Quantum computing: Its emergence and implications on information security

Mark Pecen
Chairman, ETSI TC Cyber Working Group for Quantum Safe Cryptography (QSC) (France),
Chief Operating Officer, ISARA Corporation (Canada)
Board member, Institute for Quantum Computing, (Canada)

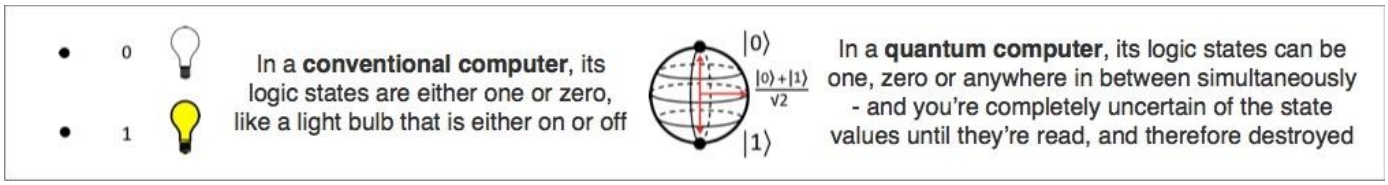
Mark Pecen, mpecen@approachinfinity.ca
April 2017

Leading governments around the globe, along with major corporations, including IBM, Google, Microsoft, have all made substantial investments in the development of large-scale quantum computers, just in the past decade. There's a reason for this prescient obsession.

What exactly is quantum computing?

Quantum computing is basically the combination of information theory and quantum mechanics. At first, this combination of domains may appear obvious. But if we think a little bit more deeply, we might notice that these two domains are probably the most unlikely combination. This is because information theory, used by your computer, smartphone, etc., is characterized by a high degree of certainty: states that are on or off, one or zero. A conventional computer treats each state like a light bulb that is on or off, one or zero.

On the other hand, quantum mechanical phenomena, such as is used in the laser or magnetic resonance imaging, is associated with a high degree of uncertainty: states that may be one, zero, or somewhere in between simultaneously. In a quantum computer, a quantum bit, or "qubit" can be on, off, or anywhere in between – *all at the same time!* This is like a light bulb that's on and off at the same time, which is, in the classical sense, impossible. So, if your quantum computer has, for example, 16 qubits, it can exist in 2^{16} = 65,536 states simultaneously.



How is this even possible? This may be the obvious first question that comes to mind, but if we think slightly more carefully, it may not be the best question. Instead, we might ask: "How can we use this interesting property to perform commercially important work?" Because it turns out that the quantum computer can solve certain classes of very difficult problems extremely rapidly and easily [1]. In fact, the quantum computer can solve certain problems that were thought to be impossible or impractical to solve within a reasonable time-frame. What makes quantum computing possible today is the use of quantum error correction – a method that resolves the uncertainty of quantum states. This means that a quantum computer enables us to calculate *with certainty* by using the effects of *uncertainty* [2].

Does this mean that a quantum computer is always faster than a conventional computer?

Not necessarily. The quantum computer excels at solving certain classes of mathematical problems. One such problem is the so-called "travelling salesman problem". To solve this problem class, the most optimal path between two points is chosen by a conventional computer by brute force, i.e. by evaluating each individual path separately, which could be time-consuming. A quantum computer can solve this problem extremely rapidly because your answer would exist because of constructive and destructive interference, the terminal states of which are known the instant that the qubits are read [3]. Certain other classes of problems may not lend themselves to solution by a quantum computer, and therefore do not execute much, if at all, faster.

But for certain types of problems, the quantum computer may revolutionize the world. Such problems include the synthesis of new chemicals and materials, modeling the action and effects of drugs on biological systems, advanced navigation systems, weather modeling, and other areas. It could completely disrupt regulators' drug approval process, creating a standard

algorithm for clinical trials, thus bringing treatment to market faster. Quantum computing brings many more academic and commercial possibilities to the world as we move forward into the future.

What about the impacts of quantum computing on information security?

It turns out that quantum computers excel at solving certain mathematical problems that are intentionally designed to be difficult or impossible to solve. These are the problems on which certain public-key cryptographic algorithms are based – the problems that protect your information, such as credit card numbers, identity information, military secrets, etc. These problems include the integer factorization problem and the discrete logarithms problem on which security systems such as Rivest Shamir Adleman (RSA) and Elliptic Curve Cryptography (ECC) are based [4 – 5]. They are two of the public-key cryptographic methods most widely-used to secure the Internet and wireless systems today. In addition, authentication methods based on these concepts are also at risk. Basically, all public-key cryptographic systems can be broken by a sufficiently powerful quantum computer, and this also means that even everything that is stored in encrypted form can eventually be indiscriminately decrypted [6].

What is being done to secure the future in a quantum world?

Fortunately, there are cryptographic techniques that are resistant to attack by both quantum computers and conventional computers alike. At present, these include cryptographic techniques that are code-based, lattice-based, or quadratic-multivariate-based, along with hash-based schemes for cryptographic signatures. They work because the underlying problems used by these techniques do not lend themselves to rapid solution by either a quantum computer or by a conventional computer. In addition, industry standardization groups have been forming around how to implement and deploy these quantum-safe techniques. The European Telecommunication Standards Institute (ETSI) created a group in March 2015, now called Technical Committee Cyber for Quantum Safe Cryptography (Cyber QSC) specifically to address these issues [7]. Since that time, the U.S. National Institute for Standards and Technology (NIST), the Internet Engineering Task Force (IETF), 3rd Generation Partnership Project (3GPP) and others have launched quantum-safe standardization efforts, each addressing different aspects of the greater problem domain.

For example, Cyber QSC addresses the problems associated with implementation, performance and architecture of real-world systems, while NIST addresses the algorithms themselves and IETF addresses the adaptation of existing security solutions to those that are quantum-safe. The notion of “quantum-safeness” is still somewhat of an emerging area, and we expect to hear much more over the coming months and years. Nevertheless, as quantum computing advances are reported on a regular basis, security experts and their clients work to ensure a quantum safe future.

Stay tuned to the Safeguard blog for future insight on quantum computing and its emerging significance.

References:

[1] "A fast quantum mechanical algorithm for database search", (Lov K. Grover, STOC 1996, pp 212-219), ACM 1996
[2] “Introduction to Quantum Error Correction”, (Emanuel Knill, Raymond Laflamme, Alexei Ashikhmin, Howard N. Barnum, Lorenza Viola, and Wojciech H. Zurek; *Los Alamos Science*, No 27), 2002
[3]"Surface codes: Towards practical large-scale quantum computation", (Austin G. Fowler, Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland; Phys. Rev. A 86, 032324), September 2012
[4] Peter W. Shor: "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM Journal on Computing, 26(5):1484-1509, 1997
[5] "Applying Grover's Algorithm to AES: quantum resource estimates", (Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt), December 2015)
[6] *Quantum Safe Cryptography and Security: an introduction, benefits, enablers and challenges,* (Pecen, et al.; European Telecommunication Standards Institute (ETSI), ISBN No. 979-10-92620-03-0), June 2015
[7] Technical Committee Cyber for Quantum Safe Cryptography (TC Cyber QSC), (European Telecommunication Standards Institute, Sophia Antipolis, FRANCE), https://portal.etsi.org/tb.aspx?tbid=824&SubTB=824,856