情報処理 12

IPSJ MAGAZINE
情報処理学会誌

Vol.47 No.12 2006年12月
通巻502号

● CONTENTS ●

特集 Special Features 量子コンピュータと量子計算

Quantum Computer and Quantum Computing

1310 編集にあたって　河野泰人・白木善尚
Foreword *Yasuhito KAWANO (NTT Corp.) and Yoshinao SHIRAKI (Shonan Institute of Technology)*

1311 1. 量子コンピューターその本質と，最近の研究展開　竹内繁樹
Quantum Computers – The Physical Essence and Recent Progresses *Shigeki TAKEUCHI (Hokkaido Univ.)*

1317 2. 量子情報処理と光による研究　井元信之
Quantum Information Processing : Research with Photons *Nobuyuki IMOTO (Osaka Univ.)*

1323 3. Shor のアルゴリズムのための効率的な量子回路　高橋康博
Efficient Quantum Circuits for Shor's Algorithm *Yasuhiro TAKAHASHI (NTT Corp.)*

1329 4. 情報・物理双方から見た量子探索アルゴリズム　加藤　豪・谷誠一郎
Computational and Physical Aspects of Quantum Search Algorithms *Go KATO (NTT Corp.) and Seiichiro TANI (NTT Corp. / JST ERATO-SORST)*

1335 5. 量子回路の自動設計手法　中島裕美・河野泰人・関川　浩
Quantum Circuit Design *Yumi NAKAJIMA, Yasuhito KAWANO and Hiroshi SEKIGAWA (NTT Corp.)*

1341 6. 量子－古典協調計算―オートマトンの場合―　中西正樹
Quantum-Classical Co-operation - Automata with Quantum and Classical Resources - *Masaki NAKANISHI (Nara Institute of Science and Technology)*

1347 7. 量子通信計算量理論 －花子から太郎へ　西村治道・レイモンド ルディ
Quantum Communication Complexity - From Alice to Bob - *Harumichi NISHIMURA (Osaka Prefecture Univ.) and Rudy RAYMOND (IBM Japan)*

解説 Articles

1357 ストリーム暗号の最新動向－ユビキタス社会を実現するセキュリティ技術－
田中俊昭・清本晋作・櫻井幸一
The Latest Trends in Stream Ciphers - Security Technology for Ubiquitous Information Society - *Toshiaki TANAKA, Shinsaku KIYOMOTO (KDDI R&D Labs. Inc.) and Kouichi SAKURAI (Kyushu Univ.)*

1365 エネルギーキーデバイスとして注目される電気二重層キャパシタ　長谷部章雄
Remarkable Electric Double Layer Capacitor as Energy Key Device *Akio HASEBE (NEC TOKIN Corp.)*

1372 教養としてのコンピュータ・サイエンス教育－東京工業大学での試み　渡辺　治
Computer Science as a Basic Course for College Freshmen *Osamu WATANABE (Tokyo Institute of Technology)*

情報処理学会事務局本部
〒101-0062 東京都千代田区神田駿河台 1-5　化学会館 4F　Tel(03)3518-8374（代表）　Fax(03)3518-8375　E-mail:somu@ipsj.or.jp　http://www.ipsj.or.jp/
郵便振替口座　00150-4-83484　　銀行振込（いずれも普通預金口座）　　みずほ銀行虎ノ門支店　1013945　　三菱東京 UFJ 銀行本店　7636858
名義人　社団法人　情報処理学会

連載 Series

1354 これからの情報処理学会　21 世紀社会における IT の役割　前田　章
Thoughts about the Future IPSJ : The Role of Information Technology in the Society of the 21st Century *Akira MAEDA (Hitachi, Ltd.)*

1382 グリッドと SOA からみる Web サービス標準技術　WS-Notification の基礎　Web サービスの非同期メッセージングの実装　丸山不二夫
Explanations of Web Service Standards from the Viewpoint of Grid Computing and Service Oriented Architecture : Foundation of WS-Notification / Implementation of Asynchronous Messaging in Web Services *Fujio MARUYAMA (Wakhok Univ.)*

1393 21世紀のコンパイラ道しるべ‥COINSをベースにして　COINS における並列化
渡邊　坦・岩澤京子・藤瀬哲朗・弓場敏嗣・福岡岳穂
A Guide for Compiler Developers Using the Latest Tool - The COINS Compiler Infrastructure - : Parallelization in COINS Compiler Infrastructure *Tan WATANABE (Association for COINS Compiler Infrastructure), Kyoko IWASAWA (Takushoku Univ.), Tetsuro FUJISE (Mitsubishi Research Institute, Inc.), Toshitsugu YUBA (The Univ. of Electro-Communications) and Takeaki FUKUOKA (Sony Computer Entertainment Inc.)*

コラム Columns

1353 標準化よもやま話　思い出に残る国際会議　吉岡稔弘
Small Talk on Standardization : The Memorable ISO Meeting *Toshihiro YOSHIOKA (AI Research Institute, Inc.)*

1378 研究会千夜一夜　ゲーム情報学とゲーム情報学研究会　金子知適
1001 SIG Nights : Game Informatics and SIG-GI *Tomoyuki KANEKO (The Univ. of Tokyo)*

1380 研究会千夜一夜　エンタテインメントコンピューティング研究会　星野准一
1001 SIG Nights : Entertainment Computing *Junichi HOSHINO (Univ. of Tsukuba)*

1390 オープンソース事情　OSS はどこまで使えるのか？　鈴木友峰
Open Source Phenomena : Overview of DBMS Benchmark Project *Tomomi SUZUKI (Hitachi, Ltd.)*

