（独）科学技術振興機構
創造科学技術推進事業
追跡評価用資料

ERATO
今井量子計算機構プロジェクト
(2000-2005 年度)

2011 年 10 月 19 日

目次

要旨

1. プロジェクトの概要

(1)体制・マネジメント

ERATO 今井量子計算機構プロジェクトは2000年10月から2005年9月までの5年間にわたり実施された。コンピュータとして量子計算が機能し、理論だけではなく工学として展開するためには、量子計算論に基づくソフトウェアを開発し、多岐に渡るシミュレーションを可能にし、誤り訂正機能を含む量子回路のデコヒーレンスのシミュレーションを通じて、新量子計算機構のデバイスに関する柔軟性を検証することが求められていた。そこで、プロジェクトでは 1)量子コンピューティンググループ、2)量子回路プログラミンググループ、3)量子情報グループの３つの研究グループを設置し、相互に連携しながら研究が展開された。

１）量子コンピューティンググループ

場所：東京オフィス

総括責任者：　　今井　浩（東京大学大学院情報理工学系研究科　教授）

技術参事：　　林　正人（※当時）

グループリーダー：松本啓史（国立情報学研究所　助教授）

２）量子回路プログラミンググループ

場所：京都オフィス

グループリーダー：岩間一雄（京都大学大学院情報学研究科　教授）

３）量子情報グループ

場所：筑波オフィス

グループリーダー：富田章久（日本電気株式会社量子情報テクノロジーグループ主任研究員※当時）

プロジェクトでは量子計算、量子情報から光を用いた量子情報実験までをカバーする包括的な研究内容であったため、研究グループ間の相互作用を重視して３つの拠点の研究交流を積極的に実施していた。

プロジェクト中期以降は、現実社会にプロトタイプシステムとして提供できるものを成果として開発するという研究目的を研究グループで共有し、研究方向の舵取りが行われた。具体的には量子暗号の実験的実現、理論的発展のどこかに参画研究者の研究テーマが貢献するように舵が切られた。その結果、理論的研究成果にとどまらず、長距離（150 km）単光子通信における世界記録の達成や、電柱間に配線された商用光ファイバーによる通信のデモンストレーションなど、量子暗号通信の実用的な展望までを示すことに成功した。

(2)成果

プロジェクトにおける画期的な研究の成果には以下のようなものが挙げられる。

《量子計算分野》

- リーダー選挙問題に対する量子アルゴリズムの開発

  ネットワーク接続された計算機同士が、通信とローカルな計算を行うことにより中心となる計算機（リーダー）を自律的に決定する問題に対応できる量子系アルゴリズムを開発した。古典系よりも量子計算が高速であることも厳密に証明した。

- 量子対話型証明系の研究

  量子系と古典系とで通信容量にどのような違いがあるかを明らかにする基礎理論を構築した。

- 量子ゼロ知識証明の研究

  認証システムや電子投票において、ユーザーの情報が漏洩しないことが保証されている量子系プロトコル創出のための研究で進展があった。

《量子情報分野》

- 量子鍵配送の研究

  量子鍵配送の実用性を向上するために、量子誤り訂正符号などの実用的なプロトコルを開発した。

- 量子エンタングルメントの研究

  量子的プロトコルの要となる現象の理解を深めるために、量子エンタングルメントに関する基礎研究を実施した。

- 量子系での統計的推測の研究

  量子状態を壊さずに測定する手法を開発した。これにより、量子コンピュータでも必須となるデータ圧縮の理論を提案した。

《システム開発･実装》

- 量子フーリエ変換

  量子ビットの代わりになる特殊な回路を作成し、素因数分解アルゴリズムの「量子フーリエ変換」についての実証実験を行った。結果、世界で初めて 1024 量子ビットの量子フーリエ変換の実験に成功した。

- 通信波長帯における高感度光子検出器

  光子受信の際の誤検出の原因となるノイズを抑圧する回路を考案し、感度が従来より 50 倍向上した光子検出器を開発した。

- 100km を超える長距離量子暗号伝送

  開発した光子検出器を用いて 150km の光ファイバを通した単一光子の伝送に成功した（NEC との共同研究)。これは世界で初めての FAX などの通信量に対応できる実用的な量子暗号システムである。

また、本プロジェクトでは量子情報科学のアジアにおける研究交流拠点を構築するため

に、EQIS（ERATO conference series on Quantum Information Science）を開催した。EQIS では毎年優れた研究者を招待講演者として招聘した。同時に、一般投稿論文も受け付け、強力なプログラム委員会を組織し、厳絡な査読を行なった。結果、同分野における海外での認知度も高まり、プロジェクト終了後はAQIS: Asian conference series on Quantum Information Science として引き継がれることになった。

2. プロジェクト終了から現在に至る状況

（1）各研究テーマの現在の状況

本プロジェクトの量子計算、量子情報に関する理論的研究は主に SORST 量子計算アーキテクチャーに引き継がれ、参画研究者の各研究室での研究テーマとして発展している。また、システム開発・実装面での研究テーマは SORST での量子暗号鍵配送（QKD）システムの開発を経て、より実用的な企業研究の場に移っている。

本プロジェクトの終了後に顕著な成果を上げている研究テーマは次のようなものがある。

《量子計算分野》

- 量子分散計算アルゴリズムの改良
- 量子誤り訂正符号のリスト復号
- ネットワークコーディングに関する研究

《量子情報分野》

- デコイ法による量子鍵配送システムの開発
- ユニバーサル符号

《システム開発・実装》

- 量子暗号鍵配送システムの実証実験
- 高速 QKD 装置の開発
- 量子リーダー選挙プロトコルの実証

（2）プロジェクトメンバーの動静

本プロジェクトでは、それまで個々の研究室レベルで実施されていた量子計算、量子情報、デバイス開発の研究を理論から実証まで包括的に展開したことで、同分野の実用化までを視野に入れた多くの研究者を育てることに成功した。

量子情報分野の次代のリーダーたる人材としては、松本啓史 NII（国立情報学研究所）准教授、林正人 東北大学准教授を輩出し、量子計算の分野では山下茂 立命館大学教授、浜田充玉川大学准教授を輩出している。また、若手研究者としては小林弘忠 NII 研究員、山上智幸 JST 研究員（※SORST から雇用契約）らが世界に通用する研究者として育っている。Xiang-Bin Wang 氏を始めとする海外からの参加研究者も ERATO での実績を評価されて国内外の研究機関でポストを得て活躍している。

3. プロジェクト成果の波及と展望

(1)科学技術への波及と展望

本プロジェクトの終了後、参加していた研究者は様々な公的資金を獲得し、量子計算、量子情報の分野で最先端の研究開発を展開している。以下では参画研究者が代表を務める研究プロジェクトを列挙する。

- 科学技術振興機構 SORST「量子情報システムアーキテクチャ」
- 科学技術振興機構戦略的国際科学技術協力推進事業「次世代情報セキュリティシステムの設計と解析」
- NICT（情報通信機構）委託研究「量子暗号の実用化のための研究開発」
- 科研費基礎研究(B)「量子情報組合せ論に基づく最適化とその量子情報科学基礎拡張の研究」
- 科研費特定領域研究「複雑な系の量子統計推測と量子相関の研究」
- 科研費若手研究(B)「量子情報時代の新暗号基礎」
- 科研費若手研究(A)「多端子量子通信ネットワークの理論的解析」
- 科研費基礎研究(C)「量子論に基づく符号理論の新展開と情報セキュリティへの応用」
- 科研費若手研究(B)「分散環境における量子計算能力のネットワーク形状に着目した解析」
- 科研費特定領域研究「現実的な状況下での量子計算の能力に関する研究」
- 科研費若手研究 B「エラー訂正を考慮した効率の良い量子回路設計手法に関する研究」
- 科研費基礎研究(B)「量子情報理論と量子計算量理論の融合とその応用」
- 科学技術振興機構さきがけ「量子と情報」「代数的量子情報処理技術の研究」
- 科学技術振興調整費先端融合領域イノベーション創出拠点プログラム「ナノ量子情報エレクトロニクス連携研究拠点」

また、本プロジェクトで開催した国際会議の後継シリーズとして AQIS（Asian conference on Quantum Information Science)が毎年アジア各国で開催され、アジアにおける量子コンピューティングの研究プラットフォームとして展開されている。このような活動と関連して、SODA（Symposium on Discrete Algorithms）が 2012 年に京都で開催することが決定し、岩間 GL が実行委員長を務めることとなっている。量子計算、量子情報研究においてわが国が国際的に一定の地位を占めていることに大きく貢献している。

受賞面では、ERATO プロジェクトの成果が受賞に結びついたものとして、林正人東北大学准教授に授与された第 24 回日本 IBM 科学賞（2010 年 11 月）が挙げられる。

- 第 24 回日本 IBM 科学賞

  林正人　東北大学大学院情報科学研究科准教授

  受賞理由

  「量子情報におけるユニバーサルプロトコル理論の構築と量子暗号への応用」

（2）社会・経済への波及と展望

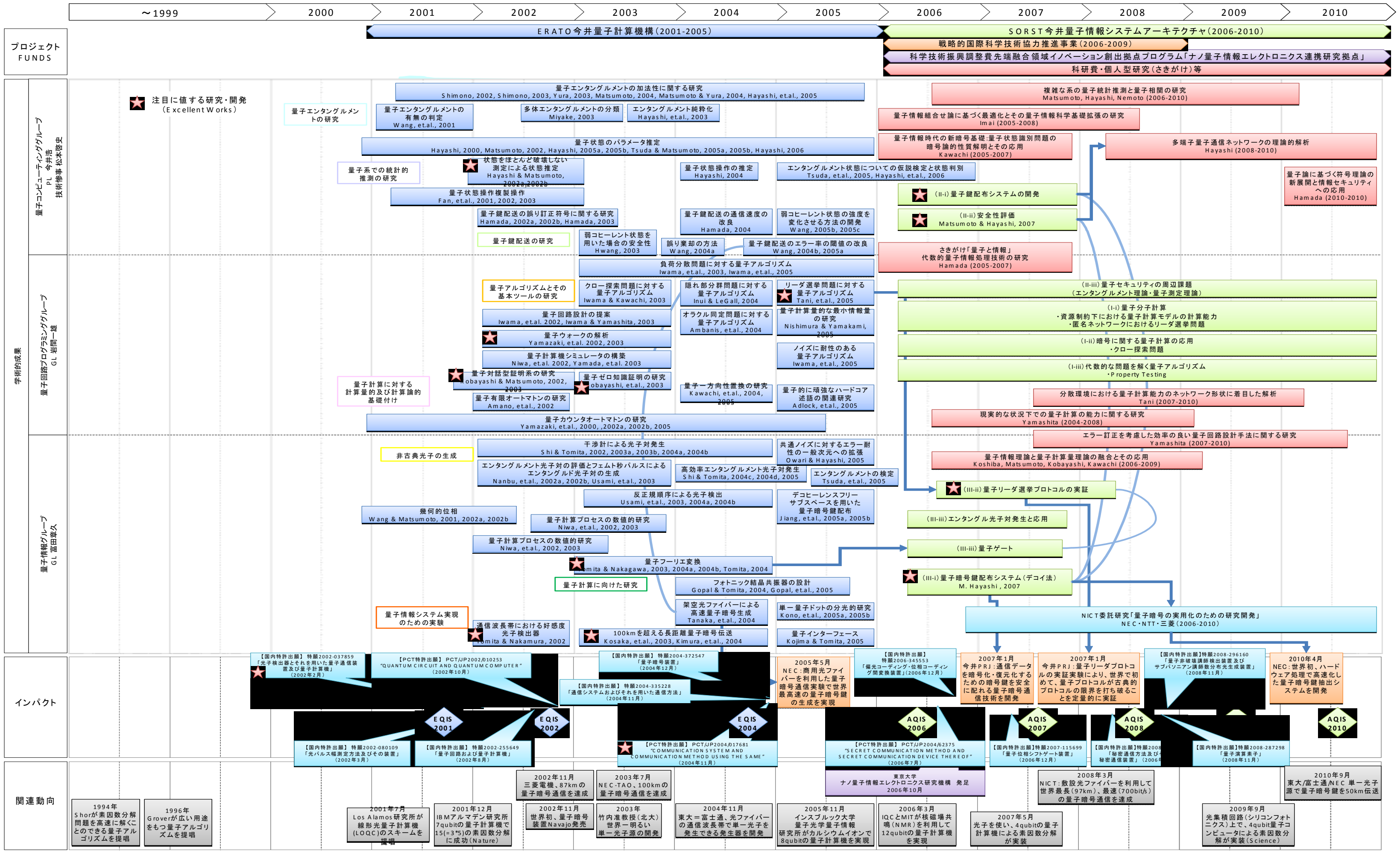
現在、国内における量子通信関連の大規模プロジェクトの代表的存在は NICT（情報通信機構）委託研究プロジェクトと SORST プロジェクトとなっている。NICT プロジェクトは富田彰久 北海道大学教授の参画を通じて、NEC においてハードウェア（高速デバイス）とシステム（鍵抽出処理）の開発が行われている。主に実験・実装を行う NICT プロジェクトと理論を構築する SORST プロジェクトとの相互のフィードバックは両プロジェクトに好影響を与え、東京 QKD ネットワークなどの先進的な試みへとつながている。

