Definition of a quantum computer resistant encryption scheme

Publication of DIN SPEC 91444

Live Online Seminar

DIN SPEC 91444

Invitation

In this online seminar DIN SPEC 91444 consortium leader Dr. Rachid El Bansarkhani (QuantiCor Security GmbH) will give a short presentation on the content of DIN‘s first post-quantum cryptography specification.

Classical public key cryptosystems can be broken by powerful quantum computers. Thus, new and secure cryptographic alternatives are needed. In this DIN SPEC 91444 a quantum computer resistant encryption and key encapsulation mechanism (KINDI-KEM) with security based on the hardness of Module-LWE (module learning with errors) is specified. The underlying encryption scheme hides arbitrary data in the error term and further encrypts a random string in the secret term of Module-LWE instances which is exploited for the key encapsulation mechanism. To this end, the necessary functionality and relevant security features are specified. Finally, different parameter sets are defined providing various levels of security and efficiency.

Agenda

- 20 min Presentation
- 20 min Questions and Answers

Date & Time

22nd April 2021 10:00 – 10:40 AM (CET)

Organizer:
DIN e. V.
Saatwinkler Damm 42/43
13627

Meeting Venue:
WebEx

Registration:
Estera.Gryska@din.de
Tel.: +49 30 2601-2019

Foto: © maxbabakov / istockphoto.com