



論文賞贈呈

(写真：敬称略)

論文賞（第 71 回）は、平成 25 年 10 月から平成 26 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 High Performance HEVC De-Blocking Filter and SAO Architecture for UHD TV Decoder

(英文論文誌 A 平成 25 年 12 月号掲載)



受賞者 竺 加毅 受賞者 周 大江 受賞者 後藤 敏

HEVC (High Efficiency Video Coding) は 2013 年 4 月に標準化された最新の動画圧縮方式で、従来の MPEG-2 や H. 264 と比較して、画像品質を保ちながら、約 4 倍、2 倍に圧縮率を高めることができるために、今後の 4K, 8K テレビ放送やインターネット、ビデオ機器で広く使われることが期待されている。圧縮率を向上させたために、アルゴリズムが複雑となり、より多くの演算量を必要とし、ハードウェア化すると回路規模が増大するという問題が生じている。ILF 機能 (In-Loop Filter, インループフィルタ) は、HEVC で追加された新しい機能で、従来の DBF (De-Blocking Filter, デブロッキングフィルタ) に SAO (Sample Adaptive Offset, サンプルアダプティブオフセット) という新しい機能を加えたものとなっており、アルゴリズムはより複雑なため、演算量を減らし、より小規模なハードウェアで高性能化を実現することが重要な課題となっている。

本論文では ILF に対して、新しい LSI アーキテクチャを提案することで、課題の解決を図っている。SAO と DBF は 8×8 ブロックを単位としてパイプライン処理する方式を採用し、現在の 8×8 ブロックの DBF 処理をしている間に、前のブロックの SAO 処理を行う。 8×8 ブロックを、DBF に対して四つの境界線と SAO に対して四つの 4×4 ブロックに分割しておき、

DBF と SAO を同時に処理する組合せ回路は 1 クロックサイクル内で DBF の一つの境界線を処理し、SAO の一つの 4×4 ブロックを処理する。このため一つの 8×8 ブロックを処理するのは 4 サイクルが必要となる。DBF から SAO へ処理を続けて行う際には、 8×8 ブロックの上辺部分と左辺部分からスタートして、下辺と右辺へ処理を順次行う。また、 4×4 ブロックのルマとクロマの各要素を、同じ記憶領域内に格納し、同時に処理を行うことで並列度を上げている。提案した新しい ILF アーキテクチャを、8K 用動画像を対象として、65 nm プロセスで可能な最高のクロック数である 240 MHz で回路実装した。回路規模は DBF は 31.0k ゲート、SAO は 36.7k ゲートとなり、1 クロックサイクル当たり 16 画素の処理が行え、3.84G 画素/秒が処理可能となった。この結果、UHD TV 4320p ($7,680 \times 4,320$) 画像に対して、60 フレーム/秒を 124.4 MHz のクロックでデコードすることが可能となった。



Comprehensive Analysis of Initial Keystream Biases of RC4

(英文論文誌 A 平成 26 年 1 月号掲載)



受賞者 五十部孝典



受賞者 大東俊博



受賞者 渡辺優平



受賞者 森井昌克

RC4 は 1987 年 Rivest により提案されたストリーム暗号である。ストリーム暗号では、秘密鍵からキーストリームと呼ばれる擬似乱数系列を発生させ、平文と排他的論理和をとることにより暗号文を生成する。RC4 は SSL/TLS, WEP, WPA-TKIP 等数多くの標準セキュリティプロトコルに採用されており、最も広く利用されている暗号アルゴリズムの一つである。1994 年に RC4 のアルゴリズムが公表されてから、過去 20 年にわたり、数多くの安全性解析が行われてきた。これまでの解析により、キーストリームの乱数性や秘密鍵とキーストリームの相関など様々なアルゴリズムのぜい弱性が指摘されている。しかしながら、既存の安全性評価は理論的な側面が強く、WEP などの特殊な運用を除いては、現実的に脅威となる攻撃には結び付いていなかった。

