TR-WEL-0007 003

エスパアンテナを用いた秘密鍵共有方式

樋口　啓介，青野　智之，太郎丸　真

2005.3.30

(株)国際電気通信基礎技術研究所
波動工学研究所
〒619-0288 京都府相楽郡精華町光台二丁目 2 番地 2
Tel: 0774-95-1501　Fax: 0774-95-1508

Advanced Telecommunications Research Institute International
Wave Engineering Laboratories
2-2-2 Hikaridai, Seika-cho, Soraku-gun, Kyoto 619-0288, Japan
Telephone: +81-774-95-1501　Fax: +81-774-95-1508

目次

1. はじめに

近年，無線通信の利便性の高さから，ブロードバンド･アクセスの手段として無線 LAN 等が急速に普及している．しかし，無線通信は，電波の傍受により盗聴される危険性があるため，情報セキュリティ面での脆弱性が問題となっている．

一般に，無線通信でのデータの暗号化には，処理が高速で大量データの扱いに有利な秘密鍵暗号方式が用いられる場合が多い．しかし，この方式には，2 つの問題点がある．1 つは秘密鍵の共有のために通信によって相手方に秘密鍵を配送する場合，配送した鍵が傍受される危険性があるという鍵配送における問題点である．もう 1 つは，通信相手毎に異なる秘密鍵が必要となり，複数鍵を管理しなければならないという鍵管理における問題点である[1][2].

これらの問題を解決するために，電波伝搬路の雑音や変動等の制御困難なランダム現象を用いた秘密鍵共有方式が研究されている[3]-[11]. このうち伝搬路の可逆性とフェージングによる不規則変動を利用し，秘密鍵を共有する方法[5]-[11]は，伝搬路状況に応じて使い捨ての鍵を生成･利用することが可能なため，鍵配送･鍵管理の問題を解決できる優れた方式である.しかし，フェージング現象は一般に端末の移動により発生するため,一般家庭やオフィス内で無線 LAN を利用する場合のような，端末が半固定位置で伝搬路の変化が起きにくい場合には，ある程度の強度を持つ鍵を得るために時間が掛かり，短時間で鍵を作成した場合には盗聴者に推定されやすい秘密鍵になるという問題点がある.

端末が固定位置の場合においても短時間で秘匿性の高い秘密鍵を生成する手段として，文献[11]では MIMO システムにおいける手法も提案されているが，ATR では可変指向性アンテナであるエスパアンテナ[12][13]を用いて，人為的に受信信号強度を変化させ，その変動をもとに秘密鍵の共有を実現する方法を提案し,検討及び装置化を行っている[14]-[20]. 本方式は，現在無線 LAN に使用されている WEP (Wired Equivalent Privacy)や WPA (Wi-Fi Protected Access)等のセキュリティ方式と競合するものではなく，本方式を既存のセキュリティ方式に組み合わせることで，より強固なセキュリティを手軽に使用できるようになる．

2. エスパアンテナを用いた秘密鍵共有方式

可変指向性アンテナを利用した秘密鍵共有方法は DBF (Digital Beam-Forming)等を用いても実現可能であるが，アンテナ素子数により回路規模・消費電力量が増加するなどの問題がある．一方，エスパアンテナは給電が一系統ですむため，低消費電力・低コスト・小型化が実現でき民生機器への搭載が期待できるため，エスパアンテナの使用を前提とした秘密鍵共有の原理について説明する．また，このエスパアンテナを用いた秘密鍵共有方式を ESPARSKey (Encryption Scheme Parasite Array Radiator Secret Key)と称している．

2.1. エスパアンテナ

エスパアンテナの一例として 7 素子エスパアンテナの概要を図 2-1 に示す．給電素子は中央の 1 素子のみでその周りに 6 素子の無給電素子が等間隔に配置されている．無給電素子には各々バラクタダイオードが並列で装荷され，逆バイアスで印加される DC 電圧を制御することにより各々リアクタンス値を変化させ，ビーム形成を行う．

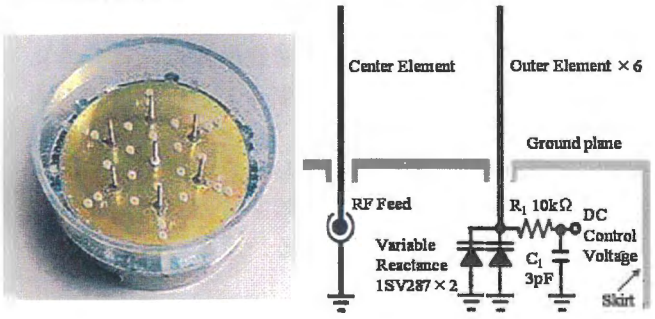


図 2-1　7 素子エスパアンテナ

2.2. 秘密鍵共有の原理

エスパアンテナが搭載された親局と，オムニアンテナが搭載されている子局の間で秘密鍵を生成・共有するための手段を説明する．前提条件を以下の通りとする．親局－子局間では時分割複信(TDD : Time Division Duplex)に代表される双方向に同一周波数を用いた時分割通信が確立している.ある時点において m-素子エスパアンテナの各無給電素子に設定されているリアクタンス値をリアクタンスベクトル(以下 RV)$\mathbf{x} = [x_1, \cdots, x_m]$と表す．また，複数個の RV のセットをリアクタンスベクトル系列 $\mathbf{X} = [\mathbf{x}_1, \cdots, \mathbf{x}_N]$と表す．秘密鍵の生成・共有手順を図 2-2 に示す.

まず，子局より鍵生成要求が行われる．要求を受けた親局は許可を通知した後に鍵生成モードに入る．鍵生成モードでは，初めにエスパアンテナを備えた親局で RV 系列を設定し，その RV を切換ながら子局に測定用パケット(下り)を送信する．このとき，パケット内の各 RV に対応する部分は，平均化による雑音軽減を行うために任意の複数シンボルの長さを持つ．このパケットを，オムニアンテナを備えた子局で受信し，RV の切換タイミングに同期させ各 RV に対応する RSSI 値を測定する.次に，子局から測定用パケット(上り)を送信する．親局では，受信した子局からのパケットを，測定用パケット(下り)送信時と同様の順序で RV を切換ながら受信し，RV 毎の RSSI 値を得る．このと

き，親局と子局での RSSI 値の履歴は伝搬路の可逆性により同一の変化特性を示す．同様の測定を所望の N 個の RSSI 値が得られるまで繰り返す． 1 パケットで取得できる RSSI 値の数は，RSSI 値の計算方法や雑音軽減のための平均化シンボル数，パケット長によって決まる．

次に，この N 個の RSSI 値に対して閾値を設定し，閾値以上のデータを 1，閾値未満のデータを 0 とする 2 値化処理を行うことで，親局と子局の間で同様の N ビットの秘密鍵候補を得ることができる．盗聴端末が同様の手法で秘密鍵を生成しても，場所が異なれば，測定される RSSI 履歴の変化特性は異なるため，親局と子局の間で生成された鍵と同じものは生成できない．

親局と子局の間で共有した秘密鍵候補は，雑音等による影響で数ビットの不一致が生じている可能性がある．この鍵の不一致対策として，シンドローム送信による誤り訂正復号の手法を利用して，不一致ビットを解消する．最後にハッシュ関数等を用いた鍵共有確認処理を行い，鍵の生成を完了する．

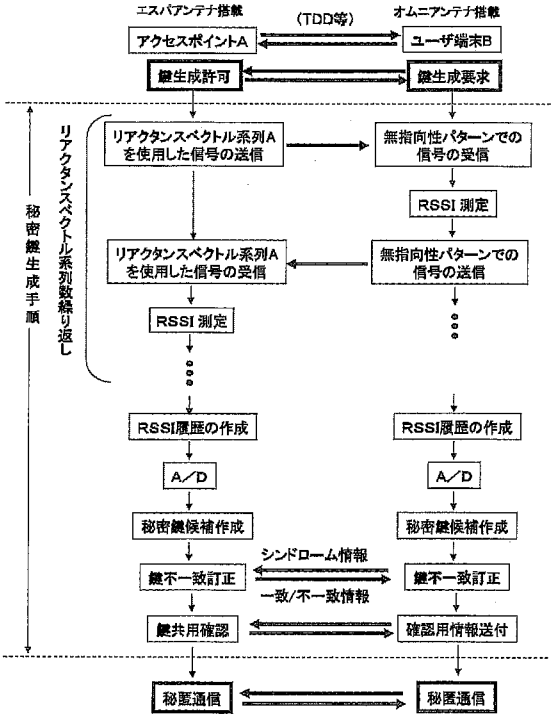


図 2-2　秘密鍵生成手順

3. 無線 LAN 版

3.1. システム構成

無線 LAN の標準規格 IEEE802.11b[21]に準拠した通信を用いる提案方式の性能評価を行う．図 3-1 にシステム構成を示す．本システムでは，屋内閉空間で無線端末局が 1 つの AP(親局)を介して通信を行うインフラストラクチャ・モードを用いたネットワークを想定する．親局である AP に対し，正規のユーザである子局(正規局)と，AP と正規局間の通信を盗聴できる局(盗聴局)から構成される．AP にエスパアンテナ，正規局と盗聴局にはオムニアンテナが搭載されているものとする．

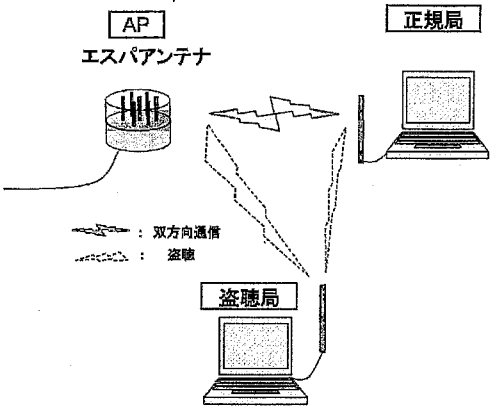


図 3-1　システム構成

3.2. 計算機シミュレーション

図 3-2 にシミュレーション用いる閉空間環境と各局の配置例を示す．想定する閉空間はコンクリート材質の壁に囲まれた部屋としている．各局は固定位置で通信を行い，周囲の人やものの移動などによる伝搬環境の変化はないものとする．また，盗聴局は一般に屋外から AP－正規局間の通信を盗聴していることが考えられるが，本シミュレーションでは，盗聴局も AP・正規局と同じ閉空間に存在し，AP－正規局間の直接波を受信できる盗聴に有利な条件を想定している．

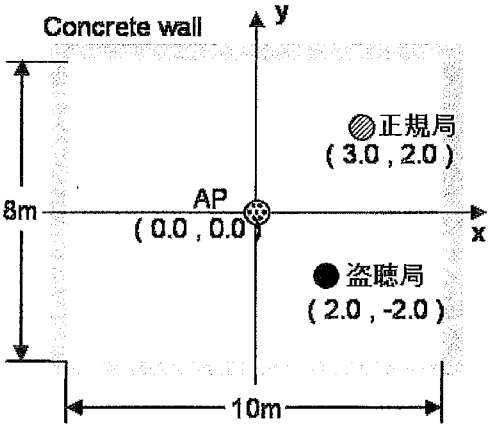


図 3-2　閉空間環境と端末配置例

表 3-1 にシミュレーション諸元を示す．シミュレーションで用いるエスパアンテナは 7 素子とし，リアクタンス値はバラクタダイオード(1SV287)のカタログ値に対応する印加電圧値を 8 ビットで刻んだ値で設定する．RSSI の測定に利用する RV 系列は，特に表記がない限りは試行毎にランダムに設定する．エスパアンテナの Y パラメータには，適応制御の検討などに用いられていた Y パラメータ(表 3-2)を使用した．この Y パラメータは RV に対してのビーム方向については実際の試作機と差異はあるが，ヌルの深さ，利得については比較的妥当でありビームパターンを変化させながらの鍵生成の検証に問題はないと考えた．

送信パケットは，一次変調 DBPSK の信号を符号長 11 の Baker 符号によって二次変調した信号で構成される．送信時には IEEE802.11b の規格にある周波数 2.484 GHz を用い，TE 波にて放射されているものとする．電波の伝搬路は，マルチパスによる受信レベル差や位相差を考慮するために，レイトレーシング法[18]を用いて設定する．簡略化のため床・天井からの反射は考慮せず，壁 4 面での 6 回反射までのモデルを用いる．

シミュレーションにおいて生成する鍵長は 128 ビット，RSSI 測定時の雑音軽減のための平均化のシンボル数は 8 シンボルとし，測定した RSSI 値を鍵候補に変換するときの閾値は得られた RSSI 値の中央値を用いるものとする．また，鍵の誤り訂正には代数的復号法を用いて，t ビット以内の誤りを訂正できるものとする．

表 3-1　シミュレーション諸元

(a) 部屋環境	
部屋の大きさ	8[m]×10[m]
アンテナ	AP (エスパアンテナ) 正規局・盗聴局 (オムニアンテナ)
反射面 材質	壁 4 面 (天井・床は考慮せず) コンクリート(ε_γ=6.76 , σ=0.023[S/m] , μ_γ=1)
各局配置位置	AP　：(0.0, 0.0) 正規局・盗聴局: ランダム
(b) 伝搬環境	
変調	DBPSK，Barker 符号(符号長 11)
搬送波周波数	2.484GHz
送信波	TE 波
伝搬路モデル	レイトレーシング法(6 次反射)
(c) 鍵生成パラメータ	
鍵長	128 ビット
平均化	8 シンボル
RV	ランダム(8 ビット刻み)
閾値	中央値
不一致訂正	代数的復号法による t ビット以内誤り訂正

表 3-2　使用 Y パラメータ

	実数	虚数
Y00	0.0008616	-0.0120795
Y01	-0.0006963	0.0036462
Y11	0.0044216	-0.0071600
Y12	0.0009721	0.0047851
Y13	-0.0005376	-0.0011297
Y14	0.0001701	-0.0002950

3.2.1. SNR 対鍵一致率

(MATLAB ファイル ：main_base_re.m)

ランダムな RV を用いて秘密鍵を生成した場合の誤り訂正ビット数をパラメータとした SNR 対鍵一致率特性を図 3-3 に示す．ここでの鍵一致率とは，パラメータとなっている t ビットの誤り訂正を行ったとき，総試行回数(1000 回)における作成した全 128 ビットが一致する回数で表している．端末は，AP を中央に配置し，正規局の配置は試行毎にランダムに設定している．このとき， AP にオムニアンテナを用いて送信した場合の，正規局での受信電力(レイトレーシングによるマルチパス合成後の電力)に対して，SNR に応じたノイズレベルを設定している．図 3-3 より 4 ビットの誤り訂正を仮定した場合，SNR 約 30[dB]で鍵の一致がほぼ 100%になっていることがわかる．また，8 ビットの誤り訂正を仮定すると，SNR=20dB でほぼ 100%の鍵一致が得られている．

図 3-4 には，平均化のサンプル数を 4，16，24 シンボルと変えたときの，4 ビットの誤り訂正を仮定した場合の一致率を示す．この図より，平均化シンボル数を 2 倍にしたときに約 3dB の改善が見られることから，雑音の影響を 1/2 にすることができていることが確認できる．

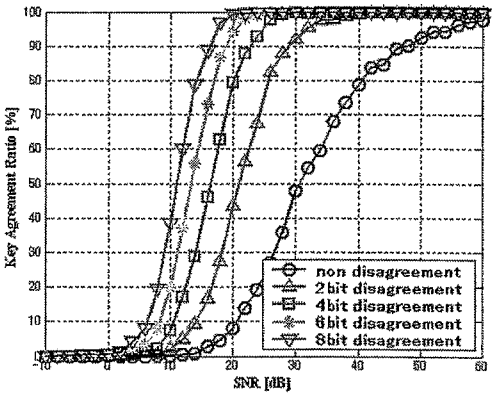


図 3-3　SNR 対鍵一致率特性
(データファイル ：SNvsKA_arandom_APmm.mat)

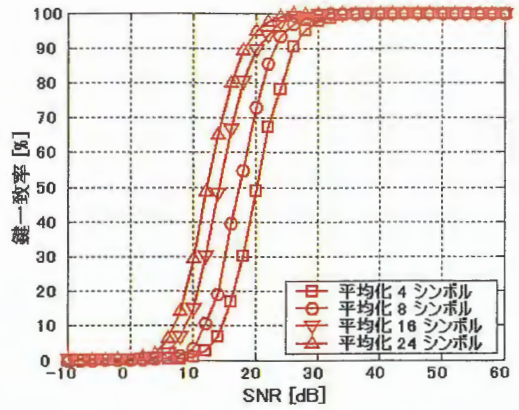


図 3-4　平均化シンボル数 SNR 対鍵一致率特性

3.2.2. 送信電力対鍵一致率

(MATLAB ファイル：main_base_tr)

ランダムな RV を用いて秘密鍵を生成した場合の誤り訂正ビット数をパラメータとした送信電力対鍵一致率特性を図 3-5 に示す．電力は距離の二乗に比例して減衰するものとし，受信機でのノイズレベルは-90 dBm に設定する．端末は，AP を中央に配置し，正規局の配置は試行毎にランダムに設定している．図 3-54 より 4 ビットの誤り訂正を仮定した場合，送信電力が約 -10dBm でほぼ 100%の鍵一致が得られていることから，想定する無線 LAN システム(最大定格送信電力 10dBm)において十分な鍵一致が得られると考えられる．

また，この結果は想定している部屋環境に依存するものなので部屋環境が変われば特性の変化があると考えられる．同様の部屋環境において部屋全体の SNR の分布を求め(conf_SNR.m)，図 3-3 の結果を送信電力対鍵一致率特性におきかえたものを図 3-6 に示す．この結果は図 3-5 とほぼ同様になっていることから，想定する部屋の SNR の分布と SNR に対する鍵一致率の特性がわかれば，図 3-5 に示すような送信電力に対する特性は推定可能であることがわかる．

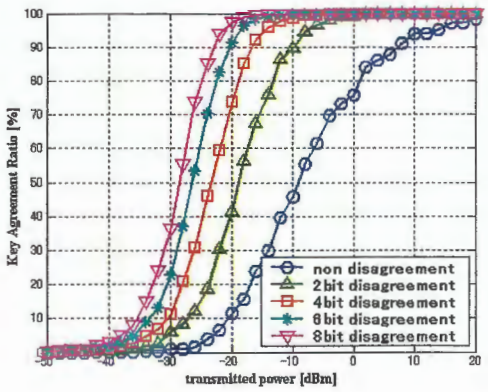


図 3-5　送信電力対鍵一致率特性
(データファイル：TPvsKA_arandom_APmm.mat)

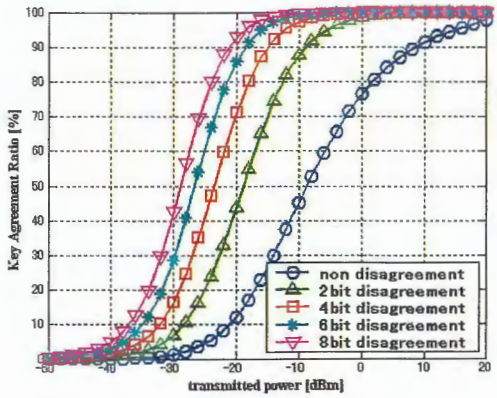


図 3-6　送信電力対鍵一致率特性

3.2.3. 部屋全体での鍵一致率

(MATLAB ファイル：all_key_agree)

鍵不一致の位置依存性を検証するため，AP を部屋の中央に設置し部屋 1/4 の各位置で鍵生成を 100 回行ったときの鍵一致率を図 3-7 に示す．送信電力は 0dBm とし，ビームパターンはランダムに設定した．また，鍵一致率は図 3-6 より，設定した送信電力で 0 ビット誤り(鍵完全一致)が約 80%という結果を考慮して，0 ビット誤りの確率を示している．図 3-7 より正規局が親局に近いと一致率が高く，遠くなると一致率が下がる傾向にあることがわかる．図 3-8 には図 3-7 と同様の条件での平均 SNR を示す．図 3-8 中の SNR と図 3-7 の鍵一致率はほぼ対応しており，子局が SNR の低くなるスポットヌルにあると一致率が低くなりやすいことがわかる．このスポットヌルは反射波等の影響によりできるため，一致率は周波数及び端末の位置に依存すると考えられる．

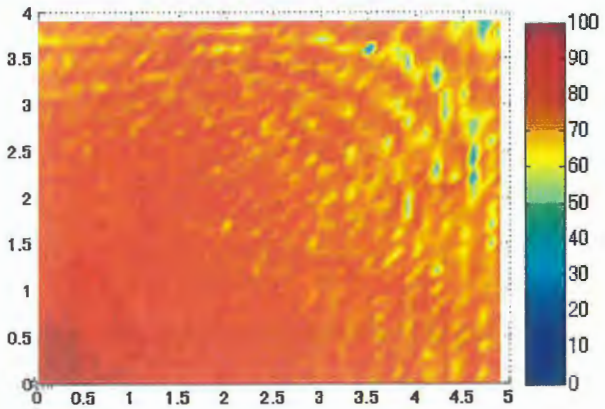


図 3-7　部屋 1/4 での鍵一致率分布
(データファイル：all_key_agree.mat)

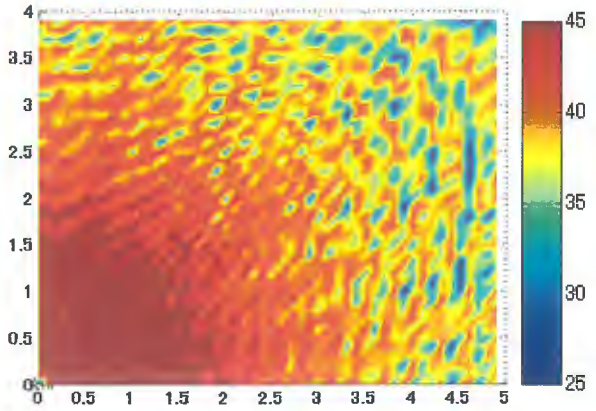


図 3-8　部屋 1/4 での SNR 分布
(データファイル ：all_key_agree.mat)

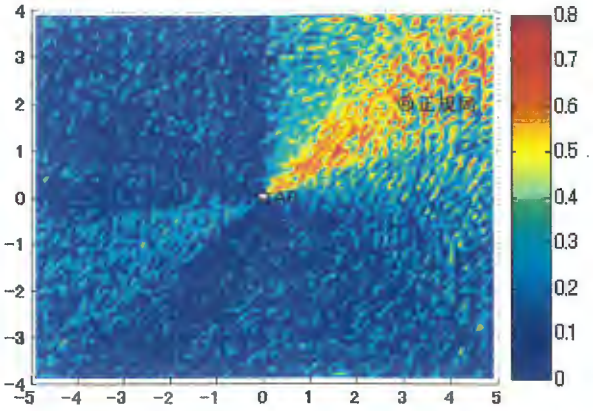


図 3-9　部屋全体での鍵の相関分布

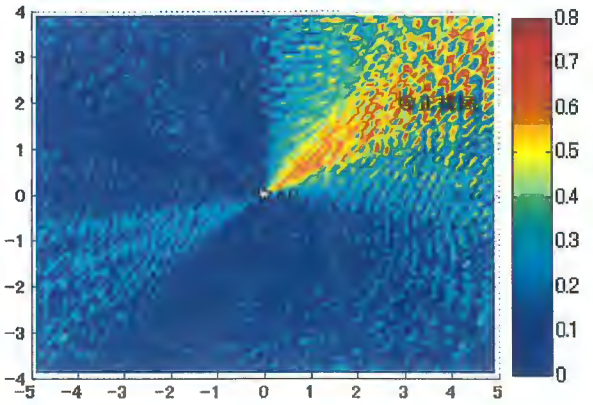


図 3-10　部屋全体での平均鍵相関分布
(データファイル ：all_key_cc.mat)

3.2.4. 部屋全体での鍵相関の分布

(MATLAB ファイル ：all_key_cc)

図 3-9 に，正規のユーザ端末を座標(3.0, 2.0)に固定し，同じ閉空間で生成される鍵の相関の分布を示す．正規局と同様の処理を行う他局を部屋の端から 10cm 刻みに移動させ，それぞれの位置における鍵の相関を算出している．相関の高い位置に盗聴局が存在すると正規局間で生成した鍵が推測される恐れがある．文献[17]においても同様の検討を行っているが，プログラム中で各到来波の到来方向に対し，アンテナの利得しか考慮に入れていない(位相を考慮していない)という不備があり相関が高い傾向を示していた．図 3-9 より，正規局間の直線上である程度広がりを持った範囲において相関の高くなることがわかった．

次に使用するビームパターンの影響を調べる．図 3-10 に鍵生成に用いる RV 系列のみを変え，他は同様の条件で 10 回シミュレーションを行ったときの平均の鍵相関分布を示す．使用するビームパターンを変化させたものを平均しているにもかかわらず相関の分布傾向は図 3-8 と同様であることから，鍵の元となる RSSI 値に対し直接波の影響が強く相関値は位置依存が大きいと考えられる．また，10 回のそれぞれの分布も細かい差異はあるがおおむね同等の分布であった．

3.2.5. その他シミュレーションについて

この章では，秘密鍵共有方式の基本的な特性についての検討を記載したが，これまでの研究会発表などでマルチローブに関する検討や多値化に関する検討を行っている．マルチローブについては[15]で示しているように正規のユーザ端末に近い位置でも相関が下がり有効な面もあるが，

