Quantum Cryptography

Advances in computer science may radically alter cryptography.

Evan James Dembskey

evan@tmg.co.za
Telemessage SA PTY (LTD), Johannesburg
evan@tmg.co.za
Technikon SA
June 2002

Tel: +27 11 340 4017 Fax: +2711 340 4001

Key words: computer science, cryptography, quantum computing, quantum communication, quantum cryptography, quantum mechanics, security, theory.

Abstract: Critical questions raised by Einstein, Podolsky and Rosen (EPR) on locality, reality and completeness inspired many researchers to study quantitatively the difference between quantum physics and classical physics. In time, these researches led naturally to the idea of quantum computing. Unlike classical computers, with quantum computers the computational space increases exponentially with the size of the system. This allows exponential parallelism, which could lead to exponentially faster quantum algorithms than is possible with non-quantum computers. If advances in quantum computing follow Moore's Law, a 30-qubit quantum computer will be available by the year 2007, which would ran at approximately 10 teraflops. Further advances in quantum computing would render current methods of encryption useless. The solution naturally lies in the application of quantum effects in the area of cryptography. Quantum cryptography is a method for secure communications offering the assurance of the inviolability of a natural physical law. Research in the area of quantum cryptography must be given a high priority to ensure the availability of new methods should the era of quantum computing dawn.

1. INTRODUCTION

Critical questions raised by Einstein, Podolsky and Rosen (EPR) on locality, reality and completeness inspired many researchers to study quantitatively the difference between quantum physics and classical physics.

In time, these researches led naturally to the idea of quantum computing. Unlike classical computers, with quantum computers the computational space increases exponentially with the size of the system. This allows exponential parallelism, which could lead to exponentially faster quantum algorithms than is possible with non-quantum computers. If advances in quantum computing follow Moore's Law, and empirical evidence supports this, a 30-qubit quantum computer will be available by approximately the year 2007. Further advances in quantum computing would render current methods of encryption useless within a few decades. The solution lies in the application quantum mechanical phenomena in the area of cryptography. Quantum cryptography is a method for secure communications offering the assurance of the inviolability of a natural physical law.

2. CLASSICAL CRYPTOGRAPHY

The two main goals of cryptography are for a sender and an intended recipient to be able to communicate in a form that is unintelligible to third parties, and for the authentication of messages to prove that they were not altered in transit [HUGH95]. One of the most secure methods is the asymmetric system. Asymmetric cryptographic methods rely on one-way functions, which can be defined as: if f is a one way function, then it is easy to work out f(x) to get a number y, but if only y and f is known then it is computationally infeasible to find x [FLAN01]. The key concept here is that it is computationally infeasible to reverse a one-way function. Mathematically, a function cannot be proved to be one-way, but for the purposes of modern cryptography meets Shannon's first requirement for a good cipher [PFLE97]. The type of one-way function of interest to cryptographers is the one-way trapdoor function. A one-way trapdoor function is identical to the one-way function defined above, but with a trapdoor, some secret information that makes it easy to find x if y and the secret trapdoor is known. [SCHN96] A good example of this is the RSA algorithm. One of the major problems is the problem of key distribution. That is, making sure that the sender and intended receiver both have the trapdoor information, or key, while ensuring that third parties cannot acquire even partial information about it [HUGH95].

There is another potential problem with modern cryptographic methods that rely on one-way functions for their security. Should it ever become computationally feasible to reverse a one-way function, then all methods based on such can no longer be considered secure. Generally, this has been thought to be a non-problem, but a serious threat is developing, based on the work not of computer scientists or mathematicians, but on the work of physicists, in particular, quantum physicists. Some basic principles of modern quantum physics must be outlined before explaining this further.

