Schedule: Dagstuhl Seminar 25431 on Quantum Cryptanalysis

	Monday	***Tuesday***	***Wednesday***	***Thursday***	***Friday***
7:30-8:45	*breakfast*	*breakfast*	*breakfast*	*breakfast*	*breakfast*
9-10:00	Announcements + Introductions (9-10:30)	Talk by Wessel van Woerden	Talk by Andre Schrottenloher	Talk by Lynn Engelberts	Final reports from breakouts and/or extra talk
10:00-11:00	*break*	*break*	*break*	*break*	*break*
11:00-12:00	Discussion of breakouts	Talk by Julian Nowakowski	Talk by Xavier Bonnetain	Tutorial by Sean Hallgren	Final reports from breakouts and/or extra talk
12:15	*lunch*	*lunch*	*lunch*	*lunch*	*lunch*
13:30-15:00	Talk by Andre Chailloux	Breakout session 2	Free time	Breakout session 3	-
15:00-16:00	*cake*	*cake*	*cake*	*cake*	-
16:00-16:30	Breakout session 1 (15:45-17:15)	Preliminary reports on breakouts	Free time	QCRAM discussion (Sam Jacques and Chris Majenz)	-
16:30-18:00	Preliminary reports on breakouts (17:15-17:45)	Talk by Hugues Randriam (16:30-17:30)	Free time	Impromptu discussion time	-
18:00	*dinner*	*dinner*	*dinner*	*dinner*	-

Andre Chailloux: *Quantum algorithms inspired by Regev's reduction*

Wessel van Woerden: *Classical & Quantum Algorithms for Solving the Lattice Isomorphism Problem*

Julian Nowakowski: *Super-Quadratic Quantum Speed-Ups and Guessing Many Likely Keys*

Hugues Randriam: *Distinguisher for McEliece public keys using syzygies*

Andre Schrottenloher: *Convolution-based quantum cryptanalysis*

Xavier Bonnetain: *A Tight Quantum Algorithm for Multiple Collision Search*

Lynn Engelberts: *An Improved Quantum Algorithm for 3-Tuple Lattice Sieving*

~~Simone Montangero: *Integer Factorization via Tensor Network Schnorr's Sieving*~~ *(cancelled)*

Sean Hallgren: *Opening the quantum black box: Kuperberg's algorithm*