectpath)))*sqrt(Pt);

    refPathRSSI(p)=rssi(p)-directPathRSSI(p);
end
------------------------------------------------------------------------
```