UNIVERSITÀ DI TRENTO
Dipartimento di Matematica

DOTTORATO

CYCLE 37th
ORAL DEFENCE OF THE PHD THESIS

Thursday 24th April 2025 – 2.00 pm

Department of Mathematics
Seminar Room 1
The event will take place in presence and online through the ZOOM platform.
To get the access codes, please contact the secretary office.

Chiara Spadafora

PhD Student in Mathematics

Combining Cryptography, Risk Assessment And Usability For Secure E-Voting Systems

Abstract:
Remote electronic voting is a multifaceted subject that cannot be fully addressed from a single perspective. The design of a secure and effective remote e-voting system requires a careful balance between mathematical rigor, robust information security measures, and usability considerations. These interconnected dimensions have been analyzed to propose a comprehensive solution, called Vote App, that ensures both security and usability. Vote App features linear vote counting and a novel approach to credential management that improves usability while maintaining strong cryptographic guarantees. The protocol also includes a ballot encryption scheme tailored to the Italian electoral law and supported by zero-knowledge proofs. On the system side, Vote App integrates OAuth token management into the protocol and introduces the Commitment Access Token, a new security mechanism that protects voter credentials and ensures the unlinkability between voters and their ballots.
In terms of threat modeling, the work adapts and extends STRIDE and LINDDUN to the specific context of e-voting, introducing a coercion-aware adversary model and refined risk assessment techniques that are applied to analyze the security of the proposed protocol.
Usability aspects are also addressed, including a glyph-based verification mechanism and a broader evaluation of user interaction with cryptographic features, emphasizing their importance for real-world deployment.
Overall, the research aims to bring remote e-voting closer to reality by developing solutions that are both secure and user-friendly.

Supervisor: Silvio Ranise

CONTATTI
Staff di Dipartimento - Matematica
tel. 0461 281508-1625-1701-3786
phd.maths@unitn.it
www.maths.unitn.it