WEIL DESCENT OF JACOBIANS

STEVEN D. GALBRAITH

Abstract. The technique of Weil restriction of scalars has significant implications for elliptic curve cryptography. In this paper we apply these ideas to the case of the discrete logarithm problem in the Jacobian of a curve of genus greater than one over a finite field $\mathbb{F}_{q^n}$ where $n > 1$.

1. Introduction

The idea of using Weil restriction of scalars as a means to solve the elliptic curve discrete logarithm problem was suggested by Frey [5] and then developed further in [6] and [9].

In this paper we consider the Jacobian of a genus $g > 1$ curve C over a finite field $\mathbb{F}_{q^n}$ where q is a prime or a power of a prime and where $n > 1$. The discrete logarithm problem is as follows: Suppose there is a divisor D_1 in the divisor class group of C over $\mathbb{F}_{q^n}$ which has (large) prime order L. Then given any other divisor D_2 in the group generated by D_1 the problem is to find an integer λ such that $D_2 = \lambda D_1$.

As in the case of elliptic curves, one can consider the Weil restriction of the g-dimensional abelian variety $\mathrm{Jac}(C)$ with respect to the Galois extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ and obtain an Abelian variety A of dimension ng over $\mathbb{F}_q$. One then searches for a curve $\mathfrak{C}$ lying on A in such a way that one can pull the divisors D_1 and D_2 back to $\mathrm{Jac}(\mathfrak{C})(\mathbb{F}_q)$ and then solve the discrete logarithm problem there using one of the available algorithms (see [1], [4], [8]) for solving such problems on 'high' genus curves.

Before giving flesh to this skeleton, we discuss the practical situation we have in mind.

2. The Cryptographic Application

The most relevant cases of Jacobians of curves for cryptography are when C is a hyperelliptic curve of genus 2 or 3 or possibly 4. For these cases there are few efficient methods to construct cryptographically suitable curves with known group order.

One commonly used method to construct curves with known group order is to use 'subfield curves', i.e., curves C defined over a small field $\mathbb{F}_q$ but considered as a group over some larger extension field $\mathbb{F}_{q^l}$ (the group order can be deduced from the characteristic polynomial of the Frobenius map).

Date: February 1, 2011.

Key words and phrases. Weil descent, hyperelliptic curve cryptography.

This research was supported by the NRW-Initiative für Wissenschaft und Wirtschaft "Innovationscluster für Neue Medien" and cv cryptovision gmbh (Gelsenkirchen).

This strategy first appeared in Koblitz [11]. His examples involve curves $C/\mathbb{F}_2$ and the group used for cryptography is $\mathrm{Jac}(C)(\mathbb{F}_{2^l})$ for some prime number l. In practice we have $g = 2, 3$ and l roughly in the range $70 < l < 100$. We emphasise that, in practice, **it is always the case that the extension degree is prime**. Since otherwise it is not possible to obtain a group order which has very large prime factor.

One advantage with using subfield curves is that the action of the Frobenius endomorphism can be used to accelerate the arithmetic on these curves [11], [10]. However, this Frobenius action also makes the Pollard methods more effective as one can consider random walks on equivalence classes as in [3]. Therefore there is slightly less security than was first imagined from using these curves. Another drawback is that there are very few curves available when one restricts to curves over $\mathbb{F}_2$.

To obtain a larger number of examples and to reduce the effectiveness of the Pollard methods one might prefer to choose the original curve C over a slightly larger extension $\mathbb{F}_{2^n}$ and consider the group as $\mathrm{Jac}(C)(\mathbb{F}_{2^{nl}})$ for some prime number l. For curves of genus 2 or 3 we then take $2 \leq n \leq 5$ and correspondingly $12 < l < 50$ so that we have $gnl \sim 200$.

It is exactly the case outlined in the previous paragraph which will be the main focus of this paper. We will consider the Weil restriction of $\mathrm{Jac}(C)(\mathbb{F}_{2^{nl}})$ with respect to the extension $\mathbb{F}_{q^{nl}}/\mathbb{F}_{q^l}$ to obtain an abelian variety of dimension ng over $\mathbb{F}_{q^l}$. We show that Weil descent can give a feasible attack in this situation.

In this case the curve C is defined over the larger field with respect to the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$. This means that, from the point of view of Weil descent, the curve is not a 'subfield curve'. As emphasised above, Weil descent is rarely interesting for subfield curves as the corresponding field extensions always have fairly large prime degree. Of course, the techniques are also applicable in the case where the curve C is actually defined over the full field $\mathbb{F}_{2^{nl}}$, though this case is not so prominent in the applications.

This paper is primarily concerned with fields of characteristic two as they are the most important in practice. The odd characteristic case is discussed in Section 7.

It is not very easy to express the complexity of Weil descent in a meaningful sense (i.e., one which can be used to determine the security of a discrete logarithm problem). Part of the problem is a lack of experience with solving discrete logarithms on high genus curves (although see [4], [8], [12]). Examples 2 and 3 (subsections 4.7 and 4.8) show that there are cases of curves of genus 3 over certain field extensions for which the discrete logarithm problem is significantly easier to solve than had been previously thought (although still exponential complexity).

To completely avoid the threat of Weil descent one may use curves over prime fields $\mathbb{F}_p$ (where p is prime). Curves over fields of the form $\mathbb{F}_{2^l}$ where l is prime (and thus $l > 40$) will in general be resistant to the Weil descent attack. In particular, the curves in Koblitz [11] seem to resist our methods.

Of course there is a 'constructive' aspect to this work as in [9] (i.e., giving a method to construct abelian varieties or Jacobians with known group order). This is not as interesting as the elliptic curve case where the Schoof-Atkin-Elkies algorithm is available. Also, the abelian varieties arising will be very special (see [7] for a discussion of the elliptic curve case).

3. The Algebraic Approach

The approach given by Gaudry, Hess and Smart in [9] used only algebraic techniques (function fields and norm maps) and was extremely successful. We will mimic that approach in this paper. First, we explain the algebraic approach in geometric terms.

Let $K = \mathbb{F}_{q^n}$, $k = \mathbb{F}_q$ (where q is a power of any prime), let C be a curve of genus g over K and suppose we have a discrete logarithm problem $D_2 = \lambda D_1$ in the divisor class group $\mathrm{Pic}^0_K(C)$ of the curve. We identify the divisor class group $\mathrm{Pic}^0_K(C)$ with the K-valued points of the Jacobian $\mathrm{Jac}(C)$. A prime divisor on C over K corresponds to a place of the function field $K(C)$ and so we can manipulate divisors by manipulating places of the field.

