様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 １５ 日現在

機関番号：１２６０１
研究種目：若手研究
研究期間：2018～2021
課題番号：１８Ｋ１３４６９

研究課題名（和文）装置不完全性を考慮した量子鍵配送理論

研究課題名（英文）Quantum key distribution with imperfect devices

研究代表者
佐々木　寿彦（Sasaki, Toshihiko）

東京大学・大学院工学系研究科（工学部）・講師

研究者番号：８０７３４３５０

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：本研究課題では、なるべく性能を犠牲にせずに量子鍵配送の装置モデルをより現実に即するよう拡張し、実験によって確認できるデータを用いて安全性を保証することを目的として研究した。量子鍵配送の装置モデルを拡張する研究は様々あるが、多くのものは解析が簡単になる実験時間が無限の場合の漸近的性能を扱っている。この課題では、実験時間が有限の場合の解析を行ったのが特徴的である。
扱った題材は、光源の厳密な検定方法、装置簡略化の悪影響の回避方法、光子検出器より安価な光検出器を使って量子鍵配送を行う方法、様々な装置不完全性に自動的に対応できる数値手法の開発である。

研究成果の学術的意義や社会的意義
量子鍵配送は遠隔2者間で安全な乱数列を共有する手法であり、これを用いることで長期的に安全な秘密通信が可能になる。この手法は実際に製品にもなり、社会に導入されようとしている。実際の装置の安全性を示すためには、理想化された状況だけでなく、現実に即したモデルを考える必要があるが。本研究課題では、現実的な制約のもとで安全性を示すための新たな手法を開発することで、理論と現実のギャップを縮め、量子鍵配送を安価に実現することに貢献した。

研究成果の概要（英文）：The purpose of this research project is to extend the device model of quantum key distribution to be more realistic without sacrificing performance as much as possible, and to guarantee security using data that can be confirmed by experiments. There are various studies on extending the device model of quantum key distribution, but most of them consider only the asymptotic performance when the experimental time is infinite, which simplifies the analysis. This project is unique in that it analyzed the case of finite experimental time.
The subjects in this project are how to rigorously test light sources, how to avoid the negative effects of substituting the devices with cheaper ones, how to perform quantum key distribution using photodetectors, which is cheaper than photon detectors, and how to develop numerical methods that can automatically deal with various device imperfections.

研究分野：量子鍵配送

キーワード：量子情報理論　量子鍵配送

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

量子鍵配送は遠隔２者が下図 1 のような系において情報理論的に安全な乱数(鍵) を共有する手法である。量子鍵配送理論では変調した光パルスを送受信するだけで量子もつれの生成すら必要ないという限りなく古典的な状況において、背後に存在している量子の性質を最大限用いて安全性を証明する。この安全性の証明は実験系が様々な性質をもっていると仮定して行うので、その目的が達成されているか否かは、その仮定が満たされているかに大きく依存している。代表的な量子鍵配送方式である Bennett-Brassard-1984 (BB84) 方式に関しては、繰り返しその安全性が証明されてきたが、その度に前提となる仮定が現実に近づいてきた。最近になって最後の課題であった有限のサンプル数が及ぼす統計的推定誤差の効果である有限鍵長効果の解析手法について大体の共通認識が得られ、量子通信路に関する仮定が取り払われたが、量子通信路以外には未だ様々な仮定が置かれている。これらの仮定の中でも特に重要なのが、通信に用いる送信機や受信機が理論のモデル通りに動いているという仮定である。そもそもとして、量子通信路に仮定を設けず有限鍵長効果を含めて現実的な性能を出しつつ安全性を厳密に示すということが難しい問題として長らく存在したため、盗聴者からの直接の干渉をうけない(と仮定している)手元の装置に関しては理想的な仮定を多く置いてきた。特に、厳密に何かが成り立つという類の仮定や実験的に確認不能な仮定を多く置いてきた。しかし、現実の装置では厳密に何かが成り立つということはないので、不完全性に対処できる柔軟なモデルへ移行する必要がある。

