擾乱計測技術に基づく安全な量子通信の研究開発（121806010）

Secure quantum communication based on disturbance measurement

研究代表者

小澤 正直　名古屋大学

Masanao Ozawa　Nagoya University

研究分担者

浜田　充†　枝松　圭一††

Mitsuru Hamada†　Keiichi Edamatsu††

†玉川大学　††東北大学

†Tamagawa University　††Tohoku University

研究期間　平成 24 年度～平成 26 年度

概要

量子測定の一般理論に基づいて誤差と擾乱に関する最良の不確定性関係を導き、それに基づいて盗聴通信路の擾乱に関する一般理論を確立するとともに、それらを現実の系に応用するために、弱測定の一般理論を展開して、弱測定によって通信路の擾乱を計測する基礎技術を開発した。また、盗聴下通信のための新しい符号化方式を考案し、量子インストルメントを用いた通信路モデルにおける符号性能の解析を行った。

１．まえがき

インターネット上の秘匿性通信として広く実用化されている公開鍵暗号は、盗聴者と正規の利用者の間の計算量ギャップをその安全性の根拠にしているが、量子計算機など、将来、画期的な計算機が発見されれば、安全性が崩壊する可能性がある。この問題を解決するために、量子鍵配送プロトコルの研究が欧米諸国や我が国で活発に進められているが、無条件安全な暗号の実現には、効率と経済性に関する大きな制約が知られている。そのため、情報通信の大容量化と高秘匿性を確保する量子情報通信ネットワークの実現のためには、現在、研究開発の主流となっている量子鍵配送プロトコルの万能性には疑問があり、将来的には、高速光ネットワークへの実装を視野に入れた物理レイヤーでの量子暗号の多様な研究開発が必要である。本研究では、この課題のために、量子インストルメントおよび量子測定の一般理論を基礎として、誤差と擾乱に関する最良の不確定性関係を導き、盗聴通信路において擾乱の計測により安全性を確保する一般的方法の構築、通信路の擾乱を計測する基礎技術の開発、盗聴通信路のための新しい符号化方式の開発を目的とする。

２．研究開発内容及び成果

２.１．不確定性原理に基づく量子暗号の安全性

量子暗号の安全性は、盗聴者の測定行為が暗号通信路を不可避に乱すという不確定性原理によって保証されると考えられてきた。しかし、近年の量子測定理論の進歩により、従来の不確定性原理からはそのような安全性が導かれないことが明らかになってきた。小澤は、1988 年にガンマ線顕微鏡の思考実験で得られた測定誤差と擾乱に関する Heisenberg の不等式が一般には成立しないことを示し、2003 年に完全に一般の測定に対して成立する新しい不等式（小澤の不等式）を世界で初めて導いた。Branciard は、2013 年に小澤の不等式が十分にタイトでないことを示し、より強力な不等式（Branciard の不等式）を導いた。ところが、Branciard の不等式は、量子暗号に応用される混合状態における測定については、全く無力であり、量子暗号の安全性を導くためには更に強力な不確定性関係を導く必要がある。本研究では、そのような不確定性関係の導出を第１の研究課題として、研究を行った結果、量子暗号の安全性に必要な混合状態の測定に関して最良の不確定性関係を導くことに成功した。この不等式は、小澤の不等式や Branciard の不等式より強力で、これまでに知られた誤差・擾乱関係式のうちで最も強力なものである。本研究では、さらに上の研究で得られた不確定性関係を完全に一般的な量子通信に対する盗聴誤差と通信路の擾乱の関係に適用し、通信路やプロトコルに限定されない普遍的な量子通信の安全性理論を確立した。

２.２．弱測定に基づく擾乱計測法

不確定性関係を量子暗号に利用するためには、通信路が盗聴により被る擾乱を実際に計測する方法が必要である。この擾乱は、送信者アリスと受信者ボブが計測可能なデータから決定されなければならないが、この問題には、量子力学特有の困難が含まれている。つまり、誤差と擾乱が２つの非可換な物理量の差の２乗平均から得られるので、測定不可能であり，操作的な関係式ではないと言う批判的な主張が文献に見られるようになった。しかし、実は、誤差と擾乱は平均量として定義されているので、この批判は根拠がない。

そこで、2004 年に小澤は、アリスが 2 種の補助状態を生成して、擾乱を測定する **3 状態法**を提案した。一方、アリスが Aharonov 等によって提唱された弱測定と呼ばれる測定をし、ボブが同じ物理量を強測定すると、その測定データから、2005 年に小澤によって得られた公式により擾乱を定めることができる。この方法を**弱測定法**と呼ぶ。Lund と Wiseman は、2010 年にこの方法で小澤の不等式の検証実験を行なうことを提唱している。3 状態法は、小澤とウィーン工科大の長谷川との共同研究で中性子スピン測定の実験で検証に成功したが、本研究の提案段階では、弱測定法の検証実験はまだ実現していなかった。本研究では、枝松によってこの弱測定擾乱計測法の光子の偏光測定における実験的検証を実現した（図 1）。

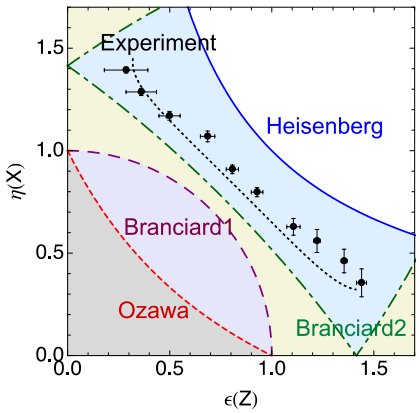

図 1. 誤差（ε）と擾乱（η）に関する測定結果と不等式の下限値をプロットしたもの。黒丸は実験結果，黒点線は測定装置の性能を加味した理論値。青の実線が Heisenberg の不等式，赤の点線が小澤の不等式，紫の破線が Branciard の不等式（一般式），緑の一点鎖線が Branciard の不等式（２値の場合）における下限値。実験値はハイゼンベルクの不等式を破り，他の不等式は満たす領域にある。特に，Branciard の不等式（２値の場合）の下限に近接している。

