Quantum Computing And Cryptography: a Telco‘s Perspective

Erwan Bigan, Swisscom CH
ITU Telecom World 2009
Oct. 8, 2009

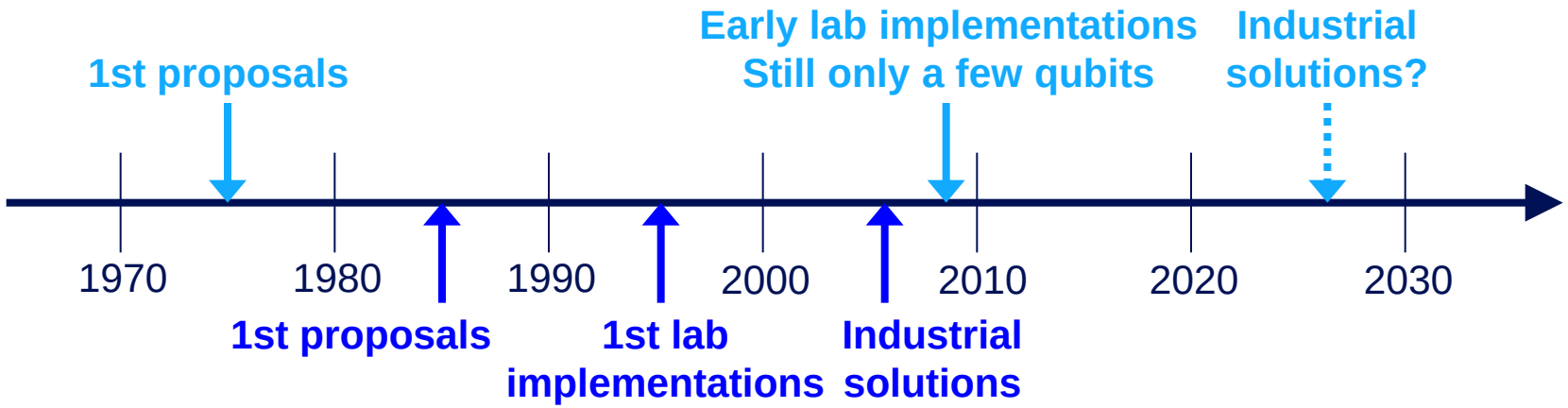
Outline

- Quantum computing and cryptography: a time-to-market perspective
- Quantum cryptography performance
- Quantum cryptography need
- How to make it grow beyond a niche?

Quantum computing and cryptography: a time-to-market perspective

Quantum computing

- Promise: massively accelerated computing
- Potential application: factorization of large numbers into primes, fast brute force search



Quantum cryptography (aka QKD)

- Promise: absolute protection against eavesdropping
- Application: highly secure key distribution

swisscom

Quantum cryptography performance

From pioneering concepts to ever better implementations: should not be a roadblock for the future

- **Higher bit rate and/or distance (for key distribution or encrypted data)**
  - *„High rate, long-distance quantum key distribution over 250km of ultra low loss fibres“, D. Stucki et al, New Journal of Physics, July 2009*

- **Point-to-point vs. Point-to-multipoint**
  - *„Multiuser quantum key distribution over telecom fiber networks“, J. Bogdanski et al, Optics Communications, January 2009*

- **Compatibility with optical fiber networking technologies (e.g. WDM)**
  - *„Quantum key distribution integrated into commercial WDM systems“, H. Rohde et al, OFC 2008*

swisscom

Quantum cryptography need

Not yet fully acknowledged

- **Value proposition: „Absolute protection against eavesdropping“**
  - Contributed to an emerging industrial ecosystem
  - Captured some mind share

    „Quantum cryptography represents the next line of IT security“, www.accenture.com/xdoc/en/services/technology/vision/quantum_cryptography.pdf

- **Scepticism in the security community**
  - Cryptography/key exchange is not the weakest link

    „still unbelievably cool, in theory, and nearly useless in real life“, www.schneier.com,
  - Would a Common Criteria system security evaluation lead to better results with QKD?

Risk that quantum cryptography will remain a niche market.

…unless a step security advantage is identified

swisscom

How to make it grow beyond a niche?

- **De-antagonize quantum optics and security/cryptography communities**
  - 1st such initiative in the context of ETSI standardization
- **Further investigate the potential of quantum cryptography from an E2E system security prospective**
  - True Random Number Generator: already proposed by IDquantique
  - Make formerly impractical crypto-algorithms or protocols possible (e.g. one-time pad)
  - …

  Already underway

  - Protect against traffic pattern analysis (e.g. encrypted VoIP content analysis without breaking the cryptography)?
  - Long-term protection of encrypted data?
  - …

  May need more than QKD?
- **Explore new concepts beyond the original pioneering work from the 80‘s and 90‘s**
  - Today, quantum cryptography = quantum key distribution
  - Tomorrow?