REPLY specialises in the design and implementation of solutions based on new communication channels and digital media. Through its network of specialist companies, Reply supports some of Europe's leading industrial groups in Telco & Media, Industry & Services, Banks & Insurance, and Public Administration to define and develop business models, suited to the new paradigms of Artificial Intelligence & Machine Learning, Big Data, Cloud Computing, Digital Media and the Internet of Things. Reply services include: Consulting, System Integration and Digital Services.

Quantum computers enable the encryption of current cryptographic systems, challenging the paradigms and principles on which traditional Cybersecurity is based. To ensure data protection and enhance security mechanisms, organizations must also learn to protect themselves in a post-quantum perspective.

www.reply.com

QUANTUM COMPUTING: SPEED, SECURITY AND RELIABILITY

Cybersecurity is now an integrated part of every organization, process and activity: protecting networks, data, transactions, products and people from possible cyber attacks or unauthorized access comes first, even of the "core" business, regardless of the sector and size of a company.

Resilience to cyber threats is the resilience of an industry. In the era of Quantum Supremacy, more and more near, there will be computers able to solve problems that cannot be solved using the current mainstream technologies: the computational capacity of Quantum Computing allows to solve in a few minutes algorithms that would take the most powerful supercomputer in the world a time estimated in the age of the Earth. Among the sectors most exposed to Quantum Disruption there is that of computer security, whose reliability depends mainly on the unsolvability of the algorithms on which it is built.

Unsolvable? A thing of the past. It is the case, for example, with the factorization of the RSA cryptographic key which, although not theoretically impossible to solve but only highly improbable due to its complexity, is currently considered a 100% secure algorithm. Thanks to a 6000-qubit quantum processor, it is estimated that RSA can be factorized in as little as 2 weeks, or even 8 hours using 20 million-qubit noisy hardware. We are talking about hardware that does not exist yet, but whose realization is expected in the next years.

FACTORIZATION OF THE RSA

6000 QUBIT - 2 WEEKS

Are you quantum-safe? From cryptography to OTP authentication processes, passing through the management of banking transactions, VPN connections, e-mail exchange, gaming, online betting and democratic voting systems. The "disruptive" power of this technology will be enormous both in the security field and in the computational field, but it can be managed and enhanced by adopting post-quantum solutions or by integrating existing technological infrastructures with sufficiently robust, mature and economically competitive solutions.

In the fields of Security and Communication Encryption, great benefits can be drawn from Quantum Computing: hardware capable of hardening security networks has already been realized, exploiting, in this case, not the computational part of quantum mechanics, but photons and entanglement.

While waiting for the Quantum Revolution. Reply's goal is to make its customers ready for Quantum Supremacy. For more than two years Reply has been working with multidisciplinary teams exclusively dedicated to Quantum Computing (QC), which also work in Practice with important international players.

AFRAID OF QUANTUM SUPREMACY?

Over time, technology become better and better: the widely used RSA encryption algorithm, for example, is based on an asymmetry in the complexity of two complementary calculations.

This means that a calculation is relatively easy and therefore quick to solve in one direction, while the way back is comparatively complex.

Multiplying two (prime) numbers with each other does not cause headaches. On the other hand, decomposing a large number into factors from which it is formed is a greater achievement.

One speaks of a "non-polynomial complexity" of such an operation - that is, a calculation that is practically impossible to solve. In the case of encryption, there is a major advantage: a long, complex key (for example 2048 bits) means that encryption is only made more difficult with a polynomial effort, meaning it is practically solvable.

Unauthorized decryption, on the other hand, becomes exponentially more complicated. In the end, this means that computers may become faster, but you only have to increase the key length to remain securely encrypted.

GOOGLE AND THE PARADIGM SHIFT

In 2019 Google caused a furore with its announcement of "Quantum Supremacy". This "supremacy" means that Google's engineers had found a problem that would have taken 10,000 years to solve on a conventional computer. On Google's quantum hardware, however, it could be solved in just little over three minutes. The reason for this: the complexity of the algorithm used on the quantum computer is polynomial. This is a major advantage over the exponential complexity of the classical computer.

The problem with which Google proved the Quantum Supremacy was of little practical relevance - a "quantum nail" for which a "quantum hammer" had been designed. For encryption, however, the situation is critical. The hitherto high complexity of decryption disappears when a corresponding quantum computer is available. Because: There is an algorithm for the task of efficiently factorizing large numbers with quantum hardware. This algorithm is named after its inventor Peter Shor and makes previous encryption vulnerable to attack. The US National Institute of Standards and Technology estimates that the capacities are sufficient for an attack on RSA encryption as early as 2027.

In addition, there is another problem for encryption, which usually receives less attention: For the encryption not to be easily guessed, the numbers that make up the key must be chosen randomly from a large number of possibilities. Generating a random number is not easy - especially for a computer. In a board game, for example, the random element resides within one or two dice.

