様式 C-19

科学研究費補助金研究成果報告書

平成２３年　５月１１日現在

機関番号：１４４０１
研究種目：基盤研究（C）
研究期間：2008～2010
課題番号：２０５４０３８９
研究課題名（和文）　量子力学の相補性を利用した量子情報処理の研究

研究課題名（英文）　Quantum information processing based on complementarity in quantum mechanics

研究代表者
小芦　雅斗（KOASHI MASATO）
大阪大学・大学院基礎工学研究科・准教授
研究者番号：９０３２２０９９

研究成果の概要（和文）：量子力学の相補性に基づいた量子鍵配送方式のセキュリティ理論を構築した。この方法は、原理的には、あらゆる量子鍵配送方式に適用することができる。現実的な装置を用いたいくつかの量子暗号方式について、セキュリティの証明を行った。また、異なる視点から量子相関の大きさを操作的に定義し、相互の普遍的な関係式を導くことで、量子もつれ、秘匿通信、および相補性という相異なる量子性の発現の定量的な関係を明らかにした。

研究成果の概要（英文）：Theory on the security of quantum key distribution (QKD) protocols based on complementarity in quantum mechanics has been developed. This method is applicable to any QKD protocols in principle. Security proofs were provided for several QKD protocols with practical devices. Quantitative relations among various properties of quantum origin (quantum entanglement, private communication, and complementarity) were revealed through derivation of universal equations connecting the measures of quantum correlation defined operationally in terms of those properties.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	1,200,000	360,000	1,560,000
２００９年度	1,300,000	390,000	1,690,000
２０１０年度	700,000	210,000	910,000
年度			
年度			
総　計	3,200,000	960,000	4,160,000

研究分野：　量子情報
科研費の分科・細目：物理学、原子・分子・量子エレクトロニクス
キーワード：相補性、量子暗号、量子鍵配送、量子もつれ

１．研究開始当初の背景

量子力学の性質を利用して、２者間で暗号通信を行う量子暗号(量子鍵配送)では、あらゆる盗聴行為に対して漏洩がないことを表す無条件安全性を証明するセキュリティ理論が重要である。無条件安全性の最初の証明は､Mayersによって1995年頃に与えられた。しかし、その手法は非常に複雑であったため、2000 年に量子もつれ抽出法に還元する簡単な証明法がShorとPreskillによって提案されると、以降はこの手法が主に用いられるようになった。しかし、量子もつれ抽出法に還元できない状況でも暗号通信が行える例が見出されるなど、この手法の限界が見え始めていた。現実的な送受信装置を用いた場合のセキュリティや、応用上の利点を追求した新しい量子暗号方式のセキュリティについては、未解決の問題が多く残されているため、適用範囲の広い強力なセキュリティ理論が

待ち望まれていた。
一方、研究代表者は、Mayers の難解な証明の本質が、量子力学の相補性にあることを指摘し、非常に簡単な証明法を提案した。この相補性による無条件安全性の証明法は、量子もつれ抽出法による証明を包含するのみならず、量子もつれ抽出法が適用できない場合でも有効である。また、従来のセキュリティ証明では、光子数識別検出器を仮定する必要があったのに対し、相補性を使うと、実際に用いられているオンオフ型の光子検出器を取り扱うことができるなど、この証明法は従来にない利点を有していた。

２．研究の目的

本研究では、研究代表者の提案による、量子力学の相補性に基づくセキュリティ理論を発展させ、その適用範囲を拡げ、現実的な送受信装置を用いた場合のセキュリティなどの未解決の問題の解決を目指す。同時に、量子もつれと、量子暗号のセキュリティ、および量子力学の相補性という、量子性の相異なる性質が、本質的にどのように結び付いているのかを、定量的に明らかにすることを目指す。また、量子もつれの測定法など、相補性の考え方を量子暗号以外に応用する可能性を検討する。

