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

Bringing Socio-Economics into a Technological Project - The SECOQC case

ERAcademy

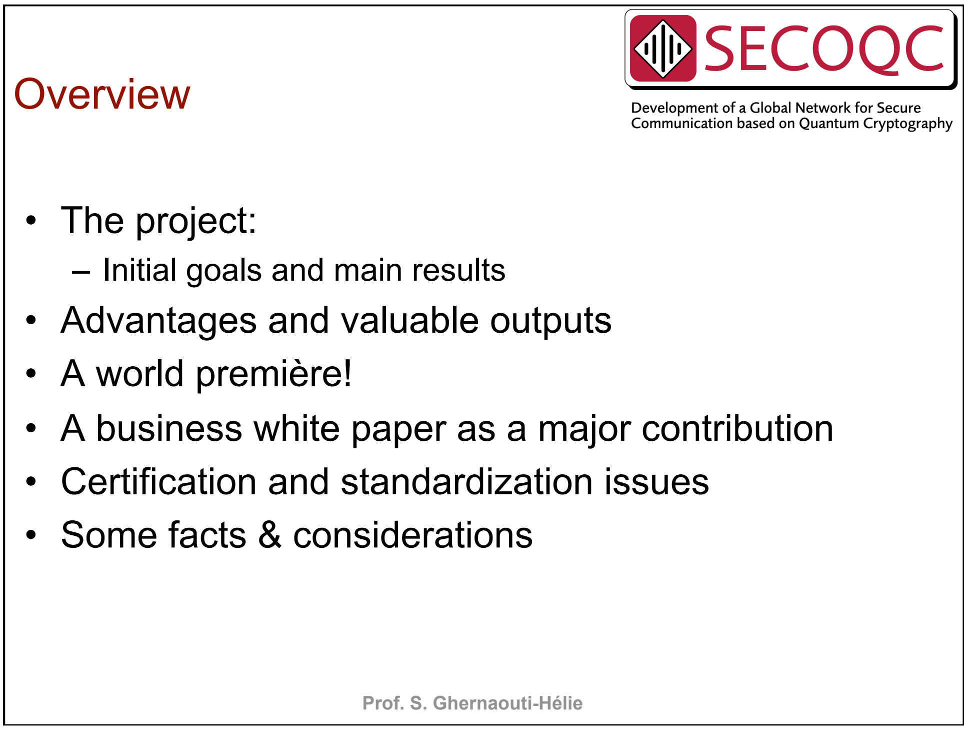
30 . 09. 2009 EPFL

Prof. Solange GHERNAOUTI-HÉLIE

Présidente de la Commission Sociale
Présidente de la Commission Egalité des Chances
www.hec.unil.ch/sgh

Faculty of Business and Economics – HEC – UNIL

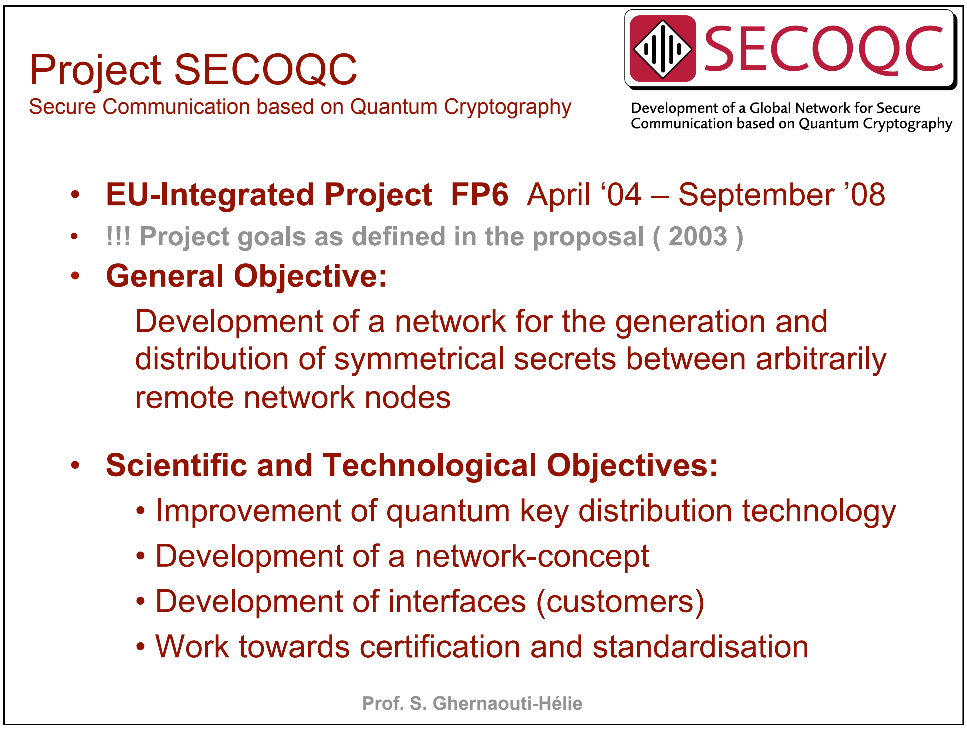
Secoqc Key researcher



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

Overview

- The project:
  - Initial goals and main results
- Advantages and valuable outputs
- A world première!
- A business white paper as a major contribution
- Certification and standardization issues
- Some facts & considerations



