# 今井量子計算機構プロジェクトの研究成果

目次

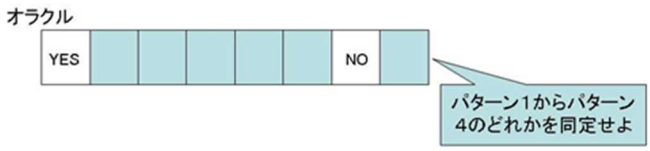
## 1. 量子計算

### 1-1. オラクル同定問題に対する量子アルゴリズム

**研究成果の概略**

計算において、問題に関する何らかの入力データを保持するデータベースへのアクセスやブラックボックスとして利用するサブルーチンへのアクセスの回数を減らすことは重要であり、それゆえ多くの研究がなされている。このとき　データベースやサブルーチンは数学モデルにおいてオラクル、オラクルへのアクセスは質問と呼ばれ、オラクルへのアクセス回数の削減とその限界に関する研究は質問計算量と呼ばれている。オラクル質問計算量に関しては、量子計算においても数多くされており、もっとも有名なものは、以下の Grover のアルゴリズムと呼ばれている量子アルゴリズムである。オラクルが N 個の質問項目を含み、各項目は Yes か No が記されているとする。簡単のためある項目のみが Yes と記されているとする。このとき Yes と答えられている項目を発見する問題（Grover の探索問題）に対して古典では Ω（N）回の質問を必要とするが、Grover の量子アルゴリズムではO（√N）回の質問で解くことが可能である。

我々は、オラクルを用いる計算の一般的な問題として、オラクル同定問題を考えた。図 1 はオラクル同定問題の例を表している。我々は、この問題に対する量子計算の質問計算量をオラクルのパターン数Mごとに詳細に解析した。その結果、Mが $2^N$よりも小さい場合、単純な Grover のアルゴリズムの適用よりも少ない質問回数でオラクルを同定する量子アルゴリズムの開発に成功した。特に、M＝Nの場合は Grover の探索問題を特別な場合として含んでいるが、我々が考案した量子アルゴリズムを使うとオラクルの同定でさえ依然O（√N）回の質問で十分である(1.)。




| 項目 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| パターン1 | NO | YES | YES | YES | NO | NO | NO | NO |
| パターン2 | YES | YES | NO | YES | NO | YES | YES | NO |
| パターン3 | YES | NO | YES | NO | YES | NO | NO | NO |
| パターン4 | NO | NO | NO | YES | YES | NO | NO | NO |

図 1.オラクル同定問題：可能なオラクルの中から一つを同定する。この例では第 0 項目に YES、第 6 項目に NO と書いてあるオラクルのパターンは第 3 パターンしかないので、2 回の質問でオラクルの同定ができる。

**成果展開可能なシーズ、用途等**

量子計算において、計算コストが非常に大きいデータへのアクセスやサブルーチンの呼び出し回数を最適にする一般的な手法。

**特許出願**

なし。

**報告書他**

1）Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Hiroyuki Masuda, Raymond H. Putra and Shigeru Yamashita, “Quantum Identification of Boolean Oracles, Proceedings of the 21st Symposium on Theoretical Computer Science,” Lecture Notes in Computer Science 3153, pp.839-850, 2004.

研究者名：岩間 一雄、河内 亮周、増田 裕之、山下 茂、Rudy Raymond Harry Putra

## 1-2. 負荷分散問題に対する量子アルゴリズム

### 研究成果の概略

Grover のアルゴリズムの応用の殆どは解の数が比較的小さいものに限られている。なぜならば解の数が大きい場合、古典でもランダムなサンプリングによってある程度高確率で成功するからである。しかし、そのような場合でも成功確率を高める上で 工夫をしたアルゴリズムがあれば望ましい。その１つの典型例は負荷分散（load balancing）問題である。N個のプロセッサがあると仮定する。M個のジョブは１つずつ到着し、各ジョブをN個のプロセッサの１つに割り当てなければならないときのプロセッサの負荷を最小化したい。この問題はN個のビンにM個のボールを入れるときの各ビンに積み上げられたボールの高さ（負荷）を最小化するという数学的問題（図 2）に置き換えられ、幅広く研究されている。

本プロジェクトでは、この問題に対する量子アルゴリズムを静的モデルと呼ばれる モデルにおいて考案した。静的モデルはM個のボールをＮ個のビンに１つずつ ランダムに入れていくという素朴なモデルである。古典では静的モデルでMがほぼＮに等しい場合、負荷は高確率で Θ（lnN/lnlnN） であることが知られている。本プロジェクトでは、量子計算を用いるとＭ＝Ｎの場合に静的モデルで負荷を２乗のオーダーで改善できることを証明した。この結果は(1.)(2.)に発表されている。

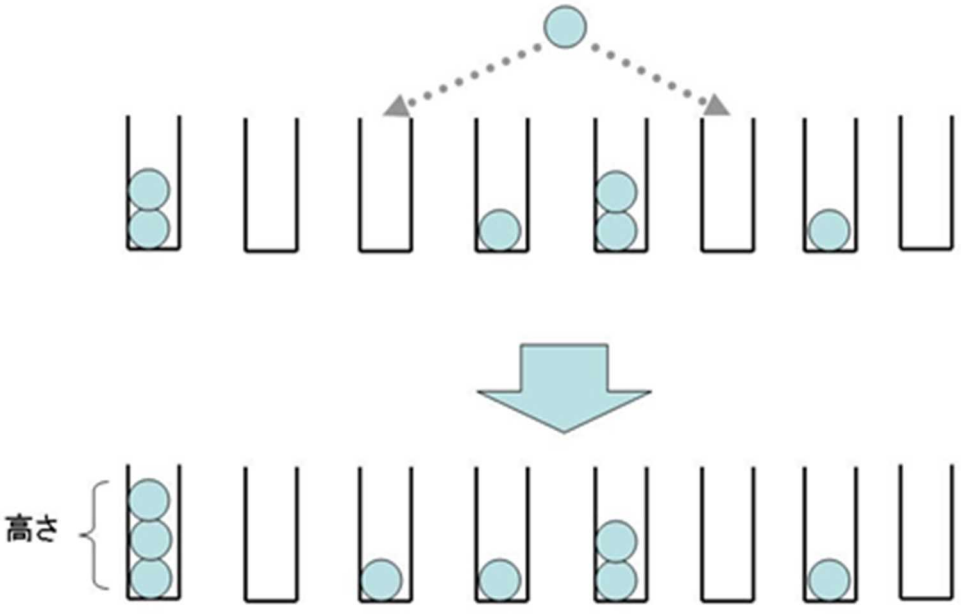



図 2.ビンとボールのゲーム： Ｎ個のビンにＮ個のボールを入れるとき、各ビンに積み上げられたボールの高さを最小化するゲーム。静的モデルでは、ランダムに選ばれたビンにボールは投入される。

**成果展開可能なシーズ、用途等**

古典的にすでに高い確率で解けるような問題に関しても、どのような場合に量子計算を用いる利点があるかについて明らかになった。また負荷分散問題は数多くの乱択アルゴリズムの解析の基礎となっており、その量子版を考えた場合の解析手法に関する知見を与えることができる。

**特許出願**

なし。

**報告書他**


1）Kazuo Iwama, Akinori Kawachi and Shigeru Yamashita, “Quantum Sampling for Balanced Allocations,” Proceedings of the 9th International Computing and Combinatorics Conference, Lecture Notes in Computer Science 2697, pp.304-318, 2003.

2）Kazuo Iwama, Akinori Kawachi and Shigeru Yamashita, “Quantum Sampling for Balanced Allocations,” IEICE Transactions on Information and Systems, Vol.E88-D No.1, pp.39-46, 2005.

3）Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Rudy Raymond, Shigeru Yamashita, “Quantum Identification of Boolean Oracles,” (Chapter 1 of Quantum Computation and Information: H. Imai and M. Hayashi eds., Springer 2006.)



研究者名：岩間 一雄、河内 亮周、山下 茂

## 1-3.　リーダ選挙問題に対する量子アルゴリズム

### 研究成果の概略

リーダ選挙問題は図 3 のようにネットワーク接続された計算機同士が、通信とローカルな計算を行うことにより中心となる計算機（リーダ）を自律的に決定する問題である。実分散環境において、特定の処理を行う計算機（リーダ）を決定すべき状況が数多く存在することから、分散計算の基本的問題として多くの研究がなされてきた。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。さらに、「各計算機が固有の識別子を持つ」とは限らないような、より一般的な条件のもとでも研究がなされており、計算機数が与えられている場合でも決定的には解けないことが証明されている。このような一般的な条件下でのリーダ選挙問題を匿名リーダ選挙問題と呼ぶ。

本プロジェクトでは、量子計算機同士が量子通信路で結ばれている場合（量子ネットワーク）、任意の計算機数および任意のネットワークトポロジーに対して有限時間かつ誤りなしで匿名リーダ選挙問題を解くアルゴリズムを発見した。これにより、任意の計算機数・ネットワークトポロジーに対して、量子ネットワークと古典ネットワークでは、その計算可能性について、決定的な違いがあることが明確になった。

これらの結果は(1.)(2.)で発表されている。

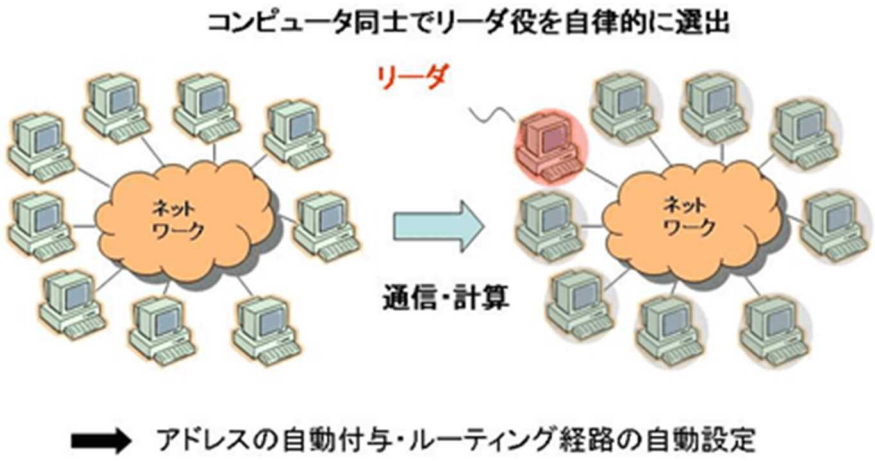



図 3.リーダ選挙問題

### 成果展開可能なシーズ、用途等

完全に自律分散的な手法による、アドレスの自動付与・ルーティング経路の自動設定。

**特許出願**

なし。

**報告書他**

1） Seiichiro Tani, Hirotada Kobayashi, and Keiji Matsumoto, “Exact Quantum Algorithms for the Leader Election Problem,” Proceedings of the 22nd Annual Symposium on Theoretical Aspects of Computer Science (STACS 2005), Lecture Notes in Computer Science 3404, pp.581-592, 2005.

2） Seiichiro Tani, Hirotada Kobayashi, and Keiji Matsumoto, “Quantum Leader Election via Exact Amplitude Amplification,” Proceedings of the 5th ERATO Conference on Quantum Information Science 2005. p. 11-12.

研究者名：谷 誠一郎、小林 弘忠、松本 啓史

## 1-4. 量子回路設計の提案

**研究成果の概略**

量子アルゴリズムを実現するためには、その量子アルゴリズムに相当する量子回路をできるだけ少ない基本ゲートの組み合わせで設計する必要がある。その中でも、古典的なブール関数を実現する量子回路の設計が本質的に重要である。古典的なブール関数は、Control-NOT(CNOT)タイプの論理ゲートを用いて実現できるため、CNOT ベースの論理設計理論の構築が重要である。そこで、我々は、CNOT ベースの量子回路設計のために、古典の回路設計では重要な概念である局所変換のルール集合を量子ブール回路に関しても提案し、そのルール集合が完全であることを証明した。ルール集合が完全であるとは、任意の回路から任意の回路にそのルール集合のルールのみで変換できることを意味する。また、提案した局所変換を組み合わせた複合ルールにより、図 4 の回路(A)をより低コストの回路(B)に変換する手法も考案した(1.)、(2.)。

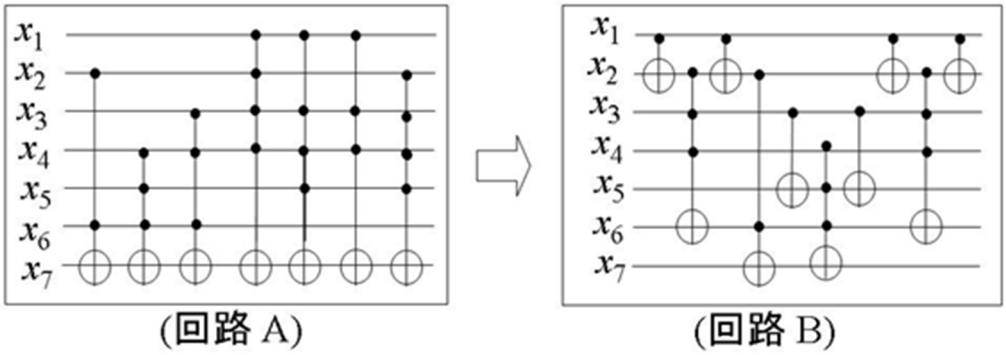



図 4.変換ルールを用いた回路の簡単化

**成果展開可能なシーズ、用途等**　効率的な量子回路設計。

**特許出願**　なし。

**報告書他**

1）Kazuo Iwama, Yahiko Kambayashi and Shigeru Yamashita, “Transformation Rules for Designing CNOT-based Quantum Circuits,” Proceedings of the 39th Design Automation Conference, 419-424, 2002.

