No. 31 1998 年 10 月 4 日発行

SITA 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

研究者との出会い ..... 阪田 省二郎 (電通大)

博士論文要旨
局所結合型ニューラルネットワークを用いた通信ネットワークルーティングおよびパターン分離に関する研究 ..... 黒川 弘章 (東京工科大)
Studies on Electronic Voting Protocols ..... 佐古 和恵 (NEC)
マルチメディア通信に適したネットワークに関する研究 ..... 塩川 茂樹 (名工大)
A Study on Security Verification of Real-time Cryptographic Protocols ..... 田中 猛彦 (奈良先端大)
系列の複雑度に基づいた定常エルゴード情報源に対するユニバーサル情報圧縮アルゴリズム ..... 村松 純 (NTT)
筆跡および音声に現れる身体的特性からのカテゴリの抽出と個人認証方式への応用に関する研究 ..... 山崎 恭 (早大)

国際会議報告
1998 IEEE Information Theory Workshop ..... 古賀 弘樹 (東大)
The First Advanced Encryption Standard Candidate Conference ..... 神田 雅透 (NTT)
CRYPTO 98 ..... 佐古 和恵 (NEC)
情報論的学習理論ワークショップ (IBIS'98) 開催報告 ..... 山西 健司 (NEC)
企画からのお知らせ ..... 企画理事 山口 和彦 (電通大)
情報理論とその応用学会ロゴマーク募集結果 ..... 庶務理事 藤原 融 (阪大)
国際会議のお知らせ
会員情報
次号のお知らせ

研究者との出会い
Encounters with Persons in Research Activities

阪田 省二郎 (電気通信大学)

「私の Key Paper」シリーズへの寄稿を、News Letter 編集委員の高田豊雄氏より最初に依頼されたのは１年前のことであったが、緊急の用件を控えていたためお断りした。ところが、先日ある会合の場で、再度の依頼を受け、今回は引き受けざるを得ない仕儀となってしまった。最近の本シリーズの傾向に便乗し、さらに脱線して、「私の Key Paper」ならぬ「私が研究上出会った人々」を中心にした回顧録を述べることにしたい。符号理論の世界にやや遅れて入った者が、先輩、友人、同僚、関連の研究者との交流を通して、どのように研究を進めていくことができたか、以下に個人的、主観的なメモを披瀝する。他に書くことを思い着かなかったので、お許しいただきたい。(本稿中、敬称はすべて「... 氏」と記す。)

1 多次元符号との最初の邂逅

私が、情報理論、とくに、符号理論の世界に足を踏み入れたのは、学生の身分を離れ、恩師のお陰で、初めて大学（現在の湘南工科大学、旧称相模工業大学）に職を得た後のことである。ともかく何か研究の種はないかと探していたとき、興味を引かれたのが W. W. Peterson 著 "Error-Correcting Codes" の青い paperback 版 [1] であった。内容の理解に手間取り、大変苦労した割には、余り研究の種に成りそうなことは見つけられずに終ってしまったような気がする。しかし、元々、趣味であった代数学を何とか応用する場を目のあたりにしたことは、貴重な体験であった。

一方、当時読み耽った B.L. van der Waerden 著 "Moderne Algebra" の銀林浩訳 [2]、とくに、第３部に書かれていた多項式イデアルの章が気になっていた。その応用を模索していた折、M 系列 (最大周期系列) の２次元化の研究

をされていた中村勝洋氏、佐藤創氏の仕事が、研究への誘い水になった。とくに、中村氏 [3] との２次元 M 系列の定義に関する論争は自分にとって刺激的であった。これらのトピックスは、２次元巡回符号および２次元線形再帰系列の研究とつながっており、この分野の先達でもあった今井秀樹氏 [4] が開かれた道の跡を辿ることになる。既に、ヨーロッパ、とくに、ロシアの研究者 S.D. Berman により、多次元巡回符号（アーベル符号とも呼ばれる）の潜在的な性能が示唆されていたが、多次元線形再帰系列の基本的な概念の定義すら、当時（1970 年代半ば頃）は未だ確定されていない状況であったと思う。試行錯誤を繰り返した結果、自然な形で、これらの基本概念の定義を与え、定係数偏差分方程式系である線形再帰関係の解集合（解空間）の性質を明らかにすることができた。その内容を論文 [5] にまとめ、IEEE Transactions on Information Theory (IT-Trans.) に投稿したが、採録決定までの過程で、当時の符号理論エディタであった Dr. Neil J.A. Sloane （今年の IEEE International Symposium on Information Theory (ISIT) における Shannon Lecturer であり、符号理論の巨星、かつ、rock-climber）からもらった直筆の手紙は、その後の自分の研究上大きな励みとなっている。

2　Gröbner 基底との廻り合わせ

ところで、多次元線形再帰系列に関して、一つの疑問が残されていた。それは、与えられた線形再帰関係の組に基づいて、適当な初期値の組から、系列の残りの部分を決定する際、用いる線形再帰関係によっては互いに矛盾する値が得られる可能性である。この疑問は、多変数多項式の除算、あるいは、その結果としての余りが明確に定義できないことに関連している。通常の１変数多項式に関しては、多項式の次数の大小に基づいて、自然に除算と余りが一意に定義される。その結果、１変数多項式環の任意のイデアルは１個の元（多項式）で生成される。しかし、２変数以上の多項式環においては、これらの事は必ずしも成立しない。つまり、多変数多項式に関して、どのようにして除算に相当する演算を定義するかが焦眉の課題であった。これを解決したのは、猪飼武夫氏 [6] である。まず、次数の概念を多次元に拡張した「準次数」（「multidegree」に相当する）に基づいて、多項式の多項式系による「除算」とその「余り」を定義し、さらに、「標準基底」という概念（「グレーブナ基底」に相当する）を導入することに成功した。このとき、私は、この基底を求めるアルゴリズムを与えることが重要であることに思い至った。これは、２次元巡回符号の構成法、あるいは、符号化法を与えることでもある。

その結果、一つのアルゴリズムの形を与え、それを用いた計算によって、準既約２次元巡回符号というクラスに属する具体的な符号をあるパラメータの範囲内で求めることができた [7]。その内容は、1981 年米国西海岸 Santa Monica で開催された ISIT で発表し、さらに、その足で東海岸に飛び、New Jersey 州、Murray Hill にある Bell 研究所（当時）を訪ね、Dr. Florence J. MacWilliams, Dr. Sloane, そして、もう一人の若い研究者 (Dr. A.M. Odlyzko?) の前で話した。 話の終了後、その若い研究者が教えてくれた論文の参考文献リスト中に B. Buchberger の名前を見つけた。帰国後、手紙のやり取りの間に送ってもらった多数の論文から、「Gröbner 基底アルゴリズム」が既に 1965 年の彼の学位論文で与えられ、1970 年にドイツ語のジャーナルに発表 [8] されていることを初めて知ったのであった。当時自分が調査可能な限りの範囲で唯一、同じ問題を扱っている論文（1926 年刊）[9] を見つけたが、そこでは２重指数オーダーの計算量の解法しか示唆されていなかった。（自分が解いたと思った問題が既に他の研究者によって解かれていたことが判明するという事態は、実際よく起こりうる。人間誰でも似たことを考える以上、それはそれで已むを得ないことであろう。）自分が同じ問題に逢着し、ともかく解を得られたのは偶然のことであったかもしれない。一方、その結果として、原著者に相見えることになった。その Buchberger 自身は、計算機科学、とくに、計算機代数、数式処理における彼のアルゴリズムの重要性が認識され始めたので、1970 年代後半になって、彼の仕事をさらに発展させた F. Winkler との共著の研究成果を次々情報科学関連のジャーナルに発表を始めたばかりであった。

3　多次元 BM アルゴリズムの構想

前述の ISIT と同じ 1981 年春に、12 年間奉職した相模工大を離れ、豊橋技術科学大学に移ることになり、当初そこの生産システム工学系、生産計画講座で主に OR や数理計画を教えるポジションに着いた。実際は、システム工学との接点において、辛うじて符号理論の研究を続けていたことになる。その頃、友人達と持った小さな研究会の場で、小林欣吾氏が Berlekamp-Massey(BM) アルゴリズムに対する関心の目を開かせてくれた。BCH 符号を含む巡回符号の自然な拡張である２次元巡回符号の復号法として、BM アルゴリズムの２次元版が有効になるであろう。しかし、この問題に対する解決の方途は一向に見えなかった。

その矢先、日本学術振興会の特定国派遣研究員として、オーストリア、Linz 大学の Bruno Buchberger の許に 1985 年 9 月から 1986 年 7 月まで滞在し、これに取り組んでみようという自分の希望が叶えられた。最初の２、３カ月は、自分と家族がオーストリアでの生活に慣れ親しみ、周囲の人々との交流に明け暮れているうちに、あっという間もなく過ぎ去ったような感がする。クリスマスの頃は、未だ、１次元の BM アルゴリズムをどう２次元に持っていくか色々模索を繰り返していた。BM アルゴリズムは、BCH 符号や RS 符号の復号法として有名であるが、実際は、任意に与えられた系列を出力することができる線形帰還シフトレジスタを合成する、つまり、その回路の結線多項式を求めるための効率的アルゴリズムである。これは、１種のシステムの実現問題である。そこで、多次元符号の復号法として与える前に、まず、２次元線形帰還シフトレジスタを合成する問題として取りかかることにした。２次元線形帰還シフトレジスタについては、今井秀樹氏の仕事を通してその概念に慣れていたことが大変助けになったと考えられる。そして、新年になって、漸くアルゴリズムの形が見えてきたような気がした。その考えは、まさに Gröbner 基底アルゴリズムとその理論的な基礎無しには成立し得ないもので

ある。実際、入力データが一つの系列である点で Gröbenr 基底アルゴリズムと違ってはいるが、データとして十分なものが与えられていれば、求めるべきは系列の特性イデアルの Gröbner 基底である。一応形をなしたつもりのアルゴリズムを Bruno のグループの若い研究者達の前で発表し、さらに、真冬の 2 月、オーストリアとイタリーの国境、雪の Brenner 峠を越えて、温度が（−/+10 度）合計 20 度も違う Roma へ旅をして、Roma 大学の Prof. Alfonso Miola 教授のゼミで講演をした。他人の前で話しをしているうちにいくつかの疑問点に思い至り、それらの解決は、ヨーロッパの長い冬が終る 4 月の末頃、日本の桜に似た花が一斉に咲き出すのと合わせたように、やっと得られた。それまでの間、Bruno とのディスカッションで「難しい?」を繰り返していたことを思い出す。出来てしまうと何でもないことが、そこに至るまでは悩みの種であり、焦点が定まり本質が見え出すと、未だ証明が不十分な段階でも、不思議にその正しさに確信が持てるようになる。

