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 cryptosystems based on the original elliptic curve. On the other hand, we show that the same technique 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 composite degree over $\mathbb{F}_2$.

As explained in [17], there is currently no practical method which generates cryptographically secure Jacobians of hyperelliptic curves that have no special added structure. We shall present a method that will produce a hyperelliptic Jacobian related to a 'random' elliptic curve, which is secure assuming one believes 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 that 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 extensions of composite degree over the field $\mathbb{F}_2$.

Let

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

denote an elliptic curve defined over a field of characteristic two, which is not defined over a proper subfield of $K = \mathbb{F}_{q^n}$. We let m denote an integer, which is defined in Lemma 6, that satisfies $1 \leq m \leq n$. We assume that our elliptic curve satisfies one of the following conditions;

$$\dagger \begin{cases} \text{either } n \text{ is odd,} \\ \text{or } m = n, \\ \text{or } \mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0. \end{cases}$$

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

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

We shall see that if n is even, then only approximately $1/(2q)$ of all elliptic curves over K are eliminated by the above condition. We shall prove the following

Theorem 1. *Let $E(\mathbb{F}_{q^n})$ denote an elliptic curve satsifying condition (†). Let $\#E(\mathbb{F}_{q^n}) = ph$, where p is a large prime. Assuming the map ϕ defined below does not have kernel divisible by p, one can solve the discrete logarithm problem in the p-cyclic subgroup of $E(\mathbb{F}_{q^n})$ in time $O(q^{2+\epsilon})$ where the complexity estimate holds for a fixed value of $n \geq 4$ as $q \to \infty$.*

The complexity in the Theorem should be compared to the time estimate of $O(q^{n/2})$ for the best general purpose algorithm, namely Pollard's rho method. We conjecture that the condition on the kernel of the map ϕ hold in all cryptographically interesting cases.

The implied constant in the $O(\cdot)$ notation of the Theorem contains a very bad dependence on n, of the order of $O(2^n!)$. 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 $\mathbb{F}_{q^4}$ our method is only asymptotically better than Pollard rho, and further practical experiments need to be carried out to deduce whether the crossover point is at a size of q which is of cryptographic interest.

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 [7] and continued in [9], 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 $\mathbb{F}_q$. As we stated earlier, if the map ϕ maps the cryptographically interesting subgroup of $E(\mathbb{F}_{q^n})$ to the zero element in $Cl^0(H)$ then our method will fail to work. However, since it is highly unlikely that the kernel of ϕ will contain almost the whole of the group $E(\mathbb{F}_{q^n})$, we expect that our method will work in all cryptographically interesting examples.

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 G. Frey, S. Galbraith, E. Scheafer and S. Vanstone, 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 and an anonymous referee, who read and commented on earlier drafts 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 $\beta \in K$. Notice that for such curves condition (†) is satisfied. 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.

Since A is isomorphic to $E(K)$ as a group, the variety A will contain an irreducible subvariety B (we do not exclude $B = A$) with group order divisible by p. In curves of cryptographic interest, where $p \approx q^n$, this subvariety will either equal the whole of A or have dimension at least $n-1$, which can be seen by simple cardinality arguments. The variety B is the part of A in which our discrete logarithm problem is defined. We wish to find a curve C in A whose Jacobian contains a subvariety isogenous to B. Recall that B is the part of A which is interesting for cryptographic applications. Hence, we must have $g = \dim \mathrm{Jac}(C) \geq \dim B$ where $\dim B$ 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 that 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 [9].

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 below 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 $h(x) = x^{2^{n-1}} + \cdots + x^4 + x^2 + x + 1$ over the field k. Hence, we clearly require that the degree of k over $\mathbb{F}_2$ must be coprime to n, which we assume to be the case for the rest of this section. 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, for this section, we have restricted the choice of q and n. 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 irreducible 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, by the arguments of Section 2 of [9]. In examples of cryptographic interest the subvariety B of A has order divisible by a large prime p, hence the degree of the isogeny is likely to be coprime to p. Therefore, we can expect that the Jacobians actually contain a subgroup isomorphic to the subgroup of B of order p.

We give the following examples:

$\underline{n = 2}$**.**

$$C_2 : y^4 + x^3y + x^6 + x^5 + b_0x^2 + b_1^2 = 0.$$

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. Substituting a large number of elements for the parameters b_0 and b_1 into the equation for C_2, we found that experimentally the genus of this curve always seems to be 2.

$\underline{n = 3}$**.**

$$C_3 : y^8 + x^7y + x^{12} + x^{10} + x^9 + b_0x^6 + b_2^2x^4 + b_1^4 = 0.$$

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.

$\underline{n = 4}$**.**

$$C_4 : y^{16} + x^{15}y + x^{24} + x^{20} + x^{18} + x^{17} + b_0x^{14} + b_3^2x^{12} + b_2^4x^8 + b_1^8 = 0.$$

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 it is reducible, one of the components is given by

$$C_{4a} : y^8 + x^4y^4 + x^6y^2 + x^7y + x^{12} + x^9 + b_0x^6 + (b_2^2 + b_1^2)x^4 + b_1^4 = 0.$$

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

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

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.

3.1. **The curve in the Weil restriction.** We shall now let K denote an arbitrary degree n extension of a finite field k of characteristic two of q elements. 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

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

where $\alpha, \beta \in K$, $\beta \neq 0$. We do not assume condition (†) unless explicitly stated.

We can form the Weil restriction as in the previous section by substituting the coordinate representations of X and Y and expanding with respect to any given basis of K over k, but for simplicity we assume that the sum of the basis elements

is one. 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 $\mathfrak{C}$ over the algebraic closure of k. In fact, we shall only need to go to the extension K.

Lemma 2. *By a linear change of variables $y_i \mapsto w_i$, defined over K, we find that $\mathfrak{C}$ is birationally equivalent to the curve $\mathfrak{D}$, defined over K, given by*

$$\mathfrak{D} : \begin{cases} w_0^2 + xw_0 + x^3 + \alpha_0 x^2 + \beta_0 = 0, \\ \qquad \vdots \\ w_{n-1}^2 + xw_{n-1} + x^3 + \alpha_{n-1} x^2 + \beta_{n-1} = 0, \end{cases}$$

where we have $\alpha_j = \sigma^j(\alpha)$ and $\beta_j = \sigma^j(\beta)$, with σ the Frobenius automorphism of K over k.

