第 XXVII 部

分散型量子計算の
ネットワーク応用技術

第 27 部
分散型量子計算のネットワーク応用技術

Abstract

In 2010, WIDE created a new working group called AQUA (Advancing Quantum Architecture), giving a formal base to continue the work that has been done for the last several years by individual members of WIDE. AQUA conducts research on quantum computing, especially quantum networking and distributed quantum computing systems. Quantum computing brings new capabilities, including the ability to solve some problems efficiently for which no efficient classical solutions are known, such as factoring large numbers (which impacts encryption key exchange mechanisms), and new, secure means for sharing information based on the physics of quantum effects rather than the mathematical difficulty of certain problems. Our research contributes to planning for the long-term evolution of the computing and networking industries as Moore's Law comes to an end. AQUA members collaborate with researchers around the world and have published research papers in top-tier conferences and journals such as ISCA and IEEE/ACM Transactions on Networking, and are pursuing standardization of a means for using quantum key distribution (QKD)-generated keys with the Internet standard IPsec.

AQUA（Advancing Quantum Architecture）Working Group は、これまでメンバー個人で取り組まれて来た研究に WIDE 内での活動基盤を与えるために、2010 年に結成された。AQUA では、量子ネットワーキングや分散量子コンピューティングシステムを中心に、量子コンピューティングの研究をおこなっている。量子コンピューティングは、巨大数の効率的な素因数分解が可能になるなど、現在我々がおこなっているコンピューティングとは異なる計算能力を持っている。巨大数の効率的な素因数分解は現在我々が利用している暗号化鍵共有アルゴリズムを脅かすが、量子コンピューティングはまた、数学的困難性に基づく暗号化鍵共有よりも安全な、物理学の原理に基づく暗号化鍵共有も実現する。AQUA の研究は、ムーアの法則が限界に近づくにつれ、コンピューティングとネットワーキングの長期的発展計画に貢献する。AQUA では世界中の研究者と協力し、ISCA や IEEE/ACM などのトップレベルの学会やジャーナルに論文を提出している。また、インターネット標準である IPsec で量子鍵配送を用いて共有した鍵を利用する手法の標準化活動もおこなっている。

第 1 章　What is AQUA?

1.1 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.

1.2 Work Areas

AQUA has current, active work in five areas contributing to distributed quantum computing systems:

- Devices: In conjunction with researchers at Stanford University, we are designing semiconductor-based chips using *quantum dots*.
- 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.

1.3 Members

The initial group of members of AQUA come from Keio's Shonan Fujisawa Campus and the University of Tokyo, with support and interest from IIJ and other organizations.

1.4 Working Style

Quantum technology remains a highly experimental area, with a potential short-term impact on Internet encryption but the primary impact on computer architecture and networking still a number of years in the future. AQUA focuses on standardization of IPsec with quantum key distribution (QKD), supported by experimental demonstrations (see Secs. 2.4 and 3.3), and on long-term research. The primary output of AQUA will be research papers in top-tier physics and computer systems journals and conferences.

Publications by group members prior to the formal founding of the AQUA WG include the International Symposium on Computer Architecture (ISCA)[180], IEEE/ACM Transactions on Networking[179], ACM's Journal of Emerging Technologies in Computing Systems[33, 181, 182] and Physical Review Letters[60, 135]. We have also written an Internet Draft which is currently under revision[136]. Members have participated and presented posters in international conferences such as the Asian Conference on Quantum Information Science (AQIS), Southwest Quantum Information Technology (SQuInT), the Workshop on Theory of Quantum Computation, Communication and Cryptography (TQC), the International Conference on Quantum Error Correction, and Updating Quantum Cryptography and Communications. At this year's AQIS conference, held in September, WIDE members presented seven posters.

AQUA members have collaborated with researchers at NII and NTT in Japan, and Stanford University, Harvard University, Seoul University and the University of Melbourne abroad. We expect continuing and new collaborations in 2011.

第 2 章　Background: FAQ on Quantum Computing

2.1 What is Quantum Computing?

Classically, a device that holds binary data can be in only one state at a time, either zero or one. However, when data is stored on systems controlled by quantum effects, the device (or *qubit*) can be in a *superposition* of states, partially in the zero state and partially in the one state. With

some restrictions, this allows a *quantum computer* to operate on an exponentially large number of inputs at the same time, e.g., n qubits can hold 2^n values at the same time. When multiple qubits are in a highly correlated state, they are *entangled*.

The difficult part, and the true art in designing algorithms for quantum computers, is extracting useful answers from the superposition state. *Interference* is used to cancel out incorrect answers and reinforce correct answers, so that *measuring* the quantum state has a high probability of giving the correct answer to a problem.