3. QUANTUM MECHANICS

Quantum mechanical phenomena are generally considered difficult to understand since our commonplace experiences are not applicable. Niels Bohr, one of the fathers of quantum mechanics, said: “Anyone who can contemplate quantum mechanics without getting dizzy hasn’t understood it.” [SING00]. Several important principles will now be outlined, hopefully sufficient to understand the basis for quantum computing and cryptography, but should by no means be considered even an adequate introduction to quantum physics

3.1 Heisenberg’s Uncertainty Principle

The first principle that must be understood is Heisenberg’s Uncertainty Principle, introduced by Werner Heisenberg in 1927. Heisenberg’s Uncertainty Principle, simply put, states that there is no way of accurately pinpointing the exact position of a sub-atomic particle unless you are willing to be uncertain about the particle’s momentum, and there is no way to pinpoint the particle’s exact momentum unless you are willing to be uncertain about its position. It is impossible to measure them both accurately at the same time. [MCEV01] To state it more formally, if a measurement of a position is made with precision Δx and a simultaneous measurement of linear momentum is made with precision Δp_x, then the product of the two uncertainties can never be smaller than $\eta/2$. It must be noted that these uncertainties do not arise from imperfections in the measuring instruments, but rather they arise from the quantum structure of matter. Position and momentum are said to be non-commuting observables, which is useful for quantum cryptography [SERW00].

3.2 Spin

The second principle is spin. Spin is an intrinsic angular momentum associated with quantum mechanical particles. Unlike classical "spinning" objects, which derive their angular momentum from the rotation of their constituent parts, spin angular momentum is not associated with any rotating internal masses. For example, an elementary particle such as the electron possesses spin angular momentum, even though it is a point particle. [MCEV01]

3.3 EPR Paradox

The third principle is the EPR paradox, named after its authors, Albert Einstein, Boris Podolsky and Nathan Rosen. It involves apparent action-at-a-distance, or faster than light communication, which is believed to be impossible. [MCEV01] It is possible to obtain a pair of particles, such as electrons, in a singlet state where their spins cancel each other out to give a total spin of zero. If these particles A and B are moved a wide distance apart, and the spin of the A electron is measured, we instantaneously know the spin of B, which will be opposite to A because the two spins cancel to zero. As A has no definite value until it is measured, at which point it collapses its spin wave function into one state, and B simultaneously into the opposite state. The combined system of A and B is in a superposition state, which is necessary for the non-classical behaviour. This has been termed quantum entanglement.

3.4 Bells Inequality Theorem

The Fourth principle is Bell’s Inequality Theorem. John Bell repeated the EPR thought experiment, but instead of using electrons, he used photons in which the polarization of light is detected instead of spin. As a result of his work, he acknowledges that hidden variable theories are possible, but only if the theories are nonlocal, meaning that we can infer that changes in the quantum system are conveyed faster than the speed of light, in violation of Einstein's special relativity theory.

3.5 Superposition

The fifth principle is superposition, which is conveniently explained by using Erwin Shrödinger’s thought experiment, designed originally to demonstrate the absurdity of the concept, but ironically is used today to teach the concepts of quantum probability and the superposition of quantum states. In this thought experiment, a cat is placed in a box with no means for an outside observer to see inside it. In the box with the cat are a tube of cyanide, a radioactive source, a device to break the tube and a Geiger counter. The radioactive source has a 50% probably of having a particle decay in a given time period. If a particle decays, the Geiger counter detects the decay, and sets off the device which breaks the tube containing the poison, thus killing the cat. So, after the given time period has passed, the cat has a 50% chance of being alive, and a 50% chance of being dead. As the outside observer has no idea whether or not the particle has decayed, the observer has no idea whether the cat is alive or dead. From the point of view of classical physics, the cat is either alive or dead. In the quantum view, the cat is both alive and dead, the particle decayed and undecayed, the bottle broken and unbroken, in essence it is in a superposition of both possible states, until the observer opens the box and observes the cat, at which point the wave-function collapses and the cat becomes either alive or dead. Despite the fact that superposition appears absurd there is evidence that it is a physical reality. This evidence is gathered from the double slit experiment, about which Richard Feynman said, "it contains the only mystery" [GRIB91]. The double slit experiment shows the impossibility of simultaneously measuring wave and particle properties and embodies all the bizarre consequences of quantum mechanics [SERW00]. It is beyond the scope of this paper to discuss the double-slit experiment, refer to [GRIB91], [GRIB01] and [SERW00] for further information

