Applications of an Entangled Quantum Internet

Rodney Van Meter
Faculty of Environment and Information Studies
Keio University
5322 Endo, Fujisawa, Kanagawa, 252-8520, Japan
Email: rdv@sfc.wide.ad.jp

Byung-Soo Choi
Department of Electronics Engineering
Ewha Womans University
11-1 Daehyun-dong, Seodaemun-gu, Seoul, 120-750, South Korea
Email: bschoi3@gmail.com

Abstract

Physicists and engineers are making technical progress toward the creation of intercontinental quantum networks. But if they succeed, what new applications will a quantum Internet enable? This paper presents a series of potential uses, some fairly well-established and some highly speculative. The entanglement generated by a quantum network will be useful both as a digital computational resource, and as a gyroscopic reference, providing both phase (time) and directional information. Computational applications include the well-known quantum key distribution (QKD) process and distributed leader election, as well as the traditional uses of networks to connect geographically distributed resources. The gyroscopic reference uses are more speculative, but include the possibility of improving some "Big Science" projects by utilizing quantum entanglement to beat single-system quantum limits on precision measurements, including the accuracy of clocks.

1 Introduction

Quantum networks, if they can be built, may enable new applications, including both distributed, digital computation and large-scale analog or semi-digital systems used as quantum sensor networks. Quantum networks come in two flavors, those that will operate by creating *entanglement* between two (or more) distant quantum systems, and those that do not. In this paper, we focus on entangling quantum networks, and in particular uses of a wide-area, many-node network [15, 3].

Quantum systems can have a shared state of a form such that it is impossible to fully describe the state of only one of the members; the state of the entire *system* is correlated. Consider a pair of quanta with quantum *spin* as the state of interest. An entangled state, for example, might be one in which either both members of the pair are spinning with their axes pointed "up", or both members are spinning with their axes pointed "down", but the state is definitely not one up and one down, and *which* state they are in is not known. When one of the members of the pair is measured, the other's state then becomes determined, even if the pair is separated by a large distance. Einstein famously referred to this phenomenon as "spooky action at a distance," but it was later shown that entanglement cannot be used to violate causality or to transmit information faster than the speed of light.

We begin with a brief, qualitative description of the operation of a network of quantum repeaters, followed by some possible uses of the entanglement. Most of the uses presented here are highly speculative, and have not yet been analyzed with any mathematical rigor; this paper should be viewed as a discussion of ideas rather than confirmed facts. We conclude with a short discussion of future work.

2 Quantum Repeaters

Large-scale quantum networks may be built using very small, special-purpose quantum computers that create and maintain distributed quantum state. The network nodes are called "quantum repeaters", but serve a role equivalent to that of Internet routers, rather than analog signal repeaters. They require only minimal quantum resources, and are not fully general quantum computers themselves, but involve a large classical component in executing the algorithms,

the performance which is primarily limited by the speed of light.

Quantum repeaters will utilize three concepts to execute a distributed algorithm that creates entangled quantum states between nodes that are far apart: a basic entanglement mechanism, *entanglement swapping* and *purification* [2, 27]. Entanglement swapping extends the span of the entanglement from single-hop distances to arbitrary nodes throughout the network, while purification is a specialized form of error correction. An entangled pair of qubits is referred to as a *Bell pair*.

Figure 1 presents the protocol stack for a quantum repeater network as defined by Van Meter *et al.* [22]. The middle layers of the stack implement a distributed algorithm that turns short-distance, medium-fidelity entangled Bell pairs into long-distance, high-fidelity Bell pairs. Thus, they collectively achieve the reliable transport that is a common characteristic of ISO Layer 4 implementations, but its distributed nature makes it questionable to simply call the total process the "transport" layer. Unlike classical networks, information does not simply propagate along the path one hop at a time. All of the repeaters along the entire path are repeatedly involved in creating each end-to-end Bell pair.

Research on the physical mechanisms for transmitting quantum states typically assumes transmission through a fiber, but free-space optical links and even satellite links can also be used, with repeater nodes at each end of the link [25].

3 Applications of Entanglement

We can safely assert that, if one quantum computer is useful, then a network of them is more useful; indeed, that has already been shown for quantum multicomputers [24, 23]. But why would we want the computers to be geographically distributed? As in classical systems, it may be the case that large quantum datasets, or large computational facilities, are in different locations for political, economic, or simply historical reasons. The motivation for creating a geographically distributed quantum network, then, is the same as for a classical network: to connect resources that are not, or cannot be, colocated. Often, the "resources" are human beings. Because quantum entanglement is a physical resource, as well as a computational one, the consumers of the entanglement can be either quantum computers or scientific instruments.

