Cryptology ePrint Archive, Report 2006/176, May 2006.

Counting points on elliptic curves in medium characteristic

Antoine Joux[1,3] and Reynald Lercier[1,2]

[1] DGA
[2] CELAR
Route de Laillé
35170 Bruz, France
Reynald.Lercier@m4x.org
[3] Université de Versailles St-Quentin-en-Yvelines
PRISM
45, avenue des Etats-Unis
78035 Versailles Cedex, France
Antoine.Joux@m4x.org

Abstract. In this paper, we revisit the problem of computing the kernel of a separable isogeny of degree ℓ between two elliptic curves defined over a finite field $\mathbb{F}_q$ of characteristic p. We describe an algorithm the asymptotic time complexity of which is equal to $\widetilde{O}(\ell^2(1+\ell/p)\log q)$ bit operations. This algorithm is particularly useful when $\ell > p$ and as a consequence, we obtain an improvement of the complexity of the SEA point counting algorithm for small values of p. More precisely, we obtain a heuristic time complexity $\widetilde{O}(\log^4 q)$ and a space complexity $O(\log^2 q)$, in the previously unfavorable case where $p \simeq \log q$. Compared to the best previous algorithms, the memory requirements of our SEA variation are smaller by a $\log^2 q$ factor.
Keywords: finite fields, elliptic curves, separable isogenies, point counting.

1 Introduction

Counting points on an elliptic curve over a finite field $\mathbb{F}_q$, $q = p^n$ is a fascinating problem, which has attracted considerable interest in the recent years. In 1997, Elkies already mentioned this keen interest at the beginning of [12]. The whole story started in 1985, with the publication by Schoof [30] of a deterministic polynomial time algorithm to compute the number of points of an elliptic curve with polynomial time complexity. This offered a strong alternative to the exponential methods. Later on, the algorithm was improved by Atkin [1, 2] and by Elkies [11, 12]. More recently, a new family of algorithms, extremely efficient in small characteristic, appeared with the work of Satoh [27] and Mestre [25].

The main idea of the algorithm given in [30] is to consider the characteristic equation $\phi^2 - [c]\circ\phi + [q] = 0$ of the Frobenius ϕ while viewing ϕ as a linear action on the $\mathbb{F}_\ell$-vector space $E[\ell]$ of ℓ-torsion points (for prime integers ℓ). This allows to determine the trace c of ϕ modulo ℓ. When sufficiently many $c \bmod \ell$ are known, it remains to apply the Chinese Remainder Theorem to compute c and find the cardinality of the curve. The complexity of the algorithm essentially depends on the degree of the extension field that one must uses to handle the ℓ-torsion. Since the algorithm of Schoof uses the polynomials of ℓ-th division $f_\ell(X)$, this degree is around $\ell^2/2$. Using asymptotically fast arithmetic, one finds a time complexity $\widetilde{O}(\log^5 q)$ and a space complexity $O(\log^3 q)$.

The improvements by Atkin and Elkies stem from the following fact: for odd primes ℓ different from the characteristic p such that the principal ideal (ℓ) splits in the imaginary quadratic field $\mathbb{Q}(\sqrt{c^2-4q})$, there exists two degree ℓ separable isogenies associated with two factors $h_\ell(X)$ of degree $(\ell-1)/2$ of $f_\ell(X)$. Such an integer ℓ is called an Elkies prime. Computing these isogenies from the polynomials $h_\ell(X)$ is feasible by formulas due to Vélu [34] but that necessitates the factorization of $f_\ell(X)$. Atkin and Elkies showed that one can go in the other direction and find the rational isogenies of degree ℓ defined from E in order to deduce, without factorization, the polynomial $h_\ell(X)$. In fields of large characteristic, the time and space complexity respectively decrease then to $\widetilde{O}(\log^4 q)$ and $O(\log^2 q)$.

In this paper, we focus on the medium case, where more precisely, $p \simeq \log q$ and $n \simeq \log q/\log\log q$, when $\log q$ tends to infinity. This choice is right on the boundary where obstructions prevent the Atkin-

Elkies' method from working. The classical workaround would be to consider the algorithm of Couveignes [10] which, for fixed p, yields the same SEA complexity as in the large prime case. Unfortunately, this algorithm also behaves badly in the medium case. Instead, we propose here a new isogeny finding algorithm which yields a SEA algorithm which still heuristically runs in $\widetilde{O}(\log^4 q)$ bit operations and $O(\log^2 q)$ memory.

At the present time, four families of algorithms are known to explicitly calculate kernels of separable isogenies of degree ℓ on elliptic curves.

- Charlap-Coley-Robbins [26] or Atkin-Elkies [2]: they are valid for $p \gg \ell$, they require $\widetilde{O}(\ell^2 \log q)$ bit operations and $O(\ell \log q)$ memory.
- First Couveignes' algorithm [8]: it is the first efficient algorithm known for small characteristic p, it consists in calculations in the formal groups defined by the elliptic curves. It requires, for fixed p, $\widetilde{O}(\ell^3 \log q)$ bit operations and $O(\ell^2 \log q)$ memory.
- Lercier [22]: it is specific to the $p = 2$ case, one gets rid of formal groups and obtains an algorithm with heuristic time complexity $\widetilde{O}(\ell^3 \log q)$ and $O(\ell^2 \log q)$ bit operations.
- Second Couveignes' algorithm [9]: it consists of the interpolation of the isogeny on the p^k-torsion points. In conjunction with other ideas of Couveignes [10], the asymptotic time complexity of this algorithm is for fixed p equal to $\widetilde{O}(\ell \log^2 q)$ bit operations.

