The GHS Attack Revisited

F. Hess

Computer Science Department,
Woodland Road, University of Bristol, BS8 1UB, UK
florian@cs.bris.ac.uk

Abstract. We generalize the Weil descent construction of the GHS attack 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 almost square 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 [7], 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 [11] and Gaudry, Hess and Smart [12], in even characteristic (i.e. for q a power of 2). The construction of [12] 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 [12] as the GHS attack.

Menezes and Qu [20] 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 $\mathbb{F}_{2^{185}}$ [16]. Hence there is considerable interest as to whether the GHS attack makes all curves over these fields vulnerable. In [22] 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 [17] 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 [18]. 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 [5] discussed the security of fields of the form $\mathbb{F}_{2^{2d}}$ where d is a Sophie-Germain prime.

Galbraith, Hess and Smart [10] extended the GHS attack to isogeny classes of elliptic curves. The 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.

The GHS attack has also been generalized to hyperelliptic curves, in even characteristic by Galbraith [9] and odd characteristic by Diem [6].

In this paper we extend the GHS attack for elliptic curves in characteristic two even further, almost squaring the number of curves for which the basic GHS attack of [12] was previously applicable. In order to do so we generalize the construction of [12] and [9] to arbitrary Artin-Schreier extensions, and this enables us to utilize different Artin-Schreier equations than have been previously considered. These new results are then combined with the technique of [10].

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 [10]. 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 generalized construction, although they have the same genera as in [12], 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 conorm-norm homomorphism. In even characteristic special versions of these results have been presented in [13], and similar statements for the conorm-norm homomorphism have been independently obtained by Diem [6]. 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 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 organized as follows. In section 2 we describe the technique of Weil descent using Artin-Schreier extensions. In section 3 we specialize to elliptic curves and even characteristic, and generalize the construction of [12]. In section 4 we combine these results with the method of [10] thereby obtaining our new construction. In section 5 we investigate various possibly more effective extensions and variations, and in section 6 we address algorithmic issues of computing the final curves and solving the discrete logarithm problem. Due to lack of space some proofs had to be omitted but will appear in the full version of the paper.

2 Weil Descent with Artin-Schreier Extensions

In this section we briefly describe Artin-Schreier extensions, defined below, and explain how the discrete logarithm in the divisor class group of an Artin-Schreier curve 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 p be a prime, $q = p^r$, $k = \mathbb{F}_q$ and $K = \mathbb{F}_{q^n}$. We abbreviate $F = K(x)$ and let $f \in F$ be a rational function. A simple Artin-Schreier extension, denoted by E_f, is given by adjoining to F a root of the polynomial $y^p - y - f \in F[y]$. Examples of such extensions are the function fields of elliptic curves in characteristic two and three.

The Artin-Schreier operator is denoted by $\wp(y) = y^p - y$. We then also write $F(\wp^{-1}(f))$ for E_f and $\wp(F) = \{\, f^p - f \mid f \in F \,\}$. More generally we will use the following construction and theorem which is a special version of [21, p. 279, Theorem 3.3]:

Theorem 1 *Let $\bar{F}$ be a fixed separable closure of F. For every additive subgroup $\Delta \leq F$ with $\wp(F) \subseteq \Delta \subseteq F$ there is a field $C = F\big(\wp^{-1}(\Delta)\big)$ with $F \subseteq C \subseteq \bar{F}$ obtained by adjoining all roots of all polynomials $y^p - y - d$ for $d \in \Delta$ in $\bar{F}$ to F. Given this, the map*

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

defines a 1-1 correspondence between such additive subgroups Δ and abelian extensions C/F in $\bar{F}$ of exponent p.

We intend to apply this construction only for very special Δ which we introduce in a moment. By a Frobenius automorphism with respect to K/k of a function field over K we mean an automorphism of order $n = [K : k]$ of that function field which extends the Frobenius automorphism of K/k. Raising the coefficients of a rational function in $F = K(x)$ to the q-th power yields for example a Frobenius automorphism of F with respect to K/k, which we denote by σ.

For $f \in F$ we define $\Delta_f := \{\, d^p - d + \sum_{i=0}^{n-1} \lambda_i \sigma^i(f) \,|\, d \in F \text{ and } \lambda_i \in \mathbb{F}_p \,\}$. Also, let $m_f = \sum_{i=0}^{m} \lambda_i t^i$ with $\lambda_m = 1$ be the unique polynomial of smallest degree in $\mathbb{F}_p[t]$ such that $\sum_{i=0}^{m} \lambda_i \sigma^i(f) = d^p - d$ for some $d \in F$.