この研究成果については、Bruno の紹介で電子メールを使って始めて知己を得たドイツ, Düsseldorf 大学の Prof. M. Pohst やフランスの Toulouse 市、Paul Sabatier 大学の Prof. Alain Poli の許をはるばる訪れ、講演をした。これらの交流を契機として、殆ど毎年のようにヨーロッパ詣でをすることになった。それは、Bruno が所長を兼ねる記号計算研究所 (RISC) 訪問に加えて、Alain が会長で、今井秀樹氏や河野隆二氏が会議委員として参加されている AAECC (Applied Algebra, Algebraic Algorithms and Error-Correcting Codes) という長い名称をもつ研究会が当初ヨーロッパの各都市で開催されていたことの恩恵でもあった。ヨーロッパの旅は、日本国内での日常の雑事や煩いを忘れさせてくれるだけでなく、現地の豊かな自然・文化との触れ合い、研究者達との出会いが新鮮かつ刺激的で、そこからまた新しい課題に取り組む元気を得ることができたように思う。一方で、旅を繰り返す毎に、田舎芝居の旅役者になったような気分を感じたこともある。(Mozart が重ねた旅での思いのわずかでも煎じて味わうことができたであろうか？）この間に、多次元システムの実現問題に対する一つのアプローチとしての意味づけを与えたり、当初の一つの多次元配列（系列と呼ぶより、配列と呼ぶ方がその多次元性が浮き彫りになるので、後者の用語を用いるようになった）に関する問題をさまざまな場合、とくに、複数個の配列やベクトル配列（配列の組合せ）に関する問題に拡張して、アルゴリズムと理論を展開していった。

4　代数幾何符号との出会い

BM アルゴリズムの多次元版を J. Symbolic Computation に出版することはできた [10] が、本来の多次元巡回符号の復号へどう適用するかは手付かずであった。折しも、1989 年夏、Sweden の Gotland で開催された Swedish-Russian Joint Workshop on Information Theory (SR-ITW) に参加した、当時の同僚、森田啓義氏が帰国土産に話してくれたその研究会のニュースが次のステップへの大きな拍車となった。デンマークの Jørn Justesen と Tom Høholdt のグループが彼等の代数幾何符号の復号法 [11] を高速化する手段として、多次元 BM アルゴリズムを使うことができると発表したことである。たった 2 頁の Abstract を目にしただけであったが、その意味を考えたとき、漸く、多次元巡回符号に対する復号法の構想が見えてきた [12]。さらに、当時、自分自身未だ本気で取り組む用意もできていなかった代数幾何符号というものに対する高速復号法のイメージが浮かんだ。Høholdt 達の主張は、その片鱗が現われはしたものの、1990 年の San Diego での ISIT の発表でも明確な姿は分からず、彼から送られてきた IT-Trans. への投稿論文 [13] 原稿を目にすることができたのは、やっとその年の終り近くになってからである。

相前後して、国外では、K. Saints & C. Heegard, B. Shen & R. Pellikaan, 国内では三浦晋示氏、神谷典史氏等が、私のアルゴリズムを代数幾何符号の高速復号法に適用できることを様々な形で示してくれつつあった。BMS アルゴリズムという呼称もその頃から現われた。これらの研究から学んだり、刺激を受けたりしたが、その結果、Tom 達が当初与えた形の復号法は一般的な配列に対する原アルゴリズムを殆ど直接適用するものであったが、代数曲線で定義される符号の場合、その特別な構造を生かした改良版が成り立つこと等が分かってきた。

その間、本来の代数幾何符号の一般的復号法についても、著しい進歩がなされた。1993 年の IT-Trans. 論文賞を受けた Feng-Rao アルゴリズム [14] の登場である。1990 年、最初に一般的な代数幾何符号の復号法として出版された Skorobogatov-Vlăduţアルゴリズムの訂正限界 (SV 設計距離) は、代数幾何符号の発見者 V.D. Goppa が示した限界 (Goppa 設計距離) までわずかに及ばず、若干の改善の余地を残していたが、G.L. Feng & T.R.N. Rao は、多数決論理による未知シンドロームの決定法を導くことによって、ついにこのギャップを克服したのである。彼等の、Ruud Pellikaan, Iwan Duursma との電子メールを通してのディスカッションがこの成果を導いたと言われている（事実、Ruud 等が導いた、Goppa 設計距離より若干大きい FR 設計距離までの訂正が可能である）。私としては、当然、FR 設計距離までの高速復号法を与えなければならない。1993 年 1 月 17 日から米国テキサス州 San Antonio で開催される ISIT 参加直前の準備をしていた 15 日、Feng-Rao 論文を読みながら、自分のアルゴリズムの性質に基づいて、全く自然に多数決論理を導入し、FR 設計距離までの高速復号法を組み立てる着想が得られた。早速、ISIT の recent results session で、機内でまとめたばかりのメモを発表した。それを聞いてくれていた Tom が、実は自分達も同じ考えを持ち、論文を既に半分完成させたところであると話しかけてきたので、共著論文とすることを提案し、合意した。

このようにして、デンマーク工科大学のグループとのより深い交流が始まることになった。その同じ年の 9 月に Sweden の Mölle で開催された SR-ITW への参加のとき以来、毎年のように、Copenhagen 近郊の小都市 Lyngby にあるデンマーク工科大学への訪問を繰り返し、共著論文を複数篇出版してきた [15][16][17]。その中でも、アメリカ Auburn 大学の Prof. Douglas Leonard も加えた、代数曲線符号の消失・誤り同時訂正に関する共著論文は、日、米、デンマークの研究者それぞれの個性の衝突で最終論文にま

とまるまで多くの時間とメールのやり取りを要したが、近刊の IT-Trans. 中 correspondence としてやっと出版するところまでこぎ着けることができたものである。

5 むすび

今年の春、東海大で開かれた電子情報通信学会ソサイエティ大会のパネルでも引用したことであるが、Shannon 情報理論創始より 50 年の間、とくに、符号理論の分野での最も重要な発明は、多項式代数に基づいて構成・復号可能な符号のクラスである「代数的符号」に関するものであり、ほぼ 10 年毎に現われた [18]：Hamming 符号 (1949)、BCH/RS 符号 (1959/60)、BM アルゴリズム (1968)、 代数幾何符号 (1981)、代数幾何符号の復号法 (1989)。多岐にわたる符号理論において代数的符号が中心的存在になる理由は、要するにその多項式オーダーの計算量にある。指数オーダーの計算量をもつ方法は実際には役に立たない。代数的符号の数学的な美しさは、その符号化法・復号法の計算量と連動しているのである。今日までの代数的符号の発展は、１次元（１変数）から多次元（多変数）への進化であり、論理的必然の結果である。多次元巡回符号そのものは、余り性能がよいものが具体的に見つけられていないために、その後目立たなくなってしまったが、そのいわば直系に当る代数幾何符号の発展は、今後の情報化社会において重要な働きをするものと予想される（代数幾何符号については、たとえば、[20] 参照）。この趨勢と並んで、Gröbner 基底アルゴリズムおよび理論は、符号理論だけでなく、暗号においても今や必要不可欠の道具となっている。

奇しくも、自分が偶然のきっかけで始めた符号理論の研究が、学問と技術の大きな発展の流れに必然的に結び付いていったことを一種の感慨を持って振り返らざるを得ない。顧みて、これまで約 10 年の周期で細く長く符号理論の研究を続けてきたが、今後も旧交を温めつつ、かつ、新たに若い研究者との出会いに触発されながら、次の段階を目指したい。実際、代数幾何符号の研究も未だ半分始まったばかりである。

この 1, 2 年、ハンドブックや雑誌、学会誌特集等で、代数幾何符号や Gröbner 基底と符号理論との結び付きについての概説を書く機会に恵まれたが、このメモは、内容的にそれらの記事と重複する箇所があることをお断りしなければならない [19][21][22]。また、以下の参考文献のリストは、本文の流れと直接関係するものに限っているので、関連する重要な文献の多くを含まないことにも注意されたい。

参考文献

[1] W.W. Peterson, *Error-Correcting Codes*, The MIT Press, 1961.

[2] ファン　デル　ヴェルデン著、銀林浩訳、「現代代数学」第 1 部、第 2 部、第 3 部、東京図書、1961.

[3] 中村勝洋, "$\gamma\beta$ 平面理論の拡張," preprint, 1971.

[4] H. Imai, "A theory of two-dimensional cyclic codes," *Inform. Control*, 34, pp.1–21, 1977.

[5] S. Sakata, "General theory of doubly periodic arrays over an arbitrary finite field and its applications," *IEEE Trans. Inform. Theory*, 24, pp.719–730, 1978.

[6] 猪飼武夫他、２次元巡回符号の基礎理論 – 生成多項式と検査記号位置、電子通信学会論文誌、59-A, pp.311–318, 1976.

[7] S. Sakata, "On determining the independent point set of doubly periodic arrays and encoding 2D cyclic codes and their duals", *IEEE Trans. Inform. Theory*, 27, pp.556–565, 1981.

[8] B. Buchberger, "Ein algorithmisches Kriterium für die Lösebarkeit eines algebraischen Gleichungssystems", *Aequ. Math.*, 4, pp.374–383, 1970.

[9] G. Herman, "Die Frage der endlich vielen Schritte in der Theorie der Polynomideale", *Math. Ann.*, 95, pp.736–788, 1926.

[10] S. Sakata, "Finding a minimal set of linear recurring relations capable of generating a given finite 2D array," *J. Symbolic Comp.*, 5, pp.321–337, 1988.

[11] J. Justesen, K.J. Larsen, H.E. Jensen, A. Havemose, T. Høholdt, "Construction and decoding of a class of AG codes," *IEEE Trans. Inform. Theory*, 35, pp.811–821, 1989.

[12] S. Sakata, "Decoding of binary $2D$ cyclic codes by the $2D$ BM algorithm," *IEEE Trans. Inform. Theory*, 37, pp.1200–1203, 1990.

[13] J. Justesen, K.J. Larsen, H.E. Jensen, T. Høholdt, "Fast decoding of codes from algebraic plane curves," *IEEE Trans. Inform. Theory*, 38, pp.111–119, 1992.

[14] G.L. Feng,T.R.N. Rao, "Decoding algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, 39, pp.37–45, 1993.

[15] S. Sakata, J. Justesen, Y. Madelung, H.E. Jensen, T. Høholdt, "Fast decoding of AG codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, 41, pp.1672–1677, 1995.

[16] S. Sakata, H.E. Jensen,T. Høholdt,"Generalized Berlekamp-Massey decoding of algebraic geometric codes up to half the Feng-Rao bound," *IEEE Trans. Inform. Theory*, 41, pp.1762–1768, 1995.

[17] S. Sakata, D. Leonard, H.E. Jensen, T. Høholdt, "Fast erasure-and-error decoding of AG codes up to the Feng-Rao bound," *IEEE Trans. Inform. Theory*, 44, pp.1558–1564, 1998.

