SCIENCE AND TECHNOLOGY BRIEFINGS
PARLIAMENTARY OFFICE FOR SCIENTIFIC AND TECHNOLOGICAL ASSESSMENT

Briefing 18 — July 2019

Quantum Technologies: Quantum and Post-Quantum Cryptography

Source: Nmedia/AdobeStock

Summary

- *Communications, whether terrestrial or by satellite, are central to our society, and effective tools have been developed in recent decades to secure data exchanges and guard against attacks.*
- *However, quantum computing and its potential computing power pose a threat to data encrypted using these methods, which quantum computers could decrypt in record time.*
- *To respond to this threat, two main and complementary aspects are being developed: post-quantum cryptography based on new mathematical concepts to encrypt communication protocols and quantum cryptography which uses the properties of quantum physics to secure data transportation.*
- *While quantum computers will only become widespread in the medium or long term, the various players must prepare for this transition to new encryption protocols to respond to strategic and sovereignty issues.*

Mr. Cédric Villani, MP (National Assembly), First Vice-Chairman

Our society is increasingly based on communications, i.e. the exchange of information.(1) Current technology allows us to exchange data over long distances and at very high speeds via terrestrial, submarine or satellite links. If two people wish to communicate confidentially, they must **encrypt the data exchanged** to prevent a third party from intercepting it, and the sender must use a **digital signature**(2) (like a physical signature) to prove the authenticity of their message and prevent it from being falsified. In many cases, whether the sensitive data come from the government (defence or diplomacy), companies (finance, space, etc.), or individuals (passwords, credit card codes, etc.), a security breach can have serious consequences. **The power of quantum computing is perceived as a threat in this regard because it will eventually allow for new attacks against some of these secure protocols.**

Current encryption methods

The earliest cryptography techniques date back to antiquity. Until the 20th century, they were generally based on a clever code using the letters of the alphabet. The protocols gradually became more complex until the German "Enigma"(3) machine whose cryptanalysis(4) became a major issue during the Second World War. In the 1940s, Claude Shannon's work laid the foundations of information theory(5) and created a rigorous framework for studying potential attacks against ciphers. In the 1970s, the US *National Institute of Standards and Technologies* (NIST) offered the first encryption standard, called the *Data Encryption Standard* (DES)(6) used in US administrations. Then, in the 1980s, using arithmetic problems paved the way for new methods of cryptography. Today, data encryption (and decryption) relies on complex mathematical techniques **that must continually adapt as computers' power and computation speed increase**. Two major types of methods are used.

First, **symmetric cryptography**, such as "historical" techniques and for which a **secret key** (for example, the number 5), **is used to encrypt and decrypt messages**. Both participants (traditionally called Alice and Bob)(7) know this key beforehand. To give a concrete and simplified example, if Alice wants to send the number 4 to Bob, she can encrypt it with the key 5 to give 9 = 4+5 and Bob will have to calculate 9-5 to find the message.(8)

Before sending any messages using symmetric encryption, Alice and Bob must "agree" on the secret key they will use. Nevertheless, they cannot exchange this key unencrypted on the network, otherwise any observer could decrypt their conversations. **Asymmetric encryption** solves this issue since it allows encrypted messages without agreeing on a shared secret beforehand. To do this, Alice creates **two separate keys** (hence the asymmetry): a **public encryption key** (for example a number) that anyone on the network can access, and a **private decryption key** that only she knows (for example, a unique mathematical method to calculate this number). If Bob wants to send a message to Alice, he uses Alice's public key to encrypt it, so that only Alice can decrypt the message with her private key.(9)

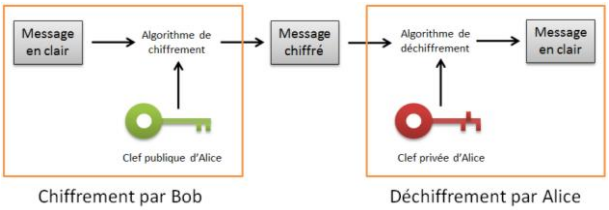

FIGURE 1. THE PRINCIPLE OF ASYMMETRIC ENCRYPTION PROTOCOLS BETWEEN TWO USERS "ALICE" AND "BOB"