2）Kazuo Iwama and Shigeru Yamashita, “Transformation Rules for CNOT-based Quantum Circuits and Their Applications,”　New Generation Computing 21(4) pp.297-317, 2003.

研究者名：岩間 一雄、山下 茂

## 1-5. 量子対話型証明系の研究

### 研究成果の概略

対話型証明は証明者と検証者の 2 人による通信モデルである。証明者は無限の計算能力を持ち、自分の主張を検証者に納得させるために最善を尽くす。一方、検証者は現実的な時間(多項式時間)内に証明者の主張の真偽を高い確率で正しく判定しなくてはならない。対話型証明はゼロ知識証明という現代暗号の基礎技術を提供する現代暗号理論の最重要概念の一つであり、また、証明という概念を計算機科学的に特徴付けるものとしても重要で、特に、その検証能力が対話をしない証拠検証型(非対話型)の場合を遥かに凌駕し、多項式空間で計算可能な問題クラス PSPACE と等価であることは 1990 年代における理論計算機科学の最重要結果の一つである。

この重要な拡張である多証明者対話型証明では、複数の証明者と 1 人の検証者との間の通信により検証を行う。このモデルのキーは各証明者間には通信を許さない点にあり、このため検証者は証明者間の矛盾を引き出すことでより強力な検証が可能で、その検証能力は PSPACE を遥かに凌駕し、非決定性指数時間で計算可能な問題クラス NEXP と一致する。本プロジェクトでは量子多証明者対話型証明(図 5)を初めてモデル化した。量子モデルにおける重要な特徴は証明者らが相関を事前共有する場合に現れる。つまり、古典的な事前相関は検証能力に影響しないが、量子的な事前相関は検証能力を変化させる可能性があり、実際、証明者間の事前量子相関を利用したより強力な検証の可能性を秘める一方、事前量子相関を利用した証明者らの不正な戦略が検証の正当性が失わせる例も知られている。本プロジェクトでは、証明者間に超多項式長の量子情報の事前相関がない限り量子モデルの検証能力は古典の場合を超え得ないことを示した。これは特に、事前量子相関がない場合には量子モデルの検証能力は古典の場合と等しいことを意味する(2.)(3.)。

本プロジェクトではさらに、非対話型モデルにおいても量子固有の性質に着目し、多証明者非対話型証明という量子特有のモデルを提案し、その性質解析の端緒を与えた(4.)。一方、ゼロ知識証明においても、非対話型量子完全ゼロ知識証明を定義してその能力を特徴付けることにより、グラフ自己非同型性判定問題などの重要な問題が非対話型量子完全ゼロ知識証明を持つことを示し、量子モデルにおいても安全なゼロ知識証明の初の例を与えた(1.)。

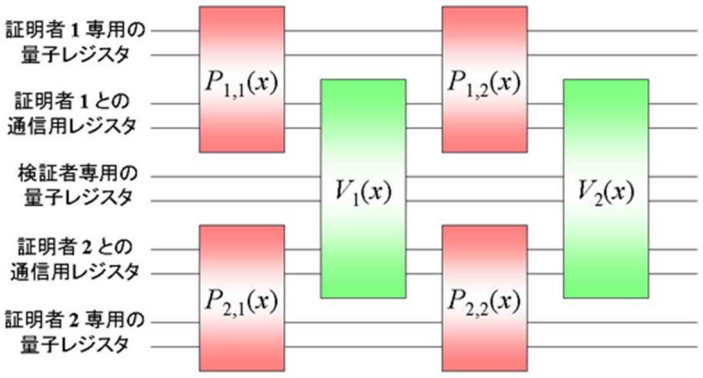



図 5.3 通信 2 証明者版量子対話型証明系：$P_1(\chi)$ は証明者 1 による計算、$P_2(\chi)$ は証明者 2 による計算、$V(\chi)$ は検証者による計算を表している。

**成果展開可能なシーズ、用途等**

量子暗号、特に多者間量子暗号システム構築のための基本プロトコルの提供、計算量理論、特に、量子計算機存在下での問題の難しさの程度の解析、エンタングルメント（量子もつれ）の性質解析。

**特許出願**

なし。

**報告書他**


1）Hirotada Kobayashi. Non-interactive quantum perfect and statistical zero-knowledge. In Algorithms and Computation, 14th International Symposium, ISAAC 2003, volume 2906 of Lecture Notes in Computer Science, pages 178-188, 2003.

2）Hirotada Kobayashi and Keiji Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. In Algorithms and Computation, 13th International Symposium, ISAAC 2002, volume 2518 of Lecture Notes in Computer Science, pages 115-127, 2002.

3）Hirotada Kobayashi and Keiji Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. Journal of Computer and System Sciences, 66(3):429-450, 2003.

4）Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? In Algorithms and Computation, 14th International Symposium, ISAAC 2003, volume 2906 of Lecture Notes in Computer Science, pages 189-198, 2003.



研究者名：小林 弘忠、松本 啓史

## 1-6. 量子公開鍵暗号の提案

### 研究成果の概略

暗号は情報理論的な（秘密鍵共有タイプ）暗号と計算量理論的な（鍵が非対称なタイプの）暗号（通称、公開鍵暗号）に大別される。情報理論的な方式は安全性を高く設定できるが、利便性の面で問題がある。一方、計算量理論的な方式は利便性がよい反面、素因数分解問題が難しいなどのある種の計算量的仮定が必要である。現在の量子暗号研究の中心である Bennett と Brassard による量子鍵配送プロトコルは情報理論的な暗号であり、現在の情報処理では不可能な秘密鍵暗号通信の安全性を達成できることが知られている。その一方で Shor のアルゴリズムとその後続研究により、量子計算機の前では現在の殆どの公開鍵暗号が破られてしまう。そこで本プロジェクトでは量子計算機に対しても安全な公開鍵暗号の構成のために、二つの量子状態が量子計算機でも効率的に識別することができないという、量子状態の計算量的識別不可能性という新しい暗号概念を導入し、それに基づいた量子公開鍵暗号を提案した（図 6）。具体的にはある特殊な 2 種類の量子状態を構成し、その二つをそれぞれ 0 と 1 に対応させることで暗号に利用する。これらの状態はある秘密情報を知っていると簡単に識別できるため、秘密情報を知っている受信者は容易に解読できるが、秘密情報を知らない盗聴者が解読するには現在量子計算機でさえ高速に解けていない問題（グラフ自己同型性判定問題）を解く必要があるため、量子アルゴリズムにブレークスルーをもたらすような技術革新なくしてその解読は困難である。本プロジェクトが提案した公開鍵暗号は量子計算機でさえ困難と思われる問題を解かない限り解読できないという意味で最初の計算量的安全性の証明を持つ量子公開鍵暗号である。この成果は(1.)において発表されている。

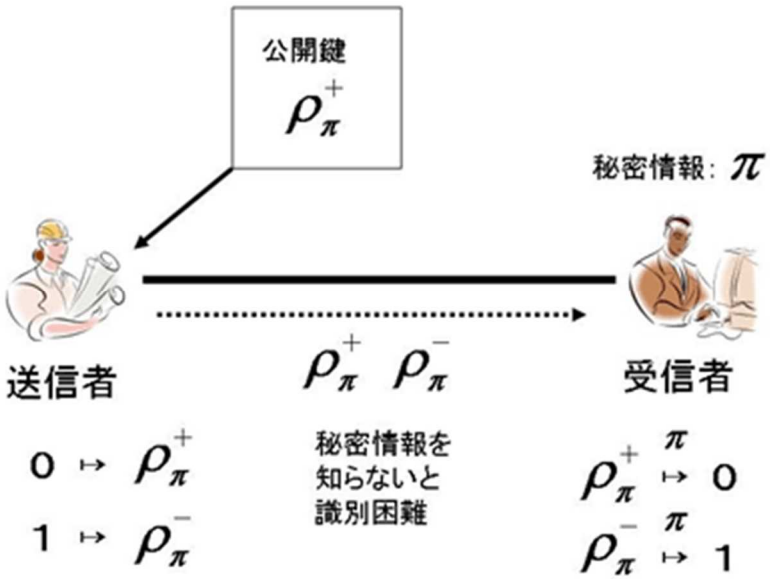



図 6.量子公開鍵暗号：送信者は公開鍵 $P^+_\pi$ を使ってビット 0 を送りたければ量子状態 $P^+_\pi$ に、ビット 1 を送りたければ量子状態 $P^-_\pi$ に暗号化。受信者だけが知る秘密情報 $\pi$ なしでは二つの状態を区別できない。

**成果展開可能なシーズ、用途等**

本プロジェクトで提案した量子状態の識別問題は非常に基本的な問題であるので、量子公開鍵暗号だけではなく、例えば電子署名といった様々な暗号システムの構成に応用することが考えられる。

**特許出願**

なし。

**報告書他**

1）Akinori Kawachi, Takeshi Koshiba, Harumichi Nishimura, and Tomoyuki Yamakami, “Computational Indistinguishability between Quantum States and Its Cryptographic Application,” Advance in Cryptography-Eurocrypt 2005, Lecture Notes in Computer Science 3494, pp.268-284, 2005.

2）Akinori Kawachi, Takeshi Koshiba, “Quantum Computational Cryptography,”（Chapter 7 of Quantum Computation and Information: H. Imai and M. Hayashi eds., Springer 2006.）

研究者名：河内 亮周、小柴 健史、西村 治道

## 2. 量子情報

### 2-1. 加法性

**研究成果の概略**

量子情報のいくつかの未解決問題は、ある量が加法的であるか否か、という 形をとっている。量子通信路の最適な古典情報伝送レートである Holevo 容量の加法性問題はその最も古いものである。また、エンタングルメントにおいては、entanglement of formation (EoF) とよばれる量の加法性、さらに強超加法性が予想されていた。この問題に関して我々は以下の成果を得た。

- 両者の間に一般的な強い関係があるのではないかと予想し、通信路と量子状態の間の MSW（Matsumoto-Shimono-Winter)対応と通信路状態の概念を提案し、両者の問題をはじめて一般的に関係付けることに成功した(1.)。（その後、Shor は我々の提案した概念を用い、Holevo 容量の加法性と EoF の加法性及び EoF の超加法性が同値であることを証明した。我々の研究は、両者の問題の関連を始めて Shor の証明の基本的ツールを提供した点で高く評価されている。）
- 対称性を持つ状態の EoF の加法性を示した(3.)(4.)(5.)、
- 半対称通信路の Holevo 容量が加法的であることを世界に先駆けて証明した(2.)。この通信路は最大 p ノルムの乗法性が成立しないことが Holevo と Werner によって示されていた。彼らはそれによって、加法性問題の否定的解決の可能性を示唆していた。（この成果は上記の対称性を持つ状態の EoF の加法性を MSW 対応を用いて Holevo 容量の加法性の問題に焼きなおすことで得た。）
- Holevo 容量の加法性は、必要なシグナルの状態の数が多いほど加法性が成り立ちにくいと考えられている。そこで、qubit 通信路において、必要なシグナルの状態の数を最大にする通信路を探し出し（図 7)、その加法性を数値的にであるが証明した(6.)。
- その他、特殊な状態において EoF の加法性を証明し、4 キュービットにおいて、超加法性の数値的検証（図 8）を行なった(8.)。
- 上記の加法性予想とその可能性が同値となる量を一つ提案した(7.)。
- 加法性問題の同値性の証明を再検証し、その構造を明らかにした(9.)。

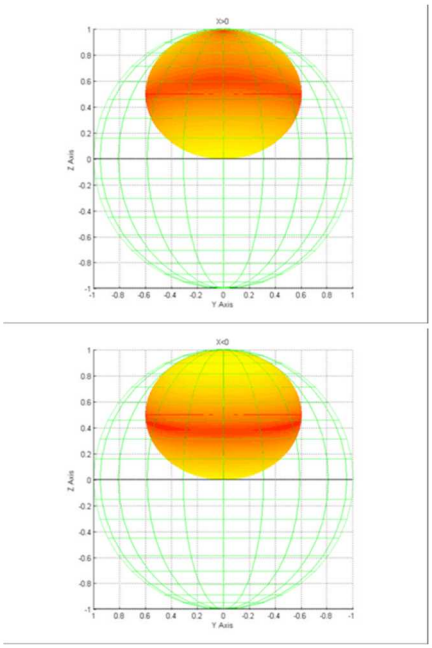


図 7.必要なシグナルの状態数が最大（４つ）になる qubit 通信路

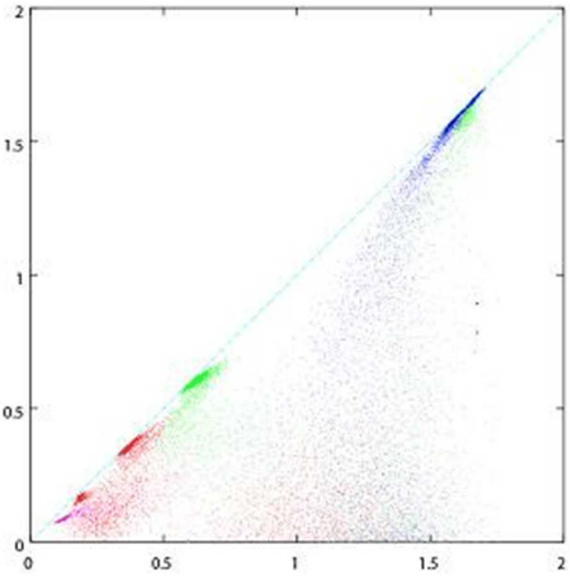


図 8.4 キュービット系における 8,000 状態の EoF の超加法性の破れの数値的検証。破線の上側が超加法性の破れに対応する。上の図では全て破線の下側になり、超加法性の破れは検出されなかった。

**成果展開可能なシーズ、用途等**

この問題を解決することで、量子通信路を用いた通信を行なった場合での通信速度の理論的限界に導出 することが期待できる。また、同時に、エンタングルメントの定量化に一定の知見を得ることができる。

**特許出願**

なし。

**報告書他**


1) K. Matsumoto, T. Shimono, and A. Winter, “Remarks on additivity of the Holevo channel capacity and of the entanglement of formation,” Comm. Math. Phys. 246(3), pp. 427-442, (2004).
2) K. Matsumoto and F. Yura, “Entanglement Cost of Antisymmetric States and Additivity of Capacity of Some Quantum Channel,” J. Phys. A: Math. Gen. 37, L167-L171, (2004).
3) F. Yura, “Entanglement Cost of Three-Level Antisymmetric States,” J. Phys. A: Math. Gen., 36, L237, (2003).

