Dagstuhl Seminar 23421: Quantum Cryptanalysis -- Draft Schedule

	Monday	**Tuesday**	**Wednesday**	**Thursday**	**Friday**
9:00 AM	Organizers: *Welcome, organization of the seminar*	Gorjan Alagic & Daniel Smith-Tone: *NIST PQC process update*	*Lightning talks*	Xavier Bonnetain: *Single-query Quantum Hidden Shift Attacks*	Breakout groups: *Updates*
9:45 AM	Break	Break	Break	Break	Break
10:15 AM	Open discussion time	Breakout groups: *Updates*	Breakout groups: *Discussion time*	Breakout groups: *Discussion time*	All: *Discussion of next steps*
11:00 AM	Breakout groups: *Discussion time*	Breakout groups: *Discussion time*			
12:15 PM	Lunch	Lunch	Lunch	Lunch	Lunch
2:30 PM	Yixin Shen: *Tutorial -- quantum algorithms for lattice problems*	André Schrottenloher: *Quantum Linear Key-recovery Attacks using the QFT*	No technical program	Péter Kutas: *Quantum algorithms in isogney-based cryptography*	Departure
3:15 PM	Coffee/Tea	Coffee/Tea		Coffee/Tea	
4:00 PM	*Open discussion time*	*Open discussion time*		Jean-Pierre Tillich: *Decoding in superposition*	