公開

研 究 終 了 報 告 書

「量子インターネットの理論的研究」

研究期間: 2018 年 10 月～2022 年 3 月
研 究 者: 東 浩司

1. 研究のねらい

インターネット上で、送信者が送信するデータは、情報処理ノードと通信路で構成されるネットワークを経由して受信者に届けられる。現在のインターネットにおけるノードと通信路は、ビットを処理する目的で構築された「古典」的なものであり、その機能や限界は従来の情報理論の範疇にある。だが、将来的には、それらのノードや通信路の構成は「量子技術」に切り替えられるはずで、量子情報理論によってはじめて記述される「量子インターネット」が、物理法則の下で許される通信ネットワークの究極像である。実際，量子インターネットは、地球上の任意のクライアント間での量子通信を可能にするだけでなく、量子コンピュータや量子計測、さらには量子多体系のシミュレーションまでをも包含する一般的パラダイムであり、その構築は分野の長期的課題であり、究極的挑戦といえる。

そこで本研究では、量子インターネットのための基礎理論の構築を目指す。具体的には、

1) 量子インターネットプロトコルの原理限界の追及
2) 実用的な量子インターネットプロトコルの提案
3) 量子インターネットの新応用の探求

の 3 課題を主な研究テーマとする。

1)の研究課題では、量子ネットワークを構成するノードや通信路の物理的性質から決まる量子インターネットの「通信容量」を定義、導出することにより、量子ネットワークのハードとしての潜在能力を明らかにする。2)の研究課題では、1)の研究で明らかにされる通信容量と遜色のない効率を持ち得るプロトコルを、実用的デバイスに基づき構成することを目指す。また、2)において得られた知見に基づき、現状で手に入るデバイスを用いて実装しても意義ある通信プロトコルの提案、あるいは将来の量子インターネットの構築に不可欠で、近い将来に実現すべき通信プロトコルの提案に繋げる。3)の研究目的は、量子インターネットの新応用を探ることである。そのような新しい応用の発見は、量子インターネット構築の価値を高めるだけでなく、応用に適した量子インターネットプロトコルの提案に繋がる。

本研究では以上の 3 課題を有機的に進めることにより、量子インターネット理論の完成を目指す。量子インターネットのようなビッグパラダイムの全体像を明らかにし、量子インターネット構築に必要な要素技術を浮き彫りにし、それによって分野の技術発展に正しい道筋をあたえることが本研究の主な狙いである。

2. 研究成果

（1）概要

与えられた量子ネットワーク上で、量子通信路の使用回数あたり、クライアントに提供でき

る最大量子もつれや秘密鍵のサイズの最大値は、それぞれ量子通信容量、秘匿通信容量と呼ばれ、学術的にも実用的にも最も基本的な量として知られる。これまでに、ベル状態／秘密鍵の分配、GHZ 状態／多者間秘密鍵の分配に関するこれら容量に対する上界と下界が導出されてきた。本さきがけ研究ではこれら上界と下界を、線形計画法に基づき、迅速に計算する手法を与えた[Stefan Bäuml, Koji Azuma, Go Kato & David Elkouss, Linear programs for entanglement and key distribution in the quantum internet, Communications Physics **3**, 55 (2020)]。この手法は、使用状況が時々刻々と変わる量子ネットワーク上のクライアントに量子もつれを、効率的かつ迅速に供給するための量子版 IP プロトコルの開発の基礎となり得る。本成果は、既存の一連の研究とともに、総説に含められた[代表的な論文 1]。

また、量子インターネットを実現するには、長距離量子通信を可能にする量子中継が必要であり、その前段階として、まずは現在のポイント・ツー・ポイントの損失ボゾン通信路の量子／秘匿通信容量を超えるプロトコルを実現する必要がある。本さきがけ研究では、そのような限界を打破すると期待される全光都市間量子鍵配送(QKD)方式に注目し、その中継ノードに必要とされる量子もつれ光源に課される条件を明らかにした[Róbert Trényi, Koji Azuma, and Marcos Curty, Beating the repeaterless bound with adaptive measurement-device-independent quantum key distribution, New J. Phys. **21**, 113052 (2019)]。また、別の候補であるツイン・フィールド QKD 方式にも注目し、実装がより簡潔な、新しいツイン・フィールド QKD 方式の提案を行うとともに、その方式に対する安全性証明を与えた[代表的な論文 2]。この簡単化された本方式の秘密鍵生成レートは、元の提案より少なくとも 10 倍以上高く、また安全性証明も極めて簡潔なものとなっている。さらに、その方式の安全性の有限長解析を行い、結果として、現実的な鍵長に対しても、その方式が、ポイント・ツー・ポイント秘匿通信容量を超えるパフォーマンスを持つことを明らかにした[Guillermo Currás Lorenzo, Álvaro Navarrete, Koji Azuma, Go Kato, Marcos Curty, and Mohsen Razavi, Tight finite-key security for twin-field quantum key distribution, npj Quantum Information **7**, 22 (2021)]。

