A Study on Error Correction in Secret Key Agreement Scheme Using ESPAR Antenna

Takayuki SHIMIZU*, Kenya HORAI*, Hisato IWAI* and Hideichi SASAOKA*

(Received July 12, 2007)

As a countermeasure scheme against eavesdroppers on wireless communication, the secret key agreement system has been proposed using an ESPAR (Electronically Steerable Parasitic Array Radiator) antenna, and using the propagation reciprocity between two users. However, this system requires an error correction process to avoid a key disagreement between regular users. This paper proposes an algorithm based on table-aided soft-decision decoding for the error correction. Simulation results conducted for an indoor IEEE802.15.4/ZigBee™ environment show that nearly 100 % successful key generation can be achieved by using the proposed key disagreement correction scheme. Moreover, compared with the conventional key disagreement correction scheme, the proposed scheme makes it possible to reduce the key correlation between regular users and eavesdroppers.

Key words : ESPAR antenna, key agreement, soft-decision decoding, table-aided decoding, radio propagation

キーワード : エスパアンテナ，鍵共有，軟判定復号法，テーブル参照復号法，電波伝搬

エスパアンテナを用いた秘密鍵共有における鍵不一致訂正方式の検討

清水　崇之，宝来　剣文，岩井　誠人，笹岡　秀一

1. まえがき

近年，個人・企業間で無線 LAN が爆発的に普及し，さらにホットスポットなどの公衆無線 LAN の利用が急増している．しかし，無線 LAN は電波を利用しているため，通信の傍受が容易に行える．そのため，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，盗聴対策として，暗号化技術がよく用いられている．無線通信において大量データの暗号化には，処理が高速な秘密鍵暗号方式が用いられる．しかし，この方式には，鍵管理と鍵配送という 2 つの問題点がある [1, 2]．これらの問題を解決するために，電波伝搬の相反性とフェージングによる不規則変動を利用した秘密鍵共有方式が研究されている [3-7]．この方式は，伝搬路状況に応じて使い捨て可能な鍵を生成・利用することができるため，鍵配送のみならず鍵管理の問題をも克服可能である．更に，伝搬路特性の変動の少ない環境においても秘匿性の高い鍵を生成する方式として，可変指向性アンテナであるエスパ（ESPAR : Electronically Steerable Parasitic Array Radiator）アンテナ [8, 9]を用いた秘密鍵共有方式が研究されている [10, 11]．

* Department of Electronics, Doshisha University, Kyotanabe, Kyoto, 610-0321, Japan
Telephone: +81-774-65-6355, Fax: +81-774-65-6801, E-mail: iwai@mail.doshisha.ac.jp

この方式では，雑音の影響によって正規局間で生成した鍵に数ビットの不一致が生じるため，鍵生成過程において，符号理論の技術を応用した鍵不一致訂正処理が施されている[3, 4, 10]．簡単なものとして，鍵候補を符号語に変換する方法[3, 4]が提案されているが，特性があまり良好でなく，適用可能な符号が限定される問題がある[12]．そこで，正規局の鍵候補のシンドローム差から鍵不一致訂正を行う手法がよく用いられている[10]．このシンドローム差を用いた鍵不一致訂正処理では，硬判定復号法である代数的復号法が用いられている．さらに，鍵の不一致が生じやすいデータの削除という手法[10]を併用することにより，鍵一致率の向上を図っている．しかし，データ削除の手法では正規局間で削除位置情報を送信し合う必要があり，削除位置情報を盗聴局に与えるので，適用可能な方式が限定される[10]．鍵不一致訂正処理では，鍵一致率と盗聴の困難さの両特性が重要であり，盗聴局との鍵相関を上げることなく鍵の不一致を訂正する必要がある．データの削除なしで高い鍵一致率を実現するためには軟判定復号法による鍵不一致訂正技術の適用が有効だと考えられる．

本稿では，鍵不一致訂正処理としてテーブル参照軟判定復号法[13, 14]を適用する．その際，誤り訂正における軟判定復号のように既知の情報を送る場合と異なり，観測データから生成した鍵の不一致訂正では距離比較の基準となる値を定めることが難しい．そこで，誤り訂正における軟判定復号で用いる受信系列と候補符号語とのユークリッド距離に代わるものとして，受信信号強度（RSSI：Received Signal Strength Indicator）の誤りビット位置の値と閾値までの距離を用いる．それらを用いて，鍵一致率特性及び盗聴局との鍵相関特性をシミュレーションにより求め，従来方式と比較して，想定した屋内環境で盗聴局との鍵相関を上げることなく鍵一致率特性を改善できることを示す．

2. エスパアンテナを用いた秘密鍵共有システム

2.1. エスパアンテナ

エスパアンテナは中央の 1 本の給電素子と周囲の複数本の無給電素子から成る．例として 7 素子エスパアンテナを Fig. 1 に示す．7 素子エスパアンテナは給電素子が中央の 1 本のみで，その周囲に 6 本の無給電素子が等間隔で配置されている．それぞれの無給電素子には可変容量ダイオードであるバラクタが装荷されており，そのバラクタのリアクタンス値を変化させることで，アンテナの指向性を制御することができる．

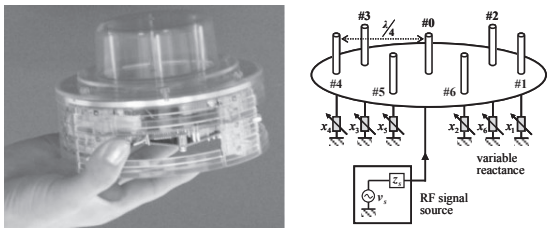

Fig. 1. 7-elements ESPAR antenna.