本論文では、RC4 のキーストリームの初期バイトの統計的偏りに関する包括的な解析を行い、それを応用することで現実的に脅威となり得る RC4 のぜい弱性を導出している。まず初めに、キーストリームの初期 257 Byte について詳細に評価し、全てのバイトにおいて最も強い偏りの値を初めて明らかにしている。同時に、強い偏りが発生する原因についても、アルゴリズムの詳細を解析することにより、理論的に明らかにしている。そして、新しく導出した初期キーストリームの偏りの集合を用い、暗号文から平文を求める攻撃、秘密鍵を求める攻撃、真性乱数と効果的に識別する攻撃を提案している。特に、暗号文から平文を求める攻撃は強力であり、同じデータを異なる秘密鍵で暗号化し配布するブロードキャストセッティングにおいては、現実的なデータ量の暗号文を集めることで平文情報を復元できることを示している。更に、この攻撃は実際のセキュリティプ

ロトコルである SSL/TLS においても適用可能である。

以上のように本論文は、広く使用されている暗号アルゴリズム RC4 に対する現実的なぜい弱性を初めて明らかにしている。この結果は 2013 年に改訂された電子政府推奨暗号リストから RC4 を除く原因にもなっており、学術面のみではならず、社会的、産業的にも影響力も大きく、高く評価できる内容である。



電力パケットによるエネルギー表現の 漸近的性質

(和文論文誌 A 平成 26 年 9 月号掲載)



受賞者 縄田信哉



受賞者 高橋 亮



受賞者 引原隆士

喜安善市賞（第 8 回）に別掲



水中のワイヤレス給電に関わる幾つかの 新しい現象

(和文論文誌 B 平成 25 年 11 月号掲載)



受賞者 粟井郁雄



受賞者 澤原裕一



受賞者 山口和也



受賞者 堀田昌志



受賞者 石崎俊雄

結合共振器型ワイヤレス給電 (WPT) システムは中距離用として大きな将来性が期待されているため、自動車、建築、家電、医療、海洋などの幅広い応用分野から熱いまなざしが注がれ、各分野の必要性に応じた研究・開発が進められている。しかし応用分野からのアプローチは、概して電気回路論、半導体回路学、電磁気学など基礎理論の裏打ちが弱い傾向が見られ、これらの専門家によるバックアップが必要である。本論文はそのような認識に立ち、電磁気学的な見地から WPT システムの各種応用分野のニーズに則した研究・開発を進め、水中給電の課題を探ろうとの目的を持って実験的検討を試みている。そしてその結果として得られた意外性に富む事実の解明を試みている。

まず第 1 に、水は誘電体であるだけでなく優れた溶媒であるために、電解質を溶かすことで導電性を持つことを定量的に示している。水の誘電率実数部は共振周波数に、虚数部 (主として導電性に基づく) は損失に影響し、後者は結局電力伝送効率を下げることは予想どおりであったが、逆に共振器間結合係数には両者とも余り影響しないことが明らかとなった。

第 2 にはこれら水の影響は磁界結合型共振器を用いることによって抑えられるが、大きな塩分濃度では磁界を通じて導電電流が誘起されるため、電界を封じ込めても損失低減効果は限定的であることを示している。

第 3 に、異なった媒質境界では電界/磁界は屈折する特性を持ち、共振器間に有限寸法の媒質を挿入する (水入りペットボトルを並べる) と収束作用が起こって、導波路ならぬ「導場路」が形成されるため伝送効率が上昇する。この現象はワイヤレス給電の長距離化に利用可能であると考えられる。

上記三つの特性については完全な理論的証明がなされているわけではないが、それなりに理解可能である。しかし第 4 に水中の塩分濃度を徐々に増大させたとき、その途中で伝送損に極大・極小が起こり最終的には上昇していくという現象が見いだされており、現時点では全く説明ができていない。

このように境界分野には未知の現象がまだまだ残っていることを示した点は刺激的であり、今後もその発見と解明は技術者・研究者に仕事と喜びを与え続けるであろう。



Efficient Lookup Scheme for Non-aggregatable Name Prefixes and Its Evaluation

(英文論文誌 B 平成 25 年 12 月号掲載)