３．研究の方法

１粒子の干渉計において、粒子として辿った経路を決める測定と、波動として干渉した時の干渉縞の測定は、同時に行うことが出来ない。このように、量子系では、一種類の測定で全ての性質を捉えることができず、両立しない複数の測定法を考える必要があり、相補性と呼ばれている。離れた場所にいる２者(Alice と Bob とする)の間の通信を考える場合にも、やはり両立しない２つのタスクが現れることがある。例えば、Alice が持つスピン 1/2 の粒子の向きを、z 軸方向で測定した場合の結果(+z 方向か-z 方向か)を、Bob が推定せよ、というタスクと、x 軸方向の測定結果を推定せよ、というタスクは、同時に遂行することは不可能である。一方、もし Bob もスピン 1/2 粒子を持ち、二人の持つ２粒子が一重項状態にあれば、Bob は２つのタスクのうちのひとつを好きに選んで遂行することは可能になる。この例は、本質的には EPR の議論にも登場するなど古くから知られているが、研究代表者によって、このような通信タスクの相補性と、暗号通信との間の強い関連性が浮かび上がってきた。具体的には、同時には実行できない２つのタスクを考え、必要に応じてどちらのタスクも実行可能であることを示すだけで、量子暗号通信が盗聴者に対して無条件に安全であることが証明できる、というものである。
本研究では、まず、このような考え方に基づく量子暗号のセキュリティの証明法を、一般的な形で整理し、セキュリティ理論を完成させる。その理論に基づき、現実的な送受信装置を用いた場合の量子暗号のセキュリティに関する未解決の問題の解決に取り組む。また、例えば、「相補性に関するタスク A がある精度で達成可能ならば、量子もつれの性質に関するタスク B が、ある精度以上で必ず実行できる」という形の命題の証明を積み上げていくことで、量子もつれ、相補性、および秘匿通信を行う能力との間の定量的な関係を明らかにする。

４．研究成果

(1)相補性に基づく量子暗号のセキュリティの証明法を、一般的な形で定式化した。具体的には、実際に秘密鍵を決定するプロセスを、キュビット列に対する Z 基底での測定の形で記述する。次に、盗聴者から見ると同じに見えるが、秘密鍵は作らずにキュビット列を X 基底の固有状態に近づけることを目標とする仮想的なプロトコルを構築する。すると、この仮想プロトコルの成功確率から、もとの量子暗号のセキュリティを表す指標が決定される。セキュリティを表す指標としては、他のプロトコルと併用した場合でも通用する指標を用いた。また、３基底が絡むために２物理量の相補性を用いる証明法と直感的には整合しにくい６状態量子暗号についても、上記の定式化によって、相補性の観点からセキュリティが証明できることを示した。

(2)送受信者の持つ２つの量子系の相関状態がどの程度量子的であるかを表す定量的な指標を、量子暗号によって秘匿通信を行う能力、量子もつれの大きさ、および相補性に関する性質という異なる観点から操作的に定義し、異なる指標の間の定量的な関係を調べることで、その間に成り立つ非常に単純な等式を導いた。この等式は、混合状態を含むあらゆる相関状態について普遍的に成立するものであるから、この結果は、相補性、秘匿通信、量子もつれという相異なる量子性の顕現の仕方が、定量的な美しい関係でとらえられる本質的な結びつきを持っていることを示している。また、量子もつれがなくても秘匿通信が可能という特異なケースが出現する理由が、相補性の観点から明らかになったと言える。さらに、この等式は、相補性に基づくセキュリティ理論が、秘匿通信の本質を正確に捕捉していることを示す。すなわち、本研究で構築された証明法は、適用範囲に原理的な限界のない究極のセキュリティ理論

になっていることがわかる。

(3)量子もつれを持つ光子対を用いる量子暗号方式について、普及型のオンオフ光子検出器を用い、光源については何の仮定も設けずにセキュリティを保証する手法を提案した。この結果は、量子もつれを持つ光子対の使用によって、光源の信頼性の問題を回避できることを示す。とくに、量子中継器を用いた長距離量子暗号では、光源が実質上盗聴者の支配化にあるので、このようなセキュリティの証明は重要である。

(4)強い位相参照光をもつ２状態量子暗号は、単純ではあるが光子分離攻撃に耐性を持つという特長を有する。しかし、その無条件安全性については、位相参照光の量子性を考慮せずに済む場合にのみ証明がなされており、その証明を適用するためには局部発振光を二つ用意するなど実装上の困難があった。本研究では、位相参照光を量子化した無条件安全性の証明を行った。この証明は、局部発振光を送信者のみが用意する通常の実装に対応している。

