A FAMILY OF PAIRING-FRIENDLY SUPERELLIPTIC CURVES OF GENUS 4

Andrzej Dąbrowski

Institute of Mathematics, University of Szczecin,
Wielkopolska 15, 70-451 Szczecin, Poland;
dabrowsk@wmf.univ.szczecin.pl

Abstract. We give explicit construction of pairing-friendly superelliptic curves of genus 4 based on the closed formulas for the orders of their Jacobians.

Keywords: superelliptic curve, Jacobian variety, Cocks-Pinch method, pairing-friendly abelian variety.

1. Introduction

There are many results for constructing pairing-friendly ordinary elliptic curves. On the other hand, there are very few results for explicit constructions of pairing-friendly abelian varieties of higher dimension. These mostly concern the cases of dimension two ordinary surfaces. Freeman constructs one such family for dimension three. The most common abelian varieties used in cryptography are elliptic curves or Jacobians of hyperelliptic curves of genus > 1. We refer to [1], [4], [5], [7], [2], [8] and references therein for further discussion.

In this paper we give explicit construction of pairing-friendly superelliptic curves of genus four based on the closed formulas for the orders of their Jacobians. Our method is an analogue of the Cocks-Pinch method and produces curves with $\rho \approx 8$ (see section 6). Our work was inspired by the article [7] by Kawazoe and Takahashi (see section 5).

2. Preliminaries

Let us recall some notations and definitions.

Let A be g-dimensional abelian variety defined over $\mathbb{F}_q$, and let l be a prime number satisfying $l \nmid q$. We say that A has *embedding degree k with respect to l* if (i) A has an $\mathbb{F}_q$-rational point of order l, and (ii) k is the smallest integer such that μ_l is contained in $\mathbb{F}_{q^k}$. The last condition is equivalent to any of the following ones: (iia) k is the smallest integer such that l divides $q^k - 1$, (iib) $\Phi_k(q) \equiv 0 (\bmod\, l)$, where Φ_k is the kth cyclotomic polynomial (see Lemma 4.1).

The embedding degree gets its name because one can use the (Weil or Tate) pairing to 'embed' a cyclic subgroup of $A(\mathbb{F}_q)$ of order l into the multiplicative group of the degree k extension of $\mathbb{F}_q$.

In pairing-based cryptography, for an abelian variety A defined over $\mathbb{F}_q$, the following conditions must be satisfied to make a system secure:

(a) the order l of a prime order subgroup of $A(\mathbb{F}_q)$, and q^k should be large enough; (b) the embedding degree k and the ratio $\rho = \frac{g \log(q)}{\log(l)}$ should be approximately small.

In practice, it is recommended that $l > 2^{160}$ and $q^k > 2^{1024}$.

Abelian varieties over $\mathbb{F}_q$ satisfying the above conditions are called *pairing-friendly.* Algebraic curves whose Jacobian varieties are pairing-friendly are also called pairing-friendly.

Let A be an abelian variety of dimension g defined over a finite field $\mathbb{F}_q$. Let $h_A(x) = x^{2g} + a_1 x^{2g-1} + ... + a_{g-1} x^{g+1} + a_g x^g + a_{g-1} q x^{g-1} + ... + a_1 q^{g-1} x + q^g$ be the characteristic polynomial of the Frobenius endomorphism of A. Note the folowing useful definitions: A is *ordinary* if the middle coefficient a_g of $h_A(x)$ is relatively prime to q, and A is *supersingular* if all of the complex roots of $h_A(x)$ are roots of unity times $\sqrt{q}$.

Note that $|A(\mathbb{F}_q)| = h_A(1)$.

3. Construction of pairing-friendly elliptic curves: the Cocks-Pinch method

Let us recall the Cocks-Pinch algorithm for finding pairing-friendly elliptic curves ([3], [2]).

Fix a positive integer k, and a prime $l \equiv 1 \bmod k$.

Choose a positive integer X of order k in $(\mathbb{Z}/l\mathbb{Z})^\times$, and a positive integer D such that $-D$ is a square modulo l.

Fix $s (\bmod\, l)$ such that $s^2 \equiv -D (\bmod\, l)$, and choose an integer Y congruent to $\pm(X-1)s^{-1}$ modulo l.

