

An Extension of Kedlaya's Algorithm to Artin-Schreier Curves in Characteristic 2

Jan Denef¹ and Frederik Vercauteren^{2,3,*}

¹ Department of Mathematics
University of Leuven

Celestijnenlaan 200B, B-3001 Leuven-Heverlee, Belgium

`jan.denef@wis.kuleuven.ac.be`

² Department of Electrical Engineering
University of Leuven

Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium

`frederik.vercauteren@esat.kuleuven.ac.be`

³ Computer Science Department
University of Bristol

Woodland Road, Bristol BS8 1UB, United Kingdom

`frederik@cs.bris.ac.uk`

Abstract. In this paper we present an extension of Kedlaya's algorithm for computing the zeta function of an Artin-Schreier curve over a finite field \mathbb{F}_q of characteristic 2. The algorithm has running time $O(g^{5+\varepsilon} \log^{3+\varepsilon} q)$ and needs $O(g^3 \log^3 q)$ storage space for a genus g curve. Our first implementation in MAGMA shows that one can now generate hyperelliptic curves suitable for cryptography in reasonable time. We also compare our algorithm with an algorithm by Lauder and Wan which has the same time and space complexity. Furthermore, the method introduced in this paper can be used for any hyperelliptic curve over a finite field of characteristic 2.

Keywords: Hyperelliptic curves, Monsky-Washnitzer cohomology, Kedlaya's algorithm, Lauder & Wan algorithm, cryptography

1 Introduction

Computing the zeta function of abelian varieties over finite fields is one of the most important problems in computational algebraic geometry and has many applications [24], e.g. the construction of cryptosystems based on Jacobians of curves. The most important systems use elliptic curves as introduced by Miller [18] and Koblitz [13] or hyperelliptic curves which were proposed by Koblitz [14]. More general, but less practical systems work in the Jacobian of superelliptic curves [9] and of \mathcal{C}_{ab} curves [1].

* F.W.O. research assistant, sponsored by the Fund for Scientific Research - Flanders (Belgium).

The problem of counting the number of points on elliptic curves over finite fields of any characteristic can be solved in polynomial time using Schoof's algorithm [26] and its improvements due to Atkin [2] and Elkies [6]. An excellent account of the resulting SEA-algorithm can be found in [3] and [17]. For finite fields of small characteristic, Satoh [25] described an algorithm based on p -adic methods which is asymptotically faster than the SEA-algorithm. Skjernaa [27] and Fouquet, Gaudry and Harley [8] extended the algorithm to characteristic 2 and Vercauteren [29] presented a memory efficient version. Recently Mestre and Harley proposed a variant of Satoh's algorithm based on the Arithmetic-Geometric Mean, which has the same asymptotic behaviour as [29], but is faster by some constant.

The equivalent problem for higher genus curves seems to be much more difficult. Pila [23] described a theoretical generalisation of Schoof's approach, but the algorithm is not practical, not even for genus 2 as shown by Gaudry and Harley [11]. An extension of Satoh's method to higher genus curves needs the Serre-Tate canonical lift of the Jacobian of the curve, which need not be a Jacobian itself and thus is difficult to compute with. The AGM method does generalise to hyperelliptic curves, but currently only the genus 2 case is practical.

Recently Kedlaya [12] described a p -adic algorithm to compute the zeta function of hyperelliptic curves over finite fields of small *odd* characteristic, using the theory of Monsky-Washnitzer cohomology. The running time of the algorithm is $O(g^{5+\varepsilon} \log^{3+\varepsilon} q)$ for a hyperelliptic curve of genus g . The algorithm readily generalises to superelliptic curves as shown by Gaudry and Gurel [10]. A related approach by Lauder and Wan [15] is based on Dwork's proof of the rationality of the zeta function and leads to a polynomial time algorithm for computing the zeta function of an arbitrary variety over a finite field. Despite its polynomial complexity, the algorithm in its most general form is not practical. Using Dwork cohomology, Lauder and Wan [16] adapted their original algorithm for the special case of Artin-Schreier curves, resulting in an $O(g^{5+\varepsilon} \log^{3+\varepsilon} q)$ time algorithm.

In this paper we extend Kedlaya's algorithm to Artin-Schreier curves defined by an equation of the form $y^2 - x^m y - f(x) = 0$ over some finite field \mathbb{F}_q of characteristic 2. The resulting algorithm has running time $O(g^{5+\varepsilon} \log^{3+\varepsilon} q)$ and needs $O(g^3 \log^3 q)$ storage space for a genus g curve. We have implemented our algorithm as well as Lauder & Wan's algorithm in the MAGMA computer algebra system and present a comparison of the efficiency of both algorithms.

Finally we remark that using the ideas introduced in this paper, we recently extended Kedlaya's algorithm to *all* hyperelliptic curves defined over a finite field of characteristic 2. More details can be found in the forthcoming paper [5].

The remainder of the paper is organised as follows: after recalling the formalism of Monsky-Washnitzer cohomology in Section 2, we show in Section 3 how to extend Kedlaya's algorithm to the aforementioned Artin-Schreier curves. Section 4 contains a ready to implement description of the resulting algorithm. In Section 5, we present running times of an implementation of both algorithms in MAGMA and compare their efficiency.

2 Monsky-Washnitzer Cohomology

In this section we briefly recall the definition and main properties of Monsky-Washnitzer cohomology. More details can be found in the seminal papers by Monsky and Washnitzer [19,20,21], the lectures by Monsky [22] and the survey by van der Put [28].

Let \overline{X} be a smooth affine variety over a finite field $k := \mathbb{F}_q$ with coordinate ring \overline{A} . Let R denote a complete discrete valuation ring with uniformizer π , residue field $R/\pi R = k$ and fraction field K of characteristic 0. Elkik [7] showed that one can always find a smooth finitely generated R -algebra A such that $A/\pi A \cong \overline{A}$. To compute the zeta function of \overline{X} one needs to lift the Frobenius endomorphism \overline{F} on \overline{A} to the R -algebra A , but in general this is not possible. Note that for elliptic curves, Satoh solves this problem by using the Serre-Tate canonical lift which does admit a lift of the Frobenius endomorphism. To remedy this difficulty one could work with the π -adic completion A^∞ of A . But again we run into difficulties since the de Rham cohomology of A^∞ is larger than that of A . As an example, consider the affine line over \mathbb{F}_p , so $A = R[x]$, then each term in $\sum_{n=0}^\infty p^n x^{p^n-1} dx$ is an exact differential form, but its sum is not, since $\sum_{n=0}^\infty x^{p^n}$ is not in A^∞ . The fundamental problem is that the series $\sum_0^\infty p^n x^{p^n-1}$ does not converge fast enough for its integral to converge as well. Monsky and Washnitzer solve this problem by working with a subalgebra A^\dagger of A^∞ , whose elements satisfy growth conditions. This *dagger ring* or *weak completion* A^\dagger is defined as follows: write $A := R[x_1, \dots, x_n]/(f_1, \dots, f_m)$, then

