Basic Study on Agreement Verification of Channel Coefficient Sequence in Mobile Communication Channel

Hideichi SASAOKA* and Hisato IWAI*

(Received October 17, 2022)

There are many studies of secret key agreement based on radio propagation characteristics, but there are few studies of the agreement of analog secret information (key). This paper deals with a technique to verify agreement of the channel coefficient sequence (analog secret key) by the information exchange using a public channel. This paper showed a principle to reduce information leakage due to information exchange and devised agreement verification to use unique event of channel coefficient sequence. This paper also showed examples of unique event such as three points of crossing with a straight line and the channel coefficient curve, and product set of the big and small decision of the channel coefficient, and this paper clarified possibility and a problem of the technique using them.

Key words: secret key agreement, analog secret key, channel coefficient sequence, agreement verification

キーワード： 秘密鍵共有，アナログ秘密鍵，チャネル係数列，一致確認

移動通信路におけるチャネル係数列の一致確認に関する基礎検討

笹岡　秀一，　岩井　誠人

1. はじめに

最近，無線通信の普及・発展が目覚しいが，無線通信は電波の傍受が容易なため盗聴や不正アクセスの対策が重要である．この対策として共通鍵暗号や公開鍵暗号などの情報セキュリティ技術があるが，演算能力に制約がある移動端末においては共通鍵暗号が一般的であり，秘密鍵の管理や配送が重要となる．これらの計算量的な複雑性を安全性の根拠とする技術と異なり，情報理論的な複雑性を安全性の根拠とする暗号技術も研究されている．これらには，雑音のある通信路（盗聴通信路）を用いた鍵配送[1]，相関情報に基づく秘密鍵共有[2,3]などがある．しかし，これらは理論的研究が多く，実用的なものは少ない．

一方，移動通信路（マルチパス伝搬環境）における電波伝搬特性の可逆性と場所依存性に基づく秘密鍵生成(Secret key generation)が提案されており[4,5]，いまでは無線物理層セキュリティと呼ばれている[6]．ここで，電波伝搬特性には，マルチトーン信号の位相差[4,5]，無線伝送路のインパルス応答[7]，振幅周波数特性の時変化[8]，受信信号強度の時変化[9,10]などがある．また，アレーアンテナの指向性パターン変動を活用した人工フェージングの受信信号強度を用い

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

た秘密鍵生成がある[11,12]．なお，秘密鍵生成の後で鍵一致(Key reconciliation)やプライバシー増幅など秘密鍵共有(Secret key agreement)プロトコルにより正味の秘密鍵が取得される[13]．ここで鍵一致には，閾値付近のデータ削除と誤り訂正の併用[11]，ビット系列を対象とするCascadeプロトコル[14]，多値量子化におけるビット不一致訂正に適した上位・下位ビット毎の誤り訂正の適用[15]やLDPC符号の適用[16]など各種の手法がある．

上記の秘密鍵共有では，電波伝搬特性（アナログ値）をディジタル化（標本化，量子化，符号化）して，量子化記号（又は，量子化符号語）を取得した後，標本数分の量子化符号語から秘密鍵候補を生成すると共に鍵一致等の秘密鍵共有プロトコルで秘密鍵を取得している．また，秘密鍵の用途は共通鍵暗号による守秘と認証への応用が想定される．しかし，その有効性は従来の鍵配送との優劣比較に依存する．このため，無線秘密鍵共有の長所を発揮するには，ディジタルの秘密鍵ではなくアナログ秘密情報（アナログ秘密鍵）に基づく新たな応用分野の開拓が有望と考えられる．一例としてアナログ秘密鍵に基づく相手認証や守秘への応用が想定される．このため，アナログ秘密鍵の一致確認が重要となるが，ディジタルの場合と異なり鍵一致が行われず，受信雑音に起因する誤差を考慮して誤差範囲内での一致確認が行われる．しかし，アナログ秘密鍵の一致確認の研究はほとんどなく，誤差を想定しない従来の秘密鍵共有をそのまま適用できない．

そこで，本論文では対向通信する正規者が公開通信路を用いた情報交換によりチャネル係数の時系列（チャネル係数列）に対してある誤差範囲での一致を盗聴者に秘密裏に確認する手法を検討対象とした．はじめに，秘密鍵共有と共通鍵に基づく相手認証など従来技術を概観した後，既存技術を応用した一致確認法の可能性と課題を検討した．次に，個々のチャネル係数列のある現象に注目して，その現象が独自で希少となる場合を探索して得られた事象（特異事象）に基づく新たな一致確認の原理を示した．また，注目する現象の例として，チャネル係数の波形と直線との３点交差，又はチャネル係数の大小判定結果の積集合を示すとともに，特異事象に基づく一致確認の実現性と課題の基礎検討を行った．

2. 秘密鍵共有の関連技術とアナログ鍵への応用

2.1 無線物理層における秘密鍵共有

2.1.1 相関情報に基づく秘密鍵共有の原理

電波伝搬特性に基づく秘密鍵共有は，相関情報に基づく秘密鍵共有の一応用である．相関情報に基づく秘密鍵共有を一般化するとFig. 1の構成になる．Fig. 1は，正規者（アリス，ボブ）が，お互いに相関のあるN個の乱数系列X^NとY^Nを受け取り，公開通信路を通して情報$(C_1, C_2, \cdot\cdot)$を送受することで，N個の乱数系列Z^Nを受け取るイブに知られない秘密鍵を共有する構成を示している．

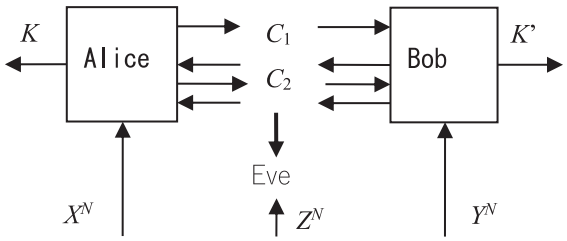


Fig. 1. Secret key agreement from correlated information.

