Generalising the GHS Attack on the Elliptic Curve Discrete Logarithm Problem

F. Hess

Technical University of Berlin,
Faculty II – Institute of Mathematics, Secr. MA8-1,
Straße des 17. Juni 136, 10623 Berlin, Germany
hess@math.tu-berlin.de

Abstract. We generalise the Weil descent construction of the GHS attack on the elliptic curve discrete logarithm problem (ECDLP) to arbitrary Artin-Schreier extensions. We give a formula for the characteristic polynomial of Frobenius of the obtained curves and prove that the large cyclic factor of the input elliptic curve is not contained in the kernel of the composition of the conorm and norm maps. As an application we considerably increase the number of elliptic curves which succumb to the basic GHS attack, thereby weakening curves over $\mathbb{F}_{2^{155}}$ further. We also discuss other possible extensions or variations of the GHS attack and conclude that they are not likely to yield further improvements.

1 Introduction

The Weil descent technique, proposed by Frey [8], provides a way of mapping the discrete logarithm problem on an elliptic curve (ECDLP) over a large finite field $\mathbb{F}_{q^n}$ to a discrete logarithm problem on a higher dimensional abelian variety defined over the small finite field $\mathbb{F}_q$. One can then study possible further constructions of such abelian varieties and the hardness of the discrete logarithm problem thereon.

This was subsequently done by Galbraith and Smart [12] and Gaudry, Hess and Smart [14], in even characteristic (i.e. for q a power of 2). The construction of [14] yields a very efficient algorithm to reduce the ECDLP to the discrete logarithm in the divisor class group of a hyperelliptic curve over $\mathbb{F}_q$. Since subexponential algorithms exist for the discrete logarithm problem in high genus hyperelliptic curves, this gives a possible method of attack against the ECDLP. We refer to the method of [14] as the GHS attack.

Menezes and Qu [22] analyzed the GHS attack in some detail and demonstrated that it did not apply to the case when $q = 2$ and n is prime. Since this is the common case in real world applications, the work of Menezes and Qu means that the GHS attack does not apply to most deployed systems. However, there are a few deployed elliptic curve systems which use the fields $\mathbb{F}_{2^{155}}$ and $\mathbb{F}_{2^{185}}$ [18]. Hence there is considerable interest as to whether the GHS attack makes all curves over these fields vulnerable. In [24] Smart examined the GHS attack for elliptic curves with respect to the field extension $\mathbb{F}_{2^{155}}/\mathbb{F}_{2^{31}}$ and concluded that such a technique was unlikely to work for any curve defined over $\mathbb{F}_{2^{155}}$.

Jacobson, Menezes and Stein [19] also examined the field $\mathbb{F}_{2^{155}}$, this time using the GHS attack down to the subfield $\mathbb{F}_{2^5}$. They concluded that such a strategy could be used in practice to attack around 2^{33} isomorphism classes of elliptic curves defined over $\mathbb{F}_{2^{155}}$. Since there are about 2^{156} isomorphism classes of elliptic curves defined over $\mathbb{F}_{2^{155}}$, the probability that the GHS attack is applicable to a randomly chosen one is negligible. A further very detailed analysis for many other fields was carried out by Maurer, Menezes and Teske [20]. They identified all extension fields $\mathbb{F}_{2^n}$, where $160 \leq n \leq 600$, for which there should exist a cryptographically interesting elliptic curve over $\mathbb{F}_{2^n}$ such that the GHS attack is more efficient for that curve than for any other cryptographically interesting elliptic curve over $\mathbb{F}_{2^n}$. Ciet, Quisquater and Sica [6] discussed the security of fields of the form $\mathbb{F}_{2^{2d}}$ where d is a Sophie-Germain prime.

Galbraith, Hess and Smart [11] extended the GHS attack to isogeny classes of elliptic curves. The basic idea is to check whether a given elliptic curve is isogenous to an elliptic curve for which the basic GHS attack is effective. Then one computes the isogeny and reduces the ECDLP to that curve. This greatly increased the number of elliptic curves which succumb to the GHS attack for certain parameters.

The GHS attack has also been generalised to hyperelliptic curves, in even characteristic by Galbraith [10] and odd characteristic by Diem [7]. Thériault [26] considers a special class of Artin-Schreier curves in any characteristic.

In this paper we extend the GHS attack for elliptic curves in characteristic two even further, thereby considerably increasing the number of curves for which the basic GHS attack of [14] was previously applicable. In order to do so we generalise the construction of [14] and [10] to arbitrary Artin-Schreier extensions, and this enables us to utilise different Artin-Schreier equations than have been previously considered. These new results are then combined with the technique of [11].

For example, for the field extension $\mathbb{F}_{2^{155}}/\mathbb{F}_{2^5}$, among the 2^{156} isomorphism classes of curves there are around 2^{104} which are vulnerable to attack under the extended method of [11]. Using the new construction we obtain that around 2^{123} additional isomorphism classes should now be attackable.

On the other hand it should be noted that the curves produced by our generalised construction, although they have the same genera as in [14], are no longer hyperelliptic. As a consequence solving the discrete logarithm problem in the divisor class group of these curves is much more complicated and in general slower by a factor polynomial in the genus. The precise efficiency and practical implications have yet to be determined.

In the paper we further give a formula for the characteristic polynomial of Frobenius of the constructed curves and discuss conditions under which the discrete logarithm problem is preserved when mapped to the corresponding divisor class group by the norm-conorm homomorphism. Similar statements for the norm-conorm homomorphism have been obtained by Diem [7]. We additionally discuss a number of other possible variations of the construction, and conclude that they are not likely to yield any further improvements. We also address the algorithmic issues of computing the final curves and solving the discrete logarithm on them.

The results of this paper show that curves defined over fields of composite extension degree over $\mathbb{F}_2$, especially 155, may possibly be more susceptible to Weil descent attacks than suggested by previous methods. Our techniques do however not pose a threat for prime extension degrees in small characteristic or prime fields in large characteristic.

The remainder of the paper is organised as follows. In section 2 we describe the general setting which is considered throughout the paper. In section 3 we provide statements on Artin-Schreier extensions and base automorphisms. In section 4 we explain the general Weil descent construction for Artin-Schreier extensions and give statements about its main invariants like its genus, the kernel of the norm-conorm homomorphism and the characteristic polynomial of Frobenius. In section 5 we specialise to the case of even characteristic and elliptic curves and generalise the original construction of [14]. In section 6 we are ready to apply the developed theory to investigate what alternative efficient constructions can be carried out in the elliptic curve case in even characteristic. In section 7 we briefly address algorithmic issues of computing the final curves and solving the discrete logarithm. In section 8 we investigate various possibly more effective extensions and variations, and in sections 9 and 10 we provide general statements on the norm-conorm homomorphism and the characteristic polynomial of Frobenius which are used in the previous sections. Section 11 finally contains the conclusion.

2 Mapping the discrete Logarithm Problem

Let E be a function field of transcendence degree one over the finite exact constant field K, C/E be a finite extension and U_1 be a finite subgroup of $\mathrm{Aut}(C)$. The fixed field of U_1 in C is denoted by C^{U_1}. We are mainly interested in the case where E is the function field of an elliptic curve.

We obtain a homomorphism of the divisor class groups $\phi : \mathcal{C}l(E) \to \mathcal{C}l(C^{U_1})$ by $\mathrm{N}_{C/C^{U_1}} \circ \mathrm{Con}_{C/E}$, the conorm from E to C followed by the norm from C to C^{U_1}. The divisor class groups of degree zero divisors are denoted by $\mathcal{C}l^0(E)$ and $\mathcal{C}l^0(C^{U_1})$. There are two main objectives: First, the norm-conorm homomorphism ϕ should map a given discrete logarithm problem in $\mathcal{C}l^0(E)$ sufficiently faithfully to $\mathcal{C}l^0(C^{U_1})$. Second, subject to the first condition, the genus and constant field of C^{U_1} should be as small as possible.

The next four sections describe how such C and U_1, not necessarily optimal in the above sense, can be constructed from E in terms of Artin-Schreier extensions, and give statements about the kernel of ϕ, the L-polynomial of C^{U_1} and its genus based on general theorems which are proved in sections 9 and 10.

3 Artin-Schreier Extensions with Base Automorphism

In this section we describe methods which lead to the Weil descent techniques for Artin-Schreier extensions of the next sections, generalising those of [7, 14]. For the following theory about Artin-Schreier extensions see [2, pp. 22–24], [23, pp. 275–281] and [25, p. 115].

Let F/K be an algebraic function field of characteristic p and transcendence degree one over the exact constant field K. Let $\wp(x) = x^p - x$ be the Artin-Schreier operator. We have a 1-1 correspondence of $\mathbb{F}_p$-modules $\Delta \leq F^+$ with $\wp(F) \subseteq \Delta$ and abelian extensions of F of exponent p within a fixed separable closure $\bar{F}$ of F, given by

$$\Delta \mapsto C = F(\wp^{-1}(\Delta)).$$

If Δ has finite dimension m then $[C : F] = p^m$. Furthermore there is a non-degenerate bilinear form

$$\langle \cdot, \cdot \rangle : G(C/F) \times \Delta/\wp(F) \to \mathbb{F}_p \tag{1}$$

given by $\langle \tau, f \rangle = y\tau - y$ where $y \in \wp^{-1}(f)$ and $y\tau = \tau^{-1}y = \tau^{-1}(y)$.

Let $\sigma \in \mathrm{Aut}(F)$ be an automorphism of finite order n, $U = \langle \sigma \rangle$ the cyclic group generated by σ, and assume from now on that Δ is σ-invariant, or in other words, that Δ is an (additive) $\mathbb{F}_p[\sigma]$-module. The extension C/F^U is then Galois of degree $p^m n$ with exact sequence

$$1 \to G(C/F) \to G(C/F^U) \to G(F/F^U) \to 1. \tag{2}$$

This means that $G(C/F^U)$ is of exponent np and that σ can be extended to an automorphism of C of order n or np, denoted by σ_1. We let $U_1 = \langle \sigma_1 \rangle$. The sequence is split if and only if $G(C/F^U)$ contains an extension of σ of order n, and a sufficient condition for this is $p \nmid n$. Namely, if σ_1 is an extension of order np then $\sigma_1^{p\lambda}$ is an extension of order n where $p\lambda \equiv 1 \bmod n$.

If $\Delta' \subseteq \Delta$ is an $\mathbb{F}_p$-submodule of Δ and $\tau \in G(C/F^U)$ we have $\tau F(\wp^{-1}(\Delta')) = F(\wp^{-1}(\tau\Delta'))$ and consequently $G(C/F(\wp^{-1}(\tau\Delta'))) = \tau G(C/F(\wp^{-1}(\Delta')))\tau^{-1}$. The group $G(C/F)$ can be viewed as a right $\mathbb{F}_p[\sigma_1]$-module via conjugation, $\tau^{\sigma_1} = \sigma_1 \tau \sigma_1^{-1}$ for $\tau \in G(C/F)$, and $\Delta/\wp(F)$ can be viewed as a right $\mathbb{F}_p[\sigma_1]$-module (or $\mathbb{F}_p[\sigma]$-module) by $f\sigma_1 = f\sigma = \sigma^{-1}(f)$. With this the pairing $\langle \cdot, \cdot \rangle$ in (1) is $\mathbb{F}_p[\sigma_1]$-linear,

$$\langle \tau^{\sigma_1}, f \rangle = \langle \tau, f\sigma_1 \rangle = \langle \tau, f\sigma \rangle.$$

By duality the pairing $\langle \cdot, \cdot \rangle$ leads to an $\mathbb{F}_p[\sigma_1]$-module isomorphism of $G(C/F)$ and $\Delta/\wp(F)$.

The following theorem gives precise conditions on when (2) is split in the case that Δ is a cyclic $\mathbb{F}_p[\sigma]$-module. For the general case one can decompose Δ into a direct sum of cyclic factors and then apply the theorem.

Theorem 3 *Let $f \in \Delta$ and assume that $\Delta/\wp(F)$ is the cyclic $\mathbb{F}_p[\sigma]$-module generated by f. Let $m_f \in \mathbb{F}_p[t]$ be the monic polynomial of smallest degree such that $fm_f(\sigma) \in \wp(F)$ and let $c_f = (t^n - 1)/m_f \in \mathbb{F}_p[t]$.*

- (i) *Any extension of σ has order n or np, the exponent of $G(C/F^U)$ is np.*
- (ii) *There are extensions of σ of order n and np if and only if $f(\sigma^n-1)/(\sigma-1) \notin \wp(F)$. In this case, if σ_1 is an extension of order n then $\sigma_1\tau$ is an extension of order np for every $\tau \in G(C/F)$ with $\langle \tau, f(\sigma^n-1)/(\sigma-1)\rangle \neq 0$. Conversely, if σ_1 has order np then there is $\tau \in G(C/F)$ with $\langle \tau, f(\sigma^n-1)/(\sigma-1)\rangle \neq 0$ such that $\sigma_1\tau$ has order n.*
- (iii) *If $f(\sigma^n-1)/(\sigma-1) \in \wp(F)$ then the extensions of σ have order n if and only if $vc_f(\sigma) = 0$ where $v \in \wp^{-1}(fm_f(\sigma))$, and order np otherwise.*

The conditions $f(\sigma^n-1)/(\sigma-1) \in \wp(F)$, $c_f(1) = 0$ and $v_{t-1}(m_f) \neq p^{v_p(n)}$ are equivalent, and $p \nmid n$ implies $f(\sigma^n-1)/(\sigma-1) \notin \wp(F)$ or $vc_f(\sigma) = 0$.

