INSIGHTS

QUANTUM COMMUNICATIONS
SECURING THE INTERNET

Quantonation is an Early Stage Venture Fund dedicated to Deep Physics start-ups with a focus on the emerging and disruptive fields of Quantum Sensing, Communications and Computing as well as other new computing paradigms. Quantonation invests worldwide out of Paris and works closely with the start-ups it invests in, leveraging its partners expertise and network to their benefit.

"INSIGHTS" are short research reports by the team at Quantonation adressing challenges and opportunities in the fields of interest.

QUANTONATION

With the development of digital computers and the emergence of a society based on information exchanges through interconnected networks, the importance of communication security through cryptography reached many essential aspects of our everyday life: file storage, access rights management (TV, GSM mobile phone, etc.), secure web browsing and banking (cash withdrawal, online payments).

Data protection is also becoming crucial with the recent increase of malicious attacks targeting sensitive data in companies, governments and critical infrastructures such as healthcare. A market analysis issued in March 2018 by TechSci Research forecast the global quantum cryptography market, which was valued at $328 millions in 2017, to grow at a CAGR of 25% during the period 2019-2023 to surpass $1.2 billion by 2023.

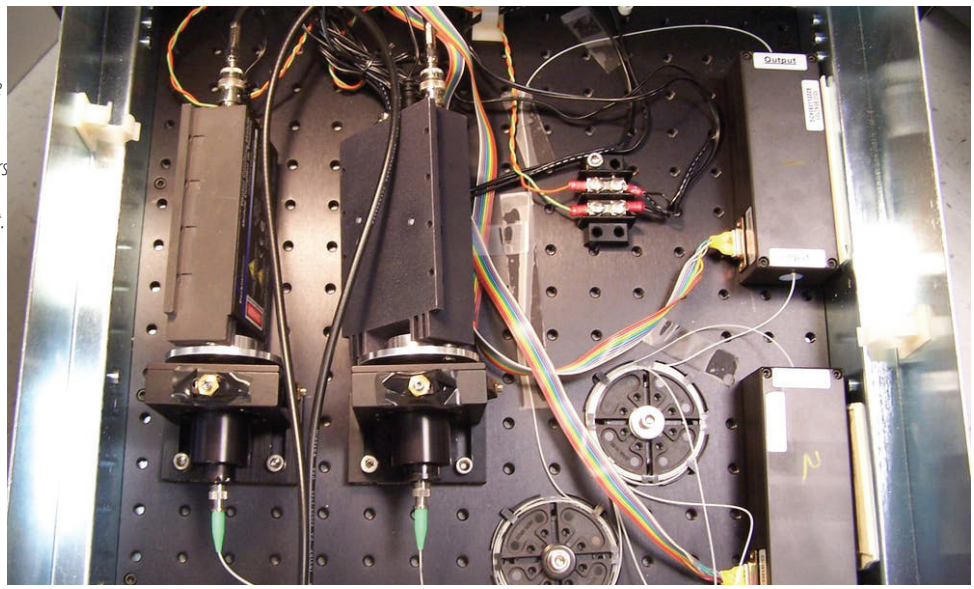
The present report aims to give some insights on the current context of data protection by addressing a major user case for quantum computers: the endangering of today's communication systems and cryptocurrencies. We first explain the role of cryptography within communication security and how a powerful quantum computer would make some crucial security protocols obsolete. After introducing the problem, quantum-safe classical solutions are presented and analyzed.

A focus is made on a completely different kind of solution whose security is ensured by laws of Quantum Physics: Quantum Key Distribution.

DR. CHRISTOPHE JURCZAK
Managing Partner

Figure 1

NIST prototype quantum key distribution (QKD) system: incoming photons already have been sorted into one of two quantum states. Photons are "up-converted" from 1310 to 710 nm by one of the two NIST-designed converters at right, then sent to one of two commercial silicon avalanche photo diode units to the left.



PART I
THREATS AGAINST CLASSICAL CRYPTOGRAPHY

An encryption key is used alongside a chosen encryption protocol to alter data and make them unintelligible for anyone who cannot reverse this process with the corresponding decryption key. Prior to encryption, careful key management is needed to securely produce and distribute the necessary key material between rightful users.

In symmetric cryptography, a pre-shared secret key is used for both encryption and decryption of the data. Asymmetric cryptography avoids the complicated requirement of pre-sharing keys: anyone can encrypt a message with its interlocutor's public key – which can be as simple as a name or email address - whereas only the recipient will be able to decrypt it with the matching secret key. But the slow execution of these protocols and their large parameters that require huge storage capabilities make them inefficient for encryption and when used in embedded systems.

Symmetric cryptography can handle large amount of data faster and with reduced parameters for a same security level than asymmetric cryptography, making them more suitable for real-time encryption and lightweight cryptography. The symmetric algorithm Advanced Encryption Standard (AES) is used in most messaging applications providing end-to-end encryption (Messenger, Telegram, Whatsapp, etc.), file transfer protocols (HTTPS, FTPS, etc) and file encryption systems (NTFS, APFS, etc). To avoid key management difficulties, asymmetric algorithms such as Rivest-Shamir-Adleman (RSA) or Diffie-Hellman (DH) are used to exchange secret key material prior symmetric encryption. Another widely used cryptographic primitive, the hash function, maps an input value of arbitrary size to a finite-size output called the hash value. Computing the hash value given the input is very easy but the reverse operation is extremely difficult to perform.

A simple user case consists in storing a password on a computer. Upon choosing a new password, only the corresponding hash value is stored in the computer's memory for security reasons. Upon re-entering the password again, the computer compares the generated hash value with the stored one and grants access if they match. Hash functions are fundamental in blockchain technologies where each block contains the hash value of the previous block plus other hash values for each new transaction. The most frequently used hashed function, called SHA-2 and Keccak/SHA-3, are respectively employed in Bitcoin and Ethereum with 256 bits hash lengths.