In practice, many encryption methods are used, often using symmetric and asymmetric techniques in a hybrid manner. Symmetric cryptography, which can encrypt several gigabytes of data per second, is used to secure digital data and everyday communications.[10] Asymmetric algorithms are slower (a few megabytes per second) and are mainly used to exchange secret keys ahead of these symmetrical communications. These are based on mathematical problems that are complex for a computer, such as a discrete logarithm.[11] Historically, the best known is **RSA encryption, whose decryption is based on prime factorization** (see box). This problem is **particularly difficult for classical computers to solve**: in 2010, during an experiment[12]developed to factor a 232-digit number, several hundred computers had to run for 2 years. The key standard used today is 617 decimal digits encoded on 2048 bits (RSA 2048). It would take a time "greater than the age of the Universe" (13.8 billion years) for the best computers to succeed in finding the prime factors (the secret key) that comprise it using current algorithms.[13]

The threat of quantum computing

Since the 1990s, researchers have highlighted the fact that **quantum computers, while potentially very powerful but then still hypothetical, could decrypt some ciphers in record time**. The **Shor algorithm**, invented in 1994 to work on a quantum computer, can factor integers exponentially faster[14] than all known classical algorithms. **It would therefore threaten the security of the current RSA[15]** by finding the private key (and therefore the messages) from the public key in just a few minutes. A variant of the algorithm can also attack other asymmetric ciphers.[16] While huge progress has been made since then, current machines only have a few dozen qubits[17] and are therefore far from an imminent threat since **it would require several thousand qubits to use Shor's algorithm in an attack against RSA 1024 or 2048 keys.[18]**

RSA encryption and factorisation:
Introduced in 1978 by Ronald Rivest, Adi Shamir, and Leonard Adleman (*), RSA encryption (named after its inventors) is based on **prime factorization.** As easy as it is to calculate a product of numbers, for example 503 × 563 = 283,189, the reverse operation, called factorisation, to find 503 and 563 from 283,189 is much more difficult for a computer. The general idea of encryption is to use **a product of prime numbers as a private key, and the value of this product as a public key**. When the integers have several hundred digits, it becomes impossible to identify the private key using the public key.

(*) Ronald Rivest, Adi Shamir, and Leonard Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 21, no 2, 1978, p. 120–126

Using a quantum computer, attacks against symmetric ciphers can also be considered using Grover's algorithm.[19] This would significantly reduce the time needed to exhaustively search for a secret key but, in practice, this vulnerability can be offset by a doubling of the size of the keys. **Other forms of quantum attacks against symmetric ciphers have recently been discovered,[20] which also requires modifying them, but the threat seems less critical than for asymmetric cryptography.**

It is impossible to predict if and when there will be a quantum computer sufficiently powerful to carry out such attacks. Nevertheless, some experts believe that there is a 50% chance that at least one of the existing cryptography methods will be broken in the next fifteen years.[21] Developing new encryption methods takes time as their robustness needs to be thoroughly tested and proven. Thus, **a system is generally considered robust after about ten years of conclusive tests**. On the other hand, **transitioning to these new systems will take many years** depending on the time needed to modify all the algorithms already implemented in applications.[22] Finally, **some of the data we produce today must remain protected for several decades** - up to 60 years for the most sensitive national defence data. Therefore, it is important to encrypt them with a protocol that cannot be broken in the years to come. Despite the level of uncertainty surrounding quantum computing, **it seems prudent to develop cryptography that is resistant to this new threat, hypothetical and incomplete though it may be.**

Towards a post-quantum cryptography

In light of this, the US National Institute of Standards and Technology (NIST) launched a global call for projects in 2017[23] to define new **"post-quantum" cryptography standards, i.e. resistant to attacks from quantum computers** for encryption, digital signatures, and key exchanges. While research had already been carried out in the field, it had remained mainly

theoretical; the NIST call united the global cryptographic community towards a concrete goal.[24] These methods are again based on abstract mathematical problems of various natures.[25] In total, 82 algorithms[26] from 26 different countries have been proposed. In January 2019, 26 candidates were selected,[27] of which a dozen came partially from French researchers, notably from INRIA and CNRS, following an initial selection phase led by NIST that drew on the many works of international experts. One or two additional phases are scheduled from now until 2022 to identify the most resistant algorithms and the new cryptography standards. For its part, China has launched its own competition, officially open to all, but on an untranslated platform written in Mandarin.