2.2. エスパアンテナを用いた秘密鍵共有の原理

エスパアンテナを用いた秘密鍵共有について説明する．エスパアンテナの指向性を変化させながら信号を送受することで，起伏に富んだ RSSI の履歴が生成可能となる．親局にエスパアンテナ，子局に無指向性アンテナであるオムニアンテナを搭載し，交互に通信を行いながら各局での RSSI 値を測定し，各局毎に RSSI の履歴を作成する．電波伝搬の相反性より，RSSI 履歴の変化特性は両局間で比例関係となるため，その情報をもとに秘密鍵を生成することで鍵の共有が可能となる．一方，受信場所の異なる盗聴局では，受信特性が異なるため RSSI 履歴の変化特性も異なり，秘密鍵の盗聴は困難になる．子局は常にオムニパターンで通信するため，RSSI 履歴の変化特性は親局のエスパアンテナのビームパターンに依存する．エスパアンテナのビームパターン情報は，親局のみが利用する情報であるため，子局と情報を共有する必要がなく，機密性の高い情報として扱うことが可能である．

2.3. 秘密鍵生成手順

従来提案されているエスパアンテナを用いた秘

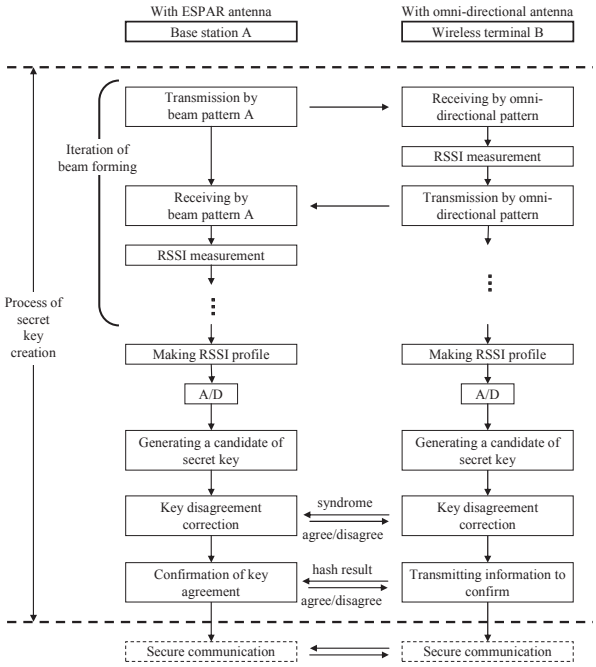

Fig. 2. Key generation procedure.

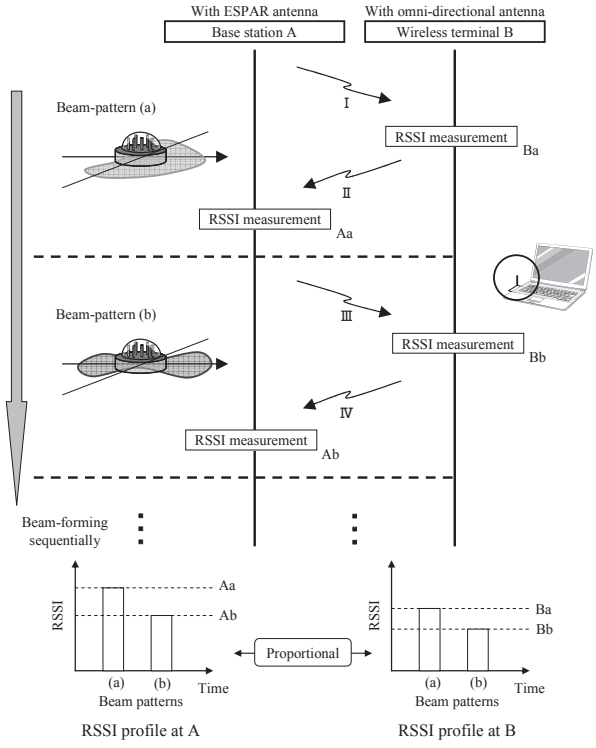

Fig. 3. Method of beam-forming.

密鍵生成手順[10]について説明する. 前提条件として, 親局にエスパアンテナ, 子局にオムニアンテナを搭載し，2 局間では時分割復信（TDD：Time Division Duplex）などのような，上り及び下りに同一周波数を用いた通信が確立されているとする. 鍵生成手順を Fig. 2 に示す．また，Fig. 2 の秘密鍵生成手順におけるエスパアンテナのビーム操作要領を Fig. 3 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．鍵生成モードに入ると，Fig. 3 では，まず親局のエスパアンテナをビームパターン(a)に設定する．そして親局と子局で交互に 1 パケットを送受信し合い，各局で RSSI 値を測定する（図中Ⅰ及びⅡ）．この間, 親局はエスパアンテナをビームパターン(a)に固定しておく．次に，親局のエスパアンテナをビームパターン(b)に変化させ，同様の操作を行う．この様な処理を，秘密鍵の所望鍵長に応じて繰り返し，親局及び子局にて, それぞれ RSSI 履歴を作成する．同じビームパターンを用いた場合の親局と子局のそれぞれの RSSI 値である Fig. 3 の「Aa と Ba」及び「Ab と Bb」の絶対値は等しい値ではないが，電波伝搬の相反性から双方の変化特性は比例関係にあるため, 両局間の共有情報として利用可能である．また，RSSI の変化特性に影響を与えるランダム性の雑音に対しては，RSSI 測定時に複数サンプルの同期加算処理を行うことで軽減可能である．次に，両局の RSSI 履歴に対して, それぞれ閾値を設定し，2 値化処理を行い，秘密鍵候補を作成する．閾値に RSSI 履歴の中央値を用いることで，2 値化後の 0,1 各ビットをほぼ均等に分散させることができる. ただし実際の装置では，この時点で雑音や測定誤差など様々な要因により不一致ビットが生じる. その対策として，所望鍵長以上のデータを取得し，不一致の生じやすい閾値付近のデータを削除することで，鍵の不一致を軽減する. このデータ削除処理については次節で述べる．次に，作成された秘密鍵候補に対し, 誤り訂正技術を応用した鍵不一致訂正処理を施す. 最後にハッシュ関数を用いて鍵共有確認を行い，秘密鍵生成手順が完了する.

