Quantum Key Distribution (QKD)

Today, we are on the edge of a quantum revolution. The advent of quantum computers in the next decade will give mankind access to unparalleled processing power with all the advantages that this brings, however this also creates challenges as they will render much of today's cybersecurity useless. So how can Quantum Key Distribution (QKD) help?

What is Quantum Cryptography (or Quantum Key Distribution)?

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 principles of quantum physics stipulate that observation of a quantum state causes perturbation. The various QKD protocols are designed to ensure that any attempt by an eavesdropper to observe the transmitted photons will indeed perturb the transmission.

This perturbation will lead to transmission errors, which can be detected by the legitimate users. This is used to verify the security of the distributed keys.

QKD implementation requires interactions between the legitimate users. These interactions need to be authenticated. This can be achieved through various cryptographic means.

The end-result is that QKD can utilize an authenticated communication channel and transform it into a secure communication channel.In theory, QKD should be combined with One-Time Pad (OTP) encryption to achieve provable security. However, an OTP requires keys, which are as long as the data to be encrypted, and can be used only once.

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.

Therefore, in practice, QKD is often combined with conventional symmetric encryption, such as AES, and used to frequently refresh short encryption keys. This is sufficient to provide quantum-safe security.

White Paper: Understanding Quantum Cryptography (https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_

What are the cybersecurity risks to current cryptographic techniques?

Our cybersecurity infrastructure requires two different functions: authentication and confidentiality. Authentication allows distant users to trust their counterpart and validate the content of their exchanges.

It is mostly implemented by public-key signature schemes. Confidentiality is required for any exchange of private information. It is often performed in a two-step process. First the users have to exchange a common secret key.

This relies on another public-key protocol, the key exchange mechanism. The secret key is then used in a symmetric key encryption scheme. Both functions therefore depend on similar cryptographic techniques, known as asymmetric or public-key cryptography.

Cybersecurity is much more than the underlying cryptography. All current hacks and security failures do not come from a weak cryptography, but rather from faulty implementation, social engineering and the like. Today, we trust the cryptography, and fight to get the implementation right.

Unfortunately, this is about to change. The point of cryptographic vulnerability today is public-key cryptography, based on algorithms such as RSA or Elliptic Curve, which are used both to authenticate data and to securely exchange data encryption keys.

The very processing power of the quantum computer can solve these mathematical problems exponentially faster than classical computers and break public-key cryptography.

This means that the currently used public-key cryptosystems are not appropriate to secure data that require long-term confidentiality. An adversary could indeed record encrypted data and wait until a quantum computer is available to decrypt it, by attacking the public keys.

We need quantum-safe cryptography today.

Why should you [illegible] quantum-safe cryptography?

The greatest threat is to public cryptography – or asymmetric algorithms – used for digital signatures and key exchange. There are already quantum algorithms, such as the famous Shor algorithm, which can break [illegible] curve algorithms, once a universal quantum computer is available.

Another famous quantum algorithm is the Grover algorithm, which attacks symmetric cryptography. Fortunately, Grover can be countered by a simple expansion of the key size. For example, AES symmetric encryption schemes with 256 bits is considered as quantum-safe.

Countermeasures against quantum computer threats rely on two pillars. On the development of new classical algorithms, which should resist the quantum computer. These are known as Post-Quantum or Quantum-Resistant algorithms.

We already encountered the example of AES above for encryption. We can also mention some signature schemes (LMS and XMSS), based on so-called hash functions.Many other algorithms, for both signature and key exchange are being developed in the framework of the NIST process. Their properties and quantum-resistance are still under test. Standardisation is expected by 2023-2024.

The second pillar, which is available today, is Quantum Key Distribution (QKD), which provide quantum-safe key exchange, based on very different principles.

Discover more (https://www.idquantique.com/resource-library/quantum-key-distribution/)

How does Quantum Key Distribution improve traditional cryptography implementations?

A security solution is as secure as its weakest link and in network encryption, the current weakest link with respect to the quantum computer threat is the secret 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 is thus guaranteed for the long-term.

What are the current QKD solutions and how do they work?

Most QKD solutions currently consist of key distribution appliances combined with link encryptors. The QKD appliances distribute the secret keys to the link encryptors. The link encryptors use the keys to encrypt large amounts of data, typically up to 100 Gb/s.

In the simplest case, two QKD appliances are connected through an optical fibre and continuously distribute key material, which they store at each end-point, until it is requested by the encryptors.

These solutions work up to an optical attenuation in the fibre of 18 dB, which corresponds to a range of about 80km, depending on the quality of the optical network.

These systems are thus typically deployed in Local Area Networks or Metropolitan Area Networks, such as corporate campuses or datacenter interconnects.

These applications have been extended to much longer distances, through the use of so-called Trusted Nodes. These trusted Nodes perform key hopping, whereby keys are generated at a starting node and transferred securely from node to node until the end node.

Instead of relying on the security of the whole transmission channel, security has to be provided at each node only. Using a similar technology, it is also possible to build various types of QKD networks, such as ring networks and star networks.