QKD システムは技術的にはほぼ実用段階まで来ており、ERATO プロジェクトで培った安全性評価に裏付けられた QKD システムが我が国の技術的な強みとなっている。量子通信の企画化、国際標準化においてもこの技術を拠り所に日本が主導的な役割を果たすことが期待されており、これに向けた活動も活発化している。特に ERATO 発の技術であるデコイ法は実質的な世界標準になりつつある（p23 参照）。

量子暗号通信の実用化に対するニーズとコストについては、以下のような点が課題となっている。

- 暗号は保険であり、保険にどれだけコストを掛けるべきかが問題。
- 現在の開発コストは量子通信暗号装置1セットで約 1000 万円。これをニーズに応じてどの程度まで下げられるかが普及のポイント。
- 装置やシステム自体もまだまだニーズと性能のマッチングができていない。例えば 50km の伝送距離で 1Mb/sec.という性能では、動画のオンデマンド送信には使用できない。今後はユーザーの参加を得て、ユーザー側からのスペックや暗号鍵の応用について検討することが重要となるだろう。
- 量子通信のニーズや経済効果については、未だ不明な点が多いが、今後のニーズを喚起するためにも、はじめは政府などの公的機関が利用することが望ましい。
- 低コストで導入するためには既存のネットワークインフラを利用すること考えられるが、その際にノイズ対策などの技術開発が不可欠。
    ① 通常の光通信からの混信を防止する必要がある。そのためのローパワーでのデータ伝送。
    ② 上記のローパワー化に加えての多重化・大容量化（量子エンタングルメントが重要な要素となる）。
    ③ さらに実用的な暗号化技術（本プロジェクトの大きな成果の一つである量子暗号技術に基づく）の実現。

上記の課題に加え、量子中継技術や量子状態を記憶するための方法に関する技術開発を進めるためには基礎研究に戻ることが重要になる。わが国が量子通信分野で主導的な地位にとどまるためには今後も公的研究資金による長期的な研究支援が必要とされる。


～1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
プロジェクト
FUNDS
ERATO今井量子計算機構(2001-2005)
SORST今井量子情報システムアーキテクチャ(2006-2010)
戦略的国際科学技術協力推進事業(2006-2009)
科学技術振興調整費先端融合領域イノベーション創出拠点プログラム「ナノ量子情報エレクトロニクス連携研究拠点」
科研費・個人型研究(さきがけ)等
学術的成果
量子コンピューティンググループ PL 今井浩 技術参事 松本啓史
量子回路プログラミンググループ GL 岩間一雄
量子情報グループ GL 富田章久
注目に値する研究・開発 (Excellent Works)
量子エンタングルメントの加法性に関する研究
Shimono, 2002, Shimono, 2003, Yura, 2003, Matsumoto, 2004, Matsumoto & Yura, 2004, Hayashi, et.al., 2005
量子エンタングルメントの研究
量子エンタングルメントの有無の判定 Wang, et.al., 2001
多体エンタングルメントの分類 Miyake, 2003
エンタングルメント純粋化 Hayashi, et.al., 2003
量子状態のパラメータ推定
Hayashi, 2000, Matsumoto, 2002, Hayashi, 2005a, 2005b, Tsuda & Matsumoto, 2005a, 2005b, Hayashi, 2006
量子系での統計的推測の研究
状態をほとんど破壊しない測定による状態推定 Hayashi & Matsumoto, 2002a, 2002b
量子状態操作の推定 Hayashi, 2004
エンタングルメント状態についての仮説検定と状態判別 Tsuda, et.al., 2005, Hayashi, et.al., 2006
量子状態操作複製操作 Fan, et.al., 2001, 2002, 2003
量子鍵配送の誤り訂正符号に関する研究 Hamada, 2002a, 2002b, Hamada, 2003
量子鍵配送の研究
弱コヒーレント状態を用いた場合の安全性 Hwang, 2003
量子鍵配送の通信速度の改良 Hamada, 2004
弱コヒーレント状態の強度を変化させる方法の開発 Wang, 2005b, 2005c
誤り棄却の方法 Wang, 2004a
量子鍵配送のエラー率の閾値の改良 Wang, 2004b, 2005a
複雑な系の量子統計推測と量子相関の研究 Matsumoto, Hayashi, Nemoto (2006-2010)
量子情報組合せ論に基づく最適化とその量子情報科学基礎拡張の研究 Imai (2005-2008)
量子情報時代の新暗号基礎:量子状態識別問題の暗号論的性質解明とその応用 Kawachi (2005-2007)
多端子量子通信ネットワークの理論的解析 Hayashi (2008-2010)
量子論に基づく符号理論の新展開と情報セキュリティへの応用 Hamada (2010-2010)
(II-i) 量子鍵配布システムの開発
(II-ii) 安全性評価 Matsumoto & Hayashi, 2007
さきがけ「量子と情報」代数的量子情報処理技術の研究 Hamada (2005-2007)
負荷分散問題に対する量子アルゴリズム Iwama, et.al., 2003, Iwama, et.al., 2005
量子アルゴリズムとその基本ツールの研究
クロー探索問題に対する量子アルゴリズム Iwama & Kawachi, 2003
隠れ部分群問題に対する量子アルゴリズム Inui & LeGall, 2004
リーダ選挙問題に対する量子アルゴリズム Tani, et.al., 2005
量子回路設計の提案 Iwama, et.al. 2002, Iwama & Yamashita, 2003
オラクル同定問題に対する量子アルゴリズム Ambainis, et.al., 2004
量子計算量学的な最小情報量の研究 Nishimura & Yamakami, 2005
量子ウォークの解析 Yamazaki, et.al. 2002, 2003
ノイズに耐性のある量子アルゴリズム Iwama, et.al., 2005
量子計算機シミュレータの構築 Niwa, et.al. 2002, Yamada, et.al. 2003
量子計算に対する計算量的及び計算的基礎付け
量子対話型証明系の研究 Kobayashi & Matsumoto, 2002, 2003
量子ゼロ知識証明の研究 Kobayashi, et.al., 2003
量子一方向性置換の研究 Kawachi, et.al., 2004, 2005
量子的に暗強なハードコア述語の関連研究 Adlock, et.al., 2005
量子有限オートマトンの研究 Amano, et.al., 2002
量子カウンタオートマトンの研究 Yamazaki, et.al., 2000, 2002a, 2002b, 2005
(II-iii) 量子セキュリティの周辺課題 (エンタングルメント理論・量子測定理論)
(I-i) 量子分子計算 ・資源制約下における量子計算モデルの計算能力 ・匿名ネットワークにおけるリーダ選挙問題
(I-ii) 暗号に関する量子計算の応用 ・クロー探索問題
(I-iii) 代数的な問題を解く量子アルゴリズム ・Property Testing
分散環境における量子計算能力のネットワーク形状に着目した解析 Tani (2007-2010)
現実的な状況下での量子計算の能力に関する研究 Yamashita (2004-2008)
エラー訂正を考慮した効率の良い量子回路設計手法に関する研究 Yamashita (2007-2010)
量子情報科学と量子計算量理論の融合とその応用 Koshiba, Matsumoto, Kobayashi, Kawachi (2006-2009)
非古典光子の生成
干渉計による光子対発生 Shi & Tomita, 2002, 2003a, 2003b, 2004a, 2004b
共通ノイズに対するエラー耐性の一般化光子への拡張 Owari & Hayashi, 2005
エンタングルメント光子対の評価とフェムト秒パルスによるエンタングルド光子対の生成 Nanbu, et.al., 2002a, 2002b, Usami, et.al., 2003
高効率エンタングルメント光子対発生 Shi & Tomita, 2004c, 2004d, 2005
エンタングルメントの検定 Tsuda, et.al., 2005
(III-ii) 量子リーダ選挙プロトコルの実証
反正規順序による光子検出 Usami, et.al., 2003, 2004a, 2004b
デコヒーレンスフリーサブスペースを用いた量子暗号鍵配布 Jiang, et.al., 2005a, 2005b
幾何的位相 Wang & Matsumoto, 2001, 2002a, 2002b
量子計算プロセスの数値的研究 Niwa, et.al., 2002, 2003
(III-iii) エンタングル光子対発生とその応用
量子計算プロセスの数値的研究 Niwa, et.al., 2002, 2003
(III-iii) 量子ゲート
量子フーリエ変換 Tomita & Nakagawa, 2003, 2004a, 2004b, Tomita, 2004
量子計算に向けた研究
(III-i) 量子暗号鍵配布システム (デコイ法) M. Hayashi, 2007
フォトニック結晶共振器の設計 Gopal & Tomita, 2004, Gopal, et.al., 2005
量子情報システム実現のための実験
架空光ファイバーによる高速量子暗号生成 Tanaka, et.al., 2004
単一量子ドットの分光的研究 Kono, et.al., 2005a, 2005b
NICT委託研究「量子暗号の実用化のための研究開発」 NEC・NTT・三菱 (2006-2010)
通信波長帯における低雑音光子検出器 Tomita & Nakamura, 2002
100kmを超える長距離量子暗号伝送 Kosaka, et.al., 2003, Kimura, et.al., 2004
量子インターフェース Kojima & Tomita, 2005
インパクト
EQIS 2001
EQIS 2002
EQIS 2004
AQIS 2006
AQIS 2007
AQIS 2008
AQIS 2010
2005年5月 NEC:商用光ファイバーを利用した量子暗号通信実験で世界最高速の量子暗号鍵の生成を実現
2007年1月 今井PRJ:通信データを暗号化・復元化するための暗号鍵を安全に配れる量子暗号通信技術を開発
2007年1月 今井PRJ:量子リーダプロトコルの実証実験により、世界で初めて、量子プロトコルが古典的プロトコルの限界を打ち破ることを定量的に実証
2010年4月 NEC:世界初、ハードウェア処理で高速化した量子暗号鍵抽出システムを開発
東京大学 ナノ量子情報エレクトロニクス研究機構 発足 2006年10月
関連動向
1994年 Shorが素因数分解問題を高速に解くことのできる量子アルゴリズムを提唱
1996年 Groverが広い用途をもつ量子アルゴリズムを提唱
2001年7月 Los Alamos研究所が線形光量子計算機(LOQC)のスキームを提唱
2001年12月 IBMアルマデン研究所7qubitの量子計算機で15(=3*5)の素因数分解に成功(Nature)
2002年11月 三菱電機、87kmの量子暗号通信を達成
2002年11月 世界初、量子暗号装置Navajo発売
2003年7月 NEC-TAO、100kmの量子暗号通信を達成
2003年 竹内准教授(北大)世界一明るい単一光子源の開発
2004年11月 東大＝富士通、光ファイバーの通信波長帯で単一光子を発生できる発生器を開発
2005年11月 インスブルック大学量子光学量子情報研究所がカルシウムイオンで8qubitの量子計算機を実現
2006年3月 IQCとMITが核磁場共鳴(NMR)を利用して12qubitの量子計算機を実現
2007年5月 光子を使い、4qubitの量子計算機による素因数分解が実装
2008年3月 NICT:敷設光ファイバーを利用して世界最長(97km)、最速(700bit/s)の量子暗号通信を達成
2009年9月 光集積回路(シリコンフォトニクス)上で、4qubit量子コンピュータによる素因数分解が実装(Science)
2010年9月 東大/富士通/NEC 単一光子源で量子暗号鍵を50km伝送