In France, the **RISQ project,**[28] **called "Digital Grand Challenge"** as part of the Invest in the Future Programme, aims to consolidate French skills in post-quantum cryptography. It has united several players from business (Thalès, Secure-IC, CryptoExperts) and academia (INRIA, CNRS) to give the French cryptographic sector weight in defining new standards.[29] **France has some of the best experts in post-quantum technology and, more generally, excellent research and teaching in cryptography that should be showcased, especially in business.**

Nevertheless, there are many obstacles in transitioning to these new methods: they are not yet mature in either design or implementation and will not be so before 5 to 10 years of study. The situation is similar to that of the RSA protocol in the 1990s: as soon as it was discovered, it generated a lot of enthusiasm, yet the first years of its use revealed that using it required many precautions[30] because the research lacked perspective. In this context, it is important **to avoid a regression towards asymmetric key exchange methods that are vulnerable to classical computing**. To maintain at least the level of security that has existed up to now, **ANSSI**[31] **recommends a hybrid solution in the short and medium term: combine a proven classical method with a post-quantum method.[32]**

Entanglement and quantum cryptography

Alongside post-quantum cryptography (which in fact relies on classical encryption algorithms), **quantum cryptography**[33] is being developed to prepare a new generation of communications protection. It uses the principles of quantum mechanics such as superposition and entanglement (see box text) and is based on the physical properties of the medium carrying the communication. In a very general way, quantum cryptography can be used to generate local or remote keys[34] and then use them in classical (symmetric or asymmetric) or, in the future, post-quantum encryption protocols. Concretely, we encode the information that we want to exchange using the state of a quantum physical system (a state corresponds to one piece of information). The most prevalent method right now uses light polarisation[35] via photons, which are light-transmitting particles.

This method consists in producing single photons by means of a specific source (most often a semiconductor quantum dot).[36] The information is then encoded using a characteristic of the photon, such as its frequency or its polarisation. In accordance with the principle of superposition, there exists a quasi-infinity of states for this photon[37], unlike the classical binary case where information can only take values 0 or 1. User A can then send their information encrypted using the state of a single photon in the clear to user B, who can read it. This method can be used to share a public key, for example.

In addition, by means of another source of photons (a non-linear crystal[38] for example), a pair of entangled particles can be produced to encode the information on a quantum object comprised of two "subsystems" that will remain entangled from creation until detection. In quantum mechanics, measurement "disturbs" the state of the system. Prepared in perfectly predefined initial states (for example, in terms of polarisation or frequency), the two photons are sent to users equipped with calibrated detectors. The two previous properties ensure that **a measurement by user A has an instantaneous impact on user B**. Very useful for sharing private keys, this method, called **Quantum Key Distribution (QKD),**[39] can also detect "intrusions" on a communication network very effectively.

Quantum superposition and entanglement:
In classical physics, a physical object (such as an atom) can be modelled by a point that is at a precise position at a given time. They are unlike waves, which describe a disturbance that propagates in space.
In quantum physics, the two concepts merge to explain the behaviour of objects on an atomic scale: this is called wave-particle duality. We can no longer predict the exact position of a body at a given moment, only the probability of finding it in a given place. These rather counter-intuitive phenomena are behind the two main concepts used by most technologies using quantum mechanics: the superposition of states and entanglement.
With the principle of **superposition**, the overall state of a system at a given moment becomes a combination of all possible states at that moment.
Entanglement connects two quantum objects and their information. A change of state in one leads to a change in the other **instantly**. We must thus consider the pair as a unique, inseparable and global system (the properties of the pair are not simply equal to the union of the properties of the two bodies).

These methods have been made possible by recent technological advances in quantum mechanics[40] that are already reaching advanced levels up to commercialisation. For the elections of the Canton of Geneva, Switzerland, a terrestrial quantum link offered by the Swiss company ID-Quantique[41] has been used since 2007[42] to send online voting records securely over 300 km.[43] **Using photons as a quantum information medium allows us to use existing optical fibre networks and reduce infrastructure costs.** Today, the cost of installing a quantum communication line is estimated at €100,000, with a potential reduction factor of 10 within 5 years.[44] However, quantum decoherence[45] is the main technological obstacle because it limits the distances over which entanglement can be maintained. A whole line of R&D has been set up to develop quantum repeaters, which would synchronously relay the quantum information to two remote locations on the line of communication.

