Constructive and Computational Aspects of Cryptographic Pairings

Michael Naehrig

Department of Mathematics and Computer Science
Technische Universiteit Eindhoven

PhD defense
7 May 2009

Pairings

A *cryptographic pairing* is a map

$$e : G_1 \times G_2 \to G_3$$

with finite abelian groups $(G_1, +), (G_2, +)$, and $(G_3, \cdot)$, which is

- *bilinear*,

$$\begin{aligned} e(P_1 + P_2, Q_1) &= e(P_1, Q_1)e(P_2, Q_1) \\ e(P_1, Q_1 + Q_2) &= e(P_1, Q_1)e(P_1, Q_2) \end{aligned}$$

- *non-degenerate*,
  given $0 \neq P \in G_1$ there is a $Q \in G_2$ with

$$e(P, Q) \neq 1$$

- *efficiently computable*.

Pairings in cryptography

Pairings turn out to be very important and surprisingly successful in the construction of cryptographic protocols.

- There is a huge amount of recent research papers on cryptographic applications of bilinear maps.
- It is very important to find secure instantiations in the form of suitable parameters and efficient algorithms to compute pairings.

Realizing efficient pairing computation

Pairings can be realized on groups arising from elliptic and hyperelliptic curves, for example the group of rational points on an elliptic curve over a finite field.

Two ingredients are required:

- suitable curves,
- efficient algorithms.

This dissertation advances the state of the art in constructing secure pairing-friendly curves which allow particularly fast arithmetic and in improving the speed of pairing computation.

Overview

The dissertation contains the following main parts:

- Chapter 2: BN curves
- Chapter 3: Compressed pairing computation
- Chapter 4: Pairings on Edwards curves
- Chapter 5: Constructing curves of genus 2 with p-rank 1

Barreto-Naehrig (BN) curves

We give a parametrized family of pairing-friendly elliptic curves.

- The embedding degree is $k = 12$, i. e. curves provide optimal conditions for the 128-bit security level,
- have a prime number of rational points, i. e. lead to particularly efficient implementation,
- and a twist of degree $d = 6$, i. e. involved groups have very efficient representation and arithmetic.

BN curves have the form

$$E : y^2 = x^3 + b,\ b \in \mathbb{F}_p$$

and are parametrized by

$$\begin{aligned} p \;=\; p(u) &\;=\; 36u^4 + 36u^3 + 24u^2 + 6u + 1, \\ n \;=\; n(u) &\;=\; 36u^4 + 36u^3 + 18u^2 + 6u + 1. \end{aligned}$$

Compressed pairing computation

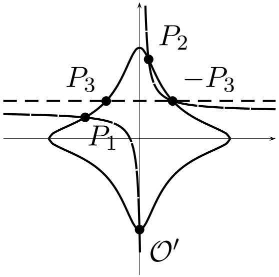
Pairing values are r-th roots of unity.

Additional structure leads to an efficient representation of pairing values in compressed form.

- For even embedding degree, we propose a method to compute pairings in compressed representation,
- directly compute compressed line functions by using part of the final exponentiation,
- avoid finite field inversions completely during one pairing computation.

Pairings on Edwards curves

Edwards curves provide the most efficient known group law for elliptic curves.



Previously, pairings on Edwards curves had only been computed by transforming to curves in Weierstraß form.

- We describe a geometric interpretation of the group law on twisted Edwards curves,
- provide functions for addition and doubling steps in Miller's algorithm to compute the Tate pairing, and
- give explicit formulas, more efficient than any previously proposed ones; even competitive with Weierstraß curves.

Constructing curves of genus 2 with *p*-rank 1

Complex multiplication (CM) methods are important tools for constructing pairing-friendly curves.

They are mainly developed for ordinary curves (*p*-rank 2).

- We describe algorithms to find curves of genus 2 with *p*-rank 1 using CM methods,
- provide examples with a prime number of rational points on their Jacobian, of cryptographic relevant bitsize, and
- give an algorithm to construct curves with a prescribed embedding degree.

Summary

Constructive and Computational Aspects of Cryptographic Pairings

- BN curves
- Compressed pairing computation
- Pairings on Edwards curves
- Constructing curves of genus 2 with *p*-rank 1