Constructive and Destructive Facets of Weil Descent on Elliptic Curves

Nigel Smart, Florian Hess, Pierrick Gaudry
Trusted e- Services
HP Laboratories Bristol

HPL-2000-10
17th January, 2000*

function fields,
divisor class
group,
cryptography,
elliptic curves

In this paper we look in detail at the curves which arise in the method of Galbraith and Smart for producing curves in the Weil restriction of an elliptic curve over a finite field of characteristic two of composite degree. We explain how this method can be used to construct hyperelliptic cryptosystems which could be as secure as cryptosystems based on the original elliptic curve. On the other hand, we show that this may provide a way of attacking the original elliptic curve cryptosystem using recent advances in the study of the discrete logarithm problem on hyperelliptic curves.

We examine the resulting higher genus curves in some detail and propose an additional check on elliptic curve systems defined over fields of characteristic two so as to make them immune from the methods in this paper.

∗ Internal Accession Date Only

CONSTRUCTIVE AND DESTRUCTIVE FACETS OF WEIL DESCENT ON ELLIPTIC CURVES

P. GAUDRY, F. HESS, AND N.P. SMART

Abstract. In this paper we look in detail at the curves which arise in the method of Galbraith and Smart for producing curves in the Weil restriction of an elliptic curve over a finite field of characteristic two of composite degree. We explain how this method can be used to construct hyperelliptic cryptosystems which could be as secure as a cryptosystems based on the original elliptic curve. On the other hand, we show that this may provide a way of attacking the original elliptic curve cryptosystem using recent advances in the study of the discrete logarithm problem on hyperelliptic curves.

We examine the resulting higher genus curves in some detail and propose an additional check on elliptic curve systems defined over fields of characteristic two so as to make them immune from the methods in this paper.

1. Introduction

In this paper we address two problems: How to construct hyperelliptic cryptosystems and how to attack elliptic curve cryptosystems defined over fields of even characteristic and of composite degree over $\mathbb{F}_2$.

As explained in [13], there is currently no practical method which generates cryptographically secure Jacobians of hyperelliptic curves, but which also produces Jacobians with no special added structure. We shall present a method that will produce a hyperelliptic Jacobian related to a 'random' elliptic curve, which could be considered to be secure as long as one believes that the discrete logarithm problem on the elliptic curve is itself hard.

For the second problem we turn our construction of hyperelliptic cryptosystems on its head and argue that this provides evidence for the weakness of the original elliptic curve discrete logarithm problem. We stress, this does not provide evidence for the weakness of elliptic curve systems in general, but only those which are defined over the special finite fields considered in this paper. These fields are those of characteristic two and of composite degree over the field $\mathbb{F}_2$. In particular we shall show the following

Theorem 1. *Let $E(\mathbb{F}_{q^n})$ denote an elliptic curve defined over a field of characteristic two. Then for a significant proportion of all such elliptic curves one can solve the discrete logarithm problem on $E(\mathbb{F}_{q^n})$ in time $O(q^{2+\epsilon})$ where the complexity estimate holds for a fixed value of $n \geq 4$ and as $q \rightarrow \infty$.*

The complexity in the Theorem should be compared to the complexity of $O(q^{n/2})$ for the best general purpose algorithm, namely Pollard's rho method. That the

1991 *Mathematics Subject Classification.* Primary: 94A60, 11T71, Secondary: 11Y99, 14H52, 14Q15.

Key words and phrases. function fields, divisor class group, cryptography, elliptic curves.

result only holds for a significant proportion of such elliptic curves is due to the fact that we cannot apply our techniques to certain special types of curves, such as those defined over a subfield of $\mathbb{F}_{q^n}$.

The implied constant in the $O(\cdot)$ notation of the Theorem contains a dependence on n. Hence for certain values of n the crossover point between the method of the Theorem and Pollard's rho method may be at higher values of q than are used in practical elliptic curve cryptosystems. However, we shall exhibit experimental evidence that for $n = 4$, and around $1/q$ of the elliptic curves defined over $\mathbb{F}_{q^4}$, the method of the above Theorem is better than Pollard rho for values of q used in practice. For other elliptic curves over F_{q^4} our method is only asymptotically better than Pollard rho, and further practical experiments need to be carried out to deduce a similar result.

Our methods are based on the idea of Weil descent on elliptic curves. Hence much of the following is an extension of the work begun by Frey in [6] and continued in [8], to which we refer the reader for further details. The details of elliptic curve cryptosystems which we shall require can be found in [3].

The paper is organized as follows. In Section 2 we give some simple examples of curves defined over a special type of field extension, for which hand calculation is particularly simple. In Section 3 we give proofs that the properties observed in the hand calculations hold in general. In addition we shall construct an explicit group homomorphism

$$\phi : E(\mathbb{F}_{q^n}) \to Cl^0(H)$$

where $Cl^0(H)$ is the degree zero divisor class group of a hyperelliptic function field over $\mathbb{F}_q$. The kernel of the map ϕ explains the fact that our method only works for a significant proportion of all elliptic curves over $\mathbb{F}_{q^n}$, since we require that the discrete logarithm problem we are trying to solve on $E(\mathbb{F}_{q^n})$ does not lie in the kernel of ϕ.

In Section 4 we show how our method of producing curves in the Weil restriction can be used to construct hyperelliptic cryptosystems, whilst in Section 5 we explain how one could possibly attack the underlying elliptic curve system using the Weil restriction. In Section 6 we report on an experiment using the index calculus algorithm of Gaudry on one of the curves of genus four produced by our method; this is used to help decide which genera should be used in practice for constructing cryptographic systems and which elliptic curve systems are made weaker by our methods. Finally in Section 7, we turn our attention to other types of finite fields and discuss why the ideas of this paper are unlikely to work in other cases. In particular for a large proportion of elliptic curves defined over $\mathbb{F}_{2^p}$, where p is prime, we show that the methods of this paper give no decrease in security of the resulting cryptosystem.

The first author would like to thank R. Harley for many fruitful discussions on the hyperelliptic discrete log; some tricks are due to him. The second author would like to thank J. Cannon for his support while this work was in preparation. The third author would like to thank S. Galbraith for various discussions whilst the work on this paper was carried out. All three authors would like to thank S. Galbraith, N. Koblitz and K. Paterson who read and commented on an earlier draft of this paper. The calculations in this paper were made possible by using a variety of packages including Magma, KASH, LiDIA, PARI/GP and ZEN.

2. Example Curves in the Weil restriction

Let $k = \mathbb{F}_q$ denote some finite field of characteristic two, and let $n \geq 2$ denote an integer. In practice we are thinking of the situation where n is quite small and q is large enough so that $q^n > 2^{160}$. Let K denote the field extension $\mathbb{F}_{q^n}$, with k-basis $\{\psi_0, \psi_1, \ldots, \psi_{n-1}\}$.

In this section we shall consider elliptic curves, E, over K, given by the equation:

$$Y^2 + XY = X^3 + \beta,$$

where $\beta \in K$. We assume $E(\mathbb{F}_{q^n})$ contains a subgroup of prime order p with $p \approx q^n$.

We set

$$\begin{aligned} \beta &= b_0\psi_0 + b_1\psi_1 + \ldots + b_{n-1}\psi_{n-1}, \\ X &= x_0\psi_0 + x_1\psi_1 + \ldots + x_{n-1}\psi_{n-1}, \\ Y &= y_0\psi_0 + y_1\psi_1 + \ldots + y_{n-1}\psi_{n-1}, \end{aligned}$$

where $b_i \in k$ are given and $x_i,\ y_i \in k$ are variables. Substituting these equations into the equation for our elliptic curve, and equating coefficients of ψ_i, we obtain an abelian variety, A, defined over k, of dimension n, the group law on A being given by the group law on $E(K)$. The variety A is called the Weil restriction, and the above process is called Weil descent.

