



# Workshop on Privacy preserving systems, software and tools

*Organized by the  
Laboratory of Cryptography and Cybersecurity  
Department of Mathematics and Physics  
Roma Tre University*

**October 24, 2022**

**Aula Urbano VIII, Argiletum - Roma Tre University**

Via della Madonna dei Monti 40



**Registration required at:** <http://www.matfis.uniroma3.it/cryptoworkshop/>

*Chair* **Marco Pedicini**, Roma Tre University

9:00 – 9:10 a.m.

**Marco Cianfriglia**, Roma Tre University  
Opening

9:10 – 9:50 a.m.

**Massimiliano Sala**, University of Trento  
On the equivalence of two post-quantum cryptographic families

9:50 – 10:30 a.m.

**Christian Mouchet**, EPFL  
Computing across Trust Boundaries with Multiparty Homomorphic Encryption and the Lattigo library

10:30 – 11:00 a.m.

**Coffee break**

11:00 - 11:40 a.m.

**Daniele Friolo**, La Sapienza University of Rome  
Multi-Key and Multi-Input Predicate Encryption from Learning With Errors

11:40 – 12:20 a.m.

**Dario Pasquini**, EPFL  
Privacy-Preserving Collaborative Machine Learning ?

12:20 a.m. - 1:00 p.m.

**Sinem Sav**, EPFL  
Privacy-Preserving Federated Learning with Multiparty Homomorphic Encryption

1:00 – 1:10 p.m.

**Closing**

