3版

様　式　C－１９、F－１９－１、Z－１９　（共通）

科研費 KAKENHI

科学研究費助成事業　　研究成果報告書

令和　元 年　　６ 月 １２ 日現在

機関番号：３２６１２
研究種目：基盤研究(B)（一般）
研究期間：2016～2018
課題番号：１６H０２８１２

研究課題名（和文）Quantum Sockets: Programming Quantum Repeater Network Testbeds

研究課題名（英文）Quantum Sockets: Programming Quantum Repeater Network Testbeds

研究代表者
Ｖａｎ・Ｍｅｔｅｒ　Ｒｏｄｎｅｙ（VAN METER, Rodney）

慶應義塾大学・環境情報学部（藤沢）・准教授

研究者番号：９０４５８９７７

交付決定額（研究期間全体）：（直接経費）　　11,600,000円

研究成果の概要（和文）：量子インターネットのエンジニアリングを推進した。Fowlerの通信アーキテクチャはsurface code誤り訂正をもとに設計される。まず最初に、我々はデバイスの欠陥からくるsurface codeの誤り耐性を向上し、資源消費の効率化を促す改善案を提案した。また、ネットワーク間での量子通信を可能とするルールベースの通信制御プロトコルを開発し、それをもとに、異なる品質のデバイスからなる量子インターネット上でより堅牢な接続を確立するために必要となる分散型量子トモグラフィプロトコルを考案した。
考案したプロトコルの評価を行うため、新しいシミュレータを開発し、性能の分析を行った。

研究成果の学術的意義や社会的意義
量子インターネットは古典通信に用いられる暗号技術に寄与することが、もっとも大きい社会的意義として挙げられる。量子コンピュータ間の接続や、高精度分散量子センサーネットワークの構築の実現可能性は日々高まっている。考案する新しいアルゴリズムや量子インターネットプロトコルは、今回開発したシミュレータの上で性能の検証を行うことができる。
よって、今後実世界でデプロイしていくプロトコルの検証を前もって行えるため、その信頼性を高めることが可能である。

研究成果の概要（英文）：We advanced the engineering of the Quantum Internet. Fowler's architecture for integrating error correction with communication depends on the surface code, while Jiang's depends on older error correction methods; we improved the tolerance of the surface code for physical defects and reduced its resource demands. We devised methods for creating entangled states that span nodes and networks using different encoding methods. One of the principal realities of quantum communication is the high error rates and heterogeneity across individual devices; we developed distributed quantum tomography protocols to support the establishment of connections across networks. Most importantly, we have created a RuleSet-based communication architecture that the nodes establishing a connection across the Quantum Internet will use to define the behavior of all nodes along the path, providing an easy-to-understand, easy-to-debug protocol framework for both applications and network routers and repeaters.

研究分野：量子インターネット

キーワード：量子中継器　量子分散アルゴリズム　量子通信

１．研究開始当初の背景

At the time we began this project, several repeater architectures had been defined: first-generation purify-and-swap repeaters; second-generation quantum error correction-based repeaters using CSS codes (Jiang) or surface code (Fowler); and third-generation direct-propagate repeaters. Nothing was known about how to interoperate between the different types of networks; that is, no *internetworking* architecture and technology existed. Only a few algorithms had been evaluated for the demands they place on a quantum repeater network: quantum key distribution, one application using blind quantum computation (Chien et al.), and astronomical interferometry (Gottesman et al.), and a few less-important applications. No one had attempted to define methods for distributed programming in quantum repeater networks, beyond QKD and ad hoc methods of using Bell pairs.

２．研究の目的

Our goal in this project was to establish methods for programming quantum repeater networks. To achieve this, we needed to improve the understanding of applications for such networks and their operation, especially concerning the interoperability between distinct types of networks to support the creation of true internetworks.

３．研究の方法

We are developing a general-purpose quantum researcher intended to support the development of both protocols for the internal operations of quantum repeater networks, and the applications of such networks.
In addition, we are working to create network protocol specifications that will advance interoperability between developing quantum network prototypes as well as serve as a vehicle for incorporating the talent of the classical Internet protocol research and development community.

