2018年度

第75回 論文賞贈呈

（写真：敬称略）

論文賞（第75回）は，2017年10月から2018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．

On the Design Rationale of Simon Block Cipher : Integral Attacks and Impossible Differential Attacks against Simon Variants

（英文論文誌A　2018年1月号掲載）

受賞者 近藤倖大

受賞者 佐々木　悠

受賞者 藤堂洋介

受賞者 岩田　哲

本論文では，軽量ブロック暗号の有力な候補としてNSAによって提案されたSimonのバリエーションに対して，積分攻撃及び不能差分攻撃に対する安全性の解析を行っている．

IoT（Internet of Things）デバイスやセンサの爆発的な普及を背景として，これらのデバイスのセキュリティに関する研究開発が盛んに行われている．計算能力や電源容量が貧弱なデバイスで暗号を利用できるようにするには，軽量暗号が必要であり，近年多くの研究がなされてきている．本論文は軽量暗号のうちで軽量ブロック暗号を対象としている．

軽量ブロック暗号SimonはNSAによって2013年に提案されており，そのパフォーマンスの高さから注目されている．Kölblらは2015年にSimonの計算で用いる三つのパラメータ値(a, b, c)を変更したバリエーションを提案し，それらの安全性の解析を行った．オリジナルのSimonはパラメータ値$(1, 8, 2)$と表現される．

本論文ではSimonのバリエーションに対して，積分攻撃及び不能差分攻撃に対する安全性の解析を行った．ブロック暗号Simonの安全性評価の計算量が膨大になる問題に対して，同値類を発見することにより，スーパコンピュータを用いれば計算可能なレベルまで計算量を減少させることに成功している．更には，Wangらの先行研究では一部の平文を選択していたために全てのケースをカバーしていなかった問題を解決し，最適な攻撃を考慮した解析を初めて行っている．この独創的な解析手法は価値が高い．

その結果としてオリジナルのパラメータ値$(1, 8, 2)$の代替パラメータ値として$(5, 12, 3)$が利用可能であることを明らかにした．オリジナルのパラメータ値が新たな解読法で安全でなくなる場合を想定して，代替パラメータ値を用意しておくことは暗号利用の観点からは非常に重要である．この成果は軽量ブロック暗号の利用に大きく寄与するものであり，本会論文賞に値する論文として高く評価できる．

Hierarchical Control of Concurrent Discrete Event Systems with Linear Temporal Logic Specifications

（英文論文誌 A　2018 年 2 月号掲載）

受賞者 **榊原愛海**

受賞者 **潮　俊光**

本論文はコンカレント離散事象システムに対するスーパバイザ制御問題を取り扱っている．コンカレント離散事象システムとは，複数の離散事象システムが共有イベントを使って同期して動くシステムである．この問題に対し，著者らは階層的な制御アーキテクチャを提案した．そのアーキテクチャは局所的なスーパバイザとコーディネータから成る．前者が局所的な仕様を保証する一方，後者は大域的な仕様を満たすように，どの共有イベントを禁止するかを決定する．著者らは当該問題に対してゲーム理論的なアプローチを採用した．まず局所的な仕様に対する Rabin ゲームによって局所的なスーパバイザを構築し，それから再び大域的な仕様に対する Rabin ゲームによってコーディネータを構築する．この制御アーキテクチャにより制御されるコンカレント離散事象システムは与えられた仕様だけでなく，デッドロックフリーの性質も満たす．

本論文の独創性は制御仕様の記述に線形時相論理が用いられる点にある．従来，制御仕様は形式言語で与えられることが多かった．しかしながら，実システムに対して望ましい動作を形式言語で記述することは難しい．時相論理では演算子に時間的な性質に対する意味付けを与えている．制御仕様を線形時相論理によって記述することによって，形式言語を用いた場合に比べて望ましい動作の特徴を理解しやすくしている．

本研究の有効性は提案法が，ファクトリーオートメーションやロボットの協調動作，高度交通システムなど様々なシステムの制御に適用可能な点にある．そのようなシステムを対象とする場合，計算の複雑さが問題となるが，本研究で提案された階層的な制御アーキテクチャは，システム全体でなく，構成要素ごとに問題を分解し，設計することにより，計算の複雑さを軽減することができる．

