

# 論文賞贈呈

(写真：敬称略)

論文賞（第66回）は、平成20年10月から平成21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。

## Strongly Secure Linear Network Coding (英文論文誌 A 平成20年10月号掲載)



受賞者 原田邦彦



受賞者 山本博資

インターネットのようなネットワークは、通信路と中継を行うコンピュータをそれぞれ辺と頂点で表し、各辺で有限体の要素を1シンボル伝送できるものとする、グラフを用いてモデル化できる。グラフ内の一つの情報源点から複数の受信点に同じ情報を伝送するマルチキャスト通信では、各頂点で単にルーティングを行うだけでなくネットワーク符号化を行うことで、より多くの情報を伝送できる。マルチキャスト通信容量  $h$  を持つネットワークにおいて、盗聴者がグラフ内のどの  $k$  ( $k < h$ ) 本の辺を盗聴しても  $r$  ( $=h-k$ ) シンボルの伝送情報が全く漏れないように工夫された符号は、「 $k$  安全なネットワーク符号」と呼ばれる。従来、 $k$  安全なネットワーク符号の構成法は知られていたが、 $k$  本以上の辺を盗聴されると、伝送情報の一部が完全に盗聴者に漏れ出す危険性があった。

本論文は、 $k$  安全なネットワーク符号がランプ形しきい値秘密分散法と密接な関係にあることを指摘し、ランプ形しきい値秘密分散法において定義されていた強い安全特性をネットワーク符号に導入している。つまり、 $k$  安全なネットワーク符号の特性に加えて、どの  $k+j$  本の辺を盗聴されても、伝送情報のどの  $r-j$  シンボルも盗聴者に漏れないという特性を持つ「強い  $k$  安全なネットワーク符号」を定義し、そのような符号を満たすべき必要十分条件を理論的に導出している。そして、その条件を用いて、具体的に強い  $k$  安全なネットワーク符

号の構成法を与えている。また、安全でないネットワーク符号が用いられているとき、伝送情報を線形変換することにより、それを強い  $k$  安全なネットワーク符号に変換するアルゴリズムも与えている。更に、本論文では、上記の強い  $k$  安全なネットワーク符号を構成できるために必要な有限体のサイズの十分条件を理論的に導出している。

以上のように、本論文は強い安全性特性を持つネットワーク符号の構成法に関して、理論的な解析だけでなく、効率の良い符号の具体的な構成法を与えており、高く評価できる。



## Extended Password Recovery Attacks against APOP, SIP, and Digest Authentication (英文論文誌 A 平成21年1月号掲載)



受賞者 佐々木 悠



受賞者 王 磊



受賞者 太田和夫



受賞者 國廣 昇

ハッシュ関数は、任意の長さの入力に対してあらかじめ定められた長さの出力を与える変換である。多対1の

対応を与えるので、同じ値を出力する異なる入力の組が存在することは明らかであるが、この組を実際に発見(衝突攻撃)するのに要する計算時間が問題となる。

近年、ハッシュ関数の衝突攻撃の研究が進展し、代表的なハッシュ関数 MD5 についても簡単に衝突を求めることができる。MD5 は、メールプロトコル APOP (Authenticated Post Office Protocol) に使われているため、APOP の安全性に影響が生じ得る。当初、衝突攻撃と秘匿パスワードの取得は無関係と思われたが、衝突攻撃を工夫すると、APOP の場合、パスワードを 3 文字まで取得可能であることが知られていた。しかし、MD5 の衝突発見手法の制約により、漏えい文字数が少ないため、深刻な脅威とはならないと判断されていた。

本研究の第 1 の貢献は、漏えいする文字数の限界を 3 文字から 31 文字に緩和することに成功したことにある。ハッシュ値の衝突を直接見つけるのではなく、攻撃条件を緩和した「擬似衝突」という中間段階を導入し、擬似衝突から真の衝突を生成するアプローチを発見することにより、効率的な攻撃導出に成功している。

第 2 の貢献は、「擬似衝突」を、APOP 以外の認証プロトコル、ダイジェスト認証と SIP (Session Initiation Protocol) に適用可能であることを発見したことにある。これらのプロトコルは、より安全なハッシュ関数の利用を規定しているが、サーバになりすました攻撃者がプロトコルのシステムパラメータを自分に都合良く設定することで、APOP と同様の攻撃を適用できることを発見した。また、実験により、攻撃していることをクライアントに検知されないままパスワードを取得する条件を導出した。