Satellite links are also concerned: in 2016, a Chinese satellite with a quantum source on board was used to distribute entangled photons between two receivers 1,200 km apart[46] instead of just a hundred kilometres as was the case before. The Micius satellite was developed by the *Chinese Academy of Sciences* with support from the University of Vienna. This experiment offers an alternative to limited terrestrial quantum links and opens the way for long-distance and even intercontinental quantum communications, **the first bricks of a potential ultra-secure quantum internet network**. To implement it on a global scale, this network will have to be multiform, i.e. combine satellite links (spatial), as in the Chinese experience, and the existing fibre network (terrestrial). Overall, Asian powers seem to have chosen to invest in the deployment of quantum communications lines[47] while Europe and the United States focus on new post-quantum methods (via the NIST call for projects).

Nevertheless, these various scenarios do not yet allow us to consider replacing classical key exchanges (current or post-quantum) with quantum cryptography in most situations (mobile equipment, internet communications through many intermediate relays, etc.).

Experts consulted

Mr. Alain Aspect, Physicist at the Institut d'Optique (Institute of Optics) and member of the Office's Scientific Council.

Ms. Astrid Lambrecht, Research Director at CNRS (French National Centre for Scientific Research), Director of the CNRS Institute of Physics (INP/CNRS), and member of the Office's scientific council.

ANSSI (Mr. Guillaume Poupard, General Manager, Mr. Vincent Strubel, Deputy Director of Expertise, Mr. Sébastien Kunz-Jacques, Deputy Head of the Scientific and Technical Division, Mr. Henri Gilbert, Head of the Cryptography Laboratory, Mr. Jérôme Plût, Researcher at the Cryptography Laboratory).

Ms. Fanny Bouton, a journalist specialising in new technologies.

Mr. Antoine Browaeys, Research Director at the Institut d'Optique.

Ms. Anne Canteaut, Research Director at INRIA, SECRET project team.

Mr. Philippe Chomaz, Executive Scientific Director of the Direction de la recherche fondamentale (Directorate of Fundamental Research) at CEA (French Atomic Energy and Renewable Energy Agency).

Mr. Thierry Debuisschert, Research Engineer, Thalès.

Mr. Bruno Desruelle, CEO of the start-up Muquans.

Ms. Eleni Diamanti, Research Fellow at the Paris 6 Computer Science Laboratory (LIP6).

Mr. Philippe Duluc, Big Data & Security Technical Director at Atos.

Mr. Daniel Estève, Research Director and Head of the Quantronique group at CEA.

Mr. Olivier Ezratty, a consultant specialising in new technologies and the author of the blog "Opinions libres".

Mr. Adrien Facon, leader of the RISQ Programme and Director of Research and Innovation at Secure-IC.

Mr. Philippe Grangier, Research Director at CNRS and Head of the Quantum Optics Group at the Institut d'Optique.

Mr. Serge Haroche, Emeritus Professor at the Collège de France and the 2012 Nobel Prize winner in Physics.

Mr Christophe Jurczak, Managing Director of the Quantonation Investment Fund.

Ms. Anne Canteaut, Research Director at INRIA, SECRET project team.

Mr. Grégoire Ribordy, co-founder and CEO of the start-up Quantum ID.

Ms. Pascale Senellart, Research Director at the CNRS Laboratory of Photonics and Nanostructures (LPN) and co-founder of the start-up Quandela.

Mr. Sébastien Tanzilli, Research Director and CNRS Quantum Technologies Project Manager.

Mr. Georges Uzbelger, AI/Advanced Analytics Solution at IBM France.

Mr. Benoit Wintrebert, Innovation Advisor at the French Ministry of the Armed Forces.

Scientific coordination by Sarah Tigrine, Scientific Advisor (with support from Mr. Gaëtan Douéneau).

Reference works consulted:

- "Comprendre l'informatique quantique" O. Ezratty, November 2018 (e-book)

- A report from the American Academies: National Academies of Science, Engineering, and Medicine. 2018 Quantum Computing: Progress and Prospects. The National Academies Press, Washington, DC. DOI: https: //doi.org/10.17226/25196.