In the following we consider the field $C = F\big(\wp^{-1}(\Delta_f)\big)$ which exists by Theorem 1. One can show that it has degree $p^{\deg(m_f)}$ over F.

Given E_f and K/k, the basic idea of Weil descent with Artin-Schreier extensions is to derive certain conditions under which C admits a Frobenius automorphism with respect to K/k extending σ. One then forms the fixed field C_0 of that automorphism, which is the function field of a curve defined over k and has the same genus as C. The discrete logarithm problem is mapped from $\mathcal{C}l^0(E_f)$ to $\mathcal{C}l^0(C_0)$, the divisor class groups of degree zero divisors of E_f and C_0, using the composition of the conorm map Con_{C/E_f} and the norm map N_{C/C_0}. There are thus three main questions:

1. Under which conditions does σ extend to a Frobenius automorphism of C with respect to K/k?
2. What is the genus of C?
3. Is the discrete logarithm problem preserved under the conorm-norm map?

In the full version of the paper we answer these questions for general Artin-Schreier extensions in every characteristic. For the sake of simplicity and since it is the most interesting case we restrict to elliptic curves in characteristic two in this paper. We only note the following theorem, where g_C and g_{E_f} denote the genus of C and E_f respectively.

Theorem 2 *Assume* $\deg(m_f) \geq 2$, $\Delta_f \cap K \subseteq \wp(F)$ *and that* $F\big(\wp^{-1}(f, \sigma(f))\big)$ *has genus greater than* 1. *The genus of* C *then satisfies*

$$g_{E_f}\, p^{\deg(m_f)-2} + 1 \;\leq\; g_C \;\leq\; g_{E_f} \cdot n\, (p^{\deg(m_f)} - 1)/(p-1).$$

The cofactor n in the upper bound can be dropped if f has σ-invariant poles. The theorem means that any attack using an Artin-Schreier construction fails if $\deg(m_f)$ is too large since the genus of C is exponential in $\deg(m_f)$. A lower bound for $\deg(m_f)$ is given by the smallest degree of a non-linear factor in $\mathbb{F}_p[t]$ of the polynomial $t^n - 1 \in \mathbb{F}_p[t]$. For prime values of n this is usually too big. We remark that the conditions of the theorem are not restrictive in our situation. If one of them is not satisfied the discrete logarithm problem would in practice not be preserved when mapped to C_0.

3 Generalizing the basic GHS Attack

The Artin-Schreier construction of [12] applies 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 of characteristic two. We now describe a generalization of this construction, along the lines of the previous section.

Let $p = 2$ and $f = \gamma/x + \alpha + \beta x$ for $\gamma, \alpha, \beta \in K$ with $\gamma\beta \neq 0$. We define Δ_f and C as in section 2. Also, we define the polynomials m_γ and m_β for γ and β as m_f for f in section 2. Then

$$m_f = \begin{cases} \mathrm{lcm}(m_\gamma, m_\beta) & \text{if } \alpha = d^2 + d \text{ for some } d \in K, \\ \mathrm{lcm}(m_\gamma, m_\beta, t+1) & \text{otherwise.} \end{cases} \tag{3}$$

We remark that $\alpha = d^2 + d$ for some $d \in K$ is equivalent to $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$.

The following two theorems answer the first two questions stated above.

Theorem 4 *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.*

If at least one of the conditions of the Theorem is satisfied, then C/F is necessarily regular (that is, K is algebraically closed in C).

Theorem 5 *If C/F is regular then the genus of $C = F(\wp^{-1}(\Delta))$ is given by*

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

Before we proceed to answer the third question stated above we pause to explain how the results of [12], except for the hyperellipticity, can be recovered from these two theorems. In [12] the special case $\gamma = 1$ is considered where C/F is necessarily regular. Let $m = \deg(m_f)$. 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 [18] is necessary and sufficient and that condition (†) of [12] is sufficient for the existence of the Frobenius automorphism. For the genus of C we obtain $2^{m-1} - 2^{m-\deg(m_\beta)} + 1$. 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 $2^{m-1} - 1$, as in [12]. In addition we now obtain the following more precise statement.

