GENERATION OF RANDOM PICARD CURVES FOR CRYPTOGRAPHY

ANNEGRET WENG

Abstract. Combining the ideas in [BTW] and [GS], we give a efficient, low memory algorithm for computing the number of points on the Jacobian of a Picard curve. We present an example of cryptographic size.

1. Introduction

Let p, $p \neq 2, 3$, be a prime. A Picard curve over $\mathbb{F}_p$ is a non-singular curve C given by an affine equation of the form

$$y^3 = f(x)$$

where $f(x) \in \mathbb{F}_p[x]$ is a polynomial of degree 4. We can define the discrete logarithm problem in the group of $\mathbb{F}_p$ rational elements of the Jacobian or the divisor class group of degree 0 of C . If p is large enough, this problem is difficult and we can use the curve C for crytosystems based on the discrete logarithm problem.

To ensure the invulnerability with respect to the attack by Pohlig and Hellmann, the group order of $J_C(\mathbb{F}_p)$ should have a large prime factor. But the determination of the group order $\#J_C(\mathbb{F}_p)$ is a non-trivial problem and has not been solved efficiently.

In this paper we apply the low-memory version of the MCT-algorithm by Gaudry and Schost to Picard curves. Using the ideas from [BTW] and some minor improvements described in Sections 4 and 5, we manage to count the number of points on a Picard curve over $\mathbb{F}_p$ where p has 16 decimal digits and $J_C(\mathbb{F}_p)$ is of size 2^{162}. This shows that determining the group order of the Jacobian of a Picard curve of cryptographic size is feasible.

We restrict to prime fields but all results are also true for arbitrary finite fields $\mathbb{F}_q$.

2. Point counting on Picard curves

We briefly summarize the main results from [BTW] which we will need to formulate the modified version of the algorithm by Gaudry and Schost.

Let C be a Picard curve over $\mathbb{F}_p$.

If $p \equiv 2 \mod 3$, point counting is relatively easy since we know that $\#C(\mathbb{F}_p) = p+1$ and $\#C(\mathbb{F}_{p^3}) = p^3+1$. Indeed, we can deduce that the L-polynomial of C splits and the group order of the Jacobian will be divisible by $(p+1)$ (cf. [BTW]). These curves are not suitable for crytography.

We now restrict to the case $p \equiv 1 \mod 3$. In this case, the automorphism $\zeta_3 : (x, y) \to (x, \zeta_3 y)$ is defined over $\mathbb{F}_p$. Let C be a Picard curve over $\mathbb{F}_p$ and let w be the Frobenius endomorphism on the

Date: November 2, 2004.
1991 *Mathematics Subject Classification.* Primary 14H45. Secondary 11Y16.
Key words and phrases. Picard curves.
The author thanks the DFG for financial support.

Jacobian J_C. For the vast majority of Picard curves over $\mathbb{F}_p$ there exists an element $\pi \in \mathbb{Z}[\zeta_3]$ with $\pi\overline{\pi} = p$ and $a_1 \in \mathbb{Z}[\zeta_3]$ with $\mathrm{Norm}_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(a_1) \leq 6p$ such that

$$(1 - a_1 + \overline{a_1}\pi - \pi p)D = \mathbf{0} \tag{2.1}$$

for all $D \in J_C(\mathbb{F}_p)$ [BTW].

This leads to the following algorithm. Set $a_1 = \frac{d_1 + d_2\sqrt{-3}}{2}$ with $d_1,\ d_2 \in \mathbb{Z}$ and choose a random element $D \in J_C(\mathbb{F}_p)$. We must have

$$(1 - a_1 + \overline{a_1}\pi - \pi p)D = \mathbf{0}$$

for some π, $\pi\overline{\pi} = p$. Note that there are exactly 12 element which satisfies the norm equation, namely $\{\pi, \overline{\pi}, -\pi, -\overline{\pi}, \zeta_3\pi, \zeta_3\overline{\pi}, -\zeta_3\pi, -\zeta_3\overline{\pi}, \zeta_3^2\pi, \zeta_3^2\overline{\pi}, -\zeta_3^2\pi, -\zeta_3^2\overline{\pi}\}$. Since $\mathrm{Norm}_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(a_1) \leq 6p$, we have $|d_1| \leq 6\sqrt{p}$ and $|d_2| \leq 2\sqrt{3p}$.

