# BUSINESS WHITE PAPER

UNIL | Université de Lausanne

SECOQC

## QUANTUM CRYPTOGRAPHY:

## An Innovation in the Domain of Secure Information Transmission

Professor Solange GHERNAOUTI – HÉLIE – Faculty of Business and Economics University of Lausanne - SWITZERLAND

**A Business White Paper to:**

**Explain** the innovation produced by the SECOQC consortium
**Promote** the use of quantum cryptography by describing the business advantages
**Facilitate** decision making processes for adoption of quantum cryptography solutions
**Raise** public awareness of the possible use of the application of quantum physics to enhance actual cryptographic security mechanisms.

**Business Context:**

Information Security is a **business enabler**
Data protection is a **concern of top management** and depends on the **level of criticality** of informational values
Several **regulations** like Sarbanes-Oxley Act and the Basel II agreements have recently emerged

Offering a good level of data confidentiality is an important feature for business realization and conformity requirements.
Contemporary commercial cryptographic solutions are not provably secure, Quantum cryptography solutions are now available to build secure communication infrastructures without intermediary – Secrecy assurance -


**Needs and Issues:**

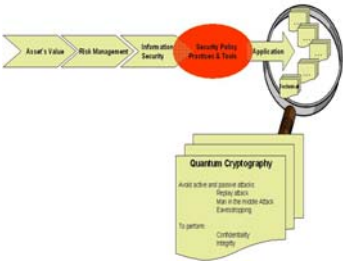
Optical fibers are vulnerable to eavesdropping

Need to encrypt data

Need to share secret keys

Symmetric and asymmetric cryptography

The Key Establishment and Distribution Problem




**QKD- a solution for secure information transmission in critical environments**:

QKD can be used to used to exchange keys between two remote sites - confirming secrecy - protecting optical fibers links against eavesdropping

Key's real randomness

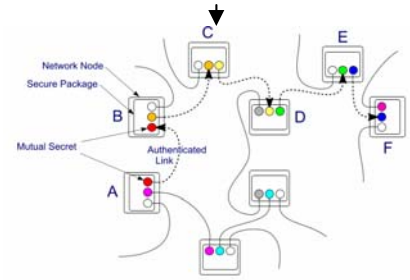
Gives a solution to the key establishment problem

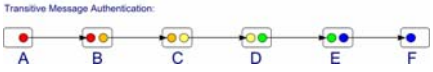
Combine the encryption, via the One-Time-Pad and QKD security everlasting security

Place security in a long run vision

A wide class of attacks could be obviated

**Quantum Cryptography is an innovative solution to classical cryptography limitations for institution's effectiveness and competitiveness**




**Competitive advantage - Image and reputation advantages**

QC can "protect informational assets in the best way" as specified by many regulations

Cost savings in term of investments, upgrading costs, changing costs, risk related costs etc.

Relatively easy adoption of QKD technology given that the historical security & legacy systems are mastered

QKD standardization process already started

**Practical and operational advantages**

Contribute to build a trusty relationship

Investment into a technology with a high potential of remaining secure for a longer time

Conformity with several IS related regulations - prevent organizations juridical risk

Common Criteria Certification (CCC) = Effectiveness + Efficiency

**Standardization activities has been proposed by University of Lausanne through ETSI**

ETSI – ISG initiative has been launched on July 2008 for business application and for technical standards

Business application : the analysis of business requirements for different groups of prospective users, as well as with the development and definition of suitable interfaces.

Technical standards: QKD specifications 'from bottom up', properties of specific macroscopic quantum optical components and interfaces between components of quantum cryptographic systems shall be subject to standardization.

**Social and Economical Impacts:**

The use of quantum key distribution for robust secret transmission will change the actual network security paradigm

Quantum cryptography can contribute to build confidence in the use of ICTs and to generate direct and indirect profits

A digital security gap will be amplified between those who use QKD and those who haven't yet access to this technology

Rethink fundamentals in cryptography is the only solution to develop a new vision of security for the benefice of transactions that are critical for institutions and people

QKD allows organizations to be no more at the same level of insecurity as their competitors

By quantum key distribution organizations have for the first time, the means to be sure that their data are under their own control and cannot be obtained by eavesdropper without the sender or recipient knowledge. Organizations who use QKD are the only owners of their secrecies

SECOQC project and operational solutions openly demonstrates that innovation in quantum physic is becoming mature to enter in industrialization phase and to produce effective security solution

contact: sgh@unil.ch

Contributing authors: S. Ghernaouti – Hélie; I. Tashi; Th. Länger; C. Monyk