4) T. Shimono, “Towards additivity of entanglement of formation. 3rd International Conference on Unconventional Models of Computation,” rd International Conference on Unconventional Models of Computation (UMC’02), Kobe, Japan, Oct. 15-19, 2002.
5) T. Shimono, “Additivity of Entanglement of Formation of Two Three-Level-Antisymmetric States,” International Journal of Quantum Information, Vol. 1, No. 2. pp.259-268, 2003.
6) M. Hayashi, H. Imai, K. Matsumoto, M.B. Ruskai, and T. Shimono, “Qubit Channels Which Require Four Inputs to Achieve Capacity: Implications for Additivity Conjectures,” Quantum Inf. Comput. 5, pp. 13-31, (2005).
7) Keiji Matsumoto, “Yet another equivalent additivity conjecture,” ERATO conference on Quantum Information Science 2005 (EQIS 05), JST, Tokyo, Japan, Aug. 26-30, 2005.
8) T. Shimono, H. Fan, “Numerical Test of Superadditivity of Entanglement of Formation for Four-Qubit States,” ERATO conference on Quantum Information Science 2003 (EQIS 03), Niijima Kaikan, Kyoto, Japan, Sep. 4-6, 2003.
9) Masahito Hayashi, An Introduction to Quantum Information Theory, Springer (2006) 。
10) Keiji Matsumoto, “On additivity Questions,” (Chapter 6 of Quantum Computation and Information: H. Imai and M. Hayashi eds., Springer 2006.)

研究者名：今井 浩、松本 啓史、Fan Heng、由良 文孝、下野 寿之、林 正人

## 2-2. エンタングルメント純粋化

### 研究成果の概略

多くのプロトコルでは 最大エンタングル状態を遠隔地間で共有する必要があるが、それは多くの場合困難である。そこで、まずややエンタングルメントの小さい状態を作り、そこから最大エンタングル状態を引き出すことが必要になる。入力状態が純粋状態の場合、これを entanglement concentration、混合状態の場合、entanglement distilation とよばれる。

我々は、入力として与えられる状態が 未知の純粋状態の場合に最適なプロトコルを提案した。そして、その性能が 入力状態が既知の場合とほぼ変わらないこと、すなわち漸近一次の項までは一致していることを証明した。また、本プロトコルの出力からエンタングルメント量の最適な推定量が得られることがわかった(5.)(6.)(7.)。この研究においては、推定理論や universal compression と同様に、群の表現論がフルに用いられた。現在、群の表現論を用いる研究は徐々に 量子情報の中で注目を集めつつあるが、我々の研究はそのさきがけをなすものである。

入力の状態が既知の場合においては、最大エンタングル状態の質に関する制約を連続的にかえたときの生成率の変化(図 9)を議論した(3.)。これにより、従来ギャップのあった、「決定論的」スキームと「近似的」スキームの間を連続的に繋ぐことに成功した。さらに、その研究の一般化にも成功した(2.)。 また、entanglement distilation に関しては、誤り訂正符号の成果を応用する形で成果を上げた(4.)。

その他、混合状態の場合については、entanglement distilation はほとんど知られていないが、今回、我々は、２つの最大エンタングル状態の混合となる場合は常に、最大相関状態となることを示した。これにより、２つの最大エンタングル状態の混合となる場合は常に、最大相関状態となる場合での、entanglement distilation を求めた(1.)。

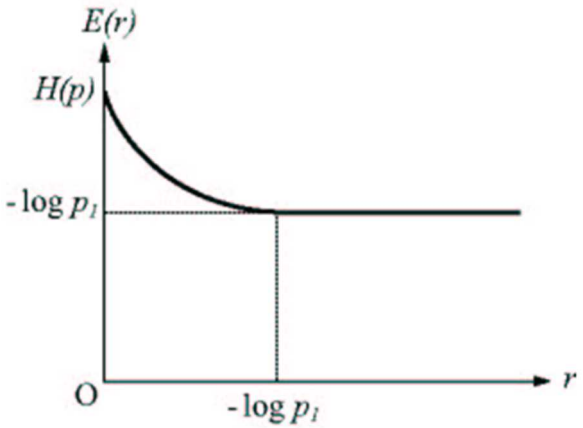



図 9.生成される最大エンタングルド状態の忠実度に対する制限ｒと 最大エンタングルド状態の生成率Ｅ（ｒ）との関係。

**成果展開可能なシーズ、用途等**

量子テレポーテーション、量子デンスコーディング、量子エンタングルメントなど。

**特許出願**

なし。

**報告書他**


1）H. Hiroshima, M. Hayashi, “Finding a maximally correlated state: Simultaneous Schmidt decomposition of bipartite pure states,” Phys. Rev. A 70, 030302 (R) (2004).

2）Hayashi, M. “General formulas for fixed-length quantum entanglement concentration,” To appear in IEEE Trans. Information Theory May (2006).

3）M. Hayashi, M. Koashi, F. Morikoshi, K. Matsumoto, and A. Winter, “Error exponents for entanglement concentration,” J. Phys. A: Math. Gen. 36, 527, (2003).

4）M. Hamada, “Teleportation and entanglement distillation in the presence of correlation among bipartite mixed states,” Phys. Rev. A 68, 012301 (2003).

5）K. Matsumoto, M. Hayashi, “Universal entanglement concentration,” Submitted to Phys. Rev. A.

6）Hayashi. M; Matsumoto, K. “Universal distortion-free entanglement concentration achieving the optimal rate,” SITA 2001, 第 24 回情報理論とその応用シンポジウム, 神戸国際会議場, Dec. 4-7, 2001.

7）Matsumoto, K.; Hayashi, M. “Universal distortion-free entanglement concentration,” IEEE International Symposium on Information Theory, Chicago, USA, June 27-July 2, 2004.


研究者名：松本 啓史、林 正人、浜田 充、廣嶋 透也

## 2-3. エンタングルド状態についての仮説検定と状態識別

### 研究成果の概略

量子系での実験より生成された状態が、本当に所望の状態であるか、否か判定するには、必ずしも状態を記述するパラメータを推定する必要はなく、その判断に対して必要な情報についてのみ最適な測定を行なった方が、より効率的である。そのような設定は仮説検定と呼ばれる。我々はこの問題に対して、以下の成果を得た。

- 理論的な設定として、局所量子操作と古典通信からなる任意の量子測定に限って、問題の持つ対称性の下で、検定のための測定について最適化を行ない、最適測定を導出した(2.)。
- 量子光学系で実装できるより限られた測定のクラスでこの最大エンタングルド状態の判定問題に有効な実験スキーム及び事後の情報処理スキームを前提知識に応じた形で提案し、それについての実証実験を SPDC(自発的パラメットリック加法変換)によって行なった(3.)。
  - ・単位時間あたりの光子の生成率が不明の場合について扱った。この場合については、visibility とよばれる手法が用いられるが、これよりも優れた性能を持つ手法を提案した(3.)。
  - ・単位時間あたりの光子の生成率が既知の場合を扱い、最適な測定を導出した。これと同種の測定は D'Ariano らによっても提案され、実験的に実装されているが、正確な統計的仮説検定の定式化に基づいた事後の情報処理を行なっておらず、十分とは言い切れない。我々の研究で、始めて統計的仮説検定のための事後の情報処理まで含めた定式化が行なわれた(1.)、(3.)。
  - ・ノイズが偏っている場合についても扱った。具体的には、ノイズの方向に応じて、適応的に各方向の測定時間を調節するのである。実際、パラメトリック下方変換によって生成された最大エンタングルド状態は特定方向に偏ったノイズを持つことが知られている。事実、我々が行なった実験では、適応的な測定時間選択を行なった場合の方が検定精度が改良されている(1.)、(3.)。
- 一方、互いに直交する最大エンタングルド状態は局所次元を d とすると、d 2 個存在する。我々は、局所操作と通信の組み合わせで誤り確率 0 で識別が可能となる最大エンタングルド状態の最大個数が d であることを示した(4.)、(5.)、(6.)。

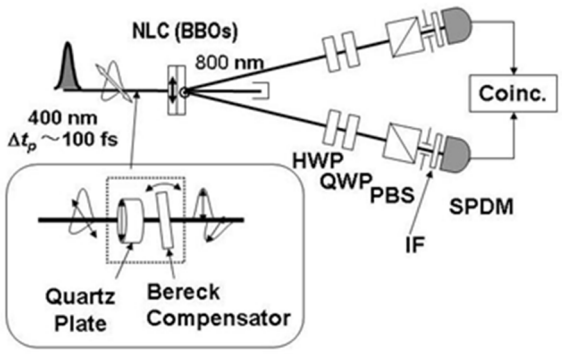



図　自発的パラメトリック下方変換による
エンタングルド状態生成の実験

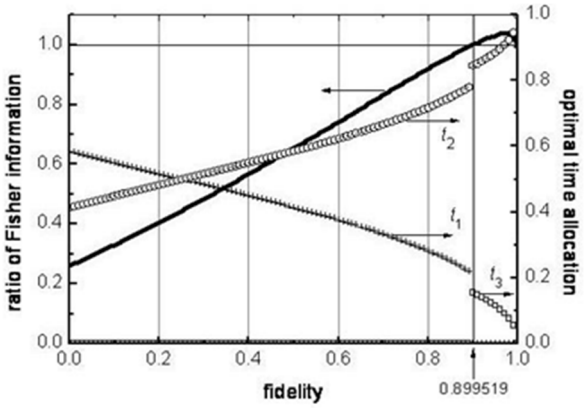



図　最適 Fisher 情報量の比、及び最適な時間配分

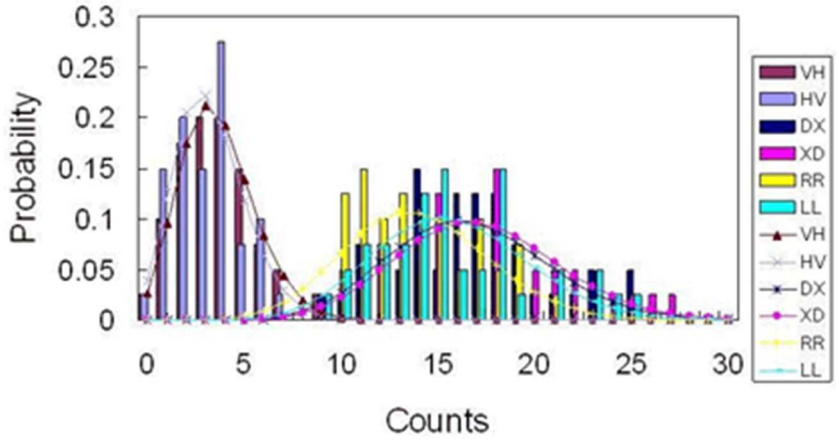



図　各測定基底の 1 秒後ごとの検出個数を測定。
棒グラフは測定基底ごとに 40 回行ったときの基底ごとの検出個数の頻度。
グラフはそれを近似するポアソン分布。

**成果展開可能なシーズ、用途等**

量子情報の分野では様々な情報処理のリソースとして、最大エンタングド状態に対する需要が高まっている。しかし、量子系である以上、いくら高性能の実験器具を使ったとしても、量子状態であるため、測定を通じた性能評価（性能の検証）は不可欠である。したがって、この最大エンタングルド状態の検定は 実験で生成した最大エンタングルド状態の精度を保証する手段として、利用されることと思われる。

**特許出願**

なし。

**報告書他**

1) Y. Tsuda, B.S. Shi, A. Tomita, M. Hayashi, K. Matsumoto, Y.K. Jiang, “Hypothesis testing for an entangled state produced by spontaneous parametric down conversion,” ERATO conference on Quantum Information Science 2005 (EQIS 05), JST, Tokyo, Japan, Aug. 26-30, 2005.

2) Y. Tsuda, K. Matsumoto, M. Hayashi, “Hypothesis testing for a maximally entangled state,” Submitted to J. Phys. A: Math. Gen.

3) M. Hayashi, B.S. Shi, A. Tomita, K. Matsumoto, Y. Tsuda, Y.K. Jinag, “Hypothesis testing for an entangled state produced by spontaneous parametric down conversion,” Submitted to Phys. Rev. A.

4) H. Fan, “Distinguishability and Indistinguishability by Local Operations and Classical Communication,” Phys. Rev. Lett. 92, 177905 (2004).

5) M. Hayashi, D. Markham, M. Murao, M. Owari, S. Virmani, “Bounds on Multipartite Entangled Orthogonal State Discrimination Using Local Operations and Classical Communication,” Phys. Rev. Lett. 96, 040501 (2006).