In our novel approach, we explain how to apply to finite fields of any characteristic an algorithm due to Charlap, Coley and Robbins, well understood over the complex field (cf. section 2) and successfully used, until now, in finite fields of large characteristic. The main ingredient is to lift the involved elliptic curves to the p-adic field, so that the inversions by p which occurs in the algorithm are no longer a problem (cf. section 3). This algorithm needs $\widetilde{O}((1+\ell/p)\ell^2 \log q)$ bit operations and a $O((1+\ell/p)\ell \log q)$ memory. As a result, we get an easy to implement variation of the SEA algorithm with time heuristic complexity equal to $\widetilde{O}(\log^4 q)$ and space complexity equal to $O(\log^2 q)$ for the forementioned case $p \simeq \log q$ (cf. section 4).

Notations. We denote $\widetilde{O}(N)$ complexities of the type $O(N(\log N)^k\ (\log\log N)^{k'} \ldots)$ for integers k, k', $\ldots$.

2 Complex field viewpoint

We recall here some well known results that can be found, for instance, in [32].

Complex tori and doubly periodic functions. Let Λ be a lattice of $\mathbb{C}$, that is a non null discrete subgroup of $\mathbb{C}$ which is non-isomorphic to $\mathbb{Z}$. It can be defined by $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with $\omega_1, \omega_2 \in \mathbb{C}$. A fundamental parallelogram for Λ is a set of the form $D = \{a + t_1\omega_1 + t_2\omega_2, 0 \leqslant t_1, t_2 < 1\}$ where $a \in \mathbb{C}$. There exists a bijective map between D and the quotient of $(\mathbb{C}, +)$ by Λ.

A meromorphic function f on $\mathbb{C}$ is an elliptic function of period Λ if for all $\omega \in \Lambda$, $f(z+\omega) = f(z)$. In particular, an elliptic function may be seen as a meromorphic function of the torus and the set of these functions forms clearly a field. Let us observe that an elliptic function without poles or without zeroes is constant (Liouville's theorem). Also, the sum of the residues of an elliptic function on a fundamental parallelogram (not meeting its poles) is null (residues theorem).

It is natural to introduce the function $\sum_{\omega\in\Lambda} 1/(z-\omega)^3$ because this series converges uniformly in every compact subset of $\mathbb{C} \setminus \Lambda$. It defines an odd elliptic function with a pole of order three at each point of Λ. Its integration, with a corrective term that guarantees uniform convergence in every compact subset of $\mathbb{C} \setminus \Lambda$, yields an elliptic function with poles of order two at each point of Λ called the function $\wp$ of Weierstraß,

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda-\{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}.$$

Focusing on the zeroes and the poles z_i of an even elliptic function $f(z)$, it is always possible to exhibit a product of functions $\wp(z) - \wp(z_i)$ the quotient with f of which is elliptic and without pole, therefore

constant. The field of even elliptic functions is just $\mathbb{C}(\wp)$ and, more widely, one can show that the elliptic functions field is $\mathbb{C}(\wp, \wp')$.

As $\wp'^2(z)$ is an even function, it is therefore natural to write it according to $\wp(z)$. One finds thus, once denoted $G_k = \sum_{\omega \in \Lambda - \{0\}} \omega^{-2k}$, that

$$\wp'^2 = 4\wp^3 - 60G_2\wp - 140G_3.$$

The map $\varphi : z \to (\wp(z), \wp'(z))$ is therefore a bijective map between the torus $\mathbb{C}/\Lambda$ and the set of the points of the plane projective curve with equation $Y^2Z = 4X^3 - 60G_2XZ^2 - 140G_3Z^3$ whose associated affine curve E is $y^2 = 4x^3 - 60G_2x - 140G_3$. These curves are called elliptic curves and the existence of φ (Riemann surfaces isomorphisms) shows that they are non singular. The field $\mathbb{C}(\wp, \wp')$ is therefore isomorphic to the fraction field of the ring $\mathbb{C}[x, y]/(y^2 - 4x^3 + 60G_2x + 140G_3)$ which contains the regular functions of E.