第 1 章　プロジェクトの概要

1-1　ERATO プロジェクトの背景

20 世紀中頃に発明されたコンピュータは、科学技術から社会活動まで世界を一新させた。しかしながら、電子デバイス性能向上による既存計算方式の高速化の限界が見え、21 世紀を支える全く新しい計算原理が待ち望まれていた。既存の古典力学計算を離れ、量子力学原理のコヒーレンスのよい状態を量子遷移させて計算する量子コンピュータがまさしくその壁を破る新方式として注目されていた。

量子コンピュータの研究は情報・物理にまたがる新学際研究分野であり、新量子デバイス技術開発と量子計算の新機構を両輪として初めて量子コンピュータが実現できる。1994 年に Shor が素因数分解アルゴリズムを考案し、量子コンピュータの実現が現在のインターネットセキュリティを支える公開鍵暗号の安全性の崩壊をもたらすことを示した。1996 年には Grover が非ソートデータの検索アルゴリズムを考案し、NP（Nondeterministic Polynominal time）完全（多項式時間限定変換によって還元可能）などの問題が指数の平方根時間で解けることを示した。この二人のアルゴリズムが量子コンピュータの有用性を世界に知らしめ、多くのコンピュータ・サイエンスの研究者が量子情報分野に入っていくことになった。一方、インターネットにおける古典暗号通信に取って代わる次世代方式として量子暗号通信が提唱され始めており、1990 年代後半には量子テレポテーションなどに関する実験が研究室レベルで開始されていた。

ERATO 今井量子計算機構プロジェクト以前の量子計算に関する研究は、量子の重ね合せ状態についてコヒーレンスを保ちながら量子回路記述に従って超並列的に量子状態遷移させていくものであった。しかし、物理的にコヒーレンスを追及するのみでは真の実用的な量子計算システムは実現できず、一連の人為的操作である計算プロセスの中で、デコヒーレンスなど各種誤りの下でも正しく計算できる制御機構が必要不可欠であった。

こうした背景を下に、ERATO 今井量子計算機構プロジェクト（以下、本プロジェクト）は立ち上げられた。2000 年当時、日本国内の量子計算、量子情報に関する研究は個人レベルの研究が主流であり、研究者の緩やかな連携の下に研究が行われていた。ERATO 今井量子計算機構プロジェクトは、国の研究開発プロジェクトとしてこの分野に大型の予算が投じられ、理論からデバイス開発まで産学官の研究グループが参加し、拠点展開された初の試みであった。

1-2　ERATO 今井量子計算機構プロジェクトの概要

本プロジェクトは 2000 年 10 月から 2005 年 9 月までの 5 年間にわたり実施された。コンピュータとして量子計算が機能し、理論だけではなく工学として展開するためには、量

子計算論に基づくソフトウェアを開発し、多岐に渡るシミュレーションを可能にし、誤り訂正機能を含む量子回路のデコヒーレンスのシミュレーションを通じて、新量子計算機構のデバイスに関する柔軟性を検証することが求められていた。そこで、本プロジェクトでは1)量子コンピューティンググループ、2)量子回路プログラミンググループ、3)量子情報グループの３つの研究グループを設置し、相互に連携しながら研究が展開された。それぞれの研究グループの研究テーマはまとめ図に示したとおりである。

（１）研究構想

プロジェクト開始段階での研究構想は以下のとおりである[1]。

１）量子コンピューティング

コヒーレントな量子重ね合せ状態を計算での表現方式とし、重ね合せ状態のもつ超並列計算性に立脚する量子計算の本質を明らかにする。量子ビットのなす状態空間の幾何構造上での量子情報・アルゴリズム理論を展開して、情報計算幾何構造を用いた研究を進める。これにより量子計算によってのみ可能になる計算パワーを解き明かす。規則的構造を活用した既存量子計算方式の限界を打破することを目指して、不規則構造も扱える計算機構として混合状態など未開拓な量子力学の種々の操作を計算単位として確立し、量子観測についても量子ビットの統計的処理の操作に着目して、量子力学操作の多面さを生かした全く新しい量子計算機構を構築する。

２）量子回路プログラミング

量子計算が理論研究の段階から工学的に実現可能な段階に昇華するためには、量子コンピュータができる以前から量子計算が検討できることが必須で、クラスタ計算を用いたシミュレーションシステムを構築する。また、デコヒーレンスによる誤りを計算機構として克服する新しい誤り訂正方式の研究を推進し、デコヒーレンスも含めた量子回路シミュレーションを通して最適量子回路設計を目指す。これは、量子コンピュータにおけるプログラミング研究というべき未到達の分野であり、量子計算機構の工学に取り組む。

３）量子コミュニケーション

計算量仮定に基づく古典的に安全なコミュニケーションにとって代わる、量子力学原理に基づいた完全に安全な量子コミュニケーション方式の確立を目指すため、量子暗号プロトコルを設計して新通信機構を構築し、量子テレポーテーションを量子中継として、長距離で安全な量子暗号の実験検証も行う。量子情報理論を量子情報計算幾何の側面からも深化させ、通信としての量子誤り訂正も含めそれらを量子コンピューティングへフィードバックさせてコンピューティングとコミュニケーションの有機的結合を実現する。

[1] http://www.jst.go.jp/pr/report/report135/kousou1.html

（２）研究拠点

３つの研究グループは東京オフィス、京都オフィス、筑波オフィスの３拠点で推進された。各拠点の情報は以下のとおりである。

東京オフィス（量子コンピューティング・グループ）

〒113-0033

東京都文京区本郷５丁目２８番３号　第二本郷ホワイトビル３階

◇総括責任者　今井　浩（東京大学大学院情報理工学系研究科　教授）

◇技術参事　林　正人

◇グループリーダー　松本　啓史（国立情報学研究所　量子コンピューティング研究部門　助教授）

京都オフィス（量子回路プログラミング・グループ）

〒602-0873

京都府京都市上京区河原町通丸太町下ル伊勢屋町 406　マツヲビル２階

◇グループリーダー　岩間　一雄（京都大学大学院情報学研究科　教授）

筑波オフィス（量子情報・グループ）

〒305-8501

茨城県つくば市御幸が丘３４　日本電気株式会社筑波研究所内　BI 棟 322B 室

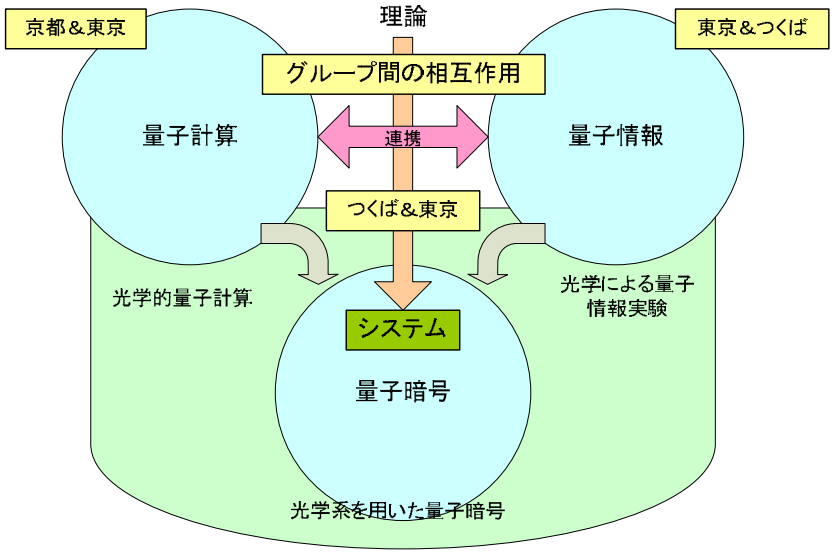
◇グループリーダー　富田　章久（日本電気株式会社量子情報テクノロジーグループ主任研究員　※当時）

（３）プロジェクトのマネジメント

本プロジェクトでは量子計算、量子情報から光を用いた量子情報実験までをカバーする包括的な研究内容であったため、研究グループ間の相互作用を重視して３つの拠点の研究交流を積極的に実施していた。

本プロジェクト開始当初は参加している研究者のバックグラウンドが異なっており、研究用語さえ互いに通じないほどの研究領域の広さを持ってスタートしたため、それぞれの研究拠点の研究者が集う研究会を集中的に開催した。

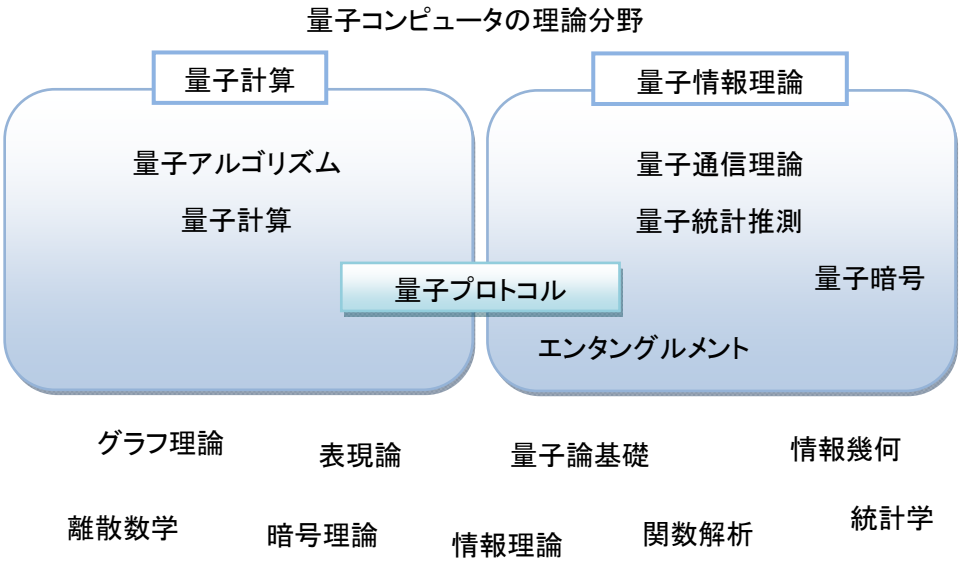
本プロジェクト中期以降は、現実社会にプロトタイプシステムとして提供できるものを成果として開発するという研究目的を研究グループで共有し、研究方向の舵取りが行われた。具体的には量子暗号の実験的実現、理論的発展のどこかに参画研究者の研究テーマが貢献するように舵が切られた（図２）。その結果、理論的研究成果にとどまらず、長距離（150 km）単光子通信における世界記録の達成や、電柱間に配線された商用光ファイバーによる通信のデモンストレーションなど、量子暗号通信の実用的な展望までを示すことに成功した。



出所）:「今井量子計算機構プロジェクト」終了報告書

図 2　プロジェクトの研究戦略

ここで、言葉の定義が難しいため、量子コンピュータの理論分野における現在の視点からの整理を図示しておく（図３）。



出所）：林正人 http://www.quest.is.uec.ac.jp/q-school/2010/archive/量子情報科学概論.pdf より作成

図 3　量子コンピュータの理論分野

それぞれの理論分野は密接に連携しており、プロジェクトにおける研究テーマの類型化についても実質的には困難であるが、ERATO プロジェクトでは量子計算分野を主に岩間グ

