PATRICK HAYDEN, McGill University, Montreal
On private communication using a shared reference frame

A private shared Cartesian frame is a novel form of private shared correlation that allows for both private classical and quantum communication. Cryptography using a private shared Cartesian frame has the remarkable property that, if perfect security is demanded, the private classical capacity is roughly three times the private quantum capacity. I'll present work done with Stephen Bartlett and Rob Spekkens demonstrating that if the requirement for perfect security is relaxed, then it is possible to use the properties of random subspaces to nearly triple the private quantum capacity.