Cryptology ePrint Archive: Report 2011/514

Milder Definitions of Computational Approximability: The Case of Zero-Knowledge Protocols

Mohammad Sadeq Dousti and Rasool Jalili

Abstract: Many cryptographic primitives---such as pseudorandom generators, encryption schemes, and zero-knowledge proofs---center around the notion of \emph{approximability}. For instance, a pseudorandom generator is an expanding function which on a random seed, \emph{approximates} the uniform distribution. In this paper, we classify different notions of computational approximability in the literature, and provide several new types of approximability. More specifically, we identify two hierarchies of computational approximability: The first hierarchy ranges from \emph{strong} approximability---which is the most common type in the cryptography---to the \emph{weak} approximability---as defined by Dwork \emph{et al.} (FOCS 1999). We define semi-strong, mild, and semi-weak types as well. The second hierarchy, termed K-approximability, is inspired by the ε-approximability of Dwork \emph{et al.} (STOC 1998). K-approximability has the same levels as the first hierarchy, ranging from strong K-approximability to weak K-approximability. While both hierarchies are general and can be used to define various cryptographic constructs with different levels of security, they are best illustrated in the context of zero-knowledge protocols.

Assuming the existence of (trapdoor) one-way permutations, and exploiting the random oracle model, we present a separation between two definitions of zero knowledge: one based on strong K-approximability, and the other based on semi-strong K-approximability. Especially, we present a protocol which is zero knowledge only in the latter sense. The protocol is interesting in its own right, and can be used for efficient identification. Next, we show that our model for zero knowledge was \emph{not} closed under sequential composition, and change the model to resolve this issue. After proving a composition theorem, we finally provide a version of the identification protocol which satisfies the requirements of the new model. Some techniques provided in this paper are of independent interest, such as proving a composition theorem in the presence of both simulator and knowledge extractor.

Category / Keywords: foundations / Approximability, Indistinguishability, Zero Knowledge, Random Oracle, Trapdoor One-Way Permutation, Sequential Composition.

Publication Info: Extended Abstract submitted to TCC 2012.

Date: received 18 Sep 2011

Contact author: msdousti at gmail com, dousti@ce sharif edu