Abstract:

Whether one-way functions (OWFs) exist is the most important outstanding problem in Cryptography. We will survey a recent thread of work (Liu-Pass, FOCS’20, Liu-Pass, STOC’21, Liu-Pass, Crypto’21) showing the equivalence of the existence of OWFs and (mild) average-case hardness of various problems related to time-bounded Kolmogorov complexity that date back to the 1960s. These results yield the first natural, and well-studied, computational problems characterizing the feasibility of the central private-key primitives and protocols in Cryptography. Based on joint works with Yanyi Liu.