また，秘密鍵共有プロトコルには，(1) Advantage distillation，(2) Information reconciliation，(3) Privacy amplification の３ステップがある[13]．ここで，ステップ(2)の情報一致はイブに秘密を保持しながらアリスとボブの乱数系列の一致を，ステップ(3)のプライバシー増幅は一致した乱数系列から正味の（イブが未知の）秘密鍵の生成を行う．また，あるプロトコルを用いてアリス・ボブ間で共有できた正味の鍵生成の速度を鍵レートと呼び，実現可能な鍵レートの上限を秘密鍵容量と呼ぶ．

2.1.2 電波伝搬特性に基づく秘密鍵共有の概要

電波を用いた秘密鍵共有の原理は，電波伝搬の可逆性と場所依存性に基づいている．電波伝搬の可逆性により正規者が電波伝搬特性を測定し，相関性の高い情報を取得する．一方，電波伝搬の場所依存性により異なる場所の盗聴者は，相関性の高い情報の

取得が困難となる．ここで，電波伝搬特性には，1章で示した各種のものがあるが，以下の説明ではチャネル係数列を用いる場合に限定する．

Fig. 2 に相関情報を取得する移動通信路モデルを示す[17]. このモデルでは, 対向通信を行う正規者（アリスとボブ）が既知信号 T を送信し，フェージング変動（チャネル係数 S) を受けた信号 $S\cdot T$ を受信し，測定値 $X = S + N_X$, $Y = S + N_Y$ を得る. また, 盗聴者（イブ）は, チャネル係数 S_E に対して, 測定値 $Z = S_E + N_Z$ を得る．なお，チャネル係数の相関係数を ρ とすると，$S_E = \rho S + \sqrt{1-\rho^2}W$ となる．ここで，W は S と独立なガウス変数である.

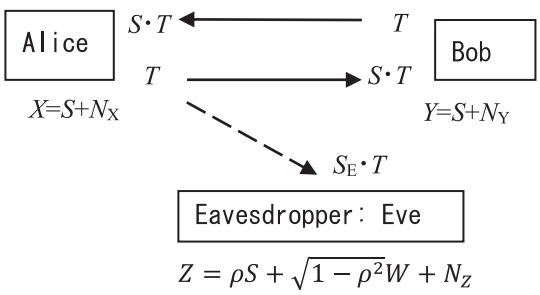


Fig. 2. Channel model of land mobile communication to obtain correlative information.

電波を用いた秘密鍵共有には，電波伝搬環境，伝送システム，秘密鍵候補の生成と最終的な秘密鍵の取得に対して各種のものがある. 移動伝搬環境では，チャネル係数の波形の標本化を行い，チャネル係数列を取得して，多数ビットの秘密鍵生成が可能である．しかし，屋内伝搬環境でチャネル係数の時変化が少ない場合には，電波伝搬特性の人工的な時間変動の発生が必要となる．また，伝送方式が複数アンテナを用いた MIMO か単一アンテナシステムか, マルチキャリアの OFDM かシングルキャリアかに依存して適した秘密鍵生成の手法が異なる．次に，チャネル係数列からの秘密鍵候補の生成には，チャネル係数列の前処理（補間，正規化など），ディジタル化（量子化，符号化など），符号語のビット不一致の軽減がある．また，秘密鍵候補から秘密鍵の取得には, 鍵ビット不一致訂正と鍵一致の最終確認がある.

2.1.3 チャネル係数列の取得と秘密鍵候補の生成

チャネル係数は受信信号を局部発信信号（又は再生搬送波）で検波して得られる．ここで，直交検波で得られた同相成分と直交成分を実部と虚部に対応させるとチャネル係数が複素数となる．なお，複素のチャネル係数を正確に一致させるには，正規者間での搬送波の周波数同調と位相同期（又は位相差の補償）が前提となる．また，時分割複信における測定時間差による誤差が無視できること，正規者間で信号の増幅率の一致が前提となる．これらの前提が難しい場合，測定値の絶対値をとった振幅値，時間差の補間値，平均値（又は中央値）で正規化した相対値を採用した共有が望ましい.

次に，チャネル係数の波形に対して，標本化，量子化，符号化を行うことで量子化記号（非負整数）又は量子化符号語（ビット列）を得る．標本化は，隣接する標本値間の相関が高い場合，標本間隔を広く設定変更する．次に，量子化において量子化レベル数を増加させると，符号語のビット数が増加するが，雑音によるビット不一致が増加する．また，符号化には，2 進符号化の他に交番２進符号化も考えられる.

次に，符号語（ビット列）を標本数分だけ接続すれば十分な長さの秘密鍵候補（ビット列）が得られるが，符号語の不一致が含まれると全体のビット不一致率も増加する．実際に量子化ステップ付近の標本値に対応する符号語では，符号語の不一致が高い頻度で発生し, 標本値の信号対雑音電力比（SN 比）を増加させても記号不一致率およびビット不一致率が急速に減少しない問題がある．このため，誤り訂正によるビット不一致訂正が有効に機能しない懸念がある．この対策には，通信路の SN 比に対して適切な量子化レベル数の設定が重要である．また，量子化ステップ付近の標本値の除去[11]，パリティの通知による記号不一致の検出と記号の除去，パリティと量子化誤差の通知による隣接記号への訂正[18]などが有効となる．これらの記号不一致の軽減を行った後，記号の符号語を標本数分だけ接続すれば秘密鍵候補となる. なお, 秘密鍵候補の生成までの処理は，無線物理層セキュリティに特徴的なものである.

