SECOQC
Development of a Global Network for Secure Communication based on Quantum Cryptography

Miloslav Dušek, Palacký University, Olomouc
On behalf of the EU-Integrated Project SECOQC
www.secoqc.net
SECOQC

- EU-Integrated Project (FP6)  
  April 2004 – September 2008

- **Scientific and Technological Objectives:**
  - Improve Quantum Key Distribution (QKD) technology
  - Develop Network Concept
  - Develop Interfaces (for Customers, QKD-Providers)

- SECOQC has initiated QKD standardization
More Facts...

- **41 Participants:**
  - 25 Universities
  - 4 National Research Centers
  - 8 Multinational Enterprises
  - 4 SMEs

- **From 11 European Countries**
  - A, B, CH, CZ, D, DK, F, I, RU, S, UK

- **Budget:** 16,5 million Euros
- **Funding:** 11,3 million Euros
Quantum key distribution

• Quantum physics solves the problem of the distribution of cryptographic keys – “unconditional” security
• Information in encoded into non-orthogonal states of quantum systems (e.g. photons)
• Any interaction with a quantum system which can lead to information leakage disturbs its state in general
• Eavesdropping can be detected – it affects quantum states of the carriers of information and causes detectable errors
• If eavesdropping is detected the key is not used
• Any “technological” errors must be treated as if they were caused by eavesdropping – privacy amplification is necessary
Limitations of QKD

- Point to point links
- Limited distance (today: ~ 100 km in fibers)
- Limited data rate (mainly due to detectors)

Solution:

*Network with trusted nodes* (main goal of SECOQC)
- Any users can be interconnected
- Nodes serve as classical repeaters
- Parallel links; key can be generated in advance
A Trusted repeater QKD-Network: Abstract Architecture

VPN-yellow
Site 1

VPN-green
Site 1

VPN-yellow
Site 2

Data layer

Key generation layer

Quantum layer

QKD Access Node

QKD Core Node
SECOQC Prototype - principle layout

QKD links - standard optical fibers
QKD Links

- **Coherent One Way System**
  
  (Univ. Genève)

- **One Way Weak Pulse System**
  
  (Toshiba)

- **Autocompensating Plug&Play**
  
  (id Quantique, Genève; 3 links)
QKD Links

• Entangled Photons
  (Univ. Vienna / ARC)

• Continuous Variables
  (CNRS / Thales)
Palacký University & SECOQC

Department of Optics of Palacký University in Olomouc participated in the work of the Quantum Information Theory group

- Evaluation of security and performance of the experimental platforms
- Security proofs for practical QKD devices
Thank you for your attention

Review article on quantum cryptography:

This paper has been written within the European Project SECOQC