The security of asymmetric cryptographic protocols depends on the impossibility for a classical computer to solve quickly - e.g.

in polynomial time – two mathematical problems that are then called “hard”: the integer factorization problem and the discrete logarithm problem. Best classical algorithms are only able to solve these problems in exponential time or sub-exponential time for some very specific cases.

For an attacker with given computational and algorithmic capabilities, any attack against a cryptographic protocol would necessitate 2b operations to recover key sizes corresponding to a b-bit security, a 128-bit AES key being equivalent in security to a 3071-bits RSA key. As this number quickly increases with large values of b, it provides an accurate estimation on how “safe” is the key.

Because it only holds for the precise depiction of a given attack, this security is not meant to last forever. A significant increase of computational power, an improvement in the efficiency of a known attack or the design of a new attack may result in a reassessment of this security. For example, the first RSA key broken during the RSA factoring challenge in 1991 was 330-bits long whereas the highest factoring record from 2009 allowed to recover a 768-bits long RSA key. As computers were becoming more powerful and our knowledge in new attacks increased, extending the size of the key have historically been the easiest way to deal with potential security breaches. In the event of a new attack targeting structural flaws or providing a considerable speed-up over previous attacks, an algorithm can become obsolete. The only solution left is to replace it by another algorithm offering better resistance.

In the last category, the quantum Shor’s algorithm (Peter Shor, 1994) solves the integer factorization and discrete logarithm problems in polynomial time when running on a large quantum computer (c.f Insert 1), leading to the compromising of all related protocols. In regard of these perspectives, several publicly renowned agencies have already expressed their concerns over the urge of replacing asymmetric protocols by quantum-resistant ones.

Symmetric protocols and hash functions are not based on such problems but they are still threatened by another quantum algorithm. Grover’s algorithm (Lov Grover, 1996) for searches in unstructured databases provides a speed up in respect to best classical attacks, but it’s only quadratic vs exponential for Shor’s. Therefore, doubling the key size and triple the hash output act as sufficient countermeasures to keep the same level of security.

Grover’s algorithm has been proven asymptotically optimal in respect to any other quantum solution [Bennett], which means that no other quantum algorithm will ever be able to significantly outperform it. In consequence, symmetric protocols and hash functions whose parameters are large enough to resist Grover’s algorithm can be considered quantum-secure.

In practice, symmetric protocols are used following a mode of operation that describes how to apply several internal procedures. Even if the algorithm is theoretically secure, tampering with this mode of operation can result in the complete

TWO KEY QUANTUM ALGORITHMS

Grover’s algorithm — a variant for hash functions.
Let us consider a hash function f, a target hash y and a suitable preimage x amongst n possible inputs.
Grover’s algorithm finds with high probability the value x such that f(x) = y in O(√n) evaluations of f where a classical computer would necessitate O(n) evaluations instead.
For a hash of length k bits, Grover’s algorithm would provide a speed-up of factor 2k/2.

Shor’s algorithm for integer factorization.
Given an integer N = p.q, the algorithm finds its prime factors p and q in polynomial time.
Solving the discrete logarithm problem with this algorithm roughly consists in a variant of solving the integer factorization where we look at pairs of integers instead of a single one.

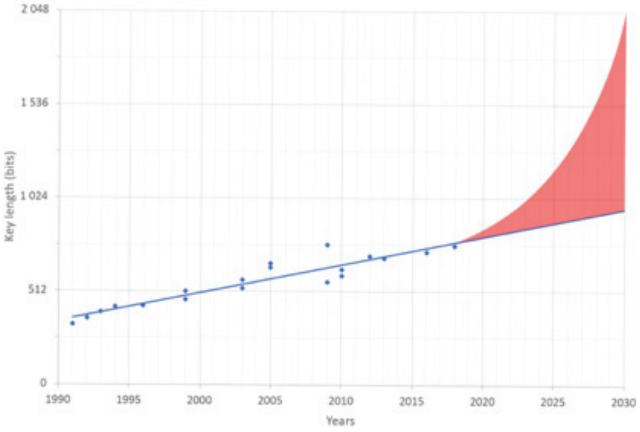


Figure 2

Breaks of public keys used by the RSA protocol in recent years with classical computation resources (in blue) and possible endangering by quantum computation resources (in red). Source: ETSI Whitepaper n°8 “Quantum Safe Cryptography and Security” (2015), updated by Quantonation (2019).

recovery of the key. In *Breaking Symmetric Cryptosystems Using Quantum Period Finding* (CRYPTO'16), Dr. Kaplan and co-authors presented a quantum attack involving Simon's algorithm that led to the compromising of several modes of operations widely used with AES. A suitable modification countering the attack was quickly suggested but other security faults could still be discovered. No implemented encryption algorithm, even quantum-resistant in term of parameters, should be considered absolutely safe.

Current cryptographic standards	Type	Purpose	Impact from large scale quantum computer
AES	Symmetric	Encryption	Larger key sizes needed (128 → 256 bits)
SHA-3	Hash function	Hashing	Larger output needed (128 → 384 bits)
RSA	Asymmetric	Signatures, key exchanges	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Asymmetric	Signatures, key exchanges	No longer secure
DSA (Finite Field Cryptography)	Asymmetric	Signatures, key exchanges	No longer secure

Figure 3
Impact of Quantum Computing on Common Cryptographic Algorithms. Source: US Department of Commerce / NIST (2015).

As alarming as they may sound, these quantum attacks still require a sufficiently large quantum computer to be performed. The following paragraph explain how quantum computing capabilities are strongly dependent of error correction strategies and gives some insight on how large a quantum computer should be to endanger the security of cryptographic protocols.

