戦略的創造研究推進事業
発展研究（SORST）

研究終了報告書

研究課題「量子情報システムアーキテクチャ」

研究期間：平成１７年１０月１日～
平成２２年９月３０日

今井　浩
（東京大学大学院情報理工学系研究科，教授）

１．研究課題名

量子情報システムアーキテクチャ

２．研究実施の概要

本 ERATO-SORST 量子情報システムアーキテクチャプロジェクト(以下,本プロジェクト)は 2000 年 10 月から 2005 年 9 月まで実施された ERATO 今井量子計算機構プロジェクト（以下，ERATO プロジェクト）の後継として，同プロジェクトの成果を元に研究を継続・発展させることにより，現実の社会にインパクトを与えうる量子情報システムのためのアーキテクチャの創出を目的として構想された．このため，本プロジェクトでは量子情報の手法によるセキュリティ技術の革新に重点を置くこととした．IT 技術のセキュリティは，Bennett-Brassard による量子暗号鍵配付や Shor による素因数分解アルゴリズムの提案等によって，量子情報技術が社会的に大きな影響を与える可能性をもつ課題として注目されてきた．本プロジェクトでは ERATO プロジェクト以来，理論・実験の双方のアプローチを有機的に結合させる研究の枠組みを活用して，確固たる理論的基礎付けの元で現実的なシステムを実現するという世界的にも例のない取り組みを行うこととした．

ERATO プロジェクトにおいては，量子暗号鍵配布の有限長符号における安全性証明，量子公開鍵暗号，量子暗号鍵配布に用いられる光子検出器開発・単一光子伝送など，理論と実験の両面から量子情報によるセキュリティ技術の基礎技術・要素技術を確立することができた．本プロジェクトにおいては，従来の理論で想定されてきた理想的な状況の成り立たない現実のシステムでの量子暗号鍵配布の安全性保証に関して，理論的解析・暗号鍵生成ソフトウェアの開発を行い，安全性を保証するシステム構成をプロジェクト全体の目標の一つとした．また，量子アルゴリズムの実証として，ERATO プロジェクトで提案された量子リーダ選挙を行うアルゴリズムを光量子システムにおいて実現することをもう一つの目標とした．これは古典的アルゴリズムでは達成不可能な課題を量子情報処理によって実現できるものの一つで，量子分散アルゴリズムとしては世界で初めて見出されたものである．分散アルゴリズムは必然的に通信を伴うため，量子通信に適した光子システムで実現することは意義が高いものと考えられる．

量子通信量・量子計算量に関する理論は ERATO プロジェクトにおける研究の柱であったが，本プロジェクトにおいてもセキュリティ技術の観点からさらに研究を進めることを目指した．多者間の量子プロトコルによる計算方式の研究，資源に制約がある場合での量子分散計算に関する研究，群判定問題や群同型問題などの代数的な問題を解く量子アルゴリズムの研究，古典暗号によるセキュリティの重要問題であるクロー探索，量子誤り訂正符号のリスト復号・量子ハードコア関数の構成など量子計算量的安全性に関する研究などによって，量子によるセキュリティ保証を様々な側面から検討することができるものと考える．これは単に量子暗号鍵配布の性能向上や実用化研究にとどまらず，量子セキュリティという，より大きな広がりをもった応用が期待できる．

一方，量子情報科学における基礎的な問題として量子測定と推定があり，これに関しては ERATO プロジェクトの時代からさまざまな成果をあげてきた．本プロジェクトでは，

量子状態の測定や推定の問題を量子セキュリティの観点から見直すことで新たな発展を目指した．量子測定の理論は，セキュリティや量子通信モデルの精密化に直結する一方， 将来の量子計算機の具体的モデルのもとで，量子誤り訂正符号の効率的生成等の問題に発展・展開するものと期待される．量子情報におけるもう一つの基本的問題である量子エンタングルメントもまた， BB84 に代表される現行の量子鍵配送（QKD）を超越するポスト QKD ともいうべき量子セキュリティプラットフォームを切り開く可能性を持っている．以上のような観点から本プロジェクトにおいても量子情報の基礎理論の研究を推し進めた．

量子情報システムの実現のための技術として，ERATO プロジェクトではエンタングル光子対の効率的発生法や，光子検出技術，量子フーリエ変換の実証に代表される光量子回路の構成の研究を行ってきた．これらの技術は光量子情報処理技術の基本であるため，さらに研究を進める必要がある．さらに高度な情報処理を行うためには制御ゲートを用いた量子回路を用いることが望まれるため，量子ゲートの実現法についても研究を行った．

本プロジェクトは様々な研究成果をあげることができたが，もう一つ忘れてはなないことに量子情報研究の振興がある．前身である ERATO プロジェクトは幅広い量子情報技術に関する国際会議（ERATO Conference on Quantum Information Science, EQIS）を毎年開催することで日本のみならず，アジアにおける分野の研究発展に貢献した．この国際会議は（Asian Conference on Quantum Information Science, AQIS）に発展し，本プロジェクトが直接主催することはなくなったが，EQIS での経験を生かし，毎回会議の運営に欠くことのできない援助をしてきた．本年 10 回目の会議を本プロジェクトで主催したが，各国の指導的な研究者から本プロジェクトの貢献について極めて高い評価が与えられた．また，ERATO プロジェクトおよび本プロジェクトでは日本国内と諸外国から有望な博士号取得者を研究者として採用したが，彼らの多くが量子情報分野で生産的で重要な成果をあげる中核的研究者に成長している．

量子コンピューティンググループは
高度な量子情報処理システムの基礎となる量子計算の理論的研究を行った．アルゴリズム論にとどまらず，その可能性を明確にする計算量の研究も同時に行い，それらの最適性に関する研究も併せて進めた．

特に，量子情報処理ネットワークシステムを意識した量子分散計算に注目し，リーダ選挙問題において従来の古典的情報処理に対する優位性を明らかにした．

また暗号への量子計算の応用として，暗号理論の基盤となるハードコア関数を構成し，効率的な量子リスト復号アルゴリズムを提案した．

さらに量子アルゴリズムの統一原理の解明に向けた，代数的な構造を持った問題を解く量子アルゴリズムを研究し，可解群の性質を持つかどうかをチェックする効率的な量子アルゴリズムや，可換群のあるクラスに関して同型判定を行う量子多項式アルゴリズムを与えた．

加えて，量子対話型証明系やネットワークコーディングという様々な観点から，量子計算能力の解析を行い，古典計算能力に比べて指数ギャップを持ついくつかの性質を明らかにした．

また，量子リーダ選挙アルゴリズムの実証を量子情報実験グループと共同で行った．

量子情報理論グループは
ERATO 今井量子計算機構プロジェクトで行った BB84 型量子暗号における有限の符号長での安全性証明を発展させた．特に，光源として通常のレーザ光を減衰させたものを用いることを想定し，有限データから来る推定の統計的揺らぎを考慮した現実的な設定における安全性証明を行い，実装のためのソフトウェアを開発し，最終的に実証実験までを量子情報実験グループと共同で行った．

これと並行して，より広い意味での量子セキュリティ理論を追求すべく，量子測定における擾乱と測定精度に関するより精密な理論の構築，量子エンタングルメントを利用した量子通信の統一的理論の構築などを行い，量子 LDPC 符号の提案，量子テレポーテーションによるユニバーサル量子プロセッサの提案などの成果に繋げることができた．

また量子エンタングルメントに関する基礎的な理論研究も進めた．

量子情報実験グループは
量子コンピューティンググループと協力して，２者間の量子リーダ選挙アルゴリズムを実装するための光量子回路の構成法を研究し，システム実証を行った．さらに，実験では不可避である装置の不完全性の影響についても検討した．必要となる平均通信量の概念を導入することで，不完全な量子システムでも古典的なリーダ選挙アルゴリズムを凌駕することを示した．

量子情報理論グループと協力して，量子暗号鍵配付システムの実証実験を行った．本実験では現実のシステムで盗聴者が持ちうる最終鍵に関する情報量の上限を定量的に保証することができた．さらに，システムの特性が時間的に変動することが安全性にどのような影響を与えるかを，実際の盗聴をシミュレートした実験で検討した．また，量子暗号の安全性の実験的証明の一環として量子クローニングによる盗聴を検討し，現在ある技術で実装可能な盗聴器を設計した．

周期分極 $LiNbO_3$ を用いた高効率エンタングル光子対の発生を行い，ループ構造による安定な偏光エンタングル光子対の発生に成功した．また，２波長，位相-偏光エンタングル光子対の発生にも成功した．

量子ゲートの実現のために，共振器と V 型原子（量子ドット励起子を想定）の組み合わせを検討し，光子非破壊測定を行う素子の提案を行った．さらに，フォトニック結晶の欠陥共振器と量子ドットの組み合わせによる構成法の検討を行った．

アバランシェフォトダイオードを用いた光子検出に関して，現在広く用いられているガイガーモードとは異なる方式の実験的検討を行った．

３．研究構想

本プロジェクトは ERATO 今井量子計算機構プロジェクトでの研究を継続・発展させ，理論，実験の双方のアプローチを有機的に結合させることで量子情報システムのためのアーキテクチャの創出を目指すことを目標として構想された．量子情報システムの中でも，特に量子計算及び量子暗号プロトコル・システムに重点をおき，同時に，これらを支える基礎的テーマとして量子情報理論及び量子統計推測についても研究を行うこととした．研究開始時の目標は以下の通りである．

量子計算：新アルゴリズムの導出

① 多者間量子分散アルゴリズムの構築

② 量子分散計算の原理検証実験

③ 量子アルゴリズムの統一原理の解明に向けた，対称構造発見量子アルゴリズム等構築

量子暗号：実際に安全な量子暗号システムの開発

① 符号化やデコイ状態法などのソフトウェア技術の開発

② 上記ソフトウェアを実装した量子暗号システムの開発

③ 長距離化へ向けた検討

量子暗号システムの実証の成功，量子リーダ選挙アルゴリズムの実証の成功などを受けて，本プロジェクトの後半では以下のような研究を行うこととした．

（1） ・量子分散計算について，通信方式やネットワークトポロジーと言った，各種パラメータによる多様なネットワークに対して，通信プロトコルの効率性に関する限界を明らかにする．

・マルチパーティプロトコルの通信量のモデル化を行い，プロトコルへの昇華を目指す．リーダ選挙問題やその他の分散計算の問題に関して様々なネットワークトポロジーにおける通信量やメッセージ回数を検討する．

・群論的構造を用いて古典計算を越える量子計算アルゴリズムの研究を行う．

以上のような研究は量子アルゴリズムの新しい応用を拓くものである．特に量子通信に関しては実験的な検証も視野に入れた研究を行う．

（2） ・量子エンタングルメントについて，セキュリティとの接点に注目し，束縛エンタングル状態に関する未解決問題の解決を図る．

・量子力学的状態の非局所的な性質を活用した状態推定や検定の問題を考える．

・量子測定の問題を引き続き考察する．量子的な特徴が露わになるコレクティブな量子測定について，具体的な測定プロセスのもとで環境系にどれだけ情報が漏れるのか，そのうちどれだけ回復できるのか，という課題をさらに精密化して研究する．従来環境系は注目する量子系のコヒーレンスを破壊する，いわば邪魔者として考えられていたが，環境系をうまく取り込むことによってどれだけ量子情報処理能力が向上するのか，といった問題も追及する．

・エンタングルメントを利用した通信プロトコルの性質，性能の評価を行う．

（3）　・量子光学実験では量子情報ハードウェアの開発を行うが，量子暗号，特に量子暗号鍵配布についてさらに研究を進める．現在の技術では最適な盗聴を行うのは難しいが，技術的に可能な受信－再送攻撃，ビームスプリッタ攻撃，クローニングなどを行い，理想的な盗聴が行われた場合の情報漏洩の大きさをシミュレートする．

・量子ゲートの構成法の研究

・光子検出の研究

以上のような研究を効率的に遂行するため，本プロジェクトでは量子計算，量子情報理論，量子情報実験の 3 グループをおいた．当初は量子コンピューティンググループと量子情報グループの 2 グループでプロジェクトを開始したが，量子状態推定や量子エンタングル理論など量子情報理論の重要性を考慮して，2 年度より量子情報理論を専門とするグループを独立させ，この分野での活動を強化した．これら 3 グループのうち，量子コンピューティンググループと量子情報理論グループは本郷のプロジェクトオフィスに集結して研究を進めた．量子情報実験グループは実験場所の確保と共同研究相手先である NEC 基礎・環境研究所（現グリーンイノベーション研究所）との連絡の便から，ERATO プロジェクトに引き続き NEC 筑波研究所内で研究を行った. 量子コンピューティンググループは量子計算の理論を担当し，量子アルゴリズムに関する基礎的な研究を進めた．量子情報理論グループは量子状態についての基礎的な理論構築と同時に実用的な量子暗号システム開発のための理論とソフトウェア開発を行った．量子情報実験グループは光子による量子情報処理の要素技術および光量子除法処理システムの構築法に関する研究を進めた．各プロジェクトはそれぞれのテーマで研究を進めるとともに，相互に交流してアイディアやそれぞれのディシプリンの持つ技術を交換することで視野の広い研究を行うことができた．特にプロジェクト全体の課題である，量子暗号鍵配付システムの開発と量子リーダ選挙については 3 グループが協力して技術を持ち寄ることでシステム実証に成功することができた．

【量子コンピューティンググループ】

量子コンピューティンググループは，
多者間の量子プロトコルによる計算方式の研究を推進するため，特に ERATO 今井量子計算機構プロジェクトで行ったリーダ選挙問題の発展を目指した．アルゴリズムの改良，特殊ケースでのより良いアルゴリズムの開発，通信計算量の下限に関した研究を進めている．また，量子分散計算モデルを発展させて，資源に制約がある場合での 量子計算に関する研究を行った．
量子アルゴリズム研究は当初 ERATO 今井量子計算機構プロジェクトで行った隠れ部分群問題の研究を発展させることを目指した．群判定問題や群同型問題などの代数的な問題を解く量子アルゴリズムの研究を行っている．また，古典暗号によるセキュリティの重要問題であるクロー探索を，量子ウォークのアルゴリズム設計への応用として研究した．
さらに，量子計算のセキュリティへの応用である量子計算量的安全性に関して，量子誤り訂正符号のリスト復号・量子ハードコア関数の構成など新しい展開があった．
また，量子の計算能力を，多証明者量子対話型証明系や量子ネットワークコーディングといった様々な観点からの解析を行うことで，量子計算の優位性とその特性を明らかにしてきた．

量子コンピューティンググループ　5 年間の実施実績

項目	平成 17 年度（6 ヶ月）	平成 18 年度	平成 19 年度	平成 20 年度	平成 21 年度	平成 22 年度
量子アルゴリズム	→	→	→	→	→	→
		対称構造等発見量子アルゴリズム				
	→	→	→	→	→	→
	量子情報グループと相互の手法を学ぶ	量子ウォーク 量子学習		量子加速一般論		
多者間量子分散計算	リーダ選挙	リーダ選挙 ビザンチン分散問題 拡張など				
	→	→	→	→	→	→
	多者間量子対話型ゲーム		多者間量子プロトコル			

【量子情報理論グループ】

量子情報理論グループは,
ERATO 今井量子計算機構プロジェクトで行った BB84 型量子暗号における有限の符号長での安全性証明を発展させ，実際の符号の設計と実装を行った．当初の予定から発展し，光源が単一光子でない通常のレーザ光を減衰させたものを用い，有限データから来る推定の統計的揺らぎを考慮した現実的な設定における安全性証明とソフトウェア開発．実装までを行うこととした．さらに理論の改良とプロトコルの効率化，適用範囲の拡大を行った．
これと同時に，BB84 型秘密鍵配布量子暗号を越えて，より広い意味での量子セキュリティを追求する観点から，量子測定，量子通信，量子誤り訂正，および量子エンタングルメントに関する理論的研究を強力に推進した．

第 1 に，量子セキュリティの観点から量子測定について理論的研究を行い，盗聴で漏洩する情報量，伝送できる情報量，種々のエントロピー関係式やエンタングルメント測度の関係を明確にした．

第 2 に，量子エンタングルメントは量子情報処理における重要な物理的リソースであるとの観点から，この量子エンタングルメントを積極的に用いた量子通信（エンタングルメント支援型量子通信）の理論的研究を進め，古典通信，量子通信，エンタングルメント操作などが同時にかかわる複雑な種々のプロトコルの統一的理論の構築を行った．この成果に基づき新プロトコルの提案を行う一方，量子テレポーテーション，LDPC（低密度パリティ・チェック）符号などの既存のプロトコルをさらに発展させ，量子情報の分野でどのような活用があるかを探った．

最後に量子エンタングルメントそのものについても理論的研究を推進した．例えば，連続変数状態の量子エンタングルメントに関する未知の関係を明らかにし，また量子セキュリティの観点からも重要な束縛エンタングルメントの抽出に関する理論的研究を行った．

量子情報理論グループ　5年間の実施実績

項目	平成17年度（6ヶ月）	平成18年度	平成19年度	平成20年度	平成21年度	平成22年度
量子暗号	符号設計	符号実装	システム	実証	装置変動	解析
	盗聴検出	実証	システム	実装	盗聴器設計	
	新	プロトコル	検討			
量子情報理論		連続変数状態のエンタングルメントの理論的研究			エンタント支援型路の統一	グルメン量子通信理論構築
					高性能量正符号の	子誤り訂提案
					量子LDの提案	PC符号
			量子測定と情報漏洩に関する理論的研究		量子エンメント抽的側面の	タングル出の数学解明
					ユニバーサル量子プロセッサの提案	

【量子情報実験グループ】

量子暗号：量子情報理論グループと共同して，ERATOプロジェクトで行ったBB84 型量子暗号における有限の符号長での安全性証明を発展させ，実際の符号の設計と実装を行った．改良されたデコイ状態を用いた量子暗号プロトコルにつき盗聴検出の原理実証と実装を行った．さらに，当初予定を越えて量子暗号ソフトウェアを実装したシステムを構築し，量子暗号鍵配布の生成まで行った．

Intercept-resend と呼ばれる最も基本的な盗聴と等価な実験を行い，装置の特性の変動の影響を実験的に評価した．また，安全性の実証の一つとして量子クローニングを用いた盗聴器の設計を行った．

量子情報システムハードウェア：ERATOプロジェクトでの自発パラメトリックダウンコンバージョンの研究を発展させ，周期分極$LiNbO_3$を用いた光通信波長帯での偏光エンタングル光子対の高効率発生を実現した．また，ファイバ通信と空間伝送のインタフェースを目的として，２波長(800nm+1550nm)，偏光-位相エンタングル光子対を実現した．

光と量子ドット励起子・原子の相互作用の解析を通して光を入出力とし，原子と共振器の結合系における非線形ゲート，光子非破壊測定法とその応用について理論的な研究を進めた．

自発パラメトリックダウンコンバージョンの生成技術を応用して，リーダ選挙プロトコルの実証を行った．

通信波長帯光子検出器の性能向上のためアバランシェフォトダイオードの試作評価を行った．また，新しい光子検出法としてサブ・ガイガーモードでの光子検出の実験を行った．さらに，光子検出を表す POVM(Positive Operator Valued Measure)についても検討を行った．

量子情報実験グループ　５年間の実施実績

項目	平成 17 年度（６ヶ月）	平成 18 年度	平成 19 年度	平成 20 年度	平成 21 年度	平成 22 年度
量子暗号	符号設計	符号実装	システム	実証	装置変動	解析
	盗聴検出	実証	システム	実装	盗聴器設計	
	新	プロトコル	検討			
量子情報システムハードウェア		光子検出器	改良		サブ・ガイガー光子検出	イガー光
	エンタン	グル発生	量子プロトコル実証			
	量子ドット	解析	量子ゲート	理論設計		

４．研究実施内容

４．１ 量子コンピューティンググループ

(1)実施の内容

①研究のねらい

量子コンピューティンググループでは高度な量子情報処理システムの基礎となる量子計算の理論的研究を行う．アルゴリズム論にとどまらず，その可能性を明確にする計算量の研究も同時に行う．これらの研究は単純にプロトコル，アルゴリズムの構成にとどまらず，それらの最適性に関する研究も併せて進めることとする．このような最適性の研究は性能限界や改良の余地がどこにあるかを示すことができ，今後の研究の指針を正確に見極める上で不可欠である．

特に，(i) 量子情報処理ネットワークシステムを意識した量子分散計算に注目し，従来の古典的情報処理に対する優位性を明らかにする．(ii) 暗号への量子計算の応用として，量子・古典それぞれの計算量的安全性解析へ応用できる量子アルゴリズムの検討を行う．従来の暗号の計算量的安全性に対する量子計算のインパクトは Shor の素因数分解アルゴリズムの例を見ても明らかである．(iii) 量子アルゴリズムの統一原理の解明に向けた，代数的な構造(ここでは特に群を考える)を持った問題を解く量子アルゴリズムの検討. (iv) 量子対話型証明系やネットワークコーディングという様々な観点からの量子計算能力の解析．という４点に狙いを定めて研究を進める．

②研究実施方法

量子コンピューティンググループは東京オフィスに本拠を置いて理論的な研究を進める．同じオフィスで研究する量子情報理論グループとは密接に討論を行い，相乗効果を高める．量子計算と量子情報理論は従来アプローチ，手法が異なっていたが，ERATO 今井量子計算機構プロジェクトでの経験から，相互の手法を適用することで新しい成果が得られることが期待される．量子情報実験グループとは，量子分散プロトコル（特に量子リーダー選挙問題）の実証実験の構想・結果の解析などで協力する．東京大学大学院情報理工学系研究科今井研究室とは「量子情報科学における計算機を用いたシミュレーション」に関して共同で研究を行う．また，ERATO 今井量子計算機構プロジェクトの研究成果と，これも大きな成果である量子計算理論の研究者のネットワークを活用するため，旧プロジェクトメンバーとも情報交換を行いながら研究を進める．

(2)得られた研究成果の状況及び今後期待される効果

(i) 量子分散計算

多者間の量子プロトコルによる計算の実現に向けて，量子分散計算の一つであるリーダ選挙問題の量子の優位性とその計算量を明らかにすることができた．今後はリーダ選挙以外の量子分散計算の研究も盛んになっていくものと思われる．また，資源制約付き計算量の

解析により，量子メモリの少ない量子計算での能力も明らかになってきたことは，大規模量子メモリの実現がまだ困難な現在の量子コンピュータ研究において，近い将来実現可能な小規模メモリ量子計算の能力を示す重要な指標となる．

■　資源制約下における量子計算モデルの計算能力の研究

計算時間を考慮すれば，量子計算モデルが古典計算より強力であることが多くの結果によって示されてきた.しかしながらメモリや通信資源に関しては量子コンピュータの計算能力がまだ明らかになっていない．大規模量子メモリの実現が技術的に可能かどうかはまだ明らかではないが， 通常の設定の場合，任意の問題を解くのに量子コンピュータと従来のコンピュータの必要なメモリのサイズはほぼ等しいことが知られている． このため，メモリの少ない量子コンピュータの計算能力の研究は大変重要である．オンライン計算という設定の場合， つまり入力が一度に 1 文字ずつ与えられるとき， 我々は大規模な古典メモリを持つコンピュータに比べて，指数的に小規模な量子メモリしか持たないコンピュータが，同程度の計算能力を示す初めての問題の例を提案した．