The starting point of the approach of [9] is to construct a certain function field F over the field K. This is an algebraic field extension of $K(C)$ constructed specifically so that there is a Galois action which allows us to view F as having constant field k. In [9] this is motivated by taking a curve $\mathfrak{C}$ which lies on the Weil restriction of E/K and defining $F = K(\mathfrak{C})$.

In this paper we mimic the construction of F given in [9] (see subsection 4.2). At first sight there seems to no longer be any geometry in the picture since we have not written down any equations for the Weil restriction of the abelian variety $\mathrm{Jac}(C)$. However, given the function field F over K there exists some curve $\mathfrak{C}$ which (except for some special cases) may be defined over K and is such that $F = K(\mathfrak{C})$. The inclusion $K(C) \hookrightarrow K(\mathfrak{C})$ induces a rational map $\phi : \mathfrak{C} \to C$ of curves over K and this then induces a map of abelian varieties $\mathrm{Jac}(\mathfrak{C}) \to \mathrm{Jac}(C)$ over K.

The next step of [9] is to pull back the discrete logarithm problem to $\mathfrak{C}$. This is done using the conorm (see Stichtenoth [14] Definition III.1.8). The geometric picture behind the definition of the conorm is simply that, under the map $\phi : \mathfrak{C} \to C$, a place of C is pulled back to a divisor of places on $\mathfrak{C}$ counted with a multiplicity which corresponds to the ramification. A principal divisor (f) on C is pulled back to the principal divisor $(f \circ \phi)$.

We can therefore transfer the discrete logarithm problem from $\mathrm{Jac}(C)(K)$ to $\mathrm{Jac}(\mathfrak{C})(K)$. Now, by the construction of $F = K(\mathfrak{C})$ it follows (at least, except for some special cases) that $\mathfrak{C}$ can be defined over k. There is the inclusion $\mathrm{Jac}(\mathfrak{C})(k) \hookrightarrow \mathrm{Jac}(\mathfrak{C})(K)$ and it remains to pull the discrete logarithm problem back along this map. The obvious method to achieve this is to take a 'trace' map $D \in \mathrm{Pic}^0_K(\mathfrak{C}) \mapsto \sum_{\sigma \in \mathrm{Gal}(K/k)} D^\sigma \in \mathrm{Pic}^0_k(\mathfrak{C})$. The norm map of [9] is precisely this trace converted to the function field notation. The image of a principal divisor (f) is simply the principal divisor $(\prod_\sigma f^\sigma)$.

It is possible that some of these maps can be degenerate on certain divisors. However, this will happen with low probability in the general case.

4. A Specific Class of Curves

The Weil descent strategy outlined in the previous section applies in a very general way. The key step is the construction of the function field F. In this section we discuss a special class of curves C over fields of characteristic two, analogous to the elliptic curves considered in [9], for which we have a construction for the function field F. We can then prove some strong results about the curves $\mathfrak{C}$ which arise. In particular it is possible to bound the genus of the curves $\mathfrak{C}$ and to prove that they are hyperelliptic.

4.1. **The Curves.**

We let $k = \mathbb{F}_q$ be a finite field of characteristic two (i.e., $q = 2^t$) and let $K = \mathbb{F}_{q^n}$ be the Galois extension of k of degree n. A general hyperelliptic curve of genus g over a characteristic two field K is given by an equation of the form $y^2 + h(x)y = f(x)$ where $\deg(h(x)) \leq g + 1$ and $\deg(f(x)) \leq 2g + 2$.

In this section we consider the most commonly appearing special case, namely C given by an equation $y^2 + xy = f(x)$ where $f(x) = x^{2g+1} + a_{2g}x^{2g} + \cdots a_1 x + a_0$ is a monic polynomial of degree $2g + 1$ over K. Up to a change of variable (defined over K) this case includes all curves with $\deg(h(x)) = 1$. The case $\deg(h(x)) = 0$ is handled with the same ease. Cases where $\deg(h(x)) > 1$ can often be handled by these methods (see Examples Four and Five), but our theoretical results do not cope with this case.

Note that there will be further conditions imposed on C below and so not all curves can be handled using the method of this section.

4.2. **Weil Restriction.**

Let C be a curve over $K = \mathbb{F}_{q^n}$ of genus g with generic point (x, y). The Weil restriction of C with respect to the Galois extension $K/k = \mathbb{F}_{q^n}/\mathbb{F}_q$ is the variety whose generic point is $\prod_{\rho \in \mathrm{Gal}(K/k)}(x^\rho, y^\rho)$. In our case we let σ be a generator for $\mathrm{Gal}(K/k)$ and write (x_i, w_i) for the point $(x^{\sigma^i}, y^{\sigma^i})$. Each such point satisfies the equation $w_i^2 + x_i w_i = f^{\sigma^i}(x_i)$.

The principle adopted in [6] and [9] of taking a product over $\mathbb{P}^1$ of Galois twists of curves (equivalently, imposing that the function x is Galois invariant) gives rise to a function field $F = K(x, w_0, w_1, \ldots w_{n-1})$ defined by the equations

$$\begin{array}{rcl} w_0^2 + xw_0 & = & f(x) \\ w_1^2 + xw_1 & = & f^\sigma(x) \\ \vdots & \vdots & \vdots \\ w_{n-1}^2 + xw_{n-1} & = & f^{\sigma^{n-1}}(x). \end{array}$$

This is analogous to the variety $\mathfrak{D}$ of Section 3.1 of [9].

The first equation implies that $K(C)$ is a subfield of F. Indeed, F may be considered as an algebraic extension of $K(C)$ obtained by taking a sequence of quadratic extensions.

4.3. **Artin-Schreier Extensions.**

We now study the results of [9] in the context of our more general extension of function fields. We define the 'magic number' m to be such that $2^m = [F : K(x)]$. In general we have $m = n$.

To generalise the expression of m in terms of the dimension of a simple vector space as in [9] requires some care as the equations under consideration have more terms on the right hand side.