A quantum state describes the state of a delimited system (e.g. single photon) who behaves accordingly to the laws of Quantum Physics, in opposition to the environment that refers to everything outside this system. When interacting with the environment, quantum states are subject to decoherence and loses information until their behavior becomes classical.

One state corresponds to one system, but what happen when we consider two systems or even more ? A superposed state is the addition of all these individual states and corresponds to a larger quantum system that contains many sub-systems. But another possibility arises when the larger system doesn't correspond to

Physical qubits, logical qubits and error correction.

In classical computing, all the processed data is translated into a sequence of bits – either the value 0 or the value 1 – that is understandable by a digital computer. The language of a quantum computer is made of qubits representing superpositions of the values 0 and 1.

Similarly to a classical algorithm, a quantum algorithm is run by applying elementary operations called quantum gates that will modify the initial quantum state, leading to a final state that can be measured to retrieve the desired result. Each of these operations introduces a small amount of errors in the state and the overall error rate after applying all the gates must be limited and controlled. The number of qubits required to execute a quantum algorithm is usually quantified in term of errorless logical qubits, as opposed to the faulty physical qubits that are implemented in practice.

Classical error correction techniques consist of adding extra information – called redundancy - to the signal sent through the communication channel, allowing to recover the correct information in the event of errors occurring during the transmission. In Quantum Error Correction (QEC), several entangled physical qubits simultaneously hold the information about the logical qubit in a similar way to classical redundancy, allowing to reconstitute the information despite errors in the channel.

The Physical-to-Logical ratio describes how many physical qubits are required to obtain one logical qubit and can greatly vary depending on the implementation and the QEC algorithm used. We estimate this ratio currently varying between 100:1 and 100,000:1 but there's still room for a lot of progress and the overhead could decrease by orders of magnitude. It is expected that startups will be active in this space.

the gathering of individual sub-systems. In this case the sub-systems must be considered collectively and their common quantum state is said to be entangled. Acting on any of these entangled sub-systems will have repercussions over all the other systems.

Approximately 3000 logical qubits (from 300,000 to 300M physical qubits) would be necessary to recover a 128-bit AES key with Grover's algorithm. When considering Shor's algorithm, 6100 logical qubits (from 610000 to 610M physical qubits) are required to recover a 3072 bits RSA key and 2300 logical qubits (from 230,000 to 230M physical qubits) are required for a 256 bits ECC key, both key sizes being equivalent to a 128-bit AES security. These estimations only hold in the context of our current technological capabilities and will decrease accordingly to future progress in quantum hardware and algorithms design, e.g. better gate fidelities and more efficient Quantum Error Correction codes.

The threshold theorem described by M. Ben-Or and D. Aharonov in *Fault Tolerant Quantum Computation with Constant Error Rate* (SIAM Journal on Computing 38, 2008) indeed asserts that these codes can be used to correct as many errors as we need provided the qubit fidelity – the error rate of individual quantum gates – is below a certain threshold. If not, applying error correction will only introduce more errors than what is corrected. This threshold depends on the code and type of errors considered: a quantum surface code that treats all errors identically can attain a threshold as high as 1-3% where thresholds for other codes vary between 0.1-1%. In classical communications, error correcting codes are dependent to a noise threshold – the classical equivalent of the fidelity threshold – that is generally higher than for quantum error correction.

The fidelity threshold strongly determines the Physical-to-Logical ratio. Error rates substantially below the threshold will allow to implement logical qubits with significantly fewer physical qubits. Although the quantum threat is still far away from now, the successful implementation of a Quantum Computer with 100,000 qubits and gate fidelities below 1% will be a strong signal of danger for classical communications.

Quantum Computing in the context of Bitcoin mining.

Some blockchains, notably Bitcoin, are based on a system called hashcash Proof-of-Work which relies on a chosen hash function, e.g. SHA-2-256 for Bitcoin. Users called miners verify the credibility of a new block of data by competing in solving a problem: find a hash value covering all the data in the block and that is inferior to a target value. This competition requires a lot of computational power, hence a high cost in processors and a huge electrical consumption, but the first miner to solve this problem is rewarded in Bitcoins. Because such problem is difficult to solve but easy to check, once an adequate hash value has been broadcasted, each user can verify the validity of the solution. If they agree on accepting the solution – reaching a consensus - the new block is validated and added to the blockchain.

The difficulty of the chosen challenge depends on how fast one can find a valid solution by trying many possible hashes. The target value is adjusted so that only one block can be validated every 10 minutes. As the security of this system is based on a consensus, a single miner concentrating 51% or more of the total computing power would be able to perform many falsifications: reverse transactions, spend the same Bitcoin multiple times, modify the order of transactions, etc.

A quantum computer running Grover's algorithm, by providing a quadratic speed in computing many possible hashes, would provide a considerable advantage over classical computers in both time and energy consumption but could also open the way for a 51% attack.

PART II
DATA PROTECTION WITH CLASSICAL CRYPTOGRAPHY

As the cryptographic world is preparing for the fall of asymmetric cryptography – either led by the increase of computing capabilities or by the discovery of more classical efficient attacks – we must envision completely new and secure cryptographic protocols to replace it. This section describes which classical solutions are considered for the future of quantum-safe cryptography.

The family of quantum-safe algorithms refers to algorithms whose secret parameters – keys, input of a hash function, etc. – cannot be recovered by any attacker having access to both classical and quantum computational power. A distinction is made between Quantum Cryptography, algorithms using quantum systems and whose security is ensured by the universal laws of Quantum Physics, and Post-Quantum cryptography, classical algorithms whose security relies on proven quantum-safe problems. Most Post-Quantum algorithms can be regrouped in six classes based on their underlying mathematical problems: lattice-based, multivariate, hash-based, code-based, supersingular elliptic curve isogeny and symmetric cryptography.