Project SECOQC

Secure Communication based on Quantum Cryptography

SECOQC

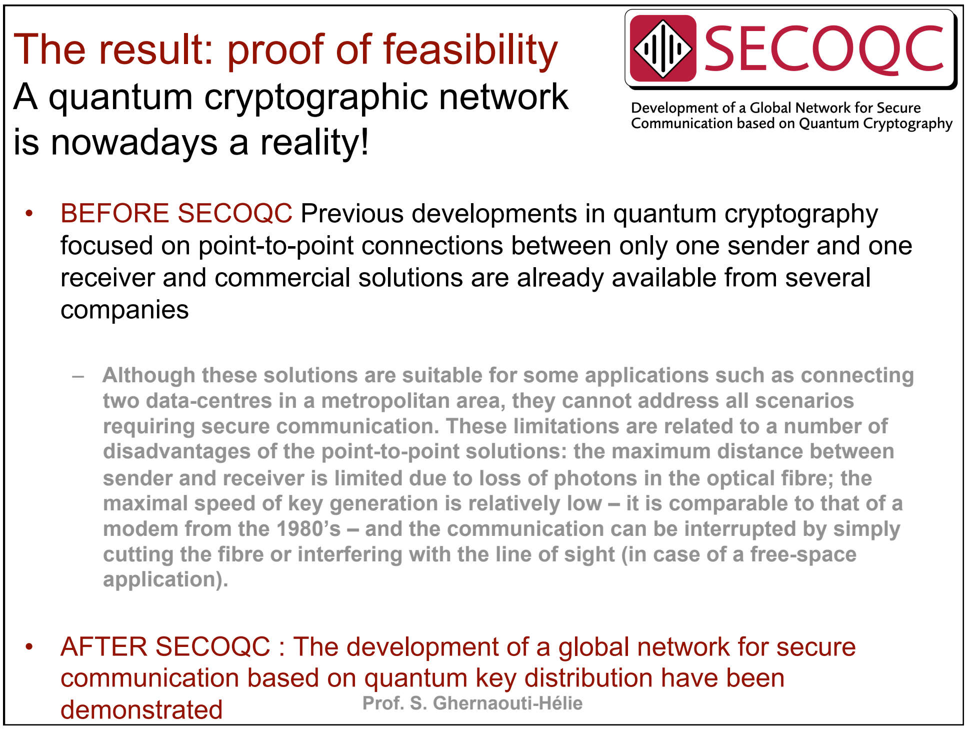
Development of a Global Network for Secure Communication based on Quantum Cryptography

- **EU-Integrated Project FP6** April '04 – September '08
- **!!! Project goals as defined in the proposal (2003)**
- **General Objective:**

  Development of a network for the generation and distribution of symmetrical secrets between arbitrarily remote network nodes

- **Scientific and Technological Objectives:**
  - Improvement of quantum key distribution technology
  - Development of a network-concept
  - Development of interfaces (customers)
  - Work towards certification and standardisation

Prof. S. Ghernaouti-Hélie



The result: proof of feasibility

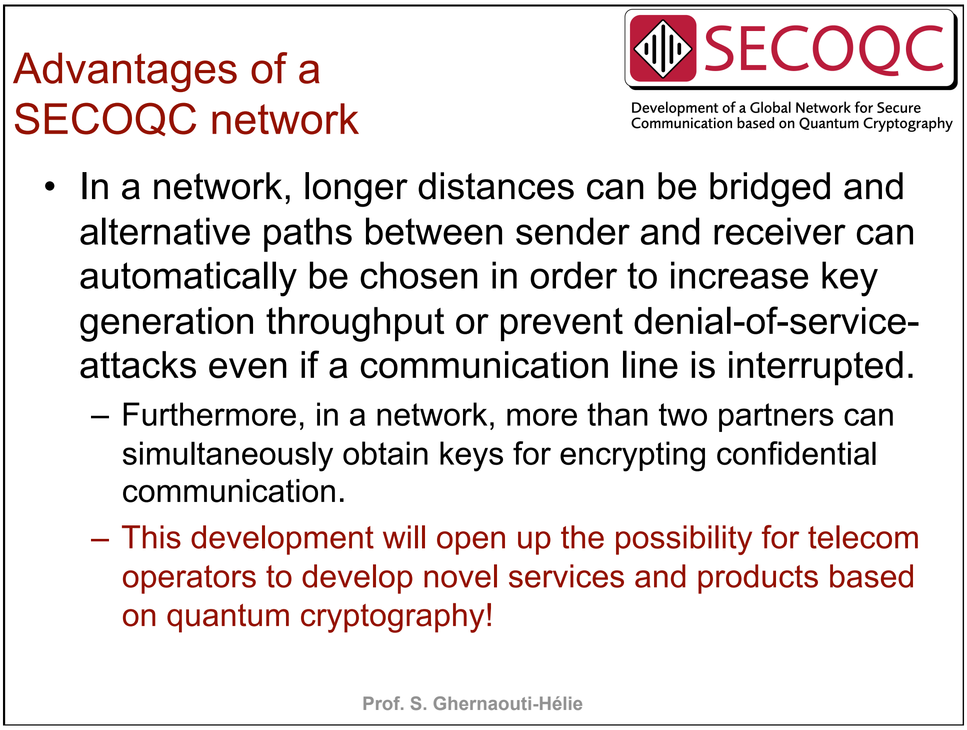
A quantum cryptographic network is nowadays a reality!

SECOQC

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

- BEFORE SECOQC Previous developments in quantum cryptography focused on point-to-point connections between only one sender and one receiver and commercial solutions are already available from several companies
  - **Although these solutions are suitable for some applications such as connecting two data-centres in a metropolitan area, they cannot address all scenarios requiring secure communication. These limitations are related to a number of disadvantages of the point-to-point solutions: the maximum distance between sender and receiver is limited due to loss of photons in the optical fibre; the maximal speed of key generation is relatively low – it is comparable to that of a modem from the 1980's – and the communication can be interrupted by simply cutting the fibre or interfering with the line of sight (in case of a free-space application).**
- AFTER SECOQC : The development of a global network for secure communication based on quantum key distribution have been demonstrated