We can extend the Frobenius automorphism σ to $K[x, w_0, \ldots, w_{n-1}]$ via $\sigma(x) = x$, $\sigma(w_i) = w_{i+1}$ for $0 \leq i < n-1$ and $\sigma(w_{n-1}) = w_0$. We obtain $\sigma(y_i) = y_i$ for all $0 \leq i \leq n-1$.

Proof. It is convenient to prove the Frobenius automorphism statement first. That σ can be extended as stated is obvious. Next set $T = \left(\sigma^j(\psi_i)\right)_{0 \leq i,j \leq n-1} \in K^{n \times n}$ and notice that T is invertible since $TT^t = \left(\mathrm{Tr}_{K/k}(\psi_i \psi_j)\right)$ is invertible because finite field extensions are separable. The linear change of variables of the Lemma is then $(w_0, \ldots, w_{n-1}) = (y_0, \ldots, y_{n-1})\, T$.

Let t_i denote the i-th column of T, for $0 \leq i \leq n-1$. The y_i are expressed as K-linear combinations of the w_i via $(y_0, \ldots, y_{n-1}) = (w_0, \ldots, w_{n-1})\, T^{-1}$. We apply σ to $(w_0, \ldots, w_{n-1}) = (y_0, \ldots, y_{n-1})\, T$ and obtain

$$\begin{aligned} (w_1, \ldots, w_{n-1}, w_0) &= (\sigma(y_0), \ldots, \sigma(y_{n-1}))\left(t_1, \ldots, t_{n-1}, t_0\right) \\ &= (y_0, \ldots, y_{n-1})\left(t_1, \ldots, t_{n-1}, t_0\right). \end{aligned}$$

The second equation holds because of the relation of the y_i and w_i. As the matrix $\left(t_1, \ldots, t_{n-1}, t_0\right)$ is invertible we conclude $\sigma(y_i) = y_i$.

We are left to prove the birational equivalence of $\mathfrak{C}$ and $\mathfrak{D}$. Let $\psi_0, \ldots, \psi_{n-1}$ be a basis of K over k with $\sum \psi_i = 1$. The equations of $\mathfrak{C}$ are obtained by expanding

$$Y = \sum y_i \psi_i, \quad \alpha = \sum a_i \psi_i \quad \beta = \sum b_i \psi_i \text{ and } X = x$$

in E, and equating the resulting coefficients of the ψ_i. We obtain $f_i \in k[x, y_0, \ldots, y_{n-1}]$ such that

$$w_0^2 + xw_0 + x^3 + \alpha_0 x^2 + \beta_0 = \sum_{i=0}^{n-1} f_i(x, y_0, \ldots, y_{n-1})\psi_i,.$$

The corresponding equations for $\mathfrak{C}$ are

$$\mathfrak{C} : \begin{cases} f_0(x, y_0, \ldots, y_{n-1}) = 0, \\ \qquad \vdots \\ f_{n-1}(x, y_0, \ldots, y_{n-1}) = 0. \end{cases}$$

We denote the left hand sides of $\mathfrak{D}$ by $g_i \in K[x, w_0, \ldots, w_{n-1}]$. Upon applying T columnwise to the equations of $\mathfrak{C}$ we then see

$$\begin{aligned}
\big(f_i(x, y_0, \ldots, y_{n-1})\big)_{0\le i\le n-1}\, T &= \Big(\sum\nolimits_i f_i(x, y_0, \ldots, y_{n-1})\, \sigma^j(\psi_i)\Big)_{0\le j\le n-1} \\
&= \Big(\sigma^j\Big(\sum\nolimits_i f_i(x, y_0, \ldots, y_{n-1})\, \psi_i\Big)\Big)_{0\le j\le n-1} \\
&= \big(\sigma^j\big(w_0^2 + xw_0 + x^3 + \alpha_0 x^2 + \beta_0\big)\big)_{0\le j\le n-1} \\
&= \big(g_i(x, w_0, \ldots, w_{n-1})\big)_{0\le i\le n-1},
\end{aligned}$$

which shows that $\mathfrak{C}$ is linearly transformed into $\mathfrak{D}$ by T. □

Let F_i be the splitting field of the i-th equation defining $\mathfrak{D}$ over $K(x)$.

Lemma 3. *We can form the compositum $F = F_0 \cdots F_{n-1}$ over $K(x)$ without ambiguity. Let $m \in \mathbb{Z}$ such that $[F : K(x)] = 2^m$. Viewed over K the curve $\mathfrak{D}$ has 2^{n-m} irreducible reduced components, each having function field K-isomorphic to F.*

Proof. We can form F without ambiguity because the extensions $F_i/K(x)$ are all quadratic, hence Galois over $K(x)$. More specificially, in order to generate F over $K(x)$ we can choose a suitable subset of m equations of the equations defining the curve $\mathfrak{D}$, such that adjoining $\bar{w}_{l_i}$, for $1 \le i \le m$, to $K(x)$ gives F, with $\bar{w}_{l_i}$ a root of the left hand side of the i-th such equation. The remaining $n - m$ equations of $\mathfrak{D}$ will each have two solutions $\bar{w}_{v_j}$ and $\bar{w}_{v_j} + x$ in F.

Consider the homomorphism

$$\phi : K[x, w_0, \ldots, w_{n-1}] \to K[x, \bar{w}_0, \ldots, \bar{w}_{n-1}] \subseteq F.$$

The kernel I of this homomorphism is a prime ideal of dimension one since F is a field of transcendence degree one over K being generated by $x, \bar{w}_0, \ldots, \bar{w}_{n-1}$ over K. This prime ideal contains the left hand sides of $\mathfrak{D}$ by construction of F. Therefore, I defines an irreducible reduced component of $\mathfrak{D}$ having function field K-isomorphic to F.

