

Understanding Multi-party Computation: Realizability & Splittability

Mike Rosulek

University of Illinois at Urbana-Champaign

Universally-Composable (UC) security, as introduced by Canetti, is a notion of cryptographic security for arbitrary protocols in networked environments. In particular, a protocol that achieves UC security retains its security even in the presence of arbitrary composition with other protocols.

It is known that not all functionalities admit secure protocols in this model. In this joint work with Manoj Prabhakaran, we introduce the notion of "splittable" functionalities. We use this new framework to derive simple new impossibility results and complete characterizations for several natural classes of functionalities.