[18] 今井秀樹、“符号理論の今後の展開,” 江藤良純・金子敏信監修、「誤り訂正符号とその応用」、オーム社、第13章、1996.

[19] 阪田省二郎、「代数幾何符号とその復号法について」、数理科学、No.7, pp.33–40; No.8, pp.58–65, 1998.

[20] 三浦晋示、「代数幾何に基づく誤り訂正符号の研究」、東京大学工学系研究科博士論文 、1997.

[21] S. Sakata, “Gröbner bases and coding theory,” (Eds. B. Buchberger, F. Winkler) *Gröbner Bases and Applications*, Cambridge University Press, pp.205–220, 1998.

[22] 阪田省二郎、「代数的誤り訂正符号：1次元から多次元へ」、電子情報通信学会誌特別企画、情報理論50年の歩みと21世紀への展望 – Shannon から50年 – [VIII]、平成10年10月刊行予定.

博士論文要旨

局所結合型ニューラルネットワークを用いた通信ネットワークルーティングおよびパターン分離に関する研究

慶応義塾大学 黒川弘章 (東京工科大)

ニューラルネットワークは複数のニューロンとその結合から構成され，並列分散処理に基づく情報処理を行う．これまでに，ニューラルネットワークに見られる競合や学習を用いたさまざまな分野への応用が示されてきたが，その一つとしてネットワークルーティングが挙げられる．ネットワークルーティングに関する従来の研究では，主にホップフィールドネットワークを用いた集中制御システムが提案され，盛んに研究されてきた．しかしながら，ルーティングシステムの耐故障性や計算コストの削減を考慮すると，分散制御型のシステムが強く求められる．一方，２素子からなるニューラルネットワーク（振動子）を結合した振動子ネットワークは，振動子の発振状態の位相差を用いることによりパターン分離に適用できることが示されている．しかしながら，従来の研究では振動子における位相や周波数の制御が不可能であったため，相互同期現象を用いて同期，非同期の２状態でパターン分離が行われており，位相状態を用いて時空間パターンを表現することは不可能であった．そのため振動子の位相状態を直接制御し，時空間パターンを表現できる振動子ネットワークが望まれてきた．本研究では，局所結合型ニューラルネットワークを用いた通信ネットワークルーティングおよびパターン分離について述べている．本研究は大きく２つの部分からなり，前半では通信ネットワークにおける分散性の高い柔軟な経路決定システムについて述べている．また，後半はニューラルネットワークに見られる発振現象を用いた時空間パターンの抽出について述べている．

第１章は序論であり， 研究の背景と目的を述べている．

第２章では，局所結合型ニューラルネットワークを用いた分散構造を持つネットワークルーティングシステムを提案している．提案システムは，小さなニューラルネットワークがネットワーク上の各ノードに分散された構造を持っている．各々のニューラルネットワークは近隣ノードからの情報のみを用いて，各ノードでのパケットの送出先を他のニューラルネットワークに対して独立に決定する．このような構成により，提案システムは従来のニューラルネットワークを用いたルーティングシステムと比較して，より少ない数のニューロンとその結合で構成することができる．

第３章は振動子を用いた情報処理のための周波数学習則について述べている．振動子を用いた情報処理においては，情報は発振状態の位相や周波数で表されるため，振動子の発振現象を制御することは重要なテーマである．提案する学習則は位相誤差を用いた学習を行うため，従来提案されてきたニューロンの出力誤差を用いた誤差逆伝播法による学習則と比べて振幅の誤差の影響が少ないため，振動子を用いた情報処理に適している．さらに自己結合荷重のみの更新則で表されるため簡単な学習則となっている．

第４章では，第３章で提案した周波数学習則を拡張することにより，振動子の同期を実現する学習則を提案し，振動子の動作や同期学習則の収束性について理論解析や数値計算を通して述べている．提案する同期学習則は位相状態を制御することが可能であり，情報を任意の位相状態で表現できるため，振動子ネットワークにおいて時空間パターンを生成することができる．

第５章では，局所結合型の振動子ネットワークを提案し，パターン分離への応用について述べている．さらに，複数の文字から構成される単語を文字ごとに分離する文字分離への応用を示している．結果として，提案する振動子ネットワークは文字分離問題において，単純に文字を分離するだけでなく文字の順序を表現でき，静的パターンから時空間パターンへの写像が可能であることが示されている．

第６章は結論であり, 本研究で得られた成果を総括している．

東京工科大学電子工学科
黒川弘章
hkuro@cc.teu.ac.jp

Studies on Electronic Voting Protocols (無記名電子投票プロトコルに関する研究)

京都大学 佐古 和恵 (NEC)

ネットワーク社会における情報漏洩や改竄、なりすましといった脅威には、暗号技術を用いて解決する研究がすすんでいる。一方、電子的に実現したい社会活動のなかには、自分の権限でシステムを利用しつつ本人のプライバシーを保護するメカニズムが必要不可欠になるものがある。暗号や認証技術を単純に組み合わせるだけでは、厳密な意味でのプライバシー保護は実現されない。各システムの目的ごとに、暗号関数や署名関数に乱数を組み合わせた暗号プロトコルを構築することが必要になってくるのである。

本稿では、不正を防止しつつ投票の秘密を保護する電子投票プロトコルを 3 方式提案し、それらの比較を行なう。また、関連するプロトコルとして、投票におけるレシート問題を解決するプロトコルや無記名アンケート集計に必要な属性値情報のみを提供する電子集計プロトコルを提案する。

電子投票において必要である、投票の秘密を守りながら不正投票を防止するメカニズムは一見矛盾するようにみえる。投票文に有権者名を書けば、有権者以外の投票や、有権者であっても二重に投票するという不正を防止できるが、投票の秘密は守られない。逆に、投票文がまったくの無記名であれば不正投票が容易に横行する可能性がある。そこで、このメカニズムを実現するためには、有権者確認手段と投票文の集計手段を、ある関係を持ちながら切り離すしかけを工夫しなくてはならない。そのしかけとして、

- ブラインド署名
- Mix-net 匿名通信路
- 準同型写像

のそれぞれを利用した電子投票プロトコルを紹介し、従来方式の欠点を補うプロトコルを提案する。さらに、上記の３つの異なるしかけに基づく投票プロトコルを比較する。比較のポイントとして、各プロトコルで想定する仮定の違い、全体の処理量、センタ側と投票者側との処理の分担比率をあげる。

上記の３つの方式のいづれも、投票を電子化することにより、従来の紙ベースの投票にはなかったレシート問題が発生する問題が発生する。レシート問題とは、各投票者が集計の正しさを検証できるという電子投票のメリットが、たとえば票の売買した時のレシート替りになるという問題である。この問題を解決するために、物理的に安全な投票ブースを仮定した投票プロトコルを提案する。提案方式は、従来方式に比べて緩い制限の投票ブースを用いてもレシート問題を解決できることを示した。

また、このレシート問題を解決する投票プロトコルに用いた要素技術を切り出し、検証者指定零知識証明プロトコルという新しい概念を提案する。この検証者指定零知識証明プロトコルは、ある事実の正しさを特定の人にのみ証明する手法である。すなわち、他の人には正しいという情報が証明付きでは流布しなくなるので、プライバシーを保護する一手段となり得る。このプロトコルを応用して、署名した事実を特定の人のみ確認できる「検証者指定デジタル署名」を提案する。

電子投票のメカニズムを用いると、無記名アンケートも実現できる。アンケートと投票と異なる点は、前者にはアンケート結果を評価するために記入者の属性が必要であるという点である。一方、属性を詳細に記述すると無記名性に反するという問題がある。そこで、各記入者の属性値を分散させ、解析に必要な属性値のみを取り出すというプロトコルを提案する。

NEC C&C メディア研究所
佐古 和恵
sako@ccm.cℓ.nec.co.jp

マルチメディア通信に適したネットワークに関する研究

慶應義塾大学 塩川 茂樹 (名工大)

B-ISDN(Broadband Integrated Services Digital Network：広帯域サービス統合ディジタル網) は, データや音声等の様々なメディアを統一したインターフェイスによって扱うことのできるマルチメディア通信網であり, 将来の通信インフラとして考えられている. ATM(asyncronous transfer mode：非同期転送モード) は B-ISDN のための 1 つの解である. B-ISDN の交換ノードである ATM 交換機で, セルを所望の出力端へと導く機能を担うのが ATM スイッチである. そして, 高速なマルチメディア通信網を実現するために, ATM スイッチにおけるセル棄却率とシステム遅延を低減させることが重要となる. さらに, 効率のよい通信網の設計法についても考える必要がある. 本研究では以上に上げた要求を満たす ATM スイッチ及び網トポロジーに着目し, それぞれの改良モデルを提案している.

第 1 章は序論であり, 研究の背景や目的について簡単に述べている.

第 2 章はホットスポットトラヒックにおいて低セル棄却率及び低システム遅延を達成できるスイッチの構成について述べている. ホットスポットトラヒックでは, 他のポートよりもアクセスされやすいポートが幾つか存在する. そしてホットスポットトラヒック下では, 棄却率特性や遅延特性が劣化してしまうことがわかっている. そこで本章では, 低セル棄却率及び低システム遅延を達成するために, ホットスポット専用ルートを設けた入出力バッファ型 2 段 ATM スイッチを提案する. 計算機シミュレーション結果より, 提案スイッチはセル棄却率を小さくし, システム遅延も低減できることを示す.

第 3 章では, マルチホップネットワークにおいて, 平均ノード間距離を小さくし, ネットワーク結合率を高くするための技術について述べている. リングネットワークとランダムに加えられるリンクから成り立つコネクティブセミランダムネットワーク (CSRN) は, 平均ノード間距離が小さいマルチホップネットワークとして知られている. しかしながら, CSRN のネットワーク結合率は他のレギュラーネットワークと比べて非常に低い. そこで本章では, 従来の CSRN よりも高いネットワーク結合率を得るために, CSRN のランダム付加リンクに制限を加える制限付き

CSRN を提案する. 理論計算及び計算機シミュレーション結果より, 制限付き CSRN は平均ノード間距離を小さくしネットワーク結合率を高くするのに有効であることを示す. さらに本章では, 従来の CSRN の平均ノード間距離を理論的に解析している.

第 4 章では, マルチホップネットワークにおいて, さらに平均ノード間距離を小さくし, ネットワーク結合率を高くするための技術について述べている. 第 3 章で提案した制限付き CSRN は, ネットワーク結合率を儒従来の CSRN より高くすることができたが, それでもレギュラーネットワークよりは小さい. そこで本章では, レギュラーネットワークと同じネットワーク結合率を維持しながら, CSRN よりも平均ノード間距離特性を小さくできるネットワークトポロジーを提案する. 提案ネットワークは, ノード順のことなる複数のリングネットワークを組み合わせることによって構成される. 理論計算及び計算機シミュレーション結果より, 提案ネットワークトポロジーは, レギュラーネットワークと同じネットワーク結合率を維持しながら, CSRN よりも平均ノード間距離特性を小さくするのに有効であることを示す.

