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　３ 年　 ６ 月 １７ 日現在

機関番号：８２６３６
研究種目：基盤研究(B)（一般）
研究期間：2018～2020
課題番号：１８Ｈ０１１５７

研究課題名（和文）ブロードキャスト型量子鍵配送の研究

研究課題名（英文）Broadcast continuous variable quantum key distribution

研究代表者
武岡　正裕（Takeoka, Masahiro）

国立研究開発法人情報通信研究機構・未来ICT研究所量子ICT先端開発センター・センター長

研究者番号：７０４１５８５０

交付決定額（研究期間全体）：（直接経費）　　13,600,000円

研究成果の概要（和文）：１対多の多端子ネットワーク通信路であるブロードキャスト光通信路を使って配信された多者間の量子相関を積極的に活用し、１体１量子鍵配送（QKD）の組合せ（時分割多重）では不可能な鍵生成レートを実現する新しいQKD、「ブロードキャスト型QKD」を提案し、その基盤技術を確立、原理実証に向けた基礎データ取得を実現した。また、新しいネットワーク型量子暗号技術の理論及び実装法の開発に取り組み、盗聴者の攻撃能力を限定した場合の連続量量子鍵配送のレート向上に関する理論解析や、波長多重型連続量量子鍵配送の実装と原理実証などに成功した。

研究成果の学術的意義や社会的意義
ブロードキャスト型QKDは本研究グループ独自の理論に基づく方式であり、その実装にいち早く取り組み原理実証を行ったことは学術的に高い意義があると考える。また、本方式がベースとしている１対１の連続量量子鍵配送（CVQKD）方式そのものは、近い将来の実用化が期待されるQKD方式であるが、実用上重要となる光通信との波長多重化や、QKD自身の波長多重化の設計と原理実証に成功したことは社会的に高い意義があると考える。

研究成果の概要（英文）：We propose a novel network-type quantum key distribution (QKD) where one sender and multiple receivers are connected via a broadcast channel and the total key rate can be increased by collaborative operation among the sender and the receivers. We implement this “broadcast-QKD” in the lab and performed its proof-of-principle experiment. We also pursued more general framework and technologies for the network based QKD and related quantum security protocols. We derive key rate increases of the continuous variable QKD (CVQKD) under the limited attack by eavesdroppers and also develop and demonstrate the wavelength multiplexing of CVQKDs and ultrahigh-speed optical communication.

研究分野：量子情報理論、量子暗号

キーワード：連続量量子鍵配送　ブロードキャスト通信路　波長多重量子鍵配送

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

光の量子力学的性質を利用した暗号通信である量子鍵配送（Quantum Key Distribution: QKD）は、盗聴者の計算能力に依らない情報理論的安全性を保証し、かつ通信路への如何なる物理的盗聴攻撃からも安全な秘密鍵の共有を実現する技術として、基礎から応用まで広く研究が進んでいる。実用に向けて、複数拠点をつなぐ QKD のネットワーク化が各地で進められているが、いずれも、本質的には従来の 1 対 1 の QKD プロトコルを単純に組み合わせた運用（時分割多重など）に止まっており、ネットワークの利点を最大限活用しているとはいい難い状況であった。理論的にも、他者間（多体系）における秘密鍵や量子相関（エンタングルメント）の共有に関する研究は未だ基礎段階に止まっており、他者間の量子相関を積極的に活用した QKD プロトコルの提案は未だ存在してなかった。

２．研究の目的

本研究の目的は、１対多の多端子ネットワーク通信路であるブロードキャスト光通信路を使って配信された多者間の量子相関を積極的に活用し、１体１QKD の組合せ（時分割多重）では不可能な鍵生成レートを実現する新しい QKD、「ブロードキャスト型 QKD」を提案し、その基盤技術を確立することであった。研究代表者らの理論研究成果[1]を元に、研究分担者が開発を進めてきた連続量 QKD（CVQKD）技術を発展させた 1 送信機―2 受信機のブロードキャスト型 QKD を実装と、その原理実証を目的とした。また、ブロードキャスト型に限らない新しいネットワーク QKD について、新しい理論の構築や実装手法の開発に取り組み、従来の QKD ネットワークの単なる延長ではない、新しいネットワーク量子暗号の実現に向けた研究領域の開拓を目指した。

３．研究の方法

研究分担者により既に開発されていた１対１の CVQKD 送受信機[2]に加えて、新たに２台目の受信機を開発し、１対２のブロードキャスト CVQKD を構築しその原理実証を目指した。また、ネットワーク量子暗号分野の開拓を目指し、様々な角度からの理論研究・実装研究に取り組んだ。

