# 第５部

# 特集5 #QuantumNative: Online Education and Research for the Next Generation
## AQUA (Advancing Quantum Architecture) Annual Report 2018

Rodney Van Meter

## Abstract

The AQUA (Advancing Quantum Architecture) working group continued research activities advancing quantum computing and communication, especially quantum networking and distributed quantum computing systems. Our research contributes to planning for the long-term evolution of the computing and networking industries as Moore's Law comes to an end. In 2017, AQUA members created a MOOC that reached over 2,500 people in 127 countries and territories, and helped establish the new IBM Q Network hub at Keio, where member companies will gather to develop quantum algorithms for production use in their business. We published four journal and peer-reviewed conference papers. WIDE members participated in the Second Workshop for Quantum Repeaters and Networks, and agreed to host the third workshop in Japan in 2019.

## 1 Introduction

WIDE, through the AQUA working group, is well positioned to participate in and help guide the field in the exciting area of quantum computing and quantum networking, particularly as it moves from theoretical papers and small laboratory technology demonstrations toward actual systems.

This report first discusses the massive open online course (MOOC) that attracted thousands of learners from around the world. We then turn to the IBM Q Network and to online experiments conducted by WIDE members and their students. This is followed by recent work in WIDE on quantum networks, then quantum error correction and quantum architecture. A brief summary of current work is followed by a description of WIDE's particiation in the quantum networking community. This report closes with a summary of major publications over the last two years. An introduction to the AQUA group and work areas is included as Appendix A. A brief introduction to the field of quantum information is included as Appendix B. Statistics on the MOOC are included in Appendix C.

=> *IBM Q Network, Shiraj, Shota, Kaaki, Amin, WQRN, MOOC, QIRG*

## 2 #QuantumNative: Online Education and Research for the Next Generation

For a number of years, the term *digital native* has been common:

> **digital native** (noun) a person born or brought up during the age of digital technology and so familiar with computers and the Internet from an early age.
> *Apple Dictionary 2.2.1, 2014*

Similarly, we can define a *quantum native*:

> **quantum native** (noun) a person born or brought up during the age of quantum technology and so familiar with quantum computers from an early age; a person whose first serious study of algorithms involved quantum algorithms, whether exclusively or in conjunction with classical algorithms.

We are using the hashtag `#QuantumNative` to describe such people. An important goal of the AQUA working group is to find and nurture quantum native talent; because the thought process for creating quantum algorithms is very different than that of classical algorithms, we believe it is important that potential quantum programmers are exposed to the concepts as early in their education as possible. For some years, WIDE member Rodney Van Meter has been teaching students as young as first-year bachelor's students, and in 2017 we extended our reach substantially.

## 2.1 FutureLearn MOOC

In October 2017, WIDE members Rodney Van Meter and Takahiko Satoh, working with WIDE member Keiko Okawa, brought online a massive online open course (MOOC) titled, "Understanding Quantum Computers" (UQC). The course was presented online through the platform FutureLearn. Keio University has partnered with FutureLearn since 2016. UQC attracted 2,555 learners from 127 countries and territories, of whom 300 completed more than 90% of the course. (This is considered a high success rate for a MOOC, where completion percentages generally run in the low single digits.) A screenshot of the trailer is shown in Fig. 1.

The structure of the course is shown in Table 1. Many MOOC platforms are ultimately passive, composed of little more than hour-long lectures by a professor or other expert, often recorded in a lecture hall and with no more attention to the clarity and attractiveness of visual aids than pointing a camera at a projection screen. FutureLearn, in contrast, emphasizes interactively for learners and high production values for audio and video. The FutureLearn philosophy features three points: (1) tell stories; (2) provoke conversation; and (3) celebrate progress. Each learning Step is targeted at approximately ten minutes. Several types of materials can be presented; we used video; articles with text and graphics; quizzes; semi-moderated

Figure 1: The trailer on the front page of the MOOC.

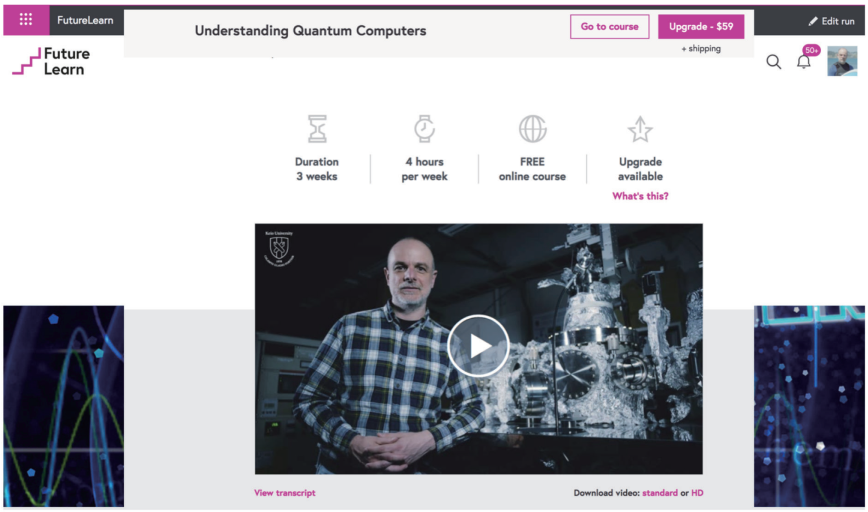


Table 1: Summary of the "Understanding Quantum Computers" MOOC

| | | |
|---|---|---|
| Week 1 | Quantum Computing Concepts | 33 Steps |
| Week 2 | Quantum Algorithms | 23 Steps |
| Week 3 | Quantum Hardware and Industry | 25 Steps |
| Total | Article: 37 Video: 22 Quiz: 9 Discussion: 9 Exercise: 4 81 | Steps |

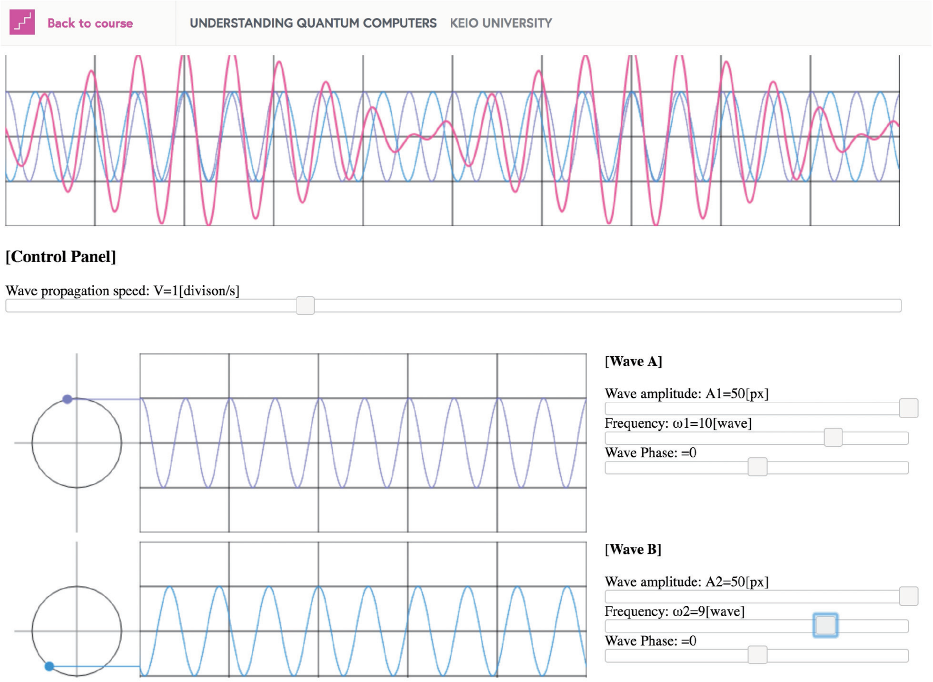
discussion boards, in which the educators and a team of assistants participated; and two types of external materials. Because the Futurelearn discussion boards do not allow learners to upload video or images, we linked to a separate site that allows this. We also included plans for 3-D printable objects for explaining some concepts.