第 5 章は結論であり, 本研究で得られた成果を総括している.

名古屋工業大学 電気情報工学科
塩川茂樹
〒 466-8555 名古屋市昭和区御器所町
TEL: 052-735-5572 (ダイヤルイン/FAX)
Email: shiokawa@elcom.nitech.ac.jp

A Study on Security Verification of Real-time Cryptographic Protocols
(時間の概念を含む暗号プロトコルの安全性検証に関する研究)

奈良先端科学技術大学院大学
田中 猛彦 (奈良先端大)

暗号プロトコルの安全性を厳密な方法で検証することを目的として，これまでさまざまな形式的検証法が提案されている．形式的検証は，まず与えられた暗号プロトコルの仕様を何らかの計算モデルに基づいて形式的に記述し，次にその記述が安全性に関する性質を満たすか否かを判定する，という手順で行われる．これにより，設計者の直観や経験を排除して，暗号プロトコルの理論的な安全性を保証することや，安全でない暗号プロトコルの欠陥を検出することが可能となる．しかし，考案されまた実用化されている暗号プロトコルではしばしば，タイムスタンプを用いて情報の新しさを判定しているが，従来の検証法では，時間の経過やタイムスタンプといった時間の概念に対してほとんど注意が払われていなかった．

本論文では，このような時間の概念を含む暗号プロトコルを対象として，その安全性の形式的検証法を提案する．ここで暗号プロトコルが安全であるとは，敵対者が，盗聴等により知り得る情報および利用可能な操作を用いたとしても，目標を達成するのに必要な情報が得られないことと定義する．提案する検証法は，形式化の枠組と判定手続きからなる．形式化のための計算モデルとして，条件付き項書換え系を用いる．時間を非負整数の集合としてモデル化し，敵対者がある情報をいつ所有するかを特別な形の項によって表現する．操作の意味および操作による時間の経過を書換え規則で記述し，タイムスタンプを用いて情報の新しさを判定する操作を条件付き書換え規則で表現する．形式化の段階で，敵対者の能力および目標についても記述する．判定手続きは，形式化の枠組に従って得られた，暗号プロトコルの形式的記述に対して，敵対者の目標となる情報に対応する項が得られるか否かを判定する．本検証法を用いることで，暗号プロトコルを現実に近い形で形式的に記述し，その安全性を議論することが可能となる．

本論文ではさらに，提案した検証法を用いて三つの暗号プロトコルの安全性を検証し，本検証法の有効性を示す．まず，認証と鍵共有を行うある暗号プロトコルについて，それが安全でない，すなわち敵対者が他者になりすまして認証を受け，鍵を共有できることを示す．このプロトコルは，BAN 論理による検証法で安全であると判定されたものである．この検証結果の違いは，時間の概念のモデル化にある．本論文で提案する検証法では，時間を定量的に取り扱っている．そのため，他者を装った通信により情報中のタイムスタンプを更新する方法を発見できた．また，実用化されている認証プロトコル Kerberos を検証し，実際的な使用環境の下で安全であることを示す.

奈良先端科学技術大学院大学 情報科学研究科
計算機言語学講座 (関研究室)
田中 猛彦
takehiko@is.aist-nara.ac.jp

Universal Data Compression Algorithms for Stationary Ergodic Sources Based on the Complexity of Sequences
(系列の複雑度に基づいた定常エルゴード情報源に対するユニバーサル情報圧縮アルゴリズム)

名古屋大学　村松 純 (NTT)

定常エルゴード情報源に対するユニバーサル情報圧縮アルゴリズムを構成する. その構成において, 系列の複雑度 (complexity) の概念を利用する. アルゴリズムの性能は定常エルゴード情報源から出力された系列の複雑度の漸近的性質を通して解析される.

第 1 章では, 本論文で必要となる諸概念の定義と, 情報源符号化に関する定理を紹介する.

第 2 章では複雑度関数 (complexity function), 固定された歪みを許す系列の複雑度 (complexity at a distortion level), 複雑度を固定した時に生ずる歪み (distortion at a complexity level) の定義とその性質について考察する.

最初に, 複雑度が一般的に持っている性質は何であるかに注目し, 新たに複雑度関数 (complexity function) の概念を定義する. 複雑度は有限列の乱雑さを量るものであり, 過去には Kolmogorov, Chaitin, Lempel と Ziv, Rissanen

らによってさまざまに定義されてきた. 本論文の定義はこれらの複雑度の概念を一般化したものである. またこの定義から複雑度関数全体と定常エルゴード情報源に対する無歪みユニバーサル符号全体が, 符号長関数が同じ無歪みユニバーサル符号を同一視すると, 一対一に対応することを証明できる. 複雑度関数の概念はユニバーサル符号の性質を抽象化したもので, それがどのように構成されているかに立ち入らずにその定量的な性質を解析することができる.

次に, 固定された歪みを許す系列の複雑度を定義する. それは, 元の系列との誤差がある固定された歪みの範囲内にあるような系列の中での複雑度の最小値として定義される. そして, 系列が定常エルゴード情報源から出力されていると仮定すると, 情報源出力の 1 文字あたりの固定された歪みを許す系列の複雑度は系列の長さが長くなるにつれて, その情報源のレート歪み関数 (rate-distortion function) に収束することを証明した. Yang と Shen はこの定理を Kolmogorov-Chaitin の複雑度関数の場合に対して証明している. また, Yang と Kieffer は複雑度関数が Lempel-Ziv 符号の符号長関数である場合を証明している. 本論文の結果はこれらの結果を任意の複雑度関数に対して一般化したものである.

上記の固定された歪みを許す系列の複雑度の性質は無歪みユニバーサル情報圧縮アルゴリズムを利用した歪みを許すユニバーサル情報圧縮アルゴリズムの性能解析に応用することが出来る. アルゴリズムは二つの段階で構成される. 最初に情報源の出力との歪みが許された範囲内にある系列を一つ選ぶ. 次にその系列を先に固定した無歪みユニバーサル符号で圧縮する. この構成において, 情報源の出力との歪みが許された範囲内にある系列は第 2 段階で用いた無歪みユニバーサル符号によってもっとも効率良く圧縮できるようなものを選び出すことによって実現される. 本論文の結果は, 任意の無歪みユニバーサル符号から構成されるこのアルゴリズムが任意の定常エルゴード情報源に対してレート歪み関数の圧縮限界を達成することを示している.

次に, 固定された歪みを許す系列の複雑度に対応する量として, 複雑度を固定した時に生ずる歪みを定義する. それは系列を記述するための情報量を固定した時に, どの程度の歪みが生じてしまうかを量るものである. そして系列が定常エルゴード情報源から出力されている時に, 複雑度を固定した時に生ずる歪みは複雑度を系列の長さに比例して大きくゆくと, 歪みレート関数 (distortion-rate function) に収束することを証明する. Yang と Kieffer は上記の定理を複雑度関数が Lemplel-Ziv 符号の符号長関数である場合に証明している. 本論文ではこれを一般の複雑度関数に対して拡張したものである. このの定理は固定レートの歪みを許すユニバーサル情報圧縮アルゴリズムの構成に応用出来る.

第 3 章では, 複雑度関数を利用したユニバーサルデータベース (universal data-base) について考察する.

符号器と復号器が共通のデータベース系列を持っている場合を考える. この場合, 情報源の出力を以下の通りに伝送することが出来る. 符号器はデータベースを参照して与えられた情報源出力に合う系列を探し, それに対応する参照番号を符号化して伝送する. 復号器は符号化された参照番号を復号してデータベースの中の参照番号に対応する系列を得る. 情報源出力そのものを符号化して送るのではなく, データベースの参照番号を符号化して送ることによって情報圧縮を構成できる. この時符号化レートは参照番号を符号化した時の長さを情報源出力の長さで割ったものになる.

データベースがユニバーサルであるとは, その構成において情報源の統計的性質に関する事前の知識がないということを指し, 最適であるとは, 任意の情報源に対してその符号化レートが最適になることである.

参照番号の符号化レートの漸近的な性能に関して多くの結果が報告されている. 無歪みの場合, Wyner と Ziv, Nobel と Wyner, Ornstein と Weiss, Ornstein と Shields による結果がある. これらの結果はいずれも出力された系列に依存してデータベースを構成する必要がある. 歪みを許す場合は Ornstein と Shields, Zhang と Wei, Zhang と Yang, Steinberg と Gutman, Kanaya と Muramatsu, Koga と Arimoto, Yang と Kieffer らによる結果がある. これらの結果はいずれも出力された系列に依存してデータベースを構成する必要があり, また, 情報源の性質に課した条件が厳しいものであった. また, 構成は決定的なものではなく, ある種のランダムな系列を利用したものであった.

本論文では, 出力された系列に依存しないユニバーサルデータベースを構成して, それが全てのエルゴード情報源に対して最適であることを証明する. データベース系列の構成は複雑度関数に基づいている. それは, 系列を複雑度の小さい順に並べたものである. さらに, データベース系列はランダム系列を利用せず, 決定的な手続きで構成される.

このユニバーサルデータベースは, 固定レートのユニバーサル符号の構成にも利用できる. 固定レートのユニバーサル符号は Ziv や Neuhoff と Gray と Davisson によってその存在が議論されている. 本論文ではユニバーサルデータベースの固定レートでの符号化における最適性も証明される.

第 4 章では符号器と復号器が共に情報源 Xと相関のある情報源 Yの出力を見ることが出来る時に, 情報源 Xを符号化する問題について考察する.

この問題は無歪みの場合は Slepian と Wolf による相関のある情報源の符号化, そして, 歪みを許す場合は Wyner と Ziv による復号器に補助情報を伴うときの情報源符号化の問題と関係があり, 本論文の枠組はこれらの研究において符号器は情報源 Xの出力しか見ることが出来ない場合に該当する. しかし, この一般性をなくすかわりに本論文では符号器と復号器が共通の情報を利用できる場合の漸近的に最適な可変長ユニバーサル符号を考える. これが前述の結果と本論文の結果の明白な違いである. 実際, 無歪みの場合で符号器が補助情報の出力を見ることが出来ない場合はユニバーサルな符号器を構成することは出来ないことを証明することができる.

無歪みの場合は, Slepian と Wolf, Cover, Miyake と Kanaya らによる結果があるが, これらの結果において, 符号はある種の乱数の系列を利用した構成になっている. 本論文における符号器の構成はランダム符号の議論を用いずに, 決定的な手続きで構成している. 最近になって, Sub-

rahmanya と Berger がユニバーサルな符号器を提案しているが, 漸近的最良性の証明はなされていない.

