PERGAMON

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Acta Astronautica 57 (2005) 224–229

ACTA ASTRONAUTICA

www.elsevier.com/locate/actaastro

Using quantum computing algorithms in future satellite communication

Laszlo Bacsardi

Budapest University of Technology and Economics, Hungary

Abstract

Since the beginning of long-distance communication, there has been a need to connect telecommunications networks of a country to another. Quantum computing offers revolutionary solutions in the field of computer science, applying the opportunities of quantum physics which are incomparably richer than those of classical physics. Although quantum computers are going to be the tools of the distant future, there already exist algorithms to solve problems which are very difficult to handle with traditional computers. Satellite communication has been used for many years, and nowadays we know its limits. In contrast, quantum computing is a fascinating new and fast improving technology. Therefore, it is indeed fascinating and well worthwhile to examine the relationship of satellite communication and quantum computing. At first, we briefly introduce some important elements of quantum information theory, including the free-space quantum key distribution. The aim is to trace some adoptable algorithms in the communication between the Earth and the satellite and also between satellites. For this reason we try to build a new model for the free-space quantum channel. This is the first report of our simulation project.

1. What is quantum computing?

1.1. The qubit

Classical computers use strings of 0s and 1s. It can perform calculations on only one set of numbers at once. In digital computers, the voltage between the plates of a capacitor represents a bit of information: a charged capacitor denotes the bit value 1 and an uncharged capacitor the bit value 0. One bit of information can be also encoded using two different polarizations of light or two different electronic states of an atom. However, if we choose an atom as a physical bit, then quantum mechanics tells us that apart from the two distinct electronic states the atom can also be present in a coherent superposition of the two states. This means that the atom is both in state 0 and state 1. Quantum computers use quantum states which can be in a superposition of many different numbers at once. A classical computer is made up of bits while a quantum computer is made up of quantum bits, or qubits. A quantum computer manipulates qubits by executing a series of quantum gates, each being unitary transformation acting on a single qubit or pair of qubits [1].

E-mail address: bacsardi.laszlo@sch.bme.hu.

0094-5765/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.actaastro.2005.03.023

In applying these gates in succession, quantum computers can perform complicated unitary transformations to a set of qubits in some initial state. The qubits can then be measured, with this measurement serving as the final computational result. This similarity in calculation between a classical and quantum computer affords that in theory, classical computers can accurately simulate quantum computers. The simulation of quantum computers on classical ones is a computationally difficult problem because the correlations among quantum bits are qualitatively different from those among classical bits, as first explained by John Bell. Take for example a system of only a few hundred qubits, this exists in a Hilbert space of dimension $\sim 10^{90}$ that in simulation would require a classical computer to work with exponentially large matrices (to perform calculations on each individual state, which is also represented as a matrix), meaning it would take an exponentially longer time than even with a primitive quantum computer. A simple quantum system is a half-state of the two-level spin. Its basic states, spin-down $|\downarrow\rangle$ and spin-up $|\uparrow\rangle$, may be relabelled to represent binary zero and one, i.e. $|0\rangle$ and $|1\rangle$, respectively. The state of a single such particle is described by the wave function $\psi = \acute{\alpha}|0\rangle + \beta|1\rangle$. The squares of the complex coefficients—$|\acute{\alpha}|^2$and $|\beta|^2$—represent the probabilities of finding the particle in the corresponding states. Generalizing this to a set of k spin-$\frac{1}{2}$ particles we find that there are now 2^k basis states (quantum mechanical vectors that span a Hilbert space) which is equivalent to stating that there are 2^k possible bit-strings of length k.

However, observing the system would cause it to collapse into a single quantum state corresponding to a single answer—a single list of 500 1s and 0s—, as dictated by the measurement axiom of quantum mechanics. The reason for this is an exciting result derived from the massive quantum parallelism achieved through superposition, which would be the equivalent of performing the same operation on a classical supercomputer with $\sim 10^{150}$ separate processors.