The variety A will contain a subvariety, B, with group order divisible by p. In practice this subvariety will either equal the whole of A or have dimension $n-1$. We wish to find a curve, C, in A whose Jacobian contains a subgroup isogenous to B. Recall that B is the part of A which is interesting for cryptographic applications. Hence we must have $g = \dim \mathrm{Jac}(C) \geq \dim B$ and $\dim B$ as stated above will be either n or $n-1$. For the applications we would like the genus of C to be linear in n, but it is highly unlikely such a curve exists at all.

For the rest of this section we shall look at a special set of finite fields for which it is relatively easy to perform calculations. Our aim is to fix the ideas and provide a rich set of examples for the reader and for later in the paper. In the next section we shall show the remarkable properties we observe, in this section, hold in general for fields of characteristic two. The method used is a natural extension of the one presented in [8].

We specialize to those fields K for which we can take $\psi_i = \theta^{2^i}$ in our basis of K over k where $\theta + \theta^2 + \theta^4 + \cdots + \theta^{2^{n-1}} = 1$. The reason for choosing such a basis is so that the curves in the Weil restriction we produce below will have 'small' degree and are easy to write down. One reason for this is that squaring an element represented by such a basis is simply a cyclic shift of the coefficients since

$$\begin{aligned} \theta^{2^n} &= \left(\theta^{2^{n-1}}\right)^2 = \left(1 + \theta + \theta^2 + \cdots + \theta^{2^{n-2}}\right)^2 \\ &= 1 + \theta^2 + \theta^4 + \cdots + \theta^{2^{n-1}} = \theta. \end{aligned}$$

However, such a basis does not always exist, since we require the existence of an irreducible factor, of degree n, of the polynomial $h(x) = x^{2^{n-1}} + \cdots + x^4 + x^2 + 1$ over the field k. In addition for a root, θ, of such an irreducible factor we require that the set $\{\theta, \theta^2, \theta^4, \ldots, \theta^{2^{n-1}}\}$ forms a basis of K over k.

Hence we have restricted the choice of q and n, but not in a significant manner. We clearly require that the degree of k over $\mathbb{F}_2$ must be coprime to n, so for the rest of this section we shall assume this is the case. For $n = 2$, we can always use the element defined by $\theta^2+\theta+1=0$ whilst for $n=3$ we can always use the element defined by $\theta^3+\theta^2+1=0$. For higher values of n we can obtain many factors of $h(x)$ of degree n over $\mathbb{F}_2$, and by the coprimality of the degree of k to n we see that such factors will be irreducible over k. For example if $n+1$ is a prime and q is a generator of the multiplicative group of the field $\mathbb{F}_{n+1}$ then we can take, θ, as a generator of K over k, where $\theta^n+\theta^{n-1}+\cdots+\theta+1=0$.

To produce a curve of low genus in A one could produce a curve of low degree, and hence of hopefully low genus. Such a curve of low degree can be obtained by intersecting A with the hyperplanes given by $x_0=x_1=\cdots=x_{n-1}=x$. Hence we look at the subvariety defined by restricting X to lie in k. We obtain a curve, $\mathfrak{C}$, defined by the equations

$$\mathfrak{C}:\begin{cases} y_{n-1}^2+xy_0+x^3+b_0=0,\\ y_0^2+xy_1+x^3+b_1=0,\\ \qquad\vdots \\ y_{n-2}^2+xy_{n-1}+x^3+b_{n-1}=0.\end{cases}$$

That we can obtain such sparse equations is due to our choice of basis of K over k. On elimination of variables we produce a curve in x and $y=y_0$ of the form

$$C: y^{2^n}+x^{2^n-1}y+\sum_{i=0}^{n-1}x^{2^n+2^i}+g(x)$$

where $g(x)$ is a polynomial, depending on $b_0,\ldots,b_{n-1}$, of degree less than or equal to 2^n. The polynomial $g(x)$ is given by the formulae:

$$g(x)=\sum_{i=1}^{n}b_i^{2^{n-i}}x^{2^n-2^{n-i+1}},$$

where we make the identification $b_n=b_0$. The Jacobians of the irreducible components of the curve C are isogenous to abelian varieties which contain subvarieties of A. Since the 'interesting' subvariety, B, of A, in examples of cryptographic interest, has large prime order, and the degree of the isogeny is likely to be coprime to the order of B, we can expect that the Jacobians actually contain a subgroup isomorphic to B, unless the genus of the components is too small.

We give the following examples:

$\underline{n=2}$.

$$C_2: y^4+x^3y+x^6+x^5+b_0x^2+b_1^2.$$

If the original elliptic curve is defined over the base field, i.e. $b_0=b_1$, then the curve C has two irreducible components, each being an elliptic curve. In all other cases it is irreducible, and experimentally the genus of this curve always seems to be 2.

$\underline{n=3}$.

$$C_3: y^8+x^7y+x^{12}+x^{10}+x^9+b_0x^6+b_2^2x^4+b_1^4.$$

The curve is reducible when $b_0=b_1=b_2$, in other words when the original elliptic curve is defined over the base field k. In all other cases it is irreducible, and experimentally the genus of this curve always seems to be 3 or 4.

$\underline{n=4}$.

$$C_4 : y^{16} + x^{15}y + x^{24} + x^{20} + x^{18} + x^{17} + b_0x^{14} + b_3^2x^{12} + b_2^4x^8 + b_1^8.$$

Experimentally, when the curve is irreducible, the genus of this curve always seems to be at most 8. This curve is reducible when $b_3 = b_0 + b_1 + b_2$, and when reducible, one of the components is given by

$$C_{4a} : y^8 + x^4y^4 + x^6y^2 + x^7y + x^{12} + x^9 + b_0x^6 + (b_2^2 + b_1^2)x^4 + b_1^4.$$

When C_{4a} is irreducible it experimentally always has genus at most 4.

Note, in all the cases above; when the curve, C, was irreducible it experimentally had genus equal to 2^{n-1} or $2^{n-1} - 1$. In addition we experimentally noticed that the irreducible components were always hyperelliptic. These remarkable properties we shall prove hold in general in the next section.

3. Hyperellipticity and genus of curves in the Weil restriction

In this section we show that the observations of the previous section about the genus, irreducibility and hyperellipticity of the curves $\mathfrak{C}$ hold in general. In addition we shall show the existence of a computable mapping from $E(\mathbb{F}_{q^n})$ to the divisor class group of a hyperelliptic curve. It is this mapping which translates the hard elliptic curve discrete logarithm problem, into a potentially easier hyperelliptic discrete logarithm problem.

We shall now let K denote an arbitrary extension, of degree n, of the field k, of characteristic two. We shall make no assumptions about the existence of special types of bases of K over k as we did in the previous section. In this section, to keep track of which fields we are considering, all fixed elements of K will be denoted by greek letters.

We take an elliptic curve

$$Y^2 + XY = X^3 + \alpha X^2 + \beta$$

where $\alpha, \beta \in K$. We can form the Weil restriction as in the previous section by expanding coordinate representations of X and Y with respect to any given basis of K over k. We intersect the resulting abelian variety, A, with the hyperplanes which mark out the subvariety of values of X which lie in k. The resulting subvariety of A will be a curve defined over k, in $n+1$ dimensional space, which we shall denote by $\mathfrak{C}$, as in the previous section.