制御仕様の記述に線形時相論理を用いるという独創性，様々なコンカレント離散事象システムに応用可能であるという有効性から，本論文は本会論文賞にふさわしいものである．

Attribute-Based Encryption for Range Attributes

（英文論文誌 A　2018 年 9 月号掲載）

受賞者 **ATTRAPADUNG Nuttapong**

受賞者 **花岡悟一郎**

受賞者 **小川一人**

受賞者 **大竹　剛**

受賞者 **渡辺　創**

受賞者 **山田翔太**

公開鍵暗号は，送り手と受け手の間で秘密鍵を共有することなく秘匿通信を実現する技術であり，情報セキュリティの基礎技術である．多様なアクセス制御を効率的に実現する公開鍵暗号として属性ベース暗号がある．属性ベース暗号では，利用者並びに暗号化する情報に属性を定め，復号のための条件（ポリシー）を満たした場合のみ暗号文が復号できる．暗号文に属性情報を埋め込み，復号鍵でポリシーを記述する方法と，それとは逆に，復号鍵に属性情報を埋め込み，暗号文にポリシーを記述する方法がある．前者の方法では，例えば，コンテンツに，“genre＝music, day＝20190501”などの属性情報を埋め込み暗号化する．利用者の復号鍵には，“(genre＝sport) OR (genre＝music)”などのポリシーが記述されており，このポリシーを満たす暗号化コンテンツだけを復号することができる．

本論文では，数値属性をポリシーにおいて「範囲」として扱う方法を，効率的かつ一般的な枠組みとして提案している．範囲として扱うとは，ポリシーが“day ∈ [20190401,20200331]”のように指定される場合である．通常の属性ベース暗号においても，論理和の組合せで実現できるが，効率が悪く，範囲要素数の線形オーダで計算量が増える．この問題に対し，範囲に含まれるか否かをセグメント木で判定することで計算量の増加を対数オーダに抑え，その場合に，ポリシーとして共通集合演算を扱えれば十分という点に着目し，それを実現するための一般的構成法を与えている．既存研究においても，計算量増加が劣線形の方式は存在したが，ポリシークラスに制限があった．提案手法では，任意の論理式を扱うことができ，ポリシーの高い表現能力と効率性を同時に達成している．

このように，本論文では属性ベース暗号の高機能化と

効率性を，同時に，かつ一般的な枠組みとして実現している．本成果は，高機能暗号の発展に大きく貢献するものであり，本会論文賞に値する論文として高く評価できる．

屋外イベントなどを想定した人群観測システムの開発と実証実験・評価

（和文論文誌 B　2018 年 2 月号掲載）」



受賞者 新井敬太　受賞者 山本　寛　受賞者 山崎克之

大規模会場におけるイベント運営の際には，来場者人数の管理が重要となる．このようなデータはイベント内容の改善に役に立つだけではなく，イベントを安全に運営するためにも利用可能である．一方，近年ではドップラーセンサなどの接近離反が検知可能なセンサが安価で利用可能である．

そこで本稿では，大規模なイベント会場の運営者が使用可能な，ドップラーセンサを使用した人群観測システムを提案している．混雑状況の測定を行うために，人数だけではなくその場での滞在時間を含む量である人群量を定義する．また，人群量とドップラーセンサの測定値をゴンペルツ曲線で近似することで，センサ値から人群量を計算可能であることを示している．

実証実験のため，新潟県長岡市の国営越後丘陵公園において，イルミネーションイベントと，コスモス・バラをメインにしたイベントにおける人群観測を行った．イルミネーションイベントで収集した解析データに対して EM アルゴリズムによってフィッティングを行い，最繁時刻と混雑時間と最大人群量の三つの特徴量を抽出した．この解析により，最繁時刻と混雑時間は日によってほとんど結果は変わらなかったが，最大人群量は日によって大きく異なることが分かった．また，この最大人群量は最低気温と負の相関があり，気温がより低い日ほど集客が見込めるということが分かった．また，コスモス・バラ祭りイベントにおいては，天候データなどとの相関は見られなかったものの，イベント後に人群量の減少が見られ，イベント効果を確認することができた．