In order to qualitatively grasp the behavior of a quantum computer, a learner needs to understand seven key concepts, introduced in Appendix B. WIDE member Keiko "Kiki" Shigeta created a native JavaScript app that interactively demonstrates interference between two simple sine waves, shown in Fig. 2. Interference can occur in more than a single dimension; student Hideo Daikoku created an app to show two-dimensional interference, using the D3 JavaScript library for 3-D rendering, as shown in Fig. 3.

We created two additional JavaScript apps for aiding the understanding of Shor's algorithm for factoring large numbers, the single most famous quantum algorithm found to date [48]. Euclid's classical algorithm serves an important supporting role in classical post-processing in the overall algorithm. Student Takafumi Oka created an app (Fig. 4) that demonstrates this 2,300 year old algorithm.

Fig. 5 shows the app created by student Kotone Itaya. The key to Shor's algorithm is recognition that, to factor the number $N$, it is sufficient to find the *period* of the function $a^x$ mod $N$, where $a$ is an arbitrarily-chosen small prime number and $x$ is the incrementing variable. The app illustrates that such a function has a period, but that the period is hard to extract without direct calculation, as no pattern is evident for most values of $N$ and $a$.

In addition to the JavaScript apps, we developed 3-D printable objects that assist in the learning process. Two-dimensional interference is compared to the propagation of a wave from a single source in Figs. 6 and 7. These two mathematical



**[Control Panel]**

Wave propagation speed: V=1[divison/s]

**[Wave A]**

Wave amplitude: A1=50[px]

Frequency: ω1=10[wave]

Wave Phase: =0

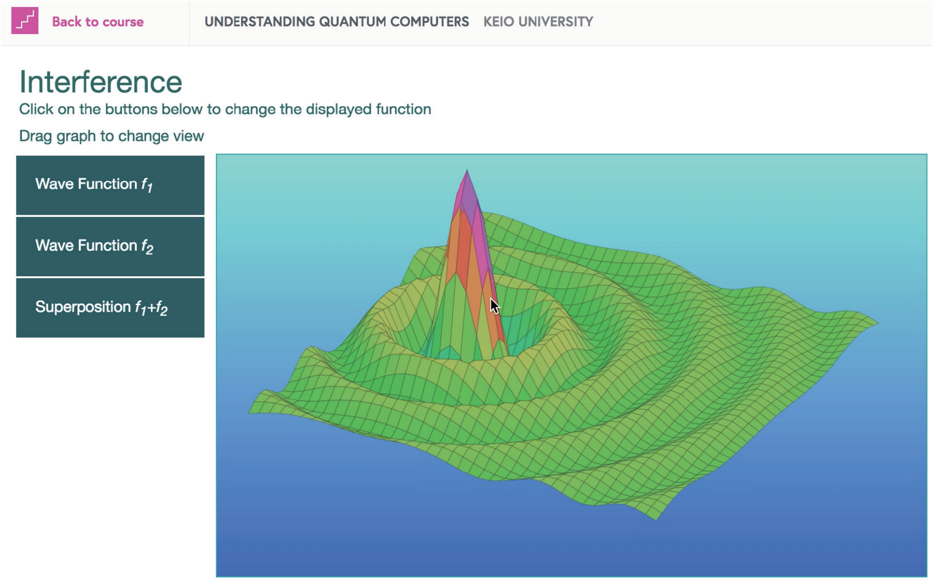
**[Wave B]**

Wave amplitude: A2=50[px]

Frequency: ω2=9[wave]

Wave Phase: =0

Figure 2: JavaScript app allowing the learner to adjust various parameters to learn about onedimensional interference. Constructive and destructive interference are the key to quantum algorithms.

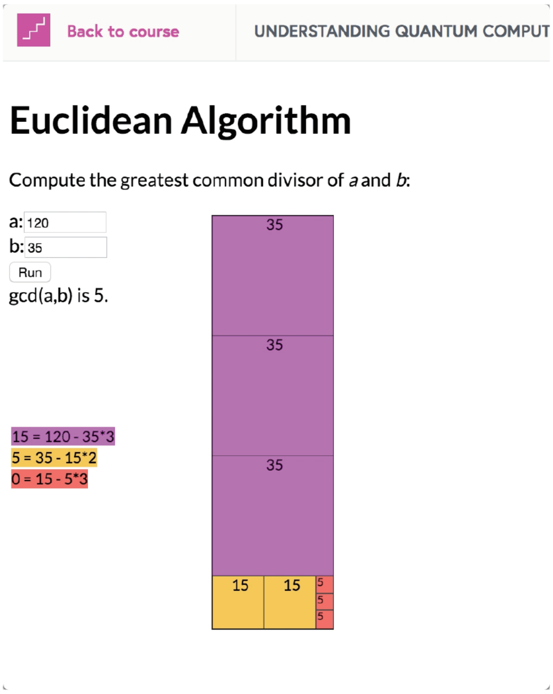


Interference

Click on the buttons below to change the displayed function

Drag graph to change view

Figure 3: JavaScript app for understanding two-dimensional interference, created using the D3 library.



Euclidean Algorithm

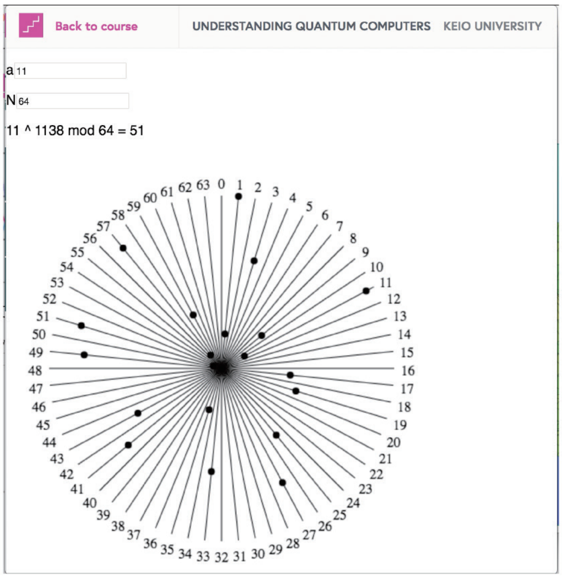
Compute the greatest common divisor of *a* and *b*:

a: 120
b: 35

gcd(a,b) is 5.

15 = 120 - 35*3
5 = 35 - 15*2
0 = 15 - 5*3

Figure 4: JavaScript app demonstrating Euclid's algorithm for finding the greatest common divisor of two numbers.



a 11

N 64

11 ^ 1138 mod 64 = 51

Figure 5: JavaScript app for demonstrating the periodicity of modular exponentiation $a^k$ mod $N$, created using the React framework.

Figure 6: 3-D printed model showing propagation of a single wave from a point source.

Figure 7: 3-D printed model showing interference of two waves emanating from point sources.

functions are similar to one shown in the JavaScript app in Fig. 3. An important notion in understanding the execution of operations on individual qubits is known as the *Bloch sphere*; a 3-D printable version is shown in Fig. 8.

## 2.2 Online Experiment

In addition to the MOOC, learners now have access through the web to several quantum computing systems of different architecture and capabilities.

IBM, with one of the world's leading industrial research efforts, has produced a fiftyqubit experimental system which remains proprietary (see the next section), a five-qubit system for which data has been published [49], and a sixteen-qubit system that is available to the public. These systems can be accessed via a web interface[1]. A screen shot of the front end is shown in Fig. 9.

NTT has made its quantum parametric oscillator (QPO, also called an optical parametric oscillator, OPO), or quantum neural network (QNN), available to the public[2]. This system is not a fully programmable computer, but instead can solve specific graph problems. The current interface does not allow programming of the system, but allows users to run specific test cases as a learning experience, as shown in Fig. 10.

