Japan IGF 2024

Advancing the security of today’s critical infrastructure

7 November 2024

QUDEF

„Securing the Quantum Frontier“

The bigger picture of Quantum Key Distribution (QKD)

Dr. Michal Krelina

CTO, Co-Founder

krelina@qudef.com

QuDef BV, NL

www.qudef.com

contact@qudef.com

QKD and it’s perception

Quantum threat from quantum computer

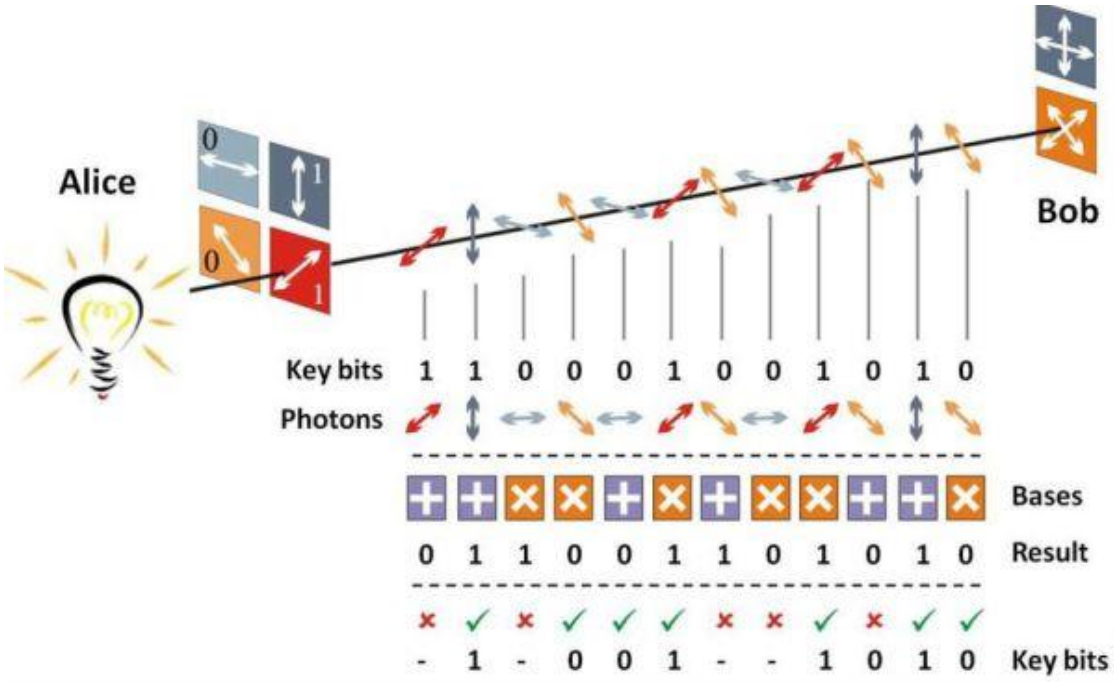
- They will break current asymmetric encryptions
- Weaken symmetric encryption and hashes
- Risk now – **Harvest now, decrypt later**

Solutions:

- Increase key size for symmetric encryption
- Replace asymmetric encryption by
  - Post-quantum cryptography
  - **Quantum key distribution**

QKD is a possible solution to quantum threat

What is QKD?



Quantum Key Distribution

- is a quantum protocol on a quantum network
- allows generate and share cryptographic key between two parties
- uses **quantum mechanics** and **its properties**
  - Usually single photons
  - Quantum superposition and/or quantum entanglement
  - No-cloning theorem
- **information-theoretically secure**
- any eavesdrop attempt **is noticed**
- represents the **future-proof** security
- is **resistant to all known quantum and classical attacks, including future advances**

QKD Deployment

If QKD is so cool, why it is not common? Especially if commercially available?

- **Example:** Personal computers handle multiple secure connections (email, messaging apps, web pages, VPNs). Each connection requires key exchanges with different servers worldwide. This is impossible to manage by QKD
- Moreover, it requires **new infrastructure, new hardware**
  - This means it is quite **expensive**
- Problem with **scalability** and **range**
- QKD is better suited **for high-security**, fixed applications due to current limitations

Quantum Communications – a bigger picture

Quantum networks 1st generation

- Services: (just) QKD
- Is it worth it?

Quantum Communications – a bigger picture

Quantum networks 1st generation

- Services: (just) QKD
- Is it worth it?