本研究は、ハッシュ関数の衝突攻撃という理論的な成果を、実サービスで実際に使われるプロトコルの安全性解析に反映させた、理論面、実用面のバランスのとれた論文である。本会論文賞としてふさわしい論文であると高く評価できる。



## Error-Trellis Construction for Convolutional Codes Using Shifted Error/Syndrome-Subsequences

(英文論文誌 A 平成 21 年 8 月号掲載)



受賞者 田島正登 受賞者 沖野浩二 受賞者 宮腰 隆

本論文は、畳込み符号の検査行列  $H(D)$  (遅延作用素  $D$  の多項式を成分とする) に基づくエラートレリスの一般的構成法について論じている。なお、 $H(D)$  は正準と仮定する。 $H(D)$  の列が ( $D$  の) 単項式因子を含む場合、Ariel らはエラートレリスの状態数を従来法より低減できる可能性があることを既に示している。その方法は  $H(D)$  から導かれるスカラ検査行列に基づくものであり、エラートレリスの構成法は複雑である。これに対し、本論文では、 $H(D)$  の列に単項式因子 (べき指数を  $p$  とする) を含む場合、その列から単項式因子を掃き出す (除する) ことと対応するエラー部分系列を  $p$  だけ (順方向に) 時間シフトさせることが同等であることに注目して、エラートレリスの状態数を低減している。エラー系列の時間シフトは非常に単純な概念であり、提案法は極めて分かりやすいことが特徴になっている。

また、提案法と Ariel らの方法の関連について例題を用いて詳細に検討しており、エラートレリスの状態数の低減について両者が同等の効果を持つことが示されている。エラー系列の時間シフトは  $H(D)$  の列から単項式因子を掃き出すことに相当するが、この論文では、更に、 $H(D)$  の列に単項式を掛けることによっても、得られた検査行列を等価変形することにより、エラートレリスの状態数を低減できる場合があることを示している。これは対応するエラー部分系列を逆方向に時間シフトすることに相当しており、この内容は Ariel らの方法からは導くことができない。なお、 $H(D)$  の行に単項式因子を含む場合も、シンドローム部分系列を時間シフトすることで状態数を低減できることが同時に示されている。

列や行に単項式因子を含む検査行列はやや特殊とも思われるが、Tanner らはこのような形の検査行列から定義される LDPC 畳込み符号を提案しており、対応するエラートレリスの状態数低減に適用できる。提案法は非常に構成的かつ具体的であり、畳込み符号のエラートレリスを最初に提案した Schalkwijk らの方法を一般化したものとみなすことができる。このように、本論文は畳込み符号のエラートレリスの構成及び構造に対し新たな視点を与えたものとして高く評価できる。

**無線センサノードのための  
ハードリアルタイム保証が可能な仮想マシン**  
(和文論文誌 B 平成 21 年 1 月号掲載)



受賞者 鈴木 誠



受賞者 猿渡俊介



受賞者 南 正輝



受賞者 森川博之

無線センサネットワークの多くのアプリケーションにおいてはリアルタイム処理が必要となる。例えば、無線通信のタスクが遅延するとパケット損などの問題が引き起こされる。また、サンプリングの実行が遅延するとサンプリング精度が劣化し、地震観測のように高精度な測定を必要とするアプリケーションを実現できない。すなわち、優先度に基づいてタスクスケジューリングを行い、すべてのタスクの時間制約を保証する必要がある。

一方、無線センサネットワークを長期運用する際にはソフトウェア保守が問題となる。これに向けて、省電力及びシステム保護の観点から、ソフトウェアを部分的に修正可能とする仮想マシンが必要である。

仮想マシンを利用する場合、実行性能が低下するためリアルタイム保証がより重要となる。しかしながら先行研究は実行性能と保護機能のトレードオフの取扱いに注力しており、タスクの時間制約を考慮していない。

このような観点から、本論文では、リアルタイム処理が可能なセンサノード用仮想マシン「VAWS」の開発について述べられている。VAWSは実行性能の改善を直接の目的とするのではなく、時間制約を満たすことが重要であるとの観点から、ハードリアルタイム処理の実現に重点を置いて設計されている。具体的には、センサノード上で時間制約のあるタスクがCPUの割込みによって発生する点に着目し、割込みベクトルごとに独立した仮想マシンをオペレーティングシステムを介することなく直接実行する。これによって、簡単な仕組みながらも低オーバーヘッドで優先度に基づくタスクスケジューリングを実現している。

