# Formal verification of quantum cryptography

Dominique Unruh

University of Tartu

**Abstract.** Formal verification of cryptographic protocols has been an active research area for several decades, mostly in idealized symbolic models, but more recently also with respect to actual computationally bounded attackers. However, verification is always restricted to classical protocols and classical adversaries (to the best of our knowledge). Yet, if quantum computers arrive some day, we need cryptography that is secure against them. In this talk, we discuss the question what challenges we face if we wish to take into account quantum adversaries and/or quantum protocols. We particularly focus on the verification of cryptography against computationally bounded attackers.
The talk does not require any prior knowledge in quantum cryptography. We will discuss the nature, relevance and threats of quantum cryptography in the talk.