Quantum computing and security of information systems

A. A. Berezin
Department of Engineering Physics, McMaster University, Canada

Abstract

Quantum computing (QC) is a fundamentally new interdisciplinary idea at the interface of physics, mathematics and informatics. Today QC is still in its initial stages in terms of its practical implementation due to difficulties related with maintaining a high level of quantum coherency at the macroscopic level. However, theoretical principles of QC are presently well understood and there is a significant on-going progress towards actual prototypes of functioning QC. Present protocols of secure electronic communication can be easily cracked by QC. Thus, the advent of QC can make almost all existing systems of confidential communications utterly unreliable. The present paper gives a non-specialist overview of the principles of QC and discusses some of its possible applications, and also addresses the above challenges concerning the reliability and security of information and communication systems.

Keywords: quantum computing, quantum communication systems, secure electronic communications, information generation systems, prime numbers, quantum nonlocality.

1 Introduction

Security and confidentiality issues related to the generation, storage and transmission of information were invariably important in the course of history in many different ways. Before the advent of modern electronic information and communication systems, information security largely consisted in physical protection of paper-bound documents and communication channels. The science and practical tools of cryptology – methods of coding and decoding of information – constituted a significant facet of the security activity. All existing methods of cryptology, some of which go back to ancient times, rely on the fact

WIT Transactions on The Built Environment, Vol 94, © 2007 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE070151

that there are tangible physical instruments (or paper-bound instructions) on how to code and how to decode the confidential messages. In practice, quite often these instructions were memorized by human information carriers to reduce the risk of interception.

As a conceptual and gnoseological extension of classical (Newtonian–Maxwellian) physics, quantum physics has offered new vistas in many key areas of human knowledge. From electronics to biology (and especially, biomedicine and neurosciences), quantum physics has led to radically new advancements. Likewise, quantum vision has enhanced understanding of "information" as a physical category, which has attained the same degree of importance as physical concepts of energy and matter. This can be discussed in a broad variety of physical contexts [1], as well as historical and philosophical reflections [2].

2 Effects of electronic revolution

Over the course of history many typical functions of human hands were gradually delegated to machines. Manual labor and our muscles have progressively less and less to do in almost all activities related to the production and distribution of material goods. A similar trend of replacing some typical human mental faculties by programmable automata has gone on since the invention of earliest informational systems. The first machines for mechanized calculations appeared long before any electronics in the modern sense. Machines like the mechanical Arithmometer (C.X. Thomas, 1820), not to mention the millennia old Abacus, can be considered prototypes of modern computers – at least in terms of their capacity of performing elementary calculations.

Electronic revolution and, especially, replacement of vacuum tube electronics by semiconductor technology in the 1950s, has lead to a radical paradigm shift in computing. The invention of Bipolar and Field Effect Transistors followed by the development of Integrated Circuit technology and VLSI (very large scale integration) gave a further boost to the whole area of information technology and communication systems. The famous "Moore Law" (doubling of chip power every 18 months) could be continuously traced from the mid 1960s to the present day and is supposed to last for at least ten more years when the projected size of transistors may reach the atomic scale [3].

An important (and often confusing) point about the above developments is the role which quantum physics plays in them. Although it is true that some aspects of operation of modern VLSI systems rely on *some* quantum effects (such as electron tunneling, scattering, trapping, etc) they, in essence, behave as *classical* systems (term "quasi-classical" is used sometimes). This means that such more fundamental quantum effects as the formation of quantum superpositions, collapse of the wave functions at the measurement process and effects of quantum non-locality are not directly involved in the operation of these devices. Thus, in spite of some references to quantum effects, modern computing up to the present day remains largely a domain of classical physics and requires for its understanding only occasional glimpses of quantum phenomena. For it, quantum effects, while sometimes significant in terms of affecting their performance, still remain largely corrections to the essentially classical viewpoint (which treats electrons as tiny particles of localized electrical charge rather than quantum waves).