Prof. S. Ghernaouti-Hélie

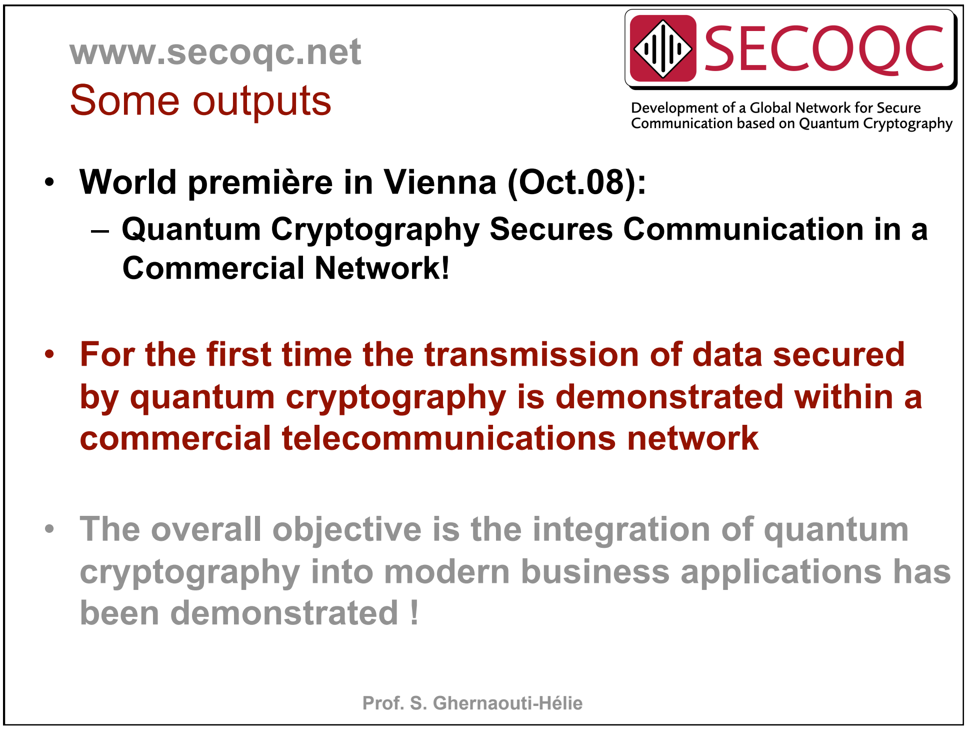


Advantages of a SECOQC network

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

- In a network, longer distances can be bridged and alternative paths between sender and receiver can automatically be chosen in order to increase key generation throughput or prevent denial-of-service-attacks even if a communication line is interrupted.
  - Furthermore, in a network, more than two partners can simultaneously obtain keys for encrypting confidential communication.
  - This development will open up the possibility for telecom operators to develop novel services and products based on quantum cryptography!

Prof. S. Ghernaouti-Hélie

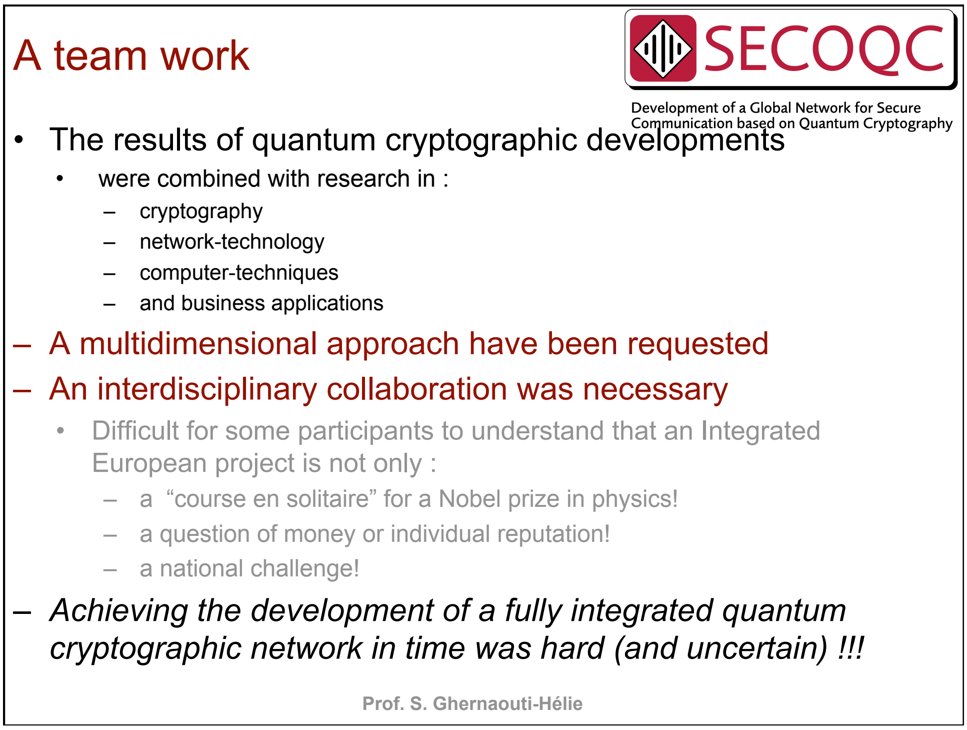


www.secoqc.net
Some outputs

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

- **World première in Vienna (Oct.08):**
  - **Quantum Cryptography Secures Communication in a Commercial Network!**
- **For the first time the transmission of data secured by quantum cryptography is demonstrated within a commercial telecommunications network**
- **The overall objective is the integration of quantum cryptography into modern business applications has been demonstrated !**

Prof. S. Ghernaouti-Hélie



A team work

SECOQC

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

- The results of quantum cryptographic developments
  - were combined with research in :
    - cryptography
    - network-technology
    - computer-techniques
    - and business applications

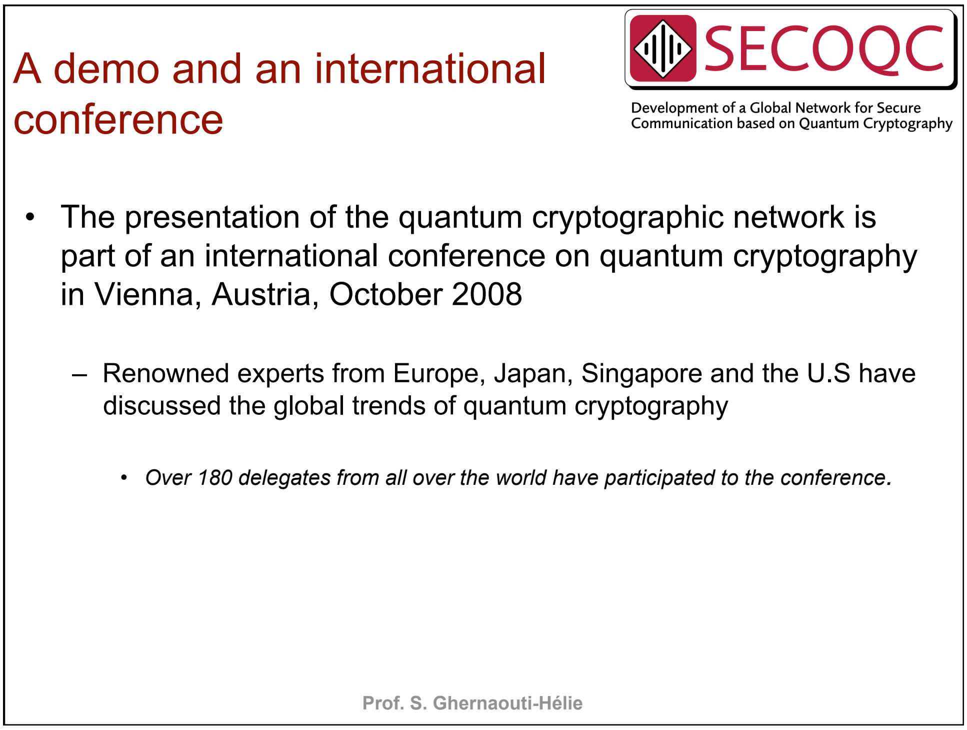
– A multidimensional approach have been requested

– An interdisciplinary collaboration was necessary

  - Difficult for some participants to understand that an Integrated European project is not only :
    - a "course en solitaire" for a Nobel prize in physics!
    - a question of money or individual reputation!
    - a national challenge!

