

論文賞贈呈

(写真：敬称略)

論文賞（第 72 回）は、平成 26 年 10 月から平成 27 年 9 月まで本会和文論文誌・英文論文誌に発表された論文のうちから下記の 12 編を選定して贈呈した。

A Process and Temperature Tolerant Oscillator-Based True Random Number Generator

(英文論文誌 A 平成 26 年 12 月号掲載)



受賞者 天木健彦



受賞者 橋本昌宜



受賞者 尾上孝雄

乱数は高いセキュリティを実現するための基盤技術の一つである。例えば、乱数は共有鍵暗号における秘密鍵や初期化ベクトル、認証の際に送受信されるランダムデータ、公開鍵暗号における鍵ペアの生成などに利用されている。このようなセキュリティ技術に用いられる乱数には、統計的に高いランダム性を持つだけでなく、予測不可能であることが要求される。物理的なランダム要因を基に生成される物理乱数のうち、ランダムビット列における 1/0 の発生確率が 50% であり、各ビットが互いに独立であるような乱数を真性乱数という。真性乱数は、擬似乱数のように計算からビット列を予測することができないため、セキュリティ技術に利用する乱数として適当である。

本研究では、オシレータの周期揺らぎをランダム源として乱数を生成する、オシレータサンプリング方式真性乱数生成器に着目し、製造ばらつきや温度変動にロバストなオシレータベース真性乱数生成回路を開発した。真性乱数生成器出力の 1 の出現確率が製造ばらつきや温度変化の影響を受けて偏る問題に対して、オシレータのデューティ比を調整することで出現確率の偏りを動的に補正する機構を提案した。65 nm プロセスを用いて、デューティ比モニタ回路及びデューティ比調整回路から構成される提案調整機構を実装した。測定結果より、デューティ比モニタ回路は、従来手法と比較して 4,100 倍高速な 1 の出現確率の推定、あるいは 70 倍精度の高い確率推定が可能であることを確認した。また、提案調

整機構により、測定した 5 チップにおいて温度が 0~75℃ と変化しても 1 の出現確率を $50 \pm 0.07\%$ の範囲内にとどめることができた。6,670 μm^2 の面積に実装された提案乱数生成器は、NIST や DIEHARD 乱数テストに合格する乱数列を 7.5 Mbit/s のスループットで出力することができた。

環境変動にロバストな真性乱数生成回路は、劣悪な環境の下でも高品質な乱数を生成するという点において非常に有用であり、乱数を用いるセキュリティシステムの信頼性向上への貢献が期待できる。



On the Wyner-Ziv Source Coding Problem with Unknown Delay

(英文論文誌 A 平成 26 年 12 月号掲載)



受賞者 松田哲直



受賞者 植松友彦

Wyner-Ziv 符号化は、複数の情報源に関する基本的かつ代表的な情報源符号化である。Wyner-Ziv 符号化では、相関を有する二つの情報源からそれぞれ生じた二つの固定長系列の片方のみを符号化器において符号化し、もう一方の系列を復号器における副情報として用い、符号化された系列を一定範囲内のひずみを許容して復号する。Wyner-Ziv 符号化は、この一連の符号化手順の類似性から、動画像符号化のモデルとして注目されることが多い。Wyner と Ziv はこの符号化に対して、実際の符号設計の指針となる最小符号化率の理論限界を明らかにした。この理論限界は、ひずみの許容値によって変化する関数となるため、「レート・ひずみ関数」と

呼ばれることが多い。

従来の Wyner-Ziv 符号化では、副情報として利用される系列が遅延なく復号器に届くことを仮定していた。しかしながら、系列が復号器に届くまでに経路遅延や処理遅延が起り得るため、この仮定は現実的ではない。これに対して本論文では、遅延が生じる場合の Wyner-Ziv 符号化を扱い、この符号化におけるレート・ひずみ関数に対して、計算可能な形式の上界と下界を与えている。また、生じ得る遅延の最大値と系列長との比が、系列長を大きくすると収束する場合、得られた上・下界が一致することを明らかにしている。更に、上・下界が一致するとき、遅延が生じない場合よりもレート・ひずみ関数が真に大きくなるための必要十分条件を明らかにするとともに、二元情報源に対してレート・ひずみ関数の具体的な数値計算例を与え、生じ得る遅延の最大値によっては、遅延が生じない場合よりもレート・ひずみ関数が真に大きくなることを確認している。これは、実際の符号設計において、遅延が無視できない重要な要素であることを意味している。