$$A^\dagger := R\langle x_1, \dots, x_n \rangle^\dagger / (f_1, \dots, f_m),$$

where $R\langle x_1, \dots, x_n \rangle^\dagger$ consists of power series

$$\left\{ \sum a_\alpha x^\alpha \in R[[x_1, \dots, x_n]] \mid \exists C, \rho \in \mathbb{R}, C > 0, 0 < \rho < 1, \forall \alpha : |a_\alpha| \leq C \rho^{|\alpha|} \right\},$$

where $\alpha := (\alpha_1, \dots, \alpha_n)$, $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $|\alpha| := \sum_{i=0}^n \alpha_i$. Equivalently, $R\langle x_1, \dots, x_n \rangle^\dagger$ can be defined as the set of overconvergent power series, i.e. elements of $R[[x_1, \dots, x_n]]$ which converge in a polydisc

$$\{(x_1, \dots, x_n) \in K^n \mid |x_1| \leq \rho_1, \dots, |x_n| \leq \rho_n\}$$

with all $\rho_i > 1$. The ring A^\dagger clearly satisfies $A^\dagger/\pi A^\dagger = \overline{A}$, is weakly complete, i.e. is equal to its weak completion and is flat over R . A finitely generated algebra which satisfies these three properties is called a *lift* of \overline{A} . One can show that if \overline{A} is smooth and finitely generated, there always exists a lift A^\dagger of \overline{A} and that every lift of \overline{A} is R -isomorphic to A^\dagger . Furthermore, let \overline{B}/k be smooth and finitely generated, with lift B^\dagger and let $g : \overline{A} \rightarrow \overline{B}$ be a morphism of k -algebra's, then there exists an R -homomorphism $G : A^\dagger \rightarrow B^\dagger$ lifting g . The last property implies that we can lift the q -power Frobenius from \overline{A} to A^\dagger .

For A^\dagger we can define the universal module $D^1(A^\dagger)$ of differentials

$$D^1(A^\dagger) := (A^\dagger dx_1 + \dots + A^\dagger dx_n) / \left(\sum_{i=1}^m A^\dagger \left(\frac{\partial f_i}{\partial x_1} dx_1 + \dots + \frac{\partial f_i}{\partial x_n} dx_n \right) \right).$$

Let $D^i(A^\dagger) := \bigwedge^i D^1(A^\dagger)$ be the i -th exterior product of $D^1(A^\dagger)$ and denote with $d_i : D^i(A^\dagger) \rightarrow D^{i+1}(A^\dagger)$ the exterior differentiation. Since $d_{i+1} \circ d_i = 0$ we get the de Rham complex $D(A^\dagger)$

$$0 \longrightarrow D^0(A^\dagger) \xrightarrow{d_0} D^1(A^\dagger) \xrightarrow{d_1} D^2(A^\dagger) \xrightarrow{d_2} D^3(A^\dagger) \dots$$

The i -th cohomology group of $D(A^\dagger)$ is defined as $H^i(\overline{A}/R) := \text{Ker } d_i / \text{Im } d_{i-1}$ and $H^i(\overline{A}/K) := H^i(\overline{A}/R) \otimes_R K$ finally defines the i -th Monsky-Washnitzer cohomology group. One can prove that for smooth, finitely generated k -algebra's \overline{A} the map $\overline{A} \mapsto H^\bullet(\overline{A}/K)$ is well defined and functorial, which justifies the notation. Let F be a lift of the q -power Frobenius endomorphism of \overline{A} to A^\dagger , then F induces an endomorphism F_* on the cohomology groups. The main theorem of Monsky-Washnitzer cohomology is that the $H^i(\overline{A}/K)$ satisfy a Lefschetz fixed point formula.

Theorem 1 (Lefschetz fixed point formula). *Let $\overline{X}/\mathbb{F}_q$ be a smooth affine variety of dimension n , then the number of \mathbb{F}_q -rational points on \overline{X} equals*

$$\sum_{i=0}^n (-1)^i \text{Tr} (q^n F_*^{-1} | H^i(\overline{A}/K)).$$

3 Cohomology of Artin-Schreier Curves over \mathbb{F}_{2^n}

Let \mathbb{F}_q be a finite field with $q = 2^n$ elements and fix an algebraic closure $\overline{\mathbb{F}}_q$. Let K be a degree n unramified extension of \mathbb{Q}_2 and let R be its valuation ring with residue field $R/2R = \mathbb{F}_q$. The Artin-Schreier curves we will consider are defined by an affine equation of the form

$$\overline{C}_{m,\overline{f}} : y^2 - x^m y - \overline{f}(x) = 0, \tag{1}$$

with $0 \leq m \leq g$, $\overline{f} \in \mathbb{F}_q[x]$ monic of degree $2g + 1$ and such that $\overline{C}_{m,\overline{f}}$ is non-singular. Let $\mathfrak{p} : \overline{C}_{m,\overline{f}}(\overline{\mathbb{F}}_q) \rightarrow \mathbb{A}^1(\overline{\mathbb{F}}_q)$ be the projection map on the x -axis, then the branch locus of \mathfrak{p} is empty if and only if $m = 0$ and consists of the singleton $\{0\}$ if and only if $m > 0$. Without loss of generality we may assume that $f(0) = 0$ if $m > 0$, i.e. that $(0, 0)$ is the unique ramification point of \mathfrak{p} . Indeed, the isomorphism defined by $x \mapsto x$ and $y \mapsto y + \overline{f}(0)^{1/2}$ shows that we can replace $\overline{f}(x)$ with $\overline{f}(x) - \overline{f}(0) + x^m \overline{f}(0)^{1/2}$, which clearly is divisible by x if $m > 0$. Note that since $\overline{C}_{m,\overline{f}}$ is non-singular we have $\overline{f}'(0) \neq 0$.

Let $\overline{H}_m(x)$ be defined as $\overline{H}_0(x) := 1$ and $\overline{H}_m(x) := x$ for $m > 0$, i.e. $\overline{H}_m(\theta)$ is zero if and only if the point with x -coordinate θ ramifies. Let $\overline{C}'_{m,\overline{f}}$ be the curve obtained from $\overline{C}_{m,\overline{f}}$ by deleting the support of $\overline{H}_m(x)$. Then the coordinate ring of $\overline{C}'_{m,\overline{f}}$ is given by $\overline{A}_{m,\overline{f}} := R[x, y, (\overline{H}_m(x))^{-1}] / (y^2 - x^m y - \overline{f}(x))$.

Take any lift $f \in R[x]$ of \overline{f} , with the restrictions that f should be monic and of degree $2g + 1$ and that $f(0) = 0$ for $m > 0$. Let $H_0(x) := 1$ and $H_m(x) := x$ for

$m > 0$ and let $C'_{m,f}$ be the curve obtained from $C_{m,f} : y^2 - x^m y - f(x) = 0$ by deleting the support of $H_m(x)$. Note that the point $(0, 0)$ still is a ramification point on $C_{m,f}$, which explains why we need the extra restriction on f if $m > 0$. The coordinate ring of $C'_{m,f}$ is $A_{m,f} := R[x, y, (H_m(x))^{-1}]/(y^2 - x^m y - f(x))$ and there exists an involution ι on $A_{m,f}$ which sends x to x and y to $-y + x^m$.

