# Quantum Networks: From Quantum Cryptography to Quantum Architecture

Tatjana Curcic and Mark E. Filipkowski
Booz Allen Hamilton, 3811 North Fairfax Drive, Suite 1000, Arlington, Virginia, 22203

Almadena Chtchelkanova
Strategic Analysis, Inc., 3601 Wilson Boulevard, Suite 500, Arlington, Virginia, 22201

Philip A. D'Ambrosio
Schafer Corporation, 3811 North Fairfax Drive, Suite 400, Arlington, Virginia, 22203

Stuart A. Wolf, Michael Foster, and Douglas Cochran
Defense Advanced Research Projects Agency, 3701 North Fairfax Drive, Arlington, Virginia, 22203

## ABSTRACT
As classical information technology approaches limits of size and functionality, practitioners are searching for new paradigms for the distribution and processing of information. Our goal in this Introduction is to provide a broad view of the beginning of a new era in information technology, an era of quantum information, where previously underutilized quantum effects, such as quantum superposition and entanglement, are employed as resources for information encoding and processing. The ability to distribute these new resources and connect distant quantum systems will be critical. We present an overview of network implications for quantum communication applications, and for quantum computing. This overview is a selection of several illustrative examples, to serve as motivation for the network research community to bring its expertise to the development of quantum information technologies.

## 1. INTRODUCTION
The past century has been influenced tremendously by both quantum mechanics and information technology. Quantum effects are pervasive in technology, central to functioning of many ubiquitous devices today, such as lasers, integrated circuits, fluorescent lights, and magnetic resonance imaging (MRI) machines, to name a few. Following the development of ARPANET under DARPA's sponsorship in the '60s, we have witnessed an explosive growth of information technology. Integrated circuits and the internet have changed our lives. If the last century was the era of quantum mechanics and information technology, the 21st century will be an era of quantum information, where previously underutilized quantum effects, such as quantum superposition and entanglement, will be essential resources for information encoding and processing. The ability to distribute these new resources and connect distant quantum systems will be critical. In this paper we present a brief overview of network implications for quantum communication applications, such as cryptography, and for quantum computing. This overview is not meant to be exhaustive. Rather, it is a selection of several illustrative examples, to serve as motivation for the network research community to bring its expertise to the development of quantum information technologies.

## 2. QUANTUM COMMUNICATION
### 2.1 Quantum Cryptography
Novel quantum systems that manipulate, store and transmit information based on laws of quantum mechanics are now being explored in many physical systems at the level of individual atoms, photons, and electrons. Quantum effects such as entanglement and superposition of quantum states, the no-cloning theorem, non-locality principles, etc. are exploited in quantum cryptography, quantum communication, and quantum computation. The most mature of all quantum information technologies, quantum cryptography [21], takes advantage of the no-cloning property [30] of quantum states to implement unbreakable secure cryptosystems.

To ensure that communications are secure, two parties exchanging sensitive information over an insecure communication channel must use a cryptographic protocol. The sending party has to use a cryptographic key to encode the information (encryption) and the receiving party has to use a key to decode the information (decryption). If a third party acquires the decoding key, he/she will be able to decode the information. There are two distinct ways to distribute the keys – *private* and *public*. In *private,* or *symmetrical,* key cryptosystems the parties have to share a secret key before they send and receive a message. If the key is the same length as the message, randomly generated every time, and is used only once, that cryptographic algorithm is called the *one-time pad* or *Vernam cipher,* the only existing provably secure cryptosystem at this time. Modern *public* or *asymmetrical* key cryptographic systems are based on two matching keys – a public

key, accessible by anyone, and a private key. Only the owner of the private key can easily decrypt a message encrypted with the public key. The security of this system is based on the difficulty of calculating the inverse of so-called "one-way" functions, where computational complexity grows exponentially with the number of bits in the key (e.g., factoring of large numbers).

