	Monday	Tuesday	Wednesday	Thursday	Friday
8:50 am	Organizers (Welcome, 10 min)				
9:00	Frank Wilhelm: *Status of the development of quantum computers*	Dan Bernstein: *Challenges in quantum algorithms for integer factorization*	Maria Naya-Plasencia: *New Results on Symmetric Quantum Cryptanalysis*	Discussion: *Challenge problems for quantum cryptanalysis*	Jean-Pierre Tillich: *Quantum algorithms for attacking code-based schemes/ decoding linear codes*
9:50 am	Break	Break	Break	Break	Break
10:15 am	Martin Roetteler: *Quantum resource estimates for computing elliptic curve discrete logarithms*	Claus Schnorr: *Factoring integers by lattice reduction*	Alexander May: *Grover Meets Simon – Quantumly Attacking the FX-construction*	Elena Kirshanova: *Connections between the Dihedral Coset Problem and LWE*	Peter Høyer: *Quantum walks*
10:45 am	Break	Break	Break	Break	Break
11:15 am	Yi-Kai Liu: *Quantum Cryptanalysis of Block Ciphers: A Case Study*	Alex Bocharov: *Factorization with qutrits*	David Jao: *Random self-reducibility of SIDH*	Shi Bai: *Improved combinatorial algorithms for ISIS problems*	Discussion time
11:45 am	Discussion time	Discussion time	Discussion time	Discussion time	
12:15 pm	Lunch	Lunch	Lunch	Lunch	Lunch
2:45 pm	Ray Perlner: *Thermodynamic Analysis of Classical and Quantum Algorithms for Preimage and Collision Search Problems*	Andreas Hülsing: *Quantum security results for the sponge construction*	Excursion	Gorjan Alagic: *Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts*	Departure
3:15 pm	Coffee/tea	Coffee/tea		Coffee/tea	
4:15 pm	Gustavo Banegas: *Low-communication parallel quantum multi-target preimage search*	Serge Fehr: *Classical Proofs for the Quantum Security of Classical Hash Functions*		Dominique Unruh: *Security of Fiat-Shamir*	