UNIVERSITÀ DI TRENTO
Dipartimento di Matematica

DOTTORATO

CYCLE 36th
ORAL DEFENCE OF THE PHD THESIS

Monday 29th April 2024 – at 10.00 am

Physics Seminar Room

The event will take place in presence and online through the ZOOM platform.
To get the access codes please contact the secretary office.

Michele Battagliola

PhD Student in Mathematics

Algebraic Construction for Multi-Party Protocols with Focus on Threshold Signatures

Abstract:
Secure multi-party computation (MPC) is a field of cryptography that aims to provide methods for parties to jointly compute a function over their inputs while keeping those inputs private. Unlike traditional cryptography where the adversary is outside the system of participants, the main task (and challenge) of MPC is to protect participants from internal adversaries, who participate in protocol and can therefore send corrupted.
The results presented in this talk touch various aspects of MPC. First, we present MPC from a theoretical standpoint, designing a new heuristic and a new proof system useful for proving the security of threshold signatures, a particular kind of MPC protocol. Next, we show some MPC primitives, with a focus on threshold signatures. Lastly, we present a coercion resistant e-voting protocol, that allows voters to freely vote without being afraid of external adversaries trying to pressure them to vote in a particular way.

Supervisor: Nadir Murru

CONTACTS
Staff Department of Mathematics
tel. 0461 281508-1625-1701-3786
phd.maths@unitn.it
www.maths.unitn.it