3 Richard Feynman enters the scene

Therefore, it is not surprising that some visionaries attempted to put forward ideas relating quantum physics with computing in a more direct way. One of the key figures in 20-th century physics Richard Feynman (1918–1988, Nobel Prize 1965) devised some principles of what later was labeled as "quantum computing" (QC). In his 1982 paper [4] he explored an analogy between quantum dynamics and computational process. Subsequent years have witnessed an explosive development of theoretical foundations of QC and quantum information communication systems (QICS). This led not only to growing expectations about the power of new emerging technology, but also to a growing appreciation of challenges it may bring, in particular to the area of informational security.

This paper gives a brief review of major security challenges emerging in connection with QC and QICS systems and mentions some tentative proposed solutions. While QC and QICS bring in a plethora of opportunities, they also open up serious challenges for the whole area of security of information. It should be noted that in any area which is experiencing an exponential growth of research activity (as QC and QICS are), all forecasts are likely to be corrected (or even completely reformulated) in the course of actual future development.

4 Why Quantum Computing matters for security

Quantum physics presents both new opportunities and new challenges for computing and communication systems. Principles and conceptual structure of quantum physics significantly differ from classical physics and some foundational ideas of quantum physics appear to contradict common sense (such as the ideas of quantum non-locality and what Einstein called "spooky actions over distance").

As a technology based on quantum physics, QC is a principally new development. It should not be seen as just a mere extrapolation of the existing designs of microchips to smaller and smaller scales where the quantum effects become more pronounced. On the contrary, QC from the very beginning uses the quantum superposition principle as the very foundation of its operation. The fact that according to the quantum view, a system (would it be a single particle of a more complicated entity, even the entire computer) can be simultaneously in many states becomes the central point for the operation of QC. A popular illustration to the idea of quantum superposition is provided by a famous metaphor of the "Schrödinger's Cat" – a macroscopic object (in this example – a cat) may, under certain conditions, be simultaneously dead and alive. What appears as being totally outside of common sense and ordinary human experience, has a convenient placement in a conceptual framework of quantum mechanics.

One of the fundamental premises of quantum physics is the principle of indistinguishability of elementary particles of the same type (electrons, protons or whole atoms of the same isotope). One cannot “label” a particular electron with some “marker” – the fact which can be formulated as a separate *principle of non-labelability* of quantum particles. If, say, two electrons collide and then fly apart, it is impossible to say “which electron is which”. At first glance it appears that indistiguishability and non-labelability provide a shield behind which one can “hide” an unspecified and unmeasurable arrays of information and hence to provide a wide avenue for secrecy and informational security. While this argument indeed has some merit, the opposite argument (that quantum physics makes information more transparent and hence less secure) also cannot be ignored. The latter is especially so for the decoding applications of QC whose power and capacity in this regard for all practical purposed is almost unlimited.

5 Codes and ciphers: a long and rich history

Numerous historical and archeological data show the persistent interest in secret communications. The famous Caesar Cipher is discussed in numerous sources. The art of cryptography can be traced to almost the beginning of written history. There is an extensive literature on this subject at all levels of scholarly inquiry, from in-depth academic studies to a popular non-fiction (e.g., [5]). The majority of coding schemes of the past used transposition of letters, replacing letters by numbers using agreed-upon (secret) texts and other similar techniques.

Except for short, “one-time” communications, most of these schemes can be relatively easily cracked on modern computers. A few exceptions, however, remain open challenges till the present day. An example of the latter is the famous “Voynich Manuscript” ([5], pp. 49-51) – a medieval well illustrated folio written in a unique script which so far has resisted all attempts to decipher it. Likewise, codes and cryptic messages were invariably a hot topic for fictional literature (e.g., a recent bestseller “Da Vinci Code”).

6 Prime numbers and RSA security code

From ancient times people were invariably fascinated by prime numbers. Primes are integers divided only by 1 and themselves (2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,…). It was proven by Euclid 23 centuries ago that the number of primes is infinite. This interest towards primes has found its way into numerous books of which we can mention only a few [6 – 9]. For the security of modern (pre-quantum) communication systems prime numbers play a central role.