We now mimic the changes of variable used in [9] so that we can study the function field F by means of the theory of Artin-Schreier extensions. We make the change of variable $s_i = (w_i + \sqrt{a_0}^{\sigma^i})x^{-1}$ for $i = 0, 1, \ldots, n - 1$ to obtain the set of equations

$$s_i^2 + s_i = x^{2g-1} + a_{2g}^{\sigma^i} x^{2g-2} + \cdots + a_2^{\sigma^i} + (a_1^{\sigma^i} + \sqrt{a_0}^{\sigma^i})x^{-1} \qquad (1)$$

where $i = 0, 1, \ldots, n-1$. We then define $t_i = s_i + s_0$ for $i = 1, \ldots, n-1$ to obtain the set of equations

$$(2) \qquad t_i^2 + t_i = (a_{2g} + a_{2g}^{\sigma^i})x^{2g-2} + \cdots + (a_1 + \sqrt{a_0} + a_1^{\sigma^i} + \sqrt{a_0}^{\sigma^i})x^{-1}$$

where $i = 1, \ldots, n-1$. Clearly, $F = K(x, s_0, s_1, \ldots, s_{n-1}) = K(x, s_0, t_1, \ldots, t_{n-1})$.

At first our Artin-Schreier extensions (2) seem much more complicated than those in [9], and it seems unlikely that we can obtain equations of the form

$$t_i^2 + t_i = \gamma_i + \delta_i x^{-1} \qquad \text{or} \qquad t_i^2 + t_i = \gamma_i + \delta_i x.$$

The crucial property of the above two equations is linearity in x^{-1} or x and we will call them 'Type A' and 'Type B' respectively. However, recall that Artin-Schreier extensions are only defined up to terms of the form $\alpha^2 + \alpha$ and so one can easily eliminate any even-degree terms from the right hand side. Also recall that odd-degree terms (e.g., the term x^{2g-1}) will possibly have been removed by subtraction using the first equation.

Nevertheless, there are curves C for which this process does not give a non-trivial linear equation and the results of this section do not apply in those cases. We give a few examples to illustrate which curves can be tackled with this approach and which cannot. In all these examples we let c_i lie in k while elements $\theta \in K$ are chosen such that $\theta^{\sigma^i} \neq \theta$ for all $1 < i < n$ where σ generates $\mathrm{Gal}(K/k)$ (in particular, if θ does not lie in any proper subfield of K then this property will hold). We first list some curves for which a Type A or B equation always arises

$$\begin{aligned}
y^2 + xy &= x^{2g+1} + \cdots + c_3x^3 + c_2x^2 + c_1x + \theta \\
y^2 + xy &= x^{2g+1} + \cdots + c_3x^3 + c_2x^2 + \theta x + c_1 \\
y^2 + xy &= x^{2g+1} + \cdots + \theta x^3 + c_3x^2 + c_2x + c_1 \\
y^2 + xy &= x^{2g+1} + \cdots + \theta' x^3 + c_1x^2 + \theta x + \theta^2.
\end{aligned}$$

Here the terms in the $\cdots$ all have coefficients defined over the small field k. On the other hand, curves of the form $y^2 + xy = x^{2g+1} + \theta x^2 + c_1x + c_2$ or $y^2 + xy = x^{2g+1} + \theta^2x^4 + \theta x^3 + c_1x^2 + c_2x + c_3$ are not amenable to our methods.

4.4. Hyperellipticity and Genus Formulae.

We now restrict to the case where the equations (2) can be massaged so that they are of Type A or B (i.e., are linear in either x or x^{-1}).

In both cases the method and result of Lemma 7 of [9] applies verbatim where $z = x^{-1}$ if we have Type A curve and $z = x$ if the curve is Type B. It follows that there is a function c (which is a linear combination of the functions t_i over K) such that $z = \Lambda(c)$ where Λ is a polynomial over K of the form $\lambda_{-1} + \sum_{j=0}^{m-1} \lambda_j c^{2^j}$. It also follows that λ_0 and λ_{m-1} are both non-zero.

We write $L = K(c)$. This rational function field is a subfield of F. Furthermore F is obtained from L by adjoining the function s_0 given by the quadratic equation (1) The following result is therefore immediate.

Proposition 1. *The function field F is hyperelliptic.*

We now want to estimate the genus of the function field F. The following result is a generalisation of Lemma 9 of [9]. We will give a different proof to the one given in [9]. Our proof is rather elementary but it has the mild disadvantage of only providing an upper bound on the genus.

Proposition 2. *Let F be the function field over K as above and suppose we are in the Type A or Type B case. Then the genus of the hyperelliptic function field F is less than or equal to $g2^{m-1}$ where g is the genus of the original curve C.*

Proof. In the Type A case we have $x^{-1} = \Lambda(c)$ while in the Type B case we have $x = \Lambda(c)$ where $\Lambda(c)$ has degree 2^{m-1}. Starting from the $i = 0$ equation in (1) we will exhibit a particular hyperelliptic equation for the function field F over L.

In the Type A case define $w = \Lambda(c)^g s_0$ and obtain (writing $a_1' = (a_1 + \sqrt{a_0})$ which in the Type A case is non-zero)

$$w^2 + \Lambda(c)^g w = \Lambda(c) + a_{2g}\Lambda(c)^2 + \cdots a_2\Lambda(c)^{2g} + a_1'\Lambda(c)^{2g+1}. \tag{3}$$

In the Type B case we define $w = \Lambda(c)s_0$ and obtain

$$w^2 + \Lambda(c)w = \Lambda(c)^{2g+1} + a_{2g}\Lambda(c)^{2g} + \cdots + a_1'\Lambda(c). \tag{4}$$

To show that the curve $y^2 + h(c)y = f(c)$ has genus $\leq g2^{m-1}$ we will show that $\deg(h(c)) \leq g2^{m-1}$ and $\deg(f(c)) \leq g2^m + 1$. For the two equations (3) and (4) we have $h(c) = \Lambda(c)^g$ or $h(c) = \Lambda(c)$ and so the condition on the degree of $h(c)$ is satisfied. However, the condition on f is initially violated since $\Lambda(c)^{2g+1}$ has terms of degree $g2^m + 2^{m-1}, g2^m + 2^{m-2}, \ldots, g2^m + 2$. Note that the powers of c appearing in the term $\Lambda(c)^{2g}$ have degree at most $g2^m$ which is no problem.