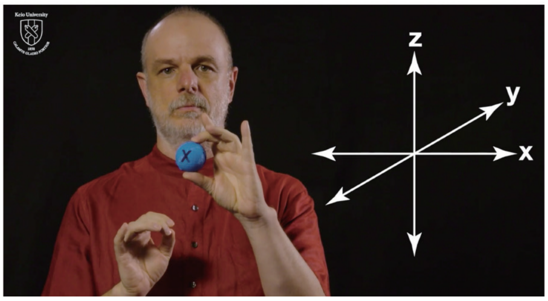
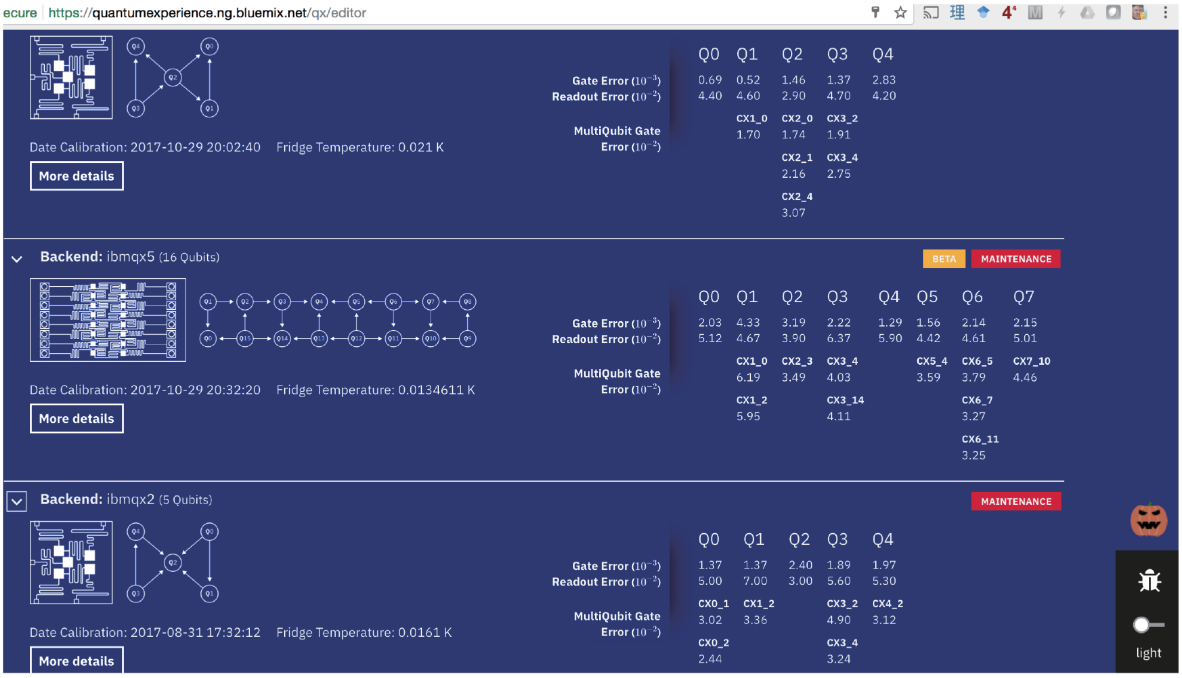


Figure 8: Explaining measurement axes for a single qubit using the 3-D printed model of the Bloch sphere.

---

[1] https://www.research.ibm.com/ibm-q/.

[2] https://qnncloud.com/index-jp.html.



ecure https://quantumexperience.ng.bluemix.net/qx/editor

| | Q0 | Q1 | Q2 | Q3 | Q4 |
|---|---|---|---|---|---|
| **Gate Error** ($10^{-3}$) | 0.69 | 0.52 | 1.46 | 1.37 | 2.83 |
| **Readout Error** ($10^{-2}$) | 4.40 | 4.60 | 2.90 | 4.70 | 4.20 |
| **MultiQubit Gate Error** ($10^{-2}$) | | CX1_0 1.70 | CX2_0 1.74<br>CX2_1 2.16<br>CX2_4 3.07 | CX3_2 1.91<br>CX3_4 2.75 | |

Date Calibration: 2017-10-29 20:02:40 Fridge Temperature: 0.021 K

**Backend:** ibmqx5 (16 Qubits)

| | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 |
|---|---|---|---|---|---|---|---|---|
| **Gate Error** ($10^{-3}$) | 2.03 | 4.33 | 3.19 | 2.22 | 1.29 | 1.56 | 2.14 | 2.15 |
| **Readout Error** ($10^{-2}$) | 5.12 | 4.67 | 3.90 | 6.37 | 5.90 | 4.42 | 4.61 | 5.01 |
| **MultiQubit Gate Error** ($10^{-2}$) | | CX1_0 6.19<br>CX1_2 5.95 | CX2_3 3.49 | CX3_4 4.03<br>CX3_14 4.11 | | CX5_4 3.59 | CX6_5 3.79<br>CX6_7 3.27<br>CX6_11 3.25 | CX7_10 4.46 |

Date Calibration: 2017-10-29 20:32:20 Fridge Temperature: 0.0134611 K

**Backend:** ibmqx2 (5 Qubits)

| | Q0 | Q1 | Q2 | Q3 | Q4 |
|---|---|---|---|---|---|
| **Gate Error** ($10^{-3}$) | 1.37 | 1.37 | 2.40 | 1.89 | 1.97 |
| **Readout Error** ($10^{-2}$) | 5.00 | 7.00 | 3.00 | 5.60 | 5.30 |
| **MultiQubit Gate Error** ($10^{-2}$) | CX0_1 3.02<br>CX0_2 2.44 | CX1_2 3.36 | | CX3_2 4.90<br>CX3_4 3.24 | CX4_2 3.12 |

Date Calibration: 2017-08-31 17:32:12 Fridge Temperature: 0.0161 K

Figure 9: The GUI element showing the IBM quantum computers available for online use as of Oct. 30, 2017.

Title 26/40: first experiment of parton

Comment 20/94: なるほど。わからん。

Type: Complete

Size: 100

Connectivity: ● Auto ○ Custom -Random seed 55816

Figure 10: The GUI for the quantum neural network, or quantum parametric oscillator, made available online by NTT [50, 51, 52].

## 3 IBM Q Network

In December 2017, IBM announced an organizational network of hubs around the world, where customers can gather to study quantum computing and develop algorithms suited to their own businesses. Members of the hubs have access to the fifty-qubit system and larger systems as they come online. Keio University is the only such hub in Asia, and WIDE Member Rodney Van Meter is the Vice Chair.

In the short run, many researchers are focusing on the development of *hybrid* algorithms, using noisy, intermediate-scale quantum computers [53] to execute specific subroutines, and augmenting the quantum computation with significant amounts of classical computation. An important element in the success of such an approach is error mitigation, before complete quantum error correction becomes technically feasible [54].

## 4 Quantum Networking Research

A quantum repeater's work consists of four tasks: (1) generation of base-level entanglement with its nearest neighbors, using fiber or free space links; (2) managing errors (via error detection or error correction); (3) coupling the singlehop entanglement into longer-distance entanglement, e.g. via a method known as entanglement swapping [55]; and (4) participating in management of the network. Experimental and theoretical physicists have worked hard on the physical layer mechanisms for generating entanglement, and theorists have studied means of managing errors while building entanglement along a chain of repeaters, but little energy has been invested so far in designing *networks* of quantum repeaters. A network diagram showing the elements of a network with Quantum Byzantine Agreement as an application is shown in Fig. 11.

Building on the work done over the last ten years, the work done by AQUA since 2016 has completed our list of provisional technical proposals for almost every aspect of creating a true entanglement-based Quantum Internet above the physical layer.

