**BARRY SANDERS**, University of Calgary, 2500 University Drive NW, Calgary, AB, T2N 1N4

*Information-theoretic security for authenticated long-distance quantum key distribution with partial trust networks*

Quantum key distribution must overcome two important hurdles: authentication to avoid the man-in-the-middle attack and relays or repeaters to allow long-distance communication. Current feasible approaches suggest complete trust of intermediate nodes in a network. We show that, in a network of partially trusted nodes (even with a low level of trust), our scheme enables probabilistic information-theoretic secure authentication and long-distance key distribution based on existing quantum key distribution technology, thus making our approach feasible now without reliance on total trust of intermediate nodes.