Monday (Sep 19)		Tuesday (Sep 20)		Wednesday (Sep 21)		Thursday (Sep 22)		Friday (Sep 23)	
09:00	Welcome								
09:15	Andrew Childs: *Constructing elliptic curve isogenies in quantum subexponential time*	09:15	Alexander Russell/ Cris Moore: *On the security of the McEliece cryptosystem*	09:15	Aram Harrow: *Random quantum circuits are polynomial designs*	09:15	Roger Colbeck: *Free randomness amplification*	09:15	Stephen Jordan: *Complexity implications of quantum field theory*
10:00	Daniel Nagaj: *Hamiltonian complexity of unfrustrated systems in 1D: what can you hide in qutrits?*	09:55	Kirill Morozov: *Proof of plaintext knowledge for code-based cryptosystems*	09:45 :00 AM	Dmitri Maslov: *Techniques for quantum circuit optimization*	09:55	Thomas Vidick: *TBA*	09:55	Matthias Christandl: *On a general result on analysing composability in a quantum setting*
10:30	Break	10:30	Break	10:15	Break	10:30	Break	10:30	Break
11:00	Igor Shparlinski: *Hidden shifted power problem*	11:00	Robert Koenig: *Simplified instantaneous non-local quantum computation with applications to position-based cryptography*	11:00	Ben Reichardt: *Self-testing sequential CHSH games/on quantum query complexity*	11:00	Serge Fehr: *TBA*	11:10	
11:35	Maris Ozols: *Quantum algorithms for the hidden shift problem of Boolean functions*	11:35	Florian Speelman: *The garden-hose game and applications to position-based cryptography*	11:35	Anne Broadbent: *Quantum computing on encrypted data*	11:35		11:35	
12:15	LUNCH	12:15	LUNCH	12:15	LUNCH	12:15	LUNCH	12:15	LUNCH
14:00	Dmitry Gavisnky: *Quantum money with classical verification*	14:15	Igor Semaev: *Improvements on the Circuit Lattice, hardware tool for cryptanalysis*	FREE AFTERNOON		14:15	Tsuyoshi Ito: *Quantum fingerprints that keep secrets*	DEPARTURE	
14:50	Avinathan Hassidim: *Quantum money from knots*	14:50	Peter Hoyer: *Schemes for establishing keys against quantum eavesdroppers*			14:55	Dan Bernstein: *State-of-the-art techniques for elliptic-curve scalar multiplication with side-channel protection*		
15:30	Break	15:30	Break			15:30	Break		
16:15	Alexander May: *Decoding random linear codes in O(2^0.054n)*	16:15	Jeremie Roland: *Quantum adversary lower bounds by polynomials*			16:15			