The statement about the number of these components follows from the possible choices of $\bar{w}_{v_j}$ or $\bar{w}_{v_j} + x$ in the definition of the homomorphism. This can be seen in detail as follows: Assume I were contained in the kernel J of a homomorphism ψ as above which maps w_{v_j} to $\bar{w}_{v_j} + x$. There are $f, g \in K[x, w_0, \ldots, w_{m-1}]$ such that $\phi(g), \psi(g) \neq 0$ and $\bar{w}_{v_j} = \phi(f)/\phi(g) = \psi(f)/\psi(g)$. Then $gw_{v_j} + f \in I \subseteq J$ and $g(w_{v_j} + x) + f \in J$ hence $gx \in J$ and $x \in J$ because $\psi(g) \neq 0$ and J is prime. This is clearly a contradiction as x is not mapped to zero by ψ. □

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

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

The advantage of this model is that we can apply Artin-Schreier theory as outlined in [2, pp. 22–24], [14, pp. 275–281] and [18, p. 115]. We will use the following special version of [14, p. 279, Thm 3.3]:

Theorem 4. *Let p be a prime number, $\wp(x) = x^p - x$ be the Artin-Schreier operator, K be a field of characteristic p and $\bar{K}$ be a fixed separable closure of K. For every additive subgroup $\Delta \leq K^+$ with $\wp(K) \subseteq \Delta \subseteq K$ there is a field $L = K\big(\wp^{-1}(\Delta)\big)$ with $K \subseteq L \subseteq \bar{K}$ obtained by adjoining all roots of all polynomials $x^p - x - d$ for $d \in \Delta$ in $\bar{K}$ to K. Given this, the map*

$$\Delta \mapsto L = K\big(\wp^{-1}(\Delta)\big)$$

defines a 1-1 correspondence between such additive subgroups Δ and Abelian extensions L/K in $\bar{K}$ of exponent p.

Before giving the result we state the following Lemma which will be used repeatedly in the sequel.

Lemma 5. *Any sum of an even number of the α_j is of the form $v^2 + v$ with a suitable $v \in \mathbb{F}_2(\alpha)$.*

Proof. For $f(t) = \sum_i d_i t^i \in \mathbb{F}_2[t]$ we define $f(t)\varepsilon = \sum_i d_i \varepsilon^{2^i}$ for all $\varepsilon \in K$, thereby turning the additive group K^+ of K into an $\mathbb{F}_2[t]$-module. The required statement is then reformulated as follows: For $f(t) \in \mathbb{F}_2[t]$ with $f(1) = 0$ there is a suitable $v \in \mathbb{F}_2(\alpha)$ such that $f(t)\alpha = (t+1)v$. But this is now easily seen to be true. Namely, $f(t)$ is divisible by $t+1$ and v can thus be chosen to be $f(t)/(t+1)\alpha$. □

Lemma 6. *For m as in Lemma 3 we have the equality*

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

The field K is the exact constant field of F (i.e. K is algebraically closed in F) and F is the compositum of the first m fields F_i over $K(z)$, i.e. $F = F_0 \cdots F_{m-1}$.

The Galois group of $F/K(z)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$. The action of $\tau \in \mathrm{Gal}(F/K(z))$ is given by $\tau(\bar{s}_i) = \bar{s}_i$ or $\tau(\bar{s}_i) = \bar{s}_i + 1$, where $\bar{s}_i$ is a root of the left hand side of the i-th equation of $\mathfrak{F}$ in F, for $0 \leq i \leq n-1$.

Proof. Consider the operator $\wp(x) = x^2 + x$ and the additive group (or $\mathbb{F}_2$-module)

$$\Delta_0 = \mathrm{Span}_{\mathbb{F}_2}\big\{z^{-1} + \alpha_0 + \beta_0^{1/2} z, \ldots, z^{-1} + \alpha_{n-1} + \beta_{n-1}^{1/2} z\big\}.$$

We further define $\Delta = \Delta_0 + \wp\big(K(z)\big)$. With this we have $F = K(z)\big(\wp^{-1}(\Delta)\big) = K(z)\big(\wp^{-1}(\Delta_0)\big)$ and

$$m = \dim_{\mathbb{F}_2}\big(\Delta/\wp\big(K(z)\big)\big) = \dim_{\mathbb{F}_2}\big(\Delta_0/\,\Delta_0 \cap \wp\big(K(z)\big)\big),$$

where the first equality holds according to Theorem 4 and the second equality holds according to the first isomorphism theorem for groups.

We have $\Delta_0 \cap \wp\big(K(z)\big) = \Delta_0 \cap \wp(K)$ because applying $\wp$ to non-constant functions in $K(z)$ would necessarily involve quadratic terms in z which are not to be found in Δ_0. Let us abbreviate $U = \mathrm{Span}_{\mathbb{F}_2}\big\{\big(1, \beta_0^{1/2}\big), \ldots, \big(1, \beta_{n-1}^{1/2}\big)\big\}$. Expanding the elements in Δ_0 into vectors in K^2 by taking the coefficients of z^{-1} and z gives a surjective linear map $\Delta_0 \to U$. Its kernel is $\Delta_0 \cap K$. But every element of the kernel must be a sum of an even number of the α_j because otherwise the z^{-1} would not cancel. From Lemma 5 we conclude that $\Delta_0 \cap K = \Delta_0 \cap \wp(K)$, and using $\Delta_0 \cap \wp(K) = \Delta_0 \cap \wp\big(K(z)\big)$, we obtain $\Delta_0/\Delta_0 \cap \wp\big(K(z)\big) \cong U$. The formula for m is thereby verified.

In order to prove that K is the exact constant field of F we have to show that $\Delta \cap K \subseteq \wp(K)$ (remember $F = K(z)\big(\wp^{-1}(\Delta)\big)$). But again every $u \in \Delta \cap K$ is

congruent to a sum of an even number of the α_j modulo $\wp(K)$. Lemma 5 gives $u \in \wp(K)$ and K is hence algebraically closed in F.

The statement about the compositum is seen as follows: The first m terms in the definition of Δ_0 constitute a basis of the $\mathbb{F}_2$-vector space Δ_0. This is due to the property that, if the i-th term is dependend of the previous j-th terms for $0 \leq j \leq i-1$, then the $i+1, i+2, \ldots$ terms would be as well because they arise by applying σ to the i-th term. Hence F is obtained by adjoining roots of the first m left hand sides of $\mathfrak{F}$ to $K(z)$ from which the statement follows.