Quantum technologies initially will not be standalone: they need to integrate with classical systems and networks. In fact, they may be deployed as coprocessors for large-scale classical systems, improving precision and runtime for large computations through "quantum-assisted computing".

2.2 Why is Quantum Computing Valuable?

For some problems, quantum computers are believed to be much faster than classical computers[10, 132]. The most famous result to date is Peter Shor's algorithm for factoring large numbers[163], which may potentially impact encryption technology, as mechanisms such as Diffie-Hellman key exchange and public-key cryptography (e.g., RSA) may be vulnerable to a practical solution to this problem. However, machines for running Shor's algorithm are known to be very large, far beyond currently-viable technology[177, 178].

Before Shor machines become viable, then, it is likely that quantum computers will be deployed for other uses. They were, in fact, originally conceived as a means for simulation other quantum systems[51]. Quantum computers with as few as 40 high-quality qubits may prove to be useful for solving problems in quantum chemistry[9]. This approach may lead to the custom design of new materials, and possibly an improved understanding of the quantum effects that result in superconductivity. Related quantum technologies are also expected to advance quantum metrology, improving our ability to measure gravitional fields and to create high-accuracy clocks capable of measuring time to an accuracy of 10^{-19}.

Above all, quantum computation promises to be a completely new theory of information, based on recognizing that information is not abstract, but must be connected to its physical representation[2, 18, 103, 104, 139].

2.3 Why is Quantum Computing Necessary?

The economic imperative of Moore's Law[131] dictates that companies in the semiconductor industry increase the density of silicon chips every year, while reducing the per-transistor price correspondingly. In recent years, the pace of improvement has slowed somewhat to a doubling approximately every three years, but the net result remains an exponential growth in the number of transistors in a chip, and therefore a reduction in the size of each transistor[49].

2.4 What is Quantum Key Distribution?

Quantum key distribution (QKD) uses quantum effects to detect the presence of an eavesdropper on a communications channel[15, 107]. QKD creates a stream of bits shared between two parties that are guaranteed by physics, rather than mathematics, to be secret (subject, of course, to the usual issues of correct and safe implementation). These secret bits are then useful as keys for standard, symmetric encryption, replacing keys generated using the Diffie-Hellman protocol. Experimental networks of QKD systems have been deployed in Boston[46], Vienna[142], and Tokyo.

2.5 What is a Quantum Repeater?

Loss of photons in a fiber is exponential in the length of the fiber, and the fidelity (quality) of the quantum state also declines, limiting practical direct quantum connections to perhaps 150 km. Quantum repeaters[43, 44] connect a series of shorter hops (perhaps as little as 10 km, depending on technology), creating entangled states over

a long distance and potentially allowing the creation of a global quantum network.

Quantum repeaters use *purification* (a quantum-specific type of error correction) and *entanglement swapping* (based on *teleportation*[16]), and must have high-quality quantum memory.

2.6 What is a Quantum Network?

Quantum networks come in two flavors: those that use long-lived entanglement, and those that do not. The latter kind are primarily useful for QKD, whereas the former are expected to be used for various distributed applications beyond QKD, such as the quantum metrology mentioned above.

Except for the physical mechanism of entangling qubits using an optical fiber (or even through free space), the problems of quantum networks are the same as for classical networks: how to choose an efficient route through a network with imperfect information, how to reliably transmit information, and how to manage the resources of the network in a distributed fashion.

Beyond the simple transfer of quantum data from one location to another, quantum networks actual act as fully distributed quantum computing systems[183]. Thus, the classical requests that support quantum communication effectively become requests for the execution of quantum algorithms. This feature of quantum networks remains to be explored.

2.7 Where is World-Leading Quantum Information Research Being Done?

Outstanding experimental work on quantum technologies is being done in over thirty laboratories here in Japan, as well as in the United States (Caltech, Stanford, Harvard, Berkeley, Duke, MIT, Los Alamos National Lab, NIST, and many others), Canada (especially Waterloo), the United Kingdom (Bristol, Oxford and others), Austria, Australia, France, and elsewhere. Within Japan, leading institutions include U. Tokyo, Osaka U., Tohoku U., NICT, NEC, RIKEN, NTT, Keio and others. Top-level theory work is also a broad international effort covering the same countries. In Japan, leading theorists work at NII, U. Tokyo, Keio, NTT, RIKEN, Osaka U., Tohoku U., and elsewhere.

