No.52 2004 年 10 月 13 日発行

情報理論とその応用学会ニューズレター

博士論文特集号

General Construction Methods of Secret Sharing Schemes and Visual Secret Sharing Schemes

岩本貢 (電気通信大学)

A *secret sharing* (SS) scheme is a method to encrypt a secret S into n pieces called *shares*, each of which has no information of the secret, but S can be decrypted from some specified collection of shares. For example, in (k, n)-*threshold* SS schemes, any k out of n shares can decrypt S while $k-1$ or less shares do not leak out any information of S. The (k, n) threshold access structure can be extended to a *general access structure*, which is specified by the families of qualified sets and forbidden sets, such that a qualified set can decrypt the secret, and a forbidden set does not leak out any information of the secret. SS schemes are one of the most important techniques for secure data storage, and hence, many researches have been devoted to this subject.

The decoding of ordinary SS schemes is implemented by a computer. But, the decoding of *visual secret sharing* (VSS) schemes is realized based on human eyesight by peering at several

shares stacked up. In this thesis, we propose some new efficient construction methods of SS and VSS schemes, which are treated in Part I and Part II, respectively.

We aim in Part I to construct efficient ordinary SS schemes. First, we derive the lower bounds of coding rates for *ramp* SS schemes. Ramp SS schemes are extensions of ordinary SS schemes, which we call *perfect* SS schemes in order to distinguish them from ramp SS schemes. Hence, our results include some known results of coding rates for prefect SS schemes as special cases.

In order to derive the lower bounds of coding rates in ramp SS schemes, we classify shares into three categories called *super-additive*, *additive*, and *sub-additive*. Then, we clarify that the coding rates for sub-additive shares are less efficient than the other two types of shares. We also derive the lower bounds of coding rates for super-additive and additive shares.

In previous works for the lower bounds of coding rates for perfect SS schemes, they are often classified into two categories called *ideal* or *non-ideal* SS schemes, and the properties of access structures are investigated in each category. In this thesis, we extend the notion of ideal perfect SS schemes to define *well-realized* ramp SS schemes. By evaluating the lower bounds of coding rates for ramp SS schemes, we analyze what kind of access structures cannot be well-realized as ramp SS schemes. These results are extensions of known ones for non-ideal perfect SS schemes and ramp SS schemes with general access structures.

Next, we propose a new method to construct SS schemes with general access structures in Part I. It is well known how to construct efficient (k, n)-threshold SS schemes although no efficient construction method is known for arbitrarily given general access structures. The *cumulative map*, which is a special case of *multiple assignment map*, is a known simple construction method of SS schemes with general access structures. But, it is generally inefficient, especially in the case that access structures are close to (k, n)-threshold access structures. In this thesis, we design the *optimal* multiple assignment maps using integer programming. The coding rate obtained by our method is optimal in the multiple assignment maps, and hence, it is more efficient than the cumulative map. Furthermore, since the proposed construction is very simple, it can easily be applied to SS schemes with general ramp and/or incomplete access structures.

In Part II, we propose some construction methods of VSS schemes, which are superior in the viewpoint of the quality of decrypted images and the generalities of access structures.

In VSS schemes, each pixel of a decrypted image consists of a set of *subpixels* which is represented by a *basis matrix*. In previous works, it was difficult to derive basis matrices since they are combinatorially defined. Hence, many known studies on VSS schemes treated only black-white (BW) binary secret images, and there are few studies of VSS schemes for color secret images because they must deal with more combinations of colors in basis matrices compared with the case of BW binary secret images. Based on such backgrounds, a simple construction method was proposed to derive VSS schemes with color images called *algebraic* construction, which does not use the combinatorial methods. It is known that the algebraic construction can realize an efficient VSS scheme, but it could not be applied to VSS schemes for BW binary secret images. In order to improve such defects, a modified algebraic construction was proposed. However, the performance of the modified method has not been studied. In this thesis, we clarify that the modified algebraic construction can attain the *optimal* (n, n)-threshold VSS

schemes for gray-scale images, and we also derive the basis matrices for the optimal (n, n)-threshold VSS schemes for gray-scale images.

We also consider VSS schemes for plural secret images in this thesis. We note that the known VSS schemes for plural secret images can treat only BW binary secret images. Furthermore, some definitions of such VSS schemes are not accurate in the sense of security. In other words, decrypted images may leak out some information of the other decrypted images in such VSS schemes. Hence, we carefully define the security condition of VSS schemes for plural secret images. We also propose the construction methods of the secure VSS schemes that satisfy such security conditions. Furthermore, we note that the proposed VSS scheme can treat color secret images with shades, and hence, our VSS scheme includes most of previous VSS schemes as special cases.

学位取得大学: 東京大学
電気通信大学大学院情報システム学研究科
岩本貢
E-mail: mitsugu@hn.is.uec.ac.jp

Copyright Protection System Using The Fingerprinting Scheme

金美羅 (情報セキュリティ大学院大学)

The digital information revolution has brought profound changes in our society and our lives. The many advantages of digital information have also generated new challenges and new opportunities for innovation. Broadband internet and wireless network environments which have made considerable progress in recent years offer many opportunities to deliver and to exchange information. The fair uses of digital contents as well as the efficient delivery of digital contents to end users are important topics. This thesis discusses issues regarding copyright protection systems using fingerprinting schemes for preventing illegal redistribution of digital contents.

First, we deal with c-secure codes in fingerprinting schemes. If a pirate copy appears, c-secure codes allow the owner of a copied digital content to trace the source of the illegal redistribution under collusion attacks. Most past proposed codes failed to obtain a good efficiency, i.e. their codeword length was too large to be embedded into digital contents. In this thesis, we propose a construction method of c-secure CRT codes based on polynomials over finite fields and show that the codeword length of our construction is shorter than that of previous schemes. We also discuss the influence of random errors on the traceability of the proposed construction.

Secondly, we deal with the distribution problem of a large number of fingerprinted contents. In order to solve this problem, we present a new model having the following features: (1) No watermarking algorithm in decoders; (2) Dynamic fingerprinting; and (3) Dynamic revocation. The proposed model employs the fact that ability to decrypt implies a certain kind of fingerprint. We also propose new revocation schemes suitable for a half-rate dynamic revocation to efficiently realize the proposed model.

Finally, we study the problem of watermarking software. We propose a new definition of software watermarking schemes (weaker than the most used definitions present in the literature) called differing-input software watermarking and study

its feasibility under the assumption that differing-inputs obfuscations and one-way functions exist.