本論文は無線センサネットワークにおいてリアルタイム処理の重要性を示し、本研究分野の新たな方向性を示

唆しているという点で高く評価できる。また、シミュレーションにとどまりがちな無線センサネットワーク分野において、アプリケーションを明確に意識し実装評価を通して有効性を示しているという点で、実装論文としての意義も高い。



**高分解能到来方向推定のための  
アレーキャリブレーション手法**  
(和文論文誌 B 平成 21 年 9 月号掲載)



受賞者 山田寛喜

喜安善市賞（第3回）に別掲



**Introduction of Frequency-Domain Signal  
Processing to Broadband Single-Carrier  
Transmissions in a Wireless Channel**

(英文論文誌 B 平成 21 年 9 月号掲載)



受賞者 安達文幸



受賞者 留場宏道



受賞者 武田一樹

広帯域無線チャネルは遅延時間の異なる多数の伝搬路から構成される周波数選択性チャネルである。周波数選択性チャネルを多数の直交チャネルに分解して並列伝送する直交周波数分割多重 (OFDM) が脚光を浴びているが、送信信号のピーク対平均信号電力比 (PAPR) が大きい。一方、シングルキャリア (SC) 伝送は PAPR が小さいという利点があるものの、符号間干渉 (ISI) に

よりビット誤り率 (BER) 特性が大幅に劣化してしまう。本論文は、他グループの研究論文も引用・紹介しながら、著者らのグループの SC 周波数領域等化 (SC-FDE) に関する先駆的研究を体系立てて整理したものである。

サイクリックプレフィックス (CP) を付加した SC 伝送のチャンネル行列は巡回行列となり、離散フーリエ変換 (DFT) によって対角化できる。これに基づけば簡単な構造の 1 タップ FDE が可能であり、最小平均二乗誤差 (MMSE) 規範を用いる MMSE-FDE では ISI を抑圧しつつ周波数ダイバーシチ利得が得られるから大幅に BER 特性を改善できる。しかし、CP 付加は伝送効率の低下を招く。DFT 区間をオーバーラップさせながら FDE を順次行うオーバーラップ MMSE-FDE は CP 付加をせずに優れた BER 特性を得ることができる。これらの MMSE-FDE では ISI が残留するため特性改善には限界があるが、残留 ISI キャンセルと MMSE-FDE とを繰り返せば、マッチドフィルタ (MF) 限界に近い BER 特性を実現できる。また、複数送受信アンテナを用いる MIMO ダイバーシチ・アレー・空間多重へ FDE を導入すれば周波数ダイバーシチ利得を得て優れた BER 特性を実現できる。

著者らのグループの先駆的研究は、SC-FDE が OFDM とそん色ない超高速伝送を実現可能であることを明らかにしたものであり、その価値は高く評価される。なお、無線チャンネルを多数の直交チャンネルに分解して周波数領域で信号処理する考えは、OFDM と SC-FDE とで原理的に同じであり、違いは信号波形にある。今後は、SC 及び OFDM を統一的にとらえた新たな波形生成と周波数領域信号処理技術へと発展することが期待されている。



## TMR ロジックに基づくルックアップテーブル回路とその瞬時復帰可能 FPGA への応用 (和文論文誌 C 平成 21 年 7 月号掲載)



受賞者 鈴木大輔



受賞者 夏井雅典



受賞者 羽生貴弘

FPGA (Field Programmable Gate Array) はユーザが所望の論理演算機能を直接プログラム可能な回路であり、様々な分野への応用が期待されている。その一方、回路情報を SRAM (Static RAM) に記憶する従来の FPGA では、トランジスタの漏れ電流に起因する非稼働時の消費電力、すなわち待機電力の増大が、その高集積化を妨げる要因となっている。回路電源の遮断による待機電力の通減技術も提案されてはいるものの、SRAM は揮発性メモリのため、電源再投入時に外部メモリを介した回路情報の再読み込みが必要となり、復帰動作における遅延と電力の増加が問題となる。