以上のように、本論文は Wyner-Ziv 符号化に対して新たな見地から解析を行っており、実用上極めて価値ある知見を与える優れた論文であり、本会の論文賞にふさわしい。

像群に関する様々な手法（群の直積によるベクトル的な利用、合成数位数群によるベクトル的な利用）を一般化、体系化するとともに、従来知られていなかった情報理論的な手法を開拓するなど新たな可能性を切り開いた。その結果、DPVS は安全かつ実用的な高機能暗号（内積述語暗号、属性ベース暗号、関数型暗号、属性ベース署名、更には電子透かしなど）を実現する有力な方法として現在に至るまで広汎に利用されている。

本論文は、この DPVS の概念を用いて得られた多くの結果を初めて体系的に論ずるものであり、著者らにより開発された様々な手法が関数型暗号などの構成、安全性証明にどのように使われるかを解き明かす。例えば、十分な安全性を持つ属性ベース暗号は DPVS により初めて素数位数群で実現することが可能となり、十分な安全性の属性秘匿内積述語暗号も DPVS によって初めて実現されたが、そこで DPVS がどのような役割を果たすかを体系的に示している。

以上のように、DPVS は高機能暗号を安全かつ実用的に実現する強力な方法論であり、本論文で示された様々な手法を更に発展させて、より広い分野に適用することは今後のこの分野の発展に大きく寄与すると考えられるため、本論文は本会論文賞にふさわしい論文として高く評価できる。



Dual Pairing Vector Spaces and Their Applications

(英文論文誌 A 平成 27 年 1 月号掲載)



受賞者 岡本龍明



受賞者 高島克幸

公開鍵暗号をより一般化し発展させた関数型暗号などの高機能暗号は、暗号化したままデータ検索や情報処理を可能とするため、クラウド計算やビッグデータ検索などのセキュリティ対策、プライバシー保護の切り札として活発な研究が行われている。このような高機能暗号を効率的かつ安全に実現する方法論として「双線形写像ベクトル空間」(DPVS: Dual Pairing Vector Spaces) という概念が、2009 年に著者らにより提案された。この概念は、双線形写像群を双対ベクトル空間として構成するものであり、それまでこの分野で使われてきた双線形写



Weighted-Combining Calibration on Multi-user MIMO Systems with Implicit Feedback

(英文論文誌 B 平成 27 年 4 月号掲載)



受賞者 福園隼人



受賞者 村上友規



受賞者 工藤理一



受賞者 鷹取泰司



受賞者 溝口匡人

喜安善市賞（第 9 回）に別掲

折返し逆 L 形アンテナの広帯域化

(和文論文誌 B 平成 27 年 6 月号掲載)



受賞者 野口啓介



受賞者 牧野 滋



受賞者 廣田哲夫



受賞者 伊東健治

スマートフォンやタブレット PC などの移動通信用端末は小形化が望まれる一方、通信容量を増大させるために広帯域な特性が要求される。今後、システムが高度化するに従って、端末に内蔵されるアンテナもこれまで以上に小形化、広帯域化が必要とされている。小形アンテナの基本的な形態の一つに、モノポールアンテナを折り曲げることによって低姿勢化した逆 L 形アンテナ (ILA) がある。一般的にアンテナを小形化すると放射抵抗が小さくなり給電線路との整合が取りにくくなるとともに動作帯域が狭くなる。その改善策として折返し構造を設けることが挙げられ、アンテナの放射インピーダンスを高めるとともに広帯域化を行うために有用である。ILA に折返し構造を設けた折返し逆 L 形アンテナ (FILA) は、放射及び伝送線路の二つのモードを発生させることができ、アンテナ自身にインピーダンス調整機能を持たせることによって広帯域化及び高効率化が可能となる。