学位取得大学: 東京大学
E-mail:mira@iisec.ac.jp

マルチメディア通信に適した高効率な交換システム及び端末の移動性に対応した網制御法に関する研究

萬代雅希 (静岡大学)

モバイルインターネット技術が進展する中，端末の移動を考慮した環境下で，ネットワークの大容量化，高速化および厳しい通信要求品質に対応する必要性が高まっている．ユーザのトラヒックは，確実性の要求されるデータや，即時性の要求される動画像のように，満たすべき要求品質が異なる．確実性の要求されるデータの場合，上位層での再送処理を行うため，交換システムにおける情報損失や遅延がスループットを劣化させる．また，上位層にて再送処理を行わないリアルタイムトラヒックの場合, ネットワークにおける情報損失がそのまま通信品質に影響するため, 交換システムの高効率化だけでなく, 端末の移動によるハンドオフ期間中の情報損失を低減することは重要な研究課題である．

本研究では, 端末の移動性を考慮したマルチメディア通信ネットワークを実現するために，ATM 及び WDM を用いた交換システムと Mobile IP を用いた網制御法を提案し，理論解析と計算機シミュレーションにより，その有効性を示している．以下に具体的内容を示す．

第 1 章は序論であり，研究背景や目的について述べている．

第 2 章は入出力バッファ型 ATM スイッチにおいて低セル棄却率及び低システム遅延を達成可能なスイッチ構成法について述べている．入出力バッファ型スイッチにおいては, 複数のセルが同一の出力ポートを目指す HOL ブロッキングによりセル棄却率特性が劣化してしまう．本章では低セル棄却率及び低システム遅延を達成するために，二つの Speedup Factor を用いた入出力バッファ型 ATM スイッチを提案し，計算機シミュレーション及び理論解析結果より，提案スイッチが遅延特性をほとんど劣化させずにセル棄却率特性を改善できることを示す．

第 3 章ではマルチキャストトラヒックにおいて高スループット及び低システム遅延を達成可能な WDM を用いた交換システムにおけるチャネル割り当てプロトコルについて述べている．目的アドレスの重複が頻発するマルチキャストトラヒック環境下では，スループット及びシステム遅延特性が劣化してしまう．本章では高スループット及び低システム遅延を達成するために，目的アドレスの重複したユーザに対して優先制御を施すチャネル割り当て方式を提案し，計算機シミュレーション及び理論解析結果より，提案方式がスループット及びシステム遅延特性を改善できることを示す．

第 4 章では Mobile IP において低ハンドオフレイテンシを達成可能な網制御法について述べている．端末が移動しながらインターネットにアクセスする環境下で再送処理の許容されないリアルタイムトラヒックを扱う場合，ハンドオフレイテンシ特性の劣化を防ぐことは重要な課題である．本章では低ハンドオフレイテンシ特性を実現するために，移動端末の位置情報を用いた新たな網制御法を提案し，計算機シミュレーション及び理論解析結果より，提案方式が有線及び無線チャネルのオーバーヘッドの増加を抑えつつハンドオフレイテンシ特性を改善できることを示す．

第 5 章は結論であり, 本研究で得られた結果を総括している．

学位取得大学: 慶應義塾大学
静岡大学 情報学部 情報科学科助手

432-8011 浜松市城北 3-5-1
Phone/Fax: 053-478-1492
E-mail: bandai@cs.inf.shizuoka.ac.jp

ネットワークシステムにおけるサイバーテロ監視技術に関する研究

竹森敬祐 (KDDI 研究所)

近年、世界的な規模で広がりをみせるサイバーテロの脅威が高まっている。2001 年 7 月には CodeRed と呼ばれるコンピュータウィルスが、2003 年 1 月には Slammer ウィルスが、同年 8 月には Blaster ウィルスが現れ、多数のホストがこれらに感染していまい、インターネットが一時的にサービス停止状態に陥るなどの影響が出た。このようなサイバーテロの脅威を最小限に抑え、安心・安全なネットワークシステムを提供するためには、各地のネットワークシステムの状態を的確に監視し、セキュリティログ等による未知の攻撃情報の収集を行い、これらの攻撃情報から、いちはやく脅威を分析して対策を促すセキュリティ監視センタ (SOC: Security Operation Center) の構築が重要な課題となっている。

本論文では、ネットワーク上で発生するコンピュータへの侵入攻撃やサービス不能攻撃等のサイバーテロを即座に発見し、その挙動の把握を可能とする SOC の運用に必須となる要素技術として、上記のシステムリモート監視、攻撃情報収集、セキュリティログ分析についてそれぞれ新たな手法を提案している。提案方式のシステム実装および評価実験を通じて、これまで検知できなかった攻撃やその被害を迅速に把握できることを明らかにし、提案方式の有効性を提示する。攻撃を的確に把握することは、ネットワークシステムの安定稼動に寄与できる。以下に具体的内容を示す。

第 1 章では、本研究の背景となるサイバーテロの検知手法に関する従来研究を概観し、本研究の目的と位置付けを明確にしている。

第 2 章では、Web サーバが管理するホームページ用のファイルをリモートから監視することで、改竄攻撃やネットワークサービス停止攻撃による異常を検知できる Web サーバリモート監視システムを提案している。本提案システムでは、リンクページを辿ることにより監視対象となるファイルを自動的に抽出する機能と、ファイルのヘッダ情報やハッシュ値の変化に注目して改竄を判定する機能を有しているため、運用者の負担がほとんど無い状態において高い確率で Web サーバに対する攻撃を検知できる。大規模監視の実現性検証のために、インターネット上での監視処理速度に関する実験を行い、ネットワークへ与える負荷を軽減しつつ、局所的な輻輳に影響を受けない安定したリモート監視システムであることを定量的に明らかにしている。

第 3 章では、未知の攻撃情報を収集するためのシステムとして、侵入検知システム（IDS: Intrusion Detection System）と連携して、不審な通信コネクションを本来のシステムからおとりシステムへと切替えて行動ログを収集するトラップ型おとりシステムの切替え手法を提案している．本切替え手法は，本来のシステムとおとりシステムの通信状態の同期をとっておくことで，切替え処理の高速性と通信シナリオの継続性を確保でき，侵入者におとりシステムの存在を気付かれない方式となっている。そして FTP サービスならびに Web サービスへの実装を行い，実験用ネットワークを用いて評価を行った結果、侵入者に気付かれないレベルの高速な切替えを実現していることを確認している．このシステムにより、本来のサービスを提供しつつも侵入者の挙動・攻撃手法を容易に収集することが可能となる。