４．研究成果

(1) **Rule-based quantum communication architecture**: Our most important technical accomplishment is the development of our RuleSet-based architecture for establishing quantum connections across a network composed of heterogeneous nodes and links whose characteristics are unknown to the connection endpoints when the connection establishment is initiated. Each *Rule* consists of a *Condition Clause* and an *Action Clause*, e.g. of the form, "When holding one entangled pair with Alice and one entangled pair with Bob, perform entanglement swapping so that the remaining entangled state is shared between Alice and Bob, and communicate the necessary byproduct operators and other information to Alice and Bob." The RuleSets collectively support all of the nodes in a path making independent but consistent decisions that advance the process of making end-to-end entanglement between two end nodes.
The validity of this architecture is being proven using a new simulator we are developing. The first paper using the simulator is under review at a journal ①.
The connection establishment procedure operates in a recursive fashion, collecting the information necessary to make decisions about the ordering of operations and the number of rounds of purification required as an outbound query message traverses the path. The receiving end node establishes the RuleSets, which are then communicated to the nodes involved in a return phase. This process is documented in an *Internet Draft*, a formal specification document similar to a network protocol specification but without the normative role of a standard ②.
(2) **Distributed state assessment protocols**: In order to establish the RuleSets, we must dynamically assess the performance of links, via a process such as e.g. tomography. Typically, tomography is performed in an offline fashion, with data collected over a period of hours or days, then batch processed to determine post hoc the state. For online network operation, we must minimize the latency of the process and share data in a distributed fashion among the nodes to collectively reconstruct the state fidelity, then use the data in devising RuleSets ②,③.
(3) **Establishment of a pre-standards industry working group**: To discuss the above topics as well as more general quantum networking issues, in conjunction with Prof. Stephanie Wehner of T.U. Delft, Prof. Van Meter has established the Quantum Internet Research Group (QIRG) underneath the Internet Research Task Force (IRTF) (https://datatracker.ietf.org/rg/qirg/about/). This group met face-to-face in Prague in March 2019, for the first meeting, with more than 150 people present. This group is bringing together people from the classical Internet industry with those from quantum

research to combine knowledge and work toward robust standards and interoperable protocols.

(4) **Circuit design for Quantum Byzantine Agreement:** Quantum key distribution in several forms is widely acknowledged as the first application of a widely deployed Quantum Internet, but the Quantum Internet is expected to be much more broadly useful. However, few proposed distributed algorithms have been evaluated for their expected performance and the demands they place on the network and node hardware. We selected Ben-Or and Hassidim's form of Quantum Byzantine Agreement (QBA) ④ for closer inspection and development of detailed circuits. While our hope was that QBA would prove to be a good second algorithm to implement on a quantum repeater network, in fact our analysis showed that the resource requirements are substantial (160 qubits per node) and that the complexity of the required computation is such that a very strict gate error rate of about one error per million gates (10^{-6}) is required ⑤. Thus, unless a new approach to the problem is found, QBA may not be practical until error-corrected quantum repeaters (2nd generation) with substantial computational resources become available.

(5) **Interoperability between different repeater generations:** We established methods for creating entangled Bell pairs where the two qubits have separate logical encodings ⑥. We simulated the creation of coding-heterogeneous Bell pairs with one physical qubit partnered with a logical qubit (either Steane [[7,1,3]] code or surface code), and between Steane code and surface code. We found that creating physical Bell pairs, then applying the standard encoding procedure to each individual qubit works well. In our opinion, this paper will serve as one of the key papers outlining the techniques necessary for quantum internetworking.

(6) **Advances in surface code engineering:** Second- and third-generation quantum repeaters as well as ship-based distribution of entanglement (below) require the use of the surface code. We developed and simulated methods for dealing with physically defective qubits ⑦ by creating "superplaquettes", allowing the individual plaquettes on the surface to merge and measuring larger stabilizers (error correction syndromes). We also developed a more compact form of the surface code that uses fewer resources ⑧.

(7) **Ship-based distribution of entanglement:** Without effective link layers, a worldwide Quantum Internet cannot be built. With collaborators, we developed methods for the distribution of quantum entanglement via ship, using logical qubits protected via strong quantum error correction and packaged in large shipping containers ⑨. The logical qubits in a container are entangled with logical qubits left onshore, and the entanglement is maintained via local quantum error correction during the several-week shipping phase. During the steady-state operational phase, the shipping latency is irrelevant, as the entangled states can be used with only the latency of classical Internet-based communication once the ship arrives at its destination. In fact, this approach offers high bandwidth and high fidelity over distances that will remain unachievable for the foreseeable future using fixed quantum repeater nodes, and allows for the establish of new transoceanic "links" on a few weeks' notice, compared to the years required for planning and implementation of new undersea fibers.

(8) **Graph-based network coding:** Network coding is a means of improving the utilization of throughput and network resources by in-network computation. Graph states are generalized many-qubit entangled states. By combining these two concepts, we reduced the complexity of the computation at individual nodes, and improved the overall error resilience of multiple application qubit teleportations competing for access to the network at the same time ⑩.