We wish to study the curves $\mathfrak{C}$ geometrically, so we consider $\mathfrak{C}$ defined over the algebraic closure of k. In fact we shall only need to go to the extension K.

By a linear change of variables, defined over K, we find that $\mathfrak{C}$ is birationally equivalent to the curve $\mathfrak{D}$, defined over K, given by

$$\mathfrak{D} : \begin{cases} w_0^2 + xw_0 + x^3 + \alpha_0x^2 + \beta_0 = 0, \\ \quad\vdots \\ w_{n-1}^2 + xw_{n-1} + x^3 + \alpha_{n-1}x^2 + \beta_{n-1} = 0. \end{cases}$$

where $\alpha_i = \sigma^i(\alpha)$ and $\beta_i = \sigma^i(\beta)$, with σ the Frobenius automorphism of K over k. Note that if $(x, y) \in E(K)$, with $x \in k$, then $w_i = \sigma^i(y)$.

Lemma 2. *Let F_i be the splitting field of the i-th such equation over $K(x)$. We can form the compositum $F = F_0 \cdots F_{n-1}$ over $K(x)$ without ambiguity. Let $[F : K(x)] = 2^m$ then viewed over K the curve $\mathfrak{D}$ then has 2^{n-m} irreducible reduced components having function fields K-isomorphic to F.*

Proof. In order to generate F we can choose a subset of m equations defining the curve $\mathfrak{D}$ which define a prime ideal of dimension $n+1-m$ in $K[x, w_0, \dots, w_{n-1}]$. Since $x = 0$ is the only finite place of $K(x)$ which ramifies in an F_i, the other equations, after multiplying by suitable minimal non-negative powers of x, will factor into linear factors modulo this prime ideal. We have thus 2^{n-m} choices to enlarge the prime ideal to a prime ideal of dimension one. □

If we multiply the equations defining $\mathfrak{D}$ by x^{-2}, substitute $w_i/x + \beta_i^{1/2}/x$ by s_i and $1/x$ by z, we see that another model for our curve $\mathfrak{D}$ is

$$\mathfrak{F} : \begin{cases} s_0^2 + s_0 + z^{-1} + \alpha_0 + \beta_0^{1/2} z = 0, \\ \qquad \vdots \\ s_{n-1}^2 + s_{n-1} + z^{-1} + \alpha_{n-1} + \beta_{n-1}^{1/2} z = 0. \end{cases}$$

Then Artin-Schreier theory [2, pp. 22] applied to the above equation implies that we have

$$m = \dim_{\mathbb{F}_2} \left(U / U \cap V \right). \tag{1}$$

where

$$\begin{aligned} U &= \operatorname{Span}_{\mathbb{F}_2} \{ (1, \alpha_0, \beta_0^{1/2}), \dots, (1, \alpha_{n-1}, \beta_{n-1}^{1/2}) \}, \\ V &= \{ (0, x^2 + x, 0) : x \in K) \}. \end{aligned}$$

Notice that when $\alpha = 0$ or 1 we have the simpler equation

$$m = \dim_{\mathbb{F}_2} \Big(\operatorname{Span}_{\mathbb{F}_2} \{ (1, \beta_0^{1/2}), \dots, (1, \beta_{n-1}^{1/2}) \} \Big).$$

Upon reordering we may assume in the following that $F = F_0 \cdots F_{m-1}$. Adding the 0-th equation to the i-th equation of $\mathfrak{F}$ for $i = 1, \dots, m-1$ and substituting t_i for $s_0 + s_i$, γ_i for $\alpha_0 + \alpha_i$ and δ_i for $\beta_0^{1/2} + \beta_i^{1/2}$ we obtain

$$t_i^2 + t_i + \delta_i z + \gamma_i = 0, \quad i = 1, \dots, m-1 \tag{2}$$

These equations define extensions L_i of $K(z)$ such that $F = F_0 L$ with $L = L_1 \cdots L_{m-1}$. The field L is crucial to establishing the hyperellipticity, since it defines a rational subfield of index two, as we shall now show.

Lemma 3. *The field L is an extension field of degree 2^{m-1} of $K(z)$. It is a rational function field $L = K(c)$ having a generator c such that $z = \lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i c^{2^i}$ with $\lambda_i \in K$ and $\lambda_0, \lambda_{m-1} \neq 0$.*

Proof. The extension field statement follows from $F = F_0 \cdots F_{m-1}$.

We now apply inductively some further transformations to (2). We wish to determine a change of variable so that we have equations of the form

$$t_i^2 + t_i + \delta_i t_{i-1} + \gamma_i = 0, \quad i = 1, \dots, m-1. \tag{3}$$

Suppose after already having done some transformations (with t_i, γ_i and δ_i substituted properly) we are given equations, for some $j \in [1, \dots, m-1]$,

$$\begin{aligned} t_i^2 + t_i + \delta_i t_{i-1} + \gamma_i &= 0, \quad i = 1, \dots, j-1, \\ t_i^2 + t_i + \delta_i z + \gamma_i &= 0, \quad i = j, \dots, m-1, \end{aligned}$$

where $t_0 = z$.

By substituting $t_j + (\delta_j/\delta_1)^{1/2} t_1$ for t_j and using the above equations with $i = 1$ we obtain

$$t_j^2 + t_j + \left(\left(\frac{\delta_j}{\delta_1} \right)^{1/2} + \frac{\delta_j}{\delta_1} \right) t_1 + \frac{\delta_j}{\delta_1} \gamma_1 + \gamma_j = 0,$$

wherein we write δ_j for the coefficient of t_1 and γ_j for the constant term. By eliminating t_1 in the same way as done with $z = t_0$ using the equation for $i = 2$, and repeating this for $t_2, t_3, \ldots$ we eventually arrive at

$$t_j^2 + t_j + \delta_j t_{j-1} + \gamma_j = 0,$$

as desired. By induction we go on until $j = m$.

Next, by expressing $z = (t_1^2 + t_1 + \gamma_1)/\delta_1$, $t_1 = (t_2^2 + t_2 + \gamma_2)/\delta_2$, and so on, we obtain $z = \lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i c^{2^i}$ with $c = t_{m-1}$ and suitable $\lambda_i \in K$. Since $L/K(z)$ is separable and $[L : K(z)] = 2^{m-1}$ we finally see that none of the δ_i will be zero in this process, and that $\lambda_0, \lambda_{m-1} \neq 0$ necessarily. □

Lemma 4. *F/K is a hyperelliptic function field of genus 2^{m-1} or genus $2^{m-1} - 1$ over the exact constant field K.*

Proof. We have $F = F_0 L$ and $[F : L] = 2$. The hyperellipticity is now clear since L is rational by Lemma 3.

Next we prove the genus statement. In order to get F from L we need to adjoint a root of the 0-th equation defining $\mathfrak{F}$ to L. We take a closer look at the absolute coefficient $u = 1/z + a + \beta_0^{1/2} z$, where we think of z as a polynomial in c of degree 2^{m-1} as in Lemma 3. Since this polynomial is separable it factors into prime polynomials with exponents one. The valuations of u at the corresponding places of the rational function field L defined above $z = 0$ are thus all -1.

The Artin-Schreier reduced pole valuations coming from the zeros of z have just been determined, we get $m_P = 1$ for all places P of L such that $v_P(z) = 0$. We also have $\sum_{v_P(z)=0} \deg P = 2^{m-1}$. We need to look at the degree valuation. But because of the particular structure of each t_i in equation (3) we can reduce u to have degree at most one in c by subtracting elements of L of the form $v^2 + v$, from which follows $m_\infty = 1$ or $m_\infty = -1$.

Summing up, using [15, p. 115], we obtain finally $g = 2^{m-1}$ or $g = 2^{m-1} - 1$.