Many of the researchers in Japan, including WIDE Board member Rodney Van Meter, are members of the FIRST Quantum Information Processing Project[1]. This four-year project, begun in 2010, is supported with 3,000,000,000 yen from the Japanese government. Most of the money is expected to be used to support continuing leading-edge experimental work.

1　http://first-quantum.net/e/index.html

第 3 章　This Year's AQUA Activities

3.1 The Founding of the WIDE AQUA Working Group

The creation of the AQUA working group and the corresponding web page and mailing list were approved on October 7, 2010. The initial co-chairs are Rodney Van Meter and Shota Nagayama.

3.2 Meetings

The AQUA group met formally for the first time during the WIDE Kenkyuukai held at the University of Tokyo in December, 2010. The meeting included a brief discussion of recent research results appearing in the literature, followed by discussion of the key networking projects going on inside of WIDE: quantum Dijkstra, quantum repeater protocol design, and standardization of IPsec with QKD.

The AQUA group also met informally as a BoF during prior WIDE Camps over the last two years. Collaborative research meetings are held weekly at SFC and via Skype, involving WIDE members from SFC and Todai.

3.3 Standardization of IPsec with Quantum Key Distribution (QKD)

QKD is a technology for establishing secret, random bits shared between two parties, but is silent on the issue of the use of those bits. The most common assumption is that the bits are to be used as key material for classical, usually symmetric encryption. One use for such key material is to replace the Diffie-Hellman key exchange that is part of the Internet Key Exchange protocol, which is part of the IPsec suite. This approach has been experimentally demonstrated[46], but the necessary changes to the IKE protocol have not been documented and standardized.

WIDE members have proposed a simple but carefully-architected approach to augmenting the IKE protocol, by adding two payload types[136]. One carries the identifier of a key created via QKD or other out-of-band means, so that the mechanism is flexible enough to use for other key decision mechanisms (e.g., one-time pad) that deliver keys outside the context of IKE. The second new payload type carries instructions for fallback operation when the QKD mechanism fails or is deliberately attacked. Because QKD is designed to detect eavesdropping, an attacker can create a denial-of-service condition by listening, so we propose to give IPsec managers a set of operational choices for what to do when this occurs.

This approach was defined in an Internet Draft in fall 2009. The I-D is currently under revision, and is expected to be resubmitted as an "individual submission" to the IETF Security Area Directors during 2011.

3.4 Quantum Dijkstra

WIDE members are the first researchers to explore the issue of path selection in realistic, heterogeneous quantum networks. As in classical networks, the selection of a path between two nodes must be done efficiently in a distributed fashion, and perhaps with imperfect information about the state of the network. The path selection algorithm impacts the stability and performance of the entire network, as well as the single communication being requested.

This problem demonstrates perfectly the operational methodology of AQUA: many classical networks use Dijkstra's shortest path first (SPF) algorithm[42, 134], but it cannot be used as-is in quantum networks. Rather than deriving a new, untested approach to path selection, we chose to adapt Dijkstra. By properly defining the link cost, we have discovered that SPF can indeed be used to select a high-bandwidth path through a network of quantum repeaters.

3.5 Quantum Repeater Protocol Design

Swap-and-purify quantum repeaters use two mechanisms, entanglement swapping and purification, to create high-fidelity, long-distance entanglement. Although these mechanisms have been studied by physicists, no formal protocol design exists. A layered architecture has been proposed[179], and WIDE members are now in the process of creating the protocol state machines and defining the contents and sequence of operations.

As with the issue of path selection, existing theoretical studies have assumed very regular networks, and hence have been able to simulate the networks with minimal attention to the issues of distributed decision making. When these protocol designs are finished and published, they can be expected to set the world standard.

3.6 Quantum Recursive Network Architecture

While the issues of cross-technology transfer of quantum data are under investigation by experimental physicists, no prior work has looked at the issues of heterogeneity in network management. Truly global-scale quantum networks require solutions that allow networks to operate autonomously, and that do not require global information about the state of the network in order to e.g. select a path through the network

or choose where to perform entanglement swapping. We have proposed a Quantum Recursive Network Architecture (QRNA) to address these problems[183].

In QRNA, a network can be abstracted as a single node, simplifying the topology of the network that must be considered when making decisions. The network protocols managing entanglement swapping and purification also "stack" nicely, creating a truly recursive protocol stack.

Rather than dealing only with the transmission of data, as in classical networks, quantum networks are also used to create specific distributed, entangled quantum states. Because the requests necessary to build these states are exactly the same as requests for distributed computation, QRNA in fact is more than just a network, it is an architecture for a complete distributed system.