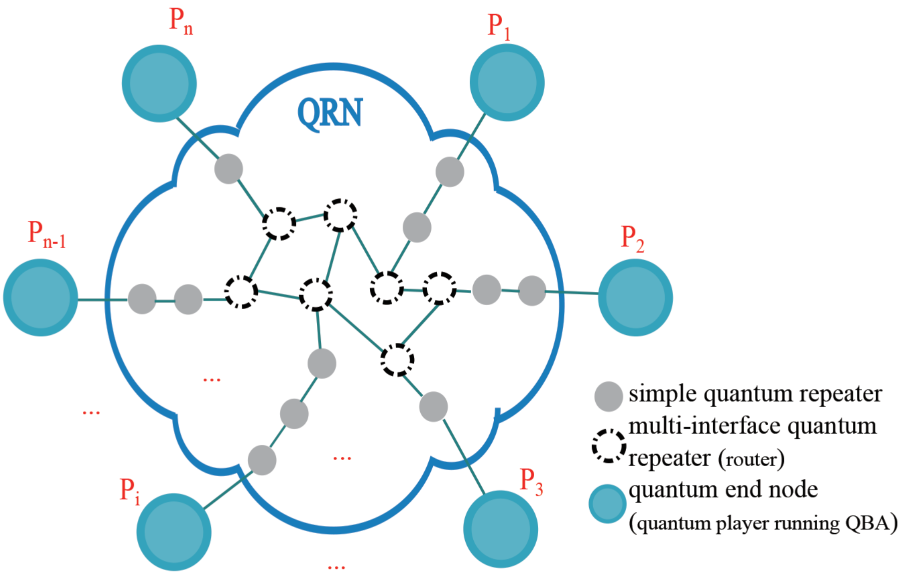


Figure 11: Required elements in Quantum Repeater Networks (QRN) for running scalable quantum distributed applications such as Quantum Byzantine Agreement. From [56].

## 4.1 2017 Accomplishments

**Resource demands of Quantum Byzantine Agreement:** The demands of quantum key distribution are relatively well understood for single-photon systems, though perhaps somewhat less so for entanglement-based QKD [57, 58]. However, the performance requirements of the broader set of applications of distributed entanglement are less well understood. We can classify applications into three groups, with some overlap: distributed cryptographic functions, wide-area sensor networks, and distributed quantum computation. In earlier years, we have worked to establish performance requirements for distributed quantum computation, in which we concluded that for many applications the performance demands are very high, leaving us very far from networks

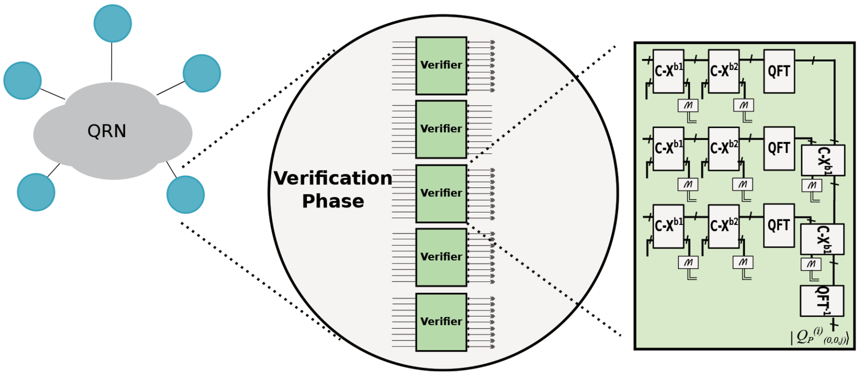


Figure 12: In the verification phase, the verifier circuit is run on the collection of qupits received during the sharing phase. From [56].

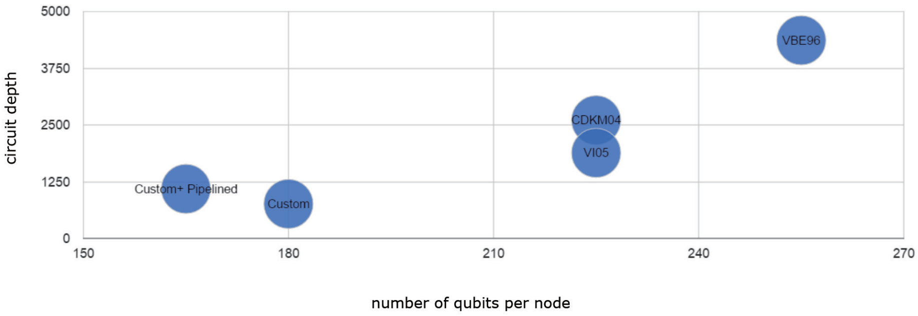


Figure 13: The number of required qubits per node versus the total required depth of the quantum circuit for the different designs. Points toward the lower left are better. From [56].

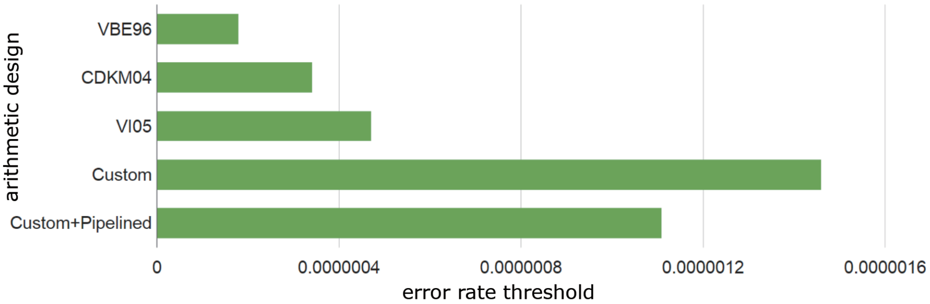


Figure 14: Threshold of the local gate error for the total design. Higher is better. From [56].

capable of supporting them [59]. Likewise, some assessments of sensor network applications are very demanding [60].

AQUA's recent work therefore returns to the question of assessing the performance of cryptographic functions other than QKD. Quantum Byzantine Agreement (QBA) appears to have the potential to be an early application of quantum repeater networks [61]. QBA provides a set of security and asymptotic performance characteristics not available in a classical Byzantine agreement protocol. Taherkhani *et al.*'s software (circuit) architecture run on each node is shown in Fig. 12 [56]. Our analysis suggests that nodes with a few hundred qubits, capable of creating several hundred of Bell pairs and performing a few thousand operations before quantum decoherence sets in, can perform the full QBA protocol designed by Ben-Or and Hassidim. Fig. 13 shows the tradeoff between node size and the execution time, and Fig. 14 shows an estimate of the required error rate in order to successfully execute the algorithm.

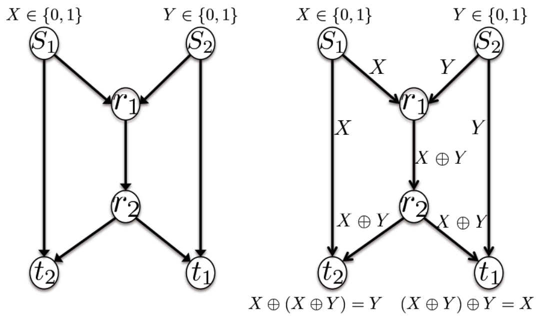


Figure 15: Fundamental network topology with bottleneck solvable via network coding. (a) The butterfly network with a bottleneck at link between intermediate resource nodes $r_1$ and $r_2$. Even with undirected channels, resource contention occurs somewhere with standard routing protocol. (b) Network coding performed to transmit two messages simultaneously. Messages are encoded at resource node $r_1$ and decoded at target nodes $t_1$ and $t_2$. From [62].

**Measurement-based quantum network coding over repeater networks:** Network coding improves the utilization of otherwise idle resources in a network, to accelerate delivery of data across multiple overlapping paths. Quantum network coding similarly builds end-to-end entanglement over overlapping paths. Prior work by Satoh et al. (discussed in the next section) took a straightforward approach to mapping the core ideas of quantum network coding, as shown in Fig. 15, to the physical structure of quantum repeater networks. Nodes are connected over physical channels, and can entangle only two qubits in a single step; the end-to-end connections then require additional operations local to the repeater nodes. First, Satoh et al. laid out the procedures in the abstract [63], then analyzed the behavior in the presence of errors [63, 64].