ループ（京都）が担い、量子情報理論に関しては主に松本グループ、林技術参事（東京）が担い、量子暗号の実装に関する分野を主に富田グループ（つくば）が担当している。

（４）主な成果

本プロジェクトにおける主な成果を以下に列挙する。ここでは、研究開発テーマの大きな分類として、量子計算、量子情報、システム開発・実装の三つに区別している。

(ア)量子アルゴリズムとその基本ツールの研究　《量子計算》

量子計算が質問計算量や通信計算量などの様々な尺度において古典計算を凌駕する可能性を探求するために、オラクル同定問題[2]やリーダ選挙問題[3]などのいくつかの重要な問題に対する新しい量子アルゴリズムが開発された。

- オラクル同定問題に対する量子アルゴリズム
- クロー探索問題に対する量子アルゴリズム
- 負荷分散問題に対する量子アルゴリズム
- ノイズに耐性のある量子アルゴリズム
- リーダー選挙問題に対する量子アルゴリズム
- 隠れ部分群問題に対する量子アルゴリズム

特に、「リーダー選挙問題に対する量子アルゴリズム[4]」は量子計算が古典計算と質的に異なることを厳密に示した点で、独創的かつ重要な研究として認知されている。

(イ)量子回路設計の提案　《量子計算》

量子アルゴリズムを開発する上で重要な基本ツールとなる量子回路の設計や量子ウォークの解析に関する研究が以下のテーマで行われた。

- 量子ウオークの解析
- 量子計算機のシミュレータの構築
- 量子的に頑強なハードコア述語の関連研究

この中で「量子ウォークの解析」はランダムウォーク問題を量子コンピュター上で実行するためのアルゴリズム開発に役立つ研究であり、本研究のシミュレーション結果から提起した問題が Ambainis によって理論的に裏付けられるなどの展開があった[5]。

---

[2] オラクル同定問題：与えられたブラックボックス関数（オラクル）に質問を行い、候補関数集合の中のどれがオラクルとして与えられているかを同定する問題。同定に必要な量子質問計算量が重要となる。

[3] ネットワーク接続された計算機同士が、通信とローカルな計算を行うことにより中心となる計算機（リーダ）を自律的に決定するという、分散計算アルゴリズムの重要な問題。

[4] Tani, S; Kobayashi, H; Matsumoto, K, “Exact quantum algorithms for the leader election problem”, *STACS 2005, PROCEEDINGS. LECTURE NOTES IN COMPUTER SCIENCE*, vol.3404, pp.581-592, 2005.

[5] Ambainis, A, “Quantum walk algorithm for element distinctness”, *SIAM J. Comput.* 37 (2007), No. 1, 210–239.

量子鍵配送は、送信者と受信者の間で盗聴不可能な「秘密鍵」を共有する方法であり、**（ウ）量子計算に対する計算量的及び計算論的基礎付け　《量子計算》**

量子コンピュータに適した計算分野を明らかにすることは非常に重要である。プロジェクトでは量子計算が古典計算より高速にできることの可能性とその限界を計算量的に解析し、量子ゼロ知識証明や量子公開鍵暗号をはじめとする計算量的暗号への応用研究を行った。具体的な項目を以下に示す。

- 量子対話型証明系の研究
- 量子ゼロ知識証明の研究
- 量子一方向性置換の研究
- 量子公開鍵暗号の提案
- 量子計算量的な最小情報量の研究

特に、「量子対話型証明系の研究」は本プロジェクトオリジナルの業績であり、量子系と古典系とで通信容量にどのような違いがあるかを明らかにする基礎理論となっている[6]。また、「量子ゼロ知識証明の研究」はユーザーの情報を漏らさない認証システムや電子投票などの匿名性が必要とされるプロトコルに応用できる研究であり、非常に最先端の研究として現在評価が高まりつつある[7]。

また、量子計算の特性を明らかにするために、量子有限オートマトンなどの簡素な量子計算モデルにおいてどのような問題が解けるのかに関する計算論的側面からの研究を以下のテーマで行った。

- 量子有限オートマトンの研究
- 量子カウンタオートマトンの研究

テープ線形時間量子 Turing 機械の研究

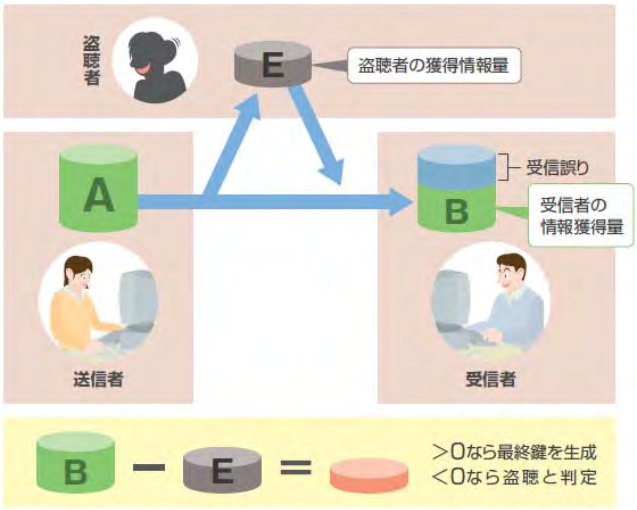
（エ）量子鍵配送の研究　《量子情報》

光子を量子通信路で伝送する。しかしながら、量子伝送には常に受信誤りが含まれており、受信者が得た情報量は全体の情報から受信誤りを差入引いた B になる（図４）。盗聴者が介在した場合、盗聴された情報量 E は操作によって量子状態を変化させ、受信誤りになる。B が E より多ければ最終鍵が生成され、逆に B が E より少ないと盗聴があったと判断され、この通信路での伝送がストップされる。つまり、できるだけ正確に E の量を推定することが理論的な課題となっていた。現実の量子通信路ではノイズが存在しており、盗聴による情報損失か、ノイズによるものなのかを区別することはできない。そこで、ノイズ に対抗し

[6] Iwama, K; Nishimura, H; Raymond, R and Yamashita, S, “Unbounded-Error Classical and Quantum Communication Complexity”, *Lecture Notes in Computer Science*, 4835 (2007), 100-111.

[7] Kobayashi, H “Non-interactive quantum perfect and statistical zero-knowledge”, *ALGORITHMS AND COMPUTATION, PROCEEDINGS. LECTURE NOTES IN COMPUTER SCIENCE*, vol.2906 (2003), 178-188.

て量子状態そのものを保存して伝送する方法として「量子誤り訂正符号」などのプロトコルが考案された。



出所）JST パンフレット「量子情報技術の潮流　量子計算・量子暗号の実現に向けて」

図4　量子鍵配送の仕組み

こうしたプロトコルには効率性の面で改良の余地があり、実用にも問題点が多くあった。「量子鍵配送の研究」では量子鍵配送の実用性を向上するために以下のような研究が展開された。

- 量子鍵配送の誤り訂正符号に関する研究
- 量子鍵配送の通信速度の改良
- 符号の構成
- 弱コヒーレント状態を用いた場合の安全性
- 誤り棄却の方法
- 弱コヒーレント状態の強度を変化させる方法の開発
- 量子鍵配送のエラー率の閾値の改良

（オ）量子エンタングルメントの研究　　《量子情報》

量子エンタングルメント（もつれ合い）はほとんどすべての量子的プロトコルの要となる現象である。例えば、量子暗号では伝送距離の長距離化のためにエンタングルメントを用いた量子中継を必要とする。本プロジェクトでは、プロトコルの研究とは別に、エンタングルメントそのものの理論的研究も以下のように展開された。

- 量子エンタングルメントの加法性に関する研究
- 量子エンタングルメントの有無の判定
- 多体エンタングルメントの分類
- エンタングルメント純粋化

・　共通ノイズに対するエラー耐性の一般次元への拡張

この中で、「量子エンタングルメントの加法性に関する研究」は量子情報の基本的問題である Holevo 容量と EoF(Entanglement of Formation)容量の加法性に一般的な関係があることを世界に先駆けて示した研究である。その後 Shor によってこの研究の概念が参考にされ、Holevo 容量の加法性と EoF の加法性が同値であることが証明された[8]。

(カ)量子系での統計的推測の研究　《量子情報》

量子力学系から情報を獲得するには測定が必要であるが、測定により不可避的に状態は変化してしまうそのため、慎重な測定方法が要求される。本プロジェクトでは量子状態の統計的推測という方法によって状態を壊さずに測定することに成功した。これにより、量子コンピュータでも必須となるデータ圧縮の理論を提案した[9]。具体的な研究テーマは以下のようである。

・　量子状態のパラメータ測定
・　状態をほとんど破壊しない測定による状態推定
・　量子状態複製操作
・　量子状態操作の推定
・　エンタングルド状態についての仮説検定と状態識別

(キ)量子処理の物理的実装　　《量子計算》

本プロジェクトでは量子計算の物理的実装に繋がる以下のような一連の研究項目が展開された。

・　幾何的位相
・　線形光学素子を用いた量子情報処理
・　量子計算プロセスの数値的研究

(ク)非古典光子の生成　《システム開発・実装》

量子力学特有の光の状態であるエンタングル光子対は、光の量子的性質を利用する量子情報通信システム（例えば、量子暗号の長距離化を可能とする量子リレー・量子中継、量子コンピュータ間をつなぐ量子ネットワークなど）を構築するための基本要素とされている。本プロジェクトではまずエンタングル光子対の評価方法を確立し、エンタングルド光子対の生成、エンタングルメント状態の検定などについて以下のような項目を研究した。

---

[8] P.W. Shor, "Equivalence of Additivity Questions in Quantum Information Theory", *Com. Math. Phys.*, 246(3), pp.453-473, (2004).
[9] M. Hayashi and K. Matsumoto, "Quantum universal variable-length cording," Phys. Rev. A 66, 022311, (2002).

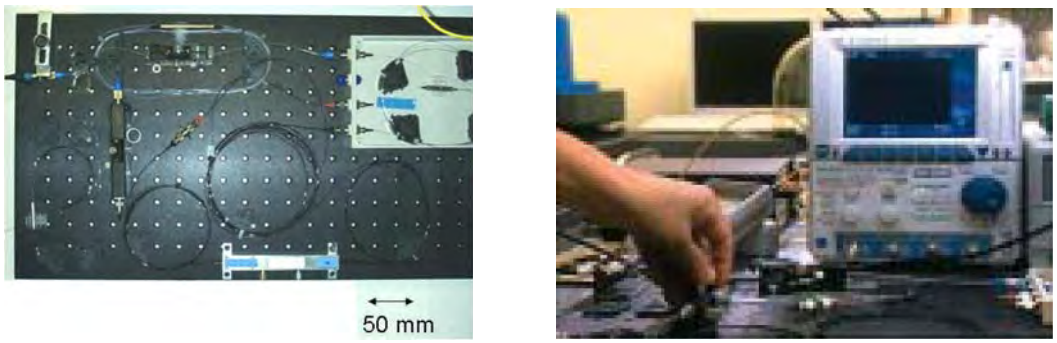
- エンタングルメント光子対の評価とフェムト秒パルスによるエンタングルメント光子対の生成
- 干渉計による光子対発生
- 高効率エンタングルメント光子対発生
- 反正規順序による光子検出
- エンタングルメントの検定
- デコヒーレンスフリーサブスペースを用いた量子暗号鍵配布

(ケ)量子計算に向けた研究　《システム開発・実装》

量子計算に向けて以下のようなシステム開発と実装に関する研究を展開した。

- 量子フーリエ変換
- フォトニック結晶共振器の設計
- 単一量子ドットの分光的研究
- 量子インターフェース

本プロジェクト開始当時、代表的な量子アルゴリズムである Shor の素因数分解アルゴリズムは理論的には証明されていたが、実験的な証明はされていなかった。プロジェクトでは、素因数分解アルゴリズムの「量子フーリエ変換」について、実際に機能するかどうか実証する実験を行った。当時実現していた量子ビットは 7 qubit であり（現在でも 12 qubit)、実用規模ではなかったため、本プロジェクトでは量子ビットの代わりになる特殊な回路を作成し、実証実験を実施した。結果、1024 量子ビットの量子フーリエ変換の実験に成功し、実用的なレベルで量子フーリエ変換が実際に機能することが確かめられた（図５)。



