Contribution ID: **50** Type: **not specified**

Moving the Goal to Post Quantum

Wednesday, 10 April 2024 09:40 (40 minutes)

Public key cryptography is the security foundation that trust and confidentiality online are built on. Many will have heard by now that current public key cryptography is under threat from being broken by powerful quantum computers. Fortunately, the academic research community has been working hard on quantum-safe cryptographic algorithms that remain secure even if practical quantum computers become a reality. This so-called post-quantum cryptography is a hot topic: the US is standardising the first set of algorithms for use and many large Internet companies are experimenting with PQC and rolling it out. Transitioning the whole Internet to these new cryptographic algorithms, however, is a major undertaking that comes with many challenges. In this talk, Roland will explain the basic need for post-quantum cryptography and will then highlight, using examples from R&E networking, what challenges we will face in the coming years.

Presenter: Prof. VAN RIJSWIJK-DEIJ, Roland (University of Twente)

Session Classification: Opening