The core idea of quantum network coding builds on a large entangled state known as a *cluster state*. Matsuo *et al.*

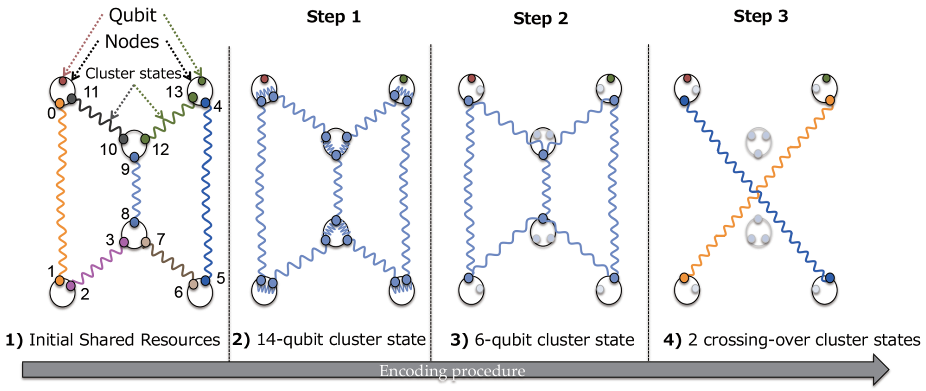


Figure 16: Step-by-step encoding procedure of MQNC. This scheme also manipulates quantum channels but without any parity creation. The topological transition via measurements on cluster states can accomplish the same goal as QNC in a simpler way. From [62].

developed a new circuit (Fig. 16) for creating such a cluster state and using it for network coding, taking into account errors and the physically distributed nature of repeater nodes [62]. Simulations of the circuit with errors show that the protocol is more robust than Satoh *et al*.'s earlier protocol, in the presence of errors on the initial entangled pairs (Fig. 17) and local gate errors (Fig. 18).

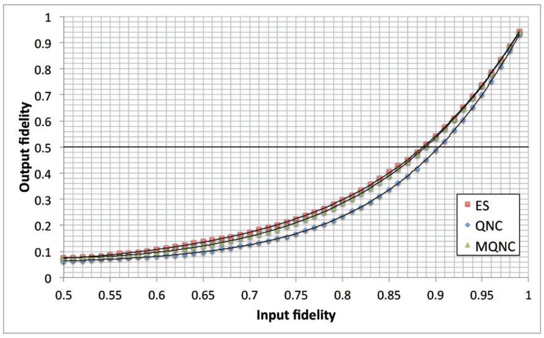


Figure 17: Impact of input fidelity on output fidelity in three protocols. All combinations of observable errors stochastically present on all qubits. Local operations are assumed to be ideal. From [62].

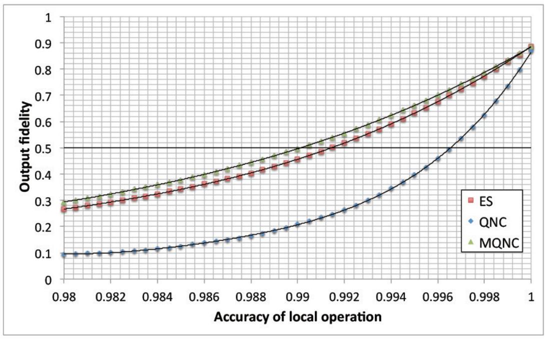


Figure 18: Impact of local operation accuracy on output fidelity in three protocols. Input fidelity is fixed to $F_{input}$ = 98%, and the local operation accuracy is changed from $F_{operation}$ = 98% to $F_{operation}$ = 100% with Δ $F_{operation}$ = 0:05%. From [62].

## 4.2 2016 Accomplishments

**Interoperability between different network types:** Quantum repeater networks will be built on a variety of different physical technologies, but from our point of view the bigger concern is whether different types of networks can be made to interoperate at the logical level. Several different types of networks have been proposed. Some depend on *entanglement purification* [65, 66], which detects but cannot correct errors, and some depend on *quantum error correction* [67, 68]. Is it possible to bridge the different types, so that a true Quantum Internet can be built?

In this work, Nagayama *et al*. examined several methods of creating *Bell pairs* (the basic form of entangled quantum state used in quantum networks) that span two different types of networks, and proposed a system that is robust and performs well. This method is optimized for use in quantum routers that sit at the boundary between two networks, and use an optical switch to connect two "line cards" that face into separate types of networks. We believe that this method will serve as the primary workhorse for interoperability in the Quantum Internet.

**Analyzing quantum network coding over repeater networks:** Like classical network coding [69], quantum network coding (QNC) is a means of utilizing computation in the middle of a network to enhance throughput by alleviating the load on bottleneck links [70, 71]. However, early analyses ignored the detailed process of executing QNC on repeater networks, which Satoh *et al*. remedied in 2012 [63].

In 2016, Satoh *et al*. extended this work to incorporate mixed states (those with some error component), assessing the output fidelity and comparing it to the simpler entanglement swapping approach. They found that QNC results in lower fidelity, and is especially sensitive to local gate error rates due to the larger number of operations, and is therefore most useful when maximizing performance is more important than the output fidelity.

**Assessing the assessment of quantum states:** Quantum tomography is the complete evaluation of a system's ability to create a particular quantum state, done by recreating the state many times and measuring it in different fashions [72]. In quantum networks, tomography, or perhaps a simplified procedure optimized for Bell pairs, will be needed both at the link level and end to end. In operational networks, the process is complicated by the need to perform tomography on quantum states that are held in distributed fashion, and the need to conduct it in real time as end-to-end connections are created across the network, rather than in batch fashion after a laboratory data collection run. Oka *et al*. created a classical network protocol to support this distributed tomography [73].

The goal of tomography is to create a description of the quantum state known as the *density matrix*, building on knowledge of the state creation process and the experimental measurement results. The reconstruction process involves two phases: the reconstruction itself, followed by evaluation of the likelihood that the observed measurements can be explained by the reconstruction. An important observation is that the latter process is inherently stochastic, hence, two parties both attempting this evaluation may reach different conclusions. In a network, this could result in different operational decisions and failure of the networking protocols, an undesirable result. Thus, the protocol created employs a master-slave architecture.

The authors also evaluated the workload imposed by tomography, and found that it may take several hours. This may be acceptable for bootstrapping a link, but is unacceptable for dynamic connection establishment, forcing us to look for other solutions. This factor will affect the design of connection establishment protocols, and ultimately important details of the entire network architecture.

**Entanglement creation via container ship:** Existing designs for quantum repeaters are likely to be physically large devices that require substantial maintenance and infrastructure, making them unsuitable for deployment along the ocean floor. Devitt *et al*. recognized that the power of quantum error correction allows us to create Bell pairs on shore, then keep one member of the pair in place while the other is carried via ship across the ocean [74]. Because quantum entanglement is a generic resource not incorporating important data, the latency of the ship is irrelevant, much like the sharing of one-time pads for encryption.

**Assessing security and stability of quantum repeater network operations:** We have estimated the impact of the hijacking of a single quantum repeater on the work executed by an entire network. Due to the fragility of quantum states, connections across quantum repeater networks are very sensitive to the presence of eavesdroppers, which is well known, but until now no one has assessed whether this fact and the distributed nature of purification and entanglement swapping make quantum networks more vulnerable to serious operational disruption.

Satoh *et al*. have taken a big step by analyzing whether the hijacking of a single repeater gives the hijacker significantly more leverage than the hijacking of a single classical Internet router would [75]. We conclude that networks that utilize purification, which already suffer a logarithmic overhead in work due to the purification, may also suffer a similar logarithmic overhead in the amount of work that can be disrupted by a single hijacker. However, we do not expect that this will make quantum repeater networks significantly less stable than classical networks. Moreover, as we apply quantum tomography throughout the network to monitor the quality of connections, the same tomography, if done in a secure fashion, can be used to scan for the presence of hijacking and assist in the isolation of the hijacked repeater.

