PrEP

Quantum-**Pr**oofing **E**uropean
Public Administrations

Next Q-PrEP Webinar

Post-Quantum Cryptography: Foundations and Challenges

Online July 09, 2026

13:00 (CEST)

NMWP. The Innovation Engineers.

Capgemini engineering

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Q-PrEP Webinars

Post-Quantum Cryptography:Foundations and Challenges

Online July 09, 2026

- What are multivariate cryptography and standard proposals in this field
- Cryptanalysis of a zero-knowledge proof of knowledge protocol based on MQ-problem
- Transition to post-quantum versions of OPRF protocol based on multivariate cryptography

Expert: Martina Vigorito (EPITA, France) graduated from the University of Salerno in 2021. She earned her Ph.D. in Algebra from the same university in 2025, under the supervision of Maria Tota (University of Salerno, Italy), Delaram Kahrobaei (CUNY, New York), and Ludovic Perret (EPITA, Paris). After completing her Ph.D., she started a postdoctoral position at LIP6, Sorbonne University, and EPITA.