1.2. Quantum interference

In the experiment (see Fig. 1) the photon first encounters a half-silvered mirror, then a fully silvered mirror, and finally another half-silvered mirror before reaching a detector, where each half-silvered mirror introduces the probability of the photon travelling down one path or the other. Once a photon strikes the mirror along either of the two paths after the first beam splitter, one might presume that the photon will reach the two detectors A and B with equal probability. However, experiments show that in reality this arrangement causes all collisions at detector A and none at detector B. The only conceivable conclusion is that the photon somehow travelled both paths simultaneously creating interference at the point of intersection that destroyed the possibility for the signal to reach detector B. This is known as quantum interference and results from the superposition of the possible photon states or potential paths. So although only a single photon is emitted, it appears as though an identical photon exists and is only detectable by the interference it causes with the original photon when their paths come together again. If, for example, either of the paths is blocked with an absorbing screen, detector B registers hits again just as in the first experiment. This unique characteristic, among others, makes the current research in quantum computing not merely a continuation of today's idea of a computer, but rather an entirely new branch of thought.

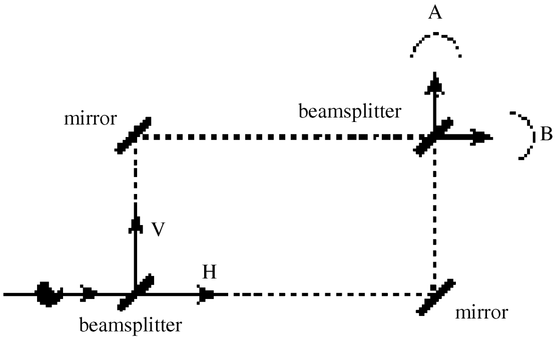

Fig. 1. Experiment for quantum-interference, showing that a qubit can exist as a 0, a 1, or simultaneously as both 0 and 1, with a numerical coefficient representing the probability for each state.

1.3. Quantum cryptography

The premier application of a quantum computer capable of implementing this algorithm lies in the field of encryption, where RSA (one common encryption code), relies heavily on the difficulty of factoring very large composite numbers into primes. A computer which can do this easily is naturally of great interest to numerous government agencies that use RSA—previously considered to be ‘uncrackable’—and anyone interested in electronic and financial privacy.

Cryptography allows two parties (‘Alice’ and ‘Bob’) to render their communications illegible to a third party (‘Eve’), provided they both possess a secret random bit sequence, known as a cryptographic key, which is required as an initial parameter in their encryption devices. Secure key distribution is then essential; Eve must not be able to obtain even partial knowledge of the key. Key distribution using a secure channel (‘trusted couriers’) is effective but cumbersome in practice, potentially vulnerable to insider betrayal and may not even be feasible in some applications.

Encryption is only one application of quantum computers. In addition, Shor, a pioneer researcher of quantum computing, has put together a toolbox of mathematical operations that can only be performed on a quantum computer, many of which he used in his factorization algorithm. Furthermore, Feynman asserted that a quantum computer could function as a kind of simulator for quantum physics, potentially opening the doors to many discoveries in the field. Nowadays the power and capability of a quantum computer is primarily theoretical speculation; the advent of the first fully functional quantum computer will undoubtedly bring many new and exciting applications [2].

2. Free-space quantum channel

2.1. Quantum channel

Perhaps the simplest example of a structure involving multiple times histories of a quantum system is a quantum channel. Typically, one is interested in some basis for the Hilbert space representing the input of a channel, which is tensored to a second Hilbert space representing the environment, and then another (possibly the same) basis for the first space at a later time (see Fig. 2). Any device taking classical or quantum systems of a certain type as input and (possibly different) classical or quantum systems as output may be referred to as a ‘channel’. Mathematically, a channel is represented by the map taking input states to output states or, dually, output observables to input observables. For many questions in quantum information theory it is crucial to characterize precisely the set of maps describing ‘possible’ devices. One way to characterize the possible channels is ‘constructive’. That is, we allow just those channels, which can be built from the basic operations of tensoring with a second system in a specified state, unitary transformation, and reduction to a subsystem. An alternative approach is ‘axiomatic’, i.e., by a set of postulates, which are required by the statistical interpretation of quantum mechanics.