2.1.4 ビット不一致訂正

秘密鍵候補のビット不一致率が過大でない場合，残されたビット不一致は誤り訂正・制御技術の適用により訂正できる．ビット不一致訂正には，ブロック誤り訂正符号のシンドロームを活用する手法がある．この手法は，ブロック内のビット誤り個数の上限を推定することで，検査ビット数（公開するビット数でもある）を必要最小限とする符号を選択する．次に，その誤り訂正符号に対して秘密鍵候補のシンドロームを算出し，２つの無線端末の秘密鍵候補のシンドローム差からビット不一致訂正を行う[11]．この手法の課題は，誤り個数を過小評価した場合にビット不一致訂正に失敗する問題がある．また，逆にビット誤り個数を過大に見積もった場合に公開するビット数が増加し，正味の秘密鍵容量が減少する問題がある．

この課題に対処する一手段は，量子鍵配送の鍵不一致解消法として提案されている Cascade の手法を適用することである[14]．Cascade では，秘密鍵候補のビット列をランダムに並べ替えた後でブロックに分割し，各ブロックのパリティを求める．このパリティ情報（1 ビット）を公開通信路により相手方に伝送し，パリティを比較することで不一致ビットの有無を判定する．不一致ビットが存在するブロックを 2 分割した後で各分割ブロックのパリティを比較することで，不一致ビットが存在するブロックを検出する．不一致ビットの含まれるブロックに対して，上記の処理を繰返すことで，不一致ビットを除去する．この手法は，①ビット不一致訂正に失敗する確率を指数的にゼロに近づけられること，②推定ビット誤り率の誤差に寛容であること，③ビット一致のために公開するビット数が理論限界に近いことが特徴である．なお，この場合にもパリティ情報の公開により秘密鍵容量が減少する．

2.1.5 鍵一致の最終確認

上記のビット不一致訂正によりビット不一致率はほぼゼロとなる．次に，公開情報による漏洩情報を考慮して鍵ビット長の短縮処理を行い，正味の秘密鍵を取得することで秘密鍵共有が完成する．なお，秘密鍵の一致確認を秘密裏に行うことが必要となる場合がある．ここで，秘密通信路を介して最終確認を行うことは無線秘密鍵共有の主旨に反する．

そこで，公開通信路を介した一確認法は，一方の正規者の秘密鍵候補に対して一方向性の変換を行い，公開通信路を介して変換結果をもう一方の正規者に送信する．もう一方の正規者は，自身の秘密鍵候補の変換結果と受信データとの一致により秘密鍵候補の一致を確認する[11]．なお，公開情報による情報漏洩を抑える観点から，変換結果のビット数が小さいことが好ましい．このため，一方向関数としてハッシュ関数が代表的であるが，入出力のビット数が一般に大きいので，必ずしも適切でない．そこで別の選択として，CRC 誤り検出符号のシンドロームの使用が考えられる．一致が確認された後は，公開情報による漏洩情報を考慮して鍵ビット長の短縮処理を行い，正味の秘密鍵を取得する．

2.2 相手認証

2.2.1 パスワード方式と１パス相手認証

パスワード認証と１パス相手認証の構成を Fig. 3 の(a)と(b)に示す．

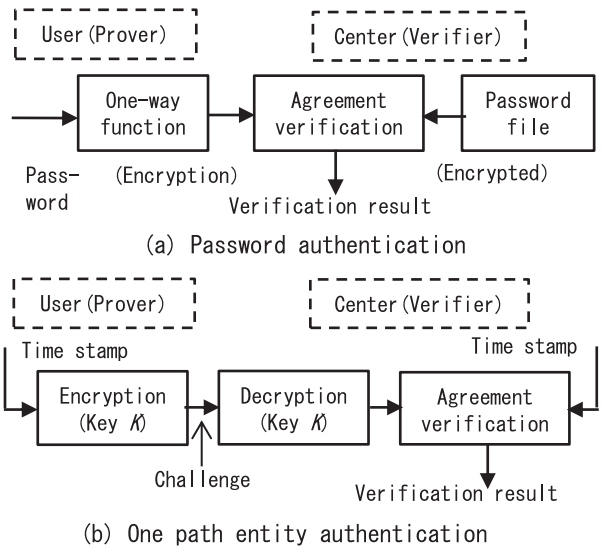


Fig. 3. Password authentication and one path entity authentication.

パスワード方式は，利用者（証明者）が秘密裏に保持するパスワードをセンターにアクセスする際にセンター（検証者）に送信することで，利用者の正

当性を証明する[19]．しかし，単純なパスワード方式は，以下のような安全上の問題がある．①パスワードが盗聴されると，認証方式の安全性が損なわれる．②センターに登録されたパスワードを秘密に管理する必要がある．この対策として，パスワードを一方向関数で暗号化してセンターのファイルに格納する手法が採用されている．

また，パスワードが頻繁に変更し難い問題を解決するために，認証の度に代わる変数（例えば，タイムスタンプ）を暗号化して送信し，受信側で復調してタイムスタンプの一致を確認する手法もある[20]．

2.2.2 共通鍵に基づく 2 パス相手認証

共通鍵に基づく 2 パス相手認証は，検証者からのチャレンジに対して，利用者がレスポンスを返す，２つの通信から構成される[19,20]．また，検証者と利用者は事前に鍵を共有している．この方式では，以下のステップで相手認証を行う．①検証者が，ランダムなメッセージ（乱数 r）を生成し，利用者に送信する．②利用者は，r を鍵 K で暗号化した結果 $X = E_K(r)$ を検証者に送る．③検証者は，$X = E_K(r)$ が成立つことを検査する．この方法は，平文 r と暗号文 X の両方が公開されるため，検証者になりすました攻撃者から選択平文攻撃を受けて，秘密の鍵 K を解読される危険がある．

この対策をした相手認証の構成を Fig. 4 に示す[19]．

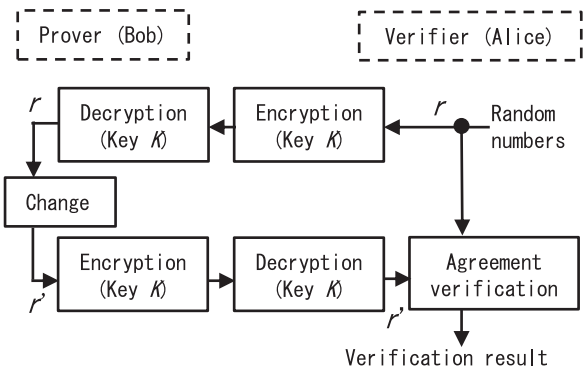


Fig. 4. Two path entity authentication using common key.