<引用文献>

① Matsuo, Takaaki、Durand, Clement、Van Meter, Rodney、Quantum link bootstrapping using a RuleSet-based communication protocol, preprint available at https://arxiv.org/abs/1904.08605

② Van Meter, Rodney、Matsuo, Takaaki、Connection setup in a quantum network, https://datatracker.ietf.org/doc/draft-van-meter-qirg-quantum-connection-setup/, Mar. 2019, expires Sept. 2019.

③ Oka, T.、Satoh, T.、Van Meter, R.、A classical network protocol to support distributed state tomography、2016 IEEE Globecom Workshops、2016

④ Ben-Or, Hassidim, Fast quantum Byzantine agreement, Proceedings of the thirty-seventh annual ACM symposium on Theory of computing, 481-485, 2005

⑤ Mohammand Amin Taherkhani、Keivan Navi、Rodney Van Meter、Resource-aware

system architecture model for implementation of quantum aided Byzantine agreement on quantum repeater networks、*Quantum Science and Technology*、査読有、3(1), 2017, 014011
DOI: https://doi.org/10.1088/2058-9565/aa9bb1

⑥ Nagayama, Shota、Choi, Byung-Soo、Devitt, Simon、Suzuki, Shigeya、Van Meter, Rodney、Interoperability in encoded quantum repeater networks、*Physical Review A*、査読有、93(4), 2016, 042338
DOI: 10.1103/PhysRevA.93.042338

⑦ Shota Nagayama、Austin G Fowler、Dominic Horsman、Simon J Devitt、Rodney Van Meter、Surface code error correction on a defective lattice、*New Journal of Physics*、査読有、19(2), 2017, 023050

⑧ Nagayama, Shota、Satoh, Takahiko、Van Meter, Rodney、State injection, lattice surgery, and dense packing of the deformation-based surface code、*Physical Review A*、査読有、95(1), 2017, 012321
DOI: 10.1103/PhysRevA.95.012321

⑨ Devitt, Simon J、Greentree, Andrew D、Stephens, Ashley M、Van Meter, Rodney、High-speed quantum networking by ship、*Scientific Reports*、査読有、6, 2016, 36163
DOI: 10.1038/srep36163

⑩ Matsuo, Takaaki、Satoh, Takahiko、Nagayama, Shota、Van Meter, Rodney、 Analysis of measurement-based quantum network coding over repeater networks under noisy conditions、*Physical Review A*、査読有、97(6), 2018, 062328
DOI: 10.1103/PhysRevA.97.062328

５．主な発表論文等

〔雑誌論文〕（計　7　件）

① Matsuo, Takaaki、Satoh, Takahiko、Nagayama, Shota、Van Meter, Rodney、 Analysis of measurement-based quantum network coding over repeater networks under noisy conditions、*Physical Review A*、査読有、97(6), 2018, 062328
DOI: 10.1103/PhysRevA.97.062328

② Mohammand Amin Taherkhani、Keivan Navi、Rodney Van Meter、Resource-aware system architecture model for implementation of quantum aided Byzantine agreement on quantum repeater networks、*Quantum Science and Technology*、査読有、3(1), 2017, 014011
DOI: https://doi.org/10.1088/2058-9565/aa9bb1

③ Shota Nagayama、Austin G Fowler、Dominic Horsman、Simon J Devitt、Rodney Van Meter、Surface code error correction on a defective lattice、*New Journal of Physics*、査読有、19(2), 2017, 023050

④ Nagayama, Shota、Satoh, Takahiko、Van Meter, Rodney、State injection, lattice surgery, and dense packing of the deformation-based surface code、*Physical Review A*、査読有、95(1), 2017, 012321
DOI: 10.1103/PhysRevA.95.012321

⑤ Nagayama, Shota、Choi, Byung-Soo、Devitt, Simon、Suzuki, Shigeya、Van Meter, Rodney、Interoperability in encoded quantum repeater networks、*Physical Review A*、査読有、93(4), 2016, 042338
DOI: 10.1103/PhysRevA.93.042338

⑥ Van Meter, Rodney、Devitt, Simon、The path to scalable distributed quantum computing、*IEEE Computer*、査読有、49(9), 2016, pp. 31-42
DOI: 10.1109/MC.2016.291

⑦ Devitt, Simon J、Greentree, Andrew D、Stephens, Ashley M、Van Meter, Rodney、High-speed quantum networking by ship、*Scientific Reports*、査読有、6, 2016, 36163
DOI: 10.1038/srep36163

