Cryptographically secure computing on the MOC

Abstract
The Modular Approach to Cloud Security (MACS) project is charged to address the grand challenges in building secure cloud services. Through our partnership with the Massachusetts Open Cloud, we have both the expertise and environment to transition some of our technologies to practice. This talk overviews the security research conducted on MACS and then details the ongoing deployment of cryptographically secure multi-party computation in the cloud.

Presenter
Mayank Varia is the Director for the MACS project. His research interests span theoretical and applied cryptography and their application to problems throughout computer science. Previously, he worked for four years at MIT Lincoln Laboratory, where he designed and evaluated high performance privacy-enhancing data search technology, created information theoretic metrics to quantify privacy, and developed algorithms to capture linguistic provenance automatically. He received a Ph.D. in mathematics from MIT for his work on program obfuscation.