id Quantique

White Paper

Future-proof Data Confidentiality with Quantum Cryptography

Version 1.0

April 2005

id Quantique

A Quantum Leap for Cryptography

id Quantique SA
Ch. de la Marbrerie, 3
1227 Carouge/Geneva
Switzerland

Tel: +41 (0)22 301 83 71
Fax: +41 (0)22 301 83 79
www.idquantique.com
info@idquantique.com

Table of contents

"Tapping a fibre-optic cable without being detected … has certainly been done by intelligence agencies for the past seven or eight years. These days, it is within the range of a well-funded attacker…"

John Pescatore, Gartner Group, former National Security Agency analyst

Vectis Link Encryptors offer :

- ✓ Security against optical fibre cable tapping
- ✓ Strong cryptography
- ✓ Automated operation
- ✓ Eavesdropping revealed

Box 1: More information on Quantum Cryptography

- Understanding Quantum Cryptography – for a first introduction to quantum cryptography and a discussion of how it fits within the framework of conventional cryptographic techniques.
- Securing Networks with the Vectis Quantum Link Encryptor – for information about practical applications of quantum cryptography and how it can be deployed in an existing network.
- Quantum Cryptography, Review Article– for more information on the scientific aspects, both theoretical and experimental, of quantum cryptography.
- Vectis Product Family Specification Sheets – for technical information on the Vectis Quantum Link Encryptor.

These documents are available online from www.idquantique.com.

1. Introduction

In a world where information has become the fuel of enterprises, protecting the confidentiality and integrity of their critical data is of vital importance for organizations. The implementation of a comprehensive and well-thought-out information security policy reinforces a company's position with regard to its customers, partners and employees.
This document describes how the deployment of quantum cryptography can help an organization to close loopholes in its information security architecture and reduce its vulnerability to cybercrime.

For more information on quantum cryptography, refer to the documents listed in Box 1.

2. The Importance of Information Security

At a time when the reliance upon electronic data transmission and processing is becoming every day more prevalent, unauthorized access to proprietary information is a real threat. In 2004, 53% of the respondents of the CSI/FBI Computer Security and Crime Survey[1] admitted having been subjected to unauthorized use of computer systems. These attacks caused a total loss of more than 140 million USD for the respondents of the survey[2]. Moreover, it is generally admitted by experts that the vast majority of information security incidents and attacks go unreported.
These facts clearly demonstrate that it is vital for organizations to implement comprehensive information security policies and countermeasures in order to protect reputation, ensure business continuity and guarantee information availability, integrity and confidentiality. Besides, legal and compliance requirements also often demand such measures. Last but not least, the way an organization protects its information assets increasingly impacts the image projected to customers and partners.

3. Protecting Information

Efficiently protecting critical information within an organization requires the definition and the implementation of a consistent information security policy. Such a policy describes which processes and means must be applied within the company to achieve this goal.
It puts into practice technologies such as biometrics or smartcards, for instance, to control access to the data processing and storage infrastructures – whether electronic or not – and guarantee the physical security of the information. It also resorts to solutions such as Intrusion Prevention and Detection systems, Firewalls and Antivirus Software to defend a secure perimeter around the internal computer network of the organization and prevent hackers from penetrating it. Finally, it defines measures to protect information transmission between remote sites. This last aspect of information security is often overlooked.

4. Tapping Optical Fibre Cables

Contrary to a false perception, intercepting information transmitted over an optical fibre cable – an optical fibre is a thin rod of glass which transmits light to carry information – is not only possible but also quite easy in practice. "Tapping a fibre-optic cable without being detected, and making sense of the information you collect isn't trivial but has certainly been done by intelligence agencies for the past seven or eight years" explains John Pescatore, VP of Security at the Gartner Group and a former US National Security Agency analyst[3]. "These days, it is within the range of a well-funded attacker, probably even a really curious college physics major with access to a fibre-optics lab and lots of time on his hands" adds Pescatore. Bending an optical fibre is indeed sufficient to extract light from it. Optical taps are readily