受賞者 福嶋正機



受賞者 田上敦士



受賞者 長谷川 亨

将来のインターネットの基盤となるアーキテクチャとして Information-Centric Networking (ICN), 特に Content-Centric Networking (CCN) が有望視されている。ICN/CCN においては、ネットワークを介して送受信される全ての情報に階層的な名前を付与し、その名前に対する最長プレフィックス一致検索により情報要求パケットを情報源までルーティングする。情報の名前によるルーティングは効率的なコンテンツ配信・モビリティ・マルチホーミング等の利点をもたらす一方、情報の名前は、従来の IP アドレス等と異なり、ネットワークトポロジー上の位置とは無関係なため、プレフィックスが集約しにくく、経路表が大きくなる問題がある。このため、ICN/CCN においては大規模な経路表に対して、いかに効率良く最長プレフィックス一致検索するかが課題となる。

本論文は、集約不可能な名前プレフィックスを含む大規模な経路表から効率良く検索を行うための新しい手法を提案している。提案方式は、大規模な経路表から最長プレフィックス一致検索する際のボトルネックが、オフチップ DRAM ヘランダムアクセスする際の大きなレイテンシであること、またこのランダムアクセスは直前のルータにおいて最長一致したプレフィックス長の情報を

活用することで削減可能であるという二つの考察に基づいて設計されている。更に、本論文では、将来想定される ICN/CCN の運用形態について妥当な仮定を置き、実際のインターネットのトポロジーデータを用いて、提案手法の有効性を定量的に示している。提案手法自体は非常にシンプルであるが、それゆえに実装は容易かつオーバーヘッドは小さく、その適用範囲は広い。

以上のように、本論文は将来のインターネットの基盤技術として期待される ICN/CCN のスケール性に関する重要課題を明確に指摘し、その解決方法を提案するとともに、提案手法の有効性を現実的なデータと評価モデルを用いて明快に示しており、本会論文賞にふさわしい論文として高く評価できる。

テイ圧縮処理も併用することで、誤り訂正能力が改善可能であることを明らかにしている。このとき、任意の符号化率を実現するために、パンクチャ処理と XOR 符号化パリティ圧縮がされるパリティビット数の比率を適切に設定する必要があることにも言及している。その比率の最適性を EXIT (EXtrinsic Information Transfer) 解析と呼ばれる、繰返し復号の振舞いを相互情報量の交換の観点から評価している点は独創的であり、本論文の顕著な貢献である。

本論文の提案方式を用いると、多くの無線通信システムで利用されているターボ符号からの単純な変更で高符号化率の伝送効率を改善可能であり、高く評価できる内容である。

XOR 符号化パリティ圧縮を用いた 高符号化率ターボ符号

(和文論文誌 B 平成 26 年 2 月号掲載)



受賞者 北村康裕



受賞者 衣斐信介



受賞者 三瓶政一

本論文では、ターボ符号を高い符号化率で利用する際に低下してしまう誤り訂正能力を改善することを目的として、XOR (eXclusive OR) 符号化パリティ圧縮とターボ符号の直列接続符号化構造とその繰返し復号法を提案している。昨今では、低い符号化率のターボ符号あるいは LDPC (Low Density Parity Check) 符号を用いることで、シャノンが示した通信路容量の理論限界に漸近する性能を達成している。一方で、余り言及されることが多くはないが、符号化率を高くすると通信路符号化の誤り訂正能力が著しく低下し、所定伝送速度を実現するために必要な受信電力の理論限界よりも過剰な電力が必要とされる。

一般に、ターボ符号では符号化率を高めるため、CBRM (Circular Buffer Rate Matching) によるパリティビットのパンクチャ処理を施す。この処理は送信機において単純にビットを除去する処理であり、受信機側ではビットが除去されているということは識別できるものの、その知識が誤り訂正能力の向上に寄与することはない。本論文では、この点に着目し、パンクチャ処理だけではなく、2 bit を 1 bit に圧縮する XOR 符号化パ

Nonlinear Modeling and Analysis on Concurrent Amplification of Dual-Band Gaussian Signals

(英文論文誌 C 平成 25 年 10 月号掲載)



受賞者 安藤生真



受賞者 タン ザカン



受賞者 荒木純道



受賞者 山田貴之



受賞者 加保貴奈



受賞者 山口 陽



受賞者 上原一浩

多様な無線方式を統合的に収容可能なユーザセントリックワイヤレスネットワークの実現に向けて、複数の周波数帯域の信号を同時に増幅可能な広帯域増幅器や複数帯域信号同時補償技術が求められている。複数帯域信号同時増幅時に線形領域を超えた高い電力レベルの信号