出所)JST パンフレット「量子情報技術の潮流　量子計算・量子暗号の実現に向けて」

図5　量子フーリエ変換回路(左)と実験の様子(右)

(コ)量子情報システム実現のための実験　《システム開発・実装》

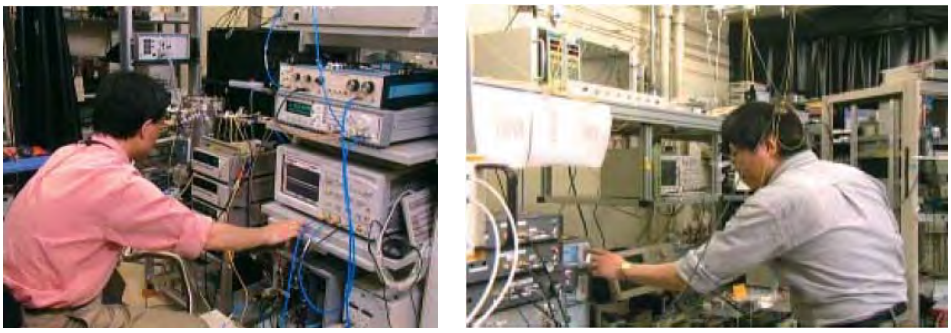
量子情報システム実現のために以下のような機器開発と伝送実験が行われた。

- 通信波長帯における高感度光子検出器

・　100km を超える長距離量子暗号伝送

現在の光通信では１ビット当たり 10 万以上の光子を使っているが、量子暗号では１個の光子で１量子ビットの情報を伝送する。極めて微弱な光信号の中から「光子１個」を検出することになるため、検出効率を高め、かつ、誤って光子を検出する確率を抑えた光子受信器が求められていた。本プロジェクトでは誤検出の原因となる雑音を抑圧する回路を考案し、感度が従来より 50 倍向上した光子検出器を開発した。

また、本プロジェクトでは、開発した光子検出器を用いて 150km の光ファイバを通した単一光子の伝送に成功した（2003 年 NEC との共同研究）。実用的な量子暗号システムには、通信装置の安定動作、高速化、そして通常のオフィス環境で動作することが必要となるが、このような条件で動作する高速量子暗号通信システムを実現し、架空アクセス系光ファイバケーブルを経由した実環境での 14 日間連続の暗号鍵生成に成功した。これは、電話やファックスの暗号化には十分な速度であった（図６）。



出所）JST パンフレット「量子情報技術の潮流　量子計算・量子暗号の実現に向けて」

図6　高感度光子検出器（左）と伝送実験の様子（右）

（５）国際会議 EQIS の開催

本プロジェクトでは 5 年間にわたり国際会議 EQIS:ERATO conference series on Quantum Information Science を関催した。会議の主な目的は、ERATO プロジェクトの成果を国内及び海外に広く知ってもらうと共に、最新の量子情報科学の成果をプロジェクトが把握し、今後の研究に役立てるためであった。同時に、国内の関連する研究者の方々にも、最先端の研究動向に触れる機会を提供することで、日本の量子情報科学の研究水準の向上も目指して開催された。EQIS では毎年優れた研究者を招待講演者として招聘した。同時に、EQIS では一般投稿論文も受け付け、強力なプログラム委員会を組織し、厳絡な査読を行なった。その結果採択率はほぼ 50%となり、一般講演の質は大変高いものとなった。量子情報科学の分野ではそれまでになかったスタイルの国際会議となり、海外での認知度も高まり、本プロジェクト終了後は AQIS: Asian conference series on Quantum Information Science として引き継がれることになった。

表１に終了報告書に記載された EQIS の概要をとりまとめる。

表１　EQIS の概要

<table>
<tr><td colspan="2">ERATO WORKSHOP ON QUANTUM INFORMATION SCIENCE 2001</td></tr>
<tr><td>■主催：JST ERATO 今井量子計算機構プロジェクト
■日程：2001 年 9 月 5－8 日
■場所：東京大学山上会館、弥生ホール
■参加人数：150 名
■講演：口頭発表 37 件
（基調講演 1 件、招待講演 11 件を含む）
ポスター発表 26 件
■基調講演：Charles H. Bennett
(IBM, Yorktown Heights)
■URL：http://www.qci.jst.go.jp/eqis/</td><td>  </td></tr>
<tr><td colspan="2">■概要
EQIS はコンピューターサイエンスと量子物理の間の新しい境界領域である童子情報科学に焦点をあてた会議として始まった。初回の EQIS'01 では特に、計算機科学的な視点に重点が置かれた。</td></tr>
<tr><td colspan="2">ERATO WORKSHOP ON QUANTUM INFORMATION SCIENCE 2002</td></tr>
<tr><td>■主催：JST ERATO 今井量子計算機構プロジェクト
■日程：2002 年 9 月 5－8 日
■場所：東京大学山上会館
■参加人数：160 名
■講演：口頭発表 33 件
（基調講演 1 件、招待講演 11 件を含む）
ポスター発表 41 件
■基調講演：Peter W. Shor (AT & T Labs Research)
■URL：http://www.qci.jst.go.jp/eqis02/</td><td>  </td></tr>
<tr><td colspan="2">■概要
EQIS'02 では量子情報科学の理論的な側面に重点が置かれた。本プロジェクトの初期の重要テーマであるエンタングルメント理論と量子通信理論を繋ぐ研究は初めてこの会議で発表された。また、状態をほとんど壊さない測定によるユニバーサルな量子情報源圧縮も EQIS'02 で初めて発表された。このワークショップの良質な講演を集めた特集号が専門誌"Quantum Information and Computation"から出版された[10]。</td></tr>
<tr><td colspan="2">ERATO CONFERENCE ON QUANTUM INFORMATION SCIENCE 2003</td></tr>
<tr><td>■主催：JST ERATO 今井量子計算機構プロジェクト
■日程：2003 年 9 月 4－6 日
■場所：同志社大学新島会館
■参加人数：190 名
■講演：口頭発表 40 件
（基調講演 1 件、招待講演 10 件を含む）
ポスター発表 42 件
■基調講演：Yoshihisa Yamamoto (Stanford Univ.)
■URL：http://www.qci.jst.go.jp/eqis03/</td><td>  </td></tr>
</table>

[10] http://www.rintonpress.com/journals/qicabstracts/qicabstracts2-s.html

■概要
EQIS'03 の招待講演と評価の高かった一般投稿論文について、林技術参事が編集委員を務めていた専門誌"International Jouranl of Quantum Information (IJQI)"から特集号を 2 巻にわたって出版することになった（IJQI 2003(1), 2004(2)）[11]。

ERATO CONFERENCE ON QUANTUM INFORMATION SCIENCE 2004

■主催：JST ERATO 今井量子計算機構プロジェクト
■協力：国立情報学研究所（NII）
■日程：2004 年 9 月 1－5 日
■場所：一ツ橋記念講堂
■参加人数：200 名
■講演：口頭発表 48 件
（基調講演 1 件、招待講演 11 件を含む）
ポスター発表 63 件
■基調講演：Richard Jozsa (Univ. Bristol)
■URL：http://www.qci.jst.go.jp/eqis04/

■概要
EQIS'04 は国立情報学研究所の協力下で開催となった。講演内容は理論から実験まで幅広いトピックスを扱った。

ERATO CONFERENCE ON QUANTUM INFORMATION SCIENCE 2005

■主催：JST ERATO 今井量子計算機構プロジェクト
■協力：国立情報学研究所（NII）
■日程：2005 年 8 月 26－30 日
■場所：JST 日本科学未来館
■参加人数：200 名
■講演：口頭発表 50 件
（基調講演 1 件、招待講演 9 件を含む）
ポスター発表 59 件
■基調講演：Richard Jozsa (Univ. Bristol)
■URL：http://www.qci.jst.go.jp/eqis05/

■概要
EQIS'05 は実行委員長に英国ブリストル大学の Richard Josza 教授を迎えて開かれた。

[11] http://www.worldscinet.com/ijqi/01/0104/S02197499030104.html
http://www.worldscinet.com/ijqi/02/0201/S02197499040201.html

第 2 章　プロジェクト終了から現在に至る状況

2-1. 各研究テーマの現在の状況

(1)量子計算

本プロジェクトの量子計算に関わる研究テーマは、「SORST 量子情報アーキテクチャー」プロジェクトとして展開されているものと、京都大学岩間教授グループを中心に展開されているものがある。SORST では、以下のような研究課題が展開された。

①量子分散計算

【資源制約下における量子計算モデルの計算能力の研究】

計算時間だけを考えれば量子計算モデルが古典計算モデルよりも強力であることは知られていたが、メモリや通信資源の制約に関しては量子系が古典系よりも優れているかどうかは未知であった。SORST では世界で初めて小規模量子メモリを持つコンピュータが大規模古典メモリのコンピュータよりも強力である計算例が提示された。

《論文》Buscemi, F., "On the minimum number of unitaries needed to describe a random-unitary channel", *PHYSICS LETTERS A*, Vol.360, No.2, pp.256-258, 2006.

【匿名ネットワークにおけるリーダー選挙問題を解く量子分散アルゴリズムの改良】

多者間の量子プロトコルによる計算方式の研究に貢献するため、E 本プロジェクトにおけるリーダー選挙問題に関する研究[12]をさらに発展させた。改良されたアルゴリズムは線形光学素子によって実装され、2 者間のリーダー選挙を扱う量子プロトコルが実現された。

②暗号に関する量子計算の応用

【量子誤り訂正符号のリスト復号】

通信の際にデータに誤りが生じる可能性があるために、誤り訂正符号が広く使用されているが、誤り率が非常に大きいと復号化が不可能な場合が存在する。その場合、元のデータの候補のいくつかを出力するというリスト復号法が有効であることが古典系アルゴリズムでの研究から明らかになっていた。SORST ではこのリスト復号を効率的に実行する量子アルゴリズムが世界で初めて提案された。また量子暗号理論の基本的な要素になっている様々な量子ハードコア関数も構成された。

《論文》"Complexity-Theoretical Quantum List Decoding and Applications to Quantum Hardcore Functions," Kawachi, A.; Yamakami, T.; 計算理論とアルゴリズムの新展開, 京都大学数理解析研究所, Jan. 30- Feb. 1, 2006.が初出の論文。国際会議レ

[12] S. Tani, H. Kobayashi, and K. Matsumoto, STACS2005; *Lecture Notes in Computer Science* 3404, (2005), p. 581.

ベルでは"Quantum Hardcore Fucntions by Comlexity-Theoretic Quantum List Decoding", ICALP 2006, Lecture Notes in Computer Science, Vol.4052, 2006, pp.216-227 が初出。

【クロー探索問題】

古典的暗号の安全性解析に関する「クロー探索問題」の量子アルゴリズムを開発した。

《論文》Tani, S., "Claw finding algorithms using quantum walk", *THEORETICAL COMPUTER SCIENCE*, vol.410, No.50, pp.5285-5297, 2009.

③代数的な問題を解く量子アルゴリズム

量子計算が古典計算よりも高速であることを証明する問題の多くが、代数系における群の構造を持っているため、量子計算による群判定問題の研究は重要となる。SORST では、対象が可解群という群のクラスの性質を持つかどうかを判定する量子アルゴリズムが提案された。

《論文》Inui, Y; Le Gall, F., "Efficient quantum algorithms for the hidden subgroup problem over semi-direct product groups", *QUANTUM INFORMATION & COMPUTATION*, vol.7, No.40304, pp.559-570, 2007.

また、岩間教授グループでは、本プロジェクトにおける「量子対話型証明系問題」を発展させ、以下のような研究成果を出している。

④量子アルゴリズムを用いた場合と古典アルゴリズムを用いた場合の通信量の比較

《論文》Iwama, K.; Nishimura, H.; Raymond, R.; Yamashita, S., "Unbounded-error one-way classical and quantum communication complexity", *Lecture Notes in Computer Science*, 2007. (Conference Paper).