歪みを許す場合において, 符号化レート限界は Wyner と Ziv, Miyake と Kanaya, Leiner と Gray らによって示された. しかし, 無歪みの場合と同様, 彼らの証明もまたランダムの系列を利用した符号の構成を用いている. これに対して, 本論文では決定的な手続きで共通の情報を伴う歪みを許すユニバーサル符号器を構成する. そのために, 第 2 章で与えた固定された歪みを許す系列の複雑度の概念を拡張する. 最初に共通の情報を伴う無歪みユニバーサル符号の符号長関数を抽象化した条件付複雑度 (condititional complexity) の概念を定義する. 次に, 条件付複雑度から導かれる固定された歪みを許す系列の条件付複雑度 (conditional complexity at a distortion level) の概念を定義する. そしてそれが任意の定常エルゴード情報源に対して情報源出力の長さが長くなるにつれて, その情報源の条件付レート歪み関数に近付くことを証明する. この結果を利用して共通の情報を伴う無歪みユニバーサル情報圧縮アルゴリズムを利用した共通の情報を伴う歪みを許すユニバーサル情報圧縮アルゴリズムの最適性の証明を与える.

NTT コミュニケーション科学研究所
小山特別研究室
村松 純 (Jun MURAMATSU)
Email: pure@cslab.kecl.ntt.co.jp

筆跡および音声に現れる身体的特性からのカテゴリの抽出と個人認証方式への応用に関する研究

早稲田大学 山崎　恭 (早大)

近年、情報通信システムのネットワーク化、パーソナル化の進展に伴い、個人情報がさまざまな形態で扱われるようになり、システム利用者のプライバシーを守るセキュリティ技術の確立がより重要な課題となってきている。しかし、システム利用者を特定するための個人認証技術として従来用いられてきたカードやパスワード等の本人の所有や知識に基づく個人認証システムでは、カードの紛失やパスワードの忘失といった安全性に関する問題とともに、ユーザの物理的・心理的負担をいかに軽減するかということが依然解決すべき課題として残されている。

そこで、この問題に対処すべく、日常的なコミュニケーション手段の要素である筆跡、音声といった個人の身体的特性に着目し、それらを用いて本人を特定するための個人認証技術に関する研究が従来から盛んに行われている。しかしながら、従来の研究では、個々の身体的特性のある一面に着目した場合の個人の特徴（以下、個人性）について論じられることは多いものの、個々の身体的特性を複数の観点から多面的にとらえたときの個人性についてはあまり論じられていない。一方、我々人間が個人の特定を行う場合には、特定対象となる個人の身体的特性をさまざまな切り口で観察し、そこから得られる個人性を複合して対象の特定を行っていると考えられる。このように、個人性を複数の観点から多面的にとらえることにより、個人性の変動に柔軟に対応でき、また多様な個人性の統合による信頼性の高い認証が可能になると考えられるが、この考え方を個人認証アルゴリズムに適用した研究事例は少ない。また、従来の研究では、本人を特定するのに有効なパラメータ（以下、特徴パラメータ）をいかに抽出するかということについての検討は数多くあるが、これらのパラメータを、文字や音声の認識といった本人の特定以外の目的にも使用することについての検討はほとんど行われていない。一方、個人の身体的特性より抽出される筆跡や音声は、本人の特定に有効であるのみならず、端末に対する簡易な情報入力手段としても優れた性質を有している。したがって、利用者・端末間のインタラクティブ性を重視したより使い易いヒューマンインタフェースを具備した個人認証方式を実現するためには、個人認証技術を文字認識技術や音声認識技術と融合し、利用者の認証のみならず、利用者の音声あるいは筆記内容の認識まで取り入れることの可能な個人認証アルゴリズムについての基礎的な検討が不可欠であると考えられる。

以上を研究動機として、本論文は、筆跡、音声といった個人の身体的特性に基づく個人認証を対象とし、より信頼性の高い個人認証に必要となる新たな個人認証アルゴリズムの提案とその信頼性を評価した結果についてまとめたものである。本論文は、以下に述べるように全６章から構成されている。

第１章は序論であり、研究の背景と論文の概要を述べている。

第２章「カテゴリ化された身体的特性に基づく個人性抽出手法の提案」では、従来検討されてきた個人の身体的特性に基づく個人認証方式の問題点を抽出し、信頼性の高い個人認証を実現するために必要となる新たな個人認証アルゴリズムを提案している。本章では、特に個人認証アルゴリズムの中核をなす個人性の抽出手法を中心に検討を加えた。提案する個人性の抽出手法は、身体的特性より抽出した特徴パラメータを、全利用者に共通する複数のグループ（以下、カテゴリ）に分類し、個人の特徴の現れ方に応じた重み付けを施して本人を確認する点に特徴がある。本提案は、我々人間が他人を特定する際に、特定対象となる人物の身体的特性を多面的にとらえている点に着目し、そのメカニズムを個人認証アルゴリズムに適用したものである。従来、特徴の現れ方に関係なく一律に扱われることの多かった特徴パラメータを、このように複数のカテゴリに分類することにより、各カテゴリに現れる利用者間の特徴の差異を詳細に解析することが可能となる。また、各カテゴリは、利用者に依存しない共通の特徴要素からなるため、個人性の抽出のみならず、筆記内容や発声内容の認識にも使用することができ、この性質を利用することにより、本人を特定する個人認証技術と内容を認識する認識技術とを効果的に組み合わせた高度なヒューマンインタフェースを具備する個人認証方式を実現することが可能となる。さらに、提案手法では、個人の特徴を登録・照合する際に使用するテキストに依存しない個人性の抽出が可能であるため、テキストを固定することの多い従来の個人認証方式に対し、登録時と照合時に異なるテキストを使用することの可能な、テキスト選択の自由度の高い個人認証方式を構築

することができる。この特徴は、詐称者に対する耐性の高さや利用者に対する利便性の高さの点で優れている。第２章で提案する個人性の抽出手法は、身体的特性の種類を問わない普遍性の高い特徴抽出手法であることも明記すべき特徴の一つである。

第３章「筆跡情報からのカテゴリの抽出」では、第２章で述べたカテゴリに基づく個人性抽出手法の一例として、個人の身体的特性の一つである筆跡情報に着目し、信頼性の高い筆者認識手法の確立に必要となる新たな個人性の抽出手法を提案している。提案手法では、テキストを固定する従来の署名照合とは異なり、字種への依存度を可変とする特徴パラメータを使用することで、登録時と照合時に異なる字種を用いることが可能となっている。本提案では、オンラインでサンプリングされた筆跡におけるストローク差分角度を特徴パラメータとし、筆順に沿って一画ずつ抽出された一組の点画と空画を特徴パラメータの抽出単位とする。次に、抽出した特徴パラメータを、平面上の曲線を周波数領域で記述するフーリエ記述子の一つであるＰ形フーリエ記述子に変換し、記述子の低周波成分から得られる筆跡の概形を登録・照合時の特徴量とする。また、カテゴリに関しては、多数の筆者から採取したさまざまな形状を含む特徴パラメータに、ベクトル量子化器の設計アルゴリズムである LBG アルゴリズムを適用してカテゴリを作成し、個人性の抽出には学習ベクトル量子化法 (LVQ) を適用する。重み付けに関しては、各カテゴリを対象とし、個人の特徴が現れ易いカテゴリを強調する重み付けと、カテゴリ間での個人性の現れ方を強調する重み付けの二条件を考慮した重み付けを行う。本章では、実際の筆記データを用いたシミュレーション実験により提案手法の信頼性を評価し、提案手法により字種に依存しない個人性情報の抽出が可能であること、また、個人の特徴の現れ易さは各カテゴリごと、各筆者ごとに異なり、個人の特徴の現れ方に応じた重み付けを施すことにより、認識の精度が向上することを明らかにする。

第４章「テキスト提示型筆者照合方式」では、オンライン筆者照合のさらなる信頼性の向上を目的とし、照合時にシステム側から任意のテキストを指定することの可能なテキスト提示型筆者照合方式を提案し、第３章で述べたカテゴリに基づく個人性の抽出手法に提案方式を適用する方法について述べている。第３章で提案した個人性の抽出手法に基づき筆者照合を行う場合、照合時に筆者が任意のテキストを選択できる一方で、選択されたテキストに含まれる字種や文字数による照合精度の変動が問題となる。すなわち、テキスト選択の自由度を損なうことなく照合の精度を確保するためには、照合時に入力するテキストをいかに選択するかという問題を解決する必要がある。そこで、この問題点を解決する一手法として、本章では、チャレンジ・レスポンス型認証手順に基づく新たな筆者照合方式（以下、テキスト提示型筆者照合方式）を提案する。本章で提案するテキスト提示型筆者照合方式は、照合時のテキストを可変とし、システム側から提示されたテキストが、正筆者により正しく入力されたときにのみ本人を受理する点に特徴がある。また、提案方式では、個人性を抽出するためのカテゴリとテキストを照合するためのカテゴリを共通化することで、本人を確認するために使用されるカテゴリと同一のカテゴリを用いて、提示されたテキストの照合を行える点も特色の一つとなっている。さらに、本章では個人性の抽出に適したカテゴリを作成するアルゴリズムとして、LBG アルゴリズムをベースとした新たなクラスタリングアルゴリズム（以下、アルゴリズム A）を提案する。アルゴリズム A は、特徴空間におけるパターンの分布状態を評価しながら、クラスタリングの過程でコードブックのレベル数を決定する点に特徴がある。ここでは、実際の筆記データを用いたシミュレーション実験により提案方式の信頼性を評価し、照合時の字種を選択しない方式に比べ、本人の特徴の現れ易い字種をシステム側で選択できる提案方式の方が信頼性の点で優れていることを示す。また、テキストの照合精度に関しては、システムの提示したテキストを筆者が正しく入力したときにのみ筆者を照合することが可能であることを示す。

第５章「音声情報からのカテゴリの抽出と話者照合方式への応用」では、第２章で述べたカテゴリに基づく個人性抽出手法のもう一つの適用例として、個人の身体的特性の一つである音声情報に着目した個人認証アルゴリズムを提案している。提案手法では、話者の発声内容に依存しない特徴パラメータを使用することで、登録時と照合時に異なる音声を用いることが可能となっている。提案手法では、従来の話者認識で有効性が評価されているケプストラムを特徴パラメータとし、カテゴリの作成および個人性の抽出に関しては、筆跡の場合と同様、アルゴリズム A および学習ベクトル量子化法 (LVQ) を適用する。また、重み付けに関しても、筆跡の場合と同様に各カテゴリおよび各個人を対象とした重み付けを行う。本章では、提案手法の信頼性を実際の音声データを用いたシミュレーション実験により評価し、提案手法により発声内容に依存しない個人性情報の抽出が可能であること、また、個人の特徴の現れ易さは各カテゴリごと、各話者ごとに異なり、個人の特徴の現れ方に応じた重み付けを施すことにより、認識の精度が向上することを明らかにする。