第 4 章では、広域ネットワークの各地に設置された IDS から出力される攻撃検知ログを統合管理し

て，異常なイベントを客観的に抽出する IDS ログ分析支援システムを提案している．本システムでは、ログに含まれる各種イベントの異常性について順位付けし、長期間のイベント傾向を比較対象として短期間のイベントの発生状況から、異常性を客観的な数値で評価する分析手法を提案している。各地で運用されている IDS の攻撃検知ログを用いて評価を行った結果，多量のイベント情報の中から、従来では発見が困難であった異常なイベントを特定できること、検証不要なイベントを排除できることを確認している。これにより、広域ネットワークを監視する運用者の作業負担を大幅に軽減すると共に、ネットワーク上で発生している攻撃の挙動を容易に把握することが可能となった。

第 5 章は結論であり、本論文の内容を総括している。

学位取得大学: 慶應義塾大学
E-mail: takemori@kddilabs.jp

Highly Efficient Spread Spectrum Techniques and Software Defined Radio Architecture for Fourth Generation Mobile Communications

庄納崇 (インテル)

近年の携帯電話や無線 LAN などのモバイル通信市場の持続的な成長は，インターネットの同様の発展と共に，第 4 世代（4G）移動通信の到来を早めると考えられる．4G 移動通信では，第 3 世代（3G）移動通信を補完し，いつでも，どこでも，広い範囲の情報やサービスにシームレスにアクセスし，大容量データのやりとりが可能になることが期待される．よって，4G のインフラは，ユーザがユーザ自身の嗜好に応じて任意のアプリケーションや環境を選択できるように，共通のプロトコルとしてインターネットプロトコル（IP）を用いた様々なネットワークを統合したものになることが想定される．また，モバイル通信の潮流を踏まえると，4G では，更に高速・広帯域な複数の異なる無線通信システムやネットワークをシームレスに渡り歩くことが必須になると考えられる．

本論文は，4G の実現に向けた実現すべき最も重要な無線通信技術である，広帯域無線アクセス技術とソフトウェア無線（SDR）に焦点を当てて検討を行っている．まず，広帯域無線アクセス技術に対しては，要素技術となる直接スペクトル拡散（DS/SS）通信における擬似雑音（PN）符号追跡ループの特性改善，及びマルチキャリア符号分割多元接続（MC-CDMA）におけるコード間干渉（ICI）の解析とそれに基づく拡散符号の制御に関して詳細な検討を行っている．また，SDR 技術に対しては，無線通信システムの環境に応じて，変復調方式や符号化方式のみならず無線通信方式そのものをダイナミックに変更するという方式ダイバーシチを重要なアプリケーション技術として提案し，特性解析を行うとともに，SDR の実装に関しても詳細な検討を行っている．

第 1 章では，携帯電話と無線 LAN の技術的な発展経緯，及び将来の無線通信の特徴について概説している．また，DS/SS，MC-CDMA，SDR などの本論文に関連する技術について，各技術分野の動向，過去の研究成果の課題をまとめた上で，本研究の新規性や有効性を述べている．

第 2 章では，航空機対地上基地局間通信に DS/SS 通信方式を適用することを想定して，位置推定のためのカルマンフィルタにより PN 系列の伝搬遅延を推定する機能と修正符号追跡ループ（MCTL）を結合した，より同期追跡性能の高い安定な符号追跡ループを提案し，計算機シミュレーションにより，提案方式が追跡誤差の軌跡と追跡ジッタ特性の観点から，従来の MCTL 単独のシステムに比べて同期追跡性能が高いことを示している．

第 3 章では，まず，MC-CDMA の周波数選択性レイリーフェージングチャネルにおける ICI を定量的に評価している．周波数選択性によるサブキャリア間の相関特性を考慮し，ICI の定量的評価量である希望波対干渉波電力比（DUR）の理論式を導出し，8 チップの Walsh-Hadamard 符号を用いた計算機シミュレーションによって，その妥当性を確認している．また，アップリンクが等利得合成（EGC），直交復元合成（ORC），最大比合成（MRC）の 3 種類，ダウンリンクが EGC と MRC の 2 種類の場合において理論解析を行い，拡散符号の組合せによって DUR に偏りが生じることを明らかにしている．次に，周波数選択性レイリーフェージングチャネルにおけるアップリンク MC-CDMA の多元接続性能を最大化する最適拡散系列が直交符号であることを明らかにしている．最後に，拡散符号の組合せによる DUR の偏りの性質を利用して，周波数選択性フェージングチャネルにおける同期 MC-CDMA システムの新しい拡散符号割当法を提案し，多元接続干渉（MAI）が低減可能であることを示している．

第 4 章では，SDR において，無線通信システムの環境に応じて，変復調方式や符号化方式のみならず無線通信方式そのものをダイナミックに変更するという方式ダイバーシチのコンセプトを提案し，3 種類の異なる無線通信システムからなる具体的なシミュレーションモデルを用いて，受信レベル，伝送速度，チャネル容量の 3 つのサービス品質（QoS）パラメータを用いた方式ダイバーシチのアルゴリズムを提案し，その効果を明らかにしている．

第 5 章では，PHS と IEEE 802.11 無線 LAN に対応した SDR プロトタイプについて，無線 LAN を実現するために採用した SDR のソフトウェアアーキテクチャに関して述べている．本プロトタイプは，CPU，DSP，FPGA から構成されるマルチプロセッサアーキテクチャを採用し，IEEE 802.11 フレームの送受信応答処理を行う機能配分として，物理層のフレーム送受信処理を DSP，MAC 層のプロトコル処理を CPU，更に高速な信号処理を FPGA に割り当てている．また，規格が要求するマイクロ秒オーダの送受信応答処理を実現するための課題に対する解決法を提案し，本プロトタイプの無線 LAN モードの実機での評価結果を示し，有効性を明らかにしている．

第 6 章は結論であり，本研究で得られた結果を総括している．

学位取得大学: 慶應義塾大学
E-mail: takashi.shono@intel.com

Identification and Detection Technologies for a Universal Receiver in Software Defined Radio

梅林健太 (Oulu 大学)

近年の無線通信分野における 1 つの特徴として多様性が挙げられる。無線機の使用目的に着目をした場合においても、使用目的別に見た場合においても、その多様性は明白である。