Proof. Since σ has order n we have $m_f \mid (t^n-1)$ and $c_f \in \mathbb{F}_p[t]$. Statement (i) follows from (2) and its exactness.

We prove (ii). If σ_1 is an extension of σ then every other extension can be written in the form $\sigma_1\tau$ with $\tau \in G(C/F)$, because (2) is exact. We have

$$(\sigma_1\tau)^n = \tau^{(\sigma_1^n-1)/(\sigma_1-1)}\sigma_1^n \tag{4}$$

by a straightforward calculation and $\tau^{\sigma_1^n} = \tau$ because $\sigma_1^n \in G(C/F)$ by (2). If there are extensions of order n and np then there exists τ such that σ_1 has order n and $\sigma_1\tau$ has order np, and hence $\tau^{(\sigma_1^n-1)/(\sigma_1-1)} \neq 1$. Then $\langle \tau^{(\sigma_1^n-1)/(\sigma_1-1)}, f\rangle \neq 0$ since otherwise, as $\tau^{(\sigma_1^n-1)/(\sigma_1-1)}$ is σ_1-invariant, $\langle \tau^{(\sigma_1^n-1)/(\sigma_1-1)}, f\sigma^i\rangle = 0$ for $1 \le i \le n$ and then $\langle \tau^{(\sigma_1^n-1)/(\sigma_1-1)}, w\rangle = 0$ for all $w \in \Delta/\wp(F)$ which is impossible because $\langle\cdot,\cdot\rangle$ is non-degenerate. We have $\langle \tau^{(\sigma_1^n-1)/(\sigma_1-1)}, f\rangle = \langle \tau, f(\sigma^n-1)/(\sigma-1)\rangle \neq 0$ and thus $f(\sigma^n-1)/(\sigma-1) \notin \wp(F)$. Conversely, assume $f(\sigma^n-1)/(\sigma-1) \notin \wp(F)$ holds true. If σ_1 has order n we choose any τ with $\langle \tau, f(\sigma^n-1)/(\sigma-1)\rangle \neq 0$. Then $\tau^{(\sigma_1^n-1)/(\sigma_1-1)} \neq 1$ and $\sigma_1\tau$ has order np by (4). If σ_1 has order np then $\tau_1 = \sigma_1^n \in G(C/F)$ by (2), $\tau_1 \neq 1$ and τ_1 is σ_1-invariant. This implies $\langle \tau_1, f\rangle \neq 0$, using an analogous reasoning as before. We can find τ with $\langle \tau, f(\sigma^n-1)/(\sigma-1)\rangle = -\langle \tau_1, f\rangle$ and hence $\langle \tau^{(\sigma_1^n-1)/(\sigma_1-1)}\tau_1, f\rangle = 0$. Now $\tau^{(\sigma_1^n-1)/(\sigma_1-1)}\tau_1$ is σ_1-invariant and we get $\langle \tau^{(\sigma_1^n-1)/(\sigma_1-1)}\tau_1, w\rangle = 0$ for all $w \in \Delta/\wp(F)$. Hence $\tau^{(\sigma_1^n-1)/(\sigma_1-1)}\tau_1 = \tau^{(\sigma_1^n-1)/(\sigma_1-1)}\sigma_1^n = 1$ and $\sigma_1\tau$ has order n by (4). This proves (ii).

We proceed to prove (iii) and the last statement. Similar as in [14] let $v \in \wp^{-1}(fm_f(\sigma)) \subseteq F$ and $y \in \wp^{-1}(f)$. Then $ym_f(\sigma_1) = v + \lambda$ for some $\lambda \in \mathbb{F}_p$ and σ_1 has order n if and only if

$$y(\sigma_1^n - 1) = ym_f(\sigma_1)c_f(\sigma_1) = vc_f(\sigma) + \lambda c_f(1) = 0. \tag{5}$$

Note that $vc_f(\sigma) \in \mathbb{F}_p$ since $\wp(vc_f(\sigma)) = \wp(y)m_f(\sigma)c_f(\sigma) = f(\sigma^n-1) = 0$. As in [14] we see that for every $\lambda \in \mathbb{F}_p$ there is an extension σ_1 with $ym_f(\sigma_1) = v + \lambda$. It follows that extensions of order n and np exist if and only if $c_f(1) \neq 0$. Thus $c_f(1) = 0$ is equivalent to $f(\sigma^n-1)/(\sigma-1) \in \wp(F)$ by (ii), and it is obviously equivalent to $v_{t-1}(m_f) \neq p^{v_p(n)}$. If $c_f(1) = 0$ then σ_1 has order n precisely if $vc_f(\sigma) = 0$ by (5). This proves (*iii*). Finally, if $p \nmid n$ then we have extensions of order n so $f(\sigma^n - 1)/(\sigma - 1) \notin \wp(F)$ or $vc_f(\sigma) = 0$ holds true by (*ii*) and (*iii*).

We remark that analogous results can be obtained for Kummer extensions.

4 Weil Descent with Artin-Schreier Extensions

We describe now how the discrete logarithm in the divisor class group of an Artin-Schreier extension of small genus over a large finite field can be related to an equivalent discrete logarithm problem in the divisor class group of a curve of larger genus but defined over a smaller finite field.

Let $q = p^r$, $k = \mathbb{F}_q$ and $K = \mathbb{F}_{q^n}$. The exact constant field of F is assumed to be K. Let σ be a Frobenius automorphism of F with respect to K/k. By this we mean that σ restricts to the Frobenius automorphism of K/k and has order $[K : k]$ on F such that F/F^U with $U = \langle\sigma\rangle$ is a constant field extension of degree n. We could for example choose $F = K(x)$ and σ to be the extension of the Frobenius automorphism of K/k via $\sigma(x) = x$.

Let $\Delta = f\mathbb{F}_p[\sigma] + \wp(F)$, $C = F(\wp^{-1}(\Delta))$, $E_h = F(\wp^{-1}(h))$ for $h \in \Delta$ and $m = \dim_{\mathbb{F}_p} \Delta/\wp(F) = \deg(m_f)$. The goal is to construct an extension σ_1 of σ on C which is a Frobenius automorphism of C with respect to K_1/k where K_1 is the exact constant field of C. One then forms C^{U_1} where $U_1 = \langle\sigma_1\rangle$ and maps the discrete logarithm problem in $\mathcal{C}l^0(E_h)$ to $\mathcal{C}l^0(C^{U_1})$ using $\phi_h : \mathcal{C}l(E_h) \to \mathcal{C}l(C^{U_1})$ defined by $\mathrm{N}_{C/C^{U_1}} \circ \mathrm{Con}_{C/E_h}$. It will not always be the case that the discrete logarithm problem in $\mathcal{C}l^0(C^{U_1})$ is equivalent to that in $\mathcal{C}l^0(E_h)$.

The extension C/K is either regular or involves a constant field extension of degree p since there are no two constant field extensions of degree p linearly disjoint over F. We can thus distinguish two cases, $K_1 = K$ and $[K_1 : K] = p$. We have $FK_1 = F(\wp^{-1}(\Delta \cap K))$ so $K_1 = K$ if and only if $\Delta \cap K \subseteq \wp(F)$.

Case $K_1 = K$. It suffices to find any extension of σ of order n, and Theorem 3 describes how this can be achieved. If $v_{t-1}(m_f) = p^{v_p(n)}$ we are in case (*ii*) and can find such an extension. Otherwise, we are in case (*iii*) and can only find an extension of order n if $vc_f(\sigma) = 0$. This criterion is reformulated in Lemma 6. By Theorem 3, $p \nmid n$ or $m = n$ are sufficient conditions for the existence of an extension of σ of order n.

Case $[K_1 : K] = p$. The extension FK_1/F^U is cyclic of order np and

$$1 \to G(C/FK_1) \to G(C/F^U) \to G(FK_1/F^U) \to 1$$

is exact. The Frobenius automorphism of FK_1/F^U thus extends to C and any such extension will have order np (see case (*iii*) in Theorem 3).

Lemma 6 *Let P be a σ-invariant place of degree one of F and $\pi \in P$ a σ-invariant uniformiser. Let $f = \sum_{i=v_P(f)}^{\infty} \lambda_i \pi^i$ be the P-adic expansion of f.*

If $[K_1 : K] = p$ then $\mathrm{Tr}_{K/\mathbb{F}_p}(\lambda_0) \neq 0$ and $v_{t-1}(m_f) \neq 0$, and σ extends to a Frobenius automorphism of C with respect to K_1/k.

If $K_1 = K$ then σ extends to a Frobenius automorphism of C with respect to K/k if and only if $\mathrm{Tr}_{K/\mathbb{F}_p}(\lambda_0) = 0$ or $v_{t-1}(m_f) = p^{v_p(n)}$.

Proof. Corresponding to P we have an embedding $\phi : F \to K((\pi))$, $\phi(x) = \sum_{i=v_P(x)}^{\infty} \phi_i(x)\pi^i$ and σ extends to an automorphism of $K((\pi))$ which operates on the coefficients and leaves π fixed. We can extend the $\mathbb{F}_p[\sigma]$-module structure of F to $K((\pi))$ accordingly and $\phi_0 : F \to K$ will be $\mathbb{F}_p[\sigma]$-linear. For t_0 transcendental over $\mathbb{F}_p$ we let $t = t_0^r$ and σ_0 the Frobenius automorphism of $K/\mathbb{F}_p$ such that $\mathbb{F}_p[t] \subseteq \mathbb{F}_p[t_0]$ and $\sigma = \sigma_0^r$.

If $[K_1 : K] = p$ then there is $a \in f\mathbb{F}_p[\sigma] \cap K$ with $a \notin \wp(F)$. Since $a(\sigma - 1) = 0$ we must have $v_{t-1}(m_f) \neq 0$. Let w be a normal basis element for $K/\mathbb{F}_p$. Then there is $h \in \mathbb{F}_p[t_0]$ such that $a = wh(\sigma_0)$. The conditions $a \notin \wp(F)$, $(t_0 - 1) \nmid h$ and $(t_0^{nr} - 1) \nmid h(t_0^{nr} - 1)/(t_0 - 1)$ are equivalent. Then

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{F}_p}(a) &= a(\sigma_0^{nr} - 1)/(\sigma_0 - 1)\\ &= wh(\sigma_0)(\sigma_0^{nr} - 1)/(\sigma_0 - 1)\end{aligned}$$

which is non zero if and only if $(t_0^{nr} - 1) \nmid h(t_0^{nr} - 1)/(t_0 - 1)$. Thus $a \notin \wp(F)$ is equivalent to $\mathrm{Tr}_{K/\mathbb{F}_p}(a) \neq 0$. Now $a \in \lambda_0\mathbb{F}_p[\sigma]$ so that $\mathrm{Tr}_{K/\mathbb{F}_p}(a) \neq 0$ implies $\mathrm{Tr}_{K/\mathbb{F}_p}(\lambda_0) \neq 0$. That the Frobenius automorphism extends follows from the discussion before Lemma 6.

The case $K_1 = K$. By Theorem 3 the Frobenius automorphism extends if and only if $v_{t-1}(m_f) = p^{v_p(n)}$ or $vc_f(\sigma) = 0$. Assume $v_{t-1}(m_f) \neq p^{v_p(n)}$, hence $c_f(1) = 0$. In the proof of Theorem 3 it was seen that $vc_f(\sigma) \in \mathbb{F}_p$ thus $\phi(vc_f(\sigma)) \in \mathbb{F}_p$ and $\phi_i(vc_f(\sigma)) = 0$ for all $i \neq 0$. We obtain that $vc_f(\sigma) = 0$ if and only if $\phi_0(vc_f(\sigma)) = \phi_0(v)c_f(\sigma) = 0$. Now $c_f = (t_0 - 1)c'_f$ for some $c'_f \in \mathbb{F}_p[t_0]$ since $c_f(1) = 0$, and $\phi_0(v)(\sigma_0 - 1) = \phi_0(v^p - v) = \phi_0(f)m_f(\sigma)$ since $v^p - v = fm_f(\sigma)$. We obtain

$$\begin{aligned}\phi_0(v)c_f(\sigma) &= \phi_0(v)(\sigma_0 - 1)c'_f(\sigma_0)\\ &= \phi_0(f)m_f(\sigma_0^r)c'_f(\sigma_0)\\ &= \phi_0(f)(\sigma_0^{nr} - 1)/(\sigma_0 - 1)\\ &= \mathrm{Tr}_{K/\mathbb{F}_p}(\phi_0(f)),\end{aligned}$$

and thus $vc_f(\sigma) = 0$ if and only if $\mathrm{Tr}_{K/\mathbb{F}_p}(\phi_0(f)) = 0$.

