Recent Results Session

Sam Jaques	Cost models of quantum claw finding
Thomas Attema	H2020 Prometheus
Ward Beullens	Practical attacks against the Walnut digital signature scheme
Gustavo Banegas	LibQuantumJ: Another library for quantum simulation
Daniel J. Bernstein	libpqcrypto
Kris Gaj	PQC Hardware API & Fair Benchmarking of PQC
Ahmed Ferozpuri	High-Speed HW Implementation of the Multivariate Signature Schemes Unbalanced Oil and Vinegar (UOV) and Rainbow
Viet Ba Dang	Hardware Implementation of DAGS
Mike Hamburg	Glowstick KEM
Kirill Morozov	RaCoSS - Random-code-based signature scheme
Wouter Castryck	Ideal Cryptography
Matthieu Lequesne	Recovering short secret keys of RLCE KEM in polynomial time
Lorenz Panny	CSIDH: an efficient post-quantum commutative group action
Michał Andrzejczak	Hardware Framework for Lattice Sieving
Aaron Hutchinson	Constructing Canonical Strategies for Parallel Implementation of Isogeny Based Cryptography
Jean-Christophe Deneuville	Ouroboros-E: An efficient Lattice-based Key-Exchange Protocol
Rakyong Choi	Subring-Identical Linearly Homomorphic Ring Signature based on Lattice
Tim Hollebeek	Transitioning the Global Financial System to Quantum Safe Algorithms: Request for Assistance