以上のように，本論文では人群量を推定するためのセンシングシステムとデータ解析手法の提案に加え，その有効性を評価するために実施した実証実験の結果を詳細に説明している．これは，実践的な研究開発に取り組むための重要な方向性を示唆するものであり，本会論文賞にふさわしい論文として高く評価できる．

Separating Predictable and Unpredictable Flows via Dynamic Flow Mining for Effective Traffic Engineering

（英文論文誌 B　2018 年 2 月号掲載）


受賞者 高橋洋介　受賞者 石橋圭介



受賞者 辻野雅之　受賞者 上山憲昭　受賞者 塩本公平



受賞者 大歳達也　受賞者 大下裕一　受賞者 村田正幸

ネットワークを流れるトラヒック量は急激に増大しており，限られたネットワークリソースでトラヒック変動に対応するためにトラヒックの経路を動的に制御するトラヒックエンジニアリングの重要性が高まっている．トラヒックエンジニアリングのパフォーマンスはトラヒック予測精度に依存する．しかしながら，コンテンツの多様化・高品質化に伴い，トラヒック量の時系列変動は大きくなっており，トラヒック予測はますます困難となっている．

本論文では，効率的なトラヒックエンジニアリングを実現するために，トラヒックを予測可能な部分と予測困難な部分に分離し，それぞれに対して異なる経路制御ポリシーを適用する新しい手法を考案した．まず，トラヒックデータをフローレベルで分析することで，トラ

ヒック量の時系列変動が緩やかで予測可能なフロー集合と，時系列変動が激しく予測困難なフロー集合に分離する．その上で，予測可能なフロー集合に対してはトラヒック予測結果に基づくリソース利用効率の高い最適経路を算出する経路制御手法を，予測困難なフロー集合に対してはリソース利用効率が若干低くなるもののふくそうリスクを低減する経路制御手法を，それぞれ選択的に適用する手法を考案した．Internet2 の実トラヒックデータを用いた評価により，提案手法は，従来の単一の経路制御アルゴリズムを用いる手法と比較して，ネットワークリソースの利用効率を向上し，ふくそうリスクを低減できることを示した．

以上のように，本論文は，トラヒック特性に応じて適切な経路制御アルゴリズムを選択的に適用することで，トラヒックエンジニアリングの性能を向上させるという全く新しいアプローチに挑戦するとともに，その有効性を実トラヒックデータを用いた評価によって実証している．本成果は，トラヒック量予測に基づく従来のネットワーク制御に代わる，トラヒック特性分析に基づく新たなネットワーク制御の有効性を示し，今後の研究の広がりが期待される．

A Novel Low-Overhead Channel Sounding Protocol for Downlink Multi-User MIMO in IEEE 802.11ax WLAN

（英文論文誌 B　2018 年 3 月号掲載）

受賞者 **鍋谷寿久**

受賞者 **Narendar MADHAVAN**

受賞者 **森　浩樹**

受賞者 **青木亜秀**

最優秀論文賞（第 1 回）に別掲

Demultiplexing Method of Variable Capacity Optical OFDM Signal Using Time Lens-Based Optical Fourier Transform

（英文論文誌 C　2018 年 2 月号掲載）

受賞者 **中川高晃**　受賞者 **三輪貴明**

受賞者 **瀧口浩一**

複数のサブキャリヤチャネル信号を，信号ボーレート間隔で周波数多重し高周波数利用効率通信を実現する OFDM は，無線のみならず一層の大容量化が必要な光通信でも重要である．OFDM 信号のチャネル分離には時間フーリエ変換が必要である．光 OFDM は，固定容量光通信のほかに，必要帯域を適応的に割り当てる次世代容量可変光ネットワークのガードバンド削減にも有用であるが，次世代光通信のチャネル速度は数十 Gbaud を超える．