Theorem 7 *Let $h \in \Delta$ and $V = \{\, \tau \in U_1 \mid h\tau \in \lambda h + \wp(F)$ for some $\lambda \in \mathbb{F}_p \,\}$. Then*

$$\mathrm{N}^{-1}_{E_h/(E_h)^V}(0) \;\subseteq\; \ker(\phi_h) \;\subseteq\; \mathrm{N}^{-1}_{E_h/(E_h)^V}\big([p^{m-1}]^{-1}(\mathrm{Con}_{(E_h)^V/F^V}(\mathcal{C}l^0(F^V)))\big)$$

where $[p^{m-1}]$ is the multiplication-by-p^{m-1} map.

Proof. The fields E_h and $\tau E_h = E_{\tau h}$ for $\tau \in U_1$ are either equal or linearly disjoint over F. The definition of V implies $VE_h \subseteq E_h$, and $E_h = \tau E_h$ if and only if $\tau \in V$. Furthermore, the kernel of the restriction map $U_1 \to \mathrm{Aut}(F)$ is zero. The conditions of Proposition 23 are therefore fulfilled. We obtain $(E_h)^V \cap \tau(E_h)^V = F^V$ for all $\tau \in U_1$ with $\tau \notin V$. Applying Theorem 18 and Theorem 24 with $\phi = \phi_h$ gives the result.

Assume $\mathcal{C}l^0(E_h)$ has a large prime factor $> p$ which is not present in $\mathcal{C}l^0(F)$. Theorem 7 says that if $K_1 = K$ and $V = \{1\}$, the large prime factor will not be mapped to zero under ϕ_h. If $V \neq \{1\}$ and the large prime factor is not present in $\mathcal{C}l^0((E_h)^V)$, then it will be mapped to zero. If on the other hand $[K_1 : K] = p$ we have that $\sigma_1^n \in G(E_h/F)$ has order p, $G(E_h/F) \subseteq V$ and thus $(E_h)^V \subseteq F^V$. This means that the large prime factor will always be mapped to zero in this case.

We now state upper and lower bounds on the genus of C.

Theorem 8 *Let $f \in \Delta$ and assume that $\Delta/\wp(F)$ is the cyclic $\mathbb{F}_p[\sigma]$-module of $\mathbb{F}_p$-dimension m generated by f. Then $m \leq n$ and*

$$g_C \leq \begin{cases} (p^m-1)/(p-1)\big(g_{E_f} - g_F\big) + g_F & \textit{if } f \textit{ has } \sigma\textit{-invariant poles,} \\ (p^m-1)/(p-1)\big(n \cdot g_{E_f} - g_F\big) + g_F & \textit{otherwise.} \end{cases}$$

On the other hand, if $m \geq 2$ and $F(\wp^{-1}(f, f\sigma))$ has a genus greater than g_{E_f} then

$$g_C \geq p^{m-2} g_{E_f}/[K_1 : K] + 1.$$

Proof. Since σ has order n we have at most n different elements $f\sigma^i$, and because Δ is generated by f it then follows that $m \leq n$.

Using the genus formula of [25, III.7.8] we see that $g_{E_h} \leq n g_{E_f}$ for any $h \in \Delta$ since h is an $\mathbb{F}_p$-linear combination of the conjugates $f\sigma^i$, and the numbers $m_{\sigma^i(P)}$ for h and any given P are thus less than or equal to the maximum of the numbers $m_{\sigma^i(P)}$ for f. Also, every place has at most n conjugate places $\sigma^i(P)$. If f has only σ-invariant poles then $g_{E_h} \leq g_{E_f}$ since the numbers m_P for h and any given P are less than or equal to the numbers m_P for f. The upper bounds then follow from Corollary 38 with $U_1 = \{1\}$ and $G = H = G(C/F)$. Here subgroups H_ν of H of index p correspond to one dimensional $\mathbb{F}_p$-vector spaces contained in $\Delta/\wp(F)$ via $H_\nu = G(C/E_{f_\nu})$ where f_ν spans a non trivial $\mathbb{F}_p$-vector space in $\Delta/\wp(F)$. There are $(p^m-1)/(p-1)$ many f_ν and H_ν. All occurring constant field extension degrees in Corollary 38 are 1 because $U_1 = \{1\}$.

The lower bounds are obtained from the Riemann-Hurwitz genus formula which gives $2g_C - 2 \geq (2(g_{E_f}+1) - 2)p^{m-2}/[K_1 : K]$.

The lower bound of Theorem 8 is not very sharp. However, the main point here is that it shows that the genus of C is exponential in m.

If (2) is split we can also apply Theorem 26 and compute the L-polynomial of C^{U_1}, using the notation $G = G(C/F^{U_1})$ and $H = G(C/F)$. Here, as in the proof of Theorem 8, subgroups H_ν of H of index p correspond to one dimensional $\mathbb{F}_p$-vector spaces contained in $\Delta/\wp(F)$ via $H_\nu = G(C/E_{f_\nu})$ where f_ν spans a non trivial $\mathbb{F}_p$-vector space in $\Delta/\wp(F)$. There are $(p^m-1)/(p-1)$ many f_ν and H_ν. Furthermore $U_{1\nu} = \{\, \tau \in U_1 \mid f_\nu\tau \in \lambda f_\nu + \wp(F) \text{ for some } \lambda \in \mathbb{F}_p \,\}$.

5 Generalising the basic GHS Attack

In [14] an Artin-Schreier construction has been applied to the case where E_f is the function field of an elliptic curve and F is the rational function field, over a finite field in characteristic two. We now describe a generalisation of this construction, obtained by specialising and applying the techniques of the previous sections.

Let $p = 2$ and $\Delta = f\mathbb{F}_2[\sigma] + \wp(F)$ where $f = \gamma/x + \alpha + \beta x$ for $\gamma, \alpha, \beta \in K$ and $\gamma\beta \neq 0$. Furthermore, let $F = K(x)$. We have

$$\Delta/\wp(F) \cong \mathbb{F}_2[t]/(m_f) \tag{9}$$

with m_f as in Theorem 3 of degree m.

More precisely, if m_γ and m_β are polynomials in $\mathbb{F}_2[t]$ of minimal degree such that $\gamma m_\gamma(\sigma) = 0$ and $\beta m_\beta(\sigma) = 0$ then

$$m_f = \begin{cases} \mathrm{lcm}(m_\gamma, m_\beta) & \text{for } \alpha \in \wp(F), \\ \mathrm{lcm}(m_\gamma, m_\beta, t+1) & \text{otherwise.} \end{cases} \tag{10}$$

We remark that $\alpha \in \wp(F)$ is equivalent to $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$.

Theorem 11 *The Frobenius automorphism σ of F with respect to K/k extends to a Frobenius automorphism of C with respect to K/k if and only if at least one of the conditions $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$, $\mathrm{Tr}_{K/k}(\gamma) \neq 0$ or $\mathrm{Tr}_{K/k}(\beta) \neq 0$ holds.*

Proof. We have $K_1 = K$ if and only if $\alpha\,\mathrm{lcm}(m_\gamma, m_\beta)(\sigma) \in \wp(F)$, and this in turn is equivalent to that at least one of the conditions $(t+1) \mid m_\gamma m_\beta$ or $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$ holds, which can be seen similar as in the proof of Lemma 6.

In the case $K_1 = K$ the Frobenius automorphism σ of F extends to a Frobenius automorphism of C with respect to K/k if and only if $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$ or $v_{t+1}(m_f) = 2^{v_2(n)}$, by Lemma 6 using the place $x = 0$ and uniformiser x. Thus there exists a Frobenius automorphism of C with respect to K/k if and only if $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$ or both conditions $(t+1) \mid m_\gamma m_\beta$ and $v_{t+1}(m_f) = 2^{v_2(n)}$ hold.

Now, if n is even then $v_{t+1}(m_f) = 2^{v_2(n)}$ implies $v_{t+1}(m_\gamma) = 2^{v_2(n)}$ or $v_{t+1}(m_\beta) = 2^{v_2(n)}$ because of the definition of m_f and (10), and conversely $v_{t+1}(m_\gamma) = 2^{v_2(n)}$ or $v_{t+1}(m_\beta) = 2^{v_2(n)}$ implies $(t+1) \mid m_\gamma m_\beta$ and $v_{t+1}(m_f) = 2^{v_2(n)}$. If n is odd then $(t+1) \mid m_\gamma m_\beta$ is equivalent to that $v_{t+1}(m_\gamma) = 2^{v_2(n)}$ or $v_{t+1}(m_\beta) = 2^{v_2(n)}$ holds, and implies $v_{t+1}(m_f) = 2^{v_2(n)}$. This shows that the Frobenius automorphism extends if and only if $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$, $v_{t+1}(m_\gamma) = 2^{v_2(n)}$ or $v_{t+1}(m_\beta) = 2^{v_2(n)}$ hold.

Finally $\mathrm{Tr}_{K/k}(\gamma) = \gamma(\sigma^n + 1)/(\sigma + 1)$, and $v_{t+1}(m_\gamma) = 2^{v_2(n)}$ is equivalent to $\gamma(\sigma^n + 1)/(\sigma + 1) \neq 0$. This proves the theorem.

If σ_1 is a Frobenius automorphism of C then the genus of C^{U_1} equals the genus of C and Theorem 8 yields appropriate bounds. For the special choice of f it is however possible to determine the genus precisely. The following result can be applied whenever the conditions in Theorem 11 are fulfilled.

Theorem 12 *Assume $K_1 = K$. The genus of $C = F(\wp^{-1}(\Delta))$ is given by*

$$g_C = 2^m - 2^{m-\deg(m_\gamma)} - 2^{m-\deg(m_\beta)} + 1.$$

Proof. One dimensional $\mathbb{F}_2$-subspaces of $\Delta/\wp(F)$ are given by non-zero elements in $\mathbb{F}_2[t]/(m_f)$ under the isomorphism (9). Let $v \in \Delta$ correspond to $w \in \mathbb{F}_2[t]$ of degree less than m. Then $v = fw(\sigma)$ and E_v has genus 0 if $\gamma w(\sigma) = 0$ or $\beta w(\sigma) = 0$, and genus 1 otherwise. Thus for genus 0 we have that w is divisible by m_γ or by m_β. If $\alpha \in \wp(F)$ then $m_f = \mathrm{lcm}(m_\gamma, m_\beta)$. If $\alpha \notin \wp(F)$ then $(t+1) \mid m_\gamma m_\beta$, because we have assumed $K_1 = K$ which implies $\alpha m_\gamma(\sigma) m_\beta(\sigma) \in \wp(F)$, and hence again $m_f = \mathrm{lcm}(m_\gamma, m_\beta)$. The two cases $m_\gamma \mid w$ and $m_\beta \mid w$ thus lead to disjoint sets of non-zero w, since no non-zero $w \in \mathbb{F}_2[t]$ with $\deg(w) < m$ can be divisible by both m_γ and m_β, as this would imply that w is divisible by $m_f = \mathrm{lcm}(m_\gamma, m_\beta)$ and hence $\deg(w) \geq m$. There are thus precisely $(2^{m-\deg(m_\gamma)} - 1) + (2^{m-\deg(m_\beta)} - 1)$ non-zero polynomials $w \in \mathbb{F}_2[t]$ of degree $< m$, which are divisible by m_γ or by m_β.

Since there are $2^m - 1$ non-zero polynomials $w \in \mathbb{F}_2[t]$ of degree less than m we obtain the number of one dimensional $\mathbb{F}_2$-subspaces of $\Delta/\wp(F)$ such that the associated degree 2 extensions have genus 1 by subtracting the number of genus 0 cases from all cases, that is $2^m - 1 - (2^{m-\deg(m_\gamma)} - 1) - (2^{m-\deg(m_\beta)} - 1)$. Using Corollary 38 and the remarks at the end of section 4 we finally obtain the result.

We want to link the results obtained so far to the results of [14]. Let $\gamma \in k$. Then $m_\gamma = t + 1$ and $\Delta \cap K \subseteq K(\sigma + 1) \subseteq \wp(F)$ so that $K_1 = K$ and C/K is regular. For the existence of the Frobenius automorphism with respect to K/k we note that $\mathrm{Tr}_{K/k}(\gamma) \equiv n \bmod 2$ holds and that $\mathrm{Tr}_{K/k}(\beta) \neq 0$ is equivalent to $(t+1)^u \mid m_\beta$ where $u = 2^{v_2(n)}$. This shows that the condition (2) in Lemma 6 of [20] is necessary and sufficient and that condition (†) of [14] is sufficient for the existence of the Frobenius automorphism. The genus of C is equal to $2^{m-1} - 2^{m-\deg(m_\beta)} + 1$. Depending on whether $(t+1) \mid m_\beta$ or not this gives $m - \deg(m_\beta) = 0$ or $m - \deg(m_\beta) = 1$ and hence a genus of 2^{m-1} or $2^{m-1} - 1$. Finally, similarly to the proof of Theorem 12, we have that $F(\wp^{-1}(\Delta(\sigma + 1)))$ has genus 0 and index 2 in C, hence C is hyperelliptic. This recovers the main results about the construction in [14]. In addition we now obtain the following more precise statement.

