Limits of Random Oracles in Secure Computation

Abstract

The seminal result of Impagliazzo and Rudich (STOC 1989) gave a black-box separation between one-way functions and public-key encryption: informally, a public-key encryption scheme cannot be constructed using one-way functions as the sole source of computational hardness. In addition, this implied a black-box separation between one-way functions and protocols for certain Secure Function Evaluation (SFE) functionalities (in particular, Oblivious Transfer). Surprisingly, however, *since then there has been no further progress in separating one-way functions and SFE functionalities* (though several other black-box separation results were shown). In this work, we present the complete picture for finite deterministic 2-party SFE functionalities, vis a vis one-way functions. We show that one-way functions are black-box separated from *all such SFE functionalities*, except the ones which have unconditionally secure protocols (and hence do not rely on any computational hardness), when secure computation against semi-honest adversaries is considered. In the case of active adversaries, a black-box one-way function is indeed useful for SFE, but we show that it is useful only as much as access to an ideal commitment functionality is useful.

Technically, our main result establishes the limitations of random oracles for secure computation. We show that a two-party deterministic functionality f has a secure function evaluation protocol in the random oracle model that is (statistically) secure against semi-honest adversaries if and only if f has a protocol *in the plain model* that is (perfectly) secure against semi-honest adversaries. Further, in the setting of active adversaries, a deterministic SFE functionality f has a (UC or standalone) statistically secure protocol in the random oracle model if and only if f has a (UC or standalone) statistically secure protocol in the commitment-hybrid model.

Our proof is based on a "frontier analysis" of two-party protocols, combining it with (extensions of) the "independence learners" of Impagliazzo-Rudich/Barak-Mahmoody. We make essential use of a combinatorial property, originally discovered by Kushilevitz (FOCS'89), of functions that have semi-honest secure protocols in the plain model (and hence our analysis applies only to functions of polynomial-sized domains, for which such a combinatorial characterization is known).

We put forth a new conjecture, called the *Many-Worlds Conjecture*: for every 2-party SFE functionality f, one can consider a "world" where f can be *semi-honest securely* realized in the computational setting; the conjecture states that there are infinitely many "distinct worlds" between *minicrypt* and *cryptomania* in the universe of Impagliazzo's Worlds. Our result in this work could be seen as a first step to proving this conjecture.

Keywords: Deterministic 2-party Secure Function Evaluation, Black-box Separation, One-way Functions, Random Oracle, Impagliazzo's Worlds.

(Joint work with Mohammad Mahmoody and Manoj Prabhakaran.)