The National Institute of Standards and Technologies (NIST) belonging to the agency of the U.S. Department of Commerce provide internationally followed industrial, academical and governmental standards in Information Technology, including cryptography. In June 2015, the U.S. National Security Agency (NSA) issued a statement which recommend avoiding a migration toward Elliptic Curve Cryptography and prepare for a migration toward quantum-safe cryptography instead. In late 2017, the NIST opened an official procedure for Post-Quantum algorithm standardization with a first draft release planned for 2022-2024 [NIST CAL]. The first round of submissions ended in November 2017 and gathered 82 propositions from all around the world. Some of them were merged or withdrawn in the following months, leaving with 72 propositions. By the end of August 2018, six of them were also withdrawn because of unavoidable security flaws. Amongst them, only 26 candidates were accepted for the second round that began Januar 31, 2019.

Developing and deploying cryptographic standards has historically been a long and complicated task, especially concerning industrial transition from old to new standards. Five years (2007-2012) of NIST competition were necessary to choose the latest standard for hash functions SHA-3. In parallel, despite concerns about SHA-1 security and the standardization of a backup solution SHA-2 in 2001, it took sixteen years and the common action of major industrial actors to force a customer transition toward the insecure SHA-1 to SHA-2. Even if Post-Quantum standards are issued in less than eight years, we should not realistically expect to see their full deployment in the industry before 2035 where the event of a large-scale quantum computer capable of factoring RSA-2048 with Shor's algorithm is considered realistic.

Not only we may be may already be short on time for this transition toward quantum-resilient cryptography, but we also need to achieve it as soon as possible considering that all sensitive data currently exchanged can be recorded for future decryption with a quantum computer. The urgency of preparing our most critical industries for a quantum-safe transition is real and must be taken very seriously.

The Post-Quantum standardization task that we are facing is even more challenging than the SHA-3 standardization contest for several reasons. The current NIST effort aims to select a new cryptographic suite that will enable a Post-Quantum transition of U.S. infrastructures at best for 2023. Not only this effort will have to comply to such restricted deadline, but its scope is also broader than for usual standardization processes. Usually, such competition is limited to one category of cryptographic algorithm (e.g. key establishment) and results in the selection of a unique algorithm. In this case, new signature, encryption and key establishment schemes are all required to allow for the transition to a quantum-safe era. Unlike previous calls for proposals that were considered as competitions aiming to select one winner, several algorithms are expected to be chosen for each role.

The security of Post-Quantum algorithms may also constitute an important challenge as their resistance against both classical and quantum attacks is still not well known. Although the factoring and discrete logarithm problems have been extensively studied during decades, the global effort to assess the security of quantum-resistant mathematical problems is very recent.

The security of Post-Quantum schemes relies on underlying mathematical problems that are known to be computationally difficult in both classical and quantum setups, resulting in no advantage provided by the use of a quantum computer. However, not every Post-Quantum schemes have been proven directly related to such problem. In particular, algorithms whose security is best understood suffer from huge parameter requirements. Considering that 2048 bits RSA public keys are already considered too large for many applications, the 1Mbit public keys used in code-based algorithms such as McEliece are way beyond realistic requirements.

Another aspect of Post-Quantum algorithms that is still widely under debate is its security against side-channels attacks targeting hardware implementations. Several algorithms were shown insecure against fault injection attacks, an attack consisting in voluntarily introducing faults during the execution of the protocol to observe their propagation and consequences. The website called *Post-Quantum Cryptography Lounge* provides a comprehensive searchable list of NIST submissions, including their current security status.

A short-term hybrid approach is currently under consideration to allow for the early deployment of Post-Quantum algorithms until their security have been fully studied. It consists in using asymmetric and post-quantum algorithms together to enhance the security of the overall system. Considering that this method partly relies on algorithms that are already known to be insecure against a quantum computer, it cannot prevent an adversary from storing encrypted data to decrypt them decades later. Critical infrastructures requiring long-term security – for example in 30 years from now – should not use this solution.

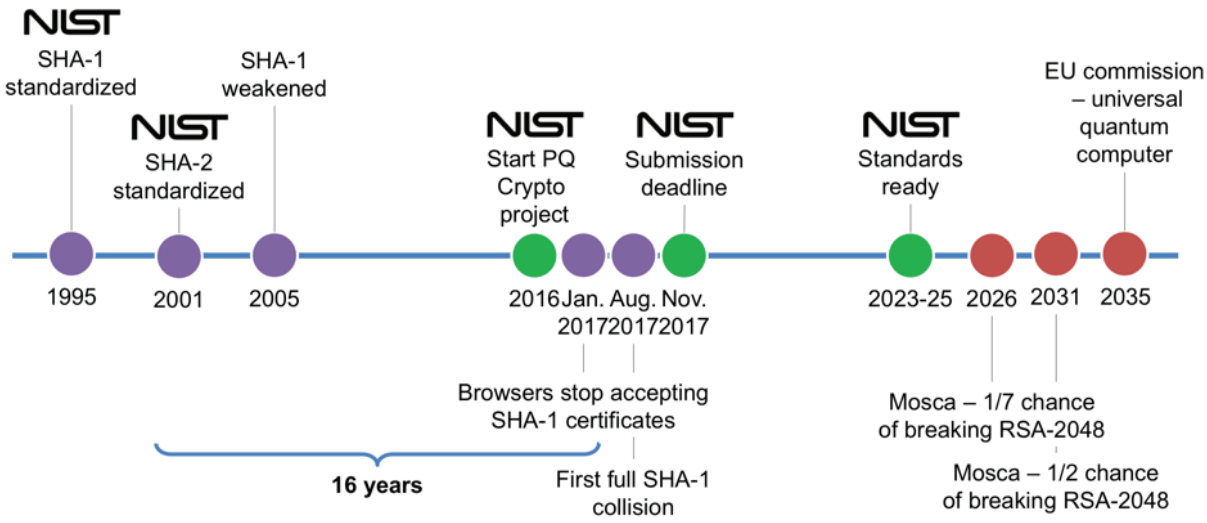


Figure 4

Timeline - SHA-1 to SHA-2 transition and Post-Quantum transition (source : Introduction to post-quantum cryptography and learning with errors, Douglas Stebila, June 2018).

