Cryptology ePrint Archive: Report 2011/443

From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again

Nir Bitansky and Ran Canetti and Alessandro Chiesa and Eran Tromer

Abstract: The existence of succinct non-interactive arguments for NP (i.e., non-interactive computationally-sound proofs where the verifier's work is essentially independent of the complexity of the NP nondeterministic verifier) has been an intriguing question for the past two decades. Other than CS proofs in the random oracle model [Micali, FOCS '94], the only existing candidate construction is based on an elaborate assumption that is tailored to a specific protocol [Di Crescenzo and Lipmaa, CiE '08].

We formulate a general and relatively natural notion of an extractable collision-resistant hash function (ECRH) and show that, if ECRHs exist, then a modified version of Di Crescenzo and Lipmaa's protocol is a succinct non-interactive argument for NP. Furthermore, the modified protocol is actually a succinct non-interactive adaptive argument of knowledge (SNARK). We then propose several candidate constructions for ECRHs and relaxations thereof.

We demonstrate the applicability of SNARKs to various forms of delegation of computation, to succinct non-interactive zero knowledge arguments, and to succinct two-party secure computation. Finally, we show that SNARKs essentially imply the existence of ECRHs, thus demonstrating the necessity of the assumption.

Category / Keywords: foundations / CS proofs, proofs of knowledge, knowledge assumptions, knowledge of exponent, knapsack

Date: received 14 Aug 2011, last revised 30 Nov 2011

Contact author: alexch at csail mit edu