Hopping Proofs of Expectation-Based Properties: Applications to Skiplists and Security Proofs

Martin Avanzini*[1]

[1]Splits – Inria Sophia Antipolis - Méditerranée – France

Abstract

In recent work, we have proposed a new approach for proving expectation-based properties of probabilistic programs, combining eHL, a Hoare style logic toreason about expectations, with a "hopping" proof rule incorporating a relational program logic (pRHL to be precise). The logic has recently been added to EasyCrypt, a proof assistant tailored for reasoning about relational properties of probabilistic programs. As one example application, we have formalised the proof of the logarithmic average case search complexity bound for skip lists, a simple but intricate to analyse probabilistic data structure for dicitionaries. Recently, Barbosa et al. employed the logic proving security of Dilithium, a post-quantum signature scheme recently standardized by the NIST (National Institute of Standards and Technology).

*Speaker