量子エンタングルメントを用いたセキュリティー技術の研究（031303020）

Researches on security systems using entanglement

研究代表者
山本喜久　国立情報学研究所
Yoshihisa Yamamoto　National Institute of Informatics

研究分担者
松本啓史　根本香絵　小林弘忠　ピーター・ファン・ルーク
Keiji Matsumoto　Kae Nemoto　Hirotada Kobayashi　Peter van Loock
国立情報学研究所
National Institute of Informatics

研究期間　平成 15 年度～平成 19 年度

本研究開発の概要

量子エンタングル状態を用いた、ネットワーク・セキュリティー技術に関して、計算機科学的・物理学的研究を行う。まず、従来の古典計算に依存した方式の理論的限界を上回る安全性と効率を持つ方式の開発のため、量子ゼロ知識証明などの計算機科学的研究を行う。このようなプロトコルの実現のためには、量子中継技術を用いて量子エンタングルメントを遠隔地間に確立し、量子メモリ技術を用いてある一定時間維持しなければならない。このため、光量子ビットの情報を電子スピンを介して原子核スピンへと変換する固体素子の開発を行う。

Abstract

Our target is computer scientific and physical research about security technology exploiting quantum entanglement. First, we will develop protocols for security which outperforms conventional one. For this, we will study quantum zero-knowledge proof and related quantum complexity theoretic topics. Second, to implement such protocols, we will study basic technologies needed for distribution and storage of entangled quantum states. Namely, we will develop solid state devices which transfer quantum information from photons to atomic nuclear via electric spins.

１．まえがき

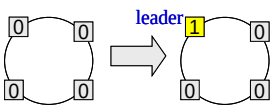
数理的な研究では、ゼロ知識対話証明で成果があった。また、匿名リーダー選挙問題の量子アルゴリズムや自己テレポーテーションのプロトコルと、新しい効率の良いエンタングルメント配信の方法を考案した。
エンタングルメント配信の実現については、まず、単一光子源、高性能の単一光子検出器の開発に成功した。また、NMR パルス技術を応用し、寿命の長い核スピンの量子メモリーを開発した。量子情報の変換については、不純物集団の EIT を用いる方法と、二次元フォトニック結晶を用いる方法の双方で開発をすすめ、さらに連続光と単一光子とのハイブリッドを推し進めた。

２．研究内容及び成果

1. 理論研究

1.1 匿名リーダー選挙

匿名リーダー選挙は、参加者全員が同じアルゴリズムに従いながら動作をしつつ、確実に対称性を破ることを目指すものである。これは「分散計算」の最も基礎的な問題の一つであり、かつ古典計算では、どれだけ時間をかけても失敗確率を 0 にすることができない。我々は、参加者の数の多項式時間で確率 1 で問題を解く量子アルゴリズムを発見した。本アルゴリズムは、Brassard-Hoyer-Tap の振幅増幅法を拡張したものである。



1.2 量子ゼロ知識証明

ゼロ知識証明は、対話型証明のうち、正直な証明者はその正当性以外の情報を何も漏らすことなく、検証者の検証に合格することができるものである。量子ゼロ知識証明においては、不明なことが多く、とくに完全ゼロ知識、計算量的ゼロ知識についてはほとんど何もわかっていなかった。（後者は応用上もっとも重要。）我々は、これらの場合において、数多くの望ましい性質を証明した。例えば、正直な検証者に対してのみ安全なプロトコルを、悪意のある検証者の攻撃に対して安全にする変換方法をこれらの場合に編み出した。

1.3 自己テレポーテーション

量子情報理論では、LOCC（局所的量子操作と古典通信）でタスクを実行するときの効率がしばしば問題にされる。例えば与えられた未知の状態やクローンなどがしばしば取り上げられる。しかし、従来は一般論はあまりなく、個別具体例の研究がほとんどであった。我々は、多数（20 程度以上）の同一純粋状態を二者が共有している場合について、これらの問題について統一的なアプローチに成功した。その理論の鍵になるプロトコルが以下に述べる自己テレポーテーションである。

プロトコルの目的は、LOCC だけを用いて、A と B が共有している状態を B の手元に集めることである。外部の量子的なリソースは使わず、共有している粒子の数も減らさない。また、粒子数の指数関数程度の誤差しか許さない。これをサブルーチンとして用いると、多くのタスクが LOCC でもほとんど精度をおとさずに達成できることがわかる。

1.4 エンタングルメント配信

エンタングルメントの共有の為には、その配信と精製を効率よく行うプロトコルが必須である。そのために、第 1 に EIT などで生成可能な弱い光学非線形性を用いる方法を提案した。例えば Bell 測定の精度の理論限界を従来の 50%から 100%へ改善できた。第 2 に、量子メモリーが組み込み可能な人工原子とコヒーレント光とを組み合わせた手法を提案した。これにより、エンタングルメントの生成効率や量子操作の自由度を大幅に改善する目途がたち、実用化にむけて前進した。