For a fixed π, we compute

$$2(1 - \pi p)D + (1 + \pi)(\zeta_3 + 1)d_2 D$$

for all $d_2 \in \mathbb{Z}$ in $[-2\sqrt{3p}, 2\sqrt{3p}]$ and store the hash value of the results in a table. We then compute

$$(1 - \pi)d_1 D$$

for $d_1 \in \mathbb{Z} \cap [-6\sqrt{p}, 6\sqrt{p}]$ and compare its hash value to the values in the table. This is a baby-step giant-step type algorithm of space and time complexity $O(\sqrt{p})$.

Note that the order of D does not have to be maximal and in general, we will only find a candidate for a_1. In practice, this is no problem and we always discover the right element a_1 (for a discussion see [BTW], Subsection 4.1).

3. A 2-dimensional random walk on Jacobians of Picard curves

This section is a very close adaptation of the two dimension random walk described by Gaudry and Schost in [GS].

We choose a random element $D \in J_C(\mathbb{F}_p)$ and fix an element $\pi \in \mathbb{Z}[\zeta_3]$ such that $\pi\overline{\pi} = p$ (for more about the choice of π, see Section 4). We will now compute the order of D.

Set

$$R = \left\{(\sigma_1, \sigma_2) : \sigma_1 \in [-6\sqrt{p}, 6\sqrt{p}], \sigma_2 \in [-2\sqrt{3p}, 2\sqrt{3p}]\right\},$$

and define two set of points

$$W = \{2(1 - \pi p)D - (1 + \pi)(\zeta_3 + 1)\sigma_2 D - (1 - \pi)\sigma_1 D : (\sigma_1, \sigma_2) \in R\}$$

and

$$T = \{-(1 + \pi)(\zeta_3 + 1)\sigma_2 D - (1 - \pi)\sigma_1 D : (\sigma_1, \sigma_2) \in R\}.$$

We will later choose random elements in T and W and hope for a collision. Note that if we find an element $P \in W \cap T$ with coordinates $(\sigma_{1W}, \sigma_{2W})$ resp. $(\sigma_{1T}, \sigma_{2T})$, then we discover a candidate for a_1 by setting $d_1 = \sigma_{1W} - \sigma_{1T}$ and $d_2 = \sigma_{2W} - \sigma_{2T}$.

Let $f_R : J_C(\mathbb{F}_p) \to \{0, 1\}$ be a pseudo-random deterministic function which takes 1 with probability $p_{\mathcal{D}}$ and 0 with probability $1 - p_{\mathcal{D}}$. It decides whether a point is distinguished or not.

For the random walk we fix parameters r, ℓ_1, ℓ_2. For each k, k' in $[1, r]$ we select random non-negative integers in $\alpha_{k,k'} \in [0, 2\ell_1]$ and $\beta_{k,k'} \in [0, 2\ell_2]$. We then precompute offsets

$$\mathcal{O}_{k,k',b} = -(1 + \pi)(\zeta_3 + 1)\sigma_2 D - (-1)^b(1 - \pi)\sigma_1 D$$

for all k, k' in $[1, r]$ and $b \in \{0, 1\}$.

We now start the random walk by choosing a random point P in W (resp. T) whose coordinates are given by (σ_1, σ_2). We compute the values k, k' and b as pseudo-random deterministic functions of P and define the next point by setting

$$Q = P + \mathcal{O}_{k,k',b}.$$

If ℓ_1, ℓ_2 are chosen small enough, we have $Q \in W$ (resp. T). The coordinates of the new point Q are $(\sigma_1 + (-1)^b \alpha_{k,k'}, \sigma_2 + \beta_{k,k'})$. For each Q we compute $f_R(Q)$. If we hit a distinguished point, we save its parameters in a list and start a new chain. For each new distinguished point we check if it occurs in the list. If yes, a collision is found and we can compute our candidates for d_1 and d_2.

Following Section 4.3 in [GS], we now chose optimal parameters.
We have

$$\#R = 48\sqrt{3}p$$

Let λ be such that the expected number of points to construct is $\lambda\sqrt{\#R}$. By [GS], Subsection 4.1, $\lambda \simeq 2.43$.
We want C to be the number of random chains we expect to construct; set $C = 1000$.
We get

$$p_{\mathcal{D}} = \frac{C}{\lambda\sqrt{\#R}} \simeq \frac{109.67}{\lambda\sqrt{p}} \simeq \frac{45.13}{\sqrt{p}}.$$