This work was preceded by work examining hardware attacks on individual nodes, which resulted in some suggested guidelines for quantum repeater hardware architectures [76].

**Optimization of performance and resource consumption for some networks:** Creation of entanglement across a link is a probabilistic process, due to the loss of photons at every optical element and interface and through the channel (e.g., fiber). We can divide the success probability into several ranges; in the “high probability” range, we can expect that enough entanglements will be created every round trip across the link that we can use quantum error correctionbased methods and effectively optimize the use of memory along the path [77].

Van Meter *et al*. showed that path utilization patterns that minimize memory buffering time (and the corresponding loss of state fidelity due to decoherence) always exist for two of the three major entanglement usage patterns: B class, which includes Bell inequality violation experiments and quantum key distribution (QKD); and C class, which execute a limited range of quantum calculations known as Clifford group operations. Buffering above the link level can be reduced to zero for these classes, whereas T class operations, including full quantum computation and teleportation, require additional buffering to accommodate the propagation of classical signals. T class operations have a range of Pareto optimal patterns on any type of path, but with non-zero buffering. Zero buffering is possible only for one particular link arrangement, discussed in the paper.

### 4.3 Prior Years

The results of 2017 and 2016 build on years of prior work quantum network and quantum internetwork architecture [78]. Almost every major network design issue has now been touched upon, though the design choices will evolve continually even after initial deployments. Our overall goal, therefore, is to build a future-proof, flexible architecture that allows indefinite innovation. A few key results are highlighted here.

**Internetwork architecture:** The Quantum Recursive Network Architecture (QRNA), building on the classical Recursive Network Architecture [79], will scale management of connections, work across heterogeneous networks, and retain autonomy and privacy of network operations [80].

**Routing:** A modified form of Dijkstra's algorithm will work for intermediate-sized networks [81].

**Multiplexing:** Assignment of resources to quantum network connections will likely follow circuit switching principles due to the need to continually execute distributed operations, but moment-by-moment allocation of entangled states may work acceptably even when performed in Internet-style best-effort, first-come, first-served fashion [82].

## 5 Quantum Error Correction and Quantum Computer Architecture Research

In addition to the work on quantum networks, AQUA members have conducted research on error correction for quantum computers and quantum computer architecture. In our opinion, as well as the opinion of a number of others, the *surface code* represents the most attractive method, encoding a logical qubit in the parity of chains of qubits on a surface [83, 84, 85].

### 5.1 2017 Accomplishments

**Surface code on a defective lattice:** Unfortunately, fabrication of solid-state qubits is expected to be far from perfect for the foreseeable future. Nagayama *et al*. recognized this difficulty, and developed methods to allow the surface code to work around physically defective qubits, then invested millions of hours of CPU time in simulating systems to determine the effectiveness [86]. They found that chips with 90% of the qubits functioning properly would allow construction of large-scale quantum computers.

**A more compact form of the surface code:** One of the drawbacks of the surface code is the high resource consumption compared to the code distance. Nagayama *et al*. found a new representation on the 2-D surface code lattice that packs logical qubits in about half the space of prior work [87].

### 5.2 2016 Accomplishments

**A road map toward scalable distributed architectures:** Van Meter and Devitt, in a recent article in a special issue of *IEEE Computer*, discussed surface code quantum computation and the prospects for several quantum information technologies.

**Designing a million-qubit quantum computer:** One of the hurdles to implementation of quantum computers is the enormous resources required, encouraging distributed architectures, as above. In collaboration with researchers from Duke University, AQUA member Van Meter studied the application and error correction behavior and hardware quality requirements assuming a distributed system of optically interconnected ion traps. Using more traditional error correcting codes, Ahsan *et al*. found that a million-qubit computer may be both achievable and useful [88].

## 6 Ongoing Quantum Research

**Quantum network security:** Work on understanding how to make quantum networks operationally robust against misbehavior (whether or not intentional) is needed as we begin to plan quantum repeater networks.

**Impact of tomography on network operations:** The tomography work and hijacking framework described above represent the first steps in understanding how the network is monitored in real time operation. A key concern is doing so in Internet-scale interconnected systems, where latencies are high and heterogeneity forces technology-independent data representations and communications.

**Connection establishment methods:** We now understand reasonably well how quantum connections want to use the network and at the abstract level how to select the resources to use. However, actually identifying and reserving the resources requires a good deal of engineering. A key concern is doing so in Internet-scale interconnected systems, where privacy and autonomy of operation are paramount.

**Application analysis:** Many more prospective applications of distributed quantum entanglement exist in the literature, but the operational demands they make of quantum networks is still poorly understood.

**Hybrid algorithms:** The current most important topic in the quantum computing community is how to combine noisy intermediate-scale quantum computers [53] with large-scale classical computers to solve problems more quickly than classical systems alone. These *hybrid algorithms* must take into account noise, and decompose larger problems into small sub-problems that can be effectively handled on existing and near-future quantum computers.

**Error mitigation:** The companion problem to developing hybrid algorithms is developing *error mitigation* techniques that will allow us to execute quantum algorithms effectively in the presence of noise, without the overhead and technical challenges of full-scale quantum error correction and fault tolerance.

## 7 Community Participation

WIDE members participate actively in theWorkshop for Quantum Repeaters and Networks (WQRN). The second WQRN was held in Seefeld, Austria, in September 2017[3]. The next WQRN is scheduled for 2019, and WIDE member Rodney Van Meter will be the general chair of the conference. Attendance of around 100 researchers, from experimental physicists to classical networking experts, gather to exchange ideas and discuss the challenges in going from a simple channel to more complete networks.

In early 2018, several researchers including Rodney Van Meter are working to create an RG (research group) on quantum networking inside the IRTF. Meetings of QIRG (the Quantum Internet Research Group) are expected during calendar 2018.

## 8 Publications

### 8.1 2017

AQUA members had three journal papers published or accepted for publication in 2017, one peer-reviewed international conference talk, several international conference poster presentations, and several additional submissions. The published and accepted papers are:

1. R. Van Meter, “Distributed quantum computing systems:

---

＊3 https://www.uibk.ac.at/congress/wqrn2/index.html.en.

Technology to quantum circuits," VLSI Symposium 2017 [89].

2. Shota Nagayama, Austin G. Fowler, Dominic Horsman, Simon J. Devitt and Rodney Van Meter, "Surface Code Error Correction on a Defective Lattice," *New Journal of Physics* 19(2), 023050, 2017 [86].

3. Shota Nagayama, Takahiko Satoh and Rodney Van Meter, "State Injection, Lattice Surgery and Dense Packing of the Defermation-Based Surface Code," *Physical Review A* 95(1), 012321, 2017 [90].

4. M. Amin Taherkhani, Keivan Navi, Rodney Van Meter, "Resource-aware architecture for implementation of quantum aided Byzantine agreement on quantum repeater networks," *Quantum Science and Technology* 3(1), 014011, 2018 [56].

Three additional papers are available as preprints or are under review at journals.

1. Takaaki Matsuo, Takahiko Satoh, Shota Nagayama and Rodney Van Meter, "Analysis of Measurement-based Quantum Network Coding over Repeater Networks under Noisy Conditions," preprint arXiv:1710.04827.

2. Takahiko Satoh, Shota Nagayama, and Rodney Van Meter, "The Network Impact of Hijacking a Quantum Repeater," preprint `arXiv:1701.04587`.

