EU Activities in Post-Quantum Cryptography

Tanja Lange

Academia Sinica

Eindhoven University of Technology

Post-quantum cryptography forum
14 January 2022

History of post-quantum cryptography

- 2003 Daniel J. Bernstein introduces term Post-quantum cryptography.
- PQCrypto 2006: International Workshop on Post-Quantum Cryptography. Held at KU Leuven, Belgium, organized by EU project ECRYPT.
- PQCrypto 2008 (US), PQCrypto 2010 (DE), PQCrypto 2011 (TW), PQCrypto 2013 (FR).
- 2014 EU publishes H2020 call including post-quantum crypto as topic. PQCRYPTO EU project is funded.

- September 2015: Initial recommendations by PQCRYPTO.
- 2015 ETSI working group "Quantum-Safe Cryptography (QSC)"
- 2016: NIST announces competition for post-quantum systems.
- November 2017: Submissions for NIST competition due. PQCRYPTO submits 22 designs (out of a total of 69).

Also in the EU: Quantum Technologies Flagship

From press release at launch, in 2018:

> *The Flagship will initially fund 20 projects with a total of 132 million via the Horizon 2020 programme, and from 2021 onwards it is expected to fund a further 130 projects. Its total budget is expected to reach 1 billion, providing funding for the entire quantum value chain in Europe, from basic research to industrialisation, and bringing together researchers and the quantum technologies industry.*

Also in the EU: Quantum Technologies Flagship

From press release at launch, in 2018:

> *The Flagship will initially fund 20 projects with a total of 132 million via the Horizon 2020 programme, and from 2021 onwards it is expected to fund a further 130 projects. Its total budget is expected to reach 1 billion, providing funding for the entire quantum value chain in Europe, from basic research to industrialisation, and bringing together researchers and the quantum technologies industry.*

. . . but post-quantum cryptography is not welcome.
Funding is restricted to using quantum technology
(as opposed to being necessary due to advances in quantum technology).

One frequently brought up argument to fund the flagship is that China is funding quantum.

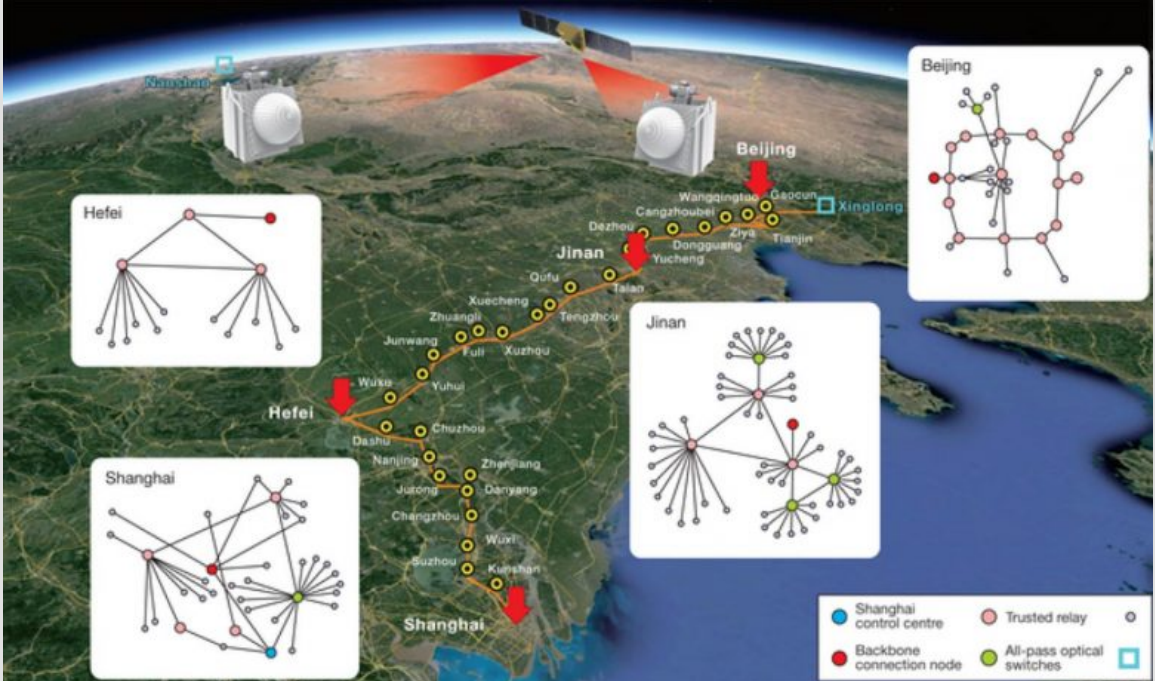
Also in the EU: Quantum Technologies Flagship