- "Clefs du CEA" issue no. 66- June 2018 "Révolutions quantiques"

Note: in concurrence with the Ethics Officer of the French National Assembly, Cédric Villani has recused himself from the ATOS Scientific Council - a non-decision-making body - for the duration of his work on quantum technologies for the Office.

References

(1) The concept of "communication" refers to all stages of the information exchange protocol, i.e. generating, distributing, processing, and storing the data.

(2) Also known as "electronic signature", these methods certify that a message comes from the indicated sender and that it has not been modified during routing. Without them, a malicious individual can impersonate something or someone else and send fraudulent e-mails ("phishing"), for example.

(3) The famous Enigma machine was developed by the German Arthur Scherbius in 1919 and was widely adopted by the German army in the 1930s. Using an electromechanical process, it encrypted and decrypted military messages and was considered inviolable. During the Second World War, the Allies, thanks in part to the work of Alan Turing, finally deciphered a large part of the intercepted messages which, according to some experts, shortened the conflict by at least two years (http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF).

(4) The term "cryptanalysis" refers to the process of attacking a cryptographic system to reveal the encrypted message without knowing the key.

(5) *Shannon, C. E. (1948). A mathematical theory of communication.* Bell system technical journal, *27(3), 379-423.*

(6) In 1973, NIST called for a new encryption standard to be defined. IBM proposed its algorithm, called Lucifer. While it had some flaws that were corrected by the NSA, the final version, called DES, was finally implemented in 1976.

(7) Alice and Bob are names that have been commonly used in cryptography since the 1970s, replacing "user A" and "user B".

(8) One can also imagine that the messages are sent in a safe to which only Alice and Bob have the key.

(9) Here, one can think of the public key as a safe and the private key as the code to this safe. Alice sends the safe to Bob and keeps the code. When Bob wants to send a message to Alice, he puts it in the safe and closes it, before sending it. The only person who can open it and read the message is Alice.

(10) Symmetric encryption, via the AES protocol, is used for online transactions, transport cards, Wi-Fi, etc. https://www.larecherche.fr/la-fragilit%C3%A9-inattendue-du-chiffrement-sym%C3%A9trique.

(11) In mathematics, the logarithm of a number Y is the number X such that $2^x = Y$. The discrete logarithm problem consists of finding the integer k such that, given two variables a and b, $a^k = b$. Asymmetric encryption can be built from this problem, using k as the private key and the pair (a, b) as the public key. It is secure (i.e. it is impossible to find the private key from the public key) because discrete logarithms are extremely difficult for computers to process.

(12) *Kleinjung, T., Aoki, K., Franke, J., Lenstra, A. K., Thomé, E., Bos, J. W., ... & Te Riele, H. (2010, August). Factorization of a 768-bit RSA modulus. In CRYPTO 2010 – 30th Annual Cryptology Conference (pp. 333-350). Springer, Berlin, Heidelberg.*

(13) https://www.larecherche.fr/informatique-cryptographie/%C2%AB-la-meilleure-garantie-de-s%C3%A9curit%C3%A9-est-l%C3%A9preuve-du-temps-%C2%BB

(14) Shor's algorithm factors numbers in *polynomial* time (i.e. whose execution time is n^a, where n depends on the size of the number provided and a is a fixed constant). On the other hand, the best classical algorithms for the factorization problem have an almost exponential execution time (2^n), which becomes impossibly longer when the input data is large. For example, 2^{100} seconds is greater than the age of the universe.

(15) In addition to RSA, many internet security protocols are threatened: for example, TLS/SSL that protects websites and file transfers via FTP, the SSH protocol for remote access to a machine, and PGP which is sometimes used to encrypt emails. The threat also extends to the electronic signature of software and their automatic updates, VPNs for remote access to the networks of protected companies, the security of the emails with S/MIME, payment systems, DSA (Digital Signature Algorithm, an electronic signature protocol), and Diffie-Hellman for sending symmetric keys and elliptic curve cryptography. Finally, the electronic signature protocols of Bitcoin and many blockchains are also threatened (source: O. Ezratty).