4. QUANTUM COMPUTERS

Modern computers operate on the same fundamental principles as the mechanical devices designed by Charles Babbage and later formalized by Alan Turing: one stable state of the machine representing one number. [RIEF00-2] They are built upon a foundation of our knowledge of classical physics, yet physicists have shown that the laws describing the natural universe are the subtler laws of quantum physics, and this lead naturally to the idea of utilizing these laws in the arena of computing. In 1984 a British physicist, David Deutsch, attended a conference on the theory of computation and realized this, which was something that had previously been overlooked [SING00]. Throughout the history of computing, the bit has remained the basic computational unit of information. [RIEF00-2] A bit can store only one value, a zero (0) or a one (1), at any one time. The basic computational unit in quantum computing is the qubit, derived from the term quantum-bit. A qubit can be put in a superposition state that stores both values simultaneously; it contains both a zero (0) and a one (1) at the same time. The qubits two states are conventionally labelled |0> and |1>. The real power of quantum computing derives from the exponential state spaces of multiple qubits. A register of n qubits can be in a superposition of all 2^n possible values. In contrast with classical computers, where the amount of parallelism increases in direct proportion to the size of the system, it increases exponentially in size for quantum computers. For example, a 250 qubit quantum computer represents approximately 10^{75} combinations, which is greater than the number of atoms in the universe. Clearly, using a classical computer this number of combinations is not feasible**.**

4.1 Methods of Quantum Computing

Most of the methods used for realizing a quantum computer are based on one of three ways of manipulating quantum particles.

- Manipulating the spin of a nucleus or subatomic particle. A qubit is derived from superpositions of up and down spins
- Manipulating electrical charge. A qubit is derived from superposition of two or more discrete locations of the charge.
- Manipulating the polarization or phase of a photon. A qubit is derived from superposition of phase or polarization angles

Currently, the five most promising possibilities for building a quantum computer are as follows [QUBY]

4.1.1 Nuclear Magnetic Resonance

A Nuclear Magnetic Resonance (NMR) quantum computer is based on control of nuclear spin. This has been achieved by manipulating the nuclear spins of atoms in a molecule. Magnetic pulses within a magnetic field produced by a NMR chamber manipulate spin. The entanglement of spins required to establish a qubit is created by the chemical bonds between neighbouring atoms. The major drawback of this method is scalability.

4.1.2 Ion Trap

An Ion Trap quantum computer is also based on control of nuclear spin. Small numbers of ions or even individual ions are trapped by an electromagnetic field. This technique is theoretically scalable, but requires a cryogenic environment. To date, only single qubit systems have been demonstrated.

4.1.3 Quantum Dot

A Quantum Dot quantum computer can involve manipulation of electrical charge, spin, or energy state. A small number of electrons or possibly an individual electron is confined with a quantum dot, usually 180 nanometers or less, the quantum dot typically being a small "hill" of molecules on a silicon substrate. A computer would be made up of a regular array of such dots. This method seems to have the highest potential for commercial scalability.

4.1.4 Josephson Junction

In a Josephson Junction QC tunnelling of electron Cooper pairs occurs through a thin layer of semi-conductor that has been sandwiched between two layers of superconductor. The probability of "which side of the sandwich" the electron pairs will reside on is manipulated by application of voltages across the junction. Two qubit operations have been demonstrated. Manufacture of these junctions is considered scalable.

The current most promising system is based on this proposal. Researchers at SPEC have constructed a qubit out of a super-conductive metal loop interrupted with Josephson Junctions. This circuit, called a "Quantronium", is, to date, the best performing qubit. The advantage of Quantronium is that it is well de-coupled from the external circuit, while remaining connected and measurable at all times. Due to this de-coupling, coherence time is adequately long to enable experiments, which have previously been unfeasible to be performed.

4.1.5 Optical

An Optical quantum computer is based on manipulating the polarization or phase of individual photons. Entanglement is achieved by coincident creation of identical photons and the superposition of polarization or phase state is manipulated using polarizing lenses, phase shifters, and beam splitters. This method is theoretically scalable to a large number of qubytes.

4.2 Problems with quantum computers

There are a number of problems with quantum QC. While a quantum system can perform massive parallel computation, access to the results of the computation is restricted. Accessing the results of the computation is equivalent to taking a measurement, which of course disturbs the quantum state. This problem makes the situation seem even worse than the classical situation; we can only read the result of one parallel thread, and because measurement is probabilistic, we cannot even choose which one we get. [RIEF00] Essentially, one question can computational result can be obtained before having to redo the entire computation.