6) M. Owari, M. Hayashi, “Local copying and local discrimination as a study for non-locality of a set,” Submitted to Phys. Rev. A.

研究者名：松本 啓史、林 正人、津田 美幸、尾張 正樹、Fan Heng 富田 章久、
Bao-Sen Shi、Yun Kun Jiang

## 2-4. 量子状態複製操作

### 研究成果の概略

我々は量子状態の近似的な複製操作についても扱った。例えば、与えられた状態が未知の純粋状態の n 個のコピーである場合の最適な近似的複製は Werner によって与えられている。我々はこれを実行するための、ハミルトニアンを構成した(2.)。さらに、未知状態が特定の部分集合に含まれている場合、その情報を利用して、どの程度近似複製の精度が向上するか、幾つかの具体例について検討した(1.)(3.)。

さらに、局所操作に限った場合での複製についても考察した。任意の量子操作が許されている場合、複製したい状態がある直交基底のどれかであることが既知である場合は、誤りなしに完全な複製が可能である。我々は、この設定で、我々の操作が局所操作と古典通信に限られている場合について、複製したい未知状態が最大エンタングルド状態の場合にこの問題を扱った。その結果、未知状態の候補が最大で少なくとも d 個（局所空間の次元）までの最大エンタングルド状態の場合、完全な複製が局所操作で可能であることがわかった(4.)。

また、d が素数である場合については、候補となる最大エンタングルド状態の数が d を超えると不可能であることも示した(4.)。

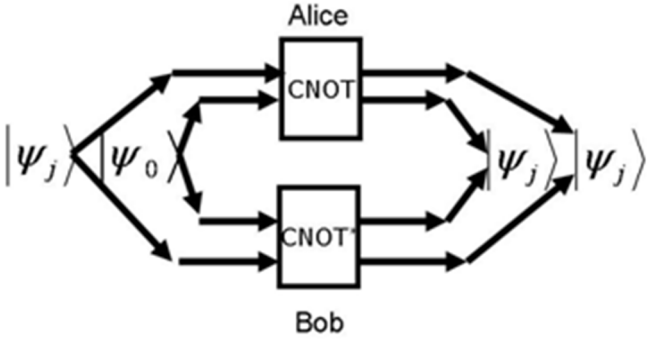



図 10.局所操作による最大エンタングルド状態のコピー

### 成果展開可能なシーズ、用途等

このような近似的複製については、量子ネットワークコーディングなどの他の量子プロトコルに利用されることが期待できる。

### 特許出願

なし。

**報告書他**

1）H. Fan, K. Matsumoto, M. Wadati, “Quantum cloning machines for equatorial qubits,” Phys. Rev. A 65 , 012304, 2001.

2）H. Fan, G. Weihs, K. Matsumoto, H. Imai, “Cloning of symmetric d-level photonic states in physical systems,” Phys. Rev. A 66, 024307, 2002.

3）H. Fan, H. Imai, K. Matsumoto, X.B. Wang, “Phase-covariant quantum cloning of qudits,” Phys. Rev. A 67, 022317 (2003).

4）M. Owari, M. Hayashi, “Local copying and local discrimination as a study for non-locality of a set,” Submitted to Phys. Rev. A.

5）H. Fan, “Quantum Cloning Machines,” (Chapter 4 of Quantum Computation and Information: H. Imai and M. Hayashi eds., Springer 2006.)

研究者名：Fan Heng、松本 啓史、尾張 正樹、林 正人、今井 浩、Wang Xiangbin

## 2-5. 状態をほとんど破壊しない測定による状態推定

### 研究成果の概略

量子系では系に対する情報を得るために、測定を行なうと、系の状態は不可避的に破壊される。そのため、量子系では、入力状態に応じて符号長を決める情報源符号化は不可能であると考えられていた。

しかし、効率的な符号化が可能となる符号長の決定のために必要な情報を獲得するには、極めて緩やかな測定で十分であることを我々は発見した。すなわち、状態推定にも 2 種類の誤差があり、真値の近傍での若干のズレによる誤差と、真値から十分に離れることによる誤差の 2 種類がある。もちろん、前者の誤差が起きる確率は、後者の誤差が起きる確率に比べると格段に大きい。しかし、わずかな確率ではあるが、後者の誤差が起きた場合のリスクは極めて大きい。一般に多くの場合、前者の誤差は平均 2 乗誤差で測られ、後者の誤差は大偏差型の評価によって測られる。統計学では、主に前者の誤差に関する議論をすることが主流である。一方、情報理論の符号化定理などでは、結果的に、大偏差型の評価を行なっている。

今回、我々は、大偏差型の誤差を最適にする測定を行なっても、ほとんど状態を破壊されないことを示した。この結果を量子ユニバーサル情報源圧縮に適用し、ユニバーサルにエントロピーレートを達成する符号を構成した(1.)、(2.)。

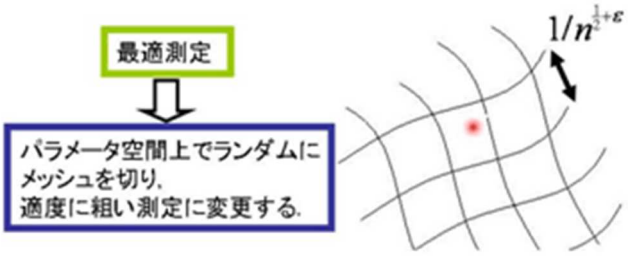



図 11.状態をほとんど破壊しない測定

### 成果展開可能なシーズ、用途等

このような測定は、ユニバーサル情報源圧縮に有効であるだけでなく、Reverse Shannon 定理の証明などに用いられると考えられている。このように理論的な意義は明確であるが、実用的にどの程度有効であるかについては今後の研究が待たれる。

### 特許出願

なし。

**報告書他**

1） M. Hayashi and K. Matsumoto, “Quantum universal veriable-length source coding,” Phys. Rev. A 66, 022311, (2002).

2） M. Hayashi and K. Matsumoto, “Simple construction of quantum universal variable-length source coding,” Quantum Information and Computation, Vol.2 (special), pp. 519-529, (2002).

研究者名：林 正人、松本 啓史

## 2-6. 幾何的位相

### 研究成果の概略

サイクリックな運動において獲得される位相因子は、力学的位相と幾何学的位相の和で表されるが、いくつかの理由から後者は前者よりも擾乱にたいして頑健であると考えられている。この点に着目した Ekert らは力学的位相を巧妙に打ち消し、システムのエラーに強いと思われる量子計算機構を提案した。しかし、彼らの提案は断熱過程を用いているため、動作速度に大きな難点がある。また、力学的位相を打ち消すためにやや複雑なサイクルが必要であった。 我々の方針は断熱過程をさけ、また最初から力学的位相のないサイクルを用いることで、高速で単純なスキームを構成することであった。前者のために、Berry の理論を非断熱過程に拡張した Aharanov-Anandan の理論を用いた。そして当初は Ekert の提案の変形からはじめ(1.)、最終的には一つのゲートの実現に二つの回転だけで十分な方法を考案した(図 12、(2.)、(3.))。

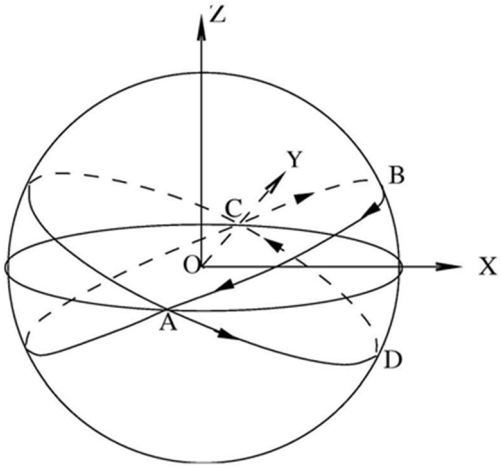



図 12.非断熱過程を用いた幾何学的量子計算のスキーム

### 成果展開可能なシーズ、用途等

量子処理の物理的実装の手段の 1 つとして有効である。

### 特許出願

なし。

### 報告書他

1) X.-B. Wang and K. Matsutmoto, “Non-adiabatic conditional geometric phase shift with NMR,” Phys Rev. Lett. 87, 097901, (2001), and (E) Phys. Rev. Lett. 88, 179901, (2002).
2) X.-B. Wang and K. Matsutmoto, “NMR C-NOT gate through Aharanov-Anandan’s phase shift,” J. Phys. A: Math. Gen. 34, L631, (2001).
3) X.-B. Wang and K. Matsutmoto, “Non-adiabatically detecting the geometric phase of the macroscopic quantum state with symmetric SQUID,” Phys. Rev. B 65, 172508, (2002).

研究者名：Wang Xiangbin、松本 啓史

## 2-7. 線型光学素子を用いた量子情報処理

### 研究成果の概略

フォトンは伝搬速度が早くデコヒーレンスがおこりにくい。また、粒子毎の操作は極めて容易である。一方、複数の粒子に跨がった操作は、ビームスプリッターなどのいわゆる線型光学素子以外は現時点での利用は難しい。

現在の量子暗号の実装は例外なくフォトンを用いているが、それはプロトコルの中で複数の粒子に跨がった操作が必要ないからである。しかし、将来的には伝送距離の向上のためには量子中継がほぼ必須だと思われる。また、よりノイズに強いプロトコルを目指すためには、多少の粒子間操作が必要になると思われる。そこで、われわれは、以下の操作の線型光学素子での実現を考案した。

1) スワッピングを用いた entanglement concentration(5.)

2) post-selection を用いない entanglement concentration(2.)

3) 誤り検出符号(3.)

上記 1-3 は量子中継実現のための部品である。1 は entanglement concentration と スワッピングを同時に実現するプロトコルであり、両者を別個に実現するよりも効率が高く、より単純な実装になる。2 は観測による post selection を用いない、entanglement concentration の実証実験の提案である。

3 は誤りを訂正せずに 検出だけを行うもので、誤り訂正よりも単純なシステムになる（図 13）。量子中継の場合、失敗時のやり直しが可能なため、特に誤り検出符号が有効である。

また、基礎研究として、ビームスプリッターで生成できる状態の数学的特徴付を試みた(1.)、(2.)。

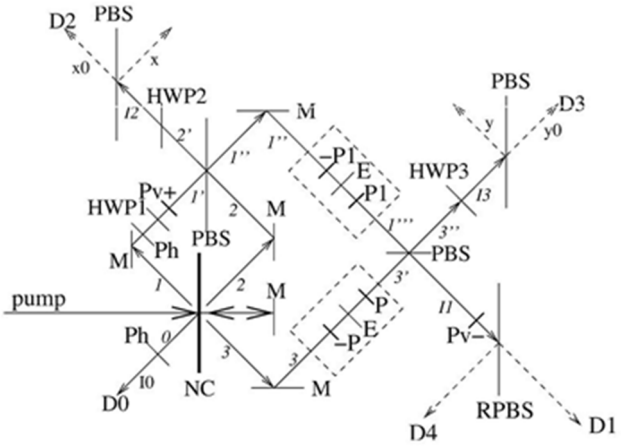



図 13.線形光学系を用いた誤り検出符号のスキーム

**成果展開可能なシーズ、用途等**

エンタングルド状態の生成、量子暗号

**特許出願**

なし。

**報告書他**

1）X. B. Wang, “Properties of a beam-splitter entangler with Gaussian input states,” Phys. Rev. A 66, 064304, (2002).
2）X. B. Wang, “Theorem for the beam splitter entangler,” Phys. Rev. A 66, 024303, (2002).
3）X.-B. Wang, “Quantum error rejection code with spontaneous parametric conversion,” Phys. Rev. A 69, 022320, (2004).
4）X.-B. Wang, “Quantum key distribution with 2-bit quantum codes,” Phys. Rev. Lett. 92, 077902, (2004).
5）X.-B. Wang, B.S. Shi, A. Tomita, and K. Matsumoto, “Quantum entanglement swapping with spontaneous parametric down-conversion,” Phys. Rev. A 69, 014303, (2004).

研究者名：Wang Xiangbin、松本 啓史、Bao-Sen Shi, 富田 章久

## 2-8. 量子計算プロセスの数値的研究

### 研究成果の概略

量子計算機は高度に複雑な物理系であり、その時間発展を完全に解析的に求めることは不可能である。そこで、われわれは、並列計算機を用いた数値計算によって、量子計算プロセスへの物理的ノイズの影響を研究した。

まず、第一に量子計算プロセスの高速なシミュレーションを可能にするためのシミュレーターを開発した。これは共有メモリー型並列計算機の特性をフルに活かせるように様々な工夫がなされている(1.)。

このシミュレータを用い、誤り訂正符号を入れ子にせず、一段だけ適応した場合、どの程度デコヒーレンスを抑えることが出来るかを調べた。適切に誤り訂正の間隔をあけることで、デコヒーレンスをうまく押さえられることを、数値的実験と大雑把な理論計算で示した(2.)。

また、量子カウンティングアルゴリズムにおけるデコヒーレンスの影響についても調べ、理論的観点から興味深い様々な知見を得た。そのなかでも実用的観点から重要なことは、実装方法によるデコヒーレンスの影響の差の問題ある。大層な違いがないように見える実装方法でも、相当特徴的な差が出ることがわかった(3.)。

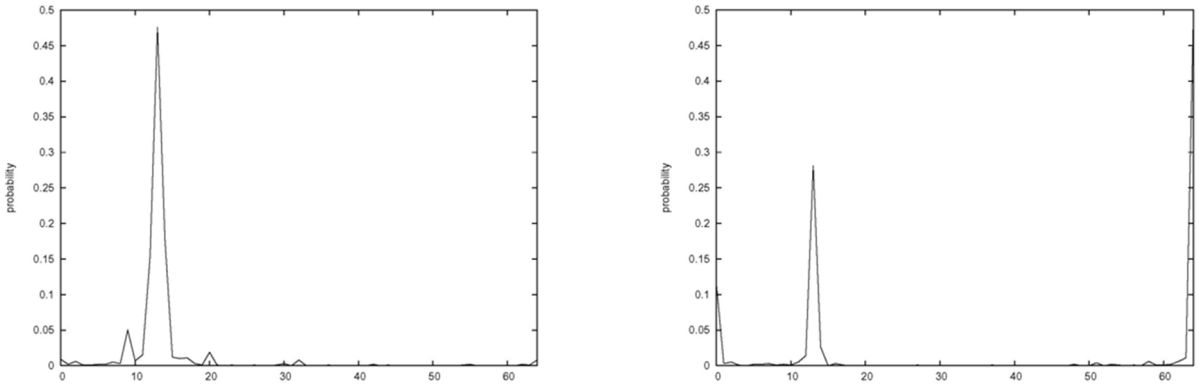



図 14.実装方法による出力 の確率分布の違い、エラーレート $d = 4 \times 10^{-3}$

### 成果展開可能なシーズ、用途等

量子計算機の実装時に発生すると思われる問題の事前検討に有効であると思われる。

### 特許出願

なし。

**報告書他**

1）J. Niwa, K. Matsumoto, and H. Imai, “General-purpose parallel simulator for quantum computing,” Phys. Rev. A 66, 062317, (2002).