⑤Network cording に関する研究

《論文》"Quantum Network Coding," Iwama, K.; Hayashi, M.; Nishimura, H.; Putra, R. R. H.; Yamashita, S. The Ninth Workshop on Quantum Information Processing, Paris, France, January 16-20, 2006.

岩間教授グループではコンピュータサイエンスとしての量子計算、量子アルゴリズムを研究しており、計算のリソースが量子を用いることによってどのように変化するかが大きなテーマとなっている。最新の業績では、数学の「偽コイン問題」[13]に関して、量子天秤を用いると古典系での計算よりも 4 乗倍まで高速化が可能になることを示した論文が発表されている[14]。また、⑤Network cording に関する研究はブール演算を用いることにより、より少ない通信容量で多くの情報を伝送できることを証明したオリジナリティの高いテーマである。

[13] 偽コイン問題：天秤を用いて与えられた集合からすべての（質量が異なる）偽コインを見つける問題。
[14] K. Iwama; H. Nishimura; R. Raymond; J. Teruyama, "Quantum Counterfeit Coin Problems", *CoRR abs*/1009.0416, 2010.

この研究成果を量子通信に適用すると、従来に比べて大幅に通信容量を削減できる可能性がある。

（2）量子情報

量子暗号鍵配布の安全性を確立するためには装置開発だけでは不十分であり、誤り訂正、秘匿性増強を伴った情報処理技術と安全性評価が必要となる。SORST プロジェクトでは本プロジェクトにおいて NEC と共同で開発した量子通信装置をベースに誤り訂正、秘匿性増強を伴った量子鍵配送システムの開発を行い、そのシステム上に適用できる安全性評価の研究が展開されている。

①デコイ法による量子鍵配送システムの開発

1984 年に Bennett andBrassard によって提案された BB84 プロトコルによる量子鍵配送は情報理論的安全性を保証するプロトコルとして量子暗号通信の方法として注目されているが、ノイズのない量子通信路を用いた場合での安全性が証明されているだけで実用化するためには多くの問題がある。SORST プロジェクトでは、それまで個別に改良が重ねられてきた量子鍵配送システムの安全性評価に対して、デバイスに実装可能な量子鍵配送システムの開発とその安全性評価を一体に行う方法を開発し、世界で初めて、ノイズ、盗聴、単一光源の不完全性、データ処理の有限性等の現実的状況を計算に入れた数十キロメートルの量子通信に関する安全性を保証した量子暗号通信システムの構築に成功した。

《論文》M. Hayashi, “Upper bounds of eavesdropper’s performances in finite-length code with the decoy method”, *Phys. Rev.*, 2007.

《特許》 M. Hayashi, WO/2008/013008/1/31/2008, “SECRET COMMUNICATION METHOD AND SECRET COMMUNICATION DEVICE THEREOF”.

②ユニバーサル符号

ユニバーサル性とは情報源や通信路の特性（確率分布）を事前に知る必要がない性質のことである。事前の観測が状態の破壊につながる量子系の情報処理ではこの性質は古典系以上に重要であるが、物理量が非可換演算子で表現される量子系に古典系の理論を直接適用することはできない。そのため、量子情報に関するユニバーサル性を備えた情報処理方式（＝量子ユニバーサルプロトコル）は従来ほとんど明らかにされていなかった。SORST プロジェクト以降、林教授（現東北大学）が群の表現論に基づいて情報理論的な解析に適した表現を量子系に導入することにより、古典情報での理論を量子情報へ拡張することに成功した。これにより、データ圧縮、誤り訂正、量子もつれ状態生成など基本的な情報処理に対して量子ユニバーサルプロトコルを統一的に与えることが可能になった。

論文》M. Hayashi, “Universal coading classical-quantum channel”, *Com. Math. Phys.*, 2009.

(3)量子暗号のシステム開発・実装

①量子暗号鍵配送(QKD)システム

SORST プロジェクトでは林教授の理論を基に、有限データ、有限符号長でも最終的に得られる鍵の安全性が定量的に保証できるシステムを開発し、実際に安全性保証付きの最終鍵を生成した。実験では 20km ファイバ伝送後、符号長 100kbits で処理を行い、最終鍵 1 ビットあたりの情報漏洩を 10^{-21} と設定して 600bps で最終鍵が得られた（図 7）。

出所）富田章久教授ご提供資料

図7　量子暗号鍵配送システム

量子暗号鍵配送装置の開発はその後、NICT 委託研究に引き継がれ、NEC ナノエレクトロニクス研究所、NEC システムプラットフォーム研究所で行われており、次のような成果を輩出している。

・QKD 装置の安定動作（14 日間連続動作）

《論文》A. Tajima, A. Tanaka, W. Maeda, S. Takahashi, and A. Tomita, "Practical Quantum Cryptosystem for Metro Area Applications," *IEEE J. Selected Topics in Quantum Electronics* 13(4), pp. 1031-1038 (2007).

・高速 QKD 装置の開発

世界初、ハードウェアで高速化した量子暗号鍵配布システムを開発。

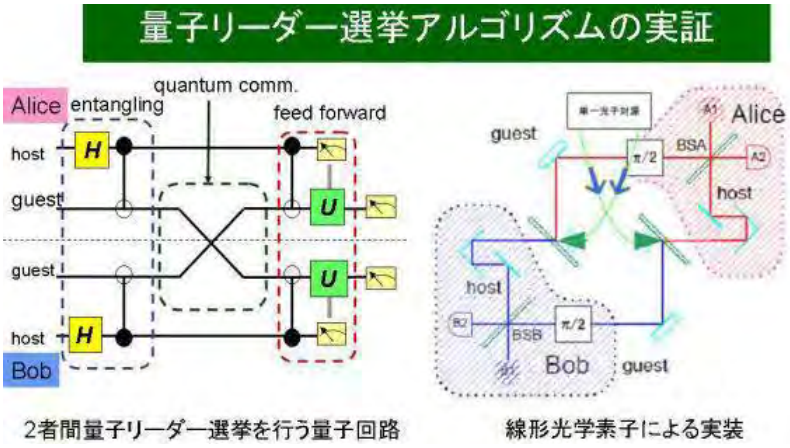
《論文》A. Tomita, K. Yoshino, Y. Nambu, A. Tajima, S. Takahashi, W. Maeda, S. Miki, Z. Wang, M. Fujiwara, and M. Sasaki, "High speed quantum key distribution system," *Optical Fiber Technology* 16 (1), pp. 55-62 (2010).

・量子暗号ネットワーク技術の開発

《論文》W. Maeda, A. Tanaka, S. Takahashi, A. Tajima, and A. Tomita, "Technologies for Quantum Key Distribution Networks Integrated With Optical Communication Networks," *IEEE J. Selected Topics on Quantum Electron.* 15 (6), pp.1591-1601 (2009).

②量子リーダー選挙プロトコルの実証

２者間の量子リーダー選挙を行う量子回路を線形光学素子によって実装することに成功し、通信量の観点から古典アルゴリズムを凌駕することが実証された（図８）。



出所）富田章久教授ご提供資料

図8　量子リーダー選挙アルゴリズムの実証

《論文》Y. Okubo, W.-B. Wang, Y.-K. Jiang, S. Tani, and A. Tomita, *Phys. Rev.* A77, 032343 (2008). arXiv:0709.4314.

③エンタングルメント光子対発生と応用

本プロジェクトで開発したエンタングルド光子対発生の装置（特願 2002-080109）をさらに改良し、PPLN 導波路を用いたエンタングル光子対光子源を開発した。

《論文》Y.-K. Jiang, and A. Tomita, “The generation of polarization-entangled photon pairs using periodically poled lithium niobate waveguides in a fibre loop”, *J. Phys. B* 40, 437 (2007).

④量子ゲート

量子中継に用いることを目標に量子非破壊測定を行うデバイスの提案と解析を実施した。

《特許》今村裕志,力武克彰,小島邦裕, 特開 2010-123761/6/3/2010, 「量子非破壊光子検出装置及びサブポアソニアン光子数分布光生成装置」.

2-2. プロジェクトメンバーの動静

本プロジェクトでは、それまで個々の研究室レベルで実施されていた量子計算、量子情報、デバイス開発の研究を理論から実証まで包括的に展開したことで、同分野の実用化までを視野に入れた多くの研究者を育てることに成功した。量子情報分野の次代のリーダーたる人材としては、松本啓史 NII 准教授、林正人東北大学准教授を輩出し、量子計算の分野では山下茂立命館大学教授、浜田充玉川大学准教授を輩出している。また、若手研究者としては小林弘忠 NII 研究員、山上智幸 JST 研究員（※SORST から雇用契約）らが世界に通用する研究者として育っている。Xiang-Bin Wang 氏を始めとする海外からの参加研究者も ERATO での実績を評価されて国内外の研究機関でポストを得て活躍している。

第 3 章　プロジェクト成果の波及と展望

3-1. 科学技術への波及と展望

(1)後継プロジェクトの展開

本プロジェクトの終了後、参加していた研究者は様々な公的資金を獲得し、研究開発を展開している。以下では主要なファンドによる研究プロジェクトを列挙する。

- 科学技術振興機構 SORST「量子情報システムアーキテクチャ」
  ERATO プロジェクトの発展研究として 2005 年 9 月～2011 年 3 月まで実施。量子分散計算、量子通信システム、量子鍵配送を中心に実用の観点から応用研究を推進している。
- 科学技術振興機構戦略的国際科学技術協力推進事業「次世代情報セキュリティシステムの設計と解析」
  2006 年から 2009 年まで実施。新世代の量子情報セキュリティシステムの設計と量子計算による現代暗号セキュリティの解析に関する研究であり、次世代情報セキュリティシステム、次世代情報セキュリティシステム（特に量子計算による解析）および情報セキュリティ基礎理論（特に計算量理論研究）に関する研究の推進をした。日本側代表者は今井教授、米国側代表者は Mario Szededy 教授（Rutgers 大学)。研究分担者として岩間教授が参加。
- NICT 委託研究「量子暗号の実用化のための研究開発」
  2006 年から 2010 年まで実施。高性能単一光子検出技術を利用して、無条件安全性が理論的に保証された高速な量子鍵配送プロトコルを都市圏ネットワークで実現するためのシステム技術の開発および量子鍵配送を基幹回線ネットワークへ適用していくための基盤技術の開発を実施。都市圏ネットワークと基幹回線ネットワークが接続したネットワーク上における量子鍵配送システムを開発して、その性能を実証している。委託先企業として NEC、三菱電機、NTT の 3 社が参画している。このうち、ERATO プロジェクトから富田教授が参加。
- 科研費基礎研究(B)「量子情報組合せ論に基づく最適化とその量子情報科学基礎拡張の研究」
  2005 年から 2008 年まで実施。研究代表者は今井 浩 教授。ERATO－SORST プロジェクトにおける量子対話型証明系の研究の発展テーマ。
- 科研費特定領域研究「複雑な系の量子統計推測と量子相関の研究」
  2006 年から 2010 年まで実施。研究代表者は松本啓史 NII 准教授。研究分担者に林正人東北大学准教授が参加。量子通信路の特性について、量子統計推測、漸近

理論、非局所性の点等から基礎研究を実施している。

- 科研費若手研究(B)「量子情報時代の新暗号基礎」

  2005 年から 2008 年まで実施。研究代表者は河内亮周東京工業大学助教。量子状態識別問題に関する基礎的研究から応用プロトコルまでの研究を実施。
- 科研費若手研究(A)「多端子量子通信ネットワークの理論的解析」

  2008 年から 2011 年まで実施。研究代表者は林正人東北大学准教授。
- 科研費基礎研究(C)「量子論に基づく符号理論の新展開と情報セキュリティへの応用」

  2010 年から 2011 年まで実施。研究代表者は浜田充玉川大学准教授。
- 科研費若手研究(B)「分散環境における量子計算能力のネットワーク形状に着目した解析」