量子分散計算では，各自入力を持つ二つのコンピュータが双方向の通信をもとにこのふたつの入力に依存する関数を計算するために送らなければならない最小のビット数を考える．様々な問題設定の下で量子分散計算が古典分散計算より強力であることが知られている．我々はさらに非決定設定（guess が与えられる設定）の分散計算を初めて研究し，量子計算の古典計算に対する計算能力の優位性を示した．

■　匿名ネットワークにおけるリーダ選挙問題を解く量子分散アルゴリズムの改良

リーダ選挙問題とは，図 4.1 のように通信ネットワークで相互接続された通信ノード同士で，局所計算およびメッセージの交換を通じて，自律的にリーダとなる通信ノードをちょうど一つ決定する問題である．ネットワーク上に入力データが分散しているような計算タスク（分散計算）やアドレスの自動付与など，リーダとなる通信ノードが決定すれば，その通信ノードが中心となって処理を行うことにより，簡単に計算タスクを実行することができる．この意味で，リーダ選挙問題は，分散計算における本質的な問題として，古典計算機科学の分野で盛んに研究されてきた．この問題において各計算機が固有の識別子を持つときは，その識別子の最大値を求める問題に帰着すればよく，効率的に解けることが知られている．しかしネットワークが大規模になると識別子の固有性を維持するのは一般的に困難であることから，各計算機が固有の識別子を持たない場合（すなわち各通信ノードは全く同一で識別できない）でのリーダ選挙が多く研究されるようになった．これを，匿名ネットワークでのリーダ選挙問題と呼ぶ．匿名リーダ選挙問題は，古典分散計算では，決定的に（すなわち，有限時間内で誤ることなく）解くことはできないことが良く知られ

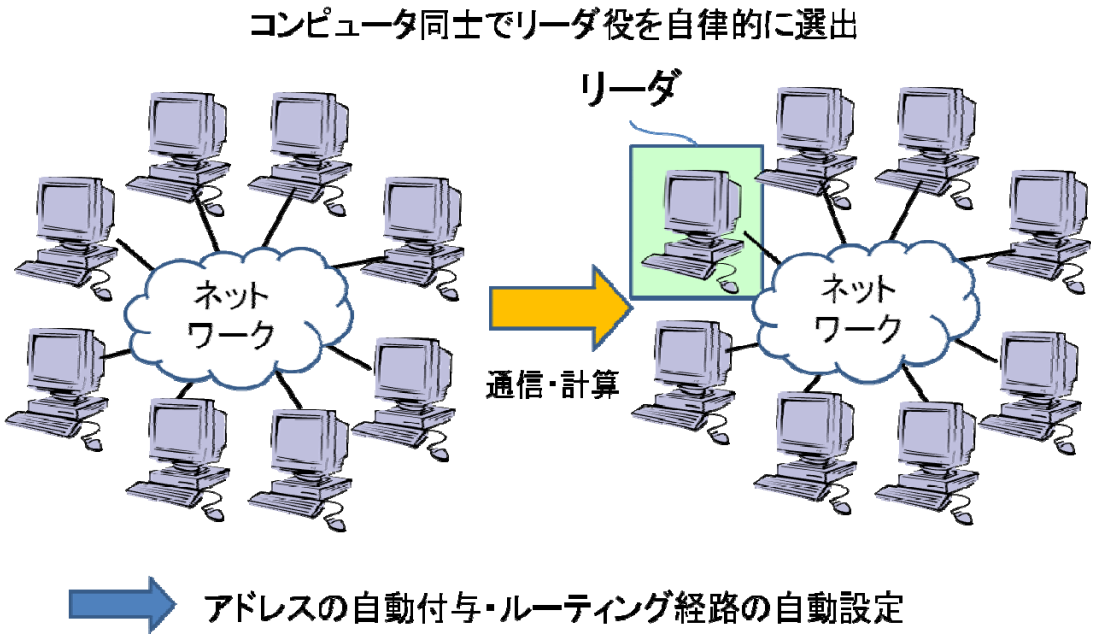


図 4.1 リーダ選挙問題

ている．これに対して，量子分散計算を用いると決定的に解くことが可能であることが谷・小林・松本により示され，量子分散計算と古典分散計算の計算能力の違いが明らかになった（表 4.1）．一方で，提示された量子分散アルゴリズムよりも少ないオーダーのメッセージ回数（通信ノード数 n に対して $O(n)$回）で，確率的に解く古典分散アルゴリズムが知られている．このため， 同程度のメッセージ回数で古典分散計算と量子分散計算の計算能力を比較することが目標であった．

我々は任意のトポロジーの匿名ネットワークにおいて，$O(n)$回のメッセージ回数で決定的にリーダ選挙問題を解く量子分散アルゴリズムを考案した．さらに，応用上重要な特殊なトポロジー（リング型や完全グラフ型）に対しては，トポロジーの特殊性を利用した，より効率的な量子アルゴリズムを考案した．考案した量子アルゴリズムの技術上のポイントは，量子計算の重要技術である，量子振幅増幅を分散的に実現したことにある．これまでも，量子振幅増幅を分散的に実現した例はあったが，量子振幅増幅を構成するアルゴリズム部分とオラクル部分のうち，オラクル部分のみを分散的に実現したものであった．しかし，提案アルゴリズムは，ネットワークの匿名性に対応するため，アルゴリズム部分とオラクル部分を共に分散的に実現した．これは，量子振幅増幅の新しい分散的実現法を与えるものである．

表 4.1 ノード数 n のときのリーダ選挙問題の時間，通信計算量

	時間	量子通信回数	総通信回数	ラウンド
Algorithm I	$O(n^4)$	$O(n^4)$	$O(n^4)$	$O(n^2)$
Algorithm II	$O(n^6(\log n)^2)$	$O(n^2)$	$O(n^6(\log n)^2)$	$O(n \log n)$

(ii) 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

現代暗号の多くの安全性は，計算困難性と擬似乱数性に基づいている．擬似乱数性は一方向性の性質を持つ関数から構成される．一方向性関数とは，その関数自身を計算することは簡単であるがその逆関数を計算することが困難な関数であり，この一方向性から擬似乱数性に変換するものがハードコア関数と呼ばれるものである．したがって，量子一方向性関数及び量子ハードコア関数は，量子計算や量子暗号理論の重要かつ基本的な概念である．

我々は，強量子一方向性関数を構成するための，新しい量子ハードコア関数を３種類提案した．さらにこの量子ハードコア関数を用いて，初めてリスト復号を効率的に行う量子アルゴリズムも提案した．通信の際データに誤りが生じる可能性があるため誤り訂正符号が広く使われているが，誤り率が非常に大きいとき，どんな誤り訂正符号を利用しても複号化が不可能の場合が存在する．そのとき元のデータの候補のいくつかを出力するというリスト複号法が有効であり，最近リスト複号を効率良く行う古典アルゴリズムの研究が大変盛んになっている．古典で知られている q-ary アダマール符号のためのリスト復号では，各通信データの候補ごとに多項式個のクエリーを必要としていたが，我々の提案した量子復号アルゴリズムでは２回のクエリーの呼び出しだけで通信データの候補を求めることができるため，非常に効率的である．

■ クロー探索問題

古典的(計算量的)暗号の安全性解析に関連して，2 つの関数f(x)，g(y)の値が等しくなる引数の対(x，y)を見出す問題である，クロー探索問題(claw finding problem)がある．この問題は collision problem, element distinctness problem とともに，古典暗号と密接な関連を持つ．それだけでなくより本質的な，量子計算能力の解明にも通じる問題であって，これまでにも盛んに研究が行われてきた．現在までに，collision problem と element distinctness problem については，量子計算機で解く際に必要な質問計算量(入力へのアクセス回数)の最適な評価値が知られている．また，最適な評価値を得る過程で，量子計算における新たな技術が開発されてきた．一方，claw finding problem については，上界及び下界は知られているものの，それらの間にはまだギャップが存在し，上界及び下界の改良は未解決の問題として良く知られていた．

我々は，これまで知られていた上界を大きく改善した．X のドメインを N，Y のドメインを M としたとき，$O((NM)^{1/3})$ $(N \leq M < N^2)$，$O(M^{1/2})$ $(M \geq N^2)$であることを示した．依然として，この上界が最適であるかは明らかでないが，興味深い特殊ケースについては最適となる．また， 上界を得るために開発した量子アルゴリズムは，claw finding problem をさらに一般化した問題にも適用することができる．例えば，k個の関数の$f_1(x_1)$，$f_2(x_2)$,…，$f_k(x_k)$の値が等しくなる引数の組$(x_1, x_2, \ldots, x_k)$

を求める問題 k-claw finding problem にも適用でき，効率的に解くことができる．開発した量子アルゴリズムは，Mario Szegedy により開発された量子ウォークを 2 分探索と組み合わせることで構成される．

(iii) 代数的な問題を解く量子アルゴリズム

■ Property Testing

一般的に，与えられた対象がある性質を持つかその性質とかけ離れているかを判定することは性質判定と呼ばれ，多くの代数的な性質が判定可能であることが知られている．しかしながら，与えられた対象が群という代数的な構造を持っているかどうかを判定する問題は未解決問題である．量子計算が古典計算より高速に解ける問題の多くが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である．ここで第一歩として，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チェックする効率的な量子アルゴリズムを提案した．
また，与えられた二つの群が同型かどうかを判定する問題も群に関する自然な基本的問題であり，古典の場合に関して広く研究されている．素因数分解やグラフ同型判定問題などもその群同型判定問題と関連があり，量子計算の観点からも非常に興味深い問題である．ここで可解群のあるクラスに関して同型判定を行う多項式時間量子アルゴリズムを与えた．

(iv) 量子計算能力解析

■ 多証明者版量子対話型証明系

対話型証明系とは，計算能力に制限のない証明者と多項式時間計算のような計算能力に制限を持つ検証者の対話によって行われる一種のゲームである．対話によって証明者は検証者に与えられた入力がある性質をみたすことを納得させようとするが，検証者は証明者に騙されないよう検証を行う．ある集合（通称，言語）L が対話型証明系を持つとは，任意の入力に対して，その入力が L に入る場合は検証者は対話の末高確率で納得し，その一方で入らない場合はどんなに証明者が手を尽くしても納得しないことを意味する．対話型証明を持つ，言い換えれば証明者との対話によって検証者が識別可能な言語のクラスは検証者単独で認識可能な言語クラスよりも一般に大きいと考えられ，実際に多項式空間で認識可能な言語クラス PSPACE と等しいことが知られている．対話型証明系はそれ自体証明という概念の計算能力的特徴付けの観点から計算量理論において重要なだけでなく，ゼロ知識証明という暗号の基礎技術を提供するために暗号の観点からも盛んな研究が行われている．

対話型証明系の重要な拡張の一つとして多証明者版対話型証明系がある．これは証明者が複数の場合であり，各証明者は他の証明者とは会話することなく検証者との通信によってゲームを進めるものである．多証明者版対話型証明系を持つ言語クラスは非決定性指数時間で認識可能な言語クラス NEXP と一致することが示されている．多証明者版量子対話型証明系は小林・松本によって提案された対話型証明系である．多証明者版量子対話型証明系における量子と古典の重要な差異は，複数の証明者が相関を事前に共有する場合である．古典の場合，事前相関を共有している場合は事前相関を共有していない場合と計算能力的に差がないのであるが，量子の場合は事前相関が量子的なため古典と違って差が出る可能性がある．小林・松本は証明者間の事前相関が多項式長の量子情報という仮定の下で，他証明者版量子対話型証明系の計算能力は NEXP で抑えられることを示した．また事前相関を持つ正直でない証明者が，対話型証明系の健全性を破る場合があることが，これまでの研究によって示されてきた．このことは事前相関が多証明者版量子対話型証明系に与える否定的な結果だと言えるが，肯定的な側面の結果はまだ知られていなかった．

我々は，事前相関が正直な証明者にどのような利点を与えるかを明らかにした．多項式会のやり取りを含む任意の k 人の証明者版量子対話型証明系が，1 回のやり取りでかつ perfect completeness（正しい言語 L の場合には確率 1 で受理する）である k+1 人の証明者版量子対話型証明系に並列化することができることを示した．また，任意の k 人の証明者版量子対話型証明系を，証明者が 1 回のコイントスの結果をブロードキャストすることを許すことで，3 回のやり取りでの k 人の証明者版量子対話型証明系に並列化できることも示した．この”public-coin”を用いる手法では，多証明者版古典対話型証明系では 1 人の証明者版古典対話型証明系と計算能力的に変わらないことが示されているので，事前相関を持った多証明者版量子対話型証明系の優位性を示す結果の一つである．

また，事前相関によって生じる，正直でない証明者による対話型証明系の健全性の破れを防ぐ研究も行った．その結果，任意の PSAPCE に属する問題が，正直でない証明者間に相関があったとしても指数的に小さい確率でしか健全性を破れない，1 回のやり取りで 2 人の対話型証明系を持っていることを示した．また，任意の NEXP に属する問題の場合は，正直でない証明者間にどんな相関があったとしても必ず健全性を保証する（つまり perfect completeness），1 回のやり取りでの 2 人の対話型証明系を持っていることも示した．

上述のような計算量解析とともに、量子非局所性の理論で出てくる Bell 不等式のモデルが多証明者版量子対話証明の 1 モデルと等価であることから、組合せ理論を適用して一般化 Bell 不等式を導出する一般的な枠組みを与えるとともに、Bell 不等式の量子破れについて半定値計画などの最適化手法を適用する展開を示した。これらにより、多証明者の量子対話型証明系が量子計算から量子非局所性まで種々の問題での数理的基礎を与え、計算量解析や非局所性解析へと発展できるというパラダイムを示した。

■　量子ネットワークコーディング

ネットワークコーディングとは，与えられたネットワーク上で複数のメッセージを効率的に送信するためのプロトコルである．図 4.2 はバタフライネットワークの例である．ネットワークコーディングは，計算能力や情報処理能力を評価する基本的な道具の一つであり，そのため量子ネットワークコーディングの研究も近年注目されてきている．古典のネットワークと量子のネットワークの大きな違いは，古典情報は複製可能であるが，任意の量子情報の複製はできない点である．そのため，一切の仮定なしにネットワークを通して任意の量子状態を効率的に送る一般的な方法は不可能であることが知られている．
我々は，付加的なリソースとしてネットワーク上の任意のノード間での自由な古典通信を許したネットワークモデルを考え，このモデル上では完全な量子ネットワークコーディングが可能であることを示した．これは，k 個の入出力ノードのペアのあるネットワーク上で古典の線形コーディング方法が存在したときに限るが，完全な量子ネットワークコーディングを達成する数少ない例となっている．また，どのくらいの古典通信があれば量子ネットワークコーディングが達成可能であるかを，ペアの個数 k に対する上限として与えた．

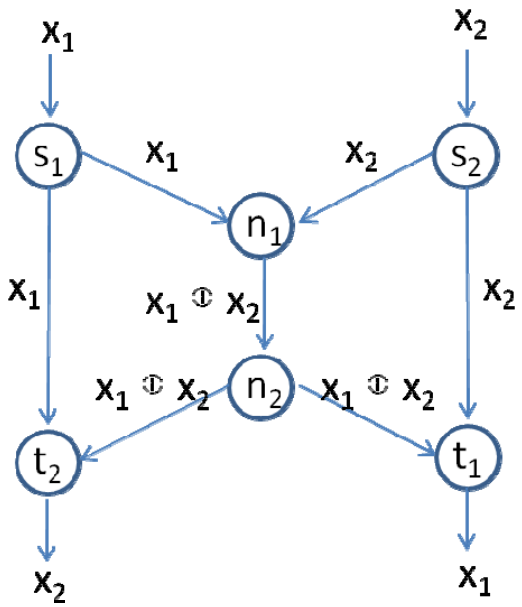


図 4.2 バタフライネットワークと古典線形コーディングの例.
ノード s_1, s_2 は入力 x_1, x_2 があるとき，x_1 を t_1 へ，x_2 を t_2 へ送るためのネットワーク．

４．２ 量子情報理論グループ　“量子鍵配送システムの開発および量子情報理論の研究”

(1)実施の内容

近年盛んに量子鍵配布のためのデバイス研究が行われているが，その安全性のためには単なる装置開発だけでは不十分であり，それを補う誤り訂正・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．多くの研究は，単一光子性の仮定や無限に大きいサイズの誤り訂正・秘匿性増強，さらには，計算量が発散する誤り訂正・秘匿性増強を仮定しており，現在実装できる現実の装置には適用できない．本当に現実の系で実現できる量子暗号システムについて厳密に安全性を示したものは本研究が初めてである．また，より効率を上げるためにはプロトコルの改良が求められる．その他，量子情報理論の側面から量子情報処理のセキュリティを多角的に捕らえるためにも関連テーマについても積極的に研究を推進した．

研究実施の具体的内容は，量子情報実験グループと協力し，前身の ERATO プロジェクトが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理論的な安全性評価を目指した．既に，誤り訂正・秘匿性増強の開発，および，我々の量子鍵配送システムに適用可能な安全性評価理論は完成し，それを用いた量子鍵配布システムの実証実験に成功した．また，改良プロトコルについてもその実証実験を行った．

また，量子セキュリティを広い立場から捉えるために，以下のような量子情報理論全般にわたる研究を行った．

①量子セキュリティの観点から量子測定について理論的研究を行い，盗聴で漏洩する情報量，伝送できる情報量，種々のエントロピー関係式やエンタングルメント測度の関係を明確にした．

②エンタングルメント支援型量子通信の理論的研究を進め，古典通信，量子通信，エンタングルメント操作などが同時にかかわる複雑な種々のプロトコルの統一的理論の構築を行った．この成果に基づき新プロトコルの提案を行う一方，ユニバーサル量子プロセッサとしての量子テレポーテーションの理論を発展させ，さらに量子 LDPC（低密度パリティ・チェック）符号を提案した．

③連続変数状態の量子エンタングルメントや量子セキュリティに関する新しい関係を明らかにし，また束縛エンタングルメントの抽出に関する理論のある種の数学的側面を解明した．

(2)得られた研究成果の状況及び今後期待される効果
本グループの成果は(i)量子鍵配布システムの開発，(ii)安全性評価，(iii)量子情報理論の 3 つに分かれる．

(i)量子鍵配布システムの開発

量子鍵配布プロトコルは、現在、量子暗号システムを実現する有力な方法の 1 つであると考えられている．しかしながら、もともとのBB84プロトコルは単一光子源を仮定しており、現実には単一光子源の代用として弱いレーザ光を用いるしかないという悩ましいギャップがあった．この単純な代用では暗号の安全性が根本的に覆されてしなうことが示されていて、この問題を回避するためにHwangやWangらによってデコイ状態法が提案されたのである．これまでのデコイ状態法の安全性解析は、無限大の符号長を仮定していたり、あるいはその結果から有限長の場合での安全性を推定したりといったものであり、最初から現実的な設定で安全性を議論したものではない．
この難点を解消すべく新しいデコイ状態法の量子鍵配布プロトコルを開発した．

このプロトコルの概要は次のようである．
一般に k+1 個の異なる平均光子数の光パルスを用いるが、2 つの基底（＋および×基底）を用いるので、都合 2k+1 個のパルスが使われる．このうち 1 つは真空状態である．
ある特定の強度のパルス i_0（i_0+k）は最終的に生成される秘密鍵を作るために用いられ、他は盗聴者あるいは通信路の性質を知るために用いられる．
まず、一定の時間に送信者は k+1 種の光パルスを、基底をランダムに選んで受信者に送る．この後、受信者は、2 つの基底のどれかで測定を行い、この結果は公開通信路を介して、送信者と受信者が共有する．基底が一致したパルス数を E_i (i=0,…,2k) と表わすことにする．この中には誤りがあるが、この数を H_i(i=1,…,2k)と書くことにすると、最終的に生成される秘密鍵の長さは、ある 1 つの基底に対して、$N\eta(H_{i0}/(E_{i0}-N))-m$ と求められる．ここで、N は符号長、η(.)は誤り訂正レートであり、m は秘匿性増強の大きさを表わす．別の基底に対しても同様である．
誤り訂正は LDPC（低密度パリティチェック）符号を用いることとする．この利点は、n を符号長として O(n)回の操作で復号できることにある．
また、秘匿性増強では、l ビットの情報から m ビットを差し引くことが必要になるが、本プロトコルでは(l-m)×l-Toeplitz 行列を用いる方法を提案した．これにより安全性評価のプロトコルが簡単になる．

(ii)安全性評価

現実的な設定の下に、安全性を評価する数値シミュレーションを行った.
まず、k+1=4 個の異なる平均光子数の光パルスを用いることにした. これは、k=3 程度が最も良い性能を示すことがわかったからである.
次に、今回開発した量子鍵配布プロトコルの性能を図 4.3 に示す. ここでは盗聴者の漏洩する情報量は 2^{-9} を超えない安全な鍵を生成したときに、$N=1.0\times10^4$、$N=1.0\times10^5$、$N=1.0\times10^6$ の 3 つの場合で評価を行った (図 4.3). この図からわかるように伝送距離 250km 程度までは送信者と受信者の間に最終的な秘密鍵を共有できることがわかる. 漸近的な場合の 250km 程度に及ばないのは有限の符号長を用いることによる揺らぎの影響である.
最後に、伝送距離 20km で、安全性パラメータ δ に対して秘密鍵の生成レートがどうなるかを調べた (図 4.4). 注目すべきは、$N=1.0\times10^6$ 程度になると、安全性パラメータを大きく取っても秘密鍵生成レートはほとんど変化しないことである. 一方で $N=1.0\times10^4$ では、安全性パラメータに対して秘密鍵生成レートは大きく減少する. これも有限の符号長を用いることによる揺らぎの影響である.