2）J. Niwa, K. Matsumoto, and H. Imai, “Simulating the Effects of Quantum Error-correction Schemes,” quant-ph/0211071.

3）Hasegawa, J.; Yura, F. “Quantum Counting with Decoherence Errors -Influence of Circuits’ Order-,”ERATO conference on Quantum Information Science 2003 (EQIS 03), Niijima Kaikan, Kyoto, Japan, Sep. 4-6, 2003.

研究者名：丹羽 純平、松本 啓史、長谷川 淳、由良 文孝、今井 浩

## 3. 量子鍵配送

### 3-1. 信頼性関数の導出

**研究成果の概略**

量子鍵配送では送信者は bit 基底及び phase 基底をランダムに選び、送信状態を決め、同時に受信者も上記の基底をランダムに選び、受信時の測定を決めることになる。そして、事後の照合通信において、選択した基底が一致した部分のデータのみを、共有鍵のソースとして用いることになる。

多くの先行研究では符号の大きさが無限大の場合の議論のみを正確に扱っており、実際に用いられる有限 n のサイズの符号でどの程度の安全性が達成されるか全く議論されていなかった。一般に、符号を構成するための複雑さは符号の性質にも依存するが、そのサイズ n にも比例して大きくなる。

今回の研究では、自己双対な符号をランダムに発生させた場合の符号の平均性能を解析し、サイズ n 依存してどのように自己双対な符号による誤り訂正符号の性能が向上するか解析した(1.)。結果として、量子状態の伝送に関する誤りはサイズ n に関して指数的に減少するのであるが、その指数の係数は最終的に鍵の生成レートに依存した信頼性関数 E(R)とよばれるもので与えられる。我々は信頼性関数についての評価式を始めて与えた(1.)。なお、この場合、量子状態の伝送に関する誤りは $2^{-nE(R)}$ となる。

さらに、これに、Schumacher の議論を組み合わせることで、量子鍵配送の際の誤り確率や盗聴者への情報漏洩の量も同様に、$2^{-nE(R)}$ で 0 に減少することを確認した。

なお、これらの研究は、プロジェクトの初期の誤り訂正符号に関する研究(2.)(3.)(4.)があって、初めて可能となったものである。

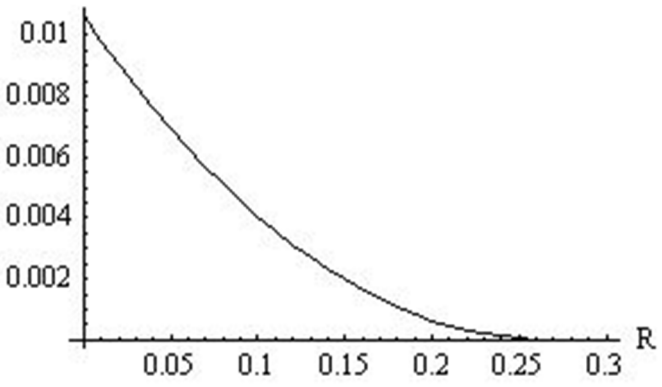



図　信頼性関数の下限のグラフ（横軸が鍵生成率、縦軸がそのときの信頼性関数の下限の値。なお、上記のグラフではエラー率が 7% のときについて扱った。）

**成果展開可能なシーズ、用途等**

量子鍵配送の実用化のために必要な符号化には今回の研究は必要不可欠となると思われる。

**特許出願**

なし

**報告書他**

1） M. Hamada, “Reliability of Calderbank-Shor-Steane Codes and Security of Quantum Key Distribution,” Journal of Physics A: Mathematical and General, vol.37, no.34, pp.8303-8328, (2004).

2） M. Hamada, “A lower bound on the quantum capacity of channels with correlated errors,” J. Math. Phys. 43, 4382-4390, (2002).

3） M. Hamada, “Lower bounds on the quantum capacity and highest error exponent of general memoryless channels,” IEEE Trans. Information Theory, 48, pp. 2547-2557, (2002).

4） M. Hamada, “Notes on the Fidelity of Symplectic Quantum Error-Correcting Codes,” International Journal of Quantum Information, Vol. 1, No. 4, pp. 443-463, (2003).

研究者名：浜田 充

### 3-2. 閾値の改良

**研究成果の概略**

先に述べたエラー率の閾値の改良は重要な課題であり、より大きなエラー率での量子鍵配送を可能にすることは重要なテーマである。上述のように、線形な符号を単純にランダムに発生させた場合での平均的な性能の符号に注目する限り、エラー率 11%が超えると、安全な量子鍵配送が不可能になる。しかし、上記の符号にいくらかの工夫を加えることで、この閾値を改良することが可能となる。この問題に対して、Gottesmann&Lo はエラー率の閾値が 18.9 %まで改良可能であることを示した。また、Chau はこれが 19.9%まで改良できることを示している。

そして、今回、我々は 26%のエラー率でも、量子鍵配送が可能であることを示した(2.)。なお、Gottesmann&Lo により通常の 4 種類の状態を送る量子鍵配送法ではエラー率が 25%を超えると、どのような符号化を用いようと、量子鍵配送が不可能であることが知られている。したがって、我々の方法では 2 量子ビットに跨る状態（一部はエンタングルド状態）を通信に用いることで、この性能を実現する。ここで鍵となったアイデアは誤り棄却の方法(3.)である。

さらに、我々は、biterror $P_x$ と phase error $P_z$ が非対称の場合についても考察した。この場合についても閾値を改良した(1.)。

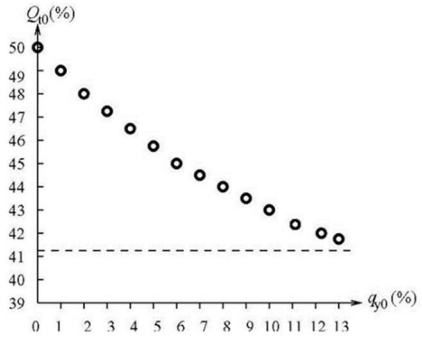



図 15. 従来手法での閾値（破線）と本研究で得られた閾値（小さい丸）との比較。$Q_{t0}$ は閾値を表す。$q_{y0}$ はノイズの形態を表すパラメータ。このパラメータが小さいほど、従来手法に比べて改良の度合が大きいことが分かる。

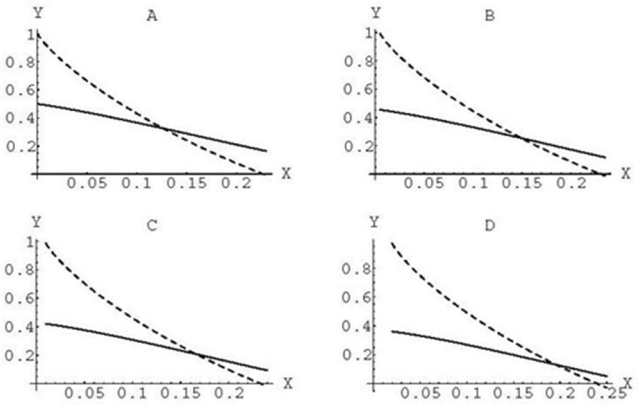



図 16. 従来手法（破線）と提案手法（実線）の最終鍵生成比率の比較。Y 軸は、最終生成鍵比率を表し、X 軸はノイズ確率の和を表す。なお、A, B, C, D はそれぞれ、ノイズの形態を表すパラメータ $q_{y0}$ がそれぞれ、0,0.5%,1%,2%である場合を表す。

**成果展開可能なシーズ、用途等**

現実の物理系を用いた量子鍵配送では、ノイズの影響は無視できない。そのため、ノイズに対する耐性を向上させることは不可欠である。本研究は、符号化を適切に組み合わせることで、ノイズに対する耐性を向上させるものである。今後、ノイズの大きい物理系での量子鍵配送で提案手法が用いられる可能性がある。

**特許出願**

なし

**報告書他**


1）X.-B. Wang, “Quantum key distribution with asymmetric channel noise,” Phys. Rev. A 71, 052328, (2005); quant-ph/0406099.

2）X.-B. Wang, “Quantum key distribution with 2-bit quantum codes,” Phys. Rev. Lett. 92, 077902, (2004).

3）X.-B. Wang, “Quantum error rejection code with spontaneous parametric conversion,” Phys. Rev. A 69, 022320, (2004).

4）X.-B. Wang, “Quantum key distribution: security, feasibility and robustness,” (Chapter 8 of Quantum Computation and Information: H. Imai and M. Hayashi eds., Springer 2006.)



研究者名：Wang Xiangbin

### 3-3. 共通ノイズに対するエラー耐性

**研究成果の概略**

ファイバーを用いた量子鍵配送では、ノイズはランダムに働くユニタリ行列で表すことができると考えられる。特に、空間的に近い位置にある２つの光子に働くユニタリな作用は同一であると考えられている。我々はこのようなノイズの性質を踏まえ、ノイズ耐性の高いプロトコルを提案した(1.)。

そして、そのプロトコルの検証実験も同時に行なった。具体的にはパラメトリックダウンコンバージョンで発生する光子対の偏光状態を上の４状態になるように設定し、波長板を挿入することでビットフリップと位相フリップのある伝送路をシミュレートし、誤り率を求めた。実験で得られた誤り率は理論の予測とよく一致した。もちろん、この方法では２光子が同時に届かなければならないため損失の大きい状況には不向きである。短距離のフリースペースリンクのように伝送損失は比較的小さいが風などによる擾乱のあるときにあるいは有効である。この結果は(2.)(3.)で発表されている。

さらに、共通ノイズの形に制約がある場合に有効に働く量子鍵配送のプロトコルを提案し、これについても海外のグループと共同で検証実験を行なった(4.)。

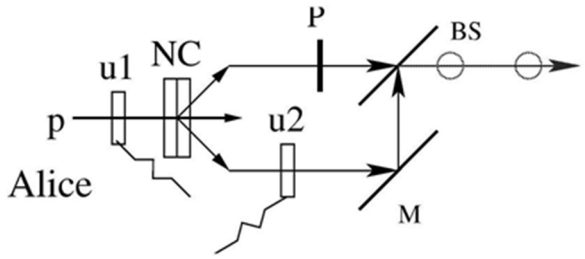



図 17. ２キュービット生成源。P:$\pi/2$ 位相回転器. BS: ビームスプリッター, M: ミラー, NC: SPDC(自発的パラメトリック加法変換)過程のための非線形結晶, p: 水平分極のためのパンプ光, u1: ユニタリ回転器, u2: 位相回転器. なお、u1 は 生成状態に応じて それぞれ、$0, \pi/2, \pi/4$ の値を取る。u2 は I もしくは $\sigma_z$ のどちらかである.

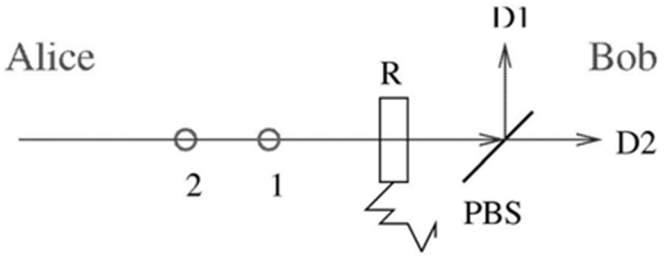



図 18. 受信者 Bob 側の測定器。R は電気的に駆動される回転器であり、同一の符号の両方の qubit に同じ回転をランダムに施す。1 つの検出器（D1 あるいは D2）が 2 回検出信号を出したときは、符号の 2 つの qubit が同一のビット値を持つことを意味し、また、2 つの検出器がそれぞれ 1 回の検出信号を出したときは、符号の 2 つの qubit が異なるビット値を持つことを意味する。

**成果展開可能なシーズ、用途等**

ファイバーを用いた量子鍵配送では、ノイズはランダムに働くユニタリ行列で表すことができると考えられる。特に、空間的に近い位置にある２つの光子を用いて符号化を行なう場合には、ここでの提案手法は有効であると考えるられている。

**特許出願**

なし

**報告書他**


1）X. B. Wang, “Fault tolerant quantum key distribution protocol with collective random unitary noise,” Phys. Rev. A 72, 050304(R) (2005).