3.1 Digital Uses

The most well-known use of quantum networks to date is *quantum key distribution*, or QKD. QKD uses a quantum channel and an authenticated, but not necessarily secret, public channel to create a "tamper-proof" shared set of random numbers between two nodes, using the laws of quantum mechanics to detect the presence of an eavesdropper. The shared stream of random numbers can then be used as a key, either for IPsec or as a one-time pad. QKD, therefore, is likely to be deployed first highly secure network environments, such a intra-bank and intelligence networks. QKD is also being considered as a technology for e.g. digital cash; in that context, QKD all the way from a centralized server to a user's home PC or to an ATM may have value.

Experimentally, QKD has already been implemented, and demonstration networks are in operation in the U.S., Europe, and Japan [7, 1, 16, 19]. Single-hop QKD necessarily faces an exponential decline in throughput as the link lengthens. If multiple unentangled hops are used, the intermediate nodes must be trusted, which is a serious drawback in a secure network architecture.

Although the existing networks and available QKD products do not depend on long-lived, long-distance entanglement, it is known that it is possible to use entanglement to execute QKD [6], meaning that are expected can be used to extend the distance. Using entanglement and repeaters allows the intermediate nodes to be untrusted. Thus, the first likely use of an entangled quantum network will be QKD.

One distributed quantum algorithm that may serve as a building block for more complex uses is leader election in anonymous networks, which utilizes entanglement to deterministically choose one node from among a set of equals in a deterministic number of rounds [20]. Quantum leader election runs in a polynomial number of rounds, and always chooses a leader deterministically, whereas no classical algorithm can elect a leader in deterministic time, given the same set of constraints. Leader election was recently experimentally demonstrated [17]. Quantum leader election has been shown to work in arbitrary network graphs, one of the few quantum problems to have been addressed in such a realistic environment. This algorithm represents an important theoretical advance, and may be a useful building block for larger quantum algorithms, but likely would not independently serve to spur development of quantum networks. Classical networks are, in general, not completely anonymous, and a variety of algorithms for solving the problem in non-anonymous networks are known, and are in use for a variety of problems.

Secret sharing is an important cryptographic primitive. In quantum secret sharing, a secret, consisting of a number of qubits, can be distributed to a number of participants, so that only a subset of the participants can reconstruct the original secret [11]. In a classical secret sharing scheme, the number of collaborators k required to reconstruct the secret can be any number, $1 \leq k \leq n$, where n is the number of secret shares. In a quantum secret sharing scheme, to satisfy the no-cloning theorem, $n/2 \leq k \leq n$ [10, 26].

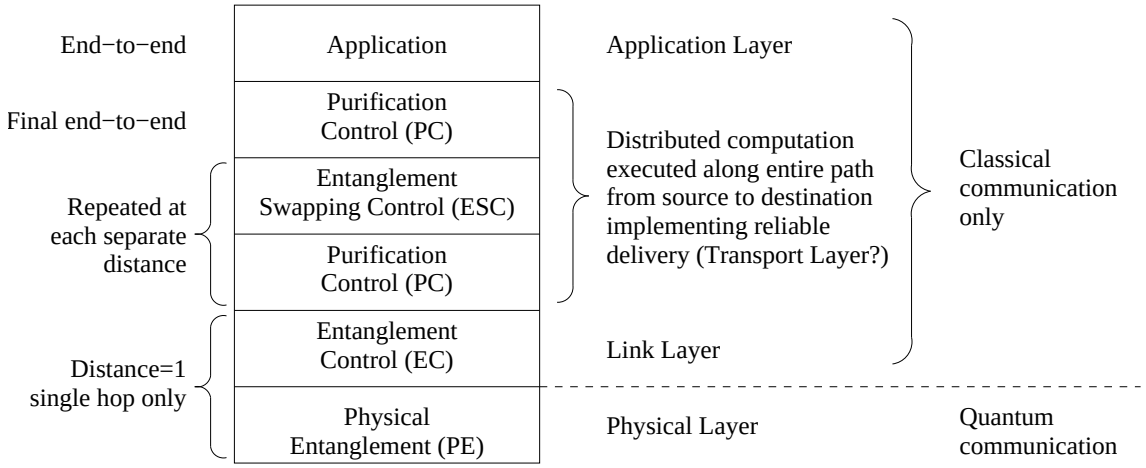

Figure 1. Quantum repeater protocol stack

Quantum secret sharing has been experimentally demonstrated [21]. As with leader election, secret sharing seems likely to be a useful building block but not provide the incentive to actually build out large-scale quantum networks.

