Mehr Licht!
More Photonics for Intelligence

#C19

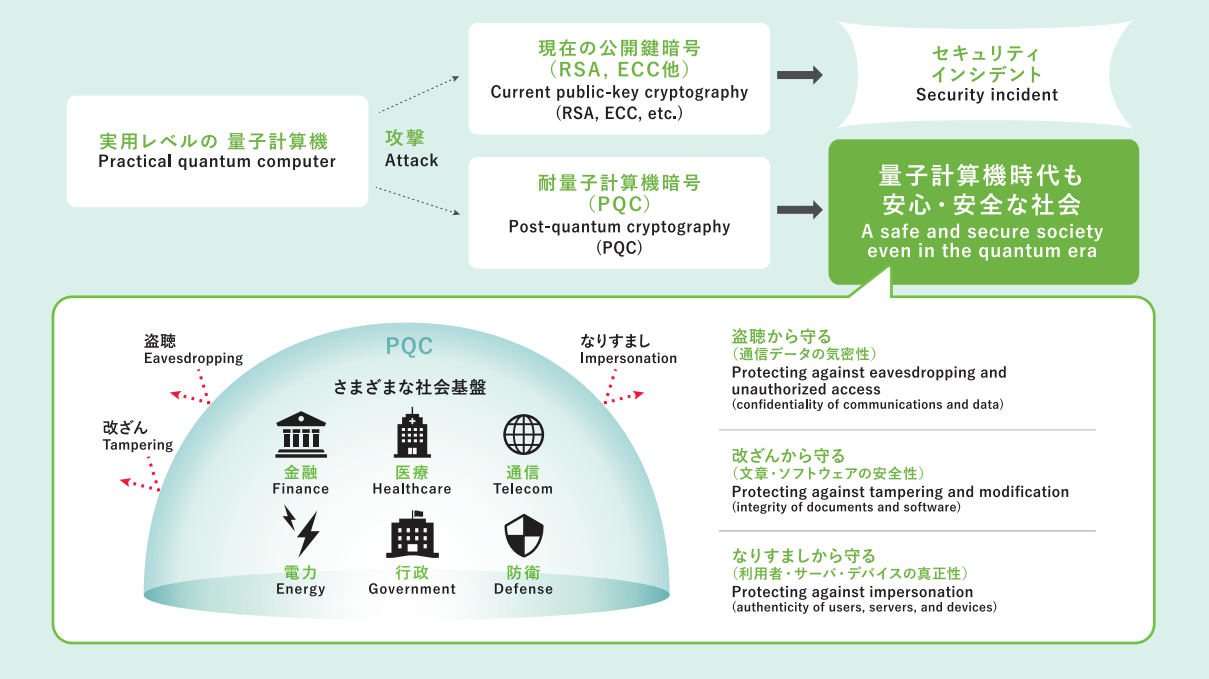
#Safety and Security #Risk Management

NTT-Developed Post-Quantum Cryptography

Building a secure and trusted society for the quantum computing era

Technical Challenges & Goals

Quantum computers may threaten the security of today's public-key cryptography. To address this problem, research and standardization of Post-Quantum Cryptography (PQC) have advanced worldwide. The deployment of PQC will enable a secure and trusted digital society throughout the quantum computing era.



Key Technologies

Core Technologies

- Efficient PQC Encryption Scheme: NTRU
- Compact PQC Signature Schemes: QR-UOV

Key Differentiators

- Highly secure (IND-CCA2/EUF-CMA) PQC encryption and signature schemes based on homegrown technology
- Japan's only PQC innovation, spanning research, standards, deployment, and fast implementation

Use Cases

Information Technology (IT)

By adopting PQC for public-key cryptography used in secure communications, digital signatures, and PKI, we enable a secure and trusted digital society throughout the quantum computing era.

Exhibitors

NTT, Inc. Social Informatics Laboratories

CONTACT：Information Security Technology Research Project