Corollary 6 *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 $u = 2^{v_2(n)}$.*

We continue the discussion and address the above third question. We assume that the conditions of Theorem 4 are fulfilled so that σ extends to a Frobenius automorphism of C with respect to K/k, again denoted by σ. For $h \in \Delta_f$ 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 yields an automorphism of E_h. This means that E_h is the constant field extension of an elliptic curve defined over $\mathbb{F}_{q^{s(h)}}$. For example, if $n/s(h)$ is odd then $E_h = E_{\tilde{h}}$ where $\tilde{h} = c/x + \mathrm{Tr}_{K/\mathbb{F}_{q^{s(h)}}}(a) + bx \in \mathbb{F}_{q^{s(h)}}(x)$. Let us denote by $\tilde{E}_h$ the fixed field of $\sigma^{s(h)}$ in E_h.

Theorem 7 *For the homomorphism* $\phi_h : \mathcal{C}l^0(E_h) \to \mathcal{C}l^0(C_0)$ *given by* $\mathrm{N}_{C/C_0} \circ \mathrm{Con}_{C/E_h}$ *we have under the conditions of Theorem 4 that*

$$\mathrm{N}^{-1}_{E_h/\tilde{E}_h}(0) \subseteq \ker(\phi_h) \subseteq \mathrm{N}^{-1}_{E_h/\tilde{E}_h}(\mathcal{C}l^0(\tilde{E}_h)[2^{\deg(m_f)-1}]).$$

We are of course mainly interested in the case $h = f$. The theorem means in words, that if E_h is not defined by a subfield curve, that is $s(h) = n$, then the kernel of the conorm-norm homomorphism contains only elements of order dividing $2^{\deg(m_f)-1}$. Since the discrete logarithm problem on E_f lives in a cyclic group of large prime order it is preserved under the conorm-norm homomorphism. On the other hand, if E_f is defined by a subfield curve, then the kernel of the conorm-norm homomorphism does contain the large prime factor and the discrete logarithm problem is not preserved. Note that by applying a suitable change of variables $x \mapsto \lambda x$ the method can be made to work for subfield curves nevertheless.

Interestingly, C_0 is in a sense universal in that it preserves discrete logarithms in large prime subgroups for all E_h and $h \in \Delta_f$ with $s(h) = n$. We also remark that if the conditions of Theorem 4 are not fulfilled, then σ may still be extended to C but not as a Frobenius automorphism with respect to K/k. Theorem 7 remains true for this case with $\tilde{E}_h$ necessarily a rational function field, so that the discrete logarithm problem is not preserved (see the full version of the paper).

We finish the general discussion with a formula for the characteristic polynomial of Frobenius of C_0 over k. Let S be a set of elements $h = c/x + a + bx$ in Δ_f such that $h_1 \neq \sigma^i(h_2)$ for all $h_1, h_2 \in S$, $h_1 \neq h_2$ and $0 \leq i \leq n-1$, and such that for every $h_1 \in \Delta_f$ there exists an $h_2 \in S$ and $0 \leq i \leq n-1$ with $h_1 = \sigma^i(h_2)$. Let us write $\chi_{\tilde{E}_h}(t)$ and $\chi_{C_0}(t)$ for the characteristic polynomials of Frobenius of $\tilde{E}_h$ and C_0 (note the different constant fields).

Theorem 8 *Under the conditions of Theorem 4 we have that*

$$\chi_{C_0}(t) = \prod_{h \in S} \chi_{\tilde{E}_h}(t^{s(h)}).$$

4 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 normalization of α is also possible for the more general Artin-Schreier equations $y^2 + y = \gamma/x + \alpha + \beta x$ of section 3.

It was the equation $y^2 + y = 1/x + \alpha + \beta^{1/2}x$ which has been used in [12] 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 also 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 2, 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 3. 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 3 and reduce the discrete logarithm problem on E to that in the divisor class group of a higher genus curve defined over k. The only 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 $\beta = \gamma_2/\gamma_1$. Heuristically we expect that the map $(\gamma_1, \gamma_2) \mapsto \gamma_2/\gamma_1$ is almost injective for the γ_1, γ_2 under consideration, and this is also confirmed by examples. It follows that we almost square 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 [10]. Assume for simplicity that r, n are odd and n is prime so that $\alpha \in \mathbb{F}_2$ according to the above. Over $\mathbb{F}_2$ we have the factorization into irreducible polynomials $t^n + 1 = (t+1)h_1 \cdots h_s$ and $\deg(h_i) = d$ such that $n = sd + 1$. In this situation the first non-trivial m satisfies $d \le m \le d+1$, yielding $m_f = h_i$ or $m_f = (t+1)h_i$ by equation (3). Due to our generalization we do not necessarily have $m = d+1$ as in [10, 12], and in fact we are now concentrating on $m = d$. The number of elliptic curves defined by an Artin-Schreier equation as in section 3 with $\alpha \in \mathbb{F}_2$ and $d \le m \le d+1$ is approximately equal to $2sq^{2d+2}$ whereas the number of elliptic curves among these with $m = d$ (implies $\alpha = 0$) is approximately equal to sq^{2d}. As in [10] we expect nr but no more of these to lie in the same isogeny class.