この方式では，以下のステップで相手認証を行う．①検証者が乱数 r を生成した後で，鍵 K を用いて暗号化した結果 $X = E_K(r)$ を利用者に送信する．②利用者は，鍵 K を用いて X を復号し r を求め，さらに，r を変形（部分ビット反転など）した r' を求めた後で，鍵 K を用いて暗号化した結果 $Y = E_K(r')$ を検証者に送る．③検証者は，$r' = D_K(Y)$ が成立つことを検査する．

2.3 チャネル係数列の一致確認への応用

2.3.1 チャネル係数列の特徴と一致確認の課題

正規局間では，電波伝搬の可逆性に基づいて相関の高いチャネル係数列が取得される．なお，チャネル係数列の取得に当たっては，秘密鍵共有の場合と同様な手法を用いる．例えば，正規者間でチャネル係数の振幅に相違がある場合には，振幅の平均値で正規化した相対値で一致確認を行う．また，チャネル係数の波形の標本は，最大ドップラー周波数で規定される標本間隔で行われ，チャネル係数列が得られる．また，このチャネル係数列から元のチャネル係数の波形が完全に再現できる．

一般に，チャネル係数列の一致確認において，暗号化による秘密通信路を用いる場合，個々のチャネル係数を十分な量子化レベル数での量子化と符号化を行うことで，情報無漏洩で一致確認が可能である．しかし，公開通信路を用いた情報交換の場合，漏洩情報量を抑えた一致確認を個々のチャネル係数に対して行うことは一般に困難である．このため，個々のチャネル係数でなくチャネル係数列に対する一致確認を検討する．

さらに，チャネル係数列の一致確認においては，受信雑音に起因した誤差を考慮して誤差範囲内で一致判定を行う必要がある．ここで，識別閾値（誤差範囲）を予め適当に設定すると，適切な判定が難しく，妥当な一致確認が行えない．このため，チャネル係数列に対して受信雑音に起因する誤差の推定を事前に行った後で一致確認を行うことが望ましい．

誤差を許容したチャネル係数列の誤差範囲内での一致確認には，2.1 節に示す秘密鍵共有（鍵一致・確認）の手法の活用，2.2 節に示す共通鍵暗号に基づく相手認証の手法の応用が考えられる．また，新たな手法として個々のチャネル係数列のある現象を対象に，独自で希少な場合を探索して得られた，特異事象の活用が考えられる．

2.3.2 秘密鍵共有と相手認証を応用した一致確認

秘密鍵共有を応用したチャネル係数列の一致確認には，チャネル係数列を量子化して代表値と量子化誤差を求め，代表値に対応する記号と符号語（ビット列）を得る．ここで，量子化ステップは，一致確認の許容誤差と同程度で少し大きめに設定する．この符号語（ビット列）に対して秘密鍵共有を実施すれば，量子化誤差を無視したチャネル係数列の一致確認が行える．しかし，チャネル係数列に含まれる雑音量および一致確認の許容誤差が不明な場合に，量子化ステップの適切な設定が難しい．また，秘密鍵共有では鍵ビットの不一致訂正が行われるので，量子化ステップの境界付近の標本値がある場合に，誤差を拡大する可能性がある．さらに，この手法は量子化が行われているためアナログ秘密鍵の一致確認と趣旨が異なるとともに，従来のディジタルの秘密鍵共有に対する優位性がない．

一方，相手認証を応用したチャネル係数列の一致確認には，共通鍵を用いた２パス相手認証を参考とした手法が考えられる．その手法は，チャネル係数列をアナログ鍵とし，誤差を許容するアナログ鍵を用いた暗号化・復号を新たに考案し，その結果（平文）の一致からアナログ系列の一致を確認する手法である．この手法の要点は，誤差を含むアナログ鍵を用いた暗号化・復号の手法である．この場合，暗号文にも復号後の平文にも誤差が影響し，平文の一致確認の仕方が課題である．現在，これに直接関係する研究は全くない．しかし，電波伝搬特性の共有に基づく秘密通信方式は，見方を変えるとアナログ鍵を用いた暗号化・復号と捉えることができる．相手認証を応用した一致確認は，興味ある研究課題を含んでいるが，別の論文で取り上げることとし，ここでは取り扱わない．

3. チャネル係数列の特異事象に基づく一致確認

3.1 特異事象に基づく一致確認の原理

チャネル係数列の一致確認の新しい手法として，個々のチャネル係数列のある現象を対象として，独自で希少な場合を探索して得られた特異事象の活用がある．Fig. 5 にチャネル係数列の一致確認方式の構成を示す．この方式では，移動通信におけるフェージング伝送路の電波伝搬特性を双方向で測定することで，無線端末 A, B 間でチャネル係数列を取得する．また，チャネル係数列の数値情報を漏らすことなく，その誤差範囲（識別閾値）の推定を公開通信路を用いた情報交換により行う．

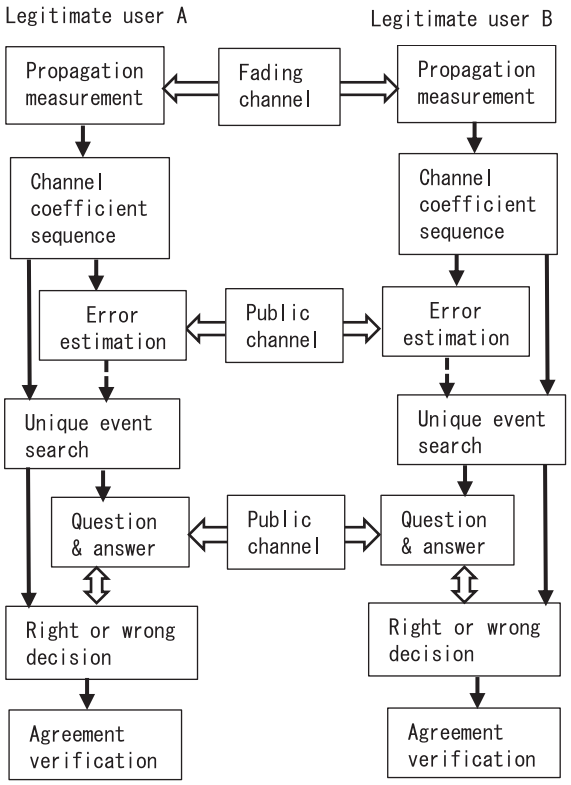


Fig. 5. Configuration of agreement verification system for fading variation.