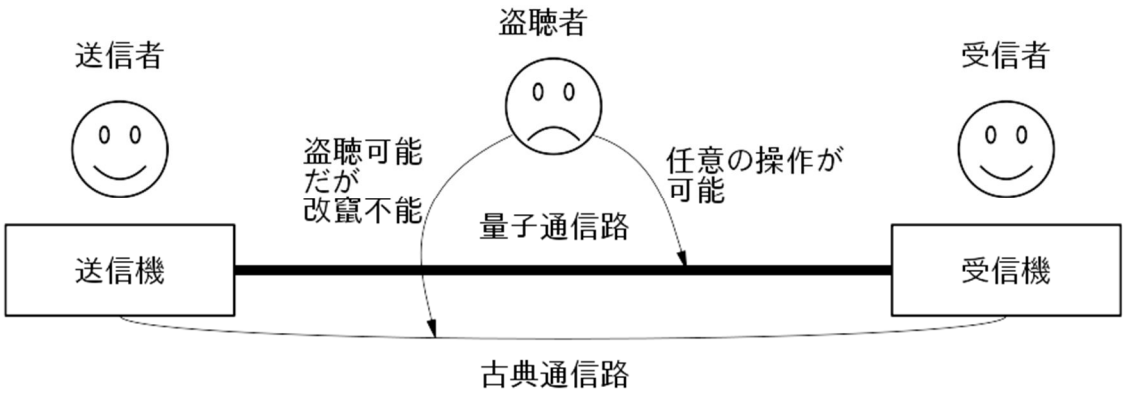

図 1：量子鍵配送の概念図

２．研究の目的

本研究課題では、なるべく性能を犠牲にせずに量子鍵配送の装置モデルをより現実に即するよう拡張し、実験によって確認できるデータを用いて安全性を保証することを目的とする。本研究課題で行うことは、現実との乖離が大きいモデルの仮定を乖離の少ない仮定に置き換えていくという作業であり、完全な解をいきなり目指すというよりは影響の大きなものから順次対処していくというものになる。そのため、量子鍵配送を実際に実験しているグループと連携して、実際の影響が大きい要素を正しく把握するということも重要となる。本研究では、特に媒体として光を用いる場合における送信機と受信機に集中して研究を進める。

３．研究の方法

量子鍵配送の安全性証明においては、有限のサンプル数が及ぼす統計的推定誤差の効果である有限鍵長効果を厳密に取り込むことが証明の難所となる。これは、盗聴者が何をしてくるかわからないなかで厳密な推定をするということであり、よく考えられている独立同分布を想定した解析に比べて使える道具が極端に制限されることを意味する。特に、これまではサンプル数が無限大の領域の漸近的な性質は独立同分布を想定した解析でき、それは有限鍵長効果を含んだ安全性解析にも自動的に拡張可能だと考えられてきたが、想定されてきた手法はそもそも適用できないか、性能が低すぎて現実的には使えないということも近年明らかになりつつある。研究代表者は有限鍵長効果をとりこんだ解析を長く研究してきており、現状で使える手法を熟知しているので、その知見を利用して本研究課題に取り組むことができる。また、研究を始める段階で、パルス光源の光子数分布の問題、受信機の動作速度の問題については一定の方針が立っていたので、それに沿って解析することができる。

４．研究成果

(1) 現状のデコイ法の解析ではレーザーパルスの光子数分布が厳密にコヒーレント状態になっていることが重要な仮定となっている。しかし、実際の量子鍵配送の送信機ではゲインスイッチを用いたパルス生成をしていることが多く、そのような場合に生成されるパルスはコヒーレント状態とは程遠いことが懸念されている。この課題に関してノイズのない閾値型光子検出器を用いて光子数分布を厳密に推定する手法を確立した。また、この手法を多モー

ドの場合に拡張することができた。

(2) 量子鍵配送の実際の装置では 1GHz を越える繰り返しレートでパルスの送受信が行われているが、それを取り扱う現状の理論では、あらゆる素子がこの動作速度で動くことが仮定されている。受動的な素子を使いつつ光検出器の数を増やすことによって、この条件を満たすことができるが、これは実験に使える素子の種類を大幅に制限することになる。一方で、量子鍵配送では送信する光がそもそも弱く、通信路で減衰したあとで検出される信号のレートは繰り返しレートよりずっと低い。よって、受信側の動作速度は送信側より遅くできる余地がある。これは実際そのようにしても性能をほとんど損なわずに安全性を示す方針をたてることができた。

(3) これまでの DPSQKD ではパルス列をブロックに区切ってブロックごとに位相ランダム化を行うということが安全性を保証するために必要となっていた。しかし、ブロックごとでの位相ランダム化処理は実験的に負担であり、現実的に実装する上で障害となる。この論文では、ブロックごとの位相ランダム化を行わない場合でも、安全性が示すことができることを初めて示した。またそれに加えて、光源に対する要求をなるべく少なくして安全性を示した。他には、量子秘匿計算に必要な資源を量子鍵配送での解析手法を用いて低減する論文と、量子サポートノードを用いてこれまでの距離と鍵レートの関係の限界を有限時間でこえる量子鍵配送方式を提案した。

(4) 通常の解析では複数の光子検出器を使っている場合、検出効率が揃っているか、せいぜい比が一定という想定をしている。実際には、暗検出を抑えるためにゲートパルスによる検出率の動的な操作が行われており、この挙動が検出器間で厳密に一致しないためタイミングによっては検出効率の比が極端な値になりえる。これを放置すれば特に遠距離通信において簡単に盗聴可能な状況になる。この問題に対して、実際の検出器のデータにそったパラメータ領域で安全性を示す方式を考案し、実際に有限鍵長効果を取り込んだ安全性証明を構築した。

(5) 検出方法としてホモダイン/ヘテロダイン検出を用いた離散変調の量子鍵配送方式の安全性証明は長らくの課題であった。これは、ホモダイン/ヘテロダイン検出が連続値で非有界であるため、厳密な有限鍵長効果の見積もり手法と相性が悪いというのが、これまでこの問題が解かれてこなかった大きな問題の一つであった。今回は、ヘテロダイン検出を入力とする有界関数を考えることでその結果からノイズなしの状態とのフィデリティを有限鍵長効果こみで厳密に見積もる手法を開発し、さらにこの量を安全性と結びつけることによって安全性証明を完成させた。