By [GS],

$$\ell_1 = \frac{(B_{2,\max} - B_{2,\min})p_{\mathcal{D}}}{10}$$

and

$$\ell_2 = \frac{(B_{1,\max} - B_{1,\min})\sqrt{p_{\mathcal{D}}}}{9}$$

where $B_{2,\max} = -B_{2,\min} = 2\sqrt{3p}$ and $B_{1,\max} = -B_{1,\min} = 6\sqrt{p}$ in our case. We find

$$\ell_1 \simeq \frac{75.98}{\lambda} \simeq 31.27.$$

and

$$\ell_2 \simeq \frac{6.98p^{\frac{1}{4}}}{\lambda^{\frac{1}{2}}} \simeq 4.47p^{1/4}.$$

Note that for about 60% of all Picard curves over a fixed field $\mathbb{F}_p$, we expect $\mathrm{Norm}_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(a_1) \leq p$. If we want to restrict to this case, the parameters have to be chosen as follows: $p_{\mathcal{D}} \simeq \frac{178.19}{\sqrt{p}}$, $\ell_1 \simeq 41.15$, $\ell_2 \simeq 5.93p^{1/4}$.

Remark 3.1. In practice, ℓ_2 turns out to be too large and many chains will go out of the interval. We have to observe the average quotient of

$$\frac{\sigma_2^D - B_{1,\min}}{B_{2,\max} - B_{1,\min}}$$

where (σ_1^D, σ_2^D) are the coordinates for a distinguished point D. We then divide ℓ_2 by some appropriate constant such that this quotient is almost always less than one.

4. The choice of π

In principal, we have 12 different possibilities for $\pi \in \mathbb{Z}[\zeta_3]$ such that $\pi\overline{\pi} = p$. In [BTW], Example 3, it is observed that only 3 different values seem to occur. We can make this more precise. For the operation of the automorphism of order 3, i.e. $(x, y) \to (x, \zeta_3 y)$ we have to make a choice of the third root of unity modulo p. Let us call this root z. The choice of π has to be consistent with the choice of the root of unity, i.e. if $\pi = a + b\zeta_3$, we must have $a + bz \equiv 0 \mod p$. We easily see that for each set of conjugates $\{\pi, \overline{\pi}\}$ there is precisely one element which satisfies this condition. Hence, we are left with 6 instead of 12 different values for π. In fact, given a prime p, all these different values can occur. But if we restrict to special curves, we can reduce the possible set of elements further

Lemma 4.1. *Let C be a Picard curve defined over $\mathbb{F}_p$ with $p \equiv 1 \mod 3$ and assume that the group order of $J_C(\mathbb{F}_p)$ is not divisible by 3. Then the element π in equation 2.1 satisfies $\pi \equiv 2 \mod (1 - \zeta_3)$.*

Proof. We have $\mathbb{Z}[\zeta_3]/(1 - \zeta_3) \simeq \mathbb{F}_3$. Obviously, $\pi \not\equiv 0 \mod (1 - \zeta_3)$, since p is prime.
Moreover, since $J_C(\mathbb{F}_p)$ is not divisible by 3,

$$1 - a_1 + \overline{a_1}\pi - \pi p \not\equiv 0 \mod (1 - \zeta_3).$$

We have

$$\begin{aligned} 1 - a_1 + \overline{a_1}\pi - \pi p &\equiv 1 - a_1 + \overline{a_1}\pi - \pi \mod (1 - \zeta_3), \text{ since } p \equiv 1 \mod 3 \\ &\equiv 1 - a_1 + a_1\pi - \pi \mod (1 - \zeta_3), \text{ since } a_1 \equiv \overline{a_1} \mod (1 - \zeta_3) \text{ for all } a_1 \in \mathbb{Z}[\zeta_3] \\ &\equiv (1 - a_1)(1 - \pi) \mod (1 - \zeta_3). \end{aligned}$$

Hence, $\pi \not\equiv 1 \mod (1 - \zeta_3)$ and the claim follows. □

5. Using the 2-torsion points

In [BTW], Section 3, the authors describe how to ensure that the Jacobian has no 2-torsion points. In fact, using the 2-torsion points we can deduce more information on π and a_1.
With the algorithm in Section 3 in [BTW] we can determine all 2-torsion elements. We then consider the action of the Frobenius on a basis $J_C[2]$ and find its matrix representation in $Gl_2(\mathbb{F}_2)$. Let $f_2(x) \in \mathbb{F}_2[x]$ be its minimal polynomial.
The prime 2 is inert in ζ_3. Consider the reduction $g_2(x) \in \mathbb{F}_4[x] = \mathbb{F}_2(\alpha)[x]$ of the polynomial $g(x) = x^3 - a_1x^2 + \overline{a_1}\pi x - \pi x$. It is of the form