The constant field statement follows from L being rational and F having genus greater than or equal to one. □

Up to now we have used the Artin-Schreier nature of the equations defining $\mathfrak{D}$ (resp. $\mathfrak{F}$) in an essential way, in order to obtain the statements on the hyperellipticity and the genus. Next, we need to restrict to a smaller constant field, and here we will use the existence of a Frobenius automorphism on F which is due to the very construction of $\mathfrak{D}$.

Theorem 5. *The Frobenius automorphism σ on K extends to a k-automorphism on F. Let F' be its fixed field. Then F' is an hyperelliptic function field of genus 2^{m-1} or $2^{m-1} - 1$ over the exact constant field k. The curve $\mathfrak{C}$ has an irreducible reduced component having F' as its function field.*

Proof. The Frobenius automorphism σ extends to a k-automorphism of $K(x)$ by leaving x fixed. Since the equations defining $\mathfrak{D}$ are conjugated under σ in the obvious way we see that it extends to a k-automorphism of F of order n mapping a root of an equation of $\mathfrak{D}$ to a root of the next equation. The fixed field F' of σ thus has index n in F and it is clear that $F' \cap K = k$ holds.

Let $L' := F' \cap L$. Then σ restricts to a k-automorphism of L of order n because it is the unique subfield of F of index 2. Thus also $[L : L'] = n$ and we get $[F' : L'] = 2$, as desired. Clearly $F = F'K$ (and also $L = L'K$) which gives the genus statement. Besides x, F' contains n elements, obtained via linear transformation from the w_i above, which generate F' over k and which satisfy the equations of $\mathfrak{C}$. We thus finally see that $\mathfrak{C}$ has an irreducible reduced component with function field F'. □

Notice that every irreducible reduced component of the curve $\mathfrak{C}$ will have the same genus as above, but the corresponding function fields will in general (except F') contain proper constant field extensions of k, making them useless. If the value of m is too small then none of the irreducible components of $\mathfrak{C}$ will have a Jacobian which contains a subvariety isogenous to the subvariety B of A. For example let $E(\mathbb{F}_{q^n})$ denote a Koblitz curve, i.e. one defined over the field $\mathbb{F}_2$. We will then obtain irreducible components of $\mathfrak{C}$ of genus one. In this case, the Weil restriction, A, factors as the product

$$A = E(\mathbb{F}_q) \times B$$

where B is an $n-1$-dimensional abelian variety defined over $\mathbb{F}_q$. The curve in the Weil restriction we have constructed has irreducible components whose Jacobians are isogenous to $E(\mathbb{F}_q)$ and so we obtain no information about the subvariety B from our curves. This does not mean that one cannot find useful curves in A, whose Jacobian contains a subvariety isogenous to B. It just means that the curves we have constructed are not useful in this context.

We let H denote the hyperelliptic curve over k which has F' as its function field. We next address the question of mapping the discrete logarithm problem on E to a suitable one in $Cl^0(F')$, where we again use the function field setting. Using the conorm, $Con_{F/K(E)}$, we map a divisor class in $Cl(K(E))$ to $Cl(F)$, and from there, using the norm $N_{F/F'}$, to $Cl(F')$. On composition we thus obtain a group homomorphism

$$\phi : Cl(K(E)) \to Cl(F'),$$

which we can then restrict to degree zero divisors.

Lemma 6. *The kernel of $Con_{F/K(E)} : Cl(K(E)) \to Cl(F)$ can only consist of 2-power torsion elements of $Cl(K(E))$.*

Proof. Let $D \in Cl(E)$, then we have $N_{F/K(E)}(Con_{F/K(E)}(D)) = [F : K(E)]D$. Thus, if $Con_{F/K(E)}(D)$ is principal, then $[F : K(E)]D$ is also principal. But $[F : K(E)] = 2^{m-1}$ which means that $[D]$ has 2-power order. □

However, the kernel of ϕ can be quite large for small m. But if m is not too small then the large prime factor of E will be preserved in many instances. Hence to solve our discrete logarithm problem

$$P_2 = [l]P_1$$

on $E(K)$ we map degree zero divisor classes representing P_2 and P_1 over to $Cl^0(F')$ using the map ϕ. Setting $D_1 = \phi([P_1])$ and $D_2 = \phi([P_2])$. Providing we do not obtain $D_1 = D_2 = 0$, which in practice is unlikely unless the elliptic curve is actually defined over a subfield of K, we can attempt to solve the discrete logarithm problem

$$D_2 = [l]D_1$$

in $Cl^0(F')$.

The computation of images under ϕ is in principle possible by general methods, such as those used for computations with algebraic number fields. Nevertheless, we want to give some indications of how to proceed in our case.

A hyperelliptic equation for F over K can be computed along the lines of the above proofs where we choose $y = w_0 \in K(E) \subseteq F$ and $c \in L$ as generators. Such an equation is obtained by substituting $\left(\lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i c^{2^i}\right)^{-1}$ for x in the equation of E, as in Lemma 3.

Let P be a place of $K(E)$ of degree one where $x, y \in K(E)$ take the values $x(P), y(P) \in K$ respectively (we assume for simplicity that $x(P) \neq 0, \infty$). Then $Con_{F/K(E)}(P)$ can be computed as the greatest common divisor of the principal divisors $(x + x(P))$ and $(y + y(P))$ in F. It is a divisor of degree 2^{m-1}.

We next have to find L' and F' and compute the norm $N_{F/F'}$. By tracing back the transformations done above we may obtain the conjugates $\sigma^i(y) = w_i \in F$, represented as rational functions in c and y. The following Lemma then gives an explicit construction of F'.

Lemma 7. *Choose* $\mu \in K$ *such that* $Tr_{K/k}(\mu) = 1$ *and set* $\tilde{c} := Tr_{L/L'}(\mu\lambda_0 c)$, $\tilde{y} := Tr_{F/F'}(\mu y)$. *We then have* $L' = k(\tilde{c})$ *and* $F' = k(\tilde{y}, \tilde{c})$.

Proof. From the extension structure $L/K(z)$, because $z = \lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i c^{2^i}$, it is clear that σ maps poles of c to poles of c. Since L is rational we readily see that there are $\lambda, \lambda' \in K$ such that $\sigma(c) = \lambda c + \lambda'$. Then

$$\begin{aligned} \sigma(z) &= \sigma\left(\lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i c^{2^i}\right) \\ &= \sigma(\lambda_{-1}) + \sum_{i=0}^{m-1} \sigma(\lambda_i)\left(\lambda'^{2^i} + \lambda^{2^i} c^{2^i}\right). \end{aligned}$$

On equating coefficients in $\sigma(z) = z$, we obtain for $\lambda_i \neq 0$ and $i \geq 0$

$$\lambda^{2^i} = \lambda_i / \sigma(\lambda_i).$$

For $i = 0$ we thus obtain

$$\sigma(\lambda_0 c) = \sigma(\lambda_0)(\lambda c + \lambda') = \lambda_0 c + \sigma(\lambda_0)\lambda'.$$

Now $\tilde{c} = Tr_{L/L'}(\mu\lambda_0 c) = \lambda_0 c + \lambda''$ for some $\lambda'' \in K$ and thus $L' = k(\tilde{c})$.