From press release at launch, in 2018:

> *The Flagship will initially fund 20 projects with a total of 132 million via the Horizon 2020 programme, and from 2021 onwards it is expected to fund a further 130 projects. Its total budget is expected to reach 1 billion, providing funding for the entire quantum value chain in Europe, from basic research to industrialisation, and bringing together researchers and the quantum technologies industry.*

. . . but post-quantum cryptography is not welcome.
Funding is restricted to using quantum technology
(as opposed to being necessary due to advances in quantum technology).

One frequently brought up argument to fund the flagship is that China is funding quantum. . . . hope they don't imitate everything that China does . . .


Beijing
Xinglong
Gaocun
Wangqingtuo
Cangzhoubei
Dezhou
Ziya
Tianjin
Dongguang
Yucheng
Jinan
Qufu
Talan
Xuecheng
Zhuangli
Tengzhou
Junwang
Fuli
Xuzhou
Wuxie
Yuhui
Hefei
Chuzhou
Dashu
Nanjing
Zhenjiang
Jurong
Danyang
Changzhou
Wuxi
Suzhou
Kunshan
Shanghai
Hefei
Shanghai
Jinan
Beijing
Shanghai control centre
Trusted relay
Backbone connection node
All-pass optical switches

Why QKD is not the solution

to any security problem I am aware of

Why QKD is not the solution

to any security problem I am aware of

This list applies to physical security in general
(locked briefcases, quantum key distribution, etc.)

- Horrendously expensive.

Why QKD is not the solution

to any security problem I am aware of

This list applies to physical security in general
(locked briefcases, quantum key distribution, etc.)

- Horrendously expensive.
- "Provably secure"—under highly questionable assumptions.
- Broken again and again. Much worse track record than normal crypto.
- Easy to screw up. Easy to backdoor. Hard to audit.

Why QKD is not the solution

to any security problem I am aware of

This list applies to physical security in general
(locked briefcases, quantum key distribution, etc.)

- Horrendously expensive.
- "Provably secure"—under highly questionable assumptions.
- Broken again and again. Much worse track record than normal crypto.
- Easy to screw up. Easy to backdoor. Hard to audit.
- Current QKD (using trusted repeaters) has backdoors built in:
  Every node decrypts and re-encrypts.

Why QKD is not the solution

to any security problem I am aware of

This list applies to physical security in general
(locked briefcases, quantum key distribution, etc.)

- Horrendously expensive.
- "Provably secure"—under highly questionable assumptions.
- Broken again and again. Much worse track record than normal crypto.
- Easy to screw up. Easy to backdoor. Hard to audit.
- Current QKD (using trusted repeaters) has backdoors built in:
  Every node decrypts and re-encrypts. Great system for China ...

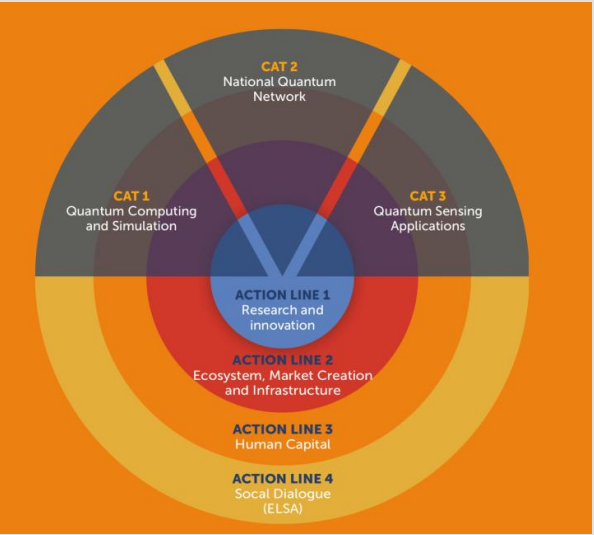
Why QKD is not the solution

to any security problem I am aware of

This list applies to physical security in general
(locked briefcases, quantum key distribution, etc.)