Corollary 13 *Let $\gamma \in k$. The genus of C is $2^{m-1} - 1$ if and only if $\mathrm{Tr}_{K/\mathbb{F}_{q^u}}(\beta) = 0$ where $u = 2^{v_2(n)}$.*

Proof. We have to prove that $(t+1) \nmid m_\beta$ is equivalent to $\mathrm{Tr}_{K/\mathbb{F}_{q^u}}(\beta) = 0$. We can write $\beta = wh(\sigma)$ with $h \in k[t]$ and $w \in K$ a normal basis element over k such that $K = wk[\sigma]$. Also, $v_{t+1}(t^n + 1) = u$.

If the genus is $2^{m-1} - 1$ then $(t+1) \nmid m_\beta$. Because $w(m_\beta h)(\sigma) = \beta m_\beta(\sigma) = 0$ and $t^n + 1$ is the $k[t]$-minimal polynomial of w we get $(t^n + 1) \mid m_\beta h$ and $(t^u + 1) \mid h$. Then $\beta = w(\sigma^u + 1)h_1$ for some $h_1 \in k[t]$ such that $h = (t^u + 1)h_1$, and $\mathrm{Tr}_{K/\mathbb{F}_{q^u}}(\beta) = \beta(\sigma^n + 1)/(\sigma^u + 1) = w(\sigma^n + 1)h_1 = 0$.

Conversely, if $\mathrm{Tr}_{K/\mathbb{F}_{q^u}}(\beta) = \beta(\sigma^n+1)/(\sigma^u+1) = 0$ then $m_\beta \mid ((t^n+1)/(t^u+1))$ since m_β is the $\mathbb{F}_2[t]$-minimal polynomial of β. But $(t^n+1)/(t^u+1)$ is coprime to $t+1$ so that $(t+1) \nmid m_\beta$. It follows that the genus is $2^{m-1}-1$.

For $h \in \Delta$ with $h = c/x + a + bx$ define $s(h) = \min\{\, s \geq 1 \mid \sigma^s(c) = c \text{ and } \sigma^s(b) = b \,\}$. Then $\sigma^{s(h)}$ is the smallest power of σ which maps the one dimensional subspace of $\Delta/\wp(F)$ generated by h to itself, or, in other words, such that $\sigma_1^{s(h)}$ yields an automorphism of E_h. For example, if $n/s(h)$ is odd then $E_h = E_{\tilde{h}}$ where $\tilde{h} = c/x + \mathrm{Tr}_{K/\mathbb{F}_{q^{s(h)}}}(a) + bx \in \mathbb{F}_{q^{s(h)}}(x)$.

Theorem 14 *For the homomorphism $\phi_h : \mathcal{C}l(E_h) \to \mathcal{C}l(C^{U_1})$ given by the composition $\mathrm{N}_{C/C^{U_1}} \circ \mathrm{Con}_{C/E_h}$ we have*

$$\mathrm{N}^{-1}_{E_h/(E_h)^{\langle \sigma_1^{s(h)} \rangle}}(0) \;\subseteq\; \ker(\phi_h) \;\subseteq\; \mathrm{N}^{-1}_{E_h/(E_h)^{\langle \sigma_1^{s(h)} \rangle}}\big(\mathcal{C}l^0((E_h)^{\langle \sigma_1^{s(h)} \rangle})[2^{m-1}]\big).$$

Proof. Follows from Theorem 7 and $\mathcal{C}l^0(F) = 0$ since F is rational.

Assume that σ_1 is a Frobenius automorphism of C with respect to K/k as in Theorem 11. Theorem 14 then means that the discrete logarithm problem in E_h will be preserved by ϕ_h in practical applications if and only if $s(h) = n$, that is, E_h does not come from a non trivial constant field extension (is not defined by a subfield curve). Interestingly, C^{U_1} is in a sense universal in that it preserves discrete logarithms in large prime subgroups for all E_h and $h \in \Delta$ such that $s(h) = n$.

The L-polynomial of C^{U_1} or the characteristic polynomial of Frobenius over k can be computed as follows.

Theorem 15 *Assume that σ_1 is a Frobenius automorphism of C with respect to K/k. Let $S \subseteq f\mathbb{F}_2[\sigma]$ be a system of representatives under the operation of U on $\Delta/\wp(F)$. Then*

$$L_{C^{U_1}}(t) = \prod_{h \in S} L_{(E_h)^{\langle \sigma_1^{s(h)} \rangle}}(t^{s(h)}).$$

Proof. We want to apply Theorem 26 using the remarks at the end of section 4. Since $E_{\sigma h} = \sigma_1(E_h)$ and $G(C/\sigma_1(E_h)) = \sigma_1 G(C/E_h)\sigma_1^{-1}$, a set of representatives H_ν under the operation of U_1 on subgroups of $G(C/F)$ of index 2 is given by $\{\, G(C/E_h) \mid h \in S, h \notin \wp(F) \,\}$. Then $U_{1\nu} = \langle \sigma_1^{s(h)} \rangle$ and $C^{H_\nu U_{1\nu}} = (E_h)^{\langle \sigma_1^{s(h)} \rangle}$ for ν corresponding to $h \in S$. Let k_h be the extension field of k of degree $s(h)$. The constant field of $(E_h)^{\langle \sigma_1^{s(h)} \rangle}$ is equal to k_h. Furthermore $C^G = k(x)$, $C^{HU_{1\nu}} = k_h(x)$ and $(E_h)^{\langle \sigma_1^{s(h)} \rangle} = k(x)$ for $h \in \wp(F)$. The result now follows from Theorem 26, since L-polynomials of rational function fields are equal to 1.

6 Applications

A representative for each isomorphism class of ordinary elliptic curves defined over K with $p = 2$ is given by $Y^2 + XY = X^3 + \alpha X^2 + \beta$ with $\beta \in K$ and $\alpha \in \{0, \omega\}$ where $\omega \in \mathbb{F}_{2^u}$ for $u = 2^{v_2(nr)}$ is a fixed element with $\mathrm{Tr}_{\mathbb{F}_{2^u}/\mathbb{F}_2}(\omega) = 1$. The associated Artin-Schreier equation is $y^2 + y = 1/x + \alpha + \beta^{1/2}x$, obtained by the transformation $Y = y/x + \beta^{1/2}$, $X = 1/x$ and multiplication by x^2. The same normalisation of α is also possible for the more general Artin-Schreier equations $y^2 + y = \gamma/x + \alpha + \beta x$ of section 5.

It was the equation $y^2 + y = 1/x + \alpha + \beta^{1/2}x$ which has been used in [14] to perform the Weil descent. However, since $(ax + b)/(cx + d)$ for $a, b, c, d \in K$ with $ad - bc \neq 0$ is also a generator of F we could make a substitution $x \mapsto (ax + b)/(cx + d)$ and apply the results of the previous sections to $f = (cx + d)/(ax + b) + \alpha + \beta^{1/2}(ax + b)/(cx + d)$. Since we aim at getting as small values of $m = \deg(m_f)$ as possible, because of Theorem 8, we require that f has σ-invariant poles. But this implies $b = \lambda a$ and $d = \mu c$ for $\lambda, \mu \in k$. Hence $(ax+b)/(cx+d) = (a/c)(x+\lambda)/(x+\mu)$. As $(x+\lambda)/(x+\mu)$ is σ-invariant we can substitute x for this. Writing $\gamma = a/c$ we obtain $f = 1/(\gamma x) + \alpha + \beta^{1/2}\gamma x$ and this is precisely of the form considered in section 5. A similar reasoning holds if $a = 0$ or $c = 0$.

The question now is whether for $\beta \in K$ there is a $\gamma \in K$ such that the polynomial $\mathrm{lcm}(m_{1/\gamma}, m_{\beta^{1/2}\gamma})$ has small degree in comparison with n. If we find such a γ we can apply the results of section 5 and reduce the discrete logarithm problem on the elliptic curve to that in the divisor class group of a higher genus curve defined over k. The only general algorithm known so far to find such a γ is by computing all γ such that $m_{1/\gamma}$ has small degree and then individually checking whether $m_{\beta^{1/2}\gamma}$ also has small degree.

On the other hand we can choose $\gamma_1, \gamma_2 \in K$ such that $\mathrm{lcm}(m_{\gamma_1}, m_{\gamma_2})$ has small degree in comparison with n and define $\beta = \gamma_1\gamma_2$. Then $y^2 + y = \gamma_1/x + \alpha + \gamma_2 x$ and $Y^2 + XY = X^3 + \alpha X^2 + \beta^2$ define isomorphic elliptic function fields. Heuristically we expect that the map $(\gamma_1, \gamma_2) \mapsto \gamma_1\gamma_2$ is almost injective for the γ_1, γ_2 under consideration, except for symmetry and scaling $\gamma_1 \mapsto \lambda\gamma_1$, $\gamma_2 \mapsto \lambda^{-1}\gamma_2$ by elements $\lambda \in k^\times$. This is also confirmed by examples. It follows that we (heuristically) considerably increase the number of elliptic curves which can be attacked by the basic GHS attack.

We now want to combine our results with the results of [11]. Assume for simplicity that r, n are odd and n is prime so that $\alpha \in \mathbb{F}_2$ according to the above normalisation. Over $\mathbb{F}_2$ we have the factorisation into irreducible polynomials $t^n + 1 = (t + 1)h_1 \cdots h_s$ and $\deg(h_i) = d$ such that $n = sd + 1$, see [22]. In this situation the first non-trivial m satisfies $d \leq m \leq d + 1$, yielding $m_f = h_i$ or $m_f = (t + 1)h_i$ by equation (10). Due to our generalisation we do not necessarily have $m = d + 1$ as in [11, 14], and in fact we are now concentrating on $m = d$. The number of Artin-Schreier equations as in section 5 with $\alpha \in \mathbb{F}_2$ and $d \leq m \leq d+1$ is approximately equal to $2sq^{2d+2}$ whereas the number of equations among these with $m = d$ (implies $\alpha = 0$) is approximately equal to sq^{2d}. From these Artin-Schreier equations we expect to obtain about $\min\{q^n, sq^{2d-1}/2\}$ associated elliptic curve equations, using the above transformations, and a system of representatives under the action of the 2-power Frobenius of cardinality $\min\{q^n/(nr), sq^{2d-1}/(2nr)\}$. Furthermore, as in [11], we expect that these representatives distribute over the isogeny classes like arbitrary elliptic curves with $a = 0$.

If $m = d$ we have $m_f = m_\gamma = m_\beta$, $(t+1) \nmid m_\gamma m_\beta$ and $\alpha = 0$. It follows that $\mathrm{Tr}_{K/k}(\gamma) = \mathrm{Tr}_{K/k}(\beta) = 0$ and by the Theorems 11 and 14 the Weil descent technique does work because $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$ and γ, β are not in a subfield of K since n is prime. The resulting genus then satisfies $g_C = 2^d - 1$ by Theorem 12. Note that in [11, 14] it is always the case that $m = d+1$ but $\deg(m_\gamma) = 1$, so that the genus is of similar size, namely $2^d - 1$ or 2^d. Back to the case $m = d$ we observe that if $\alpha = 0$ then the group order of the elliptic curve is congruent to 0 modulo 4 and if $\alpha = 1$ then it is congruent to 2 modulo 4 (see [3, p. 38]). This means that curves with $\alpha = 0$ represent half of about all $2q^{n/2}$ isogeny classes. Taking this into account we obtain from [11] that a proportion of $\min\{1, sq^{2d-1}/(2q^{n/2}nr)\}$ of all elliptic curves over K with $\alpha = 0$ leads to curves of genus $2^d - 1$ defined over k with equivalent discrete logarithm problem. Given a random elliptic curve with $\alpha = 0$ we can find the associated elliptic curve, from which such a curve of genus $2^d - 1$ can be computed, in running time $O(n \log(q) N) + O(q^{n/4+\varepsilon})$ and probability $\min\{1, N/q^{n/2}\}$, where $N \le sq^{2d-1}/(2nr)$ and $\varepsilon > 0$.

The case $n = 31$ and $r = 5$ is particularly interesting since there is an IPsec curve [18] with $\alpha = 0$ defined over $\mathbb{F}_{2^{155}}$. This case has $d = 5$, $s = 6$ and thus yields genus 31 which are feasible parameters according to [19]. The heuristic probability that a random elliptic curve gives rise to a curve of genus 31 has been approximately 2^{-52} with the method in [11] whereas now we obtain

$$sq^{2d-1}/(2q^{n/2}nr) \approx 2^{-38}.$$

The only algorithm known so far to find the elliptic curves from which the corresponding higher genus curves are computed requires the order of $sq^{2d-1}/(2nr) \approx 2^{39}$ many operations in $\mathbb{F}_{2^{155}}$ ($q^{n/4} \approx 2^{39}$ here). This is not so efficient, but still much faster than the Pollard methods on the original curves. One can however additionally argue that the security of elliptic curves over $\mathbb{F}_{2^{155}}$ does now at least partially depend on the difficulty of the problem of finding such higher genus curves.