次に，個々のチャネル係数列のある現象を対象として,独自で希少となる場合を識別閾値(誤差範囲)も考慮して探索して，特異事象を得る．ここで，注目する現象には，チャネル係数列の数値が直接に推定困難なものを選択する．また，公開通信路を用いて特異事象に関する質問･応答(情報交換)を行う．ここで，情報交換は，情報漏洩を極力抑えるため特異事象に合致（正）か否かの質問と応答とする．なお,質問の設定と質問･応答の順序は,「なりすまし」の排除のための工夫を行う．以上で得られた正否の応答結果と各無線端末で得られた正否との一致に基づいて，チャネル係数列の一致確認を行う．

この手法では，一致と判定すべき場合の識別見逃し率と不一致と判定すべき場合の誤識別率に対して識別閾値が適切であるかが課題となる．また，公開通信路の情報交換により漏洩する情報量の評価が重要となる．

3.2 公開情報による情報漏洩の評価

3.2.1 秘密鍵共有の情報漏洩の評価法

チャネル係数列の一致確認における情報漏洩について検討する前に，ディジタルの秘密鍵候補の一致確認における情報漏洩について検討する．L ビットの秘密鍵候補を $\boldsymbol{K}_L$ ，J ビットの公開情報を $\boldsymbol{C}_J$ とすると，結合エントロピーは，$H(\boldsymbol{K}_L,\boldsymbol{C}_J)=H(\boldsymbol{K}_L|\boldsymbol{C}_J)+H(\boldsymbol{C}_J)=H(\boldsymbol{C}_J|\boldsymbol{K}_L)+H(\boldsymbol{K}_L)$ の関係が成立つ．ここで，公開情報は秘密鍵候補から一意的に決定されるので，$H(\boldsymbol{C}_J|\boldsymbol{K}_L)=0$ となる．この結果，公開情報を知った条件付の秘密鍵候補のエントロピーは，

$$H(\boldsymbol{K}_L|\boldsymbol{C}_J)=H(\boldsymbol{K}_L)-H(\boldsymbol{C}_J) \tag{1}$$

となる．また，公開情報による漏洩情報量 I_{leak} は，

$$I_{\mathrm{leak}}=H(\boldsymbol{K}_L)-H(\boldsymbol{K}_L|\boldsymbol{C}_J)=H(\boldsymbol{C}_J) \tag{2}$$

となる．

ここで，$\boldsymbol{K}_L$ の各ビットの (0,1) の発生確率が 0.5 で各ビットが独立な場合に，$H(\boldsymbol{K}_L)=L$ となる．また，$\boldsymbol{C}_J$ の各ビットの (0,1) の発生確率が 0.5 で各ビットが独立な場合に，$H(\boldsymbol{C}_J)=J$ となる．その結果，漏洩情報量が $I_{\mathrm{leak}}=J$ となる．なお，$\boldsymbol{C}_J$ の各ビットの (0,1) の発生確率が p で各ビットが独立な場合に，$H(\boldsymbol{C}_J)=J\{-p\log_2 p-(1-p)\log_2(1-p)\}\leq J$ となる．また，$p\ll 1$ において，$H(\boldsymbol{C}_J)\ll J$ となる．

3.2.2 アナログ秘密鍵の一致確認における情報漏洩

チャネル係数列の一致確認の優劣評価のため，公開情報による情報漏洩の評価法を検討する．ここで，チャネル係数（アナログ値）のエントロピーは無限大であるが，２つのエントロピーの差は有限となる．このため，雑音の存在下での標本値を量子化した離散的な代表値又は，代表値に対応した記号（非負整数）から算出した相互情報量で近似できる．それゆえ，3.2.1 項と同様な取扱いが可能となる．

チャネル係数列の一致確認においては，公開通信路を用いて特異事象に関する正否の質問と応答が行われる．ここで，公開される質問が個々のチャネル係数に直接に関連しなければ，単なる質問事項は情報漏洩に無関係であり，合否 (1,0) の 1 ビットの情報が情報漏洩に関係する公開情報となる．次に，複数の質問と応答を繰り返すと，漏洩する情報量は式(2)より $H(\boldsymbol{C}_J)$ となる．この $\boldsymbol{C}_J$ の各ビットの (0,1) の発生確率 p を $p\cong 0$ （又は $p\cong 1$ ）に設定すると，漏洩する情報量を縮小することができる．ここで，$p\cong 0$ は，事象情報を満たす確率が非常に小さい（正規者以外は満たさない）特異事象であることを意味している．逆に，$p\cong 1$ は事象情報を満たす確率が非常に大きい（正規者以外は全て満たす）ことを意味している．

3.3 チャネル係数の波形と直線との交差の活用

3.3.1 絶対値の波形と直線との交差時刻の活用

チャネル係数列の一致確認には，対象とする現象の選択が独自で希少な場合の探索方法とともに重要である．チャネル係数列の数値を直接に推定困難な現象には，チャネル係数の絶対値の波形に対する同一レベル交差があり，その一対の交差時刻（又は，時間間隔）が確率的な事象となる．この事象は，複素のチャネル係数列から波形を再現し，絶対値を取って振幅変動を求め，適当に（ランダムに）最初の時刻 t_1 を適当に設定することで得られる．この場合，正規者間（無線端末 A と B 間）では複素のチャネル係数列の位相回転の補償や振幅値の補正を行うことなく，ほぼ同一の時刻対（t_1,t_2）を取得する．この事象は，チャネル係数の波形の形状に関係する事象であり，チャネル係数列の数値に直接関係しない点に特徴がある．