2. 4. 閾値付近のデータ削除処理

実際の装置では雑音や送受信のタイムラグによる伝搬路の変化，RSSI 測定時の丸め誤差など，多

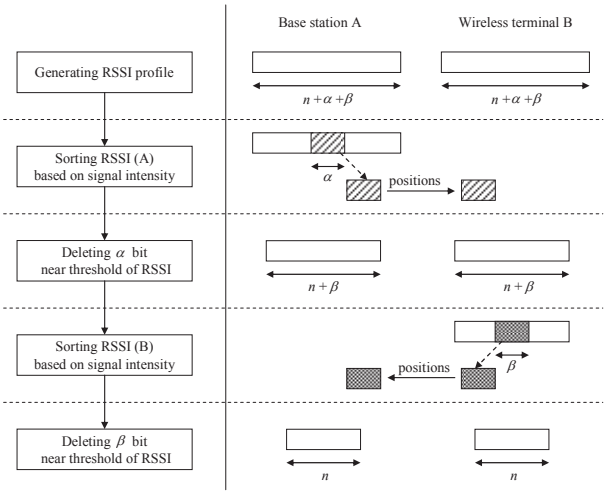

Fig. 4. Procedure of deleting data near threshold.

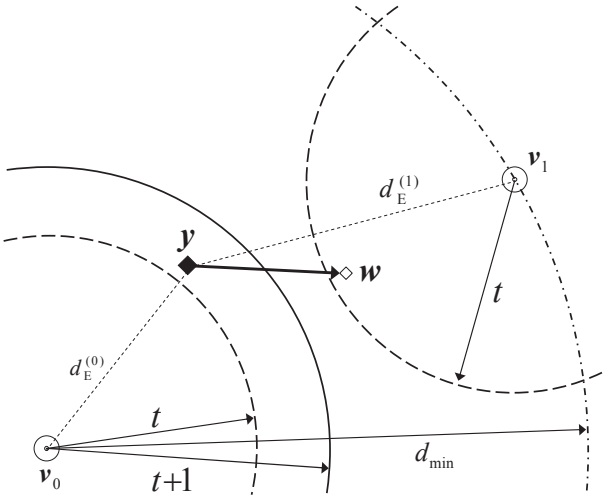

Fig. 5. Concept of error correction when error count is over $t+1$.

くの要因により, 不一致ビットが生じる. そのため, 不一致が生じやすい閾値付近のデータを削除し, 不一致の解消を図る [10]. 閾値付近のデータ削除処理の手順を Fig. 4 に示す.

所望鍵長を n ビットとすると, 閾値付近のデータを親局側で α 個, 子局側で β 個削除するため, まず $n+\alpha+\beta$ 個の RSSI 値を取得する. 次に RSSI 値に応じてソートし, 親局側で閾値に近い部分を α 個削除する. 親局は削除位置情報を子局に送信し, 子局側でそれに対応する部分を削除する. この時, 親局側で閾値付近でなくとも子局側では閾値付近にデータが存在し, 鍵の不一致が起こ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. 子局側で残りのデータを RSSI 値に応じてソートし, 閾値に近い部分を β 個削除する. そしてこの削除位置情報を親局に送信し, 親局側で同様に削除する. 最終的に両局で残った所望鍵長 n ビットのデータを 2 値化処理し, 鍵候補とする.

3. テーブル参照復号法と鍵不一致訂正への適用

3.1. 最尤復号法

最尤復号法は, 各符号語が等しい確率で送信される場合, 正復号率を最大にする復号法であり, 受信系列 $\boldsymbol{y}$ に対して, 条件付確率 $p(\boldsymbol{y}|\boldsymbol{v}_i)$ を最大とする符号語 $\hat{\boldsymbol{v}}$ が送信されたと推定する. 加法的ガウス伝送路では, 受信系列 $\boldsymbol{y}$ に対して, 符号語 $\boldsymbol{v}_i$ のすべてに対してユークリッド距離

$$d_{\mathrm{E}}(\boldsymbol{v}_i, \boldsymbol{y}) = \sqrt{(\boldsymbol{v}_i - \boldsymbol{y})^2} \tag{1}$$

を求め, ユークリッド距離を最小にする符号語 $\hat{\boldsymbol{v}}$ を送信された符号語であると推定することで復号できる.