7 Algorithmic Issues

So far our main objective was to investigate whether there exist curves of sufficiently small genus to whose divisor class group the discrete logarithm problem could be faithfully transferred. In this section we briefly discuss how to obtain explicit models for the resulting curves of section 4 and section 5 and how to perform an index calculus method for solving the discrete logarithm problem. Note that the curves we are considering are no longer necessarily hyperelliptic. Also, the most expensive step will be the solving the discrete logarithm and not the computation of the final curve and mapping the discrete logarithm.

7.1 Explicit Models and mapping the discrete Logarithm

We first exhibit an explicit model for C. Let $m = \deg(m_f)$. Note that the classes of $\sigma^i(f)$ for $0 \le i \le m-1$ form an $\mathbb{F}_p$-basis of $\Delta/\wp(F)$. It follows that C is obtained by adjoining one root of every $y^p - y - \sigma^i(f)$ to F. In other words, $C = F[y_0, \ldots, y_{m-1}]/I$ where I is the ideal of the polynomial ring $F[y_0, \ldots, y_{m-1}]$ generated by the polynomials $y_i^p - y_i - \sigma^i(f)$ for $0 \le i \le m-1$. We write $\bar{y}_i$ for the images of the y_i in C and abbreviate $\bar{y} = \bar{y}_0$.

Assume that σ extends to a Frobenius automorphism of C with respect to K/k, again denoted by σ. After possibly replacing y_i by $y_i + \mu_i$ for some $\mu_i \in \mathbb{F}_p$ we have that $\sigma(\bar{y}_i) = \bar{y}_{i+1}$ for $0 \le i < m-1$ and $\sigma(\bar{y}_{m-1}) = v - \sum_{i=0}^{m-1} \lambda_i \bar{y}_i$ holds, where the $\lambda_i \in \mathbb{F}_p$ are the coefficients of $m_f = \sum_{i=0}^{m} \lambda_i t^i$ and $v \in F$ satisfies $v^p - v = \sum_{i=0}^{m} \lambda_i \sigma^i(f)$. Such v will be determined up to addition of an element in $\mathbb{F}_p$, and usually only one of the p choices of v will be the correct choice so that σ has order n on C (see the proof of Theorem 3). We obtain an explicit representation of the operation of σ on C.

The field C^{U_1} is the fixed field of σ in C and $F^U = k(x)$ the fixed field of σ in $F = K(x)$. Define $\tilde{y} = \sum_{i=0}^{n-1} \sigma^i(\mu\bar{y})$, where μ is a normal basis element of K over $\mathbb{F}_p$. Then $C^{U_1} = F^U(\tilde{y})$, because $\tilde{y} \in C^{U_1}$ and $C = F(\tilde{y})$, which in turn holds because $\tilde{y}$ has $[C : F]$ different conjugates under $G(C/F)$. To see the last statement let $\tau \in G(C/F)$ and observe that $\sigma\tau\sigma^{-1} \in G(C/F)$. Define $\lambda(\tau) = \tau(\bar{y}) - \bar{y} \in \mathbb{F}_p$. The map $\tau \mapsto (\,\lambda(\sigma^{-i}\tau\sigma^i)\,)_{0 \le i \le n-1}$ is injective because the right hand side values determine τ on all conjugates $\sigma^i(\bar{y})$. Then

$$\begin{aligned}
\tau(\tilde{y}) &= \sum_{i=0}^{n-1} \tau\sigma^i(\mu\bar{y}) \;=\; \sum_{i=0}^{n-1} \sigma^i(\mu)\tau\sigma^i(\bar{y}) \\
&= \sum_{i=0}^{n-1} \sigma^i(\mu)\sigma^i(\sigma^{-i}\tau\sigma^i)(\bar{y}) \;=\; \sum_{i=0}^{n-1} \sigma^i(\mu)\sigma^i(\bar{y} + \lambda(\sigma^{-i}\tau\sigma^i)) \\
&= \sum_{i=0}^{n-1} \sigma^i(\mu)\sigma^i(\bar{y}) + \sum_{i=0}^{n-1} \sigma^i(\mu)\lambda(\sigma^{-i}\tau\sigma^i) \\
&= \tilde{y} + \sum_{i=0}^{n-1} \sigma^i(\mu)\lambda(\sigma^{-i}\tau\sigma^i).
\end{aligned}$$

Since μ is a normal basis element we can conclude that $\tilde{y}$ has indeed $[C : F]$ different conjugates. By computing the characteristic polynomial of $\tilde{y}$ over F in C we thus obtain a defining polynomial for C^{U_1} in $F^U[t]$. The discrete logarithm can be mapped from E_f to C^{U_1} using the conorm map Con_{C/E_f} followed by the norm map $\mathrm{N}_{C/C^{U_1}}$. We give a very rough description of how this can be accomplished. It is best to work with suitable subrings (Dedekind domains) R_{E_f}, R_C and $R_{C^{U_1}}$ and ideals in these rings such that the ideal class groups are similar enough to the divisor class groups (preserving the large prime factor for example). The conorm of a given ideal in R_{E_f} then becomes the ideal generated in R_C by the given ideal included in R_C. Using general techniques we can compute a representation

$\bar{y} = h(\tilde{y})$ with $h \in F[t]$. For the norm ideal we then form the product of the conjugated ideals in R_C using σ. Substituting $h(\tilde{y})$ for $\bar{y}$ and some further steps yield generators of the norm ideal in $R_{C^{U_1}}$.

7.2 Index Calculus

Index calculus methods are employed for solving the discrete logarithm in the multiplicative group of finite fields or the divisor class group of hyperelliptic curves. They also apply to the divisor class group of general curves. We outline some of the main issues in our situation.

The basic observation is that every divisor class of C^{U_1} of degree $g_{C^{U_1}}$ can be represented by an effective divisor of the same degree. Such a divisor decomposes uniquely into a sum of places of certain degrees and multiplicities just like the case of rational integers and prime factorisations, and smoothness probabilities hold. Computing these divisor class representatives can be done by reduction techniques as described in [16], and this leads also to a way of computing in the divisor class group of C^{U_1} which generalises the Cantor method for hyperelliptic curves. We remark that for hyperelliptic curves addition takes $O(g_{C^{U_1}}^2)$ operations in k whereas for a general C^{U_1} addition takes $O(g_{C^{U_1}}^4)$ operations in k, and is hence considerably slower.

The number of effective divisors of degree less than or equal to $g_{C^{U_1}}$ containing places of degree less than or equal to d can usually be expressed as some explicit proportion of $q^{g_{C^{U_1}}}$. For example, for $g_{C^{U_1}} \to \infty$ and q fixed we have that this number of smooth divisors is approximately at least $q^{g_{C^{U_1}}} \exp(-(g_{C^{U_1}}/d) \log(g_{C^{U_1}}/d))$ for $g_{C^{U_1}}^{c_1} \leq d \leq g_{C^{U_1}}^{c_2}$ and $0 < c_1 < c_2 < 1$ fixed. From our formula for the characteristic polynomial of Frobenius of C^{U_1} in Theorem 15 we see that $g_{C^{U_1}} = \sum_{h \in S} s(h)$ by taking degrees, and then for the cardinality of the divisor class group $\#\mathcal{C}l^0(C^{U_1}) = q^{g_{C^{U_1}}} \prod_{h \in S}(1 + O(q^{-s(h)/2}))$ by evaluating at 1. For every $h \in S$ we have that $s(h) \,|\, n$, and the number of $h \in S$ with $s(h) \,|\, s$ for given $s \,|\, n$ is less than or equal to p^s. If the number of divisors of n is $O(\log(g_{C^{U_1}}))$ and $q \geq p^2$ it follows that $\#\mathcal{C}l^0(C^{U_1}) = \prod_{s|n} \prod_{s(h)=s}(1 + O(p^{-s(h)})) = O(q^{g_{C^{U_1}}} g_{C^{U_1}}^c)$ for some constant $c > 1$, and we expect this to be essentially true for $q = p$ because of possible alternating signs of the trace terms. Dividing the number of smooth divisors by the class number it is hence reasonable to expect that a proportion of $\exp(-(1 + o(1))(g_{C^{U_1}}/d) \log(g_{C^{U_1}}/d))$ of all divisor classes of degree $g_{C^{U_1}}$ will be representable by a smooth divisor, thus leading to the usual smoothness probability. This would allow for an in $g_{C^{U_1}}$ subexponential running time with parameter $1/2$ for solving the discrete logarithm. Fore more details on computing discrete logarithms for general curves see [15, 17].

8 Further Variations and Observations

It is of interest whether there are further variations or extensions of the GHS attack which would lead to smaller genera. In this section we investigate a number of such variations.

8.1 Iterative Descent

Assume $n = n_1 n_2$. Instead of performing one descent from K to k we could consider descending first to $\mathbb{F}_{q^{n_1}}$ and then to k. The problem here is that C^{U_1} is in general not an Artin-Schreier extension anymore so our techniques would not apply immediately. If we however start with an elliptic curve as in section 6 and consider an associated Artin-Schreier model with $\gamma \in \mathbb{F}_{q^{n_1}}$ we do have that C^{U_1} is hyperelliptic, or in other words that it is an Artin-Schreier extension. This way we get the following interesting result.

Assuming the generic cases a descent from K to k leads to a hyperelliptic curve of genus of about 2^{n-1} whereas a descent from K to $\mathbb{F}_{q^{n_1}}$ gives 2^{n_1-1}. Using Theorem 8 the descent from $\mathbb{F}_{q^{n_1}}$ to k finally results in a curve of genus about $(2^{n_2} - 1)n_2 2^{n_1-1} \leq n_2 2^{n_1+n_2-1}$. Thus if $n_1 \approx n_2$ this final curve has subexponential genus $\approx 2^{(2+o(1))\sqrt{n}}$ instead of exponential genus 2^n.

Let us look at the non generic cases for $n = 155$, $n_1 = 5$, $n_2 = 31$. The smallest non-trivial descent from $\mathbb{F}_{2^{155}}$ to $\mathbb{F}_2$ leads to a genus of about 2^{20}. On the other hand there are descents from $\mathbb{F}_{2^{155}}$ to $\mathbb{F}_{2^5}$ which result in genus $2^5 - 1$. Assuming the generic case $m = 5$ for the descent from $\mathbb{F}_{2^5}$ to $\mathbb{F}_2$ then gives a genus less than or equal to $5(2^5 - 1)^2$.

While theoretically interesting we do not expect that these results have any practical implications, because of the still large resulting genera.

8.2 Descent from Extensions

If the descent from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ does not yield a small enough genus one could apply a change of variable to obtain a defining equation of E_f defined over an extension field $\mathbb{F}_{\tilde{q}^{\tilde{n}}}$ and descend to $\mathbb{F}_{\tilde{q}}$, thereby possibly yielding a smaller genus over another small base field for some suitable $\tilde{q}$ and $\tilde{n}$.

At least for prime n this approach will however not give an improvement. To see this we note that for any n the degrees of the irreducible factors in $\mathbb{F}_p[t]$ of $t^n - 1$ corresponding to primitive nth-roots of unity equal the multiplicative order m of p modulo n. This m is the smallest value of $\deg(m_f)$ which can occur for an elliptic curve over $\mathbb{F}_{q^n}$ which is not already defined over a subfield. For prime n this m is usually very big. Let $\tilde{m}$ be the multiplicative order of p modulo $\tilde{n}$. The genus for a descent by $\tilde{n}$ is then approximately at least $p^{\tilde{m}}$. Thus, if $n \mid \tilde{n}$ then $\tilde{m} \geq m$ and the genus can only be bigger than before. If otherwise $n \nmid \tilde{n}$ then $n \mid [\mathbb{F}_{\tilde{q}} : \mathbb{F}_p]$ because n is prime and thus $\mathbb{F}_{\tilde{q}}$ is too big.

For composite n there may be improvements possible. Again, there are descents from $\mathbb{F}_{2^{155}}$ to $\mathbb{F}_2$ which yield genus approximately 2^{20}, whereas the corresponding descents from $\mathbb{F}_{2^{155}}$ to $\mathbb{F}_{2^5}$ yield genus about 2^5 while $\mathbb{F}_{2^5}$ is still fairly small.

8.3 Subfields and Automorphisms

A possibility of improving the construction in section 4 and section 5 would be to consider subfields L of C^{U_1} and use $\phi_{f,L} = \mathrm{N}_{C^{U_1}/L} \circ \phi_f$ to map the discrete logarithm problem from $\mathcal{C}l^0(E_f)$ to $\mathcal{C}l^0(L)$. If the kernel of $\phi_{f,L}$ is small enough this would lead to a very substantial improvement, because the genus of subfields is usually much smaller.