Addition law. At this stage, one can express the addition law on the torus $\mathbb{C}/\Lambda$ in geometric terms on the curve E. For that, let us quickly define a divisor D of $\mathbb{C}/\Lambda$ as a finite formal combination of points of $\mathbb{C}/\Lambda$ with coefficients in $\mathbb{Z}$. It is denoted $\sum_{P \in \mathbb{C}/\Lambda} e_P[P]$. The degree of a divisor D is the sum of its coefficients. The set of degree 0 divisors, denoted $\mathrm{Div}^0(\mathbb{C}/\Lambda)$, is a subgroup of the set of divisors $\mathrm{Div}(\mathbb{C}/\Lambda)$. To each meromorphic function f of $\mathbb{C}/\Lambda$, one associates the divisor $\mathrm{Div}\, f$ of which the points are the zeroes and the poles of f and the coefficients, the corresponding valuations. Such a divisor is called a principal divisor. One can then write the following exact sequence:

$$1 \longrightarrow \mathbb{C}^* \longrightarrow \mathbb{C}(\wp, \wp')^* \longrightarrow \mathrm{Div}^0(\mathbb{C}/\Lambda) \longrightarrow \mathbb{C}/\Lambda \longrightarrow 0.$$

The exactness at $\mathbb{C}(\wp, \wp')$ results from Liouville's theorem. The exactness in $\mathrm{Div}^0(\mathbb{C}/\Lambda)$ comes back to to say that degree 0 divisors of sum 0 are divisors of elliptic functions. It follows that the Picard group $\mathrm{Pic}^0(\mathbb{C}/\Lambda)$ of $\mathbb{C}/\Lambda$, defined as the quotient of $\mathrm{Div}^0(\mathbb{C}/\Lambda)$ by the group of principal divisors, is isomorphic to $\mathbb{C}/\Lambda$. With O, the point at infinity of the projective curve, the associated isomorphism is simply $P \longrightarrow [P] - [O]$. Explaining from this isomorphism the addition on the torus yields the well known so-called "chord and tangent" method.

Morphisms between complex tori. Let E_1 and E_2 be two projective elliptic curves associated with two tori $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$. A holomorphic map of $\mathbb{C}/\Lambda_1$ towards $\mathbb{C}/\Lambda_2$ that sends O towards O is a group morphism which, when non constant, is subjective and called an isogeny. One can then show that the set of the isogenies of E_1 towards E_2 is a commutative group isomorphic to the subset of the complex values α such that $\alpha\Lambda_1 \subset \Lambda_2$. For the direct direction, it is not difficult to see that when α verifies this last condition, the application $[\alpha] : z \longrightarrow \alpha z$ is an isogeny. On the other hand, it is necessary to lift on $\mathbb{C}$ the considered isogeny to see that its derivative is holomorphic and elliptic, therefore constant.

Thus, the kernel of a non-null isogeny Φ is the finite subgroup $\alpha^{-1}\Lambda_2/\Lambda_1$. The degree of Φ denoted $\deg \Phi$ is the number of elements in the kernel of Φ. We have $\deg(\Phi) = [\Lambda_2 : \alpha\Lambda_1] = [\alpha^{-1}\Lambda_2 : \Lambda_1]$.

This yields an injective map of the function field $\mathbb{C}(\Lambda_2)$ in $\mathbb{C}(\Lambda_1)$,

$$\begin{array}{rl} \Phi^* : \mathbb{C}(\Lambda_2) & \longrightarrow \mathbb{C}(\Lambda_1), \\ f & \longrightarrow f \circ \Phi \ . \end{array}$$

This injective map defines a Galois extension of degree $\deg \Phi$. On the other hand, any injective map of $\mathbb{C}(\Lambda_2)$ in $\mathbb{C}(\Lambda_1)$ defines an holomorphic morphism of $\mathbb{C}/\Lambda_1$ in $\mathbb{C}/\Lambda_2$. Besides, Φ induces a morphism of $\mathrm{Div}\, E_1$ in $\mathrm{Div}\, E_2$ that preserves the degree, $\sum_{P \in \mathbb{C}/\Lambda} e_P[P] \longrightarrow \sum_{P \in \mathbb{C}/\Lambda} e_P[\Phi(P)]$. Using the norm of the extension $\mathbb{C}(E_1)/\mathbb{C}(E_2)$, we see that the image of a principal divisor is a principal divisor. Thus, the isogeny Φ induces a morphism of $\mathrm{Pic}^0(E_1)$ in $\mathrm{Pic}^0(E_2)$, or equivalently a morphism of E_1 in E_2.

Let d be the degree of Φ, then $\Lambda_1 \subset \alpha^{-1}\Lambda_2 \subset d^{-1}\Lambda_1$ and therefore $\Lambda_2 \subset d^{-1}\alpha\Lambda_1$. Therefore, there exists an isogeny:

$$\begin{array}{rl} \widehat{\Phi} : \mathbb{C}/\Lambda_2 & \longrightarrow \ \mathbb{C}/\Lambda_1, \\ z & \longrightarrow d\alpha^{-1}z \ . \end{array}$$

Then, $\widehat{\Phi} \circ \Phi$ is equal to the multiplication by d on $\mathbb{C}/\Lambda_1$, denoted $[d]_1$. Similarly $\Phi \circ \widehat{\Phi} = [d]_2$.