例えば、携帯電話を取り上げたときにその方式は各国による違いはもちろん、日本国内を見渡しても Personal Digital Cellular (PDC), Personal Handy phone System (PHS), Interim Standard-95 (IS-95), CDMA2000 WCDMA など多岐に渡る。一方で、身近な無線システムを取り上げてみても、以前は TV, ラジオが主であったのに対して、携帯電話をはじめ無線 LAN, Bluetooth, 衛星、及び地上波によるディジタル放送など、多様化されている。これらの無線通信における多様化に対して、Software Defined Radio (SDR) が注目され、研究がされてきている。従来の無線機は 1 つの無線アプリケーション、システムを 1 つの固定化されたハードウェアで実現しているために、ユーザが複数の無線通信方式

を使いたい場合には、複数個のハードウェアが必要となっている。それに対して、SDR では無線機の構成要素をプログラマブルデバイスで構成する部分を増やすなどの手法によって、無線機を再構成可能としている。これによって、無線機構成をソフトウェアの切り替えにより、1 つのハードウェアで複数のシステムを持たせることが対応可能となる。また、無線機中の 1 つのモジュールに着目したときにも、最適なモジュールの仕様はチャネルモデル、トラフィック、通信方式など時間的、地理的に変動する環境に依存する。この意味するところは、従来の無線機では常に最適なアルゴリズムをモジュールに実装することは困難であるのに対して、SDR では先と同様に無線機の再構成により常に最適なアルゴリズムを実装することが可能である。このように SDR は再構成可能である点、それとそれに伴う環境への適応性という大きなメリットを持っている。一方でこのような SDR の研究分野のひとつとしてユニバーサル無線機という考え方があり、研究をされてきている。本論文でもこの分野に注目をした。

ユニバーサル無線機の目指すところには究極的な柔軟性と適応性であり、そのために 3 つの大きな特徴があり、さらに、それらは、3 つの課題を伴っている。つまり、それらの特徴を実現することが大きな目標となるわけである。1 つ目は環境に対する適応性である。ユニバーサル無線機では、環境を他の補助を必要とせず自律的に推定可能とし、その結果、その時々における最適な構成を実現する。これにより、常に最適な無線機構成を可能とする。2 つ目は、機能切り替えの受信機におけるブラインド識別である。送信機が、環境に応じて送信信号のスペックを最適に切り替えた場合に、受信機がそのことを識別する必要がある。その識別を実現するために 2 つのアプローチがある。1 つはノンブラインドによるアプローチ、もうひとつはブラインドアプローチである。本論文では後者を選択した。ここで、ブラインドの意味するところは、補助情報があるか無いかを意味する。すなわち、送信機がスペック切り替えを行った際に、その切り替え情報を何らかの補助情報で伝える手法がノンブラインドに相当し、補助情報を用いずに受信機がブラインド識別アルゴリズム等を用いて識別する手法がブラインドの手法に相当する。ユニバーサル無線機が柔軟性を重要な要素と捉えていることから、ここでは、ブラインドの手法に注目をしている。3 つ目は、ユニバーサルなアルゴリズムである。これは、従来、ソフトウェア無線機では機能を切り替えるのに対して、なるべく、1 つのアルゴリズムで複数のケースに対応できることが望ましいという発想から出ている。また、これは完全なユニバーサルを狙っているのではなく、なるべく共用部分を生み出すことが目的となっている。従来のユニバーサル無線機に対する研究では、2 番目の特徴に注目したものが多く、特に、変調方式識別技術を用いた研究が盛んに行われている。本論文においても、他者との比較のしやすさなどを考慮して、同様にユニバーサル無線機における変調方式識別技術に着目をする。

従来の変調方式識別に対する研究では応用目的が軍事、または電波監視などのように非民生を意識しているケースが多い。この場合は、多種類の変調方式が必要となり、また、膨大な計算量が必要となる。一方で、SDR の研究が盛んになるのと同時期に出てきた変調方式識別に関する研究は非民生のみならず、マルチモード型の無線機に対して、この技術が利用できることに言及している。変調方式識別としての特徴は、変調方式の種類を限定していること、計算量を抑えること、さらに識別のみならず他の機能との整合を意識しているところが挙げられる。しかし、ここにおいても、チャネルの問題と、同期の問題があり、これらの問題はほぼ無視されてきているのが実情である。さらに応用目的の問題として、目標では何らかの複数の変調方式を用いるシステムに対して有効であるとしながらも、そのシステム上での評価は行われていない。

以上のことを考慮して、本論文ではユニバーサル無線機における変調方式識別と、それに付随する要素技術を検討しながら、その実現性を検証した。具体的には、変調方式識別技術として、パターン認識的アプローチ、及び、決定論的アプローチの両面から取り組んだ。実際、ユニバーサル受信機を検討し

ようとした時に、変調方式識別のみならず、キャリア同期、シンボル同期、そして、fading による歪みの問題を解決することは必要である。本論文では特に、キャリア同期、チャネルの問題である、SNR の変動及び、マルチパス対策も含めた上での検討を行っている。変調方式の他の機能との組み合わせにおける一番の問題は、一般的に、変調方式が未知の状態で他の機能が動作することを前提としていない部分にある。この点を解決する手法をそれぞれにおいて提案し、さらにそれぞれを組み合わせた統合システムを評価した。

パターン認識的アプローチによる変調方式識別においては I-Q 平面上での識別を試みた。ここでは、特にブラインド型 SNR 推定アルゴリズムを導入し、SNR 変動のある状態においても、ブラインド型 SNR 推定果を用いて識別を可能とすることを示した。キャリアオフセットに対しては、非同期系の処理として時間的に隣あう信号の位相差信号を活用することでキャリアオフセットをキャンセルする手法を提案し、それを用いることでキャリアオフセット存在下においても変調方式識別が可能であることを示した。更に、マルチパス環境下では、等化器の利用を試みた。ここでは、従来、等化器のデザインが受信信号の変調方式、特に振幅多値数に依存することを問題点としてとりあげている。この問題点に対して、変調方式識別部で等化器のデザインと受信変調方式がマッチしないケースを考慮することで、マルチパス環境での識別を可能とすることを示した。