を増幅すると、増幅器の非線形性により高調波ひずみや各帯域の信号が組み合わさった相互変調ひずみが発生する。従来研究においても異なる周波数の複数の信号が同時に受けた非線形ひずみの補償は検討がなされている。しかし、複数帯域の信号が同時に受けるひずみへの補償技術への検討は帯域間隔がそれほど広くない、若しくは広い間隔であっても調波関係にない場合においてなされており、調波関係にあるような場合は未検討である。

本論文では、調波関係時のより厳しい条件の場合へのひずみ補償技術の検討として、ボルテラ級数展開と一般化ウィナーモデルを組み合わせた非線形ひずみモデル化手法を提案し、複数帯域信号同時増幅時のような複雑な非線形ひずみのモデリングを可能にしている。また、それを用いて、増幅器出力における電力スペクトル密度、隣接チャネル漏えい電力比やエラーベクトル振幅などの様々な物理量に関する閉形式解を OFDM 信号のガウス性を用いて導出し、複数帯域信号同時増幅時の増幅器特性を簡易に評価できる手法を確立している。

以上から、本論文は入力信号がガウス性を仮定できる場合には 1 トーンテストのような比較的簡単な測定を行うことで複数帯域信号同時増幅時の増幅器の非線形特性（隣接チャネル漏えい電力比，エラーベクトル振幅）が簡易な手順で求められることを理論的，実験的に示しており，本会論文賞にふさわしい論文として高く評価できる。

ワークの高速・大容量化に関する技術が広く検討されている。その中でも、波長多重技術を用いた光パケットスイッチや光波長ルーチングに関する研究が盛んに行われている。そのようなシステムでは高速かつ高精度に波長を切り換えられるような波長可変レーザが強く求められている。その要求を満たすものとして、注入電流により発振波長を変化させることができる電流制御形の半導体レーザ (LD) が適している。

これまでに筆者らは、高速かつ高精度な波長切換を実現するための波長可変 LD として、波長可変分布活性 (TDA-) DFB-LD の開発を行ってきた。TDA-DFB-LD は、利得を生じる活性層と波長を制御する制御層が共振器方向に周期的に並んだ構造を有しており、制御層へ電流を注入することで、キャリアプラズマ効果により屈折率が下がり、発振波長が短波長側に高速に変化する。しかし、制御電流が増加することで発熱による温度変化が生じ、緩やかな波長ドリフトが生じる。この変化はキャリアプラズマ効果による波長変化とは逆に、ゆっくりと長波長側に変化し、切換時間を律速する要因となっていた。

本論文では、TDA-DFB-LD アレーを用いた波長切換動作において、上記の課題を解決し、高速な高精度波長切換を実現するために筆者らが考案した、動作 LD と隣接する LD の制御層を用いた熱補償動作について示している。更に、新たに開発した従来よりもアレー間隔が狭い狭間隔 TDA-DFB-LD アレーについて紹介している。アレー間隔を狭くすることで、熱補償動作により動作 LD のコア部の局所的な温度変動まで抑制することが可能となった。その結果、 ± 1 GHz の周波数精度で、これまでよりも 10 倍以上速い sub- μ s 領域の切換時間を実現している。

以上のように、本論文において筆者らは、半導体波長可変 LD を用いた高速な高精度波長切換を実現する技術について報告しており、将来の光パケットスイッチや光ルーチングシステムを実現するための技術として高く評価される。



高速高精度波長切替を実現する狭間隔波長可変分布活性 DFB レーザアレーの開発

(和文論文誌 C 平成 26 年 3 月号掲載)



受賞者 金井拓也



受賞者 布谷伸浩



受賞者 山中孝之



受賞者 伊賀龍三



受賞者 下小園 真



受賞者 石井啓之

将来の通信トラフィックの増加に向けて、光通信ネット

Diagnosis of Signaling and Power Noise Using In-Place Waveform Capturing for 3D Chip Stacking

(英文論文誌 C 平成 26 年 6 月号掲載)