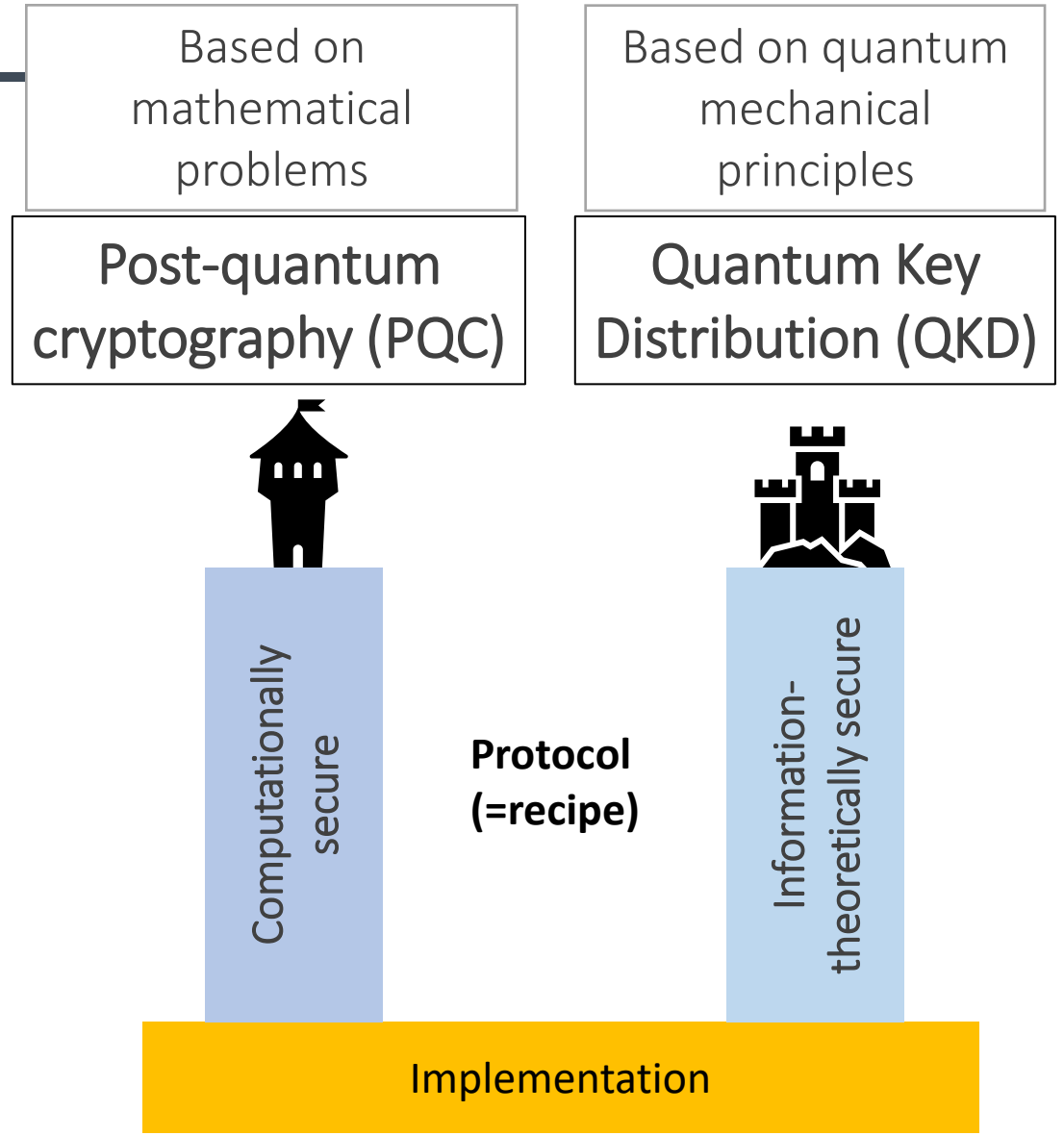
Quantum networks 2nd generation = Quantum Internet

- Just upgrade from 1st generation (we need quantum memory)
- Multiple services
  - **Security**: QKD, shared secret, conference key agreement, quantum direct messaging, secure identification, position verification, quantum digital signatures
  - **Quantum Computing**: distributed quantum computing, blind quantum computing
  - **Technical**: precise time distribution/sync, quantum networked sensing, swarm self-organisation
  - **Other**: quantum money/blockchain, quantum secure voting