[1] 2004 CSI/FBI Computer Security and Crime Survey, Computer Security Institute, www.gocsi.com.
[2] A total number of 481 organizations responded to the survey.
[3] Quotation from "Intelligence ops in Baghdad show need for physical security back hom", Dan Verton, Computerworld, April 8, 2003.

available from a variety of manufacturers and are inexpensive (less than 500 €). A typical optical tap is shown in Fig. 1. Even undersea cables may also be at risk, as illustrated by the launch in early 2005 of a submarine with alleged eavesdropping cababilities, by the US Navy.

Optical fibre cables have replaced copper cables for all high bandwidth links and they become every day more prevalent in worldwide telecommunication networks. Whether they are aware of it or not, organizations almost certainly rely on optical fibres to transmit their information. Companies typically have three possibilities to obtain connectivity. They can purchase bandwidth from a telecommunication operator. In this case, the data from the company is aggregated in a telecommunication station with that of other companies and transmitted over an optical fibre. The second possibility is to rent or purchase dedicated optical fibres (also known as dark fibres). In the most demanding applications, these dedicated optical fibres are installed specially for the company in order to guarantee that they do not pass through any telecom exchange or station.

Optical fibre cables are thus often used to carry confidential information, despite their intrinsic vulnerability. As they constitute a dangerous loophole in the information security infrastructures of an organization, the optical links used to transmit sensitive data must be identified and protected by appropriate measures.
One can assess the level of criticality of a particular link by looking at the value (confidentiality, lifetime, etc.) of the data transmitted, its volume, and the damage potential in case of breach (see Fig. 2) and by defining threat models. Examples of such critical links include the remote connection between enterprise servers and a storage and archiving site, or between local area networks carrying sensitive information.

Figure 1: Optical tap are commercially available and cost less than €500.

5. Conventional Cryptography to Encrypt Sensitive Data

As telecommunication links are intrinsically vulnerable to eavesdropping, cryptography is routinely used to protect data transmission. It consists in scrambling information prior to its transmission, by combining it with a key using a cryptographic algorithm[4]. The recipient uses the key and a decryption algorithm to reverse the process and recover the information. Even if he intercepted the encrypted information, an eavesdropper would not be able to gain knowledge about it without knowing which cryptographic key was used. The only thing he could do, is to try all the keys one by one until he finds the right one. If the key is sufficiently long and changed frequently enough, this task cannot be completed. Because of this, these algorithms are called secret key cryptography.

[4] Cryptography will not be presented in detail here. For a comprehensive discussion, refer to "Applied Cryptography", Bruce Schneier, *Wiley*. "The codebook", Simon Singh, *Fourth Estate*, presents an excellent non-technical introduction and historical perspective on cryptography.

The problem with this approach is that the key must first be exchanged between the sender and the recipient before it can be used. As the security of the whole scheme depends on the fact that the eavesdropper does not know the key, this step is critical. A trusted courier must be used to carry the key. This method is very expensive to implement and may represent a threat, as the key can be copied. Moreover, as it is not practical at all, the key is not exchanged very frequently, putting vast volumes of data at risk in case a key is compromised.

In the 1970's, a new class of cryptographic algorithms – public key cryptography – was invented and allowed to get round the problem of key distribution. With these algorithms, two different keys are used. The so-called public key is used to encrypt information, while the private key serves to decrypt it. Before the transmission of information, the recipient publicly discloses his public key, while keeping his private key secret. The sender can then encrypt the information with the public key. Only the legitimate recipient will be able to decrypt the information with his private key.