４．研究成果

（１）ブロードキャスト型 CVQKD の原理実証に向けて、1 対の CVQKD 送受信機に加えて、2 台目の受信機の製作を行った。この 2 台目の受信機は、市販部品を用いて低コストに製作することを目指した。電圧信号の入出力には、ストリーム入出力が可能な ADC ボードと DAC ボードを用い、これらのボードを自作した制御用 PC に実装した。そして、市販の ADC・DAC ボードを用いて送受信者のデータ間の対応を実現する新しい手法を考案し、このプログラムを実装した。また、光源についても、最大出力が-6dBm 程度しかなく、3dB カプラーで 2 分岐した場合、２つの受信装置のホモダイン検出器のショット雑音とアンプ雑音の比が限られていた。そのため、約 10 倍の出力が可能な特注光源による送信機の再実装を行った。

上記の開発により実験系を構築し、最終年度に原理実証実験を試みた。原理実証実験では、2 ヶ所の測定を同期して実行するために、2 台の受信装置を高度に安定化する技術を開発する必要があったが、コロナ禍で実験の進行が困難になったため、ホモダイン検出器のみを 2 台用いる簡易版の実験系に切り替えて研究を進めた。新しい実験系では、光学系と制御 PC を共有することにより、実証に必要なデータをより安定して取得できるだけでなく、２つのホモダイン検出器の手前に 90 度光ハイブリッドを設置することにより、互いに位相が直交する２つの直交振幅を安定に測定することができる。この新しい実験系の構築し、多端子通信路と実質的に同じ構成でデータを取得、更に、信号光に CV-QKD と同じ４値の位相変調を行い、量子揺らぎの評価を行った。これらの成果の解析を進めることにより、ブロードキャスト型 CVQKD の初の原理実証実験成果につなげられると期待できる。

（２）新しいネットワーク量子暗号の理論的探索においては、量子ネットワークにおける多体の秘密鍵・エンタングルメント共有に関する原理的な性能限界を明らかにするための検討を進め、1 対 1 通信路から構成される任意の量子ネットワーク上における多体エンタングルメント（GHZ 状態）生成レートの一般的な下界を導出した[3]。特に光損失通信路など、LOCC 支援量子通信路容量が明らかになっている 1 対 1 通信路から構成される任意の量子ネットワークにおいては、これらは達成可能なレートの上界、すなわち量子通信路容量であると予想されるが、その証明にはまだ至っていない。また、ネットワーク型 CVQKD の発展として、連続量量子状態を用いた新しい量子セキュリティプロトコルへの応用の可能性として、3 者間のネットワークである量子フィンガープリントプロトコルの検討を行った。量子フィンガープリントでは、2 つの連続量量子状態の同一性を高精度で比較する量子測定

が必要となる。その基礎理論として、このような量子測定をガウス操作のみで構成した場合の理論限界と、それを超える量子受信機の具体的な設計を明らかにし、その有用性を数値的に示した[4]。本成果はまだ量子測定の基礎に関するものであるが、今後の新しいネットワーク量子通信プロトコルへの展開が期待される。

一方、近年の CVQKD の急速な実用化への動きを受け、現実のネットワークにける CVQKD の新しい実装法についても研究チーム全体で検討を進めた。将来的な量子暗号の既存ネットワークへの適用を想定し、CVQKD と大容量光通信の１つのファイバー中での波長多重伝送実験を行った。QKD チャンネルへの背景光をノッチフィルター等により適切に除去することにより、18.3Tbps の超大容量光通信と CVQKD の同時伝送実験に成功した[5]。また、CVQKD そのものの波長多重化にも取り組み、194 波長の CVQKD を同時伝送できることの原理実証実験に成功した[6]。その他、波長多重における QKD のクロストークの影響[7], 盗聴者の攻撃が限定されると仮定した場合の新しいスキームの検討などを行った[8], [9]。

これらの成果は、CVQKD をベースとした今後のネットワーク型量子暗号・量子通信技術の発展に向けた重要な基礎理論・実装要素技術となることが期待される。

[1] M. Takeoka, K. P. Seshadreesan, and M. M. Wilde, “Unconstrained capacities of quantum key distribution and entanglement distillation in a pure-loss bosonic broadcast channel”, Phys. Rev. Lett. 119, 150501 (2017).

[2] T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, and T. Tsurumaru, “Implementation of continuous-variable quantum key distribution with dicrete modulation”, Quantum Sci. Technol. 2, 024010 (2017).