The usefulness of private key cryptosystems is limited by the need for secure *key distribution*, whether through a trusted communication channel or courier. When classical communication channels are used to exchange a private key, an eavesdropping third party may be able to copy the key without being detected. Quantum key distribution, or QKD, takes advantage of the basic quantum mechanical principles that the measurement of a quantum state of a system, in general, changes its state, and that unknown quantum states cannot be copied (the no-cloning theorem). When exchanging quantum information, the two communicating parties are able to determine if the quantum channel is compromised by a third party before they start the key transmission. They repeat the test process until they find a secure quantum channel over which they can safely exchange the secret key. Thus the implementation of Vernam ciphers using QKD will make a truly unbreakable *practical* cryptosystem for transmitting classical messages, combining the unbreakability of the one-time pad with the ease of key distribution of public key systems. Since the first QKD protocol was discovered in 1984 [3], commonly referred to as BB84 after its authors Bennett and Brassard, a number of different protocols have been developed for secure quantum key distribution [21].

In modern *public* or *asymmetrical* key cryptographic systems, such as RSA [34] (named after its inventors, R. Rivest, A. Shamir, L. Adelman), the key distribution scheme is based on the intractability of the factorization of large numbers. Such systems rely on the assumption of limited processing power of conventional computers as well as the conjectured computational complexity of the algorithms required to break the encryption keys to provide a level of protection that, while perishable, is thought to be secure for a sufficient length of time to safeguard sensitive messages. Over the past several years there has been a continuous improvement in computational techniques, which has led to the successful cracking of successively longer keys [41]. As computing power increases, and new classical computational techniques are developed, the length of time that a message can be considered secure will decrease, and numerical keys will no longer be able to provide acceptable levels of secure communication.

An additional threat to existing public key cryptosystems is *Shor's algorithm* [35], which relies on the laws of quantum mechanics to provide enhanced capabilities for a class of problems that includes number factoring. It is expected that Shor's algorithm, when executed on a quantum computer, will be able to factor large numbers in polynomial time, i.e. exponentially faster than a conventional computer. While any practical application may be decades away, an experimental proof-of-concept of Shor's algorithm has successfully been achieved [40]. The implication of quantum information science for secure communications is therefore twofold: While Shor's algorithm potentially renders widely used RSA encryption scheme vulnerable, QKD can counter its effects by offering provably secure communication between two parties.

Various QKD protocols have been implemented either through fiber or free space. Most of those implementations are point-to-point links. Recently, researchers from BBN Technologies, Harvard University and Boston University have built a six-node QKD network within the metropolitan Boston area [1]. The network is fully compatible with today's internet technologies. Any node in the network can act as a relay to connect two other nodes, and it contains an optical switch that can change the way the nodes are connected.

A quantum network provides a way of distributing private keys in conjunction with public or private internet networks employing internet protocol suites. The current internet security protocol, IPSec, specifies protocols, algorithms, databases and policies required for secure communications. To incorporate QKD into an internet security protocol one must implement an interface between existing internet protocols and QKD channel protocols used for key distribution [19]. In current implementations of point-to-point QKD two communicating entities must be connected by a direct link providing a path for the photons between them. This is achieved by either an optical fiber connection or, for free-space communications, a direct line of sight. A cryptographic gateway consists of a source suite and a detection suite, each composed of many optical and electronic devices connected by a "quantum channel". The throughput of the system depends on the quality of single photon sources and detectors, and the communication channel. QKD point-to-point links have been demonstrated over distances up to 150 km for fiber-based systems [36, 24], and 23 km in free-space [23, 26]. The recent free-space QKD demonstration between two peaks in the Alps [26] is an important step towards accomplishing a satellite-based global key-distribution system. Researchers at the National Institute of Standards and Technology (NIST) recently demonstrated QKD over free-space at 1.0 Mbps [7]; this figure represents a significant breakthrough in key distribution bit rates.

In current implementations of QKD, pseudo single-photon sources such as attenuated laser pulses or photon pairs generated by parametric downconversion are used. The efficiency of these two techniques is low. The result is a significant reduction of the bit rate. Even though experimental demonstrations of QKD employing these techniques have been achieved, true on-demand single photon sources are desired in order to make QKD efficient and unconditionally secure. Development of single photon sources is currently being pursued by many research groups in various physical systems, such as semiconductor structures [33, 45] color centers in diamond [6], and cavity quantum electrodynamics [25,29].