〔学会発表〕（計　16　件）

① Takahiko Satoh, Quantum Sockets for the NISQ Era Quantum Internet, 18th Asian Quantum Information Science Conference(国際学会), 2018

② Rodney Van Meter, The Quantum Internet, SPIE Remote Sensing and Defence + Security(招待講演), 2018

③ Rodney Van Meter, The Quantum Internet,　Joint Conference on Computer Science and Software Engineering (招待講演), 2018

④ Rodney Van Meter, Quantum Connections, 2018 IEEE Photonics Society Summer Topical Meeting Series(国際学会), 2018

⑤ Rodney Van Meter, Challenges in Designing the Quantum Internet, International Conference on Challenges in Quantum Information Science(国際学会), 2018

⑥ Rodney Van Meter, Stephanie Wehner, Vision for a QIRG: Quantum Internet Research Group, Internet Research Task Force(招待講演)(国際学会), 2018

⑦ Rodney Van Meter, Distributed quantum computing systems: Technology to quantum circuits, 2017 Symposium on VLSI Circuits(招待講演)(国際学会), 2017

⑧ Takaaki Matsuo, Takahiko Satoh, Shota Nagayama, Rodney Van Meter, Analysis of Measurement-based Quantum Network Coding Protocol over Repeater Networks under Noisy Conditions, 2nd Workshop for Quantum Repeaters and Networks, 2017

⑨ Takafumi Oka, Takahiko Satoh, Rodney Van Meter, Optimal Fidelity Estimation in Purification for the Fastest Bootstrap of a Quantum Link, 2nd Workshop for Quantum Repeaters and Networks, 2017

⑩ Shota Nagayama, Error and resource estimation of generalized heterogeneous coded Bell pairs, 2nd Workshop for Quantum Repeaters and Networks, 2017

⑪ Rodney Van Meter, Takahiko Satoh, Shota Nagayama, Takaaki Matsuo, Shigeya Suzuki, 2.5G Quantum Repeaters, 2nd Workshop for Quantum Repeaters and Networks, 2017

⑫ Mohammad Amin Taherkhani, Keivan Navi, Rodney Van Meter, Resource-aware system architecture model for implementation of quantum aided Byzantine agreement on quantum repeater networks, 2nd Workshop for Quantum Repeaters and Networks, 2017

⑬ Takaaki Matsuo, Takahiko Satoh, Shota Nagayama, Shigeya Suzuki and Rodney Van Meter, Wide-area topology of a Quantum Internet, International Conference on Quantum Communication, Measurement and Computing (QCMC), 2016 (国際学会)

⑭ Shigeya Suzuki, Rodney Van Meter, Shota Nagayama, Takahiko Satoh and Takaaki Matsuo, Architecture of software simulation of a Quantum Internet, International Conference on Quantum Communication, Measurement and Computing (QCMC), 2016 (国際学会)

⑮ Takahiko Satoh, Shigeya Suzuki, Shota Nagayama, Takaaki Matsuo and Rodney Van Meter, Routing on a Quantum Internet, International Conference on Quantum Communication, Measurement and Computing (QCMC), 2016 (国際学会)

⑯ Rodney Van Meter, Shigeya Suzuki, Shota Nagayama, Takahiko Satoh, Takaaki Matsuo, Amin Taherkhani, Simon Devitt and Joe Touch, Large-Scale Simulation of the Quantum Internet, International Conference on Quantum Communication, Measurement and Computing (QCMC), 2016 (国際学会)

〔図書〕（計　0　件）

〔産業財産権〕
○出願状況（計　0　件）

○取得状況（計　0　件）

〔その他〕
ホームページ等

６．研究組織

(1)研究分担者

(2)研究協力者
研究協力者氏名：佐藤 貴彦
ローマ字氏名：(SATOH, Takahiko)
研究協力者氏名：松尾 賢明
ローマ字氏名：(MATSUO, Takaaki)
研究協力者氏名：永山 翔太
ローマ字氏名：(NAGAYAMA, Shota)
研究協力者氏名：鈴木 茂哉
ローマ字氏名：(SUZUKI, Shigeya)
研究協力者氏名：TAHERKHANI, Mohammed Amin
研究協力者氏名：DEVITT, Simon
研究協力者氏名：STEPHENS, Ashley
研究協力者氏名：GREENTREE, Andrew
研究協力者氏名：HORSMAN, Dominic
研究協力者氏名：FOWLER, Austin
研究協力者氏名：CHOI, Byung-Soo