これに対し、本論文では、TMR ロジックと呼ぶ新しい回路技術による問題の解決を図っている。TMR ロジックは、スピン素子の一つである TMR (Tunneling Magneto-Resistive) 素子と MOS トランジスタの融合により実現される回路技術であり、著者らの研究グループがその回路構成及び原理動作を世界に先駆けて実証してきたものである。TMR 素子は抵抗値により情報を記憶する不揮発性素子であり、スピン注入磁化反転による低電力書き込み、高い書換え耐性、三次元積層による低い面積オーバーヘッドといった優れた特長を有する。TMR 素子の活用により回路情報を内部で不揮発的に保持できるため、電源遮断状態からの瞬時復帰が可能となる。

TMR ロジック活用の典型例として、本論文では、FPGA の主たる構成要素であるルックアップテーブル (LUT : Lookup Table) 回路の設計について述べている。従来の TMR ロジックは差動論理をベースとしており、正論理回路網と負論理回路網の電流比較により出力が決定される。この回路網は 2 進木構造となっており、実用レベルである 4 入力以上の LUT では素子数の増加が著しい。これに対し、提案方式では、片側の回路網に流れる電流を固定にし、もう一方の回路網に流れる電流の中間に設定することで素子数の削減が可能であり、従来方式と比較して高性能化を達成している。

このように本論文は FPGA 高集積化における待機電力問題を解決し得る画期的な技術であり、非常に高く評価できる。

## 高調波負荷を最適化した 高出力低位相雑音 76 GHz MMIC 発振器 (和文論文誌 C 平成 21 年 7 月号掲載)



受賞者 渡辺伸介



受賞者 松塚隆之



受賞者 天清宗山



受賞者 後藤清毅



受賞者 奥 友希



受賞者 石川高英

本論文は高周波電気信号発生器である発振器の低位相雑音化及び高出力電力化に関する研究成果を報告している。発振器は移動体通信機器や移動体レーダ等の無線装置において使用され、その特性は無線装置全体の性能に影響を及ぼす重要な回路である。このため高出力周波数、高出力電力、そして低位相雑音特性を示す発振器が望まれてきた。位相雑音とは出力周波数がどれだけ所望の周波数のみであるかを示す指標である。

発振器の位相雑音を抑制するために発振器内部回路の基本波負荷の最適化がこれまで行われてきた。しかし基本波負荷を最適化した発振器に対して、更なる低位相雑音化または高出力化を図るための手法の多くは位相雑音と出力電力との間にトレードオフが生じる問題があった。

本論文の独創的な点は、低位相雑音化と高出力電力化に対するアプローチとして 2 倍波周波数における発振器内部回路の負荷、すなわち 2 倍波負荷に注目した点である。本論文では 2 倍波負荷の最適条件を導出するために、発振器の 2 倍波周波数における等価回路を想定した解析が行われている。この解析によればバイポーラトランジスタのベース及びエミッタに付加される回路の 2 倍波負荷を短絡とすることで、最小位相雑音及び最大出力電力の同時実現が可能であることが示されている。本論文では回路シミュレーション及び電磁界シミュレーションにより、上記の回路解析から導出した最適条件の妥当性が確認されたことが報告されている。

更に本論文の著者らは発振器内部の基本波負荷を一定に保ったまま 2 倍波負荷を変えた MMIC 発振器群を試作している。これらはすべて 76GHz 信号を発生する発振器である。試作の結果、ベース及びエミッタに付加さ

れる回路の 2 倍波負荷を短絡とした発振器において最小位相雑音及び最大出力電力が実現され、回路解析及びシミュレーションとの良好な一致が得られたことを報告している。2 倍波負荷を最適化した 76GHz 発振器において  $-0.7\text{dBm}$  の出力電力及び  $-112\text{dBc/Hz}$  の 1MHz オフセット位相雑音が達成されている。この位相雑音特性はこれまでに報告された 75 ~ 110GHz 帯 MMIC 発振器の中でも最小値であり、極めて良好な特性である。