加法的ガウス伝送路において, 最尤復号法を t 重誤り訂正符号に適用した場合, $t+1$ 以上の誤りを訂正可能な場合がある. 最尤復号の $t+1$ 重以上の誤り訂正の概念図を Fig. 5 に示す. Fig. 5 は受信空間を表し, $\boldsymbol{v}_0$ 及び $\boldsymbol{v}_1$ は符号語, $d_{\min}$ は符号語間の最小ハミング距離, $\boldsymbol{y}$ は受信系列, $\boldsymbol{w}$ は受信系列の硬判定系列, $d_{\mathrm{E}}^{(0)}$ は $\boldsymbol{v}_0$ と $\boldsymbol{y}$ とのユークリッド距離, $d_{\mathrm{E}}^{(1)}$ は $\boldsymbol{v}_1$ と $\boldsymbol{y}$ とのユークリッド距離を表す. また, $d_{\mathrm{E}}^{(0)} < d_{\mathrm{E}}^{(1)}$ であるとする. Fig. 5 で送信符号語を $\boldsymbol{v}_0$ とし, 受信系列 $\boldsymbol{y}$ が受信されたとする. 受信系列の硬判定を行うことにより, $\boldsymbol{y}$ が $\boldsymbol{w}$ に移る. $\boldsymbol{w}$ を代数的復号すると $\boldsymbol{v}_1$ に復号される. 加法的ガウス伝送路を仮定しており, $d_{\mathrm{E}}^{(0)} < d_{\mathrm{E}}^{(1)}$ であるため, 受信系列 $\boldsymbol{y}$ を受信したとき, 送信符号語は $\boldsymbol{v}_0$ である確率が高く, $\boldsymbol{v}_1$ である確率は低い. 送信符号語が $\boldsymbol{v}_0$ のとき, 硬判定復号を行うと誤訂正となる. それに対して, 最尤復号法で復号を行うと $\boldsymbol{v}_0$ に復号され, $t+1$ 重以上の誤りが正しく復号される.

最尤復号法では, $t+1$ 重以上の誤りを訂正できるが, 硬判定受信系列 $\boldsymbol{w}$ と送信符号語 $\boldsymbol{v}_0$ とのハミン

グ距離がある値よりも大きくなると，その誤りは訂正できなくなる．その最尤復号で訂正可能限界の送信符号語と硬判定受信系列のハミング距離を d_{MLL} とする．すなわち d_{MLL} は最尤復号法で正しく訂正できる誤り個数の最大値であり，符号語間の最小ハミング距離を $d_{\min}$ とすると $d_{\mathrm{MLL}} = d_{\min} - 1$ 程度と考えられる．

3.2. テーブル参照復号法

最尤復号法は誤り訂正の能力を最大限に引き出すことができる復号法であるが，すべての符号語に対してユークリッド距離の比較を行うと，計算量が膨大になるという問題がある．この計算量を削減するために，テーブルを参照する方式が提案されている [13]．この方式で用いるテーブルとは，符号長 n に対して 2^n 種類の硬判定系列と，最尤復号法で得られる符号語のうち，復号される確率の高い数種類の候補符号語との対応表である．通常，テーブルは，あらかじめ作成して，メモリなどに保存しておき，復号を行うときに用いる．復号の際には，受信系列の硬判定系列でテーブルを参照することにより，限定された候補符号語群を呼び出し，その候補符号語群に対してのみ，ユークリッド距離比較を行う．この方式では，テーブルを参照することで，尤度の高い候補符号語群のみとユークリッド距離比較を行うことによって計算量の削減を図っている．しかし，この方法では符号長 n が大きくなれば，テーブルの規模が大きくなるという問題がある．

それに対して，硬判定系列の代わりにシンドロームに対するテーブルを使用した方式が提案されている [14]．この方式で用いるテーブルは，シンドローム長 m に対して 2^m 種類のシンドロームとそのシンドロームに対応する発生確率の高い誤りパターンとの対応表である．ここで，誤りパターンとは，対象としている硬判定系列に対し，誤りビット位置が 1，それ以外のビット位置が 0 で表されている 2 値系列のことである．シンドロームのテーブルを用いた方式はテーブル容量を削減できるため，本稿では，このシンドロームのテーブルを用いた方式を使用する．

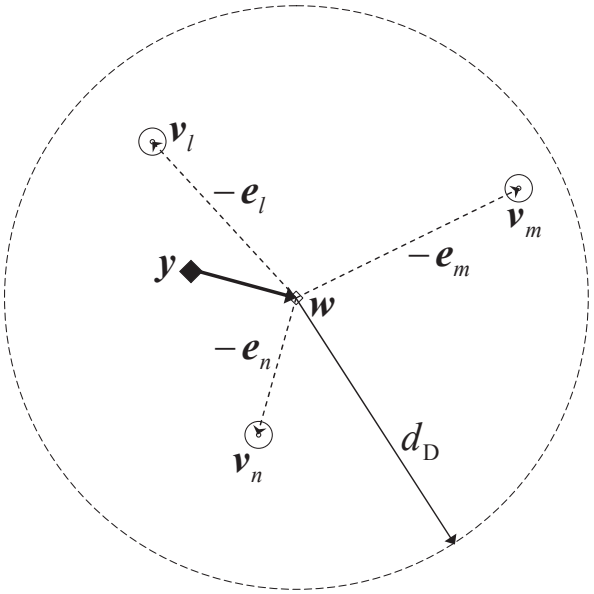

Fig. 6. Principle of table-aided soft-decision decoding.

シンドロームのテーブルを用いたテーブル参照復号法では，復号半径として，ある半径を定め，そのハミング距離を $d_{\mathrm{D}} \leqq d_{\min} - 1$ とし，送信した符号語から，この復号半径内に受信された硬判定系列の誤りを訂正する．原理図を Fig. 6 に示す．