From Theorem 4 and $[F : K(z)] = 2^m$ we obtain $\mathrm{Gal}(F/K(z)) \cong (\mathbb{Z}/2\mathbb{Z})^m$. The action of $\tau \in \mathrm{Gal}(F/K(z))$ is as stated because τ fixes all $z^{-1} + \alpha_i + \beta_i^{1/2} z$ by definition and hence has to map roots of $s_i^2 + s_i + z^{-1} + \alpha_i + \beta_i^{1/2} z$ to themselves. □

3.3. **Hyperellipticity and genus.** Adding the 0-th equation to the i-th equation of $\mathfrak{F}$ for $i = 1, \ldots, m-1$ 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

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

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

Lemma 7. *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 $2\,[L : K(z)] = [F : L][L : K(z)] = [F : K(z)] = 2^m$.

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

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

where $t_0 = z$.

We take the first equation of (2) ($i = 1$) to be the first equation of (3). Now suppose after already having performed some transformations (with t_i, γ_i and δ_i substituted properly), for some $j \in [2, \ldots, m-1]$, we are given equations

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

defining the extension $L/K(z)$ as well. All left hand sides of these equations must be irreducible due to the choice of m and hence we must have $\delta_i \neq 0$ since K is algebraically closed in F, by Lemma 6. Because of this, being true also for the next intermediate δ_i, we can carry out the following transformations:

By substituting $t_j + (\delta_j/\delta_1)^{1/2} t_1$ for t_j and using the above equation 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. Next, we use the equation for $i = 2$ to eliminate t_1 in the same way as was done with $z = t_0$,

and we repeat this for $t_2, t_3, ..., t_{j-2}$; 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 $\lambda_0, \lambda_{m-1} \neq 0$. □

To estimate the genus of our function field we shall use the following theorem, which is a special case of [18, Proposition III.7.8, pp. 115]:

Theorem 8. *Let L/K denote a rational algebraic function field of characteristic two. Suppose that $u \in L$ is an element which satisfies the following condition:*

$$u \neq w^2 + w \text{ for all } w \in L.$$

Let $F = L(y)$ with $y^2 + y = u$. For a place P of L we define the integer m_P by

$$m_P = \begin{cases} m & \text{if there is an element } z \in L \text{ such that} \\ & v_P(u + (z^2 + z)) = -m < 0 \text{ and } m \not\equiv 0 \pmod{p} \\ -1 & \text{if } v_P(u + (z^2 + z)) \geq 0 \text{ for some } z \in L. \end{cases}$$

If at least one place Q of L satisfies $m_Q > 0$ then K is algebraically closed in F, and

$$g = \frac{1}{2}\left(-2 + \sum_P (m_P + 1) \deg P\right),$$

where g is the genus of F.

Lemma 9. *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. The constant field statement is proved in Lemma 6. Recall, we have $F = F_0 L$ and $[F : L] = 2$. Hence, the hyperellipticity is clear, since L is rational by Lemma 7.

Next we prove the genus statement. In order to obtain F from L we need to adjoin to L a root of the left hand side of the 0-th equation defining $\mathfrak{F}$. We take a closer look at the constant term (in s_0) of this equation $u = 1/z + \alpha_0 + \beta_0^{1/2} z \in L$, where we think of z as a polynomial in c of degree 2^{m-1} as in Lemma 7.

Since this polynomial is separable, it factors in $K[c]$ into irreducible polynomials with all multiplicities equal to one. The valuations $v_P(u)$ of u at the places P above $z = 0$ of the rational function field L (i.e. those places satisfying $v_P(z) > 0$) are thus all -1 and we obtain $m_P = 1$. We additionally know $\sum_{v_P(z)=0} \deg P = 2^{m-1}$, this is easily seen as we are working in a rational function field.

We now consider the degree valuation ∞ of $L = K(c)$. Since $z = \lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i c^{2^i}$ there are $\tilde{u}, v \in K[c]$ such that $\beta_0^{1/2} z = \tilde{u} + v^2 + v$ and $\deg(\tilde{u}) \leq 1$. The polynomial v can be obtained e. g. by successively eliminating leading terms using elements of the form $(\lambda c)^{2^i} + (\lambda c)^{2^{i-1}}$. Thus $v_\infty(u + v^2 + v) \geq -1$ and $m_\infty = 1$ or $m_\infty = -1$.

The remaining places P of L have $v_P(u) = 0$ hence $m_P = -1$. Summing up, using Theorem 8, we finally obtain $g = 2^{m-1}$ or $g = 2^{m-1} - 1$. □

3.4. **Restriction to smaller constant field.** 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 $\mathfrak{D}$.

Lemma 10. *The Frobenius automorphism σ of K over k extends (non uniquely) to a k-automorphism on F of order n or $2n$, again denoted by σ.*

We have roots $\bar{s}_i = \sigma^i(\bar{s}_0)$ of the left hand sides of $\mathfrak{F}$ and accordingly roots $\bar{w}_i = \sigma^i(\bar{w}_0)$ of the left hand sides of $\mathfrak{D}$ with $\bar{w}_i = x\bar{s}_i + \beta_i^{1/2}$ for all $0 \leq i \leq n-1$.

Proof. The Frobenius automorphism σ extends to a k-automorphism of $K(x) = K(z)$ by leaving x, resp. z, fixed.

The field F is obtained from $K(z)$ by successively adjoining roots $\bar{s}_i$ for $0 \leq i \leq m-1$ of the left hand sides of $\mathfrak{F}$ to $K(z)$. Once these m roots $\bar{s}_i$ are adjoined roots $\bar{s}_i$ of the other equations for $m \leq i \leq n-1$ are readily to be found in F and σ will be defined on them. For $m = 1$ we can simply define $\sigma(\bar{s}_0) = \bar{s}_0$. Assume we have $m > 1$ and $\sigma : K(z)(\bar{s}_0, \ldots, \bar{s}_{i-1}) \to F$ for an i with $0 \leq i < m-1$. We can extend σ to $K(z)(\bar{s}_0, \ldots, \bar{s}_i) \to F$ by choosing $\sigma(\bar{s}_i) = \bar{s}_{i+1}$ because the left hand side of the i-th equation of $\mathfrak{F}$ is irreducible over $K(z)(\bar{s}_0, \ldots, \bar{s}_{i-1})$ and applying σ to $z^{-1} + \alpha_i + \beta_i z$ gives $z^{-1} + \alpha_{i+1} + \beta_{i+1} z$. Hence we can extend σ to the whole of F by defining σ on $\bar{s}_i$ for $0 \leq i \leq m-1$.

