北京大学前沿计算研究中心
Center on Frontiers of Computing Studies, Peking University

静园5号院
青 年 讲 座

Quantum Advantage from Any Non-Local Game

Dr. Alex Lombardi

Postdoctoral Fellow
Simons-Berkeley

Host：刘天任 助理教授
2023年8月4日 星期五 15:00
静园五院204室

Abstract

We show a general method of compiling any k-prover non-local game into a single-prover interactive game maintaining the same (quantum) completeness and (classical) soundness guarantees. Our compiler uses a quantum homomorphic encryption scheme as a cryptographic mechanism to (provably) simulate the effect of spatial separation. In conjunction with the rich literature on (entangled) multi-prover non-local games, our compiler gives a broad framework for constructing mechanisms to classically verify quantum advantage. Some follow-up work analyzing quantum soundness of some such protocols will also be discussed.

The talk is mainly based on joint work with Yael Kalai, Vinod Vaikuntanathan, and Lisa Yang (https://eprint.iacr.org/2022/400).

Biography

Alex Lombardi is a Simons-Berkeley postdoctoral fellow hosted by Shafi Goldwasser. His current interests lie mainly in the theory and foundations of cryptography. He was a graduate student at MIT, advised by Vinod Vaikuntanathan. In the coming fall, Alex will join Princeton as an Assistant Professor of Computer Science.