受信系列を $\boldsymbol{y}$，硬判定受信系列を $\boldsymbol{w}$ とし，$\boldsymbol{w}$ から得られるシンドロームを $\boldsymbol{s}_{\mathrm{c}}$ とする．硬判定受信系列 $\boldsymbol{w}$ からハミング距離 d_{D} 以内の範囲を復号領域とする．硬判定復号では，復号領域内で $\boldsymbol{w}$ からハミング距離が最小の符号語を検出し，$\boldsymbol{v}_n$ を得る．つまり，テーブルは $\boldsymbol{s}_{\mathrm{c}}$ に対して最小ハミング重みの誤りパターン $\boldsymbol{e}_n$ が，ただ 1 つ対応している．それに対し，軟判定復号では，復号領域内の候補符号語群 $\boldsymbol{v}_l$, $\boldsymbol{v}_m$, $\boldsymbol{v}_n$,…をすべて検出し，受信系列 $\boldsymbol{y}$ とのユークリッド距離比較を行い，最も尤度の高い符号語 $\boldsymbol{v}_l$ を得る．テーブルは $\boldsymbol{s}_{\mathrm{c}}$ に対してハミング重み d_{D} 以下の誤りパターン $\boldsymbol{e}_l$, $\boldsymbol{e}_m$, $\boldsymbol{e}_n$,…が対応している．このとき，$d_{\mathrm{D}} = d_{\min} - 1$ とすれば，テーブル参照軟判定復号法は最尤復号法とほぼ同じ誤り訂正能力を持つ．

3.3. テーブル参照復号法を用いた鍵不一致訂正

シンドロームテーブルを用いた鍵不一致訂正の手順を Fig. 7 に示す．この方式ではテーブルを参照して復号を行うため，まず事前にテーブルを作成し

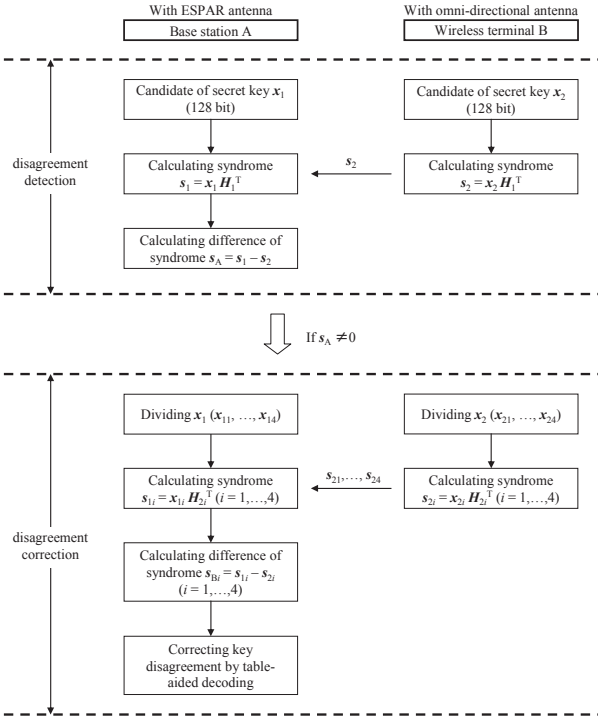

Fig. 7. Procedure of correcting key disagreement.

ておく必要がある．その上で，まず両局で生成した鍵 x_1, x_2 に検査行列の転置 H^T を掛けてシンドローム s_1, s_2 を求める．子局は求めたシンドローム s_2 を親局側に送信し，親局はシンドロームの差分 $s = s_1 - s_2$ を求める．$s = 0$ の場合，鍵の不一致はないとして，鍵の不一致訂正は行わない．$s \neq 0$ の場合は，あらかじめ作成しておいたシンドロームテーブルを参照して誤りビット位置を導出し，親局側で訂正することで不一致を解消する．

4. 鍵不一致訂正における距離比較基準の提案

3.2 で述べたように，テーブル参照軟判定復号法では，シンドロームから復号領域内の候補符号語群を，すべて検出し，受信系列とのユークリッド距離比較を行うことで，復号領域内で最も尤度の高い符号語を得る．誤り訂正における軟判定復号のユークリッド距離比較までの流れを Fig. 8 に示す．候補符号語の生成方法は，テーブルを参照してシンドロームに対応する誤りパターンを求め，これらの誤りパターンを硬判定受信系列に付加することで復号領域内の候補符号語を得ることができる．

このテーブル参照軟判定復号法を鍵不一致訂正

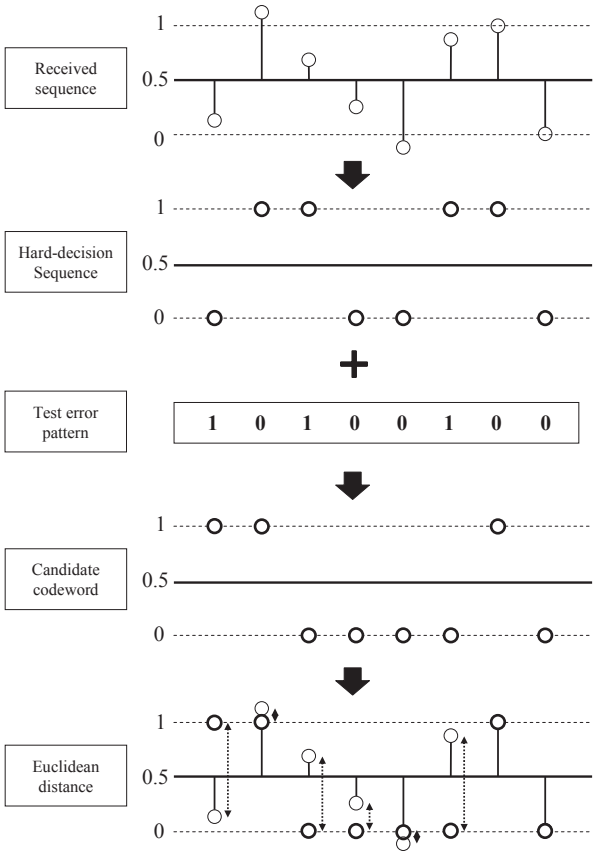

Fig. 8. Comparison of Euclidean distance in error correction.