The order of any such σ on F must be a multiple of n since $K \subseteq F$ and σ has order n on K. Furthermore, $\sigma^n(\bar{s}_0) = \bar{s}_0$ or $\sigma^n(\bar{s}_0) = \bar{s}_0 + 1$ because $\sigma^n(\bar{s}_0)$ must be a root of the left hand side of the first equation of $\mathfrak{F}$. We conclude that the order of σ on F will be n or $2n$ accordingly.

The statement on the roots is clear and serves primarily as a definition for later use. □

It is at this point that condition (†) becomes important.

Lemma 11. *If condition (†) is satisfied then the extension σ in Lemma 10 of the Frobenius to F can be chosen with order exactly n on F.*

Proof. We now need to derive a precise condition for the order of such extensions σ. It will turn out that we have to carefully choose a particular extension σ if we want to obtain order n. The precise condition will be obtained from the precise value of $\sigma^n(\bar{s}_0)$, and is then compared to condition (†).

To begin with we start with any extension σ of the Frobenius to F which will be changed later as required. It is convenient to employ the following technique: For $f(t_\sigma) = \sum_i d_i t_\sigma^i \in \mathbb{F}_2[t_\sigma]$ we define $f(t_\sigma)s = \sum_i d_i \sigma^i(s)$ where $s \in F$ arbitrarily, thereby turning F^+ into an $\mathbb{F}_2[t_\sigma]$-module. As a subgroup K^+ inherits this $\mathbb{F}_2[t_\sigma]$-module structure which is compatible with the $\mathbb{F}_2[t]$-module structure of K^+ used in the proof of Lemma 5 under the relation $t_\sigma = t^r$ for $r = \log_2(q)$.

We let $f_{\beta_0}(t_\sigma)$ be the polynomial of smallest degree such that $f_{\beta_0}(t_\sigma)\beta_0 = 0$ and set

$$f(t_\sigma) = \begin{cases} f_{\beta_0}(t_\sigma) & \text{for } \deg f_{\beta_0}(t_\sigma) \text{ even,} \\ (t_\sigma + 1) f_{\beta_0}(t_\sigma) & \text{otherwise.} \end{cases}$$

The same polynomials f_{β_0} and f are obtained upon replacing β_0 with $\beta_0^{1/2}$. From Lemma 6 and its proof it is easily seen that $\deg f(t_\sigma) = m$.

Since $(t_\sigma^n+1)\beta_0 = 0$ there is an $h(t_\sigma) \in \mathbb{F}_2[t_\sigma]$ such that $h(t_\sigma)f(t_\sigma) = t_\sigma^n + 1$. We have

$$\begin{aligned}\big(f(t_\sigma)\bar{s}_0\big)^2 + f(t_\sigma)\bar{s}_0 &= f(t_\sigma)\big(\bar{s}_0^2 + \bar{s}_0\big)\\ &= f(t_\sigma)\big(z^{-1} + \alpha_0 + \beta_0^{1/2} z\big)\\ &= f(t_\sigma)\alpha_0.\end{aligned}$$

Now, as $f(1) = 0$, we can apply Lemma 5 to the last right hand side above and find a $v \in K$ with $v^2 + v = f(t_\sigma)\alpha_0$. Here we actually have a choice between v and $v+1$ which will be important later. Adding $v^2 + v$ to the first left hand side above we obtain $f(t_\sigma)\bar{s}_0 + v \in \{0, 1\}$. It is now that we have to choose the correct extension of σ, depending on the choice of v: If we have $f(t_\sigma)\bar{s}_0 + v = 1$ we replace σ by a σ' which satisfies $\sigma'(\bar{s}_i) = \sigma(\bar{s}_i)$ for $0 \le i < m-1$ and $\sigma'(\bar{s}_{m-1}) = \sigma(\bar{s}_{m-1}) + 1$, which we can do according to the extension process at the beginning of the proof. Since the leading term of $f(t_\sigma)$ is t_σ^m and $\bar{s}_{m-1} = \sigma^{m-1}(\bar{s}_0)$ we can hence assume

$$f(t_\sigma)\bar{s}_0 + v = 0. \tag{4}$$

Multiplying this with $h(t_\sigma)$ yields $(t_\sigma^n+1)\bar{s}_0 + h(t_\sigma)v = 0$ from which we draw the conclusion: σ has order n on F if and only if $h(t_\sigma)v = 0$. The rest of the proof deals with the relation of this condition and (†), and the suitable choice of v.

Using the proof of Lemma 5 and the above compatibility remark we see that we can choose between $v = f(t^r)/(t+1)\alpha_0$ and $v = f(t^r)/(t+1)\alpha_0 + 1$. Multiplying the first v with $h(t^r)$ we obtain $h(t^r)f(t^r)/(t+1)\alpha_0 = (t^{rn}+1)/(t+1)\alpha_0 = \mathrm{Tr}_{K/\mathbb{F}_2}(\alpha_0)$. Thus, depending on the choice of v,

$$h(t_\sigma)v = \begin{cases} \mathrm{Tr}_{K/\mathbb{F}_2}(\alpha_0) & \text{or}\\ \mathrm{Tr}_{K/\mathbb{F}_2}(\alpha_0) + h(1). \end{cases} \tag{5}$$

Our k-automorphism σ on F, depending on v, has order n if and only if we obtain zero for at least for one of the cases in the right hand side of (5). But this is implied by (†): The case $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha_0) = 0$ is clear. For n odd we obtain $h(1) = 1$ because $t_\sigma + 1$ divides $t_\sigma^n + 1$ only once. For $n = m$ we obtain $h(t_\sigma) = 1$ hence $h(1) = 1$ too. □

We remark that the conditions (†) are sufficient but not necessary for the existence of an extension of the Frobenius automorphism of K/k to F of order n. Precise conditions can be derived from (5) and may be summarized as follows: " The extension exists either for all $\alpha \in K$ or only for those $\alpha \in K$ with $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$, given any fixed $\beta \in K^\times$ ".