Let $A_{m,f}^\dagger$ be the dagger ring of $A_{m,f}$. Using the equation of the curve we can always represent elements of $A_{m,f}^\dagger$ as a series $\sum_{l=-\infty}^{+\infty} (a_l + b_l y)x^l$ with $a_l, b_l \in R$. If $m = 0$ then all a_l, b_l with $l < 0$ are zero. Furthermore, the growth condition implies that there exists some real numbers δ and $\epsilon > 0$ such that $v_2(a_l) \geq \epsilon \cdot |l| + \delta$ and $v_2(b_l) \geq \epsilon \cdot |l + 1| + \delta$.

Lift the p -power Frobenius $\bar{\sigma}$ on \mathbb{F}_q to the Frobenius substitution σ on R . We extend σ to an endomorphism of $A_{m,f}^\dagger$ by mapping x to x^2 and y to y^σ , with

$$(y^\sigma)^2 - x^{2m}y^\sigma - f(x)^\sigma = 0 \text{ and } y^\sigma \equiv y^2 \pmod{2}.$$

Using Newton iteration we can compute the solution to the above equations as an element of the 2-adic completion of $A_{m,f}$, but it is not immediately clear that there exists a solution in $A_{m,f}^\dagger$. The existence of such a solution follows immediately from a theorem by Bosch [4], but since we need an explicit estimate of the rate of convergence, we prove the following lemma.

Lemma 1. *For $k \geq 1$, let $W_k(x, y) := \sum_{l=-L_k}^{A_k} a_l x^l + \sum_{l=-L_k}^{B_k} b_l x^l y \in A_{m,f}$ satisfy*

$$W_k(x, y)^2 - x^{2m}W_k(x, y) - f(x)^\sigma \equiv 0 \pmod{2^k} \text{ and } W_k(x, y) \equiv y^2 \pmod{2}$$

with $a_{A_k} \neq 0, b_{B_k} \neq 0, a_{-L_k} \neq 0$ or $b_{-L_k} \neq 0$ and such that $a_l = 0$ or $v_2(a_l) < k$ for $-L_k \leq l \leq A_k$ and $b_l = 0$ or $v_2(b_l) < k$ for $-L_k \leq l \leq B_k$. Then the degrees A_k, B_k and L_k can be bounded for $k \geq 2$ as

$$\begin{aligned} A_k &\leq 2(k-1)(\deg f - 2m) + 2m, \\ B_k &\leq 2(k-2)(\deg f - 2m) + \deg f - m, \\ L_k &\leq 2(k-1)(2m) - 2m. \end{aligned} \tag{2}$$

Proof: An easy calculation shows that $W_1(x, y) = f(x) + x^m y$ and

$$W_2(x, y) = \frac{(f(x)^2 - f(x)^\sigma) + x^{2m}f(x)}{x^{2m}} + y \frac{2x^m f(x) + x^{3m}}{x^{2m}},$$

so that W_2 indeed satisfies the lemma.

Newton iteration on $Y^2 - x^{2m}Y - f(x)^\sigma = 0$ gives

$$W_{k+1} \equiv W_k - \frac{W_k^2 - x^{2m}W_k - f(x)^\sigma}{2W_k - x^{2m}} \pmod{2^{k+1}} \equiv \frac{W_k^2 - f(x)^\sigma}{x^{2m}} \pmod{2^{k+1}}.$$

Let $\alpha_k(x) := \sum_{l=-L_k}^{A_k} a_l x^l, \beta_k(x) := \sum_{l=-L_k}^{B_k} b_l x^l$ such that $W_k = \alpha_k + \beta_k y$. Note that $W_k \equiv W_{k-1} \pmod{2^{k-1}}$, so we can define

$$\Delta_{\alpha,k}(x) := \frac{\alpha_k(x) - \alpha_{k-1}(x)}{2^{k-1}} \quad \text{and} \quad \Delta_{\beta,k}(x) := \frac{\beta_k(x) - \beta_{k-1}(x)}{2^{k-1}},$$

for $k \geq 1$ with $\Delta_{\alpha,0}(x) := \Delta_{\beta,0}(x) := 0$. It is clear that W_k can be written as

$$W_k = \Delta_{\alpha,1} + 2\Delta_{\alpha,2} + \cdots + 2^{k-1}\Delta_{\alpha,k} + y (\Delta_{\beta,1} + 2\Delta_{\beta,2} + \cdots + 2^{k-1}\Delta_{\beta,k}).$$

Plugging this into the Newton iteration gives the following equation

$$x^{2m}W_{k+1} \equiv \sum_{\substack{1 \leq i < j \\ i+j-1 < k+1}} 2^{i+j-1} (\Delta_{\alpha,i}\Delta_{\alpha,j} + (f(x) + x^m y) \Delta_{\beta,i}\Delta_{\beta,j}) - f(x)^\sigma + y \sum_{i+j-1 < k+1} 2^{i+j-1} \Delta_{\alpha,i}\Delta_{\beta,j} + \sum_{2(i-1) < k+1} 2^{2(i-1)} (\Delta_{\alpha,i}^2 + (f(x) + x^m y)\Delta_{\beta,i}^2) \pmod{2^{k+1}}.$$

Since $\deg \Delta_{\alpha,i} \leq A_i$ and $\deg \Delta_{\beta,i} \leq B_i$, we get that A_{k+1} is less or equal than

$$\max \left(\deg f^\sigma, \max_{i+j < k+2} (A_i + A_j, B_i + B_j + \deg f), \max_{2i < k+3} (2A_i, 2B_i + \deg f) \right) - 2m.$$

Using the bounds given in (2) for A_i and B_i we see that A_{k+1} also satisfies the bounds (2). Note that we have to take into account the values for $\deg \Delta_{\alpha_1} = \deg f$ and $\deg \Delta_{\beta_1} = m$ since these do not satisfy the bounds (2), but this does not cause any problems. A similar reasoning for B_{k+1} and L_{k+1} shows that these also satisfy the given bounds. □ **Remark.** If we want to compute

an approximation $W_N(x, y)$ of y^σ modulo 2^N for a certain precision N , then the total degree $A_N + L_N$ of the Laurent polynomials is bounded by $2(N - 1) \deg f$.

The above lemma indeed shows that we can lift the q -power Frobenius \overline{F} to an endomorphism F on the dagger ring $A_{m,f}^\dagger$; it suffices to take $F := \sigma^n$. Before we can actually compute the zeta function using the Lefschetz fixed point theorem, we need to determine a basis of the K -vectorspace $H^1(\overline{A}_{m,\overline{f}}/K)$.

