IDQ
FROM VISION TO TECHNOLOGY

REDEFINING SECURITY

ID Quantique White Paper

IDQ ON QUANTUM TECHNOLOGIES

Version 2.0

Oct 2014

ID Quantique SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 83 79
info@idquantique.com
www.idquantique.com

Table of contents

1. Context

What is the problem with current cryptographic techniques?

The transmission of data is protected using encryption. The information is encrypted using an encryption algorithm and an encryption key, before being sent across a network. The recipient then decrypts the information by reversing the process using the key. Such a scheme is known as secret key cryptography. As the key is used both to encrypt and decrypt the data, its transfer from the sender side to the receiver side must be protected. This is known as the key distribution problem.

In conventional solutions, this problem is solved using a cryptographic scheme known as public key cryptography, where encryption is performed using a so-called “public key” while decryption requires the use of a “private key”. As the public key is only useful to encrypt, it can be distributed without special care, as long as the private key is kept secure. In practice, public key cryptography is not used for bulk data encryption, but securely to exchange a key, which is then used with a secret encryption scheme.

The problem with this approach is that the security of the currently used public key cryptosystems is not well established and they are vulnerable to:

- Human ingenuity: Public key cryptography is based on mathematical problems, which could be broken by future progress.
- Moore’s law: The increase in computing power makes it increasingly easier to break public key cryptography.
- Quantum physics: Public key cryptography is vulnerable to quantum computing, which can solve certain mathematical problems exponentially faster than classical computers.

These three vulnerabilities means that the currently used public key cryptosystems are not appropriate to secure data that require long-term security. An adversary could indeed record encrypted data today and wait until one of these vulnerabilities materializes to decrypt it.

Quantum Cryptography is an alternative solution to the key distribution problem, whose security is based on quantum physics and not on mathematical assumptions.

Note that over the past few years, cryptographers have devised a new class of public key cryptosystems, which are resilient to currently known quantum attacks. These algorithms represent an improvement compared to traditional public key cryptography, but they come no way near quantum cryptography, as they remain vulnerable to the first two threats mentioned above. Moreover there is no guarantee that new quantum attacks will not be devised against them.

IDQ believes that it is essential for organizations that have long-term security requirements to deploy a quantum-safe cryptographic infrastructure. Such an infrastructure may consist of a combination of quantum cryptography – for example to secure backbone communications – and of post-quantum cryptography – for example for end-point security.

2. Current Quantum Key Distribution (QKD)

What is Quantum Cryptography?

Quantum cryptography is a technology that uses quantum physics to secure the distribution of symmetric encryption keys. A more accurate name for it is quantum key distribution (QKD). It works by sending photons, which are “quantum particles” of light, across an optical link. The Heisenberg Uncertainty Principle stipulates that in quantum physics observation causes perturbation. This is used to verify the security of the distributed keys.

In theory, QKD should be combined to One-Time Pad (OTP) encryption to achieve provable security. However in practice, this would impose strong limitations on the available bandwidth due to the fact that the key distribution rate of QKD is typically 1’000 to 10’000 times lower than conventional optical communications.

In practice, QKD is combined with conventional symmetric encryption, such as AES, and used to frequently refresh encryption keys.

How does QKD improve traditional cryptography implementations?

A security solution is as secure as its weakest link and in network encryption, the current weakest link is the key distribution based on public key cryptography. As its name says, QKD is used to distribute encryption keys, whose security is based on quantum physics and which are therefore resilient against attacks by brute force or quantum computers. It is therefore acknowledged to be "quantum safe" (resilient to quantum computers) and is recommended for use to protect data with long-term sensitivity.

What QKD solutions currently exist?

QKD solutions currently consist of key distribution appliances combined with link encryptors.

Two QKD appliances are connected through an optical fiber and continuously distribute key material, which they store until it is requested by an encryptor. These solutions work up to a range of 100km (optical attenuation corresponding to 20dB) and are thus deployed in metropolitan area networks.

Typical applications include secure LAN extension in corporate campuses or datacenter interconnects.
The encryptors currently compatible with QKD (i.e. “Quantum enabled”) are ISO layer 2 encryptors for Ethernet and Fibre Channel with link bandwidth up to 10Gbps and aggregated bandwidth up to 100Gbps.

What market does IDQ address?

IDQ’s quantum-safe solutions are used in the financial and government sectors, as well as in enterprises with the requirement to protect IP for the long-term.

Typical applications include secure LAN extension in corporate campuses or datacenter interconnections.

The market is expanding due to the following megatrends:

- **Computing power increases**, making public key cryptography ever more vulnerable;
- **Hacking is on the rise** in a society increasingly relying on IT;

- It is now common knowledge that governments are also engaged in **massive eavesdropping projects.**

Can QKD be used as a watchdog to detect optical intrusion?

The fact that the security of QKD is based on the Heisenberg Uncertainty Principle (interception causes perturbation) may lead to think that this technology can be used as a watchdog to detection optical intrusion. This is unfortunately not true.