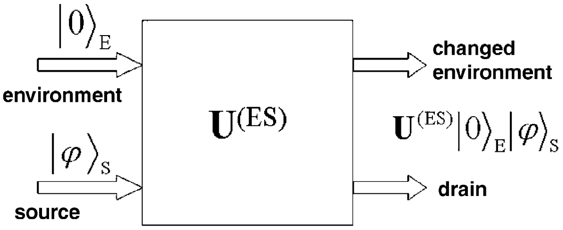

Fig. 2. In the channel, appearing noise is the result of interlocking with the environment.

2.2. Quantum key distribution

Quantum cryptography was introduced in the mid-1980s as a new method for generating the shared, secret random number sequences, known as cryptographic keys that are used in cryptosystems to provide communications security. The appeal of quantum cryptography is that its security is based on laws of nature, in contrast to existing methods of key distribution that derive their security from the perceived intractability of certain problems in number theory, or from the physical security of the distribution process. Since the introduction of quantum cryptography, several groups have demonstrated quantum communications and quantum key distribution over multikilometre distances of optical fibre [4].

Quantum key distribution (QKD) is a promising approach to the ancient problem of protecting sensitive communications from the enemy. QKD is not in itself a method of enciphering information: it is instead a means of arranging that separated parties may share a completely secret, random sequence of symbols to be used as a key for the purpose of enciphering a message.

2.3. Free-space QKD

Free-space QKD (over an optical path of about 30 cm) was first introduced in 1991, and recent advances have led to demonstrations of QKD over free-space indoor optical paths of 205 m, and outdoor optical paths of 75 m. These demonstrations increase the utility of QKD by extending it to line-of-site laser communications systems. Indeed, there are certain key distribution problems in this category for which free-space QKD would have definite practical advantages (for example, it is impractical to send a courier to a satellite).

The researching group at the Los Alamos National Laboratory developed a free-space QKD, and in 1998 published their results of free-space QKD over outdoor optical paths of up to 950 m under nighttime conditions [4].

Four years later, in 2002, the same laboratory has demonstrated that free-space QKD is possible in daylight or at night, protected against intercept/resend, beamsplitting and unambiguous state discrimination (USD) eavesdropping, and even photon number splitting (PNS) eavesdropping at night, over a 10 km, 1-airmass path, which is representative of potential ground-to-ground applications and is several times longer than any previously reported results. The system provided cryptographic quality secret key transfer with a number of secret bits per 1 s quantums. This research published in their report is as follows: 'we believe that the methodology that we have developed for relating the overall system performance to instrumental and quantum channel properties may also be applicable to other QKD systems, including optical fibre based ones' [5].

2.4. Earth–satellite connection

To detect a single QKD photon it is necessary to know when it will arrive. The photon arrival time can be communicated to the receiver by using a bright precursor reference pulse. Received bright pulses allow the receiver to set a 1 ns time window within which to look for the QKD-photon. This short time window reduces background photon counts dramatically, and the background can be further reduced by using narrow bandwidth filters.

According to Buttler's report, the atmospheric turbulence impacts the rate at which QKD photons would be received at a satellite from a ground station transmitter. Assuming 30 cm diameter optics at both the transmitter and the satellite receiver, the diffraction-limited spot size would be 1.2 m diameter at a 300 km altitude satellite.

Errors would arise from background photons collected at the satellite. The background rate depends on full or new moon: the error rate will be dominated by background photons during full moon periods and by detector noise during a new moon. During daytime orbits of the background radiance would be much larger. Because the optical influence of turbulence is dominated by the lowest 2 km of the atmosphere, the results show 'that QKD between a ground station and a low-earth orbit satellite should be possible on nighttime orbits and possibly even in full daylight. During the several minutes that a satellite would be in view of the ground station there would be adequate time to generate tens of thousands of raw key bits, from which a shorter error-free key stream of several thousand bits would be produced after error correction and privacy amplification' [4].