本論文では、FILA の動作原理に基づく広帯域化について詳細な検討を行い、広帯域化の設計方法と理論的な限界値を明らかにしている。FILA についてその等価回路を基に周波数の変化率の関数として入力アドミタンスの理論式を求め、広帯域化に必要な二重共振特性が得られる条件によりシステムでの許容 VSWR に対する最大比帯域幅を求めた。FILA が従来の ILA に比べ、許容 VSWR が 2 の場合に約 2.4 倍の帯域幅を持つことを示すとともに、最大比帯域幅を得るために必要となる折返し構造での伝送線路の特性インピーダンスを求め、許容 VSWR とアンテナの Q 値との関係を求めた。

本論文の重要な点として、FILA の放射抵抗、Q 値、共振周波数を基にした等価回路による理論検討が挙げられる。更に折返し構造で生じる二つのモードを効果的に

用い、直列共振特性の放射インピーダンスを並列共振特性の伝送線路インピーダンスで打ち消すことにより広帯域化を実現した。これを理論的、数値的及び実験的に明らかにしたことは、今後の移動通信用小形アンテナの発展に寄与するものと考えられる。



Design of mm-Wave RLSAs with Lossy Waveguides by Slot Coupling Control Techniques

(英文論文誌 B 平成 27 年 9 月号掲載)



受賞者 Tung NGUYEN



受賞者 広川二郎



受賞者 安藤 眞



受賞者 Manuel Sierra-Castaner

近年の地上衛星間通信の急速な発展に応じて、衛星搭載アンテナに関する多くの研究が行われている。衛星通信には、軽量で高効率なアンテナが求められるが、高利得アンテナとして反射鏡アンテナが最も用いられている。しかし反射鏡アンテナは曲面形状であることに加えて一次放射器も含めるとアンテナシステムとしての大きな体積を占める。一方、平面アンテナは太陽照射が一様で熱変形が少なく、衛星きょう体への装着時にかさばらないなど、衛星搭載用として利点が多い。ラジアルラインスロットアンテナ (RLSA) の平行平板間の誘電体スペーサとしてハネカム構造を導入したものは、極めて軽量であり、例えば直径 900 mm の RLSA が約 1 kg の重さになり、衛星搭載用として十分魅力的である。一方、このアンテナでミリ波における高利得かつ軽量の平面アンテナを実現するには、ハネカム構造の損失は大きく、これによる効率低下、利得低下をいかに抑制するかが、重要な課題である。

本論文では、損失の大きい材料で導波路を充填した RLSA の効率低下を抑制する設計を議論している。著者らは、RLSA について、スペーサの与えられた損失に対し利得低下を抑制し、開口上スロットの結合分布の新し

い設計を導入した。新たに定義したスロット結合量分布に基づき、開口径や損失係数の異なる数多くの RLSA を解析し、特性を評価した。理論計算により、新しい設計法を適用しても、利得はラジアル線路における材料損に極めて敏感であることが分かった。一方、新しい結合分布公式を用いた利得の改善量は、アンテナの大きさが大きいほど、誘電体材料の損失が大きいほどに顕著であることを示した。異なる結合分布により、三つの RLSA を 60 GHz 帯で設計、試作し、測定によりこの理論を実証した。

以上述べたように、本論文では、損失の大きい誘電体材料を用いた RLSA の利得低下を抑制する新しい設計法を提案した。更に、その設計法の有効性を実験により確認している。よって、本論文は本会論文賞に値する。



Multiband Sector Antenna with the Same Beamwidth Employing Multiple Woodpile Metamaterial Reflectors

(英文論文誌 C 平成 26 年 10 月号掲載)



受賞者 宗 秀哉



受賞者 安藤篤也



受賞者 関 智弘



受賞者 川島宗也



受賞者 杉山隆利

陸上移動無線通信システム用基地局アンテナでは、複数の周波数帯において、同一のセクタを、同一の水平面内ビーム幅でカバーする等ビーム多周波数共用セクタアンテナが用いられている。コーナレフレクタアンテナに代表される従来の等ビーム多周波数共用アンテナは、1枚の金属反射板とマルチバンド放射素子から構成されているため、共用周波数帯数の増加とともに設計の自由度が制限され、全ての共用周波数帯にわたって等ビームを実現するのは困難であった。この主な原因は、放射素子と反射板との電氣的距離や、反射板の電氣的寸法を全ての共用周波数帯にわたって一定に保持できないことであ