We first prove that $x^i y dx$ with $i = 0, \dots, 2g - 1$, and $\frac{dx}{x}$ if $m > 0$, form a basis for the algebraic de Rham cohomology $H_{DR}^1(A_{m,f}/K)$ of $A_{m,f}$. The extra $\frac{dx}{x}$ for $m > 0$ is caused by the fact that we removed the point $(0, 0)$ from the curve $C_{m,f}$. Every element of $H_{DR}^1(A_{m,f}/K)$ can be written as a linear combination of differentials of the form $x^k y^l dx, x^k y^l dy$ with $k \in \mathbb{Z}, l \in \mathbb{N}$ and $k \geq 0$ if $m = 0$. Using the equation of the curve, we can reduce to the case $l = 0$ or 1 . Since $d(x^k y)$ and $d(x^k y^2)$ are exact, we conclude that $H_{DR}^1(A_{m,f}/K)$ is generated by differentials of the form $x^i y dx$ with $i \in \mathbb{Z}$ ($i \in \mathbb{N}$ for $m = 0$) and $\frac{dx}{x}$ if $m > 0$.

Rewriting the equation of the curve as $(2y - x^m)^2 = 4f + x^{2m}$ and differentiating gives the equality $(2y - x^m) d(2y - x^m) = (2f' + mx^{2m-1}) dx$. For all $k > 0$ we therefore have

$$\begin{aligned} x^k(2f' + mx^{2m-1})(2y - x^m) dx &= x^k(2y - x^m)^2 d(2y - x^m) \\ &\equiv -\frac{k}{3}x^{k-1}(2y - x^m)^3 dx \\ &= -\frac{k}{3}x^{k-1}(4f + x^{2m})(2y - x^m) dx, \end{aligned} \tag{3}$$

where \equiv means equality modulo exact differentials. Thus we conclude that $[x^k(2f' + mx^{2m-1}) + \frac{k}{3}x^{k-1}(4f + x^{2m})] y dx$ is exact. The polynomial between brackets has degree $2g + k$ and non-zero leading coefficient $2(2g + 1) + 4\frac{k}{3} \neq 0$. A similar argument for $k = 0$ shows that $(2f' + mx^{2m-1})y dx$ is exact and clearly has degree $2g$ in x . With these formulae we can express $x^{2g+k}y dx$ for $k \geq 0$ as a linear combination of $x^i y dx$ with $0 \leq i < 2g$.

For $m > 0$ and $k < 0$ the formulae 3 are still valid, but now the conclusion is that $[x^k(2f' + mx^{2m-1}) + \frac{k}{3}x^{k-1}(4f + x^{2m})] y dx + \beta \frac{dx}{x}$ is exact for some suitable element $\beta \in K$. The Laurent polynomial between brackets has valuation at zero k , since $f(0) = 0$, but $f'(0) \neq 0$. The term x^k has coefficient $2f'(0)(1 + \frac{2k}{3})$ which clearly is different from zero, since $f'(0) \neq 0$. Therefore we can express all differentials of the form $x^k y dx$ with $k < 0$ as a linear combination of $x^i y dx$ for $i = 0, \dots, 2g - 1$ and $\frac{dx}{x}$ if $m > 0$.

A consequence of Lemma 3 will be that all these differential forms are linear independent and thus form a basis for the algebraic de Rham cohomology $H^1_{DR}(A_{m,f}/K)$. To show that this is also a basis of the Monsky-Washnitzer cohomology $H^1(\overline{A}_{m,\overline{f}}/K)$, we need to bound the denominators which are introduced during the reduction process. Therefore we prove the following two lemmata.

Lemma 2. *Let $A := R[x, y]/(y^2 - x^m y - f(x))$ and suppose that*

$$x^r y dx = \sum_{i=0}^{2g-1} a_i x^i y dx + ds, \tag{4}$$

with $r \in \mathbb{N}$, $a_i \in K$ and $s \in A \otimes K$. Then $2^c a_i \in R$, $2^{c'} s - \beta \in A$, where $c = 3 + \lfloor \log_2(r + g + 1) \rfloor$, $c' = 1 + c + \lfloor \log_2(2g + m) \rfloor$ and β some suitable element in K .

Proof: The proof has two distinct parts. The first part is similar to Kedlaya's argument in [12, Lemma 3], and is based on a local analysis around the point at infinity of the curve $C_{m,f}$. Put $t = x^g/y$, then one easily verifies that

$$x = t^{-2} \left(1 + \sum_{j=1}^{\infty} \alpha_j t^j \right), y = t^{-2g-1} \left(1 + \sum_{j=1}^{\infty} \beta_j t^j \right), \tag{5}$$

with $\alpha_j, \beta_j \in R$. To see this, put $z = 1/x$, rewrite the equation of the curve $C_{m,f}$ as $z - z^{g-m+1} - t^2 z^{2g+1} f(1/z) = 0$ and write z as a power series in t using Newton iteration. The relation (4) can be rewritten as

$$2^{c-1} x^r (2y - x^m) dx = \sum_{i=0}^{2g-1} 2^{c-1} a_i x^i (2y - x^m) dx + dS, \tag{6}$$

with $S \in A \otimes K$. Considering the involution of A which sends x to x and $2y - x^m$ to $-(2y - x^m)$, we see that we can write $S = \sum_{i=0}^N A_i x^i (2y - x^m)$, with N big enough and $A_i \in K$. This yields

$$2^{c-1} x^r (2y - x^m) dx - \sum_{i=0}^{2g-1} 2^{c-1} a_i x^i (2y - x^m) dx = d \left(\sum_{i=0}^N A_i x^i (2y - x^m) \right). \tag{7}$$

In the above equation we express x and y in terms of t using equalities (5). Since $x^i y = t^{-2i-2g-1} + \dots$, we get $x^i(2y - x^m) dx = (-4t^{-2i-2g-4} + \dots) dt$, which yields

$$2^{c-1} \sum_{j=-\max(2r+2g+4, 6g+2)} \gamma_j t^j dt = d \left(\sum_{i=0}^N 2A_i(t^{-2i-2g-1} + \dots) - A_i(t^{-2i-2m} + \dots) \right),$$

with $\gamma_j \in K$ for all j and $\gamma_j \in R$ when $j < -2(2g - 1) - 2g - 4 = -6g - 2$. Integrating with respect to t and dividing by 2 gives

$$\sum_{j \geq -\max(2r+2g+3, 6g+1)} \gamma'_j t^j = \sum_{i=0}^N A_i(t^{-2i-2g-1} + \dots) - \sum_{i=0}^N \frac{A_i}{2}(t^{-2i-2m} + \dots), \tag{8}$$

with $\gamma'_j \in K$ for all j and $\gamma'_j \in R$ when $j < -6g - 1$. Indeed the integration process introduces denominators which become integral after multiplication with $2^{\lfloor \log(2r+2g+2) \rfloor} = 2^{c-2}$ if $r \geq 2g - 1$. A first consequence of (8) is that $A_i = 0$ for all $i > \max(r + 1, 2g)$. We claim that (8) implies that $A_i \in R$ for all $i > 2g$. Suppose the claim is false. Then let i_0 be the largest integer with $i_0 > 2g$ and $A_{i_0} \notin R$. Note that $-2i_0 - 2g - 1 < -6g - 1$, since $i_0 > 2g$. Hence the monomials in the left hand side of (8) with degree $\leq -2i_0 - 2g - 1$ have coefficients in R . Moreover the monomials of degree $< -2i_0 - 2g - 1$, in the first sum in the right hand side of (8) also have coefficients in R , but this is false for the monomial of degree $-2i_0 - 2g - 1$. Hence the second sum in the right hand side of (8) contains a monomial of degree $-2i_0 - 2g - 1$ whose coefficient is not in R . That means that there is a maximal i_1 with $A_{i_1}/2 \notin R$ and $-2i_1 - 2m \leq -2i_0 - 2g - 1$. Because of parity we have that $-2i_1 - 2m < -2i_0 - 2g - 1$. Hence the right hand side of (8) contains a monomial of degree $-2i_1 - 2m < -2i_0 - 2g - 1$ whose coefficient is not in R . But this contradicts what we said about the left hand side. This finishes the claim that $A_i \in R$ for all $i > 2g$.