Objections to QKD

U.S. NSA's objections:

- Partial Solution
- Special Hardware Required
- Increased Costs and Risks
- Challenging Security Validation
- Denial of Service Risk



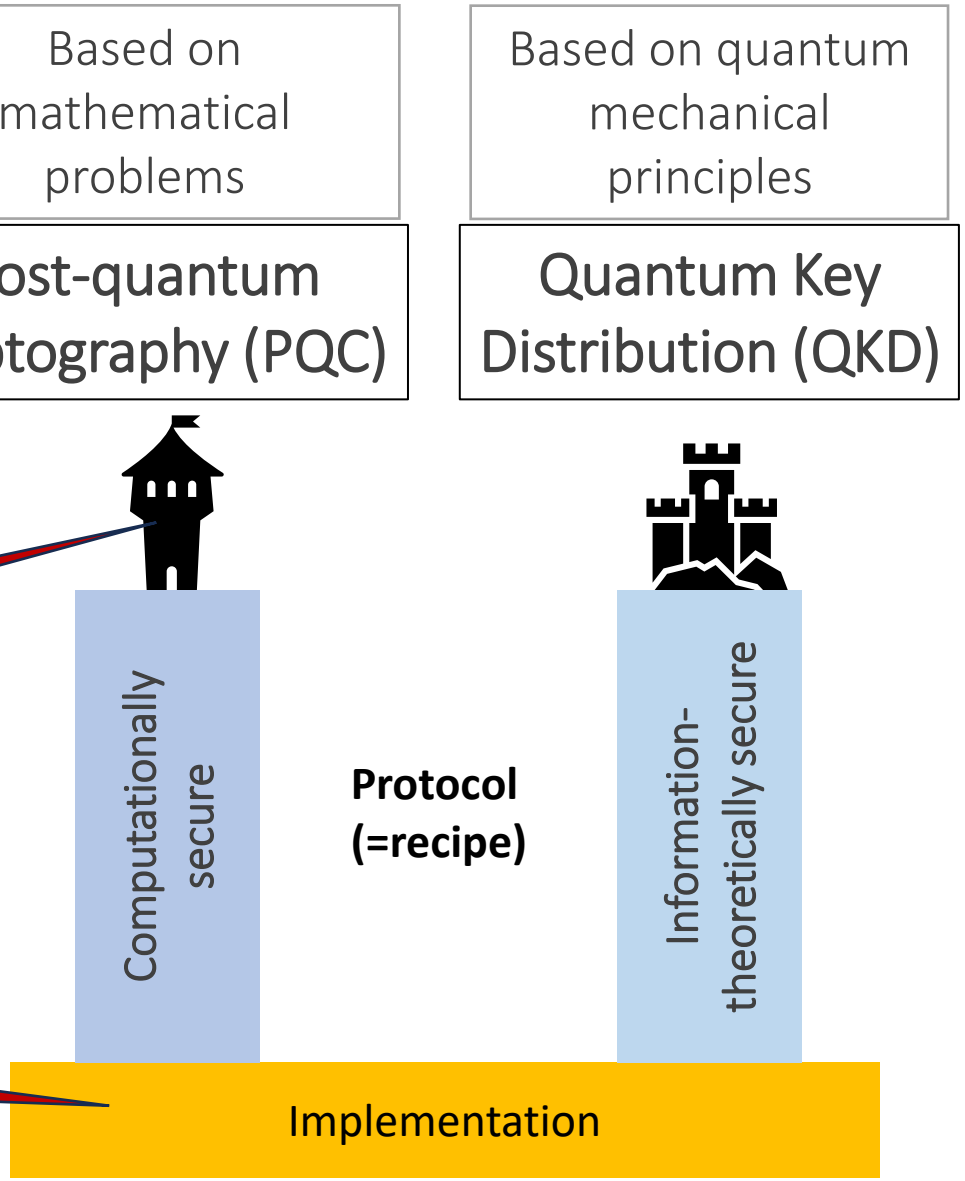
Objections to QKD

US NSA's objections:

- Partial Solution
- Special Hardware Required
- Increased Costs and Risks
- Challenging Security Validation
- Denial of Service Risk