3.7 Publications

Since the formal founding of the AQUA working group, members have had two publications accepted to peer-reviewed international journals:

- Byung-Soo Choi and Rodney Van Meter, "On the Effect of Quantum Interaction Distance on Quantum Addition Circuits," *ACM Journal of Emerging Technologies in Computing Systems*, 2011, to appear.

  Abstract We investigate the theoretical limits of the effect of the quantum interaction distance on the speed of exact quantum addition circuits. For this study, we exploit graph embedding for quantum circuit analysis. We study a logical mapping of qubits and gates of any $\Omega(\log n)$-depth quantum adder circuit for two n-qubit registers onto a practical architecture, which limits interaction distance to the nearest neighbors only and supports only one- and two-qubit logical gates. Unfortunately, on the chosen k-dimensional practical architecture, we prove that the depth lower bound of any exact quantum addition circuits is no longer $\Omega(\log n)$, but $\Omega(\sqrt[k]{n})$. This result, the first application of graph embedding to quantum circuits and devices, provides a new tool for compiler development, emphasizes the impact of quantum computer architecture on performance, and acts as a cautionary note when evaluating the time performance of quantum algorithms.

- Rodney Van Meter, Joe Touch and Clare Horsman, "Recursive Quantum Repeater Networks," *Progress in Informatics*, 2011, to appear.

  Abstract Internet-scale quantum repeater networks will be heterogeneous in physical technology, repeater functionality, and management. The classical control necessary to use the network will therefore face similar issues as Internet data transmission. Many scalability and management problems that arose during the development of the Internet might have been solved in a more uniform fashion, improving flexibility and reducing redundant engineering effort. Quantum repeater network development is currently at the stage where we risk similar duplication when separate systems are combined. We propose a unifying framework that can be used with all existing repeater designs. We introduce the notion of a Quantum Recursive Network Architecture, developed from the emerging classical concept of *recursive networks*, extending recursive mechanisms from a focus on data forwarding to a more general distributed computing request framework. Recursion abstracts independent transit networks as single relay nodes, unifies software layering, and virtualizes the addresses of resources to improve information hiding and resource management. Our architecture is useful for building arbitrary distributed states, including fundamental distributed states such Bell pairs and GHZ, W, and cluster states.

In addition, AQUA members published several papers earlier in 2010:

- Agung Trisetyarso and Rodney Van Meter, "Circuit Design for a Measurement-Based Quantum Carry-Lookahead Adder," *International Journal of Quantum Information*, 8, 5 (2010) pp. 843–867; preprint available from the arXiv as quant-ph:0903.0748.
- Austin G. Fowler, David S. Wang, Thaddeus D. Ladd, Rodney Van Meter, and Lloyd C. Hollenberg, "Surface code quantum communication," *Phys. Rev. Letters*, 104, 180503, May 2010; available from the arXiv as quant-ph:0910.4074.
- Rodney Van Meter, Thaddeus D. Ladd, Austin G. Fowler, and Yoshihisa Yamamoto, "Distributed Quantum Computation Architecture Using Semiconductor Nanophotonics," *International Journal of Quantum Information*, Volume: 8, Issues: 1-2 (2010) pp. 295–323, 2010. preprint available from the arXiv as quant-ph:0906.2686.

第 4 章　AQUA's Plans For the Coming Year

4.1 Standardization of IPsec with Quantum Key Distribution (QKD)

The I-D for IPsec with QKD is currently under revision, and is expected to be resubmitted as an "individual submission" to the IETF Security Area Directors during 2011. ITU is currently in the process of standarding low-level aspects of QKD, and would like to have this portion of the technology documented and standardized.

4.2 Other Technical Topics

Papers on qDijkstra, resource management in quantum networks, and protocol design for swap-and-purify repeaters are expected to be submitted early in 2011. Technical work will continue on these topics, as well as on QRNA.

A critical issue in device design is dealing with hard faults (non-functional qubits) in the surface code error correction mechanism. Our ability to allow the system to work with hard faults will likely determine the success or failure of a promising hardware/software approach to large-scale system architecture, and therefore is high-priority work.

Issues of optimizing circuits and matching circuits to architectures continue to be important, and work on graph embedding (both tools and principles) will continue in 2011.

4.3 Meetings, Etc.

AQUA WG meetings are expected to continue during 2011 at WIDE Camps and Kenkyuukai, as well as informal weekly cross-institutional research meetings. AQUA members are already planning to attend the upcoming International Workshop on Quantum Information Processing (QIP) in Singapore in January, 2011. AQUA members will also attend the FIRST Summer School to be held in Okinawa in August, 2011.