It remains to perform an inductive sequence of changes of variable to remove the terms of degree more than $g2^m + 1$. Set $v_1 = w$ and suppose that our equation is of the form

$$v_i^2 + h(c)v_i = f(c)$$

where the leading term of $f(c)$ is $\alpha c^{g2^m + 2^{m-i}}$ and where the only terms in $f(c)$ of degree greater than $g2^m + 1$ have degrees of the form $g2^m + 2^k$ (with $k \leq (m-i)$). Define $v_{i+1} = v_i + \sqrt{\alpha}c^{g2^{m-1}+2^{m-i-1}}$. Then we have

$$v_{i+1}^2 + h(c)v_{i+1} = f(c) + \alpha c^{g2^m+2^{m-i}} + h(c)\sqrt{\alpha}c^{g2^{m-1}+2^{m-i-1}}. \tag{5}$$

It remains to show that the high degree terms in the right hand side have degree $g2^m + 2^k$ with $k \leq (m-i)$. In the Type B case this is immediate since $\deg(h(c)) \leq 2^{m-1}$ and so no new terms of high degree have appeared. In the Type A case observe that $h(c) = h_0c^{g2^{m-1}} + h_1c^{g2^{m-1}-2^{m-2}} + \cdots$ and so $h(c)c^{g2^{m-1}+2^{m-i-1}} = h_0c^{g2^m+2^{m-i-1}} + h_1c^{g2^m+2^{m-i-1}-2^{m-2}} + \cdots$ and since $i \geq 1$ the second term above has degree $\leq g2^m+1$. Hence our new equation does satisfy the inductive hypothesis.

Eventually we obtain an equation for the function field F of the form $v_m^2 + h(c)v_m = f(c)$ where $\deg(f(c)) \leq g2^m+1$. Of course it is possible that the equation be singular or that $\deg(f(c)) < g2^m+1$ in which case the genus is smaller than our bound. But in the case when the equation is non-singular and $\deg(f(c)) = g2^m+1$ then one can show that the hyperelliptic curve has genus $g2^{m-1}$ and that there is only one point at infinity. □

4.5. **Finding the Curve $\mathfrak{C}$ over k.** The function field F is defined over K. We can take the fixed field F' of F with respect to the Galois action as in [9] to obtain a function field corresponding to a curve $\mathfrak{C}'$ over k. In general we have $K(\mathfrak{C}') \cong F = K(\mathfrak{C})$ and thus have obtained an equation for $\mathfrak{C}$ which is defined over k. Note that there is the possibility that $K(\mathfrak{C}')$ is a proper subfield of F which could mean that the Weil descent strategy has failed. This special situation is excluded in [9] by the condition (†) (see Section 1 of [9]).

The curve $\mathfrak{C}$ can be constructed explicitly using the method of Lemma 13 of [9] which is as follows: Let $\mu \in K$ be such that $\mathrm{Tr}_{K/k}(\mu) = 1$ and define

$$X = \mathrm{Tr}_{K/k}(\mu\lambda_0 c) \qquad \text{and} \qquad Y' = \mathrm{Tr}_{K/k}(\mu w_0).$$

Then $X = \lambda_0 c + \lambda''$ for some $\lambda'' \in K$ and $Y' = w_0 + r(c)$ for some polynomial r over K. It follows that $k(X)$ is a subfield of L which is fixed by the Galois action and that $K(X) = L$. It also follows that $k(X, Y')$ is a subfield of F, $[k(X, Y') : k(X)] = n$ and that $K(X, Y') = F$ which shows that the functions X and Y' are the functions we require.

An equation relating X and Y' may be easily obtained from the earlier equations. To get an equation of small degree it will be necessary to perform a change of variable in Y' analogous to those used in the proof of Proposition 2. This process is illustrated in the examples given below.

Finally, one must consider the norm maps which enable the pulling-back of the discrete logarithm problem. This stage proceeds exactly as in [9].

In cases where the curve $\mathfrak{C}$ has more than one point at infinity, the base point for the divisor representation on $\mathfrak{C}$ can be chosen arbitrarily. This is because we are only concerned with divisor classes.

4.6. **Example One.** We consider the curve $C : y^2 + xy = x^5 + x^4 + \theta^2 x^2 + \theta x + 1$ over $K = \mathbb{F}_{2^2} = \mathbb{F}_2[\theta]$ where $\theta^2 + \theta + 1 = 0$. This curve has characteristic polynomial of Frobenius equal to $P(T) = T^4 + T^3 + 4T + 16$ and $\#\mathrm{Jac}(C)(\mathbb{F}_{2^{122}}) = 2 \cdot 11 \cdot 28549 \cdot L$ where L is the 225 bit prime

$$45009621474489074968234394447177137700613877917580561425898884250597.$$

We perform the Weil descent of $\mathrm{Jac}(C)$ with respect to the extension $\mathbb{F}_{2^2}/\mathbb{F}_2$ (note that the curve is not a 'subfield curve' with respect to this extension). We can worry about the divisors over $\mathbb{F}_{2^{122}}$ in the final stage, but the job of finding $\mathfrak{C}$ can be performed completely over $\mathbb{F}_{2^2}$. We first obtain the pair of equations (where $s_i = (w_i + 1)x^{-1}$)

$$s_0^2 + s_0 = x^3 + x^2 + \theta^2 + \theta^2 x^{-1} \tag{6}$$

$$s_1^2 + s_1 = x^3 + x^2 + \theta + \theta x^{-1} \tag{7}$$

and we see that $m = 2$. Setting $t = s_0 + s_1$ and subtracting we get

$$t^2 + t = 1 + x^{-1} \tag{8}$$

and so the curve is Type A. This immediately gives the rational function field $L = K(t)$ with $x = (t^2 + t + 1)^{-1}$.

As an aside we note that it is crucial that equation (8) only contains a term x^{-1}. For instance, if equation (8) was $t^2 + t = 1 + x^{-1} + x^{-2}$ then we could eliminate all the x terms and we would find that we have $m = 1$ and that the function field F is isomorphic to the function field of the original curve C. Of course, $t^2 + t = 1 + x^{-2}$ would be fine as modifying the equation by $x^{-1} + x^{-2}$ gives an acceptable form. On the other hand, if equation (8) was $t^2 + t = x + 1 + x^{-1}$ then it would no longer be true that x lies in the rational field generated by t.

Continuing with the example, we obtain an equation for F over K by combining these equations, i.e.,

$$s_0^2 + s_0 = (t^2 + t + 1)^{-3} + (t^2 + t + 1)^{-2} + \theta^2 + \theta^2(t^2 + t + 1).$$

To obtain a model for $\mathfrak{C}$ over $\mathbb{F}_2$ we follow the method of subsection 4.5 with $c = t$, $\lambda_0 = 1$ and $\mu = \theta$. We find that $\mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(\mu\lambda_0 c) = \theta t + \theta^2 t = t$. To compute $Y' = \mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(\mu w_0)$ we note that $w_i = xs_i + 1$ and so $Y' = x(\theta s_0 + \theta^2 s_1) + (\theta + \theta^2) = x(\theta^2 t + s_0) + 1$.