First, QKD performs a statistical assessment of intrusion, which means that a sufficiently large sample of data must be collected and processed. In practice, this data acquisition and processing takes a few minutes, which means that an alarm would be triggered with a delay of several minutes.

Second, using QKD as a watchdog would not protect the data transmitted in the same fiber, but at other wavelengths, which could be tapped without perturbing the quantum signals.
Symbolically, using QKD as a watchdog is analogous to installing a speed radar on a highway monitoring a single lane. The drivers in the other lane could still exceed the speed limit without being caught.

Last but not least, optical watchdogs don't work well in practical settings. Setting boundaries that are small enough to be useful, but large enough not to trigger too many false alarms is difficult. Various phenomena, such as for example component aging or optical fiber manipulation by technicians, cause the optical power in a fiber to vary over time.

Is Quantum Hacking a threat to IDQ's solutions?

Although the term "Quantum Hacking" sounds scary, it is nothing more than the translation into the quantum technology world of the security best practice of independent evaluation.

The security of QKD solutions is based on two assumptions:

- that the laws of quantum physics are correct

and

- that the actual QKD implementation complies with a model.

The field of quantum hacking actually aims at testing this second assumption and demonstrating if a practical QKD system is compatible with its model or not.
IDQ collaborates with and supports – by providing free hardware - the best quantum hacking groups worldwide to have its technology tested.
In the past, quantum hackers have demonstrated cases where commercial QKD implementations and models differed, leading to potential vulnerabilities. However, these attacks were academic and would not have worked in practical situations, as they required direct access to the equipment for calibration.
Moreover, patches to prevent these attacks, even in cases where an adversary had access to the target equipment, were developed by IDQ.

What is IDQ's approach to solving the range limitation problem?

As an optical communication technique, QKD transmission is subject to optical attenuation.
In conventional communication, this problem is solved by amplifying optical signal every 100 kilometers.
This is not possible with quantum signals, as it would induce perturbations.
IDQ pursues both short-term and long-term solutions to this limitation:

In the short-term, the approach selected by IDQ is based on trusted nodes, which consists of a receiver and an emitter used to detect the quantum signal, process it classically and re-emit it as quantum signal.

IDQ is currently jointly developing this technology with its US partner Battelle.
Trusted-nodes will require appropriate tamper protection of their cryptographically sensitive parts, which is addressed in the project.

In the long-term, IDQ's vision is to deploy quantum repeaters instead of trusted-nodes.
These devices will relay quantum signals without measuring them, and will thus not require any specific cryptographic protection.
The University of Geneva, IDQ's research partner, is one of the world leaders in this research field. However, no practical advances are expected before 5 to 10 years.

Finally IDQ is working on assessing the suitability and industrialization potential of satellite-based QKD for commercial and government applications.

3. Quantum Computing and Cryptography

What would be the impact of a Quantum Computer on the cryptographic infrastructure?

Quantum algorithms are procedures for calculation that can be run efficiently only on quantum computers. There currently exists two such algorithms that have a relevant impact on cryptographic infrastructure.

The first one is known as Shor's algorithm and it allows to efficiently factor large integers.
This problem is cryptographically relevant, as the most commonly used public key cryptography schemes – such as RSA; elliptic curves or Diffie-Hellman – are based on this problem or equivalent variants. Shor's algorithm implementation would immediately render these cryptosystems useless, no matter how long the key is.

The second algorithm is known as Grover's algorithm. It allows optimizing databases searches, which could be used in exhaustive key searches against symmetric cryptosystems. Its implementation would effectively render symmetric encryption with key length of less than 160 bits useless.
However, this means that the AES algorithm used with a key length of 256 bits can be considered as resilient to quantum computing, particularly if the key is refreshed frequently.

Finally, it is possible that other quantum algorithms threatening conventional cryptography may be discovered in the future, easing attacks even further.

When will a quantum computer be available?

It is IDQ's position that the first unclassified demonstration of the first small scale universal quantum computer will take place within the next five to ten years.

This estimate is based on the scientific state of the art for technologies such as superconducting qubits and ion traps as well as the level of investment by public funding agencies.

Government agencies are also working on this topic and investing significant resources in classified projects, so that they are likely to be ahead of public research.

Is D-Wave's Quantum Computer cryptographically relevant?

D-Wave, a Canadian company, which is developing a quantum computing platform receives a lot of publicity. This platform implements a technology known as adiabatic quantum computing, which allows to implement certain quantum algorithms – for example to perform optimization tasks – but which does not allow them to build a universal quantum computer.

Based on publicly available information, DWave's computing platform is currently not considered as cryptographically useful.

It is however important to realize that in order to implement its quantum computing platform, DWave is solving practical problems, such as optimization of Inputs/Outputs, which may be relevant to realize a universal – i.e. cryptographically relevant – quantum computer.

What is quantum-safe cryptography?

The concept of "quantum-safe" is well defined in the white paper on "Quantum-Safe Security and Cryptography"[1] by the European Telecommunications Standards Institute (ETSI). Quantum-safe cryptography are security controls which are resilient to attacks by a quantum computer. Quantum key distribution (QKD) is known to be quantum-safe. Some "post-quantum" cryptographic primitives, such as lattice-, code- or hash-based cryptosystems, are currently believed to be quantum-safe until proven otherwise.