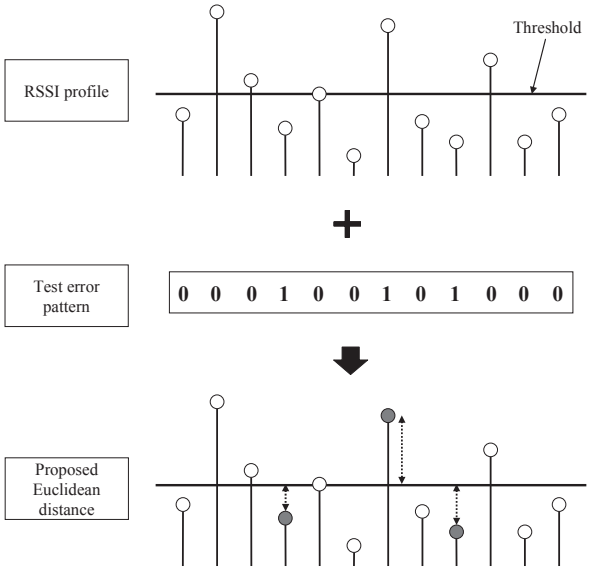

Fig. 9. Comparison of Euclidean distance in key disagreement correction.

方式として適用した場合，距離比較の基準となる既知信号がないという問題がある．そのため，距離比

較の基準となる値を設定する必要がある.

本稿では, 誤り訂正の軟判定復号で用いる受信系列と候補符号語とのユークリッド距離に代わるものとして，受信系列である RSSI 履歴の誤りビット位置の値と閾値とのユークリッド距離を用いる方法を提案する. 鍵不一致訂正における軟判定復号のユークリッド距離比較までの流れを Fig. 9 に示す. そして，その距離が最小となる誤りパターンを，RSSI 履歴に加えることで，鍵不一致訂正を行う.

5. シミュレーションシステム

5.1. システムモデル

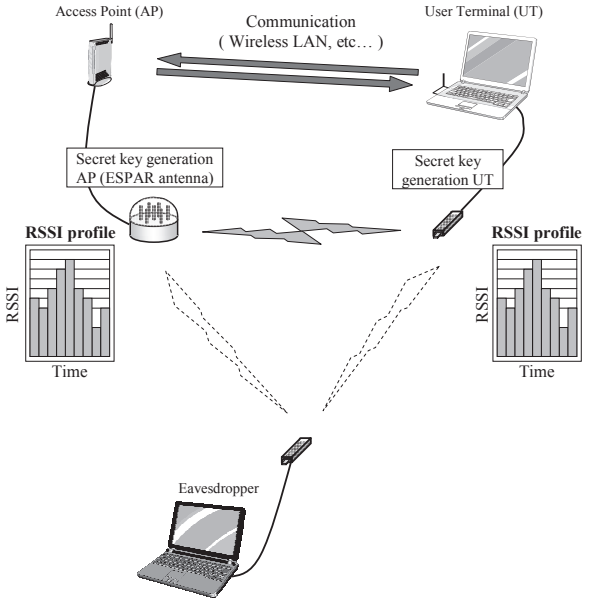

Fig. 10. Configuration of secret key agreement system using ESPAR antenna.

IEEE802.15.4/ZigBee^{TM} を無線システムとして用いた既存の秘密鍵共有システムをモデルとして特性評価を行う. Fig. 10 にシステムモデルを示す. 親局に対し，正規のユーザである子局と，親局と子局間の通信を傍受できる盗聴局から構成される. 親局にエスパアンテナ, 子局と盗聴局にはオムニアンテナが搭載されている. また，各局は固定位置で通信を行うものとし, 周囲の人や物の移動などによる伝搬環境の変化はないものとする. Fig. 11 にシミュレーションに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. また，盗聴局は一般に屋外から親局と子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，盗聴局も親局・子局間と同じ閉空間に存在し，親局と子局間の直接波を受信できる盗聴に有利な環境を想定している.

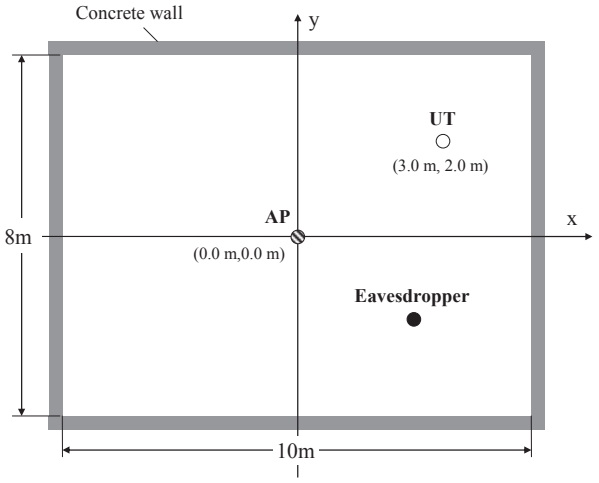

Fig. 11. Simulation environment and example of terminal position.

5.2. シミュレーションシステム諸元

Table 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 256 ステップで刻んだ値で設定する. RSSI の測定に利用する RV 系列（6 個のリアクタンス値）は，試行毎にランダムに設定する. 使用する搬送波周波数は 2.484 GHz 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 [15] を用いて設定する. 簡略化のため，床及び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.

生成する鍵長は 128 ビットとする. RSSI 測定時の雑音軽減のために行う平均化処理のシンボル数は 32 シンボルとし，RSSI 値を鍵候補に変換する閾値は得られた RSSI 値の中央値を用いるものとする.

Table 1. Simulation system parameters.