量子インターネットという概念の新応用を探る一環として、量子インターネットプロトコルの理論限界を用いて、ブラックホールに対するベッケンシュタイン・ホーキングの面積則を理解することを試みていた。この取り組みの中で明らかとなったのは、ベッケンシュタイン・ホーキングの面積則、ブラックホールの第一法則、ホーキング放射の微視的描像、量子力学のユニタリー性の間に生じる矛盾の存在だった。本さきがけ研究では、この矛盾を、既存のアプローチでは通常捨て去られる「ホーキング放射の微視的描像」を維持したまま解決する方法として、ベッケンシュタイン・ホーキングの面積則中のエントロピーを、量子もつれ量を表すコヒーレント情報に置き換えることを提案した。さらに、この修正されたブラックホールの面積則と、量子熱力学の定式化を組み合わせることで、ブラックホールに対する熱力学第 2 法則の導出を行った[代表的な論文 3]。

（2）詳細

さきがけ期間中の研究を含む、私のここ 10 年の研究の位置づけを図 1 でまとめた。

最初に、課題 1)と 2)に関わる研究成果を報告する。量子インターネットプロトコルの主な役割は、量子ネットワーク上に存在するクライアントに対し、量子通信のリソースである量子

もつれを効率的に提供することにある。なかでも与えられた量子ネットワーク上で、量子通信路の使用回数あたり、クライアントに提供できる最大量子もつれや秘密鍵のサイズの最大値は、それぞれ量子通信容量、秘匿通信容量と呼ばれ、学術的にも実用的にも最も基本的な量として知られる。さきがけ開始以前に、ベル状態／秘密鍵の分配、GHZ 状態／多者間秘密鍵の分配に関するこれら容量に対する上界と下界が導出されてきた[1-6]。特に、光ファイバネットワークのような損失ボゾン通信路で構成された量子ネットワーク（より厳密には蒸留可能通信路で構成された量子ネットワーク）上での 2 者間量子／秘匿通信の場合には、これらの上界と下界は一致し、量子／秘匿通信容量を与える[2,5]。しかし、実用上大事なことは、量子ネットワークの使用状況が時々刻々と変わる中、クライアントからの要求に応じ、必要とされる量子もつれを効率的かつ迅速に供給することである。そのためには、与えられた量子ネットワークに応じ、素早く量子／秘匿通信容量の上界と下界を考慮に入れ、使用するプロトコルやルーティング法を決定することが大事になる。

本さきがけ研究を通じ、ベル状態／秘密鍵の分配、GHZ 状態／多者間秘密鍵の分配に関して導出されてきた一連の量子／秘匿通信容量の上界と下界を、線形計画法に基づき、迅速に計算するための手法を与えた[Stefan Bäuml, Koji Azuma, Go Kato & David Elkouss, Linear programs for entanglement and key distribution in the quantum internet, Communications Physics **3**, 55 (2020)]。これは、既存の上界と下界の実用的価値を高めるだけでなく、量子版IPプロトコル構築への足掛かりとなる。実際、この成果がきっかけとなり、AVS Quantum Science 誌から、本成果だけでなく（[1-6]などを含む）量子インターネット構築の基礎となるツールを集めた総説論文の執筆が依頼され、27 ページに及ぶ総説論文の出版に至った[代表的な論文 1]。

次に、課題 2)に関する研究成果を報告する。量子インターネットを実現するには、長距離量子通信を可能にする量子中継が必要であり、その前段階として、まずは現在のポイント・ツー・ポイントの損失ボゾン通信路の量子／秘匿通信容量を超えるプロトコルを実現する必要がある。この容量を超える可能性を持つ方式として近年注目を浴びているのは、送受信者間に設置された一つのノードのみを利用する全光都市間量子鍵配送(QKD)方式[7]や、ツイン・フィールド QKD 方式[8]である。