3. Rodney Van Meter, Takahiko Satoh, Shota Nagayama, Takaaki Matsuo and Shigeya Suzuki, "Optimizing Timing of High- Success-Probability Quantum Repeaters," preprint `arXiv:1701.04586.`

### 8.2 2016

AQUA members had five journal papers published in 2016 and one peer-reviewed workshop paper, and several international conference poster presentations. The published papers are:

1. Rodney Van Meter and Simon Devitt, "The Path to Scalable Distributed Quantum Computing," *IEEE Computer* 49(9), 31–42, Sept. 2016, [91].

2. Takahiko Satoh, Kaori Ishizaki, Shota Nagayama and Rodney Van Meter, "Analysis of quantum network coding for realistic repeater networks," *Physical Review A* 93(3), 032302, 2016, [64].

3. Shota Nagayama, Byung-Soo Choi, Simon Devitt, Shigeya Suzuki and Rodney Van Meter, "Interoperability in encoded quantum repeater networks," *Physical Review A* 93(4), 042338, 2016, [92].

4. Simon J. Devitt, Andrew D. Greentree, Ashley M. Stephens and Rodney Van Meter, "High-speed quantum networking by ship," *Scientific Reports* 6, 36163, 2016, [74].

5. Takafumi Oka and Takahiko Satoh and Rodney Van Meter, "A Classical Network Protocol to Support Distributed Quantum State Tomography," *Proc. Quantum Communications and Information Technology*, Dec. 2016, [73].

6. Muhammad Ahsan, Rodney Van Meter and Jungsang Kim, "Designing a Million-Qubit Quantum Computer Using a Resource Performance Simulator," *J. Emerg. Technol. Comput. Syst.* 12(4), 39, 2016, [93].

## A What is AQUA?

### A.1 Goals

The primary goal of AQUA is to advance the deployment of quantum technologies in the real world, principally by applying known techniques from classical computer architecture, networking and distributed systems to the problems of scalability in quantum systems. This work will both bring new computational capabilities and help ensure that the progress of information technology does not end when the size of transistors can no longer be reduced.

The physical technology on which modern computing systems are built will change dramatically over the course of the next several decades. Beyond the research goals, AQUA also aims to expose the current generation of students to the principles that drive the evolution of computing technology, and the underlying physics of computation, preparing the students for forty-year careers in which they will work with applied physicists and electrical engineers to drive the coming technological revolutions.

### A.2 Work Areas

AQUA works in five areas contributing to distributed quantum computing systems:

- Devices: In conjunction with researchers at Stanford University, RIKEN, and the University of Tokyo we are designing semiconductor-based chips using opticallycontrolled quantum dots and superconducting flux qubits.

- Workloads: Although AQUA does not focus on the creation of new quantum algorithms, we do work on how to implement known quantum algorithms efficiently on realizable architectures. We also perform the reverse analysis: to implement a given algorithm, how large and how accurate a quantum system is required?

- Tools: Proper analysis of new ideas in architecture and networks requires software tools for compiling programs and optimizing their mapping to particular systems, as well as physical simulation of quantum devices and effects.

- Principles: We are searching for new principles in quantum architecture and networking, as well as applications of known principles.

- Networks: Large systems must combine multiple devices into one system that can compute collaboratively, as well as share information; we are investigating both system-area and wide-area quantum networks.

Underlying all of these is the critical issue of error management in quantum systems; quantum data is far too fragile to store or compute upon without continuous, active correction. Our primary focus is on the promising surface code error correction, looking for ways to makes its implementation resource-friendly and robust in the face of various system constraints.

## B Quantum Concepts

The following is a brief summary of the key aspects of quantum communication and computation that impact network and system architecture.

**Qubits**. Quantum information is most often discussed in terms of *qubits*. A qubit, like a classical bit, is something with two possible values that we can label zero and one. Unlike a classical bit, a qubit can occupy both values simultaneously, known as *superposition*.

**Superposition and measurement.** A qubit can represent multiple values in different proportions at the same time, e.g., two-thirds of a “one” and one-third of a “zero”. This *superposition* determines the relative probability of finding each value when we *measure* the state. When we measure the qubit, we get only a single classical bit of information (the “one” or “zero”) with 100% probability, and the superposition *collapses*.

**Entanglement and Bell pairs.** Some groups of qubits exhibit strong correlation between the qubits that cannot be explained by independent probabilities for individual qubits. Instead, the group must be considered as a whole, with interdependent probabilities. This phenomenon is known as *quantum entanglement*. A special entangled state known as a *Bell pair* or *EPR pair*, consisting of two quantum bits, figures prominently in quantum communication. Each qubit in the pair has a 50%

probability of having a value of 1 and a 50% probability of having a value of 0 when we measure it. Although we cannot predict which will be found, when we measure one member of the pair, the value of the other is immediately determined. This happens independent of the distance between the two members of the Bell pair.

**Interference.** Quantum algorithms use some building blocks derived from classical concepts, such as adder designs, but the overall thrust of a quantum algorithm is very different from that of a classical algorithm. Rather than attempting to solve a problem and checking for the answer, a quantum algorithm's goal is to create *interference* between the elements of a superposition quantum state. The basic concept is shown in Figs. 2 and 3 in the main text, while in quantum computers the interference happens across a much larger space. Constructive interference reinforces desirable states, increasing the probability of finding a desirable outcome on measurement, while destructive interference reduces the probability.

**No cloning.** As mentioned above, a key restriction of quantum systems is that we cannot make *independent* copies of an unknown state [94]. This makes error correction exceedingly difficult.

**Fidelity.** The quality of a quantum state is described by its fidelity, which is, roughly, the probability that we correctly understand the state – if we ran the same experiment many times and measured the results, how close to our desired statistics would we be? Unfortunately, any physical operation results in a loss of fidelity, gradually degrading the state as we manipulate or even store it. We can counter this by using a form of error correction or detection.

**Purification.** The form of error detection historically favored in quantum repeater networks is purification, which uses minimal resources [95]. It sacrifices some quantum states to test the fidelity of others. There are various purification mechanisms, with different purification algorithms and different methods for determining which states are sacrificed, each with particular tradeoffs.

**Quantum error correction (QEC).** QEC may be based on classical codes or purely quantum concepts. The primary difficulties are extraction of errors without damaging quantum state, avoiding error propagation, and the increased resources required. (See references contained in [96], [67] and [68].)

**Teleportation.** Teleportation destroys the state of a qubit at the sender and recreates that state at the destination, teleporting information rather than matter, as explained in Figure 19 [97]. The process uses a Bell pair's long-distance correlation, followed by transmission of a pair of classical bits.

With these basic concepts, we can begin to construct networks. Bell pairs are consumed by teleportation, so one way to organize a network is to create a continuous stream of Bell pairs between source and destination – as long as we identify those sources and destinations, choose paths to get there, and manage the resources along the way.

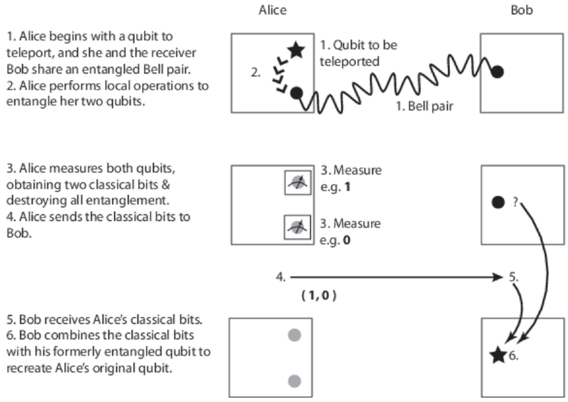


Figure 19: Operations in teleporting a qubit from Alice to Bob.

## C MOOC Statistics

Table 2 and 3 provide, respectively, the progress statistics and locations of learners who participated in the “Understanding Quantum Computers” MOOC in fall 2017. The Run Retention Index is calculated similar to a scholarly h-index. The value of 0.407 means that 40.7% of the learners completed at least 40% of the steps in the MOOC.