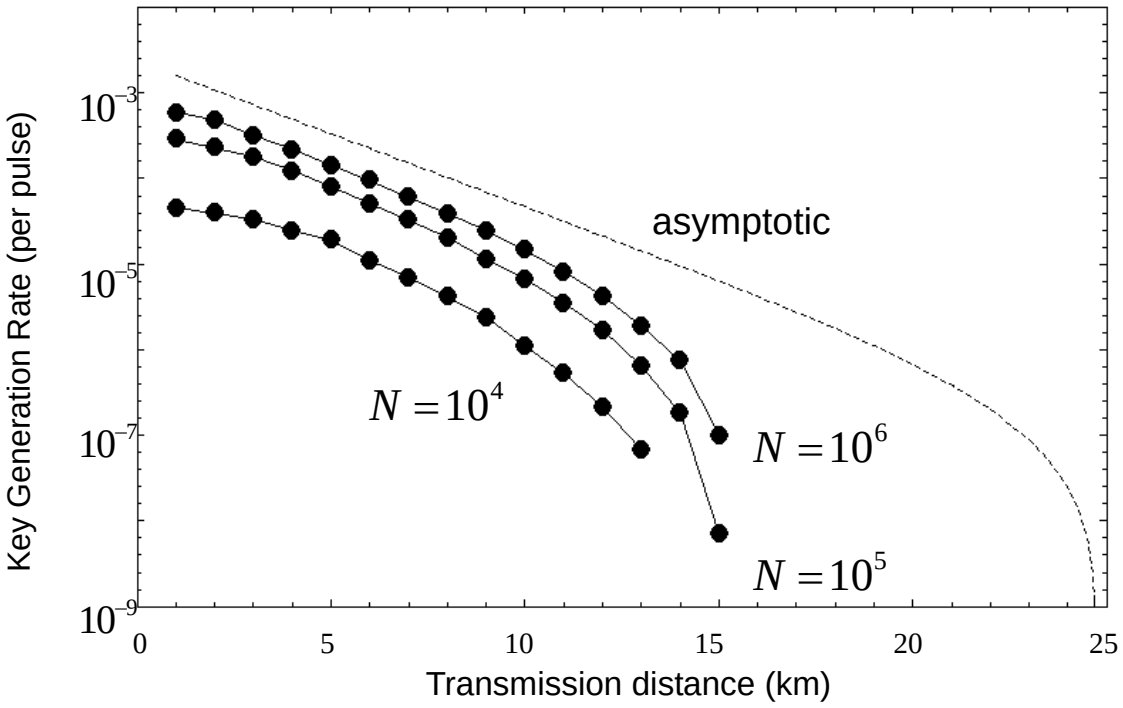


図 4.3　秘密鍵生成レートと伝送距離

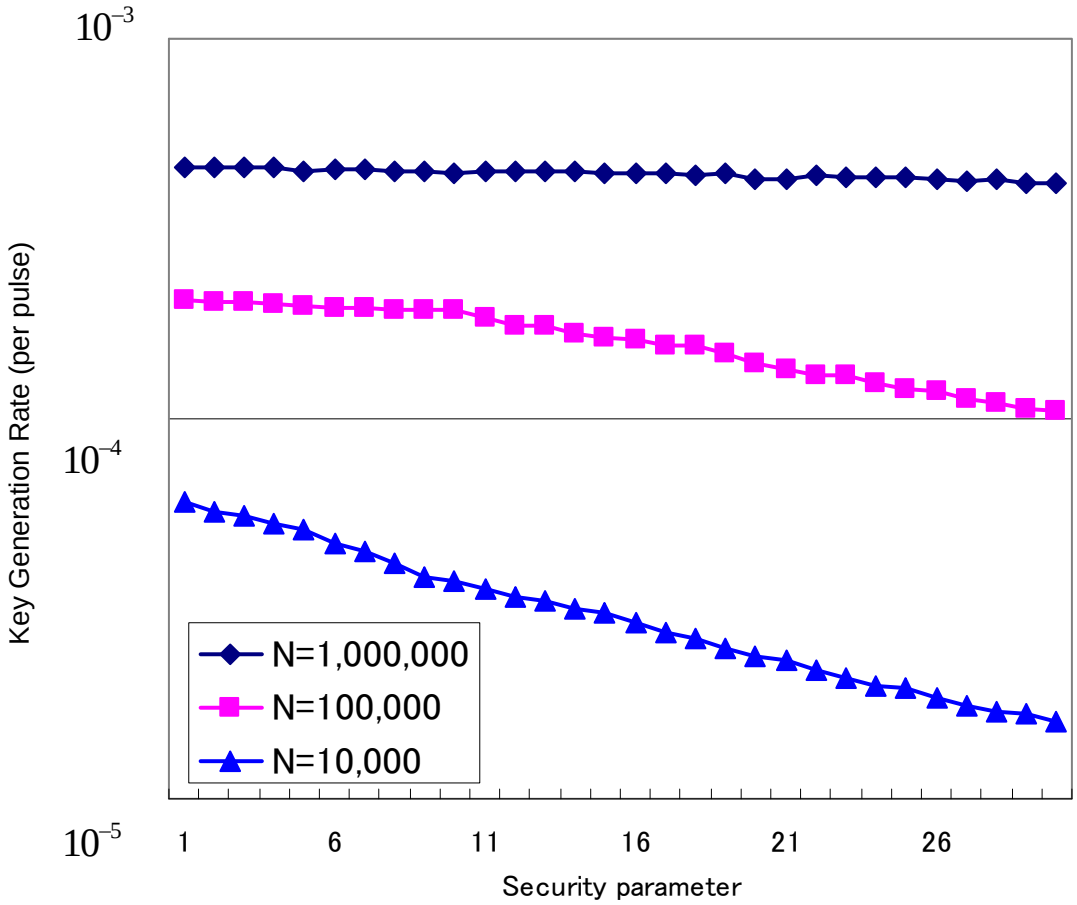


図 4.4　安全性パラメータと秘密鍵生成レート

図 4.5 鍵蒸留のためのソフトウェアを実装した量子暗号鍵配布システム

(iii)量子情報理論

■　量子エンタングルメント支援型量子通信理論

いわゆる Shannon 理論は，2 つの柱，すなわち情報源符号化定理と通信路符号化定理からなっており，これらに対応する量子版ともいうべきものは既に Schumacher，Holevo－Schumacher－Westmoreland，Lloyd－Shor－Devetak らによって得られている．一方で，量子エンタングルメントは量子情報操作における 1 つの重要な物理的リソースと考えられ，これを導入することで上の一群の量子プロトコルをさらに一般化できると考えられる．一般化というのは，単に数学的な抽象化を行うというのではなく，それによってより高いステージに立ち新天地を切り開こうとするものである．従ってこの方向での量子情報の理論的研究を強力に推進した．

量子エンタングルメント支援型量子通信路を介して古典情報および量子情報を伝送する問題を考察し，古典通信容量，量子通信容量，および量子エンタングルメント消費レートのすべての達成可能レートを与える 1 つの容量定理を得た．すなわち，古典通信容量，量子通信容量，および量子エンタングルメント消費レートからなる 3 次元空間において，1 つの通信方式（符号化）を与えたときに達成できるこれら 3 組の量のトレードオフの関係を与え，定量化することに成功した．特にこの 3 次元領域の境界点（限界点）に対応するプロトコルを古典的支援型ファーザー・プロトコルと名付けた．

量子エンタングルメントを用いた量子プロトコルとして，量子テレポーテーション，スーパーデンス・コーディング，量子エンタングルメント分配という 3 つの基本プロトコルが知られている．この 3 つの基本プロトコルを統一的に記述することに成功し，次の 2 つの結果を得た．

第 1 に，送信者と受信者がノイズのある量子エンタングルメントを任意に多く共有できるとき，上の 3 つの基本プロトコルをどのように配分すれば最適プロトコルが得られるかを示した．このプロトコルは（この研究において命名した）古典的支援型状態再配分プロトコルと上の 3 つの基本プロトコルを組み合わせたものになっている．
第 2 に，送信者と受信者がノイズのある量子通信路を任意に多く共有できるとき，ノイズのない上の 3 つの基本プロトコルを用いて最適プロトコルを構成することに成功した．これは上に述べた古典的支援型ファーザー・プロトコルと 3 つの基本プロトコルを組み合わせたものになっている．

■　量子秘匿通信

ノイズのある量子通信路と秘密鍵を用いて，ノイズのない公開通信とノイズのない秘匿通信を行うプロトコルを提案した．このプロトコルは，いわゆるランダム・コーディングと秘密鍵に守られた秘密符号を公開通信路に載せることによって得られる．これは，以前に提案されていたHsieh－Luo－Brunによる秘密鍵支援型プロトコルやDevetak－Shorによる公開・秘匿同時通信プロトコルの一般化である．

■　量子誤り訂正符号

通信路状態符号化プロトコルと呼ぶ新しいプロトコルを提案した．このプロトコルは，ノイズのある量子通信路とノイズのある量子状態を用いて，送信者と受信者の間に量子エンタングルメントを生成するもので，共有した量子エンタングルメントに対してノイズ耐性の強い量子エンタングルメント支援型量子誤り訂正プロトコルを与える．
また，古典的にはよく知られたLDPC（低密度パリティ・チェック）符号化方式を量子エンタングルメント支援型の量子LDPC符号化方式に拡張した．特に，符号長の関数として量子エンタングルメント消費量が線形に減少する非常に性質のい符号化を見い出した．これにより高性能量子誤り訂正符号を構成することができる．

以上の研究は、M.-S. Hsieh研究員（現、ケンブリッジ大）が、海外からの訪問研究者、特にM. Wildeとの研究討論を通して行ったものである．

■　ユニバーサル量子プロセッサとしての量子テレポーテーション

単純な量子テレポーテーションでは，送信者と受信者が量子エンタングルメントを共有し，プロトコルの第 1 段階で，送信者が量子エンタングルメントの自分側の部分と送りたい量子状態の合成系に量子測定を行い，プロトコルの最終段階で受信者が送信者から送られてきた古典情報をもとにユニタリー変換を行う必要がある．量子テレポーテーションは，Knill－Laflamme－Milburn によって指摘されたように（いわゆる KLM 量子計算スキーム）量子計算機の1つの構成要素と捉えることができるが,ユニタリー変換が必要になるため，ユニバーサルな量子プロセッサにはならない.

この点に関し，次のような新しい量子テレポーテーションのスキームを提案した.

すなわち，受信者が（送信者と）共有する量子エンタングルメントの N 個のポートを持っていて，送信者から送られてきた古典情報をもとに単にあるポートを選択するだけでよいというものである.

この量子テレポーテーションの解析を行い，確率論的な場合と決定論的な場合の２つについて，さらに(i)共有する量子エンタングルメントが最大エンタングルメントに固定した場合，(ii)共有する量子エンタングルメントとともに送信者側での量子測定を最適化した場合，のすべてについて解析解を得た.（いずれも N が無限大の極限で完全な量子テレポーテーションになる）先に述べたように，この新しい量子テレポーテーションのスキームは，ユニバーサル量子プロセッサとして用いることができる.

■　束縛エンタングルメントの存在問題

量子エンタングルメントは,2 者間のみで共有されるという最も簡単な場合においてすらその完全な分類はなされていない. ネックになっているのは，NPT 束縛エンタングルメントが存在するかどうかということである． NPT というのは量子エンタングルメントを記述する密度行列にある種の数学的な操作を行ったときの密度行列の性質の変化によるもので，量子エンタングルメント状態は大きく NPT 状態と PPT 状態にわかれる．一方，束縛エンタングルメントというのは，エンタングルしているにもかかわらず，そこからエンタングルメントを局所的な量子操作と古典的な通信によって抽出することができないという非常に奇妙な状態である．これまで，PPT 状態はすべて束縛エンタングルメントであるか，あるいはもともとエンタングルしていない状態であるかのいずれかであることが解明されている．一方，NPT 状態はすべて束縛していないエンタングル状態であるかは未だに解明されていない．もしこれが解明させれば，束縛エンタングルメントからの古典的秘密鍵の抽出という量子セキュリティの問題が大きく前進することになるわけで，本プロジェクトにおいても解明に注力したが，最終的な解決には至らなかった．しかしながら，この問題が意外なことにヒルベルトの第17問題というある種の数学的な問題と密接に関係していることを明らかにできた．一般に，多項式の自乗和は非負値であるが，逆に非負値の多項式を与えたときに，これがいくつかの多項式の自乗和になる場合（SOS 型）とならない場合（非 SOS 型）があり，ちょうど NPT 束縛エンタングルメントが存在するであろうと考えられるとこ

ろでは，束縛性を示す多項式が非 SOS 型になることを発見した．これは，代数幾何学的な方向での問題の解明を強く示唆している．

■　連続変数状態の量子エンタングルメント

3 者以上のパーティーに分配されたエンタングルメントには，モノガミー性（単婚性）という性質があることが示唆され，既に，離散変数状態ではこれが示されていた．これは古典情報（古典相関）とは完全に異なる量子エンタングルメント（量子相関）独特の性質で，複数のグループで十分なエンタングルメント（量子相関）が確保できれば，他への情報漏えいが無いことを示しており，量子セキュリティに有益な示唆を与える．このモノガミー性が連続変数のエンタングルメントにもあることを証明した．この成果は，連続変数状態，例えばスクイーズド状態を用いた量子暗号システムに応用できる．

■　量子測定と情報漏洩に関する理論的研究

量子測定での状態破壊と情報獲得と間のトレードオフについて，種々のエントロピー関数、例えばコヒーレント情報量や相互情報量、およびいくつかのエンタングルメント測度、特に形成エンタングル、EF に関する定量的な関係を得た．この成果は，状態破壊の程度が少ないと，盗聴者による情報獲得が少ないことを示している．これは定性的には自明ではあるが，数学的に定式化したということが重要で，これにより応用の範囲が一気に拡大する．この方向での１つの応用として、1 対 3 位相共変型量子クローン生成機による BB84 量子鍵配布における盗聴実験の提案があり、これは量子情報実験グループとの共同研究である．この研究は F. Buscemi 研究員（現、名古屋大学）が行い、ERATO-SORST として国際交流の１つの重要な成果の１つである．

４．３ 量子情報実験グループ

(1)実施の内容

①研究のねらい

量子情報実験グループは光子を用いた量子情報システムの構築を目指して，そのための基盤技術の確立，量子プロトコルの実証実験を行う．本プロジェクトの特徴は理論と実験との有機的な結合であって，そのために理論グループの成果に立脚した実証実験を行うと共に，理論グループに対しても実験と理論のギャップを埋めるべく，実現可能性，実現の意義などを提言していく．テーマとしては(i)量子暗号システム，(ii)光子を用いた量子プロトコル実証，(iii)エンタングル光子対,(iv)量子ゲートに注力する．

特に，量子鍵暗号システムにおいては，現実的な設定のもとで安全なシステムの構築を目指す．このために必要なハードウェアについての研究を進め，理論グループの成果であるソフトウェアを実装して実証実験を行う．また，ERATO プロジェクトで提案された匿名量子リーダ選挙問題を解くアルゴリズムの実証を行う．

さらに，高度な量子情報システムの構築のため，エンタングル光子対の生成と制御，測定とエンタングル光子対の応用についても研究を行う．また，光子を入出力とする量子ゲート次元のための理論研究を進める．具体的には量子ドットなどで実現される原子系と光子の相互作用の制御とそれを利用したデバイスを提案し，性能の見積もりを行う．

②研究実施方法

量子情報実験グループは日本電気(株)筑波研究所内に専用スペースを賃借して研究を進めている．量子情報処理の実現に向けた実証実験では理論との連携が不可欠であり，東京オフィスの量子情報理論グループ・量子コンピューティンググループとは密接に連絡を取り合って研究を進めている．同時に，材料・デバイスも量子情報処理に向けて，これまで以上の性能向上や新しい概念に基づくデバイスの開発が必要である．これについては日本電気(株)基礎･環境研究所（現グリーンイノベーション研究所）と共同研究契約を結び，光子検出器，量子ドットデバイス，量子暗号装置について協力して研究を行った．

(2)得られた研究成果の状況及び今後期待される効果

(i)量子暗号鍵配布システム

量子情報理論グループが開発した安全性が定量的に保証できる量子暗号鍵配布ソフトウェアを実際に使用するため，量子通信装置の改良を行った．半導体レーザ光（弱コヒーレント光）を光源とするため，デコイ法を用いることが必要であり，このためには量子通信に用いる光の強度をパルスごとにランダムに変調することが要求される．今回用いた往復型（プラグ&プレイ）の装置に適用できる変調法を開発し，実際真空を含む 4 種類の強度での送信を行った．なお，量子通信装置の改良は NEC と共同で行い，NEC 製の装置を基本にしている．量子通信装置にプログラムを実装し，リアルタイムに安全な量子暗号鍵を

生成することに成功した．量子通信を行って得た生鍵を用いて誤り訂正，秘匿性増強を含むソフトウェアを実行し，漏洩情報量が 2^{-9} 以下という条件で暗号鍵生成レート 200b/s を得た．盗聴者に漏洩した情報量の上限を定量的に保証した量子暗号鍵を実際に生成したのは世界で初めてである．

(ii)量子リーダ選挙プロトコルの実証

リーダ選挙問題を解く量子プロトコルは ERATO プロジェクトにおいて量子コンピューティンググループの谷らによって初めて与えられた．本プロジェクトでは線形光学素子による実装を行った．まず，2 者間の量子リーダ選挙プロトコルはエンタングル光子対と線形光学素子で確定的に実行できることを示した．一般に線形光学素子を用いた量子ゲートは確率的にしか動作しないが，量子リーダ選挙問題では通常失敗とみなされる事象でもリーダの判定に用いることができる．真空と 1 光子状態を qubit として 2 光子干渉計による実験を構成して量子リーダ選挙プロトコルを実行したところ, 95.7%の確率でリーダが決定され，プロトコルの実証に成功した．

装置の不完全性がある場合，厳密な意味での確定的動作はできなくなるが，この時の性能指標として，リーダが決まるまでに必要な通信量の期待値を用いることを提案した．2 者間古典プロトコルでは最適なプロトコルにおいても 4bit の通信が必要であるのに対して，装置が完全であることが分かっている量子プロトコルでは 2bit，不完全性があるかもしれない場合には装置が完全であるとき 3bit の通信でリーダが選べることを示した．つまり，装置が完全であることを知っていることは 1bit 分の知識であることが分かる．このことから，装置が不完全な場合でも量子プロトコルは古典プロトコルに対して 1bit 優位性があることが明らかになった．本実験で見積もられた必要な通信量の期待値 3.13bit となり，装置が完全なものに近いことが示された．

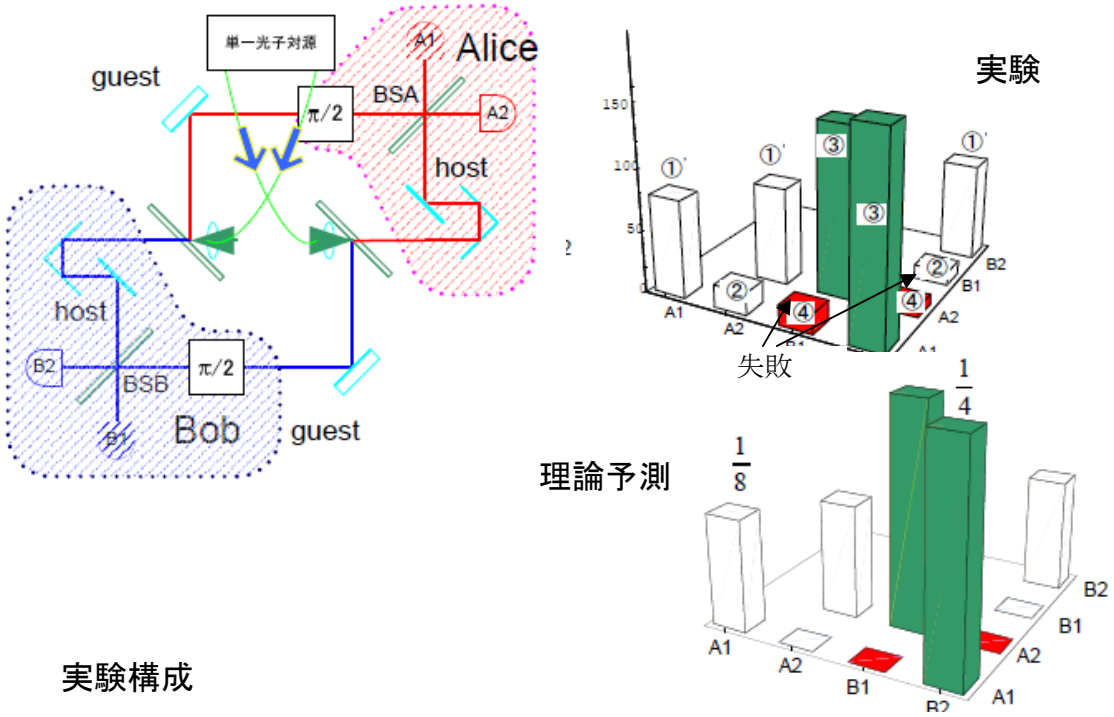


図 4.6. 量子リーダ選挙アルゴリズムの実証実験：実験構成図，理論予測，実験結果

(iii)エンタングル光子対発生と応用

① 周期分極 $LiNbO_3$（ニオブ酸リチウム）結晶(PPLN)を用いたエンタングル光子対光源を開発した．周期の異なる PPLN を集積し，それぞれ第二高調波発生とパラメトリックダウンコンバージョンに用いることで 1.55μm 帯のレーザ光源から 1.55μm 帯の偏光エンタングル光子対を得た．

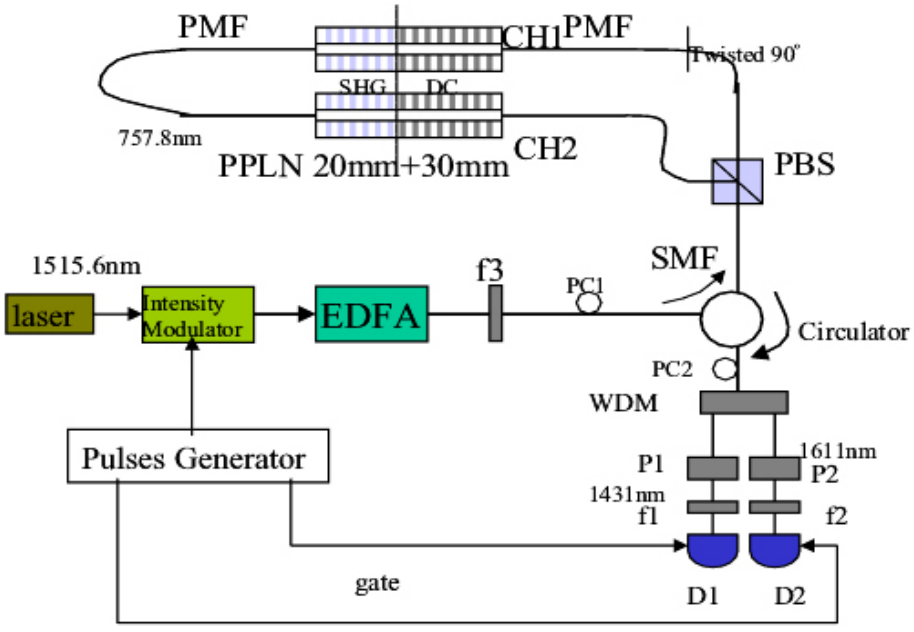


図 4.7　偏光エンタングル光子対光源の構成図

② 2 光子干渉を用いて混合状態の幾何学的位相の非対角成分を観測した.