PART III
DATA PROTECTION WITH QUANTUM MECHANISMS

Post-quantum algorithms could provide an interesting replacement for asymmetric algorithms and are currently being extensively studied and standardized. But they still lack of convincing security proofs against both classical and quantum attacks, in addition to unrealistically large parameters, which is why they are competing with another promising candidate, Quantum Key Distribution, in the crucial task of key establishment.

The security of Quantum Key Distribution does not rely on supposedly hard mathematical problems but on several properties of Quantum Physics that have been shown advantageous for cryptographic purposes. From the postulates of Quantum Mechanisms, it is impossible to recover a result from a quantum state without disturbing it – the measurement postulate. Given an arbitrary unknown quantum state, it is also impossible to build a device copying this state with perfect accuracy - the no-cloning theorem. This theorem do not forbid to manufacture many qubits in a chosen state as long as this state is known, but it prevents an eavesdropper to copy a state that is exchanged during a cryptographic protocol.

Post-Quantum algorithms can be directly run on conventional computers provided that their software implementation is optimized enough for realistic uses. Quantum Key Distribution protocols rely on a whole range of optical components that are necessary to exploit the capabilities of a quantum communication channel. Some of these components are already manufactured and used in telecommunications, but others need to be specifically engineered for quantum purposes.

In optical communications, classical information is carried by modulated light waves either in free-space or through a fiber network. Amongst the several characteristics of light that can be used to encode information, modulated frequency and amplitude are the most frequent. Fundamental quantum phenomena such as superposition and entanglement naturally arise in light but they are still being harnessed to be used by our current telecommunication networks.

A quantum communication channel exploits the full capabilities of these quantum phenomena by transmitting qubits via the states of travelling quantum systems. The most frequent information carriers in quantum communications are single photons containing information encoded along the direction of the polarization of light, but many other encoding methods and elementary particles can be used.

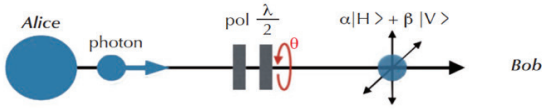


Figure 4 - Preparation stages of a photonic qubit.
An input light with wavelenght λ is sent by Alice. Each photon is polarized in the horizontal (H) direction by going through a polarizer. As the photon crosses a half-wave plate (of refractive indice 2) rotated along an angle Φ, its polarization becomes a superposition of the horizontal (H) and vertical (V) directions. When received by Bob, it is in a superposed quantum state with parameters α = sin(Φ) and β = cos(Φ). By assigning the bit value 0 to H and 1 to V, we obtain a qubit that, upon measurement, will outcome either the value 0 with probability $|\alpha|^2$ or 1 with probability $|\beta|^2$.

Because quantum states are subject to many perturbations when interacting with their environment, sustaining and controlling these quantum phenomena is still a tremendous technological challenge. It requires the development of new dedicated technologies such as single-photon sources and detectors, but also their integration within existing optical infrastructures for simplicity and cost reduction. Years of academical studies and R&D have paved the way toward harnessing and exploiting these quantum properties, leading to the current revolution in Quantum Technologies.

Quantum communication protocols can be classified into several families depending on their information encoding strategies and how they are implemented.

In Discrete Variable (DV) coding, information is encoded by modifying physical properties of single photons such as their polarization direction which can be in the superposition or the vertical or horizontal directions. In consequence, the measurement of the resulting quantum system will return a finite number of results. These single-photons can either be produced by attenuating a coherent laser or by using True Single-Photon

Sources (TSPS) that, despite being costly and difficult to engineer, stay the best solution to produce on-demand indistinguishable single photons for quantum communications, without emitting empty pulses or pulses containing more than one photon at a time. Apart from the performances of the photon source, bit rates achieved with DV coding are strongly dependent of the efficiency of single-photon detectors - the probability of registering a count when a photon arrives. Today's best efficiencies attain 93% at telecom wavelength in laboratories and exceed 85% for commercial devices.

Continuous Variable (CV) coding takes advantage of homodyne and heterodyne detectors to measure amplitude and phase quadratures of the electromagnetic field that are shaped by a weakly modulated coherent laser. These detection techniques are already widely used in classical optical communications and, unlike single-photon detectors, do not require cooling at low temperatures, which makes CV coding most suitable for easy interoperability with existing telecom infrastructures and more advantageous for small form factors and for a low-cost production thanks to their off-the-shelf components. But detectors with low shot noise and electronic noise are necessary to attain high detection efficiencies and these high raw performances are mitigated by the need to discretize the continuous results obtained after measurement into binary results. This necessary discretization makes efficient post-processing a crucial performance factor in CV protocols. In addition, these CV protocols are quite recent in comparison to DV protocols and their security proofs have been less extensively studied, especially when dealing with finite-size effects.
In the following we will describe the main industrial application of Quantum Communications : the establishment of secret keys