２.３．通信路非依存的秘匿性を持つ誤り訂正符号

擾乱計測技術を用いた新しい暗号方式は、これまでのプロトコルと異なる広い汎用性があり、その実装には、通信路に依存しない秘匿性を有する新しい量子符号が必要となる。浜田は、2008 年に量子インストルメントの数学理論に基づき、通信路に依存しない多項式時間構成可能な安全な符号化方式の存在を証明している。本研究では、この符号の具現化を行った。また、このような有限シンプレクティック構造を生かした復号の容易さや安全性を有する符号を体系的に扱う理論を構築し、符号の安全性の評価を与えた。

これまで、浜田は、剰余符号という線形符号の一般化と見なせる符号を自ら提唱し、その構成法を探究してきた。特に 2009 年頃提案した連接符号化方式が、情報理論において有名な盗聴通信路モデルにおいて漸近的最良であることを証明した。本研究開発はその連接符号化方式をベースにして行った。この連接符号化法の漸近的最良性の証明では、(1) まず有限の符号長で性能指標である正規通信路における誤り確率と盗聴者への情報漏えい量を評価し、(2) それらの符号長が大きくなるにつれて零に近づくというということを示している。本研究開発では、(1) の安全性評価が有限の符号長で為されていたことに注目し、具体的な符号について情報漏えい量を評価した。これは、Fano の不等式と呼ばれる情報理論における基本的な不等式を改良することで得られた。

また、浜田は、量子計算のための回路（アルゴリズム）のユニバーサルな構成の問題を動機として、SU(2)において任意の元を積に分解する問題を提起し解決した。SU(2)から 3 次元ユークリッド空間における回転のなす乗法群 SO(3)への準同型により、同時に、任意の回転を回転の積に分解する問題も解決した。具体的には、分解後の要素はあらかじめ与えられた 2 軸のまわりの回転に限るという制約の下、任意の回転を分解するのに必要な分解要素の最小数を決定し、また、その分解を与えるアルゴリズムを与えた。

３．今後の研究開発成果の展開及び波及効果創出への取り組み

不確定性原理は、量子論の基本原理として広く知られてきたが、その科学的解明は、ごく最近始められたばかりである。本研究開発では、不確定性原理に現れる「誤差」と「擾乱」という数学的に定義された変数に対して、擾乱計測法という新しい科学的計測方法を確立し、実験でそれを実現して、「不確定性原理」を実験データとして目に見える関係にまで具現化することに成功した。このような新しい計測可能な量の出現は、量子情報通信の分野に新たな技術革新をもたらすものとして非常に大きなインパクトをもつ。本研究開発以前は、小澤の不等式の実験的検証は中性子を用いた研究で端緒がつけられたばかりであり、その適用範囲は未だ限定的であった。本研究開発では、量子情報通信分野で最も良く利用される媒体である光子を用いることで、射影測定のみならず一般的な測定相互作用に拡張した検証実験が可能となった。そのため、更に強化された測定に関する不確定性原理の応用範囲が飛躍的に広がった。特に、弱測定に伴う擾乱計測の理論の構築とその実験的検証は、量子通信のみならず量子情報技術全般における道標的成果となり、今後、精密測定技術全般に波及することが期待される。また、本研究開発の手法を発展させることで、単一光子の偏光（スピン）という二準位系のみならず、多光子数状態などの高次元系や直交位相などの連続変数、またはそれらの間のハイブリッド系などへの応用も可能となり、本研究における検証実験はその先鞭として重大な意義をもつ。

４．むすび

物理レイヤーでの量子暗号技術の多様な研究開発に柔軟かつ確実に対応するために、本研究では、誤差と擾乱に関する最良の不確定性関係を導き、盗聴通信路において擾乱の計測により安全性を確保する一般的方法の構築、通信路の擾乱を計測する基礎技術の開発、盗聴通信路のための新しい符号化方式の開発に成功した。

【誌上発表リスト】

[1]F. Buscemi, M. J. W. Hall, M. Ozawa, and M. M. Wilde, “Noise and disturbance in quantum measurements: Information-theoretic approach”, Physical Review Letters 112, 050401 (2014 年 2 月 3 日)
[2] F. Kaneda, S.-Y. Baek, M. Ozawa, and K. Edamatsu, “Experimental test of error-disturbance uncertainty relations by weak measurement”, Physical Review Letters 112, 020402 (2014 年 1 月 13 日)
[3]M. Hamada、“The minimum number of rotations about two axes for constructing an arbitrarily fixed rotation”, Royal Society Open Science 1, 140145 (2014 年 11 月 26 日)

【受賞リスト】

[1]小澤正直、第 1 回藤原洋数理科学賞大賞、“量子情報理論の数学的基礎付け”、2012 年 9 月 0 日
[2]小澤正直、第 66 回中日文化賞、“「小澤の不等式」の発見”、平成 2013 年 5 月 30 日

【報道掲載リスト】

[1] “「小澤の不等式」光で証明”，読売新聞，2013 年 7 月 18 日
[2] “量子力学の原則　新理論提唱　「小澤の不等式」裏付け”，朝日新聞，2013 年 8 月 8 日
[3] “新理論「小澤の不等式」　新測定法で実証”，日本経済新聞，2013 年 12 月 25 日