We find the equation

$$(Y')^2 + xY' = x^5 + x^4 + x^2(\theta t^2 + \theta^2 t + \theta^2) + \theta x + 1.$$

To get this in terms of a polynomial in t we multiply by x^{-6} and find $(x^{-3}Y')^2 + x^{-2}(x^{-3}Y') = t^{12} + t^{10} + t^9 + t^8 + t^6 + t^5 + t^2$. The degree of the right hand side now appears to be too large. We therefore perform the change of variable $Y = x^{-3}Y' + t^6$ to obtain

$$Y^2 + (t^4 + t^2 + 1)Y = t^9 + t^5 + t^2$$

which is a genus 4 curve over $\mathbb{F}_2$.

We can now pull divisors on $\mathrm{Jac}(C)(\mathbb{F}_{2^{122}})$ back to divisors on $\mathrm{Jac}(\mathfrak{C})(\mathbb{F}_{2^{61}})$ using the conorm and norm maps.

The solution of the discrete logarithm problem in $\mathrm{Jac}(\mathfrak{C})$ can be found using a version of Gaudry's algorithm [8]. It was shown in [9] that for curves of genus four this algorithm does run slightly faster than the Pollard method on an elliptic curve and so we are sure that we have transformed the discrete logarithm problem from $\mathrm{Jac}(C)$ to an easier problem (though still exponential time). In this case (as with the other examples in this paper) the use of the Frobenius endomorphism gives a very important improvement to the running time of Gaudry's algorithm (see [3], [8]).

4.7. **Example Two.** We now consider a Type B example. Consider the genus 3 curve over $\mathbb{F}_{2^2}$

$$C : y^2 + xy = x^7 + x^5 + \theta x^3 + 1$$

which has characteristic polynomial of Frobenius equal to $T^6 - T^5 - 4T^3 - 16T + 64$. We find that $\#\mathrm{Jac}(C)(\mathbb{F}_{2^{58}}) = 2^2 \cdot 11 \cdot L$ where L is the 169 bit prime

$$544210065162879673276249722680357412546827447416957.$$

We can perform Weil descent of $\mathrm{Jac}(C)$ with respect to the extension $\mathbb{F}_{2^2}/\mathbb{F}_2$ as outlined above.

We first obtain the equations

$$\begin{array}{rcl} w_0^2 + xw_0 & = & x^7 + x^5 + \theta x^3 + 1 \\ w_1^2 + xw_1 & = & x^7 + x^5 + \theta^2 x^3 + 1. \end{array}$$

We then perform the usual changes of variable to get $s_0^2 + s_0 = x^5 + x^3 + \theta x + x^{-1}$ and $t^2 + t = x$ which shows that we have a Type B curve. We have $m = n = 2$ for this example.

The function field $F = \mathbb{F}_{2^2}(x, w_0, w_1) = \mathbb{F}_{2^2}(s_0, t)$ is thus a hyperelliptic function field over the rational function field $L = \mathbb{F}_{2^2}(t)$.

To obtain a model over $\mathbb{F}_2$ we write $Y' = x(s_0 + \theta^2 t) + 1$. From this we obtain the equation

$$(Y')^2 + xY' = x^7 + x^5 + \theta x^3 + (\theta t^2 + \theta^2 t)x^2 + 1.$$

Expanding out the terms and setting $Y = Y' + t^7$ gives

$$\mathfrak{C} : Y^2 + (t^2 + t)Y = t^{13} + t^{11} + t^9 + t^8 + t^6 + t^3 + 1$$

which is a genus 6 curve over $\mathbb{F}_2$ and one can check that $\#\mathrm{Jac}(\mathfrak{C})(\mathbb{F}_{2^{29}}) = 2^2 \cdot 11 \cdot L$ as expected.

Once again, one can pull a discrete logarithm problem from $\mathrm{Jac}(C)(\mathbb{F}_{2^{58}})$ to $\mathrm{Jac}(\mathfrak{C})(\mathbb{F}_{2^{29}})$ using conorms and norms and then solve the discrete logarithm problem in the genus six Jacobian.

4.8. **Example Three.** Let $\mathbb{F}_{2^3} = \mathbb{F}_2(\theta)$ where $\theta^3 + \theta + 1 = 0$. Consider the curve

$$C : y^2 + xy = x^7 + x^4 + \theta x^3 + 1$$

of genus 3. The characteristic polynomial of Frobenius for this curve is $P(T) = T^6 - T^5 + 4T^4 + 32T^2 - 64T + 512$. Thus $\#\mathrm{Jac}(C)(\mathbb{F}_{2^{3 \cdot 23}}) = 2^2 \cdot 11^2 \cdot 796813 \cdot L$ where L is the 179 bit prime

$$533343896894265191739797030807410720780166091007800491.$$

Performing the method as described gives $s_0^2 + s_0 = x^5 + x^2 + \theta x + x^{-1}$ and similarly for s_1 and s_2. We get $t_1^2 + t_1 = \theta^4 x$ and $t_2^2 + t_2 = \theta^2 x$ and $m = 3$.

Put $c = t_2 + \theta^6 t_1$. Then $c^2 + c = \theta t_1$ from which we obtain $t_1 = \theta^6 c^2 + \theta^6 c$, $t_2 = \theta^5 c^2 + \theta^4 c$ and $x = \theta c^4 + \theta^4 c^2 + \theta^2 c$. It follows that $K(c) = K(x, t_1, t_2)$.

To get functions over $\mathbb{F}_2$ we find $X = \theta^2 c$ and $Y' = x(s_0 + t_1 + t_2) + 1$. We obtain $(Y')^2 + xY' = X^{28} + X^{26} + X^{25} + \cdots + 1$. Putting $Y = Y' + X^{14} + X^{13}$ gives

$$\mathfrak{C} : Y^2 + (X^4 + X^2 + X)Y = X^{25} + X^{24} + X^{21} + X^{19} + X^{11} + X^9 + X^7 + X^4 + 1$$

which is a non-singular hyperelliptic curve of genus 12 as expected.

One can compute the characteristic polynomial of Frobenius for this curve and see that it is $P(T^3)(T^6 - T^5 - 4T + 8)$.

Once again we can transfer discrete logarithms from the Jacobian of the genus 3 curve over $\mathbb{F}_{2^{69}}$ to the Jacobian of the genus 12 curve over $\mathbb{F}_{2^{23}}$. Since the Pollard methods on the original curve will take time $O(q^{9/2})$ (where $q = 2^{23}$) we expect the solution of the discrete logarithm problem on the genus 12 curve to be rather easy compared with the original problem.

