SAVE-THE-DATE

SAVE-THE-DATE September 25, 2024

QSIP Workshop: Quantum & Cyber Security

12.15 -16.00, Drottning Kristinas väg 61 (Innoversum), Stockholm

Quantum computers have the potential to break widely used public-key cryptosystems, such as RSA and elliptic-curve cryptography (ECC), which are omnipresent in our communication infrastructures including the Internet. All data exchange using RSA and ECC protocols is at risk - those includes the key exchange procedures as well as the digital signatures based on RSA and ECC. Decrypting RSA and ECC is equivalent to moving back to the early days of the Internet when only a fraction of digital assets was protected. Today, when many if not most of our living aspects are digitalized, there is much more at stake.

”Collect now, decrypt later”. This principle means that data sessions of today can be recorded and decrypted later when a powerful enough quantum computer will be available. It applies for example to medical records and other sensitive personal data which needs to be stored long term by regulation. In practice, it means that migration to quantum-safe solutions needs to start already today – we need to begin making the public and private sectors aware about the necessity and support their transition to the post-quantum secure future.

In this workshop, we elaborate on recent and projected developments in quantum computing (QC), how a QC is capable to break some of the wide-spread encryption systems, and what we can do about it, covering a general and industry-specific use-cases.

Program

12.15	Registration and light lunch
13.00	Welcome and introduction
13.05	Katja Gallo, KTH and Mikhail Popov, RISE “Quantum computing and post-quantum resilience: securing our digital assets long term”
13.50	Q&A
14.00	Potential risks and solutions in - The Energy Sector - The Healthcare Sector
15.00	Workshop
15.50	Wrap-up
16.00	End

Join us at the workshop on September 25! Please register here.