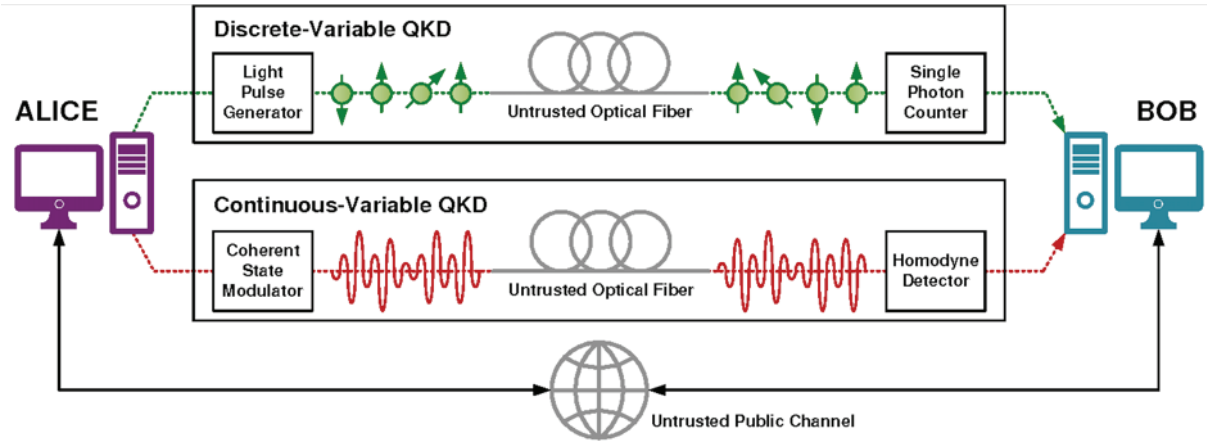


Figure 5

Discrete Variable and Continuous Variable codings and the role of a QKD protocol in communication security.

between users thanks to Quantum Key Distribution.
QKD protocols use measurements of quantum states to produce and share secret key material for symmetric encryption. The sensitive information itself travels via classical communications and is protected through encryption protocols such as AES, but the classical key material required for a secure encryption will be shared via a quantum communication channel.
Most QKD protocols fall into one of these two families: prepare-and-measure protocols and entangled protocols. They differ by the nature of the transmitted quantum states, entangled or not, leading to different state preparation steps and specific security checks.

The most famous example of prepare-and-measure protocol is the BB84 protocol invented by Charles Bennet and Gilles Brassard in 1984, which is also the first historical QKD protocol. In this protocol, a sender – traditionally called Alice - prepare and relay over an authenticated quantum channel a sequence of indistinguishable quantum states that are randomly chosen amongst four possibilities. A receiver called Bob randomly choose amongst four measurements and recovers a binary result for each state. Quantum Mechanisms will ensure that, when Alice's state and Bob's measurement match, they obtain the same result. By publicly discussing, they will be able to identify which results they have in common without disclosing them. A small part of these results will still be revealed later to evaluate how many errors – divergent results that should have matched – occurred during the protocol. An adversary trying to steal the secret by interacting with the travelling quantum states will always introduce a minimal amount of errors that will be noticed.

The first historical entangled protocol is the E91 protocol invented by Artur Ekert in 1991. In this protocol, a source produces pairs of quantum systems in one entangled quantum state and shares them between two participants. Upon randomly measuring their systems, the participants obtain perfectly correlated results every time they select the same measurement – which they can check by publicly disclosing their sequences of measurements.

The matching results can be used to create a shared secret key. Intrusion is detected by checking the violation of a mathematical object called “Bell inequality” which turns out to be verified by classical results but not by results obtained upon measuring entangled quantum states. This inequality efficiently acts as a “fire detector” that only activates in presence of entangled quantum states. An adversary tampering with the quantum states will introduce enough errors to decrease the amount of entanglement below what is required to violate the inequality, revealing its presence.

Commercial end-to-end QKD protocols are already able to attain 100 kbit/s key rate over small distances (<50 km), which is sufficient for a realistic use of 256-bit key encryption with the AES algorithm. Multiple QKD-secured networks based on trusted nodes have also been successfully deployed in several countries all over the world – United States, Switzerland, China, Japan, etc. - in order to test the efficiency of numerous QKD protocols. These efficiencies strongly vary depending on the encoding method, the protocol, the hardware implementation, the transmission mode – fiber or free-space - and the distance considered. The currently largest quantum networks are located in China, with the Hefei and Jinan star-shaped networks – respectively 46 and 56 nodes - and the huge 32-nodes 2000-km-long quantum link connecting Beijing and Shanghai.

Environmental perturbations such as depolarization of photons increase with the communication distance and introduce errors in the quantum channel. When exceeding the maximal distance tolerated by the protocol, these perturbations result in the erasing of the quantum properties of the travelling states – decoherence - and the key rate quickly decreases to zero. Environments that

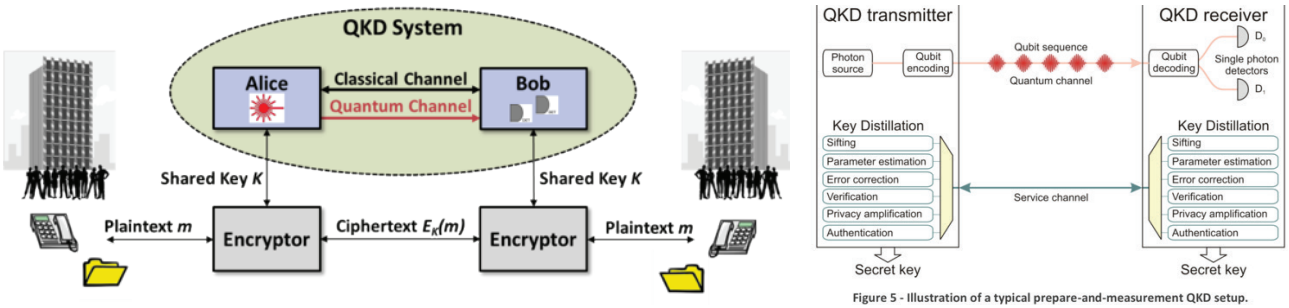


Figure 5 - Illustration of a typical prepare-and-measurement QKD setup.