・マルチローブパターンを多く確保することが困難．
・パターン依存が大きく位置によっては相関低下の効果が得られない場合もある．
・マルチローブのビームを端末方向に向ける必要があるため，到来方向推定などが必要．

など様々な問題点があり実機でマルチローブを用いることは困難だと考え，ランダムパターンのみの検討結果を記載した．

また，多値化については，多値化することで閾値付近の RSSI 値の数が増加し不一致数が増加してしまうという問題があるが，周辺での鍵相関の低下や，鍵生成処理時間の短縮が可能であると言う点で有効である．無線 LAN 版のシミュレーションでは有効な手段であ

るが，実環境では誤りが増えると考えられるため，鍵長の確保が問題となる．また，次項に示すZigBee版では分解能が粗いため，多値化は困難だと考えられる．

3.3. 試作機

無線LANチップを用いたESPARSKey試作機では，既存の無線LANチップにRSSIを出力するものがないため，IQチャネル信号を取り出しソフトウェアで同期を取り受信電力を測定するという改造を行った．そのため，同期捕捉ミスの発生や，データ取得に時間がかかる(16ビットの鍵を1回取得に約30秒)等，様々な問題が存在し性能の評価が困難であった．後述のZigBee版の試作機が問題なく動作していることから，RSSIを出力するなど受信電界強度が測定できる無線LANチップがあれば無線LAN版でも問題なく動作すると考えられる．

4. ZigBee 版

無線 LAN 版で問題があり，また無線 LAN モジュール内蔵型 PC の普及により機能付加の改造が困難になってきている．このため，無線 PAN の規格の一つである IEEE 802.15.4 に準拠した ZigBee^{TM}[22]を用いて，既存の通信システムに接続するだけでそのシステムの持つセキュリティ機能を利用できる秘密鍵共有装置を試作した．ZigBee を採用した理由として，

・ 消費電力が少なく PC からの USB バスパワーでも十分に動作する．

・ 採用した ZigBee チップが RSSI を出力する仕様なので秘密鍵生成のために改造の必要がない．

といったことがあげられる．

4.1. システム構成

図 4-1 に無線 LAN 通信を行っているシステムに秘密鍵共有装置を付加する場合のシステム構成を示す．このとき無線 LAN は，無線端末局が 1 つの AP(Access Point)を介して通信を行うインフラストラクチャ・モードでネットワークを構成している．図 4-1 に示すように，無線 LAN の AP に本装置の親局，ユーザ端末に本装置の子局をそれぞれ Ether，USB により接続する構成となっている．

本装置の親局が設置された AP と通信を行っているユーザ端末の USB ポートに本装置の子局を接続すると，親局 - 子局間において前述の秘密鍵生成手順を行い，秘密鍵を生成・共有する．その共有した秘密鍵を AP・ユーザ端末の無線 LAN 機能にそれぞれ通知し，無線 LAN は以後その秘密鍵を用いた秘匿通信を行う．

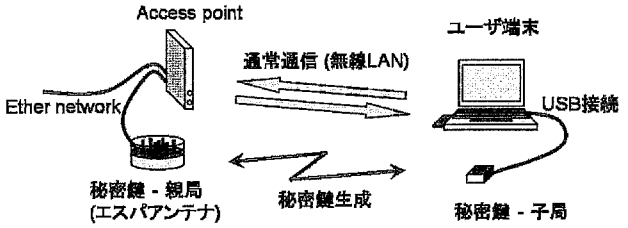


図 4-1　システム構成図

4.2. 計算機シミュレーション

ZigBee も無線 LAN の IEEE802.11b と同様に 2.4GHz 帯の電波を使用する．しかし，無線 LAN 版との相違点として，変調方式，平均化シンボル数，試作機に用いる ZigBee チップの RSSI 分解能(1dB 刻み)がある．この点を考慮したシミュレーションを行う．表 3-1 に示した無線 LAN 版のシミュレーション諸元との相違点のみを表 4-1 に示す．

表 4-1　シミュレーション諸元

(b) 伝搬環境

変調	QPSK

(c) 鍵生成パラメータ

RSSI 分解能	1 dB 刻み
平均化	Preamble Sequence (4byte)
RV	ランダム(4 ビット刻み)
不一致訂正	代数的復号法による t ビット以内誤り訂正 or　32bit ブロック毎に t ビット訂正

4.2.1. SNR 対鍵一致率

(MATLAB ファイル：main_base_re_ZigBee.m)

ランダムな RV を用いて秘密鍵を生成した場合の誤り訂正ビット数をパラメータとした SNR 対鍵一致率特性を図 4-2 に示す．図 4-2 より 4 ビット以内の誤り訂正を仮定すると，一致率が 100%近くになるのは SNR が約 40dB であり，無線 LAN 版と比較して大幅に劣化していることがわかる．この原因として，まず平均化のサンプル数がある．無線 LAN 版ではバーカー符号 11 チップを 8 シンボル使用していたため，雑音に対して 88 サンプルの平均化を行っていた．しかし，ZigBee 版の場合，チップの仕様にあわせプリアンブル部分の 4byte を用いることにしているため平均化のサンプル数は 32 サンプルとなり 4dB 強の劣化が起こる計算になる．RSSI の分解能を 1dB 刻みとしているため，その丸め誤差も影響しノイズが小さくなっても数ビットの誤りが残っている．また，SNR が 0dB 以下において，RSSI の変動が分解能以下となりすべて同一の RSSI 値を示し，オール 1 またはそれに近い鍵が双方でできて鍵一致となることがあった．このような鍵は実際に用いるには不適切であるので，取り除いて一致率を計算している．

図 4-2 では，先の無線 LAN 版のシミュレーションにあわせ 128 ビット中の t ビット以内の誤り訂正により評価したが，誤り訂正を 128 ビットで行うとすると，検査行列やシンドロームのサイズが大きくなり装置に負荷がかかってしまうため，32 ビット毎に 4 ブロックに区切り，その 32 ビット中で t ビットの誤り訂正を行うものとして評価する．図 4-3 に 32 ビット中で t ビットの誤り訂正を行う場合の鍵一致率特性を示す．128 ビットでの訂正ビット数に換算すると，0，4，8，12 ビットとなる．図 4-2 のグラフに比べ 2 倍の訂正ビット数になっているが特性は同等か少し劣化しているということから，32 ビット毎に誤り訂正を行うことは，装置負荷の観点では有効であるが誤り訂正の効率としては性能が劣化すると言える．

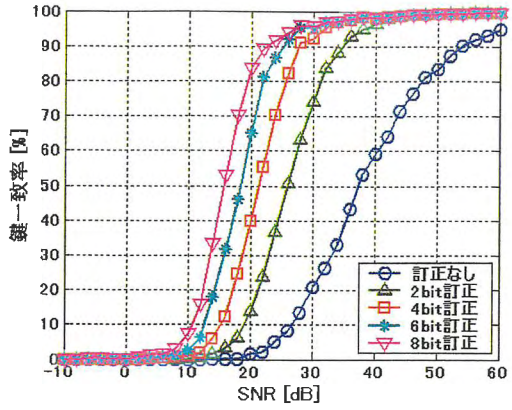


図 4-2　SNR 対鍵一致率特性
(データファイル ：SNvsKA_ZigBee.mat)

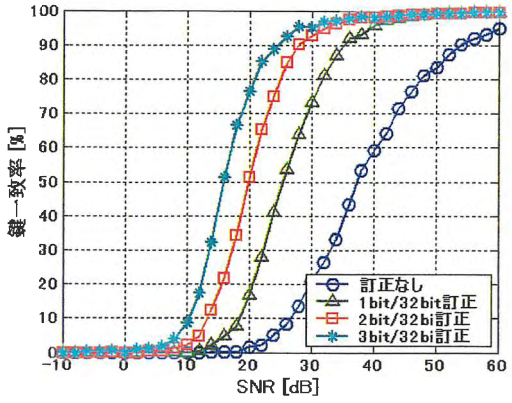


図 4-3　SNR 対鍵一致率特性(ブロック毎誤り訂正)
(データファイル ：SNvsKA_ZigBee.mat)

4.2.2. RSSI 分解能の影響

図 4-4 に送受信にレベル差がある場合の SNR 対鍵一致率特性を示す.誤り訂正は 32 ビット毎に 2 ビット行うものとした．グラフから，レベル差が無いときや RSSI の分解能と同じ 1dB の差がついているときには SNR が 40dB でほぼ 100%の一致が得られているが，レベル差が分解能より細かい場合一致率が劣化し，SNR が高くなっても一致率は向上しないことがわかる．これは丸め誤差による数ビットの誤りが常に発生してしまうためである．図 4-5 には送受信のレベレ差がない場合の誤り個数分布を，図 4-6 には送受信のレベル差を 0.5dB とした場合の鍵の誤り個数分布をそれぞれ SNR が 50dB，10dB に場合について示す．SNR が 10dB のときは送受のレベル差と丸め誤差の影響よりノイズの影響の方が支配的になっていると考えられほぼ同様の分布となっているが，SNR が 50dB のときは丸め誤差の影響で 10 ビット程度の誤りが残っており，丸め誤差が存在することで SNR が高いときに影響を受け不一致が起こりやすいことがわかる．

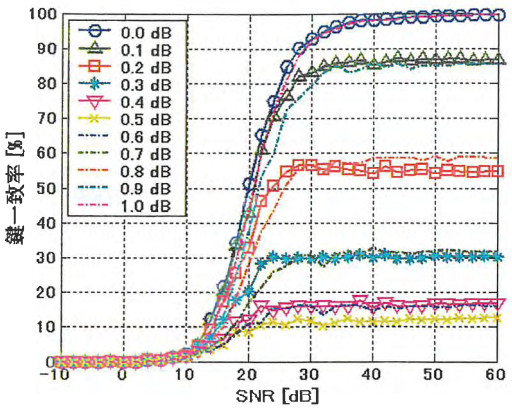
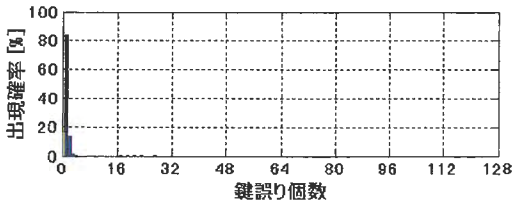
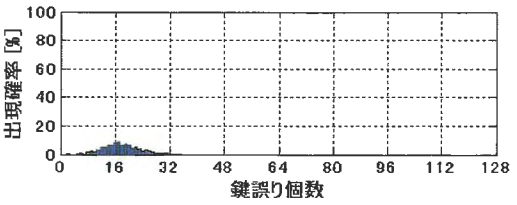


図 4-4　SNR 対鍵一致率特性(送受信レベル差)
(データファイル ：SNvsKA_ZigBee.mat)

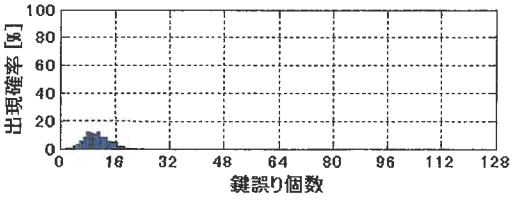


(a) SNR 50dB

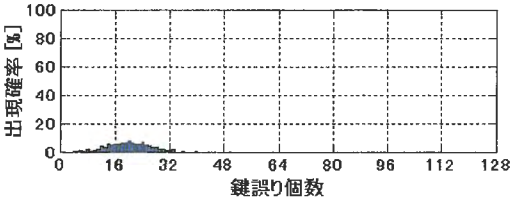


(b) SNR 10dB

図 4-5　誤り個数分布(送受信レベル差なし)



(a) SNR 50dB



(b) SNR 10dB

図 4-6　誤り個数分布(送受信レベル差 0.5dB)

4.2.3. 部屋全体での鍵一致率

(MATLAB ファイル ：all_key_agree_ZigBee.m)

図 4-7 に，AP を部屋の中央に設置し部屋 1/4 の各位置で鍵生成を 100 回行ったときの鍵一致率を示す．図 4-3 に示した鍵一致率特性の結果からもわかるように無線 LAN 版で行ったシミュレーション結果(図 3-6)と比較して一致率の低い領域が増加している．図 3-6 と同様に SNR の低い位置で鍵一致率が低くなりやすく，鍵の一致率は端末の位置に依存することが確認できる．

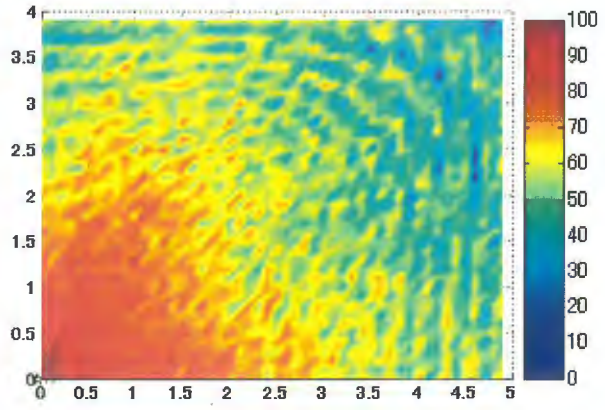


図 4-7　部屋 1/4 での鍵一致率

(データファイル ：all_key_agree_ZigBee.mat)

4.2.4. 部屋全体での鍵相関の分布

(MATLAB ファイル ：all_key_cc_ZigBee.m)

図 4-8 に，正規のユーザ端末を座標(3.0, 2.0)に固定し，同じ閉空間で生成される鍵の相関の分布を示す．この結果も無線 LAN 版とほぼ同様の特性になっており，正規局方向に少し広がりをもって相関が高い位置が分布している．RV 系列を変え 10 回シミュレーションを行ったが，こちらも同様に 10 回とも細かい差異はあるが同様の傾向を示していた．

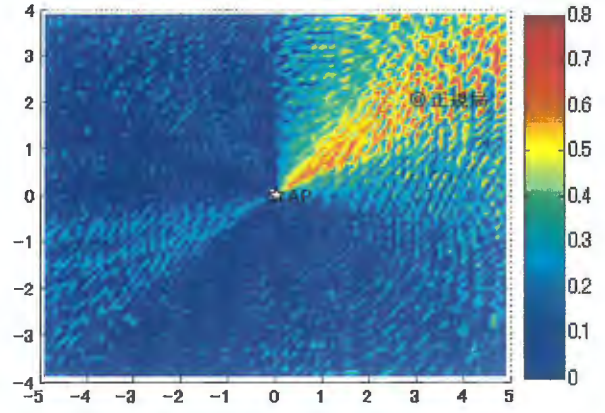


図 4-8　部屋全体での鍵相関の分布

(データファイル ：all_key_cc_ZigBee.mat)

4.2.5. 周波数依存の確認

(MATLAB ファイル ：main_base_f_ZigBee.m)

(MATLAB ファイル ：all_key_agree_ZigBee.m)要変更

(MATLAB ファイル ：all_key_cc_f_ZigBee.m)

ここまでのシミュレーションでは周波数として表 3-1 に示したように 2.484GHz を用いていたが，ZigBee の仕様として，次項の表 4-1 に示すように中心周波数が 2.405GHz から 2.480GHz まで 5MHz 刻みで 11 チャネルから 26 チャネルまでの 16 チャネル設定されている．これまで検討してきた鍵の一致率や相関の分布は基地局の設置位置に依存するため，周波数・波長が変化することにより，それぞれの位置における特性も変わってくると考えられる．そこで，各周波数での鍵一致率，鍵相関の分布等をシミュレーションにより比較する．この時，コンクリートの誘電率，導電率等のパラメータは各周波数チャネルによって変化のないものとし，伝搬経路と波長による信号の位相回転と反射係数の変化のみを考慮した．

図 4-9 に周波数チャネルに対する鍵一致率特性を示す．周波数依存性を見るため，送信電力を誤り訂正 bit 数に対するそれぞれの一致率特性が 0~100%の範囲に分布している-10dBm に固定し，試行毎に端末位置をランダムに設定し 1000 回試行の一致率を計算した．図 4-9 より周波数により若干特性に差がでているが，大きな差はなく部屋全体での平均的な特性は同様であると言える．しかし，若干の差があることから，各設置位置での特性には差があると考えられる．

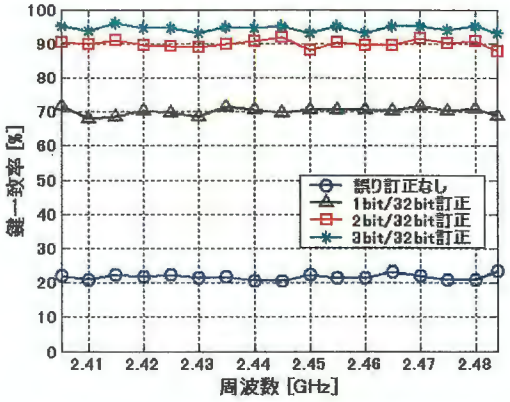


図 4-9　周波数チャネル対鍵一致率

(データファイル ：main_base_f_ZigBee.mat)

各周波数による一致率の位置依存を見るため，部屋の 1/4 での一致率の分布を調べる．11 チャネル(2.405GHz), 16 チャネル(2.430GHz), 21 チャネル(2.455 GHz)の一致率分布をそれぞれ図 4-10, 4-11, 4-12 に示す．各図とも子局が親局に近いと一致率が高く，遠い

と一致率が低いと言う傾向は同様だが，一致率が低くなるスポットヌルの位置は周波数により変化し，図4-7で一致率が低い(図中青色)位置でも図 4-10~12 では一致率が低くはない場合がある．(図 4-7，4-10~12 では特に一致率の低い部分がわかりにくいため，128 ビット全体で2ビットの誤り訂正を行った場合の一致率分布を次ページに図 4-7'，4-10'，4-11'，4-12'として記載する．この場合，一致率が特に低い位置は各周波数において数箇所であるため位置の違いが比較しやすい．) このことから，鍵の一致率は周波数と端末の位置に依存することが確認できる．また，ある位置において鍵生成を行ったとき一致率が悪ければ周波数を切り換え鍵生成を行うことで鍵の一致が得られる可能性があることがわかる．

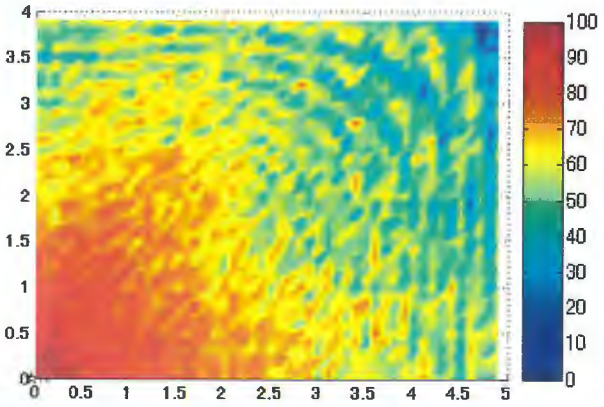


図 4-10　部屋 1/4 での鍵一致率(ch11)
(データファイル ：all_key_agree_ZigBee_ch11.mat)

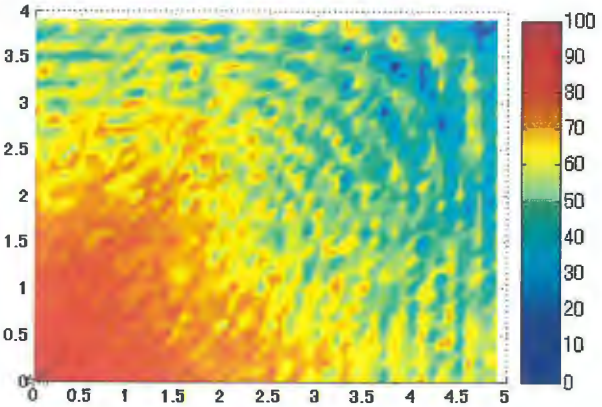


図 4-11　部屋 1/4 での鍵一致率(ch16)
(データファイル ：all_key_agree_ZigBee_ch16.mat)

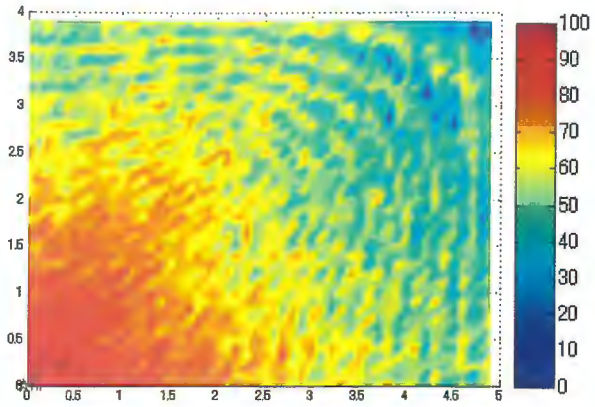


図 4-12　部屋 1/4 での鍵一致率(ch21)
(データファイル ：all_key_agree_ZigBee_ch21.mat)

次に部屋全体での 16 チャネルにすべてについて鍵相関の分布を示すが，図表の数が多いため別途記載する．正規のユーザ端末の位置はこれまでと同様に座標(3.0, 2.0)に固定する．図 f-1～f-16 までが周波数チャネル 11～26 に対応，図 f-17 はすべての周波数について平均したものであり，それぞれの右側にはカラーバー代わりに部屋の側面から見た図を掲載している．これらの図は，ある RV 系列により鍵生成を行ったときの結果であるが，別の RV 系列を用いた場合でも同様の傾向を示すことは確認済みである．

図 f-8(ch8)，f-10(ch10)のように相関の高い部分の多いチャネルもあれば，図 f-5(ch5)，f-6(ch6)のように相関の高い領域が少ないチャネルもあることがわかる．相関の高い領域が少ないチャネルを用いて鍵生成を行えば盗聴される可能性は減少するが，実環境において部屋の異なる位置での相関の分布を調べることは困難である．また，今回の正規ユーザ位置では，以上のような結果となっているが，ユーザの位置により相関の高い領域が少ないチャネルは異なると考えられるため，ある相関の低い周波数を固定で使用するということは不可能である．図 f-17 に示すすべての周波数チャネルを平均した特性を見ると，相関が極端に高い位置は減少していることがわかる．その右側の図より正規局と同じ位置以外では相関が高くても 0.6 程度であることがわかる．この結果から，盗聴対策として，いくつかの周波数チャネルを用いて鍵生成を行う方法が考えられる．厳密には図 f-17 に示した平均特性と複数チャネルを用いた鍵生成は異なるが，正規局と同方向に盗聴局が存在しても，推測されにくい鍵を生成できると考えられる．

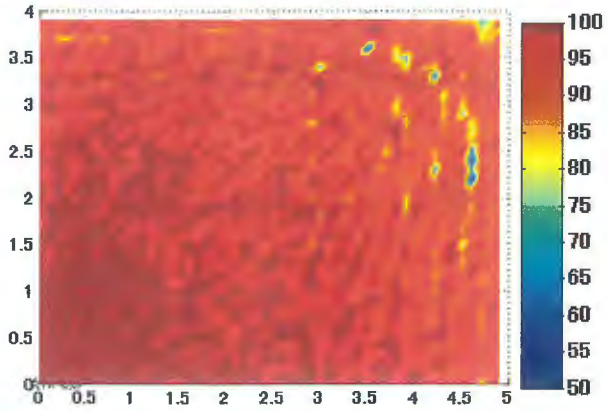


図 4-7’　部屋 1/4 での鍵一致率
(2bit/128bit 訂正)
(データファイル ：all_key_agree_ZigBee.mat)

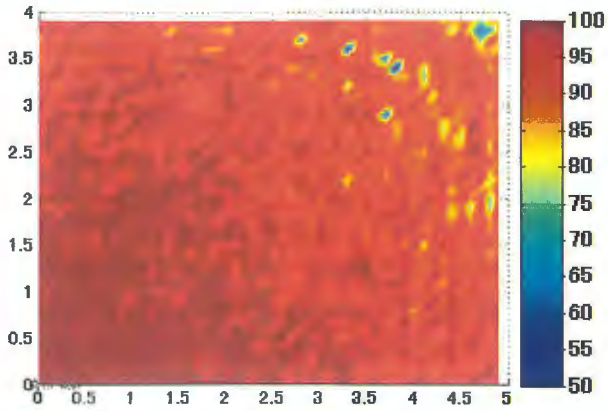


図 4-11’　部屋 1/4 での鍵一致率
(チャネル 16・2bit/128bit 訂正)
(データファイル ：all_key_agree_ZigBee_ch16.mat)

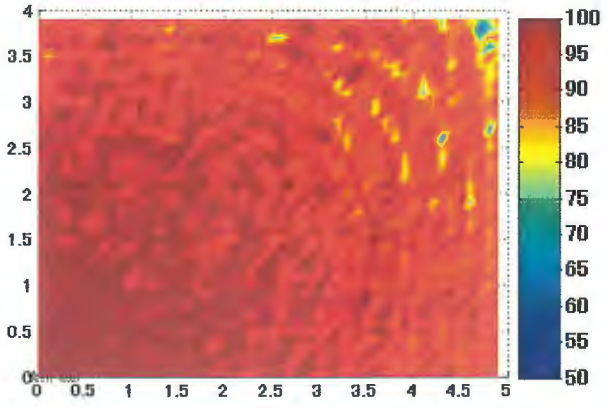


図 4-10’　部屋 1/4 での鍵一致率
(チャネル 11・2bit/128bit 訂正)
(データファイル ：all_key_agree_ZigBee_ch11.mat)