Compute $q = ((X+1)^2 + DY^2)/4$.

If q is a prime, use CM method to construct elliptic curve E over $\mathbb{F}_q$ such that $|E(\mathbb{F}_q)| = q - X$ (see, for instance, [1], chapter VIII). If q is not a prime number, start again with a different X and/or Y.

Remarks. (i) We obtain $q \equiv X (\bmod\, l)$, hence l divides $|E(\mathbb{F}_q)|$ and k is an embedding degree of $E/\mathbb{F}_q$ with respect to l. (ii) This method usually gives elliptic curves with $\rho \approx 2$. However, the smallest known values of ρ for even embedding degrees $14 \leq k \leq 38$ (limit as $q, l \to \infty$) were obtained by the Cocks-Pinch method. For instance, $\rho = 7/6$ for $k = 38$ and $\rho = 11/8$ for $k = 20$ (see [3]).

4. Some useful Lemma

Let Φ_k denote the k-th cyclotomic polynomial: $\Phi_k(x) = \prod(x - \zeta_k^m)$, where $1 \leq m \leq k$, $(m, k) = 1$. We have the folowing useful result ([4], Prop. 2.3).

Lemma 4.1. (Freeman) *Let A be an abelian variety defined over $\mathbb{F}_q$. Let l be a prime number satisfying $l \nmid q$, and let k be a positive integer. Assume that the following conditions are satisfied:*

(i) $h_A(1) \equiv 0 (\operatorname{mod} l)$,

(ii) $\Phi_k(q) \equiv 0 (\operatorname{mod} l)$.

Then A has embedding degree k with respect to l.

Remark. The condition $l \mid h_A(1)$ guarantees that A has an $\mathbb{F}_q$-rational point of order l, and the condition $l \mid \Phi_k(q)$ implies that A has embedding degree k with respect to l.

5. A family of pairing-friendly hyperelliptic curves of genus 2

Here we recall the main results of [7]. The authors apply an analogue of the Cocks-Pinch method to construct a family of pairing-friendly hyperelliptic curves of genus 2 with a prescribed embedding degree. Let us stress that the method is based on closed formulas for the orders of the Jacobians, hence it allows to construct pairing-friendly hyperelliptic curves in a very short time.

Theorem 5.1. *If $p \equiv 1 \,(\operatorname{mod} 8)$, $p = c^2 + 2d^2$, $c \equiv 1 \,(\operatorname{mod} 4)$, $a^{\frac{p-1}{2}} \equiv -1 \,(\operatorname{mod} p)$, $2(-1)^{\frac{p-1}{8}} d \equiv (a^{\frac{p-1}{8}} + a^{\frac{3(p-1)}{8}}) c \,(\operatorname{mod} p)$, then the Jacobian variety J_a of $C_a : y^2 = x^5 + ax$ is simple over $\mathbb{F}_p$, and $h_{J_a}(T) = T^4 - 4dT^3 + 8d^2T^2 - 4dpT + p^2$.*

Theorem 5.2. *Fix a positive integer k. Moreover:*

(i) let l be a prime number satisfying $\operatorname{LCM}(8, k) \mid l - 1$;

(ii) *let α be a primitive kth root of unity in $(\mathbb{Z}/l\mathbb{Z})^{\times}$; let $\beta, \gamma \in \mathbb{N}$ be such that $\beta^2 \equiv -1 \pmod{l}$ and $\gamma^2 \equiv 2 \pmod{l}$;*

(iii) *let $c, d \in \mathbb{Z}$ satisfy*

$$c \equiv (\alpha+\beta)\,(\gamma(\beta+1))^{-1} \pmod{l}$$
$$d \equiv (\alpha\beta+1)\,(2(\beta+1))^{-1} \pmod{l}.$$

Then for a and p satisfying the assumptions of Theorem 5.1, the number k is the embedding degree of $Jac(C_a)$ over $\mathbb{F}_p$ with respect to l.

The above method produces curves of genus 2 with simple jacobians, and with $\rho \approx 4$, for $l \in (2^{160}, 2^{160}+2^{20})$ or $l \in (2^{256}, 2^{256}+2^{20})$, $k \leq 32$.