5. More General Algebraic Approach

The above strategy, which is generalised from the method of [9], seems to be very effective. However, there are many curves for which the method does not seem to apply: we may have difficulties when $\deg(h(x)) > 1$, the magic number m may be too small or the 't_i equations' may not reduce to a simple enough form to have a Type A or Type B curve (and thus to be able to deduce hyperellipticity).

On the other hand, we stress that the philosophy of the method does not depend on these details and, in principle, any discrete logarithm problem on any curve over any extension of fields can be approached using these techniques. To illustrate this point we now give some examples which are not covered by the results of Section 4.

5.1. **Example Four.** This example concerns the case where $\deg(h(x)) > 1$. Let $\mathbb{F}_{2^2} = \mathbb{F}_2(\theta)$ and consider the curve $C : y^2 + x(x+1)y = x^5 + \theta x^2 + 1$ which has $P(T) = T^4 - T^2 + 16$.

Performing Weil descent in the usual manner results in the two equations

$$\begin{aligned} y_0^2 + x(x+1)y_0 &= x^5 + \theta x^2 + 1 \\ y_1^2 + x(x+1)y_1 &= x^5 + \theta^2 x^2 + 1. \end{aligned}$$

Define $t' = y_0+y_1$ to get $(t')^2+x(x+1)t' = x^2$. Thus $t = x^{-1}t'$ satisfies $t^2+(x+1)t = 1$ and so we have $x = (t^2+t+1)/t$ and the function field $\mathbb{F}_{2^2}(x, y_0, y_1) = \mathbb{F}_{2^2}(t, y_0)$.

To get an equation over $\mathbb{F}_2$ we define $Y' = \mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(\theta y_0) = y_0+\theta^2 xt$. We therefore obtain the equation $(Y')^2+(t^2+1)(t^2+t+1)/t^2Y' = (t+1)^3(t^7+t^7+t^5+t^4+1)/t^5$. Setting $Y = t^3Y'/(t+1)$ yields

$$\mathfrak{C} : Y^2 + (t^4 + t)Y = t^9 + t^5 + t^2 + t$$

which is a genus 4 curve having characteristic polynomial of Frobenius equal to $P(T^2)$.

This example shows that there are cases when $\deg(h(x)) > 1$ which still yield a nice hyperelliptic curve.

5.2. **Example Five.** In this case we consider what happens when $\deg(h(x)) > 1$ and when $h(x)$ is defined over K rather than k. Consider the genus two curve over $\mathbb{F}_{2^2}$ given by

$$C : y^2 + (x^2 + \theta)y = x^5 + \theta x.$$

The usual Weil descent construction gives two equations

$$\begin{aligned} w_0^2 + (x^2+\theta)w_0 &= x^5 + \theta x \\ w_1^2 + (x^2+\theta^2)w_1 &= x^5 + \theta^2 x. \end{aligned}$$

Writing $t = w_0 + w_1$ gives

$$t^2 + (x^2 + \theta)t + w_1 = x.$$

Therefore we can write $w_1 = t^2 + (x^2 + \theta) + x$ and insert into the second equation to obtain

$$\mathfrak{C} : t^4 + (x^4 + x^2)t^2 + (x^4 + x^2 + 1)t + x^5 + x^3 + x^2 = 0$$

which is a genus 7 curve over $\mathbb{F}_2$ with singular points only at infinity.

We see that this curve does not satisfy the theoretical results of the previous section. Nevertheless, it is possible to transfer a discrete logarithm problem in $\mathrm{Jac}(C)(\mathbb{F}_{2^{2l}})$ to a discrete logarithm problem in $\mathrm{Jac}(\mathfrak{C})(\mathbb{F}_{2^l})$. It is not clear how efficiently the discrete logarithm problem can be solved on $\mathrm{Jac}(\mathfrak{C})$ in practice, but in theory (using methods like those of [8]) one can achieve a complexity which is better than the Pollard methods on $\mathrm{Jac}(C)$.

Another approach for performing Weil descent would be to use a more geometric strategy. We briefly discuss this approach below.

6. The Geometric Approach

As we noted in the previous sections, the algebraic approach is very successful. However, there are cases to which it does not seem to apply. One could attempt a more geometric approach following the methods of [6]. The basic idea of this approach is to represent $\mathrm{Jac}(C)$ as an affine variety, take Weil restriction of scalars explicitly to get an affine part of A, find a curve $\mathfrak{C}$ on A, pull back the discrete logarithm problem from A to $\mathrm{Jac}(\mathfrak{C})$ and then solve it as before.

The representation of $\mathrm{Jac}(C)$ as an affine variety uses a technique going back to Mumford which was explicitly described by Spallek [13]. To be precise we recall the Cantor representation of a reduced divisor of degree g on C. A generic divisor on C has degree g and is represented as a pair of polynomials $(u(x), v(x))$ where $u(x) = x^g + u_{g-1}x^{g-1} + \cdots + u_0$ and $v(x) = v_{g-1}x^{g-1} + \cdots + v_0$. The points

(x_0, y_0) in the support correspond to those values of x_0 which satisfy $u(x_0) = 0$ and where $y_0 = v(x_0)$. It follows from the equation $y^2 + h(x)y = f(x)$ that we have $u(x)|(v(x)^2 + h(x)v(x) - f(x))$. This means that the divisor corresponding to (u, v) may be represented as the element $(u_0, u_1, \ldots, u_{g-1}, v_0, \ldots, v_{g-1})$ in $2g$-dimensional affine space. The Jacobian is then the set of points for which the equation $(v(x)^2 + h(x)v(x) - f(x)) \equiv 0 \pmod{u(x)}$ is satisfied.

This is of course only generic (it misses the so-called theta divisor which is a flag variety of dimension $g - 1$). If given target divisors do not have the full degree g then they can be easily modified by adding a small multiple of the base point.

Once an affine equation for A is obtained it remains to find a suitable affine curve $\mathfrak{C}$ on A and to pull back the discrete logarithm problem to a divisor on $\mathfrak{C}$. To achieve this seems to require considerable computer algebra computations. This leads to a situation where the security of the original discrete logarithm problem is now related to the difficulty of solving some non-linear multivariate equations. These calculations seem to be difficult to perform in practice, but we do not know if they are as difficult as solving discrete logarithm problems. We give an example.

6.1. **Example Six.** Consider the genus two curve

$$C : y^2 + xy = x^5 + \theta x^2 + 1$$

over $\mathbb{F}_{2^2} = \mathbb{F}_2[\theta]$ where $\theta^2 + \theta + 1 = 0$.