り、放射素子構造の工夫による自由度確保の試みも共用数の増加に伴い限界が見える。これらの困難さから、これまで3周波数以上の共用数に対する等ビーム多周波数共用セクタアンテナの検討例はなく、任意の共用数に対する一般性を有する設計法の確立が課題であった。

本論文では、マルチバンド放射素子と共用周波数帯の数に対応した複数のメタマテリアル反射板から構成される等ビーム多周波数共用セクタアンテナを提案している。提案構成は、メタマテリアルの持つ EBG 特性を利用して、マルチバンド放射素子と、放射素子の各々の共用周波数帯に対応した電磁波を反射する複数のメタマテリアル反射板を、各々の反射板と放射素子間の電気長や、各々の反射板の電氣的寸法が全ての共用周波数にわたって一定に保持されるように設計配置することにより、全ての共用周波数帯においてビーム幅を同一とすることができる。また、提案設計法は任意の共用数に対して適用可能な設計の自由度と一般性を有する。0.8/2/4 GHz の3周波数において 90° ビーム幅を有するプロトタイプを設計試作した結果、実測値と電磁界解析値はほぼ一致し、提案アンテナ設計法の妥当性を確認している。

本論文は、メタマテリアルの EBG 特性を利用して複数の反射板に新たな機能を持たせた独創的な構成を提案することによって、等ビーム多周波数共用セクタアンテナの統一的設計法確立への新たな道を切り開いた点で高く評価される。



電波吸収/反射切替板を用いた X 帯アレーアンテナの電波反射低減効果に関する検討

(和文論文誌 C 平成 26 年 12 月号掲載)



受賞者 北川真也



受賞者 須賀良介



受賞者 橋本 修

近年の様々な電子機器の普及に伴う電波環境の悪化に対して、周囲からの反射波低減のために古くから電波吸収体が研究及び実用化されている。しかし、アンテナレフレクタのようにアンテナの送受信時では電波の反射が必要となり、非送受信時では電磁環境改善のため電波の吸収が必要となる場合においては、通常の電波吸収体はアンテナの性能を低下させるため適用することが困難で

あった。

一方、反射板の構造にダイオードを組み入れ、そのダイオードのオン／オフによって反射率を切替可能な電波吸収／反射切替板が提案されている。これらの切替板は、抵抗素子等の損失材料は組み入れず、電波吸収体として動作する場合はダイオードがオフ状態の寄生抵抗のみを損失材料として用いているため、ダイオードがオン状態で反射板として動作する場合は損失材料がほとんどなくなり、金属板と同等な反射率となる。

本論文では、アンテナリフレクタに適用可能な電波吸収／反射切替板を提案し、その切替板をアレーアンテナのレフレクタに適用した場合のアンテナ特性を評価している。提案した切替板はレフレクタに適用可能な簡易な構造であり、アンテナを半波長間隔でアレー化して設置することが可能な構造となっている。まず、切替板単体の反射率を評価し、9 GHz において設計どおり電波吸収体と反射板で切替可能であることを確認している。次にその切替板を 9 GHz で動作する 4 素子のダイポールアレーのレフレクタに適用し、放射パターン及び反射波低減効果を評価している。切替板を反射板として動作させた場合は、金属板とほぼ同等なレフレクタとして機能しており、切替板を電波吸収体として動作させた場合は、金属板をレフレクタとした場合と比較して反射波を 10 dB 以上低減できることを確認している。

このように、本論文は今まで報告例がなかった切替板の応用例の一つとしてアンテナの反射波低減を示しており、このような切替板は様々な分野への応用が期待されるため、論文賞にふさわしい論文として高く評価できる。



自律型光ファイバ断線復旧技術による Radio-over-Fiber 有無線シームレス伝送システム

(和文論文誌 C 平成 27 年 7 月号掲載)