Figure 6

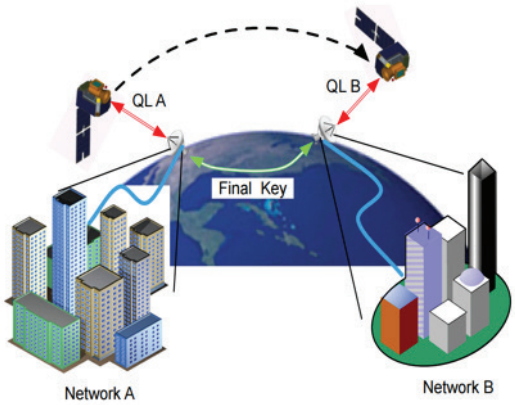
Left : integration of QKD in the cryptographic process. Right : prepare-and-measure QKD protocol. Preparation, transmission and measurement of quantum states with single-photon devices and classical post-processing for key derivation, error correction and security checks.

introduce a minimal amount of errors such as low-loss optical fiber or space are the most suitable to achieve long distances.

Quantum repeaters or trusted nodes are necessary to increase this maximal distance, which range between 100-400 kilometers depending on the protocol and quantum states employed. In particular, QKD-secured networks using satellites as trusted nodes have attracted a lot of attention with the launch of the first satellite with a specific quantum payload Mozi (also called Micius) in August 2016. As most of the errors are caused by atmosphere-induced perturbations, space-based networks using satellites as trusted relays are a promising platform to extend communication distances by limiting these perturbations to the entrance and exit in the atmosphere. A worldwide QKD-secured communication network can be envisioned by using large space-based networks to link smaller distant terrestrial networks.

As we have seen before, laws of Quantum Physics ensure the detection of eavesdropping during the execution of the QKD protocol. A malicious user trying to illegally recover the secret key, either by measuring or cloning the travelling quantum states, will introduce errors that will be quantified during the security check. Although the participants cannot discriminate the cause of these errors between environmental noise and malicious attempt, the key will be considered compromised. This unique characteristic without any classical counterpart ensures that no attack against the quantum algorithm will go unnoticed. When used alongside a classical encryption algorithm, QKD has the ability to provide an excellent long-term security solution for key establishment.

One of the most promising features of Quantum Key Distribution lies in the possibility of achieving information-theoretic (IT) security. This strong security notion developed in 1949 by the mathematician Claude Shannon ensures that a cryptographic algorithm cannot be broken even by an adversary with unlimited computational power, including a quantum computer. Although it provides IT-security, the One-Time Pad (OTP) encryption scheme is not used in practice because no key establishment



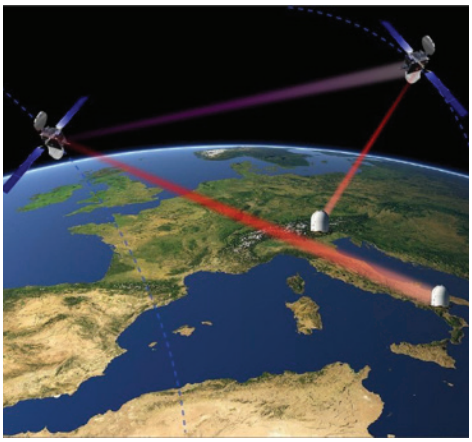


Figure 7

Left : satellite acting as a trusted relay to establish a common secret key between two ground-based networks via QKD. Right : two satellites form a QKD space-based network linking several ground-based locations on Earth.

scheme can match its unrealistic requirements: the secure pre-sharing of one-use random keys as long as the message for each communication. However, a high-rate QKD protocol attaining at least 10Gbit/s would provide enough truly random key material to ensure a realistic use of OTP, enabling IT-secure communications.

In the light of this "perfect" security promise, it is important to recall that strong security proofs against algorithmic attacks and theoretical IT-security are not sufficient to claim that a cryptographic protocol, even a quantum one, is completely immune to threats. Side-channels attacks targeting the implementation rather than the protocol itself can not only be performed against both quantum and classical cryptographic algorithms, but they have also been proven devastatingly efficient in comparison to algorithmic attacks and must not be taken lightly. Thankfully, Quantum Mechanisms provide a way to prevent such attacks with a specific security model called Device-Independence.

Quantum attacks targeting imperfections in the implemented devices are called Quantum Hacking. A famous example is the Photon Number Splitting (PNS) attack. It targets multi-photon states generated by imperfect single-photon sources and uses the extra photons to recover information about the secret key. Several countermeasures include the use of decoy states - additional quantum states that cannot be distinguished from the genuine quantum signal and that act as baits - or well-designed QKD protocols. In 2010, a phase-remapping attack successfully recovered the secret key generated by a commercial ID-500 QKD device – from 2004 - designed by the company ID Quantique.

More generally, attacks targeting the implementation can be dealt with by applying adequate countermeasures or by the use of a specific security model called Device-Independence. In this model, one do not need to assume that the implementation is truthful. The users can check if the measurement data provided by their devices behave as expected, meaning if they comply to well-defined statistical tests. In classical cryptography, similar security attempts are made with proposals of formal proofs to ensure that a target hardware satisfies predefined properties, such as described by E. Love and co-authors in *Enhancing Security via Provably Trustworthy Hardware Intellectual Property* (IEEE Symposium on Hardware-Oriented Security and Threats, 2011).

The security and liability of a lot of applications, including cryptography and lottery games, are based on the necessity of generating sequences of random numbers that cannot be predicted in advance. QKD is no exception as the measurements performed over the quantum states during the execution of the protocol must be chosen at random.

Pseudo Random Number Generators (PRNGs) use algorithms to produce sequences of "almost random" bits which are as indistinguishable as possible from true random numbers. The generated sequences are completely determined by an initial seed value, random or not. Because this process is deterministic and consequently predictable, PRNGs are progressively being dismissed in favor of more secure solution.