Algorithmic viewpoint. In the SEA point counting algorithm, we need, given two isogeneous curves of degree ℓ, to compute the kernel C_ℓ of the corresponding isogeny. More precisely, let E be defined by the Weierstraß equation $y^2 = x^3 + a_4x + a_6$ and the isogeneous elliptic curve of degree ℓ, $\tilde{E} = E/C_\ell$ defined by $y^2 = x^3 + \tilde{a}_4x + \tilde{a}_6$, we would like to compute the polynomial

$$h_\ell(X) = \prod_{\pm P \in C_\ell \setminus \{O\}} (X - x(P)).$$

Over $\mathbb{C}$, we can associate to E the reduced Weierstraß $\wp$-function given by

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} c_k z^{2k}$$

where the coefficients are

$$c_1 = -\frac{a_4}{5},\ \ c_2 = -\frac{a_6}{7},\ \ c_k = \frac{3}{(k-2)(2k+3)} \sum_{j=1}^{k-2} c_j c_{k-1-j},\quad \text{for } k \geq 3.$$

The function $\tilde{\wp}$ for $\widetilde{E}$ is defined similarly using the coefficients $\tilde{a}_4$ and $\tilde{a}_6$. Seen in terms of lattices, the isogeny is quite simple,

$$\begin{aligned} \mathbb{C}/(\omega_1\mathbb{Z} + \omega_2\mathbb{Z}) &\to \mathbb{C}/(\tfrac{\omega_1}{\ell}\mathbb{Z} + \omega_2\mathbb{Z}), \\ z &\mapsto z. \end{aligned}$$

The following observation gives a first relation between $\wp(z)$ and $\tilde{\wp}(z)$.

Lemma 1. *Let $\wp(z)$ and $\tilde{\wp}(z)$ be two Weierstraß functions respectively defined over the lattices $\omega_1\mathbb{Z}+\omega_2\mathbb{Z}$ et $\frac{\omega_1}{\ell}\mathbb{Z} + \omega_2\mathbb{Z}$. Then*

$$\forall z \in \mathbb{C},\ \ \tilde{\wp}(z) = \sum_{i=0}^{l-1} \wp(z + i\frac{\omega_1}{\ell}) - \sum_{i=0}^{l-1} \wp(i\frac{\omega_1}{\ell}).$$

We are now ready to give a short summary of the method of Charlap, Coley and Robbins. For more details, the reader can refer to the presentation given by Morain in [26]. We proceed in two steps. First, we calculate the sums

$$p_k = \sum_{i=1}^{(\ell-1)/2} \wp^k\left(i\frac{\omega_1}{\ell}\right),\ k \in \mathbb{N},$$

and in a second step obtain $h_\ell(X)$ using Newton's formulas [6, p. 161]. To this effect, we compute the derivative of the differential equation satisfied by $\wp$, $\left(\frac{d\wp}{dz}\right)^2 = 4\wp^3 + 4a_4\wp + 4a_6$, and obtain $\frac{d^2\wp}{dz^2} = 6\wp^2 + 2a_4$. Computing the second derivative yields $\frac{d^4\wp}{dz^4} = 120\wp^3 + 72a_4\wp + 48a_6$. Similarly, further derivatives yield equations

$$\forall k \in \mathbb{N}^*, \forall z \in \mathbb{C}, \frac{d^{2k}\wp}{dz^{2k}}(z) = (2k+2)!\wp^{k+1}(z) + \cdots$$

Evaluating these derivates at $\frac{\omega_1}{\ell}, \ldots, \frac{(\ell-1)\omega_1}{\ell}$ and summing up, we find

$$\forall k \in \mathbb{N}^*, \sum_{i=1}^{l-1} \frac{d^{2k}\wp}{dz^{2k}}\left(i\frac{\omega_1}{\ell}\right) = 2\left((2k+2)!p_{k+1} + \cdots\right).$$

Using Lemma 1, we get

$$\sum_{i=1}^{l-1} \frac{d^{2k}\wp}{dz^{2k}}\left(i\frac{\omega_1}{\ell}\right) = (2k)!(\tilde{b}_k - c_k)$$

and therefore

$$(2k)!(\tilde{c}_k - c_k) = 2(2k+2)!\wp^{k+1}(z) + \cdots$$

In particular,

$$a_4 - \tilde{a}_4 = 5(6p_2 + 2a_4p_0),$$
$$a_6 - \tilde{b}_6 = 7(10p_3 + 6a_4p_1 + 4a_6p_0).$$

As a consequence, the computation of the p_k becomes a simple inversion of a triangular linear system of equations.

3 Back to finite fields

For elliptic curves defined over finite fields, the situation is slightly more difficult. In order to compute $h_\ell(X)$, we first need a model for the isogeneous curve of degree ℓ. This was solved by Elkies with the help of the ℓ-th modular polynomials. In the same manner, Elkies describes how we can obtain the sum p_1 of the x-coordinates of the nonzero points in $E[\ell]$. We refer to [11, 31] for details. The remaining of the computation is then a direct application of the formulas given above.

Let us note that these algebraic relations are reductions of relations over $\mathbb{C}$; for these relations to hold over a finite field, the characteristic p must be large enough since the coefficients c_k and $\tilde{c}_k$ need inversions of integers of the form $(k-2)(2k+3)$, which can be equal to zero modulo p when $\ell \geq (p-3)/2$. When p is large enough, everything proceeds correctly and it is not difficult to see that the time complexity is equal to $\widetilde{O}(\ell^2 \log q)$.

