Proceedings Symposium IEEE/LEOS Benelux Chapter, 2005, Mons

Protocols for Quantum Communication

S. Massar

Laboratoire d'Information Quantique and QUIC, C.P. 165/59, Université Libre de Bruxelles,
50 Av. F.-D. Roosevelt, B-1050 Bruxelles, Belgium

We show how the techniques developed for long distance quantum key distribution in optical fibers can be used to demonstrate other quantum information processing and communication protocols. We present a fiber optics realization of the Deutsch-Jozsa and Bernstein-Vazirani algorithms. We describe a method, called "error filtration", for reducing errors in quantum communication channels, and present an experimental implementation thereof. We discuss the cryptographic primitive of string flipping, and present an experimental implementation which has higher security than achievable using any classical protocol.

Introduction

The field of quantum information is based upon the idea that one should use the specific features of quantum mechanics to carry out information processing tasks that are impossible classical. Some of the landmarks in this field were the realization in 1984 by Bennett and Brassard that quantum mechanics could be used for secure cryptography[1] -technically called Quantum Key Distribution (QKD)- and the first quantum algorithm proposed in 1985 by Deutsch[2]. The 1990's saw many significant discoveries -described for instance in [3]-, such as quantum teleportation, quantum error correction and entanglement purification, a quantum algorithm that solves a problem of practical interest (Shor's factoring algorithm), the first realistic proposals for building a quantum computer, etc... Since then the field has progressed significantly, both from the theoretical and practical aspects.

The most advanced application is undoubtedly QKD. This is because QKD requires that only a single photon be manipulated, which is much easier than most other applications of quantum information. There are at present two startup's that commercialize quantum cryptography systems, and several multinational companies are actively involved in R & D on quantum key distribution. Nowadays quantum cryptography can reach ranges of over 100km[4, 5].

In the work reported here we show how the "plug and play" system[6] developed for long distance QKD can be adapted for use in other quantum information tasks. We present applications to quantum algorithms, quantum error detection, and quantum string flipping. These works show that the plug and play system can be used for many applications other than QKD.

Fiber optics implementation of Deutsch-Jozsa and Bernstein-Vazirani algorithms

Deutsch's algorithm [2] and its extensions by Deutsch and Jozsa [7] and Bernstein and Vazirani[8, 9] belong to the class of "oracle" based algorithms. An oracle is a black box, which given an input $\mathbf{x} = x_1 x_2 \ldots x_n$ consisting of n bits, computes a single bit, the function $f(\mathbf{x})$. The aim is to learn some property of f with as few queries to the oracle as possible.

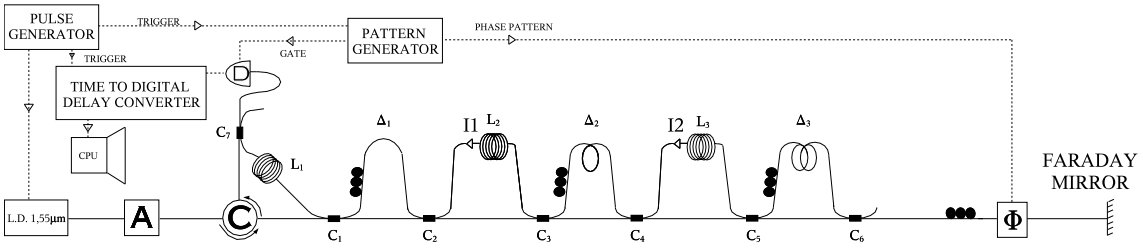

Figure 1: Experimental setup for the fiber optics realization of the Deutsch-Jozsa and Bernstein-Vazirani algorithms. L.D. Laser Diode, A Attenuator, C Circulator, $C_1 \ldots C_7$ Couplers, $I_1 I_2$ Isolators, $L_1 L_2 L_3$ delay lines, Φ Phase Modulator, D Photon Counter