A common security protocol, the so called RSA code (by names of Ron Rivest, Adi Shamir, and Leonard Adleman, who proposed it in 1977 at MIT) is based on the computational difficulty of finding prime factors of large integer numbers. While the details of it can be found in numerous printed and Web sources, in a nut shell the idea behind it is as follows.

Step 1: The expected recipient ("Bob") chooses two large prime numbers P and Q (normally, about 100 decimal digits each);

Step 2: He then computes the product of P and Q as N = P•Q;

Step 3: He then chooses some integer E which is coprime to the so called totient of N which is T = (P-1)•(Q-1);

Step 4: Finally, he computes another integer D which satisfies congruence relation D•E = 1 (mod T), i.e., D•E = 1 + K•T for some integer K.

All steps 1 to 4 can be easily done on almost any (classical) computer. After these steps are done, Bob announces *publicly* numbers N and E (so called "public key"), but keeps D as his "secret" number ("private key"). It should be noted that in order to calculate D one needs to know separately P and Q (which are kept secret by Bob) and not just their product N (which is publicly known). The whole scheme is also known as a public key encryption.

Using publicly known N and E anyone (say, "Alice") can encrypt her message and send it to Bob using a public channel (say, by publishing a scrambled message as an advertisement in a newspaper). But only Bob can decode and read the message using his secret decryption key D. Anyone can obtain scrambled message and anyone can know public keys N and E, but no-one can decode it without knowledge of number D. But in order to figure out D one needs to know P and Q (prime factors of N) separately, which means one should be able to factor N – a prohibitively difficult task when N is several hundred digits long.

Why it is so difficult to factor the large integer N? For example, anyone can easily factor 35 (= 5•7) or 50 (= 2•5•5), but to factor, say, 16837 (= 113•149) may take some time. In order to find these prime factors by "brutal force", one needs to try successful division on all consecutive primes until the division produces an integer (which, in turn, needs to be checked on primality). Although, there are mathematical methods of factorization which work faster than "brutal force" method, for long enough primes (several hundred decimal digits), these methods are still prohibitively slow. As a rule, the difficulty (and the required time) for factoring increases exponentially with the number of digits of N.

For N which is 200 decimal digits long and which is the product of two primes, each about 100 digits long, there is no known algorithm which can find these prime factors on any present-day computer (unless, of course, we allow the computer to run for billions of years). According to the Prime Number Theorem, the number of primes less that N is (asymptotically) equal to N/ln(N). For N of about 10^{200}, the number of prime factors to be tested is [all primes smaller than SQR(N)] is about 10100/ln(10^{100}) = $10^{100}/230 \approx 10^{97}$. The latter number is greater than the total number of elementary particles in the whole visible Universe, the latter is estimated "only" as about 10^{90}. No ordinary (classical) computer can test that many primes to find factors of N. Thus, the entire reliability of the RSA communication protocol is based on the fact that it is beyond the capacity of the existing computers to find (in a reasonable time) the prime factors P and Q of the large composite integer N.

The major potential problem, in fact a challenge, which QC brings into this game is that QC, at least, in principle, can factor any number in the so called *polynomial time*, as opposed to an ordinary ("classical") computer with can only do it in *exponential time*. Polynomial time means that the time required for the factorization increases as some power of the number of digits in N. For N with several hundred digits polynomial algorithms perform enormously faster than the exponential algorithms (on classical computers). For large N some polynomial algorithms (one was discovered by Peter Shor in 1994) can run on QC, but so far no polynomial factorization algorithm which can run on classical computers was discovered.

7 Quantum computing and non-locality

One of the key ideas of quantum physics is the Superposition Principle which lies at the heart of QC. Although there are many popular explanations of it (such as already mentioned "Schrödinger's Cat"), for QC the usual conceptual illustration is an (infinite) set of identical computers each performing same algorithmic calculation on all possible values of the input. Because all possible algorithmic inputs form a countable set (according to a classification of infinite sets by Georg Cantor, 1845-1918), the set of all possible integers constitutes an exhaustive set of all possible inputs. Each computer running its "own" input produces its own output of a given algorithmic calculation.