(a) Room environment, propagation path parameters

Room size	8 m × 10 m
Antenna	Base station（ESPAR Antenna） User terminal, Eavesdropper（Omni-Antenna）
Carrier frequency	2.484 GHz
Wall material	concrete（$\varepsilon_\gamma = 6.76$, $\sigma = 0.023$ S/m, $\mu_\gamma = 1$）
Terminal position [m]	Base station：（0.0 m, 0.0 m） User terminal, Eavesdropper：random
Channel model	Ray-tracing（reflection : up to 6 times）

(b) Key parameters

Key length	128 bit
Averaging	32 symbol
RV (reactance vector)	Random selection from 256 steps
Threshold for binarization	Median
Code for detection	Extended BCH(128,112)
Code for correction	Extended BCH(32,21)

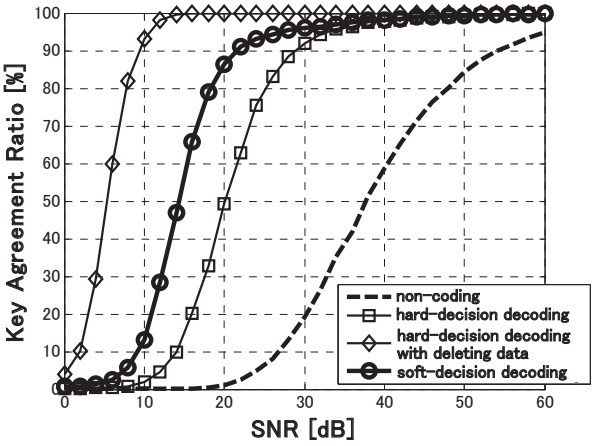

Fig. 12. Performance of key agreement ratio versus SNR.

また，閾値付近のデータ削除処理は，取得 RSSI データ数を鍵長の 3 倍の 384 ビットとし，両局でそれぞれ 128 ビットずつ削除する．

鍵不一致訂正処理は 2 段階で構成され，まず生成した鍵に対して不一致の検出を行う．不一致が検出された場合は鍵を 4 分割して不一致訂正を行う．これは 4 分割することで，作成するテーブルの容量を削減できるためである．鍵不一致検出には拡大 BCH(128,113)の検査行列，鍵不一致訂正には拡大 BCH(32,21)の検査行列を用いる．

6. 計算機シミュレーション

6.1. SNR 対鍵一致率特性

不一致訂正方式を変化させたときの SNR 対鍵一致率特性を Fig. 12 に示す．ここでの鍵一致率とは，各方式で不一致訂正を行ったとき，総試行回数（1000 回）中で作成した全 128 ビットが一致する回数をパーセンテージで表している．端末配置は，親局を中央(0.0 m, 0.0 m)，子局を室内でランダムな位置とする．

Fig. 12 より，テーブル参照軟判定復号法で不一致訂正を行った場合，SNR 約 22 dB で鍵一致率 90 % となっており，硬判定復号法で行った場合と比較して約 8 dB 改善されている．このことより，提案した距離比較方法の有効性が確認できる．また，閾値付近のデータ削除後に硬判定復号法を行った場合は SNR 約 10 dB で鍵一致率 90 %となっている．図には示していないが，削除するデータ数を変化させながら同様のシミュレーションを行った結果，データ削除数を増やすと訂正能力も向上することが確認された．

6.2. 盗聴局との鍵相関特性

親局を部屋の中央(0.0 m, 0.0 m)，子局を座標(3.0 m, 2.0 m)に固定し，各方式で不一致訂正を行ったときの部屋全体での盗聴局と子局間の鍵相関の分布を調べる．Fig. 13-15 はそれぞれ「閾値付近のデータ削除を用いない硬判定復号法」,「閾値付近のデータ削除を用いない軟判定復号法」,「閾値付近のデータ削除を用いる硬判定復号法」を適用したときの鍵相関分布を示している．Fig. 13 に示すカラーバーは共通で対応する．盗聴局は部屋の端から 10 cm 刻みに移動させる．また，データ削除を行う方式では削除位置情報を送信し合うため，盗聴局はその情報を得て同じ位置を削除できたと想定する．同様に，不一致訂正処理ではシンドローム情報が送信されるため，盗聴局は子局のシンドロームをもとにテーブル参照復号法を適用したとする．

Fig. 13-15 より，部屋の大部分で盗聴局と子局間の鍵の相関は低いが，正規局間の直線状の領域で，ある程度の広がりを持って相関が高くなっている．

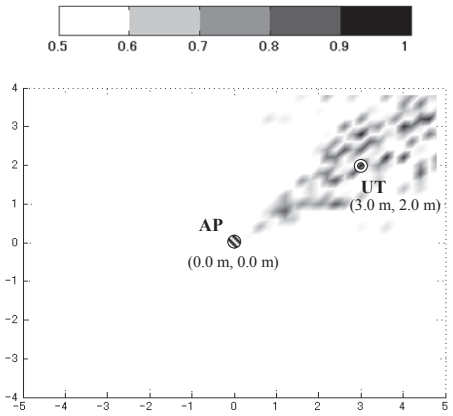

Fig. 13. Performance of correlation between user terminal and eavesdropper (hard-decision decoding).

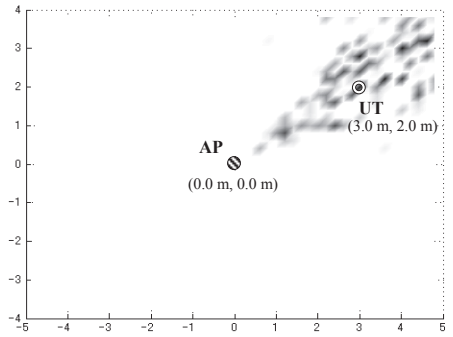

Fig. 14. Performance of correlation between user terminal and eavesdropper (soft-decision decoding).

