Robust Combiners and Secure Function Evaluation

Moni Naor

The Weizmann Institute

<moni.naor@weizmann.ac.il>

Abstract

Suppose that we have a two cryptographic schemes that we generally trust to be secure for some task. It makes a lot of sense to try and combine these two into one scheme that is guaranteed to be secure even in the unfortunate case that one of the two original schemes is broken. Call such a mechanism a Robust Combiner. In general a (k, n)-Robust Combiner for a cryptographic primitive is a method for taking n candidate implementations for the primitive and combining them into a single scheme such that if at least k of the candidates indeed implement the primitive. Robust combiners are a useful tool for ensuring better security in applied cryptography, and also a handy tool for constructing cryptographic protocols. In this talk I will discuss which primitives have roubst combiners and the difficulty of coming up with combiners for Secure Function Evaluation.

Based on joint work with Danny Harnik, Joe Kilian, Omer Reingold and Alon Rosen