[3] E. Kaur, M. Takeoka, M. M. Wilde, and W. Roga, “Multipartite entanglement and secret key distribution in quantum networks”, 22nd Annual Southwest Quantum Information and Technology Workshop (SQuinT), Eugene, Oregon, USA, February 8-10, 2020.

[4] D. E. Roberson, S. Izumi, W. Roga, J. S. Neergaard-Nielsen, M. Takeoka, U. L. Andersen, “Limit of Gaussian operations and measurements for Gaussian state discrimination and its application to state comparison”, Phys. Rev. A 103, 022423 (2021).

[5] T. A. Eriksson, T. Hirano, B. J. Puttnam, G. Rademacher, R. S. Luis, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. W. and M. Sasaki, “Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels”, Commun. Phys. 2, 9 (2019).

[6] T. A. Eriksson, R. S. Luis, B. J. Puttnam, G. Rademacher, M. Fujiwara, Y. Awaji, H. Furukawa, N. Wada, M. Takeoka, and M. Sasaki, “Wavelength division multiplexing of 194 continuous variable quantum key distribution channels”, J. Light. Technol. 38, 2214 (2020).

[7] T. A. Eriksson, B. J. Puttnam, G. Rademacher, R. S. Luis, M. Fujiwara, M. Takeoka, Y. Awaji, M. Sasaki, and N. Wada, “Crosstalk impact on continuous variable quantum key distribution in multicore fiber transmission”, IEEE Photon. Technol. Lett., 31, 467 (2019).

[8] T. A. Eriksson, P. V. Trinh, H. Endo, M. Takeoka, and M. Sasaki, “Secret key rates for intensity-modulated dual-threshold detection key distribution under individual beam splitting attacks”, Opt. Express 26, 20409 (2018).

[9] R. Namiki, A. Kitagawa, and T. Hirano, “Secret key rate of a continuous-variable quantum-key-distribution scheme when the detection process is inaccessible to eavesdroppers”, Phys. Rev. A 98, 042319 (2018).

５．主な発表論文等

〔雑誌論文〕　計6件（うち査読付論文　4件／うち国際共著　1件／うちオープンアクセス　2件）

１．著者名 Eriksson Tobias A.、Puttnam Benjamin J.、Rademacher Georg、Luis Ruben S.、Fujiwara Mikio、Takeoka Masahiro、Awaji Yoshinari、Sasaki Masahide、Wada Naoya	４．巻 31
２．論文標題 Crosstalk Impact on Continuous Variable Quantum Key Distribution in Multicore Fiber Transmission	５．発行年 2019年
３．雑誌名 IEEE Photonics Technology Letters	６．最初と最後の頁 467～470
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/LPT.2019.2898458	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 Eriksson Tobias A.、Hirano Takuya、Puttnam Benjamin J.、Rademacher Georg、Lu?s Ruben S.、Fujiwara Mikio、Namiki Ryo、Awaji Yoshinari、Takeoka Masahiro、Wada Naoya、Sasaki Masahide	４．巻 2
２．論文標題 Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels	５．発行年 2019年
３．雑誌名 Communications Physics	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1038/s42005-018-0105-5	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 Eriksson Tobias A.、Trinh Phuc V.、Endo Hiroyuki、Takeoka Masahiro、Sasaki Masahide	４．巻 26
２．論文標題 Secret key rates for intensity-modulated dual-threshold detection key distribution under individual beam splitting attacks	５．発行年 2018年
３．雑誌名 Optics Express	６．最初と最後の頁 20409～20419
掲載論文のDOI（デジタルオブジェクト識別子） 10.1364/OE.26.020409	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 Namiki Ryo、Kitagawa Akira、Hirano Takuya	４．巻 98
２．論文標題 Secret key rate of a continuous-variable quantum-key-distribution scheme when the detection process is inaccessible to eavesdroppers	５．発行年 2018年
３．雑誌名 Physical Review A	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevA.98.042319	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 Eriksson Tobias A.、Luis Ruben S.、Puttnam Benjamin J.、Rademacher Georg、Fujiwara Mikio、Awaji Yoshinari、Furukawa Hideaki、Wada Naoya、Takeoka Masahiro、Sasaki Masahide	4．巻 38
2．論文標題 Wavelength Division Multiplexing of 194 Continuous Variable Quantum Key Distribution Channels	5．発行年 2020年
3．雑誌名 Journal of Lightwave Technology	6．最初と最後の頁 2214～2218
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JLT.2020.2970179	査読の有無 無
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 Roberson David E.、Izumi Shuro、Roga Wojciech、Neergaard-Nielsen Jonas S.、Takeoka Masahiro、Andersen Ulrik L.	4．巻 103
2．論文標題 Limit of Gaussian operations and measurements for Gaussian state discrimination and its application to state comparison	5．発行年 2021年
3．雑誌名 Physical Review A	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevA.103.022423	査読の有無 無
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 該当する