第６章は結論であり、本論文で得られた成果を総括している。

早稲田大学大学院 理工学研究科
山崎 恭
〒 169–8555 東京都新宿区大久保 3–4–1
早稲田大学理工学部 電子・情報通信学科 小松研究室
TEL: 03–5286–3390
FAX: 03–5273–7367
Email: yamazaki@kom.comm.waseda.ac.jp

1998 IEEE Information Theory Workshop

古賀 弘樹 (東京大学)

1998 IEEE Information Theory Workshop (ITW'98) は，1998 年 6 月 22 日から 6 月 26 日にかけて，アイルランド南部の町 Killarney の Great Southen Hotel で開催されました．Killarney はアイルランドの首都 Dublin から列車で 4 時間ほど，アイルランド第二の都市 Cork からバスで 1 時間ほどの所にある小さな町です．Killarney は Killarney 国立公園のちょうど入口にあたることもあり，町には観光客や観光客のための馬車 (国立公園の中はエンジンを搭載している乗り物は禁止されている) も多く見られました．このITW'98 の開催時期は，昼が長く緑も美しいヨーロッパのベストシーズン (だと個人的には思っている) である夏至のころと重なっていますので，この町の賑わいも理解できるというものです．しかし残念ながら，このITW'98 の期間中は半袖では肌寒い小雨混じりの日が続きました．もっとも，この天気の悪さが「一日に 4 つの四季をもつ」と言われる南アイルランド特有の変わりやすい気候そのものなのか，または単にITW'98 参加者の運が悪いだけなのかは未だに謎のままですが．

ご存知の方も多いとは思いますが，ITW はISIT(International Symposium on Information Theory, 約 1 年半おきに開催) とは独立に，ほぼ年に 1 回の割合で開かれている情報理論関連の学会です．今回の ITW'98 の参加者は全部で 127 人で，日本からの参加者は，今井先生 (東大生産研)，阪田先生 (電通大)，山本先生 (東大)，植松先生 (東工大)，古賀の 5 人でした．ITW と ISIT の一番の大きな違いは，ISIT が 6~8 パラレルセッションあるのに対し，ITW のセッションは基本的にシリアルで，いくつかの話題に絞って詳細に講演者の話を聞こうとする姿勢にあるといえましょう．今回の ITW'98 は下の表のようなセッション構成になっていました．

	セッション名	講演数
月曜午前	Coded Modulation	6
月曜午後	Source Coding	6
火曜午前	Algebraic Geometry Code	9
火曜午後	Coding Theory	6
水曜午前	Shannon Theory	7
木曜午前	Decoding	7
木曜午後	Contributed Session A	12
木曜午後	Contributed Session B	11
金曜午後	Network	7
金曜午後	Cryptography	6

唯一 2 パラレルセッションで行われた Contributed Session を除くと，1 つの発表あたりの持ち時間は 25~30 分で ISIT と比べると長く，このあたりに ITW らしさが表れているといえるでしょう．各セッションの構成はそのセッションのオーガナイザに任されているようで，例えば今回の Shannon 理論のセッションのように多重アクセス通信路に焦点を絞ったセッションもあれば，暗号のセッションのように特にテーマを決めないセッションもあったようです．今回の ITW'98 では Prenary talk はなく，また Excursion が水曜日の午後に，Banquet が木曜日の夕方にそれぞれ行われました．

私自身が興味深いと思ったのは Contributed Session A の中の，Kieffer と Yang の "Design of Context-Free Grammers for Lossless Data Compression" と，Zamir と Shamai の "Nested Linear/Lattice Codes for Wyner-Ziv Encoding" という 2 つの講演です．前者は文脈自由文法を用いた無歪ユニバーサルデータ圧縮に関する話題で，最大マッチを新たな 1 シンボルで置き換えるという単純な文法を用いて長さ n の系列を圧縮したときに，冗長度が $O(\frac{1}{\log n})$ になることが証明できるというものでした．Kieffer は，この話を完成させるために彼の sabbatical year の多くを費したそうです．後者は，有名な多端子通信システムである Wyner-Ziv システムに対する漸近最良の符号を構成することが目標で，ある特殊な場合には漸近最良性をもつ符号が Lattice を用いて構成できるという話だったと思います．この他にも興味深い話はあり，興味をお持ちの方は是非予稿集をご覧になって頂きたいのですが，例えば Shannon Theory のセッション中の Verdú と Shamai の共著の論文は，同様の興味をもっている人が多いのか，講演の後でも熱心な議論が続けられていたようです．

次の ITW は 1999 年の 6 月 20 日–25 日に，南アフリカ共和国の Kruger 国立公園で行われます．さらに南アフリカでの ITW に引き続き，6 月 27 日–7 月 1 日に，1999 Information Theory and Networking Workshop がギリシャの Metsovo で開催されることになっています．(詳細は `http://it.ucsd.edu` から辿れます．) この 2 つのワークショップは互いに相補的になるようにオーガナイズされるという話ですし，再び興味深い話が聴けると思いますので，ご興味のおありの方は参加されてみて下さい．南アフリカからギリシャ行きの直行便もあるそうです．

東京大学
古賀 弘樹
koga@sr3.t.u-tokyo.ac.jp

The First Advanced Encryption Standard Candidate Conference

神田 雅透 (NTT)

The First Advanced Encryption Standard (AES) Candidate Conference は、1998 年 8 月 20 日から 22 日の日程で、カリフォルニア州 Ventura の DoubleTree Hotel において、世界約 30ヶ国から約 200 名の暗号研究者等 (日本からは 16 名) を集めて開催されました。この会議は、次世代米国政府標準暗号となる AES 暗号を選定するために、NIST (National Institute of Standards and Technology) が主催して開催されたものです。

現在の米国政府標準暗号は、DES (Data Encryption Standard) 暗号と呼ばれています。DES 暗号は NBS (National Bureau of Standards, NIST の前身) が 1977 年に策定したものですが、すでに 20 年が経過し、最近ではその安全性に疑問符がつけられるようになりました。特に、RSA Data Security 社が主催している DES Challenge II (http://www.rsa.com/rsalabs/des2/) において、1998 年 7 月 17 日に米国の Electronic Frontier Foundation (EFF) のグループが約 25 万ドルで開発した専用解読装置によってわずか 3 日で解読されてしまった事実 (http://www.eff.org/descracker.html) は、DES 暗号の寿命がそう遠くない時期に完全に尽きてしまうことの証明ともいえます。また、NIST によって DES 暗号の安全性に関する再評価が 5 年ごとに行われることになっており、1998 年はその再評価の年に当たっていました。しかし、NIST はすでに 1998 年の再評価は行わないことを決定しています。

このため、NIST が中心となって、DES 暗号の後継となる次世代米国政府標準暗号 AES の選定を進めることになり、1997 年 9 月にインターネットを通じて全世界に対して、AES 暗号候補の公募要領を公開しました。そして、1998 年 6 月 15 日に締め切られたこの公募に対して、全世界から 21 件の応募があり、そのうち書類審査を通過した 15 件 (うち米国からは 5 件、日本からは NTT の 1 件) が最終的に NIST によって AES 暗号の候補として受理されました。

AES 暗号の選定までのスケジュールとしては、今回公開された 15 件から 5 件に絞る Round 1 と、5 件から AES 暗号を選定する Round 2 の評価期間を設けています。NIST は、AES Candidate Conference(今回を含めて両方の評価期間中に合計 3 回開催される予定) での議論や各候補のコメント等を参考にして、AES 暗号をできるだけ公開の場で選定することを表明しています。なお、これらの詳細について興味がある方は、AES のホームページ http://csrc.nist.gov/encryption/aes/aes_home.htm を参照してください。

さて、第 1 回目である今回の会議は、受理された 15 件の候補を正式に一般に公開する目的で開催されました。いわば、お披露目の場です。各暗号候補の提案者には、質疑応答の時間を含めて 45 分 (発表時間は 30-35 分程度) が割り当てられ、そのなかで提案した暗号の仕様や設計方針、実装速度、安全性の評価などをアピールするようになっていました。なかでも、NIST の意向があったこともあり、設計方針と実装速度を重点的に明らかにしたものが多かったことが特徴的であったように思われます。しかし、お披露目とはいっても、このように、世界中の第一線の共通鍵暗号研究者が多数集う場において、候補の暗号方式が一斉に発表させると、提案者が予期しないようなバグ (あるいは不注意?) が見つかるものです。これこそが、NIST の目論見ともいえるのですが、“MAGENTA”のように発表直後の質疑応答で即座に解読されてしまった候補もあります。それだけに、私を含め提案者側である NTT の人間にとっては、NTT の新暗号 E2 のお披露目の場というよりは、むしろ判決を待つ身に近いように感じました。無事に発表を終えた今、E2 も名実ともに AES 候補として国際的にも認知されたかと思います。

会議場の外では、今回の会議で Round 1 の評価期間が正式にスタートしたことになるため、参加者は 15 件の候補の中のどれが有望であるのか、あるいは解読できるのかといった意見交換が活発に行われていました。特に、“選抜する”という目的のために会議が開催されていますから、どうしても通常の国際学会とは異なり、研究成果を議論するというよりは候補となっている暗号のバグを見つけだすことにエネルギーが費やされているという点が特徴的であったように思われます。NIST の Miles E. Smid 氏が述べた、「ローマ (次回の AES Conference の開催地) といえばコロシアム。15 候補はまさに奴隷であり、猛獣が暗号研究者達である。どの奴隷が生き残れるか。NIST はそれを見守るローマ皇帝だ。」という台詞が今後をまさに象徴している発言でした。

AES 暗号は、DES 暗号の後継とはいえ、本来、米国の公官庁が使用することを目的とした暗号です。にもかかわらず、全世界に対して公募を行い、できるだけオープンな場で AES 暗号を選定しようとする方針は、米国が 21 世紀も情報セキュリティの分野で世界の盟主でありたいと強く願う意図を感じます。一方で、これだけオープンな場で行うことを表明した以上、下手な決着の仕方をすれば AES 暗号の信頼性そのものを失墜させてしまうことになりかねません。ただ、今回の試み自体が壮大な実験であり、そしてこの試みによって、暗号解読技術が進展することはまず間違いないでしょう。その意味で、今回の会議全体を通じて、参加者は今回の試みをかなり好意的に受け止めているように感じましたし、私も今後を期待しています。(もっともそれが米国政府の思惑通りになるのかどうかはわかりませんが、、、、)

なお、今後の予定では、1999 年 3 月 22 日と 23 日に Second AES Candidate Conference がローマで開催されることが決まっています。ここでは、候補アルゴリズムに対する解析結果、解読法などが報告される予定となっています。