(16) A variant of the Shor algorithm could be applied to the discrete logarithm problem (see note 10) used in many other asymmetric ciphers.

(17) In a classical computer, the basic brick of information is a bit: a unit that can take one of two possible values (states): 0 or 1. In the world of quantum computing, its equivalent is called the qubit. Concretely, it uses a physical system (atoms, ions, etc.) in a quantum state. According to the superposition principle, a qubit's state is a linear combination of states of 0 and 1; thanks to entanglement, different qubits can be linked together. In classical physics, adding an extra bit can only describe one more value; in quantum physics, adding a new qubit doubles the theoretical computing power. So, a quantum machine of 10 qubits can simultaneously process $2^{10} = 1024$ values (compared to 10 for a classical 10-bit machine).

(18) We would need a few thousand "logical", i.e. physical, qubits. In practice, however, physical qubits are imperfect, and good logical qubits are obtained by combining many physical qubits (see Briefing N° 15: "Quantum Technologies: Quantum Computers"). For Shor's algorithm, optimistic estimates require tens or hundreds of millions of physical qubits.

(19) To find an n-bit key used by a symmetric encryption algorithm with no weaknesses, a classical computer must try all possible combinations, which requires up to 2^n operations. This number is usually too great for the attack to be feasible. So, for the AES standard, the key is 128 bits long, and as $2^{128} \approx 10^{39}$, it is a 39-digit number, while the best supercomputers know how to handle only 10^{15} operations per second. Grover's algorithm, introduced in 1996, requires only $2^{n/2}$ operations to find the key. Using AES as an example, $2^{64} \approx 10^{20}$ operations would be enough, which is much closer to being realistic. To return to a suitable level of security, one possible solution would be to use a key that is twice as long. AES can actually work with keys of $2 \times 128 = 256$ bits; it was one of the arguments that led to choosing it as a standard.

(20) The QUASYModo project at INRIA is investigating this question: https://project.inria.fr/quasymodo/

(21) According to Michele Mosca, a researcher at the University of Waterloo (Canada): https://www.larecherche.fr/informatique-cryptographie/%C2%AB-la-meilleure-garantie-de-s%C3%A9curit%C3%A9-est-l%C3%A9preuve-du-temps-%C2%BB

(22) Historically, some encryption protocols have continued to be used for many years after being broken (by a typical computer) because the network infrastructure had not been changed.

(23) https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

(24) This method of scientific competition is not new and, historically, NIST is already behind the development of several cryptography standards, such as AES (Advanced Encryption Standard, 2002) and SHA-3 (2012).

(25) Most mathematical problems used by NIST submissions fall into four broad categories based on the mathematical objects they use: error-correcting codes, Euclidean networks, multivariate polynomials and elliptic curve isogenies.

For the past several decades, error-correcting codes have been used to prevent certain data from being "lost" during transmission, for example, if the communication channel introduces noise into the messages. They are also used for CDs or DVDs so that a small imperfection does not make a file unreadable. In 1978, a few months after RSA was discovered, RJ McEliece showed how to use these techniques to build an asymmetric cryptographic system. This encryption has since been improved, but its major flaw is having large public keys.

Introduced in 1996, Euclidean network cryptography is based on solving systems of linear diophantine equations (equations on whole numbers). Under certain circumstances, resolving these systems can be very difficult from a computational point of view. Thus, we can use a system of equations as a public key and a method of resolution as a private key.

A multivariate polynomial (for example, x, y and z) is an expression P involving sums and products of these variables (e.g. $P = xy + y^2 + z^3x + z$). Introduced in 1988, the idea of multivariate cryptography is to use several polynomials of this form (for example P, Q and R). If we know the values of x, y and z, it is very easy to calculate P, Q and R; on the other hand, the reverse operation is particularly difficult for computers. Therefore, it is possible to use polynomials as a public key for an encryption system and an "inversion method" as a private key. So that the opposite is not easily computable, we must use a very large number of variables, which limits the speed of the encryption.

Elliptic curves are a well-known mathematical object in cryptography behind several current encryption protocols (see below). Researchers do not use them directly for post-quantum encryption, but they are interested in certain functions called isogenies, which make it possible to go from one curve to another while preserving their structure.