We now turn to the second part of the proof. Note that $(2y - x^m)^2 = v(x)$ with $v(x) := 4f + x^{2m}$. Moreover, $d(2y - x^m) = \frac{w(x)}{2y-x^m} dx$, where $w(x) := 2f' + mx^{2m-1}$. We will use these formulae to deduce from (7) a relation which does not involve y . For this purpose we multiply (7) with $\frac{2y-x^m}{dx} = \frac{w(x)}{d(2y-x^m)}$ obtaining

$$2^{c-1} x^r v(x) - \sum_{i=0}^{2g-1} 2^{c-1} a_i x^i v(x) = \sum_{i=0}^N A_i i x^{i-1} v(x) + \sum_{i=0}^N A_i x^i w(x).$$

We rewrite this in the form

$$\left(\sum_{i=0}^{2g-1} 2^{c-1} a_i x^i \right) v(x) + \left(\sum_{i=0}^{2g} A_i i x^{i-1} \right) v(x) + \left(\sum_{i=0}^{2g} A_i x^i \right) w(x) = F(x), \tag{9}$$

where

$$F(x) := 2^{c-1} x^r v(x) - \sum_{i=2g+1}^N A_i i x^{i-1} v(x) - \sum_{i=2g+1}^N A_i x^i w(x) \tag{10}$$

is a polynomial over R , since $A_i \in R$ for all $i > 2g$. To get rid of the disturbing factor 2 in the definition of $w(x)$, we consider $u(x) := \frac{1}{2}(xw(x) - mv(x)) = xf' - 2mf$. We rewrite (9) in such a way that $w(x)$ gets replaced by $u(x)$:

$$\left(\sum_{i=0}^{2g} (2^{c-1}a_{i-1} + iA_i + mA_i)x^i \right) v(x) + \left(\sum_{i=0}^{2g} 2A_i x^i \right) u(x) = xF(x), \quad (11)$$

with the convention that $a_{-1} = 0$. We consider (11) as a linear system of $4g + 2$ equations in the unknowns $2^{c-1}a_{i-1} + iA_i + mA_i$ and $2A_i$ for $i = 0, \dots, 2g$. The determinant of this system is the resultant $\text{Res}(v, u)$ of u and v , because $\deg v(x) = \deg u(x) = 2g + 1$. Since the leading coefficient of u is a unit, we have $\text{Res}(u, v) = \text{unit} \cdot \prod_{u(\theta)=0} v(\theta)$, where θ ranges over all roots of u in the algebraic closure of K . All these roots θ have non-negative valuation.

Suppose first that $m = 0$. Then $\text{Res}(u, v)$ is a unit in R since $v(\theta) = 4f(\theta) + 1$ is a unit for each root θ of u . The determinant of the system being a unit, we conclude that $2A_i$ and $2^{c-1}a_{i-1} + iA_i + mA_i$ are in R for $i = 0, \dots, 2g$. Hence $2^c a_i \in R$ and $2S \in A$. So for $m = 0$ the lemma then follows directly from (6).

Suppose now that $m \geq 1$. The restrictions on f imply that $f(0) = 0$ and $f'(0) \not\equiv 0 \pmod{2}$. Hence 0 is a common zero of u and v and $\text{Res}(u, v) = 0$. From (10) it follows that $F(0) = 0$, hence $A_0 = 0$ by (9), since $w(0) = 2f'(0) \neq 0$. We now consider (11) divided by x^2 as a linear system of $4g$ equations in the unknowns $2^{c-1}a_{i-1} + iA_i + mA_i$ and $2A_i$ for $i = 1, \dots, 2g$. The determinant of this system is the resultant $\text{Res}(\frac{v}{x}, \frac{u}{x})$. Let θ be a root of $u/x = f'(x) - 2mf(x)/x$, then θ has valuation zero since $f'(0) \not\equiv 0 \pmod{2}$. Hence $v(\theta) = 4f(\theta) + \theta^{2m}$ is a unit. Thus $\text{Res}(\frac{v}{x}, \frac{u}{x})$ is a unit and both $2A_i$ and $2^{c-1}a_{i-1} + iA_i + mA_i$ are in R for $i = 1, \dots, 2g$. We now continue as in the case $m = 0$. This ends the proof of the lemma. □

Remark. Lemma 2 remains valid when we replace $\sum_{i=0}^{2g-1}$ by $\sum_{i=\kappa}^{2g-1+\kappa}$ whenever $r \geq \kappa \in \mathbb{N}$. The proof is the same, except that we also have to show that $A_i = 0$ for all $i < \kappa$. This follows from (7) by a local analysis at a point on the curve with $x = 0$.

Lemma 3. *With the above notation and $m > 0$, suppose that*

$$x^{-r}y \, dx = \sum_{i=0}^{2g-1} a_i x^i y \, dx + b \frac{dx}{x} + ds, \quad (12)$$

where $r \in \mathbb{N}$, $a_i, b \in K$ and $s \in A_{m,f} \otimes K$. Then $2^c a_i \in R$, $2^{c'} b \in R$, $2^{c'} s - \beta \in A_{m,f}$, with $c = 3 + \lfloor \log_2(r + 1) \rfloor$, $c' = 1 + c + \lfloor \log_2(2g + m) \rfloor$ and $\beta \in K$.

Remark. Actually one can take $c = 3 + \lfloor \log_2(r - 2) \rfloor$ when $r \geq 3$ and $c = 0$ when $0 \leq r \leq 2$.

Proof: The proof again consists of two distinct parts. The first part is similar to Kedlaya’s argument in [12, Lemma 2] and is based on a local analysis around the ramification point $(0, 0)$ on the curve. In the completion of the local ring of

the curve at $(0, 0)$ we can write

$$x = \gamma_2 y^2 + \sum_{j \geq 3} \gamma_j y^j, \tag{13}$$

with $\gamma_j \in R$ and γ_2 a unit in R . Indeed, to see this use the equation of the curve and the conditions $f(0) = 0, f'(0) \not\equiv 0 \pmod{2}$, to express x as a power series in y using Newton iteration.

Considering the involution as in the proof of Lemma 2, we can transform relation (12) to the form

$$2^{c-1} x^{-r} (2y - x^m) dx - \sum_{i=0}^{2g-1} 2^{c-1} a_i x^i (2y - x^m) dx = d \left(\sum_{i=-N}^M A_i x^i (2y - x^m) \right),$$

with N and M large enough integers. Using the expansion at infinity given by the formulae (5) in the proof of Lemma 2 and substituting them in the above equation, one verifies that we can take $M = 2g$.