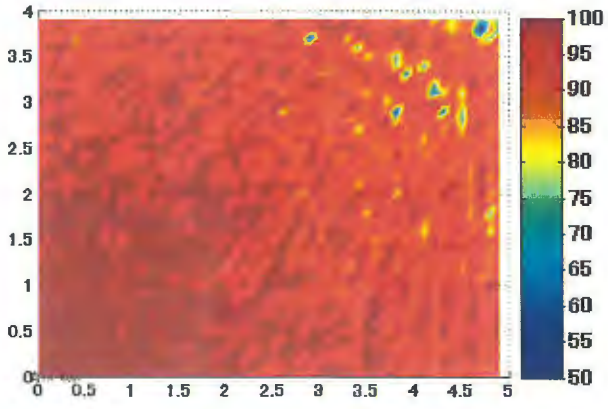


図 4-12’　部屋 1/4 での鍵一致率
(チャネル 21・2bit/128bit 訂正)
(データファイル ：all_key_agree_ZigBee_ch21.mat)

4.3. 実験

4.3.1. 実験装置

今回の試作機に搭載されている Chipcon 社の ZigBee チップ CC2420[23]の基本的な仕様を表 4-1 に示す．また，試作した親局，子局の外観を図 4-13 に示す．

エスパアンテナの RV は，現在の試作機に用いられているバラクタダイオード（1SV287）に 0～20V の電圧を 8 ビット刻みでランダムに印加することで設定する．RSSI 値の測定は，チップの持つ RSSI 計測機能を用いる．この RSSI 計測機能はパケットの先頭 4byte の Preamble Sequence 区間で計算を行い，1 パケットに対し 1dB 刻みの RSSI 値を出力するものである．最小の 1 パケットに対して 1 つの RV を設定し，出力する RSSI 値をそのまま鍵生成に用いる． また，最小パケットは 16byte ，512 μsec であり，1 つの RV に対する送受信には送受の切換時間も含め約 2msec 必要となる．

測定した全 RSSI 値の中央値を閾値として 2 値化することで 128 ビットの鍵の生成を行う．誤り訂正は 32 ビット毎に 4 ブロックに区切り，その 32 ビット中で t ビットの誤り訂正を行うものとして評価する．

表 4-1　ZigBee チップ(CC2420)の仕様

周波数	2.405-2480(16ch)	GHz
送信電力	1	mW
データ変調方式(一次)	offset-QPSK	
データ変調方式(二次)	DS-SS	
データレート	250	kbps
チップレート	2	Mcps

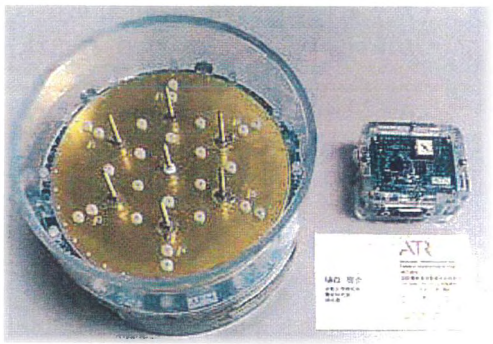


図 4-13　秘密鍵共有装置の外観

4.3.2. 実験環境

秘密鍵共有装置の評価を行う実験室の環境を図 4-14 に示す．実験室は三方が金属壁で囲まれ，残りの一方はコンクリート壁とガラス窓という構造になっている．この室内にエスパアンテナを搭載した親局，パッチアンテナを搭載した子局，そして子局と同一構造の盗聴局をそれぞれ測定用の PC とともに高さ約 80[cm]の台上に設置する．基本的に測定中は部屋の中には動くものがなく，静的な環境としている．

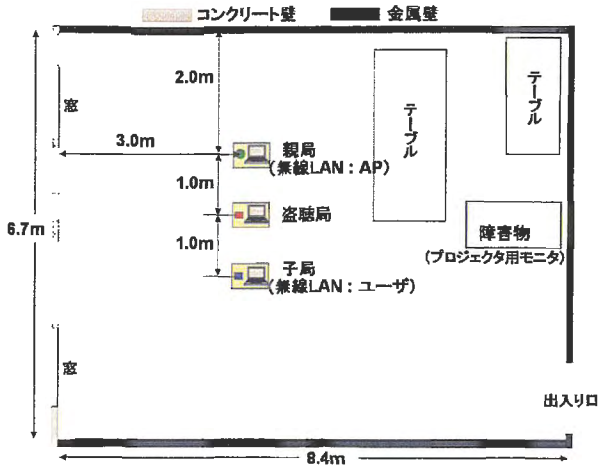


図 4-14　実験室概要

4.3.3. 鍵一致率改善手法(閾値付近データ削除)

ZigBee 版の ESPARSKey 装置においても前述の秘密鍵共有の原理は同様だが，実際の装置では雑音の影響だけではなく，送受信のタイムラグによる伝搬路の変化や装置の個体差，RSSI 測定時の丸め誤差など多くの要因により不一致数が増加すると考えられる．不一致数が増加すると，鍵不一致訂正を行っても訂正できず鍵が共有できない可能性がある．その対策として，鍵の不一致が起こりやすい閾値付近のデータを図 4-15 に示す手順で削除することで，鍵不一致数の削減を図る．この手順は図 2-2 の「秘密鍵候補作成」と「鍵不一致訂正」の間に行うものとする．

通常は所望の鍵長分の RSSI 値を測定し，鍵候補とするが，この場合は閾値付近のデータを α 個削除するため，所望の鍵長+α 個の RSSI 値を取得する．この RSSI 値に対し閾値を設定し 0,1 のビット系列を得る．ビット系列を RSSI の値に応じてソートし，RSSI 値が大きな部分から(所望鍵長+β)/2 個，RSSI 値が小さな部分から(所望鍵長+β)/2 個を残し，間の閾値に近い部分を削除する．このとき，親局側で閾値付近でなくても子局側では閾値付近にデータが存在し，ビットが不一致となることも考えられるため子局側でも閾値付近のデータを削除する．β は子局側で削除するビット数を表す．次に親局は位置情報を子局に送信し，子局側では受信した位置情報に対応する部分を削除する．親局側からの情報に応じて削除を行った後，ビット系列を RSSI 値に応じてソートし，RSSI 値が大きな部分から所望鍵長/2 個，RSSI 値が小さな部分から所望鍵長/2 個を残し，間の閾値に近い部分を β 個削除する．この削除位置情報を親局側に送信し，最終的に双方で残った所望鍵長分の 0,1 系列を鍵候補とし鍵不一致訂正処

理を行う．子局側でデータ処理を行うときに，残すデータを大小から所望鍵長/2 ではなく，任意に設定することで共有鍵の 0,1 の個数を分散させることもできる．

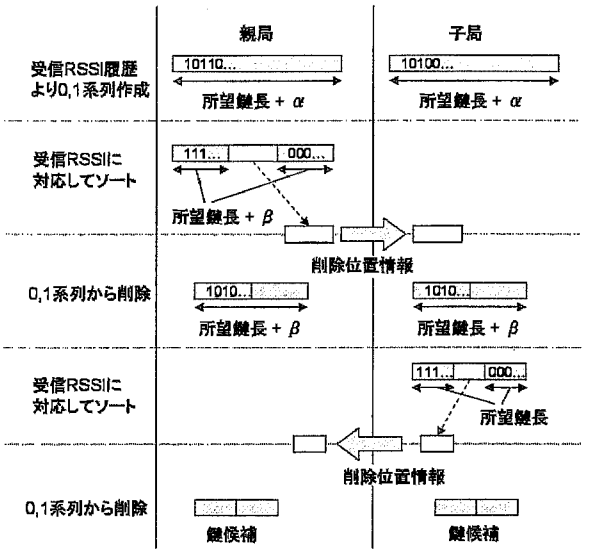


図 4-15　閾値付近データ削減の手順

4.3.4. 乱数性向上手法(RSSI インターリーブ)

生成した秘密鍵の有効性を考えたとき，鍵の乱数性が重要となる．複数個の鍵を生成するときに連続のビット系列として偏りを持っていれば，盗聴者による鍵の推測が簡易になる恐れがある．個々の 128 ビットの鍵が偏っていても，連続のビット系列として乱数性があれば複数の鍵の傾向から鍵を推測することは困難となる．乱数性の評価方法として，FIPS PUB 140-2 に設けられている乱数検定がある(付録)．

本秘密鍵共有方式では RSSI 測定毎にビームパターンをランダムに変えているため，測定した RSSI，そこから生成する秘密鍵ともに乱数性が高いと考えられる．しかし，これはこれまでシミュレーションで検討してきた端末の周辺で移動のない静的な環境においてのことで，端末の移動や周囲での人の移動がある実使用環境において，鍵生成のためのデータ取得中に環境の変化があれば RSSI や鍵が偏ってしまう恐れがある．特に前述のデータ削除を行った場合，削除前より偏りが大きくなってしまう．

このような鍵の偏りを減らし乱数性を向上するために RSSI インターリーブを行う．偏りが大きい場合には，1 回のインターリーブだけだと偏りが残り乱数検定を通らない場合もあるため，2 回のインターリーブを行うものとする．この 2 回のインターリーブ間隔を固定するよりランダムに変化させて方が毎回の周期性が変化し乱数性が高くなると考えられる．このランダムな変化量として，試行回数 1 回前の生成鍵の一部(例えば鍵の 1~6 の 6 ビット)を 10 進数として用いるものとする．この場合，盗聴局において前回の鍵が推測できていないと，インターリーブ間隔がわからなくなりそのときの鍵の推定がより困難となる効果もある．また，RSSI インターリーブ後にデータ削除を行うことで，インターリーブを行っても残ってしまうような周期性を減少でき，より乱数性の高い鍵が生成できる．

4.3.5. 盗聴対策(キャリア周波数切換)

4.2.4.のシミュレーションで示したように，正規ユーザと同方向に盗聴者が存在する場合，正規ユーザ間の鍵と盗聴局において同様の方法で生成された鍵の相関が高くなり，正規の鍵を推測されてしまう恐れがある．この盗聴対策としてキャリア周波数切換生成を行う．盗聴局との鍵の相関は 4.2.5.で示したように各局の配置，周波数チャネルに依存する．実際の場合，盗聴局の配置はわからないため，盗聴局において相関の低いチャネルを推定することは不可能である．しかし，相関の低いチャネルが存在していることを考慮すると，複数のキャリア周波数を切り換えながら秘密鍵を生成することにより，盗聴局との鍵相関を低く抑えることが可能であると考えられる．

4.4. 実験結果

4.4.1. 閾値付近データ削除

a. データ削除の効果

図 4-16 にデータ削除を行っていない測定データを示す．この図は 128 個の RSSI 値を取得し，そのすべてを用いて 128 ビットの鍵生成を 500 回行ったときの鍵の誤りビット数の分布である．図より，正規局間での誤りビット数が 20 個付近に分散しており，誤り訂正処理を行っても鍵一致が難しいことがわかる．鍵の一致率は 32 ビット中で 3 ビットの誤り訂正を行っても，ほぼ 0%であった．この結果は，丸め誤差を考慮して最も誤りが増加していたときのシミュレーション結果より悪く，シミュレーションでは考慮していない装置の個体差，伝搬路の変動等の影響と考えられる．

図 4-17 に示す RSSI 履歴の一例を見ると親局・子局の履歴の変化特性は似通っているので伝搬路の相反性は成り立っていることがわかる．しかし，数 dB の微妙なずれが閾値付近で誤りになっている．

測定当時，試作機は閾値付近の削除を行う機能を有していなかったため，実測した RSSI 履歴を用いコンピュータによるデータ処理を行うことで評価を行う．データ処理の内容は 128 個の RSSI 値 3 回分の 384 個の RSSI 値使用し，親局側で 128 個を削除，子局側で 128b 個を削除することで 128 ビットの鍵を得るものとする．

図 4-16 に示したものと同一のデータを用いてデー

タ処理により閾値付近を削除した鍵生成を 170 回行ったときの鍵の誤りビット数分布を図 4-18 に，32 ビット毎に行う誤り訂正のビット数に対する鍵一致率のグラフを図 4-19 に示す．これらの図より閾値付近のデータ削除を行い，32 ビット毎に 2 ビットの誤り訂正を行えば試行回数の 95%以上の確率で鍵一致が得られる程度まで不一致ビットを減少できていることがわかる．また，参考としてデータ削除を行った場合の SNR 対鍵一致率のシミュレーション結果を別途記載する(図 d-1,2)．図 4-6 で示したような誤りのある SNR10dB において 2 ビットの誤り訂正を行うと約 95%の一致が得られている．

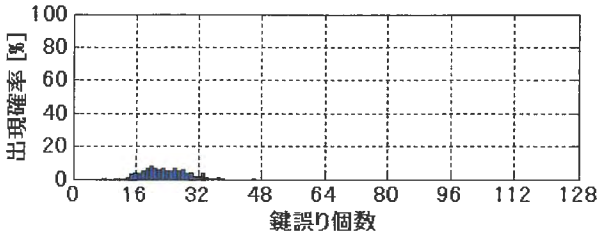


図 4-16　鍵誤り個数分布(データ削除なし)

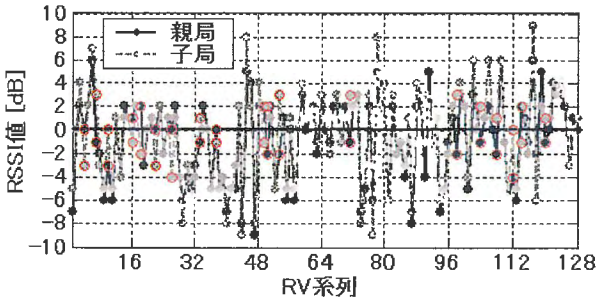


図 4-17　RSSI 履歴

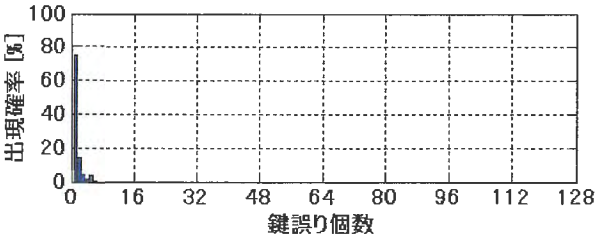


図 4-18　鍵誤り個数分布(データ削除あり)

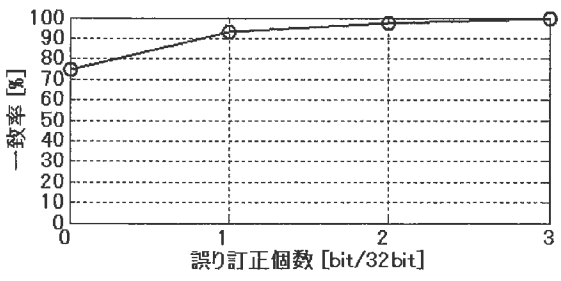


図 4-19　誤り訂正ビット数に対する鍵一致率

b. 位置による正規局での鍵一致特性

次に子局を図 4-26 に示す①から⑤の位置に動かし測定を行ったときの正規局間での鍵の一致率を調べる．このときの正規局間での鍵一致率を図 4-27 に，鍵の相関を図 4-28 に示す．図 4-27 より閾値付近のデータ削除をしない場合は一番良い④の位置において 2bit の誤り訂正を行っても試行回数の 10%程度しか一致しない．データ削除を行うと，一番一致率の低い⑤の位置でも 2bit の誤り訂正を行うことで 90%以上の一致率が得られている．図 4-28 に示すようにデータ削除なしのときは鍵の相関が 0.4～0.9 と広く分布しているが，データ削除を行うことで鍵の一致率と同時に鍵の相関も向上することがわかる．また，これらの結果より，このような電波が問題なく届く屋内環境では，一致率は距離より親局・子局の位置に依存すると考えられる．

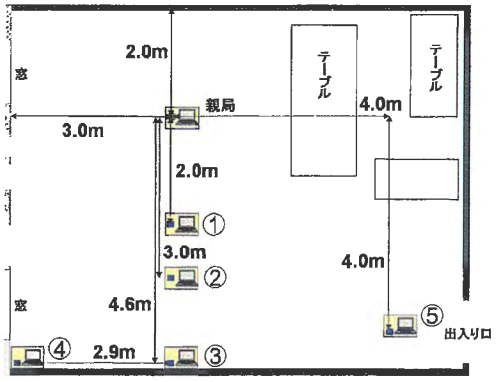


図 4-26　端末配置

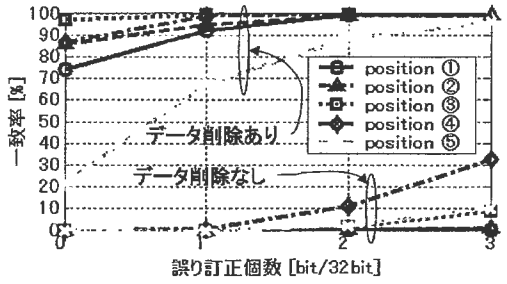


図 4-27　正規局間での鍵一致率

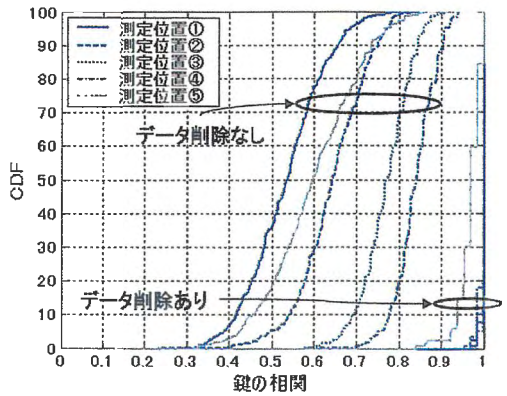


図 4-28　正規局間での鍵相関

c. 盗聴局での RSSI の相関特性

図 4-26 の配置において，親局 - 子局間の子局から 1 mの位置に盗聴局を設置した場合の，子局と盗聴局の鍵の相関を図 4-29 に示す．この図より盗聴局での相関値も位置によって大きく異なることがわかる．この場合のデータ削除を行って相関が最も高い⑤の位置においても盗聴局の鍵一致率は 0%であった．しかし，相関が高いと鍵が一致していなくても，取得したデータより鍵が推測される恐れがあるため相関を下げる工夫は必要である．なお，この章の相関は絶対値にした相関値のみを示している．実際には負の相関もあるが，ここでは相関の正負はあまり関係しないため絶対値で示した．

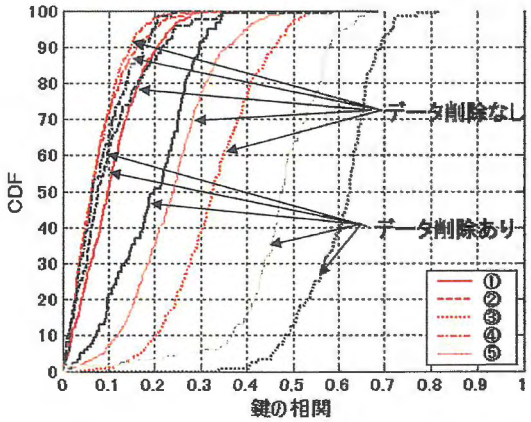


図 4-28　子局 - 盗聴局間での鍵相関

4.4.2. RSSI インターリーブの効果

環境の変化のあるときの RSSI 履歴として，子局を持って室内を歩行速度程度で無作為に移動したときの RSSI 履歴の一例を図 4-20 に示す．また，これについてデータ削除を行った場合の RSSI 履歴を図 4-21 に示す．図 4-20，図 4-21 において 0 以上が鍵'1'，0 以下が鍵'0'となる．図 4-20 の網掛け部分は閾値付近のデータ削除を行うときに削除される範囲である．図 4-20，図 4-21 より，端末が歩行速度で移動することで生成する鍵に大きな偏りがでてしまうことがわかる．

次に，図 4-20 と同様のデータに 2 回のインターリーブを行った(図 4-26 のフローチャート参照)RSSI 履歴を図 4-22 に，その後データ削除を行った RSSI 履歴を図 4-23 に示す．図 4-22 よりインターリーブ前に見られるような偏りがなくなっていることが確認できる．図 4-23 より最終的な鍵としても'0','1'が適度に分散したユニークなものができていることがわかる．

また，表 4-2 よりインターリーブは 3 回，またはインターリーブ → データ削除(親局) → インターリーブ → データ削除(子局)と 2 回行えば(図 4-27 のフローチャート参照)乱数性の高い鍵ができることがわかる．インターリーブなし，ありでそれぞれ 200 回鍵生成を行ったとき，生成された鍵の'0','1'のマップを図 4-24，4-25 に示す．横一列が縦軸の生成回数番目の鍵 128 ビットであり，黒部分が鍵の'0'白部分が鍵'1'を表している．これらの図からも全般的に偏りの多い鍵ができてしまう場合においても，インターリーブを行うことで'0','1'が均等に分散している偏りのない鍵が生成できることが確認できる．乱数検定の詳細は後の付録に記載している．

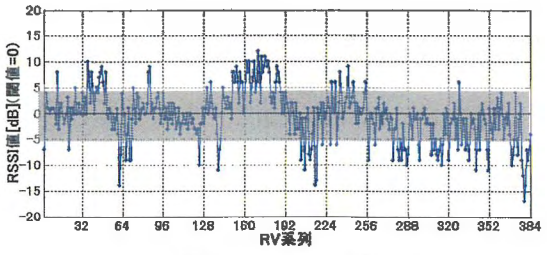


図 4-20　RSSI 履歴

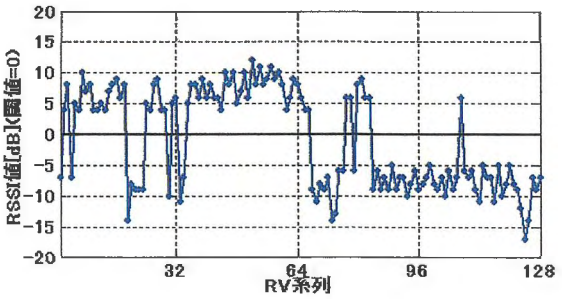


図 4-21　RSSI 履歴(データ削除)

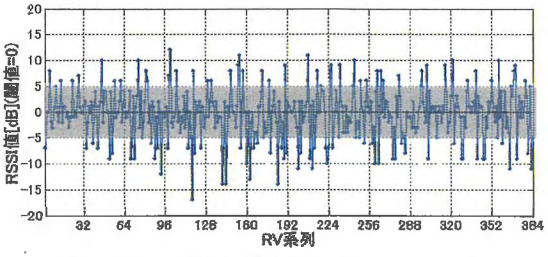


図 4-22　RSSI 履歴(インターリーブ)

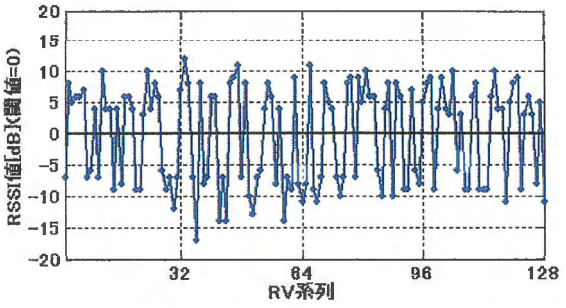


図 4-23　RSSI 履歴(インターリーブ・データ削除)

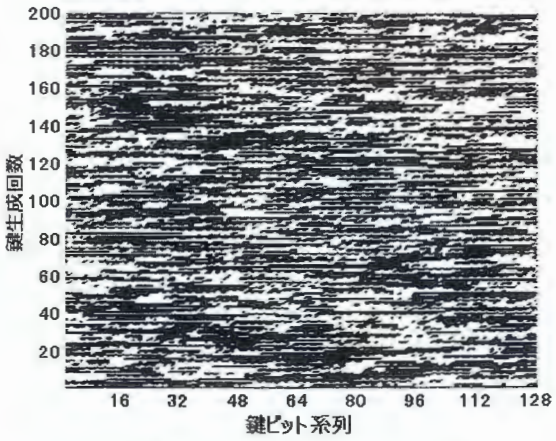


図 4-24　生成鍵の'0','1'分布

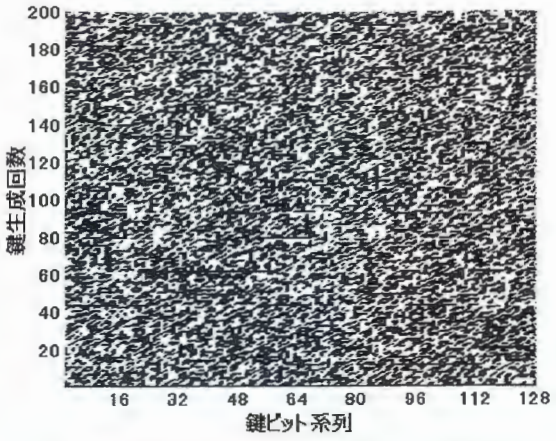


図 4-25　生成鍵の'0','1'分布(インターリーブ)

表 4-2　インターリーブ回数による乱数検定パス確率 [%]

(a) Poker 検定

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	96	97	94	95	100	97	98	99	96	98	96	95	100	97	99	99
2	83	90	95	88	92	85	94	89	81	91	95	94	92	90	92	96
3	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
2'	100	100	100	98	100	100	100	100	100	100	100	100	100	100	100	100

(a) Runs 検定

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	71	61	63	63	72	83	80	73	76	79	92	71	83	78	75	91
2	92	96	97	97	98	97	97	93	97	95	99	98	95	97	98	97
3	100	98	100	100	100	99	100	100	100	99	99	100	100	100	97	100
2'	100	100	100	98	100	100	100	100	100	100	96	100	100	100	100	100