Unfortunately this type of cryptographic techniques is at risk. It is indeed based on the assumption that it is not possible for an adversary to deduce the private key from the public one. Doing so is not impossible, but very time consuming. The fact that computing power increases means that it progressively becomes simpler. Data that are secure today will not necessarily be secure next year. In addition, there is no theoretical proof that this operation could not be done significantly faster. This means that someone could, by following new approaches, invent a novel method to crack keys with limited computing resources. Finally, it is already proven that quantum computers[5] will allow to break public key cryptography. To illustrate these vulnerabilities, one should remember that some of the inventors of public key cryptography challenged the scientific community in an article entitled "A new kind of cipher that would take million of years to break" and published in the late seventies to try to break a key (428 bits long). Although they had estimated that the key would be secure for 40 quadrillion years, it was broken in the mid 90's.

Public key cryptography is appropriate to ensure short-term confidentiality of data, but does not offer future-proof security, as it is not built on solid ground. The only way to guarantee long-term security of critical data is to use secret key cryptography and to carefully manage and frequently refresh keys.

6. Quantum Cryptography to Securely Exchange Keys

Quantum cryptography was invented about twenty years ago and complements conventional cryptographic techniques to raise security of data transmission over optical fibre links to an unprecedented level. It exploits the laws of quantum physics[6] to reveal the interception of information exchanged between two stations. According to the Heisenberg Uncertainty Principle, it is not possible to observe a quantum object without modifying it. In quantum cryptography, single light particles – also known as photons – which are described by the laws of quantum physics, are used to carry information over an optical fibre cable. By checking for the presence of disturbances, it is possible to verify if a transmission has been intercepted or not. Quantum physics guarantees indeed that the interception of the single photons necessarily translates into perturbations which can be observed.

This technology can be used to exchange keys between two remote sites connected by an optical fibre cable, and to confirm their secrecy. The keys are then used with secret key algorithms to securely encrypt information. With such an approach, it is possible to guarantee future-proof data confidentiality based on the laws of quantum physics. Its deployment on critical links allows thus to raise the information security level of an organization.
Recognizing this, the MIT Technology Review and Newsweek magazine identified quantum cryptography in 2003 as one of the "ten technologies that will change the world"[7].

For more information on Quantum Cryptography, refer to the documents listed in Box 1.

[5] Quantum computers are computers that exploit the laws of quantum physics to process information. They are still in the realm of experimental research, but will eventually be built.

[6] Quantum physics is the set of theories describing the microscopic world.

[7] MIT Technology Review, February 2003 and Newsweek, July 7 2003.

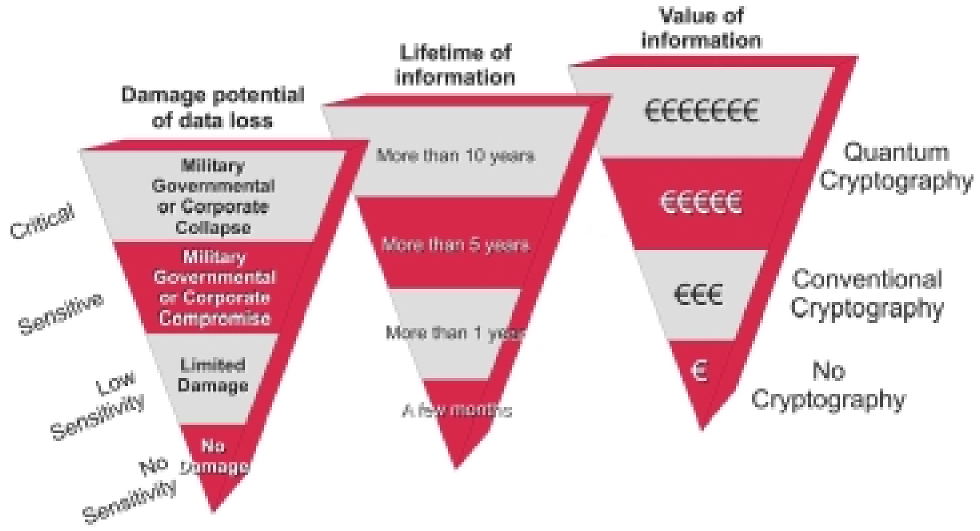

Figure 2: Schematic showing the different degrees of importance of three parameters: damage potential of data loss, lifetime of information and value of information.