According to David Deutsch, one of the key founders of QC [10], one can envision each separate QC as performing a calculation in one of the (countably infinite number of) "parallel universes". In each such universe, QC executes the same program but on different inputs. This situation is often referred as the Many World Interpretation (MWI) of Quantum Mechanics which was first proposed by Hugh Everett in 1957 and since than attained popularity and produced an extensive literature. An enormous level of choices which is provided by the MWI nature of QC can be provisionally referred to as manifestation of the *free will* existing in an anthropomorphic analogy to the free will of the common (human) sense.

In QC information is coded and processed in qubits - quantum bits. In a binary notation each qubit is a quantum superposition of (0) and (1) of classical binary code. Superposition normally adds "0" and "1" with arbitrary weights, e.g., A•(0) + B•(1), where A and B are complex numbers (normalized to unity). When measured, the qubit is always found in a state (0) or (1), but when it is stored and manipulated on QC, it remains in a "suspended" state of a mixed quantum superposition.

8 Quantum communication systems and their quantum-based security

In spite of its enormous potential computer power and speed, QC is subjected to severe physical constrains. For its proper operation, QC needs to maintain the quantum coherent state. This requirement turns into a major weakness, because quantum coherency can be easily destroyed by almost any interaction of the quantum system with the environment (potentially, any noise can do that).

It is to some degree a fortunate circumstance that Quantum Communication Systems (QCS) have less stringent requirements to the degree of quantum coherency and are far less sensitive to weak interactions with the environment. This is one of the reasons why QCS at this moment are somewhat more advanced in terms of their practical implementation than QC. The operation of QCS is based on the use of polarized photons. The direction of angular polarization of photons is used as a basis for the binary coding of the signal. The advantage of QCS is that quantum communication (quantumly coded message) cannot be intercepted without the possibility that a sender and/or receiver can detect the fact of interception. Classical communication systems using ordinary electrical or optical (fiber-optics) signals do not have such an advantage – in these systems interception can go undetected (even if the message later cannot be decoded by an eavesdropper).

This property (non-eavesdroppability) of the QCS is based on the fact that every act of eavesdropping inevitably involves the measurement of the polarization of the information-carrying photon. In quantum physics the act of measurement almost always affects the system in an irreversible way (in terms of changing its quantum state). This sensitivity of QCS turns into a major advantage in terms of its protection against eavesdropping.

9 Normal numbers and information generation by Quantum Computers

If we (theoretically, at least) write down a number, the so called Champernowne constant, C = 0.1234567891011121314151617… (to infinity), this real number (infinite non-cycling string of digits) gives an example of the so called "normal number" (NN). By definition, NN is any non-periodical infinite string of digits in which all combinations of digits of the same length appear with equal probability. It is believed (though it is not rigorously proven) that major irrational constants of mathematics, such as π = 3.14159. . . , e = 2.71828. . . SQR(2) = 1.41421. . ., etc are all NN. Prove of their normality may (or may not) be an eventually unsolvable issue due to the Gödel theorem demonstrating the existence of true but unprovable mathematical statements. However, it was proven in 1909 by Emil Borel that almost all real numbers on the [0, 1) interval are NN with respect of their Lebesgue measure (non-NN form a Cantor set with zero Lesbesgue measure).

From the above definition of NN it follows that *any* possible textual message is contained in *any* NN infinitely many times [11]. In other words, (infinite) decimal expansion of, say, number π contains (in any possible type of digitized coding) an infinite number of complete works of Shakespeare (or any other book for that matter). Of course, among all "books" which can be "extracted" from consecutive segments of any NN (say, π) almost all of them will be a meaningless jumble of letters and yet, somewhere, all "true" books will show up. This was the idea of the famous narrative "*The Library of Babel*" by Jorge Luis Borges (1899 – 1986), which describes a huge (in the limit - infinite) "library of all possible books".