Theorem 12. *Let σ be an extension of the Frobenius automorphism of K/k to F, having order n, and let F' be the field of elements of F fixed by σ. The field F' is a 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.*

Such a k-automorphism σ exists if the condition (†) is satisfied.

Proof. We let $L' = F' \cap L$. The relations between the fields F, F', L and L' are described by Figure 1.

The fixed field F' of σ has index n in F because σ is of order n on F and it is clear that $F' \cap K = k$ holds because σ is of order n on K as well.

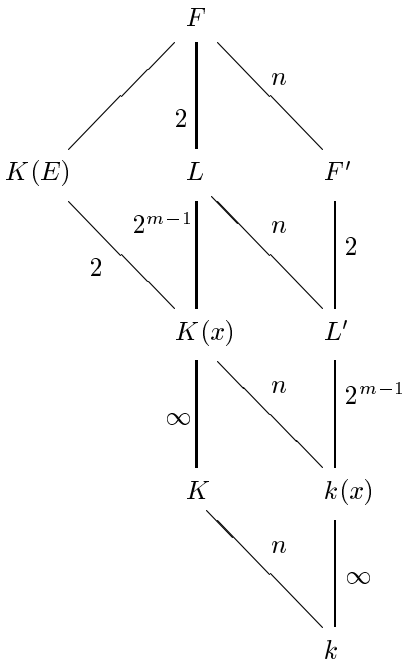

FIGURE 1. Lattice Diagram of Fields

The automorphism σ restricts to a k-automorphism of L of order n because it is the unique subfield of F of index 2 and $K \subseteq L$. Thus, $[L : L'] = n$, since L' is the fixed field of σ restricted to L and we obtain $[F' : L'] = 2$, as desired. Clearly $F = F'K$ (and also $L = L'K$) which gives the genus statement.

From the $\bar{w}_i$ we obtain n, not necessarily distinct, elements $\bar{y}_i$ via the linear transformation of Lemma 2. The automorphism σ operates cyclically on the $\bar{w}_i$ so that we have $\sigma(\bar{y}_i) = \bar{y}_i$, as was proved generically in Lemma 2. The $\bar{y}_i$ are thus in F' and together with x they generate F' over k (because the $\bar{w}_i$ can be obtained from the $\bar{y}_i$ over K). Due to Lemma 2 the $\bar{y}_i$ satisfy the equations of $\mathfrak{C}$, from which we finally see that $\mathfrak{C}$ has an irreducible reduced component with function field F' (we can for example again use the kernel technique from the proof of Lemma 3).

The existence of σ under condition (†) was proved in Lemma 11. □

Note, that if condition (†) is not satisfied and σ has order $2n$, then we could have $F' = L'$ in the arguments of the proof of Theorem 12, and hence we could not guarantee finding a curve defined over k which is hyperelliptic and has genus 2^{m-1} or $2^{m-1} - 1$.

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, by the definition of m. 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. This is why we have assumed throughout that E is not defined over a proper subfield of K.

In view of Theorem 12 and Lemma 11 we assume for the rest of Section 3 that we are given an extension σ of the Frobenius automorphismus of K/k on F of order n and that σ operates cyclically on the $\bar{s}_i$ and $\bar{w}_i$ while leaving x and z fixed. This can be reached when the condition (†) is fulfilled.

3.5. **Determination of an explicit model for F and F'.** We describe how to obtain Artin-Schreier equations defining F over L and F' over L'. The corresponding hyperelliptic equations are easily obtained by similar (reversed) transformations as done in the beginning of 3.2.

To compute an Artin-Schreier equation in s_0 and c for F over L for the generators $\bar{s}_0 \in K(E) \subseteq F$ and $c \in L$, we only need to substitute $\left(\lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i c^{2^i}\right)^{-1}$ for z in the first equation $s_0^2 + s_0 + z^{-1} + \alpha_0 + \beta_0^{1/2} z = 0$ of $\mathfrak{F}$, due to Lemma 7.

In order to determine the action of σ on F we need to compute $\sigma^i(c)$ and $\sigma^i(\bar{s}_0)$ for $0 \leq i \leq n-1$ as expressions in c and $\bar{s}_0$. This can be done using the operation of σ as given in (4) and by tracing back the transformations of Lemma 7. Note that c is a K-linear combination of z and the $\sigma^i(\bar{s}_0)$ for $0 \leq i \leq m-1$ and that each of these can in return be expressed in c ($z = f(c)$ resp. $\sigma^i(\bar{s}_0) = f_i(c) + \bar{s}_0$ for suitable $f, f_i \in K[c]$).

Given c and $\bar{s}_0$ and the action of σ on c and $\bar{s}_0$ we can explicitly construct F' and L' as follows:

Lemma 13. *Choose $\mu \in K$ such that $\mathrm{Tr}_{K/k}(\mu) = 1$ and set $\tilde{c} = \mathrm{Tr}_{L/L'}(\mu\lambda_0 c)$, $\tilde{s} = \mathrm{Tr}_{F/F'}(\mu\bar{s}_0)$. We then have $L' = k(\tilde{c})$ and $F' = k(\tilde{s}, \tilde{c})$. An Artin-Schreier equation defining the field F' over L' is given by*

$$\begin{aligned} \tilde{s}^2 + \tilde{s} + 1/z + \mathrm{Tr}_{K/k}(\mu^2\alpha) + \mathrm{Tr}_{K/k}(\mu^2\beta^{1/2})\, z \\ + \left(\mathrm{Tr}_{F/F'}(\mu^2\bar{s}_0) + \mathrm{Tr}_{F/F'}(\mu\bar{s}_0)\right) = 0, \end{aligned} \tag{6}$$

where the absolute coeffcient in $\tilde{s}$ of the left hand side of this equation, the element z and hence the last line $\mathrm{Tr}_{F/F'}(\mu^2\bar{s}_0) + \mathrm{Tr}_{F/F'}(\mu\bar{s}_0)$ are in L'.