Consider the Galois group of $F/K(x)$. It is an elementary abelian 2-group whose elements send each $\sigma^i(y)$ to $\sigma^i(y)$ or $\sigma^i(y) + x$. Now let τ be the hyperelliptic involution on F/L. Since τ fixes L we have $\tau(\sigma(y)) = \sigma(y) + x = \sigma(\tau(y))$. It operates by restriction on F'/L'. We again consider the equations defining $\mathfrak{F}$. Since $y = xs_0 + \beta^{1/2}$ we observe

$$Tr_{F/F'}(\mu y) = xTr_{F/F'}(\mu s_0) + Tr_{K/k}(\mu\beta^{1/2}).$$

Let us abbreviate $\tilde{s} := Tr_{F/F'}(\mu s_0)$. Then, as $\tau(\tilde{s}) = \tilde{s} + 1$, we have

$$Tr_{F'/L'}(\tilde{s}) = \tilde{s} + \tau(\tilde{s}) = 1.$$

Using

$$\tilde{s}^2 = Tr_{F/F'}(\mu^2 s_0^2) = Tr_{F/F'}(\mu^2(s_0 + 1/z + \alpha + \beta^{1/2} z))$$

we obtain for the norm

$$\begin{aligned} N_{F'/L'}(\tilde{s}) &= \tilde{s}(\tilde{s}+1) \\ &= 1/z + Tr_{K/k}(\mu^2\alpha) + Tr_{K/k}(\mu^2\beta^{1/2})\, z \\ &\qquad + \big(Tr_{F/F'}(\mu^2 s_0) + Tr_{F/F'}(\mu s_0)\big). \end{aligned}$$

Putting together we thus get

$$\begin{aligned} \tilde{s}^2 + \tilde{s} + 1/z + Tr_{K/k}(\mu^2\alpha) + Tr_{K/k}(\mu^2\beta^{1/2})\, z \\ + \big(Tr_{F/F'}(\mu^2 s_0) + Tr_{F/F'}(\mu s_0)\big) = 0. \end{aligned} \tag{4}$$

This equation is separable in $\tilde{s}$, and by construction it has coefficients in L'. Looking at the equations defining $\mathfrak{F}$ gives that the valuation of s_i at the zeros of z is only half the valuation of $1/z$. The term in the second line of (4) is a K-linear combination of the s_i and, as element of L', has no poles except at $\tilde{c} = \infty$. It is therefore a polynomial in $\tilde{c}$ and we can conclude that the left hand side of (4) is indeed irreducible. □

In the case of odd n we can choose $\mu = 1$. We then obtain the equation

$$\tilde{y}^2 + x\tilde{y} + x^3 + Tr_{K/k}(\alpha)x^2 + Tr_{K/k}(\beta),$$

where x is the inverse of the separable polynomial $\lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i((\tilde{c} + \lambda'')/\lambda_0)^{2^i} \in k[\tilde{c}]$. We remark that in this case the genus of F'/k is $2^{m-1} - 1$ if $Tr_{K/k}(\beta) = 0$.

Let P be a place of F dividing $Con_{F/K(E)}(P_1)$ for some place P_1 of $K(E)$ of degree one. We can represent P as the greatest common divisor of the numerators of the principal divisors $(\tilde{y} + \tilde{y}(P))$ and $(f(\tilde{c}))$ where f is the minimal polynomial of $\tilde{c}(P)$ over K (provided that $x(P_1) \neq 0$, which we assume). In order to determine the underlying place $P' = F' \cap P$ of F' we need to express the situation "symbolically".

The place $L' \cap P$ is determined by the numerator of $(\tilde{f}(\tilde{c}))$, where $\tilde{f}$ is the minimal polynomial of $\tilde{c}(P)$ over k, and the principal divisor is taken in L'. The place P' is obtained as follows: Let h be a bivariate polynomial over k such that $h(\cdot, \tilde{c}(P))$ is the minimal polynomial of $\tilde{y}(P)$ over $k(\tilde{c}(P))$. Then we obtain P' by computing the greatest common divisor of the numerators of $(\tilde{f}(\tilde{c}))$ and $(h(\tilde{y}, \tilde{c}))$, where the principal divisors are taken in F'. Finally, $N_{F/F'}(P) = f(P, P')P'$ where $f(P, P') = n \deg(P)/\deg(P')$ is the residue class degree of P over P'. We will have that $\deg\big(N_{F/F'}(Con_{F/K(E)}(P_1))\big) = n2^{m-1}$.

A program for computing F' and ϕ given $E(\mathbb{F}_{q^n})$ is planned to be written for inclusion in the Magma computer algebra system.

4. Constructing Hyperelliptic Cryptosystems

Our method for constructing hyperelliptic cryptosystems is now immediate.

1. Fix a field $k = \mathbb{F}_q$ and an integer n such that $K = \mathbb{F}_{q^n}$.
2. Using the algorithm of Schoof, [12], determine an elliptic curve, E, over K of order $2^l p$ where p is a prime and l is a small integer.
3. Construct the Weil restriction and the curve $\mathfrak{C}$ as we did in Section 3.
4. Find a model, H, of an irreducible component of $\mathfrak{C}$ in hyperelliptic form.
5. Check that the divisor class group of H over k has a subgroup of order p.

The final condition is necessary since we only know that a subvariety of A is isogenous to a subvariety of the Jacobian of H.

If in the above algorithm we choose $n = 4$, $b_3 = b_0 + b_1 + b_2$, with the special examples of Section 2, we will expect to obtain a hyperelliptic curve of genus 3 or 4, defined over k, whose Jacobian will, in general, have order $2^l p$. If l is chosen small then we do not expect to obtain genus 3. If we choose $n = 2$, and a very small value for l, then we expect to obtain a hyperelliptic curve of genus 2, defined over k, whose Jacobian has order divisible by p.

4.1. **Genus Four Example.** We consider an example where $p \approx 2^{80}$. Clearly this is not large enough for cryptographic use, but it is illustrative for example purposes, both here and later. Curves with $p > 2^{160}$ are just as easy to produce, they just require more paper to write down.

Consider the field $k = \mathbb{F}_{2^{21}}$ generated over $\mathbb{F}_2$ by a root of the polynomial:

$$w^{21} + w^2 + 1.$$

Let $K = \mathbb{F}_{2^{84}}$ be generated over k by a root of the polynomial

$$\theta^4 + \theta^3 + \theta^2 + \theta + 1.$$

We construct the elliptic curve

$$E : Y^2 + XY = X^3 + b_0\theta + b_1\theta^2 + b_2\theta^4 + b_3\theta^8$$

where

$$b_0 = 0,\ b_1 = w^{1127280},\ b_2 = w^{171398},\ b_3 = w^{1370436}.$$

Notice that $b_3 = b_0 + b_1 + b_2$, and hence we expect to obtain a hyperelliptic curve of genus four. The order of $E(K)$ is computed using the algorithm of Schoof [12] and it is equal to $2^4 p$, where

$$p = 1208925819614311295169073.$$

Our algorithm for producing a curve of genus four in the Weil restriction produces the curve C_{4a}, of Section 2. This curve has Jacobian also of order $2^4 p$. But the curve C_{4a} is birationally equivalent to the hyperelliptic curve

$$H : Y^2 + G(X)Y + F(X) \tag{5}$$

where $G(x)$ is given by

$$X^4 + w^{624429}X^3 + w^{1248858}X^2 + w^{1442662}X + w^{386860}$$

and $F(X)$ is given by

$$\begin{aligned} X^9 \quad &+ \quad w^{1859582}X^6 + w^{293124}X^4 + w^{1783647}X^3 \\ &+ \quad w^{1541982}X^2 + w^{1370912}X + w^{1888298}. \end{aligned}$$

4.2. **Genus Two Example.** We construct an elliptic curve over the field $K = \mathbb{F}_{2^{162}}$ with group order equal to

$$5846006549323611672814739995379292203636332479268$$

which is four times a prime, p. We do not give the details of this elliptic curve here for reasons of space. The Weil restriction, and our construction of the associated hyperelliptic curves, produces the following example of a genus two hyperelliptic curve defined over $k = \mathbb{F}_{2^{81}}$.