To approach this question we first consider intermediate fields of the extension C^{U_1}/F^{U_1}. This extension is in general not Galois and any intermediate field L leads to an intermediate field LK of C/F with $\sigma_1(LK) = LK$. Thus $LK = F(\wp^{-1}(\Delta_L))$ for a unique Δ_L with $\wp(F) \subseteq \Delta_L \subseteq \Delta$ and $\sigma(\Delta_L) = \Delta_L$. If $\Delta_L \neq \Delta$ then $f \notin \Delta_L$ and E_f and LK are thus linearly disjoint over F. Now $\mathrm{N}_{C/LK} \circ \mathrm{Con}_{C/E_f} = 0$ by Lemma 16, and since $\mathrm{N}_{C^{U_1}/L} \circ \mathrm{N}_{C/C^{U_1}} = \mathrm{N}_{LK/L} \circ \mathrm{N}_{C/LK}$ we obtain $\phi_{f,L} = 0$. Thus $\phi_{f,L}$ and intermediate fields of C^{U_1}/F^{U_1} are not of any use.

We could still search for other subfields L of C^{U_1} which do not contain F^{U_1} and yield a small kernel of $\phi_{f,L}$. One way of obtaining such subfields could be via the fixed fields of automorphism groups of C containing the Frobenius automorphism. Indeed, if we had automorphisms $\rho \in \mathrm{Aut}(F/K)$ with $\rho(\Delta) \subseteq \Delta$ it should be possible to extend ρ to C in a similar way as it was done with σ, under not too restrictive conditions. We have not found such automorphisms for $F = K(x)$ and E_f defined by non-subfield curves. Even if such automorphisms do not exist there could still be useful subfields L, but this appears unlikely to happen except maybe in very rare cases.

Although automorphisms of C^{U_1}/F^{U_1} may not be useful to find suitable subfields L as shown above, they could be of use to speed up the discrete logarithm computation in C^{U_1}. We are given 2^m automorphisms in $G(C/F)$. For $\tau \in G(C/F)$ with $\tau \neq 1$ to restrict to an automorphism of C^{U_1} we need $\tau\sigma_1\tau^{-1} \in U_1$. We have $\tau\sigma_1\tau^{-1} = \tau^{1-\sigma_1}\sigma_1$ and thus $\tau^{1-\sigma_1} = \tau\sigma_1\tau^{-1}\sigma_1^{-1} \in G(C/F) \cap U_1$. As $G(C/F) \cap U_1 = \{1\}$ we obtain $\tau^{1-\sigma_1} = 1$. Since $G(C/F)$ and $\Delta/\wp(F)$ are $\mathbb{F}_p[\sigma_1]$-isomorphic, it follows that if $m_f(1) = 0$ then there is precisely one such τ, and otherwise there is no such τ. We remark that τ is the hyperelliptic involution in the case that C^{U_1} is hyperelliptic. Thus $G(C^{U_1}/F^{U_1})$ consists either of the identity only or the identity and the hyperelliptic involution. However, it is still possible that C^{U_1} has non trivial automorphisms obtained in a different way.

8.4 Other Composita

The field composita in section 4 and section 5 depend on the choice of the base field $F = K(x)$ within the function field E_f. We want to investigate what happens if other or no subfields are used, in the case of elliptic function fields E_f in characteristic two.

If $K(x_1)$ and $K(x_2)$ are any two rational subfields of index 2 of the elliptic function field E_f then there is an automorphism $\tau_Q \in \mathrm{Aut}(E_f/K)$ induced by a point translation map $P \mapsto P + Q$ such that $\tau_Q(K(x_1)) = K(x_2)$. Namely, we may assume that x_1 and x_2 are x-coordinates of Weierstrass models. Then Q is the point where x_2 has its pole. We conclude that $E_f/K(x_1)$ and $E_f/K(x_2)$ are isomorphic and hence it does not matter which rational subfield of index two is taken in section 4 and section 5.

The methods of section 4 and section 5 do not apply readily to other subfields of E_f. We make a few comments on what can be expected in terms of arbitrary field composita.

Elliptic subfields as common base fields F are not of any use. The extensions E_f/F are abelian and unramified so any compositum C will be unramified over F as well. This however means that C has genus 1 and is again an elliptic function field. The corresponding elliptic curves are all isogenous. Should there be a Frobenius automorphism on C then this would mean that the elliptic curve corresponding to E_f is isogenous to an elliptic curve defined over the small finite field k. Other aspects of isogenous elliptic curves have been exploited in [11].

All other subfields F must be rational of index ≥ 3, and such fields will indeed lead to alternative constructions. In order to estimate the resulting genus we remark that essentially the lower bound in Theorem 8 remains valid in more general situations: Similar to section 4 assume we are given C with a Frobenius automorphism σ with respect to K/k and an elliptic function field E with $E \subseteq C$ such that $C = E(\sigma E) \cdots (\sigma^{m-1}E)$ for $m \leq n$ minimal. If $E(\sigma E)$ does not have genus ≥ 2 then it has genus 1 and $E(\sigma E)/E$ as well as $E(\sigma E)/\sigma E$ are unramified. This yields an unramified pyramid of fields. It follows that C is unramified over E and is hence elliptic, which reduces us to the uninteresting case discussed above. So assume that $E(\sigma E)$ has genus ≥ 2. Using the Riemann-Hurwitz genus formula we obtain that the genus of C is then bounded by $g_C \geq [C : E(\sigma E)] + 1$ and $[C : E(\sigma E)] \geq 2^{m-2}$. If the fields $\sigma^i E$ are linearly disjoint over a common base field F with $\sigma F \subseteq F$ we even have $[C : E(\sigma E)] \geq [E : F]^{m-2}$. The genus is thus exponential in m.

The main objective is hence again to minimise m in comparison with n. A possible generalisation of the Artin-Schreier construction could be to use additive polynomials over a common rational base field F. This would lead to values of m similar as in section 5 but could apply in more or additional cases. However, as F would have index 2^s in E for $s \geq 2$ the genus bound would rather be $g_C \geq 2^{s(m-2)} + 1$, much larger than the construction of section 5.

Theoretically there could also be completely different constructions of C given E and its conjugated fields. To be effective they would need to achieve a good “compression” rate, i.e. small value of m, because of the above lower bound for the genus. We do not know whether such constructions exist.

8.5 Characteristic Three

Weil descent with Artin-Schreier extensions as in section 4 can also be carried out for elliptic curves in characteristic three. Here Artin-Schreier equations which define elliptic curves have to be of the form $y^3 - y = ax^2 + b$ with $a, b \in K$. We thus expect to map the discrete logarithm problem to curves of genus $\Theta(3^{\deg(m_f)})$ with $f = ay^2 + b$. We remark that if $a = 1$ we would again obtain an Artin-Schreier extension of degree 3.

Elliptic curves defined in this way are always supersingular and admit subexponential attacks via the MOV and FR reductions anyway [9, 21] (with subexponential parameter 1/3 instead of 1/2). We would expect these attacks to be more efficient than the GHS attack. Of course, analogous remarks hold for elliptic curves in even characteristic.

We remark that the main use of elliptic curves in characteristic three appears to be in identity based cryptography [4]. For efficiency reasons one usually considers supersingular curves. An alternative Weil descent construction for ordinary elliptic curves in characteristic three is described in [1].

9 The Kernel of the Norm-Conorm Homomorphisms

In this section we prove the main results about the norm-conorm homomorphism which have been used in the proofs of Theorem 7 and Theorem 14.

Lemma 16 *Let C/F be a finite extension of function fields and E_1, E_2 two intermediate function fields which are linearly disjoint over F. We have*

$$\mathrm{N}_{C/E_2}(\mathrm{Con}_{C/E_1}(x)) \;=\; [C : E_1E_2]\,\mathrm{Con}_{E_2/F}(\mathrm{N}_{E_1/F}(x))$$

for all divisor classes $x \in \mathcal{C}l(E_1)$.

Proof. We have $\mathrm{N}_{C/E_1E_2}(\mathrm{Con}_{C/E_1E_2}(y)) = [C : E_1E_2]\, y$ so by the transitivity of the norm and conorm we can assume $C = E_1E_2$. Furthermore, it suffices to prove the assertion for all but finitely many places $x = P$ of E_1. Namely, given any finite set of places of E_1, every divisor class in E_1 has a representing divisor whose support is disjoint from this set of places, by the approximation theorem.

Because E_1 and E_2 are linearly disjoint over F we have $[E_1E_2 : E_1] = [E_2 : F]$ and $E_1 \cap E_2 = F$. Furthermore, for almost all places P of E_1, the splitting behaviour of P in E_1E_2 is the same as that of $P \cap F$ in E_2 (i.e. their respective conorms $\mathrm{Con}_{E_1E_2/E_1}(P)$ and $\mathrm{Con}_{E_2/F}(P \cap F)$ consist of the same number of places with the same relative degrees and ramification indices). If P' is any place of E_1E_2 above such a P, then by symmetry we have for the relative degrees $f(P'/P' \cap E_2) = f(P/P \cap F)$. Since $\mathrm{N}_{E_1E_2/E_2}(P') = f(P'/P' \cap E_2)(P' \cap E_2)$ and $\mathrm{N}_{E_1/F}(P) = f(P/P \cap F)(P \cap F)$ this gives $\mathrm{N}_{E_1E_2/E_2}(\mathrm{Con}_{E_1E_2/E_1}(P)) = f(P/P \cap F)\mathrm{Con}_{E_2/F}(P \cap F) = \mathrm{Con}_{E_2/F}(\mathrm{N}_{E_1/F}(P))$.

The multiplication-by-m map for $m \in \mathbb{Z}$ is denoted by $[m]$. In the following we use the notation and situation of section 2, and view the norm and conorm maps as maps of the corresponding divisor class groups. Let V denote a subgroup of U_1 such that $VE \subseteq E$, that is, V restricts to a subgroup of $\mathrm{Aut}(E)$. Let W denote the largest subgroup of V such that $E^W = E$. We define

$$\phi^V : \mathcal{C}l(E^V) \to \mathcal{C}l(C^{U_1}) \qquad (17)$$

via the composition $\phi^V = \mathrm{N}_{C^V/C^{U_1}} \circ \mathrm{Con}_{C^V/E^V}$.

Theorem 18 *We have*

$$\phi \;=\; \phi^V \circ [\#W] \circ \mathrm{N}_{E/E^V}. \tag{19}$$

The kernel of ϕ thus consists at least of all elements contained in the kernel of the map $[\#W] \circ \mathrm{N}_{E/E^V}$.

Proof. The extensions C^W/C^V and E/E^V are Galois with group V/W since W is the kernel of the restriction map $V \to \mathrm{Aut}(E)$ and is hence normal in V. The fields E and C^V are then linearly disjoint over E^V because $E \cap C^V = E^V$, $[E : E^V] = (V : W)$, $EC^V = C^W$ and $[EC^V : C^V] = [C^W : C^V] = (V : W)$ by the definition of W and Galois theory. From Lemma 16, the transitivity of the norm and conorm maps and $\mathrm{N}_{C/C^W} \circ \mathrm{Con}_{C/C^W} = [\#W]$ we obtain

$$\begin{aligned}
\phi &= \mathrm{N}_{C/C^{U_1}} \circ \mathrm{Con}_{C/E} \\
&= [\#W] \circ \mathrm{N}_{C^W/C^{U_1}} \circ \mathrm{Con}_{C^W/E} \\
&= [\#W] \circ \mathrm{N}_{C^V/C^{U_1}} \circ \mathrm{Con}_{C^V/E^V} \circ N_{E/E^V} \\
&= [\#W] \circ \phi^V \circ \mathrm{N}_{E/E^V} \\
&= \phi^V \circ [\#W] \circ \mathrm{N}_{E/E^V},
\end{aligned}$$

which proves (19). The statement about the kernel of ϕ is clear.

We remark that Theorem 18 can basically be applied recursively in the following way. Let C_V be the normal closure of C^V over C^{U_1}, and let $\phi_V : \mathcal{C}l(E^V) \to \mathcal{C}l(C^{U_1})$ be defined by $\phi_V = \mathrm{N}_{C_V/C^{U_1}} \circ \mathrm{Con}_{C_V/E^V}$. Then $\phi_V = [[C_V : C^V]] \circ \phi^V$ and Theorem 18 can be applied to ϕ_V with V replaced by any larger group V' such that $V'E^V \subseteq E^V$.

Let $U_1//V$ denote a set of coset representatives such that $U_1 = \cup_{\sigma \in U_1//V} \sigma V$ and $1 \in U_1//V$, and denote the restriction of σ to E by σ_E. We assume in the following that $E \cap \sigma E$ is a function field and that E and σE are linearly disjoint over $E \cap \sigma E$ for every $\sigma \in U_1$. The latter will for example be the case if at least one of E and σE is Galois over $E \cap \sigma E$.