③ PPLN 結晶による光子対発生と干渉計による時間差-偏光変換装置を開発した．これにより，波長が 800nm と 1550nm の光子の偏光と位相がエンタングルする 2 波長異自由度ハイブリッドのエンタングル光子対光源を実現した．この成果は NEC と(独)情報通信研究機構との共同研究による.

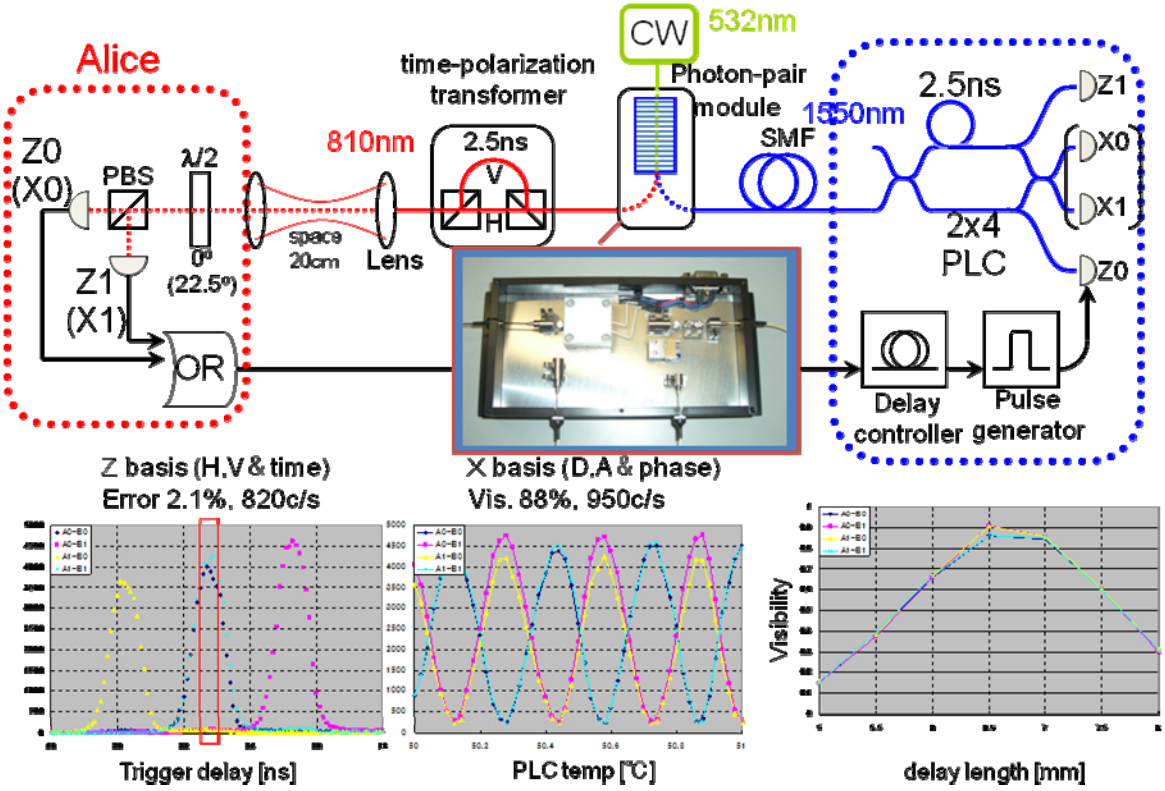


図 4.8　2 波長ハイブリッドエンタングル光子対光源の構成図と実験結果

(iv)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行った．特に原子と共振器が結合した系について検討し，光子到着の量子非破壊測定デバイスを解析した. また, 量子位相シフトゲートに基づくパリティチェックゲートとそれを用いた Bell 測定装置を考案し特許出願した.

(v) アバランシェフォトダイオード（ＡＰＤ）を用いた光子検出器

光子検出器は 1 光子レベルの微弱な光を検出可能な装置である．量子情報科学の分野においては，量子暗号，光を用いた量子計算，量子通信には必須の装置である．また，単一原子，単一分子，量子ドットからの微弱発光測定や，癌診断の装置として注目が集まっているＰＥＴ（ポジトロン断層法，positron emission tomography）への適用にむけた研究も行われており，他分野においても重要な装置となっている.

光子検出器の種類としては，従来から用いられてきている光電子増倍管や，最近では超伝導素子を用いたものなど，様々なものが存在する．なかでも，半導体受光素子であるアバランシェフォトダイオード（ＡＰＤ）を用いた光子検出器は，大量生産可能，小型化・

集積化が可能などメリットは大きい．ＡＰＤで光子を検出するためには，ＡＰＤに対して，ブレークダウンを引き起こす電圧を印加しておく．光子入射によりブレークダウンが引き起こされ，ブレークダウンにより発生した電流を測定することで光子入射イベントが検知可能となる．この方法はガイガーモード動作と呼ばれ，現在市販されているＡＰＤ光子検出器はこの方法を用いている．しかしながら，ガイガーモード動作に起因する問題が複数存在し，ＡＰＤ光子検出器の性能を抑制している．上述の背景から，ガイガーモード動作以外の方法による光子検出や，ＡＰＤアレイを用いることで，ＡＰＤ性能の大幅な改善はもとより，質的な改善をも視野にいれ，研究を行った．

①┌サブ･ガイガーモード動作によるＩｎＧａＡｓ　ＡＰＤ光子検出器の開発

ＩｎＧａＡｓ　ＡＰＤは通信波長帯に感度を持つＡＰＤである．現在，量子暗号や量子通信実験において用いられている．ＩｎＧａＡｓ　ＡＰＤの暗電流は印加電圧の増加により急増する．ガイガーモードで使用した場合，光子入射によらないブレークダウンのイベントが大量に発生してしまう．このことを回避するため，現在は光子の入射タイミングに

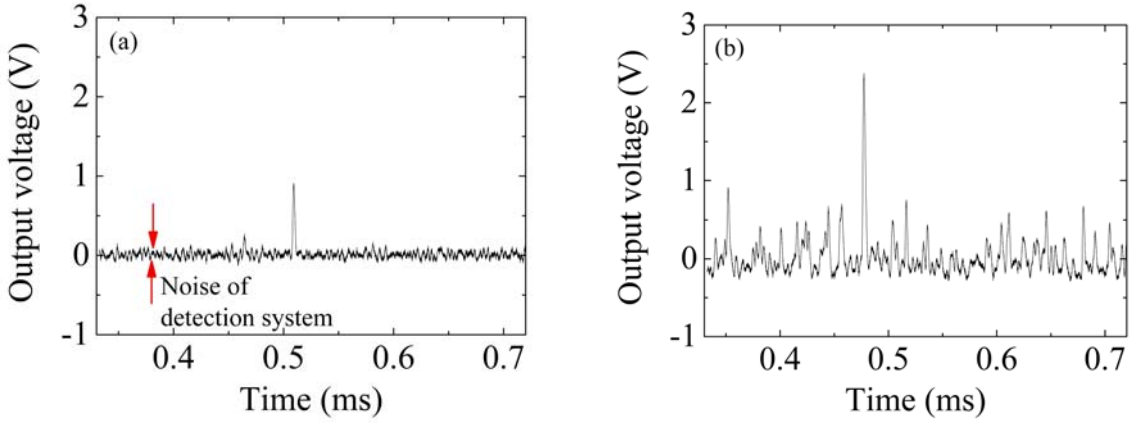


図 4.9　サブ･ガイガーモード動作 InGaAs APD からの出力波形。(a)は光子が入射していない場合、(b)は連続波レーザを光子レベルまで減光し入射した場合のもの。ランダムなタイミングで到来する光子を検出している。

合わせて，ＡＰＤ自体に電圧を印加している．この方法では，非同期に到来する光子には対応ができない．また，光子の入射するタイミングが短くなるほど，同期が困難となる．我々はＡＰＤをサブ・ガイガーモード動作させることで，この問題を克服した（図 4.9 参照）．サブ･ガイガーモードとは，ＡＰＤにブレークダウン電圧以下の電圧を印加して光子を検出する手法である．サブ・ガイガーモードでＡＰＤを低電圧で駆動することにより，暗電流が低下し上述の問題が克服できる．ただし，光子入射により発生した光電流も低下するため，ＡＰＤ後段には高い信号対雑音比をもつ電荷積分アンプを使用した．この成果により，信号と検出器の同期が必要でないため，量子暗号システムの低コスト化につながると期待している．

② サブ･ガイガーモード動作によるＳｉ　ＡＰＤ光子検出器の開発

光を用いた量子計算や量子通信では，光子検出器の光子検出効率がそのまま，成功確率に直結する．したがって，光子検出効率に対する下限値が存在する．例えば，完全な量子もつれ合いの実験をするためには，最低でも検出効率が 83%以上必要である．ＡＰＤ光子検出器の光子検出効率は，シリコン素材のＡＰＤ（Ｓｉ　ＡＰＤ）において 76%という値が報告されている．ＡＰＤの検出効率は，量子効率と光電子検出確率の積で表される．量子効率は，光子がＡＰＤ内部で光電子に変換される効率である．光電子検出確率は発生した光電子の検出の成功確率である．Ｓｉ　ＡＰＤでは量子効率は原理上ほぼ 100%を達成可能である．一方で光電子検出確率は，ＡＰＤ自体の性能向上，使用する増幅器の性能によって左右される．現状では８０%程度であり，この値は 1990 年代前半から改善はない．光電子検出確率を向上させるためには，ＡＰＤ後段の電気回路の低雑音化と高増幅率化が必要となる．我々は 1 電子を数 V にまで増幅可能で，かつ，そのときの入力換算雑音が平均 4 電子であるといった，超低雑音電荷積分アンプの開発に成功している．しかしこのアンプは大量の電流が流れることで，出力が飽和してしまうため，接続するＡＰＤはサブ・ガイガー動作させることが必要となる．我々は，調停雑音電荷積分アンプを使用することで，光電子検出確率を約 90%に向上させることに成功した. また, 浜松ホトニクス社と共同で，量子効率が 90%以上を達成するＳｉ　ＡＰＤの開発にも成功している．これらの成果により，光子検出効率を 80%以上にまで高めることが可能となる．

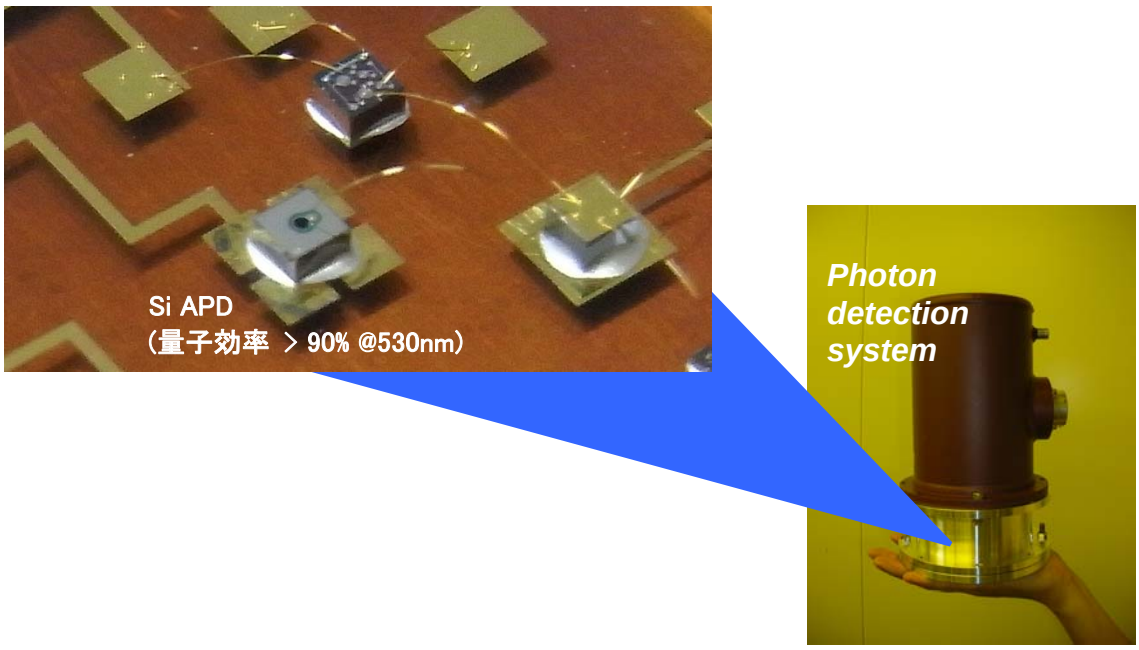


図 4.10　開発した光子検出器システム

③ ＡＰＤ光子検出器のＰＯＶＭに関する研究

光子検出器による測定を Positive Operator Valued Measure(POVM)として定式化することで，実験の予測などが可能である．光子検出の成功を $\mathbf{\Pi}_{\mathrm{on}}$，光子検出の失敗を $\mathbf{\Pi}_{\mathrm{off}}$ とすると，一般的に光子検出器の POVM は以下のように表される．

$$\mathbf{\Pi}_{\mathrm{off}} = \sum (1-P_d)^n |n\rangle\langle n|, \quad \mathbf{\Pi}_{\mathrm{on}} = \hat{\mathbf{I}} - \mathbf{\Pi}_{\mathrm{off}}$$

ここで，n は光子検出器に入射する光子数であり，P_d は単一光子検出効率，$\hat{\mathbf{I}}$ 単位行列である．しかしながら，全ての光子検出器が上述の POVM で表現できるかは自明ではない．特に，ＡＰＤ光子検出器は，複数個の光子が同時入射した場合の効率を，単純に単一光子検出効率だけで表せない．我々はＡＰＤの光子検出過程を考慮した POVM を導出し，従来の POVM との比較を行った．その結果として，一般的構造である reach-through APD において，導出した POVM と従来の POVM では光子数が多くなるほど違いが顕著になった．一方で，Superlow-k APD ではその差は見られなかった．また，印加電圧の上昇に伴い，二つの POVM の差は減少する．この成果により，ＡＰＤ光子検出器の POVM の詳細な定式化することで，より正確な実験結果の予測が可能となる．

５．類似研究の国内外の研究動向・状況と本研究課題の位置づけ

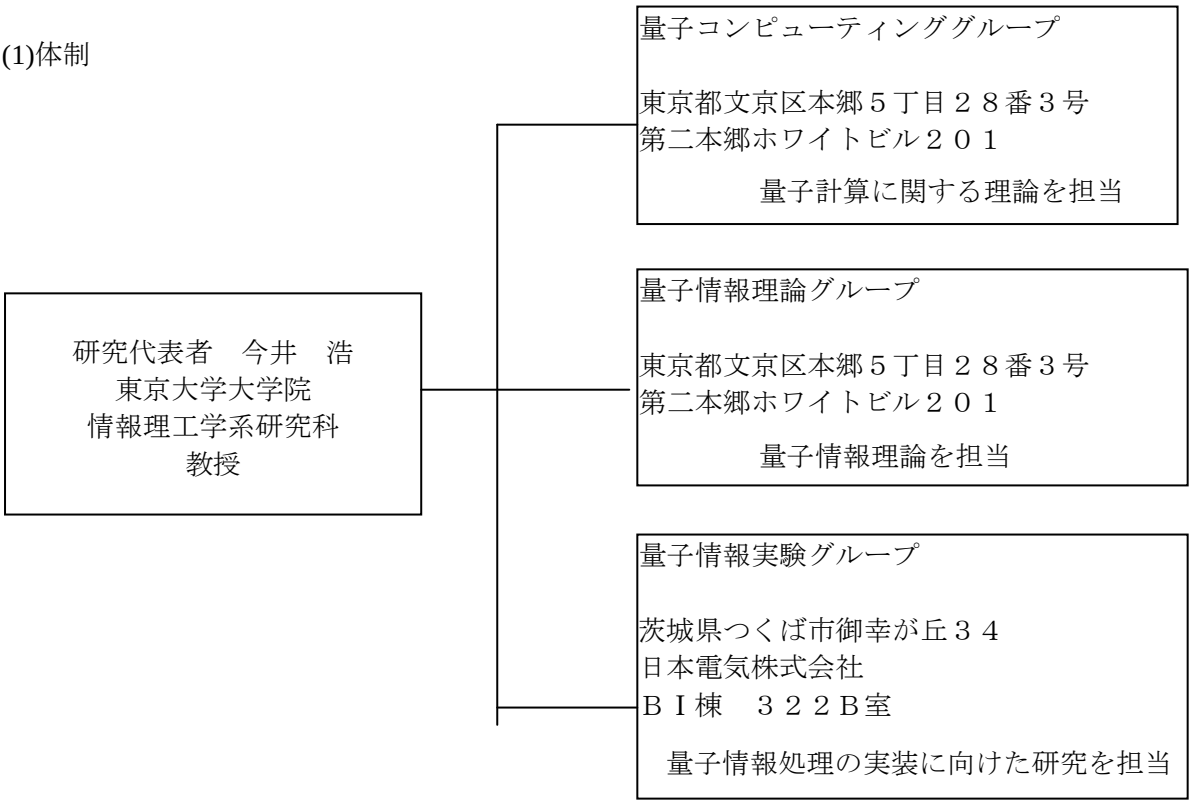
量子情報システムの構築を目指して理論と実験が有機的に結合した本プロジェクトは世界的にもユニークな存在である．もちろん，複数の研究機関が参加するプロジェクトは多いが，それらは独立な研究グループの集合であって，グループ間の活動の相乗効果はあまり大きいとはいえない．欧米の大学には理論と実験の研究者を集めたグループもあるが，アクティビティは一般にリーダの関心の範囲にとどまり，本プロジェクトのように量子情報理論，量子計算理論と実験グループが広い分野をカバーできるものはまれである．量子コンピューティンググループと量子情報実験グループが共同して行った量子リーダ選挙, 3 グループの共同で行った量子暗号鍵配布システムの開発はそのよい例である．

以下，本プロジェクトの大きな成果である弱コヒーレント光を用いた量子鍵配布の安全性研究について述べる．Hwang により decoy 法が提案され，前身の ERATO での我々の研究と Toronto の Lo のグループにより，漸近的な伝送レートに関する研究がなされている．しかし，不完全な光子源を用いた有限長の符号の下での安全性の議論は他の研究グループではほとんどなされておらず，わずかに，Inamori-Lutkenhaus-Mayers による結果があるのみである．また，この成果による伝送レートには向上させる余地が複数あり，この成果を用いても十分な伝送距離が得られない．最近この他にも現実のデバイスの不完全性を考慮した安全性の解析の研究が現われ, 大筋では我々と同様の結果が得られており, 我々が考えている方向へ議論が収束しつつある．装置実証に関しても，実際に有限の鍵について定量的な安全性を保証したのは我々の実験が最初である．量子暗号鍵配布の研究は，実用化を意識したものにシフトしており，その中で我々が現実的な設定の下での安全性保証を行ったことは重要な成果であると考えられる．我々の結果に触発されて，諸外国でも現実的な条件を課した安全性解析の研究が一つのトレンドとなっている．しかしながら，本プロジェクトのように理論と実験が真摯に対話してシステムを作り上げていくという体制をとっていないため，欧米での実験レベルでの安全性保証は比較的低いレベルにとどまっている．これに対して，日本では本プロジェクトの成果をもとに NEC，三菱電機，NTT の 3 者が(独)情報通信機構の委託研究で安全性保証を行った量子暗号鍵配布装置の開発を進めており，今秋東京都内で量子暗号通信ネットワークが稼働を開始する．

各グループが行った研究でも世界的な研究の流れを作ったものが数多くみられる．例えば，量子分散計算は ERATO プロジェクトから本プロジェクトの一つの中心的課題であったが，本プロジェクトで行った解析を発展させた研究がいくつか発表されている．多証明者版量子対話型証明を用いた量子計算量と量子非局所性の解析では、分野を先導した多証明版の提案と解析の成果の重要性が近年認められてきているのも、本プロジェクトによる先駆的理論研究の一例となっている。

６．研究実施体制

(1)体制



(2)メンバー表

①研究総括

氏　名	所　属	役　職	研究項目	参加時期
今井（いまい）　浩（ひろし）	兼務: 東京大学大学院情報理工学系研究科 教授	研究総括	総括・管理	平成 17 年 10 月～

①量子コンピューティンググループ

氏　名	所　属	役　職	研究項目	参加時期
松本（まつもと） 啓史（けいじ）	兼務: NII, 量子コンピューティング研究部門,助教授	グループリーダー	・量子分散計算 ・暗号に関する量子計算の応用 ・量子アルゴリズム	平成 17 年 10 月～
谷（たに） 誠一郎（せいいちろう）	兼務: NTT コミュニケーション科学基礎研究所, 研究主任	ＪＳＴ研究員	・量子分散計算	平成 17 年 10 月～ 平成 21 年 9 月

Le Gall Francois	派遣先	①非常勤技術員 ②ＪＳＴ研究員	・量子分散計算 ・量子アルゴリズム	①平成 17 年 10 月～ 平成 18 年 3 月 ②平成 18 年 4 月～ 平成 21 年 11 月
Wang Xiang Bin	派遣先	ＪＳＴ研究員	・暗号に関する量子計算の応用	平成 17 年 10 月～ 平成 18 年 5 月
菊地 洋右	派遣先	ＪＳＴ研究員	・暗号に関する量子計算の応用 ・量子アルゴリズム	平成 17 年 10 月～ 平成 18 年 3 月
山上 智幸	派遣先	ＪＳＴ研究員	・暗号に関する量子計算の応用	平成 17 年 10 月～ 平成 18 年 3 月
長谷川 淳	東京大学情報理工学系研究科　コンピュータ科学専攻博士課程	①研究補助員Ｐ ②ＪＳＴ非常勤研究員 ③ＪＳＴ研究員	・暗号に関する量子計算の応用 ・量子アルゴリズム	①平成 17 年 10 月～ 平成 18 年 3 月 ②平成 18 年 4 月～ 平成 20 年 3 月 ③平成 22 年 4 月～
西鳥羽 二郎	東京大学情報理工学系研究科　コンピュータ科学専攻修士課程	研究補助員Ｐ		平成 17 年 10 月～ 平成 19 年 3 月
乾 義文	東京大学情報理工学系研究科　コンピュータ科学専攻修士課程	研究補助員Ｐ	量子アルゴリズム	平成 17 年 10 月～ 平成 19 年 3 月
浅田 益仁	東京大学情報理工学系研究科　コンピュータ科学専攻修士課程	研究補助員Ｐ		平成 18 年 8 月～ 平成 19 年 9 月
永岡 悟	東京大学情報理工学系研究科　コンピュータ科学専攻修士課程	研究補助員Ｐ		平成 18 年 8 月～ 平成 20 年 3 月
小島　晃司	東京大学情報理工学系研究科　コンピュータ科学専攻修士課程	研究補助員Ｐ		平成 19 年 4 月～ 平成 21 年 3 月
徳田　優	東京大学情報理工学系研究科　コンピュータ科学専攻修士課程	研究補助員Ｐ		平成 19 年 4 月～ 平成 21 年 3 月
小林　弘忠	国立情報学研究所 専任研究員	客員研究員（研究補助員Ｐ）	・量子計算理論 ・量子計算アルゴリズム	平成 20 年 5 月～ 平成 22 年 3 月