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

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

For $i = 0$ we thus obtain

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

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

Consider the Galois group of $F/K(z)$. According to Lemma 6 it is an elementary abelian 2-group whose elements send each $\sigma^i(\bar{s}_0)$ to $\sigma^i(\bar{s}_0)$ or $\sigma^i(\bar{s}_0) + 1$. Now let τ be the hyperelliptic involution on F/L, being an element of this Galois group. Since τ fixes L and any of the $\sigma^i(\bar{s}_0)$ generates F over L we must have $\tau(\sigma^i(\bar{s}_0)) = \sigma^i(\bar{s}_0) + 1 = \sigma^i(\tau(\bar{s}_0))$ for all i. We thus see that σ and τ commute in their action on F and that hence τ operates by restriction on F'/L'. We again consider the equations defining $\mathfrak{F}$. Using $\mathrm{Tr}_{K/k}(\mu) = 1$ we obtain $\tau(\tilde{s}) = \tilde{s} + 1$ and

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

Using

$$\tilde{s}^2 = \mathrm{Tr}_{F/F'}(\mu^2 \bar{s}_0^2) = \mathrm{Tr}_{F/F'}(\mu^2(\bar{s}_0 + 1/z + \alpha + \beta^{1/2} z))$$

we obtain for the norm

$$\begin{aligned} \mathrm{N}_{F'/L'}(\tilde{s}) &= \tilde{s}(\tilde{s} + 1) \\ &= 1/z + \mathrm{Tr}_{K/k}(\mu^2\alpha) + \mathrm{Tr}_{K/k}(\mu^2\beta^{1/2})\, z \\ &\qquad + \big(\mathrm{Tr}_{F/F'}(\mu^2 \bar{s}_0) + \mathrm{Tr}_{F/F'}(\mu \bar{s}_0)\big). \end{aligned}$$

Putting together we thus arrive at equation (6). 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 $\bar{s}_i$ at the zeros of z is only half the valuation of $1/z$. The term in the second line of (6) is a K-linear combination of the $\bar{s}_i$ and, as element of L', has therefore no poles except at $\tilde{c} = \infty$. It is hence a polynomial in $\tilde{c}$ and we can conclude that the left hand side of (6) is indeed irreducible. □

The elements $\tilde{s}$ and $\tilde{c}$ can be computed in F using σ. The absolute coefficient in equation (6) is first computed in $K(c)$ and lies in $k(\tilde{c})$ after substituting $c = (\tilde{c} + \lambda'')/\lambda_0$.

We let $\bar{y} = x\bar{s}_0 + \beta^{1/2}$ and $\tilde{y} = \mathrm{Tr}_{F/F'}(\mu\bar{y})$ so that $\tilde{y} = x\tilde{s} + \mathrm{Tr}_{K/k}(\mu\beta^{1/2})$. In the case of odd n we can choose $\mu = 1$ and obtain the equation

$$\tilde{y}^2 + x\tilde{y} + x^3 + \mathrm{Tr}_{K/k}(\alpha)x^2 + \mathrm{Tr}_{K/k}(\beta) = 0,$$

for x 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 $\mathrm{Tr}_{K/k}(\beta) = 0$.

3.6. **Mapping the discrete logarithm problem.** We next address the question of mapping the discrete logarithm problem from E to F', where we again use the function field setting. We let $Cl^0(K(E))$ denote the group of divisor classes of degree zero of the function field $K(E)$ of E, and similarly for $Cl^0(F)$. The divisor class of the divisor D is written $[D]$.

The conorm $\mathrm{Con}_{F/K(E)}$ and norm $\mathrm{N}_{F/F'}$ maps we define as in [5, pp. 65] (cf. [18, pp. 63 and 239]), on recalling that F is a function field extension of both $K(E)$ and F'. Both conorm and norm are homomorphisms of divisor groups, are well defined on divisor classes and map divisor classes of degree zero to divisor classes of degree zero.

The point group $E(K)$ of the elliptic curve E is isomorphic to the group of divisor classes of degree zero of $K(E)$ [16, p. 66, Prop. 3.4]. The mapping of

the discrete logarithm problem in the point group $E(K)$ of E is then achieved as follows: First we translate the problem into $Cl^0(K(E))$. From there we use the conorm $\mathrm{Con}_{F/K(E)}$ in order to map it to $Cl^0(F)$, and from there, using the norm $\mathrm{N}_{F/F'}$, to $Cl^0(F')$. On composition we thus obtain a group homomorphism

$$\phi : E(K) \to Cl^0(F').$$

The important question now is whether the large cyclic factor of $E(K)$ of order p is preserved by this homomorphism.

Lemma 14. *The kernel of* $\mathrm{Con}_{F/K(E)} : Cl^0(K(E)) \to Cl^0(F)$ *can only consist of* 2*-power torsion elements of* $Cl^0(K(E))$.

Proof. Let D be a degree zero divisor of $K(E)$. We have according to [5, pp. 66, line 21] that

$$\mathrm{N}_{F/K(E)}(\mathrm{Con}_{F/K(E)}(D)) = [F : K(E)]D.$$

Thus, if $\mathrm{Con}_{F/K(E)}(D)$ 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. □

According to the lemma the large cyclic factor can only be mapped to zero under ϕ by the norm $\mathrm{N}_{F/F'}$.

For very small values of m, such as those obtained for Koblitz curves, the kernel of ϕ will necessarily be divisible by the large prime p. But if m is larger than $\log_2(n)$, then the large prime factor of the order of $E(K)$ 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. Set $D_1 = \phi(P_1)$ and $D_2 = \phi(P_2)$. If 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 feasible by general methods, such as those used for computations with algebraic number fields and their extensions. Nevertheless, we want to give some rough indications on a method for our case. We assume that we can compute sufficiently well with finite fields and that we can define the function field of an irreducible affine plane curve, that we can compute the decomposition into places of the principal divisor of an element and of effective divisors and that we can evaluate elements at places.

Let P_1 be a place of $K(E)$ of degree one where $x, y \in K(E)$ take the values $x(P_1), y(P_1) \in K$ respectively (we assume for simplicity that $x(P_1) \neq 0, \infty$). The place P_1 is clearly the unique common zero of $x + x(P_1) \in K(E)$ and $y + y(P_1) \in K(E)$. Then $\mathrm{Con}_{F/K(E)}(P_1)$ can be computed as the greatest common divisor of the numerators of the principal divisors $\big(x + x(P_1)\big)$ and $\big(y + y(P_1)\big)$ taken in F. It is a divisor of degree 2^{m-1} according to [5, pp. 65, Lemma 1].