NTT 情報通信研究所
神田 雅透
Email: kanda@sucaba.isl.ntt.co.jp

CRYPTO 98 参加報告

報告者： NEC C&C メディア研究所 佐古 和恵

【 日程 】 1998 年 8 月 23 日〜27 日
【 会場 】 University of California Santa Barbara
【 主催 】 IACR
【参加者】 約 500 名 うち日本より 35 名弱
【発表数】 33 件, 招待講演 3 件, Rump Session 43 件

年々参加者数が増えている本会議であるが、今年は AES 会議と連続して開催されたこともあって、世界中から 500 名もの聴講者が集まった。報告者はプログラム委員として参加し、セッションチェアを務めた。

今年は Technion 大の Hugo Krawczyk プログラム委員長のもと、144 件の投稿論文うち、33 件が採択された。理論的成果の進展が多数見受けられたが、特にインパクトの大きい下記 4 点について述べる。

- SSL などに使われている PKCS#1 のフォーマットによる RSA 暗号は選択暗号文攻撃により解読可能であることを Bleichenbacher が報告した。この解読手法を適用すると、下記のような状況が可能になる。あるクライアントからサーバにおくられる同フォーマットの暗号文を解読したいとする。攻撃者はその暗号文を変形した変形暗号文を多数作り、これをサーバに送り付ける。サーバは変形暗号文を復号した結果が同フォーマットに準拠していないとエラーメッセージを返答する。本解読方法では、この応答を利用してもともとの暗号文の推定を可能にする。対策として RSA 社は PKCS#1 の ver2 を提案している。

- Shoup らが adaptive chosen ciphertext attack に強いことを証明できる公開鍵暗号を提案した。このような強い性質をもつ暗号アルゴリズムを具体的に DH 判定問題に基づいて構築できた意義は大きい。

- Rump session で Shamir が Impossible differential attacks という共通鍵暗号の新解読方法を発表した。内容は「differential cryptanalysis に強いように入出力に特定の関係が生じる確率を小さくするという手法が取られているが、逆に、特定の関係が生じる確率が 0 に近いとそれを利用して攻撃できる」というもので、実際 Biham らが IDEA や skipjack に適用して今までよりも効率のよい攻撃に成功した。

- 同じく Rump session で Kocher ら Electronic Frontier Foundation (EFF) のグループが開発した DES 専用暗号解読装置についての報告があった。本装置により RSA 社の DES 懸賞問題の解読に 56 時間で成功したため、この場で Rivest 教授から賞金の 1 万ドルの贈呈式が行われた。なお、装置開発には約 25 万ドルの費用がかかっている。

来年は 8 月 15 日から 19 日まで、同キャンパスで Program Chair Mike Wiener、General Chair Don Beaver で開催される。詳細は `http://www.iacr.org` を参照されたい。

本年度から電子投稿が可能になり、電子的な予稿集も Springer-Verlag 社より販売される予定である。また、同社は 97 年までの全 Crypto, Eurocrypt の論文を 1 枚に収めた CD-ROM の発行も準備中であり、文献の検索が今後一層便利になると思われる。

情報論的学習理論ワークショップ (IBIS'98) 開催報告

山西 健司 (NEC)

会議名： 1998 年情報論的学習理論ワークショップ
(1998 Workshop on Information-Based Induction Sciences (IBIS'98))
主催： 情報理論とその応用学会
協賛： 電子情報通信学会情報理論研究専門委員会、人工知能学会
場所： 神奈川県足柄下郡箱根町 専修大学箱根セミナーハウス
日時： 1998 年 7 月 11,12 日
参加人数： 95 名
発表数： 招待講演 13 件、impromptu 講演 10 件、セッション数：8
実行世話役： 山西 健司, 竹内 純一、中村 勝洋 (NEC)
会場世話役： 佐藤 創

本会議 (IBIS'98) は、人工知能における「機械学習」に関する問題を情報理論、統計学, 統計物理学等の視点から総合的に捉えた新しい知識情報処理の体系を目指して、「情報論的学習理論」なる旗のもとに企画したワークショップでした。

本会議で扱ったテーマとしては、知識情報処理における統計的モデル選択 (AIC, MDL 等)、オンライン学習、確率的コンプレキシティ、ベイズ学習、統計力学的学習、幾何学的学習、各種知識表現系 (ニューロ、ベイジアンネット等)、計算論的統計学、Kolmogorov コンプレキシティ理論、応用 (画像処理、理解、自然言語処理、複雑系) などが挙げられます。

本企画の意図は、様々な分野に分散していながら上記テーマに関して共通の問題意識をもっていた研究者が交流を深め、最新の成果について情報交換できるような場を提供することでした。当初は、30 名程が集まる小さなワークショップを想定していました。しかし、いざ蓋を開けてみると、参加者数は 90 余名に膨れ、大変活気のある学際的な会議となりました。実際、SITA 以外からも統計、物理、ニューロ、AI、画像、自然言語、計算機科学の分野から、主に若手の研究者がそれぞれ 10–20 名程度づつ参加しました。(SITA 会員は全体の約 2 割でした。) これは、「学習」を通じて情報論的手法が他分野からいかに注目されているかを示すものでありましょう。

発表は統計的モデル選択の問題が中心でした。情報源符号化の文脈で誕生した MDL(Minimum Description Length) 原理が知識処理のための仮説選択原理として応用されてから 10 余年が経ちます。本会議では「MDL その後」に関する様々な結果が発表されました。伊藤先生 (電通大)、李氏 (NEC)、鈴木先生 (阪大) の講演では、それぞれ MDL の画像セグメント化、自然言語の構文解析、ベイジアンネット学習への応用が示されました。MDL が用いられるまでのモデリング、MDL 解の探索アルゴリズム、強一致性の証明などに新しい知見がありました。MDL 以外の規準については、幾何学的情報量規準 (金谷先生 (群馬大))、モデル選択そのもののばらつきの評価規準と AIC(下平先生 (統数研))、ミニマックス リグレット解析 (竹内氏 (NEC)) の発表があり、モデル選択理論の深さとますますの発展可能性が示唆されました。

また、学習の問題は情報理論的枠組では捉え切れない場合も多くあります。情報理論的な設定はあくまで、知識表現が「確率分布」であり、歪み尺度を「対数損失」で測った特殊な場合です。そこで、推定や予測の問題を、一般の歪み尺度を許すような統計的決定理論の枠組で捉え直す立場からの発表がありました。例えば、ベイズ決定理論における最適推論と学習との関係を示した講演 (松嶋先生 (早大)) や、Rissanen の確率的コンプレキシティを統計的決定理論の枠組に拡張した ESC (Extended Stochastic Complexity) の提案と、これに基づく最適学習アルゴリズムの導出 (山西 (NEC)) や、一般化誤差最小規準のもとでのパラメータ推定における正規化項の最適選択 (村田先生 (理研)) などの発表がありました。いずれも確率論の域を越える新しい学習パラダイムを提示するものでした。

テーマはモデル選択や予測問題にとどまっていたわけではありません。甘利先生 (理研) からは、信号処理の分野でホットな独立成分解析を情報幾何学に結び付ける話がありました。また、樺島先生 (東工大) の「統計力学的学習」や上田氏 (NTT) の「確定的アニーリング」の発表は、「学習」を通じて情報理論と統計力学をつなぐ興味深いものでした。

本会議の反省点として、 時間的スケジュールがタイトであったため、参加者がフリーに議論する時間が少かったことが挙げられます。また、MDL と AIC が直接ぶつかりあうようなパネル討論も企画すれば、より盛り上がったのではないかと思います。

会議を終えて、「このような会議が以前から欲しかった」、「今後も続けて欲しい」との声を多く頂きました。こうした意見は反映させていきたいと思います。

尚、上記レポートでは講演の極一部しか紹介出来ませんでしたが、他にも興味深い講演は沢山ありました。詳細は予稿集で御覧になれます。予稿集をお求めになりたい方は tak@ccm.cl.nec.co.jp(竹内 純一 (NEC)) まで御連絡下さるようお願い致します。

企画からのお知らせ

企画理事 山口和彦（電通大）

今、情報理論とその応用学会企画では、以下の講演会シンポジウムの計画を進めています。

- 情報理論ゴールデンジュビリーアワード記念講演会　－今井・平川法から、ターボ符号まで－
  平成 10 年 11 月 27 日（金）詳細は次ページの案内を御参照下さい

- シャノン理論 50 年：SITA 20 年記念ワークショップ　－アールスウェーデ教授を迎えて－
  平成 11 年 1 月 22 日（金）〜1 月 24 日（日）

- 「電子透かし技術とディジタル著作権」講習会平成 11 年冬を予定
- ハーゲナウアー教授による「ターボ符号」講習会平成 11 年 3 月を予定

最新の情報は http://www.lit.cs.uec.ac.jp/sita/を御覧下さい。sita-ml でも随時御案内する予定です。

情報理論とその応用学会ロゴマーク募集結果のお知らせ

庶務理事 藤原 融 (阪大)

情報理論とその応用学会では, 情報理論とその応用 (SITA) シンポジウム 20 回開催を記念して, 学会のマークを募集いたしました.

４点の応募があり, 理事会で慎重審議の結果, 残念ながら入選作品なしとし, ３点を佳作として選定致しました.