美添（よしぞえ） 一樹（かずき）	派遣先	ＪＳＴ研究員	・量子暗号秘匿性増強の数値的解析 ・大規模行列演算による量子計算シミュレーション	平成 20 年 4 月～ 平成 22 年 5 月
Josef（ヨセフ） Sprojcar（シュプロイサル）	派遣先	ＪＳＴ研究員	・量子セキュリティ理論	平成 21 年 6 月～ 平成 22 年 6 月
鍾（ちょん） 啓源（かいゆん）	派遣先	①研究補助員Ｐ ②ＪＳＴ研究員	・量子セキュリティ解析	①平成 21 年 11 月～ 平成 22 年 1 月 ②平成 22 年 1 月～ 平成 22 年 6 月
夫（ふ） 紀恵（のりえ）	東京大学情報理工学系研究科　コンピュータ科学専攻博士課程	研究補助員Ｐ		平成 21 年 5 月～
青島（あおしま） 良一（よしかず）	東京大学情報理工学系研究科　コンピュータ科学専攻修士課程	研究補助員Ｐ		平成 22 年 2 月～
佐藤（さとう） 貴彦（たかひこ）	東京大学情報理工学系研究科　コンピュータ科学専攻修士課程	研究補助員Ｐ		平成 22 年 6 月～

②量子情報理論グループ

氏　名	所　属	役　職	研究項目	参加時期
林（はやし） 正人（まさひと）	派遣先	ＪＳＴ研究員（グループリーダー）	・量子暗号鍵配布システム・安全性評価 ・量子測定理論	平成 17 年 10 月～ 平成 19 年 8 月
廣嶋（ひろしま） 透也（とおや）	兼業: NEC, ナノエレクトロニクス研究所 主任研究員	ＪＳＴ研究員 グループリーダー	・量子暗号鍵配布システム・安全性評価 ・エンタングルメント理論	平成 17 年 10 月～
竹島（たけしま） 比呂子（ひろこ）	派遣先	研究補助員		平成 17 年 12 月～
Francesco（フランチェスコ） Buscemi（ブシェーミ）	派遣先	ＪＳＴ研究員	・量子測定理論	平成 18 年 5 月～ 平成 20 年 10 月

謝（シエ）　明修（ミンシュウ）	派遣先	ＪＳＴ研究員	・量子符号理論 ・量子通信路容量理論	平成 20 年 11 月～ 平成 22 年 9 月
Vorapong（ボラポン） Suppakit-（スッパキット・） paisarn（パイサーン）	東京大学情報理工学系研究科　コンピュータ科学専攻博士課程	研究補助員Ｐ		平成 21 年 5 月～

③量子情報実験グループ

氏　名	所　属	役　職	研究項目	参加時期
富田（とみた） 章久（あきひさ）	兼業: 北海道大学大学院情報科学研究科 教授	連絡調整担当（技術参事） グループリーダー	・量子暗号システム ・光子を用いた量子プロトコル実証 ・エンタングル光子対	平成 17 年 10 月～
Yun Kun（ユンクン） Jiang（ジャン）	派遣先	ＪＳＴ研究員	・エンタングル光子対	平成 17 年 10 月～ 平成 20 年 1 月
小島（こじま） 邦裕（くにひろ）	派遣先	ＪＳＴ研究員	・量子ゲート	平成 17 年 10 月～ 平成 21 年 3 月
大久保（おおくぼ）雄太（ゆうた）	筑波大学大学院数理物質科学研究科物質創成先端科学専攻博士課程後期	研究補助員Ｐ	・光子を用いた量子プロトコル実証	平成 18 年 4 月～ 平成 22 年 3 月
辻野（つじの）　賢治（けんじ）	派遣先	ＪＳＴ研究員	・高効率光子検出の実証	平成 21 年 4 月～

７．研究期間中の主な活動

(1)ワークショップ・シンポジウム等

年月日	名称	場所	参加人数	概要
2006 年 5 月 11-12 日	Joint meeting of ERATO-SORST QCI Project & NEC Tsukuba Research Laboratory	ＮＥＣ 筑波研究所	１９名	共同研究相手先の一つである NEC の量子譲歩研究者と最新研究成果につて意見交換を行う
2007 年 6 月 18-19 日	第１回京都懇話会	みやこめっせ 第一会議室	２０名	ERATO プロジェクトにより形成された人的ネットワークを有効活用し量子情報分野の研究討論を行うことで、ERATO での成果を現在の SORST プロジェクトにて更なる発展を目指す
2008 年 1 月 11-12 日	第２回京都懇話会	メルパルク京都	２５名	
2010 年 3 月 8 日	2010 International Workshop on Quantum Information Science	東京大学 弥生講堂アネックス	３２名	量子情報科学分野の最近の研究状況を内外研究者と共に討議する
2010 年 8 月 27-31 日	AQIS'10 10th Asian Conference on Quantum Information Science	東京大学 27 日 小柴ホール 28-31 日 弥生講堂・一条ホール／アネックス	１９４名	27 日 Tutorial 28-31 日 AQIS 量子情報科学分野の内外の研究者による講演及びＰＪの 5 年間の研究成果報告

(2)招聘した研究者等

氏名(所属, 役職)		招聘目的	滞在先	滞在期間
Dr. Francesco Buscemi	Pavia University	面接	旅館鳳明館	2005/1/16-2006/1/18
Dr. Mattew Leifer	University of Bristol	面接	ホテルフォーレスト本郷	2005/2/6-2006/2/8
Dr. Anirban Roy	The Abdus Salam International Center for Theoretical Physics	面接	ホテルフォーレスト本郷	2005/2/8-2006/2/10
Dr. Adel Bririd	University of Cambridge	面接	ホテルフォーレスト本郷	2005/2/13-2006/2/15
Dr. Elham Kashefi	Oxford University	セミナー	勝太郎旅館	2005/2/20-2006/2/24
Prof. David Avis	McGill University	共同研究打ち合わせ	ウィークリーマンション	2006/4/3-2006/4/28
Dr. Michal Horodecki	Department of Mathematics and physics, University of Gdansk	セミナー・研究打ち合わせ	ホテル東横イン文京区役所前	2006/11/22-2006/11/28
Prof. Giacomo Mauro D'Ariano	Quantum Oprics and Information Group (QUIT) of the Instituto Nazionale di Fisica della Materia (INFM) at Pavia	セミナー・研究打ち合わせ	ホテルフォーレスト本郷	2006/12/5-2006/12/7
Prof. Jozef Gruska	Masaryk University, Faculty of informatics	研究打ち合わせ	勝太郎旅館	2007/1/27-2007/1/31
Dr. David Bremner	New Brunswick University, Dept. of Mathematics and Statistics	セミナー・研究打ち合わせ	山上会館	2007/4/17-2007/4/24
Prof. David Avis	McGill University	セミナー・研究打ち合わせ	マンスリーマンション	2007/12/6-2007/12/28

Prof. Rahul Tripathi	サウス･フロリダ大学	セミナー・研究打ち合わせ	旅館鳳明館	2007/12/13-2007/12/14
Prof. Andrew Childs	Department of Combinatorics & Optimization and Institute for Quantum Computing, University of Waterloo, Assistant Professor	セミナー・研究打ち合わせ	フォーレスト本郷	2008/1/28-2008/1/29
Dr. Damian Markham	Paris University	セミナー・研究打ち合わせ	東横イン・旅館鳳明館	2008/1/28-2008/2/9
Prof. Wang Xiangbin	清華大学　物理系・教授	セミナー・研究打ち合わせ	サクラハウス（蔵前）	2008/1/21-2008/2/20
Dr. Giulio Chiribella	Quantum Information Theory Group, Pavia University, ポスドク研究員	セミナー・研究打ち合わせ	東横イン	2008/2/17-2008/2/21
Prof. Wang Xiangbin	清華大学　物理系・教授	セミナー・研究打ち合わせ	サクラハウス（リケン）	2008/5/20-2008/5/26
Dr. Dagomir Kaszlikowski	National University of Singapore	セミナー・研究打ち合わせ	機山館	2008/6/10-2008/6/17
Ms. Qin Wang	Royal institute of technology	面接	旅館鳳明館・ホテルグランド東雲	2008/6/23-2008/6/27
Mr. Min-Hsiu Hsieh	University of Southen California, Research Assistant	面接	機山館	2008/6/24-2008/6/28
Mr. Kavan Modi	KTH Royal institute of technology	面接	R&B 上野	2008/07/30-2008/08/01
Mr. Troy Lee	Columbia University	面接	澤野や旅館	2008/11/23-2008/12/05
Prof. David Avis	McGill University	セミナー・研究打ち合わせ	マンスリーマンション	2009/2/2-2009/2/27

Prof. Andrei Khrennikov	Sweeden Vaxjo Univ	セミナー		2009/ 3/27
Prof. David Avis	McGill University	セミナー・研究打ち合わせ	マンスリーマンション	2009/11/30- 2010/1/22
Dr. Cedric Beny	National University of Singapore	セミナー		2009/ 12/1
Dr. Mark Wilde	McGill University	セミナー・研究打ち合わせ	マンスリーマンション	2010/2/15- 2010/3/16
Prof. Shengmei Zhao	南京郵電大学	セミナー・研究打ち合わせ	東横イン文京区役所前	2010/2/21- 2010/3/21
Dr. David Wineland	Time and Frequency Division, National Institute of Standards and Technology	AQIS10 基調講演	東京ドームホテル	2010/8/26- 2010/8/30
Prof. Andrew C.-C. Yao	Institute for Theoretical Computer Science, Tsinghua University	AQIS10 基調講演	東京ドームホテル	2010/8/26- 2010/8/31
Prof. Dagmar Bruss	Heinrich-Heine-Universita t Dusseldorf, Institut fur Theoretische Physik III	AQIS10 招待講演	東京ドームホテル	2010/8/26- 2010/9/15
Prof. Harry Buhrman	Computer Science, University of Amsterdam / CWI	AQIS10 Tutorial/ 招待講演	フォーレスト本郷	2010/8/26- 2010/9/2
Dr. Bill Coish	Institute for Quantum Computing, University of Waterloo	AQIS10 招待講演	東京ドームホテル	2010/8/25- 2010/9/1
Prof. Jonathan P. Dowling	Quantum Science and Technologies Group, Department of Physics and Astronomy, Horace C. Hearne Jr. Institute for Theoretical Physics, Louisiana State University	AQIS10 招待講演	フォーレスト本郷	2010/8/26- 2010/8/31
Dr. 中村　泰信	NEC グリーンイノベーション研究所	AQIS10 招待講演	フォーレスト本郷	2010/8/27- 2010/8/31

Dr. Maarten Van den Nest	Max-Planck-Institut für Quantenoptik	AQIS10 招待講演	ANNEX 勝太郎旅館	2010/8/24-2010/9/1
Dr. Charles Bennett	IBM Research	AQIS10 Tutorial 講演	フォーレスト本郷	2010/8/24-2010/9/1
Prof. Richard Jozsa	DAMTP, Centre for Mathematical Sciences, University of Cambridge	AQIS10 Tutorial 講演	フォーレスト本郷	2010/8/25-2010/8/31
Prof. Jozef Gruska	Faculty of Informatics Masaryk University	AQIS10 Committee Chair	ANNEX 勝太郎旅館	2010/8/26-2010/9/2
Dr. Mark Wilde	McGill University	AQIS10 Long Talk セミナー 研究打ち合わせ	マンスリーマンション	2010/8/10-2010/9/2

８．発展研究による主な研究成果

(1)論文発表
①原著論文（国内（和文）誌　３件　　国際（欧文）誌　６４件）

	著者	発表論文名	掲載誌
	Hiroshima, T.	Additivity and multiplicativity properties of some Gaussian channels for Gaussian inputs	Phys.Rev.A 73, 012330 (2006) DOI: 10.1103/PhysRevA.73.012330
	Matsumoto, K.	On Additivity Questions.	Topics in Applied Physics, 2006, Volume 102/2006, 133-164.
	Ito, T; Imai, H.; Avis, D.	Bell inequalities stronger than the Clauser-Horne-Shimony-Holt inequality for three-level isotropic states	Phys.Rev.A 73, 042109 (2006) DOI: 10.1103/PhysRevA.73.042109
	Hayashi, M.	Optimal Visible Compression Rate For Mixed States Is Determined By Entanglement Purification	Phys.Rev.A , 73, 060301(R), (2006) DOI: 10.1103/PhysRevA.73.060301
	Hayashi, M.; Iwama, K.; Nishimura, H.; Raymond, R.; Yamashita, S.	(4,1)-Quantum Random Access Coding Does Not Exist--One qubit is not enough to recover one of four bits	New J. Phys. 8, 129 (2006) DOI: 10.1088/1367-2630/8/8/129

	Le Gall, F	Quantum Weakly Nondeterministic Communication Complexity	Lecture Notes in Computer Science 4162, 658-669, Springer, (2006) DOI: 10.1007/11821069_57
	Avis, D.; Imai, H.; Ito, T	On the Relationship between Convex Bodies Related to Correlation Experiments with Dichotomic Observables	J. of Phys. A: Math. Gen., Vol. 39 No. 36, pp.11283-11299 (8 September 2006) DOI: 10.1088/0305-4470/39/36/010
	Hayashi, M.	Practical Evaluation of Security for Quantum Key Distribution	Phys.Rev.A 74, 022307 (2006) DOI: 10.1103/PhysRevA.74.022307
	Buscemi, F.; Sacchi, M.F.	Information-Disturbance Tradeoff in Quantum State Discrimination	Phys.Rev. A74, 052320 (2006) DOI: 10.1103/PhysRevA.74.052320
	Jiang, Y. K.; Tomita, A.	Highly efficient polarization entangled-photon source from Periodically Poled Lithium Niobate wavegides	Optics communications, 267, 278-281(2006) DOI: 10.1016/j.optcom.2006.05.060
	Buscemi, F.	On the minimum number of unitaries needed to describe a random-unitary channel	Phys. Lett. A 360, 256(2006) DOI: 10.1016/j.physleta.2006.08.038
	Sirane, M.; Kono, S.; Ohkouchi, S.; Tomita, A.; Ikeda, N.; Sugimoto, Y.	Mode Identification of High-quality-factor Single-defect Nanocavities in Quantum Dot-embedded Photonic Crystals	J. Appl. Phys. 101, 073107 (2007) DOI: 10.1063/1.2714644
	King, C.; Matsumoto, K.; Nathanson, M.; Ruskai, M.B.	Properties of Conjugate Channels with Applications to Additivity and Multiplicativity	Markov Processes and Related Fields special issue in memory of John T. Lewis, vol.13, No.2, 391-423(2007)
	Buscemi, F.; Chiribella, G.; D'Ariano, G. M.; Macchiavello, C.; Perinotti, P.	Superbroadcasting and classical information	Phys.Rev.A 75, 012315 (2007) DOI: 10.1103/PhysRevA.75.012315
	Kojima, K.; Tomita, A.	Quantum-nondemolition measurement of photon-arrival using an atom-cavity system	Phys.Rev. A 75, 032320(2007) DOI: 10.1103/PhysRevA.75.032320
	Jiang, Y. K.; Tomita, A.	Generation of Polarization-entangled Photom Pairs Using Periodically Poled Lithium Niobate Waveguides in a Fiver Loop	J. of Phys. B, 40, 437-443(2007) DOI: 10.1109/CLEO.2006.4628944

	Hiroshima, T.; Adesso, G.; Illuminati, F.	Monogamy inequality for multipartite distributed Gaussian entanglement	Phys.Rev.Lett., 98, 050503(2007) DOI: 10.1103/PhysRevLett.98.050503
	Buscemi, F.; Sacchi, M.F.	A minimum-disturbing quantum state discriminator	Open Sys. And Inf. Dyn.14, 17-24(2007) DOI: 10.1007/s11080-007-9033-7
	Buscemi, F.; Chiribella, G.; D'Ariano	Quantum Erasure of Decoherence	Open Sys. And Inf. Dyn.14, 53-61(2007) DOI: 10.1007/s11080-007-9028-4
	Li, J.; Jiang, Y.-K.; Tomita, A	Measurement of the off-diagonal geometric phase of a mixed-state photon via a Franson interferometer	Physics Letters A 362, 2269-272 (2007) DOI: 10.1016/j.physleta.2006.10.033
	谷誠一郎, フランソワ・ルガル	量子分散コンピューティング	電子情報通信学会 和文論文誌 A, Vol.J90-A, No.5(2007), pp.393-402
	富田章久	量子暗号鍵配布システムの実際	電子情報通信学会 和文論文誌 A, Vol.J90-A, No.5(2007), pp.358-367
	松本啓史	エンタングルメントと量子情報処理	電子情報通信学会論文誌 A, Vol.J90-A, No.5 (2007), pp.340-347
	Matsumoto, K.; Hayashi, M.	Universal distortion-free entanglement concentration	Phys. Rev. A 75, 062338 (2007) DOI: 10.1103/PhysRevA.75.062338
	Inui, Y.; Le Gall, F	Efficient Quantum Algorithms for the Hidden Subgroup Problem over Semi-direct Product groups	Quantum Information & Computation, Vol.7 No.5&6 (2007), pp.559-570
	Tajima, A.; Tanaka, A.; Maeda, W.; Takahashi, S.; Tomita, A.	Practical quantum cryptosystem for metro area applications	IEEE J. Selected Topics in Quantum Electronics, Vol. 13, Issue 4, 1031 - 1038, July-Aug. 2007 DOI: 10.1109/JSTQE.2007.902841
○	Hayashi, M.	Upper bounds of eavesdropper's performances in finite-length code with the decoy method	Phys.Rev.A 76, 012329 (2007) DOI: 10.1103/PhysRevA.76.012329
	Hayashi, M.	Prior entanglement between senders enables perfect quantum network coding with modification	Phys.Rev.76, 040301 (2007) DOI: 10.1103/PhysRevA.76.040301
	Wang, X. B.; Hiroshima, T.; Tomita, A.; Hayashi, M.	Quantum information with Gaussian states	Physics Reports Vol.448, Issues 1-4, Pages 1-111 DOI: 10.1016/j.physrep.2007.04.005

	Tani, S.	An Improved Claw Finding Algorithm Using Quantum Walk	Lecture Notes in Computer Science 4708, 536-547, Springer, (2007) DOI: 10.1007/978-3-540-74456-6_48
	Hayashi, M.	General theory for decoy-state quantum key distribution with arbitrary number of intensities	New J. Phys. 9, 284 (2007) DOI: 10.1088/1367-2630/9/8/284
	Buscemi, F.	Channel Correction via Quantum Erasure	Phys.Rev.Lett. 99, 180501 (2007) DOI: 10.1103/PhysRevLett.99.180501
	Shi, B. S.; Shai, C.; Guo, G. C.; Jang, Y. K.; Tomita, A.	Efficient generation of a photon pair in a bulk periodically poled potassium titanyl phosphate	Optics communications, 278, 363-367 (2007) DOI: 10.1016/j.optcom.2007.06.044
	Avis, D.; Imai, H.; Ito, T	Generating facets for the cut polytope of a graph by triangular elimination	Mathematical Programming: Series A and B, Vol.112, No.2, 303-325(2007) DOI: 10.1007/s10107-006-0018-z
○	Okubo, Y.; Wang, Xiang-Bin ; Jiang, Y.-K.; Tani, S.; Tomita, A.	Experimental demonstration of quantum leader election in liner optics	Phys.Rev.A 77, 032343 (2008) DOI: 10.1103/PhysRevA.77.032343
	Buscemi, F.	Entanglement measures and approximate quantum error correction	Phys.Rev.A 77, 012309 (2008) DOI: 10.1103/PhysRevA.77.012309
	Buscemi, F.	Irreversibility of entanglement loss	Springer Lecture Note in Computer Science, 5106, 16(2008) DOI: 10.1007/978-3-540-89304-2_3
	Inui, Y.; Le Gall, F	Quantum Property Testing of Group Solvability	Springer Lecture Notes in Computer Science 4957, pp.772-783 DOI: 10.1007/978-3-540-78773-0_66
	Hayashi, M.; Tomita, A.; Matsumoto, K.	Statistical analysis of testing of an entangled state based on the Poisson distribution framework	New J. Phys., 10, 043029, (2008) DOI: 10.1088/1367-2630/10/4/043029

○	Buscemi, F.; Hayashi, M.; Horodecki, M.	Global information balance in quantum measurements	Phys.Rev.Letters, 100, 210504(2008) DOI: 10.1103/PhysRevLett.100.210504
	Tanaka, A.; Fujiwara, M.; Nam, S.-W.; Nambu, Y.; Takahashi, S.; Maeda, W.; Yoshino, K.; Miki, S.; Baek, B.; Zhen, W.; Tajima, A.; Sasaki, M.; Tomita, A.	Ultra fast quantum key distribution over a 97-km installed telecom fibre with wavelength-division multiplexing clock synchronization	Optics Express, Vol.16, Issue15, pp. 11354-11360 (2008) DOI: 10.1364/OE.16.011354
	Buscemi, F.; Hayashi, M.; Horodecki, M.	Information extraction versus irreversibility in quantum measurement processes	International Journal of Quantum Information (Int. J. Quant. Inf.) Vol. 6, Suppl , pp. 613-619. July 2008 DOI: 10.1142/S0219749908003852
	Hayashi, M.; Matsumoto, K.	Asymptotic performance of optimal state estimation in qubit system	J. Math. Phys. 49, 102101 (2008). DOI: 10.1063/1.2988130
	Ishizaka, S.; Hiroshima, T.	Quantum teleportation to enable universal quantum processor	Phys.Rev., 101, 240501(2008) DOI: 10.1103/PhysRevLett.101.240501
	Buscemi, F.; Horodecki, M.	Towards a unified approach to information-disturbance tradeoffs in quantum measurements	Open systems and Information Dynamics Vol.16, No.29, pp.29 – 48, (2009) DOI: 10.1142/S1230161209000037
	Ishizaka, T.; Hiroshima, T.	Quantum teleportation scheme by selecting one of multiple output ports	Physical Review A 79, 042306, 2009 DOI: 10.1103/PhysRevA.79.042306
	Kojima, K.; Tomita, A.	Photon-arrival detector with a controlled phase flip operation between a photon and a V-type atomic system	JOSA B: OPTICAL PHYSICS, 26, 4 2—9, pp.836-848. DOI:10.1364/JOSAB.26.000836
	Miyata, H.; Moriyama, S.; Imai, H.	Deciding non-realizability of oriented matroids by semidefinite programming	Pacific Journal of Optimization, Vol.5, No.2 (May 2009), pp. 211--224.