本さきがけ研究では、全光都市間量子鍵配送方式の中継ノードに必要とされる量子もつれ光源に課される条件を明らかにした[Róbert Trényi, Koji Azuma, and Marcos Curty, Beating the repeaterless bound with adaptive measurement-device-independent quantum key distribution, New J. Phys. **21**, 113052 (2019)]。この条件により、全光都市間量子鍵配送方式は、量子もつれ光源として、現実的なパラメトリック下方変換を利用した場合に、ポイント・ツー・ポイント量子通信の理論限界を超えられないことがわかり、理論限界の超越には、より効率的で忠実な量子もつれ光源を必要とすることが明らかになった。

本さきがけ期間中に、QKD 分野で一大ブームとなったツイン・フィールド QKD 方式[8]に関する研究も行った。具体的には、実装がより簡潔なツイン・フィールド QKD 方式の提案を行うとともに、その方式に対する安全性証明を与えた[代表的な論文 2]。この簡単化された本方式の秘密鍵生成レートは、元々の提案のものより少なくとも 10 倍以上高く、さらに元の提案

の安全性証明[9,10]に比べ、本方式に対する安全性証明は極めて簡潔なものとなっている。事実、本方式は、その実装の簡潔さと効率性から、様々なチームのツイン・フィールド QKD 方式の原理検証実験で採用されている[11-15]。さらに、その方式の安全性の有限長解析を行い、結果として、現実の実装上理にかなった鍵長に対しても、その方式が、ポイント・ツー・ポイント秘匿通信容量を超えるパフォーマンスをもつことが明らかになった[Guillermo Currás Lorenzo, Álvaro Navarrete, Koji Azuma, Go Kato, Marcos Curty, and Mohsen Razavi, Tight finite-key security for twin-field quantum key distribution, npj Quantum Information **7**, 22 (2021)]。加えて、ツイン・フィールド QKD 方式を中心とした QKD の最新動向についての総説を Physics Today 誌から依頼され、執筆し、出版に至った[Marcos Curty, Koji Azuma, and Hoi-Kwong Lo, A quantum leap in security, Physics Today **74**, 3, 36 (2021)]。

次に課題 3)に関する研究成果を報告する。課題 3)では、量子インターネットという概念の新応用を探っている。その一環として、本さきがけ研究開始前から始めているものとして、量子インターネットプロトコルの理論限界を用いて、ブラックホールの面積則を理解する試みがある。しかし、この取り組みを進める中で明らかになったのは、ブラックホールの面積則として知られるベッケンシュタイン・ホーキング方程式と、一般相対論の枠組みで現れるブラックホールの第一法則、ホーキング放射の微視的描像、量子力学のユニタリー性の間の矛盾の存在だった。そこで、この矛盾を、既存のアプローチでは通常捨て去られる「ホーキング放射の微視的描像」を維持したまま解決する方法として、ベッケンシュタイン・ホーキング方程式中のエントロピーを、量子もつれ量を表すコヒーレント情報に置き換えることを提案していた[16]。

本さきがけ期間中、私たちはこの修正されたブラックホールの面積則と、量子熱力学の定式化を組み合わせることで、ブラックホールに対する熱力学第 2 法則の導出を行った[17]。この法則の妥当性は、イベントホライゾンテレスコープなどを利用することにより、熱浴中のブラックホールが見つかるたびに、実験により検証できる。もし、私たちの第 2 法則が十分にチェックされ、私たちが提案する面積則の正当性が認められれば、自然法則を記述する基礎方程式の中に、初めて量子情報理論特有の量(コヒーレント情報)が登場することになる。結果として、量子情報理論の言語としての価値を高めるだけでなく、量子ネットワークに関して量子情報分野で得られた知見から直接的に、ブラックホール物理が理解できる可能性がある。現在、[16]と[17]の論文は組み合わされ、1 本の論文として査読を受けている[代表的な論文 3]。