決定論的アプローチによる変調方式識別においては Multimode Phase Locked Loop (PLL) を提案した。ここでの変調方式識別は Phase Lock Detector を用いて実現している。具体的には位相の同期獲得判定処理と変調方式識別の類似性に着目し、その判定結果を用いて識別を行っている。また、キャリアオフセット存在下においてその基本的な特性の解析を行った。その解析結果を用いて、より現実的なケースにおける Multimode PLL の改善を行い具体的なシステムとして ISDB-S を考慮し、現実的なチャネルモデル上で従来のアプローチによる適応変調方式と Multimode PLL に実現の場合の評価を行った。これにより、Multimode PLL の場合が従来アプローチよりスループット特性において優れることを示した。

以下に論文構成を紹介する。１章においてはイントロダクションとして研究の背景と狙い、及び、研究成果について簡単に紹介している。２章では、ユニバーサル無線機についての説明と、論文において仮定するシステム及び、諸仮定を示している。次に、３章では、変調方式識別の手法として決定論的アプローチによる手法と、パターン認識低アプローチに関して、それぞれ提案方式を示してある。ここでは、特に、理想的な状態、すなわち、ＡＷＧＮ通信路、キャリアオフセット無しの状態を仮定して議論を進めている。４章では、キャリアオフセットのあるシチュエーションを前提とし、変調方式識別のためのキャリアオフセット対策をそれぞれの提案方式に対して提案している。５章ではさらにマルチパス環境おいて、変調方式識別法とブラインド等化を如何に組み合わせるかを論じている。特に、振幅多値数が異なる変調方式に対して同時に対応可能なブラインド等化を提案している。６章では、３章から５章で提案したそれぞれを組み合わせた統合システムの評価を行っている。最後に、７章で結論と今後の課題を示している。

学位取得大学: 横浜国立大学
Kenta Umebayashi
E-mail:ume@ee.oulu.fi
Address : P.O.Box 4500 FIN-90014
University of Oulu Finland
Tel +358 40 744 1069 (GSM)
FAX +358 8 553 2845

Orthogonal Designs for Advanced Wireless Communications

Giuseppe Thadeu Freitas de Abreu(Oulu 大学)

今日の無線通信システムには多大な要求が求められている。それは、現代の社会において高速な伝送レートを要求する高性能なパソコン、テレビ、オーディオ機器などを日常生活に用いることが常識になってきた。これにより、ユビキタスかつ高速な情報が不可欠である世界に変化してきた。先進国では、有線通信システムにおいて通話に用いる情報量がデータ通信量に上回られたが、無線システムではこの現象が未だ起こっていない。なぜなら、それは要求が無いからではなく、無線通信技術が十分に発展していないからである。

日本は、音声、メール、データと画像の無線通信サービスを安価な値段で供給する第 3 世代セルラーシステムが成功している唯一つの国である。この日本の成功例は無線通信の資源である「時間」、「周波数」、「空間」を「符号」などの先端技術を用いることにより、高速な伝送レートの要求を実現可能な方法で満たしていることを表す。

さらに無線通信路の最大キャパシティを満たすためには、これら空間－周波数－時間の組み合わせを高度に設計することにより、多次元無線通信をすることが考えられる。多次元無線通信を最適に構成する設計方法として、各次元を直交させる方法がある。しかし、現実的には通信路の影響で直交性が崩れてしまう問題がある。

本博士論文では、高速伝送の多次元無線通信システムにおける直交性の維持、修復を可能とする設計方法を、近年注目度が高く発展性のある「時空間符号化技術」と「スマートアンテナ技術」と「多次元超広帯域システム技術」の３つの技術において提案する。本論文の構成は、上記の３つの技術をそれぞれ部に分けて、述べる。

第１部では、無相関の同等な統計分布モデルにより定義されていた通信路状態での時空間ブロック符号の定義を一般化した通信路状態での時空間ブロック符号の直交性について検討する。具体的には、多次元無線通信路において、非定常状態、空間相関や統計分布の違いを考慮した時空間符号について解析し、それに対応した復号方法を提案する。

多次元無線通信路において、空間相関は統計分布の違いに相当し、線形復号によって復号された時空間符号化利得の劣化の原因になる。しかし時空間符号の直交性は保たれているので、信号雑音比に比例して誤り率が改善される。次に非定常状態の場合において解析する。この場合においては、時空間符号に深刻な影響を受け、従来の線形最尤複号方式では復号された時空間符号の直交性を崩し、信号雑音比に高くても誤り率の改善効果が得られない。その対策として、非定常状態チャンネルにおける時空間符号の直交性を保つ新たな線形最尤複号方式を提案する。非定常状態チャンネルというのは、OFDM 伝送通信路によく見られる。OFDM 伝送に提案する直交性を保つ線形最尤複号方式を用いることにより、時間選択性フェージングに対応した時空間符号と周波数選択性フェージングに対応した OFDM 伝送を組み合わせたロバストな高速伝送レート無線移動通信システムが実現できる。

第 2 部では、空間分割を利用する多次元無線通信システムのためのスマートアンテナ技術について述べる。まず、新たな準直交ビームパターンの設計アルゴリズムを提案する。このアルゴリズムは古典的な Dolph-Chebyshev アレー設計の拡張であり、従来のビーム幅が調整出来る低サイドローブビームパターン作成方式に比べて計算量が少ない技術である。

提案アルゴリズムは簡易であるため、適応性のある直交ビームパターンを動的に作成する必要のあるシステムに応用できる。例えば、第 1 部の解析によると空間相関や非同等統計分布が時空間符号の特性劣化の原因となる。この問題に対する 1 つの解として「アンテナ空間」を「ビーム空間」にし、これらのビームパターンの特性（サイドローブとビーム幅）を変更しながら独立同等統計分布（Independent and

Identically Distributed - IID）のチャンネルを作ることができる。そこで計算量の少なく、かつ適応性のある直交ビームパターンを作成する提案方式が利用できる 1 つのアルゴリズムであると言える。

しかし、このようなアプローチを用いるためにはマルチパスチャンネルの到来角度に対する電力分布が既知で無ければならない。多くの場合、この角度/電力分布はガウス分布に近似することができ、「中心到来角度」と「角度広がり」というパラメータによって特徴付けられる。この仮定を用いて、中心到来角度と角度広がりを同時に推定する新たな方式も第 2 部で提案する。

最後に、第 3 部では超広帯域通信システムについて検討する。まず、送受信機のクロックの不安定や不完全な遅延推定などにより生じる「ジッター」と、容量性を持つ一般的なアンテナ「入力信号を微分するアンテナ」による超広帯域の直交波形変調方式への影響の解析を行う。さらに、これらのパフォーマンスの劣化をもたらす原因に対応した新しい直交波形成形方法を提案する。