2': インターリーブ 2 回　インターリーブ → データ削除(AP) → インターリーブ → データ削除(UT)

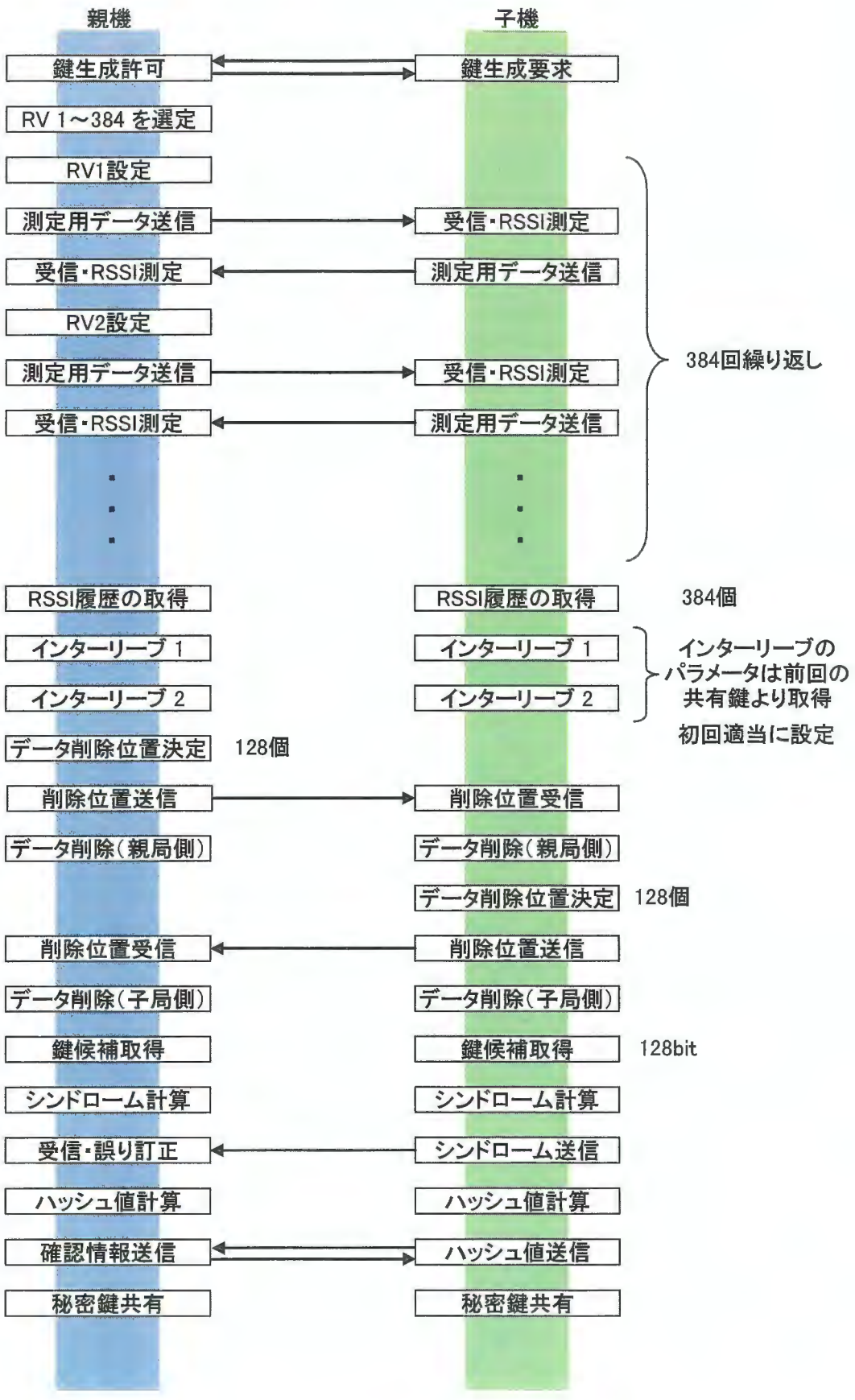


図 4-26　フローチャート（データ削除前にインターリーブ）

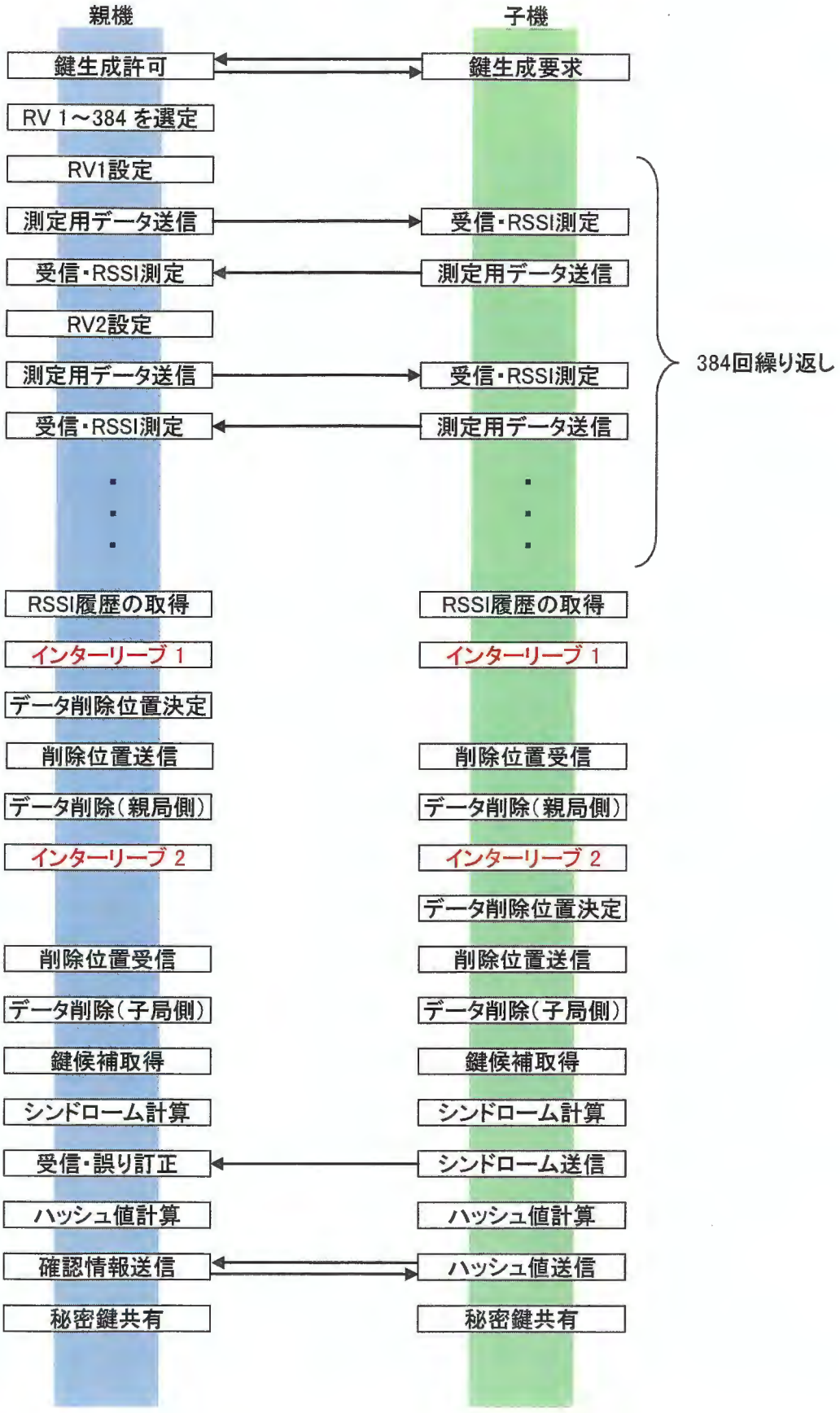


図 4-27　フローチャート（データ削除の間でインターリーブ）

4.4.3. キャリア周波数切換による鍵生成

キャリア周波数切り換えを行った場合の特性については文献[19]にて述べているので図表は省略する．ある周波数において盗聴局との相関が高い場合においても，キャリア周波数を切り換えながら鍵を生成することで，盗聴局との相関を低く抑えることができる可能性が確認できている．

しかし，正規局の位置によってはある周波数を用いて鍵生成を行った場合に，一致率が低い場合がある．盗聴対策として，キャリア周波数を切り換え鍵生成を行ったとき，一致率の低い周波数を用いてしまうことで平均的な一致率も低下してしまうと考えられる．そのため，全周波数のレベルを見て用いる周波数を決定する等の工夫が必要であると考えられる．

4.4.4. 様々な条件での実験結果

次に，

E1：盗聴局にて ch23 の相関が高くなるよう設置
E2：盗聴局にて ch26 の相関が高くなるよう設置
E3：AP が天井付近になるよう設置
E4：E3 の位置で AP を上下逆に配置
E5：E3 の測定を，日を変えて測定
E6：E4 の測定を，日を変えて測定
E7：実験室内を歩行速度で移動
E8：居室内に設置
E9：1F 食堂前に設置

の 8 箇所において周波数を切り換え測定を行ったときの実験結果を後ろに別途記載する．それぞれの位置において正規局での鍵相関，盗聴局と正規局間での鍵相関，データ削除ありなしでの一致率，データ削除時の乱数検定結果，親局・子局での平均 RSSI と RSSI 差を示す．

正規局での鍵相関，盗聴局と正規局間での鍵相関については，データ削除あり・なしについて記載し，データ削除を行うことで鍵の相関が高くなる(マイナス相関の場合は低くなる)ことが確認できる．

データ削除ありなしでの一致率を見れば，データ削除を行うことで鍵の一致率が格段に向上することがわかる．また，測定位置により，一致しにくい周波数も存在することが確認できる．

乱数検定については，インターリーブを行っていない場合の結果を示している．共有が成功した鍵を 2 値系列とし，20000 ビットを用いて検定を行うため，一致率の低いときは検定結果なしとなっている．結果より，インターリーブを行わないでも検定をパスする位置・周波数，パスしない位置・周波数があることがわかる．先のインターリーブの効果に示した UT が移動しているような場合は，偏りが大きくまったく検定をパスしないことがわかる．

親局・子局での平均 RSSI と RSSI 差からは周波数チャネルごとに，親局と子局間の RSSI のレベル差に違いがあることがわかる．各々の位置での結果を一まとめにした表・グラフを実験結果の最後に記載しているが，ここの図 E-3 より，測定を行った位置によらずチャネル 11 では親局での受信 RSSI レベルが高くなり，チャネルが大きくなると親局のレベルが低くなり，19 チャネルあたりでレベル差が最大に，そしてレベル差が小さくなり 26 チャネルでは再び親局のレベルが高くなる，といった特性になっていることがわかる．このことから，装置に依存する周波数特性があると考えられる．また，UT が移動するときの RSSI の平均値を考えると，周波数が変わることでの位置依存のレベル差は平均化されると考えられる．図 E-1 と図 E-2 の UT 移動時の特性を比較すると，図 E-2 の子局側での受信 RSSI がほぼ平坦になっていることから，親局に何らかの周波数依存があると考えられる．

全周波数のデータがそろっているものに関しては，周波数切換にて鍵生成を行った場合の正規局・盗聴局においての鍵不一致個数分布，鍵の相関，RSSI インターリーブをデータ削除の間で 2 回行った場合の各種乱数検定結果を示している．このとき，各周波数のでたについては取得データをそのまま用い，データのレベル差の補正は行っていない．

5. まとめ

以上の実験結果を踏まえた ZigBee –ESPARSKey の仕様案を巻末に示す．要求条件として，生成鍵ビットは 128 ビット，鍵生成にかかる時間が 1 秒程度，鍵の一致率は 90%あれば，失敗時に N 回リトライを行えば $(1-10^{-N})$の一致率が得られ，数秒でほぼ 100%の鍵一致となることから 90%を条件とする．

以上を満たす仕様案として，取得する RSSI の個数を 384 個とし，データ削除により親局にて 128 個，子局にて 128 個を削除する．

RSSIインターリーブは2回を仕様案と同様に示すフローチャートのようにデータ削除の間にかますかたちで行う．

盗聴対策として周波数切り換え生成を行うものとするが．このときの使用周波数・切り換えタイミングや周波数毎のレベル差の補正については今後の検討課題である．また，誤り訂正についても今回は 32 ビットのブロックで 2 ビット程度の訂正を行うものとして評価しているが，シンドローム送信による冗長ビット分のデータを省くなど検討課題は残っている．

付録

・乱数検定

米国連邦政府の情報処理設備調達基準 FIPS(Federal Information Processing Standards)のうちFIPS PUB 140-2には,暗号モジュールに関する基準が設けられている.この中の乱数に関する項目として,4 種類の統計検定が設けられている.

1. The Monobit Test

二値数列 20,000bit 中に現われる'1'の数を数える.

統計量 x ：20,000bit 中の'1'の数

採択域 ：$9{,}725 < x < 10{,}275$

2. The Poker Test

二値数列 20,000bit を 4bit ずつ 5,000 個のセルに区切る.セルのパターンとして 2^4=16 種類あり,各々のパターン(パターン番号を i=0~15 とする)について出現数 g_i をカウントする.あるパターンの出現頻度が高く(低く)なると統計量 x は大きくなる.

統計量 x ： $x = (16/5000) \times \sum_{i=0}^{15} g_i^{\,2} - 5000$

採択域 ：$2.16 < x < 46.17$

3. The Runs Test

同じ数列の続きを連と言い,この検定では二値数列 20,000bit 内に現れた,ある長さの連の個数をカウントする.検定は連の長さ 1,2,3,4,5,及び 6 以上に関して個別に行う.さらに乱数値'1'と'0'についてそれぞれ行うため,計 12 個の検定になる.

統計量 x ：20,000bit 中に現れる各長さの連の数

採択域 ：

連の長さ	採択域
1	$2{,}315 \leqq x \leqq 2{,}685$
2	$1{,}114 \leqq x \leqq 1{,}386$
3	$527 \leqq x \leqq 723$
4	$240 \leqq x \leqq 384$
5	$103 \leqq x \leqq 209$
6 以上	$103 \leqq x \leqq 209$

4. The Longruns Test

二値数列 20,000bit 中に現れる連のうち,最長の連の長さ.

統計量 x ：20,000bit 中で最長の連の長さ
(ビット値の区別なし)

採択域 ：$x < 26$

・盗聴局での鍵解読に対する安全性

どの程度まで相関が低ければ盗聴に対し安全かという議論もあるが,細かな計算コストは盗聴者の前提条件や解読方法など様々な要素が入ってくるため,具体的に示すことは困難である.解読法の一例として,盗聴者が自身の取得した鍵より総当りで,鍵を推測する場合の方法として,鍵が一致しているものとして検証,鍵が 1 ビット誤っているものとして 1 ビットを反転し検証…と言う風に検証していくとすると,鍵長 k 誤り x ビットの時の演算量 R は,

$$R = \sum_{i=1}^{x} {}_k C_i$$

となる.

例えば,鍵長 128 ビットで誤りが 20 ビット,誤り訂正用のシンドロームも利用され計 8 ビットの訂正が行われたと仮定した場合,誤ビット数 x は 12 ビットと等価になるため,この計算方法で考えると $R = 2.6 \times 10^{16}$ となり,DES の総当りの演算量 $2^{56} = 7.2 \times 10^{16}$ と比較が約 22 時間で解読されたことを考慮すると,解読される危険性が高いと言える.また,相関が高い場合に盗聴局において鍵の不一致となっている位置は取得した RSSI の閾値付近である可能性が高いため,その点も考慮して解読を行うとコンビネーションの左の数が小さくなり,R がさらに減少するとも考えられる.

しかし,この秘密鍵共有方式においては,鍵長を長くすれば,推測した鍵から解読を行うための場合の数は大きく増加する.

同じ割合で鍵誤りが発生している場合,鍵長が 256 ビットで誤りが 24 ビットの演算量は,$R = 3.3 \times 10^{33}$ となり,鍵長の線形増加に対し演算量が指数的に増加していることがわかる.鍵長を 2 倍にするには鍵生成時間を 2 倍かければよいので,鍵生成に時間をかければ,盗聴局での演算量は指数的に増加し,鍵の推測はより困難になっていくことがわかる.

このことから,秘密鍵共有方式では鍵生成に時間さえかければ相関がある程度高い位置で盗聴されても演算量的に推測不可能な鍵を生成でき安全な鍵生成共有方法であると言える.

参考文献

[1] 笹原正雄，境隆一，暗号，共立出版，2002.

[2] 岡本龍明，山本博資，現代暗号，産業図書，1979.

[3] U.M.Maure，“Secret Key Agreement by Public Discussion from Common Information，” IEEE Trans. Inform. Theory vol.39, no.3, May 1993.

[4] 中山清喬，笹岡秀一，“陸上移動通信における通信路雑音を用いたセキュリティ通信方式の検討，” 信学総大，B-5-73, Mar. 2002.

[5] J.E.Hershey，A.A.Hassan，and R.yarlagadda，“Unconventional Cryptographic Keying Variable Management，” IEEE Trans. Commun., vol.43, pp.3-6, Jan. 1995.

[6] H.Koorapaty, A.A.Hassan, S.Chennakeshu, “Secure Information Transmission for Mobile Radio，” IEEE Commun. Letters, vol.4, pp52-55, Feb.2000.

[7] 本多真，原田博司，藤瀬雅行，“伝播路特性を生成源とする暗号鍵生成手法，” 信学技報，SR02-04, pp.23-29, Apr. 2002.

[8] 堀池元樹，笹岡秀一，“陸上移動通信路の不規則変動に基づく秘密鍵共有方式，” 信学技報，RCS2002-173, pp.7-12, Oct. 2002.

[9] 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，” 信学技報，RCS2003-121, pp.23-28, Aug. 2003.

[10] 北浦明人，笹岡秀一，“陸上移動通信におけるアンテナ切換えによる受信信号強度変化を利用した秘密鍵共有方式，” 信学技報，RCS2004-257, pp.121-126, Jan. 2004.

[11] 小川佳彦，笹岡秀一，今井友裕，“MIMO-OFDM システムにおける相関行列の固有値変動に基づく秘密鍵共有方式の検討，” 信学技報，RCS2004-257, pp.127-132, Jan. 2004.

[12] T.Ohira and J.Cheng, “Analog smart antennas，” Adaptive Antenna Arrays, pp.184-204, ISBN3-540-20199-8, Berlin: Springer Verlag, June 2004.

[13] 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)J87-C, no.1, pp.12-31 Jan. 2004.

[14] 青野智之，俵覚，大平孝，小宮山牧兒，北浦明人，森浩樹，笹岡秀一，“リアクタンスドメインRSSI プロファイルを用いた秘密鍵生成共有方式の提案，” 信学技報，RCS2003-242, pp45-50, Jan. 2004.

[15] 森浩樹，笹岡秀一，大平孝，“エスパアンテナによる受信信号強度変化を用いた秘密鍵共有方式における鍵一致率特性の評価，” 信学技報，RCS2003-356, pp19-24, March 2004.

[16] 青野智之，大平孝，小宮山牧兒，笹岡秀一，“エスパアンテナを駆使して秘密鍵を生成共有する無線 LAN アクセスポイント試作機：物理層技術による無線セキュリティ，” 信学技報，SR04-2, pp21-24, May 2004.

[17] 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, pp7-12, July 2004.

[18] 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IEEE802.15.4 無線 PAN 秘密鍵共有方式の評価実験，” 信学技報，RCS2004-258, pp133-138, Jan. 2005.

[19] 青野智之，樋口啓介，太郎丸眞，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秘密鍵共有方式～キャリア周波数切換による生成鍵の特性評価実験，” 信学技報，RCS2004-334, pp61-66, March 2005.

[20] 大平孝，笹岡秀一，“盗聴防止アンテナ：セキュリティ対策への物理層アプローチ，” 信学誌 vol.88, No.3, pp190-194, March 2005.

[21] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4GHz Band, IEEE.

[22] http://www.zigbee.org/

[23] http://www.chipcon.com/

プログラムリスト

すべてに共通
- time_disp1：経過時間等表示用
- time_disp2：経過時間等表示用
- time_disp3：経過時間等表示用

無線 LAN 版

SNR 対鍵一致率

main_base_re
- steer_vector：ステアリングベクトル計算
- ray_tracing1：レイトレーシング
- RSSI_to_KEY：RSSI を鍵に変換

送信電力対鍵一致率

main_base_tr
- 同上

部屋全体での鍵一致率

all_key_agree
- 同上

部屋全体での盗聴率

all_key_cc
- 同上

ZigBee 版

シミュレーション

SNR 対鍵一致率

main_base_re_ZigBee
- steer_vector：ステアリングベクトル計算
- ray_tracing1：レイトレーシング
- RSSI_to_KEY：RSSI を鍵に変換

送信電力対鍵一致率

main_base_tr_ZigBee
- 同上

部屋全体での鍵一致率

all_key_agree_ZigBee
- 同上

部屋全体での盗聴率

all_key_cc_ZigBee
- 同上

周波数チャネル対鍵一致率

main_base_f_ZigBee
- steer_vector：ステアリングベクトル計算
- ray_tracing1_f：レイトレーシング
- RSSI_to_KEY：RSSI を鍵に変換

部屋全体での盗聴率(周波数可変)

all_key_cc_f_ZigBee
- 同上

SNR 対鍵一致率(データ削除あり)

main_real_re_ZigBee
- interleave：インターリーブ
- threshold_RSSI：閾値でデータを正規化
- del_data：データ削除
- R2Key_exdata：RSSI を入力閾値で鍵に変換
- bitTestPoker：乱数検定(Poker)

実測データ処理

ファイル 1 種類の処理

read_RSSI
- RSSI_rep：実測 RSSI の記録ずれ簡易補正
- interleave：インターリーブ
- threshold_RSSI：閾値でデータを正規化
- del_data：データ削除
- R2Key_exdata：RSSI を入力閾値で鍵に変換
- bitTestPoker：乱数検定(Poker)
- bitTestRuns：乱数検定(Runs, longRuns)

同一条件のすべての周波数を処理

read_RSSI_fall
- 同上

選択周波数を用いた鍵生成処理

read_RSSI_fconv
- 同上

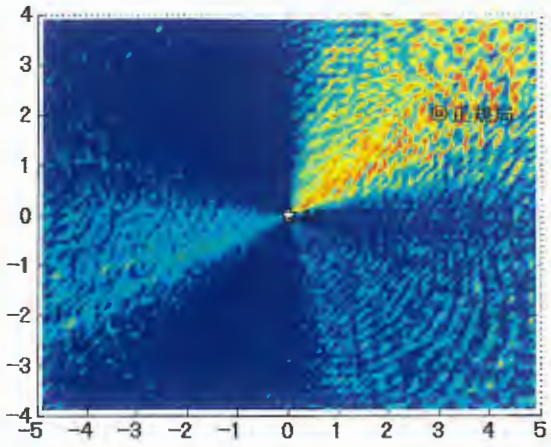
シミュレーション結果

シミュレーション結果の項目

・周波数チャネル毎の鍵相関分布 (ch11~26 + 平均)

・データ削除を行った場合の SNR 対鍵一致率

周波数チャネル毎の鍵相関分布 (ch11~13)
(データファイル ：all_key_cc_f_ZigBee.mat)



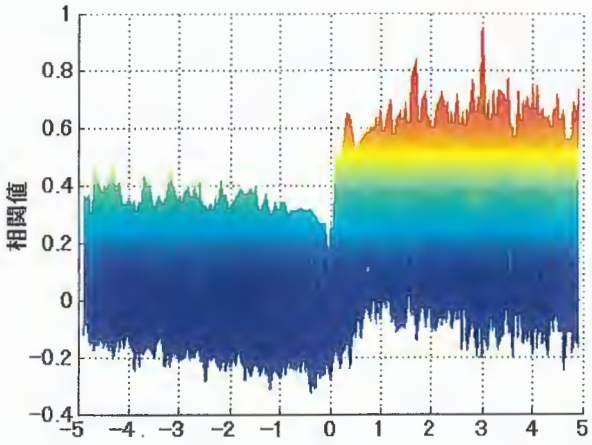
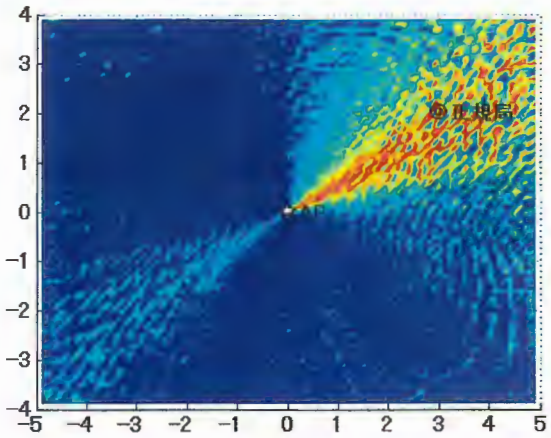


図 f-1　部屋全体での鍵相関分布(ch11)