Expressing x in terms of y using (13) and dividing by 2 we obtain

$$2^{c-2} \sum_{j \geq -2r+2} \gamma'_j y^j dy = d \left(\sum_{i=-N}^{2g} A_i (\gamma_2^i y^{2i+1} + \dots) \right) - d \left(\sum_{i=-N}^{2g} \frac{A_i}{2} (\gamma_2^{i+m} y^{2i+2m} + \dots) \right),$$

with $\gamma'_j \in K$ for all j and $\gamma'_j \in R$ when $j \leq 0$. Integrating the left hand side of this equation with respect to y yields a series whose terms of degree ≤ 1 have coefficients in R . Thus the same argument as in the proof of Lemma 2 shows that $A_i \in R$ for all $i \leq 0$. Moreover if $r = 0$, then $A_i = 0$ when $i \leq 0$. This terminates the first part of the proof.

We still have to prove that $2^c a_i \in R$ for $i = 0, \dots, 2g - 1$ and that $2A_i \in R$ for $i = 1, \dots, 2g$. This follows by the same argument as in the second part of the proof of Lemma 2. However, in the present situation A_0 might not be zero, but we proved already that $A_0 \in R$. Therefore we bring the terms which contain A_0 to the other side in equation (11) from the proof of Lemma 2. This then ends the proof of Lemma 3. □

Remark. Lemma 3 remains valid when we replace $\sum_{i=0}^{2g-1}$ by $\sum_{i=-\kappa}^{2g-1-\kappa}$ whenever $r \geq \kappa \in \mathbb{N}$. The proof is exactly the same.

Remark. If $r = 0$, then in the above proof the A_i are zero for all $i \leq 0$, and for $0 \leq i \leq 2g - 1$ the a_i are completely determined by (11) as we saw by considering resultants. This shows that the $x^i y dx$ for $i = 0, \dots, 2g - 1$ and $\frac{dx}{x}$ are linearly independent in $H^1_{DR}(A_{m,f}/K)$.

Lemma 2 and 3 show that the basis for $H^1_{DR}(A_{m,f}/K)$ is a generating set for $H^1(\overline{A}_{m,\overline{f}}/K)$, since the reduction process converges. Indeed, for $a_k x^k y \in A^\dagger_{m,f}$ the valuation of a_k grows as a linear function of $|k|$, while the valuation of the

denominators introduced during the reduction of $a_k x^k y \, dx$ are only logarithmic in $|k|$.

The Monsky-Washnitzer cohomology $H^1(\overline{A}_{m,\overline{f}}/K)$ is the direct sum of the ι -invariant part $H^1(\overline{A}_{m,\overline{f}}/K)^+$ on which ι acts trivially and the ι -anti invariant part $H^1(\overline{A}_{m,\overline{f}}/K)^-$ on which ι acts by multiplication by -1 . Note that $\frac{dx}{x}$ is a basis for the invariant part $H^1(\overline{A}_{m,\overline{f}}/K)^+$ for $m > 0$ and the Frobenius acts on it by multiplication with q . Hence for $m > 0$ the Lefschetz fixed point theorem yields

$$\begin{aligned} \#\overline{C}_{m,\overline{f}}(\mathbb{F}_{q^k}) &= 1 + \#\overline{C}'_{m,\overline{f}}(\mathbb{F}_{q^k}) \\ &= 1 + \text{Tr}\left(q^k F_*^{-k} | H^0(\overline{A}_{m,\overline{f}}/K)\right) - \text{Tr}\left(q^k F_*^{-k} | H^1(\overline{A}_{m,\overline{f}}/K)\right) \\ &= 1 + q^k - \text{Tr}\left(q^k F_*^{-k} | H^1(\overline{A}_{m,\overline{f}}/K)^+\right) \\ &\quad - \text{Tr}\left(q^k F_*^{-k} | H^1(\overline{A}_{m,\overline{f}}/K)^-\right) \\ &= q^k - \text{Tr}\left(q^k F_*^{-k} | H^1(\overline{A}_{m,\overline{f}}/K)^-\right). \end{aligned}$$

Let $\tilde{C}_{m,\overline{f}}$ be the unique smooth projective curve birational to $\overline{C}_{m,\overline{f}}$, then

$$\#\tilde{C}_{m,\overline{f}}(\mathbb{F}_{q^k}) = q^k + 1 - \text{Tr}\left(q^k F_*^{-k} | H^1(\overline{A}_{m,\overline{f}}/K)^-\right) = q^k + 1 - \sum_{i=1}^{2g} \alpha_i^k,$$

where α_i are the eigenvalues of qF_*^{-1} on $H^1(\overline{A}_{m,\overline{f}}/K)^-$. By the Weil conjectures there exists a polynomial $\chi(t) \in \mathbb{Z}[t]$ of the form $t^{2g} + a_1 t^{2g-1} + \dots + a_{2g}$, whose roots $\beta_1, \dots, \beta_{2g}$ satisfy $\beta_i \beta_{g+i} = q$ for $i = 1, \dots, g$, $|\beta_i| = \sqrt{q}$ for $i = 1, \dots, 2g$ and $\#\tilde{C}_{m,\overline{f}}(\mathbb{F}_{q^k}) = q^k + 1 - \sum_{i=1}^{2g} \beta_i^k$ for all $k > 0$. This implies that we can label the β 's such that $\alpha_i = \beta_i$ for $i = 1, \dots, 2g$. Since $\alpha_i \alpha_{g+i} = q$, the α_i are also the eigenvalues of F_* on $H^1(\overline{A}_{m,\overline{f}}/K)^-$. It is well known that the zeta function $Z(\tilde{C}_{m,\overline{f}}/\mathbb{F}_q; t)$ can be written as $Z(\tilde{C}_{m,\overline{f}}/\mathbb{F}_q; t) = \frac{t^{2g} \chi(1/t)}{(1-t)(1-qt)}$. Therefore, it is sufficient to compute $\chi(t)$ as the characteristic polynomial of F_* on $H^1(\overline{A}_{m,\overline{f}}/K)^-$.

4 Detailed Algorithm and Complexity

Using the results of the previous section, we describe an algorithm for computing the characteristic polynomial of Frobenius $\chi(t)$ and the zeta function of a smooth projective Artin-Schreier curve $\tilde{C}_{m,\overline{f}}$ of genus g over \mathbb{F}_q with $q = 2^n$. We have shown that we can compute $\chi(t) = t^{2g} + a_1 t^{2g-1} + \dots + a_{2g}$ as the characteristic polynomial of F_* on $H^1(\overline{A}_{m,\overline{f}}/K)^-$. The Weil conjectures imply that $q^{g-i} a_i = a_{2g-i}$, so it suffices to compute a_1, \dots, a_g , and that for $i = 1, \dots, g$ the a_i can be bounded by

$$|a_i| \leq \binom{2g}{i} q^{i/2} \leq \binom{2g}{g} q^{g/2} \leq 2^{2g} q^{g/2}.$$

Thus to determine the zeta function, we have to compute the action of F_* on a basis of $H^1(\overline{A}_{m,\overline{f}}/K)^-$ modulo 2^B with $B \geq \left\lceil \log_2 \left(2 \binom{2g}{g} q^{g/2} \right) \right\rceil$. However, we need to take into account the loss of precision caused by the reduction process.

