	Monday	Tuesday	Wednesday	Thursday	Friday
8:50 am	Organizers' welcome (10 min)				
9:00	David Jao: *Using isogenies for post-quantum cryptography*	André Schrottenloher: *Quantum Merging Algorithms*	Martin Ekerå: *On factoring RSA integers and computing discrete logarithms on quantum computers*	Fernando Virdia: *Implementing Grover oracles for key search on AES and LowMC*	Antoine Joux: *The Fermat-FHE system*
9:50 am	Break	Break	Break	Break	Break
10:15 am	Tanja Lange: *Quantum circuits for the CSIDH: optimizing quantum evaluation of isogenies*	Elena Kirshanova: *Quantum speed-ups for sieving algorithms*	Alexander May: *Quantum Period Finding with a Single Output Qubit - Factoring n-bit RSA with n/2 Qubits?*	Xavier Bonnetain: *The offline Simon's algorithm*	Daniel Apon/Ray Perlner: *An attack on LEDAcrypt*
10:45 am	Break	Break	Break	Break	Break
11:15 am	Jean-François Biasse: *On quantum algorithms for isogenies*	Daniel Bernstein: *Challenges in evaluating costs of known lattice attacks*	Sam Jaques: *Improved quantum circuits for modular arithmetic and elliptic curve discrete log*	Akinori Hosoyamada: *Finding Hash Collisions with Quantum Computers by Using Differential Trails with Smaller Probability than Birthday Bound*	Rachel Player: *On the condition number of Macaulay matrices as used in the Chen-Gao variant of HHL*
11:45 am	Discussion time	Discussion time	Discussion time	Discussion time	Discussion time
12:15 pm	Lunch	Lunch	Lunch	Lunch	Lunch
2:45 pm	Harry Buhrman: *On quantum versions of the Strong Exponential Time Hypothesis*	Priyanka Mukhopadhyay: *Faster provable sieving algorithms for SVP and CVP in ℓ_p norm*	Excursion	András Gilyén: *Some new distributional property testing results*	Departure
3:15 pm	Coffee/tea	Coffee/tea		Coffee/tea	
4:15 pm	Philippe Gaborit: *Using coding theory for post-quantum cryptography*	Gorjan Alagic/Daniel Apon/Dustin Moody/Ray Perlner/Daniel Smith Tone: *NIST discussion*		John Schanck: *Quantum speedups for lattice sieves are tenuous at best*	
5:00 pm				Christian Bischof: *Modeling the Runtime of Cryptanalytic Algorithms*	