## A 5-bit 4.2-GS/s Flash ADC in 0.13- $\mu\text{m}$ CMOS Process (英文論文誌 C 平成 21 年 2 月号掲載)



受賞者 Ying-Zu LIN



受賞者 Soon-Jyh CHANG



受賞者 Yen-Ting LIU

画像センサなどにより得られるリアルワールドの情報は通常アナログ信号である。そのような信号をデジタル LSI やコンピュータで処理するためには、デジタル信号に変換するためのアナログ・デジタル変換器 (A-D 変換器) が必須となる。近年、高解像度な画像センサにより得られた大容量なデータを転送・記憶・処理する必要性が高まっているため、高速な A-D 変換器として用いられるフラッシュ形 A-D 変換器の高精度化・高速性・低消費電力性は極めて重要となっている。CMOS 技術の進歩と回路寸法の小形化でフラッシュ形 A-D 変換器の変換速度がギガヘルツ領域に達したが、これに伴う電源電圧の低下で入力信号電圧と基準電圧アレー間のオフセット電圧に由来する誤差が無視できなくなった。また、フラッシュ A-D 変換器ではビット数の増加に従い回路規模が急激に増加するという問題もある。これらの問題を解決するために“補間法”や“抵抗性平均化ネットワーク法”といった手法が提案されている。“補間法”は回路規模を削減できるが、消費電力を増加させるという欠点がある。一方、“抵抗性平均化ネットワーク法”はオフセット電圧を減少するために用いられ、消費電力を削減できるが、回路規模を増加させるという欠点がある。このようなトレードオフのため、これらの手法をどのように組み合わせるかは、従来は設計者の経験に基づいて決定されており、種々の要求仕

様を満たす回路を設計するのが極めて難しくなっている。

本論文は、補間法と抵抗性平均化ネットワーク法が消費電力・回路規模に与える影響を数学的にモデル化した極めて学術性の高い論文である。また、提案の数学的モデルを用いることにより、設計者は消費電力・回路規模の仕様を満たす回路構成を導出することが可能となり実用性も極めて高い。提案の設計手法に基づき、 $0.13\mu\text{m}$  プロセスを用いて5ビットA-D変換器を試作し、最新の種々のA-D変換器と性能比較を行い、高速性・低消費電力性において優れた結果を得ている。このように本論文は、学術面と産業的な実用性の両面において有用性の高い技術を提案しておりその価値は高く評価できる。



### パターン識別のための錐制約部分空間法

(和文論文誌D 平成21年1月号掲載)



受賞者 小林 匠



受賞者 大津展之

パターン認識分野で用いられる識別法の一つとして部分空間法がある。日本のパターン認識コミュニティにおいて、近年「部分空間法研究会」が立ち上がり、様々な発展を遂げるとともに、実用面についても、文字認識、顔認識といった場面で利用されている手法である。

本論文では、その部分空間法に対し、分布の近似を超平面で行うのではなく、ベクトル空間内の「錐」で近似して識別を行う、錐制約部分空間法を提案した。パターンの特徴量として用いられる画像濃淡値の物理量や、最近、頻繁に利用されているこう配方向ヒストグラムに基づいた局所特徴量は、非負領域のみに存在しており、ベクトルのスケール変化、ベクトルの加法による変動により、ベクトル空間内で錐形状をなす。この性質に着目した近似であることから、従来の部分空間法と同様に広い変動を許容するとともに、超平面による粗い近似とは異なり、識別性能の改善が見込まれる。

また、計算量や分布の近似度合いに関連して複数の手法が考察されており、サンプルの張る厳密な凸錐、そのサンプルを包括する凸錐による近似、円錐による近似の三つの手法が提案されている。これらは従来の部分空間

法と異なり次元数がある程度高くとれば認識率が一定となり、次元数の設定が容易となるという性質があるとしている。認識は入力ベクトルと最も近い錐への正射影ベクトルとの角度を用いており、非負最小二乗法を用いて計算できる。実験においては、顔検出と人物検出の公開データを用いて評価しており、提案した三手法と従来法との比較を行って、有効性を確認している。

特徴ベクトルの非負性に着目し、特徴ベクトルが張る空間を錐でとらえた議論は非常に興味深い。非負特徴ベクトルの変動を許容し、特徴ベクトルが張る領域を凸錐でとらえようとする発想は、まさに部分空間法を更に進化させるものであると思われる。また、原理は単純であるにもかかわらず、識別能力が大きく向上することが期待され、その有効性も高く評価できる。今後、凸錐で表現された部分空間の性質に関する議論や識別時の計算の効率化に関する議論などが繰り返されるのが予想され、新たな方向性を示す論文である。学術的にも今後の開発にも重要な知見を与える価値の高い論文である。



### 視覚的文脈を用いた人物動作のカテゴリ学習

(和文論文誌D 平成21年8月号掲載)