Note that this curve is actually isomorphic to one defined over $\mathbb{F}_2$ under the map $(x, y) \mapsto (X, Y + \alpha X)$ where $\alpha^2 + \alpha + \theta = 0$ (so $\alpha \in \mathbb{F}_{2^4}$). Thus the curve C can be called a quartic twist of the genus two curve $C' : Y^2 + XY = X^5 + 1$ over $\mathbb{F}_2$.

We will perform a Weil descent of $\mathrm{Jac}(C)$ with respect to the extension $\mathbb{F}_{2^2}/\mathbb{F}_2$. Using the algebraic approach developed above one finds oneself in a degenerate case (in fact, the function field F contains a proper constant field extension and so the curve $\mathfrak{C}$ cannot be defined over $\mathbb{F}_2$).

Taking the geometric approach, we first construct a model for $\mathrm{Jac}(C)$ in terms of the generic polynomials $x^2 + u_1 x + u_0$ and $v_1 x + v_0$. The hyperelliptic involution on C corresponds to the involution $v_1 \mapsto v_1 + 1$ on this model. We aim to preserve this involution.

One obtains the equations

$$\begin{aligned} 0 &= u_0 u_1^3 + u_0 v_1^2 + u_0 v_1 + \theta u_0 + v_0^2 + 1 \\ 0 &= u_0^2 + u_0 u_1^2 + u_1^4 + u_1 v_1^2 + u_1 v_1 + \theta u_1 + v_0 \end{aligned}$$

for $\mathrm{Jac}(C)$ as a two dimensional variety in four dimensional affine space.

One can then perform a Weil descent on this in the usual manner by writing $u_0 = u_{0,1} + u_{0,2}\theta$ etc. One obtains a four dimensional variety in eight dimensional affine space.

Two of these equations have the form $v_{0,i} = p_i(u_{0,1}, u_{0,2}, u_{1,1}, u_{1,2}, v_{1,1}, v_{1,2})$ and so these two variables are immediately eliminated to obtain a two dimensional variety in six dimensional affine space.

We want to intersect this variety with hypersurfaces. The first choice is to set $u_{1,1} = u_{1,2} = 0$ since these variables appear to the highest degree. This is interpreted as setting $u_1 = 0$ or, in other words, restricting the curve to lie on the divisors of the form $2(x_1, y_1) - 2P_\infty$ (this will not be a problem since we are interested in divisors of odd order). One obtains the equations

$$\begin{aligned} 0 &= u_{0,1}^4 + u_{0,1}v_{1,1}^2 + u_{0,1}v_{1,1} + u_{0,1}v_{1,2}^2 + u_{0,2}v_{1,2}^2 + u_{0,2}v_{1,2} + u_{0,2} + 1 \\ 0 &= u_{0,1}v_{1,2}^2 + u_{0,1}v_{1,2} + u_{0,1} + u_{0,2}^4 + u_{0,2}v_{1,1}^2 + u_{0,2}v_{1,1} + u_{0,2}v_{1,2} + u_{0,2}. \end{aligned}$$

We now intersect with the hypersurface $u_{0,1} = 0$ to obtain a very simple pair of equations. Writing x for $u_{0,2}$, y for $v_{1,1}$ (recall that the hyperelliptic involution is $v_{1,1} \mapsto v_{1,1} + 1$) and w for $v_{1,2}$ we have

$$\begin{aligned} x &= (w^2 + w + 1)^{-1} \\ y^2 + y &= x^3 + w + 1. \end{aligned}$$

From this we obtain the genus 4 curve (writing $Y = (w^2 + w + 1)^2 y$)

$$\mathfrak{C} : Y^2 + (w^4 + w^2 + 1)Y = w^9 + w^8 + w^5 + w^4 + w^2.$$

The hyperelliptic involution on $\mathfrak{C}$ is inherited from that on the original curve C.

It remains to transfer instances of the discrete logarithm problem on $\mathrm{Jac}(C)$ to $\mathrm{Jac}(\mathfrak{C})$. This is not at all easy and so we give some discussion.

Consider a point (w, Y) of $\mathfrak{C}$. By substituting back into the formulae above one sees that this point corresponds to the point

$$(u_{0,1}, u_{0,2}, u_{1,1}, u_{1,2}, v_{0,1}, v_{0,2}, v_{1,1}, v_{1,2}) = (0, \alpha^{-1}, 0, 0, \alpha^{-2}, \alpha^{-2}, Y\alpha^{-2}, w) \tag{9}$$

where $\alpha = w^2 + w + 1$. As an example, the point $(0, 1) \in \mathfrak{C}(\mathbb{F}_2)$ corresponds to the divisor $(x^2 + \theta, x + \theta^2)$ on $C(\mathbb{F}_{2^2})$. One can see from equation (9) that the process is undefined when w satisfies $w^2 + w + 1 = 0$. This is a reflection of the fact that the group homomorphism from $\mathrm{Jac}(\mathfrak{C})(\mathbb{F}_{2^m}) \to \mathrm{Jac}(C)(\mathbb{F}_{2^{2m}})$ is only defined when m is odd.

To pull back a target divisor D_1 in $\mathrm{Jac}(C)$ we aim to find k reduced divisor classs B_i in $\mathrm{Jac}(C)$ coming from divisor classes $(w_i, Y_i) - (\infty)$ in $\mathrm{Jac}(\mathfrak{C})$ such that $B_1 + B_2 + \cdots + B_k = D_1$ in $\mathrm{Jac}(C)$. Ideally we would take $k = g = 4$, however these points will be Galois conjugates over an extension of degree k and our mappings may not be defined when the field extension is not coprime to n. Therefore we should take $k = 5$ in our example, though $k = 3$ would span a set of divisors of density $1/q$.

The easiest way to find this seems to be to split it into halves. In the case $k = 3$ we must solve solve $(B_1 + B_2) = -(B_3 - D_1)$ using the fact that inverses in the additive group can be easily understood. To do this we need some kind of 'addition formulae' rather than the addition algorithm for divisors. Such a mechanism was provided by Spallek [13] in the case of genus two and, as we may assume that our initial points are generic, the numerous special cases do not arise.

Given the resulting expressions in terms of the variables w_i and Y_i we hope to be able to find a solution defined over the ground field. Experiments using Magma indicate that solving these sorts of equations using Groebner basis techniques requires significant computing resources. We have not been able to pull back a target divisor for this example.