(6) 単独要因ではなく、様々な不完全性を同時に扱うモデルでは内部パラメータが増大し、人の直感による性能向上には限界がでてくる。そのため、数値的手法を考える動機はこれまでもあり、先行研究も存在した。しかし、それらは実験時間を無限とした極限での性能を予想するものであり、現実の実験に適用できなかった。今回の結果は有限長といわれる現実の実験時間に対応できる鍵効率公式と安全性証明になっており、現実的な状況で数値的手法による性能改善を導入できるようになった。

５．主な発表論文等

〔雑誌論文〕　計6件（うち査読付論文　6件／うち国際共著　0件／うちオープンアクセス　3件）

１．著者名 Matsuura Takaya、Maeda Kento、Sasaki Toshihiko、Koashi Masato	４．巻 12
２．論文標題 Finite-size security of continuous-variable quantum key distribution with digital signal processing	５．発行年 2021年
３．雑誌名 Nature Communications	６．最初と最後の頁 252
掲載論文のDOI（デジタルオブジェクト識別子） 10.1038/s41467-020-19916-1	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Matsuura Takaya、Sasaki Toshihiko、Koashi Masato	４．巻 99
２．論文標題 Refined security proof of the round-robin differential-phase-shift quantum key distribution and its improved performance in the finite-sized case	５．発行年 2019年
３．雑誌名 Physical Review A	６．最初と最後の頁 42303
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevA.99.042303	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Nagao Kurumiko、Horikiri Tomoyuki、Sasaki Toshihiko	４．巻 99
２．論文標題 Blind quantum computation with a heralded single-photon source	５．発行年 2019年
３．雑誌名 Physical Review A	６．最初と最後の頁 42324
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevA.99.042324	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Maeda Kento、Sasaki Toshihiko、Koashi Masato	４．巻 10
２．論文標題 Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit	５．発行年 2019年
３．雑誌名 Nature Communications	６．最初と最後の頁 3140
掲載論文のDOI（デジタルオブジェクト識別子） 10.1038/s41467-019-11008-z	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Mizutani Akihiro、Sasaki Toshihiko、Takeuchi Yuki、Tamaki Kiyoshi、Koashi Masato	4．巻 5
2．論文標題 Quantum key distribution with simply characterized light sources	5．発行年 2019年
3．雑誌名 npj Quantum Information	6．最初と最後の頁 87
掲載論文のDOI（デジタルオブジェクト識別子） 10.1038/s41534-019-0194-3	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Kumazawa Masahiro、Sasaki Toshihiko、Koashi Masato	4．巻 27
2．論文標題 Rigorous characterization method for photon-number statistics	5．発行年 2019年
3．雑誌名 Optics Express	6．最初と最後の頁 5297～5297
掲載論文のDOI（デジタルオブジェクト識別子） 10.1364/OE.27.005297	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計8件（うち招待講演　4件／うち国際学会　3件）

1．発表者名 佐々木寿彦
2．発表標題 量子暗号通信の安全性
3．学会等名 日本銀行金融研究所 情報技術研究センター 情報セキュリティ・セミナー（招待講演）
4．発表年 2022年

1．発表者名 佐々木寿彦
2．発表標題 量子鍵配送の有限長安全性証明手法の現状について
3．学会等名 第45回量子情報技術研究会（QIT45）（招待講演）
4．発表年 2021年

１．発表者名
佐々木寿彦

２．発表標題
量子鍵配送の現状と理論的課題について

３．学会等名
第3回量子ソフトウェア研究発表会

４．発表年
2021年

１．発表者名
Toshihiko Sasaki

２．発表標題
Estimation protocol: its definition and usage in security proofs

３．学会等名
Security proofs in QKD Workshop（国際学会）

４．発表年
2020年

１．発表者名
佐々木寿彦

２．発表標題
量子鍵配送の安全性が証明できる状況について

３．学会等名
量子論の諸問題と今後の発展（招待講演）

４．発表年
2020年

１．発表者名
Toshihiko Sasaki

２．発表標題
Security proof of QKD as a combination of classical arguments: Based on the twin-field-type QKD

３．学会等名
Quantum computation, post-quantum cryptography and quantum codes（招待講演）

４．発表年
2019年

１．発表者名
Toshihiko Sasaki

２．発表標題
Rigorous calibration method for photon-number statistics

３．学会等名
CQIS2018（国際学会）

４．発表年
2018年

１．発表者名
Toshihiko Sasaki

２．発表標題
Feedforward attack in decoy-state quantum key distribution

３．学会等名
QCrypt2018（国際学会）

４．発表年
2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

量子暗号の到達距離を２倍に―新しい推定手法で盗聴監視の困難を解決―：物理工学専攻　小芦雅斗教授ら
https://www.t.u-tokyo.ac.jp/soe/press/setnws_20190718163151842396417 8.html

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関