– *Achieving the development of a fully integrated quantum cryptographic network in time was hard (and uncertain) !!!*

Prof. S. Ghernaouti-Hélie



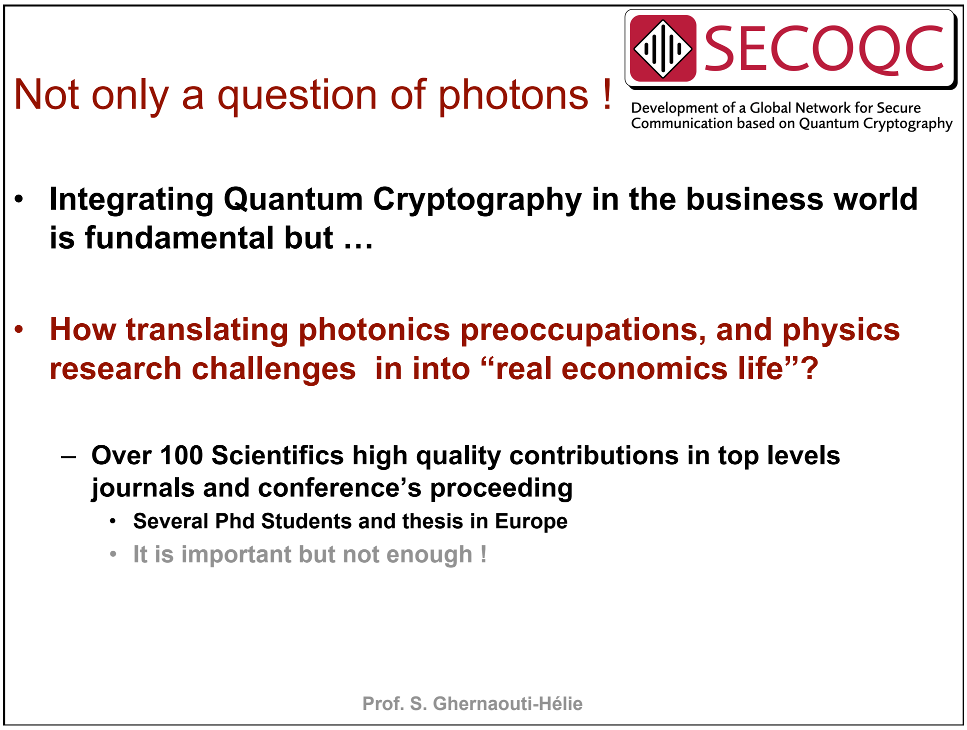
A demo and an international conference

SECOQC

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

- The presentation of the quantum cryptographic network is part of an international conference on quantum cryptography in Vienna, Austria, October 2008
  - Renowned experts from Europe, Japan, Singapore and the U.S have discussed the global trends of quantum cryptography
    - *Over 180 delegates from all over the world have participated to the conference.*

Prof. S. Ghernaouti-Hélie

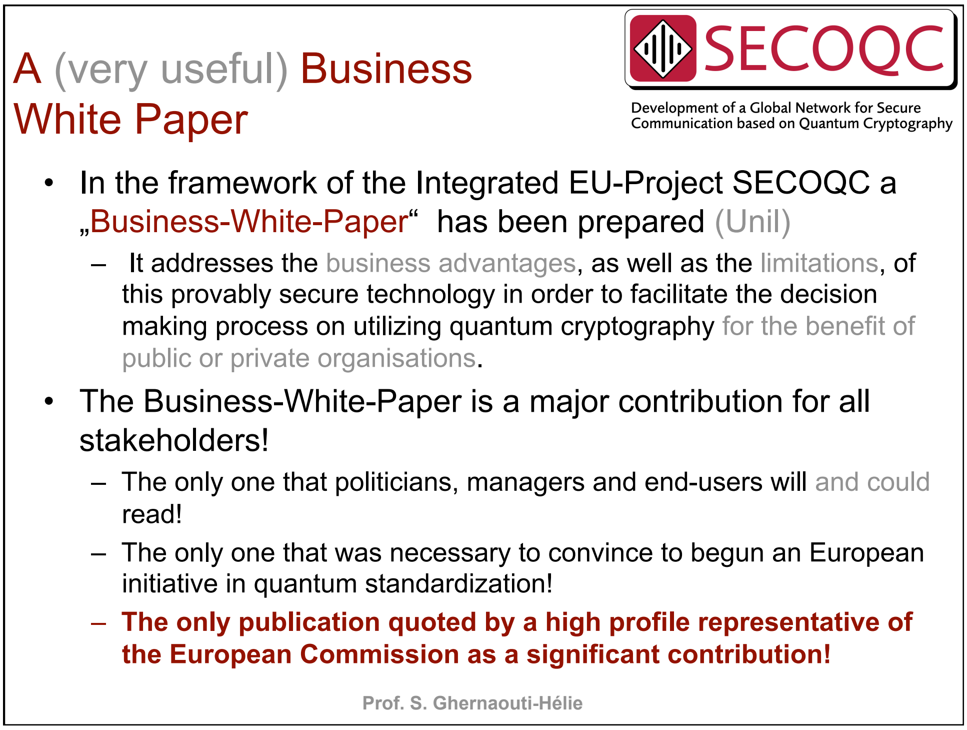


Not only a question of photons !

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

- **Integrating Quantum Cryptography in the business world is fundamental but …**
- **How translating photonics preoccupations, and physics research challenges in into "real economics life"?**
  - **Over 100 Scientifics high quality contributions in top levels journals and conference's proceeding**
    - **Several Phd Students and thesis in Europe**
    - **It is important but not enough !**