The numbers are distributed throughout the evening according to statistical rules. What we perceive here as randomness is in reality just the human inability to control all physical parameters. If you know the centre of gravity of the dice, the unevenness of the table and can precisely control the swing of your own hand, any desired result is possible.

NO CHANCE FOR A MAN-IN-THE-MIDDLE ATTACK

A physicist uses a measurement to determine whether an event has occurred. Until the time of the measurement, the physical system is miraculously not fixed and hovers in a superposition of all possible states.

This unusual feature can be used to encrypt data. A message sent in a quantum code can only be read if you "measure" the characters of which it is composed. The typical quantum superposition is lost and cannot be recovered. An unwanted eavesdropper would now have to express the message in a new quantum state. The two honest parties, the sender and the intended receiver, make an agreement on how they want to perform the measurement.

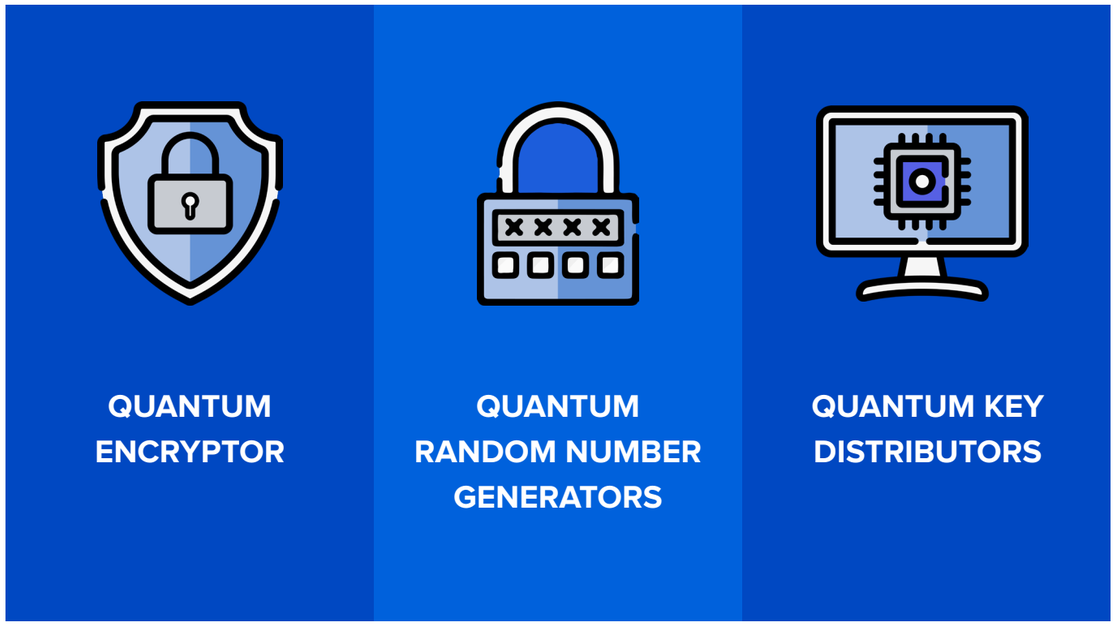
If the individual quantum bits have been created by someone other than the authorised interlocutor, this will be noticed during the measurement because more and more characters arrive incorrectly. The two communication partners notice this inconsistency. They lose their confidence in the communication channel and set up a new one. In this way, they can neutralize the eavesdropper who is carrying out a man-in-the-middle attack.

In practice, such a quantum phone is difficult to create. Quantum states are relatively fleeting. Quantum mechanics contradicts our intuition, because nothing in our familiar living environment behaves quantum mechanically. The properties are lost through external influences. This susceptibility to errors prevents us from being able to use quantum computers today and costs the developers of appropriate hardware a lot of money and effort.

RANDOMNESS AS A SERVICE TO IOT

For some time now, the company IDQuantique, a spin-off of the University of Geneva, has been developing such a system for the market and offers "Randomness-as-a-service". Fortinet, a major security software provider, recently announced a collaboration with IDQuantique and will equip the next generation of its firewall with a quantum key interface.

Some companies have already started using post-quantum technologies. Although these are very large organizations that decided to invest in QC, these solutions are very flexible and can be used in any context where key exchange and authentication mechanisms need to be strengthened.



Swiss Government

The goal was to create a new online voting platform, both to strengthen voter indication mechanisms (ensuring greater protection and confidentiality), and to prevent election fraud (countering malicious or fake votes). The solution integrates Quantum Encryptors and Quantum Key Distributor to enhance authentication mechanisms with OTP password (generated by Encryptor) and to prevent potential MITM.