  2007 年から 2009 年まで実施。研究代表者は谷誠一郎 NTT コミュニケーション基礎科学研究員。
- 科研費特定領域研究「現実的な状況下での量子計算の能力に関する研究」

  2004 年から 2008 年まで実施。研究代表者は山下茂立命館大学教授。
- 科研費若手研究 B「エラー訂正を考慮した効率の良い量子回路設計手法に関する研究」

  2007 年から 2010 年まで実施。研究代表者は山下茂立命館大学准教授。
- 科研費基礎研究(B)「量子情報理論と量子計算量理論の融合とその応用」

  2006 年から 2008 年まで実施。研究代表者は小柴健史埼玉大学准教授。研究分担者として松本啓史 NII 准教授、小林弘忠 NII 研究員、河内亮周東京工業大学助教が参画。
- 科学技術振興機構さきがけ「量子と情報」「代数的量子情報処理技術の研究」

  2004 年から 2008 年まで実施。研究代表者は濱田充玉川大学准教授。ERATO プロジェクトで理論的・定量的に存在を証明してきた高性能な符号をベースにして現実的に利用可能な量子符号や量子情報処理方式の設計を実施。
- 科学技術振興調整費先端融合領域イノベーション創出拠点プログラム「ナノ量子情報エレクトロニクス連携研究拠点」

  2006 年から 2016 年まで実施。総括責任者は小宮山宏東京大学総長（当時)。産学が協働してナノ技術、量子科学、IT ハードウェアの先端的融合領域を開拓し、ナノ技術及び量子科学技術に立脚したハードウェア開発により、持続的なイノベーションの創出を目指した研究・教育拠点。協働企業としてシャープ、NEC、日立製作所、富士通研究所が参画。今井 浩 教授がナノ量子エレクトロニクス基盤技術の研究開発と、拠点運営に関わっている。

(2)国際会議 AQIS の開催

AQIS (Asian Conference on Quantum Information Science)は EQIS の後継シリーズと

してアジアにおける量子コンピューティングの研究プラットフォームとして展開されている。AQIS の扱う主な研究領域は以下のとおりである。

- Quantum computation, algorithms and complexity
- Quantum information theory
- Quantum error-correction and fault-tolerance, thresholds
- Quantum cryptography
- Quantum communications experiments and theory
- Quantum optics, NMR and solid-state technologies
- Quantum processors and computers design
- Quantum programming languages and semantics

AQIS の実行委員長は 2006 より Jozef Gruska 教授（Masaryk University, Czech Republik）が努め、今井教授や岩間教授が日本開催時の実行委員として参加している。表２に AQIS の開催概要をとりまとめた。

表2 AQIS の開催実績の概要

<table>
<tr><td colspan="2">Asian Conference on Quantum Information Science 2006 (6th AQIS)</td></tr>
<tr><td>■日程：2006 年 9 月 1−4 日
■場所：北京フレンドシップホテル、北京
■参加人数：　名
■講演：口頭発表 56 件
（基調講演 2 件、招待講演 7 件を含む）
ポスター発表 52 件
■基調講演：Nicolas Gisin (University of Geneva)
Peter Zoller (Universität Innsbruck)
■URL：http://lqcc.ustc.edu.cn/aqis06/</td><td></td></tr>
<tr><td colspan="2">Asian Conference on Quantum Information Science 2007 (7th AQIS)</td></tr>
<tr><td>■日程：2007 年 9 月 3−6 日
■場所：京都大学芝蘭会館
■参加人数：名
■講演：口頭発表 54 件
（招待講演 7 件を含む）
ポスター発表 58 件
■URL：http://qc.naist.jp/aqis07/index.html
■共催・後援
JST−SORST、情報処理学会、井上科学振興財団、国際通信財団（ICF 韓国）、京都大学財団、村田学術振興財団、文部科学省、財団法人テレコム先端技術研究支援センター</td><td>  </td></tr>
</table>

Asian Conference on Quantum Information Science 2008 (8th AQIS)

■主催:KIAS(Korean Institute for Advanced Study)
■日程：2008 年 8 月 25－31 日
■場所：KIAS、ソウル
■参加人数：名
■講演：口頭発表 51 件
（基調講演 2 件、招待講演 6 件を含む）
ポスター発表　件
■基調講演：Sandu Popescu (University of Bristol)
Anton Zeilinger (University of Vienna/IQOQI)
■URL：http://newton.kias.re.kr/aqis08/

Asian Conference on Quantum Information Science 2009 (9th AQIS)

■主催：南京邮電大学（NUPT）
■日程：2009 年 8 月 26－29 日
■場所：南京邮電大学, 南京
■参加人数：名
■講演：口頭発表 42 件
（基調講演 2 件、招待講演 6 件を含む）
ポスター発表　件
■基調講演：Charles H. Bennett (IBM Research)
Lu-Ming Duan (Uni. of Michigan)
■URL：http://spt.njupt.edu.cn/aqis09/
■共催
IEEE Communications Society 南京センター
CIC Communications & Signal Processing Society
Jiangsu Institute of Communications (JSIC)

Asian Conference on Quantum Information Science 2010(10th AQIS)

■主催：JST –SORST QIC プロジェクト
■協力：国立情報学研究所（NII）・東京大学
■日程：2010 年 8 月 27－31 日
■場所：東京大学
■参加人数：　名
■講演：口頭発表 42 件
（基調講演 2 件、招待講演 6 件を含む）
ポスター発表 91 件
■基調講演：David Wineland (NIST, U.S.A.)
Andrew Yao (Tsinghua Univ., Beijing)
■URL：http://www.qci.jst.go.jp/aqis10/

その他の国際会議との連携

本プロジェクト参画者はこの他にも次のような学会に所属し、研究発表や編集、実行委員等の役割を果たしている。

- QIP（Quantum Information Processing）[15]　北米
- FOCS（Foundations of Computer Science）[16]　北米
- STOC（Symposium on Theory of Computing）[17]　北米
- SODA（Symposium on Discrete Algorithms）[18]　北米
- ICCAR（International Conference on Control, Automation and Robotics）[19]欧州
- ESA（European Symposium on Algorithms）[20]　欧州

特に、SODA については、2012 年の開催を京都に誘致することに成功しており、岩間京都大学教授が実行委員長を務めている。SODA が北米以外の地域で開催されるのは初めてのことであり、日本が量子計算、量子情報研究において国際的に一定の地位を占めていることを示している。

(3)受賞

本プロジェクトの成果が受賞に結びついたものとして、林正人東北大学准教授に授与された第 24 回日本 IBM 科学賞（2010 年 11 月）が挙げられる。

- 第 24 回日本 IBM 科学賞

  林正人　東北大学大学院情報科学研究科准教授

  受賞理由

  「量子情報におけるユニバーサルプロトコル理論の構築と量子暗号への応用」

「量子暗号通信分野での本賞の受賞は、本分野の研究が思考実験的な段階から理論の確立の段階へと移行したと認められたからではないかと思う」と受賞者はインタビューでコメントしている。

(4)その他の成果

本プロジェクトでの研究成果は以下のような教科書として出版されている。

- 林 正人著,「量子情報理論入門」 サイエンス社、2004 年.
- M. Hayashi, Quantum Information: An Introduction, Springer, 2006.

  ※東京大学大学院理学系研究科物理学専攻において修士課程のテキストに指定
- H. Imai and M. Hayashi, ed.: *Quantum Computation and Information --- From Theory to Experiment* ---, Springer, 2006.

---

[15] http://www.qip2010.ethz.ch/index
[16] http://www.egr.unlv.edu/~larmore/FOCS/focs2010/
[17] http://research.microsoft.com/en-us/um/newengland/events/stoc2010/
[18] http://www.siam.org/meetings/da12/
[19] http://www.waset.org/conferences/2010/france/iccar/
[20] http://algo2010.csc.liv.ac.uk/esa/

3-2. 社会・経済への波及と展望

(1)量子暗号通信の実用化に向けて

【ERATO 発技術の現状】

現在、国内における量子通信関連の大規模プロジェクトの代表的存在は NICT 委託研究プロジェクトと SORST プロジェクトとなっている。NICT プロジェクトは富田北海道大学教授の参画を通じて、NEC においてハードウェア（高速デバイス）とシステム（鍵抽出処理）の開発が行われている。主に実験・実装を行う NICT プロジェクトと理論を構築する SORST プロジェクトとの相互のフィードバックは両プロジェクトに好影響を与え、東京 QKD ネットワークなどの先進的な試みへとつながっている。

東京 QKD(Quantum Key Distribution)ネットワークは、NICT の研究開発用テストベッドネットワークである JGN2plus を元に構成されており、その中で大手町、小金井、白山、本郷の 4 つの拠点を結ぶネットワークである（図９）。

図9　東京 QKD ネットワークの構成

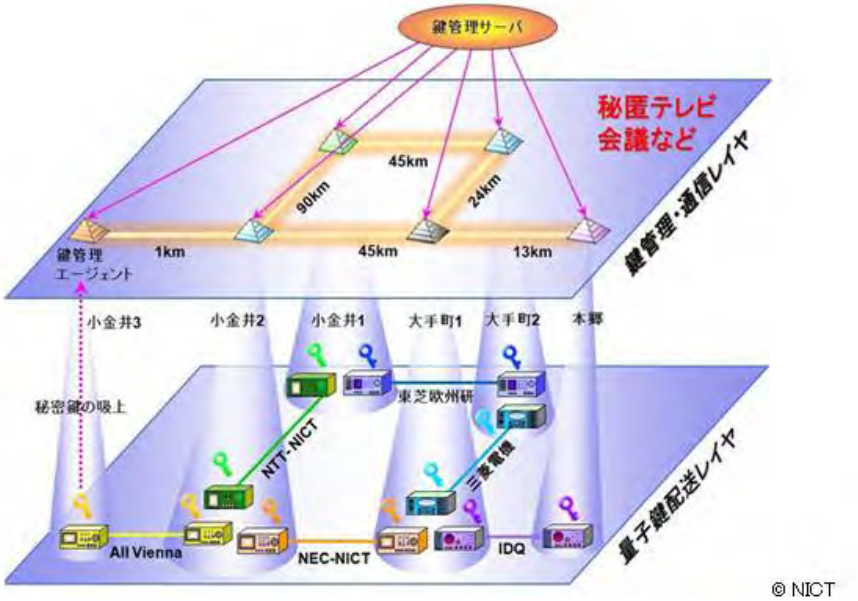


図10　東京 QKD ネットワークの構成と鍵管理のためのレイヤ構成

東京 QKD ネットワークは２層構造を有し、下層は量子鍵配送（QKD）レイヤであり、量子鍵配送により生成された秘密鍵は、物理的に同じ場所に配置される上位の鍵管理レイヤの鍵管理エージェントに吸い上げられる（図１０）。鍵管理エージェントは、秘密鍵と各リンクの鍵の量を常に把握し、鍵の量やリンクの状況を、さらにその上の鍵管理サーバに知らせ、鍵管理サーバはユーザの要求に基づき、複数の鍵管理エージェントに指示を出して、直接 QKD リンクのない場所にも適当な中継ノードを経由した安全な経路を設定し、必要な量の鍵を転送させる（鍵カプセルリレー）。また、ある QKD リンクに盗聴が検知された場合、鍵管理サーバは他の安全な経路を迅速に見出し、経路を切り替えることで秘匿通信を途切れることなく維持するよう鍵管理エージェントに指示を出す。東京 QKD ネットワークでは、このような鍵カプセルリレーや経路切り替えの試験を行い、秘匿通信の性能評価を実施している。

2010 年 10 月、NICT、NEC、三菱電機及び NTT は東京 QKD ネットワーク上で世界初、完全秘匿な多地点テレビ会議を実現した。秘密鍵の生成速度は 45km の光ファイバ回線で毎秒約 10 万ビットであり、これまで音声データの暗号化が限界であったものを動画データの暗号化に成功した。また伝送距離も 90km まで延長している。