これらの波形成形方法を考えることによって、超広帯域の直交波形の一般的な成形理論を確立する。この新しい超広帯域の直交波形成形の原理では、Hermite 多項式に基づいた単純な直交 Hermite 波形のセットによって定義される「Hermite 空間」を用いた畳み込み演算によって表されるチャンネルの効果を行列の積によってモデル化することが出来る。以上に述べたチャンネルの効果だけではなく、様々な超広帯域チャンネルの欠陥を直交波形成形することにより、軽減することが可能である。

学位取得大学: 横浜国立大学
Giuseppe Abreu, Ph.D.
Centre for Wireless Communications (CWC)
University of Oulu.
Tutkijantie 2E
90100 Oulu, Finland
email: Giuseppe.Abreu@ee.oulu.fi
Mobile: +358 40 744 1395
http://www.cwc.oulu.fi/∼giuseppe

電子透かし技術とその応用に関する研究

栗林稔 (神戸大学)

ディジタル情報はコピーが容易であり，コピーしても全く劣化がなく，オリジナルにその痕跡を残さない，というディジタル情報特有の性質を有するために，ディジタルコンテンツの著作権侵害が大きな問題になっている．この問題を解決する一手法として電子透かし技術が脚光を浴びている．本論文では，ディジタル情報の著作権保護を目的として，電子透かし技術とその応用に関する研究を行い，その研究成果をまとめている．

第 1 章では，著作権侵害の問題とその対策について考察して，従来の対策技術に潜む問題点を指摘している．また，本論文の各章で論述する内容の概要，提案手法の発想と着眼点についてまとめている．

第 2 章では，ディジタル画像の電子透かし技術並びにその評価に適用される各種の画像処理技術を述べている．また，電子透かし技術を応用した電子指紋技術の概要を説明し，その技術を用いた不正者追跡のプロトコルを示している．

第 3 章では，人間の視覚特性に基づき，ディジタル画像の低周波成分に透かし情報を埋め込む新しい電子透かし技術を提案している．低周波成分への透かし情報の埋め込みは，各種の攻撃に対して耐性は高いが，ブロック歪みが生じやすい．このブロック歪みの問題を解決するために DCT 係数の低周波成分の特性を詳細に検討し，特定の 4 つの DCT 係数を加えることにより，透かし情報の信号エネルギーがブロック内の中央付近の領域に緩やかな曲線を描いた模様として現われ，ブロックの端ではその振幅

がほとんど変化しないという重要な特性を発見した．この DCT 係数間の加法特性を利用してブロック歪みを抑圧し，各種攻撃に対する耐性を向上した新しい電子透かし技術を提案している．更に微小な回転，拡大・縮小，平行移動，などの幾何学的改変が加えられた場合でも透かし信号が検出できるように，同期を回復する信号処理技術も提案している．

第 4 章では，画像の局所的な情報に基づいて，適応的に透かし情報を埋め込む手法を提案している．一般に画素の信号値が激しく変化する領域では，人間の視覚特性により信号の歪みが知覚されにくい．そこで画像から局所的に抽出したブロック内の信号の分散を調べることにより，埋め込みに適した領域を選別している．また，抽出したブロックにウェーブレット変換を適用して周波数成分に分解し，PN 信号によりスペクトル拡散した透かし信号を低周波成分に埋め込んでいる．

第 5 章では，データ量が多くリアルタイム性が要求される動画像の電子透かし技術の研究成果をまとめている．透かし情報を検出するための計算量が重要な問題となるので，比較的計算量が少ない電子透かし技術を目指し，パルス位置変調の概念を電子透かし技術に応用した新しい手法を提案している．幾何学的な改変を考慮して同期信号を埋め込む従来の手法では，歪みを補正した後に透かし情報を抽出する必要があるので，計算量が膨大になる．提案方式では微小な回転，拡大・縮小，平行移動による同期点を検出できれば，補正を行わずに隣接する同期信号の信号間距離を計算することにより，透かし情報を容易に検出できる．

第 6 章では，岡本–内山暗号の加法性準同型写像の性質を利用して，暗号化された透かし情報を暗号化されたコンテンツに埋め込む電子指紋プロトコルを提案し，その安全性を証明している．このプロトコルを利用すれば，購入者は匿名で電子指紋の埋め込まれたコンテンツを購入できることのみならず，もし購入者が不正にコピーを配布すれば，販売者はその不正コピーから不正配布者を特定でき，それを証拠として不正配布を行った購入者を訴えることができる．さらに，従来の手法では，購入者の電子指紋を埋め込んだ 1MB のコンテンツを安全に販売する為に，1GB 以上のデータを伝送する必要があったが，提案手法では伝送するデータを 3MB 程度まで抑えられることを示している．

第 7 章は結論であり，本論文で得られた成果を総括している．

学位取得大学: 神戸大学
E-mail: minoru@eedept.kobe-u.ac.jp

他局間干渉の無い CDMA 通信を実現する最適な ZCZ 符号の設計

高務健二 (富士電機アドバンストテクノロジー)

携帯電話に代表されるセルラー移動体通信において，基地局と移動局間の無線通信方式は、刻々と変化するような通信路環境に対しても耐性の高い符号分割多元接続 (CDMA: Code Division Multiple Access）方式が主流となっている。最近では，音声、動画、ソフトウェアなどの大容量のマルチメディア情報をリアルタイムに伝送できることが要求されている．

本論文は，上記要求に答えるために，高信頼でかつ大容量の情報伝送可能な CDMA 方式を実現する零相関領域 (zero correlation zone) を有する符号 (ZCZ 符号) に関してまとめたもので 6 章からなる．第 1 章では，研究の背景と目的，研究の位置付け，および本論文の構成について述べている．また，この研究の期間中に他に同じような研究内容が発表されているので，その関連性についても説明している．

第 2 章では，セルラー移動体通信方式や CDMA 方式の基本事項について述べ，近似同期（準同期）方

式に ZCZ 符号をうまく取り入れた他局間干渉を完全に削除できる近似同期 CDMA 方式の原理を説明している．特に，平均 SN 比に対する情報誤り率を示して、干渉除去の効果を理論的に検討し，その方式の有用性を示している．

