Cryptology ePrint Archive: Report 2011/490

Tools for Simulating Features of Composite Order Bilinear Groups in the Prime Order Setting

Allison Lewko

Abstract: In this paper, we explore a general methodology for converting composite order pairing-based cryptosystems into the prime order setting. We employ the dual pairing vector space approach initiated by Okamoto and Takashima and formulate versatile tools in this framework that can be used to translate composite order schemes for which the prior techniques of Freeman were insufficient. Our techniques are typically applicable for composite order schemes relying on the canceling property and proven secure from variants of the subgroup decision assumption, and will result in prime order schemes that are proven secure from the decisional linear assumption. As an instructive example, we obtain a translation of the Lewko-Waters composite order IBE scheme. This provides a close analog of the Boneh-Boyen IBE scheme that is proven fully secure from the decisional linear assumption. We also provide a translation of the Lewko-Waters unbounded HIBE scheme.

Category / Keywords:

Date: received 9 Sep 2011, last revised 18 Jan 2012

Contact author: alewko at cs utexas edu

Available formats: PDF | BibTeX Citation

Version: 20120118:071543 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]