Understanding the Quantum Technology Landscape

This presentation explores the capabilities and limitations of quantum computing, the quantum hardware landscape as of October 2026, and the potential impact of quantum advances on widely used cryptographic algorithms, including RSA, ECC, and AES.

It examines the main Post-Quantum Cryptography (PQC) families and NIST standards, compares Quantum Key Distribution (QKD) with PQC, and reviews the guidance and recommendations of leading cybersecurity agencies, including the NSA, NCSC, ANSSI, and BSI.

Key Audience Takeaway

Participants will gain a clearer understanding of the quantum threat to today's cryptographic systems, the urgency of preparing for the post-quantum transition, and the practical steps organizations should take to assess cryptographic exposure, prioritize vulnerable systems, and develop a roadmap toward quantum-resistant security.

The presentation concludes with a critical question for every organization:
Where does your cryptography stand today—and will it remain secure in the quantum era?



Prof. Dr, Christian Schaffner

Full Professor of Theoretical Computer Science, University of Amsterdam · Director QuSoft

Prof. Dr. Christian Schaffner is a world-leading expert in quantum cryptography, with nearly two decades of research experience at the intersection of cryptography, quantum computing and information theory. His work covers both conventional cryptography that remains secure against quantum attackers (post-quantum cryptography) and the design of protocols that solve cryptographic problems involving quantum data and quantum communication. He advises industry and public institutions on the transition to quantum-safe security.

He is full professor in Theoretical Computer Science and leads the Theory of Computer Science (TCS) group at the Informatics Institute of the University of Amsterdam. He is director of QuSoft, the Dutch research center for quantum software, where he helps shape the national and European research agenda in the field. His teaching and supervision cover cryptography, quantum information and theoretical computer science, and he has mentored a new generation of researchers in quantum-safe security.

Bridging research and practice, he is co-founder of Eoncore, a startup that develops post-quantum cryptography software to help organizations protect their data against future quantum attacks. He received his diploma in mathematics from ETH Zurich (Switzerland) in 2003 and his PhD in computer science from Aarhus University (Denmark) in 2007.