This requires more complex Key Management Schemes, which distribute the keys from and to any node in the network. For global reach, the Trusted Nodes can be implemented in satellites, with free-space QKD.

Thanks to the rapid development of QKD solutions, many encryptor manufacturers now offer “quantum enabled” devices, which accept keys from QKD appliances. These encryptors are compatible with Ethernet and Fibre Channel with link bandwidth up to 10Gbps and aggregated bandwidth up to 100Gbps.

In addition, a standard QKD interface has been developed by the ETSI (European Telecommunication Standards Institute). This will facilitate the introduction of QKD for OTN vendors.

Is QKD technology mature?

IDQ has deployed QKD systems commercially since 2007. One of the first QKD implementations was to secure elections in Geneva (see Geneva Government use case (https://marketing.idquantique.com/acton/attachment/11868/f-020f/1/-/-/-/-/Geneva%20Govt_%20DCI%20QKD%20Use%20Case.pdf)) in 2007, and this installation has been working reliably since its installation.

Since then numerous government and commercial institutions have installed the IDQ Cerberis System (https://www.idquantique.com/quantum-safe-security/products/cerberis3-qkd-system/) for secure data [illegible] in Cerberis Resource Center (https://www.idquantique.com/resource-library/quantum-key-distribution/)).

QKD users include banking and governments worldwide. Quantum cryptography, or more correctly QKD, is now a well-established commercial solution.

Standardisation work on QKD is also taking place at an increasing pace. In addition to the ETSI mentioned above, the ITU (https://www.idquantique.com/id-quantique-and-sk-telecom-le[illegible]ternational-standardizati[illegible]safe-technolog[illegible]IEEE organisations have all started working on quantum communication and QKD. Industry is getting organized for full-scale deployment of this technology.

Cerberis QKD System Brochure (https://marketing.idquantique.com/acton/attachment/11868/f-021a/1/-/-/-/-/Cerberis%20QKD%20System_Brochure.pdf)

Does Quantum Key Distribution offer absolute security?

Generally speaking, there are two conditions for a system to be secure:

- It must be based on sound principles
- Its implementation must be correct and must not open up vulnerabilities

Contrary to classical key distribution techniques, which rely on unproven assumptions and thus do not fulfil the first criterion, the security of QKD is based on the laws of quantum physics and can be rigorously proven.

This having been said, it is then important to make sure that the practical embodiment of a QKD system also fulfils the second criterion and does not have any implementation flaws.

IDQ actively participates in quantum hacking projects with well-respected academic partners, with the goal of understanding quantum-specific side channel attacks and of improving implementation security of QKD devices.

All the announcements about QKD having been hacked actually dealt with implementation flaws. These flaws are important but are inherent to any technological system.

Moreover such quantum hacking projects use open QKD systems, designed for R&D research. The quantum hacks which have been discovered to date are not viable attacks on commercial QKD systems with anti-tamper proofing and other standard security features.

In summary, the security of QKD is based on sound principles and, if properly implemented, it guarantees absolute security for key distribution.

How can IDQ help me?

Quantum Technologies are creating a world of opportunities across almost every aspect of modern life. IDQ helps you build a trusted future by preparing your organisation now. Data security is a never-ending marathon.

Adding quantum gives you a step ahead in this race. Getting prepared must be considered as a journey where every step completed adds a layer of trust and preparedness.

eBook: Quantum-Proofing Your Organisation

Recommended products

Cerberis^3 QKD System

(https://www.idquantique.com/quantum-safe-security/products/cerberis3-qkd-system/)

Centauris CN9000 Series

(https://www.idquantique.com/quantum-safe-security/products/centauris-cn9000-series/)

Centauri 800

dquantic om/
entauris-cn8000-series/)

Centauris CN6000 Series

(https://www.idquantique.com/quantum-safe-security/products/centauris-cn6000-series/)

Discover more

Products

(https://www.idquantique.com/random-number-generation/products/)

Applications

(https://www.idquantique.com/random-number-generation/applications/)

How to Buy

(https://www.idquantique.com/random-number-generation/how-to-buy/)

Connect with IDQ

ID Quantique SA | Chemin de la Marbrerie 3
1227 Carouge - Genève | Switzerland

T +41 22 301 83 71
F +41 22 301 83 79
info@idquantique.com

(https://twitter.com/idquantique) (https://www.linkedin.com/company/id-quantique-sa)

First Name *

Last Name *

Company *

Email *

Phone *

Message

From t[illegible]me, we would like to s[illegible]you i[illegible]nation regardi[illegible]odu[illegible]d services we b[illegible]e will be of interest. To do so, we require your consent. Please use the tick boxes below (tick all that are ap[illegible]ri[illegible]o indicate your pre[illegible]ce.

☐ Ema[illegible] ☐ Telepho[illegible] ☐ Post

We will treat your data with respect and in accordance with our Contact Promise (https://www.idquantique.com/contact-promise/).

I'm not a robot

reCAPTCHA
Privacy - Terms

Arrange a Call Back