The quantum channel carries information encoded in the state of a *single* quantum system, a single photon, as opposed to classical communications where many photons carry the same information. In current implementations of QKD single-mode telecom or specialized (ultra-low-loss) fiber [37], or a free-space line of sight link are used as the quantum channel. In telecom fiber transmission losses, birefringence effects, chromatic dispersion and polarization mode dispersion lead to exponential decay of the signal and as a result to reduced bit rate. Free-space links are also affected by drawbacks such as ambient light, atmospheric conditions, beam divergence, etc. Continuous improvement in telecom fibers is critical, to ensure that many of the loss mechanisms listed above are minimized in the future.

Another important part of a quantum cryptography system is single photon detection. Current implementations use a variety of techniques such as avalanche photo-diodes (APDs), photo-multipliers, multichannel plates, and superconducting Josephson junctions. Unfortunately, none of the existing approaches can provide high quantum detection efficiency over a broad spectral range, a small dark count, good timing resolution and small dead (recovery) time, all required for fast and reliable QKD. Improvement of single photon detectors is the subject of active current research.

## 2.2 Quantum Repeaters

An essential component for long-distance quantum communication is a quantum repeater. The challenge is to repeat an arbitrary quantum signal while preserving its quantum nature, which cannot be accomplished using classical methods of amplification. This can be achieved, however, using shared distant entanglement, which enables teleportation of an arbitrary quantum state [4]. There are two key issues with distributing photon entanglement over long distance: (1) photon absorption in the fiber, which is exponential with the channel length, and (2) degradation of the fidelity [30] of the quantum state of a photon due to decoherence, which is also exponential with length. In one scheme for a quantum repeater [11], the quantum channel is divided into segments whose length is determined by the absorption length of the fiber, to address the absorption issue. The segments are connected by nodes that are simple "quantum processors" consisting of a few quantum bits, or *qubits*, which can store the quantum states of qubits, and perform quantum operations that preserve the entanglement, so that it can be transferred from segment to segment. The fidelity issue is addressed by adding an entanglement purification protocol [5], both locally, at each node, and with a global protocol called nested entanglement purification. Some of the most challenging implementation issues include realization of robust quantum memory, and quantum state transfer from photons to material qubits in which quantum information can be stored. There are experimental efforts currently under way to demonstrate some of the essential components of a quantum repeater, such as the quantum interface between photons and material qubits [42]. A recent demonstration of high-fidelity teleportation of photons in optical fiber across the Danube in Vienna is another important step towards the implementation of a quantum repeater [38].

Recently, a novel scheme for a quantum repeater was proposed using atomic ensembles and linear optics [16]. This scheme has built-in entanglement purification and resilience to realistic noise. The communication efficiency in this scheme scales polynomially with the channel length, allowing for long-distance quantum communication. The approach involves laser manipulation of atomic ensembles, beam splitters, and single-photon detectors with moderate efficiencies, and is therefore compatible with current technology. Some ingredients of the scheme have already been demonstrated experimentally [27, 39], but a realization of a complete physical system has not yet been attained.

## 2.3 Commercialization of Quantum Communication Tools

Quantum communication systems and networks are starting to enter the commercial world. In addition to research in government, university and industry labs there are a few private companies, including MagiQ (US), ID Quantique (Switzerland), and Qinetiq (UK), that are commercializing QKD and related products. As previously noted, BBN recently demonstrated the first quantum network with multiple nodes. While there is promise of extending the range of such quantum networks, secure connectivity across much longer distances is dependent on the research challenges discussed above.

