QKD, Security and the Competitive Advantage

11/11/20

Catherine White, Researcher, BT PLC

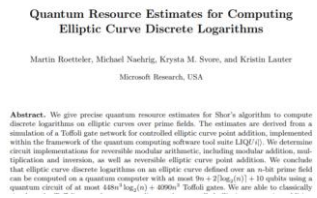
EPIC Online Technology Meeting on Quantum Communication & Quantum Key Distribution

Network Security Threats

Implementation flaws affecting RSA and Diffie Hellman

Example, 2017 ROCA attack based on prime number generation in Infineon chipset

Quantum Computing


Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms

Martin Roetteler, Michael Naehrig, Krysta M. Svore, and Kristin Lauter

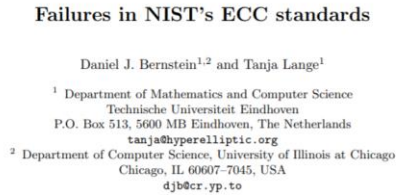
Microsoft Research, USA


ScienceNews

Rumors hint that Google has accomplished quantum supremacy

https://eprint.iacr.org/2017/598.pdf

Possible weaknesses and backdoors


Failures in NIST's ECC standards

Daniel J. Bernstein[1,2] and Tanja Lange[1]

[1] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
tanja@hyperelliptic.org

[2] Department of Computer Science, University of Illinois at Chicago
Chicago, IL 60607–7045, USA
djb@cr.yp.to

*https://cr.yp.to/newelliptic/**nistecc**-20160106.pdf*

Unknown vulnerabilities in new key exchange algorithms that emerge post-2022/3 from NIST PQC program?

Quantum Comms and QKD advantages

Immune to all foreseen and unforeseen advances in computational methods
(Information Theoretically Secure)

Potential for **detection of tapping** (even on the data channel if using Quantum Direct Communications, Quantum Alarm)

Network approach a good fit for integration with **hardware network encryptors**

Can be **combined** with other methods of key exchange, and other quantum safe cryptographic functions, e.g for encryption and authentication.

True non-deterministic randomness (QRNGs)

Possibility for **Device Independence**

Replaces Courier

QKD Milestones to Readiness

Standards and Assurance
ISO Standards

ETSI ISG Standards

ITU Standards

Assurance: Common Criteria Framework
Protection Profile Underway

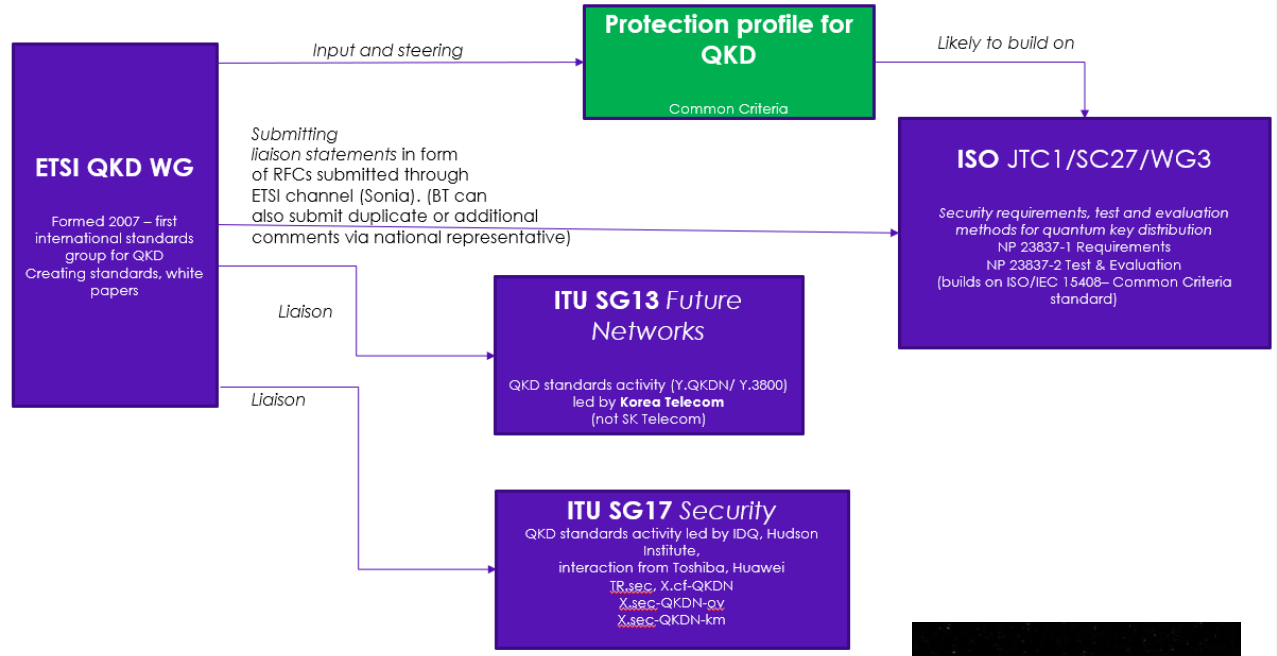
Global Programs, e.g.:

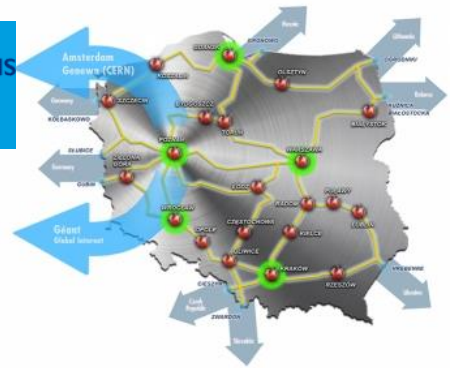
UK Quantum Network and Quantum Comms Hub

OpenQKD – EU Quantum Network

CA, CN, JP, RU, SK, US…

Standards and assurance landscape





OPEN QKD

Continued Evolution of Quantum Comms

e.g. …
MDI-QKD
Device independent

Untrusted Nodes

Enabling components and technologies…
Photonic Integrated Circuits
Improved single photon detectors (low noise, high speed, short deadtime)
Single photon emitters
Photon counting detectors
Entanglement sources
Telecoms wavelengths
Quantum memories
More stable frequency sources

…and of course Cheaper, Better, Faster, **Smaller, Lower Power**