In a certain way QC is a physical implementation of the set of all NN as well as an entity which is potentially equivalent to the Library of Babel. Any quantum superposition is potentially capable of carrying and infinite amount of information. This is because in any qubit, which is the above mentioned superposition A•(0) + B•(1), the ratio A/B can be any complex number, for example, any NN. The latter contain infinite information (actually, all possible information). In practical implementations we, of course, are working on a finite basis, to which the infinity (e.g., infinite informational content) is an asymptotic limit.

The principle advantage of QC is that they can be programmed to select a meaningful and targeted information out of an enormous ocean of gibberish contained in almost any NN. One can say that properly programmed QC can filter out informationaly rich messages from the background noise. Symbolically, this amount to the possibility of picking up the "right" book from the shelves of the Library of Babel.

10 Challenges to the privacy, intellectual property, and the safety of the creative effort

It is becoming obvious that if QC will reach a stage of widespread technical implementation (and perhaps, even mass production), it will open up serious social challenges. The almost unlimited capacity of QC to generate meaningful information, pieces of art, studies in mathematics, etc (it all can be enhanced by many orders of magnitude in comparison of what pre-QC computer technology can produce) - all that is bound to affect the existing notions of information ownership, intellectual property, copyright and authorship. It is quite possible that these developments may trigger some kind of a neo-Luddistic reaction with its implications to social stability and the overall societal safety [12].

As an information-generation technology, QC has a number of pre-courses. One such fantastic machine was described by Jonathan Swift (1667 -1745) in his "Gulliver Travels". Scientists on the flying island Laputa used rotating cubs with words to generate various texts. Recently, so called "Dada engines" (computer programs) were used to automatically produce scientifically-looking articles. Use of QC can drastically amplify the capacity of such programs. These developments, though fascinating, may lead to the questioning of the stability and safety of the creative efforts of individuals.

Due to the deeply ingrained sense in most people of the value of own individuality, it is highly unlikely that the present level of the creative output of the humanity in sciences, arts, literature, or music can be sustained in the society with mass anonymous production of information. Most people will be demotivated to create. In a way, QC may well move plagiarism (which is one of the key threats to the creative effort) to its new, much higher, "quantum" level. Likewise, modern copyright and patent systems will be under a threat of dismantling or radical reforms (with QC "anybody can discover or invent anything").

Another aspect of QC, QCS and other quantum-based technologies may be an emergence of a post-Orwellian (or trans-Orwellian) society which instead of being controlled in centralized way (“Big Brother”) will decent into lawlessness and anarchy. In such a society there will be no more secrets and no more confidentiality (QC will beat any attempt to have or keep secret information). Society in which “everybody knows everything” may appeal to some, but it is unlikely it will be welcomed by the majority. At any rate, QC will likely to lead to some form of a conflict between individuality and collective consciousness.

A matter of special interest is whether QC result in a simulation of the true human consciousness (or perhaps, exceeding it). Recent discourse (mostly on the Web) discusses such possibilities in terms of “Superintelligence” (sometimes called “Ultraintelligence”). These can be defined as a capacity to radically outperform the best human brains in practically every field, including scientific creativity, general wisdom, and social skills [13-15]. On a radical side of this thinking are the notions of Singularity and Transhumanism. Some futurologists (Nick Bostrom, Eliezer Yudkowsky, etc.) predict on the basis of extrapolation of the present trends a state of almost unlimited (“singular”) explosion of new technologies which, in a sense, make humans obsolete. Not as fantastic as they may appear at first glance, these predictions are based, at least partially, on an enormous anticipated power of QC for simulation of human intelligence. In the limit of it, QC simulated reality may become indistinguishable from the “actual” reality. Nick Bostrom recently went as far as to suggest that there is a finite (and not small) probability that we are, perhaps, *already* may be “virtual people” who “live” inside some huge computer simulation on some supercomputer, which is most likely a QC [16].

11 Conclusion: looking to the future

The trust of this paper was to indicate that the present trend in moving communication and information generation technology to a quantum level is most likely to open up safety issues of a qualitatively new type. Not all details of these emerging safety concerns can be assessed and even predicted at the present, still incipient, stage of development. Specifically, a potentially almost unlimited power of QC will likely render obsolete our established notions of confidentiality and privacy. At the same time, the situation is perhaps not without its bright spots.

