ABSTRACT

CFEM workshop: Theory and Practice
of Multiparty Computation
4 to 8 June, 2012
Aarhus University, Denmark

Speaker: Ran Canetti, Boston University and Tel Aviv University

Title: How to Bootstrap a SNARK in Public

Publicly verifiable succinct non-interactive arguments of knowledge (SNARKs) are concise, easily-checkable proofs for the correct execution of long computations. These proofs require a public and reusable reference string, that allows proofs to be created and checked by anyone. Generalizing SNARKs, Proof-carrying data systems (PCDs) provide a powerful tool for verifying correctness of distributed computations. So far, publicly-verifiable SNARKs and PCDs were only known to exist either in the random oracle model or in a "signing oracle" model.

We present recursive composition and bootstrapping techniques for SNARKs and PCDs that:
1. Transform SNARKs that have a long reference string but are otherwise succinct into fully succinct SNARKs.
2. Transform any SNARK into a PCD system for distributed computations
over chains of fixed polynomial length.
Applying our transformations to the succinct NIZKs of Groth [ASIACRYPT11], or of Gentry et al. [EPRINT12], whose security is based on a Knowledge of Exponent assumption in bilinear groups, we obtain the first publicly-verifiable SNARKs and PCDs in the plain model. Interestingly, the resulting constructions do not rely on the PCP Theorem and enjoy several efficiency benefits. We also obtain analogous results for privately-verifiable PCDs and SNARKs.

We note that the PCD abstraction plays a central role in our construction and analysis, not only as a goal but also as a main tool.
In particular, PCDs allow us to present and prove our constructions in a relatively clean and concise way.

Joint work with Nir Bitansky, Alessandro Chiesa and Eran Tromer.