A *p*-adic version. In the same spirit as the results published in the last few years for counting points on algebraic curves of small genus, we make the previous algorithm work in finite finite fields of small characteristic by lifting the isogeneous elliptic curves in an unramified extension denoted $\mathbb{Q}_q$ of the p-adic, corresponding to the extension $\mathbb{F}_q$ of $\mathbb{F}_p$. This yields algorithm 3.1.

Algorithm 3.1 `CCRLifted`

Algorithm to compute separable kernels of isogenies of degree ℓ

INPUT: An non-supersingular elliptic curve given over $\mathbb{F}_q$ by $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_x + a_6$ and an Elkies prime ℓ.
OUTPUT: Two polynomials in $\mathbb{F}_q[X]$ of degree $\lfloor \ell/2 \rfloor$ the roots of which are x-coordinates of points of $E[\ell]$.

Step 1. Let w be a p-adic precision given by $\begin{cases} \lfloor 15 + 3\ell/2 \rfloor \text{ if } p = 2, \\ 5 + \ell \text{ if } p = 3, \\ \lfloor 1 + 2\ell/p \rfloor \text{ otherwise.} \end{cases}$
Step 2. Lift E in $\mathbb{Q}_q$ in a arbitrary way.
Step 3. Compute an isomorphic Weierstraß model $\mathcal{E} : y^2 = x^3 + A_4x + A_6$ isomorphic by λ to $E/\mathbb{Q}_q$.
Step 4. Use Atkin-Elkies' algorithm to get at precision w in $\mathbb{Q}_q$ two isogeneous curves $\tilde{\mathcal{E}}$ and $\tilde{\mathcal{E}}'$.
Step 5. Use Atkin-Elkies' algorithm to get at precision w in $\mathbb{Q}_q$ the sums p_1 and p_1'.
Step 6. Use Charlap-Coley-Robbins algorithm to get from $(\tilde{\mathcal{E}}, p_1)$ and $(\tilde{\mathcal{E}}', p_1')$ two polynomials $\mathcal{H}_\ell(X)$ and $\mathcal{H}'_\ell(X)$.
Step 7. return $\{\lambda^{-1}(\mathcal{H}_\ell(X)) \bmod p,\ \lambda^{-1}(\mathcal{H}'_\ell(X)) \bmod p\}$.

Some comments on this algorithm follow.

- It may happen that Atkin-Elkies' algorithms fail with inputs supersingular curves or $\ell = p$ (cf. [31]). We thus do not authorize such inputs in this algorithm. But Charlap-Coley-Robbins' method, at the opposite of Couveignes' algorithms, do not need any non-trivial p-torsion point.
- When the characteristic p of the field is greater than 2ℓ, algorithm 3.1 is the same algorithm as the classical Charlap-Coley-Robbins algorithm since working with precision one in $\mathbb{Q}_q$ is obviously the same things as working in $\mathbb{F}_q$.

- The precision needed depends on the number of non invertible elements that the algorithm will encounter in the Charlap-Coley-Robbins computations, mainly in the c_k's computations, and it is not hard to see that this precision must be mainly proportional to $2\ell/p$ in general, to ℓ in fields of characteristic 3 and to $3\ell/2$ in fields of characteristic 2. The additional terms of 15 in characteristic 2 and 5 in characteristic 3 was determined experimentally. It mostly comes from the change of variable needed to get an isomorphic Weierstraß model of the form $\mathcal{E} : y^2 = x^3 + A_4x + A_6$ and from the few inversions by two or three needed in Atkin-Elkies formulas.
- The complexity in time of the algorithm is still $\widetilde{O}(\ell^2)$ multiplications. When p is large these are multiplications in $\mathbb{F}_q$, otherwise, these are multiplications in $\mathbb{Q}_q$ at precision $\widetilde{O}(\ell/p)$. We therefore have a total complexity in time equal to $\widetilde{O}((1+\ell/p)\ell^2 \log q)$. The complexity in space is $O((1+\ell/p)\ell \log q)$.

We have implemented this algorithm using the Magma computer algebra system, version 2.12 [3]. We give below examples in characteristics 23 and 2.

A characteristic 23 example. Let $E/\mathbb{F}_{23}$ be the elliptic curve $y^2 = x^3 + 6\,x + 17$. We are looking for isogenies of degree 13. We simply take as Weierstraß model isomorphic to E in $\mathbb{Q}_{23}$ at precision 2 the curve $\mathcal{E} : y^2 = x^3 + (6 + O(23^2))\,x + (17 + O(23^2))$. Atkin-Elkies' algorithms then enable us to find that $\mathcal{E}$ is 13-isogeneous to a curve approximated by $\tilde{\mathcal{E}} : y^2 = x^3 + (99 + O(23^2))\,x$. Similarly, we find that $p_1 = -19 + O(23^2)$. Charlap-Coley-Robbins algorithm applied to these inputs yields

$$\mathcal{H}_{23}(X) = X^6 + (19 + O(23^2))\,X^5 - (50 + O(23^2))\,X^4 + (208 + O(23^2))\,X^3 \\ - (119 + O(23^2))\,X^2 - (252 + O(23^2))\,X - 231 + O(23^2).$$

Reducing the result modulo 23, we finally find that

$$h_{23}(X) = X^6 + 19\,X^5 + 19\,X^4 + X^3 + 19\,X^2 + X + 22.$$

A characteristic 2 example. Let $\mathbb{F}_{2^{10}} \simeq \mathbb{F}_2[t]/(t^{10} + t^6 + t^5 + t^3 + t^2 + t + 1)$ and E be the elliptic curve $y^2 + xy = x^3 + t^{457}$. We are looking for isogenies of degree 7.