Theorem 20 *Abbreviating $Z = \mathrm{Con}_{E/E^V}(\mathrm{N}_{E/E^V}(\ker \phi))$ we have*

$$[C : E](V : W)Z \;\subseteq\; \sum_{\substack{\sigma \,\in\, U_1//V \\ \sigma \,\neq\, 1}} [C : E\,\sigma E]\,(V : W)\,\mathrm{Con}_{E/E\cap\sigma E}(\mathrm{N}_{\sigma E/E\cap\sigma E}(\sigma_E(Z))). \tag{21}$$

Proof. The extensions C/C^{U_1} and E/E^V are Galois with groups U_1 and V/W respectively. We have

$$\begin{aligned}
\mathrm{Con}_{C/C^{U_1}} \circ \mathrm{N}_{C/C^{U_1}} &= \sum_{\sigma \in U_1} \sigma, \\
\sigma \circ \mathrm{Con}_{C/E} &= \mathrm{Con}_{C/\sigma E} \circ \sigma_E, \\
\sum_{\tau \in V} \tau_E &= [(V : W)] \circ \mathrm{Con}_{E/E^V} \circ \mathrm{N}_{E/E^V}
\end{aligned}$$

for any $\sigma \in U_1$. We obtain using Lemma 16 in the fifth equation

$$\begin{aligned}
\mathrm{N}_{C/E}\circ \mathrm{Con}_{C/C^{U_1}} \circ \phi \;&=\; \mathrm{N}_{C/E} \circ \mathrm{Con}_{C/C^{U_1}} \circ \mathrm{N}_{C/C^{U_1}} \circ \mathrm{Con}_{C/E} \\
&= \mathrm{N}_{C/E} \circ \Big(\sum_{\sigma\in U_1} \sigma\Big) \circ \mathrm{Con}_{C/E} \\
&= \sum_{\sigma\in U_1} \mathrm{N}_{C/E} \circ \sigma \circ \mathrm{Con}_{C/E} \qquad (22)\\
&= \sum_{\sigma\in U_1} \mathrm{N}_{C/E} \circ \mathrm{Con}_{C/\sigma E} \circ \sigma_E \\
&= \sum_{\sigma\in U_1} [[C : E\,\sigma E]] \circ \mathrm{Con}_{E/E\cap\sigma E} \circ \mathrm{N}_{\sigma E/E\cap\sigma E} \circ \sigma_E \\
&= \sum_{\sigma\in U_1//V} [[C : E\,\sigma E]] \circ \mathrm{Con}_{E/E\cap\sigma E} \circ \mathrm{N}_{\sigma E/E\cap\sigma E} \circ \sigma_E \circ \Big(\sum_{\tau\in V} \tau_E\Big) \\
&= \sum_{\sigma\in U_1//V} [[C : E\,\sigma E]] \circ \mathrm{Con}_{E/E\cap\sigma E} \circ \mathrm{N}_{\sigma E/E\cap\sigma E} \circ \sigma_E \circ \\
&\qquad \circ [(V : W)] \circ \mathrm{Con}_{E/E^V} \circ \mathrm{N}_{E/E^V}.
\end{aligned}$$

If $x \in \ker\phi$ and $z = \mathrm{Con}_{E/E^V}(\mathrm{N}_{E/E^V}(x))$, writing the summand for $\sigma = 1$ separately we thus have

$$\begin{aligned}
\mathrm{N}_{C/E}(\mathrm{Con}_{C/C^{U_1}}(\phi(x))) \;&=\; [C : E](V : W) \cdot z \\
&+ \sum_{\substack{\sigma\,\in\, U_1//V \\ \sigma\,\neq\,1}} [C : E\,\sigma E]\,(V : W)\,\mathrm{Con}_{E/E\cap\sigma E}(\mathrm{N}_{\sigma E/E\cap\sigma E}(\sigma_E(z))) \;=\; 0,
\end{aligned}$$

thereby proving equation (21) and the theorem.

Proposition 23 *Assume that V is normal in U_1. Then $\sigma(E^V) = (\sigma E)^V$ and $E^V \cap \sigma E^V = (E \cap \sigma E)^V$ is a function field for every $\sigma \in U_1$. Furthermore, if the kernel of the restriction map $V \to \mathrm{Aut}(E)$ is equal to the kernel of the restriction map $V \to \mathrm{Aut}(E\cap\sigma E)$, then E^V and σE^V are linearly disjoint over $E^V \cap \sigma E^V$.*

Proof. Since V is normal in U_1 it is an automorphism group of E and σE, and we have $\sigma(E^V) = (\sigma E)^V$. Thus $E^V \cap \sigma(E^V) = E^V \cap (\sigma E)^V \subseteq (E \cap \sigma E)^V$ because $E^V \cap (\sigma E)^V$ is contained in $E\cap\sigma E$ and fixed by V. Conversely, $(E \cap \sigma E)^V \subseteq E^V$ and $(E \cap \sigma E)^V \subseteq (\sigma E)^V$ and hence $(E \cap \sigma E)^V \subseteq E^V \cap (\sigma E)^V$ and in conclusion $E^V \cap \sigma E^V = (E \cap \sigma E)^V$. By Galois theory, $E \cap \sigma E$ is of finite degree over $E^V \cap \sigma E^V$ since V is finite, and thus $E^V \cap \sigma E^V$ is a function field because $E \cap \sigma E$ is a function field.

The group W is the kernel of the restriction map $V \to \mathrm{Aut}(E)$, and is normal in V. Furthermore $\sigma W \sigma^{-1} \subseteq V$ for any $\sigma \in U_1$, and $W \sigma W \sigma^{-1} \subseteq \ker(V \to \mathrm{Aut}(E \cap \sigma E)) = W$, where the last equation holds by assumption. It follows that $\sigma W \sigma^{-1} = W$, and that W is normal in U_1.

We have $E^V\sigma E^V \subseteq (E\sigma E)^V$ and want to show equality. The extension $E\sigma E/(E\sigma E)^V$ is Galois with group V/W, using that $\ker(V \to \mathrm{Aut}(E\sigma E)) = W \cap \sigma W \sigma^{-1} = W$. Thus $(V : W) = [E\sigma E : (E\sigma E)^V] \leq [E\sigma E : E^V\sigma E^V]$. On the other hand, we obtain $(V : W) \geq [E\sigma E : E^V\sigma E^V]$ as follows. We have $E = E^V(E \cap \sigma E)$, because $E^V(E \cap \sigma E)$ is an intermediate field of the Galois extension E/E^V with group V/W, and its fix group is W/W using that $W = \ker(V \to \mathrm{Aut}(E \cap \sigma E))$. Similarly $\sigma E = \sigma E^V(E \cap \sigma E)$. It follows that $E\sigma E = E^V\sigma E^V(E \cap \sigma E)$. Then $(V : W) = [E \cap \sigma E : (E \cap \sigma E)^V] \geq [E^V\sigma E^V(E \cap \sigma E) : E^V\sigma E^V(E \cap \sigma E)^V] = [E\sigma E : E^V\sigma E^V]$, as desired. We obtain that $[(E\sigma E)^V : E^V\sigma E^V] = 1$ and thus $(E\sigma E)^V = E^V\sigma E^V$.

The linear disjointness of E^V and σE^V over $E^V \cap \sigma E^V$ now follows because E and σE are linearly disjoint over $E \cap \sigma E$ and the indices $[E : E^V]$, $[\sigma E : \sigma E^V]$, $[E\sigma E : E^V\sigma E^V]$ and $[E \cap \sigma E : E^V \cap \sigma E^V]$ are all equal to $(V : W)$, observing $(E\sigma E)^V = E^V\sigma E^V$ and $(E \cap \sigma E)^V = E^V \cap \sigma E^V$.

Theorem 24 *Under the assumptions of Proposition 23 we have that*

$$[C^V : E^V] \cdot \ker \phi^V \subseteq \sum_{\substack{\sigma \in U_1/V \\ \sigma \neq V}} \mathrm{Con}_{E^V/E^V \cap \sigma E^V}\big(\mathcal{C}l^0(E^V \cap \sigma E^V)\big), \tag{25}$$

and the kernel of ϕ is contained in the preimage of the right hand side under the map $[[C : E]] \circ \mathrm{N}_{E/E^V}$.

Proof. By Proposition 23 we can apply Theorem 20 replacing ϕ by ϕ^V and V by $\{1\}$. Then $W = \{1\}$ and (25) follows from Theorem 20, (21). Oberserving $[C : E](V : W) = \#V[C^V : E^V]$ and hence $[C^V : E^V]\#W = [C : E]$ we obtain $[[C^V : E^V]\#W] \circ \mathrm{N}_{E/E^V} = [[C : E]] \circ \mathrm{N}_{E/E^V}$. The statement about the kernel of ϕ then follows from (25) and Theorem 18.

10 *L*-Polynomials

In this section we prove a general theorem about the L-polynomials of certain subfields of a Galois extension of global function fields with Galois group a semidirect product. The theorem and its corollary are used in the proofs of Theorem 12 and Theorem 15. We remark that the L-polynomial of a global function field is the characteristic polynomial of Frobenius with the coefficients in reversed order.

Let G be a finite subgroup of $\mathrm{Aut}(C)$ and let H and U_1 be subgroups of G such that H is normal in G, $H \cap U_1 = \{1\}$ and $G = HU_1$. The subgroup U_1 operates on H by conjugation. Assume further that H is elementary abelian of prime exponent l and let $\{\, H_\nu \mid \nu \in I \,\}$ be a system of representatives under the operation of U_1 on the subgroups of H of index l for some index set I. Let $U_{1\nu}$ be the largest subgroup of U_1 which leaves H_ν invariant, and for any subgroup A of G denote the degree of the exact constant field of C^A over that of C^G by d_{C^A}.

Theorem 26 *Under the above assumptions the L-polynomials satisfy*

$$L_{C^{U_1}}(t^{d_{C^{U_1}}}) \,/\, L_{C^G}(t) \;=\; \prod_{\nu\in I} L_{C^{H_\nu U_{1\nu}}}(t^{d_{C^{H_\nu U_{1\nu}}}}) \,/\, L_{C^{HU_{1\nu}}}(t^{d_{C^{HU_{1\nu}}}}). \tag{27}$$

Proof. Since conjugation by elements of $U_{1\nu}$ maps H_ν and H to themselves, $H_\nu U_{1\nu}$ and $HU_{1\nu}$ are subgroups of G. Furthermore, $HU_{1\nu}$ is in fact the normaliser of H_ν in G because $G = HU_1$ and H_ν is normal in H. The factor group $HU_{1\nu}/H_\nu$ is then a semi direct product of H/H_ν and $H_\nu U_{1\nu}/H_\nu$.

We start with a statement on (non-abelian) characters. The following notation is used: Principal characters are denoted by 1, induced characters are prefixed by ind with the subgroup and group as subscript and superscript, and $\chi^{(\nu)}$ denotes the character obtained by lifting a character χ of $HU_{1\nu}/H_\nu$ to $HU_{1\nu}$. We claim

$$\mathrm{ind}_{U_1}^G(1) - 1 \;=\; \sum_{\nu\in I} \mathrm{ind}_{HU_{1\nu}}^G\Big(\big(\mathrm{ind}_{H_\nu U_{1\nu}/H_\nu}^{HU_{1\nu}/H_\nu}(1) - 1\big)^{(\nu)}\Big). \tag{28}$$

We postpone the proof of (28) and continue to prove (27). Using Artin L-series and their functorial properties (see [23, VII.10]) we obtain straightforward

$$\begin{aligned}
\zeta_{C^{U_1}}(s)\,/\,\zeta_{C^G}(s) \;&=\; L\big(C/C^{U_1}, 1, s\big) \,/\, L\big(C/C^G, 1, s\big)\\
&=\; L\big(C/C^G, \mathrm{ind}_{U_1}^G(1) - 1, s\big)\\
&=\; \prod_{\nu\in I} L\Big(C/C^G, \mathrm{ind}_{HU_{1\nu}}^G\Big(\big(\mathrm{ind}_{H_\nu U_{1\nu}/H_\nu}^{HU_{1\nu}/H_\nu}(1) - 1\big)^{(\nu)}\Big), s\Big)\\
&=\; \prod_{\nu\in I} L\Big(C/C^{HU_{1\nu}}, \big(\mathrm{ind}_{H_\nu U_{1\nu}/H_\nu}^{HU_{1\nu}/H_\nu}(1) - 1\big)^{(\nu)}, s\Big)\\
&=\; \prod_{\nu\in I} L\big(C^{H_\nu}/C^{HU_{1\nu}}, \mathrm{ind}_{H_\nu U_{1\nu}/H_\nu}^{HU_{1\nu}/H_\nu}(1) - 1, s\big)\\
&=\; \prod_{\nu\in I} L\big(C^{H_\nu}/C^{H_\nu U_{1\nu}}, 1, s\big) \,/\, L\big(C^{H_\nu}/C^{HU_{1\nu}}, 1, s\big)\\
&=\; \prod_{\nu\in I} \zeta_{C^{H_\nu U_{1\nu}}}(s) \,/\, \zeta_{C^{HU_{1\nu}}}(s).
\end{aligned}$$

Let q denote the cardinality of the exact constant field of C^G. Switching from the s-definition to the t-definition of the Zeta function of a global function field over the full constant field of q^d elements happens by composing $\zeta^{(t)} = \zeta^{(s)} \circ (-\log_{q^d})$. Observing $\log_{q^d}(t^d) = \log_q(t) = -s$ we obtain under abuse of notation

$$\zeta_{C^{U_1}}(t^{d_{C^{U_1}}}) \,/\, \zeta_{C^G}(t) \;=\; \prod_{\nu\in I} \zeta_{C^{H_\nu U_{1\nu}}}(t^{d_{C^{H_\nu U_{1\nu}}}}) \,/\, \zeta_{C^{HU_{1\nu}}}(t^{d_{C^{HU_{1\nu}}}}). \tag{29}$$

In general $\zeta^{(t)}(t^d) = L(t^d)/\big((1 - q^d t^d)(1 - t^d)\big)$ where $L(t)$ is the L-polynomial of a global function field over the full constant field of q^d elements. Furthermore,

$L(a^d) \neq 0$ for $|a| = 1$ or $|a| = q^{-1}$. Bringing the denominators $(1 - q^d t^d)(1 - t^d)$ to one side and the L-polynomials to the other side in (29) and comparing zeros and poles on each side we see that the denominators of the Zeta functions cancel out so that we obtain (27).