$$g_2(x) = x^3 + ax^2 + a^2bx + b$$

where $a_1 \equiv a \mod 2$ and $\pi \equiv b \mod 2$. Moreover we have

$$g_2(x)g_2^{(2)}(x) = f_2(x)$$

where $g_2^{(2)}$ is the polynomial we obtain by raising all coefficient of g_2 to the second power.
We now run through all possible choices for b and a. Note that $b \not\equiv 0 \mod 2$, since p is odd. We

get the following table:

b	a	$g_2(x)$	$f_2(x)$
1	0	x^3+1	x^6+1
1	1	x^3+x^2+x+1	$x^6+x^4+x^2+1$
1	α	$x^3+\alpha x^2+\alpha^2 x+1$	$x^6+x^5+x^3+x+1$
1	α^2	$x^3+\alpha^2 x^2+\alpha x+1$	$x^6+x^5+x^3+x+1$
α	0	$x^3+\alpha$	x^6+x^3+1
α	1	$x^3+x^2+\alpha x+\alpha$	x^6+1
α	α	$x^3+\alpha x^2+x+\alpha$	$x^6+x^5+x^4+x^2+x+1$
α	α^2	$x^3+\alpha^2 x^2+\alpha^2 x+\alpha$	$x^6+x^5+x^3+x+1$
α^2	0	$x^3+\alpha^2$	x^6+x^3+1
α^2	1	$x^3+x^2+\alpha^2 x+\alpha^2$	x^6+1
α^2	α	$x^3+\alpha x^2+\alpha x+\alpha^2$	$x^6+x^5+x^3+x+1$
α^2	α^2	$x^3+\alpha^2 x^2+x+\alpha^2$	$x^6+x^5+x^4+x^2+x+1$

This tables helps us to deduce some information on $\pi \mod 2$ or the relation between $\pi \mod 2$ and $a_1 \mod 2$ and will speed up the algorithm.
Using the 2-torsion we can extract even more information. Set

$$g_2(x) = x^3 + \alpha x + \alpha^2 \beta x + \beta \in \mathbb{F}_4[x].$$

Let w be the Frobenius endomorphism on the Jacobian. We now search for solutions α, $\beta \in \mathbb{F}_4$ with $\beta \neq 0$ such that

$$\left(w^3 + \alpha w^2 + \alpha^2 \beta w + \beta\right) D_i = 0 \tag{5.1}$$

for all elements $\{D_1, D_2, \ldots, D_6\}$ in a basis of $J_C[2]$.
In most cases, we will find precisely one pair (α, β) for equation (5.1). Together with the results in Section 4 this allows us to compute $\pi \in \mathbb{Z}[\zeta_3]$ with $\pi\overline{\pi} = p$ completely. Moreover we get $a_1 \mod 2$.
These improvements lead to a further speed up by a factor of 6.

6. Twists of Picard curves

Suppose we have chosen a Picard curve

$$y^3 = f(x)$$

and using the algorithm in [BTW] and its modification described above we could determine $a_1 \in \mathbb{Z}[\zeta_3]$ such that

$$(1 - a_1 + \overline{a_1}\pi - \pi p)D = \mathbf{0} \tag{6.1}$$

for some $D \in J_C(\mathbb{F}_p)$. Most likely, D will have an order which is large enough to ensure the equality 6.1 for all divisors $D \in J_C(\mathbb{F}_p)$.
In this case, the characteristic polynomial of the Frobenius is given by

$$f(x) = g(x)\overline{g(x)} \text{ where } g(x) = x^3 - a_1 x^2 + \overline{a_1}\pi x - \pi p \tag{6.2}$$

and $\overline{g(x)}$ is the conjugate of $g(x)$.
If $f(1)$ is an integers with a large prime factor, we found a curve of cryptographic relevance.
Suppose that $f(1)$ is not prime or nearly a prime (which is sufficient for most applications). We can then still hope that one of the two other cubic twists of C has a prime order. If C is given in canonical form $y^3 = x^4 + g_2x^2 + g_3x + g_4$, the cubic twist can be described by

$$C^{(k)} : y^3 = x^4 + b^{2k}g_2 + b^{3k}g_3x + b^{4k}g_4, \qquad k = 1, 2$$

where b is a cubic non-residue modulo p.
We find their orders by computing a root w_1 of the characteristic polynomial of the Frobenius $f(x)$ and determining the minimal polynomials of $\zeta_3 w_1$ resp. $\zeta_3^2 w_1$. This can for instance be done using the LLL-algorithm. For each $k \in \{1,2\}$ there exists some $j \in \{1,2\}$ such that $\#J_{C^{(k)}}(\mathbb{F}_p) = f^{(j)}(1)$.