3.2 Gyroscopic Uses

Beyond the uses with the familiar feel of digital behavior (albeit with the complexity of quantum mechanics), we note that high-fidelity entanglement can serve as a gyroscopic reference. That reference provides both time and directional synchronization. Are there ways in which this effect can be used?

The most obvious areas in which to pursue these kinds of uses would be in "Big Science" applications that might desire long-distance clock synchronization or directional information. Entangled quantum states are known to improve the precision of measuring a variety of phenomena, though those algorithms have not been adapted to use the form of entanglement we will generate using a network of quantum repeaters, and not all forms of entanglement are easily transformable into each other. Giovannetti *et al.* described a variety of uses of entanglement in scientific applications, including improved interferometry, positional measurement, tests of relativity, and metrology [8]. Some of these are best suited to single-laboratory work, others, such as the tests of relativity, are inherently distributed. We are most interested in those that use entanglement as gyroscopic information, including time reference and directional reference (which Giovannetti called *coordinate transfer*).

The LIGO gravity wave observatory can use "squeezed light", which is a highly non-classical state of light, to improve its precision for measuring vibrational movement of the system within one location [9]. It is an open question whether entanglement between Lousiana and Washington state could improve the sensitivity; it may be possible to convert an entangled Bell pair to coordinated squeezed states at both locations that can be used.

Distributed quantum algorithms have also been proposed that will synchronize clocks to better-than-atomic-clock precision over a distance [5, 14, 12]. Is it possible that a worldwide quantum network could provide a clock reference that is better than GPS? What value would such a network have?

GPS is known to provide synchronization to about 0.1-1.0 nanosecond (10^{-9}s to 10^{-10}s) [13], and further improvement is considered to be possible. Optical lattice clocks (a candidate to succeed atomic clocks, whose precision is nearly played out), operate with an accuracy of one part in 10^{15}, and further improvements (possibly as far as one part in 10^{18}) are expected [18]. At that level of accuracy, the relativistic gravitational red shift of frequencies will be measurable with an altitude difference of 1cm!

One obvious demanding application for clock synchronization is very long baseline interferometry (VLBI), a form of radio astronomy. However, the current operational accuracy of ~ 1 nsec is considered acceptable, and the GPS system can be improved by several orders of magnitude. Interferometry does not require improvement of accuracy linear in the wavelength being used, so the shift from performing interferometry on radio frequencies to optical frequencies may be feasible even with current technology.

4 Future Work

To date, repeater research has primarily focused on the physical and mathematical tools for building repeaters, some of which have been experimentally demonstrated [4], but little direct attention has been given to the need for network protocols to manage the information flow nor the necessity of consistent decisions being made in a widely-

distributed system in a timely fashion. Routing and resource management in quantum networks are important problems [22].

Finally, we wish to note that the term *internet* is appropriate in this context; quantum networks are highly likely to involve different physical entanglement mechanisms, including different wavelengths of light and physical qubit representations, purification algorithms, and routing algorithms, and likely will span multiple administrative domains. Bridging those differences will exercise many of the same organizational and technological capabilities built up in the Internet community over the last forty years.

Entangled quantum networks are on the technological horizon, and it is time to focus more effort on finding uses for the technology. Quantum key distribution is already commercially available for single hops, and should reach distances of 100km or so; extending that distance will require repeaters and the use of entanglement. Additional new functionality, such as leader election and secret sharing, provide distributed building blocks for new computational uses, and entanglement is a promising avenue for improvement in various scientific experiments. We expect the results to more than repay the R&D costs with new functionality, some of which has not yet been conceived.

Acknowledgments

The authors thank T.D. Ladd, W.J. Munro, G. Milburn, K. Nemoto, C. Walker, and M. Yun for interesting conversations, though we alone bear the responsibility for the wildness of any included ideas.

References

[1] R. Alleaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Langer, A. Leverrier, N. Lutkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger. SECOQC white paper on quantum key distribution and cryptography. quant-ph/0701168, Jan. 2007.

[2] H.-J. Briegel, W. Dür, J. Cirac, and P. Zoller. Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81:5932–5935, 1998.

[3] B.-S. Choi and J.-D. Cho. Quantum Internet: An advanced Internet exploiting quantum properties. In *International Conference on the Ubiquitous Information Management and Communication*, pages 410–420, Feb. 2007.

