Abstract:

Succinct non-interactive arguments (SNARGs) are a powerful cryptographic primitive whose feasibility is still poorly understood. However, over the last few years, a successful paradigm for building SNARGs from standard cryptographic assumptions has emerged: 1) First, build a non-interactive *batch* argument system (BARG) for NP. 2) Then, use BARGs for NP to build SNARGs for various NP languages of interest. In this talk, we will discuss recent progress on constructing SNARGs within this paradigm. Specifically, we study: 1) Under what computational assumptions can we build BARGs for NP? 2) For which NP languages can we build SNARGs within this paradigm? This talk is based on joint works with Zvika Brakerski, Maya Brodsky, Yael Kalai, Omer Paneth, Vinod Vaikuntanathan, and Daniel Wichs.