(5)単一光子光源は、理想的であれば光子分離攻撃を受けつけないために、単純な量子暗号方式により高効率を達成できるはずである。しかし、実際の単一光子光源は、２個以上の光子を放出する確率がゼロではないため、光子分離攻撃を受ける可能性があり、距離が伸びるにつれて、２光子放出確率に対する要求が厳しくなっていく。本研究では、光の一部を分岐して光子検出を行うという単純な改良によって、光子分離攻撃に対する耐性を向上させる手法を提案した。この手法は、３光子以上の放出確率分布の知識を利用しており、同じ光源であっても、高次の光子統計を把握する精度を上げると、実効的には２光子放出確率を下げたのと同様に通信効率が向上するという特長を持つ。

(6)３基底を切り替える６状態量子暗号方式は、よく用いられる２基底の BB84 方式に比べ、似たような装置でも鍵生成レートやビット誤り耐性を向上できる手法として知られているが、光子数を峻別できない普及型の光子検出器を用いた場合に、そのような優位性が維持できるかどうかは不明であった。まず、３基底を均等に切り替える方式では、検出器の同時計数率を手掛かりとすることで、多光子攻撃の頻度を見積もり、簡単に安全な鍵生成レートを導けることを示した。しかし、この手法は送受信者間で基底が一致したケースを選択する過程が BB84 方式よりも非効率となり、多くの場合に優位性が失われてしまう。そこで、３基底を不均等に切り替える方式のセキュリティ確立が重要になる。この場合には、均等切替えの場合にはなかった３光子攻撃が存在することを示した。さらに、そのような攻撃も含めた最終的なセキュリティの証明を行うことで、あらゆる場面で BB84 方式よりも高い鍵生成レートが得られることを示した。

(7)量子暗号では光子の量子状態をなるべく壊さずに受信者に届ける必要があるが、光ファイバ等を用いた通信路では、様々な雑音が混入してくる。その中で、屈折率ゆらぎのようなゆっくりした雑音は、異なるパルスに同じ変化が加わる形をしており、この場合にはＤＦＳと呼ばれる量子状態保護の手法の適用が可能になる。これまで、ＤＦＳの状態を直接発生させて、その状態が保護されることは実験で確認されているが、そのような手法は他の系と量子もつれを持つ量子系の送信には適用できない。本研究では、与えられた任意の量子状態をＤＦＳの状態に変換して通信する手法を用い、量子もつれをもつ量子系をＤＦＳにより雑音から保護できることを実験的に示した。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１２件）

① R. Ikuta, Y. Ono, T. Tashima, T. Yamamoto, M. Koashi, and N. Imoto: Efficient Decoherence-Free Entanglement Distribution over Lossy Quantum Channels, Physical Review Letters Vol.106, 110503:1--4 (2011), 査読有.

②R. Ikuta, T. Tashima, T. Yamamoto, M. Koashi, and N. Imoto: Optimal local expansion of W states using linear optics and Fock states, Physical Review A Vol.83, 012314:1--8 (2010), 査読有.

③T. Tashima, T. Kitano, S. K. Ozdemir, M. Koashi, and N. Imoto: Demonstration of Local Expansion Toward Large-Scale Entangled Webs, Physical Review Letters Vol. 105, 210503:1--4 (2010), 査読有.

④K. Azuma, N. Sota, M. Koashi, and N. Imoto: Tight bound on coherent-state-based entanglement generation over lossy channels, Physical Review A Vol. 81, 022325:1--6 (2010), 査読有.

⑤K. Azuma, N. Sota, R. Namiki, S. K. Ozdemir, T. Yamamoto, M. Koashi, and N. Imoto: Optimal entanglement generation for efficient hybrid quantum repeaters, Physical Review A Vol. 80, 060303(R):1--4 (2009), 査読有.

⑥Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto: Boosting up quantum key distribution by learning statistics of practical single-photon sources, New Journal of Physics Vol.11, 113033:1--10 (2009), 査読有.

⑦K. Tamaki, N. Lutkenhaus, M. Koashi, and J. Batuwantudawe: Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse, Physical Review A Vol.80, 032302:1--9 (2009), 査読有.