〔学会発表〕　計11件（うち招待講演　1件／うち国際学会　7件）

1．発表者名 Tobias Eriksson, Takuya Hirano, Benjamin Puttnam, Georg Rademacher, Ruben Luis, Mikio Fujiwara, Ryo Namiki, Yoshinari Awaji, Masahiro Takeoka, Naoya Wada and Masahide Sasaki
2．発表標題 Continuous variable quantum key distribution multiplexed with high throughput coherent channels
3．学会等名 9th International Conference on Quantum Cryptography (QCrypt 2019)（国際学会）
4．発表年 2019年

1．発表者名 Takuya Hirano and Ryo Namiki
2．発表標題 Continuous operation of four-states continuous-variable quantum key distribution system
3．学会等名 日米欧量子科学技術国際シンポジウム（国際学会）
4．発表年 2019年

１．発表者名
Eneet Kaur, Masahiro Takeoka, Mark M. Wilde, and Wojciech Roga

２．発表標題
Multipartite entanglement and secret key distribution in quantum networks

３．学会等名
22nd Annual Southwest Quantum Information and Technology Workshop (SQuinT)（国際学会）

４．発表年
2020年

１．発表者名
武岡 正裕

２．発表標題
量子ネットワークの量子通信路容量について

３．学会等名
電子情報通信学会2020年総合大会（招待講演）

４．発表年
2020年

１．発表者名
Tobias Eriksson, Takuya Hirano, Motoharu Ono, Mikio Fujiwara, Ryo Namiki, Ken-ichiro Yoshino, Akio Tajima, Masahiro Takeoka and Masahide Sasaki,

２．発表標題
Coexistence of Continuous Variable Quantum Key Distribution and 7 × 12.5 Gbit/s Classical Channels

３．学会等名
IEEE Summer Topicals Meeting Series（国際学会）

４．発表年
2018年

１．発表者名
Ami Shinjjo, Yujiro Eto,and Takuya Hirano

２．発表標題
Time-Domain Measurement of Continuous-Variable Entanglement Using Temporally Shaped Local Oscillator Pulses

３．学会等名
IEEE Summer Topicals Meeting Series（国際学会）

４．発表年
2018年

１．発表者名
Tobias Eriksson, Takuya Hirano, Georg Rademacher, Benjamin Puttnam, Ruben Luis, Mikio Fujiwara, Ryo Namiki, Ken-Ichiro Yoshino, Akio Tajima, Yoshinari Awaji, Masahiro Takeoka, Naoya Wada and Masahide Sasaki

２．発表標題
Continuous Variable Quantum Key Distribution Multiplexed with Classical Channels

３．学会等名
8th International Conference on Quantum Cryptography（国際学会）

４．発表年
2018年

１．発表者名
Tobias A. Eriksson, Takuya Hirano, Georg Rademacher, Benjamin J. Puttnam, Ruben S. Luis, Mikio Fujiwara, Ryo Namiki, Yoshinari Awaji, Masahiro Takeoka, Naoya Wada and Masahide Sasaki

２．発表標題
Joint Propagation of Continuous Variable Quantum Key Distribution and18×24.5Gbaud PM-16QAM Channels

３．学会等名
2018 European Conference on Optical Communication (ECOC)（国際学会）

４．発表年
2018年

１．発表者名
新城亜美，片山拓哉，衞藤雄二郎，平野琢也

２．発表標題
時間幅の短い局部発振光を用いたパルス光連続変数エンタングルメントの時間領域測定II

３．学会等名
日本物理学会 2018年 秋季大会

４．発表年
2018年

１．発表者名
Ami Shinjo、Takuya Katayama、Yujiro Eto、Takuya Hirano

２．発表標題
Pulse-resolved measurement of continuous-variable EPR entanglement with shaped local oscillators

３．学会等名
第79回 応用物理学会 秋季学術講演会

４．発表年
2018年

１．発表者名 新城 亜美，片山 拓哉，衛藤 雄二郎，平野 琢也
２．発表標題 波形整形した局部発振光を用いたパルス光連続変数エンタングルメントの時間領域測定
３．学会等名 第66回応用物理学会 春季学術講演会
４．発表年 2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

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
研究分担者	平野　琢也 (Hirano Takuya) (00251330)	学習院大学・理学部・教授 (32606)	

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			
米国	ルイジアナ州立大学			
デンマーク	デンマーク工科大学			