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 Theorem 4 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 5. Note that in [10, 12] 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 [2, 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 [10] that a proportion of $\min\{1, sq^{2d}/(q^{n/2}nr)\}$ 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 $N + O(q^{n/4+\varepsilon})$ and probability $\min\{1, N/q^{n/2}\}$, where $N \leq sq^{2d}/(nr)$.

The case $n = 31$ and $r = 5$ is particularly interesting since there is an IPsec curve [16] 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 [17]. The heuristic probability that a random elliptic curve gives rise to a curve of genus 31 is approximately 2^{-52} with the method in [10], whereas now we obtain

$$sq^{2d}/(q^{n/2}nr) \approx 2^{-32}.$$

The only algorithm known so far to find the elliptic curves from which the corresponding higher genus curve are computed requires the order of $sq^{2d}/(nr) \approx 2^{45}$ many operations in $\mathbb{F}_{2^{155}}$ ($q^{n/4} \approx 2^{38}$ 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, and this problem has not been studied in detail yet.

5 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.

5.1 Subfields and Automorphisms

A possibility of improving the construction in section 2 and section 3 would be to consider subfields L of C_0 and use $\phi_{f,L} = \mathrm{N}_{C_0/L} \circ \phi_f$ with ϕ_f from Theorem 7 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_0/F_0. But in this case the kernel of $\phi_{f,L}$ would contain the large prime factor, as shown in the full version of the paper, hence $\phi_{f,L}$ and intermediate fields of C_0/F_0 are not of any use.

We could still search for other subfields L of C_0 which do not contain F_0 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 $\rho(\Delta_f) \subseteq \Delta_f$ it should be possible to extend ρ to C in a similar way as it was done with σ, under not too restrictive conditions. However, we have not found such automorphisms for non-subfield curves. This does not rule out the existence of useful subfields L but it appears unlikely that such subfields exist except maybe in very rare cases.

Although automorphisms of C_0/F_0 may not be useful to find suitable subfields L as indicated above, they could be of use to speed up the discrete logarithm computation in C_0. We are given $2^{\deg(m_f)}$ automorphisms in $G(C/F)$. As shown in the full version of the paper, no automorphism in $G(C/F)$ restricts to an automorphism of C_0, except when C_0 is hyperelliptic, in which case we only obtain the hyperelliptic involution. It is still possible that C_0 has automorphisms, but again we expect this to happen only in very rare cases.

5.2 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_0 is in general not an Artin-Schreier extension of degree 2 anymore so our techniques would not apply immediately. If we however start with an elliptic curve as in section 4 and consider an associated Artin-Schreier equation with $\gamma \in \mathbb{F}_{q^{n_1}}$ we do have that C_0 is hyperelliptic, or in other words that it is an Artin-Schreier extension of degree 2. 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 a genus of about 2^{n_1-1}. Using Theorem 2 the descent from $\mathbb{F}_{q^{n_1}}$ to k finally results in a curve of genus about $(2^{n_2}-1)2^{n_1-1} \le 2^{n_1+n_2-1}$. Thus if $n_1 \approx n_2$ this final curve has subexponential genus $\approx 2^{2\sqrt{n}}$ instead of exponential genus $\approx 2^n$.

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 $(2^5-1)^2$.

While theoretically interesting it does not appear that these results have any practical implications.

5.3 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 $\tilde{m} \ge m$ 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.

5.4 Other Composita

The field composita in section 2 and section 3 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 2 and section 3.

The methods of section 2 and section 3 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 [10].

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 2 remains valid in more general situations: Similar to section 2 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 minimize m in comparison with n. A possible generalization 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 3 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 3.

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.

5.5 The GHS Attack in Characteristic Three

Weil descent with Artin-Schreier extensions 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 [8, 19] (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 [3]. For efficiency reasons one usually considers supersingular curves. An alternative Weil descent construction for ordinary elliptic curves in characteristic three is described in [1].

6 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 2 and section 3 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.

