Cryptology ePrint Archive: Report 2011/504

From Non-Adaptive to Adaptive Pseudorandom Functions

Iftach Haitner and Itay Berman

Abstract: Unlike the standard notion of pseudorandom functions (PRF), a non-adaptive PRF is only required to be indistinguishable from a random function in the eyes of a non-adaptive distinguisher (i.e., one that prepares its oracle calls in advance). A recent line of research has studied the possibility of a direct construction of adaptive PRFs from non-adaptive ones, where direct means that the constructed adaptive PRF uses only few (ideally, constant number of) calls to the underlying non-adaptive PRF. Unfortunately, this study has only yielded negative results, showing that ``natural" such constructions are unlikely to exist (e.g., Myers [EUROCRYPT '04], Pietrzak05 [CRYPTO '05, EUROCRYPT '06]).

We give an affirmative answer to the above question, presenting a direct construction of adaptive PRFs from non-adaptive ones. The suggested construction is extremely simple, a composition of the non-adaptive PRF with an appropriate pairwise independent hash function.

Category / Keywords: foundations / Adaptive Pseudoerandom functions; Composition

Publication Info: TCC 2012 proceedings

Date: received 15 Sep 2011, last revised 11 Jan 2012

Contact author: iftachh at cs tau ac il, itayberm@post tau ac il

Available formats: PDF | BibTeX Citation

Version: 20120111:215927 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]