Some possible “control valves” hidden in the emergent quantum technology may stem from some most fundamental aspects of mathematics and logic which inevitably lie behind the operation of any computer system, quantum or not. In terms of safety and stability of society, one such escape clause may be due to one of the central results of the 20-th century logic known as Gödel incompleteness theorem (GIT) or undecidability theorem [17]. It says that that there are some mathematical statements which are either true or false but that there are no means in mathematics (even in principle) to find out (and proof) if they are true or not.

The latter is a result of a mere structure of mathematics, the metaphor for which is the ideal Platonic World of Numbers [18, 19], it does not depend on any "physics" or a particular technology. Thus, GIT remains true within any physical model of the world, quantum or classical. In classical physics such an effect as anharmonicity leads to the symmetry breaking in molecular forces (and, among other things, is responsible for the thermal expansion of solids). Using such an analogy as a mere illustration, one can invoke GIT to argue that any computer technology, even QC, will always have some inherent limitations and these, eventually, can turn out to be safeguards against possible perils of the emerging quantum technology.

References

[1] Berezin, A.A. Quantum effects in electrostatic precipitation of aerosol and dust particles. *Air Pollution XIII*, ed. C.A. Brebbia, WIT Press: Southampton, pp. 509-518, 2005.

[2] Berezin, A.A. Energy, information, and emergence in the context of ultimate reality and meaning. *Ultimate Reality and Meaning*, 24, pp. 256–273, 2002.

[3] Kurzweil, R. *The Age of Spiritual Machines: When computers exceed human intelligence*. Viking Press, New York, 1999.

[4] Feynman, R.P. Simulating physics with computers. *International Journal of Theoretical Physics*, 21, pp. 467-488, 1982.

[5] Pincock, S. *Codebreaker – The History of Codes and Ciphers, From The Ancient Pharaohs to Quantum Cryptography.* Walker & Company, New York, 2006.

[6] Du Sautoy, M. *The Music of the Primes: Searching to Solve the Greatest Mystery in Mathematics*. HarperCollins, New York, 2003.

[7] Riesel, H. *Prime Numbers and Computer Methods for Factorization*. 2nd ed., Birkhäuser Boston, 1994.

[8] Derbyshire, J. *Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics*. Joseph Henry Press, Washington, D.C., 2003.

[9] Plichta, P. *God's Secret Formula: Deciphering the Riddle of the Universe and the Prime Number Code*. Element Books, Inc. Rockport, Massachusetts, 1997.

[10] Deutsch, D. *The Fabric of Reality*. Allen Lane - Penguin Press, London, 1997.

[11] Berezin, A.A. Variational principles, Occam razor and simplicity paradox. *Bulletin of the American Physical Society*, 49 (2), p. 43, 2004.

[12] Noble, D.F. *Progress Without People*. Between the Lines Press, Toronto, 1995.

[13] Kurzweil, R. *The Singularity is Near" (when humans transcend biology)*. Penguin Books, New York, 2005.

[14] Minsky, M. Will Robots Inherit the Earth? *Scientific American*, Vol. 271(4), pp. 109-113, 1994.

[15] Moravec, H. *Robot: Mere Machine to Transcendent Mind*, Oxford University Press Inc., New York, 1999.

[16] Bostrom, N. Are You Living in a Computer Simulation? *Philosophical Quarterly*, Vol. 53, No. 211, pp. 243-255, 2003.

[17] Goldstein, R. *Incompleteness: The Proof and Paradox of Kurt Gödel*. W.W. Norton & Company, New York, 2005.

[18] Penrose, R. *Shadows of the Mind*. Oxford University Press Inc., New York, 1994.

[19] Berezin, A.A. Isotopic diversity in natural and engineering design. *Design and Nature II*, ed. M. Collins & C.A. Brebbia, WIT Press: Southampton, pp. 411-419, 2004.