⑧M. Koashi: Simple security proof of quantum key distribution based on complementarity, New Journal of Physics Vol.11, 045018:1--12 (2009), 査読有.

⑨T. Tashima, T. Wakatsuki, S. K. Ozdemir, T. Yamamoto, M. Koashi, and N. Imoto: Local transformation of two Einstein-Podolsky-Rosen photon pairs into a three-photon W state, Physical Review Letters Vol.102, 130502:1--4 (2009), 査読有.

⑩M. S. Tame, S. K. Ozdemir, M. Koashi, N. Imoto, and M. S. Kim: Compact Toffoli gate using weighted graph states, Physical Review A Vol.79, 020302(R):1--4 (2009), 査読有.

⑪T. Tashima, S. K. Ozdemir, T. Yamamoto, M. Koashi, and N. Imoto: Local expansion of photonic W state using a polarization dependent beamsplitter, New Journal of Physics Vol.11, 023024:1--10 (2009), 査読有.

⑫T. Yamamoto, K. Hayashi, S. K. Ozdemir, M. Koashi, and N. Imoto: Robust photonic entanglement distribution by state-independent encoding onto decoherence-free subspace, Nature Photonics Vol.2, 488--491 (2008), 査読有.

〔学会発表〕(計３０件)

①Masato Koashi: Complementarity approach to security of quantum key distribution with practical devices, Updating Quantum Cryptography and Communications (UQCC2010) (招待講演), 2010/10/19, ANA InterContinental Hotel, Tokyo, Japan.

②Masato Koashi: Security of quantum key distribution with practical devices, International Conference on Core Research and Engineering Science of Advanced Materials (Global COE Program), Third International Conference on Nanospintronics Design and Realization (3rd-ICNDR) (招待講演), 2010/5/30, Convention Center, Osaka University, Osaka, Japan.

③Masato Koashi: Understanding security of quantum key distribution via complementarity, 2010 International Symposium on Physics of Quantum Technology (2010 ISPQT) (招待講演), 2010/4/9, Hitotsubashi memorial hall, Tokyo, Japan.

④Masato Koashi: Security of key distribution and complementarity in quantum mechanics, The 4th International Conference on Information Theoretic Security (ICITS2009) (招待講演), 2009/12/4, Granship, Shizuoka, Japan.

⑤Masato Koashi: Complementarity and security of quantum key distribution, The 3rd Conference on Quantum Information and Quantum Control (CQIQCIII) (招待講演), 2009/8/27, Fields Institute, Toronto, Canada.

⑥Masato Koashi: Quantitative relations among different aspects of quantum correlations, The 4th Workshop on Theory of Quantum Computation, Communication, and Cryptography (TQC 2009) (招待講演), 2009/5/13, University of Waterloo, Canada.

⑦小芦雅斗、相補性及びエンタングルメントと量子暗号、日本物理学会第６４回年次大会 29pTB-5(シンポジウム講演)、2009/3/29、立教大学.

⑧Masato Koashi: Quantum nonlocality without entanglement in a pair of qubits, DEX-SMI Workshop on Quantum Statistical Inference(招待講演), 2009/3/2, National Institute of Informatics (NII), Tokyo, Japan.

⑨Masato Koashi: Entanglement, monogamy, and complementarity, UK-Japan Quantum Information Workshop(招待講演), 2009/1/22, British Embassy Tokyo, Japan.

⑩Masato Koashi: On the irreversiblity of measurements of correlations, International Workshop on Statistical-Mechanical Informatics 2008(招待講演), 2008/9/14, Sendai International Center, Japan.

⑪小芦雅斗、量子暗号に現れる量子力学の諸性質、科学基礎論学会２００８年度講演会シンポジウム(招待講演), 2008/6/21, 東京電機大学.

〔図書〕(計１件)
①小芦雅斗、小柴健史、サイエンス社、SGC ライブラリ 67:量子暗号理論の展開、2008 年、1-78.

６．研究組織
(1)研究代表者
小芦　雅斗 (KOASHI MASATO)
大阪大学・大学院基礎工学研究科・准教授
研究者番号：９０３２２０９９

(2)研究分担者
(　　)

研究者番号：

(3)連携研究者
(　　)

研究者番号：