A Weierstraß model isomorphic to E in $\mathbb{Q}_{2^{10}}$ is given at precision 25 by

$$\mathcal{E} : y^2 = x^3 - (27 + O(2^{25}))x + (2\,(23328\,t^9 + 23328\,t^5 + 23328\,t^2 + 23355) + O(2^{26}))$$

with $\lambda : (x, y) \mapsto ((9.2^2 + O(2^{27}))\,x + (3 + O(2^{25})), (27.2^3 + O(2^{28}))y + (27.2^2 + O(2^{27}))x + O(2^{27}))$. Atkin-Elkies' algorithms then enable us to find that $\mathcal{E}$ is 7-isogeneous to a curve approximated by

$$\tilde{\mathcal{E}} : y^2 = x^3 + (48432\,t^9 + 3072\,t^8 - 56864\,t^7 + 38944\,t^6 + 108896\,t^5 - 93264\,t^4 \\ + 9264\,t^3 - 38080\,t^2 + 608\,t - 114731 + O(2^{18}))\,x + ((27064\,t^9 - 5248\,t^8 - 18512\,t^7 \\ - 25712\,t^6 + 13520\,t^5 - 7016\,t^4 + 2328\,t^3 - 13056\,t^2 - 12816\,t - 8461)\,2 + O(2^{17})).$$

Similarly, we find that $p_1 = -8660\,t^9 + 9992\,t^8 + 9528\,t^7 - 31720\,t^6 + 14456\,t^5 + 20204\,t^4 - 21212\,t^3 + 26264\,t^2 - 3472\,t + 29477 + O(2^{16})$.

Charlap-Coley-Robbins algorithm applied to these inputs yields

$$\mathcal{H}_7(X) = X^3 + (8660\,t^9 - 9992\,t^8 - 9528\,t^7 + 31720\,t^6 - 14456\,t^5 - 20204\,t^4 \\ + 21212\,t^3 - 26264\,t^2 + 3472\,t - 29477 + O(2^{16}))\,X^2 + (-10232\,t^9 - 3440\,t^8 \\ + 9936\,t^7 + 576\,t^6 + 6896\,t^5 + 2216\,t^4 - 4456\,t^3 + 7360\,t^2 + 15872\,t \\ + 11907 + O(2^{15}))\,X + 6324\,t^9 + 11608\,t^8 + 200\,t^7 - 15592\,t^6 \\ + 4840\,t^5 + 4692\,t^4 + 15292\,t^3 - 104\,t^2 - 13584\,t + 6121 + O(2^{15}).$$

Applying then λ^{-1} and reducing the result modulo two, we finally find

$$h_7(X) = X^3 + t^{889}X^2 + t^{256}X + t^{591}.$$

4 Point counting on elliptic curves

Plugging `CCRLifted` in SEA yields an algorithm of asymptotic time complexity $\widetilde{O}((1+\log q/p)\log^4 q)$ and space complexity $O((1+\log q/p)\log^2 q)$. It is especially interesting when $p \simeq \log q$ because in this case we have an algorithm of time complexity $\widetilde{O}(\log^4 q)$ and space complexity $O(\log^2 q)$, which compares well with classical SEA complexities analysis (where either p or n is fixed).

We further compare this SEA algorithm to other efficient point counting algorithms which work for smaller p, that is SEA with second Couveignes finding isogeny algorithm, Satoh-Mestre and Kedlaya's approaches.

Couveignes' approach. The heart of second Couveignes' algorithm consists in computing an isomorphism between two towers of Artin-Schreier extensions. The complexity of this algorithm, for *varying* p, is at least the cost of computing an isomorphism between two Artin-Schreier extensions defined over $\mathbb{F}_q$. The classical way to solve this problem is to factor in one extension the defining polynomial of the other one, that is a polynomial of the form $X^p - X = \gamma$ with $\gamma \in \mathbb{F}_q$. Since $X^p - X$ is $\mathbb{F}_p$-linear, this may be done by precomputing the inverse of a $pn \times pn$ matrix defined over $\mathbb{F}_p$ (this already yields a $\widetilde{O}((pn)^\omega)$ time complexity with the Winograd constant ω greater than 2.3). Then, each isogeny kernel computation involves a matrix-vector multiplication by such a matrix, that is $\widetilde{O}((pn)^2)$ bit operations.

In the case $p \simeq \log q$, the corresponding SEA algorithm runs thus in $\widetilde{O}(\log^5 q)$ bit operations, which is larger than the complexity of our variation.