2）Yun-Kun Jiang, Xiang-Bin Wang, Bao-Sen Shi, and Akihisa Tomita, “Experimental verification of fault tolerant quantum key distribution protocol,” Proceedings of ERATO conference on Quantum Information science, 2005 (EQIS’05).

3）Yun-Kun Jiang, Xiang-Bin Wang, Bao-Sen Shi, and Akihisa Tomita, “Experimental verification of fault tolerant quantum key distribution protocol,” Optics Express, Vol. 13, 9415-9421 (2005).

4）Zhang, Q.; Yin, J.; Chen, T.-Y.; Lu, S.; Zhang, J.; Li, X.-Q.; Yang, T.; Wang, X.-B.; Pan, J.-W. “Experimental fault-tolerant quantum cryptography in a decoherence-free subspace,” Phys. Rev. A 73, 020301(R) (2006).

5）X.-B. Wang, “Quantum key distribution: security, feasibility and robustness,” (Chapter 8 of Quantum Computation and Information: H. Imai and M. Hayashi eds., Springer 2006.)


研究者名：Wang Xiangbin、Yun-Kun Jiang、Bao-Sen Shi、富田 章久

## 4. 弱コヒーレント状態を用いた場合の安全性

### 研究成果の概略

多くの量子鍵配送実験では、弱コヒーレント状態を単一光子状態の代わりに用いているのが現状である。しかし、弱コヒーレント状態は複数の個数状態の重ね合わせ状態であるため、単一光子状態だけでなく、２光子状態も含んでいる。そのため、2 光子の部分に注目し、それから 1 光子分の情報を抜き取ることが可能となる。このような盗聴方法は photonnumberspritting (PNS)攻撃と呼ばれ、単一光子状態の代わりに弱コヒーレント状態を用いた場合には極めて有効である。したがって、弱コヒーレント状態を用いた量子鍵配送において、このような PNS 攻撃を含む全ての攻撃に対して、安全な鍵配送プロトコルが望まれている。

Gottesman らは不完全な量子状態を用いた場合での量子鍵配送について考察し、Hwang はこのアイデアを弱コヒーレント状態の場合に検討した。我々は、これらの考察をさらに進め、弱コヒーレント状態の強度を 4 種類（もしくは 3 種類）に変化させることで、弱コヒーレント状態の場合でも効果的に量子鍵配送を行なう方法を提案した(1.)(2.)。

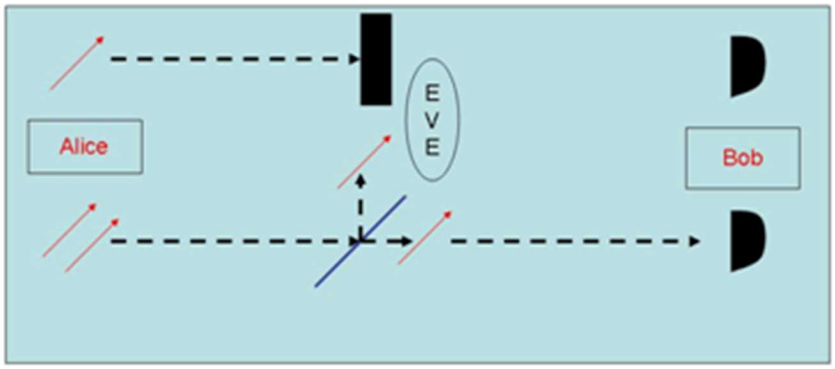



図 19. PNS 攻撃による盗聴

### 成果展開可能なシーズ、用途等

多くの量子鍵配送実験では、弱コヒーレント状態を単一光子状態の代わりに用いているのが現状であるため、この性質を用いた盗聴が可能であることが知られている。これを防ぐのが、上述の方法である。今後の量子鍵配送実験では、この方法が用いられると思われる。

### 特許出願

なし

**報告書他**

1）X.-B. Wang, “Decoy-state protocol for quantum cryptography with four different intensities of coherent light,” Phys. Rev. A 72, 012322 (2005).

2）X. B. Wang, “Beating the PNS attack in practical quantum cryptography,” Phys. Rev. Lett. 94, 230503, (2005); quant-ph/0410075.

3）X.-B. Wang, “Quantum key distribution: security, feasibility and robustness,” (Chapter 8 of Quantum Computation and Information: H. Imai and M. Hayashi eds., Springer 2006.)

研究者名：Wang Xiangbin

## 5. 量子情報システム-実現のための実験研究

### 5-1. 量子暗号鍵配布実験

### 5-1-1. 通信波長帯における高感度光子検出器

**研究成果の概略**

量子暗号鍵配布において最も重要なデバイスは光子検出器である。量子暗号伝送可能な距離は光子検出器の性能（ダークカウント確率と量子効率の比）で決定される。

光子検出にはアバランシェフォトダイオード（APD）を光子計数(ガイガー)モードで用いる。従来ダークカウント確率を減らすため、光子が存在する可能性のある時間にだけ APD に対する印加電圧がブレークダウン電圧を越えるように DC バイアスにパルスを重畳するゲート法が広く用いられている。しかし、充放電で生じるスパイクパルスのため光子検出の閾値を高く設定する必要があり、ダークカウント確率と量子効率がトレードオフの関係にあった。

これに対して我々は２つの APD のスパイクパルスをキャンセルする新しい差動回路を考案し、量子効率を犠牲にすることなくダークカウント確率を低減させた。温度を-106.5℃としたとき量子効率 10%においてダークカウント確率２×１０$^{-7}$と従来より１桁以上性能を向上させた。

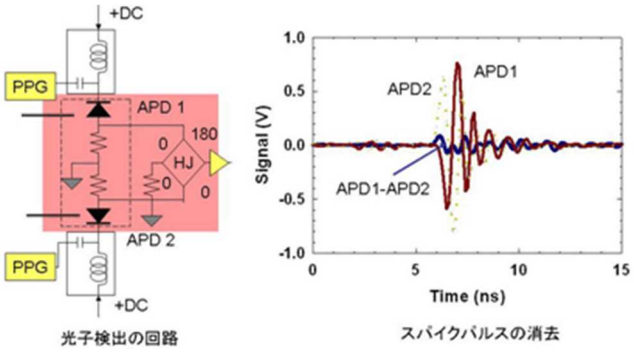



図 20.光子検出の回路とスパイクパルスの消去

**成果展開可能なシーズ、用途等**

量子暗号鍵配布の長距離化、高速化に直接寄与する。光子を用いる量子情報処理の基本素子となるだけでなく、生物・化学分析などの近赤外領域での極微弱光検出に利用できる。

**特許出願**

1) 特願 2002-37859「光子検出器とそれを用いた量子通信装置及び量子計算機」
出願人: 科学技術振興事業団、富田章久、発明者: 富田章久、出願日 2002 年 2 月 15 日

**報告書他**

1) Akihisa Tomita and Kazuo Nakamura, “Balanced, gated-mode photon detector for qubit discrimination at 1550 nm,” Optics Letters 27(10), pp.1827-1829, (2002).

研究者名：富田 章久

### 5-1-2.　100km を越える長距離量子暗号伝送

**研究成果の概略**

性能が向上した光子検出器を用いることで量子暗号伝送の長距離化が期待できる。まず、我々はプラグ＆プレイ方式で 100km の伝送に成功した。さらに長距離伝送に適した単一方向型で 150km に成功した。量子暗号の伝送距離としては現在最長である。

単一方向型では送受信器に光路差の等しい非対称干渉計が必要である。我々は平面光回路（Planar Lightwave Circuit: PLC）技術を利用した単一方向型量子暗号システムの開発を行った。PLC 技術により小型で機械的に安定な干渉計が得られる。挿入図は光ファイバ 150km 伝送後の干渉パターンで、アクティブな光路差制御をしないにもかかわらず明瞭度 82%～84%が得られ（誤り率 9%と 8%に相当）安全な量子暗号鍵生成が可能である。この研究は NEC 基礎･環境研究所、NICT と共同で行われた。

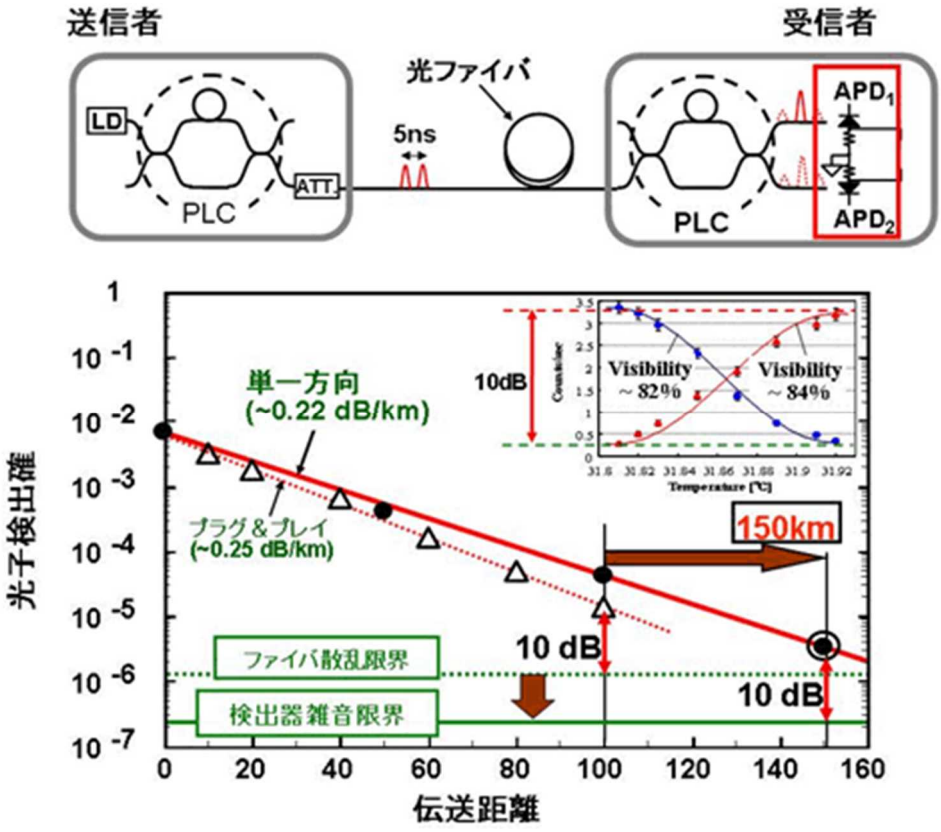



図 21. PLC を用いた一方向量子暗号システムと伝送特性

**成果展開可能なシーズ、用途等**

大都市圏（100km 圏）での高度に安全な暗号鍵配布

**特許出願**

なし

**報告書他**

1） Hideo Kosaka, Akihisa Tomita, Yoshihiro Nambu, Tadamasa Kimura, and Kazuo Nakamura, “Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector,” Electronics Letters 39(16), pp.1199-1201, (2003).

2） Tadamasa Kimura, Yoshihiro Nambu, Takaaki Hatanaka, Akihisa Tomita, Hideo Kosaka, and Kazuo Nakamura, “Single-photon Interference over 150km Transmission Using Silica-based Integrated-optic Interferometers for Quantum Cryptography,” Jpn. J. Appl. Phys. 43(9A/B), pp.L1217-L1219, (2004).

研究者名：富田 章久

### 5-1-3.　架空光ファイバによる高速量子暗号生成

**研究成果の概略**

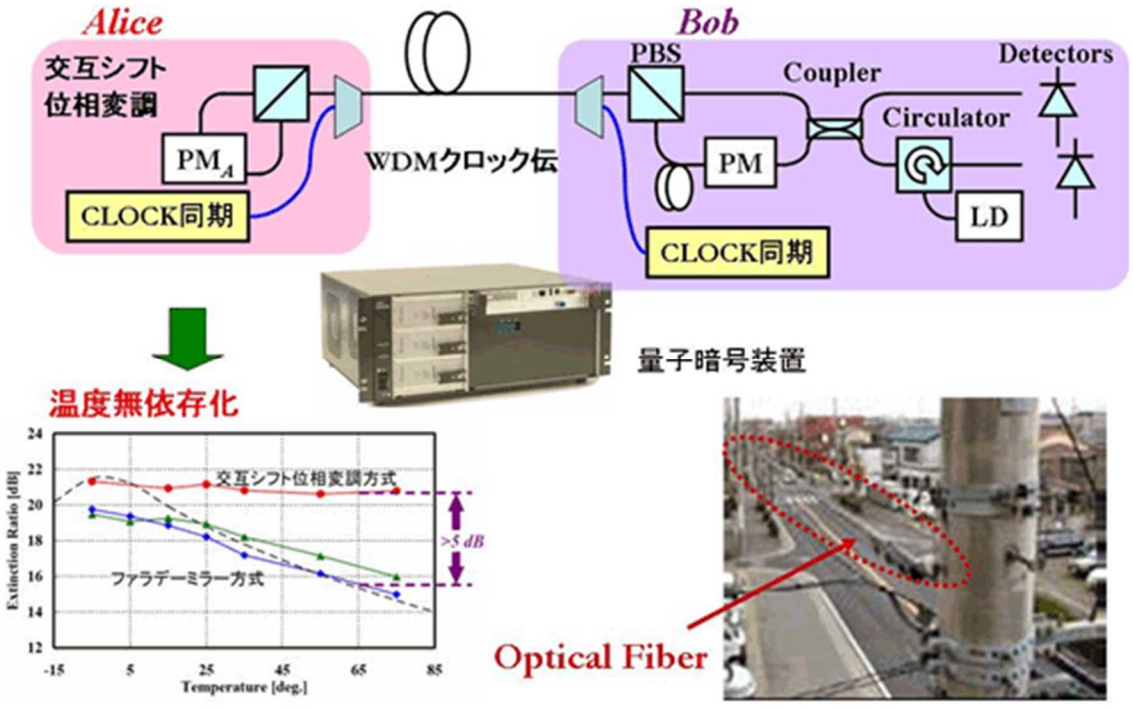
我々は広い温度範囲で安定に高いレートで暗号鍵を生成する実用的なシステムを開発した。このシステムではプラグ＆プレイ方式を採用し