Combining Lemmata 1-3 one can prove that it is sufficient to compute with a precision N which satisfies $N - 3 - \lfloor \log_2(2N \deg f + g) \rfloor \geq B$.

Algorithms 1-3 contain a detailed description of the most important subroutines of our algorithm. The function `Artin_Schreier_Zeta_Function` essentially computes an approximation M of the matrix through which the p -th power Frobenius acts on a basis of $H^1(\overline{A}_{m,\overline{f}}/K)^-$. The function `Lift_p_Frobenius_y` computes a sufficiently precise approximation of y^σ using a Newton iteration on the equation $Y^2 - x^{2m}Y - f(x)^\sigma = 0$ and `Series_Invert` computes the inverse of an invertible element of $A_{m,f}^\dagger$ up to precision N . In step 4 of Algorithm 1 we call `Reduce_MW_Cohomology` to express a differential $Gy dx$ with $G \in R[x, x^{-1}]$ on a basis of $H^1(\overline{A}_{m,\overline{f}}/K)^-$. The result of this function is a polynomial $S \in K[x]$, with $\deg S < 2g$ such that for a given precision B we have the following equivalence modulo exact forms and invariant forms $G(x, x^{-1})y dx \sim R(x)y dx \pmod{2^B}$, where $\pmod{2^B}$ means modulo $2^B(Ry dx + \dots + Rx^{2g-1}y dx)$. Once we have found the matrix M , we compute $\text{Norm}(M) = MM^\sigma \dots M^{\sigma^{n-1}}$ which is an approximation of the action of Frobenius on $H^1(\overline{A}_{m,f}/K)^-$. Finally, we determine its characteristic polynomial with precision $\left\lceil \log_2 \left(2 \binom{2g}{g} q^{g/2} \right) \right\rceil$ and recover the characteristic polynomial of Frobenius $\chi(t)$ from the first g coefficients. Note that M is not necessarily defined over R , so we have to increase B if necessary to obtain the desired precision.

The complexity analysis of the algorithm is similar to Kedlaya's algorithm in [12, Section 5], except that in our case the reduction takes $O(g^{5+\varepsilon}n^{3+\varepsilon})$ time instead of $O(g^{4+\varepsilon}n^{3+\varepsilon})$ time. A detailed complexity analysis can be found in [5], which proves that the zeta function of a genus g Artin-Schreier curve $\tilde{C}_{m,\overline{f}}$ over a finite field \mathbb{F}_q with $q = 2^n$ elements, can be computed deterministically in $O(g^{5+\varepsilon}n^{3+\varepsilon})$ bit operations with space complexity $O(g^3n^3)$.

5 Implementation and Numerical Results

In this section we compare the efficiency of our algorithm with an algorithm by Lauder and Wan [16], which also runs in $O(g^{5+\varepsilon}n^{3+\varepsilon})$ bit operations and needs $O(g^3n^3)$ storage space. As far as we know, Lauder & Wan's algorithm has not been implemented before.

Table 1 presents running times of our algorithm and Lauder & Wan's algorithm for genus 2 and genus 3 Artin-Schreier curves over various finite fields of characteristic 2 obtained on a Sun UltraSparc III 600 MHz running Solaris 5.8 and MAGMA V2.8-1. In these examples we have taken $B = \left\lceil \log_2 \left(2 \binom{2g}{g} q^{g/2} \right) \right\rceil$ and the results were verified by checking the group order of the Jacobian.

Algorithm 1 (Artin_Schreier_Zeta_Function).

IN: Artin-Schreier curve $\bar{C}_{m,\bar{f}}$ over \mathbb{F}_q given by equation $y^2 - x^m y = \bar{f}(x)$.

OUT: The zeta function $Z(\bar{C}_{m,\bar{f}}/\mathbb{F}_q; t)$.

-
1. Compute $N \in \mathbb{N}$ with $N - 3 - \lfloor \log_2(2N \deg f + g) \rfloor \geq B$;
 2. $\bar{f} = \bar{f} - \bar{f}(0) + \sqrt{\bar{f}(0)x^m}$; $f = R[x] \leftarrow \bar{f} \bmod 2^N$;
 3. $\alpha_N(x), \beta_N(x) = \text{Lift_p_Frobenius_y}(m, f, N)$;
 4. For $i = 0$ To $2g - 1$ Do
 - 4.1. $\text{Red}_i(x) = \text{Reduce_MW_Cohomology}(2x^{2i+1}\beta_N(x), m, f, B)$;
 - 4.2. For $j = 0$ To $2g - 1$ Do $M[j][i] = \text{Coeff}(\text{Red}_i, j)$;
 5. $\text{Norm}_M = MM^\sigma \dots M^{\sigma^{n-1}} \bmod 2^B$;
 6. $\chi(t) = \text{Characteristic_Pol}(\text{Norm}_M) \bmod 2^B$;
 7. For $i = 0$ To $i = g$ Do
 - 7.1. If $\text{Coeff}(\chi, 2g - i) > \binom{2g}{i} q^{i/2}$ Then $\text{Coeff}(\chi, 2g - i) - = 2^B$;
 - 7.2. $\text{Coeff}(\chi, i) = q^{g-i} \text{Coeff}(\chi, 2g - i)$;
 8. Return $Z(\bar{C}_{m,\bar{f}}/\mathbb{F}_q; t) = \frac{t^{2g} \chi(1/t)}{(1-t)(1-qt)}$.

Algorithm 2 (Lift_p_Frobenius_y).

IN: Artin-Schreier curve $C_{m,f}$ over R and precision N .

OUT: $\alpha_N, \beta_N \in R[x, x^{-1}]$ with $y^\sigma \equiv \alpha_N(x, x^{-1}) + \beta_N(x, x^{-1})y \bmod 2^N$.

-
1. If $N = 1$ Then $\alpha_N = f(x)$; $\beta_N = x^m$;
 2. Else
 - 2.1. $N' = \lceil \frac{N}{2} \rceil$;
 - 2.2. $\alpha_{N'}, \beta_{N'} = \text{Lift_p_Frobenius_y}(m, f(x), N')$;
 - 2.3. $\gamma_N, \delta_N = \text{Series_Invert}(1 - \frac{2(\alpha_{N'}(x) + \beta_{N'}(x)y)}{x^{2m}}, m, f(x), N)$;
 - 2.4. $\mu_N \equiv -\alpha_{N'} + x^{-2m}(\alpha_{N'}^2 + \beta_{N'}^2 f(x) - f(x)^\sigma) \bmod 2^N$;
 - 2.5. $\nu_N \equiv -\beta_{N'} + x^{-2m}(2\alpha_{N'}\beta_{N'} + \beta_{N'}^2 x^m) \bmod 2^N$;
 - 2.6. $\alpha_N \equiv \alpha_{N'} + \mu_N \gamma_N + \nu_N \delta_N f(x) \bmod 2^N$;
 - 2.7. $\beta_N \equiv \beta_{N'} + \mu_N \delta_N + \nu_N (\gamma_N + \delta_N x^m) \bmod 2^N$;
 3. Return α_N, β_N .