受賞者 大石将之



受賞者 神谷尚保



受賞者 萩原 敦彦



受賞者 西村公佐



受賞者 田中啓仁

光ファイバ伝送システムは、大容量通信サービスを支える重要なインフラであるため、災害などにより光ファイバ断線が生じた場合に迅速な復旧が求められる。現状のシステムでは、作業者が断線箇所に出向いて復旧するため、最低でも数時間程度を要する。一方で無線伝送は、光ファイバのように物理的に断線することがないため、光ファイバ断線の危険性が伴う特定の区間に無線伝送によるバックアップ回線をあらかじめ組み込んでおけば、迅速に復旧対応でき効果的である。伝送技術としては、光ファイバ伝送と無線伝送をシームレスに変換可能な Radio-over-Fiber (RoF) 技術が有望である。複数区間で発生する光ファイバ断線に対応するためには、断線区間を検出し無線バックアップ回線へ自律的に切り換える技術が必要となる。また、無線バックアップ区間数や光ファイバ伝送距離などのシステムパラメータを設計するためには、光ファイバ伝送を無線伝送に切り換えた場合の信号品質の劣化を定量的に把握する必要があるが、このようなシステム設計に関する検討は十分になされていなかった。

本論文では、ファブリペローレーザの自己注入同期を利用した新たな光ファイバ断線復旧方式を提案し、ネットワークライフラインに求められる復旧時間内に、光ファイバ断線区間を無線バックアップ回線へ自律的に切替可能であることを実証している。提案方式により、従来は作業者が出向いて対応していた複数箇所の光ファイバ断線を、信頼性高く自律的に、かつ迅速に復旧可能となる。更に、提案方式を組み込んだ RoF 伝送実験により、有無線回線切替による信号品質の劣化を定量化することで、複数のバックアップ区間を含む有無線シームレス伝送を実現するためのシステム設計指針を明示してい

る。

以上のように本論文は、光ファイバ通信インフラに対して社会的に求められている耐災害性を向上させるために非常に有益となり、本会論文賞にふさわしい論文として高く評価できる。



局所線形写像に基づくハッシング

(和文論文誌 D 平成 26 年 12 月号掲載)



受賞者 入江 豪



受賞者 新井啓之



受賞者 谷口行信

画像をクエリとしてデータベースから類似する画像を検索する技術は、情報検索サービスに対する需要の高まりとともにその重要性が年々高まっている。このような技術は類似画像検索と呼ばれ、パターン認識、コンピュータビジョン、マルチメディア処理といった様々な分野で扱われる基本的な問題となっている。しかしながら、データベースの大規模化に伴って検索精度と速度の両立が難しくなるという問題があり、この問題の解決法としてハッシングに基づく類似画像検索手法が注目を集めている。

これまでに、多種多様なハッシング法が提案されており、その多くは特徴量空間上でのユークリッド距離の近接性を保存するようにハッシングを行うものであった。一般に、同じ物体であったとしても、撮影する向きが異なれば特徴量空間上での距離は大きくなる。このような異なる向きの画像を類似画像検索により得ようとした場合、単純なユークリッド距離による近接性では所望の画像を得ることはできない。このような問題に対し、本論文では検索対象と類似する画像が特徴量空間上で非線形多様体を形成するという知見に基づき、この多様体の構造を適切に捉えるようにハッシングを行う手法を提案している。著者らは、非線形多様体が局所的な線形幾何構造として捉えることができ、かつこのような構造を局所線形スプース再構成により求めることができることを示している。そして、局所線形写像によりこのような構造をハミング空間に最適に保存することが可能であることを定式化を通して示している。

実験では、3種類の著名なデータセットを用いた類似画像検索問題に対して、8種類の既存ハッシング法と比

較を行っている。その結果、提案手法により有意に性能が向上することが示されている。そして、提案手法の計算量は画像枚数に対して線形のオーダーであることも示されており、ハッシングに基づく高速な類似画像検索の特徴が十分に生かされていることが分かる。

以上のように、提案手法はハッシングの利点である高速性を十分に担保しつつ、また、多様体の特徴を捉えることで従来のハッシング法の弱点を克服した実用面でも有用な手法である。これらのことから、本会論文賞にふさわしい論文として高く評価できる。



The Case for Network Coding for Collective Communication on HPC Interconnection Networks

