Preliminary Schedule Dagstuhl Seminar Public-Key Cryptography

Monday (the day of the talks with long titles)

9:15- 9:30	- Welcome
9:30-10:30	- Krzysztof Pietrzak: How to Overcome Hellman's Time/Memory Trade-Offs with Applications to Proofs of Space
10:30-11:00	- Coffe break
11:00-11:35	- Dennis Hofheinz: How to make Kurosawa-Desmedt encryption tightly secure
11:35-12:10	- Jörn-Müller Quade: Composable Protocols from Encapsulated Superpolynomial Helpers
12:15-14:15	- Lunch
14:15-14:50	- Pierre-Alain Fouque: Comparison between Subfield and Straightforward Attacks on NTRU
14:50-15:30	- David Cash: What Else is Revealed by Order-Revealing Encryption?
15:30-16:00	- Coffe break
16:00-16:35	- Eike Kiltz: Schnorr signatures in the multi-user setting

Tuesday

9:15- 9:50	- David Pointcheval: Integer Commitments
9:50-10:30	- Antoine Joux: Even-Mansour in the Multi-user Setting
10:30-11:00	- Coffe break
11:00-12:10	- Vipul Goyal: Non-malleable commitments
12:15-14:15	- Lunch
14:15-15:30	- Discussion Reviewing System
15:30-16:00	- Coffe break

Wednesday

9:15- 9:55	- Antoine Joux: Lattice Reduction with Interval Arithmetic
9:55-10:30	- Phong Nguyen: Lattice enumeration with discrete pruning
10:30-11:00	- Coffe break
11:00-11:35	- Iftach Haitner: Fair Coin Flipping: Tighter Analysis and the Many-Party Case
11:35-12:15	- Hoeteck Wee: OPTLS
12:15-14:15	- Lunch
	- free afternoon/ social activities (hike, soccer, …)
15:30-16:00	- Coffe break

Thursday

9:15- 9:50	- Sven Schäge: On the Impossibility of Tight Reductions
9:50-10:30	- Alex May: Practical LPN Cryptanalysis
10:30-10:50	- Coffe break
10:50-11:20	-Jacob Schuldt: Public-key Cryptography with Imperfect Randomness
11:20-12:10	- Phong Nguyen: Discussion - NIST's Post-Quantum Crypto
12:15-14:15	- Lunch
	- research afternoon (work on proposals, papers, … with your peers and let the organizers know about success stories)
15:30-16:00	- Coffe break

Friday

9:15- 9:50	- Vinod Vaikuntanathan: ½ FHE from DDH
9:50-10:30	- Suzanna Schmeelk: On Android Security
10:30-11:00	- Coffe break
11:00-11:40	- Fabrice Benhamouda: Diverse Moduls in Zero Knowledge
11:40-12:15	- Alexander Koch: Computational Arithmetic Secret Sharing
12:15-14:15	- Lunch