受賞者 高谷 聡



受賞者 池田博明



受賞者 永田 真

三次元積層技術の進歩により、電子デバイスの低消費電力が進んでいる。これは、シリコン貫通ビア (TSV) 技術により、積層チップ間の信号配線長と寄生容量を減らすことで可能となった。FR-4 基板やインタポーザ上に作られた平面のバス配線に比べ、メモリとロジックチップ間のデータ通信は、データ帯域幅だけでなく電力効率も大きく向上している。特にメモリチップの三次元積層は、モバイル用途だけでなく、ハイパフォーマンスコンピューティングにおいても有用である。

内部信号線の観測や回路動作の確認のためには、物理的に回路の内部ノードに針を当てるなどの方法が用いられるが、三次元実装においてはこの観測手法は不可能であり、オンチップでの電氣的な観測が必須である。また、垂直チャンネル内の信号伝搬の様子を観測や、接続が弱くなっている箇所の同定、複数層間の背景雑音のカップリングなどの評価のため、三次元積層内の信号や電源配線のアナログ波形の観測手法の確立が求められている。

本論文では、三次元チップスタックにおけるその場合波形取得手法を提案している。本論文で用いている 4,096 bit 幅の I/O デモンストレータを搭載した三次元積層デバイスは、スタック内のインタポーザ上にその場合波形取得回路を備えている。この回路は、信号配線と電源配線に接続されたプローブチャンネルを持ち、三次元積層内の回路診断のためのアナログ波形を観測する。9.9 mm×9.9 mm のチップ面積に配置された垂直 I/O チャンネル 8 バンクのうち、128 信号がその場合波形取得の対象である。アナログ波形の観測により、帯域幅 100 GByte/s のデータ転送時において、垂直信号チャンネル間のスキューやスルーも小さく、1.2 V フルスイングの信号伝送が確認された。また、信号振幅を 0.75 V まで下げた場合でもエラーなしの 100 GByte/s の転送が可能なこと、その際のエネルギー効率が 0.21 pJ/bit であることが実験的に確認された。

本論文におけるその場合波形評価技術は、三次元積層の電氣的、物理的特性の評価だけでなく、実装技術の開発においても有用である。

多言語音声翻訳システム “VoiceTra” の構築と 実運用による大規模実証実験

(和文論文誌 D 平成 25 年 10 月号掲載)



受賞者 松田繁樹



受賞者 林 輝昭



受賞者 葦苜 豊



受賞者 志賀芳則



受賞者 柏岡秀紀



受賞者 安田圭志



受賞者 大熊英男



受賞者 内山将夫



受賞者 隅田英一郎



受賞者 河井 恒



受賞者 中村 哲

本論文では、国立研究開発法人情報通信研究機構 (NICT) が開発した世界初のスマートフォン用多言語音声翻訳 “VoiceTra” のシステム概要、個々のモジュールの詳細、同システムを用いた大規模実証実験について述べられている。VoiceTra は、音声入力と翻訳結果の表示、外国語合成音声の再生などを行うクライアントアプリと、音声認識、言語翻訳、音声合成の処理を行うサーバから構成されており、クライアントとサーバ間の通信には独自の通信プロトコルが用いられている。VoiceTra の最大の特徴は多言語翻訳に対応しているという点であり、音声入力は 6 言語に限定されるものの、テキスト入力であれば全 21 言語の相互翻訳に対応しているため、様々な国の人々が音声翻訳サービスを楽しむことができる。また、ユーザインタフェースについても工夫がされており、単なるモジュールのつなぎ合わせ

ではなく、システム全体が綿密に設計されている。

VoiceTraの大規模実証実験は2010年7月末から始まり、2012年12月末の時点で1,000万アクセスがあり、実験にて収集された大規模データの分析がなされている。このような大規模実証実験による収集データの詳細は多くの場合非公開とされるが、本論文で示されている分析結果は今後の音声翻訳システム開発の在り方に大きなインパクトを与える貴重な情報である。

以上、実用的な性能を持つ音声翻訳システムをモバイル端末で実装し、気軽に多言語翻訳サービスを利用できる枠組みを構築したことは、今後の国際社会における大きな貢献であり、高く評価すべき点である。また詳細な分析により実用面における音声翻訳システムの課題を明らかにするなど、示唆に富んでいる。これらの点から本論文は、本会論文賞にふさわしいものと言える。



