scademy
secure coding academy

POST-QUANTUM CRYPTOGRAPHY

CL-PQC | Onsite / Virtual classroom | 3 days

Audience: Professionals
Preparedness: General knowledge of cryptography
Exercises: Hands-on

Post-quantum cryptography is no longer just a futuristic concept, but a necessity in the present day. Anyone who works in the field and ignores its principles and techniques could be left at a severe disadvantage. This course offers a comprehensive overview of post-quantum cryptography.

Day 1 explores quantum-based attacks, lattices, and their applications in schemes and key exchange. Day 2 delves into error-correcting codes, isogenies, and their security implications. Day 3 covers the MQ problem, various schemes, including oil and vinegar, rainbow, and their cryptanalysis.

Other candidates, such as hash-based signatures and MPC-in-the-head signatures, and side-channel attacks, are also discussed. Participants will gain a thorough understanding of post-quantum cryptography and its potential impact on modern cryptography.

Outline:

Introduction to post-quantum cryptography
Attacks on DLOG and factoring
Lattices and related algorithms
LWE and Regev's encryption scheme
NTRU and NTRUPrime
Codes and cryptosystems
Isogenies and elliptic curves
MQ problem and its variants
Other candidates for PQC
Side-channel attacks and countermeasures

Participants attending this course will:

Have a deep understanding of the post-quantum cryptographic landscape

Be able to evaluate the security of different cryptographic primitives

Be able to select suitable cryptographic algorithms for their specific use case and deployment scenario

Have practical experience implementing and using post-quantum cryptographic schemes

Understand the mathematical foundations of post-quantum cryptography

Be familiar with the state-of-the-art in post-quantum cryptography

Possess knowledge and skills to defend against side-channel and physical attacks on cryptographic implementations

Related courses:

- CL-QCF - Quantum Computing Fundamentals (Onsite / Virtual classroom, 3 days)
- CL-QCI - Quantum Communication (Onsite / Virtual classroom, 3 days)

Detailed table of contents

Day 1

Intro

Attacks Against DLOG and Factoring

- Shor's Algorithm
- NIST Competition

Lattices

- Definitions
- SVP, CVP, BDD
- Good and Bad Basis
- Babai Nearest Plane Algorithm
- GGH Schemes and Attack Against Digital Signature Scheme
- LWE
- Regev's Encryption Scheme
- Key Exchange from LWE
- Ring LWE
- Module LWE and LWR
- Frodo, Kyber, Saber
- NTRU and NTRUPrime
- SIS Problem, Hash Function, and Digital Signature from SIS
- Falcon
- Lyubashevskys's ID Scheme
- Dilithium
- IBE and FHE

Day 2

Codes

- Error Correcting Codes in General
- Goppa Codes, Decoding Algorithm
- McEliece Cryptosystem, Cryptanalysis History

- BIKE and HQC
- Niederreiter Cryptosystem, Syndrome Decoding
- Trapdoor One-Way Function
- Digital Signature Scheme Wave
- Rank Metric Codes and Cryptosystems

Isogenies

- Crash Course on Isogenies and Elliptic Curves
- CGL Hash Function and SIDH
- Security of SIDH, SIKE
- Group Actions, CSIDH, and Applications
- SQISign (High-Level Discussion)

Day 3

MQ

- MQ Problem
- Discussion about Its Hardness
- Linearization, Gröbner Basis (High-Level Discussion)
- Benchmarking Systems
- Imai-Matsumoto, Hidden Field Equations
- Variants of HFE
- Oil and Vinegar Scheme, Kipnis-Shamir Attack, UOV
- Rainbow and Cryptanalysis Results for Both UOV and Rainbow
- ID Scheme and GeMSS

Other Candidates

- Hash-Based Signatures (SPHINCS+)
- MPC-in-the-Head Signatures (Picnic)

Side-Channel Attacks

- Basic Attacks
- Countermeasures Against Physical and Implementation Attacks