Table 2: Learner progress in
“Understanding Quantum Computers” MOOC.

| | | |
|---|---|---|
| Joiners | 2,555 | |
| Leavers | 388 | 15.2% |
| Learners | 1,645 | 64.4% |
| Active Learners | 1,200 | 72.9% |
| Social Learners | 378 | 23.0% |
| Upgrades Sold | 55 | 3.3% |
| Learners with ≧ 50% step completion | 414 | 25.2% |
| Learners with ≧ 90% step completion | 300 | 18.2% |
| Run Retention Index | 0.407 | 40.7% |

Table 3: Locations of learners who joined the “Understanding Quantum Computers” MOOC, ordered by number of joiners.

| country_name | country_code | country_continent | joiner_count | active_learner_count |
|---|---|---|---|---|
| United Kingdom | GB | Europe | 815 | 453 |
| United States of America | US | North America | 262 | 110 |
| India | IN | Asia | 144 | 44 |
| Japan | JP | Asia | 140 | 62 |
| unknown | – | unknown | 95 | 45 |
| Australia | AU | Australia | 73 | 34 |
| France | FR | Europe | 49 | 27 |
| Germany | DE | Europe | 49 | 22 |
| Canada | CA | North America | 48 | 22 |
| Netherlands | NL | Europe | 43 | 22 |
| Spain | ES | Europe | 39 | 16 |
| Italy | IT | Europe | 38 | 20 |
| Mexico | MX | North America | 38 | 18 |
| Egypt | EG | Africa | 34 | 9 |
| Brazil | BR | South America | 33 | 14 |
| Russia | RU | Europe | 29 | 12 |
| Ukraine | UA | Europe | 27 | 13 |
| Ireland | IE | Europe | 26 | 16 |
| Nigeria | NG | Africa | 23 | 6 |
| Saudi Arabia | SA | Asia | 21 | 6 |
| Thailand | TH | Asia | 20 | 7 |
| Belgium | BE | Europe | 20 | 11 |
| Malaysia | MY | Asia | 19 | 3 |
| Indonesia | ID | Asia | 18 | 5 |
| Pakistan | PK | Asia | 16 | 3 |
| Greece | GR | Europe | 16 | 5 |
| Poland | PL | Europe | 15 | 10 |
| Algeria | DZ | Africa | 14 | 2 |
| China | CN | Asia | 13 | 6 |
| South Africa | ZA | Africa | 13 | 8 |
| Switzerland | CH | Europe | 12 | 10 |
| United Arab Emirates | AE | Asia | 12 | 5 |
| Romania | RO | Europe | 12 | 2 |
| New Zealand | NZ | Australia | 11 | 6 |
| Colombia | CO | South America | 11 | 9 |
| Turkey | TR | Europe | 11 | 1 |
| Sweden | SE | Europe | 11 | 5 |
| Bangladesh | BD | Asia | 10 | 2 |
| Hong Kong | HK | Asia | 9 | 4 |
| Morocco | MA | Africa | 9 | 4 |
| Singapore | SG | Asia | 9 | 7 |
| Czech Republic | CZ | Europe | 8 | 4 |
| Hungary | HU | Europe | 8 | 6 |

| | | | | |
|---|---|---|---|---|
| Serbia | RS | Europe | 8 | 3 |
| Israel | IL | Asia | 7 | 4 |
| Albania | AL | Europe | 7 | 2 |
| Vietnam | VN | Asia | 7 | 2 |
| Ethiopia | ET | Africa | 7 | 1 |
| Korea (South) | KR | Asia | 7 | 4 |
| Argentina | AR | South America | 6 | 2 |
| Taiwan | TW | Asia | 6 | 2 |
| Portugal | PT | Europe | 6 | 2 |
| Sudan | SD | Africa | 6 | 3 |
| Ghana | GH | Africa | 6 | 1 |
| Philippines | PH | Asia | 6 | 2 |
| Norway | NO | Europe | 5 | 1 |
| Finland | FI | Europe | 5 | 4 |
| Trinidad and Tobago | TT | North America | 5 | 4 |
| Myanmar | MM | Asia | 5 | 3 |
| Cameroon | CM | Africa | 4 | 1 |
| Jordan | JO | Asia | 4 | 2 |
| Sri Lanka | LK | Asia | 4 | 0 |
| Qatar | QA | Asia | 4 | 0 |
| Kenya | KE | Africa | 4 | 0 |
| Croatia | HR | Europe | 4 | 1 |
| Bulgaria | BG | Europe | 4 | 0 |
| Iran | IR | Asia | 4 | 3 |
| Tunisia | TN | Africa | 4 | 1 |
| Denmark | DK | Europe | 4 | 3 |
| Belarus | BY | Europe | 4 | 2 |
| Zimbabwe | ZW | Africa | 3 | 1 |
| Estonia | EE | Europe | 3 | 1 |
| Slovenia | SI | Europe | 3 | 1 |
| Costa Rica | CR | North America | 3 | 1 |
| Ecuador | EC | South America | 3 | 2 |
| Guatemala | GT | North America | 3 | 2 |
| Mozambique | MZ | Africa | 3 | 0 |
| Papua New Guinea | PG | Australia | 3 | 1 |
| Venezuela | VE | South America | 3 | 2 |
| Slovakia | SK | Europe | 2 | 0 |
| Luxembourg | LU | Europe | 2 | 2 |
| Lithuania | LT | Europe | 2 | 1 |
| Kazakhstan | KZ | Asia | 2 | 1 |
| Chile | CL | South America | 2 | 2 |
| Uganda | UG | Africa | 2 | 0 |
| Georgia | GE | Asia | 2 | 2 |
| Austria | AT | Europe | 2 | 1 |
| Cyprus | CY | Asia | 2 | 0 |

| | | | | |
|---|---|---|---|---|
| Nepal | NP | Asia | 2 | 1 |
| Paraguay | PY | South America | 2 | 1 |
| Lebanon | LB | Asia | 2 | 0 |
| Kuwait | KW | Asia | 2 | 0 |
| Yemen | YE | Asia | 1 | 1 |
| Bolivia | BO | South America | 1 | 1 |
| Brunei | BN | Asia | 1 | 1 |
| Panama | PA | North America | 1 | 1 |
| Peru | PE | South America | 1 | 1 |
| Bosnia and Herzegovina | BA | Europe | 1 | 0 |
| Burundi | BI | Africa | 1 | 0 |
| Afghanistan | AF | Asia | 1 | 0 |
| Puerto Rico | PR | North America | 1 | 0 |
| Palestine | PS | Asia | 1 | 0 |
| Uzbekistan | UZ | Asia | 1 | 0 |
| Rwanda | RW | Africa | 1 | 0 |
| Montenegro | ME | Europe | 1 | 0 |
| Moldova | MD | Europe | 1 | 1 |
| Somalia | SO | Africa | 1 | 0 |
| El Salvador | SV | North America | 1 | 0 |
| Syria | SY | Asia | 1 | 1 |
| Macedonia | MK | Europe | 1 | 0 |
| Tanzania | TZ | Africa | 1 | 0 |
| Vanuatu | VU | Australia | 1 | 0 |
| Iraq | IQ | Asia | 1 | 1 |
| Jamaica | JM | North America | 1 | 0 |
| Guadeloupe | GP | North America | 1 | 0 |
| Isle of Man | IM | Europe | 1 | 1 |
| Gambia | GM | Africa | 1 | 0 |
| Cambodia | KH | Asia | 1 | 0 |
| Guernsey and Alderney | GG | Europe | 1 | 1 |
| Fiji | FJ | Australia | 1 | 0 |
| Libya | LY | Africa | 1 | 0 |
| Cape Verde | CV | Africa | 1 | 1 |
| Madagascar | MG | Africa | 1 | 0 |
| Mali | ML | Africa | 1 | 0 |
| Mauritius | MU | Africa | 1 | 0 |
| Malawi | MW | Africa | 1 | 0 |
| Cote D'Ivoire | CI | Africa | 1 | 0 |
| Botswana | BW | Africa | 1 | 0 |