Loterie Romande

Loterie Romande is the company that organizes and manages lottery games and sports bets throughout French-speaking Switzerland. Reply has integrated a quantum number generator into their systems for an overall enhancement of the security of all mechanisms related to core activity, freeing the Customer from the pseudo-randomness of number generation mechanisms using algorithms.

British Telecom

British Telecom has launched a plan to strengthen its backbones, in particular for what concerns the risk of MITM attacks, difficult to recognize because of the great amount of information that on average passes inside a backbone. The proposed solution was the integration of Gemalto solutions with Quantum Encryptor technologies. The result is the creation of new 100 gig backbones that operate with quantum key exchange mechanisms and have the advantage of being able to immediately detect potential MITM within the communication, in order to block the attempt of information theft (sniffing). Currently there are two active backbones and they are still in an experimental phase.

The European Central Bank

As part of the activities connected with the issue of CBDC - Central Bank Digital Currency (the ECB's digital currency), had to create a platform that would allow users/investors to manage this new currency securely, starting with payments. The implemented solution has led to the creation of a new authentication mechanism based on Gemalto technology (leading company in the Digital Security sector) with token generation for OTP communication carried out in a quantum way (integration with Quantum Encryptor), concretely demonstrating how this type of technology is flexible and integrable to solutions already present on the market.

NS&I - National Savings and Investments

A British savings and bond bank, has adopted Encryptors to enhance the bond generation mechanisms on its online platform. The integration of quantum random number generators implemented by Reply makes it more difficult for an attacker to trace the keys used to generate applications within NS&I systems.

South Korea Telecom

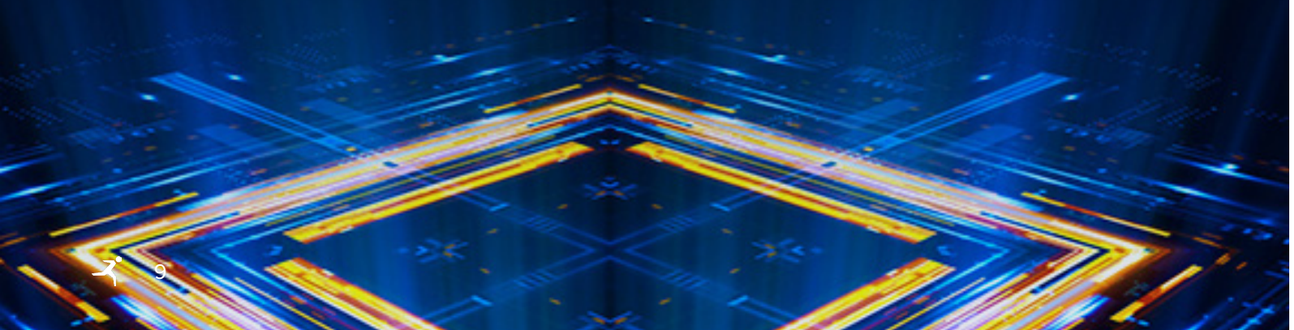
South Korea Telecom has launched a project to strengthen the authentication principles (those based on key generation) of mobile and IoT devices on 5G technology. Quantum Encryptors have been integrated within their Data Centers to provide a more secure connection.

QUANTUM COMPUTING IS NOT SCI-FI

Quantum Cybersecurity is definitely an emerging market in which specialized technological players, able to perform data integration in quantum-resilient logic, are still a few.

The advent of quantum computers allows to encrypt the current encryption systems, thus inexorably challenging the paradigms and principles on which traditional Cybersecurity is based. To ensure data protection and enhance security mechanisms, organizations must learn how to protect themselves, in time, even in a post-quantum logic.

Long-term solutions such as quantum key distributors, which require replacing the technology infrastructure with a larger upfront investment, and intermediate solutions such as quantum encryptors or quantum random number generators are not much different in cost than pre-quantum solutions.



REPLY: DOING BUSINESS IN THE QUANTUM ERA

As a thought leader and advisor to its customers, Reply is constantly committed to identifying and managing emerging opportunities and use cases enabled by Quantum Computing.

Quantum Computing is a new technology that offers many opportunities in a wide range of industries. It represents the basis for advanced applications in the fields of Artificial Intelligence, Quantum Machine Learning, Cybersecurity, Finance, Logistics and Transportation, Telco, Medical and many more.

Reply is committed to developing proof-of-concepts and projects that apply quantum algorithms to real use cases in many business areas and offers concrete and effective answers to its customers' challenges. The 2020 Springer Journal Quantum Machine Intelligence published a study conducted by Reply on how a Quantum Annealer can be used to solve complex optimization problems.

In 2018, as part of the Quantum Artificial Intelligence Research Program in which NASA and Google also participated, Reply was awarded a research grant to use the D-Wave Quantum Annealer from the Universities Space Research Association.