

A Unified Characterization of Completeness and Triviality for Secure Function Evaluation

Abstract

We present unified combinatorial characterizations of completeness for 2-party secure function evaluation (SFE) against passive and active corruptions in the information-theoretic setting, so that all known characterizations appear as special cases.

In doing so we develop new technical concepts. We define several notions of isomorphism of SFE functionalities and define the “*kernel*” of an SFE functionality. An SFE functionality is then said to be “*simple*” if and only if it is strongly isomorphic to its kernel. An SFE functionality \mathcal{F}' is a core of an SFE functionality \mathcal{F} if it is “redundancy free” and is weakly isomorphic to \mathcal{F} . Then:

- An SFE functionality is complete for security against passive corruptions if and only if it is not simple.
- A deterministic SFE functionality is complete for security against active corruptions if and only if it has a core that is not simple. We conjecture that this characterization extends to randomized SFE as well.

We further give explicit combinatorial characterizations of simple SFE functionalities.

Finally, we apply our new notions of isomorphism to reduce the problem of characterization of trivial functionalities (i.e., those securely realizable without setups) for the case of general SFE to the same problem for the case of simple symmetric SFE.

Keywords: Secure 2-party Randomized Function Evaluation, Completeness Characterization, Semi-honest Security, Information-theoretic Reduction

(Joint work with Manoj Prabhakaran and Mike Rosulek.)