○	Kobayashi, H.; Matsumoto, K.; Yamakami, T.	Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur?	Chicago Journal of Theoretical Computer Science, Article 3,2009
	Ito, T.; Kobayashi, H.; Matsumoto, K.	Oracularization and Two-Prover One-Round Interactive Proofs against Nonlocal Strategies.	IEEE Computational Complexity （CCC), 2009: 217-228 DOI: 10.1109/CCC.2009.22
○	Le Gall, F	Exponential Separation of Quantum and Classical Online Space Complexity	Theory of Computing Systems, 45, 188-202 (2009) DOI: 10.1007/s00224-007-9097-3
	Hsieh, M.-H., Wilde, M.-M.	Public and private communication with a quantum channel and a secret key	Phys. Rev. A 80, 022306 (2009) DOI: 10.1103/PhysRevA.80.022306
	Akiba, M.; Tsujino, K.; Sasaki, M.	Multipixel silicon avalanche photodiode with ultralow dark count rate at liquid nitrogen temperature	Optics Express, Vol. 17, Issue 19, pp.16885-16897 (2009). DOI: 10.1364/OE.17.016885
	Tani, S.	Claw Finding Algorithm Using Quantum Walk	Theoretical Computer Science, 410(50): 5285-5297 (2009). DOI: 10.1007/978-3-540-74456-6_48
	Kimikazu Kato, Mayumi Oto, Hiroshi Imai and Keiko Imai	Computational Geometry Analysis of Quantum State Space and Its Applications	Generalized Voronoi Diagram: *A Geometry-Based Approach to Computational Intelligence* DOI: 10.1007/978-3-540-85126-4_4
	Tanaka, A.; Maeda, W.; Takahashi, S.; Tajima, A.; Tomita, A.	Ensuring Quality of Shared Keys through Quantum Key Distribution for Practical Application	IEEE Journal of Selected Topics in Quantum Electronics, 15(6), pp.1622-1629(2009) DOI:10.1109/JSTQE.2009.2028243
	Fujiwara, M.; Toyoshima, M.; Sasaki, M.; Yoshino, K.; Nambu, Y.; Tomita, A.	Performance of hybrid entanglement photon pair source for quantum key distribution	Applied Physics Letters, 95,261103(2009) DOI:10.1063/1.3276559
	Maeda, W.; Tanaka, A.; Takahashi, S.; Tajima, A.; Tomita, A.	Technologies for Quantum Key Distribution Networks Integrated With Optical Communication Networks	IEEE Journal of Selected Topics in Quantum Electronics, 15(6), pp.1591-1601(2009) DOI:10.1109/JSTQE.2009.2032664

	Takemoto, K.; Nambu, Y.; Miyazawa, T.; Wakui, K.; Hirose, S.; Usuki, T.; Takatsu, M.; Yokoyama, N.; Yoshino, K.; Tomita, A.; Yorozu, S.; Sakuma, Y.; Arakawa, Y.	Transmission Experiment of Quantum Keys over 50 km Using High-Performance Quantum-Dot Single-Photon Source at 1.5 μm Wavelength	Applied Physics Express 3, 092802(2010) DOI: 10.1143/APEX.3.092802
	Tsujino, K.; Fukuda, D.; Fujii, S.; Inoue, M.; Fujiwara, M.; Tkeoka, M.; Sasaki, M.	Sub-shot-noise-limit discrimination of on-off keyed coherent signals via a quantum receiver with a superconducting transition edge sensor	Optics Express, Vol. 18, Issue 8, pp.8107-8114 (2010). DOI: 10.1364/OE.18.008107
	Takeoka, M.; Tsujino, K.; Sasaki, M.	Cut-off rate analysis of practical quantum receivers	Journal of Modern Optics, Vol. 57, Issue 3, pages 207 - 212 (2010). DOI: 10.1080/09500340903203103
	Akiba, M.; Tsujino, K.; Sasaki, M.	Ultrahigh-sensitivity single-photon detection with linear-mode silicon avalanche photodiode	Optics Letters, Vol. 35, Issue 15, pp.2621-2623 (2010). DOI: 10.1364/OL.35.002621
	Tomita, A.; Yoshino, K.; Nambu, Y.; Tajima, A.; Takahashi, S.; Maeda, W,; Miki, S.; Wang, Z.; Fujiwara, M.; Sasaki, M.	High speed quantum key distribution system	Optical Fiber Technology, 16(1), pp. 55-62(2010) DOI:10.1016/j.yofte.2009.10.003
	Ambainis, A.; Childs, A.; Le Gall, F.; Tani, S.	The quantum query complexity of certification	Quantum Information & Computation, Vol.10, No. 3&4, pp. 181-189 (2010)
In Press	Le Gall, F	Quantum Weakly Nondeterministic Communication Complexity	Theoretical Computer Science
In Press	Inui, Y.; Le Gall, F	Quantum Property Testing of Group Solvability	Algorithmica DOI: 10.1007/s00453-009-9338-8

In Press	Sprojcar, J.; Bouda, J.	Quantum Communication Between Anonymous Sender and Anonymous Receiver in Presence of Strong Adversary	International Journal of Foundations of Quantum Information

②その他の著作物（総説，書籍など）

	著者	発表論文名	掲載誌	
	加藤豪; 谷誠一郎	情報・物理双方から見た量子探索アルゴリズム	情報処理学会誌 Vol.47, No.12 (2006)	
	富田章久	パラメトリックダウンコンバージョンによるもつれ光子の生成	光技術コンタクト 44 巻 11 月号 pp.621-630 (2006)	
	今井浩	量子情報学-物理学と情報学の融合と展開-	電子情報通信学会誌創立 90 周年記念特集号, Vol.90, No.5 (2007), pp.340-344	
	富田章久	Theory on security issues in Quantum key distribution	オプトロニクス Vol.26, No.308, pp.147-155 (2007)	
	富田章久	量子もつれ光子対の発生 パラメトリックダウンコンバージョン光子対発生の原理と実際	光アライアンス20巻10月号 pp.5-9 (2009)	
	富田章久	単一光子による量子暗号鍵配布付システム	光学 39 巻1号 pp.10-16(2010)	

(2) 口頭発表

①招待講演　（国内　２６件,　国際２９件）

②口頭発表　（国内　９０件,　国際５５件）

③ポスター発表　（国内　３２件,　国際２１件）

1 Kawachi, A.; Yamakami, T.,How to Construct Quantum Hard-Core Predicates from Any Quantum One-Way Functions,The 2006 Symposium on Cryptography and Information Security (SCIS 2006), Hiroshima, Japan, January 17-20, 2006

2 林正人; 岩間一雄; 西村治道; Putra, R. R. H.; 山下茂, 量子ネットワーク上での効率的な情報の伝送 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.

3 Kawachi, A.; Yamakami, T.,Complexity-Theoretical Quantum List Decoding and Applications to Quantum Hardcore Functions,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.

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

5 Matsumoto, K.,Reverse estimation theory, Complementarity between SLD and RLD ,The Ninth Workshop on Quantum Information Processing, Paris, France, January 16-20, 2006

6 Owari, M.; Hayashi, M.,Local discrimination: one-way LOCC VS two-way LOCC,The Ninth Workshop on Quantum Information Processing, Paris, France, January 16-20, 2006

7 長谷川淳; 由良文孝,デコヒーレンスエラーに対する量子数え上げアルゴリズムの理論的解析,第14回非平衡系の統計物理シンポジウム, Jan. 25-27, 2006

8 Jiang, Y. K.; Tomita, A.,Generation of Polarization-entangled Photon Pairs Using Periodically Poled Lithium Niobate Waveguides in a Fiber Loop,CLEO/QELS, Long Beach, California, USA, May 21-26, 2006

9 Matsumoto, K.,Reverse estimation theory, monotone distances, and RLD based geometry,2nd International Symposium on Information Geometry and its Applications, Sanjo Conference Hall, University of Tokyo, December 12-16, 2005

10 Hayashi, M.,Characterization of several kinds of quantum analogues of relative entropy,2nd International Symposium on Information Geometry and its Applications, Sanjo Conference Hall, University of Tokyo, December 12-16, 2005

11 松本啓史,量子もつれ合い(勉強会講師として),量子情報勉強会2006初春編, 国立情報学研究所 12 階1208号室, Jan. 11-13, 2006

12 林正人,量子推定理論(勉強会講師として),量子情報勉強会2006初春編, 国立情報学研究所 12 階1208号室, Jan. 11-13, 2006

13 Matsumoto, K.,Some Results on Quantum Interactive Proof Systems,Workshop on Theory of Quantum Computation, Communication, Cryptography, NTT R&D Center, Atsugi, Kanagawa, Japan, Feb. 22-23, 2006

14 Matsumoto, K.,On the Quantum Central Limit Theorem in d-dimensional Case, and its Applications,50 Years Later Conference on Stochastics in Science in Honor of Ole E. Barndorff-Nielsen, Guanajuato, Mexico, Mar. 20-24, 2006

15 Hayashi, M.; Iwama, K.; Nishimura, H.; Raymond, R.; Yamashita,

S.,Quantum Random Access Coding Does Not Exist,電子情報通信学会, コンピューテーション研究会, 九州工業大学, May 24-25, 2006

16 高橋成五; 中田武志; 田島章雄; 富田章久,量子暗号用 APD のノイズキャリア発生率評価,第14回量子情報技術研究会(QIT14), 東京工業大学大岡山キャンパス, May 29-30, 2006

17 林正人,量子鍵配送における実用的安全性,第14回量子情報技術研究会(QIT14), 東京工業大学大岡山キャンパス, May 29-30, 2006

18 Jiang, Y. K.; Tomita, A.,Generation of Polarization-entangled Photon Pairs Using Periodically Poled Lithium Niobate Waveguides in a Fiber Loop,第14回量子情報技術研究会(QIT14), 東京工業大学大岡山キャンパス, May 29-30, 2006

19 谷誠一郎,量子分散計算の基礎,第14回量子情報技術研究会(QIT14), 東京工業大学大岡山キャンパス, May 29-30, 2006

20 松本啓史,対称化操作と量子対話証明,第14回量子情報技術研究会(QIT14), 東京工業大学大岡山キャンパス, May 29-30, 2006

21 Le Gall, F,Quantum Weakly Nondeterministic Communication Complexity,第14回量子情報技術研究会(QIT14), 東京工業大学大岡山キャンパス, May 29-30, 2006

22 河内亮周; 山上智幸,計算量理論的な量子リスト復号による量子ハードコア関数の構成,第14回量子情報技術研究会(QIT14), 東京工業大学大岡山キャンパス, May 29-30, 2006

23 廣嶋透也,量子ガウス状態入力に対する量子ガウス通信路の加法的及び乗法的性質,第14回量子情報技術研究会(QIT14), 東京工業大学大岡山キャンパス, May 29-30, 2006

24 南部芳弘; 吉野健一郎; 富田章久,導波路型PPLNを用いた1．5um 帯相関光子対光源の評価,第14回量子情報技術研究会(QIT14), 東京工業大学大岡山キャンパス, May 29-30, 2006

25 尾張正樹; 林正人,状態識別における一方向 LOCC と二方向 LOCC の違いについて,第14回量子情報技術研究会(QIT14), 東京工業大学大岡山キャンパス, May 29-30, 2006

26 吉野健一郎; 南部芳弘; 富田章久,PLC を用いた受動基底選択型量子暗号システム,第14回量子情報技術研究会(QIT14), 東京工業大学大岡山キャンパス, May 29-30, 2006

27 Matsumoto, K.,Hypothesis testing for a Bell pair,Quantum 2006: Ⅲ workshop ad memoriam of Carlo Novero Advances in Foundations of Quantum Mechanics and Quantum Information with atoms and photons, Turin, Italy, May 2-5 2006

28 Buscemi, F; Chiribella, G; D'Ariano, G. M.,Information Flow in Decoherence Processes,38th symposium on mathematical physics, Torun, Poland, June 4-7, 2006

29 Tomita, A.,R&D activities on Quantum Key Distribution in Japan,Towards Quantum Standard, London, England, May 25-26, 2006

30 Le Gall, F,Exponential Separation of Quantum and Classical Online Space Complexity,18th ACM Symposium on Parallelism in Algorithms and Architectures (SPAA 06), Cambridge, MA, USA, July 30-Aug. 2, 2006

31 廣嶋透也,Additivity and multiplicativity properties of some Gaussian channels for Gaussain inputs,The 8th International Conference on Quantum Communication, Measurement and Computing, つくば市, 茨城, Nov. 28-Dec. 3, 2006

32 Le Gall, F,Quantum Weakly Nondeterministic Communication Complexity,31st International Symposium of Mathematical Foundations of Computer Science (MFCS 2006), Stara Lesna, Slovakia, Aug.28-Sep.1,2006

33 林正人,Testing for Maximally Entangled State(Theory and Experiment),15th

International Laser Physics workshop, Lausanne, Switzerland, July 24-28, 2006

34 林正人,Practical Evaluation of Security for Quantum Key Distribution,A conference on Quantum Statistics, Information and Control, Nottingham University, England, July 15-19, 2006

35 林正人,Future research direction of quantum information,情報物理学の数学的構造, 京都大学数理解析研究所, June 29th, 2006

36 白根昌之; 牛田淳; 河野俊介; 池田直樹; 杉本喜正; 大河内俊介; 富田章久,H1 型フォトニック結晶共振器のモード同定,第67回応用物理学会学術講演会, 立命館大学びわこ・くさつキャンパス, Aug. 29-Sep. 1, 2006

37 白根昌之; 河野俊介; 池田直樹; 杉本喜正; 大河内俊介; 富田章久,高 Q 値 H1 型フォトニック結晶共振器,第67回応用物理学会学術講演会, 立命館大学びわこ・くさつキャンパス, Aug. 29-Sep. 1, 2006

38 Kato, K.; Oto, M.; Imai, H.; Imai, K.,Notes on Voronoi Diagrams for Pure Quantum States,電子情報通信学会コンピュテーション研究会, 埼玉大学, Jun. 23, 2006

39 Kato, K.; Oto, M.; Imai, H.; Imai, K.,On a Geometric Structure of Pure Multi-qubit Quantum States and Its Applicability to a Numerical Computation,3rd International Symposium on Voronoi Diagrams in Science and Engineering (ISVD'06),IEEE CS Press, Banff, Canada, July 2-5, 2006

40 Tomita, A.,Sagnac interferometers in quantum information technology,15th International Laser Physics workshop, Lausanne, Switzerland, July 24-28, 2006

41 Shi, B-S.; Tomita, A.,Four photons interfering but showing the two-photon interference behavior,15th International Laser Physics workshop, Lausanne, Switzerland, July 24-28, 2006

42 Hiroshima, T.; Adesso, G.; Illuminati, F.,Monogamy inequality for distributed Gaussian entanglement,Asian Conference on Quantum Information Science 2006, Peking, China, Sep.1-4, 2006

43 Tomita, A.,Recent development on practical quantum key distribution systems,The 8th International Conference on Quantum Communication, Measurement and Computing, つくば市, 茨城, Nov. 28-Dec. 3, 2006

44 Buscemi, F.; Sacchi, M. F.,Information-Disturbance Tradeoff in Quantum State Discrimination,Asian Conference on Quantum Information Science 2006, Peking, China, Sep.1-4, 2006

45 Tani, S.,New Quantum Bounds for the Claw Finding Problem,Asian Conference on Quantum Information Science 2006, Peking, China, Sep.1-4, 2006

46 Inui, Y.,Quantum Property Testing for Solvable Groups,Asian Conference on Quantum Information Science 2006, Peking, China, Sep.1-4, 2006

47 Hayashi, M.,Practical Evaluation of Security for Quantum Key Distribution,Asian Conference on Quantum Information Science 2006, Peking, China, Sep.1-4, 2006

48 Hayashi, M.; Iwama, K.; Nishimura, H.; Raymond, R.; Yamashita, S.,(4,1)-Quantum Random Access Coding Does Not Exist--One qubit is not enough to recover one of four bits--,Asian Conference on Quantum Information Science 2006, Peking, China, Sep.1-4, 2006

49 Tomita, A.,Research directions toward quantum networks,Asian Conference on Quantum Information Science 2006, Peking, China, Sep.1-4, 2006

50 Hayashi, M.; Tomita, A.; Matsumoto, K.,Statistical analysis on testing of an entangled state based on Poisson distribution framework,FOCUS MEETING: Quantum Process Estimation, Budmerice, Slovakia, Sep. 27- Oct. 1, 2006

51 林正人,量子プロトコルとその理論展開,電子情報通信学会, 東京支部シンポジウム「量

子計算・量子通信の最前線」, 東京, Aug.23, 2006

52 富田章久,BB84 プロトコルによる量子暗号鍵配布の実用化技術,電子情報通信学会, 東京支部シンポジウム「量子計算・量子通信の最前線」, 東京, Aug.23, 2006

53 富田章久,量子暗号技術の最近の進展,STARC シンポジウム2006, 新横浜国際ホテル, Sep. 8, 2006

54 Kojima.K.; Tomita, A.,Proposal for QND-measurement of phonton-arrival with an atom-cavity system,The 8th International Conference on Quantum Communication, Measurement and Computing, つくば市, 茨城, Nov. 28-Dec. 3, 2006

55 Kojima.K.; Tomita, A.,Proposal for QND-measurement of phonton-arrival with an atom-cavity system,第15回量子情報技術研究会(QIT15), キャンパスプラザ京都, Nov. 21-22, 2006

56 Hiroshima, T.; Adesso, G.; Illuminati, F.,Monogamy inequality for distributed Gaussian entanglement,第15回量子情報技術研究会(QIT15), キャンパスプラザ京都, Nov. 21-22, 2006

57 Buscemi, F.; Sacchi, M. F.,Information-Disturbance Tradeoff in Quantum State Discrimination,The 8th International Conference on Quantum Communication, Measurement and Computing, つくば市, 茨城, Nov. 28-Dec. 3, 2006

58 Imai, H.,Polyhedral Approaches to Quantum Information,Polyhedral Computation Combinatorial Oprimization Theme Semester, Centre de recherches mathematiques, Montreal, Canada, Oct. 17-20, 2006

59 Tomita, A.,Practical implementation and security of quantum key distribution,2006 US-Japan Workshop on Quantum Information Science in Hawaii, Hawaii, U.S.A., Oct. 16-20, 2006

60 Jiang, Y. K.; Li, J.; Tomita, A.,Off-diagonal geometric phase for mixed states in experiment of Franson interferometer,Asian Conference on Quantum Information Science 2006, Peking, China, Sep.1-4, 2006

61 Le Gall, F,Quantum Online Space Complexity,第15回量子情報技術研究会(QIT15), キャンパスプラザ京都, Nov. 21-22, 2006

62 Le Gall, F,Sur la Puissance de Calcul d'un Ordinateur Quantique a Memoire Limitee,French Science Day 2006, 東京大学本郷キャンパス武田先端知ビル, Dec. 1, 2006

63 林正人; 富田章久; 廣嶋透也; 長谷川淳,デコイを用いた量子鍵配送の改良とその安全性解析,第15回量子情報技術研究会(QIT15), キャンパスプラザ京都, Nov. 21-22, 2006

64 大久保雄太; Xiang-Bin Wang; 富田章久,線形光学による量子リーダー選挙の実装, 第15回量子情報技術研究会(QIT15), キャンパスプラザ京都, Nov. 21-22, 2006

65 Buscemi, F.; Chiribella, G.; D'Ariano, G. M.; Macchiavello, C.; Perinotti, P.,Superbroadcasting and classical information,第15回量子情報技術研究会(QIT15), キャンパスプラザ京都, Nov. 21-22, 2006

66 Hayashi, M.,Gallager Bound of Classical-Quantum Channel Coding,The 8th International Conference on Quantum Communication, Measurement and Computing, つくば市, 茨城, Nov. 28-Dec. 3, 2006

67 Hayashi, M.; Iwama, K.; Nishimura, H.; Raymond, R.; Yamashita, S.,(4,1)-Quantum Random Access Coding Does Not Exist--One qubit is not enough to recover one of four bits--,ISIT 2006, the 2006 IEEE International Symposium on Information Theory, Washington, USA, July 9-14, 2006

68 Tajima, A.; Tanaka, A.; Maeda, W.; Takahashi, S.; Nambu, Y.; Tomita, A.,Quantum Key Distribution Network,31st European Conf on Optical Communication(ECOC), Cannes, France, Sep. 24-28, 2006

69 Tajima, A.; Tanaka, A.; Maeda, W.; Takahashi, S.; Nambu, Y.; Tomita, A.,Realizing Decoy State on a High-Speed Quantum Cryptosystem,32nd

European Conf on Optical Communication(ECOC), Cannes, France, Sep. 24-28, 2006

70 南部芳弘; 吉野健一郎; 富田章久,変調器フリーPLC 量子暗号システムの開発,第15回量子情報技術研究会(QIT15), キャンパスプラザ京都, Nov. 21-22, 2006

71 南部芳弘; 吉野健一郎; 富田章久,平面光回路(PLC)干渉計と導波路型PPLN結晶を用いた 1.5um 帯2光子干渉実験,第15回量子情報技術研究会(QIT15), キャンパスプラザ京都, Nov. 21-22, 2006

72 Tanaka, A.; Tomita, A.; Maeda, W.; Takahashi, Y.; Tajima, A.,Decoy-State Design for use in a High-Speed QKD,The 8th International Conference on Quantum Communication, Measurement and Computing, つくば市, 茨城, Nov. 28-Dec. 3, 2006

73 Nambu, A.; Yoshino, K.; Tomita, A.,Quantum key distribution systems without optical switching using planar lightwave circuit,The 8th International Conference on Quantum Communication, Measurement and Computing, つくば市, 茨城, Nov. 28-Dec. 3, 2007

74 Jiang, Y. K.; Li, J.; Tomita, A.,Off-diagonal geometric phase for mixed states in experiment of Franson interferometer,第15回量子情報技術研究会(QIT15), キャンパスプラザ京都, Nov. 21-22, 2006

75 今井浩,量子情報を数理計画する,日本オペレーションズ・リサーチ学会計算と最適化研究会、電気通信大学青山スカイオフィス, Nov. 25, 2006

76 Le Gall, F,Exponential Separation of Quantum and Classical Online Space Complexity,Workshop on Quantum Information Processing, QIP Workshop 2007, Brisbane, Australia, Jan. 30-Feb. 3, 2007

77 Le Gall, F,量子コンピューターを使った素因数分解,夢の科学技術を子供たちの手にシンポジウム2006, 会津大学, 福島, Nov.4th, 2006

78 富田章久,パラメトリックダウンコンバージョンによるもつれ光子の生成,JOEM 日本オプトメカトロニクス協会部会セミナー,機械振興会館, 東京, Dec. 7th, 2006

79 Tani, S.,Improved Quantum Bounds for the Claw Finding Problem,Workshop on Quantum Information Processing, QIP Workshop 2007, Brisbane, Australia, Jan. 30-Feb. 3, 2007

80 林正人; 富田章久; 廣嶋透也; 長谷川淳,デコイ法によって実現可能な量子鍵配送システムの安全評価,科研費特定領域研究「情報統計力学の深化と展開」平成18年度研究成果発表会, 大手町サンケイプラザ, 東京, Dec. 18-20, 2006