It remains to prove (28). If A is a finite group we denote by $\mathbb{C}[A]$ the regular representation space with character r_A, by $I_A = \{ \sum_{a \in A} \lambda_a a \mid \sum_{a \in A} \lambda_a = 0 \}$ the augmentation representation space with character $r_A - 1$ and by $\mathbb{C}\mathrm{N}_A$ for $\mathrm{N}_A = \sum_{a \in A} a$ the trivial representation space with character 1 of A.

In the following, all modules will be left modules. Assume that N is a normal subgroup of a finite group A with complement B (such that $NB = A$ is a semidirect product). The subgroup B operates by conjugation on N and from this the N-module structure of $\mathbb{C}[N]$ can be extended to an A-module structure, via $(nb)x = nbxb^{-1}$ for $n \in N$, $b \in B$ and $x \in \mathbb{C}[N]$. As A-modules we have

$$\mathbb{C}[N] \cong I_N \oplus \mathbb{C}\mathrm{N}_N \quad \text{and} \quad \mathbb{C}[N] \cong \mathbb{C}[A] \otimes_{\mathbb{C}[B]} \mathbb{C}\mathrm{N}_B = \mathrm{Ind}_B^A(\mathbb{C}\mathrm{N}_B) \tag{30}$$

where the second isomorphism is given by $x \mapsto x \otimes \mathrm{N}_B$, observing that N is a set of coset representatives for B in A and that B operates trivially on N_B. The equality holds by definition. We apply these observations to our case and obtain as G-modules

$$I_H \oplus \mathbb{C}\mathrm{N}_H \;\cong\; \mathrm{Ind}_{U_1}^G(\mathbb{C}\mathrm{N}_{U_1}) \tag{31}$$

and as $HU_{1\nu}/H_\nu$-modules

$$I_{H/H_\nu} \oplus \mathbb{C}\mathrm{N}_{H/H_\nu} \;\cong\; \mathrm{Ind}_{H_\nu U_{1\nu}/H_\nu}^{HU_{1\nu}/H_\nu}(\mathbb{C}\mathrm{N}_{H_\nu U_{1\nu}/H_\nu}), \tag{32}$$

taking the remarks at the beginning of the proof into account.

Next, let $\{ H_\nu \mid \nu \in J \}$ be the set of all subgroups of H of index l for some index set J such that $I \subseteq J$. Since H is elementary abelian we have

$$r_H - 1 = \sum_{\nu \in J} (r_{H/H_\nu} - 1)^{(*)} \tag{33}$$

where $(*)$ denotes the pull-back character with respect to $H \to H/H_\nu$. This can be seen as follows: The characters r_H and r_{H/H_ν} are the sums of all irreducible characters of H and H/H_ν respectively, and these characters are homomorphisms into μ_l, the group of l-th roots of unity in $\mathbb{C}$. Now every non-trivial irreducible character of H has precisely one of the H_ν as kernel due to the assumptions on H and is hence the pull-back of a uniquely defined non-trivial character of H/H_ν. Grouping together irreducible characters with the same kernel and summing up yields (33).

Using (33) we see that as H-modules

$$I_H \cong \sum_{\nu \in J} {I_{H/H_\nu}}^{(*)} \tag{34}$$

where ${I_{H/H_\nu}}^{(*)}$ is I_{H/H_ν} viewed as H-module. In fact, I_{H/H_ν} is even an $HU_{1\nu}$-module and we denote this by ${I_{H/H_\nu}}^{(\nu)}$. Let $\mathbb{C}[H]^{H_\nu}$ and $I_H^{H_\nu}$ be the submodules of $\mathbb{C}[H]$ and I_H fixed by H_ν respectively. For a system of coset representatives $H/\!/H_\nu$ it holds that $\mathbb{C}[H]^{H_\nu} = \{ \sum_{h \in H/\!/H_\nu} \lambda_h h \mathrm{N}_{H_\nu} \mid \lambda_h \in \mathbb{C} \}$ and

$I_H^{H_\nu} = \{ \sum_{h\in H//H_\nu, h\notin H_\nu} \lambda_h h \mathrm{N}_{H_\nu} \mid \lambda_h \in \mathbb{C} \}$, hence $\mathbb{C}[H]^{H_\nu} \cong \mathbb{C}[H/H_\nu]$ as $HU_{1\nu}$- and $HU_{1\nu}/H_\nu$-modules and $I_H^{H_\nu} \cong {I_{H/H_\nu}}^{(\nu)}$ as $HU_{1\nu}$-modules. The images of the ${I_{H/H_\nu}}^{(*)}$ under (34) in I_H are contained in and are in fact equal to the $I_H^{H_\nu}$, because H_ν operates trivially on these images and ${I_{H/H_\nu}}^{(*)} \cong I_H^{H_\nu}$. Equation 34 translates into the inner direct sum

$$I_H = \sum_{\nu\in J} I_H^{H_\nu}. \tag{35}$$

Now U_1 operates on the left and right hand side of (35) by conjugation, permuting the direct summands. More precisely we have $\sigma I_H^{H_\nu} = I_H^{\sigma H_\nu \sigma^{-1}}$ for $\sigma \in U_1$. The group $HU_{1\nu}$ is the largest subgroup of G which fixes H_ν, and a system $U_1//U_{1\nu}$ of coset representatives for $U_{1\nu}$ in U_1, such that $U_1 = \cup_{\sigma\in U_1//U_{1\nu}} \sigma U_{1\nu}$, is also a system of coset representatives for $HU_{1\nu}$ in G because H is normal in G. From these statements and the definition of I and J we obtain that as G-modules $\mathrm{Ind}_{HU_{1\nu}}^G(I_H^{H_\nu}) \cong \sum_{\sigma\in U_1//U_{1\nu}} I_H^{\sigma H_\nu \sigma^{-1}}$ and

$$I_H \cong \sum_{\nu\in I} \mathrm{Ind}_{HU_{1\nu}}^G(I_H^{H_\nu}), \tag{36}$$

all sums being direct. Substituting ${I_{H/H_\nu}}^{(\nu)}$ for $I_H^{H_\nu}$ in (36) gives

$$I_H \cong \sum_{\nu\in I} \mathrm{Ind}_{HU_{1\nu}}^G({I_{H/H_\nu}}^{(\nu)}) \tag{37}$$

as G-modules. Combining (31), (32) and (37) we obtain (28).

Corollary 38 *The genera satisfy the equation*

$$d_{C^{U_1}}\, g_{C^{U_1}} - g_{C^G} = \sum_{\nu\in I} \big(d_{C^{H_\nu U_{1\nu}}}\, g_{C^{H_\nu U_{1\nu}}} - d_{C^{HU_{1\nu}}}\, g_{C^{HU_{1\nu}}} \big). \tag{39}$$

Proof. Follows from taking the degrees on both sides of (27) since the degree of an L-polynomial is twice the genus.

The proof of Theorem 26 simplifies greatly for $U_1 = \{1\}$ using (28) only in the form (33), and then gives an alternative, short proof of the genus formula in [13].

11 Conclusion

Using statements for extensions with certain automorphism groups we have investigated the Weil descent methodology for general Artin-Schreier extensions. We have given a formula for the resulting genera and the zeta function and have discussed the kernel of the norm-conorm homomorphism. Our results apply in particular to hyperelliptic and elliptic curves in characteristic two. We have obtained a generalisation of the GHS attack making more elliptic curves vulnerable. The precise practical implications of the new construction are yet to be determined. We have also given a brief discussion of index calculus in the divisor class groups of the resulting curves and of further possible generalisations and applications of our techniques.

12 Acknowledgements

The author thanks C. Diem for helpful comments. This work was supported by the EPSRC.

References

1. S. Arita. Weil descent of elliptic curves over finite fields of characteristic three. In T. Okamoto, editor, *Advances in Cryptology - ASIACRYPT 2000*, LNCS 1976, pages 248–258, Kyoto, Japan, 2000. Springer-Verlag, Berlin-Heidelberg-New York.
2. E. Artin and J. Tate. *Class Field Theory*. Benjamin, New York, 1968.
3. I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography*. LMS Lecture Notes Series 265. Cambridge University Press, Cambridge, 1999.
4. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In J. Kilian, editor, *Advances in Cryptology - CRYPTO 2001*, LNCS 2139, pages 213–229. Springer-Verlag, Berlin-Heidelberg-New York, 2001.
5. C. Pandu Rangan and C. Ding, editors. *Progress in Cryptology - INDOCRYPT 2001*, LNCS 2247, Chennai, India, 2001. Springer-Verlag, Berlin-Heidelberg-New York.
6. M. Ciet, J.-J. Quisquater, and F. Sica. A secure family of composite finite fields suitable for fast implementation of elliptic curve cryptography. In C. Pandu Rangan and C. Ding [5], pages 108–116.
7. C. Diem. The GHS-attack in odd characteristic. *J. Ramanujan Math. Soc.*, 18(1), 2002.
8. G. Frey. How to disguise an elliptic curve. Talk at ECC'98, Waterloo, 1998.
9. G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62:865–874, 1994.
10. S. Galbraith. Weil descent of Jacobians. In D. Augot and C. Carlet, editors, *WCC2001 International workshop on coding and cryptography*, Electron. Notes Discrete Math. 6, Paris, 2001. Elsevier, Amsterdam.
11. S. Galbraith, F. Hess, and N. P. Smart. Extending the GHS Weil descent attack. In L. R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002*, LNCS 2332, pages 29–44, Amsterdam, 2002. Springer-Verlag, Berlin-Heidelberg-New York.
12. S. Galbraith and N. P. Smart. A cryptographic application of Weil descent. In M. Walker, editor, *Cryptography and Coding*, LNCS 1746, pages 191–200, Cirencester, 1999. Springer-Verlag, Berlin-Heidelberg-New York.
13. A. Garcia and H. Stichtenoth. Elementary abelian p-extensions of algebraic function fields. *manuscripta math.*, 72:67–79, 1991.
14. P. Gaudry, F. Hess, and N. P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. Cryptology*, 15(1):19–46, 2002.
15. F. Hess. *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern*. PhD Thesis, Technische Universität Berlin, 1999.

16. F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comp.*, 33(4):425–445, 2002.
17. F. Hess. Computing relations in divisor class groups of algebraic curves over finite fields. Submitted, 2003.
18. IETF. The Oakley key determination protocol. IETF RFC 2412, 1998.
19. M. Jacobson, A. Menezes, and A. Stein. Solving elliptic curve discrete logarithm problems using Weil descent. *J. Ramanujan Math. Soc.*, 16(3):231–260, 2001.
20. M. Maurer, A. Menezes, and E. Teske. Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree. In C. Pandu Rangan and C. Ding [5], pages 195–213.
21. A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Info. Theory*, 39:1639–1646, 1993.
22. A. Menezes and M. Qu. Analysis of the Weil descent attack of Gaudry, Hess and Smart. In D. Naccache, editor, *Progress in Cryptology - CT-RSA 2001*, LNCS 2020, pages 308–318, San Francisco, 2001. Springer-Verlag, Berlin-Heidelberg-New York.
23. J. Neukirch. *Algebraic Number Theory*. Springer-Verlag, Berlin-Heidelberg-New York, 1999.
24. N. P. Smart. How secure are elliptic curves over composite extension fields? In B. Pfitzmann, editor, *Advances in Cryptology - EUROCRYPT 2001*, LNCS 2045, pages 30–39, Innsbruck, 2001. Springer-Verlag, Berlin-Heidelberg-New York.
25. H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, Berlin-Heidelberg-New York, 1993.
26. N. Thériault. Weil descent attack for Artin-Schreier curves. Submitted, 2003.