# Towards new cryptographic concepts 2/2

General Military Review No. 54

le chef de bataillon Mathieu MORALES

Published on 22/03/2019

Sciences & technologies

**The quantum computer**

**Moore's famous law predicted that the number of transistors on a microprocessor would double every eighteen months. Based on these calculations, by 2020, the size of a transistor will approach that of an atom, marking the end of Moore's Law as the need for computing capacity continues to increase. It was therefore necessary to imagine a new type of computer using the quantum properties of the atom.**

Three concepts of quantum physics are of particular interest to researchers in the field.

First, quantum superposition. It is accepted in quantum physics that a particle can be in an indeterminate state or rather in several states at the same time. Like a lottery ticket that, until the draw is made, is neither a winner nor a loser, but a superposition of these two states weighted by a certain probability.

Second, quantum entanglement. Although this subject is still the subject of much research, it is possible to bind several particles together so that they continue to form a single system regardless of the distance between them. An operation on one will affect all the others.

Finally, quantum decoherence. The quantum properties are retained as long as the system is isolated and has no contact with the outside world. However, in order to exploit the results, a measurement is necessary. Thus, to use the analogy with the lottery ticket, the latter is in a state of superposition (both winning and losing) until the draw. Once this measurement is made, the ticket becomes either a winner or a loser and regains properties of classical physics.

It is on this basis that researchers imagine how the quantum computer works. Thus, whereas classical computer science sequentially manipulates bits that can be either 0 or

1, quantum computing uses simultaneous quantum bits or qbits, which take as their value a superposition of 0 and 1. The time savings are considerable because a ten-qbit quantum computer will be able to test all combinations of ten bits in a single computation where a conventional computer would require 1024 operations (i.e. 210 operations). Algorithms already exist but are not yet efficient enough on current machines. The best known is the SHOR algorithm, which decomposes prime numbers into operational times that would make crypto-systems such as RSA obsolete.

In practice, research faces several complications since the manipulation of quantum elements requires very specific physical conditions, including isolating the particles at temperatures close to absolute zero and maintaining quantum coherence long enough to perform all the calculations. However, research is progressing and the question is no longer whether the quantum computer, as we imagine it, will exist, but when it will exist. Large companies such as IBM, Microsoft, Google and ATOS have engaged in research on the computer.

quantum and the announcements are multiplying. IBM has been allowing researchers to try out their algorithms on a five-qbit computer for the past year and promises a 50-qbit processor.[58] in the years to come. The NSA, for its part, has invested $80 million through the "Penetrating hard targets" program to acquire a computer powerful enough to decipher all secure Internet connections.

**Modern Cryptography**

Faced with these technological advances and the threat posed by quantum computers to the security of communications, two fields of cryptography have recently emerged.

Quantum cryptography makes it possible to protect against quantum attacks by quantum means, particularly in transmission modes. In this field, China has a head start, since it managed last summer to achieve the first intercontinental communication with an inviolable cryptographic system between Vienna and Beijing. The communication takes place by conventional means, but the encryption key is transmitted by quantum means. Until now, this kind of transmission has been done by optical fibre, which limited the transmission distance to 200 km. This technological leap was made possible by the Micius satellite, which was launched into orbit on 16 August 2016. Able to manufacture and transmit pairs of interlocking photons, it ensures that both communicators have the same key. Quantum decoherence ensures that the key has not been intercepted, because if it were, the system would lose its quantum character and the recipients, noticing the attack, would not use the key. The quantum communication test is expected to be repeated soon between Beijing and Singapore, and then with Italy, Germany and Russia, and could pave the way for a global quantum Internet network.

The second area of study is post-quantum cryptography. Because of their cost and their particular conditions of use, quantum means are not likely to become popular and replace all current information systems. The challenge for this branch of cryptography is to design new protocols for conventional information systems that would resist a quantum attack. Every year, the PQ-Crypto conferences bring together researchers in the field to present and compare new algorithms and mathematical concepts that could form the basis of tomorrow's exchanges.

The "Jean-Claude Cassaing Innovation Prize" was awarded on 14 April 2017 to Jean-Christophe Deneuville for his work on "Contributions to post-quantum cryptography". In his thesis[59]he proposes different protocols based on alternative mathematical tools

(Euclidean networks and error-correcting codes) a priori resistant to these new computers. These protocols are, in the long term, destined to replace the existing ones in order to provide the same security guarantees. Some of the work of this thesis will be proposed soon to the American standards agency (NIST) for their large-scale use.

## Conclusion

As massive attacks multiply and more and more security and data transmission vulnerabilities are exposed, advances in quantum computing are challenging the very foundations of all current security protocols. Some states are investing considerable sums of money to be the first to adopt these technologies and thus to master communications. It is true that these supercomputers are not yet fully operational, but the race is on and performance is increasing at an ever-increasing rate. In view of the time needed to update and standardize exchange protocols, palliative measures must be thought out and even tested now.

Thus, the coming years will be dedicated to redefining cryptographic concepts and secure transmission protocols to deal with interception threats to the confidentiality of information.

An engineering officer, Battalion Commander Morales spent his early career in aeronautical engineering at 1 Airfield Engineering Operational Company. As part of his technical degree, he completed a specialized master's degree in information systems management at Centrale-Supélec.

**57** Pretty Good Privacy: free cryptography software.

**58** There are inaccuracies in the definitions of qbits and quantum computers. The D-Wave company, for example, announces the marketing of a 2,000 qbit quantum computer, but it is in fact a quantum simulator capable only of solving very specific optimization problems. At present, it would appear that the best quantum computers have a power of around 17 qbits.

**59** Thesis available at: http://www.unilim.fr/pages_perso/deneuville/files/phd_thesis.pdf

**Title :** le chef de bataillon Mathieu MORALES

**Author (s) :** le chef de bataillon Mathieu MORALES

**Release date** 14/03/2019