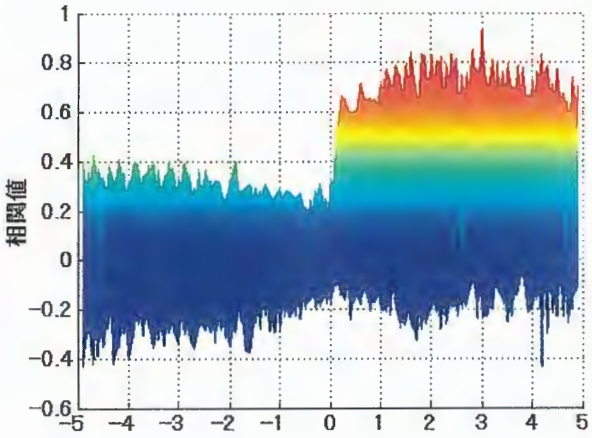
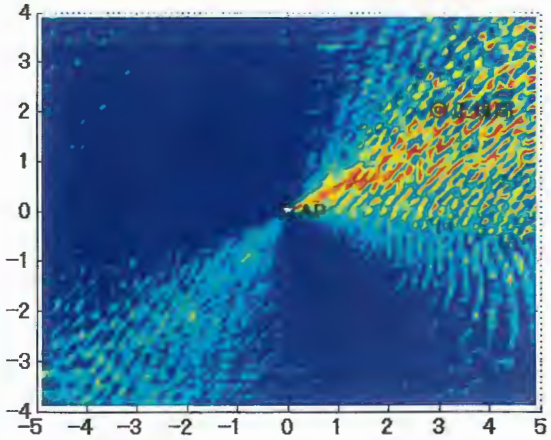


図 f-2　部屋全体での鍵相関分布(ch12)



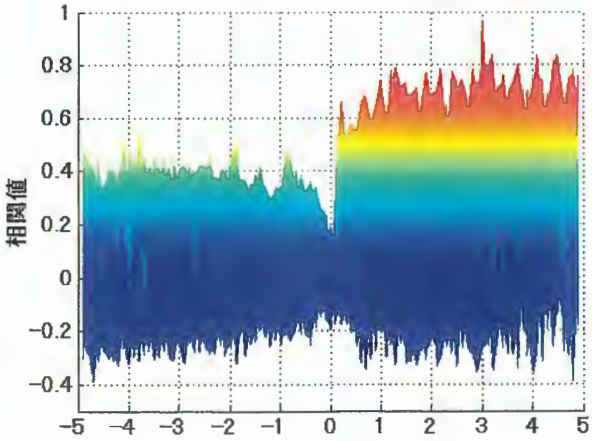


図 f-3　部屋全体での鍵相関分布(ch13)

周波数チャネル毎の鍵相関分布 (ch14~16)
(データファイル ：all_key_cc_f_ZigBee.mat)

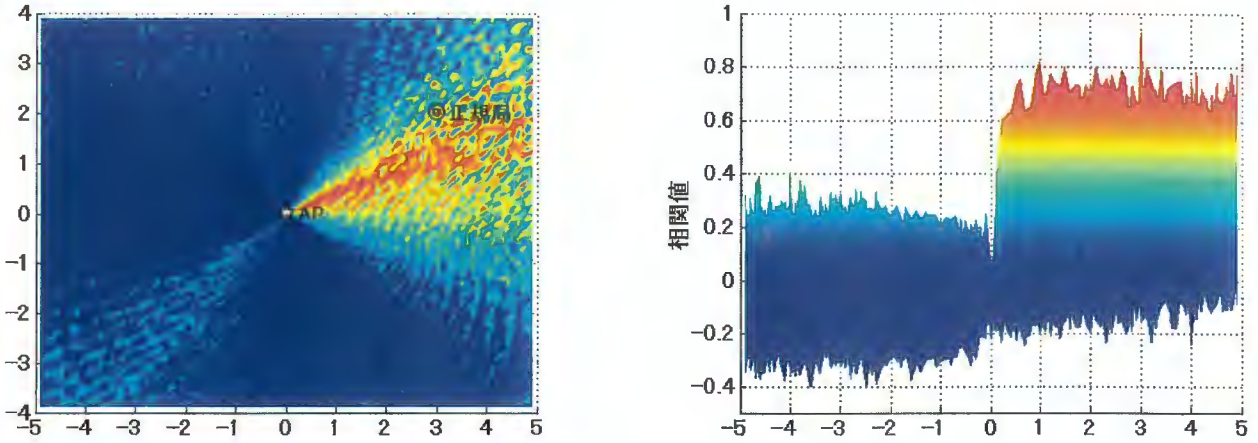


図 f-4　部屋全体での鍵相関分布(ch14)

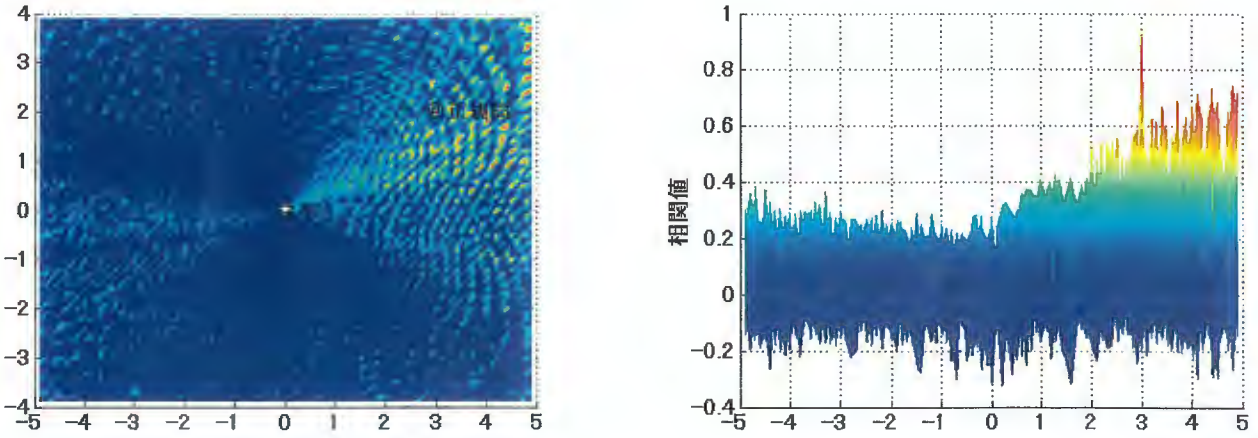


図 f-5　部屋全体での鍵相関分布(ch15)

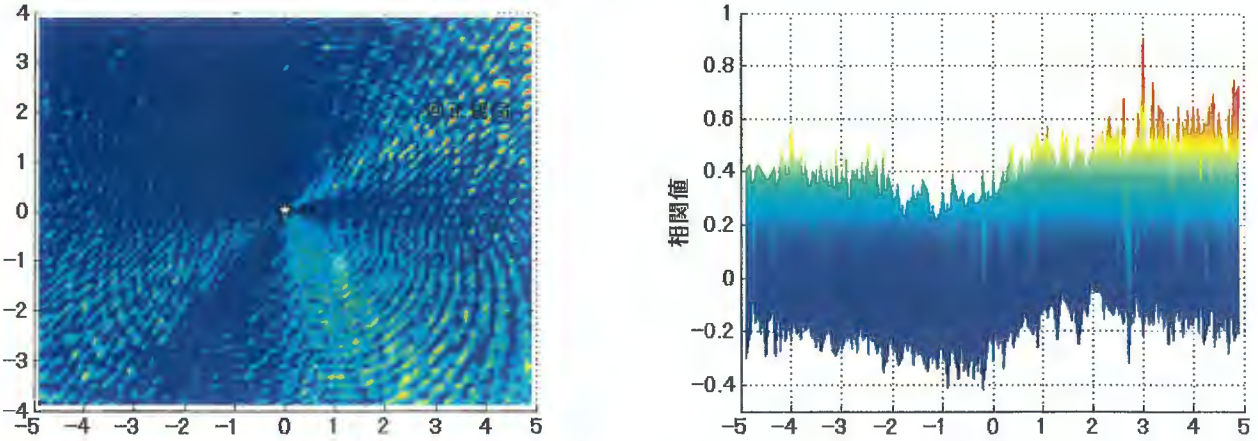


図 f-6　部屋全体での鍵相関分布(ch16)

周波数チャネル毎の鍵相関分布 (ch17~19)
(データファイル ：all_key_cc_f_ZigBee.mat)

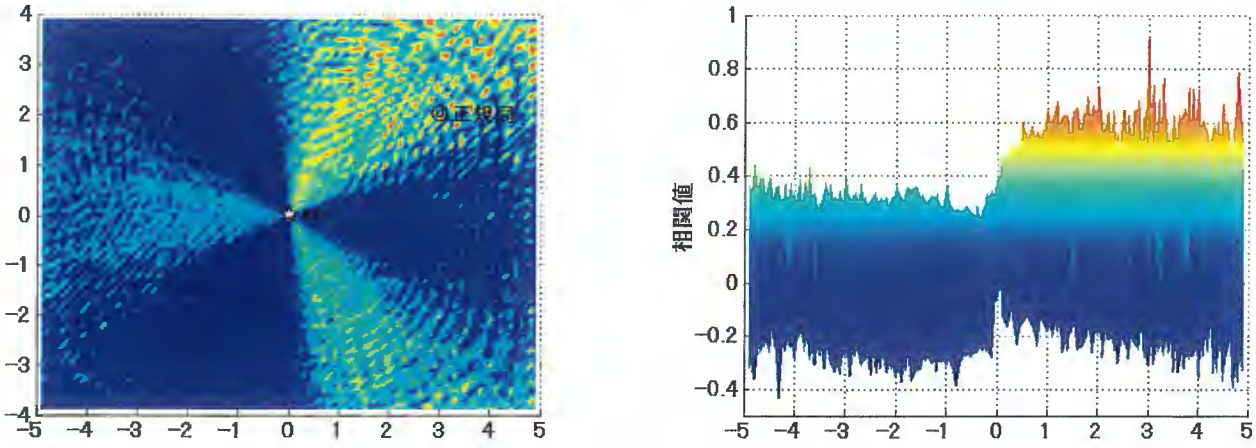


図 f-7　部屋全体での鍵相関分布(ch17)

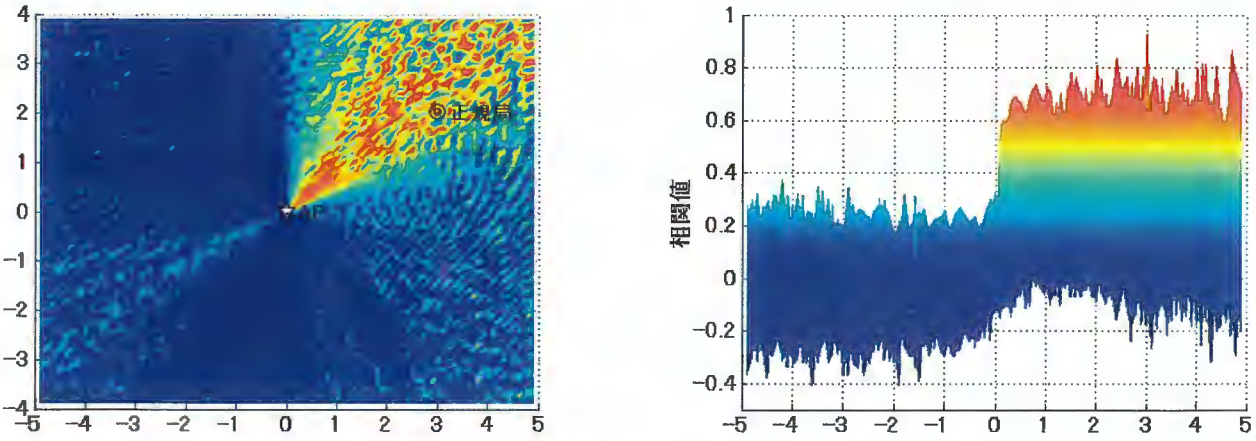


図 f-8　部屋全体での鍵相関分布(ch18)

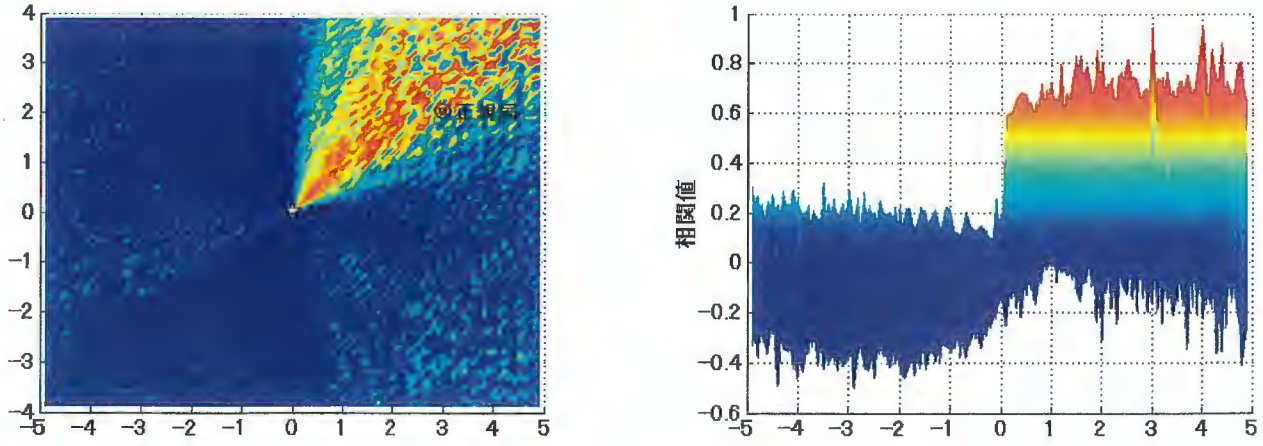


図 f-9　部屋全体での鍵相関分布(ch19)

周波数チャネル毎の鍵相関分布 (ch20~22)
(データファイル ：all_key_cc_f_ZigBee_+-.mat)

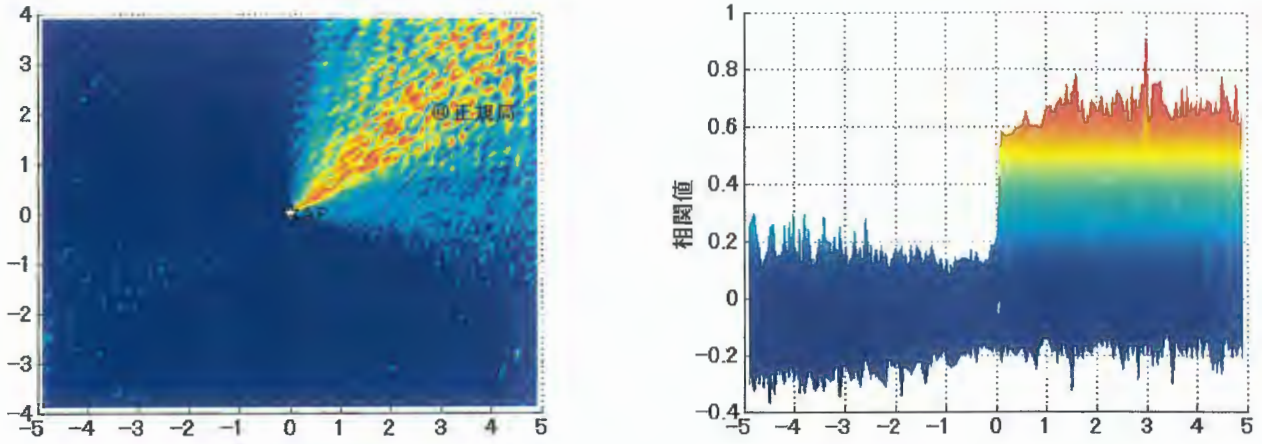


図 f-10　部屋全体での鍵相関分布(ch20)

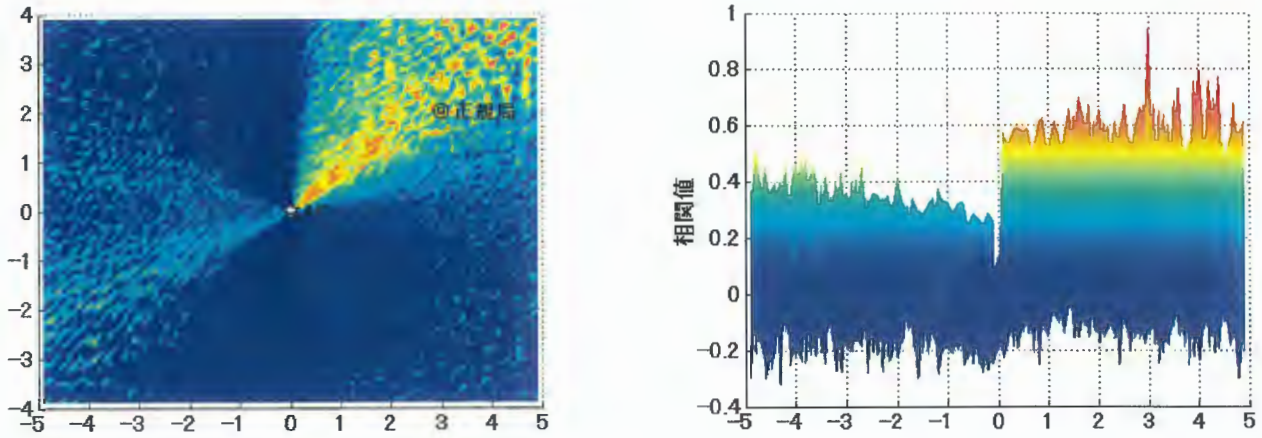


図 f-11　部屋全体での鍵相関分布(ch21)

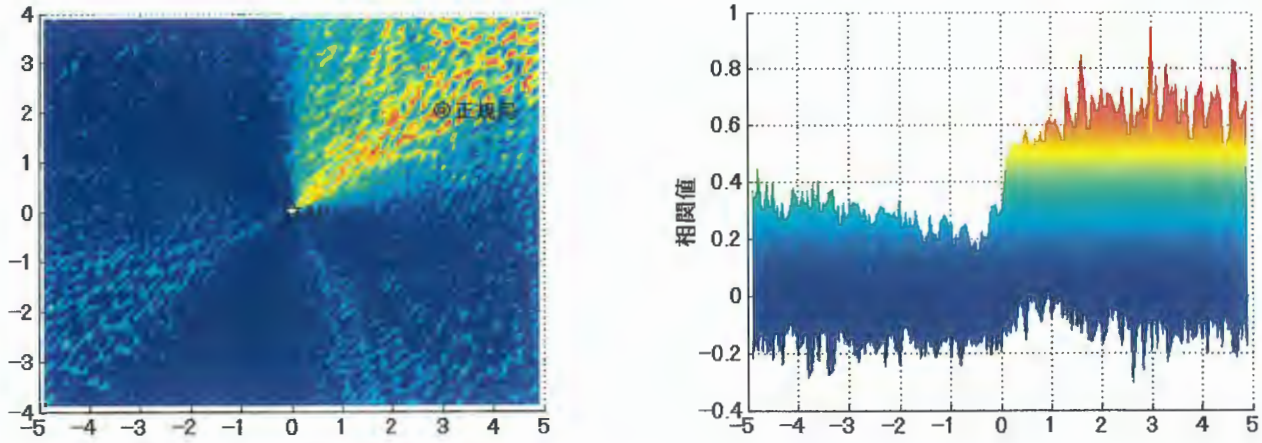


図 f-12　部屋全体での鍵相関分布(ch22)

周波数チャネル毎の鍵相関分布 (ch23~25)
(データファイル ：all_key_cc_f_ZigBee_+-.mat)

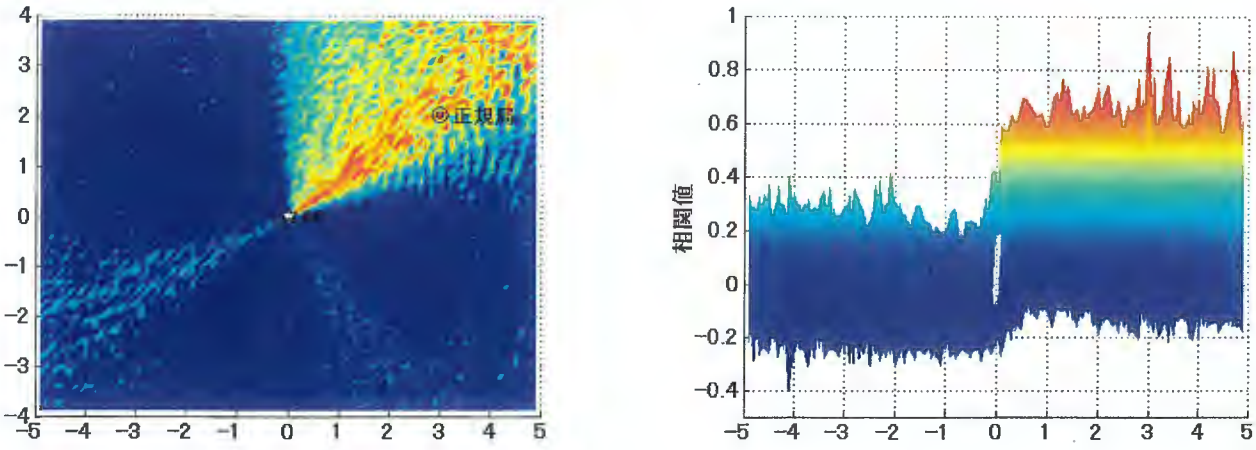


図 f-13　部屋全体での鍵相関分布(ch23)

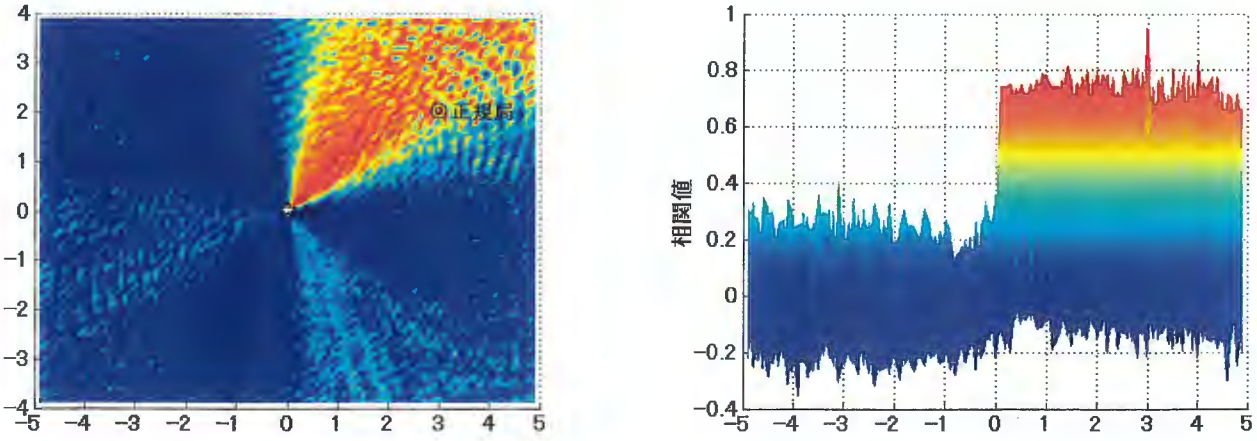


図 f-14　部屋全体での鍵相関分布(ch24)

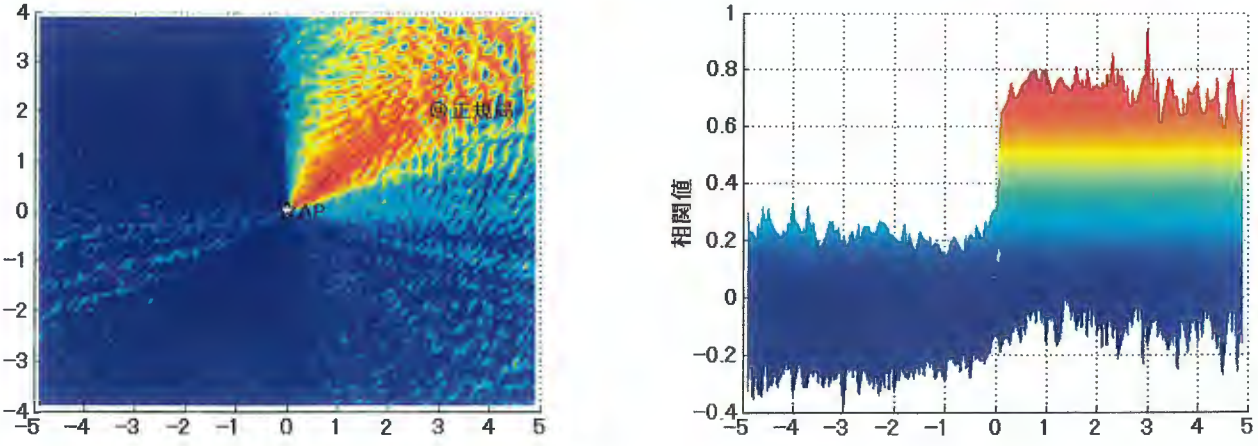


図 f-15　部屋全体での鍵相関分布(ch25)

周波数チャネル毎の鍵相関分布 (ch26 + 平均)
(データファイル : all_key_cc_f_ZigBee_+-.mat)