この同一レベル交差は全てのチャネル係数列に普遍的な現象であり，同一の交差時刻対を取得する事象が正規者以外でも起こる確率が無視できない．このため，単独の交差時刻対からは特異事象が得られない．しかし，多数の交差時刻対の積集合をとると，正規者以外でも積集合が一致する確率が低下するので，特異事象として利用できる可能性がある．

一方，端末 A と B で取得される交差時刻対は，受信雑音に起因する誤差の影響で多少不一致となるが，多数の時刻対の情報を公開通信路で交換することで，

不一致の程度が評価できる．また，チャネル係数の誤差と交差時刻対（又は，時間間隔）の誤差との関連性を求めることで，端末 A と B のチャネル係数列における受信雑音に起因する誤差の推定に有効である．

次に，チャネル係数列の数値を直接に推定困難な別の現象には，チャネル係数の絶対値の波形と直線との３点交差（以下，直線３点交差と呼ぶ）があり，その直線３点交差の時刻セット（時刻 t_1と t_3の標本値を結ぶ直線が時刻 t_2で交差）が確率的な事象となる．この事象も同一レベル交差時刻と同様な特徴があるが，直線３点交差の方が時刻（t_1, t_3）の設定の自由度が大きく，多様な事象が得られる．しかし，同一レベル交差時刻の場合と同様に，正規者以外でも交差時刻 t_2 が一致する確率を無視できない．このため，単独の時刻対からは特異事象が得られない．

3.3.2 実部・虚部の同時直線３点交差の活用

上記のチャネル係数列の絶対値に対する直線３点交差と同様な現象として，複素のチャネル係数の波形（実部と虚部）に対する直線３点交差がある．ここで，複素の場合に正規者間で同一の事象を得るには位相回転の補償が必要となる．また，実部と虚部に対して時刻 t_1と t_3の標本値を結ぶ直線がチャネル係数の波形と交差する時刻は，実部と虚部に対して t_{r2}, t_{i2} となり，一般に一致しない．

ここで，$t_{r2} = t_{i2}$ と一致する事象（実部と虚部の同時直線３点交差）は，個々のチャネル係数に独自で希少な特異事象であり，時刻 t_1と t_3を適切に設定しないと出現しない．得られた特異事象を複素平面と時間軸からなる３次元空間で表示すると，「複素のチャネル係数の螺旋曲線の時刻 t_1と t_3の標本値を結ぶ直線が時刻 t_3 で螺旋曲線と交差する」ことになる．このため，この事象は正規者間での位相回転の影響を受けず，位相回転補償が必要でない．

この特異事象の検出は，時刻 t_1 と t_3 の時間間隔を適当に設定し，両時刻を移動させながら交差時刻 t_{r2}, t_{i2} を観測し，両方が一致する場合を探索して得られる．また，事象例が不足する場合は，時間間隔の設定を変更して探索を継続する．

次に，得られた特異事象に基づいて，「複素のチャネル係数の実部と虚部の波形において，時刻 t_1と t_3の標本値を結ぶ直線が同一時刻で実部と虚部の波形と交差する」の質問に対して，正否の応答を行う．ここで，3.1 節で述べたように「なりすまし」の危険性があるので，その排除のための配慮と工夫が必要である．そこで，「なりすまし」を排除するため，①正解が正否となる質問をランダムに選択する，②正の応答には交差時刻を質問する，③質問者・応答者を順次交代するなどの工夫を行う．

3.3.3 提案手法の実現性と要検討の諸特性

上記を用いた一致確認の実現性は，特異事象の発生頻度が十分かに依存する．また，一致確認を行う判定閾値が適切に設定可能かにも依存する．そこで，実部・虚部の同時直線３点交差の現象の探索をシミュレーションで実施した．はじめに，チャネル係数列からチャネル係数の波形を再生した．Fig. 6 に雑音なし，SN 比が 30 dB と 15 dB のチャネル係数（実部，虚部）の波形を示す．図において雑音がなしと SN 比が 30 dB のチャネル係数はほぼ一致しているが，SN 比が 15 dB では不一致が顕著となる．

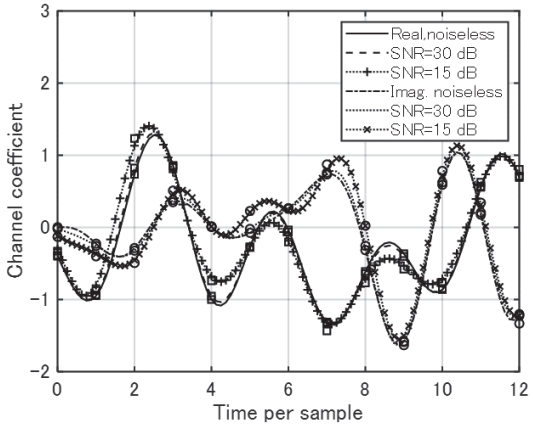
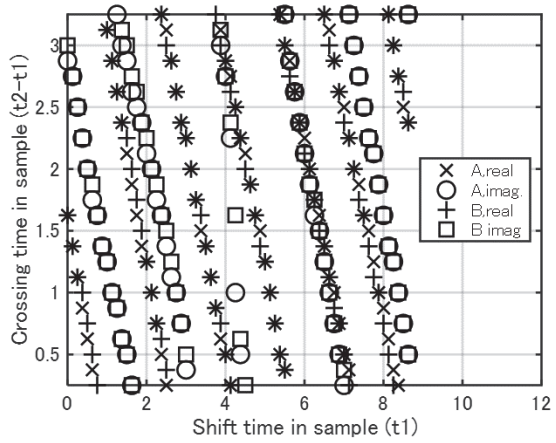


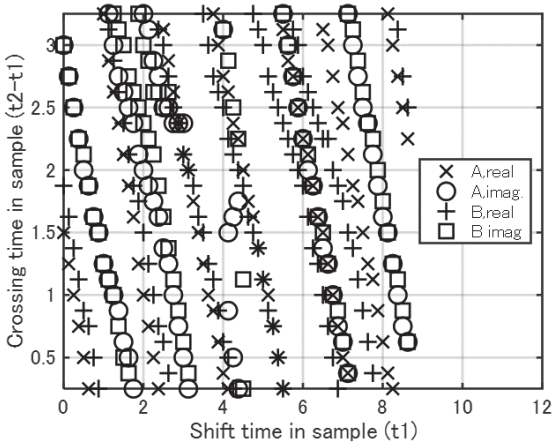
Fig. 6. Real and imaginal part of channel coefficient in the case of no noise and SNR=30, 15 dB.