第 3 章では，ZCZ 符号を定義し，その数学的上界を説明し，システム構成を容易にする 2 種類の 2 値 ZCZ 符号を提案している．ここで，零相関範囲が最小の場合，数学的上界に到達するので，最適な CDMA システムが構築可能となる．また，ほぼ同じ時期に提案された ZCZ 符号は周期的に同じ系列を含むので，遅延の長いマルチパスの影響など不具合が生じたときに，伝送効率の低下につながる．そこで，互いに異なる系列からなる符号の条件を検討している．さらに，系列長が 2 の冪乗となる場合の発生関数を公式化している．この発生関数は，2 値ベクトルを入力とする排他的論理和と論理積からなる論理関数であり，簡単なパラメータを与えることで任意の系列が容易に発生できる．これにより，コンパクトなシステムが設計可能となる．

第 4 章では，2 値 ZCZ 符号と非 2 値 ZCZ 符号の差違を説明し，上界を満足する非 2 値 ZCZ 符号の幾つかの構成法を示している．ここでは，特に，2 値 ZCZ 符号と同様にシステム構成容易な 3 値 ZCZ 符号を中心に議論している．零相関領域に自由度を持ち，系列構成も容易なこと，そして，系列数が数学的上界に到達することから，3 値 ZCZ 符号は 2 値 ZCZ 符号にとって代わるものと考えられる．

第 5 章では，先ず，隣接するセルには異なる ZCZ 符号を割り当て，セル間は同期が取れないと仮定したセルラー近似同期 CDMA 方式の基本モデルを与えている．これは，セル内の干渉は全く無く，セル間干渉はできるだけ低減する方式である．次に，各種の ZCZ 符号における干渉を評価し，非同期 CDMA 方式の場合と対比している．その結果，特異な相関特性を有する ZCZ 符号を用いたとしても，セル外からのセル間干渉は非同期方式と同じであることが示された．しかし，セル内の干渉はまったく無いことから，提案するセルラー方式は，今までの非同期 CDMA 方式より優れていることが平均 SN 比に対する情報誤り率の評価により示されている．

第 6 章で本論文をまとめ，今後の課題や展望を述べている．

学位取得大学: 山口大学
E-mail: takatsukasa-kenji@fujielectric.co.jp

ISIT2004 参加報告

松本渉 (三菱電機)

2004 年 6 月 27 日から 7 月 2 日までの 6 日間、アメリカのシカゴにおいて、2004 IEEE International Symposium on Information Theory (ISIT 2004) が開催されました。多くの SITA 関係者のご尽力により大盛況の内に終了しました昨年の ISIT2003 に続き、今年のシカゴの ISIT2004 も大変な熱気に包まれておりました。投稿数も約 958 件にのぼり、570 件が採録となったとの事で、例年に比べても規模が大きかったようです。開催期間中は連日快晴でミシガン湖のほとりのさわやかな風や抜けるような初夏の青空のもとランチやディナーに出かけるのも楽しみの一つでした。ディナーといってもサマータイムで 8 時ごろまで日が暮れませんので美しい湖畔の景色や摩天楼群の景観を堪能できました。もちろんシカゴの夜景もすばらしかったですが...

さて、会議の内容の報告に移りますが、多くの興味あるセッションが平行で進行しており、残念ながらどれか一つに絞り込んで参加することになりますので、この報告も私が興味を持っている分野である LDPC 符号関連に偏ってしまっていることを予めご了承ください。

ISIT のメインイベントであるシャノン講演では、

カリフォルニア工科大学の Robert J. McElice 教授により”Are there Turbo-Codes on Mars?” の講演が行われました。また、基調講演では、Swiss Federal Institute of Technology の Ueli Maurer 教授による”Information Theory in Cryptography”, スタンフォード大学の Perisi Diacoins 教授による”The Mathematics of Making a Mess”, Flarion Technologies 社の Thomas J. Richardson 氏による”The Methods of Iterative Methods” の講演が行われました。最先端の分野の興味深い講演に講演用の大ホールは連日ほぼ満席の盛況振りでした。

Technical Program では、Fountain Codes や Network coding など、Multicast システム, Ad hoc network や Sensor network を背景とした複雑化するネットワークトポロジーに対する頑強で効率的な通信手段としての符号化復号問題が話題になっておりました。

また LDPC 符号等の繰り返し復号の性能解析の手段として着目されている Pseudocodewords や Stopping Sets の議論が活発に行われており、これらの影響を考慮にいれたグラフ上での設計手法や、組み合わせ論、代数的な表現を用いた LDPC 符号構成法もいくつか提案されていました。

繰り返し復号法の目新しい提案としては、コロンビア大学の J. Feldman らによる線形計画法を用いた復号法 (LP Decoding) やハーバード大学の N.Varnica らによる最尤復号に近い復号性能を示す Improved Near Maximum-Likelihood Decoding など興味深いものがいくつかありました。

実際の通信システムの際に問題の対象となるマルコフ通信路やフェージング通信路に対する符号設計法、また、再送を考慮に入れた RC（Rate-Compatible）LDPC 符号や Space-Time 符号と LDPC 符号を組み合わせた LDPC space-time codes などの符号設計法などは、実機に携わる企業側の立場から見ても大変参考になる内容でした。

さて毎回趣向を凝らした ISIT の Banquet も楽しみの一つです。今回の Banquet は７／１の木曜日に開催されましたが、IEEE Information Theory Society の President として今井秀樹先生のウィットに富んだご挨拶や IEEE 賞の表彰式、その後に行われた情報理論研究者らをモチーフにしたコント仕立ての演劇など会場から笑いや歓声が途切れることの無いすばらしいイベントでした。

２００５年はオーストラリアのアデレードでの開催とのことです。通信路・情報源符号化から、暗号、量子理論への応用や最近の推論・学習問題との連携による応用範囲の拡大により情報理論は更なる発展が期待されています。来年もまた社会的な期待を背景に活気にあふれる会議となることでしょう。

2004 年度第 2 回理事会報告

情報理論とその応用学会
2004 年度第 2 回理事会
2004 年 7 月 31 日 (土)12:00–17:00
於　千葉大学大学院 自然科学研究科 一階大会議室
議事次第

1. 会長挨拶
2. 2004 年度第 1 回理事会議事録確認
3. 2003 年度会計決算中間報告
4. 2004 年度予算執行状況及び会費集金状況
5. 2004 年度事業中間報告及び計画
6. 2004 年度ニューズレター発行状況及び計画
7. SITA2003 決算報告
8. SITA2004 開催計画及び準備状況報告
9. ISITA2004 開催計画及び準備状況報告
10. 謝金の源泉徴収について
11. ISITA における Financial Aid について
12. SITA2005 について
13. ISITA2006 について
14. 名誉会員の推薦について
15. IEEE IT Soc.-bog Meeting の報告

16. SITA 奨励賞選考について
17. 会員名簿作成について
18. 新規入退会者の承認について
19. その他

国際会議のお知らせ

以下のご案内する内容につきましては, 変更になっている場合もありますので, ご自身でのご確認をお願い致します. 最新情報は以下のサイトなどをご覧下さい.