最後に本さきがけの取り組み全般についてまとめた記事を、Delft 工科大学の The VvTP (Vereniging voor Technische Physica)の依頼に応じて執筆し[Koji Azuma, Journey towards the quantum internet, De Physicus, January 2019, 52-54 (edited by Maia Rigot)]、応用物理学会フォトニクス分科会が出版するフォトニクスニュース誌からの依頼に応じて執筆した[東浩司, 量子インターネットに向けて, フォトニクスニュース, 第 6 巻, 第 3 号, 91-96 (2020)]。また、本さきがけの対象を超え、量子中継や最近の分野の技術進展も含む総説論文をアメリカ物理学会の Reviews of Modern Physics(RMP)へ提出している。

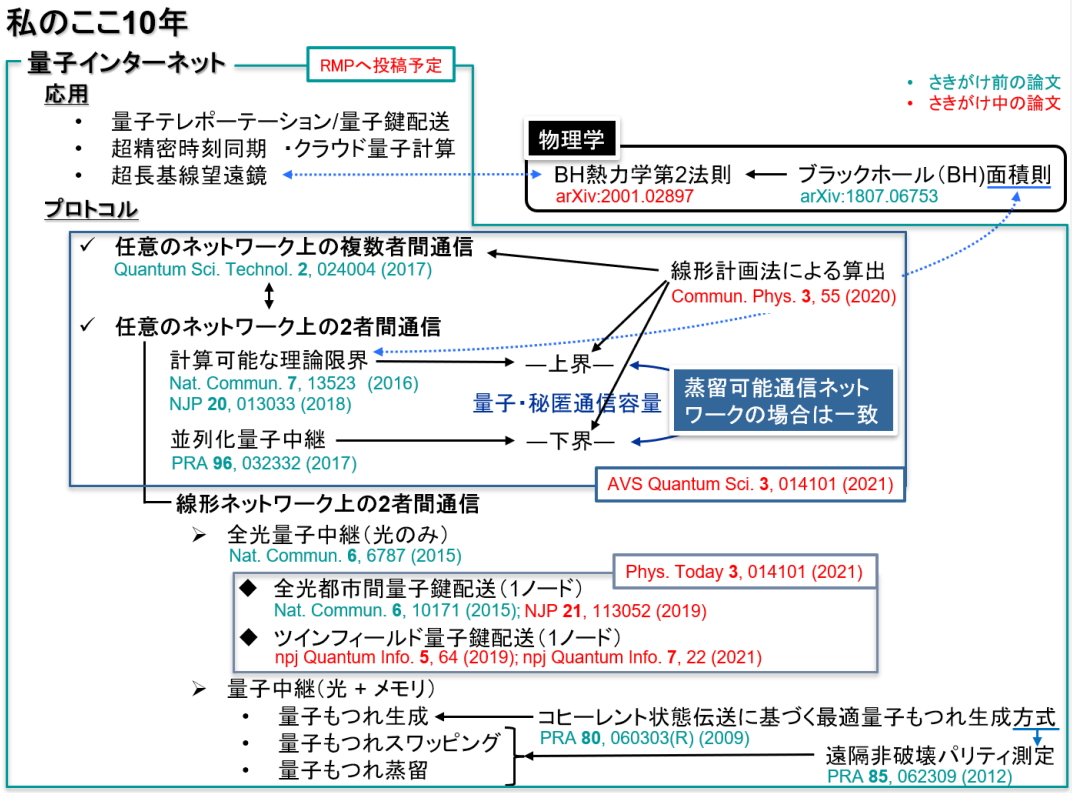

図 1:さきがけ研究を含む、私のここ 10 年の研究

参考文献

[1] Azuma, K., Mizutani, A. & Lo, H.-K. Fundamental rate-loss tradeoff for the quantum internet. Nat. Commun. **7**, 13523 (2016).

[2] Azuma, K. & Kato, G. Aggregating quantum repeaters for the quantum internet. Phys. Rev. A **96**, 032332 (2017).

[3] Bäuml, S. & Azuma, K. Fundamental limitation on quantum broadcast networks. Quantum Sci. Technol. **2**, 024004 (2017).

[4] Rigovacca, L. *et al.* Versatile relative entropy bounds for quantum networks. New J. Phys. **20**, 013033 (2018).

[5] Pirandola, S. End-to-end capacities of a quantum communication network. Commun. Phys. **2**, 51 (2019).

[6] Pirandola, S. Bounds for multi-end communication over quantum networks. Quantum Sci. Technol. **4**, 045006 (2019).