【国際標準化への動き】

QKD システムは技術的にはほぼ実用段階まで来ており、ERATO プロジェクトで培った安全性評価に裏付けられた QKD システムが我が国の技術的な強みとなっている。量子通信の企画化、国際標準化においてもこの技術を拠り所に日本が主導的な役割を果たすことが期待されており、これに向けた活動も活発化している。特に ERATO 発の技術であるデコイ法は実質的な世界標準になりつつある。

【量子通信分野の競争的環境】

国外では以下の機関が量子通信に関して大規模な研究を行っている。

- 米国では主たる機関として DARPA（国防高等研究計画局）が挙げられる。
  - Quantum Information Science and Technology (QuIST) Program -2006[21]
  - Quantum Entanglement Science and Technology (QuEST) Program 2008-[22]
- NIST（国立標準技術研究所）でも量子情報科学のプログラムが展開されていた。
  - Quantum Information Program[23]
- ジュネーブ大学では、Nicolas Gisin 教授を中心に原理の研究に注力している。また、スピンオフ企業も有している[24]。

ウィーン大学では、Anton Zeilinger 教授を中心に研究が行われている。また、量子通

[21] http://www.darpa.mil/dso/archives/qist/index.htm
[22] http://www.darpa.mil/mto/programs/quest/index.html
[23] http://www.nist.gov/pml/div684/qip.cfm
[24] http://www.gap-optique.unige.ch/Members/Nicolas/Resume.htm

・　信の宇宙での利用も視野に入れている[25]。
・　東芝と英国ケンブリッジ大学キャベンディッシュ研究所の共同研究チーム
　➢　電圧制御による量子もつれ光子対の発生に成功[26]
・　上記以外の機関としては、カナダのウォータールー大学[27]が挙げられる。

国内外の研究開発面での競争力については、関係者からのインタビュー調査で次のようなコメントを得た。
・　国外の量子暗号通信研究は科学研究の側面（量子力学からのアプローチ）が強いが、日本では必ずしもそうではない。
・　日本では需要側の圧力が強いためか、理論と実験が高いレベルで融合しており、企業が研究開発の中心となっている。
・　国内企業では NEC と三菱電気が安全性の面から高い技術力を持っている。

（2）量子暗号通信の実用化に対するニーズとコストについて

量子暗号通信技術の実用化にむけた課題として、ニーズとコストの面について、関係者からのインタビュー調査で以下のようなコメントを得た。
・　暗号は保険であり、保険にどれだけコストを掛けるべきかが問題。
・　低コストで導入するためには既存のネットワークインフラを利用すること考えられるが、その際にノイズ対策などの技術開発が不可欠。
・　現在の開発コストは量子通信暗号装置 1 セットで約 1000 万円。これをニーズに応じてどの程度まで下げられるかが普及のポイント。
・　装置やシステム自体もまだまだニーズと性能のマッチングができていない。例えば 50km の伝送距離で 1Mb/sec.という性能では、動画のオンデマンド送信には使用できない。今後はユーザーの参加を得て、ユーザー側からのスペックや暗号鍵の応用について検討することが重要となるだろう。
・　量子通信のニーズや経済効果については、未だ不明な点が多いが、今後のニーズを喚起するためにも、はじめは政府機関が利用することが望ましいのではないか。
・　量子通信技術を実用化して既存の通信ネットワークで使用するためには以下の点が課題となる。
　① 通常の光通信からの混信を防止する必要がある。そのためのローパワーでのデータ伝送。
　② 上記のローパワー化に加えての多重化・大容量化（量子エンタングルメントが重要な要素となる）。
　③ さらに実用的な暗号化技術（本プロジェクトの大きな成果の一つである量子暗号技術に基づく）の実現。

[25] http://www.quantum.at/
[26] http://www.toshiba.co.jp/rdc/rd/detail_j/1006_01.htm
[27] http://new.iqc.ca/

・　量子中継に向けたより実用的な中継器、光アンプの実現（これには、東京 QKD ネットワーク構築・運用において蓄積されたノウハウの活用が期待される）。
・　量子通信のアプリケーション、換言すれば付加価値は未成熟であり、今後も研究を続けるべきである。

（3）今後の研究開発課題について

【量子暗号通信】

今後の量子暗号通信の実用化に向けた研究開発課題については、関係者からのインタビュー調査で以下のようなコメントを得た。

・　量子通信技術を前半部分と後半部分とに分けるとすれば、前半部分はデバイス関連技術であり、後半部分は量子フーリエ変換、つまり答えをだすための手法である。前半部分は、本プロジェクト、SORST プロジェクトにより進展したが、今後は、単一の量子ゲートではなく、複数の量子ゲートにより通信を行うための量子ゲートの作製技術等が課題となる。
・　QKD ハードウェアの実装→QKD ネットワークの構築へと進むためには、アプリケーションを使用するにあたっての安全性の検証をさらに進める必要がある。
・　量子テレポーテーションを用いた将来の量子中継や衛星中継を行なうためには、「基礎研究への回帰」が必要となるであろう。このためには、今後も公的研究開発資金による長期的な研究支援が必要である。
  - 量子中継技術の研究
  - 量子状態を記憶する方法に関する研究
・　現代のコンピュータ・サイエンスは、コンピュータという土台の上にデバイス、メソッドおよびプリンシプルが乗っているといえる。量子暗号通信の研究にもこれが当てはまる。
・　安全性評価の研究（universal cording 等）の促進が期待される。
・　量子符号化をにらんだ情報源圧縮の研究が進むと思われる。
・　量子暗号通信では、暗号鍵の配送をリアルタイムで行わない。この特徴は携帯電話やスマートフォンで有効利用できる。具体的にいえば、充電中に暗号鍵を転送・記憶させることができる（図１１）。

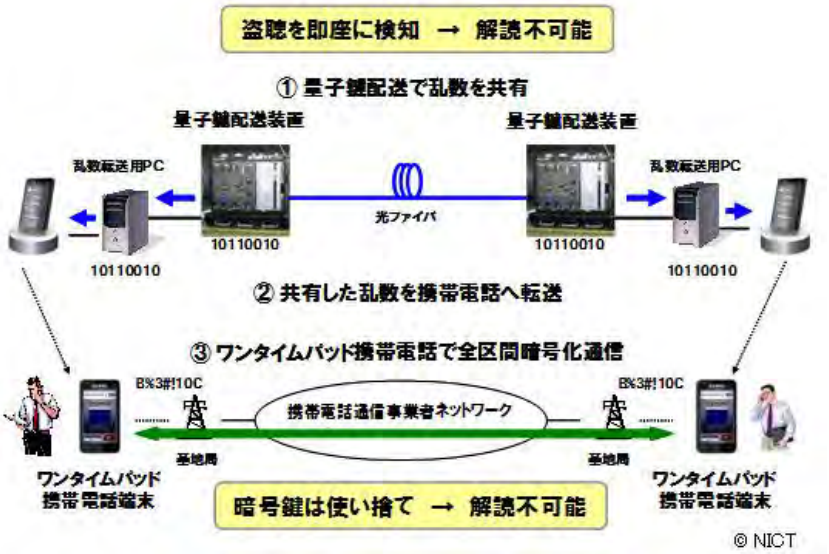


図11　量子鍵配送を用いたワンタイムパッド携帯電話による秘密通信

【量子計算】

量子計算の理論面における研究テーマの発展性については関係者からのインタビュー調査で以下のようなコメントを得た。

- 量子計算の代表的な問題はここ 10 年でほぼ解決してきた。残されている個々の問題の解決は研究テーマとして大きな発展性があるかどうかの判断が難しいところである。
  - 例）グラフ同定問題：量子系では計算量が分かっているが、古典系では判明していない。数学の大問題。
- そのような中でも、複数パーティー間の対話型情報通信で量子をどのように扱うのかという対話型証明系問題は大きな応用の可能性があるだろう。
- また、量子ランダムウォークに関わる諸問題も未解決である。
- 量子計算の功績として、古典系で上手く証明できない時は量子系で上手くいくという証明手法として発達している側面がある（量子で扱うところの連続系での近似手法が古典計算に役立っている）。

第 4 章　事業運営に関する意見等

ここでは今井量子計算機構プロジェクトに関わった研究者へのインタビューに基づき、ERATO プロジェクトの運営に関する意見をとりまとめた。

4-1. ERATO プロジェクトについて

【当時における量子計算・量子情報分野へのファンディングの意義】

- 大学の研究開発環境も近年では大変向上してきたが、10 年前は企業の基礎研究所の方が良い環境にあった。そのような時期に ERATO によってオフキャンパスで研究ができたことは当時としては画期的であった。
- オフキャンパスのおかげで大学の研究室とは全く違う経験ができた。雑用に追われず集中的に議論ができたのは何物にも代えられない経験だった。
- 量子情報、量子暗号の研究は本来大学でやるのは難しい。大学で実施する場合には理論研究になり、デバイスから独立して研究テーマが分化してしまう。ERATO のようなプロジェクトだから実現できたことだと思う。
- ERATO では研究をゼロからスタートできた。これは制度の大きな利点である。量子情報、量子暗号通信の分野がコンピュータ・サイエンスの１つの分野として認められたこと、これが ERATO 今井量子計算機構プロジェクトの最大の成果だと思われる。

【量子情報科学の拠点形成】

- 企業研究者がもっと大学に出向して共同研究が展開できればと考えていたので、ERATO の特徴であるオフキャンパスは、産学官連携の推進にも寄与し、メリットは非常に大であった。
- 大学だけだとついつい量子力学の基礎研究主体になってしまうところを実用的な研究成果の輩出までこぎつけたのは ERATO のオフキャンパスのおかげだと思う。量子計算のような学際的な研究領域では特にメリットとして機能したと思う。

【若手研究人材育成】

- 本プロジェクトによって世界に伍する量子計算分野の人材（若手を含む）を輩出することができた。

【マルチディシプリン研究へのファンディングの難しさ】

- 研究者のモチベーションの方向性とプロジェクト組織としての方向性の管理が難しい。学際的なプロジェクトや新領域のプロジェクトに参加した研究者がそこで成果を上げるということは、バックグラウンドでの主流から外れることでもある。

・ 量子情報分野の課題としては、50 歳前後の研究者のポジションが国内で確立されていないため、若手を引き上げることができないという事情がある。量子情報で国内でテニュアを得ようとすると、旧教育系の数学科か、独立大学院しかないのが現状。
・ 異なるバックグラウンドを持つ研究者が集う組織において、研究代表者が一人でプロジェクトの全責任を負うというのも相当なプレッシャーであり、研究の運営としても問題があると思う。

4-2. 課題・JST への要望等

(1)採択・評価に関わる問題

・ 現行のファンドの評価において過去のファンドの獲得実績を偏重すべきではない。学際的研究、新領域の研究では特にそう。
・ 研究者が報告書を作ることは相当な時間を割いているにも関わらず実績として全く評価されない。クローズドな報告書ではなく、出版されるべき。

(2)制度への改善要望

・ 年度末までの予算の使い切りは利便性に欠けていたと思う。また、継続研究プロジェクトへの資金の移管も場合によっては必要ではないか (ERATO と SORST の切り分けが大変だった)。
・ 大学側で本来はきちんと管理すべき点であるが、外部研究資金等で運営される研究組織における事務部門のあり方を検討する必要がある。プロジェクト資金で都度事務員を採用するのではなく常勤のスタッフを配置し、研究者が研究により専念できる環境を整備すべき。

(3)ファンディングに対する要望

・ 日本の科学技術政策には一貫性に欠けるのではないだろうか。量子情報のような新しい分野にファンディングしても研究分野として 5 年や 10 年では定着しない。資金が尽きると参加した研究者は元の研究領域に戻ってしまう。
・ 持続的な研究拠点の構築が必要。プロジェクト資金では新領域における研究開発の競争力を維持できない。
・ 日本にはファンディングソースがいくつもありすぎるのではないか？一元化や透明性を高めるための努力をすべきだと思う。