- 環境温度無依存化を実現する交互シフト位相変調技術
- 高速・安定動作を実現する位相変調及び光子検出の量子信号への同期技術
- 光子伝送情報(生鍵)を元に暗号化鍵を生成する最終暗号鍵生成機能
- 装置の初期化及び監視制御を行うシステム制御機能
- 生成した暗号鍵を用いて通信を行う暗号化通信機能

を開発した。装置は一体化され 19inch ラックに収容できる。

従来用いられるファラディミラーは温度によって特性が変化する。我々は温度補償ができる交互シフト位相変調型プラグ＆プレイ方式を開発した。位相変調器で直交偏光間に 180 度の位相差を与えることでファラディミラーと同じ効果を実現している。また、高速化のため光子検出器の動作条件を検討し、クロック周波数 62.5MH z での安定な動作を実現した。

この装置を用いて 40km の光ファイバ伝送を行った結果、生鍵生成レート 100kbps を得た。また、パワードコム所有の商用架空ファイバ 16.3km を用いてフィールドテストを行い、14 日間連続動作に成功した。なお、研究は NEC 基礎・環境研究所、NICT と共同で行った。



**成果展開可能なシーズ、用途等**

LAN など近距離における高度に安全性が保証された暗号鍵配布

**特許出願**

1）特願 2004-372547「量子暗号装置」
出願人: 科学技術振興機構、富田章久、発明者: 富田章久、林正人、出願日 2004 年 12 月 24 日

2）特願 2004-335228「通信システム及びそれを用いた通信方法」
出願人: 富田章久、中村和夫、田島章雄、田中聡寛、南部芳弘、鈴木修司、竹内剛、前田和佳子、高橋成五、発明者: 科学技術振興機構、富田章久、日本電気株式会社、出願日 2004 年 11 月 19 日

**報告書他**

1）Akihiro Tanaka, Akihisa Tomita, Akira Tajima, Takeshi Takeuchi, Seigo Takahashi, Yoshihiro Nambu, “Temperature independent QKD system using alternative-shifted phase modulation method,” The 30th European Conference on Optical Communication (ECOC), Tu4.5.3, 2004.

2）A. Tajima, A. Tanaka, W. Maeda, S. Takahashi, A. Tomita, and N. Nambu: “Continuous Key Generation Technologies for Practical Quantum Cryptosystems,” Invited at Int. Symp. on Contemporary Photonic Technologies (CPT), Tokyo, Japan (Jan. 13, 2006)

研究者名：富田 章久

## 5-2. 非古典光子の生成

### 5-2-1. エンタングル光子対の評価とフェムト秒パルスによるエンタングルド光子対の生成

**研究成果の概略**

混合状態も含んだ一般的なエンタングル状態をあらわすにはの密度行列を用いればよい。我々は量子状態トモグラフィーを用いてパラメトリックダウンコンバージョン（SPDC）で発生する光子対の密度行列の 16 個の成分を実験から定めた。具体的には同じ状態にある多数の光子対に対して 16 種類の同時計測を行い、その結果から密度行列を推定する。

量子テレポーテーションなどの量子プロセスではフェムト秒光パルスでポンプしたエンタングル光子対が必要である。パルス光を用いると時間的な分離の可能性が生まれるため、エンタングルメントが失われやすくなる。我々はポンプ光の直交偏光成分間にあらかじめ時間差を与えて（pre-compensation）このような区別の可能性を消すことによってフェムト秒ポンプしたにもかかわらず高いエンタングルメントを実現した。量子状態トモグラフィーで密度行列を推定してエンタングルメントの指標である concurrence を求めると、pre-compensation が最適値 135fs のとき最大値 0.956 を得た。

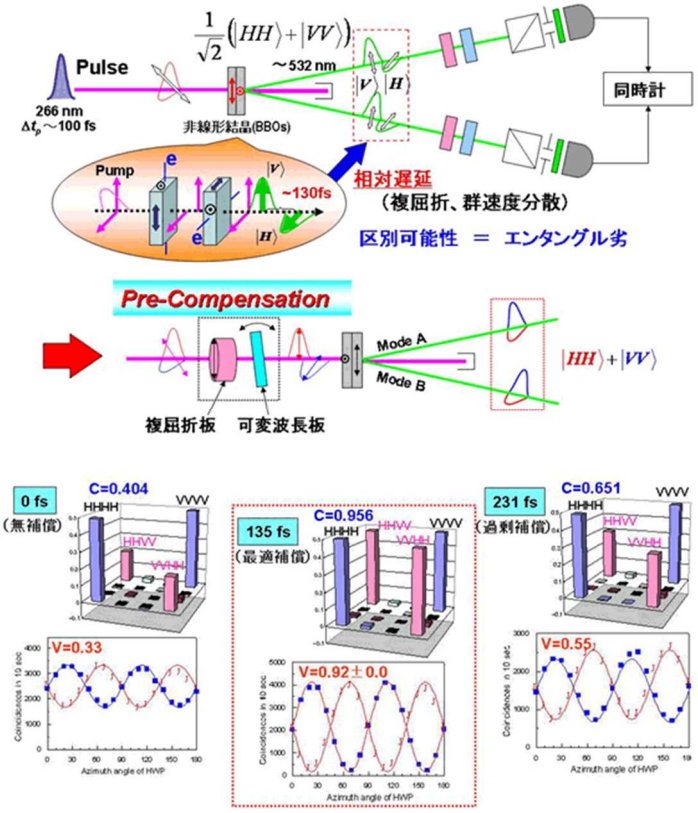



図 22. パラメトリックダウンコンバージョンによるエンタングルメント光子対の発生と評価

**成果展開可能なシーズ、用途等**

エンタングルメントの評価、高いエンタングルメントを持つパルス光子対光源

**特許出願**

1）特願 2002-080109「光パルス幅測定方法及びその装置」

出願人: 科学技術振興事業団、日本電気、富田章久、発明者: 南部芳弘、富田章久、数井賢治、出願日 2002 年 3 月 26 日

報告書他

1） Koji Usami, Yoshihiko Nambu, Yoshiyuki Tsuda, Keiji Matsumoto, and Kazuo Nakamura, “Accuracy of quantum state estimation utilizing Akaike’s information criterion,” Phys. Rev. A 68, 022314, (2003).

2） Yoshihiro Nambu, Koji Usami, Yoshiyuki Tsuda, Keiji Matsumoto, and Kazuo Nakamura, “Generation of polarization-entangled photon pairs in a cascade of two type-I crystals pumped by femtosecond pulses,” Phys. Rev. A 66, 033816, 2002).

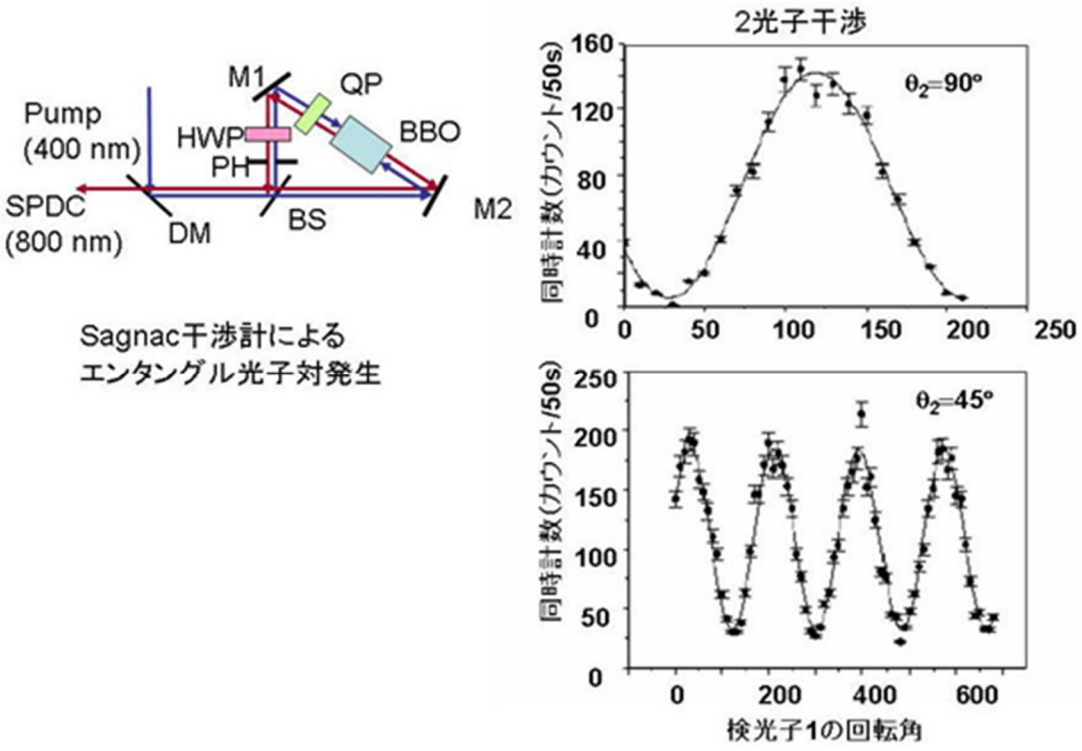
3） Yoshiro Nambu, Koji Usami, Akihisa Tomita, Satoshi Ishizaka, Tohya Hiroshima, Y. Tsuda, Keiji Matsumoto, and Kazuo Nakamura, “Experimental Investigation of Pulsed Entangled Photons and Photonic Quantum Channels (Invited paper),” Photonics Asia, (2002).

研究者名：津田 美幸、松本 啓史、富田 章久、数井 賢治

### 5-2-2.　干渉計による光子対発生

**研究成果の概略**

エンタングルド光子対の発生は干渉計を利用して行うこともできる。干渉計の 2 つの経路の途中に非線形光学結晶を挿入して SPDC 光を発生させ、経路を合成して出力とする。干渉計のアームに補償素子を入れることができるため分散や複屈折に対する補正の自由度が大きく、またコリニア配置とすることで原理的には結晶の長さに制限がなくなるといった利点がある。一方、干渉計の 2 つの経路を完全に合わせなければ区別可能性が生じてエンタングルメントが低下する。特に我々は Sagnac 干渉計による機械的な擾乱に対して安定なエンタングルド光子対発生を実現した。実験で得られた 2 光子干渉パターンは 71%-93%の明瞭度を示した。ポンプ光の平均出力は 15mW で同時計数レートは毎秒 4 カウント程度であった。ただし、これにはファイバとの結合などの損失を考慮していない。




Sagnac干渉計による
エンタングル光子対発生

**成果展開可能なシーズ、用途等**

高いエンタングルメントを持つパルス光子対光源

**特許出願**

なし

**報告書他**

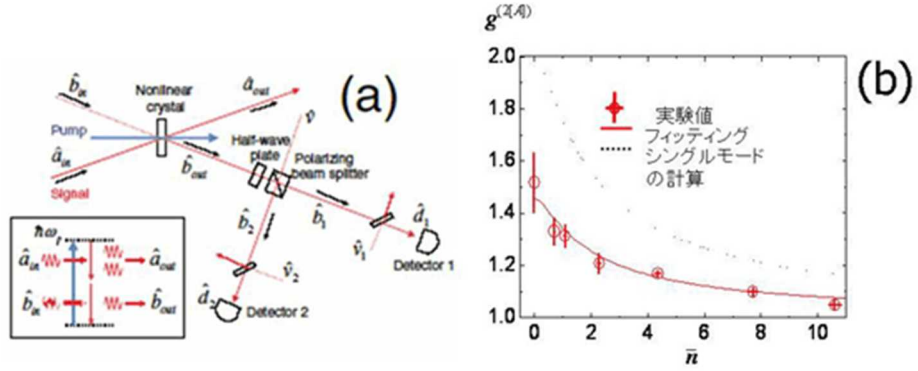
1) Bao-Sen Shi and Akihisa Tomita, “A novel way for preparation of Bell state using femtosecond pulse pumped spontaneous parametric down-conversion,” Proceedins of ERATO workshop on Quantum Information science 2002 (EQIS,02), (2002).
2) Bao-Sen Shi and Akihisa Tomita, “Generation of a pulsed polarization entangled-photon pair via a two-crystal geometry,” Phys. Rev. A 67, 043804, (2003).
3) Bao-Sen Shi and Akihisa Tomita, “Preparation of a pulsed polarization entangled photon pair via interference,” Optics Communications 235, pp.247-252, (2004).
4) Bao-Sen Shi and Akihisa Tomita, “Generation of pulsed polarization entangled photon pair using a Sganac interferometer,” Proceedings of ERATO conference on Quantum Information science 2003 (EQIS’03).
5) Bao-Sen Shi and Akihisa Tomita, “Generation of a pulsed polarization entangled photon pair using a Sagnac interferometer,” Phys. Rev. A 69, 013803, (2004).

