

Post-quantum Group-based Cryptography Special Session B24

Delaram Kahrobaei

The City University of New York, Queens College, USA

Antonio Tortora

Università della Campania "Luigi Vanvitelli", ITALY

Maria Tota

Università di Salerno, ITALY

This session is scheduled on July 25-26. We bring cryptographers, group theorists, quantum computational theorists to discuss various aspects of post-quantum group-based cryptography. Group-based cryptography is a relatively new family of classes of post-quantum primitives with great potential. Due to the diversity of backgrounds of the speakers, we are aiming to create interdisciplinary areas for collaborations. The topics of talks could generate new mathematical questions for group theorists as well as for cryptographers striking applying new mathematical objects and problems for the cryptographic schemes. This meeting is designed to exchange the new results in this direction and well as creating national and international collaborations among the speakers and attendees.