

Quantum Information and Security

By Andrea Pasquinucci

Introduction

One duty of a Security Professional is to prepare her/himself for what could happen tomorrow. Moreover, when planning or assessing ICT Security Systems, it is important to consider not only today's threats and vulnerabilities, but also possible future scenarios.

One quite interesting field that will affect the future landscape of ICT Security is *Quantum Information*. Quantum Information can be briefly described as the discipline that studies how information can be encoded in elementary particles and what can be done when information is encoded in this way. Quantum Information today is mostly still a branch of pure research in fundamental physics, with some striking practical applications. From the end of the 1960s, physicists have been studying how to use elementary particles directly in computer applications—encode bits (of information) in them.

The principle interest for doing this is that elementary particles follow laws dictated by the theory of Quantum Mechanics and their behavior under many aspects is quite different from that of any object we deal with everyday. There are profound differences between the *Classical* laws of physics we all well know, from Newton's dynamics to Maxwell's electromagnetism and even Einstein's relativity, and Quantum Physics. For example, it is not usually possible to *measure* an elementary particle without modifying it, which also implies that it is impossible to make exact *copies* of it. This is quite different from our direct experience with macroscopic objects, which we can measure without modifying and of which we can make identical copies. Thus, elementary particles behave very differently from the objects we are used to handling everyday and it is possible to exploit this fact to do something really new.

Quantum Computers are based on the idea of encoding the value of a bit in a property of an elementary particle. As a trivial example, we could assume that if a particle is spinning clockwise, the value of the bit is 1 and if it is spinning counter-clockwise the value is 0. Thus, instead of having electrical currents inside our CPUs, we should imagine having elementary particles, each one carrying the value of one bit. A bit encoded in an elementary particle is called a *quantum bit*, *qubit* for short, and operations in these quantum CPUs are done by transforming the status of the elementary particles.

Shor's algorithm is the most famous algorithm that can be implemented on a Quantum Computer. This algorithm finds in *short time* (technically *polynomial time*) solutions to mathematical problems like the 'factorization problem' (how to factorize the product of two prime numbers) or the 'discrete logarithm problem'. With conventional computers, these problems are very hard to solve in the sense that if the numbers involved are large (at least a few hundred decimal digits) with current known (classical) algorithms and all the computer power available, it could take hundreds if not thousands of years to solve. Instead a Quantum Computer would do it practically instantaneously.

The security of the asymmetric, also called public-key, algorithms, like the famous RSA, are based on such mathematical problems, and a Quantum Computer would make them all insecure!

Are They Real?

Do Quantum Computers exist? Prototypes have been built, the biggest of which was built in 2001 by IBM and factorized 15 in 5 times 3. Even if this does not look like a big result, it is enough to make us think about not if but when Quantum Computers will arrive. Quantum Computing is still in its infancy and could mature in 5 to 100 years. How long it will really take is very difficult to say, but, for example, a Canadian company believes it can build the first commercial Quantum Computer by 2008, even if this first model will not be able to run Shor's algorithm and will not be able to break asymmetric cryptography. If history taught us anything, it is that the future can arrive much sooner than expected. Just think about the history of computers in the last 30 years from the birth of the first personal computer to today.

As security experts we should be aware of all possible limitations of the technologies we use. Suppose, for example, that our company has invested in systems and technologies to manage securely all company digital documents. This obviously would be a big and long-term investment with technological, organizational and management costs. And, inevitably today, asymmetric cryptography would be one of the technical pillars of its security.

Did we consider what could happen if Quantum Computers will arrive soon? (Obviously the same holds for any other development that would make asymmetric cryptography insecure.) It is important to understand if this is a threat to our system and how remote it is. We need to understand how we should manage this risk and if we should have some countermeasures in place. It could be that we do not need to worry about Quantum Computers, but this decision must be based on the appropriate evaluation. If a big investment has been done, which usually is expected to give a return over the next years, we should be prepared if something foreseeable happens and know what it could mean, and also what it could cost, to act accordingly. If asymmetric cryptography will not be secure anymore, we better know what we should do to substitute it with something else and how costly that will be.