Define k by $k = \mathbb{F}_2[w]/(1 + w^4 + w^{81})$. The Jacobian of the hyperelliptic curve of genus two given by

$$\begin{aligned} H : Y^2 \quad &+ \quad (X^2 + w^{2012013793551629036365609} X)Y \\ &= \quad X^5 + X^4 + w^{1586464037343056940725724} X^2 \\ &\qquad +w^{4333422298784960095154 7} X + w^{7747883459877983146322 40} \end{aligned}$$

has order divisible by p. Its group structure is given by $C_2 \times C_{2p}$ and it is not subject to the Tate-pairing attack [7] since p does not divide $q^k - 1$ for small values of k.

5. Attacking Elliptic Curve Cryptosystems

The question remains as to whether the above construction provides either a mechanism to attack elliptic curve cryptosystems or whether the hyperelliptic cryptosystems proposed above are strong. In this section we discuss the difficulty of solving the discrete logarithm problem in the Picard group of the hyperelliptic curves we have constructed. We shall assume a fixed, small, value of n and we look at the situation as q tends to infinity.

For any group, the rho method (with Pohlig-Hellman) provides an algorithm for computing the discrete logarithm in time $O(\sqrt{p})$ where p is the largest prime factor of the order of the group. For general elliptic curves, this is the best known algorithm. For the curves defined over $\mathbb{F}_{q^n}$ considered in this paper we obtain a complexity of $O(q^{n/2})$ in general.

For hyperelliptic curves, we can get a better complexity by using an index-calculus method. If the curve is defined over $\mathbb{F}_q$ and the genus is not too high (say at most 8), we can proceed as follows. We consider a factor base containing all the prime divisors of the Jacobian of degree one. We can then proceed in two phases. In the first phase, relations are found between the elements of the factor base, whilst in the second phase we perform sparse linear algebra to solve the original discrete logarithm problem. The details of this algorithm are in [9], but we give some details in an example below.

Theorem 8 (Gaudry, [9])**.** *There is an index calculus style algorithm to solve the hyperelliptic discrete logarithm problem in a hyperelliptic curve of genus g over the field $\mathbb{F}_q$ which requires a factor base of size $O(q)$ and which runs in time*

$$O\left(g^3 g! q \log^\gamma q\right) + O\left(g^3 q^2 \log^\gamma q\right)$$

for some fixed integer γ.

Hence for fixed values of g the complexity of this algorithm is $O(q^{2+\epsilon})$, which is better than the rho method for a (almost) cyclic Jacobian of genus at least 5. However, it is unclear where the exact crossover point between Gaudry's method and the rho method lies.

The theoretical complexity can be improved by reducing the size of the factor base. The smoothness bound is already minimal, but we can decide that some of the prime divisors of degree one are 'good' (we keep them in the factor base), whereas others are rejected. If we set the proportion of 'good' divisors to $1/l$, then the time for finding a relation will be increased by a factor l^g. However, we will need l times less such relations, and the cost of the linear algebra will be reduced by a factor $1/l^2$. If we try to optimize the choice of l, we get $l = \Theta(q^{1/(g+1)})$, and the complexity becomes $O(q^{\frac{2g}{g+1}+\epsilon})$, as $q \to \infty$.

In the following table we give the complexities of the discrete logarithm problem on the elliptic curves studied in the previous sections and on the corresponding Jacobians. We only look at the genera which are likely to occur in practice for the example curves in Section 2 and we ignore the q^ϵ term in the complexity estimate. Notice that for the 'interesting' subvariety of $\mathrm{Jac}(C)$ in our Weil-descent examples the complexity of the rho method on $\mathrm{Jac}(C)$ is equal to the complexity of the rho method on $E(\mathbb{F}_{q^n})$. For a general Jacobian of genus g the rho method has complexity $O(q^{g/2})$.

Example Curve	C_2	C_3	C_3	C_4	C_4	C_{4a}
n, g	2,2	3,3	3,4	4,8	4,7	4,4
rho on $E(\mathbb{F}_{q^n})$	q	$q^{3/2}$	$q^{3/2}$	q^2	q^2	q^2
Index on $\mathrm{Jac}(C)$	$q^{4/3}$	$q^{3/2}$	$q^{8/5}$	$q^{16/9}$	$q^{7/4}$	$q^{8/5}$

We stress that these complexities hold as q tends to infinity and with n and g fixed. Hence for $g \geq 4$ we obtain a complexity which is better than that of Pollard rho.

In a context where we would like to *build* a hyperelliptic cryptosystem by a Weil descent, the Jacobians have to be almost cyclic, which occurs for the cases C_2, C_3 and C_{4a}. For the first two, this seems to be a good way to build a cryptosystem in genus two or three; however, for the last one the index-calculus provides an attack with a better theoretical complexity than the rho method, and the security is asymptotically lower than with an elliptic curve cryptosystem with the same key size.

On the other hand, if we want to *attack* an elliptic curve cryptosystem, we see that for C_4 and C_{4a} the complexity of index-calculus is better than for the rho method. Thus, asymptotically, it is a good way to attack such elliptic curve cryptosystems by transferring the problem to a hyperelliptic curve.

However experiments have to be done, for each fixed value of n and g, to see where is the crossover between the two attacks, since the group operations in $E(\mathbb{F}_{q^n})$ and in $\mathrm{Jac}(C)$ will have different complexities. Such an experiment is carried out in the next section.

6. Solving a hyperelliptic DLOG problem

It is important to decide, not only for the Weil descent attack but also for our construction of hyperelliptic cryptosystems in genus four, whether Gaudry's method is practical in genus four. In this section we consider the example given by the curve in equation (5). The fields size is $q = 2^{21}$ and the curve has genus 4, so the Jacobian has size approximately 2^{84}. We will solve a discrete logarithm problem in this group using Gaudry's method and then compare the running time to known efficient implementations of the rho method in an elliptic curve group of the same size. Since the rho method applied to a hyperelliptic curve will run slower than on an equivalently sized elliptic curve, if Gaudry's method runs faster on the hyperelliptic curve compared to rho on an elliptic curve we will know that

- Genus four systems are less secure than the equivalent elliptic curve system, for field sizes greater than 2^{21}. We would then conclude that genus four hyperelliptic systems should not be deployed in real life.

- Elliptic curves defined over $\mathbb{F}_{q^n}$, with $m = 3$ and $q = 2^t$, are weaker than those defined over $\mathbb{F}_{2^p}$ with p prime and of the order of nt.

We attempted to solve the discrete logarithm problem given by

$$D_2 = [l]D_1$$

where

$$\begin{aligned} D_1 &= (X^4 + w^{1277131}X^3 + w^{1087066}X^2 + w^{1391819}X + w^{1964994}, \\ &\quad w^{1784094}X^3 + w^{131164}X^2 + w^{1975559}X + w^{2073352}), \\ D_2 &= (X^4 + w^{895988}X^3 + w^{1765969}X^2 + w^{1667155}X + w^{1531893}, \\ &\quad w^{110642}X^3 + w^{2014036}X^2 + w^{927941}X + w^{1063447}), \end{aligned}$$

where the divisors are given in the reduced representation as in the paper by Cantor, [4]. In this notation, the point at infinity is implicitly subtracted with the correct multiplicity in order to obtain a divisor of degree zero. The divisor D_1, above, is a generator of the subgroup of prime order $p \approx 2^{80}$.