3. Distant future?

At present, quantum computers and quantum information technology remains in its pioneering stage. Error correction has made promising progress to date, nearing a point now where we may have the tools required to build a computer robust enough to adequately withstand the effects of decoherence. Quantum hardware, on the other hand, remains an emerging field, but the work done thus far suggests that it will only be a matter of time before having devices large enough to test Shor's and others' quantum algorithms. Thereby, quantum computers will emerge as the superior computational devices at the very least, and perhaps one day make today's modern computer obsolete. Quantum computation has its origins in the highly specialized field of theoretical physics, but its future undoubtedly lies in the profound effect.

Quantum computing algorithms can be used to affirm our communication in three ways:

1. Open-air communication (below 100 km, instead of optical cable, using the twisted surface of Earth).

2. Satellite communications (between 300 and 800 km altitude, signal encoding and decoding). Quantum error correction allows quantum computation in a noisy environment. Quantum computation of any length can be created as accurately as desired, as long as the noise is below a certain threshold, e.g. $P < 10^{-4}$.

3. Satellite broadcast (our broadcast satellite) orbit at 36,000 km, using 27 MHz signal. In quadrature phase shift keying (QPSK) every symbolum contains two bits, this is why the bit speed is 55 Mbs. Half the bits is for error coding, in the best case we only have 38 Mbs, but in common solutions there is only 27–28 Mbs, in which 5–6 TV-channels can be stored with a bandwidth of 2–5 Mbs each. The quantum algorithms can prove the effective bandwidth to fill better the brand as in the traditional case.

4. Simulating a free-space quantum channel

Hopefully the free-space quantum channel will be an important part of our communication, as we could see so far. This is why we are studying the free-space quantum channel at the Budapest University of Technology and Economics, Faculty of Electrical Engineering and Informatics, Department of Telecommunications. Our project is to study and understand this type of channel and to set up a working model. Two students are working on this project (Attila Pereszlenyi, Laszlo Bacsardi), the supervisor is Dr. Sandor Imre. The project has started in September 2003, the scheduled end is in May 2005.

We set up our quantum-channel model in the following three ways:

1. distance-independent model (infinite channel with a source and a drain),

2. linear model (linear parameter for noise) and

3. fractional distances model (different items have their own noise parameters).

In each case we start by examining the bit error rate (BER) on the empty channel, in the second phase we attack the channel, finally we try to find different methods to protect the channel.

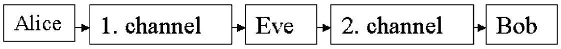

Fig. 3. Our channel overview. Some elements between Alice (source) and Bob (drain) can be dropped out (like 1. channel, Eve or 2. channel).

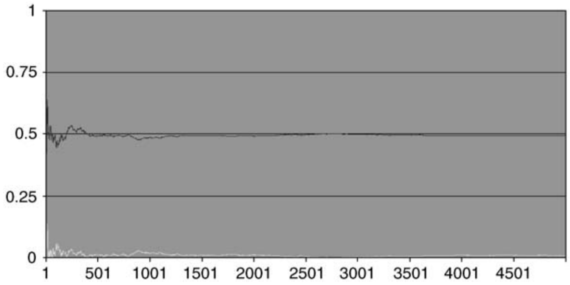

Fig. 4. Independent, depolarizing errors at BB84-simulated channel. The horizontal axis is represents the number of bits. On the graph the BER (bit error rate) and the ABS (0.5-BER) are visible.

In the third case (the distance exists fractional) the distances are divided into three items:

1. item: 0–2 km (bottom layer of atmosphere),

2. item: 2–10 km (top layer of atmosphere) and

3. item: 10–36,000 km (space).

Firstly each of this items will be characterized by a constant noise parameter depending on different physical parameters, like probability of turbulence, cloudy or rainy weather, etc. These parameters will be increasing as a function of the distance simulating the real environment. These noise parameters will be refined by comparing our results with the effective physical measures from across the world.