[7] Azuma, K., Tamaki, K. & Munro, W. J. All-photonic intercity quantum key distribution. Nat. Commun. **6**, 10171 (2015).

[8] Lucamarini, M. *et al.* Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature **557**, 400–403 (2018).
[9] Tamaki, K. *et al.* Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. Preprint at http://arxiv.org/abs/1805.05511.
[10] Ma, X., Zeng, P. & Zhou, H. Phase–matching quantum key distribution. Phys. Rev. X **8**, 031043 (2018).
[11] Minder, M. *et al.* Experimental quantum key distribution beyond the repeaterless secret key capacity. Nat. Photon. **13**, 334–338 (2019).
[12] Wang, S. *et al.* Beating the fundamental rate–distance limit in a proof–of–principle quantum key distribution system. Phys. Rev. X **9**, 021046 (2019).
[13] Zhong, X., Hu, J., Curty, M., Qian, L. & Lo, H.–K. Proof–of–principle experimental demonstration of twin–field type quantum key distribution. Phys. Rev. Lett. **123**, 100506 (2019).
[14] Pittaluga, M. *et al.* 600–km repeater–like quantum communications with dual–band stabilization. Nat. Photon. **15**, 530–535 (2021).
[15] Clivati, C. *et al.* Coherent phase transfer for real–world twin–field quantum key distribution. Nat. Commun. **13**, 157 (2022).
[16] Azuma, K & Subramanian, S. Do black holes store negative entropy? Preprint at https://arxiv.org/abs/1807.06753.
[17] Azuma, K & Kato, G. Second law of black hole thermodynamics. Preprint at https://arxiv.org/abs/2001.02897.

3. 今後の展開

ここ 5, 6 年で量子ネットワークの潜在能力について基本的な理解が得られてきた。特に、量子ネットワーク、ひいては量子インターネット構築において、量子中継が基礎となることも明らかにされてきた。このような最近の著しい理論的進展から、学術業界では量子ネットワーク、量子インターネットに関する総説論文が出版される段階にまできている。ここでは、次の 10 年に量子インターネット構築に必要とされる今後の展開について述べる。

まず、近年技術的進展が著しい量子コンピュータと、量子インターネットの本質的な違いである「計算」と「通信」について言及する。計算機は元来、それ単独で機能が閉じている。そのため独自の規格で開発・発展が可能で、製造や販売までをも単独で行える。従って、技術レベルがある程度伴ってくれば、学術業界だけではなく、企業でも研究が始まり、製品化に向け発展が加速する。これが現在量子コンピュータについて起きていることである。他方で、通信は元来、万人に使われることで機能性が充実し、本当に意味のあるものとなる。言い換えれば、通信はあくまでインフラであるため、拡張可能なグランドデザインに基づき、協調して国家レベルで構築・拡大していく必要がある。これについては、量子通信ネットワークについても同様である。

実際、世界に目を向けてみると、例えば中国は、量子中継を使用するまでには至っていな

いが、人工衛星を加えることで量子鍵配送ネットワークを拡大している[Y.-A. Chen *et al.*, Nature **589**, 214 (2021)]。米国においても、エネルギー省が量子インターネット研究に対し、次の5年に625百万ドル規模の予算計上の可能性がある[Report of the DOE Quantum Internet Blueprint Workshop <https://www.osti.gov/servlets/purl/1638794>]。欧米においては、デルフト工科大を中心とした「Quantum internet alliance」でプロジェクトが進行中である[https://quantum-internet.team/]。つまり、量子通信ネットワークの構築に向け、国家レベルでの取り組みが実際に数多くみられる。

一方で日本はどうだろうか。残念ながら、現在では量子インターネットを主とするプロジェクトはまだない。Q-LEAP は量子コンピュータと量子シミュレータであり、ムーンショット目標 6 は誤り耐性型汎用量子コンピュータ、総務省の「グローバル量子暗号通信網構築のための研究開発」についてはポイント・ツー・ポイントの量子鍵配送の研究がメインで、量子中継などの研究開発はサブであるという印象は拭えない。従って、今後、欧米と中国に対抗し、量子インターネット開発において先取特権をとり、その研究開発を先導していくためには、国家レベルで量子インターネットの構築に向けて取り組む必要がある。

一方で今後学術的に行っていく必要があるのは、拡張可能なグランドデザインの構築である。このグラインドデザインの構築には、物理レイヤだけではなく、ミドルウェア、ソフトウェアのデザインについても明確化していく必要があり、今後はこのような研究が大事になっていくと予想される。