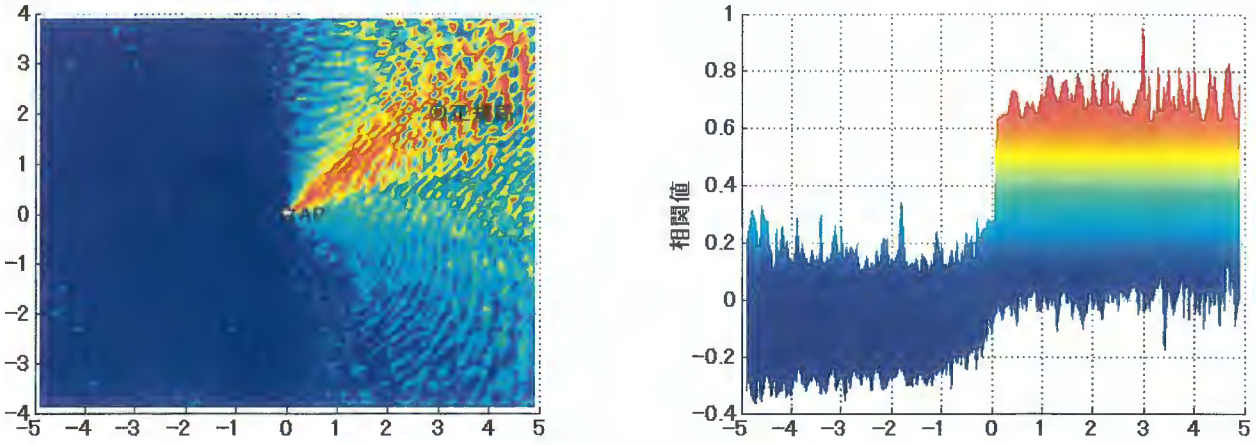


図 f-16　部屋全体での鍵相関分布(ch26)

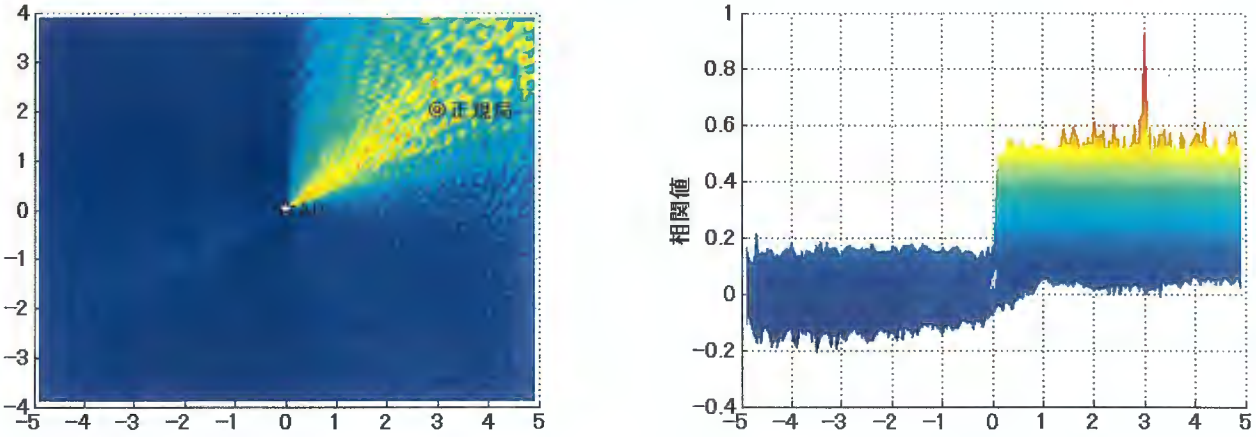


図 f-17　部屋全体での鍵相関分布(平均)

SNR 対鍵一致率
データ削除を行った場合のシミュレーション

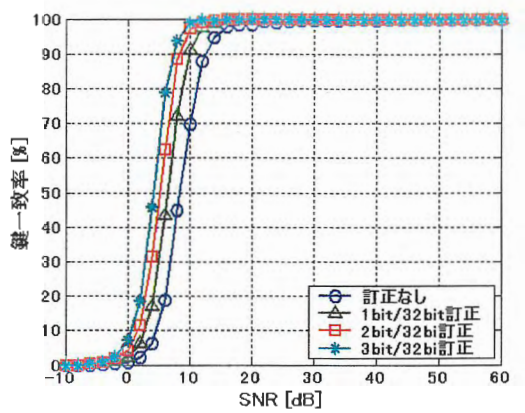


図 d-1　SNR 対鍵一致率特性(丸め誤差なし)

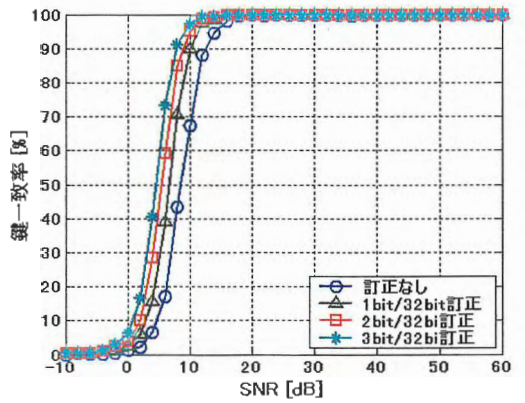


図 d-2　SNR 対鍵一致率特性
(送受信のレベル差 0.5dB 丸め誤差あり)

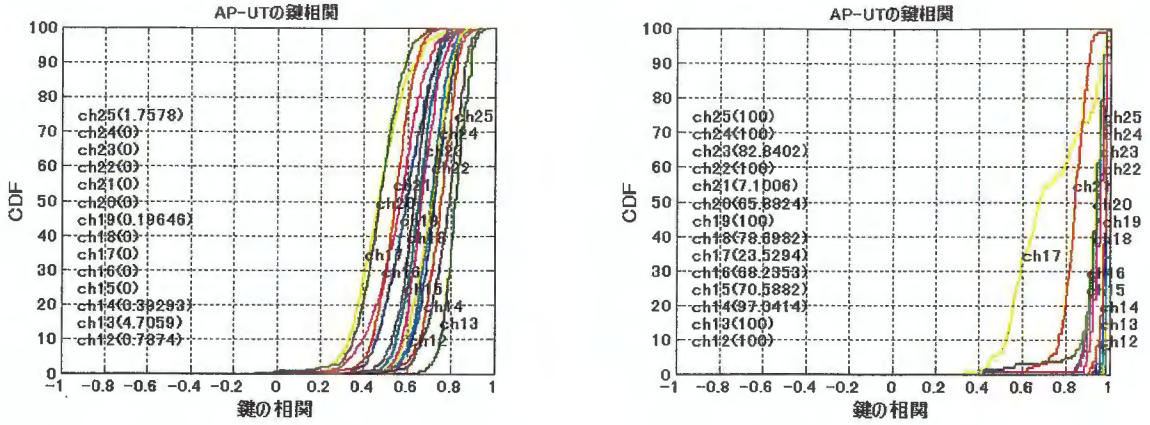
実験結果

E1：実験室内で ch23 の相関が高くなる位置に設置　2005 / 01 / 25 測定
E2：実験室内で ch26 の相関が高くなる位置に設置　2005 / 02 / 01 測定
E3：AP 天井付近に配置　2005 / 02 / 07 測定
E4：AP 天井付近に配置(アンテナを上下逆向きに配置)　2005 / 02 / 08 測定
E5：AP 天井付近に配置 その 2(前回と同じ位置) 2005 / 02 / 09 測定
E6：AP 天井付近に配置 その 2 (アンテナを上下逆向きに配置) (前回と同じ位置) 2005 / 02 / 09 測定
E7：実験室内にて歩行速度程度で UT 移動　2005 / 02 / 10 測定
E8：居室(AP：青野さん横 UT：平田さん横)　2005 / 02 / 14 測定
E9：１Ｆ食堂前　2005 / 02 / 16 測定

結果の項目
図 E○-1　正規局間の鍵相関
　　… 正規局間での鍵相関をデータ削除あり・なしで比較
図 E○-2　正規局と盗聴局間の鍵相関
　　… 正規局と盗聴局間での鍵相関をデータ削除あり・なしで比較
表 E○-1　データ削除ありなしでの鍵一致率 (2bit/32bit 誤り訂正)
　　… 正規局間の鍵一致率をデータ削除あり・なしで比較
表 E○-2　乱数検定結果
　　… データ削除ありのときの乱数検定結果 (Poker 検定・Runs 検定) インターリーブなし
表 E○-3　親局・子局での平均 RSSI 及び RSSI 差
　　… 周波数毎の RSSI 値の平均値

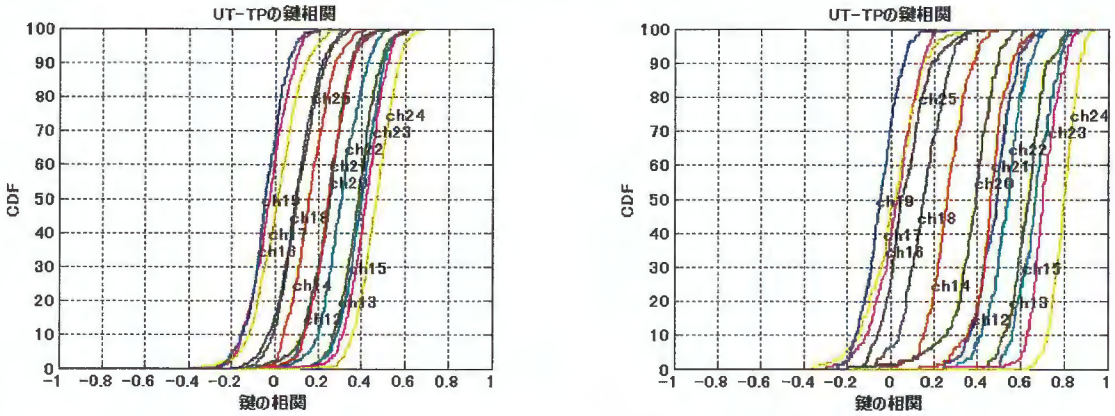
図 E○-3　周波数切り換え生成結果 (全周波数使用)
　　… 全周波数データがあるもののみ結果あり
表 E○-4　各種検定結果及び鍵一致率
　　… 周波数切り換え生成を行った場合の各種結果

E1：実験室内で ch23 の相関が高くなる位置に設置　2005 / 01 / 25 測定



(a) データ削除なし　　(b) データ削除あり

図 E1-1　正規局間の鍵相関



(a) データ削除なし　　(b) データ削除あり

図 E1-2　正規局と盗聴局間の鍵相関

表 E1-1　データ削除ありなしでの鍵一致率（2bit/32bit 誤り訂正）

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
なし	—	0.79	4.71	0.39	0	0	0	0	0.20	0	0	0	0	0	1.76	—
あり	—	100	100	97.0	70.6	68.2	23.5	78.7	100	65.9	7.10	100	82.8	100	100	—

表 E1-2 乱数検定結果

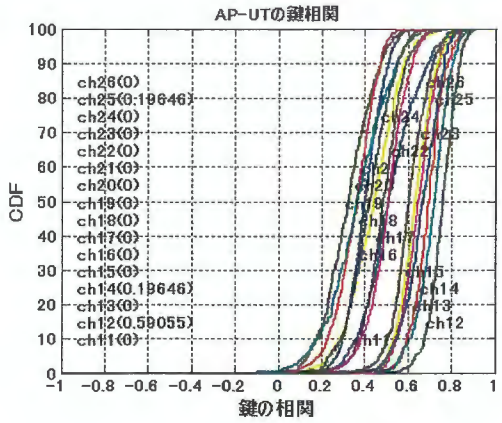
P	—	OK	OK	OK	—	—	—	—	OK	—	—	OK	—	OK	OK	—
R	—	OK	OK	OK	—	—	—	—	OK	—	—	OK	—	OK	OK	—

P：Poker 検定　　R：Runs 検定

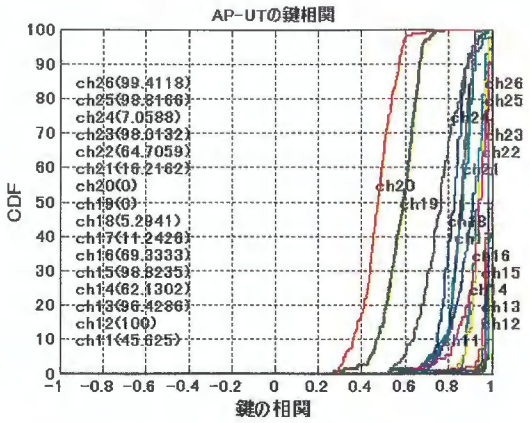
表 E1-3　親局・子局での平均 RSSI 及び RSSI 差

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
親	—	-11	-9.1	-11	-11	-15	-11	-11	-15	-9.7	-11	-4.2	-1.7	-0.1	-1.2	—
子	—	-10	-7.7	-8.8	-8.2	-12	-6.9	-7	-12	-5.5	-7.7	-2.6	-1.3	-1.1	-3.7	—
差	—	-0.5	-1.4	-2.5	-3.3	-3.1	-4.2	-4.2	-3.6	-4.2	-2.9	-1.6	-0.4	0.95	2.51	—

E2：実験室内で ch26 の相関が高くなる位置に設置　2005 / 02 / 01 測定
データ数 510

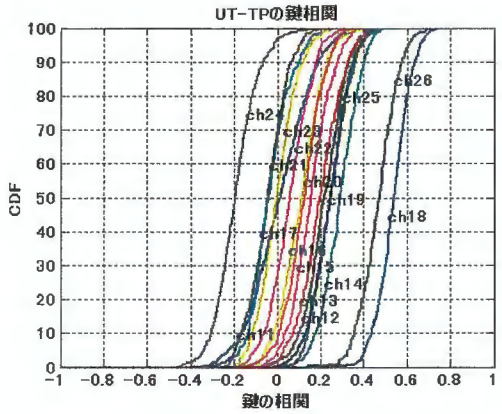


(a) データ削除なし

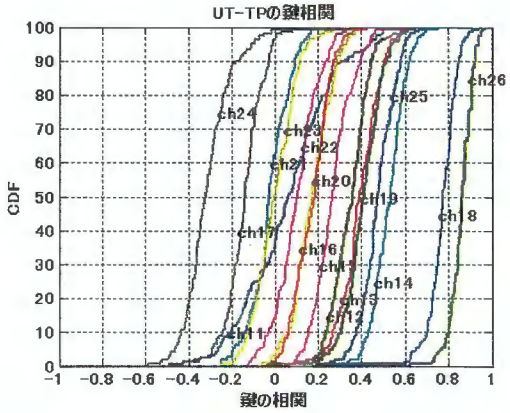


(b) データ削除あり

図 E2-1　正規局間の鍵相関



(a) データ削除なし



(b) データ削除あり

図 E2-2　正規局と盗聴局間の鍵相関

表 E2-1　データ削除ありなしでの鍵一致率（2bit/32bit 誤り訂正）

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
なし	0	0.59	0	0.20	0	0	0	0	0	0	0	0	0	0	0.20	0
あり	45.6	100	98.4	62.1	98.8	69.3	11.2	5.29	0	0	16.2	64.7	98.0	7.05	98.8	99.4

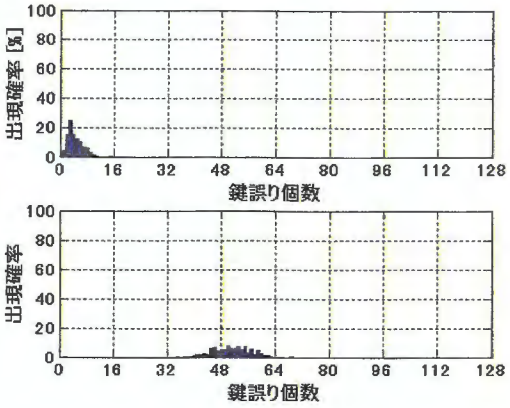
表 E2-2　乱数検定結果

P	—	OK	OK	—	OK	—	—	—	—	—	—	—	—	—	OK	OK
R	—	OK	OK	—	OK	—	—	—	—	—	—	—	—	—	OK	OK

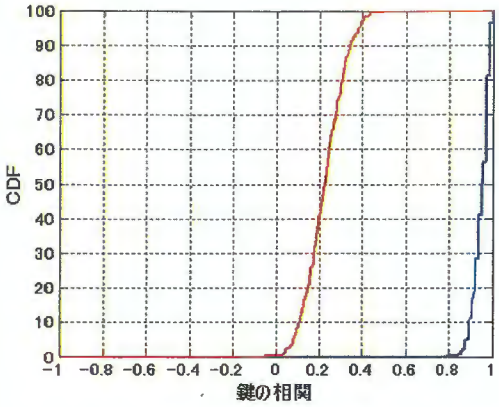
P：Poker 検定　　R：Runs 検定

表 E2-3　親局・子局での平均 RSSI 及び RSSI 差

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
親	-11	-10	-13	-11	-9.1	-13	-11	-7.4	-12	-11	-15	-8.1	-8.7	-12	-9.4	-6.8
子	-11	-9.5	-12	-8.1	-5.3	-9.8	-6.6	-2.1	-8	-8.1	-13	-6.1	-8.1	-12	-11	-10
差	0.09	-0.5	-1.4	-2.5	-3.8	-3.5	-4.6	-5.2	-3.5	-3.1	-1.8	-2	-0.6	0.68	1.83	3.28



(a) 誤り個数分布（上:正規局間 下:盗聴局）



(b) 鍵の相関（青:正規局 赤:盗聴局）

図 E2-3　周波数切り換え生成結果（全周波数使用）

表 E2-4　各種検定結果及び鍵一致率

Poker 検定	
採択域	
2.16 - 46.17	23.0912

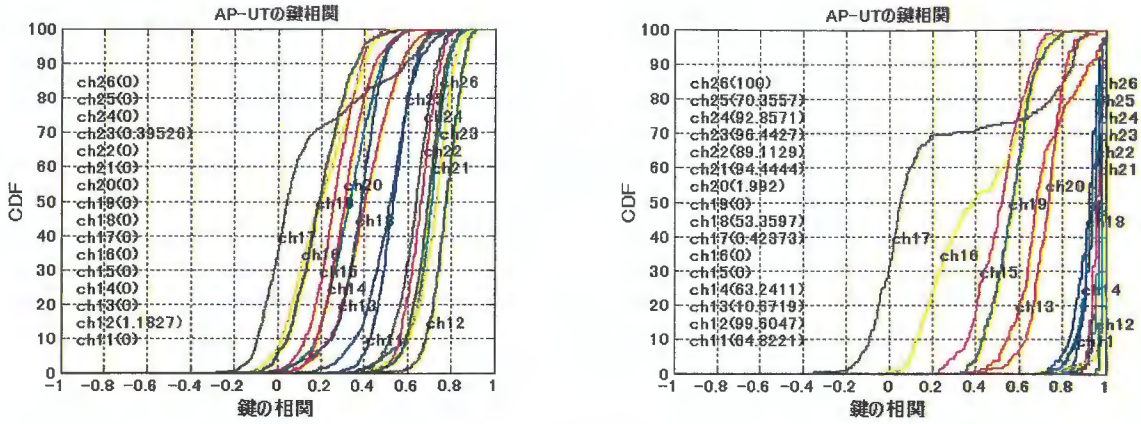
Monobit 検定	
採択域	
9725 - 10275	10047

Runs 検定		
採択域	ビット'0'	ビット'1'
2315 - 2685	2543	2521
1114 - 1386	1280	1277
527 - 723	612	613
240 - 384	297	330
103 - 209	155	143
103 - 209	147	151

longRuns 検定	
<26	19

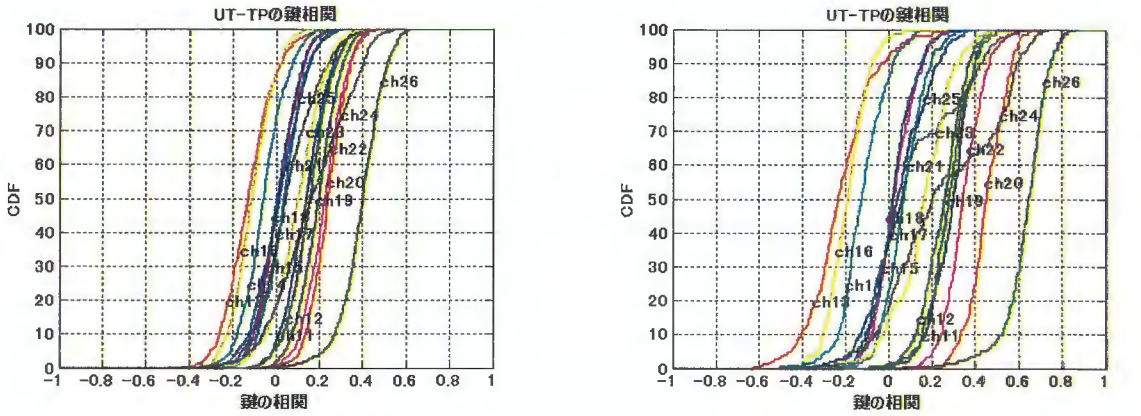
訂正ビット数	鍵一致率
0	5.5172
1	41.3793
2	76.8966
3	94.4828

E3：AP 天井付近に配置　2005 / 02 / 07 測定
データ数 750



(a) データ削除なし　　(b) データ削除あり

図 E3-1　正規局間の鍵相関



(a) データ削除なし　　(b) データ削除あり

図 E3-2　正規局と盗聴局間の鍵相関

表 E3-1　データ削除ありなしでの鍵一致率（2bit/32bit 誤り訂正）

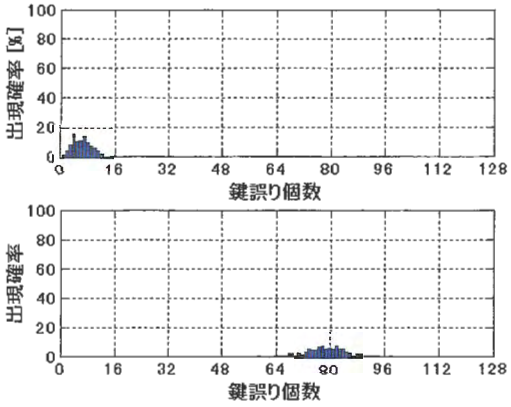
	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
なし	0	1.18	0	0	0	0	0	0	0	0	0	0	0.40	0	0	0
あり	64.8	99.6	10.7	63.2	0	0	0.42	53.4	0	1.99	94.4	89.1	96.4	92.9	70.4	100

表 E3-2 乱数検定結果

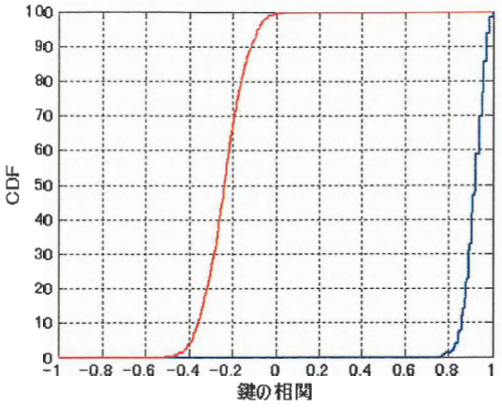
P	OK	OK	—	OK	—	—	—	—	—	—	OK	OK	NG	NG	NG	OK
R	OK	OK	—	OK	—	—	—	—	—	—	OK	OK	NG	NG	NG	NG

表 E3-3　親局・子局での平均 RSSI 及び RSSI 差

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
親	-12	-9.8	-11	-13	-11	-11	-10	-12	-12	-11	-6.9	-4.7	-3.2	-12	-5.2	-8.2
子	-13	-9.1	-8.9	-9.8	-6.7	-5.3	-3.1	-6	-6.8	-5.2	-0.6	-0.1	-0.4	-11	-5.3	-9.3
差	0.49	-0.8	-2	-2.8	-4.5	-5.5	-7.2	-5.9	-5.4	-5.5	-6.2	-4.7	-2.8	-1.2	0.13	1.07



(a) 誤り個数分布（上:正規局間　下:盗聴局）



(b) 鍵の相関（青:正規局　赤:盗聴局）

図 E3-3　周波数切り換え生成結果（全周波数使用）

表 E3-4　各種検定結果及び鍵一致率

Poker 検定	
採択域	
2.16 - 46.17	30.5536

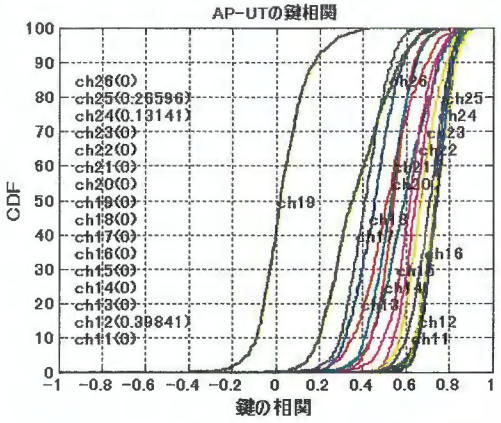
Monobit 検定	
採択域	
9725 - 10275	10059

Runs 検定		
採択域	ビット'0'	ビット'1'
2315 - 2685	2518	2514
1114 - 1386	1330	1270
527 - 723	596	623
240 - 384	288	303
103 - 209	141	157
103 - 209	151	157