次に，Fig. 6 に示すようなチャネル係数の波形に対する直線３点交差時刻（t_1, t_2, t_3）を Fig. 7 に示す．図において，時間間隔 $(t_3 - t_1) = 3.5$ は固定で，横軸は交差時刻 t_1 で，縦軸は交差時刻差 $(t_2 - t_1)$ である．Fig. 7 の×印と＋印は端末 A と B における実部の交差時刻，○印と□印は端末 A と B における

虚部の交差時刻を示している．また，×印と○印の重なり，および＋印と□印の重なりは，端末 A と B における実部と虚部の交差時刻 t_{r2}, t_{i2} が一致，即ち，同時直性３点交差の特異事象を示している．



(a) SNR=30 dB.



(b) SNR=15 dB.

Fig. 7. Crossing time for real and imaginal part of channel coefficient with time interval (t_3-t_1) of 3.5.

Fig. 7 (a)の SN 比 30 dB の場合，×印と＋印の重なり（又は，○印と□印の重なり）が多く，実部（又は，虚部）の交差時刻が端末 A と B でよく一致することが分かる．また，実部と虚部の交差時刻が一致する同時直線３点交差は発生頻度が多少あるが，端末 A と B で発生時刻が若干相違する場合がある．一方，Fig .7 (b)の SN 比 15 dB の場合，実部（又は，虚部）の交差時刻が端末 A と B であまり一致しないことが分かる．また，同時直線３点交差は発生頻度が激減し，端末 A と B で発生時刻の相違が顕著となる．この結果，同時直線３点交差の識別には，雑音による誤差を考慮した手法が重要となる．

次に，検討した一致確認法の有効性は，以下のような諸性能に依存する．諸性能には，識別閾値，特異事象の発生頻度，漏洩情報量，正規者の識別見逃し率，盗聴者の誤識別率などがある．このうち，一致確認の性能に直接関係する重要なものに，SN 比に対する識別見逃し率と誤識別率特性がある．なお，この誤識別率は，チャネル係数列が高相関の場合でも小さいことが必要となる．これらの諸特性に基づいて一致確認法を改良することが今後の課題となる．

3.4 大小判定結果の積集合による実現法

3.4.1 チャネル係数列の大小判定結果の活用

チャネル係数列の数値を直接に推定できない事象として，チャネル係数列の要素（チャネル係数の実部と虚部）の大小判定の活用がある．この手法は，多数の一対（２個で一組）のチャネル係数列の要素を選択し，一対の要素の大小判定の結果（正しい場合に１）の積集合を特異事象とする．チャネル係数列の数が N の場合，一方の要素の重複を許容すれば $N(2N-1)$ 個の一対の要素が選択候補となる．ここから，独立な M 個の一対の要素を選択すると，端末 A と B では個々の大小判定の結果の積集合が１となる確率が非常に高い．一方，盗聴者が取得するチャネル係数列が正規者のものと独立な場合，大小判定の結果が１となる確率は 1/2 であり，積集合が１となる確率は 2^{-M} となる．ここで，$M = 10, 20$ に対して，$2^{-M} \approx 10^{-3}, 10^{-6}$ となり，M を十分に大きくすれば，ほとんど発生しない特異事象となる．

次に，独立な多数の一対の要素の選択方法を検討する．はじめに，独立でない一対の要素が選択される例を示す．$N = 2$ の場合，$2N$ の要素を大きい順に (A, B, C, D) とすると，$N(2N-1) = 6$ の大小比較の組合わせ$\{(A>B), (A>C), (A>D), (B>C), (B>D), (C>D)\}$がある．ここで，$\{(A>B), (B>C), (C>D)\}$が与えられると，他の$\{(A>C), (A>D), (B>D)\}$は必然的に成り立つ．また，組合せの数が $2N-1=3$ と小さくなる．一方，大きな (A, B) と小さな (C, D) との間の総当たりにより，$\{(A>C), (A>D), (B>C), (B>D)\}$と独立な組合せが得られ，その数が $N*N=4$ となる．同様な

手法を用いることで，独立な一対の要素の選択が可能であり，Nの増加に対して組合せの数を $N*N$ と大きく設定できる．

3.4.2 一対の要素の選択における留意点

ここでは，多数の一対のチャネル係数列の要素の選択における留意点を示す．留意点の一つは，受信雑音による正規者間（端末AとB）での大小判定の不一致である．このため，誤差を考慮した一致確認を行わないと識別見逃し率が増加する．この対策には，事前に取得した識別閾値（誤差範囲）を用いて，大小判定する一対の要素間の差を識別閾値より大きく設定する（又は，一対の要素間の差が識別閾値より小さいものを除外する）ことが有効である．なお，識別閾値には各種の取得法が考えられるが，一対の要素間の差が小さい集合に対する正規者間の大小判定の不一致率から推定する手法もある．

また，別の留意点は，正規者と盗聴者のチャネル係数が高相関となる場合における誤識別率の増加の対策である．この対策には，一対の要素の組み合わせの中に，要素間の差が小さいが識別閾値以上となるものを含めることが有効となる．このため，識別見逃し率とチャネル係数の高相関による誤識別率の許容値に基づいて要素間の差を設定する必要がある．

