Quantum and quantum safe crypto technologies in Europe

Ales Fiala
Future and Emerging Technologies
European Commission
Outline

Future and Emerging Technologies (FET) basics
Quantum Technologies in Europe
Highlights on Quantum Cryptography in Europe
The role of the Secocq project
Recent developments at European level and challenges ahead
FET mission

- To turn Europe's excellent science base into a competitive advantage by uncovering radically new technological possibilities
- To turn Europe into the best place for collaborative research and innovation in future and emerging technologies
FET – 3 complementary approaches

Open, light and agile  Roadmap based research

Individual research projects
- Early Ideas
  - FET Open
  - Exploring novel ideas

Research clusters
- Incubation
  - FET Proactive
  - Developing topics & communities

Common research agendas
- Large-Scale Partnering Initiatives
  - FET Flagships
  - Addressing grand challenges
EU investments pioneered in FET...

- ~20 years of European investment in quantum sensing & metrology, communication, computing
- World-class scientific and technical expertise
- Nobel prize laureates

- Steady increase of funding: ~350 M€ until now
  - FET ~250 M€, ERC ~100 M€, MSCA ~100 M€, EMRP (European Metrology Research Programme) & EMPIR (European Metrology Programme for I&R) in the area of metrology

- National initiatives recently launched
  - NL QuTech 135 M€, UK Quantum Hubs 270 M£
~50 projects funded (~97 M€, 2007-2013)

FET-Open: ~60 M€, 36 research projects

- Sensing
  - 8 projects
  - ~13 M€

- Computing & simulation
  - 20 projects
  - ~33 M€

- Communication
  - 8 projects
  - ~14 M€

FET Proactive: ~37 M€, 9 research projects

- Sensing
  - 2 projects
  - ~7 M€

- Communication
  - 1 project
  - ~5 M€

- Computing & simulation
  - 6 projects
  - ~25 M€

2 thematic calls: - Quantum Information Foundations & Technologies
                 - Quantum ICT
Recent QT funding in FET

**Work Programme 2014-2015**

**FET Open:**
5 projects funded in the first 2 calls (metrology, sensing), ~17 M€ (15% of FET Open budget)

**FET Proactive:**
5 projects funded on Quantum Simulation, ~14 M€

**Work Programme 2016-2017**

**FET-Open:** 240 M€ budget
3 call deadlines; competition from other disciplines

**FET Proactive** on Quantum Engineering: max 30 M€ for the area
Quantum Engineering is 1 out of 3 thematic calls in the area of Disruptive information technologies, paving the way for industry take-up.

**ERA-Net Cofund:** 10 M€ budget
To coordinate national and regional programmes for research in the area of quantum technologies by implementing a call jointly funded by the participating states with EU co-funding.
Examples of QT research topics

- Atomic, molecular and solid-state systems for quantum processing
- Interfaces between quantum communication, computation and storage
- Sources and detectors for single photons, atoms, ions
- Quantum algorithms and protocols
- Decoherence, quantum noise and thermodynamics
- Quantum repeaters
- Miniaturization and chip components

Many of these topics are relevant across the application spectrum of Quantum Technologies
Coordination and support actions

Actions targeted to:
• support the targeted research communities,
• assess the impact of research,
• increase the visibility and communicate key results to target audiences,
• consolidate research agendas.

2006-2009
Quantum Information Processing and Communication in Europe

2010-2013
Quantum Information Entanglement-Enabled Technologies

2013-2016
Quantum Technologies for Europe

2012-2015
Optimal Control Technologies in Quantum Information Processing
Funding in QT

550M€

¹Estimated
Quantum cryptography

• **Application**
  - Secure communication (QKD)
    - Security, health, finance, government, critical infrastructures

• **Maturity**
  - Expanding from niche commercial product (< 5 years) to possibly general/consumer use within 10 years.
  - QKD pilot infrastructure deployment and long-term operation.

• **Industrial base in Europe**
  - Id Quantique, Toshiba, HP, Thales, Siemens, Nokia, Alcatel-Lucent, Huawei, KPN & others
2000:
Researchers in Austria and Switzerland* demonstrate first implementation of Quantum Key Distribution using variants of a protocol developed in the early 1990s in Oxford by Polish physicist Artur Ekert.

* With support from European and national funding bodies

2002:
Researchers in Germany and British SME collaborate in European project EQCSPOT to demonstrate QKD over a 23.4 km free-space link.

2004:
Researchers in France and Belgium with support from FET projects 'QUICOV' and 'EQUIP' collaborate to demonstrate the first continuous variable implementation of QKD.
Recent developments in Europe

2009-2011: Researchers in Switzerland* report on the performance of the SwissQuantum quantum key distribution (QKD) network over more than one and a half years with the purpose of testing the reliability of the quantum layer over time in production environment.

*mainly funded by Swiss funding bodies, support from European projects 'QuReP' and 'Q-Essence' (FET) are acknowledged.

2010: First QKD demonstration with conventional components in Spain

2013: Longest single fibre link of 309 km shown in Switzerland

2014: Highest secure key rate of 2.38 Mb/s over 35km fibre demonstrated in the United Kingdom

2015: First QKD demonstration on live network in the United Kingdom
The Secoqc project

Secure Communication based on Quantum Cryptography

A few facts:

- Funded by the European Commission
- Running from 2004 to 2008
- ~16.8 M€ budget
- 48 participants from 11 countries
- 9 participants from industry/SME
Main SECOQC technological achievements

- Established first QKD network worldwide
- Increased to 144 km free-space QKD demonstration on Canary Islands*
- Developed the Coherent-One-Way QKD protocol

* With support from European Space Agency and national funding bodies
Discussions on standardization of quantum crypto initiated within SECOQC.

Standardisation process passed over to European Telecomunications Standards Institute (ETSI) in 2008 establishing an Industry Specification Group (ISG) on Quantum Key Distribution.

Secoqc originator of QKD standardisation

ETSI sets new standards for trust in communication security

ETSI Headquarters, Sophia Antipolis, France - 28 July 2008

It sounds like science fiction, but quantum cryptography will bring new levels of confidentiality and privacy of communication in the future ICT world and thus become the driver for the success of numerous services in the fields of e-government, e-commerce, e-health, transmission of biometric data, intelligent transport systems and many others. Due to the astonishing effects of quantum physics, quantum encrypted messages are totally immune from eavesdropping.
ETSI launched ISG QSF (Quantum Safe Cryptography)

Focus on
• Quantum safe algorithmic framework
• Cryptographic primitive characterization
• Cryptographic primitive suitability assessment
• Quantum safe threat assessment
• Quantum safe standards assessment
EU Challenges

Turning scientific excellence into industrial success...

• Maintain attractive research opportunities in Europe and expand programmes from research to engineering
• Engage with industry, funders & investors and stimulate their involvement
• Develop a common EU roadmap going beyond research
• Manage risks expected at different levels, from technology and supply chain to market and skills
• Develop plans for future large scale initiatives
Thank you for your attention

About FET: http://ec.europa.eu/digital-agenda/FET

Contact FET: CNECT-FET@ec.europa.eu

Twitter: @FET_EU