6.1 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 $0 \leq i \leq m-1$ form an $\mathbb{F}_p$-basis of $\Delta_f/\wp(F)$. From Theorem 1 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 $0 \leq i \leq m-1$. 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. We obtain an explicit representation of the operation of σ on C.

The field C_0 is the fixed field of σ in C. Let $F_0 = k(x)$ be 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 $C_0 = F_0(\tilde{y})$, because $\tilde{y} \in C_0$ 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 a short calculation shows $\tau(\tilde{y}) = \tilde{y} + \sum_{i=0}^{n-1} \sigma^i(\mu)\lambda(\sigma^{-i}\tau\sigma^i)$. 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_0 in $F_0[t]$.

The discrete logarithm can be mapped from E_f to C_0 using the conorm map Con_{C/E_f} followed by the norm map N_{C/C_0}. 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_0} 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_0}.

6.2 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_0 of degree g_{C_0} 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 factorizations, and smoothness probabilities hold. Computing these divisor class representatives can be done by reduction techniques as described in [14], and this leads also to a way of computing in the divisor class group of C_0 which generalizes the Cantor method for hyperelliptic curves. We remark that for hyperelliptic curves addition takes $O(g_{C_0}^2)$ operations in k whereas for a general C_0 addition takes $O(g_{C_0}^4)$ operations in k, and is hence considerably slower.

The number of effective divisors of degree less than or equal to g_{C_0} containing places of degree less than or equal to d can usually be expressed as some explicit proportion of $q^{g_{C_0}}$. For example, for $g_{C_0} \to \infty$ and q fixed we have that this number of smooth divisors is approximately at least $q^{g_{C_0}} \exp(-(g_{C_0}/d)\log(g_{C_0}/d))$ for $g_{C_0}^{c_1} \leq d \leq g_{C_0}^{c_2}$ and $0 < c_1 < c_2 < 1$ fixed. From our formula for the characteristic polynomial of Frobenius of C_0 in Theorem 8 we see that $g_{C_0} = \sum_{h \in S} s(h)$ by taking degrees, and then for the cardinality of the divisor class group $\#\mathcal{C}l^0(C_0) = q^{g_{C_0}} \prod_{h \in S}(1 + O(q^{-s(h)/2}))$ 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 $O(\log(g_{C_0}))$ and $q \geq p^2$ it follows that $\#\mathcal{C}l^0(C_0) = q^{g_{C_0}} \prod_{s|n} \prod_{s(h)=s}(1 + O(p^{-s(h)})) = O(q^{g_{C_0}} g_{C_0}^c)$ 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 $\exp(-(1 + o(1))(g_{C_0}/d)\log(g_{C_0}/d))$ of all divisor classes of degree g_{C_0} will be representable by a smooth divisor, thus leading to the usual smoothness probability. This would allow for an in g_{C_0} subexponential running time with parameter 1/2 for solving the discrete logarithm. Fore more details on computing discrete logarithms for general curves see [15].

7 Acknowledgements

The author would like to thank N. P. Smart and S. Galbraith for helpful comments, and for the support by an EPSRC grant.

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, 2000. Springer-Verlag, Berlin-Heidelberg-New York.
2. I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography.* LMS Lecture Notes Series 265. Cambridge University Press, Cambridge, 1999.
3. 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.
4. C. Pandu Rangan and C. Ding, editors. *Progress in Cryptology - INDOCRYPT 2001*, LNCS 2247, Chennai, India, 2001. Springer-Verlag, Berlin-Heidelberg-New York.
5. 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 [4], pages 108–116.
6. C. Diem. The GHS-attack in odd characteristic. submitted, 2002.
7. G. Frey. How to disguise an elliptic curve. Talk at ECC' 98, Waterloo, 1998.
8. 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.

9. 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.
10. 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.
11. 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.
12. 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.
13. F. Hess. Extending the GHS Weil descent attack. Talk at ECC' 01, Waterloo, 2001.
14. F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comp.*, 33(4):425–445, 2002.
15. F. Hess. Computing relations in divisor class groups of algebraic curves over finite fields. Preprint, 2003.
16. IETF. The Oakley key determination protocol. IETF RFC 2412, 1998.
17. 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.
18. 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 [4], pages 195–213.
19. A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Info. Th.*, 39:1639–1646, 1993.
20. 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.
21. J. Neukirch. *Algebraic Number Theory.* Springer-Verlag, Berlin-Heidelberg-New York, 1999.
22. 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.