可変容量光 OFDM 信号を光領域で直接，高速，低消費電力に分離する光フーリエ変換を実現する手法として時間レンズ法に着目し，検討を行った．信号に周期的な線形周波数チャープ（二次位相変調）と，波長分散を与えることで光時間フーリエ変換が実現される．光パルス波形が群速度分散で広がることと，光の空間パターンがフレネル回折で広がることは数学的に同等の方程式に従うため，レンズに対応して時間レンズ法と呼ばれる．将来の集積光回路化を見据え，かつ広範囲の容量変化に精度良く対応するため，チャープ，波長分散生成にはそれぞれ，LN 位相変調器，グレーティング型可変波長分散補償器を用いた．本論文では，提案構成の動作原理を説明した後，位相変調器駆動電圧と必要波長分散値の関係，チャネル周波数間隔と最大分離チャネル数との関係など，動作条件，現状のデバイス性能で実現可能な特性（200 Gbaud 程度までの OFDM 信号分離）を計算で明らかにした．計算結果に基づき，32～40 Gbaud の範囲の可変光 OFDM 信号分離実験を行い，提案手法の原理検証に成功した．位相変調器駆動に必要な 10 GHz オーダの周期二次波形電圧の生成は難しいが，基本波，2 倍波発生用の同期発振器 2 台で簡便に合成できる近似波形を用いて，OFDM 信号を分離可能なことも実験的に明らかにした．

以上本論文では，次世代光通信での適用が期待される可変光 OFDM 信号のチャネル分離法として，時間レンズ法型光フーリエ変換とその集積化に適した構成を提案した．また特性を明らかにし，原理検証実験を行った．今後の光 OFDM の進展に寄与し，本会論文賞にふさわしい．

ビーム伝搬解析と随伴変数法による感度解析を用いた非線形光学デバイスのトポロジー最適設計に関する検討

（和文論文誌 C　2018 年 5 月号掲載）

受賞者 森　洸遥

受賞者 辻　寧英

近年，情報通信サービスが急速に普及しており，基盤となる光通信システムの更なる高速大容量化が求められている．光通信の高速性を最大限生かすには，電気的処理をなくし，光信号を光のまま処理する全光ネットワークの構築が重要である．なかでも，非線形光学効果の一つであるカー効果は高速応答が期待できるため，これを利用した光スイッチや光論理ゲートなどの信号処理デバイスに関する研究が盛んに行われている．

光デバイスの開発は，これまで既存の構造の改良や発見的な方法により行われてきたが，近年，シミュレーション技術の発展と計算機処理能力の向上により，計算機シミュレーションを用いた最適設計法の研究が活発化し，寸法や形状の最適化だけでなく，構造のトポロジーまで含めた非常に自由度の高い設計が可能となってきている．一般に，非線形デバイスの設計は線形デバイスの設計に比べて難易度が高く，こうしたトポロジー最適設計法を非線形デバイスの設計に活用できれば，これまでに考えられなかった全く新しい光デバイスの開発が可能になると期待される．

本論文では，光カー効果を利用した光デバイスのトポロジー最適設計法の開発を行っている．数値解析には波長に比べて数千倍の素子長であっても効率的に解析できるビーム伝搬法を，設計領域内の構造表現には任意のトポロジーを持った構造を表現可能な密度法を採用し，その密度パラメータを勾配法により最適化する．トポロジー最適設計は斬新な構造を自動的に発現できる反面，設計すべき変数が数十万以上にも及び，全ての設計変数の変化に対する特性の感度を効率的に求める必要がある．そのため，設計変数の数によらず 2 回のビーム伝搬解析程度のコストでそれが可能な随伴変数法を非線形デバイスの感度評価に適用できるように新たに定式化を行い，具体的に光スイッチ・光論理ゲートの設計を通してその有効性を確かめている．本設計手法は，フォトニクス分野の様々な次世代素子の開発への応用が期待でき，本会の論文賞にふさわしい論文として高く評価できる．