[4] C.-W. Chou, J. Laurat, H. Deng, K. S. Choi, H. de Riedmatten, D. Felinto, and H. J. Kimble. Functional quantum nodes for entanglement distribution over scalable quantum networks. *Science*, 316(5829):1316–1320, 2007.

[5] I. Chuang. Quantum algorithm for distributed clock synchronization. *Physical Review Letters*, 85(9):2006–2009, 2000.

[6] A. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[7] C. Elliott, D. Pearson, and G. Troxel. Quantum cryptography in practice. In *Proc. SIGCOMM 2003*. ACM, ACM, Aug. 2003.

[8] V. Giovannetti, S. Lloyd, and L. Maccone. Quantum-enhanced measurements: Beating the standard quantum limit. *Science*, 306(5700):1330–1336, 2004.

[9] K. Goda, O. Miyakawa, E. Mikhailov, S. Saraf, R. Adhikari, K. McKenzie, R. Ward, S. Vass, A. Weinstein, and N. Mavalvala. A quantum-enhanced prototype gravitational-wave detector. *Nature Physics*, 2008. published online 30 March 2008.

[10] D. Gottesman. Theory of quantum secret sharing. *Physical Review A*, 61(4):42311, 2000.

[11] M. Hillery, V. Bužek, and A. Berthiaume. Quantum secret sharing. *Physical Review A*, 59(3):1829–1834, 1999.

[12] W. Hwang, D. Ahn, S. Hwang, and Y. Han. Entangled quantum clocks for measuring proper-time difference. *The European Physical Journal D-Atomic, Molecular and Optical Physics*, 19(1):129–132, 2002.

[13] D. Jefferson, S. Lichten, and L. Young. A test of precision GPS clock synchronization. *Frequency Control Symposium, 1996. 50th., Proceedings of the 1996 IEEE International.*, pages 1206–1210, 1996.

[14] R. Jozsa, D. Abrams, J. Dowling, and C. Williams. Quantum clock synchronization based on shared prior entanglement. *Physical Review Letters*, 85(9):2010–2013, 2000.

[15] S. Lloyd, M. S. Shahriar, and P. Hemmer. Teleportation and the quantum Internet, 2000. http://arXiv.org/quant-ph/0003147.

[16] Y. Nambu, K. Yoshino, and A. Tomita. One-way quantum key distribution system based on planar lightwave circuits. *Japanese Journal of Applied Physics*, 45:5344, 2006.

[17] Y. Okubo, X. Wang, Y. Jiang, S. Tani, and A. Tomita. Experimental demonstration of quantum leader election in linear optics. *Physical Review A*, 77(3):32343, 2008.

[18] M. Takamoto, F. Hong, R. Higashi, and H. Katori. An optical lattice clock. *Nature*, 435(7040):321–324, 2005.

[19] A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K. ichiro Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki, and A. Tomita. Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength-division multiplexing clock synchronization. arxiv:0805.2193v1.

[20] S. Tani, H. Kobayashi, and K. Matsumoto. Exact quantum algorithms for the leader election problem. In *Proc. STACS 2005: 22nd Annual Symposium on Theoretical Aspects of Computer Science*, volume 3404 of *Lecture Notes in Computer Science*, pages 581–592. Springer-Verlag, 2005.

[21] W. Tittel, H. Zbinden, and N. Gisin. Experimental demonstration of quantum secret sharing. *Physical Review A*, 63(4):42301, 2001.

[22] R. Van Meter, T. D. Ladd, W. J. Munro, and K. Nemoto. System design for a long-line quantum repeater, 2007. to appear in IEEE/ACM Transactions on Networking; preprint available as arXiv:0705.4128v1.

[23] R. Van Meter, W. J. Munro, K. Nemoto, and K. M. Itoh. Distributed arithmetic on a quantum multicomputer. In

Computer Architecture News, Proc. 33rd Annual International Symposium on Computer Architecture, pages 354–365. ACM, June 2006.

[24] R. D. Van Meter III. *Architecture of a Quantum Multicomputer Optimized for Shor's Factoring Algorithm*. PhD thesis, Keio University, 2006. available as arXiv:quant-ph/0607065.

[25] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri. Experimental verification of the feasibility of a quantum channel between Space and Earth. *New Journal of Physics*, 10:033038, 2008.

[26] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802, Oct. 1982.

[27] Z. Zhao, T. Yang, Y. Chen, A. Zhang, and J. Pan. Experimental realization of entanglement concentration and a quantum repeater. *Physical Review Letters*, 90(20):207901, 2003.