Explicit Non-Malleable Codes Resistant to Permutations

Abstract

We settle a long standing open problem which has pursued a full characterization of completeness of (potentially randomized) finite functions for 2-party computation that is secure against active adversaries. Since the first such complete function was discovered [Kilian, FOCS 1988], the question of which finite 2-party functions are complete has been studied extensively, leading to characterization in many special cases. In this work, we completely settle this problem.

We provide a polynomial time algorithm to test whether a 2-party finite secure function evaluation (SFE) functionality (possibly randomized) is complete or not. The main tools in our solution include:

- A formal linear algebraic notion of *redundancy* in a general 2-party randomized function.
- A notion of *statistically testable games*. A kind of interactive proof in the information-theoretic setting where *both* parties are computationally unbounded but differ in their knowledge of a secret.
- An extension of the (weak) *converse of Shannon's channel coding theorem*, where an adversary can adaptively choose the channel based on it view.

We show that any function f, if complete, can implement any (randomized) circuit C using only $O(|C| + \kappa)$ calls to f, where κ is the statistical security parameter. In particular, for any two-party functionality g, this establishes a universal notion of its quantitative "cryptographic complexity" independent of the setup and has close connections to circuit complexity.

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

(Joint work with Daniel Kraschewski, Manoj Prabhakaran and Amit Sahai.)