(26) Only a minority of them are subject to a patent, a criterion which is also considered as a drawback in their assessment for this open call for projects. The terms are available on the NIST website: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

(27) https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals

(28) https://risq.fr/?page_id=8&lang=fr

(29) The companies finance part of the project using their own funds. The projected capital base for the RISQ initiative is approximately €8 million.

(30) https://www.pourlascience.fr/sr/article/strategies-dattaques-4764.php

(31) French National Agency for Information System Security (http://ssi.gouv.fr/).

(32) Adding an extra layer consisting of a proven classical method only adds up to a few percent of the processing power compared to using post-quantum methods alone because classical methods are very efficient after years of development. For example, here are the sizes of the messages sent for the ECDH-256 (classical) and NewHope512 (one of the most compact post-quantum candidates) mechanisms: 32 bytes for ECDH versus 1120 bytes for NewHope. Adding an ECDH layer to a NewHope exchange therefore entails an additional cost of a little less than 3% and guarantees a non-regression of security compared to current techniques.

(33) The term "post-quantum" refers to any method that is resistant to the power of a quantum computer and is understood as "post-quantum computing". Meanwhile, the term "quantum cryptography" refers to key exchange methods that rely on an infrastructure using quantum properties but that do not correspond to cryptography in the broad sense. For these two aspects, it is highly likely that the names, which are quite imprecise and confusing, will change as technology progresses in the coming years.

(34) Quantum cryptography can only be used between correspondents with a direct physical link, such as an optical fibre or an open-air link.

(35) More generally, the polarisation of a wave describes a preferred orientation in the distribution of the oscillations that compose it. Polarisation can be unidirectional (linear, vertical, or horizontal polarisation with respect to the direction of propagation). In the case of an electromagnetic wave, if the electrical and magnetic components are phase shifted by 90°, the polarisation can then be circular or elliptical.

(36) A quantum dot (of nanometric size) consists of inserting one semiconductor material into another to create a trap that is very effective for electrons. These will emit photons one by one, with characteristics (wavelength, flux) that are more or less controllable. The current challenge for R&D for communication purposes is not to generate too many pulses containing more than one photon, which, in return, reduces the photon emission rate and, therefore, the quality of the communication (https://www.photoniques.com/articles/photon/pdf/2015/04/photon201577p36.pdf). The French company Quandela specialises in this technology.

(37) In quantum physics, energy exchanges are made discontinuously in packets called "quantas". See Briefing N° 13 on "Quantum Technologies: Introduction and Challenges" from the Office. http://www2.assemblee-nationale.fr/content/download/79022/810034/version/2/file/Note_TechnologiesQuantiques_Introduction_versionFinale.pdf

(38) Nonlinear optics is concerned with the environments that modify properties of the light they receive at the output. More particularly, non-linear crystals can produce a pair of photons from a single photon by splitting its energy in two.

(39) Diamanti, Eleni, et al. "Practical challenges in quantum key distribution." npj Quantum Information 2 (2016): 16025

(40) The development of methods to produce unique photons or entangled photon pairs has been a real boost to developing these techniques.

(41) https://www.idquantique.com/

(42) https://www.ge.ch/document/etat-geneve-mise-cryptographie-quantique

(43) https://www.ge.ch/document/etat-geneve-mise-cryptographie-quantique

(44) Message from the company Quantum ID.

(45) The phenomenon of decoherence reflects a loss of quantum information to the system's environment. The system's wave function (the state) is "scattered" by the multiple external interactions and ends up losing its undulatory character and, thus, its quantum behaviour. The notion of decoherence was highlighted in 1970 by the physicist Dieter Zeh and allows us to better understand the frontier between the quantum and classical world: classical objects may just be quantum objects that have undergone decoherence through interaction with their environment.

(46) https://science.sciencemag.org/content/356/6343/1140 for the scientific article and for a good analysis of the issues: https://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance

(47) In addition, there are other projects in Asia: since 2011, the city of Tokyo has been deploying a permanent quantum communication network, and China wants to install a quantum line between Beijing and Shanghai (over a distance of about 1,000 km). Finally, the South Korean company SK Telecom has become the majority shareholder in Quantum ID to secure the next 5G networks to the ground.

(48) In terms of security, bandwidth, range, and speed.