Another problem is that there are very few physical systems that are amenable to the task of quantum computing. This is because a quantum computer must (i) interact very weakly with the environment to preserve the coherence of the superpositions, and (ii) interact very strongly with other quantum bits to facilitate the construction of quantum logic gates necessary for computing [BRAU99].

Despite these problems, it is generally thought that a commercial quantum computer will be feasible in fifty years.

5. QUANTUM COMPUTERS AND CRYPTOGRAPHY

5.1 Quantum computers versus classical cryptography

As stated previously, the real power of quantum computing derives from the exponential state spaces of multiple qubits. A register of *n* qubits can be in a superposition of all   possible values. This computational power can be harnessed to reverse the one-way trapdoor functions that are typically used in modern cryptography, such as factoring large numbers or finding the password that decrypts a file. Of course, there are many equally secure public-key cryptography schemes that have nothing whatsoever to do with factoring, and may be difficult even for quantum computers to break.

I will briefly examine the problem of password guessing/cracking in this context, as it demonstrates one of the major strengths of quantum computing. The problem has four characteristics:

- The only way to solve it is to guess answers repeatedly and check them
- There are *n* possible answers to check
- Every possible answer takes the same amount of time to check
- There are no clues about which answers might be better. Generating possibilities randomly is just as good as checking them in some special order

For problems with all four properties, it will take an average of *n/2* guesses to find the answer using a classical computer. The time for a quantum computer to solve this will be proportional to the square root of n. Clearly this can be a very large speedup, reducing some problems by orders of magnitude. This would be particularly useful to attack symmetric ciphers such as 3DES and AES.

5.2 Quantum cryptography

As mentioned before, one of the problems of classical cryptography is key distribution. It is provably impossible to establish a secret key with conventional communications. Keys can be intercepted, or inferred from intercepted data, or in the case of ciphers based on hard problems such as large-number factorisation, potentially broken by the computational power afforded by quantum computers.

Provable secure key distribution becomes possible with quantum communications It is impossible to tap single quantum signals in the conventional sense, as Heisenberg's Uncertainly Principle ensures that any eavesdropper's activities must produce an irreversible change in the quantum states (the wave-function collapse mentioned earlier) before they are retransmitted to the intended recipient. [HUGH95]

Quantum cryptography is in essence a solution to the key distribution problem, and can be termed Quantum Key Distribution (QKD) [HUGH95]. There are at least three methods for QKD. They are:

- Cryptosystems using quantum entanglement
- Cryptosystems using two non-commuting observables
- Cryptosystems using two non-orthogonal state vectors

Cryptosystems based on quantum entanglement seem to offer the greatest promise. A sequence of correlated particle pairs, for example, a pair of EPR photons, is generated, with one member of each pair being detected by each party. A third-party would have to detect a particle to read the signal, and retransmit it to remain undetected. However, the act of detection of one particle of a pair destroys its quantum correlation with the other, and the two parties can easily detect the interference without revealing the results of their own measurements [QUBI]. Quantum entanglement has been tested over a distance of 4 km. This method promises secure key distribution even in the presence of environmental noise [EKER97].

Systems using two non-commuting observables can be explained with the following simple example. The system includes a transmitter and a receiver. The sender transmits photons in one of four polarisations: 0, 45, 90, or 135 degrees. The receiver measures the polarisation. The receiver can be quickly configured to distinguish between rectilinear polarisations (0 and 90) and diagonal polarisations (45 and 135); it cannot, however, distinguish both types simultaneously. QKD then requires several steps. The sender sends photons with one of the four polarisations chosen at random. For each incoming photon, the receiver chooses at random the type of measurement: either the rectilinear type or the diagonal type. The receiver records the results of the measurements but keeps them secret. The receiver then publicly announces the type of measurement and the sender tells the receiver which measurements were of the correct type. The two parties retain all cases in which the receiver measurements were of the correct type. These cases are then translated into bits (1's and 0's), which is, in essence, the key. A third-party will introduce errors to this transmission because he/she does not know in advance the type of polarisation of each photon and quantum mechanics does not allow him/her to acquire sharp values of two non-commuting observables. Although eavesdropping cannot be prevented, it will be detected no matter how subtle and sophisticated the attempt. Polarization based schemes has been successfully tested over a distance of 1 km [QUBI].

