Title: Towards undetectable quantum communications

Abstract: Despite steady progress in “post-quantum” cryptography, quantum-secured communication, especially in the form of Quantum Key Distribution (QKD), remains to date the only unconditionally secure technology to distribute secret keys. Quantum communication has effectively “leaped out of the lab” as most recently demonstrated in January 2018 with the deployment of a satellite-relayed intercontinental quantum network between China and Austria, leveraging the unique possibilities offered by the Micius quantum communication satellite.

We will discuss the possibility of deploying quantum key distribution that are also covert, in the sense of being provable undetectable by an adversary. While covert key generation over quantum channels is not possible under the same assumptions as QKD, we will show that, perhaps surprisingly, covert secret key generation is possible under mild assumptions regarding the quantum channels. We will also discuss the construction of reconciliation algorithms for covert secret key generation, where the main challenge is to efficiently process the diffuse information that is embedded in covert signals. We show that astute signaling and coding techniques enable one to "concentrate" the information and approach the information-theoretic performance with low-complexity.