Hardware Random Number Generators (HRNGs) produce randomness through physical properties - electrical noise, decay of radioactive material - that are very difficult to predict, ensuring that the sequences generated are closer to true randomness than those obtained with PRNGs. As the outcome of a quantum measurement is ensured to be random by the laws of Quantum Physics, Quantum Random Number Generators (QRNGs) are natural sources of true randomness. With a Bell inequality check, it is possible to verify if the randomness generated from a QRNG arises from a quantum process and even to certify its quality. Such test allows the user to ensure that the quantum behavior in

the device has not been replaced by a deterministic process, even by a malicious QRNG manufacturer.

Commercial QRNGs with random bit rates ranging from a few Mbit/s up to more than 1Gbit/s and whose randomness has been certified following the recommendations of internationally renowned organisms – e.g. the NIST SP800-22, Diehard and ENT statistical test suites - are already available for prices below 5000$. A wide range of possible implementations is investigated by both researchers and industry, with final rates varying with the chosen encoding method and the choices in hardware design [QRNG].

QRNGs are the natural choice to provide true randomness during the execution of a QKD protocols. The need for high-rate QKD is determined by the encryption protocol subsequently used. Whereas AES only needs 256 bits for each key, OTP requires keys as long as the encrypted message and is extremely bit-consuming. A fast randomness generation rate actively participates in increasing the final key rate, enabling the use for a secure but key-consuming encryption system such as OTP.

Commercial QRNGs with low randomness production capabilities such as the QRNG family Quantis from ID Quantique which provides 4-16 Mbit/s can considerably extend this rate by using the true randomness as seed and by generating more randomness with classical post-processing. This solution is not ideal because it degrades the quality of the final randomness but it can be used to avoid rate limitations for some very consuming applications. An example of implementation producing 40 Gbit/s of randomness for QKD with a 4 Mbit/s Quantis QRNG, which also achieve the largest distance of 421 km, is described by H. Zbinden and co-authors in the article *Secure Quantum Key Distribution over 421 km of optical fiber* (Phys. Rev. Lett. 121, 190502, 2018).

Either by new classical attacks or by quantum attacks, asymmetric algorithms based on the integer factorization and discrete logarithm problems will inevitably be broken. As we need to prepare for the era of quantum-safe algorithms, many parameters must be considered in the evaluation of future candidates.

When considering implementations, Post-Quantum algorithms benefit from the easiest transition as they do not require specific optical devices. However, a lot of efforts are made to facilitate the integration of Quantum Key Distribution hardware into standard telecom components and to allow its interoperability with already-existing systems.

From a security point of view, the strength of Post-Quantum algorithms against both classical and quantum attacks still require considerable investigation and candidates with the most convincing security proofs are flawed by unrealistic parameter requirements. Moreover, the security of these algorithms is being assessed in the light of our current knowledge and may not hold against future attacks. Quantum Key Distribution benefits from two unique abilities: to prevent information copying and to detect eavesdropping attempts. It could also enable IT-secure communications if used with the One-Time Pad encryption algorithm. Post-Quantum and QKD are both insecure against side-channel attacks and are developing various strategies to counter them.

An hybrid quantum-safe solution could use a Post-Quantum algorithm for the quantum channel authentication and Quantum Key Distribution to establish long-term secret keys, providing a solid compromise in term of implementation and security. In Quantonation, we believe that although Quantum Key Distribution is still some years ahead, its fast implementation progress and its unique security features make it an unavoidable actor in the construction of our quantum-safe future.

TO KNOW MORE

Global Quantum Cryptography Market By Component (Hardware & Service), By Enterprise (Large & Small Enterprise), By Application (Data Base Encryption, Network Layer Encryption, etc.), By End-User, By Region, Competition Forecast & Opportunities, 2023, TechSci Research (March 2018).

Breaking Symmetric Cryptosystems Using Quantum Period Finding, M. Kaplan et al., CRYPTO'16.

Quantum Computing in the NISQ era and beyond. John Preskill. Quantum 2, 79 (2018).

Applying Grover's Algorithm to AES: Quantum Resource Estimates. Markus Grassl, Brandon Langenberg, Martin Roetteler and Rainer Steinwandt. PQCrypto 2016: Post-Quantum Cryptography pp 29-43 (2016).

Factoring with n+2 clean qubits and n-1 dirty qubits. Craig Gidney. arXiv:1706.07884 (2017).

Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms, M. Roetteler et al, ASIACRYPT 2017.

Fault Tolerant Quantum Computation with Constant Error Rate, M. Ben-Or and D. Aharonov, SIAM Journal on Computing 38 (2008).

Strenghts and Weaknesses of Quantum Computing, C.H. Bennett et al, SIAM J. Comput. 26 (1997).

Quantum attacks on Bitcoin, and how to protect against them. Divesh Aggarwal, Gavin Brennen, Troy Lee, Miklos Santha, Marco Tomamichel. Ledger Vol. 3 (2018).

Quantum-secured blockchain. E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A. S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky and A.K. Fedorov. Quantum Science and Technology Vol. 3, 3 (2018).

Quantum Digital Signatures. Daniel Gottesman and Isaac Chuang. arXiv:quant-ph/0105032 (2001).

Secure Quantum Key Distribution over 421 km of optical fiber, H. Zbinden et al, Phys. Rev. Lett. 121, 190502 (2018).

Practical challenges in quantum key distribution, Eleni Diamanti et al, npj Quantum Information (2016).

Quantum Random Number Generation, X. Ma and al, npj Quantum Information (2016).

Single-Photon detectors for optical quantum applications, R. H. Hadfield, Nature Photonics (2009).

Secure Quantum Key Distribution, H-K Lo et al, Nature Photonics 8 (2014).

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

https://www.safecrypto.eu/pqclounge/

QUANTONATION

58, rue d'Hauteville
75010 Paris - France

Contact
christophe@quantonation.com

Medium

Edition: January 2019