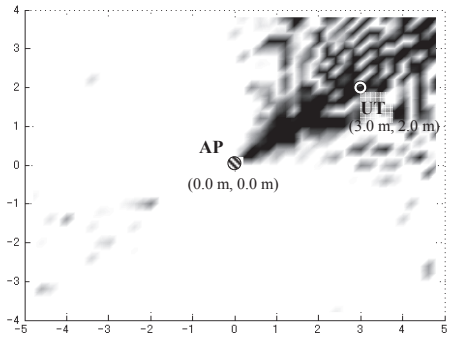

Fig. 15. Performance of correlation between user terminal and eavesdropper (hard-decision decoding with deleting data).

これは直接波の影響が大きいためだと考えられる．また Fig. 13,14 では，ほとんど特性に差はなく，「閾値付近のデータ削除を用いない硬判定復号法」と「閾値付近のデータ削除を用いない軟判定復号法」の違いで盗聴局との鍵相関に影響がほとんどない．それに対し，「閾値付近のデータ削除を用いる硬判定復号法」を用いた Fig. 15 では鍵相関の高い範囲が広がっている．これは削除前の鍵候補において，閾値付近のデータは鍵の不一致が多いため互いに相関が低く，閾値から離れたデータでは鍵の不一致が少ないため，互いの相関が高い．そのため，閾値付近を削除することによって，相関の高い部分が残ったためだと考えられる．

6. 3. 各不一致訂正方式の総合的評価

Fig. 12 の鍵一致率特性より，今回提案したテーブル参照軟判定復号法を用いた方式を適用することで，従来の「閾値付近のデータ削除を用いない硬判定復号法」より鍵一致率を上げることが可能であることがわかった．また，Fig. 13-15 の盗聴局との鍵相関特性より，閾値付近のデータ削除を用いた場合，データ削除の影響で盗聴局との鍵相関が高くなっていることがわかる．それに対し，閾値付近のデータ削除を用いない場合，硬判定と軟判定の復号法の違いによる鍵相関への影響は，ほとんどない．そのため，「閾値付近のデータ削除を用いる硬判定復号法」は，盗聴の困難さよりも鍵の一致に重点を置いた方式であると言える．

以上のことから，鍵一致率と盗聴の困難さの両面から各方式を比較した結果，鍵の不一致訂正方式としては，今回提案したテーブル参照軟判定復号法を用いた方式が適していると考えられる．

7. まとめ

本稿では，エスパアンテナを用いた秘密鍵共有方式における鍵不一致訂正方式としてテーブル参照軟判定復号法を適用する手法を検討した．鍵不一致訂正では，距離比較の基準となる既知の信号がないため，通常の軟判定復号における受信系列と候補符号語のユークリッド距離に変わるものとして，RSSI

履歴の閾値までの距離を用いることを提案した．そして，提案方式と従来方式の「閾値付近のデータ削除を用いる硬判定復号法」と「閾値付近のデータ削除を用いない硬判定復号法」に対し，鍵一致率特性，及び盗聴局と子局間の鍵相関特性を計算機シミュレーションにより求め，特性評価を行った．その結果，従来方式の「閾値付近のデータ削除を用いる硬判定復号法」では十分な鍵一致率を達成できるが，データ削除の影響によって鍵一致率と盗聴局との鍵相関にトレードオフの関係があり，削除データ数を増やして鍵一致率を上げると盗聴局と子局間の鍵相関も高くなることが確認された．それに対し，提案方式ではデータ削除なしでも従来方式の「閾値付近のデータ削除を用いない硬判定復号法」と比較して，鍵相関特性を劣化させることなく鍵一致率特性を改善できることが確認された．

今後は，「閾値付近のデータ削除を用いる軟判定復号法」の特性評価と，さらに訂正能力の高い誤り訂正方式を検討し，本システムに適用した場合の特性評価を行う予定である．そして本システムに限らず，秘密鍵共有方式における鍵不一致訂正方式として最適な誤り訂正技術を確立することが今後の課題である．

参考文献

1) 笠原正雄，境隆一，暗号，(共立出版，東京，2002).
2) 岡本龍明，山本博資，現代暗号，(産業図書，東京，1979).
3) J. E. Hershey, A. A. Hassan and R. Yarlagadda, “Unconventional Cryptographic Keying Variable Management,” IEEE Trans. Commun. , vol. 43, pp. 1-6 (1995-01).
4) A. Hassan, W. E. Stark, J. E. Hershey and S. Chennakeshu, “Cryptographic key agreement for mobile radio,” Digital Signal Processing, vol. 6, pp. 207-212 (1996).
5) 本多誠，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 (2002-04).
6) 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 (2004-10).
7) 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 (2007-03).
8) T. Ohira and J. Cheng, “Analog smart antennas,” Adaptive Antenna Arrays, pp. 184-204, ISBN3-540-20199-8, Berlin: Springer Verlag (2004-06).
9) 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 (2004-01).
10) 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 (2005-09).
11) T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, “Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multiplath Fading Channeles,” IEEE Trans. Antennas Propag. , vol. 53, No. 11, pp. 3776-3784 (2005-11).
12) 大平孝，笹岡秀一，“解説　盗聴防止アンテナ，”信学誌, vol. 88, no. 2, pp. 190-194 (2005-03).
13) 南英城，笹岡秀一，“ブロック符号のテーブル参照による軟判定復号法，”信学論(B), vol. J79-B, no. 11, pp. 728-737 (1996-11).
14) 清水隆史，笹岡秀一，“リードソロモン符号のテーブル参照軟判定復号法の検討，”信学技報, IT2004-67, pp. 101-106 (2005-03).
15) 細矢良雄（監修），電波伝搬ハンドブック，(リアライズ社，東京，1999).