研究者名：Bao-Sen Shi、富田 章久

### 5-2-3. 反正規順序による光子検出

**研究成果の概略**

パラメトリックダウンコンバージョン技術の応用として、我々は反正規順序による光子検出を初めて実現した。通常光子検出の過程は光子の生成消滅演算子が正規順序で並んだ過程（光子の吸収)で表される。この場合、電磁場の真空揺らぎは測定結果には現れない。そのため、測定前の場の密度行列は測定後の密度行列と測定結果から再現することはできない（論理的に不可逆な）。真空揺らぎを観測するには反正規順序による光子検出が必要である。我々は誘導パラメトリックダウンコンバージョンの出力の HanburyBrown-Twiss 型の 2 光子相関を測定することで、誘導パラメトリックダウンコンバージョンが反正規順序による光子検出過程であることを示した。コヒーレント光の 2 光子相関は正規順序の光子検出では 2 光子の検出時間の差によらないが、誘導パラメトリックダウンコンバージョンによる測定ではバンチング（時間差 0 で分布が大きくなる)が観測され反正規順序による光子検出の場合の予測と一致した。




パラメトリック増幅による反正規順序光検出

2次相関関数：
光子数が小さいときバンチング

**成果展開可能なシーズ、用途等**

論理的に可逆な測定による量子状態の再構成

**特許出願**

なし

**報告書他**

1） Koji Usami, Yoshihiro Nambu, Bao-Sen Shi, Akihisa Tomita and Kazuo Nakamura、
“Observation of Antinormally-ordered Intensity Correlation of Electromagnetic Field via

Stimulated Parametric Down-conversion," Non-locality of Quantum Mechanics and Statistical Inference, (2003).

2) Koji Usami, Yoshihiro Nambu, Bao-Sen Shi, Akihisa Tomita, and Kazuo Nakamura, "Observation of Antinormally Ordered Hanbury Brown-Twiss Correlations," Phys. Rev. Lett. 92, 113601 (2004).

3) Koji Usami, Akihisa Tomita, Kazuo Nakamura, "Antinormally ordered photodetection of continuous-mode field," International Journal of Quantum Information 2(1), pp.101-117, (2004).

研究者名：富田 章久

## 5-3. 量子計算にむけて

### 5-3-1. 量子フーリエ変換

**研究成果の概略**

量子フーリエ変換は量子計算における重要なサブルーチンである。最後に制御ビットの状態を測定する場合には古典的に制御される回転ゲートを用いて逐次的に実行できることが知られている。我々は逐次的な量子フーリエ変換を行う量子回路は光学的に実現が可能であることを示した。図に示すような回路を用いてビットあたりの誤り確率 p=0.01 を得た。さらに測定により確定したビット値を求める場合には多数決によって誤り確率を小さくできることが示し、実際に 1024 キュービットに対する量子フーリエ変換に成功した。誤り確率の平均値は 1 キュービットあたり $2.2\times10^{-4}$ と多数決で期待される値とほぼ一致している。以上のように逐次的な動作をするファイバオプティクスによる光回路を用いて実用レベルの量子ビット数での量子フーリエ変換に初めて成功した。

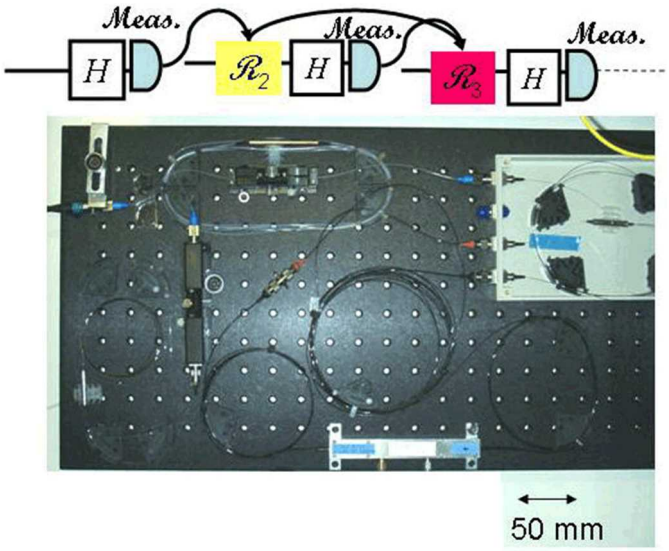



図 23. 光ファイバ素子による量子フーリエ変換回路

**成果展開可能なシーズ、用途等**

ショアの素因数分解アルゴリズム等、最後に制御ビットを測定する量子計算アルゴリズムの最終段

**特許出願**

1）特願 2002-255649「量子回路および量子計算機」

出願人: 富田章久、科学技術振興事業団、発明者: 富田章久、出願日: 2002 年 8 月 30 日

**報告書他**

1) Akihisa Tomita and Kazuo Nakamura, “Measured Quantum Fourier Transform on Fiber optics,” Proceedings of ERATO conference on Quantum Information science, 2003 (EQIS’03).
2) Akihisa Tomita and Kazuo Nakamura, “Measured Quantum Fourier Transform of 1024 Qubits on Fiber Optics,” Int. J. Quantum Information, 2(1), pp.119-131, (2004).
3) Akihisa Tomita, “Quantum Information Processing with fiber optics: Quantum Fourier Transform of 1024 Qubits (Invited Paper),” The 10th International Conference on Quantum Optics, (2004). Published in Optics and Spectroscopy 99, No. 2 (2005) pp. 204-210.
4) Akihisa Tomita and Kazuo Nakamura, “1024-qubits quantum Fourier transform on a fiber optics circuit,” Quantum Informatics, (2004).

研究者名：富田 章久

### 5-3-2. フォトニック結晶共振器の設計

**研究成果の概略**

光子と励起子の相互作用を大きくするためには微小共振器に光子を閉じ込めて電場の強度を大きくすることと、共振器の Q 値を上げて実効的な相互作用時間を増大させることが有効である。つまり Q 値を上げると同時に共振器内の電磁場モードの体積を小さくする必要である。従来報告されているフォトニック結晶の欠陥を利用した共振器ではこれらの両立は難しかった。我々は 2 次元の FDTD(FiniteDifferenceTimeDomain)法によるシミュレーションでフォトニック結晶構造を最適化した。

基本となる構造は 2 次元六方格子である。我々は欠陥の周りを非対称にすることで Q 値が 1 桁増大することを見出した。得られた Q 値の最大値 1 。 $7\times10^{5}$ は、このときのモード体積は $3.5\times10^{-14}cm^{3}$ となり、波長の 3 乗から見積もられる値の 0.42 倍となった。

さらに共振器には外部と結合しないモードも存在し、このモードと外部と結合するモードの間で干渉が起きることも明らかになった。この現象は内部の量子ドットの励起子と結合させると興味ある量子光学現象が引き起こされる可能性もあり、量子ゲートに応用が可能かもしれない。

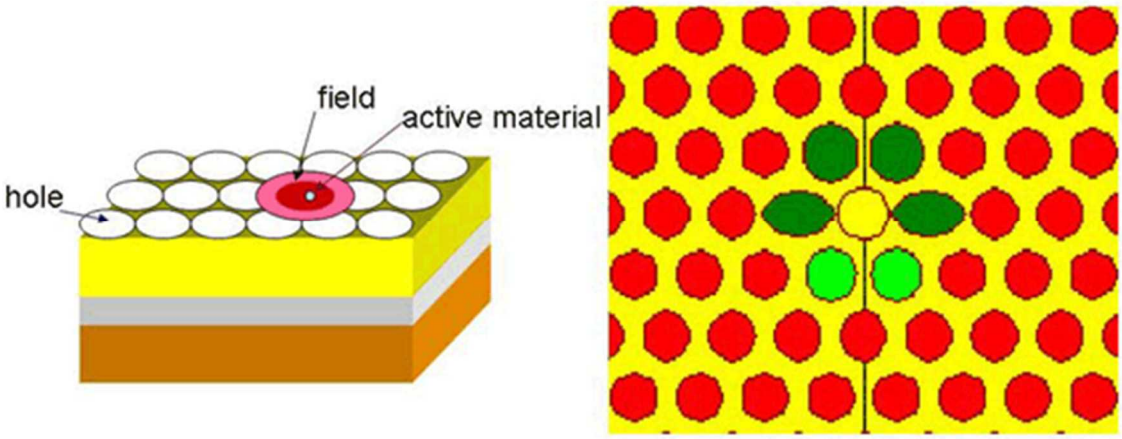



図 24. フォトニック結晶共振器の構造

**成果展開可能なシーズ、用途等**

光と物質の相互作用増強、量子インターフェース、量子ゲート

**特許出願**

なし

**報告書他**

1) Achanta Venu Gopal and Akihisa Tomita, “High Quality Factor Photonic Crystal Microcavity Design for Solid-State Quantum Phase Gate,” Proceedings of ERATO conference on Quantum Information science, 2004 (EQIS’04).
2) Achanta Venu Gopal, Akihisa Tomita, Hirohito Yamada, and Sheng Lan, “Temporal behaviour of field in high quality factor photonic crystal microcavity structure,” Optics Express 13(2), pp.460-467, (2005).

研究者名：Achanta Venu Gopal、富田章久

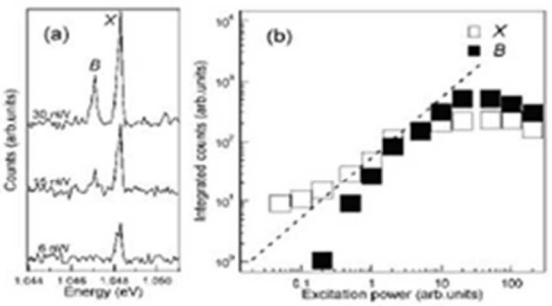
### 5-3-3. 単一量子ドットの分光的研究

**研究成果の概略**

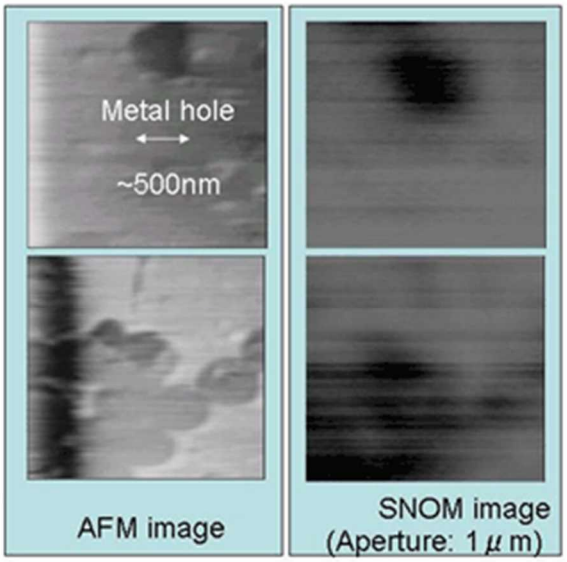
量子ゲート、量子インターフェースの能動物質として量子ドット励起子が期待される。特に量子暗号通信への応用を念頭に、光ファイバ伝送に適した波長1 $\mu$m 以上に共鳴する量子ドットの光学応答を理論的・実験的に検討した。共鳴波長が 1m を超える InAs/GaAs 量子ドットは、その強い閉じ込め効果によって物理的にも興味深い性質が期待される。励起子1個が量子ビットとなるため量子情報への応用では単一量子ドットを分離する必要がある。我々は共焦点顕微鏡を基本にした顕微分光装置と近接場光学顕微鏡を開発した。

我々は顕微鏡の視野の動きを補正し長時間に渡って安定な測定ができる位置決め制御系を開発した。1.18$\mu$m 付近に第1励起状態のある単一の量子ドットに由来する励起子・励起子分子の蛍光寿命を時間相関光子計数法によって測定した。

我々は、近接場光学顕微鏡(SNOM)を単なる高分解能顕微鏡ではなく、試料に対し局所的な外場制御を行う装置として位置づけている。このため、我々の装置は低温(10K)、強磁場(7T)環境下での試料の局所応答を観測できるように設計されている。装置は原子間力顕微鏡(AFM)を基本とし、金属コートして不透明にしたカンチレバーにあけた直径 500-1000nm の穴から漏れ出す近接場を伝搬光に変換する。超伝導マグネットの細いボアを空間光が伝わるため新たな無限共役光学系を開発した。カンチレバーが金属コートされて導電性を持つため、局所的な電場印加や電流測定が可能である。現在、低温・強磁場のそれぞれで AFM 像に対応した SNOM 像が得られている。




単一量子ドットからの発光と励起強度依存性




SNOM像

**成果展開可能なシーズ、用途等**

ナノ材料デバイスの低温での光学評価（磁場印加、局所的な電場印加、電流注入などが可能）

**特許出願**

なし

**報告書他**


1）Kunihiro Kojima and Akihisa Tomita, “Influence of pure-dephasing by phonons on exciton-photon interface,” Proceedings of ERATO conference on Quantum Information science, 2005 (EQIS’05).

2）Shunsuke Kono, Akihiro Kirihara, Akihisa Tomita, Kazuo Nakamura, Kenichi Nishi, Hideaki Saito, Junichi Fujikata, and Keishi Ohashi, “Time-resolved photoluminescence measurement of exciton and biexciton in an InAs/GaAs single quantum dot,” International Quantum Electronics Conference, (2005).

3）Shunsuke Kono, Akihiro Kirihara, Akihisa Tomita, Kazuo Nakamura, Junichi Fujikata, Hideaki Saito, and Kenichi Nishi, “Excitonic molecule in a quantum dot: Photoluminescence lifetime measurement of an InAs/GaAs single quantum dot,” Phys. Rev. B 72, 155307 (2005).

4）A. Kirihara, S. Kono, A. Tomita, K. Nakamura, K. Naoi: “Development of Scanning Near-field Optical Microscope Working Under Low Temperature and Strong Magnetic Field,” submitted to Asia-Pacific Conference on Near-Field Optics (APNF), Niigata, Japan.


研究者名：小島 邦裕、富田 章久