Satoh's and Mestre's approaches. Satoh [27] noticed first that the results of Lubin, Serre and Tate [24] lead to an algorithm which efficiently calculate the canonical lift of an elliptic curve defined in a finite field of small characteristic. It obtains an algorithm with time complexity $\widetilde{O}(p^2n^3)$ and space complexity $O(p^2n^2\log q)$. One year later, Vercauteren, Preneel and Vandewalle [36] reduce in the general case the space complexity down to $O(p^2n\log q)$.

During the same period, Mestre proposed an algorithm of an astonishing simplicity and nevertheless with the same complexity to calculate the cardinality of an elliptic curve in finite fields of characteristic two, the so-called AGM method [25]. A generalization have been performed by Carls [5] (another attempt is explored in [21]). This also yields algorithms of time complexity $\widetilde{O}(p^2n^3)$ and space complexity $O(p^2n\log q)$.

Further algorithmic improvements are due to Satoh-Skjernaa-Taguchi [29, 28], Lercier-Lubicz [23] and Harley [19]. As described in the most complete text on the subject [35, Chapter 3], the best algorithms among those run in $\widetilde{O}(p^2n^2)$ bit operations and requires a $O(p^2n^2)$ memory (one bottleneck is that we can not avoid the calculation of the p-torsion part of the curve and this involves the computation in the p-adics of the p-th division polynomial).

Thus, all algorithms in this family have the same time complexity and larger memory complexity than our SEA variation, in the case $p \simeq \log q$.

Kedlaya's approach. Kedlaya's algorithm [20] to count points on hyperelliptic curve as a function of both p and n has been studied in [16]. For elliptic curves, the complexity, both in time and space, is reported to be $\widetilde{O}(pn^3)$.

When $p \simeq \log q$, time complexity is the same as in our case but, again, space complexity is much larger.

Comparison summary. As a conclusion, all these algorithms have got at best the same time complexity as our SEA variation in the case $p \simeq \log q$ that we are considering. However, their memory requirements are much larger. Moreover, when time and memory requirements are comparable, as is the case here, memory is the bottleneck and the practical impact of our improvement is noteworthy.

5 Other applications

Besides point counting, some applications may take advantage of an "easy to implement" algorithm for isogeny computation. We give two examples below.

Improvements to the Weil descent. The Weil descent is a method that allows bringing back the discrete logarithm on elliptic curves defined over an extension $\mathbb{F}_{p^n}$ of a small finite field $\mathbb{F}_{p^m}$ to the discrete logarithm on a curve of larger genus defined over $\mathbb{F}_{p^m}$. It was initially proposed by Frey [13], deepened by Galbraith and Smart [15], then made effective by Gaudry, Hess and Smart [17].

Now, the hardness of performing the Weil descent varies between isogeneous curves. To improve the attack, being given a curve E, one may try to transport the discrete logarithm defined by E to an easier one on an isogeneous curve. This strategy was studied by Galbraith, Hess and Smart in [14].

Cryptographic protections against side-channel attacks. Side-channel attacks are a recent development of cryptanalysis, where one studies the precise physical behavior of cryptographic protocols and algorithms (execution times, electric consumption, ...) to recover keys or other secrets. Since their discovery in the 90's, they are considered as a serious threat.

Of course, the elliptic curve based cryptography, especially its point by scalar multiplication, does not escape these attacks. Some of very popular countermeasures were proposed by Coron [7]. Unfortunately, some of them were defeated by Goubin [18] that using the specific representation of some points on the considered curve, typically the points with zero x-coordinates. Nevertheless, it is possible to counter the corresponding attacks, as proposed by Smart [33], by replacing the known curve by an isogeneous random curve.

6 Conclusion

Lifting elliptic curves in the p-adics, we give a generalization of the easy to implement algorithm of Charlap, Coley and Robbins for finding isogenies. Our approach, can also be successfully applied to similar algorithms, for instance the isogeny finding algorithm given in [31] or more recently in [4]. An important consequence of these isogeny finding algorithms is to extend the scope of the SEA algorithm toward fields of smaller characteristic. In particular, in medium characteristic, this SEA variation turns out to be the most efficient point counting algorithm available at the present time.

References

[1] A.O.L. Atkin. The number of points on an elliptic curve modulo a prime, 1988. Email on the NMBRTHRY mailing list.

[2] A.O.L. Atkin. The number of points on an elliptic curve modulo a prime, 1992. Email on the NMBRTHRY mailing list.

[3] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma Algebra System I: The User Language. *J. Symbolic Comp.*, 24(3):235–265, 1997.

[4] A. Bostan, F. Morain, B. Salvy, and É Schost. Fast algorithms for computing isogenies between elliptic curves. Preprint, 2006.

[5] Robert Carls. *A Generalized Arithmetic Geometric Mean.* Doctoral these, Rijksuniversiteit Groningen, November 2004.

[6] H. Cohen. *A course in computational algebric number theory*, volume 138 of *Graduate Texts in Mathematics.* Springer Verlag, 1993.