- Horrendously expensive.
- "Provably secure"—under highly questionable assumptions.
- Broken again and again. Much worse track record than normal crypto.
- Easy to screw up. Easy to backdoor. Hard to audit.
- Current QKD (using trusted repeaters) has backdoors built in:
  Every node decrypts and re-encrypts. Great system for China ...
- Very limited functionality: e.g., no public-key signatures.

Somewhat better: Quantum Delta NL



Action line 1: Realization of research and innovation breakthroughs in six fields:

- Quantum computing
- Quantum sensing
- Quantum simulation
- Quantum algorithms
- Quantum communication
- Post-quantum cryptography

Action line 2: Ecosystem development, market creation and infrastructure

Action line 3: Human capital: education, knowledge and skills

Action line 4: Promotion of social dialogue regarding quantum technology

Detailed information: https://quantumdelta.nl/informationsession/

EU efforts involving post-quantum cryptography

H2020 projects:

- PQCRYPTO (2015–2018)
- SAFEcrypto (2015–2019)
- FutureTPM (2018–2021)
- PROMETHEUS

Upcoming call: Transition towards Quantum-Resistant Cryptography (Nov 2022).

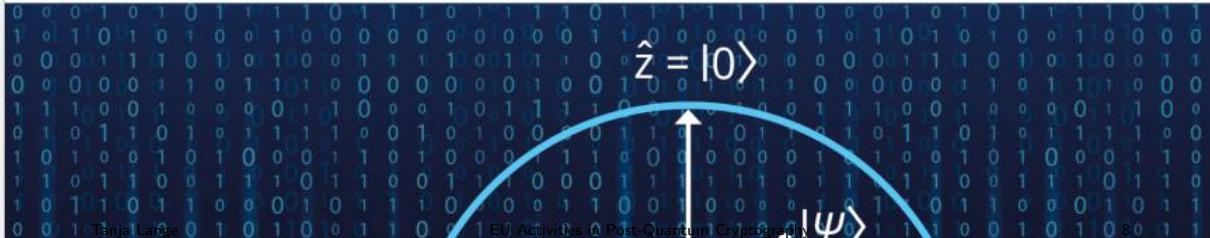
National initiatives:

- Quantum-safe cryptography (NCSC-UK Whitepaper)
- Factsheet Post-quantum cryptography (by NCSC-NL)
- TechDispatch #2/2020: Quantum Computing and Cryptography (by European Data Protection Supervisor)
- Status of quantum computer development (by German BSI)
- ANSSI views on the Post-Quantum Cryptography transition (French agency)

Post-Quantum Cryptography: Current state and quantum mitigation

Ward Beullens, Jan-Pieter D'Anvers, Andreas Hülsing, Tanja Lange, Lorenz Panny, Cyprien de Saint Guilhem, Nigel P. Smart.
Evangelos Rekleitis, Angeliki Aktypi, Athanasios-Vasileios Grammatopoulos.

EUROPEAN UNION AGE
FOR CYBERSECU



ENISA report: Current state and quantum mitigation

Chapters

1. Introduction
2. Families of Post-Quantum Algorithms
3. Security Notions and Generic Transforms
4. NIST Round 3 Finalists
5. Alternate Candidates
6. Quantum Mitigation
   - 6.1 Hybrid schemes
   - 6.2 Protective measures for pre-quantum cryptography

Report available from ENISA's website.

ENISA report: Current state and quantum mitigation

Chapters

1. Introduction
2. Families of Post-Quantum Algorithms
3. Security Notions and Generic Transforms
4. NIST Round 3 Finalists
5. Alternate Candidates
6. Quantum Mitigation
   - 6.1 Hybrid schemes
   - 6.2 Protective measures for pre-quantum cryptography

Report available from ENISA's website.
Upcoming report: ENISA PQC Integration Study.