Many PQC candidates were broken. And still can be…

Attacks on PQC and QCD side channels demonstrated



QKD in the World

USA: not a centrally-driven topic

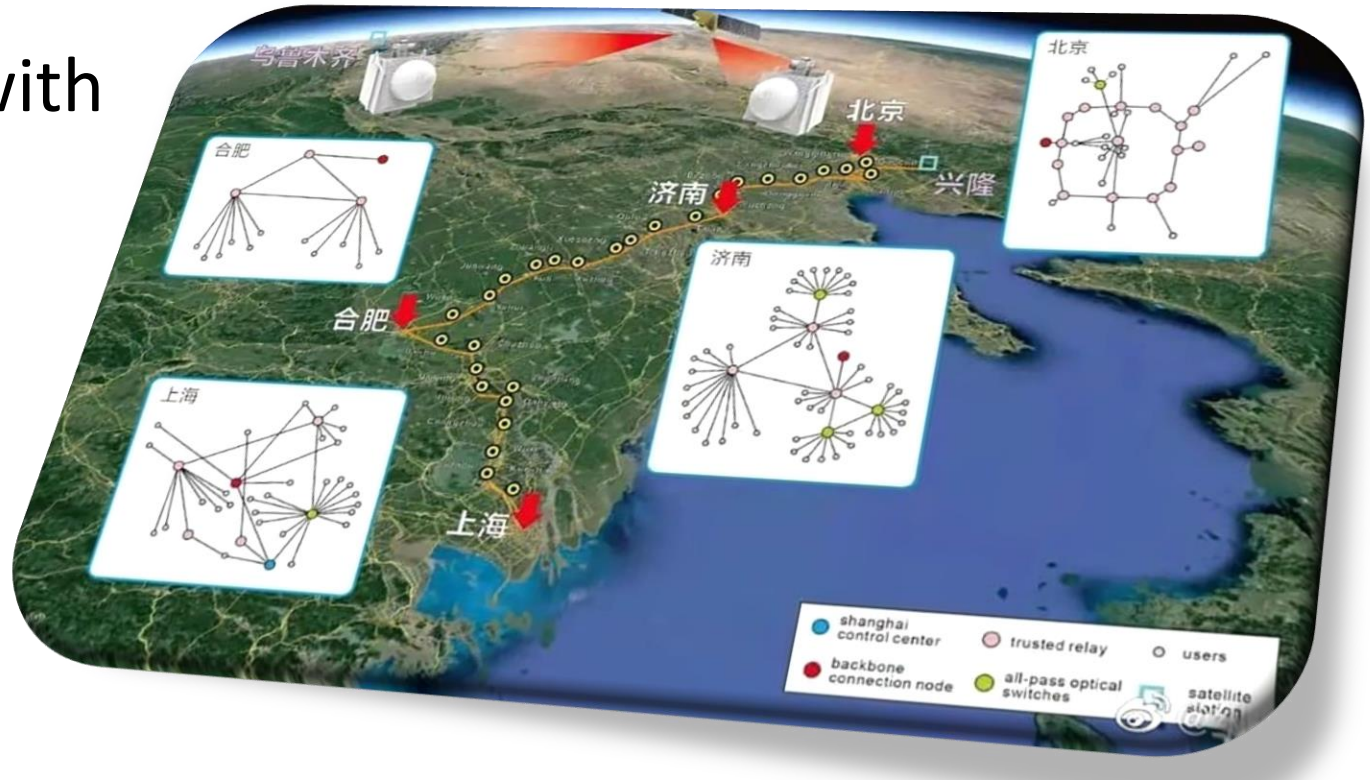
EU: EuroQCI – National quantum networks + their interconnections

QKD in the World

USA: not a centrally-driven topic

EU: EuroQCI – National quantum networks + their interconnections

China: over 2000 km of QKD with already 2nd generation of quantum satellites up!



QKD in the World

USA: not a centrally-driven topic

EU: EuroQCI – National quantum networks + their interconnections

China: over 2000 km of QKD + already 2nd generation of quantum satellites up!

Standards:

- ETSI: 13
- ITU: 31
- ISO: 2
- IRTF: 2
- But not yet standard of QKD protocols

QUDEF

Thank you for your attention!

QuDef BV, NL

www.qudef.com

contact@qudef.com

Who is QuDef

We are a fresh quantum startup based in House of Quantum in Delft, NL focusing on the security of quantum technologies.

Our focus:

- Develop Quantum Technology Threat Intelligence Platform
- Quantum Technology Security Assessment and Evaluation
- Quantum GRC (Governance, Risk, Compliance) Service Providing
- Quantum Technology Expert Consultation, Training, Intelligence
  - Especially on military applications