[7] J.-S. Coron. Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems. In *CHES'99*, volume 1717 of *Lecture Notes in Computer Science*, pages 292–302, Berlin, 1999. Springer-Verlag.

[8] J.-M. Couveignes. *Quelques calculs en théorie des nombres.* Doctoral these, Université de Bordeaux I, July 1994.

[9] J.-M. Couveignes. Computing l-isogenies with the p-torsion. In H. Cohen, editor, *ANTS-II*, volume 1122 of *Lecture Notes in Computer Science*, pages 59–65. Springer-Verlag, 1996.

[10] J.-M. Couveignes. Isomorphisms between Artin-Schreier towers. *Mathematics of Computation*, 69(232):1625–1631, 2000.
[11] N.D. Elkies. Explicit isogenies. Preprint, 1991.
[12] N.D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational Perspectives On Number Theory*, volume 7 of *AMS/IP Stud. Adv. Math.* Amer. Math. Soc., Providence, RI, 1998.
[13] G. Frey. How to disguise an elliptic curve. Talk at ECC'98, 1998. Waterloo.
[14] S.D. Galbraith, F. Hess, and N.P. Smart. Extending the GHS Weil Descent Attack. In L. Knudsen, editor, *Advances in Cryptology — EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 29–44, Berlin, 2002. Springer.
[15] S.D. Galbraith and N.P. Smart. A Cryptographic application of Weil descent. In *Codes and Cryptography*, volume 1746 of *Lecture Notes in Computer Science*, pages 191–200, Berlin, 1999. Springer-Verlag.
[16] P. Gaudry and N. Gürel. Counting points in medium characteristic using Kedlaya's algorithm. *Experiment. Math.*, 12(4):395–402, 2003.
[17] P. Gaudry, F. Hesse, and N.P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *Journal of Cryptology*, 15:19–46, 2002.
[18] L. Goubin. A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems. In *PKC'2003*, volume 2567 of *Lecture Notes in Computer Science*, pages 199–211, Berlin, 2003. Springer-Verlag.
[19] R. Harley. *Algorithmes avancés pour l'arithmétique des courbes*. Doctoral these, Université Paris 7, 2002.
[20] K.S. Kedlaya. Counting points on hyperelliptic curves using Monsky Washnitzer cohomology. *Journal of the Ramanujan Mathematical Society*, 16:323–328, 2001.
[21] D. R. Kohel. The AGM-X0(N) Heegner point lifting algorithm and elliptic curve point counting. In Chi Sung Laih, editor, *Advances in Cryptology - Asiacrypt 2003*, volume 2894, pages 124–136. Springer, December 2003.
[22] R. Lercier. Computing isogenies in $\mathbf{F}_{2^n}$. In *Algorithmic number theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Computer Science*, pages 197–212. Springer, Berlin, 1996.
[23] R. Lercier and D. Lubicz. Counting Points on Elliptic Curves over Finite Fields of Small Characteristic in Quasi Quadratic Time. In E. Biham, editor, *Advances in Cryptology — EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 360–373, Berlin, May 2003. Springer.
[24] J. Lubin, J.-P. Serre, and J. Tate. Elliptic curves and formal groups. Available at *http://-/ma.utexas.edu/users/voloch/lst.html*, 1964.
[25] J.-F. Mestre. AGM pour le genre 1 et 2, 2001. Lettre à Gaudry et Harley. Available at *http://www.math.jussieu.fr/˜mestre*.
[26] F. Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *Journal de Theorie des nombres de Bordeaux*, 7:255–282, 1995.
[27] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.
[28] T. Satoh. On p-adic point counting algorithms for elliptic curves over finite fields. In C. Fieker and D.R. Kohel, editors, *Algorithmic Number Theory, 5th International Symposium, ANTS-V*, pages 43–66, Berlin, July 2002. Springer Verlag.
[29] T. Satoh, B. Skjernaa, and Y. Taguchi. Fast computation of canonical lifts of elliptic curves and its application to point counting. *Finite Fields and Their Applications*, 9(1):89–101, 2003.
[30] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44:483–494, 1985.
[31] R. Schoof. Counting points on elliptic curves over finite fields. *Journal de Theorie des nombres de Bordeaux*, 7:219–254, 1995. Available at *http://www.cirm.univ-mrs.fr/EMIS/journals/JTNB/*.
[32] J.H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.
[33] N.P. Smart. An Analysis of Goubin's Refined Power Analysis Attack. In *CHES'2003*, volume 2779 of *Lecture Notes in Computer Science*, pages 281–290, Berlin, 2003. Springer-Verlag.
[34] J. Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences de Paris*, 273:238–241, 1971. Série A.
[35] F. Vercauteren. *Computing Zeta Functions of Curves over Finite Fields*. Doctoral these, Katholieke Universiteit Leuven, November 2003.
[36] F. Vercauteren, B. Preneel, and J. Vandewalle. A memory efficient version of Satoh's algorithm. In *Advances in Cryptology — EUROCRYPT 2001 (Innsbruck)*, volume 2045 of *Lecture Notes in Comput. Sci.*, pages 1–13. Springer, Berlin, 2001.