システム LSI 搭載 FPGA-IP コア向け 物理故障検出及び回避手法

(和文論文誌 D 平成 25 年 12 月号掲載)



受賞者 尼崎太樹



受賞者 西谷祐樹



受賞者 井上万輝



受賞者 飯田全広



受賞者 久我守弘



受賞者 末吉敏則

医療機器や自動車などの高い信頼性が求められるシステムにおいて、システムの耐故障性を高めることは非常に重要である。更に今日の耐故障システムにおいては、消費電力、面積、遅延などのオーバーヘッドが小さいことも求められている。本論文は、FPGA (Field Programmable Gate Array)-IP (Intellectual Property) コアを対象にした耐故障システムを提案している。FPGA は内部の論理を書き換えることができる柔軟性を持つデバイスである。この柔軟性を生かし、提案システムは故障した部分をシステムから切り離し、故障していない正常な

部分だけでシステムを再構成することで障害から復旧する。あらかじめ予備部品を用意したり多数決を行うような機構(冗長設計)は不要であるため、オーバーヘッドは小さく抑えることができる。

このような耐故障設計を行う場合、二つのことが重要となる。一つは故障箇所を特定する故障診断法である。著者らは、これまでに提案している FPGA の出荷テスト法を応用することにより、僅かなテスト時間の増加で完全な診断ができる方法を提案している。この提案故障診断法は解析と実験の両面からその有効性が評価されている。もう一つは、故障したブロックを避けて再構成を行う故障回避手法である。著者らは配置・配線能力の高い CAD (Computer-Aided Design) ツールを利用することで、効果的に再構成を行う方法を提案している。実験結果からは、提案システムが故障箇所を完全に推定し、パフォーマンス低下をほぼゼロに抑えて再構成できることが分かる。このような結果は、提案システムがすぐにも実社会のシステムに応用できることを期待させる。

柔軟性と高いパフォーマンスを備えた FPGA-IP コアは、今後もますます利用範囲が広がると予想できる。よって、FPGA-IP コアを利用した耐故障システムの研究は今後ますます重要な研究テーマになっていくだろう。本論文の成果はその一つの到達点であり、本会論文賞にふさわしい論文として高く評価できる。



Hadoop をはじめとする並列データ処理系への アウトオブオーダー型実行方式の適用と その有効性の検証

(和文論文誌 D 平成 26 年 4 月号掲載)



受賞者 山田浩之



受賞者 合田和生



受賞者 喜連川 優

近年、様々な情報がデジタルデータとして蓄積されており、学術研究のみならず企業における経営の効率化や意思決定の高度化などに活用されつつある。このようなデータはその数、規模、共に飛躍的に増大しており、大規模データ処理基盤の開発は極めて重要な課題となっている。

著者らは、これまで関係データベースにおける非順序型（アウトオブオーダー型）実行方式を提案してきたが、複数の計算機による分散並列処理は考慮されていなかった。本論文で提案されている Hadoopde は、非順序型実行方式を Hadoop とその上位層である Hive に適用した並列データ処理系である。本処理系において、それぞれの計算機はデータ処理時にタスク分解を行い、そのタスクが必要とするデータの入出力を自身の二次記憶のみならず、ネットワーク上に存在する他計算機の二次記憶に対しても非同期的に行い、入出力の完了に伴い関連する演算を実行する。これにより、並列データ処理系全体の入出力が非同期化され、処理効率の大幅な向上を実現している。更に、提案手法では非順序型実行方式を Hive に適用し、処理効率の向上を図っている。オリジナルの

Hive 問合せ処理は関係表の全走査を基本としているが、Hadoopde では索引走査を用いた問合せ最適化が行われており、特に選択率の小さい問合せにおける処理効率の大幅な向上を実現している。

評価実験において、ローカルな二次記憶やネットワークを介した他計算機の二次記憶に対するアクセスの一部または全てが非順序型化されていないほかの方式と処理時間を比較しており、特に選択率の小さい問合せに対しては 100 倍以上の大幅な高速化を達成している。更に、ほかの Hadoop 処理系と比較して高いノードスケラビリティを有することを示している。

このように、提案手法はいわゆるビッグデータを活用するための基盤システムとして非常に有望であり、論文賞にふさわしい優れた研究である。