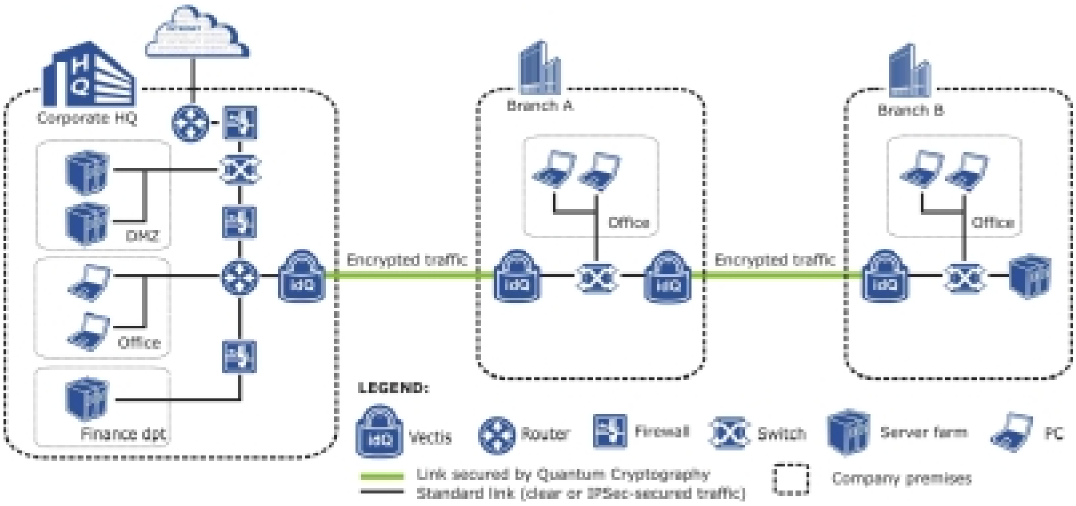

Figure 3: The network of company XYZ Corp., consisting of three local area networks (LANs) connected by two pairs of Vectis LEs. The optical links connecting the company's headquarters and branches A and B are secured with Vectis Link Encryptors, the strongest-available encryption technology based on Quantum Cryptography.

7. Vectis Link Encryptor

Vectis is the name of id Quantique's link encryptor implementing quantum cryptography for commercial applications. Vectis Link Encryptors are used in pairs, one connected at each end of a dedicated optical fibre. They allow to remotely connect computer networks with an unprecedented level of security. They encrypt Ethernet traffic transmitted between two sites and they can be integrated very easily into a network, usually without any impact to the existing infrastructure. Applications include the secure connection of two or more remote local area networks located in different sites, as shown in Fig. 3, or the secure transmission of data to remote storage and backup sites. Current Vectis Quantum Link Encryptors have a transmission range of 100 kilometers (60 miles), which is sufficient to cover the vast majority of applications worldwide where dedicated optical fibre links are used. Longer distances can be achieved by chaining Vectis network appliances, as shown in Fig. 3.

The Vectis Quantum Link Encryptors are essential pieces of equipment for organizations wishing to deploy secure networks. They enable to raise the confidentiality of data transmissions over critical links to unprecedented levels, thanks to the future-proof security they offer. By making it possible to use non-proprietary optical fibre cables, such as metro loops built by telecommunication companies, for critical links, without compromising security, they allow to reduce overall telecommunication costs. Finally, their operation is fully automated, which constitutes an additional protection against human errors, whether spiteful or not. This feature also ensures that the overall cost of ownership is low.

For more information on the Vectis Link Encryptor, refer to the documents listed in Box 1.

8. Conclusion

Quantum cryptography allows to reach unprecedented levels of security guaranteed by quantum physics for data transmissions over optical networks. The Vectis Link Encryptor features an excellent security over costs ratio. It allows to protect optical fibre links against eavesdropping, without the vulnerabilities of conventional cryptographic techniques. Because of this, it is essential for organizations exchanging confidential data between remote sites to consider Vectis to secure their critical links.