

**From Theory to Deployment:  
Insights from the Swiss Post E-Voting Protocol**

Chiara Spadafora

Abstract: How do cryptography and real-world constraints meet in an e-voting system? This talk examines how cryptographic protocols are translated into a real-world e-voting system, involving legal requirements, operational procedures, and human factors. The main focus of the talk is the e-voting protocol currently deployed by some Swiss cantons to enable citizens to securely cast their votes online in legally binding elections. We then move from the present to the near future, detailing the new protocol under development and highlighting how it is expected to improve both the security and the verifiability of the system.

Throughout the talk, we keep an eye on practical constraints: how the Federal Ordinance on electronic voting shapes trust assumptions and transparency requirements, and how operational procedures influence the generation of election parameters and the verification of protocol steps. We also address usability and accessibility, discussing how the voting process can be made understandable and verifiable for all voters. We close by outlining how external experts and independent implementations contribute to the continuous evaluation and analysis of the protocol.