Prof. S. Ghernaouti-Hélie

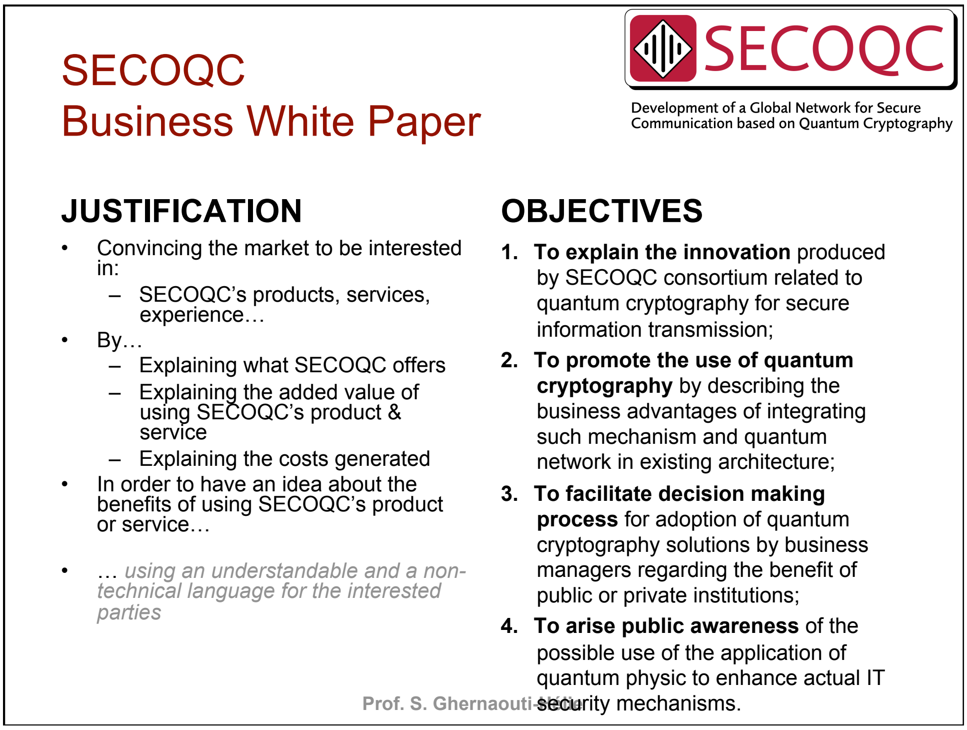


A (very useful) Business White Paper

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

- In the framework of the Integrated EU-Project SECOQC a „Business-White-Paper" has been prepared (Unil)
  - It addresses the business advantages, as well as the limitations, of this provably secure technology in order to facilitate the decision making process on utilizing quantum cryptography for the benefit of public or private organisations.
- The Business-White-Paper is a major contribution for all stakeholders!
  - The only one that politicians, managers and end-users will and could read!
  - The only one that was necessary to convince to begun an European initiative in quantum standardization!
  - **The only publication quoted by a high profile representative of the European Commission as a significant contribution!**

Prof. S. Ghernaouti-Hélie



SECOQC Business White Paper

SECOQC

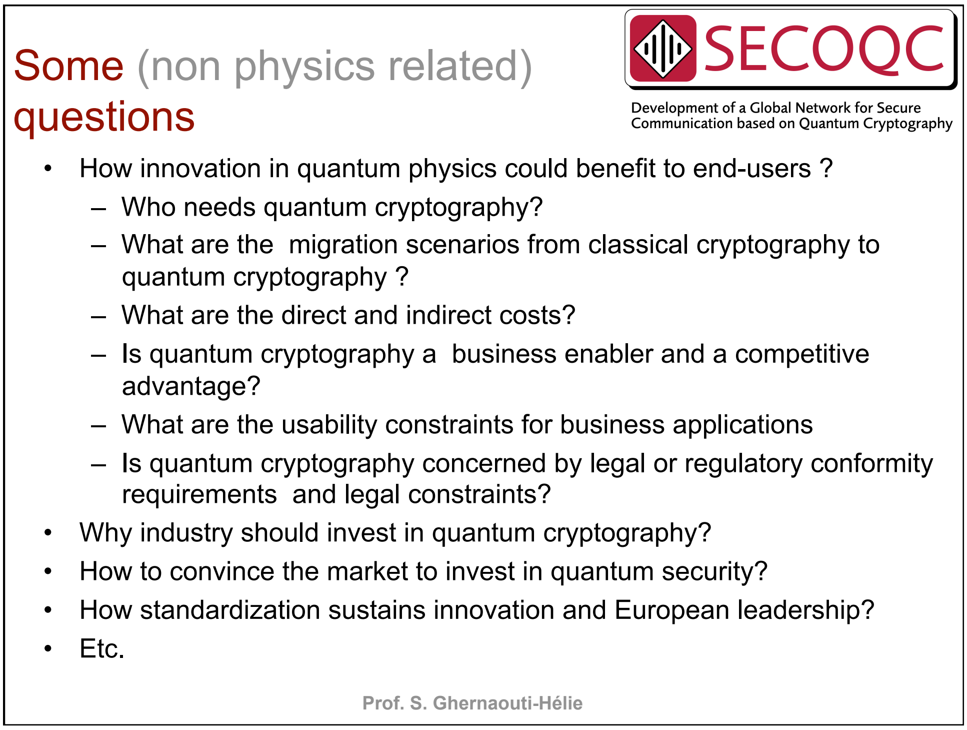
Development of a Global Network for Secure Communication based on Quantum Cryptography

JUSTIFICATION

- Convincing the market to be interested in:
  - SECOQC's products, services, experience…
- By…
  - Explaining what SECOQC offers
  - Explaining the added value of using SECOQC's product & service
  - Explaining the costs generated
- In order to have an idea about the benefits of using SECOQC's product or service…
- … *using an understandable and a non-technical language for the interested parties*

OBJECTIVES

1. **To explain the innovation** produced by SECOQC consortium related to quantum cryptography for secure information transmission;
2. **To promote the use of quantum cryptography** by describing the business advantages of integrating such mechanism and quantum network in existing architecture;
3. **To facilitate decision making process** for adoption of quantum cryptography solutions by business managers regarding the benefit of public or private institutions;
4. **To arise public awareness** of the possible use of the application of quantum physic to enhance actual IT security mechanisms.



Some (non physics related) questions

SECOQC

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

- How innovation in quantum physics could benefit to end-users ?
  - Who needs quantum cryptography?
  - What are the migration scenarios from classical cryptography to quantum cryptography ?
  - What are the direct and indirect costs?
  - Is quantum cryptography a business enabler and a competitive advantage?
  - What are the usability constraints for business applications
  - Is quantum cryptography concerned by legal or regulatory conformity requirements and legal constraints?
- Why industry should invest in quantum cryptography?
- How to convince the market to invest in quantum security?
- How standardization sustains innovation and European leadership?
- Etc.

A unique initiative
A step ahead!

