Cryptology ePrint Archive: Report 2011/465

Attractive Subfamilies of BLS Curves for Implementing High-Security Pairings

Craig Costello and Kristin Lauter and Michael Naehrig

Abstract: Barreto-Lynn-Scott (BLS) curves are a stand-out candidate for implementing high-security pairings. This paper shows that particular choices of the pairing-friendly search parameter give rise to four subfamilies of BLS curves, all of which offer highly efficient and implementation- friendly pairing instantiations.

Curves from these particular subfamilies are defined over prime fields that support very efficient towering options for the full extension field. The coefficients for a specific curve and its correct twist are automat- ically determined without any computational effort. The choice of an extremely sparse search parameter is immediately reflected by a highly efficient optimal ate Miller loop and final exponentiation. As a resource for implementors, we give a list with examples of implementation-friendly BLS curves through several high-security levels.

Category / Keywords: Pairing-friendly, high-security pairings, BLS curves.

Date: received 27 Aug 2011, last revised 13 Oct 2011

Contact author: craig costello at qut edu au

Available formats: PDF | BibTeX Citation

Version: 20111014:040121 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]