32-Gbit/s CMOS Receivers in 300-GHz Band

（英文論文誌 C　2018 年 7 月号掲載）

受賞者 原　紳介

受賞者 片山光亮

受賞者 高野恭弥

受賞者 Ruibing DONG

受賞者 渡邊一世

受賞者 関根徳彦

受賞者 笠松章史

受賞者 吉田　毅

受賞者 天川修平

受賞者 藤島　実

300 GHz 帯の電磁波は，「電波」と「光」の中間のテラヘルツ波の周波数帯に当たり，利活用が進んでいない“未開拓の周波数資源”の一つである．テラヘルツ波は大気による吸収が大きいが，300 GHz 付近の帯域は，その中でも大気吸収減衰が小さい「大気の窓」の領域に当たり，比較的長距離の通信が可能であることが示唆されている．もしこの帯域で無線通信用途に幅広い周波数が割り当てられて利用が始まれば，ICT 技術による産業構造の変革を加速させる超高速無線通信技術が実現できると予想される．この期待の下，フォーラムスタンダードとして IEEE 802.15.3d において約 70 GHz にわたる広い帯域に複数のパターンでチャネルが割り当てられ，また国際的な周波数割当の議論も進んでいる．

このテラヘルツ波帯域を利用した無線通信技術を広く一般普及させるためには，量産性に優れるシリコン CMOS 集積回路技術によるトランシーバの開発が望まれる．しかし，最大発振周波数 f_{max} が化合物半導体に

比べて劣るシリコン CMOS ではキャリヤ周波数での信号の増幅ができない．そのため初段に低雑音増幅器（LNA）を配置する従来の無線受信機のアーキテクチャを採用することが困難となる．

本論文は，シリコン CMOS プロセスによる周波数変換器（ミクサ）を初段に配置した 300 GHz 帯の無線受信機の開発を報告した．受信信号を雑音に埋もれないようにするためには，初段ミクサの雑音指数を下げるとともに，変換損を可能な限り低くする必要がある．本論文では，ダブルバランス形の基本波ミクサを採用し，更に 300 GHz 帯で高い出力の局部発振器（LO）信号用ドライバを組み合わせることで，受信性能の劣化を抑制した．同プロセスで開発した CMOS 無線送信機との近距離通信実験において最大 32 Gbit/s の無線通信速度を実証した．300 GHz 帯の無線通信技術の開発は始まったばかりであり，今後，性能の向上とともに，実用化に向けた更なる開発が期待される．

高階エネルギー最小化による医用画像セグメンテーション

（和文論文誌 D　2018 年 1 月号掲載）

受賞者 北村嘉郎

受賞者 石川　博

本論文は，医用画像に対するデータ解析の自動化を目指して，その実現に必須かつ基礎のプロセスであるセグメンテーションの問題に取り組んでいる．セグメンテーションを実現する代表的な手法にグラフカットによるエネルギー最小化がある．ここで，従来の 2 画素間の関係を表す 1 階エネルギーに対して，複数画素間の関係を表すことは高階エネルギーと呼ばれ，最近の発展により 3 画素以上の任意の高階関数を最適化可能になりつつある．したがって，本論文の主題は，セグメンテーションに有効な高階グラフカットの活用方法を確立することである．

特筆すべき本論文の優位性として，解剖学的知見を先見情報としてモデル若しくは探索に反映していることが挙げられる．すなわち，高階化により増大する評価すべき変数や画素の組（クリーク）の形状を，事前知識に従って選択・削減することで高精度なセグメンテーションを可能にしている．更に，著者らがこれまでにも精力的に取り組んできたサブモジュラー関数に着目し，そのエネルギーをグラフカットで高速に最小化することで高階関数導入の有効性と高速性を両立させる枠組みを確立している．

上記の実用性を，造影 CT 画像からの肺動静脈セグメンテーションなど 3 種類のアプリケーションにおいて示している．特に肺動静脈については評価も手厚く実施しており，客観評価に加えて，臨床現場での主観評価を行い，実用性を確認している．本アルゴリズムを搭載した画像診断装置が臨床現場で実用化され，医療の質と効率の向上を実現していることから当該分野における貢献は顕著であり，本賞がふさわしい．