IEEE ConferenceSearch
⟨http://www.ieee.org/conferencesearch/⟩

Globecom 2006
日時　2006 年 11 月 27 日–12 月 1 日
場所　未定
URL　未定
締切　未定

ICC 2006
日時　2006 年 6 月 12 日–6 月 16 日
場所　Istanbul, Turkey
URL　未定
締切　未定

ISIT 2006
日時　2006 年 7 月 9 日–7 月 16 日
場所　Seattle, WA USA
URL　http://www.isit2006.org/
締切　未定

Globecom 2005
日時　2005 年 11 月 28 日–12 月 2 日
場所　St.Louis, MO USA
URL　http://www.ieee-globecom.org/2005/
締切　2005 年 3 月 1 日

MILCOM 2005
日時　2005 年 10 月 17 日–10 月 21 日
場所　Atlantic City, NJ USA
URL　未定
締切　未定

VTC 2005-Fall
日時　2005 年 9 月 26 日–9 月 29 日
場所　Dallas, TX USA
URL　未定
締切　2005 年 1 月 15 日

PIMRC 2005
日時　2005 年 9 月 11 日–9 月 14 日
場所　Berlin, Germany
URL　未定
締切　未定

ISIT 2005
日時　2005 年 9 月 4 日–9 月 9 日
場所　Adelaide, Australia
URL　http://www.isit2005.org/
締切　2005 年 1 月 30 日

ITW 2005
日時　2005 年 8 月 29 日–9 月 1 日
場所　Rotoruna, New Zealand
URL　http://www.cs.auckland.ac.nz/itw2005/
締切　2005 年 1 月 31 日

VTC 2005-Spring
日時　2005 年 5 月 29 日–6 月 1 日
場所　Stockholm, Sweden
URL　http://www.vtc2005spring.org/
締切　2004 年 10 月 1 日

ICC 2005
日時　2005 年 5 月 16 日–5 月 20 日
場所　Seoul, Korea
URL　http://www.icc05.org/main/main.html
締切　2004 年 9 月 1 日

ICASSP'05
日時　2005 年 3 月 19 日–3 月 23 日
場所　Philadelphia, PA USA
URL　http://www.icassp2005.com/
締切　2004 年 9 月 17 日

WCNC 2005
日時　2005 年 3 月 13 日–3 月 17 日
場所　New Orleans, LA USA
URL　http://www.wcnc.org/
締切　2004 年 8 月 1 日

INFOCOM 2005
日時　2005 年 3 月 13 日–3 月 17 日
場所　Miami, FL USA
URL　http://www.ieee-infocom.org/2005/
締切　2004 年 7 月 7 日

Globecom 2004
日時　2004 年 11 月 29 日–12 月 3 日
場所　Dallas, TX USA
URL　http://www.globecom2004.org/
締切　2004 年 3 月 1 日

TENCON 2004
日時　2004 年 11 月 21 日–11 月 24 日
場所　Chiang Mai,Thailand
URL　http://www.tencon2004.com/
締切　2004 年 3 月 30 日

MILCOM 2004
日時　2004 年 10 月 31 日–11 月 3 日
場所　Monterey, CA USA
URL　http://www.milcom.org/2004/
締切　2004 年 2 月 27 日

ISITA 2004
日時　2004 年 10 月 10 日–10 月 13 日
場所　Parma, Italy
URL　http://www.sita.gr.jp/ISITA2004/
締切　2004 年 3 月 26 日

編集後記

前号の編集後記でも異常気象の話から始めましたが、その後も台風 18, 22 号や浅間山噴火など痛ましい災害が続いておりますが会員の皆様にはお変わりございませんでしょうか。

前号では一部に校正みおとしをしてしまい、会員の皆様には大変御迷惑をおかけし申し訳ございませんでした。

さて、今号は博士論文要旨特集号とさせていただきました。9 名の方から博士論文要旨を頂きました。御寄稿頂きました皆様に深く感謝致します。前回の特集である 49 号 (2003 年 8 月 29 日発行) は 36 号 (2001 年 1 月 24 日発行) 以来、2 年半ぶりの博士論文特集号で、今回の特集は約 1 年の間隔で、正直どれ位集まるのか不安な部分がありましたが、9 名の方から博士論文を頂き、この分野の発展を再確認したように思います。

また、三菱電機の松本さんにはシカゴの ISIT 参加報告を頂きました。急なお願いにもかかわらず快く御執筆をお引き受けくださいました松本さんに深く感謝致します。

次号は年末発行を予定しておりますが、会員の皆様には企画等ございましたら、是非編集担当までお知らせくださいますようお願い申し上げます。(高田)

編集担当者

高田豊雄 (編集理事)
〒 020-0173 岩手県岩手郡滝沢村滝沢字巣子 152-52
岩手県立大学ソフトウェア情報学部
Tel. 019-694-2606
Fax. 019-694-2657
E-mail takata@iwate-pu.ac.jp

常盤欣一朗 (編集理事)
〒 574-8530 大阪府大東市中垣内 3-1-1
大阪産業大学工学部電気電子工学科
Tel. 072-875-3001 (内線 4015)
Fax. 072-870-8189 (学科事務室)
E-mail tokiwa@elec.osaka-sandai.ac.jp

山本宙 (編集幹事)
〒 259-1292 神奈川県平塚市北金目 1117 番地
東海大学電子情報学部情報メディア学科
Tel. 0463-58-2122 (内線 4099)
Fax. 0463-50-2412 (学科事務室)
E-mail hiroshi@tokai.ac.jp

鴻巣敏之 (編集幹事)
〒 572-8530 大阪府寝屋川市初町 18-8
大阪電気通信大学総合情報学部情報工学科
Tel. 072-824-1131 (内線 2370)
Fax. 072-880-5623
E-mail kohnosu@kns.osakac.ac.jp

情報理論とその応用学会事務局, http://www.sita.gr.jp/, E-mail: sita-office@sita.gr.jp
〒184-8584 東京都小金井市梶野町 3-7-2
法政大学情報科学部ディジタルメディア学科内, 西島利尚 気付
Tel: 042-387-4534（直通）, Fax: 042-387-4560