The Deutsch-Jozsa and Bernstein-Vazirani problems require $2^{n-1}+1$ and n calls to the oracle respectively when classical computers are used, but only a single query when a quantum computer is used.
In [10] we reported on a fiber optics implementation of the Deutsch-Jozsa and Bernstein-Vazirani algorithms with quantum states of dimension 8, corresponding to 3 qubits. The experimental setup is described in Fig. 1. It is realized at telecommunication wavelengths (1.55μm) using standard fibers (SMF28). The protocol starts by producing a short laser pulse. The pulse is then sent through 3 unbalanced Mach-Zehnder interferometers, with path length differences Δ_1, $\Delta_2 \simeq 2\Delta_1$, $\Delta_3 \simeq 4\Delta_1$. This realizes an equal superposition of 8 time bins. The action of the oracle is implemented by a phase modulator Φ which puts a pattern of 0 or π phases on the successive time bins. The 8 pulses are then reflected by the Faraday mirror, and pass a second time through the 3 Mach-Zehnder interferometers. The time of arrival of the pulse is recorded using a single photon detector. The time of arrival encodes the result of the measurement. We checked that this implementation reproduces well the predictions of the Deutsch-Jozsa and Bernstein-Vazirani algorithms, with visibilities of approximately 97%.

Error Filtration

One of the major advances in quantum information is that one can in principle correct errors that occur in quantum memories[11], in quantum communication[12], and in quantum computers. However it is very difficult to implement these ideas in practice because they require multi particle interactions, and only a few proof of principle laboratory demonstrations have been realized. An alternative method, called *error filtration*, allows errors to be filtered out during quantum communication, and can in contrast be easily implemented using present technology [13]. The main idea of error filtration is to encode one qubit in a single particle within a Hilbert space of dimension greater than two. It is then possible, using a simple interferometer, to detect with high probability whether a phase error has occurred, and, if so, to discard the state. This quantum error detection scheme is less powerful than full error correction, but for many applications such as quantum key distribution (QKD) discarding the state affected by noise is sufficient.
In order to implement error filtration one constructs an equal superposition of the different basis states. After the noise has acted one lets the different basis states interfere, and uses only the state in which there is constructive interference. If the noise acting on the different basis states is independent, it will have a tendency to average out in the

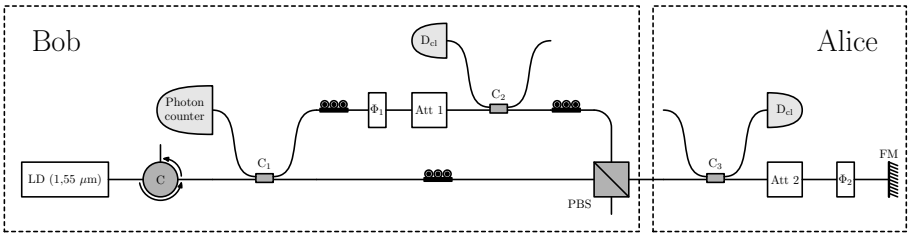

Figure 2: Experimental setup for quantum string flipping. D_{cl} Classical Detector, PBS Polarizing Beam Splitter, FM Faraday Mirror, Att Attenuator, $C_1C_2C_3$ Couplers

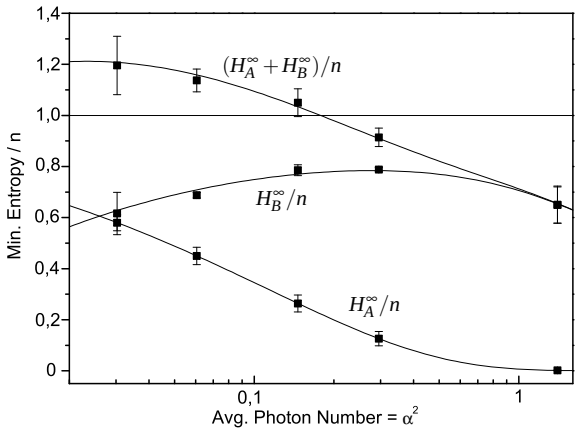

Figure 3: Results for the quantum string flipping experiment as a function of the mean number of photons sent from Alice to Bob. Classically $H_A^\infty + H_B^\infty$ is always less then n.

constructive output. The net effect is to reduce the noise at the expense of intensity.
In our implementation of error filtration [14], a 4 dimensional state, corresponding to 4 time bins propagating in optical fibers, is produced using 2 unbalanced Mach-Zehnder interferometers. A single qubit is encoded in this 4 dimensional space. During propagation the qubit is affected by noise. The decoding and measurement operations are performed by sending a second time the 4 time bins through the 2 unbalanced Mach-Zehnder interferometers. Finally the output path and time of arrival is measured using a single photon detector. This allowed us to realize the optical part of a QKD scheme in an environment too noisy to implement the standard BB84 protocol. Using error filtration the amount of noise was reduced and the BB84 protocol was rendered secure.