# 3. QUANTUM COMPUTING

## 3.1 Networking Quantum Computers

The utility of quantum networks goes well beyond secure communication applications. Ultimately, one can envision a future "quantum internet" which consists of quantum computers (nodes) connected by classical and quantum communication channels. Each node in the network stores *quantum* information qubits, and processes this information locally using quantum gates. Information is exchanged between the nodes via quantum and classical channels. Typically, storage and processing of quantum information are physically implemented in *material* qubits, such as trapped ions or atoms, electron or nuclear spins, or Josephson junction superconducting qubits. Transfer of quantum information over a distance is best realized via "*flying*" qubits, for example, polarization states of photons. A key component of such a network is a quantum interface between stationary and flying qubits, i.e., conversion of the quantum state of the stationary qubit into that of a flying qubit, and the inverse, with high fidelity. The first theoretical proposal for realizing quantum state transfer between stationary and flying qubits and entanglement distribution among distant nodes was put forth in 1997 [14]. In this scheme, trapped neutral atoms provide quantum memory at each node of the network, and optical cavity quantum electrodynamics (QED) is utilized both to perform quantum operations and to transfer quantum information between nodes. This approach is being pursued experimentally in the Caltech MURI Center for Quantum Networks [28]. In their implementation, the Caltech team is exploring a new technical paradigm for cavity QED based on magnetic microtraps and optical photonic bandgap structures, which are amenable to integration. Another group, at the University of Michigan, has recently achieved an experimental breakthrough: they have demonstrated entanglement between a single trapped atom and a single photon [8]. In the case of solid-state technologies, a recent theoretical proposal considers a scheme for coupling electron spins in semiconductor quantum dots with photons in a fiber (or a waveguide) via microcavities (or micro-rings) [43].

Although stand-alone quantum processors that would perform calculations not possible with conventional computers are still in the distant future, quantum processors with a few qubits could be achieved in the next few years. A quantum network of such processors would enable distributed quantum computation. A "distributed quantum computer" is a multiprocessor device where each processor would contain only a small number of qubits, but the processors would work together via the quantum network to effectively simulate a larger computer. The interaction between qubits on different processors can be implemented by physically transporting qubits back and forth, or by teleporting the qubit state from one node onto another, followed by local operations. Eisert and coworkers have theoretically established optimal implementations of quantum gates between qubits that are located in different nodes of the distributed quantum computer, so-called non-local gates [17]. The resources required for non-local gates

are previously shared entanglement between nodes and local operations and classical communication (LOCC). Using this computational paradigm, it has recently been shown that Shor's quantum factoring algorithm can be implemented on a distributed quantum network model without changing the complexity class of the problem, although with an additional overhead [44]. Whether this would make cracking RSA codes possible sooner than previously thought is still an open question, due to the challenges associated with connecting small quantum processors. Even without the ability to implement non-local operations one can, in theory, achieve a quadratic speedup for the task of appointment-scheduling between distant parties, compared to the best classical algorithm [12, 22]. This quantum scheduling algorithm requires only a distributed search with the qubits being transferred between the nodes, again raising the possibility of useful quantum computation before full-up processors are available.

Taking this idea a step further, quantum information processing, together with quantum networks, can be used for practical purposes even before we have several-qubit quantum processors available — in quantum games. Quantum games might have an economic or social impact, as in provisioning for public goods, or a political impact, as in voting. In a general game situation, a collection of players have a set of shared information, both private and public, and a set of rules for making decisions. A trusted third party is often needed to enforce the rules. If the players share entangled qubits, however, then they have a greater number of strategies to choose from than in classical games. A group at Hewlett Packard Laboratories has utilized quantum strategies to create a practical quantum mechanism for the public goods game [13]. Their recent quantum algorithm offers a solution to the free-rider problem in the n-player public goods game, without the need of third party enforcement or repeated play. This potentially economically significant algorithm requires only two-particle entanglement distributed among the players, which is technologically feasible in the near future. The field of quantum games is still in its infancy and is likely to grow at a steady pace, thus opening prospects for more applications for quantum networks.

There remain many technical difficulties and challenges related to quantum networks and quantum computation. Although it is not within the scope of this paper to address these challenges in depth, it is worthwhile listing some of them. Almost all of the aforementioned applications of quantum networks rely on shared entanglement between nodes. While the quantum optics community has been generating two-photon entanglement using parametric downconversion for some time [18], we are still faced with the problem of practical, reliable, fast, on-demand entanglement sources. Distribution of entangled photon pairs among nodes is also problematic: entanglement purification will likely be needed for most applications [9], and for long-distance scenarios one will need quantum repeaters. Then there is the difficulty of implementing a quantum interface between stationary and flying qubits. As noted above, this is one of the fundamental obstacles to quantum network implementations. Finally, before we can have distributed quantum computers using quantum networks, we still need to be able to build processors consisting of several logical qubits, and demonstrate quantum error correction.