In our channel overview the third party called Eve (the eavesdropper) can step between the two communication parties, called Alice and Bob (see Fig. 3).

First of all we simulated the Bennett–Brassard 1984 (BB84) QKD protocol, which is the simplest quantum key distribution protocol. Shor and Preskill already proved concisely the unconditional security of this protocol [8].

One of our first tasks was to test the empty channel (without Eve), with different signals: all 0s (00000000), all 1s (11111111), 0–1 sequences (01010101), 0–1 sequence in blocks (00001111) and random bit sequences. We had to find the BER of the empty channel, to be able to calculate with it fur-

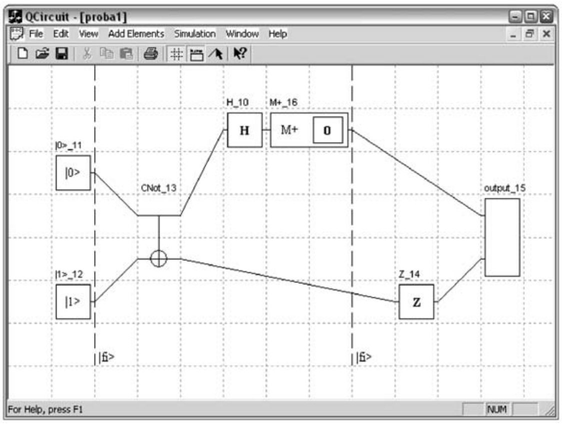

Fig. 5. Screenshot of our program, showing three elementary channels with quantum-gates and measurement.

thermore. After we simulated a successful QKD with BB84 and we built a complicated channel (see Fig. 4).

The first version of our program was written in Microsoft C++, after it we changed to Microsoft .NET to make it easier and more comfortable to design as can be seen in Fig. 5. Now we are able to handle different gates which allows one to use any algorithm other than the BB84 algorithm.

5. Summary

Quantum mechanics forces us to redefine the notions of information, information processing and computational complexity. New technologies for realizing quantum computers are being proposed, and new types of quantum computation with various advantages over classical computation are continually being discovered and analysed. The quantum theory of computation must in any case be an integral part of the world view of anyone who seeks a fundamental understanding of the quantum theory and the processing of information. Large-scale quantum information processing seems possible, though technologically very challenging to realize, this is why a major focus for experimental physics today.

Hopefully in the next 10 years quantum computing algorithms will appear in more technologies and probably the success in free-space quantum channel experiments can result in development in satellite communication. At the University we are working to complete our free-space quantum channel model to diagnose and to simulate the satellite communication. At first we finish the setting-up process, later on, we can start testing it with different parameters. We hope to publish the results next year.

The newest beta version of our program can be found on Pereszlenyi's homepage (it is still in the development phase): (http://www.hszk.bme.hu/∼pa310/quantum/).

I would like to thank Dr. Eva Godor, Dr. Sandor Imre and Andras Keri for their assistance.

References

[1] R.B. Griffiths, The nature and location of quantum information, (arXiv:quant-ph/0203058).

[2] A. Barenco, A. Ekert, A. Sanpera, C. Machiavello, Short Introduction to Quantum Computing, La Recherche, 1996.

[4] W.T. Buttler, R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, C.M. Simmons, Practical free-space quantum key distribution over 1 km, (arXiv:quant-ph/9805071).

[5] R.J. Hughes, J.E. Nordholt, D. Derkacs, C.G. Peterson, Practical free-space quantum key distribution over 10 km in daylight and at night, New Journal of Physics 4 (2002) 43.1–43.14.

[8] C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, IEEE, New York, 1984, pp. 175–179.

Further reading

[3] A. Gschwindt, Satellite broadcast, Müszaki Könyvkiadó, Budapest, 1997.

[6] E. Knill, R. Laflamme, A. Ashikhmin, H. Barnum, L. Viola, W.H. Zurek, Introduction to Quantum Error Correction, (arXiv:quant-ph/0207170).

[7] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, Capacities of Quantum Erasure Channels, (arXiv:quant-ph/9701015).