

VIE-CRYPT'25: Workshop on Quantum Cryptography beyond QKD

16 – 18 June 2025



Time	16 June (Mon)	17 June (Tue)	18 June (Wed)
08:45 – 09:00	Opening Remarks		
09:00 – 09:45	Jérémie Roland Quantum weak coin flipping	Tomoyuki Morimae Quantum cryptography without one-way functions	Petros Wallden (online) Quantum attacks to lattice problems
09:45 – 10:30	Gláucia Murta Anonymous communication in quantum networks	Claude Crépeau Relativistic zero-knowledge proofs	Atul Mantri Quantum security analysis of the key-alternating ciphers
10:30 – 11:00	Coffee Break	Coffee Break	Coffee Break
11:00 – 11:45	Michal Vyvlečka Quantum dot sources for long-distance quantum internet	Paolo Villoresi Quantum communications in space as a global resource for fundamental studies and applications beyond QKD	Hua-Lei Yin Quantum digital signatures theory and its application in quantum networks
11:45 – 12:30	Mariano Lemus Oblivious transfer in quantum cryptography: an overview	Qiang Zhang Device-independent quantum random number beacon and its application	Lorenzo Coccia Device-independent randomness, quantum bounds, and sequential protocols
12:30 – 14:00	Lunch Break	Lunch Break	12:30 – 12:45 Closing Remarks 12:45 – 14:00 Lunch Break
14:00 – 14:45	Cosmo Lupo Error-tolerant oblivious transfer in the noisy-storage model	Adrian Kent (online) <i>To be announced</i>	14:00 Lab Tours
14:45 – 15:30	Paula Alonso Blanco Secure multi-party computation from entanglement-based quantum oblivious transfer in the noisy quantum storage model	Eleni Diamanti <i>Cryptographic applications of multipartite entanglement certification</i>	
15:30 – 16:00	Coffee Break	Coffee Break	
16:00 – 16:45	Hannes Hübel Quantum-enabled secure multiparty computation: a practical implementation of quantum oblivious transfer	Omri Shmueli (online) <i>One-shot signatures and quantum vs. classical binding</i>	
17:00	Poster Session		
18:00		Conference Dinner	