If Quantum Computers today are seen mostly as a threat to ICT Security (obviously they can do other computations, but as of today these are not particularly relevant to security), Quantum Cryptography instead provides us with a security tool believed to be extremely secure.

Quantum cryptography is actually a misnomer—the correct name is *Quantum Key Distribution* (QKD). By encoding bits in elementary particles,

in practice photons, and exchanging them, QKD protocols create and exchange secret keys between two parties. The laws of Quantum Physics guarantee that any attack that could disclose to a third party any information on the secret key while created and exchanged is detected by the two generating parties. Thus, the two parties creating the secret keys know if they have been eavesdropped by someone else. Of course, these results are valid only for the QKD system itself, an attacker can always adopt other strategies to learn the secret keys, from social engineering to physical attacks. Today QKD is much more developed than Quantum Computers, indeed commercial products are already on the market. Moreover, both in Europe and in the US there are large research projects publicly financed to speed up the deployment of QKD. For example, the EU has financed a very large Information Society Technologies (IST) project in QKD, under the Sixth Framework Programme (FP6). This Integrated Project is called *Development of a Global Network for Secure Communication based on Quantum Cryptography* (SECOQC). It involves companies, universities and research centers and aims at realizing a *fully functional, real-time, ready-to-market Quantum Key Distribution point-to-point communication technology*. In other words, the main purpose of the project is to make QKD available to the average ICT Security department. In the US, DARPA has sponsored and financed the *DARPA Quantum Network*, which involves numerous universities and research centers with the aim to build a fully interoperable secure ICT network based on various QKD technologies.

QKD systems have a very well defined and unique purpose—to create and exchange secret keys—but today are still expensive and difficult to implement. Besides the instruments needed to manipulate single photons, today QKD requires optical fiber connections without any repeater, even if free-space QKD, also through satellites, could arrive in the near future.

Criticisms of QKD


One of the main criticisms often heard about QKD is that it is an *expensive solution to a non-existent problem*. Obviously this statement has a part of truth in it, but it should be understood within its correct context. It is true that as of today, asymmetric cryptography, using the Diffie-Hellman algorithm for key exchange, can accomplish similar tasks as QKD in a much easier, less expensive and much more portable way. Moreover, critics say that the security of a full QKD system is still yet to be fully understood, because besides the *quantum* part of the system, it must also be connected to a network, have a managing console, reporting devices, etc. All these *classical* parts interact with the secure QKD system and can have vulnerabilities that could spoil the security provided by the quantum part. Obviously these are all aspects that are and will be addressed in the first generations of QKD devices.

But what it is important for us is that QKD should be considered as a possible technology to adopt in the future. Besides the current cost of a QKD system, which is likely to change dramatically in the next few years, it could be useful to think now if our security infrastructure can accommodate QKD without any major restructuring. It would be nice to be prepared for when Quantum Computers arrive. Our security infrastructure will include QKD as one of its tools.

Conclusion

In the last 10 years, the field of Quantum Information has brought many surprises to Information Technology and in particular to Security. Still this field is dominated by quantum physicists, but more and more computer scientists and cryptographers are getting interested in this subject. For example, the IST FP6 project ECRYPT (Network of Excellence in Cryptology) organized an inter-

national conference in May 2006 entitled *PQCrypto 2006: International Workshop on Post-Quantum Cryptography*. The main subject of this conference was to debate the following two questions: Will large quantum computers be built? If so, what will they do to the cryptographic landscape?

But as we have seen, not only should researchers consider Quantum Information, but also security experts must start considering which threats or tools Quantum Information can bring to them in the near future. 

Andrea Pasquinucci, PhD, CISA, CISSP, works as a senior security professional.