String Flipping

Coin tossing is a cryptographic primitive in which 2 parties which do not trust each other want to choose a random bit. String flipping is a generalization in which the two mistrustful parties want to choose a string of n random bits. If both parties are honest, then the probability of each string $\mathbf{c} = c_1c_2\ldots c_n$ is 2^{-n}. If party A (B) is dishonest, we denote by $2^{-H_{A(B)}^\infty}$ the probability that he can force the outcome to be $\mathbf{c}$. If the parties only have a classical communication channel, then one can show that $H_A^\infty + H_B^\infty \leq n$. On the other

hand if the parties use a quantum communication channel, and if a dishonest party wants to the probability that he is caught cheating to be small, then $H_A^\infty + H_B^\infty$ can be kept arbitrarily close to $2n$: under this condition a cheater can only very slightly influence the outcome of the string flipping.
In [15] we reported on a fiber optics implementation of string flipping. The experimental setup is illustrated in Fig. 2. It uses techniques very similar to those used for long distance QKD, and is therefore suitable for long distance implementation over telecom fibers. In the experiment we were able to ensure that $H_A^\infty + H_B^\infty > n$, see Fig. 3. Thus the experiment generated strings more random than could be obtained using any classical protocol.

I would like to thank all my collaborators who helped in the realization of the work reported here. We acknowledge financial support by project IAP-V-18 of the Belgian Federal Government, ARC00/05-251 of the Communauté Française de Belgique, and RESQ IST-2001-37559 of the IST-FET program of the EU.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175-179, IEEE, New York, 1984. Bangalore, India, December 1984.

[2] D. Deutsch, "Quantum theory, the Church-Turing Principle and the universal quantum computer", *Proc. R. Soc. Lond. A*, vol. 400, 97 (1985)

[3] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press, 2004

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

[5] C. Gobby, Z. L. Yuan, A. Shields, "Quantum key distribution over 122km of standard telecom fiber", *Appl. Phys. Lett.*, vol. 84, 3762-3764, 2004

[6] G. Ribordy, J-D. Gautier, N. Gisin, O. Guinnard and H. Zbinden, "Automated "plug & play" Quantum Key Distribution", *Elect. Lett.*,vol. 34, pp. 2116 - 2117, 1998

[7] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation", *Proc. R. Soc. Lond. A*, vol. 439, 553 (1992)

[8] E. Bernstein and U.V. Vazirani, "Quantum complexity theory", *SIAM J. Comput.*, vol. 26, 1411, 1997

[9] B. M. Terhal1 and J. A. Smolin, "Single quantum querying of a database", *Phys. Rev. A*, vol. 58, 1822 - 1826 (1998)

[10] E. Brainis, L.-P. Lamoureux, N. J. Cerf, Ph. Emplit, M. Haelterman, and S. Massar, "Fiber-Optics Implementation of the Deutsch-Jozsa and Bernstein-Vazirani Quantum Algorithms with Three Qubits", *Phys. Rev. Lett.*, vol. 90, 157902 (2003)

[11] P. Shor, "Scheme for reducing decoherence in quantum computer memory", *Phys. Rev. A*, vol 52, 2493, 1995

[12] C. H. Bennett, et al., "Purification of noisy entanglement and faithful teleportation via noisy channels", *Phys. Rev. Lett.*, vol 76, 722, 1996

[13] N. Gisin, N. Linden, S. Massar, S. Popescu, "Error filtration and entanglement purification for quantum communication", *Phys. Rev. A*, vol. 72, 012338 (2005)

[14] L.-P. Lamoureux, E. Brainis, N. J. Cerf, Ph. Emplit, M. Haelterman, and S. Massar, "Experimental Error Filtration for Quantum Communication Over Highly Noisy Channels", *Phys. Rev. Lett.*, vol. 94, 230501, 2005

[15] L. P. Lamoureux, E. Brainis, D. Amans, J. Barrett, and S. Massar, "Provably Secure Experimental Quantum Bit-String Generation", *Phys. Rev. Lett.*, vol. 94, 050503, 2005

[16] J. Barrett and S. Massar, in preparation, 2005