

Prof. Dr. Norbert Lütkenhaus (University of Waterloo)

Implementation und Protocol Security of Quantum Key Distribution

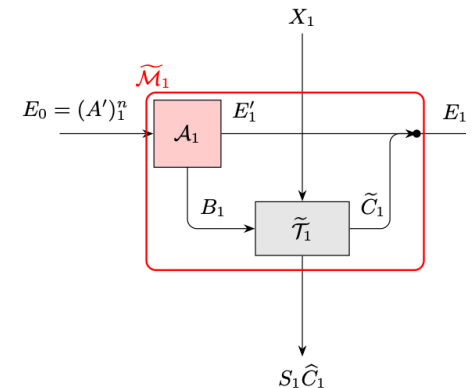
Date: **Monday, September 28, 2026**

Time: **12:00 – 13:00**

Location: Building E2 6, Room E.04

Quantum Key Distribution (QKD) is nearing commercial deployment, where standardization and certification must ensure devices meet their security guarantees. I will review security-proof concepts, common gaps and misconceptions, and questions we address. Protocol security is a theorem proving a fully specified protocol secure under device model assumptions; implementation security asks how the model–reality gap affects it. I will clarify what implementation security entails and examine device imperfections affecting performance and security proofs. Unlike quantum optics experiments, QKD implementations require scrutinizing device physics: Which model deviations exist, are they exploitable, and how can they be characterized? The talk draws on work by our group and colleagues: a QKD security definition [1], a review of proof gaps [2], complete decoy-state BB84 proofs [3, 4], analyses of device imperfections [5–7], and open-source software [8].

[1] C. Ferradini et al., arXiv:2509.13405; [2] D. Tupkary et al., Rev. Mod. Phys. 98, 035003 (2026); [3] D. Tupkary et al., arXiv:2601.18035; [4] A. Mizutani et al., arXiv:2511.21253; [5] J. Wiesemann et al., arXiv:2609.15790; [6] A. Navarrete et al., arXiv:2605.12984; [7] X. Sixto et al., arXiv:2606.29943; [8] openqkdsecurity.wordpress.com



From: J. Wiesemann et al. arXiv:2609.15790 (2026).