When do I need to start worrying about Quantum Computers?

Even if the first public demonstration of a universal quantum computer will take place in the next five to ten years, this does not mean that the implementation of a quantum-safe infrastructure can be postponed until then.

For data which require long-term confidentiality, such an infrastructure must be implemented early enough, as an adversary could tap communications and store encrypted data until a quantum computer becomes available.

More specifically, one must ensure that the sum of the time needed to implement a quantum-safe infrastructure (from months to years depending on the application) and of the lifetime of the information (from seconds to decades depending on the type of information) does not exceed the time required for an adversary to develop a quantum computer (five to ten years according to IDQ's estimate).

In a wide range of cases, such as government secrets, strategic corporate information or health data to name a few, where long-term security is important, one is already in a critical situation today.

[1] ETSI white paper "Quantum-Safe Security and Cryptography"
http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/Quantum_Safe_Whitepaper_1_0_0.pdf

4. Future directions for QKD technology

Is IDQ considering QKD over satellite links?

Although it is traditionally implemented over optical fiber links, QKD could also work over satellite links. In such a scenario, a low orbit satellite or drone would be used as a moving trusted-node.

The current status of QKD over satellite links is the following:

- Demonstrations of quantum communications from ground telescope to ground telescope have been performed. Some of these demonstrations have targeted long distance, while others have looked at the tracking problem. They have confirmed the general feasibility of QKD over satellite links.
- These demonstrations have been complemented by simulations of ground to space quantum communications, which confirm feasibility but identify challenges.
- A number of projects to send a satellite with quantum communication payload are under preparation, for example in China, Canada and Europe.

IDQ is working on a feasibility study on QKD over satellite links, and the possibility to industrialize it for specific industries and applications.

Is IDQ considering QKD for mobile devices?

Although it is traditionally implemented over optical fiber links, QKD could also work over a free-space link between a handheld device and a fixed terminal such as an ATM.
Researchers have demonstrated this approach using optical hardware connected to a smart phone.

The use-case put forward by proponent of this approach is to load cryptographic keys to a handheld device by bringing it in close proximity to a fixed station, instead of connecting using a USB cable. Once loaded, key material is gradually consumed to secure communications.

The business case for QKD for handheld devices is questionable. The primary reason is the fact that long-term security – the main promise of QKD – is not needed by most end-users, which means that the price premium to introduce it would be hard to justify.
Moreover, QKD is an expensive replacement to a USB cable which is not justified by any sound threat model.

IDQ's strategy to bring QKD technology to the market is to follow a top-down approach, by targeting first the most demanding applications in terms of security, before gradually expanding to less demanding markets.
In this strategy, QKD for handheld devices is not a priority. Finally, one must note that this use-case requires QKD trusted-node to connect the fixed stations with a centralized key management system, which will allow IDQ to play in this market if a clear opportunity is identified.

What is Device Independent QKD and is it relevant?

The security of traditional QKD is based on two assumptions:

- The laws of quantum physics are correct
- The actual QKD implementation complies with a model QKD system

The first assumption cannot be formally proven, but the fact that the world behaves according to quantum physics at the microscopic level has been established by experimental evidence accumulated over more than half a century.

As for the second assumption, it is validated through security evaluation and certification, which, as with any other security solution, tests that a system behaves as expected.

The fact that the security of QKD can be established on these two simple assumptions is what gives its appeal to QKD. However, over the past few years, researchers have discovered that it is actually possible to devise QKD protocols, which can provide self-testing of the quantum layer. With these protocols, a system can perform measurements that demonstrate that it is working properly. These protocols are known as “Device Independent QKD” and they basically enable to automatically test the second assumption above.

In spite of its appeal, Device Independent QKD is not practical yet, as its implementation would require hardware that does not exist yet. Moreover, the range and the bit rate of these protocols are so low that they would serve little real purpose. Progress is nevertheless to be expected in this fruitful research field, and IDQ watches developments in order to be at the forefront of the introduction of this technology when it matures.

5. Corporate questions

What is IDQ's position on collaborating with governments?

As an independent vendor, IDQ collaborates with governments and other organizations for the evaluation and certification of its solutions, but does not engage in activities that would compromise the security offered to end-users by its products.

As a Swiss company, IDQ is also operating in an environment where government interference is forbidden by law.

Why can a non-US cryptography supplier offer better security guarantees

The Snowden scandal has demonstrated that certain technology companies have collaborated with the US government to enable it to access information that was supposed to be protected.

IDQ is a Swiss company, which guarantees its independence because:

- Switzerland is a neutral, thus independent country, and, as such, not part of any geopolitical alliance. The Swiss government does not interfere with commercial activities.
- Switzerland is a stable country both at the financial and political level, which means that IDQ can operate in a stable environment and develop a long-term strategy.

At the corporate level, IDQ implements strict governance and confidentiality principles to ensure products offer uncompromised security and that customer data are protected.