The factor base consists of all prime divisors of the form

$$\mathfrak{p} = (X + \alpha, \beta)$$

where $\alpha, \beta \in k = \mathbb{F}_q$, and

$$\beta^2 + G(\alpha)\beta + F(\alpha) = 0.$$

To each α there are two corresponding values of β, but we only choose one of these to be in our factor base, since the two prime divisors are related by the equation:

$$(X + \alpha, \beta) + (X + \alpha, G(\alpha) + \beta) \equiv 0,$$

in the divisor class group.

To reduce the factor base even further we only use divisors in the factor base such that the binary representation of α has a bit representation with its three most significant bits set of zero. Where the bit representation is in the polynomial basis with respect to w. Such prime divisors will be called 'good'. In our example the number of such good divisors which make up our factor base, **F**, is 131294.

Consider the following general reduced divisor

$$D = (a(X), b(X))$$

with $\deg b < \deg a \leq g$. A necessary condition for this divisor to factor over our factor base of 'good' divisors will be for the binary representation of $a_{\deg a - 1}$, the $(\deg a - 1)$th coefficient of $a(X)$, to have its three most significant bits set to zero. This gives us a simple test to eliminate lots of divisors which are not smooth over our set of good divisors.

The algorithm proceeds as follows. We compute a set of 'random' multipliers

$$M_i = [r_i]D_1 + [s_i]D_2, \text{ for } 1 \leq i \leq 20,$$

for some random integers r_i and s_i. Then setting $R_1 = M_1$, say, we compute the following random walk

$$R_{i+1} = R_i + M_{h(R_i)}$$

where $h : \mathrm{Jac}(H) \to [1, \ldots, 20]$ is some hash function. Notice that every value R_i can be written as

$$R_i = [a_i]D_1 + [b_i]D_2.$$

We then try to 'factor' R_i over our factor base to obtain a relation of the form

$$R_i = \sum_{\mathfrak{p}\in\mathbf{F}} [t_{\mathfrak{p}}]\mathfrak{p}.$$

Due to our choice of factor base this factorization can be achieved using root extraction techniques over finite fields rather than general polynomial factoring techniques. We eliminate many divisors, before we apply root extraction, by our test for smoothness over the good divisors which we described above. The resulting $t_{\mathfrak{p}}$ lie in $[-g, \dots, g]$, where for our example $g = 4$. We store the $t_{\mathfrak{p}}$ in a matrix as a column, which will have at most g non-zero entries in each column. Almost all relations we obtain will have $t_{\mathfrak{p}} \in \{-1, 0, 1\}$ and will have exactly g non-zero values of $t_{\mathfrak{p}}$ in each column.

After collecting more relations than elements in our factor base we can apply sparse matrix techniques modulo p, such as the Lanczos method, to find a non-trivial element in the kernel of the matrix. Using the element in the kernel we can then find the solution to the original discrete logarithm problem, with overwhelming probability, in the standard manner.

We run the above algorithm on the above example. The relation collection phase took about two weeks of calendar time, using the idle time of a disparate set of machines. If we had run this task on a single Pentium II 450 MHz, the timing would have been about 31 weeks. The linear algebra step took 64.4 hours using the same machine. After which we determined the solution to $D_2 = [l]D_1$ was given by

$$l = 12345678.$$

An equivalent calculation on an 84 bit elliptic curve, using Pollard's rho method, would have taken 44 weeks on the same machine, with a program with a similar level of optimizations applied. Since the crossover point is for a value of q less than what would be used in practice, we can conclude that genus four hyperelliptic systems are weaker than an elliptic curve system with the same size group order.

7. Other Types of Finite Fields

7.1. **Non-composite Fields Of Even Characteristic.** In Section 5 we looked at what happens when n is fixed and we let q tend to infinity. In practice the elliptic curves over even characteristic fields which are used are ones defined over $\mathbb{F}_{2^p}$, with p a prime. Hence we need to look at the situation where q is fixed and n tends to infinity.

Let E denote an elliptic curve, defined over $\mathbb{F}_{2^p}$ where p is prime. We expect that the methods of this paper would produce a hyperelliptic curve of genus 2^{p-1} over the field $\mathbb{F}_2$. It seems unlikely that one would, in general, be able to find a curve of significantly smaller genus in the Weil restriction of $E(\mathbb{F}_{2^p})$ over $\mathbb{F}_2$.

However, using equation (1) one may be able to find, in very special circumstances, certain elliptic curves which have values of m slightly larger than $\log_2 p$ and hence for which there exist curves in the Weil restriction of genus slightly larger than p, as the following example shows:

Consider $K = \mathbb{F}_2[w]/(1 + w + w^{127})$ and the elliptic curve defined by $(a, \beta) = (0, w)$, i.e.

$$E : Y^2 + XY = X^3 + w.$$

The number points on $E(K)$ is computed to be

$$\#E(\mathbb{F}_{2^{127}}) = 2^{20} \cdot 3^2 \cdot 45615671 \cdot 395232781659164075412101.$$

Along the arguments of Section 3 we computed its Weil restriction for $n = 127$ down to $\mathbb{F}_2$, obtaining the hyperelliptic curve

$$H : y^2 + (x^{128} + x^{64} + x)y + x^{128} + x^{64} + x.$$

The curve H has genus 127 and its Jacobian contains an element of order $\#E(\mathbb{F}_{2^{127}})/2$.

We constructed this example by trying to make m as small as possible. It appears that one can obtain very small values of m for β a zero of a polynomial with only 2-power coefficients. In the above case $\beta^{128} + \beta^2 + \beta = 0$. Another similar value for β may be obtained by a zero of the irreducible factor of degree 127 of $x^{2^{10}} + x^2 + x$ over $\mathbb{F}_2$.

In general, for random β, a small value of m is very unlikely as we shall now show.

Lemma 9. *We expect at least fifty percent of all the elliptic curves over $K = \mathbb{F}_{2^p}$, for p prime to produce a value of m equal to p.*

Proof. By a change of variables we can put our curve in the form

$$Y^2 + XY = X^3 + \alpha X^2 + \beta$$

where $\alpha = 0$ or 1 and $\beta \in K$. Now by the definition of m in (1), if $\{\beta, \beta^2, \ldots, \beta^{2^{p-1}}\}$ is a normal basis of K over $\mathbb{F}_2$ then $m = p$. But around fifty percent of all elements of K generate a normal basis, as we shall now show.

By Lemma 3.69 and Theorem 3.73 of [11] the number of elements, $\beta \in K$, which generate a normal basis over $\mathbb{F}_2$ is equal to

$$2^p \prod_{i=1}^{t} (1 - 2^{-n_i})$$

where n_i denotes the degrees of the distinct monic irreducible factors of the polynomial $X^p - 1$ over $\mathbb{F}_2$. But by Theorem 2.47 of the same book we see that this is equal to

$$\left(2^{(p-1)/d} - 1\right)^d = O(2^{p-1}),$$

where d is the number of distinct factors of the polynomial $X^{p-1} + X^{p-2} + \cdots + X + 1$ over $\mathbb{F}_2$. Hence around fifty percent of all elements in K generate a normal basis. □

For general curves, where $m = p$ and $g = 2^{p-1}$, one needs to bear in mind that although there is a sub-exponential algorithm for the discrete logarithm problem on hyperelliptic curves of large genus, it is sub-exponential in the size of the Jacobian, which will be of the order of

$$2^g = 2^{2^{p-1}}.$$

But we are really aiming for a sub-exponential algorithm in the size of the original elliptic curve, which is 2^p. On the other hand, for the very special elliptic curve in the above example, we indeed obtain a possible subexponential attack. Note that Gaudry's method should not be used in this case since it is only efficient for 'small' genera.