6. A family of pairing-friendly superelliptic curves of genus 4

Here we modify (a variant of) the Cocks-Pinch method (used in [7]) to construct a family of pairing-friendly superelliptic curves of genus 4 with a prescribed embedding degree.

Let J_a denote the Jacobian variety of $C_a : y^3 = x^5 + a$ over $\mathbb{F}_p$. We start with the following explicit calculations ([6], Prop. 13).

Theorem 6.1. *Let a be a nonzero integer, and p an odd prime with $p \nmid a$. If $p \equiv 2, 8 \pmod{15}$, $p = 3c^2 + 5d^2$, then we have $h_{J_a}(T) = T^8 + 2p(3c^2 - 5d^2)T^4 + p^4$.*

Remark. (i) $J(C_a)$ are simple over $\mathbb{F}_p$ for a and p satisfying the assumptions above (simple argument using Theorem 6.1). (ii) $J(C_a)$ (under the same assumptions on a and p) are neither ordinary nor supersingular (use Theorem 6.1 and definitions from section 2).

Now we are ready to state the main result of this paper.

Theorem 6.2. *Fix a positive integer k. Moreover:*

(i) *let l be a prime number satisfying $k|l-1$;*

(ii) *let α be a primitive kth root of unity in $(\mathbb{Z}/l\mathbb{Z})^{\times}$; let $\beta, \gamma, \delta, \omega \in \mathbb{N}$ be such that $\beta^2 \equiv -1 \pmod{l}$, $\gamma^2 \equiv 3 \pmod{l}$, $\delta^2 \equiv 5 \pmod{l}$ and $\omega^2 \equiv \alpha \pmod{l}$;*

(iii) *let $c, d \in \mathbb{Z}$ satisfy*

$$c \equiv \frac{\beta(\alpha^2-1)}{2\gamma\omega} \pmod{l}$$
$$d \equiv \frac{(\alpha^2+1)}{2\delta\omega} \pmod{l}.$$

Then for a and p satisfying the assumptions of Theorem 6.1, the number k is the embedding degree of $Jac(C_a)$ over $\mathbb{F}_p$ with respect to l.

Proof of this result uses Lemma 4.1 and Theorem 6.1. We omit the details.

Our method produces curves of genus 4 with simple jacobians, and with $\rho \approx 8$, for $l \in (2^{160}, 2^{160} + 2^{20})$, $k \leq 50$ (calculations were made by T. Jędrzejak).

References

[1] I. Blake, G. Seroussi, N. Smart, *Elliptic curves in cryptography*, The Press Syndicate of the University of Cambridge, 2002

[2] D. Boneh, K. Rubin, A. Silverberg, *Finding composite order ordinary elliptic curves using the Cocks-Pinch method*, J. Number Theory **131** (2011), 832-841

[3] D. Freeman, *Methods for constructing pairing-friendly elliptic curves*, lecture at ECC 2006, available online

[4] D. Freeman, *Constructing pairing-friendly genus 2 curves over prime fields with ordinary Jacobians*, Lecture Notes in Computer Science **4575** (2007), 152-176

[5] D. Freeman, T. Satoh, *Constructing pairing-friendly hyperelliptic curves using Weil restriction*, J. Number Theory **131** (2011), 959-983

[6] T. Jędrzejak, *On the torsion of the Jacobians of superelliptic curves $y^q = x^p + a$*, Journal of Number Theory **145** (2014), 402-425

[7] M. Kawazoe, T. Takahashi, *Pairing-friendly hyperelliptic curves with ordinary Jacobians of type $y^2 = x^5 + ax$*, Lecture Notes in Computer Science **5209** (2008), 164-177

[8] K. Lauter, N. Shang, *Generating pairing-friendly parameters for the CM construction of genus 2 curves over prime fields*, Des. Codes Cryptogr. **67** (2013), 341–355

RODZINA PF (PAIRING-FRIENDLY) KRZYWYCH SUPERELIPTYCZNYCH GENUSU 4

Streszczenie. Podajemy jawną konstrukcję pf (pairing-friendly) krzywych supereliptycznych genusu 4, bazując na formułach dokładnych dla rzędów ich jakobianów.

Słowa kluczowe: krzywa supereliptyczna, rozmaitość Jakobiego, metoda Cocksa-Pincha, pf (pairing-friendly) rozmaitość abelowa.