7. Two experimental examples

Let $p = 18014398509482143 \equiv 1 \mod 3$ and choose $\alpha = 17273671983260821$. We have $\alpha^2+\alpha+1 \equiv 0 \mod p$. Using Lemma 4.1 we get the following three possibilities for π in formula (6.1):

$$\pi \in \{-140475539 - 126933146\zeta_3, 126933146 - 13542393\zeta_3, 13542393 + 140475539\zeta_3\}.$$

We now choose random curves until we find a curve C whose Jacobian has neither 2 nor 3-torsion points (see [BTW] how this can be checked) and count the number of points. The 24th curve we tried was

$$C: y^3 = x^4 + 7763767191750169x^2 + 8830812181647934x + 6270991928220054.$$

By considering the 2-torsion points, we find that

$$w \equiv 1 + \zeta_3 \mod 2, \text{ i.e. } w = 13542393 + 140475539\zeta_3,$$

and

$$a_1 \equiv 0 \mod 2.$$

We now use the random walk described in Section 3 to find g in equation (6.2). After determining a few distinguished points, we see that we often jump out of the box R and that ℓ_2 has been chosen to large. A more appropriate value for ℓ_2 in this case is given by

$$\frac{1}{128}p^{\frac{1}{4}}.$$

After a total number of 285565533 jumps we find a collision and recover

$$a_1 = -96325782 - 175278454\zeta_3$$

and hence

$$f_C(x) = x^6 + 17373110x^5 - 12831169373438532x^4 - 1203166213468120809454997x^3 - 231145798435784013559166562134076x^2 + 5637896529748849474572066416236002446390x + 5846006549323766468164834401780073670200191178207.$$

The group order $f(1) = 5846006554961662766767884237401900227979465970103$ is not prime. We now compute a root w of $f(x)$ and determine the minimal polynomials $f_1(x)$ and $f_2(x)$ of $\zeta_3 w$ and $\zeta_3 w$. In fact, one of them leads to a prime group order and the corresponding curve is given by

$$\tilde{C}: y^3 = x^4 + 11722105437014538x^2 + 8830812181647934x + 10542915522985670.$$

Its characteristic polynomial is equal to

$$f_{\tilde{C}}(x) = x^6 + 254231126x^5 + 57828212190899298x^4 + 8245950918421015447423279x^3 + 1041740459497753404970703442235614x^2 + 82502717304474702521596007459025101647574x + 5846006549323766468164834401780073670200191178207$$

and

$$f_{\tilde{C}}(1) = 5846006631826484814380004667080462349156627615099$$

which is a prime of size 2^{162}.
The computation took 5919.02 seconds.
Next we tried a larger example with $p = 288230376151711813$. Here, we were lucky, since the first

curve had already a prime group order.
The curve

$$y^3 = x^4 + 211939155673366998x^2 + 180771375410752024x + 192949046001937542$$

has no 2 and 3-torsion points. The Frobenius element can be computed and we find

$$\pi = 194769756 + 607070009\zeta_3.$$

We now started our random walk and after 2681105003 jumps and 58406.90 seconds we found

$$a_1 = 29876544 - 135474292\zeta_3.$$

The corresponding group order is

$$23945242809810674383789064863599186983250020224864027$$

which is a prime with 53 decimal digits or 174 binary digits.

Acknowledgements

I am grateful to Pierrick Gaudry for the source code of his implementation of the parallel version of Matsuo, Chao and Tsujii's algorithm and for answering many question concerning [GS] and its realization.
For our computation I used three Linux machines with altogether six AMD Opteron 250 processors (2,4 GHz). The implementation uses a C++ program, NTL, GMP and MPICH and for the information on the 2-torsion points we used the function field arithmetic by Florian Hess implemented in Magma.

References

[BTW] M. Bauer, E. Teske, A. Weng. Point counting on Picard curves. preprint, 2003
[GS] P. Gaudry, É. Schost. A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm. ANTS VI, LNCS 3076, p. 208-222, 2004

Laboratoire d'Informatique (LIX), cole polytechnique, 91128 Palaiseau CEDEX, France

E-mail address: weng@lix.polytechnique.fr