To obtain a sub-exponential algorithm for very large genera the methods from [1, 8, 10, 14] should be combined after suitable modification for our hyperelliptic even characteristic case.

Hence for curves defined over non-composite fields of characteristic two, we do not expect the techniques in this paper to contribute a significant threat to elliptic curve cryptosystems. This last statement holds assuming curves are either chosen with values of m of the order of p, or are chosen to be curves which are defined over $\mathbb{F}_2$, i.e. a Koblitz curve.

7.2. **Odd Characteristic Fields.** The question arises as to whether the process of Weil descent can be applied to fields of the form $\mathbb{F}_{p^n}$ where p is an odd prime. Clearly we must have $n \geq 2$ and by similar arguments to those above n should not be too large.

The proofs in Section 3 relied heavily on the Artin-Schreier nature of the extensions. It appears hard to see how they can be modified to apply in the odd characteristic case. Indeed in the few examples we have calculated we see that the resulting curves neither have such nice genera nor are they hyperelliptic in nature. Hence using odd characteristic fields does not seem helpful in constructing higher genus hyperelliptic cryptosystems.

Let us turn to attacking elliptic curve systems based on fields of the form $\mathbb{F}_{p^n}$. This is an open problem which we now outline with an example: Consider the field

$$F_{p^3} = F_p[t]/(t^3 + 3491750t^2 + 217412320t + 795426309)$$

where $p = 1073741839 = 2^{30} + 15$. An elliptic curve defined over $\mathbb{F}_{p^3}$ is given by

$$Y^2 = X^3 + AX + B$$

where

$$\begin{aligned} A &= 787621733t^2 + 572191144t + 6271705, \\ B &= 167167209t^2 + 739374709t + 362095083. \end{aligned}$$

For this curve it is readily verified that the group order is

$$\#E(\mathbb{F}_{p^3}) = 2^4 \cdot 59 \cdot 2261143 \cdot 579962087855207501.$$

Setting

$$X = x_0 + x_1 t + x_2 t^2 \text{ and } Y = y_0 + y_1 t + y_2 t^2$$

one can construct the Weil restriction.

Suppose the method of Gaudry could be extended to arbitrary Jacobians and not just hyperelliptic Jacobians with almost prime group orders. This at first sight does not seem too implausible but is the subject of ongoing research, [5]. One would expect the resulting algorithm to have complexity at best $O(p^{\frac{2g}{g+1}})$. Hence to beat the asymptotic complexity of Pollard's rho method on $E(\mathbb{F}_{p^3})$ we would require a curve of genus at most 3.

Naively mimicking our method of Weil descent in characteristic two one forms the curve, C, defined by the hyperplanes $x_1 = x_2 = 0$, i.e. specializing to those x-coordinates which are fixed under the Frobenius automorphism. The resulting curve has genus 13 and is not hyperelliptic. Trying different types of bases for $\mathbb{F}_{p^3}$ over $\mathbb{F}_p$ and different hyperplanes does not appear to result in anything better.

This is an avenue for further work and the construction of a suitably well behaved curve in the Weil restriction cannot be ruled out at present.

8. Conclusion

Let $E(\mathbb{F}_{q^n})$ denote an elliptic curve over a field of even characteristic, which is not defined over a subfield of $\mathbb{F}_{q^n}$. Then we have shown how the Weil restriction produces a hyperelliptic Jacobian of genus at most 2^{n-1} which, for examples of cryptographic interest, contains a subgroup isomorphic to a subgroup of $E(\mathbb{F}_{q^n})$.

Using this observation we can construct hyperelliptic cryptosystems by first constructing elliptic curves using the Schoof algorithm and then determining the associated hyperelliptic curve. This appears to be a way to produce secure hyperelliptic cryptosystems in genus two and three. We recommend against using this method in genus four and above because of our experiment in solving discrete logarithm problems in genus four, where we showed that the discrete logarithm problem in the Jacobian of a curve of genus four was easier than on an elliptic curve of the same group order, with a security level of at least 80 bits.

However, for fixed values of $n \geq 4$, this provides evidence for the weakness of the original elliptic curve discrete logarithm problem. We have shown that for $n = 4$ and around $1/q$ of all such curves the crossover point, between our method and Pollard rho, is at a value of q less than 2^{21}. However, for larger fixed values of n, say $n = 11$ or 13, the crossover between our method and Pollard rho will be much higher. Hence, further experiments are needed in determining the exact crossover point between the two methods for various values of n.

We have no evidence to suggest that the discrete logarithm problem on general elliptic curves, defined over fields of the form $\mathbb{F}_{2^p}$ where p is prime, has complexity smaller than $O(2^{p/2})$. Since these are the fields of characteristic two which are recommended in the elliptic curve standards, Weil descent does not appear to be a threat to standards compliant elliptic curve systems in the real world.

We do, however, recommend that elliptic curves defined over $\mathbb{F}_{2^p}$, for p prime, should be checked to be sure that they produce a value for m in equation (1) which is of order around p or equal to one, as in the case of curves defined over $\mathbb{F}_2$. Only curves with these values for m should be deployed in real world cryptosystems. In practice most elliptic curves over $\mathbb{F}_{2^p}$ will satisfy such a requirement, but it is worth adding this check to curve generation programs and to standards documents.

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 *ANTS-1: Algorithmic Number Theory*, L.M. Adleman and M-D. Huang, editors. Springer-Verlag, LNCS 877, 28–40, 1994.

[2] E. Artin and J. Tate. *Class Field Theory.* Benjamin, 1967.

[3] I.F. Blake, G. Seroussi and N.P. Smart. *Elliptic Curves in Cryptography.* Cambridge University Press, 1999.

[4] D.G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, **48**, 95–101, 1987.

[5] A. Enge and P. Gaudry. A general framework for the discrete logarithm index calculus. In Preparation.

[6] G. Frey. Weil descent. Talk at Waterloo workshop on the ECDLP, 1998. **http://cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html**

[7] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves. *Math. Comp.*, **62**, 865–874, 1994.

[8] S.D. Galbraith and N.P. Smart. A cryptographic application of Weil descent. *Cryptography and Coding, 7th IMA Conference*, Springer-Verlag, LNCS 1746, 191–200, 1999. The full version of the paper is *HP Labs Technical Report, HPL-1999-70.*

[9] P. Gaudry. A variant of the Adleman–DeMarrais–Huang algorithm and its application to small genera. Submitted to *EUROCRYPT 2000.*

[10] F. Heß. Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern. Dissertation, TU Berlin, 1999.

[11] R. Lidl and H. Niederreiter. *Finite Fields,* in *Encyclopedia of Mathematics and its Applications,* G.-C. Rota, editor, Addison-Wesley, 1983.

[12] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, **44**, 483–494, 1985.

[13] N.P. Smart. On the performance of hyperelliptic cryptosystems. *Advances in Cryptology, EUROCRYPT '99*, Springer-Verlag, LNCS 1592, 165–175, 1999.

[14] V. Müller, A. Stein and C. Thiel. Computing discrete logarithms in real quadratic function fields of large genus. *Math. Comp.*, **68**, 807–822, 1999.

[15] H. Stichtenoth. *Algebraic function fields and Codes.* Springer-Verlag, 1993.

LIX, École Polytechnique, 91128 Palaiseau, France.
E-mail address: gaudry@lix.polytechnique.fr

School of Mathematics and Statistics F07, University of Sydney NSW 2006, Australia.
E-mail address: florian@maths.usyd.edu.au

Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol, BS34 6QZ, United Kingdom.
E-mail address: nigel_smart@hpl.hp.com