81 林正人,情報符号化における量子・古典対応,日本物理学会2007年春季大会, 鹿児島大学郡元キャンパス, Mar. 18-21, 2007

82 長谷川淳; 林正人; 富田章久; 廣嶋透也,デコイ法による現実的な設定の下で安全な量子鍵配送実験,The 2007 Symposium on Cryptography and Information Security (SCIS2007), ハウステンボス・ユトレヒト, 長崎, Jan. 23-26, 2007

83 Le Gall, F,Space Efficient Quantum Algorithms for Data Streams,Workshop on Theory of Quantum Computation, Communication and Cryptography, Nara, Japan, Jan. 24-25, 2007

84 Tani, S.,Distributed Grover Search and Its Applications,Nara Advanced Interdisciplinary Workshop on Quantum Information Science, 奈良先端科学技術大学院大学, Nara, Japan, Jan. 25-26, 2007

85 廣嶋透也; Adesso, G.; Illuminati, F.,多者間の量子ガウス状態エンタングルメントに対するモノガミー不等式,日本物理学会2007年春季大会, 鹿児島大学郡元キャンパス, Mar. 18-21, 2007

86 林正人; 富田章久; 廣嶋透也; 長谷川淳,デコイ法を用いた量子鍵配送の改良とその安全性解析,日本物理学会2007年春季大会, 鹿児島大学郡元キャンパス, Mar. 18-21, 2007

87 林正人; 富田章久; 長谷川淳; 廣嶋透也,弱コヒーレント光によるセキュリティ精度保証つき量子鍵配送,情報理論研究会, 群馬大学桐生キャンパス, Mar. 15-16, 2007

88 林正人; 富田章久; 長谷川淳; 廣嶋透也,実用的な設定での量子鍵配送の安全性評価,日本物理学会北陸支部講演会, 福井大学工学部, Mar. 27, 2007

89 Hayashi, M.; Iwama, K.; Nishimura, H.; Raymond, R.; Yamashita, S.,Quantum Network Coding,24th Intenational Symposium on Theoretical Aspects of Computer Science STACS 2007, Aachen, Germany, Feb. 22-24, 2007

90 富田章久,量子暗号実現化のための研究開発,情報通信研究機構 情報セキュリティシンポジウム「トラクタブルネットワークの実現に向けて」, 青山, Feb. 7, 2007

91 田島章雄; 高橋成五; 富田章久,量子暗号の高速化に向けた単一光子検出回路の提案,電子情報通信学会総合大会, 名城大学, Mar. 20-23, 2007

92 高橋成五; 田島章雄; 富田章久,量子暗号通信における光子検出器,電子情報通信学会総合大会, 名城大学, Mar. 20-23, 2007

93 桐原明宏; 大河内俊介; 藤方潤一; 河野俊介; 富田章久; 萬伸一,電荷制御可能なInAs 量子ドットデバイスによる高次荷電励起子発光の観測,応用物理学会春季応用物理学関係連合講演会, 青山学院大学, Mar. 27-30, 2007

94 中田武志; 水木恵美子; 牧田紀久夫; 高橋成五; 富田章久,三元 APD のアフターパルス評価: 光検出信号とダーク検出信号のアフターパルス比較,応用物理学会春季応用物理学関係連合講演会, 青山学院大学, Mar. 27-30, 2007

95 白根昌之; 河野俊介; 大河内俊介; 富田章久; 池田直樹; 杉本喜正,単一量子ドットと単一欠陥フォトニック結晶ナノ共振器の結合,応用物理学会春季応用物理学関係連合講演会, 青山学院大学, Mar. 27-30, 2007

96 河野俊介; 白根昌之; 池田直樹; 杉本喜正; 大河内俊介; 富田章久,H1 型フォトニック結晶共振器におけるパーセル効果,応用物理学会春季応用物理学関係連合講演会, 青山学院大学, Mar. 27-30, 2007

97 Tomita, A.,Stable operation of a Secure QKD system in the real-world setting,The DAMOP/DAMP Joint Meeting, Calgary, Canada, Jun. 5-9, 2007

98 桐原明宏; 大河内俊介; 藤方潤一; 河野俊介; 富田章久; 萬伸一,Optical Spectroscopy of Charge-tunable Quantum Dots Emittimg at 1.2 um,International Quantum Electronics Conference (IQEC), Munchen, Germany, Jun. 17, 2007

99 河野俊介; 白根昌之; 池田直樹; 杉本喜正; 大河内俊介; 富田章久,Coherent Control of InAs/GaAs Single Quantum Dots,International Quantum Electronics Conference (IQEC), Munchen, Germany, Jun. 17, 2007

100 Buscemi, F.; Hayashi, M.; Horodecki, M.,Information gain and approximate reversibility of quantum measurements: an entropic approach,第 16 回量子情報技術研究会(QIT16), NTT 厚木研究開発センタ, May 17-18, 2007

101 Hasegawa, J.; Hayashi, M.; Hiroshima, T.; Tomita, A.,Experimental Decoy State Quantum Key Distribution with Unconditional Security Incorprorating Finite Statistics,ナノ光・電子デバイスと量子エレクトロニクス, 東京ガーデンパレス, March 20, 2007

102 林 正人,Theoretical security analysis on quantum key distribution based on decoy method,第 16 回量子情報技術研究会(QIT16), NTT 厚木研究開発センタ, May 17-18, 2007

103 大久保雄太; Xiang-Bin Wang; 富田章久,線形光学による量子リーダー選挙の実装,日本物理学会2007年春季大会, 鹿児島大学郡元キャンパス, Mar. 18-21, 2007

104 Nishitoba, J.; Kato, K.; Moriyama, S.; Nakayama, H.; Imai, H.,Smallest Enclsoing Balls and an Effective Calculation of a Quantum Channel Capacity.,2nd Doctoral Workshop on Mathematical and Engineering Methods in Computer Science (MEMICS 2006), Mikulov, Czech Republic, October 27-29, 2006

105 Inaba, M.; Tanaka, M.; Tamatsukuri, J.; Hiraki, K.; Imai, H.,Avoidable Packet Losses on Long Fat Pipe Network --- Effects of Bottlenecks and

Intermediate Switches. ,IFIP International Conference on Network and Parallel Computing (NPC 2006), Tokyo, October 2006

106 Kato, K.; Oto, M.; Imai, H.; Imai, K.,Voronoi Diagrams and a Numerical Estimation of a Quantum Channel Capacity,2nd Doctoral Workshop on Mathematical and Engineering Methods in Computer Science (MEMICS 2006), Mikulov, Czech Republic, October 27-29, 2006

107 大久保雄太; Xiang-Bin Wang; 富田章久,線形光学による量子リーダー選挙の実装, 第 16 回量子情報技術研究会(QIT16), NTT 厚木研究開発センタ, May 17-18, 2007

108 Inui, Y.; Le Gall, F.,Quantum Property Testing for Group Solvability,第 16 回量子情報技術研究会(QIT16), NTT 厚木研究開発センタ, May 17-18, 2007

109 Okubo, Y.; Xiang-Bin Wang; Tomita, A.,Experimental demonstration of quantum leader election in linear optics,Frontiers in Optics 2007, Fairmont Hotel, San Jose, California, USA, Sep. 16-20, 2007

110 小島邦裕,エンタングルメント共有と量子中継,産業総合研究所ナノテクノロジー部門セミナー, つくば市, May 18, 2007

111 Hasegawa, J.; Hayashi, M.; Hiroshima, T.; Tomita, A.,Numerical Analysis of Decoy State Quantum Key Distribution with Unconditional Security Incorporating Finite Statistics,第 16 回量子情報技術研究会(QIT16), NTT 厚木研究開発センタ, May 17-18, 2007

112 Buscemi, F.; Hayashi, M.; Horodecki, M.,Information gain and approximate reversibility of quantum measurements: an entropic approach,APWQIS: Forth Asia Pacific Workshop & Third Asia Pacific Conference on Quantum Information Science, Singapore, July. 30-Aug. 2, 2007

113 Hayashi, M.,Security analysis on quantum key distribution with practical setting,2007 KIAS-KAIST Workshop on Quantum Information Science, Soeul, Korea, June 25-27, 2007

114 Buscemi, F.; Hayashi, M.; Horodecki, M.,Information dynamics in quantum measurements: an entropic approach to the information-disturbance tradeoff problem,IICQI 2007, International Iran Conference on Quantum Information, Kishi Island, Iran, Sep. 7-10, 2007

115 Hayashi, M.,Security of implementable QKD system by the decoy method,Theory and Realisation of Practical Quantum Key Distribution, Waterloo, Canada, Jun. 11-14, 2007

116 Hayashi, M.,Theoretical analysis and implementation on QKD with the decoy-state method,APWQIS: Forth Asia Pacific Workshop & Third Asia Pacific Conference on Quantum Information Science, Singapore, July. 30-Aug. 2, 2007

117 Hasegawa, J.; Hayashi, M.; Hiroshima, T.; Tomita, A.,Security analysis and experiment of decoy state quantum key distribution incorporating finite statistics,Asian Conference on Quantum Information Science 2007, Shiran-kaikan, Kyoto, Sep.3-6, 2007

118 Le Gall, F.; Yamakami, T.,Self-Correcting Quantum Programs,Asian Conference on Quantum Information Science 2007, Shiran-kaikan, Kyoto, Sep.3-6, 2007

119 Inui, Y.; Le Gall, F.,Quantum Algorithm for some Instances of Solvable Group Isomorphism,Asian Conference on Quantum Information Science 2007, Shiran-kaikan, Kyoto, Sep.3-6, 2007

120 Buscemi, F.; Hayashi, M.; Horodecki, M.,A general entropic approach to the information-disturbance tradeoff problem in quantum measurements,Asian Conference on Quantum Information Science 2007, Shiran-kaikan, Kyoto, Sep.3-6, 2007

121 Tani, S.,An improved claw finding algorithm using quantum walk,Symposium on Mathematical Foundations of Computer Science (MFCS 2007), Cesky Krumlov, Czech, Aug. 27-31, 2007

122 大久保雄太; Xiang-Bin Wang; 富田章久,線形光学による量子リーダー選挙の実装, 第3回量子情報未来テーマ開拓研究会, ホテルサンライズ知念, 沖縄, Aug. 28-Sep. 7, 2007

123 Kojima.K.; Tomita, A.,Quantum nondemolition measurement of photon-arrival for Bell state measurement,Asian Conference on Quantum Information Science 2007, Shiran-kaikan, Kyoto, Sep.3-6, 2007

124 小島邦裕; 富田章久,原子ー共振器系を用いた量子非破壊2光子ベル状態測定,日本物理学会 第62回年次大会, 北海道大学札幌キャンパス, 北海道, Sep. 21-24, 2007

125 Hayashi, M.,Prior entanglement between senders enables perfect quantum network coding,Asian Conference on Quantum Information Science 2007, Shiran-kaikan, Kyoto, Sep.3-6, 2007

126 Hayashi, M.,General theory for decoy-state QKD with arbitrary number of intensities,Asian Conference on Quantum Information Science 2007, Shiran-kaikan, Kyoto, Sep.3-6, 2008

127 Tomita, A.,Implementing QKD to metro-networks,Theory and Realisation of Practical Quantum Key Distribution, Waterloo, Canada, Jun. 11-14, 2007

128 Tomita, A.,Quantum key distribution system for metropolitan-area networks,Quantum Communications Realized, Optics East 2007, Boston, Sep. 9-12, 2007

129 Yoshino, K.; Tanaka, T.; Nambu, Y.; Tajima, A.; Tomita, A.,Dual-mode Time-bin Coding for Quantum Key Distribution Using Dual-drive Mach-Zehnder Modulator,European Conference on Optical Communication (ECOC), Berlin, Sep. 16-20, 2007

130 Tomita, A.,Experimental decoy state method for secure quantum key distribution,20th Annual Meeting of the IEEE Lasers and Electro-optics Society, Lake Buena Vista, Fl., USA, Oct. 21-25, 2007

131 Tomita, A.,安全な量子鍵配送技術の最新事情,量子暗号国際会議, 東京, Oct. 1-3, 2007

132 Kato, K.; Oto, M.; Imai, H.; Imai, K.,Coincidence of Voronoi Diagrams in a Quantum State Space,Asian Conference on Quantum Information Science 2007, Shiran-kaikan, Kyoto, Sep.3-6, 2007

133 Takahashi, T.; Imai, H.; Moriyama, S.,Maximum quantum violation of Bell inequalities as 2-Prover 1-Round Game,Asian Conference on Quantum Information Science 2007, Shiran-kaikan, Kyoto, Sep.3-6, 2008

134 Buscemi, F.; Hayashi, M.; Horodecki, M.,Information dynamics in quantum measurements: an entropic approach to the information-disturbance tradeoff problem,Noise, Information and Complexity @ Quantum Scale, Majorana Center, Erice, Italy, Nov. 4-11, 2007

135 Buscemi, F.,Entanglement loss along a channel,TQC2008, Tokyo University, Tokyo, Jan. 30-Feb. 1, 2008

136 LeGall, F.; Yamakami, T.,Self-Correcting Quantum Programs,第17回量子情報技術研究会(QIT17), 岡山市山陽新聞本社さん太ホール, Nov. 21-22, 2007

137 Kobayashi, H.; Matsumoto, K.; Tani, S.,Quantum Leader Election: How to Convert(Almost) Any Probabilistic Algorithm into Quantum Exact Algorithm, 第17回量子情報技術研究会(QIT17), 岡山市山陽新聞本社さん太ホール, Nov. 21-22, 2007

138 Buscemi, F.,Entanglement loss along a channel and approximate error correction,第17回量子情報技術研究会(QIT17), 岡山市山陽新聞本社さん太ホール, Nov. 21-22, 2007

139 高橋成五; 田島章雄; 富田章久,超小型APDモジュールを用いた量子暗号システム用光子検出器,第17回量子情報技術研究会(QIT17), 岡山市山陽新聞本社さん太ホール, Nov. 21-22, 2007

140 Takahashi, S.; Tajima, A.; Tomita, A.,A high efficiency single phonton

detector combined with an ultra-small APD module and a self-training discriminator for high speed quantum cryptosystem,The 13th Micro-optics Conference, 松山, Oct. 28-31, 2007

141 富田章久,究極のセキュリティー量子暗号の将来,日本光学会年次学術講演会, 大阪, Nov. 26-28, 2007

142 Tanaka, A.; Fujiwara, M.; Nam, S.-W.; Nambu, Y.; Takahashi, S.; Maeda, W.; Yoshino, K.; Miki, S.; Baek, B.; Zhen, W.; Tajima, A.; Tomita, A.; Sasaki, M.,97-km QKD field trial using PLC-based one-way interferometers, SSPDs and WDM synchronization,The Optical Fiber Communication Conference & Exposition and the National Fiber Optic Engineers Conference (OFC/NFOEC), San Diego, Feb. 24-28, 2008

143 Inui, Y.; Le Gall, F.,Quantum Property Testing of Group Solvability,11th Workshop on Quantum Information Processing (QIP 2008), New Delhi, India, Dec. 17-21, 2007

144 Inui, Y.; Le Gall, F.,Quantum Property Testing of Group Solvability,8th Latin American Theoretical Informatics Symposium (LATIN 2008), Buzios, Rio de Janeiro, Brazil, Apr. 7-11, 2008

145 富田章久; 廣嶋透也; 長谷川淳; 今井浩,定量的な安全性を永久に保証する量子暗号鍵配布システム,つくばテクノロジーショーケース, つくば国際会議場, Jan. 25-26, 2008

146 前田和佳子; 藤原幹生; Sae Woo Nam; 南部芳弘; 高橋成五; 田中聡寛; 吉野健一郎; 三木茂人; Burm Baek; 王鎮; 田島章雄; 富田章久; 佐々木雅英,97km 量子鍵配送フィールドトライアル,電子情報通信学会総合大会, 北九州学術研究都市, Mar. 18-21, 2008

147 南部芳弘; 吉野健一郎; 田中聡寛; 高橋成五; 前田和佳子; 田島章雄; 藤原幹生; 三木茂人; 王鎮; 佐々木雅英; Sae Woo Nam; Burm Baek; 富田章久,実用的なファイバ量子暗号システムに向けた集積光学とそのフィールド実証,第55回応用物理学関係連合講演会, 日大理工学部船橋キャンパス, Mar. 27-30, 2008

148 Tomita, A.,Performance measures on QKD systems (in Layer1),Telcordia Quantum Key Distribution Workshop, Piscataway, N.J., USA, Mar. 3, 2008

149 Inui, Y.; Le Gall, F.,Quantum Isomorphism Testing for Semidirect Product Groups,電子情報通信学会コンピュテーション研究会, 大阪府立大学, Apr. 18, 2008

150 Matsumoto, K.,Self-teleportation and its application on LOCC estimation and other tasks,The Eleventh Workshop on Quantum Information Processing, New Delhi, India, Dec. 17-21, 2007

151 Matsumoto, K.,Self-teleportation and its application on LOCC estimation and other tasks,the third Workshop on Theory of Quantum Information, Communication, and Cryptography (TQC 2008), The University of Tokyo, Tokyo, Jan. 30-Feb. 1, 2008

152 Matsumoto, K.,Asymptotic local copying of bipartite pure states,the third Workshop on Theory of Quantum Information, Communication, and Cryptography (TQC 2008), The University of Tokyo, Tokyo, Jan. 30-Feb. 1, 2008

153 Kato, K.; Imai, H.; Imai, K.,Error Analysis of a Numerical Calculation about One-qubit Quantum Channel Capacity,4th International Symposium on Voronoi Diagrams in Science and Engineering, ISVD 2007, Pontypridd, Wales, UK, 9-11 July 2007

154 Takahashi, T.; Imai, H.; Moriyama, S.; Avis, D.,Quantum correlation and semidefinite relaxation through 2-prover 1-round interactive proof,Annual Doctoral Workshop on Mathematical and Engineering Methods in Computer Science(MEMICS 2007), Hotel Galant, Mikulov, Czech Republic, Oct. 26-28, 2007

155 Okubo, Y.; Buscemi, F.; Tomita, A.,Proposal of an eavesdropping experiment

for BB84 QKD protocol with 1-2-3 phase-covariant quantum cloner,International Conference on Quantum Communication, Measurement and Computing (QCMC), University of Calgary, Canada, Aug. 19-24, 2008

156 Okubo, Y.; Buscemi, F.; Tomita, A.,Proposal of an eavesdropping experiment for BB84 QKD protocol with 1-2-3 phase-covariant quantum cloner,第18回量子情報技術研究会(QIT18), 東京大学小柴ホール, May 22-23, 2008

157 Tani, S.,Claw Finding Algorithms Using Quantum Walk,第18回量子情報技術研究会(QIT18), 東京大学小柴ホール, May 22-23, 2008

158 廣嶋透也,NPPT 束縛エンタングルメントの存在,第18回量子情報技術研究会(QIT18), 東京大学小柴ホール, May 22-23, 2009

159 Tomita, A.,Practical QKD system and field trial,The Information Security in a Quantum World (IQC) summer school, Waterloo, Canada, Aug. 7-11, 2007

160 富田章久; 中田武志; 水木恵美子; 牧田紀久; 夫高橋成五,ゲートモードアバランシェフォトダイオード光子検出器のアフターパルスモデル,電子情報通信学会総合大会, 明治大学生田キャンパス, Sep. 16-19, 2008

161 Tomita, A.; Tajima, A.; Nambu, Y.; Yoshino, K.; Maeda, W.; Takahashi, S.,High speed QKD system and its key transmission performances,XII International Conference on Quantum Optics and Quantum Information

162 Tanaka, A.; Tajima, A.; Tomita, A.,Quantum key distribution systems and field trials,European Conference on Optical Communication (ECOC), Brussel, Sep. 21-25, 2008

163 Le Gall, F.,Quantum Isomorphism Testing for Semidirect Product Groups,8th Asian Conference on Quantum Information Science (AQIS 2008), KIAS, Seoul, Korea, Aug. 25-31, 2008

164 Kojima.K.; Tomita, A.,Quantum information transfer between a photon and a V-type atomic system,8th Asian Conference on Quantum Information Science (AQIS 2008), KIAS, Seoul, Korea, Aug. 25-31, 2008

165 Tokuda, Y.; Hasegawa, J.,Analysis of Quantum Walk on Bipartite Graph against Decoherence Error,8th Asian Conference on Quantum Information Science (AQIS 2008), KIAS, Seoul, Korea, Aug. 25-31, 2008

166 Kobayashi, H.; Matsumoto, K.; Tani, S.,Fast Exact Quantum Leader Election on Anonymous Rings,8th Asian Conference on Quantum Information Science (AQIS 2008), KIAS, Seoul, Korea, Aug. 25-31, 2008

167 Fu, N.; Imai, H.,Shiftability of Atoms on a Lattice to Any Configuration in Minimum Moves,WAAC08: The 11th Japan-Korea Joint Workshop on Algorithms and Computation, 九州大学西新ホール, Jul. 19-20,2008

168 今井浩,量子情報と組合せ・半定値最適化,CoSS 組合せ最適化セミナー, 京都大学数理解析研究所, Jul. 28-30, 2008

169 Le Gall, F.,Quantum Algorithms for the Group Isomorphism Problem,第19回量子情報技術研究会(QIT19), 大阪府立大学, Nov. 20-21, 2008

170 石坂智; 廣嶋透也,漸近的量子テレポーテーション,第19回量子情報技術研究会(QIT19), 大阪府立大学, Nov. 20-21, 2008

171 今井浩,BDDを用いたグラフのTutte多項式計算の再考察,電子情報通信学会コンピューテーション研究会, 東北大学青葉山キャンパス, Oct. 10, 2008

172 Tomita, A.,Photonic systems for quantum information processing,8th Asian Conference on Quantum Information Science (AQIS 2008), KIAS, Seoul, Korea, Aug. 25-31, 2008

173 Kojima.K.,Mutual information transfer between a photon and a V-type atomic system,JST 主催　国際シンポジウムー量子技術に関する物理ー, 奈良県市公開堂, Nov. 25-28, 2008

174 小島邦弘; 富田章久,V 型3準位系と1光子との間での量子情報転写の効率と忠実性,第19回量子情報技術研究会(QIT19), 大阪府立大学学術交流会館, Nov. 20-21, 2008

175 Ito, T.; Kobayashi, H.; Matsumoto, K.,Oracularization and Two-Prover One-Round Interactive Proofs against Nonlocal Strategies,The Twelffth Workshop on Quantum Information Processing, Santa Fe, NM, USA, Jan. 12-16, 2009

176 Le Gall, F.,Efficient Isomorphism Testing for a Class of Group Extensions,26th International Symposium on Theoretical Aspects of Computer Science (STACS 2009), Freiburg, Germany, Feb. 26-28, 2009

177 Tomita, A.,Test and measurement on quantum key distribution systems,Photonics West 2009 Quantum Communication Realized Ⅱ, San Jose Convention Center, San Jose, CA, USA, Jan. 27-29, 2009