SECOQC

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

- **European standardization: „ETSI Industry Specification Group“ a value added for Europe**
  - In the framework of the conference the kick-off-meeting of the „Industry Specification Group on Quantum Key Distribution and Quantum Technologies“ has taken place.
- Under the direction of the European Telecommunication Standards Institute (ETSI) representatives of industries and future users have started to develop international standards for this new technology.
- This group is a result of the standardization initiatives started in the framework of the SECOQC – Standardization and Certification Subproject by the Austrian Research Centers and the **University of Lausanne**.
- The standardization initiative is a major step for European competiveness in security & cryptography

Prof. S. Ghernaouti-Hélie

Standardisation in SECOQC

SECOQC

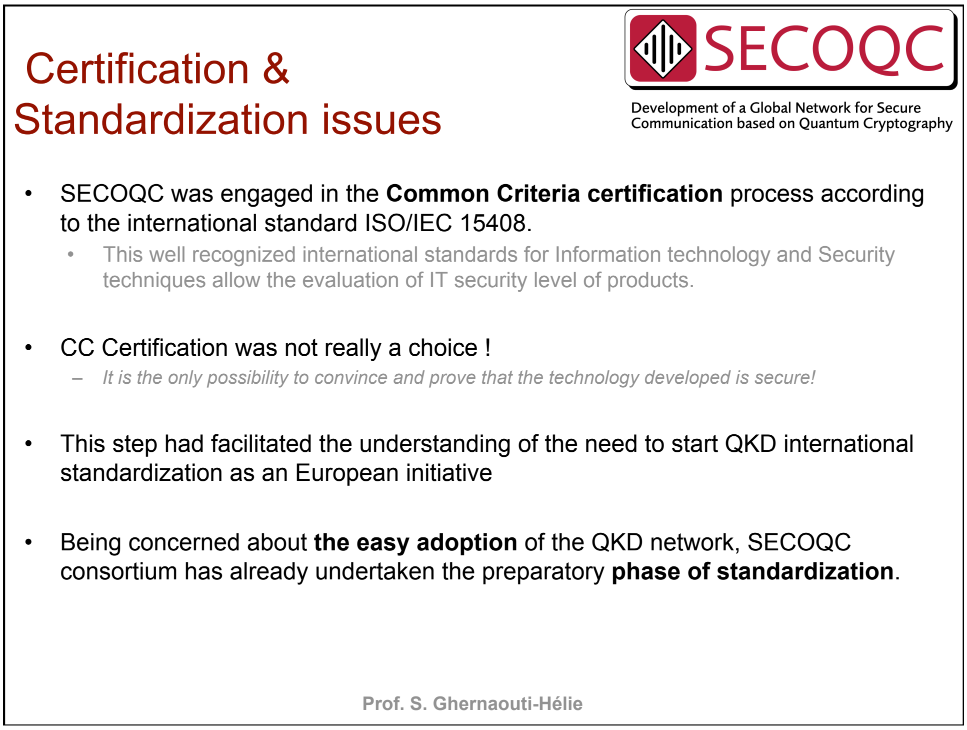
Development of a Global Network for Secure Communication based on Quantum Cryptography

- **Certification according to Common Criteria sub-project:**
  - Need for standardisation arose gradually
  - Had to combine different links
  - Needed a basis for security evaluation

  ➔ **Release SECOQC Node-Link Interface as de-facto standard**

  ➔ **Develop and promote detailed plan for standardisation activity**

Prof. S. Ghernaouti-Hélie



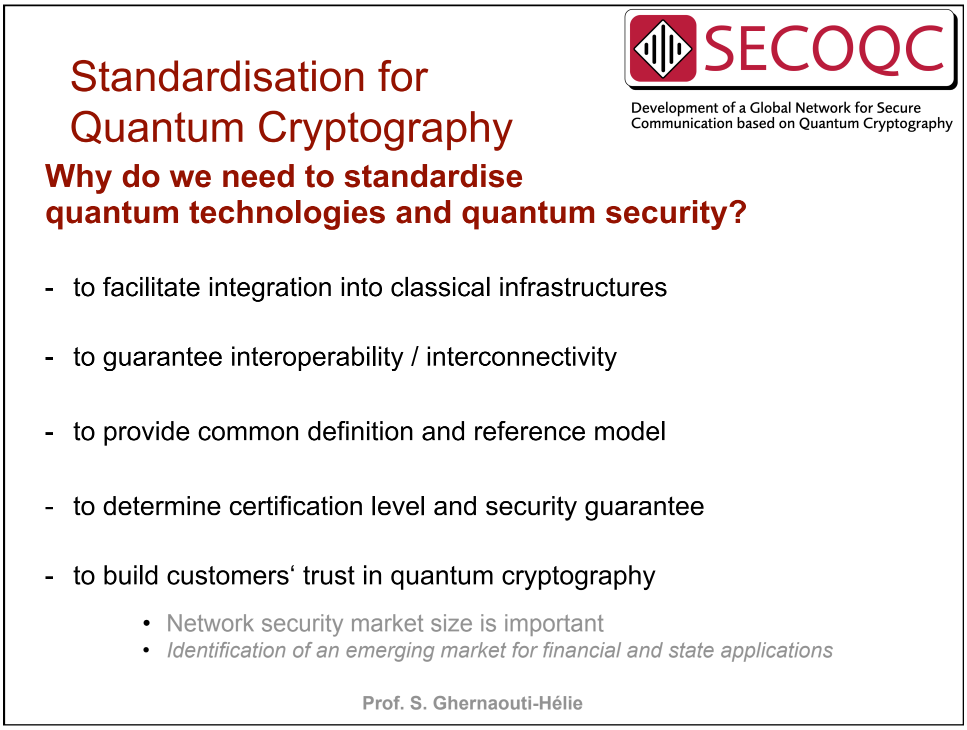
SECOQC

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

Certification & Standardization issues

- SECOQC was engaged in the **Common Criteria certification** process according to the international standard ISO/IEC 15408.
  - This well recognized international standards for Information technology and Security techniques allow the evaluation of IT security level of products.
- CC Certification was not really a choice !
  - *It is the only possibility to convince and prove that the technology developed is secure!*
- This step had facilitated the understanding of the need to start QKD international standardization as an European initiative
- Being concerned about **the easy adoption** of the QKD network, SECOQC consortium has already undertaken the preparatory **phase of standardization**.