その他

1402 会員の広場
1404 IPSJ カレンダー
1406 人材募集
1409 有料会告
1415 有料会告について
1417 おふぃすらん
1419 アンケート用紙
1420 編集室／次号予定目次
1421 掲載広告カタログ・資料請求用紙
1422 賛助会員のご紹介
巻末 「情報処理」第 47 巻総目次

規格部
〒 105-0011 東京都港区芝公園 3-5-8　機械振興会館 308-3　Tel(03)3431-2808　Fax(03)3431-6493　E-mail:standards@itscj.ipsj.or.jp　http://www.itscj.ipsj.or.jp/
支　部
北海道／東北／東海／北陸／関西／中国／四国／九州

編集子独白

- editor's monologue -

アインシュタインの相対性理論については「そんな筈はない」という反論（にも値しない議論）がたくさん出され，エセ科学の常として一般向けの書物が数多く出版されている．このような書物が売れるのも，相対性理論と常識との乖離の大きさによるのだろう．ところが常識との乖離という意味では，極微の世界を扱う量子力学の方が相対性理論よりも数段上である．何しろ，世界の根本原理の中に確率や複素数を持ち込み，「物の実在は存在確率でしか定義できない」というとんでもないことを主張する．量子力学の枠組みが常識とはあまりにもかけ離れているので，エセ科学の題材にもほとんどなっていないぐらいである．

今月号の特集は「量子コンピュータと量子計算」．**白木善尚，河野泰人**がエディタ．量子力学を知らないと理解が困難である量子計算の実態を，物理法則の入門的解説から始め，通信計算量の話までをカバーする．「当初よりはかなり研究が進んだが，これから行くべき道のりもかなり遠い」というのが取り組んでいる方々の本音か．盗聴に対抗するための量子暗号に関する研究が実用に一番近くなっているように見える．量子計算機がすぐにでも実現されると思っている向きも，実現はまったく絶望的だと考えている方も，この特集を気を入れて読むことをおすすめする．

「教養としてのコンピュータ・サイエンス教育ー東京工業大学での試みー」（**渡辺治**）は，情報教育として，狭い意味でのコンピュータリテラシーの次の段階をどのように設定するかについての著者の大学での試み（コンピュータサイエンスへの誘導）の紹介．

「エネルギーキーデバイスとして注目される電気二重層キャパシタ」（**長谷部章雄**）は，通常の大容量コンデンサと普通の電池（二次電池）との間の特性を持つ素子についての解説．化学反応をともなわないので，特性の劣化も少なく充電時間が短いというものらしい．

「ストリーム暗号の最新動向」（**田中俊昭，清本晋作，櫻井幸一**）は，鍵を連続的に生成して暗号化する方式の解説．SSLや無線LANで使われているという．暗号の安全性については，「xxx攻撃」という，素人目にはアドホックに見えるカテゴリーが山ほど登場してわずらわしい．もっとすっきりとした定式化はないものか．

「WS-Notificationの基礎　Webサービスの非同期メッセージングの実装」（**丸山不二夫**）は“グリッドとSOAからみるWebサービス標準技術”のシリーズ．「メッセージの向きはどう決まるか」というコラムが面白かった．

「COINSにおける並列化」（**渡邊坦**他）は“21世紀のコンパイラ道しるべ”のシリーズ最終回．いろいろな側面を紹介してきた最後として，並列実行機構への対応を示している．

「21世紀社会におけるITの役割」（**前田章**）は連載“これからの情報処理学会”の一話．「ローエンド破壊型もしくは無消費への対抗」といった難しい語句が並ぶ．

「OSSはどこまで使えるのか？」（**鈴木友峰**）は“オープンソース事情”のシリーズ．今回はOSSのミドルウェアとしてのDBMSの性能の話．チューニングが重要なのだそうだ．

「ゲーム情報学とゲーム情報学研究会」（**金子知適**）と「エンタテインメントコンピューティング研究会」（**星野准一**）は連載“研究会千夜一夜”のシリーズ．期せずして楽しい研究会の組合せとなった．

「思い出に残る国際会議」（**吉岡稔弘**）は連載“標準化よもやま話”の1つ．9.11直前の大阪での会議の後日談と，大量のコメントの「うまい」さばき方の話．（*Kuwm*）

会誌編集委員会
編 集 長
川合　慧
担当理事
石田　亨
長谷川　亨
本号エディタ
天野　真家
大谷　真
片山　博
兼宗　進
河野　泰人
木戸　彰夫
久門　耕一
坂井　修一
白木　善尚
鈴木　貢
田中　哲朗
田中　穂積
土井美和子
比屋根一雄
前田　英作
間瀬　久雄
三浦健次郎
室岡　孝宏
安信千津子

編集スタッフ
後路　啓子
町田　善江
綿谷　亜樹

■ 47巻12号掲載広告目次（五十音順）

インタフェース…… 表2対向
オーム社…… 前付3
サイエンス社…… 目次前，前付最終
情報処理学会短期集中セミナ…… 表2
ソフト・リサーチ・センター…… 前付2上

＊掲載広告のカタログ・資料をご希望の方は，お名前，電話番号，勤務先または学校名を明記の上，E-mail または Fax にてご請求ください．

広告総代理店　（株）精機通信社
E-mail:sei@ss-com.co.jp
Fax(03)3368-1519

Copyright 2006 IPSJ
本誌に出てくる製品名等は，各社の商標または登録商標です．