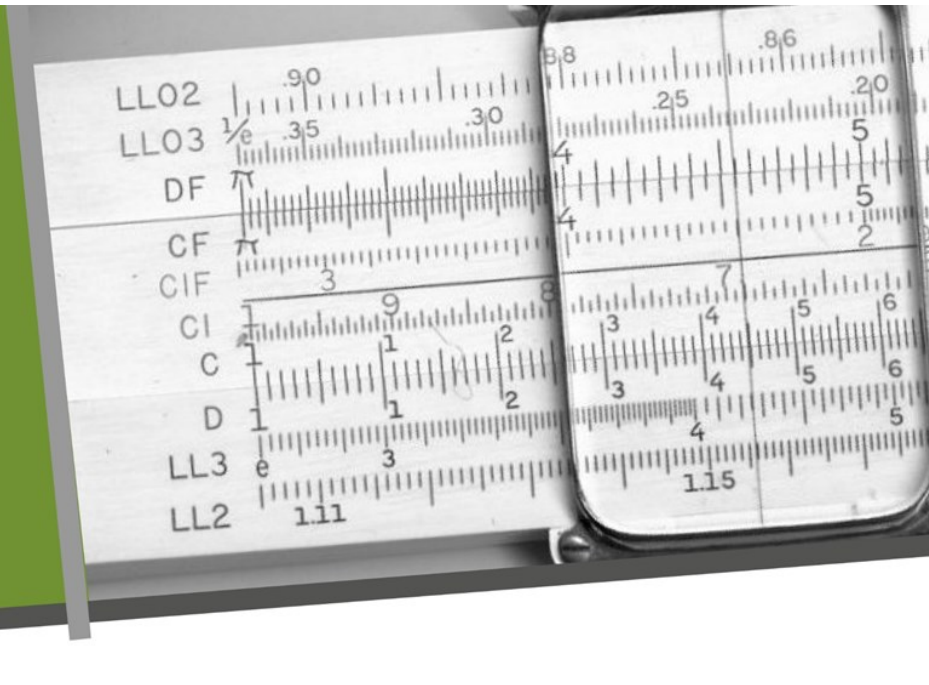
UNIVERSITÀ DI TRENTO
Dipartimento di Matematica



Research at CryptoLabTN: Post-Quantum Cryptography

Wednesday 31 May – starting from 2:30 p.m.

Room A109 – Povo1, Via Sommarive 5

Post-Quantum Cryptography is the branch of cryptography dedicated to studying systems capable of withstanding attacks from both classical and quantum computers. Currently, cryptographers are exploring several mathematical approaches that are believed to be resistant against quantum adversaries, including code-based, isogeny-based, and multivariate cryptosystems. In this mini-workshop, we present our recent research activities in this field, with a specific focus on designing and analyzing quantum-safe protocols for decentralized systems.

Program

14:30 – 14:40 **Massimiliano Sala**, University of Trento
The Laboratory of Cryptography in Trento

14:40 – 15:00 **Alessio Meneghetti**, University of Trento
Introduction to Post-Quantum Cryptography and research directions

15:00 – 15:20 **Michele Battagliola**, University of Trento
Threshold Signature from group action

15:20 – 15:40 **Giacomo Borin**, University of Trento
General threshold functionalities for LESS

15:40 – 16:00 **Giovanni Tognolini**, University of Trento
Information Leakage and Code-Based Cryptography

16:00 – 16:20 *Break*

16:20 – 16:40 **Federico Pintore**, University of Bari “Aldo Moro”
Can we still rely on SIDH?

16:40 – 17:00 **Marzio Mula**, University of Trento
Can pairings break CSIDH?

17:00 – 17:20 **Arianna Gringiani**, University of Trento
Multivariate Cryptography: A Revision of MAYO Parameters

17:20 – 17:40 **Edoardo Signorini**, Telsy
Sequential Aggregation of Multivariate Trapdoor Signatures

Contact person: Alessio Meneghetti