4. 自己評価

研究目的として非常に広範な課題 1)-3)を掲げたにも拘らず、その課題に対応する研究成果を挙げられてきたことには満足している。特に課題 1)と 2)の研究については複数の有名ジャーナルから総説を依頼されるレベルになった。これは、私たちが行ってきた一連の研究の完成度や、分野の量子ネットワークへの理解が一定レベルに達したこと、また学術業界において研究の重要性の認知度が上がってきたことを示唆していると思われる。研究の進め方について、当初の予定よりも遅れてしまったのが課題 3)である。これは、私たちのブラックホールに関する主張が、既存分野の定説に従わず、全く新しいものであるがために、なかなか出版に至れないのが原因である。だが、その研究内容が持つインパクトの大きさを考えると致し方ないのかもしれない。

課題 1)と 2)については、それと関連するムーンショット目標 6 のプロジェクト「誤り耐性型量子コンピュータにおける理論・ソフトウェアの研究開発」(PM:東大 小芦雅斗)における「分散型構造を持つ誤り耐性型量子コンピュータの研究開発」の課題推進者として、発展させていく。課題 3)については、令和 3 年度から始まった学術変革領域(A)研究課題「極限宇宙の物理法則を創る－量子情報で拓く時空と物質の新しいパラダイム」(領域代表:京大 高柳匡)の研究分担者として、継続し、発展させていく。さきがけ研究者、あるいは理論研究者として蒔いてきた種を、これらチーム型研究プロジェクトへの参加を通じ、育てていく機会が与えられていることに感謝したい。

5. 主な研究成果リスト

(1)代表的な論文(原著論文)発表

研究期間累積件数：8件（総説4件含む）

1. Koji Azuma, Stefan Bäuml, Tim Coopmans, David Elkouss, and Boxi Li. Tools for quantum network design. AVS Quantum Science **3**, 014101 (2021).
量子ネットワークは、現在の通信ネットワークとは質的に異なる通信タスクを可能にする。小規模の量子ネットワークは近い将来に実現すると見込まれるが、それらを拡大していくためには多くの課題が残されている。様々な解決策を比較し、パラメータ空間における最適化を行い、実験家と情報を共有するには、具体的な量子ネットワークシナリオのパフォーマンスを評価することが必要である。本論文では、そのような評価に関する最新の理論ツールを総説する。
2. Marcos Curty, Koji Azuma, and Hoi-Kwong Lo. Simple security proof of twin-field type quantum key distribution protocol. npj Quantum Information **5**, 64 (2019).
ツイン・フィールド量子鍵配送（TF QKD）は、送受信者間に設置された測定器における単一光子干渉を利用することによって、ポイント・ツー・ポイント QKD の秘匿通信容量を凌駕するパフォーマンスを持つと予想された。本論文では、元の提案より概念的に簡潔な TF QKD プロトコルを導入する。これにより、安全性が簡潔に証明されるだけでなく、実装も単純化された。また、本方式の鍵配送レートは、当初予想された通り、ポイント・ツー・ポイント QKD の秘匿通信容量を超える。
3. Koji Azuma, Sathyawageeswar Subramanian, and Go Kato. Do black holes store negative entropy? 投稿中（arXiv:1807.06753, arXiv:2001.02897）
ホーキング放射の微視的描像は、正と負のエネルギーを持つ粒子の対生成に基づき、ブラックホールの第一法則、Bekenstein の主張、量子力学のユニタリ性の間で矛盾を引き起こす。本論文では、量子情報理論の観点から、ベッケンシュタイン・ホーキングの面積則の代わりとなる面積則を提案することで、ホーキング放射の微視的描像を変更することなしに、この矛盾を解決する。また、この新たな面積則から熱浴中にあるブラックホールに対する熱力学第 2 法則を導出する。

（2）特許出願

特許出願なし。

（3）その他の成果（主要な学会発表、受賞、著作物、プレスリリース等）

1. 東　浩司, V. Bastidas, Y. Zhang, and W. J. Munro, 量子情報処理を飛躍的に発展させる量子通信・量子シミュレーション理論の提案と実証, 2019 年度　NTT 先端技術総合研究所長表彰（研究開発賞）, 2019 年 12 月 11 日.