佳作の作品は,

http://www-itl.ics.es.osaka-u.ac.jp/logo.html

にありますので御覧下さい。

情報理論ゴールデンジュビリーアワード記念講演会

－今井・平川法から、ターボ符号まで－

シャノンが A mathematical theory of communication を１９４８年に発表してから５０年、人間の生活は目まぐるしく変わりました。その大きな要素にシャノン理論を基礎とする通信・記録技術の進展があります。IEEE 情報理論ソサイエティは、この５０周年を振り返って、この分野での優れた基礎的業績および論文に対して、ゴールデンジュビリーアワード（50 周年記念賞）を授与しました。　日本人による研究としては、今井、平川両氏により発表された論文がこの表彰を受けました。後に今井・平川法と呼ばれるこの研究は、多値変調に適する誤り制御方式として、Ungerboeck と同時期に符号化変調の基本的概念を提示したのみならず、多段階の符号化、多段階復号というアプローチを提示しました。同じくアワードを受賞し、今、符号に関する最もホットなトピックとなっている、フランスの Berou らのターボ符号とも、要素符号に分解される構造を持ち，要素符号個々の復号を基盤にする点，軟判定の適切な利用が重要である点等が共通しています。

IEEE 情報理論東京支部、および情報理論とその応用学会は、この２つの研究にスポットを当てた講演会を以下のように開催します。今井・平川法、ターボ符号に御興味のある方、次世代の通信システムにおける誤り制御について関心をお持ちの方は是非ご参加下さい。また、まわりにこのテーマに興味をお持ちの方がいらっしゃいましたら、本講演会を是非ご紹介下さい。

主催：　IEEE Information Theory Tokyo Chapter 情報理論とその応用学会
協賛：　電子情報通信学会情報理論研究専門委員会
日時：　平成１０年１１月２７日（金）13:00 〜 17:40
会場：　東京大学数理科学研究科　数理科学研究棟　大講義室
交通：　京王電鉄井の頭線　駒場東大前駅下車
アクセス情報：　http://liaison.ms.u-tokyo.ac.jp/Access.html
参加費：無料 (※注：準備の都合上、参加を希望される方はできる限り事前にお申し込み下さい。)

題目：

- 13:00-13:10 開催の挨拶
- 13:10-14:00 「ターボ復号、MAP と SOVA」　山口 和彦 (電通大)
- 14:00-14:50 「マルチレベル符号研究の最近まで」　井坂 元彦 (東大)
- 14:50-15:10 休憩
- 15:10-16:00 「トレリス構造を用いた復号法」　藤原 融 (阪大)
- 16:00-16:50 「ターボ符号の移動通信への応用」　須田 博人・藤原 淳 (NTT DoCoMo)
- 16:50-17:40 「多レベル符号とデジタル放送の誤り制御」　平川 秀治 (東芝)
- 講演会終了後、18:00 頃より、ささやかな懇親会を予定しています。ぜひ、御参加下さい。(若干の会費を申し受ける予定です。御了承下さい。)

申込先：■電子メールの場合: golden@lit.cs.uec.ac.jp
■ Fax の場合: 0424-43-5314　電通大Ｊ科西１　山口和彦
まで、記念講演会参加申込と書いて御連絡下さい。懇親会ご出欠のご予定もできましたらお書き添え下さい。なるべく電子メールを御利用頂くようにお願いします。申し込み期限はありませんが、１１月１９日頃までに御連絡下さると助かります。人数が多い場合は先着順と致します。

国際会議のお知らせ

1998 International Symposium on Information Theory and Its Applications (ISITA '98)

日時	1998 年 10 月 14 日 – 10 月 16 日
場所	Mexico City, Mexico
連絡先	Prof. Kohichi Sakaniwa Dept. of Electrical and Electronic Engineering Tokyo Institute of Technology 2-12-1 O-okayama, Meguro-ku, Tokyo, 152 Japan Email: sakaniwa@ss.titech.ac.jp http://www.academic.ipn.mx/isita98
原稿	締切終了 (1998 年 4 月 30 日)

ASIACRYPT '98

日時	1998 年 10 月 18 日 – 10 月 22 日
場所	Friendship Hotel, Beijing, P.R.China
連絡先	Prof. Keqin Feng, General Chair, ASIACRYPT'98 Graduate School of USTC #19A Yu Quan Road, Beijing 100039, P.R.China Tel: +86-10-6821-3046 Fax: +86-10-6821-0501 Email: acrypt@public2.bta.net.cn http://www.bta.net.cn/asiacrypt98/index.htm
原稿	締切終了 (1998 年 4 月 26 日)

GLOBECOMM '98

日時	1998 年 11 月 8 日 – 11 月 12 日
場所	Darling Harbor, Convention & Exhibition Centre, Sydney, Australia
連絡先	Interim GLOBECOM '98 Secretariat c/o Ollencio D'Souza 149 Milton Street, Ashfield N.S.W. 2131, Australia Email: globecom@elec.uow.edu.au Tel: + 612 9304213 Fax: + 612 9304273 http://www.ozemail.com.au/~globecom/
原稿	締切終了 (1998 年 1 月 31 日)

PKC '99

日時	1999 年 3 月 1 日 – 3 月 3 日
場所	Kamakura Prince Hotel, Kamakura,Kanagawa, Japan
原稿送付先	Email: pkc99@imailab.iis.u-tokyo.ac.jp
連絡先	PKC'99 Secretariat Imai-Lab, the Third Department Institute of Industrial Science, the University of Tokyo 7-22-1 Roppongi, Minato-ku, Tokyo 106-8558, JAPAN Tel: +81 3 3402 6231 ext. 2327 Fax: +81 3 3402 7365 http://hideki.iis.u-tokyo.ac.jp/pkc99/
原稿	締切終了 (1998 年 9 月 25 日)

EUROCRYPT '99

日時　1999 年 5 月 2 日 – 5 月 6 日
場所　Hotel Hilton, Prague, Czech Republic
原稿送付先　Jacques Stern, Program Chair Eurocrypt '99
Department of Mathematics and Computer Science
Ecole Normale Supérieure
4S, rue d'Ulm
7S230 Paris cedex OS, France
連絡先　Jaroslav Hruby, General Chair Eurocrypt '99
Konevova 41, 130 00 Praha 3, Czech Republic
Email: hruby@gcu.cmp.cz
締切日　1998 年 10 月 12 日
(12 ページ原稿)

IEEE International Conference on Communications (ICC '99)

日時　1999 年 6 月 6 日 – 6 月 10 日
場所　Pan Pacific Hotel, Vancouver, B.C., Canada
連絡先　Ms. Peggy Shepard
Venue West Conf. Services Ltd.
#645-375 Water St.
Vancouver, BC, V6B 5C6, Canada
Tel: +1-604-681-5226
Fax: +1-604-681-2503
Email: congress@venue.west.com
原稿送付先　Prof. Vijay K. Bhargava
ICC 9 TPC Chair
Dept. of Elec. & Comp. Eng.
3800 Finnerty Road, P.O. Box 3055
Victoria, BC, Canada V8W 3P6
Fax: +1-250-721-6048
Tel: +1-250-721-8617
Email: bhargava@ece.uvic.ca
http://www.icc99.com/
原稿　締切終了 (1998 年 8 月 15 日)

1999 IEEE Information Theory Workshop

日時　1999 年 6 月 20 日 – 6 月 25 日
場所　Kruger National Park, South Africa
連絡先　Prof. Hendrik Ferreira
Dept. of Electrical Engineering
Rand Afrikaans University
P.O. Box 524, Auckland Park, 2006, South Africa
Email: hcf@ing1.rau.ac.za
Tel: +27 11 489-2463
Fax: +27 11 489-2357
締切日　1999 年 1 月 31 日 (Recent Results,
ISIT スタイルアブストラクト)

CRYPT '99

日時　1999 年 8 月 15 日 – 8 月 19 日
場所　Santa Barbara, California, U.S.A.

The Twentieth IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC'99)

日時　1999 年 9 月 12 日 – 9 月 16 日
場所　Kyoto, Japan

ASIACRYPT '99

日時	1999 年 11 月 15 日 – 11 月 18 日
場所	Singapore
原稿送付先	Dr. Kwok Yan Lam, Co-Chair Asiacrypt '99 School of Computing National University of Singapore Kent Ridge Crescent, Singapore 119260 Email: lamky@comp.nus.edu.sg Tel: +65-8746613 Fax: +65-7794580
連絡先	Dr. Chaoping Xing, Organizing Chair Asiacrypt '99 School of Computing National University of Singapore Kent Ridge Crescent, Singapore 119260 Email: xingcp@comp.nus.edu.sg Tel: +65-8742790 Fax: +65-7794580 http://www.comp.nus.edu.sg/ asia99/
締切日	1999 年 5 月 10 日 (15 ページ以内)

GLOBECOMM '99

日時	1999 年 12 月 5 日 – 12 月 9 日
場所	Rio de Janeiro, Brazil
連絡先	Professor Raimundo Sampaio Neto PUC-Rio/CETUC Rua Marques de Sao Vicente 225-22453-900 Rio de Janeiro, RJ BRAZIL Tel: +55-21-274-3664 Fax: +55-21-274-3664 Email: raimundo@cetuc.puc-rio.br

2000 IEEE International Symposium on Information Theory

日時	2000 年 6 月 25 日 – 6 月 30 日
場所	Sorrento Palace Hotel, Sorrento, Italy
原稿送付先	Prof. Thomas Ericson Linköpings Universitet ISY, Datatransmission SE-581 83 Linköping, Sweden
連絡先	Prof. Giorgio Taricco Dipartimento di Elettronica Politecnico di Torino Corso Duca Degli Abruzzi, 24 I-10129, Torino, Italy Email: taricco@polito.it Tel: +39-11-564-4084 Fax: +39-11-564-4099 http://www.unisa.it/isit2000
締切日	1999 年 9 月 15 日 (拡大アブストラクト (short paper)/ 原稿 (long paper) 送付)

会 員 情 報

新入会会員

(学生会員)　内田 理 (電気通信大)

退会会員

(正会員)　美濃 道彦 (京大)　小倉 久直 (近畿大)　高橋 磐郎 (日大)
浜田 健生 (富士通研)　宮部 義幸 (情報通信研)　松尾 孝美 (大分大)
三枝 一主 (三菱電機)　長谷部 忍 (沖電気)　杉坂 政典 (大分大)
六浦 光一 (信州大)　永野 宏治 (室蘭工大)

学生員から正員へ変更

高橋 明一 (法政大)

会員数　名誉会員 3 名　正会員 434 名　学生会員 21 名
(98/7/15 現在)　賛助会員 19 社

次号のお知らせ

次号は、「私の Key Papers」を中心に 12 月下旬に発行する予定です。

編 集 後 記

ニューズレター第 71 号をお届けします。皆様のご支援により今号もなんとか発行の運びとなりました。

今号は恒例の博士論文特集号ですが、昨年度も多くの方が博士号を取得されたようで、本学会の活動分野の発展を考えましても大変喜ばしいことであると思います。

ニューズレター活性化のため、何か企画提案等ございましたら、どしどしおしらせさい。ニューズレターに対する、御意見、御要望、企画提案等は下の編集理事、幹事までおよせ頂き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@soft.iwate-pu.ac.jp

佐古 和恵 (編集幹事)
〒 216-8555 神奈川県川崎市宮前区宮崎 4–1–1
NEC C& C メディア研究所
Tel. 044-856-2141
Fax. 044-856-2235
E-mail sako@ccm.CL.nec.co.jp

内匠 逸 (編集理事)
〒 466-8555 名古屋市昭和区御器所町
名古屋工業大学知能情報システム学科
Tel. 052-735-5472
Fax. 052-735-5477
E-mail takumi@ics.nitech.ac.jp

松嶋 智子 (編集幹事)
〒 229-1196 神奈川県相模原市橋本台 4-1-1
職業能力開発大学校情報工学科
Tel. 0427-63-9182
Fax. 0427-63-9186
E-mail tomoko@uitec.ac.jp

情報理論とその応用学会事務局
〒 152-8552 東京都目黒区大岡山 2–12–1
東京工業大学 電気電子工学科
植松研究室 気付
Tel. 03–5734–3243　　Fax. 03–5734–2905　　E-mail sita@ss.titech.ac.jp