2　実験的研究

2.1 単一光子、エンタングル光子対の生成、検出

InAs 単一量子ドットをポスト形のマイクロキャビティの中央に配し、デバイスをピコ秒パルスで光ポンプすることにより、識別できる同一量子粒子としての単一光子パルスを発生することに成功し、これを線形光学系を用いて、Bell 状態に効率 50%で変換することに成功した。

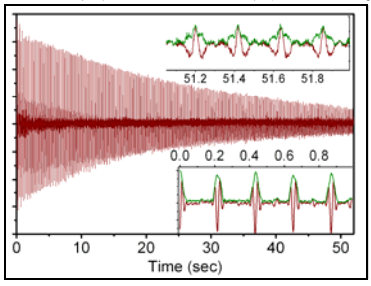
Bell 状態の生成の確認のため、状態トモグラフィーを実行し、CHSH 型のベルの不等式の破れを検証した。また、Bell 状態を二つ発生させ、エンタングルメントスワッピングをすることにも成功した。

光子の検出のために、バルク Si 結晶中にドナー不純物として As を選択ドープした検出器(Visible Light Photon Counter, VLPC) 系を開発した。この検出器は非常に低雑音であり、光子の数を識別することができる。

また、光ファイバー伝送には波長 1.5μm が適しているが、暗検出率が小さいなどの良い特性をもつシリコン APD は、短波長領域にのみ感度がある。そこで、周期的にドメインを反転させた $LiNbU_3$ 導波路（PPLN）を用いて、パラメトリック上方変換で波長 0.7μm の単一光子へと変換することを試み、効率 99%を達成した。

2.2　核スピン量子メモリ

エンタングルメント中継に必要なコヒーレンス時間を達成するために、我々は、シリコン単結晶中の ^{29}Si 原子核スピンの量子メモリを開発した。そして、NMR パルス技術で緩和を抑制することに成功し、室温(300K) で T_2=25sec という極めて長いコヒーレンス時間を達成した。これは、固体素子では最長である。



2.3 光子と量子メモリの間の量子情報の転送

2 次元のフォトニック結晶を用いる方法を理論的に検討した結果、高い Q 値と小さな光モード体積が実現でき、単一量子ドットメモリへの応用が有望であることが判明した。そこで MBE 成長技術と電子ビーム露光技術を用いて、デバイスを作製し、有望な結果を得た。

また、光子 qubit を一度不純物に束縛された電子スピン に EIT で変換し、さらに hyperfine 相互作用を介して、原子核スピン集団の qubit へ変換する方法も研究を進めた。その結果、前半部分で以下の成果があった。

GaAs 中にドープされたドナー不純物(S)に束縛された電子スピンのゼーマン分裂準位を 2 つの基底状態とし、この中性ドナーに束縛されたエキシトンを励起状態とするラムダ構造を用い、半導体素子としては世界初の EIT の観測に成功した。また、1～10GHz という広帯域を実現している。これに対し、従来の原子ガス集団を用いる EIT が帯域幅が狭く、量子ネットワークへの応用には向かない。

３．むすび

数理的研究においては、特に最終年度にいたってゼロ知識証明、自己テレポーテーションなどの大きな成果があった。実装への理論的なアプローチでは、エンタングルメント配信の方法を中心に新しい提案で大きな進歩があった。物理的実装については、単一光子を軸にした技術の開発から始まって、連続光とのハイブリッド技術への進展があり、着実に成果を挙げ続けてきた。各々の分野で成果があった一方、両者の橋渡しが弱かった点は反省点である。

【誌上発表リスト】

[1] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, Y. Yamamoto “Hybrid quantum repeater using bright coherent light”, Phys. Rev. Lett. 96, 240501 (19 June, 2006)

[2] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, “Quantum key distribution over 40 dB channel loss using superconducting single photon detectors”, Nature Photonics 1, 343 (01 June 2007)

[3] K. Matsumoto, M. Hayashi, “Universal distortion-free entanglement concentration,” Phys. Rev. A **75**, 062338 (29 June 2007)

【申請特許リスト】

[1] Y. Yamamoto, E. Diamanti, E. Waks, K. Inoue, H. Takesue, T. Honjo, Differential phase shift keying quantum key distribution, The Board of Trustees of the Leland Stanford Junior University （USA), NTT Corporation (Japan), 2005 年 4 月 11 日

[2] Kae Nemoto, Peter van Loock, Yoshihisa Yamamoto, William J. Munro, Quantum repeater, England, 2005 年 8 月 12 日

【受賞リスト】

[1]山本喜久、紫綬褒章、2005 年 11 月 3 日
[2]山本喜久、志田林三郎賞、2006 年 6 月 1 日
[3]山本喜久、米国物理学会フェロー、2007 年 11 月 19 日

【報道発表リスト】

[1] “「量子暗号」実用化へ―盗聴を完全防止、新聞 4 ページ 1 秒で伝送”、日本経済新聞、2005 年 8 月 19 日
[2]“連続光使い量子中継”、日経産業新聞、2006 年 6 月 20 日
[3]“「量子暗号」で新方式”、朝日新聞、2006 年 7 月 25 日

【本研究開発課題を掲載したホームページ】

http://www.nii.ac.jp/research/project_gaiyo-j.shtml