Cryptology ePrint Archive: Report 2011/479

Identity-Based (Lossy) Trapdoor Functions and Applications

Mihir Bellare and Eike Kiltz and Chris Peikert and Brent Waters

Abstract: We provide the first constructions of identity-based (injective) trapdoor functions. Furthermore, they are lossy. Constructions are given both with pairings (DLIN) and lattices (LWE). Our lossy identity-based trapdoor functions provide an automatic way to realize, in the identity-based setting, many functionalities previously known only in the public-key setting. In particular we obtain the first deterministic and efficiently searchable IBE schemes and the first hedged IBE schemes, which achieve best possible security in the face of bad randomness. Underlying our constructs is a new definition, of partial lossiness, that may be of broader interest.

Category / Keywords: Identity-based encryption, pairings, lattices, lossiness

Date: received 3 Sep 2011, last revised 9 Sep 2011

Contact author: mihir at eng ucsd edu

Available formats: PDF | BibTeX Citation

Version: 20110910:041654 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]