次に，一対の要素の選択に当たっては，情報漏洩の対策も重要である．すなわち，大小関係の情報から大まかな数値が推定される危険性に留意する必要がある．例えば，各要素を数値の大小で二分して，大小のそれぞれから一対の要素を選択すると，大まかな数値（上位１ビット）が容易に推定できる．この対策の一つは，要素を数値の大きさで複数（L個）の集合に区分けして，それぞれの集合内で一対の要素を選択することである．なお，この場合に一対の組合せの数が $L(2N/L)^2 = 4N^2/L$ となり，Lの増加とともに減少する問題がある．

別の情報漏洩の対策は，個々の要素の数値を推定困難とすることである．具体的には，複素のチャネル係数に一方向性の変換（例えば絶対値）があり，この変換を行った場合に実部と虚部を個々に推定できない．また，別の手法は，チャネル係数値でなくチャネル係数列の全体に関係する数値列に変換することである．この変換に離散フーリエ変換や離散ウオルシュ・アダマール変換がある．しかし，この変換は可逆な変換であるため，可逆とならない一方向性の変換（例えば，絶対値）を併用すると，推定がほぼ困難となると思われる．

検討した一致確認法の有効性は，識別閾値，漏洩情報量，正規者の識別見逃し率，盗聴者の誤識別率などの諸特性に依存する．これらの諸特性に基づいて一致確認法を改良することが今後の課題となる．

4. まとめ

移動通信路におけるチャネル係数列に対して，誤差を考慮した一致確認を盗聴者に秘密裏に確認する手法を検討した．はじめに，秘密鍵共有や共通鍵に基づく相手認証など従来技術を応用した手法を紹介し，従来技術の応用の課題を明らかにした．一方，アナログ秘密鍵に特化した新手法として，チャネル係数列に独自な特異事象に基づく一致確認の原理を示し，公開情報による情報漏洩が十分に小さいことを明らかした．次に，特異事象の一例として，複素チャネル係数の波形と直線との３点交差を示し，それに基づく一致確認の実現性とその課題を明らかにした．また，別の特異事象の例として，チャネル係数の大小判定結果の積集合を示し，その実現性と課題を明らかにした．

今回の基礎検討では，検討した手法の性能・特性に関して，識別閾値，特異事象の発生頻度，漏洩情報量，識別見逃し率，誤識別率などを評価していない．今後の課題は，諸特性に基づいて提案手法の改良を行うと共に，その有効性を定量的に評価することである．

参考文献

1) A. D. Wyner, “The Wired-tap Channel”, *Bell Syst. Tech. J.*, **54**, 1355-1387 (1975).

2) U. M. Maurer, “Secret Key Agreement by Public Discussion from Common Information”, *IEEE Trans. Inform. Theory*, **39**[3], 733-742 (1993).

3) U. M. Maurer, and S. Wolf, “Unconditional Secure Key Agreement and the Intrinsic Conditional Information”, *IEEE Trans. Inform. Theory,* **45**[2], 499-514 (1999).

4) J. E. Hershy, A. A. Hassan, and R. Yarlagadda, “Unconditional Cryptographic Keying Variable Management”, *IEEE Trans. Commun.*, **43**[1], 3-6 (1995).
5) A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, “Cryptographic Key Agreement for Mobile Radio”, *Digital Signal Processing*, **6**, 207-212 (2000).
6) K. Zeng, “Physical layer Key Generation in Wireless Networks: Challenges and Opportunities”, *IEEE Comm. Magazine,* **53**[6], 33-39 (2015).
7) S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel”, *Proc. ACM MobiCom*, 128-139 (2008).
8) 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”, 電子情報通信学会論文誌(A), **87**[10], 1320-1328 (2004).
9) B. Azimi-sadjadi, A. Kiayias, A. Mercado, and B. Yener, “Robust Key Generation from Signal Envelopes in Wireless Networks”, *Proc. ACM conf. Computer and Comm. Security* (*CCS*), 401-410 (2007).
10) S. Jana, S. Premnath, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy, “On Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environment”, *Proc. ACM MobiCom*, 321-332 (2009).
11) 青野智之, 樋口啓介, 大平孝, 小宮山牧児, 笹岡秀一, “エスパアンテナを用いた IEEE802.15.4 無線秘密鍵共有システム”, 電子情報通信学会論文誌(B), **88**[9], 1801-1812 (2005).
12) T. Aono, K. Higuchi, T. Ohira, T. Komiyama, and H. Sasaoka, “Wireless Secret Key Generation Exploiting Reactance-domain Scalar Response of Multipath Fading Channel”, *IEEE Trans. Antenna Propag.*, **53**[11], 3776-3784 (2005).
13) C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, “Generalized Privacy Amplification”, *IEEE Trans. Inform. Theory*, **41**[6], 1915-1923 (1995).
14) G. Brassard and L. Salvail, “Secret Key Reconciliation by Public Discussion”, *Advances in Cryptlogy-EUROCRY PT' 93, Lecture Note in Computer Science*, **765**, 410-423 (1994).
15) G. Assche, J. Cardinal, and N. Cerf, “Reconciliation of a Quantum-distributed Gaussian Key”, *IEEE Trans. Inform. Theory,* **50**[2], 394-400 (2004).
16) M. Bloch, A. Thangaraj, S. McLaughlin, and J. Merolla, “LDPC-based Gaussian Key Reconciliation”, *Proc. 2006 IEEE Inform. Theory Workshop* (*ITW'*06), 116-120 (2006).
17) 笹岡秀一, “無線通信におけるガウス性相関情報に基づく秘密鍵共有方式の秘密鍵容量―（その２）移動通信路モデル―”, 同志社大学ハリス理化学研究報告, **57**[1], 47-56 (2016).
18) 笹岡秀一, 岩井誠人, “無線ネットワークにおける電波伝搬特性に基づくグループ秘密鍵共有に向けた鍵不一致訂正の検討”, 電子情報通信学会信学技術研究報告, RCS2019-242, 31-36 (2019).
19) 岡本竜明, 山本博資, 現代暗号, (産業図書, 東京, 1997), 151-162.
20) 電子情報通信学会編, 情報セキュリティハンドブック, (オーム社, 東京, 2004), 17-18.