The proposal using non-orthogonal state vectors can be described, very basically, as follows. Alice and Bob have devices that generate pulses of light in any of four different polarizations and light polarization detectors. To generate a key, Alice generates two random bits B_1 and B_2 and sends a pulse of light to Bob. B_1 selects the basis and B_2 the polarization within that basis. Bob generates a random bit B_3 and sets his polarization detector to that basis. He reads bit B_4. Bob and Alice tell each other B_3 and B_1. If they agree, they add B_2 and B_4 to their keys, knowing that they are the same unless Eve is eavesdropping. Eve does not know B_1, so she might interfere with it. To send a message, Alice takes a message bit and two key bits. She uses one key bit to set the basis, xors the other with the message, and uses it to select the polarization, then transmits. Bob takes the two key bits, sets the basis according to the first, receives the light pulse, and xors it with the second to get the data bit.

6. CONCLUSION

With the limit to the size of transistors approaching in approximately twenty years, the development of faster processors and more memory will cease unless a new technology is born. Theoretically, the construction of quantum computers is possible. Therefore, the research into building a quantum computer is presently a strong research area in physics and computer science. If quantum computing proves to be feasible, it is likely that quantum computers capable of breaking the hardest modern ciphers will be available in 50 years, which places an upper limit on the usefulness of modern cryptographic methods. Further research into quantum cryptography is a necessity, and such research would not be wasted even if quantum computers were found to be infeasible, as quantum cryptography is not reliant on the existence of quantum computers to function, and will be a very useful technology in its own right.

7. LIST OF SOURCES CONSULTED

[QUBI] anonymous, (2002). QUBIT.COM

[QUBY] anonymous, (2002). www.qubyte.com

[BOUW02] Bouwmeester, D., Ekert, A., Zeilinger, A. (2000). The Physics of Quantum Information. Berlin: Springer

[BRAU99] Braunstein, S. (1999). Quantum Computing. New York: Wiley-VCH.

[DENN83] Denning, D. (1983). Cryptography and Data Security. Massachusetts: Addison-Wesley

[DIVI00] DiVincenzo, D. (2000). The Physical Implementation of Quantum Computing. New York: IBM T.J. Watson Research Center

[EKER97] Ekert, A. (1997). From Quantum code-making to quantum code-breaking. Clarendon Lab, Oxford

[FLAN01] Flannery, S. & Flannery, D. (2001). In Code. London: Profile Books.

[GISI01] Gisin, N, Ribordy, G., Tittel, W. & Zbinden, H. (2001). Quantum Cryptography. University of Geneva: Group of Applied Physics.

[GRIB91] Gribbin, J. (1991). In Search of Shrödinger's Cat. In: anonymous, editors. London: Black Swan

[GRIB01] Gribbin, J. (2001). Shrödinger's Kittens. In: anonymous, editors. London: Phoenix

[HOHL01] Höhler, G. (2001). Quantum Information. Berlin, Springer

[HUGH95] Hughes, R.J., Alde, D.M., Dyer, G.G., Morgan. G.L. & Schauer. (1995) Quantum Cryptography. Los Alamos Laboratory

[MCEV01] McEvoy, J. & Zarate, O. (2001). Introducing Quantum Theory. Icon Books

[PFLE97] Pfleeger, C. (1997). Security in Computing. New Jersey, Prentice-Hall

[RIEF00] Rieffel, E&Polak, W. (2000). An introduction to Quantum

Computing for non-physicists. California: FX Palo Alto Laboratory.

[RIEF00-2] Rieffel, E. & Steane, A.M. (2000). Beyond Bits: The Future of Quantum Information Processing

[SCHN96] Shneier, B. (1996). Applied Cryptography. New York: John Wiley & Sons.

[SERW00] Serway, R. & Beichner, R.J. (2000). Physics for Scientists and Engineers. Florida: Saunders College Publishers.

[SING00] Singh, S. (2000). The Code Book. London: Fourth Estate.

[STAL99] Stallings, W. (1999). Cryptography and Network Security. New Jersey: Prentice Hall.

[WILL98] Williams, C (Ed). (1998). Quantum Computing and Quantum Communications: First NASA International Conference, QCQC 1998. Springer: