Hyperelliptic Curves With Compact Parameters

Ezra Brown
Virginia Tech, Blacksburg, VA 24061-0123, USA

Bruce T. Myers
Wheaton College, Wheaton, IL 60187, USA

Jerome A. Solinas
National Security Agency, Ft. Meade, MD 20755-6511, USA

Communicated by: A. Menezes
Received June 24, 2003; Revised December 30, 2003; Accepted February 4, 2004

Abstract. We present a family of hyperelliptic curves whose Jacobians are suitable for cryptographic use, and whose parameters can be specified in a highly efficient way. This is done via complex multiplication and identity-based parameters. We also present some novel computational shortcuts for these families.

Keywords: hyperelliptic curves, certificates, public-key cryptography, complex multiplication

AMS Classification: 14G50, 11G20, 14K22, 14H45

1. Introduction

In our earlier paper [1] we introduced the notion of elliptic curves with compact parameters. These are fixed-coefficient elliptic curves having complex multiplication over the rationals, but implemented as curves defined over a finite field \( \mathbb{F}_p \), where each user can specify his own prime \( p \). Finding an appropriate prime \( p \) is a simple search process, beginning with a random start value. We suggested that this random start value be determined by the hash output of an ID string chosen by the user. A small integer – the offset – determines how far past the random start value the user searched before finding \( p \). To enable communication, the user need only transmit the domain ID and (optionally) the offset to another user. This represents a savings of bandwidth when compared to transmission of the typical set of elliptic curve parameters (see [1] for a fuller discussion).

Compact elliptic curves are easy to use because they come equipped with convenient base points, independent of the prime \( p \). Furthermore, the complex-multiplication feature, which enables the order of the curve to be quickly computed, also enables the use of an ingenious speedup to scalar multiplication, as presented in [3].

In recent years, hyperelliptic curves (particularly of genus 2) have emerged as a viable alternative to elliptic curves. (See, e.g. [7].) Since genus 2 curves achieve the same security level using smaller base fields, they can sometimes be preferable to
elliptic curves when used on embedded processors where memory and speed are
constrained. The mathematics of compact elliptic curves generalizes to the genus-2 case. The
present paper explores this generalization. Our family of compact Jacobians is
based on the hyperelliptic curve

\[ y^2 = x^5 + 8, \]

embedded in the Jacobian of \( H \). As a curve defined over the rationals, \( H/\mathbb{Q} \) has
genus 2 and admits complex multiplication by the 5th roots of unity. For a prime of the form
\( p \equiv 1 \pmod{10} \) we consider the curve \( H/F_p \), that is, the reduction of \( H \) to \( F_p \). Since 5 divides the order of \( F_p^\times \), complex multiplication descends
to \( H/F_p \). This means we can quickly compute the order # \( H(F_p) \) of the set of \( F_p \)-rational points of
\( H/F_p \) and the order # \( J_H(F_p) \) of the group of \( F_p \)-rational points
in the Jacobian of \( H \), using the technique of Jacobi sums. The user of this cryp-
tosystem will presumably want to work in a Jacobian group of prime order, so several primes
\( p \) will have to be tried until the associated Jacobian group order # \( J_H(F_p) \) is prime. In this case, the base point
\( (1, 3) \) is a generator of the group \( J_H(F_p) \).

The 'compact' aspects of compact elliptic curve cryptosystems – low-bandwidth
transmission of domain ID and offset, plus quick extraction of system parameters
– carry over to compact Jacobians. In addition, the speedup of Gallant et al. [3]
generalizes to scalar multiplication in the Jacobian of \( H \).

2. A Cyclotomic Number Ring

We introduce notation which will remain fixed throughout the paper. Let
\( K = \mathbb{Q}(\nu) \), where \( \nu = e^{2\pi i/5} \) is a primitive 5th root of unity. Thus, \( \nu \)
satisfies the cyclotomic polynomial

\[ \Phi_5(x) = x^4 + x^3 + x^2 + x + 1 = 0. \]

We will reserve the symbol \( \zeta \) for the
particular 10th root of unity \( \zeta = -\nu^3 = e^{2\pi i/10} \).

Let \( O \) be the ring of integers of \( K \). By well-known results on cyclotomic fields
(see [12], for example), we have

\[ O = \mathbb{Z}[\nu] = \mathbb{Z} \oplus \mathbb{Z} \nu \oplus \mathbb{Z} \nu^2 \oplus \mathbb{Z} \nu^3. \]

\( O \) is a principal ideal domain, and so \( O \) has unique factorization of elements.

We denote by \( U \) the units group of \( O \). There are no real embeddings and two con-
jugate pairs of complex embeddings of \( K \). The Dirichlet Unit Theorem states that the
\( \mathbb{Z} \)-rank of \( U \) is 1. More precisely, we have

\[ U \cong \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}. \]