Prof. S. Ghernaouti-Hélie



SECOQC

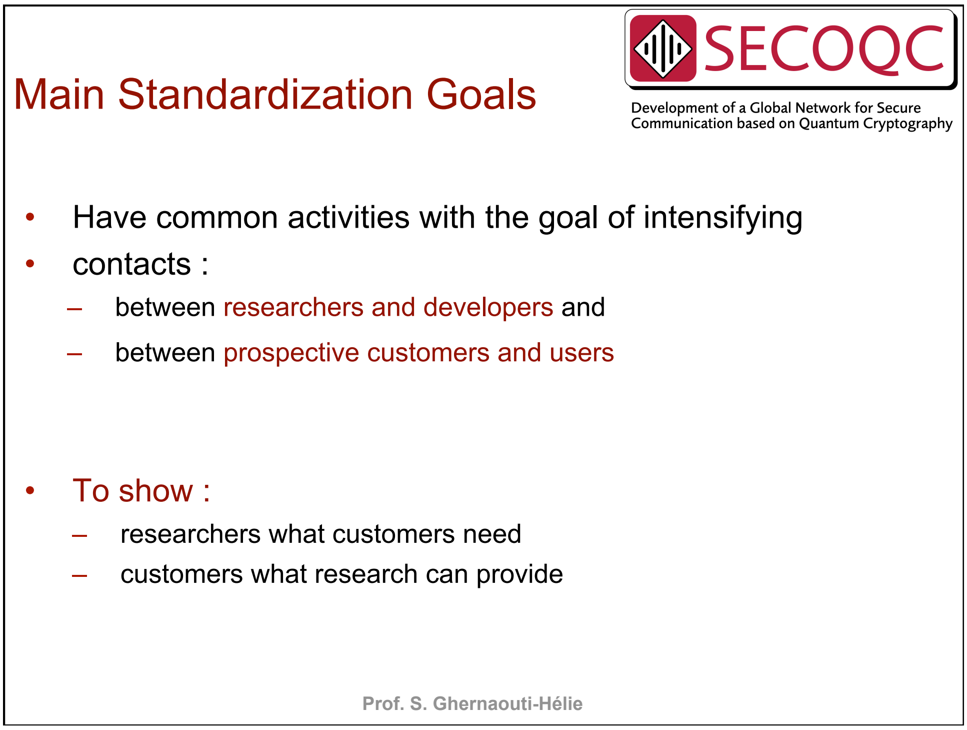
Development of a Global Network for Secure Communication based on Quantum Cryptography

Standardisation for Quantum Cryptography

Why do we need to standardise quantum technologies and quantum security?

- to facilitate integration into classical infrastructures
- to guarantee interoperability / interconnectivity
- to provide common definition and reference model
- to determine certification level and security guarantee
- to build customers‘ trust in quantum cryptography
  - Network security market size is important
  - *Identification of an emerging market for financial and state applications*

Prof. S. Ghernaouti-Hélie



Main Standardization Goals

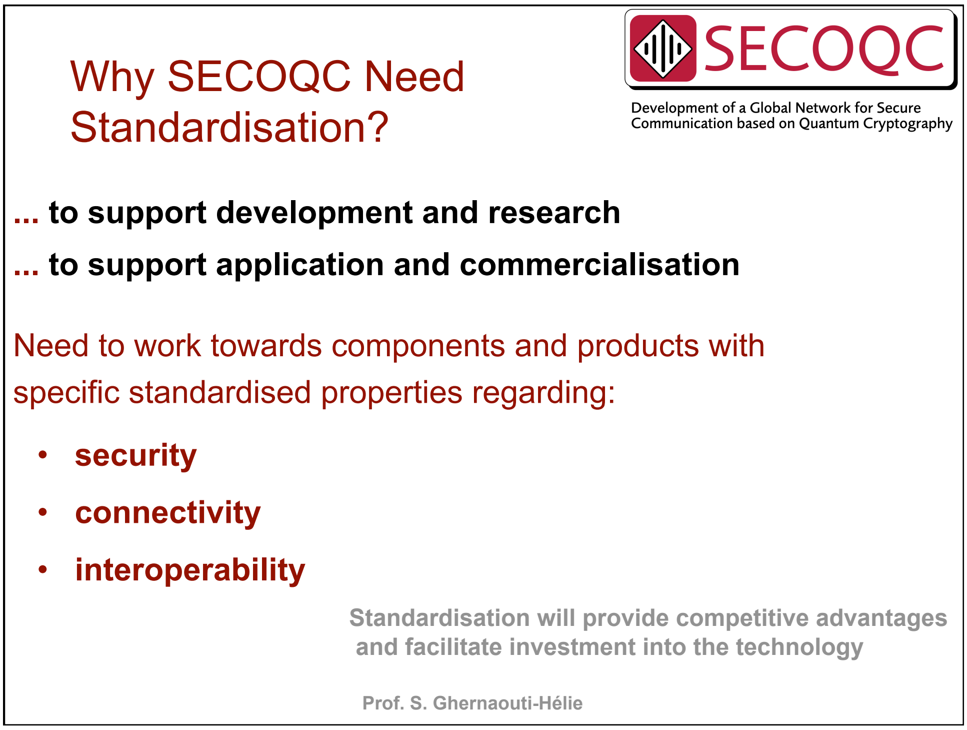
SECOQC

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

- Have common activities with the goal of intensifying
- contacts :
  - between researchers and developers and
  - between prospective customers and users

- To show :
  - researchers what customers need
  - customers what research can provide

Prof. S. Ghernaouti-Hélie



Why SECOQC Need Standardisation?

SECOQC

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

... to support development and research

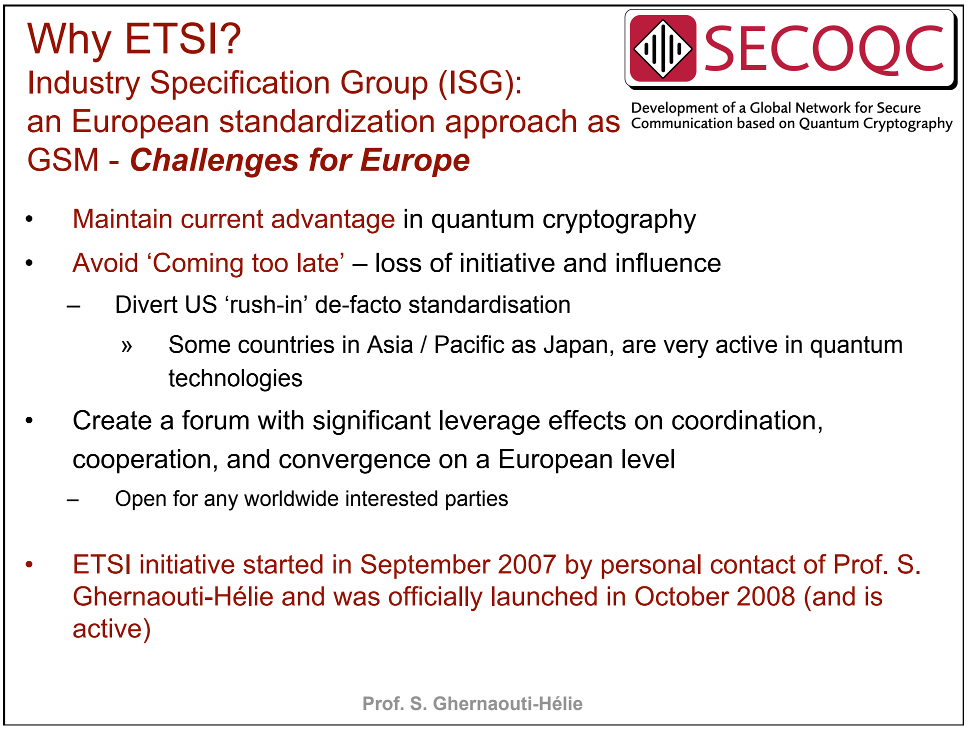
... to support application and commercialisation