An Efficient Algorithm for Location-Aware Query Autocompletion

（英文論文誌 D　2018 年 1 月号掲載）

受賞者 Sheng HU　受賞者 Chuan XIAO　受賞者 石川佳治

例えば地図を見ながらなじみのコーヒー系列店を探すときのように，位置情報を踏まえた（Location-aware な）検索を高速に行えるようにするアルゴリズムは，今日の我々の生活を豊かにするために大きな役割を果たすようになってきている．本論文では，こうした場面で，先頭の数文字を（例えば，「star...」のように）入力したときに，それに続くような文字列を自動的に補完してそれに合った名前を持つお店などを地図上に高速に表示できるようにするための基盤となるアルゴリズムを提案し，その性能特性を実験により確認している．

このようなアルゴリズムの実現では，range クエリ（ある範囲にあるものを検索するクエリ）と top-k クエリ（最も適切と思われる上位 k 件のみの提示を求める検索クエリ）という 2 種類のクエリを扱えるようにしながら，それらを効率的にかつスケーラブルに動作させるような探索の枝刈り手法が導入され，更に入力エラーに

も柔軟にかつ高速に対処できるような工夫が必要となる．本論文では，これらを満たすようなアルゴリズムを巧妙に設計すると同時に，それを可能にするためのデータ構造としてトライ木を拡張したものを用意し，その課題を解決している．

この目的のための効率的なアルゴリズムは，先ほどの例のような具体的なアプリケーションでのニーズが既にあると同時に，潜在的に適用可能な問題は更に多くあると考えられることから，その大幅な効率化の実現は社会に与えるインパクトも大きなものである．本論文が提案するアルゴリズムの実現は，以上の点から社会に大きなインパクトを与える可能性のある重要な貢献であり，本賞受賞にふさわしい内容である．

複数人による双方向の対面行動を計量する頭部装着型デバイス

（和文論文誌 D　2018 年 2 月号掲載）

受賞者 **蜂須　拓**

受賞者 **Yadong PAN**

受賞者 **松田壮一郎**

受賞者 **Baptiste BOURREAU**

受賞者 **鈴木健嗣**

他者と顔を向かい合わせる行動は社会において重要である．コミュニケーション相手の顔を見ることは，視線や表情を手掛かりとすることで，相手の意図や感情といった内部状態の推定を可能にする．例えば，「休みが取れていいなぁ」という上司の言葉は，笑っていない目を見ることによって「この忙しいときに休みを取るなよ」という意味を持つ皮肉であることが理解できる．また，乳幼児が物理世界及び社会に関する知識を分節化する（知識獲得）際には，養育者の視線や表情が重要なキューになると言われている．一方で，発達障害の一つである自閉スペクトラム症者は顔を見ることを避けたり，相手と視線を合わせにくいことが知られており，このことが自閉スペクトラム症者の社会的コミュニケーションの困難さを引き起こしていると考えられている．このような背景から，本研究では，対面行動の計量及び対面の促進を目的とするデバイスを開発した．本デバイスはコミュニケーションの当事者が頭部前部に装着するヘアバンド状のシンプルな発光デバイスである．デバイスには赤外線通信モジュールが搭載されており，相互に光軸の状態を計測することで，両者ともに向き合ってない状態，片方だけが見ている状態，お互いに向き合っている状態を識別することができ，その状態に応じて発光色を変化させることができる．本論文では，実際に制作した装置を用いて性能評価実験を行い，基本的な性能を有することを示した．このデバイスは定型発達者のデータを用いることで，自閉スペクトラム症者に対してどのような対面行動をとるべきかを明示することを可能にする．すなわち，暗黙的な社会ルールの見える化である．自閉スペクトラム症者に対して社会ルールの明示化は有効である．本デバイスはシンプルでかつ分かりやすい方法で見える化を実現した．以上のことから，本デバイスは発達障害者の抱える困難さを解消する可能性を有しており，実社会での貢献が期待されるため，本会論文賞にふさわしい論文として高く評価できる．