(英文論文誌 D 平成 27 年 3 月号掲載)



受賞者 Ahmed SHALABY



受賞者 藤原一毅



受賞者 鯉淵道紘

本論文では、ハイパフォーマンスコンピューティングにおけるグループ通信の効率化を目的として、ユニキャストの回数と通信データ量を削減可能なネットワークコーディング手法を提案している。ネットワークコーディングは、ネットワークを中継するノードにおいて、複数の異なったデータを組み合わせることで、ネットワーク全体のスループットを向上させる技術である。

提案法では、ノードを複数のグループへと分割した上で、グループ内とグループ間のユニキャスト通信に基づいた階層的なマルチキャスト処理を行うことで、ネットワークコーディングの効果を大幅に向上することに成功している。階層的なユニキャストをネットワークコーディングに導入することによる性能向上の実現が、本論文における大きな独創性の一つである。

本論文では、提案するネットワークコーディング手法の有効性を、解析的評価とシミュレーションにより示している。まず、定量的分析により、スイッチ数が4,096個のネットワークを仮定した場合、提案するマルチキャスト方式では、従来のユニキャストに基づくマルチキャスト方式と比較してユニキャストの総ホップ数を94%程度削減可能であることを示している。更に、パケット

ベースシミュレータである BookSim を用いたサイクル精度のシミュレーションにより、提案するネットワークコーディングを用いることにより、ネットワークの規模やパケット長が大きくなるに従って、レイテンシの削減への効果が大きくなることを示すとともに、中継ノードにおける計算オーバーヘッドに起因するレイテンシの増加が全体の処理速度にほぼ影響を及ぼさないことを明らかにしている。

本論文の成果により、ネットワークコーディングの性能を大きく向上させることが可能であり、ハイパフォーマンスコンピューティング分野の発展への貢献は極めて大きい。また、詳細な解析及びシミュレーションに基づくパラメータの最適化に関しても議論がなされていることから、実問題への適用可能性も高く、論文賞にふさわしい優れた研究と言える。



Personalized PageRank に対する アドホックな検索手法

(和文論文誌 D 平成 27 年 5 月号掲載)



受賞者 藤原靖宏



受賞者 中辻 真



受賞者 塩川浩昭



受賞者 三島 健



受賞者 鬼塚 真

ソーシャルネットワークに代表される大規模グラフが出現し、当該グラフを積極的に活用するアプリケーションが見られるようになってきている。PageRank の発表以降、グラフのリンク構造に基づいたノードの類似度を用いるアプローチが頻繁にとられ、とりわけ近年においては、Personalized Page Rank (PPR) が代表的な類似度として広く用いられている。

PPR は、問合せノードを起点としてランダムウォークを行った後の定常状態の確率に相当し、グラフ全体におけるノードの重要度を個々のユーザごとに個別化することができる点に特徴を備える。一方で、多くの現実の

アプリケーションにおいては、グラフは動的に変化し得る特性を有するものであるから、PPR に対してアドホックな検索、すなわち、都度に検索条件を変更して検索を行うことができることが望ましい。しかしながら、PPR を用いてグラフの検索を行う場合、グラフの規模が拡大するとアドホックに計算する時間が大きく増大するという点が問題であった。過去、PPR の計算量の低減を目指す研究は行われてきたものの、事前の計算が必要である、若しくは、近似的な計算を許すといった制限が課されていた。これらに対して、本論文で著者らが提案する Castanet なる検索手法は、任意のグラフに対する Top-k グラフ検索において、再帰的に PPR のスコアの下限・上限値を推定し、不必要ノードの枝刈りを行う点に特徴を有し、PPR のスコアに基づく正確な Top-k ランキングを高速に行うことを可能とする。

本論文は、Castanet における検索アルゴリズムを提案し、理論計算量上の優位性を示すとともに、複数の異なるグラフアプリケーションを対象に行った実験の結果を示して既存手法に対する有効性を明らかにしている。このように、本論文は、大規模グラフに対する高速かつ正確な検索を可能とする極めて有望なアルゴリズムを提案しており、本会論文賞にふさわしい論文として極めて高く評価できる。