## 3.2 Quantum-Computer Architecture

Another area where networking can play an important role concerns interconnects in a quantum processor, i.e., "networking" qubits on a quantum chip. Quantum computing derives its power from a number of unique algorithmic elements made available by the quantum mechanical nature of the qubit. The primary goal of quantum architecture, just as is the case with classical architecture, is to determine the best way to assemble the available hardware primitives, such as qubits, into a network that can implement such algorithmic capabilities. An important example is *quantum parallelism*: N qubits can encode $2^N$ binary numbers *simultaneously*. An *oracle*, a quantum-mechanical unitary operator that encodes a mathematical function, can operate on all $2^N$ numbers simultaneously, and thus calculate the value of this function for $2^N$ input values simultaneously.

In principle, in order to implement such features of quantum computing, it must be possible to arbitrarily entangle all possible subsets of the qubits that comprise the quantum processor. This means it must be possible to interact a given qubit with all other qubits in the processor, including those that are physically nonadjacent. Interacting arbitrary nonadjacent qubits in a scalable fashion may be the single greatest challenge of quantum architecture. Proposed schemes make use of flying qubits, quantum teleportation, and non-local gates [10, 31] to form the required network of qubits. In the context of architecture, the term "quantum wires" is often used to denote such quantum data pathways [32, 15].

For some of the hardware primitives that are being considered to serve as qubits, it may be much easier to create interactions between nearest neighbors than between nonadjacent qubits. "Swap chains", in which the states of adjacent qubits are entangled and then swapped until the desired states are brought into contact, have been shown to involve an impractically large temporal overhead [15]. Fowler et al. have developed an approach to implementation of Shor's algorithm on one-dimensional chains of qubits using only nearest neighbor interactions, with efficiency comparable to the general (i.e., arbitrary interaction) case [20], although quantum error correction has yet to be investigated in this implementation. Alternatively, as discussed above, it may be possible to create a quantum computer using a distributed approach. In this scheme, small clusters of nearest neighbor interacting qubits would form efficient, localized processors. Then, by some means, the localized processors would be interconnected using flying qubits, quantum teleportation, or non-local gates.

A fundamental aspect of quantum computing is that the interactions between qubits will, at some level, involve intervention by classical bits; i.e., the quantum computer will be controlled by a classical computer. Thus, in order to develop a functioning and useful quantum computer one will, of necessity, need to address classical-to-quantum networking issues as well. The precise form of this classical control, and at what level it will occur is unclear at present. If the quantum computer is composed of quantum adders or multipliers [2], then the classical bits may be required to determine the action within the adders or multipliers ("add one", "add zero", etc.). Alternatively, the classical bits may be asked to configure the qubit network in an optimized way, determined by analysis of the required number-theoretic results on the classical computer. The optimized interactions between qubits would be implemented analogous to a

field-programmable gate array, in which the gates are quantum mechanical and the programming takes place classically. With such fundamental questions remaining open, it is clear that quantum architecture is in its infancy.

## 4. CONCLUSION

Realization of practical quantum information technologies cannot be accomplished without involvement of the network research community. Network expertise is required not only to address fundamental problems in quantum communication applications, but also in quantum computing, from the basic form of quantum information processor architecture to the possibility of distributed quantum computing. As the quantum information community advances from fundamental demonstrations of a few coupled qubits in various physical implementations, it will be essential for further progress in quantum information technologies to develop a synergistic community of physicists, computer scientists, network engineers, and systems engineers who will amass their expertise to bring about the next technological revolution.

## 5. REFERENCES


[1] BBN Press release, 3 June 2004.

[2] Beckman, D., Chari, A. N., Devabhaktuni, S., and Preskill, J. Efficient networks for quantum factoring. *Phys. Rev. A* **54**, 1034, 1996.

[3] Bennett, C. H. and Brassard G. Quantum cryptography: Public key distribution and coin tossing. *Proc. of IEEE Int. Conference on Computers, Systems and Signal Processing*, 175, IEEE, New York, 1984.

[4] Bennett, C. H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A., and Wootters, W. K. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895, 1993.

[5] Bennett, C. H., Brassard, G., Popescu, S., Schumacher, B., Solin, J. A., and Wootters, W. K. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **76**, 722, 1996.