Algorithm 3 (Reduce_MW_Cohomology).*IN:* Artin-Schreier curve $C_{m,f}$, precision B and element $G \in R[x, x^{-1}]$.*OUT:* $S \in K[x]$, with $\deg S < 2g$ such that $Sy \, dx \sim Gy \, dx \pmod{2^B}$.

-
1. Compute $N \in \mathbb{N}$ with $N - 3 - \lfloor \log_2(2N \deg f + g) \rfloor \geq B$;
 2. $D = \text{Degree}(G)$; $V = \text{Valuation}(G)$; $T = G$;
 3. For $i = D$ To $2g$ By -1
 - 3.1. $P \equiv x^{i-2g}(2f' + mx^{2m-1}) + \frac{i-2g}{3}x^{i-2g-1}(4f + x^{2m}) \pmod{2^N}$;
 - 3.2. $T \equiv T - (\text{Coeff}(T, i) \cdot P) / (2(2g + 1) + \frac{4(i-2g)}{3}) \pmod{2^N}$;
 4. For $i = V$ To -1
 - 4.1. $P \equiv x^i(2f' + mx^{2m-1}) + \frac{i}{3}x^{i-1}(4f + x^{2m}) \pmod{2^N}$;
 - 4.2. $T \equiv T - (\text{Coeff}(T, i) \cdot P) / (2(1 + \frac{2i}{3})f'(0)) \pmod{2^N}$;
 5. Return $S \equiv T \pmod{2^B}$.

Table 1. Running times for genus 2 and genus 3 Artin-Schreier curves over \mathbb{F}_{2^n} of Denef-Vercauteren (D-V) vs. Lauder-Wan (L-W) algorithm.

Genus 2 curves			Genus 3 curves		
Field Size	Time D-V (s)	Time L-W (s)	Field Size	Time D-V (s)	Time L-W (s)
13 bits	2.7	6.0	11 bits	7.0	24.3
23 bits	12.9	22.9	17 bits	29.6	85.1
37 bits	93.5	141	23 bits	76.2	219
47 bits	178	259	31 bits	189	501
59 bits	347	465	41 bits	663	1231
71 bits	983	973	47 bits	1067	1773
83 bits	1207	1493	59 bits	1724	3156

6 Conclusion

We have presented an extension of Kedlaya's algorithm to Artin-Schreier curves over finite fields of characteristic 2. The resulting algorithm runs in $O(g^{5+\varepsilon}n^{3+\varepsilon})$ bit operations and needs $O(g^3n^3)$ storage space for a genus g curve over \mathbb{F}_{2^n} . The ideas presented in this paper can also be used to devise an algorithm for computing the zeta function of an arbitrary hyperelliptic curve over a finite field of characteristic 2 as shown in [5].

References

1. S. Arita. Algorithms for computations in jacobians of C_{ab} curve and their application to discrete-log-based public key cryptosystems. In *Proceedings of Conference on The Mathematics of Public Key Cryptography*, Toronto, June 1999.
2. A.O.L. Atkin. The number of points on an elliptic curve modulo a prime. *Series of e-mails to the NMBRTHRY mailing list*, 1992.
3. I.F. Blake, G. Seroussi, and N.P. Smart. *Elliptic curves in cryptography*. volume 265 of *London Mathematical Society Lecture Note Series*, 1999.
4. S. Bosch. A rigid analytic version of M. Artin's theorem on analytic equations. *Math. Ann.*, 255:395–404, 1981.
5. J. Denef and F. Vercauteren. An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2. *Preprint*, 2002.
6. N. Elkies. Elliptic and modular curves over finite fields and related computational issues. *Computational Perspectives on Number Theory*, pages 21–76, 1998.
7. R. Elkik. Solutions d'équations à coefficients dans un anneau hensélien. *Ann. Scient. Ec. Norm. Sup.*, 6(4):553–604, 1973.
8. M. Fouquet, P. Gaudry, and R. Harley. On Satoh's algorithm and its implementation. *J. Ramanujan Math. Soc.*, 15:281–318, 2000.
9. S. Galbraith, S. Paulus, and N. Smart. Arithmetic on superelliptic curves. *Math. Comp.*, 71(237):393–405, 2002.
10. P. Gaudry and N. Gürel. An extension of Kedlaya's algorithm for counting points on superelliptic curves. In *Advances in Cryptology - ASIACRYPT 2001*, Lecture Notes in Computer Science, 2001.
11. P. Gaudry and R. Harley. Counting points on hyperelliptic curves over finite fields. *Bosma, Wieb (ed.), ANTS-IV, Lect. Notes Comput. Sci. 1838, 313-332*, 2000.
12. K.S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. Preprint 2001.
13. N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48:203–209, 1987.
14. N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1(3):139–150, 1989.
15. A.G.B. Lauder and D. Wan. Counting points on varieties over finite fields of small characteristic. Preprint 2001.
16. A.G.B. Lauder and D. Wan. Computing zeta functions of Artin-Schreier curves over finite fields. Preprint 2001.
17. R. Lercier. *Algorithmique des courbes elliptiques dans les corps finis*. PhD thesis, Laboratoire d'Informatique de l'École polytechnique (LIX), 1997.
18. V. Miller. Uses of elliptic curves in cryptography. *Advances in Cryptology - ASIACRYPT '91, Lecture notes in Computer Science*, 218:460–469, 1993.
19. P. Monsky and G. Washnitzer. Formal cohomology. I. *Ann. of Math.*, 88:181–217, 1968.
20. P. Monsky. Formal cohomology. II: The cohomology sequence of a pair. *Ann. of Math.*, 88:218–238, 1968.
21. P. Monsky. Formal cohomology. III: Fixed point theorems. *Ann. of Math.*, 93:315–343, 1971.
22. P. Monsky. *p-adic analysis and zeta functions*. Lectures in Mathematics, Department of Mathematics Kyoto University. 4. Tokyo, Japan, 1970.
23. J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, 55(192):745–763, 1990.
24. B. Poonen. Computational aspects of curves of genus at least 2. *Cohen, Henri (ed.), ANTS-II, Lect. Notes Comput. Sci. 1122, 283-306*, 1996.

25. T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15:247–270, 2000.
26. R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p . *Math. Comp.*, 44:483–494, 1985.
27. B. Skjernaa. Satoh's algorithm in characteristic 2. *To appear in Math. Comp.*, 2000.
28. M. van der Put. The cohomology of Monsky and Washnitzer. *Mém. Soc. Math. France*, 23:33–60, 1986.
29. F. Vercauteren, B. Preneel, and J. Vandewalle. A memory efficient version of Satoh's algorithm. In *Advances in Cryptology - EUROCRYPT 2001*, number 2045 in Lecture Notes in Computer Science, pages 1–13, 2001.