7. Characteristic Greater than Two

One can also consider Jacobians of curves over fields of characteristic $p > 2$. Even for elliptic curves the techniques are not very well developed in the odd characteristic case, though see Diem [2]. In general we cannot apply the theory of

Artin-Schreier extensions. Nevertheless, in some cases the Weil descent strategy can be performed.

7.1. **Example Seven.** Let θ be the generator of $\mathbb{F}_{19^2}^*$ which satisfies $\theta^2 - \theta + 2 = 0$ (we use Magma for computations and so will represent field elements in terms of powers of the generator) and consider the genus two curve $C : y^2 = x^5 + x + \theta$.

Performing Weil descent as usual gives the two equations

$$\begin{aligned} w_0^2 &= x^5 + x + \theta \\ w_1^2 &= x^5 + x + \theta^{19}. \end{aligned}$$

Subtracting these two equations gives the conic $w_1^2 = w_0^2 + \theta^{150}$ whose solutions are parameterised as $w_1 = \theta^{75}(s^2 + 1)/(s^2 - 1)$ and $w_0 = 2\theta^{75}s/(s^2 - 1)$. It therefore follows that the function field $F = \mathbb{F}_{19^2}(x, s)$ contains the function field $\mathbb{F}_{19^2}(x, w_0, w_1)$. Indeed, $s = (w_0+w_1+\theta^{75})/(w_0+w_1-\theta^{75})$ and so $F = \mathbb{F}_{19^2}(x, s) \cong \mathbb{F}_{19^2}(x, w_0, w_1)$.

One can compute the equation

$$\mathfrak{C} : x^5(s^4 - 2s^2 + 1) + x(s^4 - 2s^2 + 1) + \theta^{181}s^4 + \theta^{24}s^2 + \theta^{181} = 0 \tag{10}$$

for the curve corresponding to the field F.

It remains to construct a model for $\mathfrak{C}$ over $\mathbb{F}_{19}$. This is done by first calculating the action of $\mathrm{Gal}(\mathbb{F}_{19^2}/\mathbb{F}_{19}) = \langle\sigma\rangle$ on s by using the fact that $\sigma : w_0 \mapsto w_1$. One gets $\sigma(s) = \sqrt{-1}(s \pm \sqrt{-1})^2/(s^2 + 1) = \sqrt{-1}(s \pm \sqrt{-1})/(s \mp \sqrt{-1})$ (the choice of sign in the $\pm$ depends on the selection of $\sqrt{-1}$; a coherent choice is $\sigma(s) = (\theta^{270}s + 1)/(s + \theta^{270})$) and one can verify that $\sigma^2(s) = s$.

It is necessary to find a function Y which is Galois invariant and is such that $\mathbb{F}_{19^2}(x, Y) \cong \mathbb{F}_{19^2}(x, s)$. This can be done by writing $Y = (s + b)/(cs + d)$ with unknowns $b, c, d \in \mathbb{F}_{19^2}$ and solving for $Y^\sigma = Y$. One solution is

$$Y = \frac{s + \theta^{333}}{\theta^{233}s + 3}.$$

It is then clear that $\mathbb{F}_{19^2}(x, Y) \cong \mathbb{F}_{19^2}(x, s)$. Substituting into equation (10) yields the curve

$$(x^5 + x + 9)(Y^4 + 4Y^2 + 4) + Y^3 - 2Y = 0$$

over $\mathbb{F}_{19}$. Magma calculates that this curve has genus 8. The 'ideal' genus for a curve arising from a degree two Weil descent of a genus two curve would be 4. It is probably not significantly easier to solve the discrete logarithm problem on this genus 8 curves than on the original genus two curve.

8. Conclusions

We have shown that the Weil descent strategy does extend to the higher dimensional situation. For a large class of curves over certain finite fields we obtain a reduction of the discrete logarithm problem to a computationally easier problem. Nevertheless, there are many cases of curves and fields for which these techniques do not seem to apply.

9. Acknowledgement

I thank Florian Hess and Claus Diem for discussions on this topic, and the anonymous referees for helpful comments.

References

[1] L. Adleman, J. De Marrais, and M.-D. Huang, A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields, In L. M. Adleman and M-D. Huang (eds.), Ants-I, Springer, lncs 877 (1994) 28–40.

[2] C. Diem, *The GHS attack in odd characteristic*, preprint (2001). Available from `http://www.exp-math.uni-essen.de/~diem/`

[3] I. Duursma, P. Gaudry and F. Morain, Speeding up the discrete log computation on curves with automorphisms, In Lam et al (ed.), Asiacrypt '99, Springer lncs 1716 (1999) 103–121.

[4] R. Flassenberg and S. Paulus, Sieving in function fields, *Experimental Mathematics*, **8**, no. 4 (1997) 339–349.

[5] G. Frey, *How to disguise an elliptic curve*, Talk at ECC '98, Waterloo, (1998) `http://cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html`

[6] S. D. Galbraith and N. P. Smart, A Cryptographic Application of Weil Descent, In M. Walker (ed.), Codes and Cryptography, Cirencester, Springer lncs 1746 (1999) 191–200.

[7] S. D. Galbraith, Limitations of constructive Weil descent, in K. Alster et al. (eds.), *Public-Key Cryptography and Computational Number Theory*, Walter de Gruyter (2001) 59–70.

[8] P. Gaudry, An algorithm for solving the discrete log problem on hyperelliptic curves, In B. Preneel (ed.), Eurocrypt 2000, Springer lncs 1807, 19–34, 2000.

[9] P. Gaudry, F. Hess and N. P. Smart, Constructive and destructive facets of Weil descent on elliptic curves, *J. Cryptology*, **15**, no. 1, 2002, 19–46.

[10] C. Günther, T. Lange and A. Stein, Speeding up the arithmetic on Koblitz curves of genus two, in D. Stinson et al. (eds.), SAC 2001, Springer lncs 2012 (2001) 106–117.

[11] N. Koblitz, Hyperelliptic cryptosystems, *J. Cryptology*, **1**, no. 3, (1989) 139–150.

[12] N. P. Smart, How secure are elliptic curves over composite extension fields?, in B. Pfitzmann (ed.), Eurocrypt 2001, Springer lncs 2045 (2001) 30–39.

[13] A.-M. Spallek, *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*, PhD Thesis, IEM Essen, 1994.

[14] H. Stichtenoth, *Algebraic function fields and codes*, Springer Universitext, 1993.

E-mail address: `steven.galbraith@rhul.ac.uk`

Mathematics Department, Royal Holloway University of London, Egham, Surrey TW20 0EX, UK.