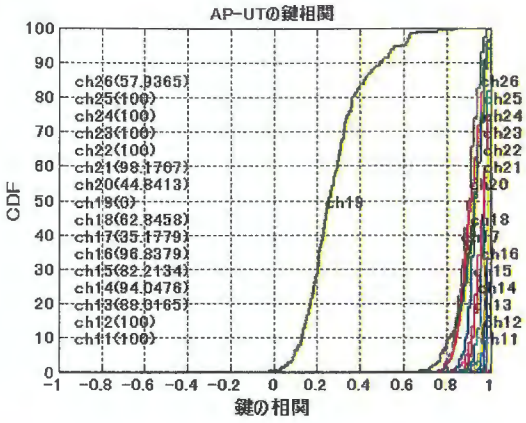
longRuns 検定	
<26	36

訂正ビット数	鍵一致率
0	1.6
1	20.8
2	54.6
3	79.6

E4：AP 天井付近に配置(アンテナを上下逆向きに配置)　2005 / 02 / 08 測定
データ数 750

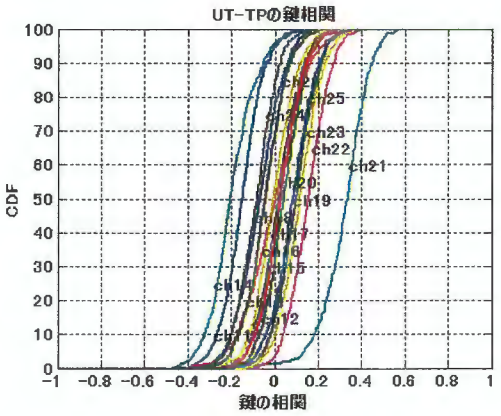


(a) データ削除なし

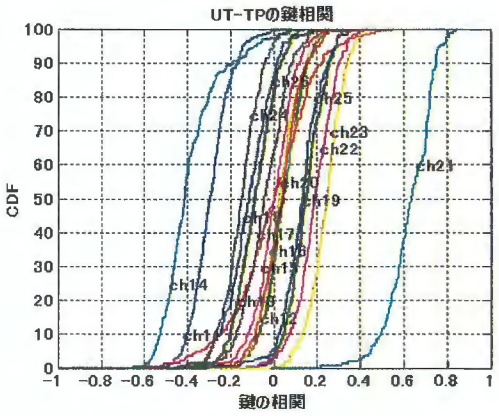


(b) データ削除あり

図 E4-1　正規局間の鍵相関



(a) データ削除なし



(b) データ削除あり

図 E4-2　正規局と盗聴局間の鍵相関

表 E4-1　データ削除ありなしでの鍵一致率（2bit/32bit 誤り訂正）

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
なし	0	0.40	0	0	0	0	0	0	0	0	0	0	0	0.13	0.27	0
あり	100	100	88.0	94.0	82.2	96.8	35.2	62.8	0	44.8	98.2	100	100	100	100	57.9

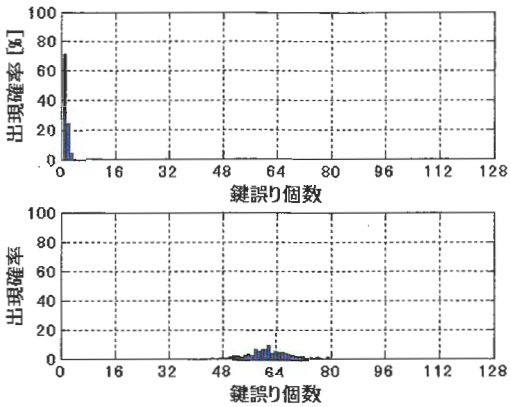
表 E4-2　乱数検定結果

P	OK	OK	NG	NG	NG	OK	—	OK	—	—	OK	OK	OK	OK	OK	—
R	OK	OK	NG	NG	NG	OK	—	OK	—	—	OK	OK	OK	OK	OK	—

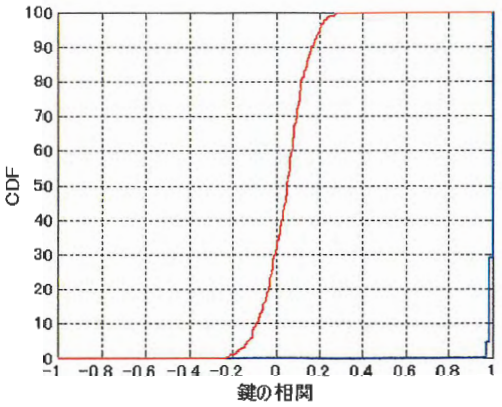
P：Poker 検定　　R：Runs 検定

表 E4-3　親局・子局での平均 RSSI 及び RSSI 差

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
親	-10	-7.3	-13	-16	-11	-6.8	-11	-16	-13	-8.4	-8.3	-7.5	-6.7	-6.5	-8.7	-9.7
子	-11	-6.4	-12	-14	-6.9	-1.4	-7.1	-13	-10	-2.8	-4	-4.2	-4.8	-5.6	-9	-10
差	0.25	-0.9	-1.8	-2.5	-3.8	-5.4	-4.3	-3.8	-2.7	-5.6	-4.3	-3.2	-1.9	-0.9	0.22	0.75



(a) 誤り個数分布（上:正規局間　下:盗聴局）



(b) 鍵の相関（青:正規局　赤:盗聴局）

図 E4-3　周波数切り換え生成結果（全周波数使用）

表 E4-4　各種検定結果及び鍵一致率

Poker 検定	
採択域	
2.16 - 46.17	25.056

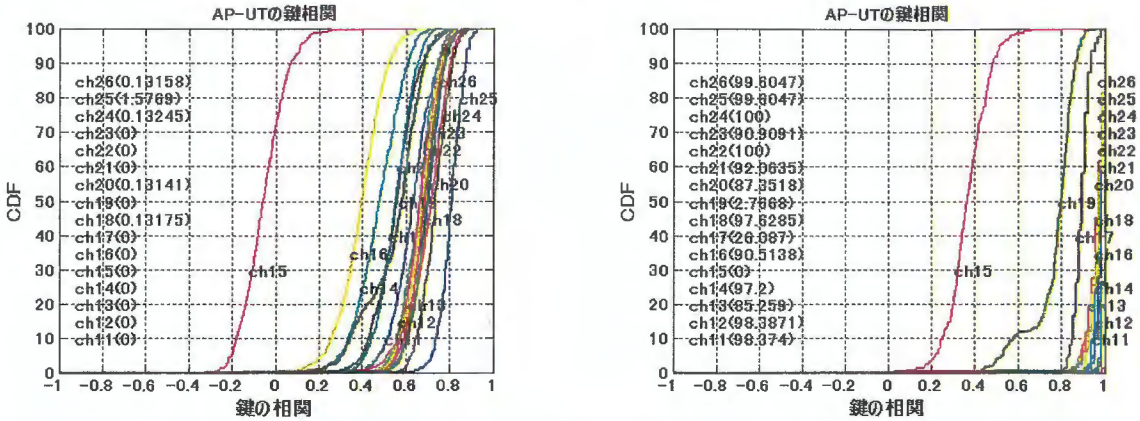
Monobit 検定	
採択域	
9725 - 10275	9957

Runs 検定		
採択域	ビット'0'	ビット'1'
2315 - 2685	2470	2522
1114 - 1386	1258	1215
527 - 723	624	641
240 - 384	339	303
103 - 209	145	154
103 - 209	156	158

longRuns 検定	
<26	16

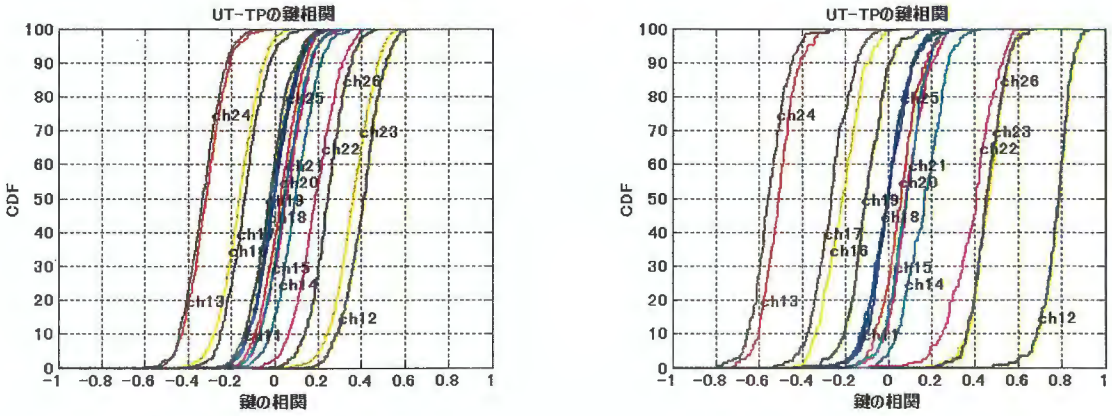
訂正ビット数	鍵一致率
0	70.8889
1	99.1111
2	99.7778
3	100

E5：AP 天井付近に配置 その 2(前回と同じ位置) 2005 / 02 / 09 測定
データ数 750



(a) データ削除なし　　(b) データ削除あり

図 E5-1　正規局間の鍵相関



(a) データ削除なし　　(b) データ削除あり

図 E5-2　正規局と盗聴局間の鍵相関

表 E5-1　データ削除ありなしでの鍵一致率（2bit/32bit 誤り訂正）

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
non	0	0	0	0	0	0	0	0.13	0	0.13	0	0	0	0.13	1.58	0.13
del	98.4	98.4	85.3	97.2	0	90.5	26.1	97.6	2.77	87.4	92.1	100	90.9	100	99.6	99.6

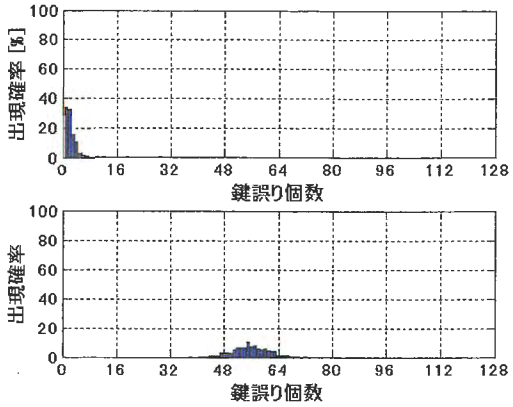
表 E5-2 乱数検定結果

P	OK	OK	OK	OK	—	OK	—	OK	—	OK	OK	OK	OK	OK	OK	OK
R	OK	OK	OK	OK	—	OK	—	OK	—	OK	OK	OK	OK	OK	OK	OK

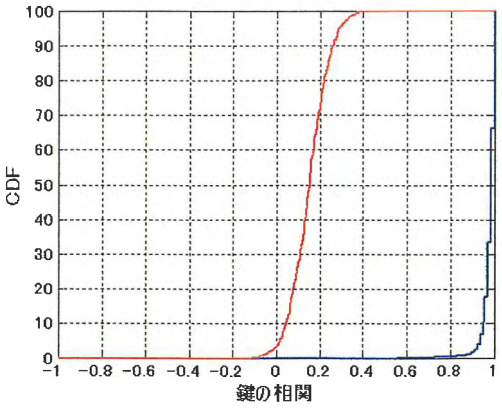
P：Poker 検定　　R：Runs 検定

表 E5-3　親局・子局での平均 RSSI 及び RSSI 差

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
親	-14	-12	-11	-13	-11	-12	-11	-8.2	-8.8	-8.9	-16	-8.3	-10	-10	-8.5	-4.3
子	-14	-11	-8.4	-9.8	-8.7	-6.6	-4.3	-0.3	-1.4	-2.3	-12	-4	-7.7	-8.7	-8.9	-6
差	0.49	-0.9	-2.3	-3	-2.7	-5.1	-6.5	-7.9	-7.4	-6.7	-4	-4.3	-2.2	-1.3	0.35	1.71



(a) 誤り個数分布（上:正規局間 下:盗聴局）



(b) 鍵の相関（青:正規局 赤:盗聴局）

図 E5-3 周波数切り換え生成結果（全周波数使用）

表 E5-4 各種検定結果及び鍵一致率

Poker 検定	
採択域	
2.16 - 46.17	25.0432

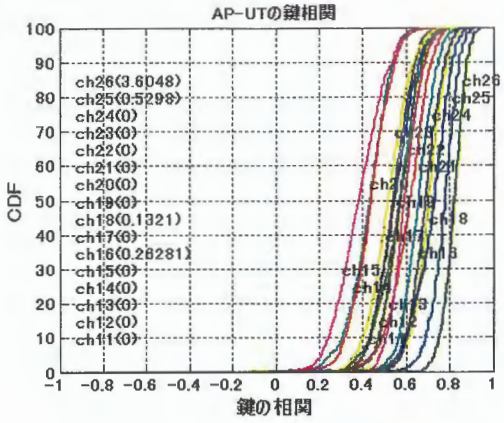
Monobit 検定	
採択域	
9725 - 10275	10047

Runs 検定		
採択域	ビット'0'	ビット'1'
2315 - 2685	2566	2489
1114 - 1386	1215	1293
527 - 723	573	619
240 - 384	326	277
103 - 209	154	157
103 - 209	172	170

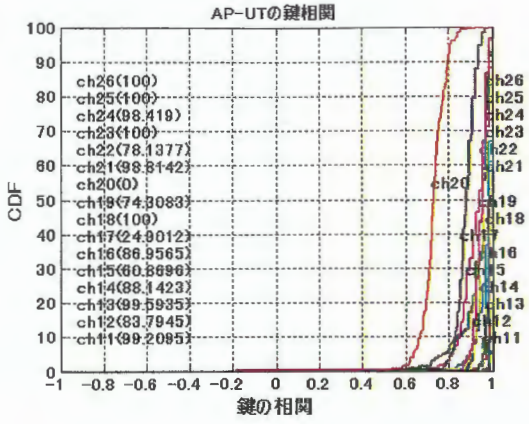
longRuns 検定	
<26	14

訂正ビット数	鍵一致率
0	98.4
1	99.8
2	99.8
3	99.8

E6：AP 天井付近に配置 その 2（アンテナを上下逆向きに配置）（前回と同じ位置） 2005 / 02 / 09 測定
データ数 750

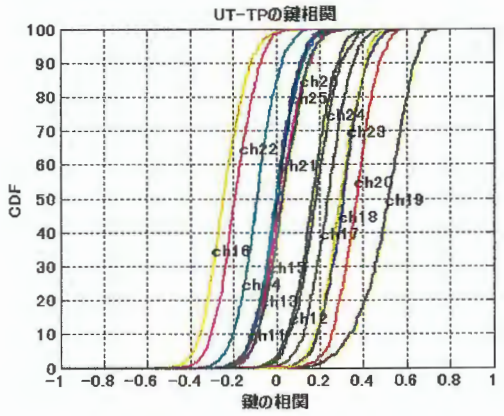


(a) データ削除なし

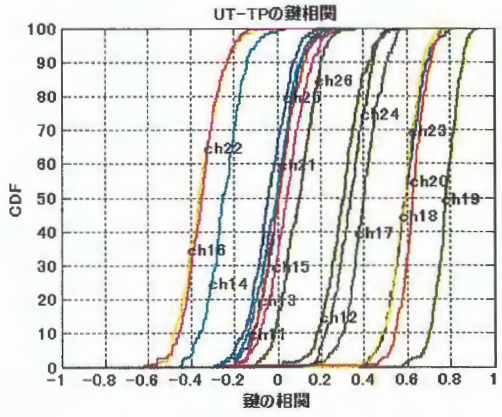


(b) データ削除あり

図 E6-1 正規局間の鍵相関



(a) データ削除なし



(b) データ削除あり

図 E6-2 正規局と盗聴局間の鍵相関

表 E6-1 データ削除ありなしでの鍵一致率（2bit/32bit 誤り訂正）

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
non	0	0	0	0	0	0.26	0	0.13	0	0	0	0	0	0	0.53	3.60
del	99.2	83.8	99.6	88.1	60.9	87.0	24.9	100	74.3	0	98.8	78.1	100	98.4	100	100

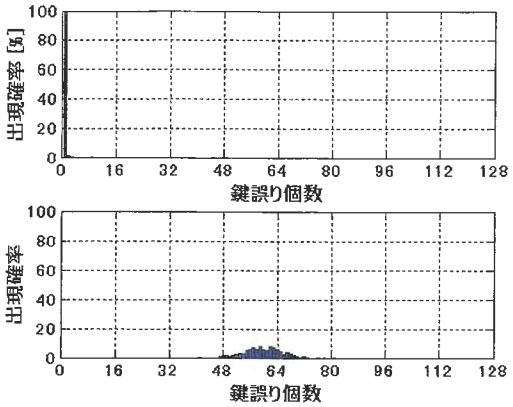
表 E6-2 乱数検定結果

P	OK	OK	OK	OK	—	OK	—	OK	OK	—	OK	OK	OK	OK	OK	OK
R	OK	OK	OK	OK	—	OK	—	OK	OK	—	OK	OK	OK	OK	OK	OK

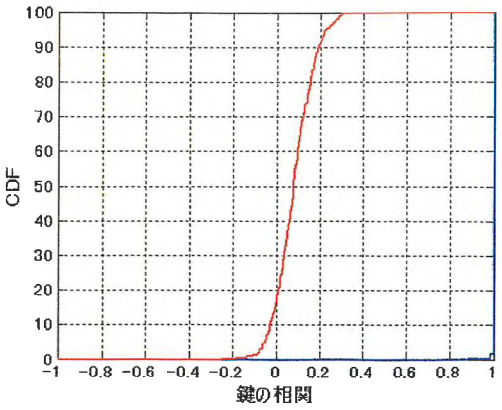
P：Poker 検定　　R：Runs 検定

表 E6-3 親局・子局での平均 RSSI 及び RSSI 差

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
親	-4.1	-14	-12	-13	-14	-19	-10	-5	-5.3	-11	-5.8	-4.3	-5.1	-12	-7.2	-0
子	-4.7	-13	-9.9	-11	-11	-15	-5.1	0.6	0.5	-6.7	-1.3	-0.9	-3.2	-11	-7.8	-1.9
差	0.55	-0.6	-1.9	-2.2	-3	-4.1	-5.1	-5.7	-5.8	-4.3	-4.4	-3.4	-1.9	-0.8	0.57	1.94



(a) 誤り個数分布（上:正規局間　下:盗聴局）



(b) 鍵の相関（青:正規局　赤:盗聴局）

図 E6-3　周波数切り換え生成結果（全周波数使用）

表 E6-4　各種検定結果及び鍵一致率

Poker 検定	
採択域	
2.16 - 46.17	7.9424

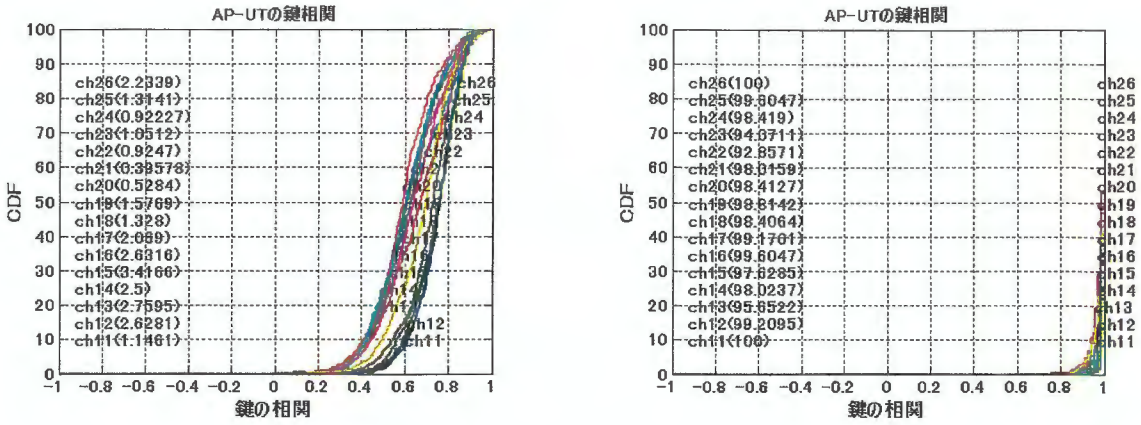
Monobit 検定	
採択域	
9725 - 10275	10001

Runs 検定		
採択域	ビット'0'	ビット'1'
2315 - 2685	2534	2499
1114 - 1386	1236	1249
527 - 723	621	655
240 - 384	329	322
103 - 209	126	125
103 - 209	164	161

longRuns 検定	
<26	16

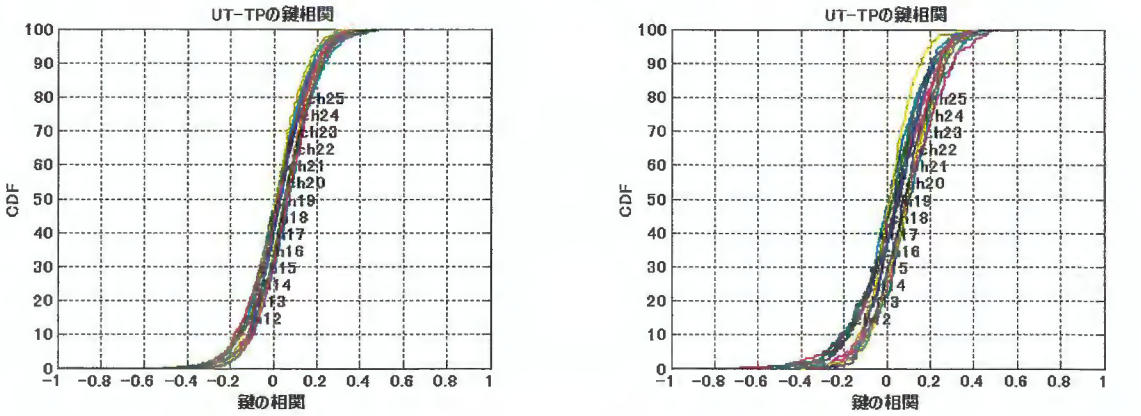
訂正ビット数	鍵一致率
0	99.8
1	99.8
2	99.8
3	100

E7：実験室内にて歩行速度程度で UT 移動　2005 / 02 / 10 測定



(a) データ削除なし　　(b) データ削除あり

図 E7-1　正規局間の鍵相関



(a) データ削除なし　　(b) データ削除あり

図 E7-2　正規局と盗聴局間の鍵相関

表 E7-1　データ削除ありなしでの鍵一致率（2bit/32bit 誤り訂正）

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
non	1.15	2.63	2.76	2.5	3.42	2.63	2.07	1.33	1.58	0.53	0.40	0.92	1.05	0.92	1.31	1.23
del	100	99.2	95.7	98.0	97.6	99.6	99.2	98.4	98.8	98.4	98.0	92.9	94.1	98.4	99.6	100

表 E7-2　乱数検定結果

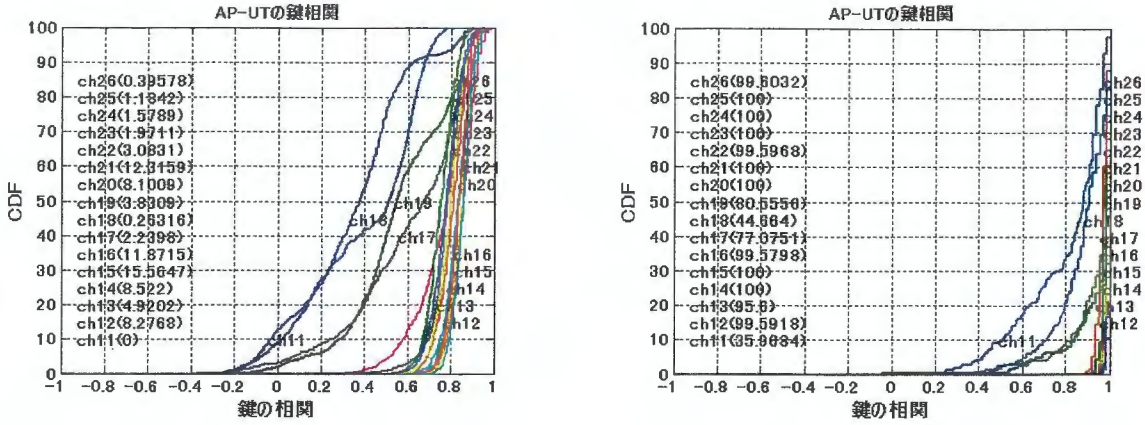
P	NG	NG	NG	NG	NG	NG	NG	NG	NG	NG	NG	NG	NG	NG	NG	NG
R	NG	NG	NG	NG	NG	NG	NG	NG	NG	NG	NG	NG	NG	NG	NG	NG

P：Poker 検定　　R：Runs 検定

表 E7-3　親局・子局での平均 RSSI 及び RSSI 差

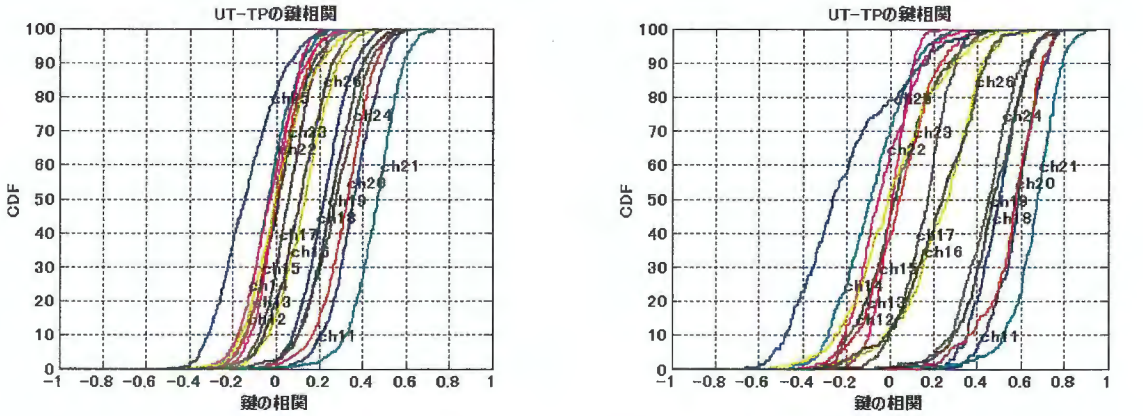
	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
親	-7.2	-8.3	-10	-11	-11	-12	-13	-13	-13	-13	-11	-10	-9.4	-8.4	-7.3	-6.8
子	-7.6	-7.5	-7.9	-7.3	-6.6	-7	-7.1	-6.8	-7.3	-7.3	-6.5	-6.5	-7	-7.3	-7.7	-8.3
差	0.43	-0.8	-2.3	-3.5	-4.6	-5.2	-5.6	-5.7	-5.6	-5.3	-4.7	-3.6	-2.3	-1.2	0.39	1.4