[6] Beveratos, A., Kühn, S., Brouri R., Gacoin, T., Poizat, J. P., and Grangier, P. Room temperature stable single photon source. *Eur. Phys. J.* D **18,** 191, 2002.

[7] Bienfang, J. C., Gross, A. J., Mink, A., Hershman, B. J., Nakassis, A., Tang, X., Lu, R., Su, D. H., Clark, C. W., Williams, C. J., Hagley, E. W., and Wen J. Quantum key distribution with 1.25 Gbps clock synchronization. *Optics Express* **12**, 2011, 2004.

[8] Blinov, B. B., Moehring, D. L., Duan, L.-M., and Monroe, C. Observation of entanglement between a single trapped atom and a single photon. *Nature* **428**, 153, 2004.

[9] Bouwmeester, D., Ekert, A., and Zeilinger, A. (Eds.) The physics of quantum information. Springer-Verlag Berlin, 2000.

[10] Brennen, G. K., Daegene, S., and Williams, C. J. Quantum-computer architecture using non-local interactions. *Phys. Rev. A* **67**, 50302, 2003.

[11] Briegel, H.-J., Dür, W., Cirac, J. I., and Zoller, P. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932, 1998.

[12] Buhrman, H., Cleve, R., and Wigderson, A. Quantum vs. classical communication and computation. *Proc. 30th ACM Symposium on Theory of Computing (STOC)*, 63, 1998.

[13] Chen, K.-Y., Hogg, T., and Beausoleil, R. A practical quantum mechanism for the public goods game. E-print quant-ph/0301013, 2003, http://arxiv.org/PS_cache/quant-ph/pdf/0301/0301013.pdf

[14] Cirac, J. I., Zoller, P., Kimble, H. J., and Mabuchi, H. Quantum state transfer and entanglement distribution among distant nodes in a quantum network. *Phys. Rev. Lett.* **78**, 3221, 1997.

[15] Copsey, D., Oskin, M., Impens, F., Metodiev, T., Cross, A., Chong, F. T., Chuang, I. L., and Kubiatowicz, J. Toward a scalable, silicon-based quantum computing architecture. *IEEE Journal of Selected Topics in Quantum Electronics* **9,** 1552, 2003.

[16] Duan, L.-M., Lukin, M. D., Cirac, J. I., and Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414**, 413, 2001.

[17] Eisert, J., Jacobs, K., Papadopoulos, P., and Plenio, M. B. Optimal local implementation of non-local quantum gates. *Phys. Rev. A* **62**, 052317, 2000.

[18] Ekert, A. K., Rarity, J. G., Tapster, P. R., and Palma, G. M. Practical quantum cryptography based on two-photon interferometry. *Phys. Rev. Lett.* **69**, 1293, 1992.

[19] Elliott, C. Building the quantum network. *New Journal of Physics* **4**, 46.1, 2002.

[20] Fowler, A. G., Devitt, S. J., and Hollenberg, L. C. L. Implementation of Shor's algorithm on a linear nearest neighbour qubit array. E-print quant-ph/0402196, 2004, http://arxiv.org/PS_cache/quant-ph/pdf/0402/0402196.pdf

[21] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., Quantum cryptography. *Rev. Mod. Phys.* **74**, 41, 2002.

[22] Grover, L. K. An improved quantum scheduling algorithm. E-print quant-ph/0202033, 2002, http://arxiv.org/PS_cache/quant-ph/pdf/0202/0202033.pdf

[23] Hughes, R. J., Nordholt, J. E., Derkacs, D., and Peterson, C. G. Practical free-space quantum key distribution over 10 km in daylight and at night. *New J. Phys.* **4**, 43.1, 2002.

[24] Kimura, T., Nambu, Y., Hatanaka, T., Tomita, A., Kosaka, H., and Nakamura, K. Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography. E-print quant-ph/0403104, 2004, http://arxiv.org/ftp/quant-ph/papers/0403/0403104.pdf

[25] Kühn, A., Hennrich, M., and Rempe, G. Deterministic single-photon source for distributed quantum networking. *Phys. Rev. Lett.* **89**, 067901, 2002.