Need to work towards components and products with specific standardised properties regarding:

- **security**
- **connectivity**
- **interoperability**

Standardisation will provide competitive advantages and facilitate investment into the technology

Prof. S. Ghernaouti-Hélie



Why ETSI?

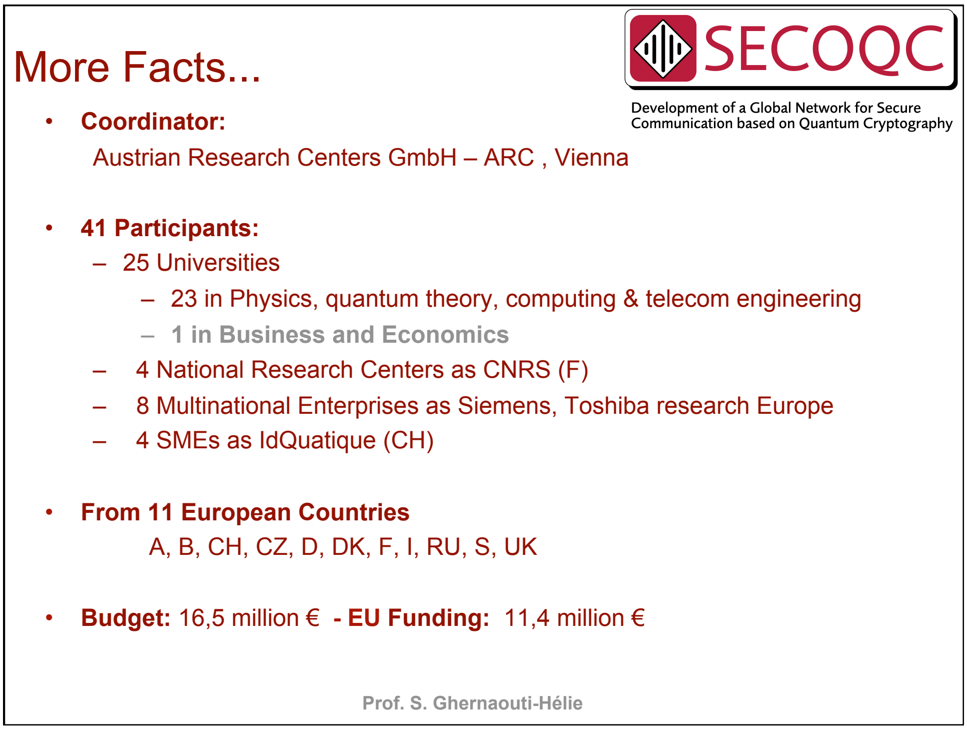
Industry Specification Group (ISG): an European standardization approach as GSM - ***Challenges for Europe***

SECOQC

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

- Maintain current advantage in quantum cryptography
- Avoid ‘Coming too late’ – loss of initiative and influence
  - Divert US ‘rush-in’ de-facto standardisation
    - Some countries in Asia / Pacific as Japan, are very active in quantum technologies
- Create a forum with significant leverage effects on coordination, cooperation, and convergence on a European level
  - Open for any worldwide interested parties
- ETSI initiative started in September 2007 by personal contact of Prof. S. Ghernaouti-Hélie and was officially launched in October 2008 (and is active)

Prof. S. Ghernaouti-Hélie



More Facts...

SECOQC

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

- **Coordinator:**

  Austrian Research Centers GmbH – ARC , Vienna

- **41 Participants:**
  - 25 Universities
    - 23 in Physics, quantum theory, computing & telecom engineering
    - **1 in Business and Economics**
  - 4 National Research Centers as CNRS (F)
  - 8 Multinational Enterprises as Siemens, Toshiba research Europe
  - 4 SMEs as IdQuatique (CH)

- **From 11 European Countries**

  A, B, CH, CZ, D, DK, F, I, RU, S, UK

- **Budget:** 16,5 million € - **EU Funding:** 11,4 million €

Prof. S. Ghernaouti-Hélie

Project Structure:

SECOQC

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

- **Quantum Part**
  - – Quantum Optical Components (COM)
  - – Experimental Quantum Key Distribution (QKD)
  - – Quantum Information Theory (QIT)
- **Infrastructure Part**
  - – Security and Cryptography (SEC)
  - – Network Architecture (NET)
  - – System Integration and Requirements Analysis (SYS)
  - – **Certification According to Common Criteria (CCC) - UNIL**
- **Implementation Part**
  - – Quantum Back-Bone (QBB)
  - – Quantum Access Network (QAN)
  - – Network Implementation (NI)

A huge team !

A lot of men in physics, optics, electronics, …

Only one woman! in security and legal & socio economics fields

Prof. S. Ghernaouti-Hélie

Some considerations

SECOQC

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

- The demo / conference was a success
- The project was a great and sometime difficult adventure
- **Thinking in terms of Quantum cryptography solutions to answer effective security needs is**
  - ***very different of thinking of issues related to photons transmission …***

– There is a gap between fundamentals research needs and society needs

- There is always a need for socio and economics partners in technological projects
  - – *There are effective roles to play in such scientific projects*
    - » *The key factor of success of such collaborative efforts is to know very well the context (technologies and economics and social needs)*

Prof. S. Ghernaouti-Hélie

SECOQC

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

Thank you for your attention

Solange Ghernaouti-Hélie

Secoqc Key researcher

www.secoqc.net

SEDGE
SECURITY IN DIGITAL ENVIRONMENTS

Prof. S. Ghernaouti-Hélie