Quantum(-Safe) Networks at TNO

Quantum(-Safe) Networks at TNO

TNO innovation for life

TNO's portfolio in Quantum Information Networks, Quantum Key Distribution and Post-Quantum Cryptography

November 2024

As TNO we regularly engage with industry and society on technologies like Quantum Information Networks, Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC). But we notice that it isn't always clear with our partners how these interrelate. This paper describes the current state of affairs around these technologies and their relation, and can be used as a reference for engaging with these technologies, with or without TNO.

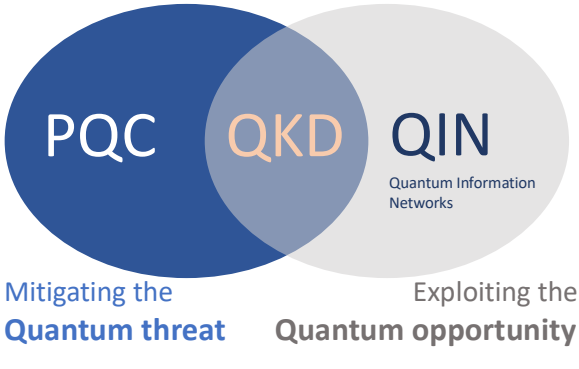
Summary

Quantum technologies provide both a potential threat and an opportunity to users and providers in the ICT industry, including government. The threat is that quantum computers may break conventional cryptography. Opportunities are new services and applications that are enabled by quantum technologies, including solutions to mitigate the aforementioned threat.

We provide an overview of TNO's activities in this area with a focus on networked technologies, specifically Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and Quantum Information Networks (QINs). As TNO, we invest in each of these. The main purpose of these investments is to achieve hands-on understanding of these technologies, the technology choices, the problems they address, their maturity, the standards and the opportunities and risks. This helps us to provide balanced advice and to support our current and future customers in harnessing the potential of quantum (network) technologies, while mitigating the risks they introduce.

1. Quantum: opportunity and threat

The Venn diagram illustrates the quantum threat, quantum opportunities and their overlap. PQC does not require quantum technology, but still protects users against attackers with quantum capabilities. QKD provides a specific cryptographic functionality, harnessing quantum mechanical effects to ensure security against those attackers. QKD has the potential, in specific scenarios, to enhance the security offered by PQC. Alternatively, QKD variants that use entanglement and/or quantum correlation can be seen as a first step towards the "Quantum Internet": in its ultimate form a network of Quantum Information Networks in which entanglement is distributed between end-nodes.



2. The need to provide "Quantum nuance"

QKD and PQC are both technologies promoted to mitigate the quantum threat. As an independent research organisation, we strive to objectively inform others about both technologies. For instance, by providing an overview of the advantages and disadvantages of each technology.
To serve the need of our stakeholders, we elaborate on the nuances of the quantum threat, and the arguments about maturity and security of PQC and QKD, as well as economic considerations. We understand why certain parties may be enthusiastic about the quantum opportunities for networking, and others sceptical. Depending on a customer's (knowledge) need, we provide balanced advice and support with technical reports, technology development and proofs-of-concept and collaborative projects.

3. TNO investments: hands-on knowledge

At TNO we conduct a wide range of activities on PQC, QKD and quantum information networks, e.g. we:

- Create awareness about the quantum threat in society, for instance by organising national PQC symposia since 2021;
- Publish advice and guidelines on how to mitigate the quantum threat;
- Analyse the security of standardised PQC solutions and develop tools to speed-up their deployment;
- Study the security and performance of PQC implementations in various application domains;
- Develop technology and proofs-of-concepts for QKD and advanced quantum-internet technologies, including entanglement distribution, quantum repeaters, terrestrial and space-based systems;
- Develop new methods to analyse the supply chains for these strategic technologies; We develop standards for interoperable, harmonized quantum internet supply chains; and translate insights into societal terms, like envisioned quantum-internet products, services and applications;
- Integrate commercially available quantum hard- and software components into fully functional quantum communication links;
- Simulate the performance of different algorithms and network protocols to quantify the result and impact of using quantum approaches, without having to implement these approaches in practice;
- Design quantum network architectures based on use cases via a system engineering approach;
- Study applications (Quantum Application Lab), network protocols and hardware implications for integration and interworking of quantum technology with existing classical networks and cloud ecosystems.

To do all of the above, we bring together experts in various disciplines such as mathematics, physics, cryptography, strategic business analysis, ICT, system engineering, space systems, optics, project management and business development.

4. TNO partners: progress through collaboration

Whereas we possess extensive multidisciplinary knowledge ourselves, much of our strength lies within our partner networks.

We are fostering a growing national PQC community with stakeholders from academia (e.g., CWI), cryptographic solution providers (e.g., Fox-IT, NXP) and end-users (e.g., banks, government). Moreover, we closely collaborate with the Dutch government to advice on PQC migration policy.

In collaboration with TU Delft, through the QuTech partnership, we work towards prototyping and demonstrating novel quantum technologies, while more mature technologies are advanced through spin-offs and start-ups. We play leading roles in the Quantum Delta Netherlands ecosystem, leveraging Dutch National Growth Fund investments to establish, develop, and accelerate a Dutch quantum technology industry. TKI-funded projects enable us to address quantum-related topics of concern to a broad range of stakeholders.

We also regularly lead and participate in European collaborative projects, both on PQC, QKD and quantum information networks. Together with partners from the space industry, we are working towards a global quantum internet enabled from space. We support the industry with early analysis and modelling of quantum communication links, and we design, build, and test new enabling technologies for quantum communication via ground and space, including the interface between them.

Acknowledgements

Authors: Oskar van Deventer, Bob Dirks, Rob Smets, Niels Neumann, Teun van der Veen, Frederik Kerling, Juan Boschero, Thomas Attema, Chris Klompenhouwer.
Reviewers: Maaike van Leuken, Mark Buningh, Theo Lodewijkx, Dimitri Hehanussa

Publicatienummer: TNO 2024 P12148

Contact
Teun van der Veen
Oskar van Deventer

teun.vanderveen@tno.nl
+31 (0)88-8667332
linkedin.com/tno

Enabling a global quantum internet via space

Cyber security through quantum-safe crypto