[26] Kurtsiefer, C., Zarda, P., Halder, M., Weinfurter, H., Gorman, P. M., Tapster, P. R., and Rarity, J. G. A step towards global key distribution. *Nature* **419**, 450, 2002.

[27] Kuzmich, A., Bowen, W. P., Boozer, A. D., Boca, A., Chou, C. W., Duan, L.-M., and Kimble, H. J. Generation of nonclassical photon pairs for scalable quantum communication with atomic ensembles. *Nature* **423**, 731, 2003.

[28] Mabuchi, H., Armen, M., Lev, B., Loncar, M., Vu_kovi_, J., Kimble, H. J., Preskill, J., Roukes, M. L., and Scherer, A. Quantum networks based on cavity QED. *Quantum Information and Computation* **1**, Special Issue 7, 2001.

[29] McKeever, J., Boca, A., Boozer, A. D., Miller, R., Buck, J. R., Kuzmich, A., and Kimble, A. J. Deterministic generation of single photons from one atom trapped in a cavity. *Science* **303**, 1992, 2004.

[30] Nielsen, M. A. and Chuang, I. L. Quantum computation and quantum information. Cambridge University Press, 2000.

[31] Oskin, M., Chong, F. T., and Chuang, I. L. A practical architecture for reliable quantum computers. *IEEE Computer* **35,** 79, 2002.

[32] Oskin, M., Chong, F. T., Chuang, I. L., and Kubiatowicz, J. Building quantum wires: the long and the short of it. *ISCA 2003: 30th International Symposium on Computer Architecture*, 374, 2003.

[33] Pelton, M., Santori, C., Vu_kovi_, J., Zhang, B., Solomon, G. S., Plant, J., and Yamamoto, Y. Efficient source of single photons: A single quantum dot in a micropost microcavity. *Phys. Rev. Lett.* **89**, 233602, 2002.

[34] Rivest, R., Shamir, A., and Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* **21**, 120, 1978.

[35] Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Computing* **26**, 1484, 1997.

[36] Stucki, D., Gisin, N., Guinnard, O., Ribordy, G., and Zbinden, H. Quantum key distribution over 67 km with a plug & play system. *New J. Phys.* **4**, 41, 2002.

[37] Temelkuran, B., Hart, S. D., Benoit, G., Joannopoulos, J. D., and Fink, Y. Wavelength-scalable hollow optical fibres with large photonic bandgaps for $CO_2$ laser transmission. *Nature* **420**, 650, 2002.

[38] Ursin, R., Jennewein, T., Aspelmeyer, M., Kaltenbaek, R., Lindenthal, M., Walther, P., and Zeilinger, A. Quantum teleportation across the Danube. *Nature* **430**, 849, 2004.

[39] van der Wal, C. H., Eisaman, M. D., Andre, A., Walsworth, R. L., Phillips, D. F., Zibrov, A. S., and Lukin, M. D. Atomic memory for correlated photon states. *Science* **301**, 196, 2003.

[40] Vandersypen, L., Steffen, M., Breyta, G., Yannoni, C., Sherwood, M., and Chuang, I. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* **414,** 883, 2001.

[41] Weisstein, Eric W. http://mathworld.wolfram.com/news/2003-12-05/rsa/

[42] Yablonovitch, E., Jiang, H., Kosaka, H., Robinson, H., Rao, D., and Szkopek, T. Optoelectronic quantum telecommunications based on spins in semocinductors. *Proceedings of the IEEE* **91**, 761, 2003.

[43] Yao, W., Liu, R.-B., and Sham, L. J. Theory of control of spin/photon interface for quantum networks. E-print quant-ph/0407060, 2004, http://arxiv.org/PS_cache/quant-ph/pdf/0407/0407060.pdf

[44] Yimsiriwattana, A. and Lomonaco Jr., S. J. Distributed quantum computing: A distributed Shor algorithm. E-print quant-ph/0403146, 2004, http://arxiv.org/PS_cache/quant-ph/pdf/0403/0403146.pdf

[45] Yuan, Z., Kardynal, B. E., Stevenson, R. M., Shields, A. J., Lobo, C. J., Cooper, K., Beattie, N. S., Ritchie, D. A., and Pepper, M. Electrically driven single photon source. *Science* **295,** 102, 2002.