# Towards Automated Proving of Relational Properties of Probabilistic Programs (Invited Talk)

Klaus v. Gleissenthall[1], Andrey Rybalchenko[2], and Santiago Zanella-Béguelin[2]

[1] Technische Universität München
[2] Microsoft Research

### Abstract

Some security properties go beyond what is expressible in terms of an individual execution of a single program. In particular, many security policies in cryptography can be naturally phrased as relational properties of two open probabilistic programs. Writing and verifying proofs of such properties is an error-prone task that calls for automation and tool support. One of the main difficulties in automating these proofs lies in finding adequate relational invariants for loops and specifications for program holes. In this talk we show how to automate proofs of relational properties of open probabilistic programs by adapting techniques for the automatic generation of universally quantified invariants in a non-relational setting.