178 Imai, H.,Guaranteeing the security quantitive for a generalized decoy state quantum key protocol incorporationg finite satistics,JST 主催　国際シンポジウム－量子技術に関する物理－, 奈良県市公開堂, Nov. 25-28, 2008

179 Ambainis, A.; Iwama, K.; Nakanishi, M.; Nishimura, H.; Raymond, R.; Tani, S.; Yamashita, S.,Average/Worst-Case Gap of Quantum Query Complexities,The Twelffth Workshop on Quantum Information Processing, Santa Fe, NM, USA, Jan. 12-16, 2009

180 Kojima, K.,Biometrics Hash Functions against Quantum Adversaries,Mathematical and Engineering Methods in Computer Science (MEMICS2008), Znojmo, Czechia, Nov. 14-16, 2008

181 Kobayashi, H.; Le Gall, F.; Nishimura, H.; Roetteler, M.,General Scheme for Perfect Quantum Network Coding with Free Classical Communication,京都大学　数理解析研究所, 京都, April 17, 2009

182 Kobayashi, H.; Le Gall, F.; Nishimura, H.; Roetteler, M.,General Scheme for Perfect Quantum Network Coding with Free Classical Communication,広島大学, 広島, May 20-21, 2009

183 Hsieh, M.-H.; Wilde, M. M.,Public and private communication with a quantum channel and a secret key,CEQIP'09, Czech Republic, June 1-4, 2009

184 K. Kato, H. Imai and K. Imai,Smallest enclosing ball problem in a quantum state space and its application,Proceedings of the 5th International Symposium on Voronoi Diagrams in Science and Engineering (ISVD-2008), National Pedagogical University, Kyiv Ukraine, Sep. 22-28,2008

185 Matsumoto, K.,Asymptotic theory of LOCC estimation of quantum state,Quantum 2008:IV workshop ad memoriam of Carlo Novero Advances in Foundations of Quantum Mechanics and Quantum Information with atoms and photons, Turn, Italy, May 19-23, 2008

186 Matsumoto, K.,Prohibiting correlations between provers,Workshop on Quantum Algorithms and Complexity Theory, NUS, Singapore, November 17-21, 2008

187 Matsumoto, K.,On the first order asymptotic theory of quantum estimation,Recent Advances in Statistical Inference - in Honor of Professor Masafumi　Akahira、筑波大学, Dec. 15-17, 2008

188 Kobayashi, H.; Le Gall, F.; Nishimura, H.; Roetteler, M.,General Scheme for Perfect Quantum Network Coding with Free Classical Communication,The 36th International Colloquium on Automata, Languages and Programming, Rhodes, Greece, July 5-12, 2009

189 Ito, T.; Kobayashi, H.; Matsumoto, K.,Oracularization and Two-Prover One-Round Interactive Proofs against Nonlocal Strategies,The 24th IEEE Conference on Computational Complexity, Paris, France, July 15-18,2009

190 Tsujino, K.; Fukuda, D.; Fujii, G.; Takeoka, M.; Fujiwara, M.; Inoue, S.; Sasaki, M.,Experimental demonstration of near-optimal quantum receiver using a superconducting transition edge sensor,CLEO/EUROPE-EQEC 2009, Munich, Germany, June 14-19, 2009

191 Imai, H.,Quantum Computational Geometry and Quantum

Cryptography,2009 International Workshop on Computing, Academia Scinica, 台北 台湾 , June 16-17, 2009

192 Tsujino, K.; Tomita, A.,Positive operator valued measures for a practical single-photon avalanche diode,9th Asian Conference on Quantum Information Science AQIS'09, Nanjing, China, Aug. 26-29, 2009

193 Wilde, M-M.; Hsieh, M.-H.,Superactive entanglement generation with a zero-capacity quantum channel and a non-distillable shared state,9th Asian Conference on Quantum Information Science AQIS'09, Nanjing, China, Aug. 26-29, 2009

194 Sprojcar, J.,Contract signing using a multi-party non-local box,9th Asian Conference on Quantum Information Science AQIS'09, Nanjing, China, Aug. 26-29, 2009

195 Tanabe, Y.; Yoshizoe, K.; Imai, H.,A Study on Security Evaluation Methodology for Image based Biometrics Authentication Systems,IEEE Third International Conference on Biometrics: Theory, Applications and Systems, Washington DC, United States, Sep. 28-30, 2009

196 Hsieh, M.-H., Wilde, M.-M.,Optimal trading of classical communication, quantum communication, and entanglement in quantum Shannon theory,QIT 20, 広島大学 東広島キャンパス 学士会館, May 21-22, 2009

197 Kobayashi, H.; Matsumoto, K.; Tani, S.,Exactly Electing a Unique Leader is not Harder than Computing Symmetric Functions on Anonymous Quantum Networks,Twenty-Eighth Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing, Calgary, Canada, Aug. 10-12, 2009

198 Ambainis, A.; Childs, A.; Le Gall, F.; Tani, S.,The quantum query complexity of certification,LA シンポジウム, 松島 宮城県, Jul. 22-24, 2009

199 田中聡寛; 田島章雄; 富田章久,WDM による QKD 大量化の為の干渉計波長無依存化技術,電子情報通信学会総合大会, 新潟大学, Sep.15-18, 2009

200 Tomita, A.,A possible role of QKD in photonic networks,European Conference on Optical Communication (ECOC) Workshop 9, Wien, Austria, Sep.20-24, 2009

201 Hsieh, M.-H.; Yen, W.-T.; Hsu, L.-Y.,High performance entanglement-assisted quantum LDPC codes need little entanglement,第 21 回量子情報技術研究会(QIT21), 電気通信大学, Nov. 4-5, 2009

202 Sprojcar, J.,Multi-party quantum non-local boxes can be used to build contract signing protocol,第 21 回量子情報技術研究会(QIT21), 電気通信大学, Nov. 4-5, 2009

203 辻野賢治; 富田章久,APD を用いた単一光子検出器に対する POVM の再考,第 21 回量子情報技術研究会(QIT21), 電気通信大学, Nov. 4-5, 2009

204 長谷川淳; 田中聡寛; 富田章久,量子デバイスの時間変動のある QKD に対する受信再送攻撃の実証実験,第 21 回量子情報技術研究会(QIT21), 電気通信大学, Nov. 4-5, 2009

205 Sprojcar, J.,Are there any untraceable quantum ballots?,QIP 2010, 13th workshop on quantum information, ETH, Zurich, Switzerland, Jan. 15-22, 2009

206 Hsieh, M.-H.; Yen, W.-T.; Hsu, L.-Y.,High performance entanglement-assisted quantum LDPC codes need little entanglement,QIP 2010, 13th workshop on quantum information, ETH, Zurich, Switzerland, Jan. 15-22, 2010

207 辻野賢治; 富田章久,アバランシェフォトダイオード光子検出器における POVM の再検証,日本物理学会 第65回年次大会, 岡山市, March 20-23, 2010

208 Le Gall, F.,An Efficient Quantum Algorithm for some Instances of the Group Isomorphism problem,27th International Symposium on Theoretical Aspects of Computer Science (STACS2010), Nancy France, March 4-6, 2010

209 Kobayashi, H.; Le Gall, F.; Nishimura, H.; Roetteler, M.,Perfect Quantum

Network Coding with Free Classical Communication,QIP 2010, 13th workshop on quantum information, ETH, Zurich, Switzerland, Jan. 15-22, 2010

210 Tomita, A.,Quantum Key Distribution in Photonic Networks,International Conference on Quantum Information Technology, NII, Tokyo, Dec. 2-5, 2009

211 Tomita, A.,量子暗号実験－ BB84-Quantum Key Distribution in Photonic Networks,応用物理学会量子エレクトロニクス研究会「量子情報の最前線と今後10年の展開」, 軽井沢, 長野, Jan. 8-10, 2010

212 辻野賢治; 宮本義人; 片岡淳; 富田章久,Sub-Geiger mode InGaAs APD を用いた光子検出器の動作検証,第57回応用物理学関連連合講演会, 平塚市, 神奈川, March 17-20, 2010

213 Tomita, A.,Implementation of a High-Speed Quantum Key Distribution System for Metropolitan Networks,Optical Fiber Conference, San Diego, USA, March 21-26, 2010

214 Sprojcar, J.,Are there any untraceable quantum ballots?,TCQ 2010 5th Theory of Quantum Computation, Communication and Cryptography, Leeds, UK, Apr. 13-15, 2010

215 Hasegawa, J.; Tanaka, A.; Tomita, A.,Experimental Demonstration of Intercept-Resend Attack with Fluctuation of Quantum Devices on a Quantum Key Distribution,9th Asian Conference on Quantum Information Science AQIS'09, Nanjing, China, Aug. 26-29, 2009

216 Tanaka, A.; Tomita, A.; Tajima, A.,Colorless Interferometric Technique for Large Capacity Quantum Key Distribution Systems by Use of Wavelength Division Multiplexing,European Conference on Optical Communication (ECOC), Wien, Sep. 20-24, 2009

217 中田武志; 水木恵美子; 高橋成五; 牧田紀久夫; 富田章久,結晶性改良を施したメサ型 InAlAs-APD の光子検出特性,応用物理学会学術講演会, 富山大学, 富山, Sep. 8-11, 2009

218 廣嶋 透也,NPT 束縛エンタングルメントの存在問題,第22回量子情報技術研究会(QIT22), 大阪府立大学, May, 10-11, 2010

219 辻野賢治; 宮本義人; 片岡淳; 富田章久,Sub-Geiger mode InGaAs APD を用いた光子検出器の検証実験,第22回量子情報技術研究会(QIT22), 大阪府立大学, May, 10-11, 2011

220 Yoshizoe, K.,Quantum Computer Simulation Based on High Speed External Storage,CREST2010 International Symposium on Physics of Quantum Technology(2010 ISPQT), 一橋記念講堂 東京, Apr. 6-9, 2010

221 Kobayashi, H.; Le Gall, F.; Nishimura, H.; Roetteler, M.,Perfect Quantum Network Communication Protocol Based on Classical Network Coding,The 2010 IEEE International Symposium on Information Theory, Austin, TX, USA, Jun. 13-18, 2010

222 Hsieh, M.-H.,Entanglement-assisted quantum error correction,2010 International Workshop on Quantum Information Science, University of Tokyo, Mar. 8, 2010

223 Sprojcar, J.,Untraceable Quantum Ballots?,2010 International Workshop on Quantum Information Science, University of Tokyo, Mar. 8, 2010

224 Cheong, K.-Y.; Hsieh, M.-H.; Koshiba, T.; Toda, K. ,On quantum based oblivious transfer,2010 International Workshop on Quantum Information Science, University of Tokyo, Mar. 8, 2010

225 Tsujino, K.; Fukuda, D.; Fujii, G.; Takeoka, M.; Fujiwara, M.; Inoue, S.; Sasaki, M.,Sub-shot-noise-limit discrimination of on-off keyed coherent signals via a quantum receiver with a superconducting transition edge sensor,2010 International Workshop on Quantum Information Science, University of Tokyo, Mar. 8, 2010

226 Sprojcar, J.,Mayers-Lo-Chau entanglement attack and Rabin oblivious transfer,ASIACRYPT 2010, Singapore, Dec. 5-9, 2010
227 Sprojcar, J.,Are there any untraceable quantum ballots?,7th Central European Quantum Information Processing Workshop
228 Tsujino, K.; Miyamoto, Y.; Kataoka, J.; Tomita, A.,Expreimental demonstration of photon detector based on InGaAs avalanche photodiode with sub-Geiger mode operation,The Tenth International Conference on Quantum Communication, Measurement and Computation (QCMC), Brisbane, Queensland, Australia, July 17-23,2010
229 Fu, N.; Imai, H.,Explicit Shortest Path Functions of Periodic Graphs toward Investigations on Quantum Computation based on Periodic Structures,10th Asian Conference on Quantum Information Science(AQIS'10), The University of Tokyo, Tokyo, Aug.27-31, 2010
230 Satoh, T.; Van Meter, R.,Path Selection in Heterogeneous Quantum Networks,10th Asian Conference on Quantum Information Science(AQIS'10), The University of Tokyo, Tokyo, Aug.27-31, 2010
231 Tsujino, K.; Tomita, A.,Sub-Geiger Mode Silicon Avalanche Photodiode: Toward High Detection Efficiency,10th Asian Conference on Quantum Information Science(AQIS'10), The University of Tokyo, Tokyo, Aug.27-31, 2010
232 宮本義人; 辻野賢治; 片岡淳; 富田章久,低暗電流 InGaAs APD を用いたサブ・ガイガーモード光子検出器の検証,2010年秋季 第71回応用物理学会学術講演会, 長崎大学, Sep. 14-17, 2010
233 辻野賢治; 富田章久,サブ・ガイガーモード動作 SiAPD を用いた高効率・光子検出器の検討,2010年秋季 第71回応用物理学会学術講演会, 長崎大学, Sep. 14-17, 2010
234 Tsujino, K.; Miyamoto, Y.; Kataoka, J.; Tomita, A.,Phonton Counter Based on Avalanche Photodiode Operating In Sub-Geiger Mode,Updating Quantum Cryptography and Communications 2010(UQCC 2010), Tokyo, Oct. 18-20, 2010
235 Matsumoto, K.,On metric of quantum channel spaces,10th Asian Conference on Quantum Information Science(AQIS'10), The University of Tokyo, Tokyo, Aug.27-31, 2010
236 Matsumoto, K.,Reverse estimation, Reverse test, and Characterization of Quantum Relative Entropy,10th Asian Conference on Quantum Information Science(AQIS'10), The University of Tokyo, Tokyo, Aug.27-31, 2010
237 Hasegawa, J.; Tanaka, A.; Tomita, A.; Yorozu, S.,Experimental Demonstration of Intercept-Resend Attack with Time Fluctuation of Quantum Devices on QKD,Updating Quantum Cryptography and Communications 2010(UQCC 2010), Tokyo, Oct. 18-20, 2010
238 Cheong, K.-Y.; Hsieh, M.-H.; Koshiba, T.,A Weak Quantum Oblivious Transfer,10th Asian Conference on Quantum Information Science(AQIS'10), The University of Tokyo, Tokyo, Aug.27-31, 2010
239 Wilde, M-M.; Hsieh, M.-H.,Trading Resources in Quantum Communication,10th Asian Conference on Quantum Information Science(AQIS'10), The University of Tokyo, Tokyo, Aug.27-31, 2010
240 Suppakitpaisarn, V.; Edahiro, M.; Imai, H.,Minimal Weight Conversion Algorithm for Any Digit Sets and Its Analysis,21st International Workshop on Combinatorial Algorithms(IWOCA 2010), King's College London, Jul. 26-28, 2010
241 Fu, N.; Imai, H.; Moriyama, S.,Voronoi Diagrams on Periodic Graphs,The 7th International Symposium on Voronoi Diagrams in Science and Engineering (ISVD 2010), Laval University, Canada, Jun. 28-30, 2010
242 Tomita, A.,Interplay between Quantum Computation and Quantum

Information,10th Asian Conference on Quantum Information Science(AQIS'10), The University of Tokyo, Tokyo, Aug.27-31, 2010

243 Tomita, A.; Tajima, A.; Tanaka, A..; Yoshino, K.; Nambu, Y.; Takahashi, S.; Yorozu, S.,High-speed Quantum Key Distribution System for Metropolitan Networks,Updating Quantum Cryptography and Communications 2010(UQCC 2010), Tokyo, Oct. 18-20, 2010

244 Satoh, T.; Van Meter, R.,Path Selection in Heterogeneous Quantum Networks,FIRST Quantum Information Processing Project: Summer school 2010 in Okinawa, ホテルサンライズ知念, 沖縄, Aug. 18-28, 2010

245 Satoh, T.; Van Meter, R.,Path Selection in Heterogeneous Quantum Networks,2010 年秋 WIDE 研究会, 信州松代ロイヤルホテル, 長野, Sep. 8-11,2010

246 Fu, N.; Imai, H.; Moriyama, S.,On Solving Parametric Interger Linear Programming for Explicit Shortest Function on Periodic Graphs,The Third International Congress on Mathematical Software (ICMS 2010), 神戸大学, Sep. 13-17, 2010

247 Fu, N.; Imai, H.; Moriyama, S.,On Solving Parametric Interger Linear Programming for Explicit Shortest Function on Periodic Graphs,若手研究集会 −グレブナー基底の周辺−, 神戸大学, Oct. 9-10, 2010

248 辻野賢治,「ショット雑音限界を超えたコヒーレント光信号識別実験」～TES カロリーメータを用いた量子最適受信機～,東北大学電気通信研究所共同プロジェクト研究会, 東北大学, Nov. 15-16, 2010

249 辻野賢治; 富田章久,サブ・ガイガーモード動作 SiAPD 光子検出器:高検出効率を目指して,第 23 回量子情報技術研究会(QIT23), 東京大学, Nov. 15-16, 2010

250 Hasegawa, J.; Tanaka, A.; Tomita, A.,Experimental Demonstration of Influences of Fluctuation of Quantum Devices on Intercept-Resend Attack against Quantum Key Distribution,International Symposium on Quantum Nanophotonics and Nanoelectoronics(ISQNN 2009), 東京大学, Nov. 18-20, 2009

251 Kobayashi, H.; Le Gall, F.; Nishimura, H.; Roetteler, M.,Constructing Quantum Network Coding Schemes from Classical Nonlinear Protocols,The 28th International Symposium on Theoretical Aspects of Computer Science, Dortmund, Germany, Mar.10-12, 2011

252 Tanuma, T.; Imai, H.; Moriyama, S.,Revisiting Hyperbolic Voronoi Diagrams from Theoretical, Applied and Generalized Viewpoints,2010 International Symposium on Voronoi Diagrams in Science and Engineering (ISVD2010), Quebec, Canada, June 28-30, 2010

253 今井浩,Feynman の2つの提唱からグラフと計算量への展開,第 23 回量子情報技術研究会(QIT23), 東京大学, Nov. 15-16, 2010

(3)特許出願（SORST 研究の成果に関わる特許（出願人が JST 以外のものを含む））

	件数
国内出願	6 件
海外出願	1 件
計	7 件

(4)その他特記事項

〔プレス発表〕平成 19 年 1 月 17 日
安全性を定量的に保証する量子暗号鍵配布システムを開発
[掲載紙：日本経済新聞・朝日新聞・日経産業新聞・読売新聞・
電波新聞・日刊工業新聞・化学工業日報]

〔取材〕平成 19 年 1 月 23 日 東京新聞　永井記者
[掲載紙：東京新聞・中日新聞]

〔取材〕平成 19 年 4 月 17 日　政策科学研究所　川島氏・ESRI 担当　中川氏・
サイエンスライター　小林氏
[掲載紙：内閣府経済社会総合研究所編　イノベーション事例集 2007]

９．結び

当初研究の目標とした，現実的な設定のもとでの量子暗号システムの安全性解析は定量的な安全性を保証できる量子暗号システムの実証実験に結実した．この成果は世界的にも大きな影響を与え，量子暗号の安全性解析の進展の一つの流れを作ることができた．

このような理論と実験との連携は量子リーダ選挙の光子による実証とその能力の解析にも見ることができた．この他にも，量子分散計算の研究においても量子情報理論の手法を量子計算の問題に適用することで，量子マーリーン - アーサーアルゴリズムや量子ネットワークコーディングなどの問題に新しい知見を得ることができた．理論と実験，量子情報理論と量子計算といった異なるバックグラウンドを持つ研究者を結集して相互にアイディアや手法を交換し合うという本プロジェクトが特徴とする研究の仕掛けがまさに功を奏したものと考えている．

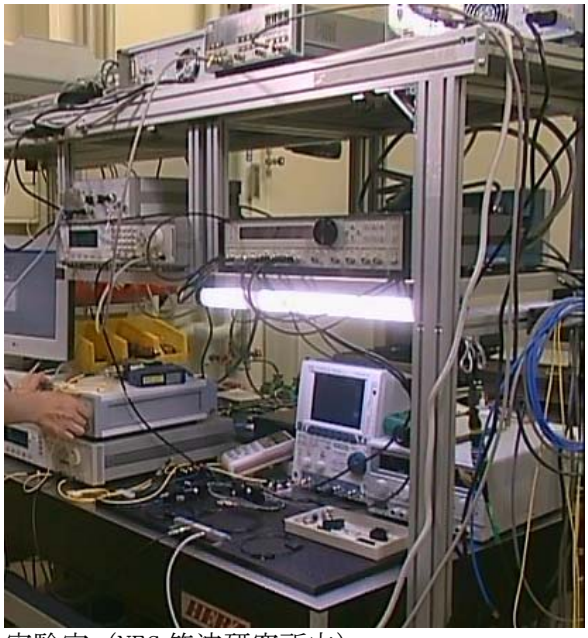
今後もこのような学際的な研究手法が量子情報科学の発展には欠かせないものと考えている．この意味で，オフキャンパスでの研究遂行を可能にした ERATO，ERATO－SORST の枠組みに感謝したい．量子情報技術は量子暗号システムの実用的なネットワーク稼働に見られるように，現実のものとなりつつあるが，真に大きなインパクトを社会に与えるためにはもう一度原理に戻ることも必要であると考えている．JST のような長期的かつ視野の広い研究支援を行える機構の役割はさらに重要である．

また，本プロジェクトの大きな成果として人材育成と量子情報研究の振興があると考えている．前身である ERATO プロジェクトは幅広い量子情報科学に関する国際会議（ERATO Conference on Quantum Information Science, EQIS）を毎年開催することで日本のみならず，アジアにおける分野の研究発展に貢献した．この国際会議は（Asian Conference on Quantum Information Science, AQIS）に発展し，本プロジェクトが直接主催することはなくなったが，EQIS での経験を生かし，毎回会議の運営に欠くことのできない援助をしてきた．本年 10 回目の会議を本プロジェクトで主催したが，各国の指導的な研究者から本プロジェクトの貢献について極めて高い評価が与えられた．この会議を継続し

て開催することによって量子情報科学の振興のみならず，この分野における日本のプレゼンス向上に有効であったと考えている．

また，ERATO プロジェクトおよび本プロジェクトでは日本国内と諸外国から有望な博士号取得者を研究者として採用したが，彼らの多くが量子情報分野で生産的で重要な成果をあげる中核的研究者に成長している．このことは人材育成のみならず，研究の国際交流としても意義深く，例えばイタリア出身の Buccemi 研究員は本プロジェクトでの研究の中でイギリスの研究者と交流を深め，さらにイギリスに渡って優れた成果をあげ，再び日本（名古屋大学）に戻って研究を進めている．この例は，本プロジェクトが国際的な研究交流を活発にし，さらにそのことが日本での研究アクティビティ向上につながったものであり，ERATO-SORST の枠組みの有効性を示している．

研究室風景(本郷)



実験室 (NEC 筑波研究所内)

EQIS-AQIS の 10 年：量子情報科学研究の振興と日本のプレゼンス向上に貢献した