受賞者 木谷クリス真実



受賞者 岡部孝弘



受賞者 佐藤洋一



受賞者 杉本晃宏

大量に蓄積されたビデオデータベースを利活用する取組み、中でも、人物行動の認識・理解を行う研究に、安心・安全な社会の実現に向けた期待が集まっている。人物行動は、短時間で行われる動作によって構成されるため、動作カテゴリ学習は、その基盤となる重要な研究課題である。大規模なビデオデータベースが処理対象となるため、学習の自動化が不可欠である一方、正確な動作認識のためには、複雑な見え方のシーンに対しても高

い学習精度を実現する必要がある。

このような挑戦的な研究課題に対し、本論文では、人物動作が“動き（時間的特徴）”と“見え（空間的特徴）”から構成されていることに着目し、視覚的文脈という新しいアプローチを用いて、ビデオデータベースから教師なしで人物の動作カテゴリーを学習する手法を提案している。複雑な背景を有するなど、シーンごとに大きく変動する情報量を取り扱う必要があるが、クラスタリング手法の改良や動作学習における雑音対策などを提案し、目的実現に向け総合的に取り組んでいる。

まず、ビデオデータベースを数秒間のビデオセグメントに分割し、それらから空間的特徴である視覚的文脈と、時間的特徴である動作特徴量を抽出する。次に、2段階クラスタリング手法を用いて、各ビデオセグメントの動作特徴のヒストグラムを生成する。最後に、特徴ヒストグラムに二つのモードを持つ潜在変数モデルを適用し、教師なし動作カテゴリー学習を実現する。

提案手法の有効性は、「動作・動作に関係のある物体・背景」を含むデータベースを用いた実験により実証されている。データベースの動き特徴に従来手法を適用した動作カテゴリーの学習結果から、動きのみでは正しい学習が困難であることを示し、提案手法の学習結果により、視覚的情報を併用する有効性を示している。更に、視覚的情報を用いることで類似動作の区別が可能になることや、提案手法が背景に含まれる視覚的雑音による影響を受けずに、動作に関係のある視覚的情報だけを利用することを示している。

以上のように、本論文は、人間の知覚行動を慎重に分析し、それを計算機上で実行するための手法を、堅実なアプローチで実現している。時間的・空間的特徴を併用するシーン理解は、人物動作以外の応用の可能性もあり、蓄積された大量の映像情報の利活用を推進する基盤技術の一つに位置付けられ、その価値が高く評価できる。



## Approximate Nearest Neighbor Search for a Dataset of Normalized Vectors

(英文論文誌 D 平成 21 年 9 月号掲載)



受賞者 寺沢憲吾



受賞者 田中 謙

最近傍探索 (Nearest Neighbor Search) は、与えられたデータ集合の中から、問合せデータに最も近いデータを探索する問題であり、パターン認識、機械学習、データマイニングなどをはじめとする多くの情報処理課題における基本問題の一つである。近年、様々なデータの蓄積や流通手段の進歩に伴い、膨大なデータ集合に対して最近傍探索を効率的に行うことの重要性が高まっており、とりわけ、テキスト、音、画像などのようにデータが高次元ベクトルで表現される場合に、良い近似解を高速に求める手法の研究が盛んである。

本論文は、近似最近傍探索の手法として近年注目を集めている LSH (Locality-Sensitive Hashing) と呼ばれる枠組みにおいて、新たな探索アルゴリズムを提案するのである。LSH は、通常のハッシュ法と同様に、データをハッシュ関数によって分類しておくことで探索範囲を限定し高速化を図る枠組みであるが、最近傍探索では厳密一致だけではなく近傍の探索を行う必要があるために、近傍のデータが近傍のハッシュ値に変換されやすいようなハッシュ関数の集合を用いる。このような LSH の基本的な手法は約 10 年前に提案され、これまでも様々な改良が報告されてきたが、本論文では、すべてのデータが単位円上に存在するというデータに関する仮定を導入して、そのもとで既知の方法をしのぐ性能を持つアルゴリズムを導いた点に特徴がある。この仮定はパターン認識分野などにおいて現実的に想定し得る範囲といえる点が重要である。提案アルゴリズムは、データが上記制約を満たすときには、ハッシュ関数における次元の縮退に起因するハッシュ値の衝突を回避し得るなどのメリットを活用したものとなっている。また、本論文では、処理時間・所要記憶量の両面において提案アルゴリズムの有効性を丁寧に考察し、検証している。

このように、本論文は、重要な問題に対して独自の着想のもとに有効な手法を導いたものであり、研究分野の発展に貢献する優れた論文である。