E8：居室(AP：青野さん横 UT：平田さん横)　2005 / 02 / 14 測定



(a) データ削除なし　　(b) データ削除あり

図 E8-1　正規局間の鍵相関



(a) データ削除なし　　(b) データ削除あり

図 E8-2　正規局と盗聴局間の鍵相関

表 E8-1　データ削除ありなしでの鍵一致率（2bit/32bit 誤り訂正）

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
non	0	8.28	4.92	8.52	15.6	11.9	2.24	0.26	3.83	8.10	12.3	3.08	1.97	1.58	1.18	0.40
del	36.0	99.6	95.6	100	100	99.6	77.1	44.7	80.6	100	100	99.6	100	100	100	99.6

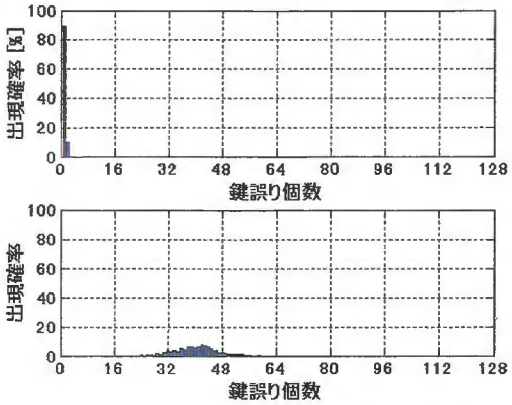
表 E8-2　乱数検定結果

P	—	NG	OK	OK	OK	OK	OK	—	OK	OK	OK	OK	OK	OK	OK	NG
R	—	NG	OK	OK	OK	OK	OK	—	OK	OK	OK	OK	OK	OK	OK	NG

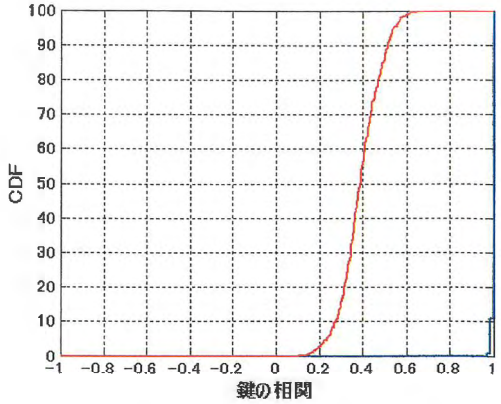
P：Poker 検定　　R：Runs 検定

表 E8-3　親局・子局での平均 RSSI 及び RSSI 差

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
親	-12	-23	-28	-25	-26	-28	-20	-19	-20	-25	-22	-19	-22	-17	-18	-21
子	-13	-23	-25	-22	-21	-22	-14	-13	-14	-19	-17	-15	-20	-16	-19	-23
差	0.68	-0.6	-2.2	-3.5	-4.7	-5.6	-5.9	-6.1	-6	-5.6	-4.8	-3.5	-2.2	-0.6	0.65	1.72



(a) 誤り個数分布（上:正規局間 下:盗聴局）



(b) 鍵の相関（青:正規局 赤:盗聴局）

図 E8-3　周波数切り換え生成結果（全周波数使用）

表 E8-4　各種検定結果及び鍵一致率

Poker 検定	
採択域	
2.16 - 46.17	26.2208

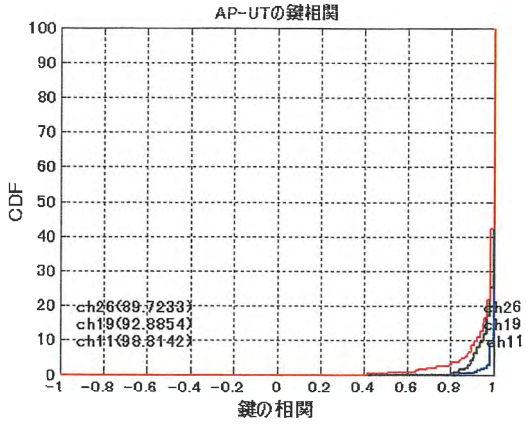
Monobit 検定	
採択域	
9725 - 10275	10032

Runs 検定		
採択域	ビット'0'	ビット'1'
2315 - 2685	2434	2437
1114 - 1386	1234	1269
527 - 723	685	635
240 - 384	315	316
103 - 209	163	149
103 - 209	133	158

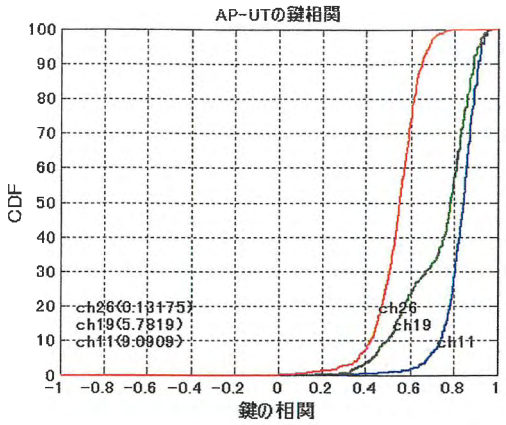
longRuns 検定	
<26	13

訂正ビット数	鍵一致率
0	89.1111
1	99.7778
2	100
3	100

E9：1F 食堂前　2005 / 02 / 16 測定

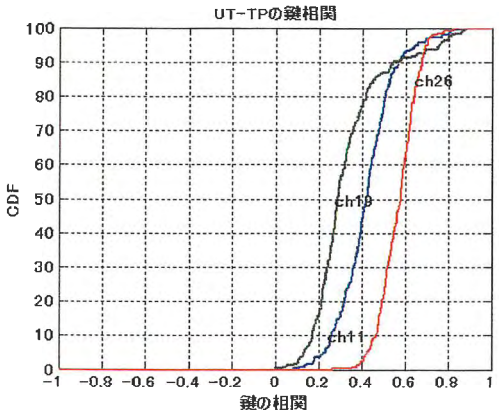


(a) データ削除なし

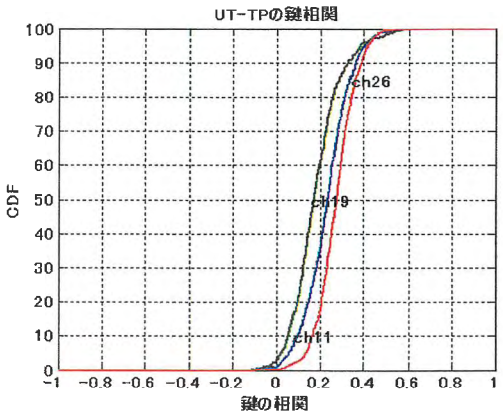


(b) データ削除あり

図 E9-1　正規局間の鍵相関



(a) データ削除なし



(b) データ削除あり

図 E9-2　正規局と盗聴局間の鍵相関

表 E9-1　データ削除ありなしでの鍵一致率（2bit/32bit 誤り訂正）

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	ch26
non	9.09	—	—	—	—	—	—	—	5.78	—	—	—	—	—	—	0.13
del	98.8	—	—	—	—	—	—	—	92.9	—	—	—	—	—	—	89.7

表 E9-2　乱数検定結果

P	NG	—	—	—	—	—	—	—	NG	—	—	—	—	—	—	OK
R	NG	—	—	—	—	—	—	—	NG	—	—	—	—	—	—	OK

P：Poker 検定　　R：Runs 検定

表 E9-3　親局・子局での平均 RSSI 及び RSSI 差

	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19	ch20	ch21	ch22	ch23	ch24	ch25	Ch26
親	-15	—	—	—	—	—	—	—	-21	—	—	—	—	—	—	-9.4
子	-15	—	—	—	—	—	—	—	-14	—	—	—	—	—	—	-10
差	0.59	—	—	—	—	—	—	—	-6.3	—	—	—	—	—	—	0.94

結果の項目
E1：実験室内でch23の相関が高くなる位置に設置　2005 / 01 / 25 測定
E2：実験室内でch26の相関が高くなる位置に設置　2005 / 02 / 01 測定
E3：AP天井付近に配置　2005 / 02 / 07 測定
E4：AP天井付近に配置(アンテナを上下逆向きに配置)　2005 / 02 / 08 測定
E5：AP天井付近に配置 その2(前回と同じ位置)　2005 / 02 / 09 測定
E6：AP天井付近に配置 その2(アンテナを上下逆向きに配置)(前回と同じ位置)　2005 / 02 / 09 測定
E7：実験室内にて歩行速度程度でUT移動　2005 / 02 / 10 測定
E8：居室(AP：青野さん横 UT：平田さん横)　2005 / 02 / 14 測定
E9：１Ｆ食堂前　2005 / 02 / 16 測定

表E-1　各実験場所における親局での平均RSSI
表E-2　各実験場所における子局での平均RSSI
表E-3　各実験場所における親局・子局のRSSIレベル差

図E-1　各実験場所における親局での平均RSSI
図E-2　各実験場所における子局での平均RSSI
図E-3　各実験場所における親局・子局のRSSIレベル差

表 E-1　各実験場所における親局での平均 RSSI

	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
E1		-11	-9.1	-11	-11	-15	-11	-11	-15	-9.7	-11	-4.2	-1.7	-0.1	-1.2	
E2	-11	-10	-13	-11	-9.1	-13	-11	-7.4	-12	-11	-15	-8.1	-8.7	-12	-9.4	-6.8
E3	-12	-9.8	-11	-13	-11	-11	-10	-12	-12	-11	-6.9	-4.7	-3.2	-12	-5.2	-8.2
E4	-10	-7.3	-13	-16	-11	-6.8	-11	-16	-13	-8.4	-8.3	-7.5	-6.7	-6.5	-8.7	-9.7
E5	-14	-12	-11	-13	-11	-12	-11	-8.2	-8.8	-8.9	-16	-8.3	-10	-10	-8.5	-4.3
E6	-4.1	-14	-12	-13	-14	-19	-10	-5	-5.3	-11	-5.8	-4.3	-5.1	-12	-7.2	-0
E7	-7.2	-8.3	-10	-11	-11	-12	-13	-13	-13	-13	-11	-10	-9.4	-8.4	-7.3	-6.8
E8	-12	-23	-28	-25	-26	-28	-20	-19	-20	-25	-22	-19	-22	-17	-18	-21
E9	-15								-21							-9.4

表 E-2　各実験場所における子局での平均 RSSI

	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
E1		-10	-7.7	-8.8	-8.2	-12	-6.9	-7	-12	-5.5	-7.7	-2.6	-1.3	-1.1	-3.7	
E2	-11	-9.5	-12	-8.1	-5.3	-9.8	-6.6	-2.1	-8	-8.1	-13	-6.1	-8.1	-12	-11	-10
E3	-13	-9.1	-8.9	-9.8	-6.7	-5.3	-3.1	-6	-6.8	-5.2	-0.6	-0.1	-0.4	-11	-5.3	-9.3
E4	-11	-6.4	-12	-14	-6.9	-1.4	-7.1	-13	-10	-2.8	-4	-4.2	-4.8	-5.6	-9	-10
E5	-14	-11	-8.4	-9.8	-8.7	-6.6	-4.3	-0.3	-1.4	-2.3	-12	-4	-7.7	-8.7	-8.9	-6
E6	-4.7	-13	-9.9	-11	-11	-15	-5.1	0.6	0.5	-6.7	-1.3	-0.9	-3.2	-11	-7.8	-1.9
E7	-7.6	-7.5	-7.9	-7.3	-6.6	-7	-7.1	-6.8	-7.3	-7.3	-6.5	-6.5	-7	-7.3	-7.7	-8.3
E8	-13	-23	-25	-22	-21	-22	-14	-13	-14	-19	-17	-15	-20	-16	-19	-23
E9	-15								-14							-10

表 E-3　各実験場所における親局・子局の RSSI レベル差

	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
E1		-0.5	-1.4	-2.5	-3.3	-3.1	-4.2	-4.2	-3.6	-4.2	-2.9	-1.6	-0.4	0.95	2.51	
E2	0.09	-0.5	-1.4	-2.5	-3.8	-3.5	-4.6	-5.2	-3.5	-3.1	-1.8	-2	-0.6	0.68	1.83	3.28
E3	0.49	-0.8	-2	-2.8	-4.5	-5.5	-7.2	-5.9	-5.4	-5.5	-6.2	-4.7	-2.8	-1.2	0.13	1.07
E4	0.25	-0.9	-1.8	-2.5	-3.8	-5.4	-4.3	-3.8	-2.7	-5.6	-4.3	-3.2	-1.9	-0.9	0.22	0.75
E5	0.49	-0.9	-2.3	-3	-2.7	-5.1	-6.5	-7.9	-7.4	-6.7	-4	-4.3	-2.2	-1.3	0.35	1.71
E6	0.55	-0.6	-1.9	-2.2	-3	-4.1	-5.1	-5.7	-5.8	-4.3	-4.4	-3.4	-1.9	-0.8	0.57	1.94
E7	0.43	-0.8	-2.3	-3.5	-4.6	-5.2	-5.6	-5.7	-5.6	-5.3	-4.7	-3.6	-2.3	-1.2	0.39	1.4
E8	0.68	-0.6	-2.2	-3.5	-4.7	-5.6	-5.9	-6.1	-6	-5.6	-4.8	-3.5	-2.2	-0.6	0.65	1.72
E9	0.59								-6.3							0.94

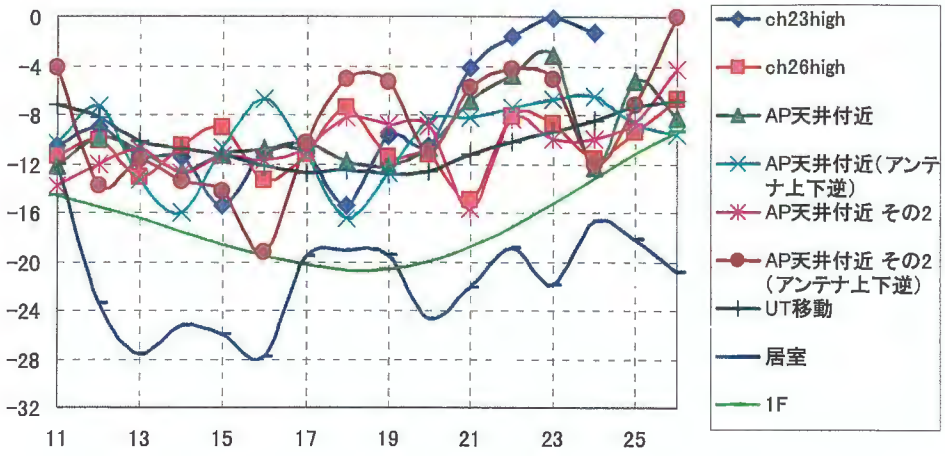


図 E-1　各実験場所における親局の平均 RSSI レベル

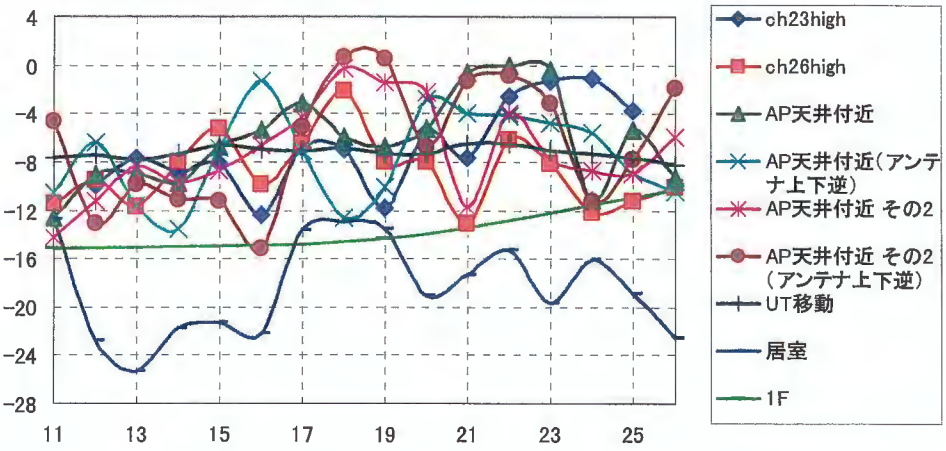


図 E-2　各実験場所における子局の平均 RSSI レベル

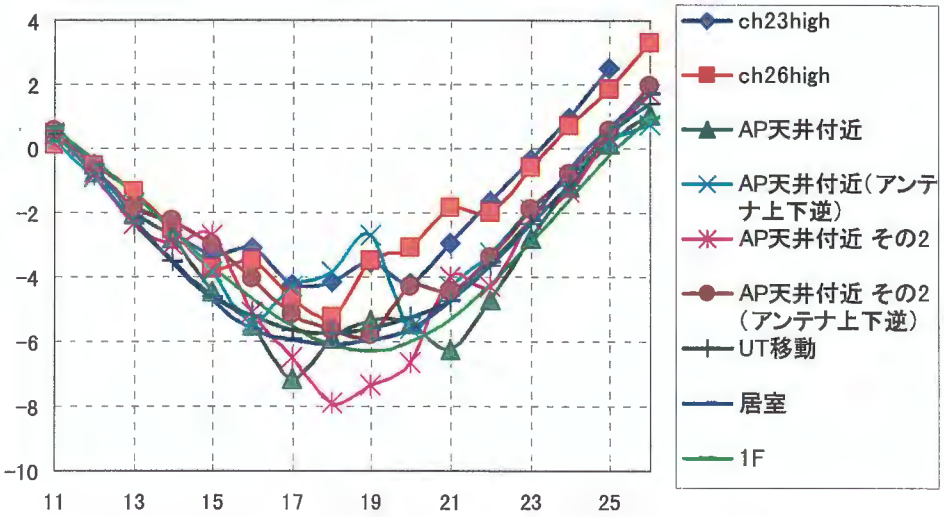


図 E-3　各実験場所における親局・子局の RSSI レベル差

・ZigBee-ESPARSKey仕様案

生成鍵bit数	128bit
鍵生成時間	1秒程度
鍵一致率(全試行回数中)	90%以上
鍵の乱数性	FIPS PUB140-2 の乱数検定にパスすること

RSSI母集団	384

鍵の不一致が起こりやすい閾値付近のデータを削除するため
生成鍵bit数より多くのRSSIを取得する
RSSIの送受一回につき約2ms
鍵生成のためのRSSIの母集団を128の倍数とすると
鍵生成時間が1秒程度なので、母集団は384以内が望ましい
鍵の一致率を考えて、その中でも最大の384を採用

インターリーブ	2回

乱数性の向上のために行う
周囲の環境に変化が無ければインターリーブなしでもOKの場合もあり
子局が移動する等、環境変化が多いときに鍵が偏り乱数検定をパスしない
子局の移動が歩行速度程度のときインターリーブを3回行うと乱数検定をパス
また，2回でもデータ削除をかませれば(フローチャート参照)乱数性は高くなる

付加効果	インターリーブ間隔

前回の鍵の一部をインターリーブ間隔に設定する(別シート参照)ことで
盗聴局にて前回の鍵が盗聴できていなければこの間隔はわからなくなり
盗聴局での取得データにからの鍵の推測がより困難になる
またインターリーブ間隔には毎回違う値を用いる方が乱数性が増す

データ削除個数(親局)	128
データ削除個数(子局)	128

親局・子局の双方で鍵の誤りになりやすい閾値付近のデータを削除する
削除位置情報はデータにより送信するため盗聴局でも取得可能
しかし情報データを暗号化していれば削除位置はわからないため
盗聴局での鍵の推測は困難になる
インターリーブ後にデータ削除を行うことで乱数性が増す
また子局側での削除位置の調整で鍵の0,1の個数を調節できる

誤り訂正	2/32bit

128bit全体について誤り訂正を行うと、検査行列・シンドロームが大
現実的なデータ量を考え32bitブロック毎に訂正を行う
訂正数が少ない(0 or 1bit)と鍵一致率が満たない可能性あり
シンドロームの長さ分，鍵の実効長が減ってしまう可能性があるため
取得RSSI数や削除数を調整し，冗長ビットを除去する必要がある(検討課題)

盗聴対策	周波数切換

周波数チャネルにより鍵の相関が異なる
相関の高いチャネルを使用すると鍵が盗られる心配がある
相関の高いチャネルもあれば低いチャネルもあるので
複数のチャネルを使用して鍵を生成すれば極端に高い相関はなくなる

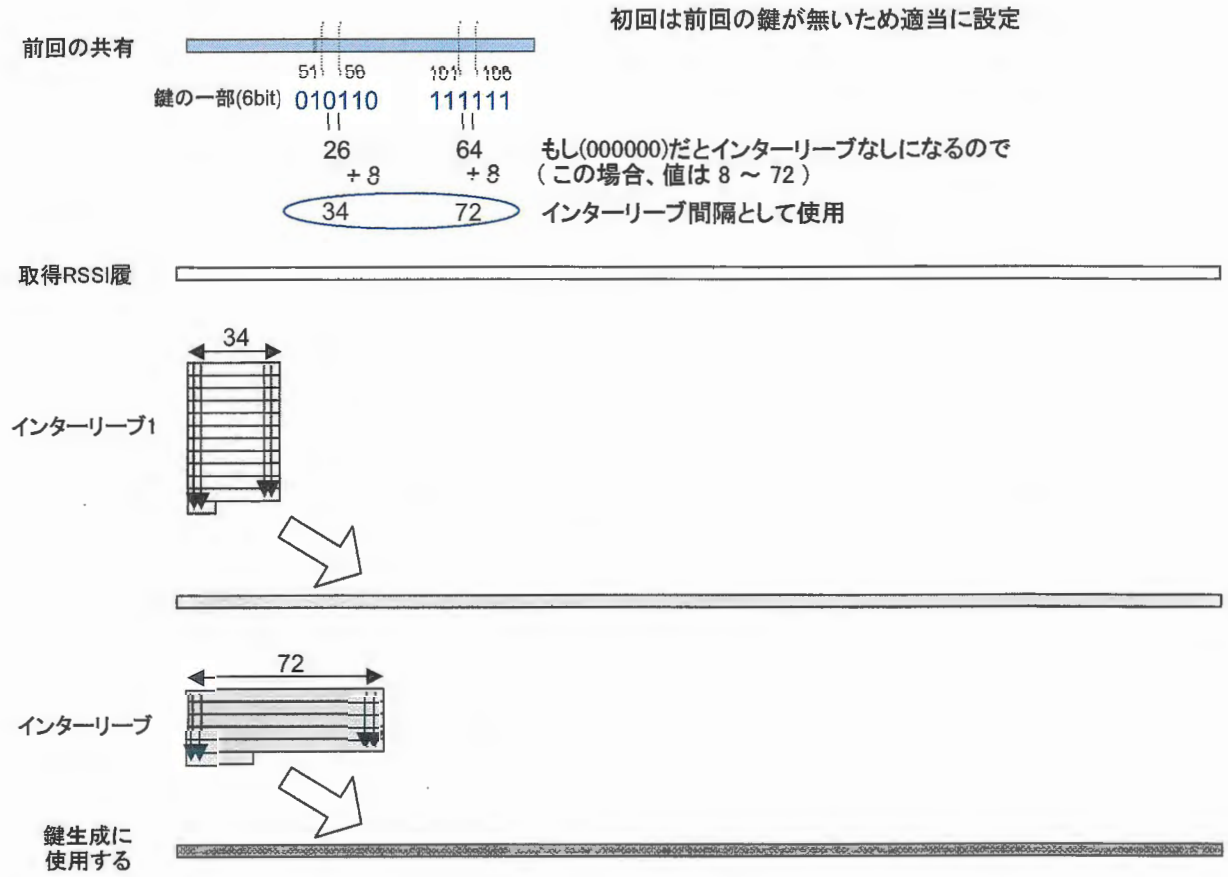
周波数切換方法	RSSI 24個毎

周波数は11ch～26chまでの16チャネルある
384個のRSSIをすべてのチャネルを使用して取得すると
1つのチャネルで取得するデータ数は24個

局所的に一致率の低くなるチャネルがあるため
そういったチャネル以外の8チャネル選び
48個ずつデータを取得するという方法も考えられる
局所的に一致率の低くなるチャネルの選定が困難(検討課題)

インターリーブについて

ランダムなインターリーブを2回することで鍵の偏りが減少
ランダムな値として前回に共有した鍵の一部が使用できる
盗聴局において前回の鍵を取得できていなければインターリーブ間隔がわからない
そのため、より盗聴での鍵の推測が困難になる



削除処理手順

閾値付近のデータを削除(位置はランダム)
不一致になりやすいデータを削除することで一致率を確保
削除位置はランダムなので乱数性が向上する
削除位置情報を送信するが暗号化等により盗聴局において
削除位置がわからなければ盗聴での鍵の推測が困難になる