Let P be a place of F dividing $\mathrm{Con}_{F/K(E)}(P_1)$ for some place P_1 of $K(E)$ of degree one (we decompose $\mathrm{Con}_{F/K(E)}(P_1)$ to compute P). The place $L \cap P$ can be described as the numerator of $\big(f(\tilde{c})\big)$, where f is the minimal polynomial of $\tilde{c}(P)$ over K and the principal divisor is taken in L. This is possible as $\tilde{c}$ has

no pole at P because $x(P) = x(P_1) \neq 0$, which we have assumed above ($\tilde{c}$ and $\tilde{y}$ are defined after Lemma 13 and given as elements of F and generators of F'). The place P can similarly be given 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 $K(\tilde{c}(P))$. $\tilde{y}$ is defined at P because all of the $\sigma^i(\bar{y})$ are as $x(P) \neq \infty$. We may represent P as the the greatest common divisor of the numerators of $\big(f(\tilde{c})\big)$ and $\big(h(\tilde{y}, \tilde{c})\big)$, where the principal divisors are taken in F. This divisor consists of only P without multiplicities because as $x(P_1) \neq 0$ we have that $L \cap P$ is unramified in F, hence there are at most two places in the numerator of $\big(f(\tilde{c})\big)$ and each of them occurs with multiplicity one. Furthermore, if the other place $Q \neq P$ above $L \cap P$ exists then $h(\cdot, \tilde{c})$ has degree one as the residue class degree of P over $L \cap P$ is one. We also obtain $\tilde{y}(Q) = \tilde{y}(P) + x(P) \neq \tilde{y}(P)$ and $h(\tilde{y}(Q), \tilde{c}(Q)) \neq 0$, hence Q does not occur in the numerator of $\big(h(\tilde{y}, \tilde{c})\big)$ (cf. [18, p. 76, Thm. III.3.7.] and its proof, h is one of the φ_i and φ is the minimal polynomial of $\tilde{y}$ over $K(\tilde{c})$). We are actually interested in determining the underlying place $P' = F' \cap P$ of F', so we need to express the situation with coefficients in k rather than K.

For this we simply compute minimal polynomials $\tilde{f}, \tilde{h}$ as above, but over k instead, and compute P' as the greatest common divisor of the numerators of $\big(\tilde{f}(\tilde{c})\big)$ and $\big(\tilde{h}(\tilde{y}, \tilde{c})\big)$, where the principal divisors are now taken in F'. This divisor consists of only P' without multiplicities because of the same reasons as above.

Finally, $\mathrm{N}_{F/F'}(P) = f(P, P')P'$ where $f(P, P') = n \deg(P)/\deg(P')$ is the residue class degree of P over P'. We will have that $\mathrm{N}_{F/F'}(\mathrm{Con}_{F/K(E)}(P_1))$ is effective and that its degree equals $n2^{m-1}$, for the later taking [5, pp. 66, Lemma 2] and its proof into account.

A program for computing F' and ϕ given E has been written in KASH and 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. Choose an E over K of order $2^l p$ where p is a prime and l is a small integer. This can be achieved by generating curves at random and computing their group orders using the algorithm of Schoof [15].
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. Clearly in step 2 we should only choose curves for which condition (†) will automatically hold, i.e. n odd or $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$.

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 we use it for illustrative 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 so we expect to obtain a hyperelliptic curve of genus four. The order of $E(K)$ is computed using the algorithm of Schoof [15] 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 following hyperelliptic curve, which we calculated using the method in Section 3,

$$H : Y^2 + G(X)Y + F(X) = 0 \tag{7}$$

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

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

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

$$\begin{aligned} H : Y^2 &+ (X^2 + w^{2012013793551629036365609}X)Y \\ &= X^5 + X^4 + w^{1586464037343056940725724}X^2 \\ &\quad + w^{43334222987849600951547}X + w^{7747883459877983146322 40} \end{aligned}$$

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 [8] since p does not divide $q^k - 1$ for small values of k.

Notice, that if the original elliptic curve $E(\mathbb{F}_{q^n})$ resists the Tate pairing attack, i.e. there does not exist a small value of k for which $q^{nk} - 1 \equiv 1 \pmod{p}$, then the analogous test for the Jacobian is obviously satisfied 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 obtain 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 [10], but we give some details in an example below.

Theorem 15 (Gaudry [10])**.** *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 the method of [10] 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 obtain $l = \Theta((q/g!)^{1/(g+1)})$ 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 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 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 the method of [10] is practical in genus four. In this section we consider the example given by the curve in equation (7). 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 the method of [10] 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 the method of [10] 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 above divisor D_1 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 $\mathbf{F}$ 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 $[-g, \ldots, g]$, 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 ran 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 ran 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 $\log_2 p$, 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

$$\#E(\mathbb{F}_{2^{127}}) = 2^{20} \cdot 3^2 \cdot 45615671 \cdot 3952327816591640754121 01.$$

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

$$H : y^2 + (x^{128} + x^{64} + x)y + x^{128} + x^{64} + x = 0.$$

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 16. *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 [12] 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 the method of [10] 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, 9, 11, 13] 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 easily 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 [6]. 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 $\mathbb{F}_{q^n}$ and which satisfies condition (†). 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.

However, we do 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] C. Chevalley. *Introduction to the theory of algebraic functions of one variable* Mathematical Surveys Number VI, American Mathematical Society, 1951.

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

[7] G. Frey. How to disguise an elliptic curve. Talk at Waterloo workshop on the ECDLP, 1998. **http://cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html**.

[8] 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.

[9] 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.*
[10] P. Gaudry. An algorithm for solving the discrete logarithm problem on hyperelliptic curves. In *Advanced in cryptology - EUROCRYPT 2000*, Springer-Verlag LNCS 1807, 19–34, 2000.
[11] F. Heß. Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern. Dissertation, TU Berlin, 1999.
[12] R. Lidl and H. Niederreiter. *Finite Fields,* Addison-Wesley, 1983.
[13] V. Müller, A. Stein and C. Thiel. Computing discrete logarithms in real quadratic function fields of large genus. *Math. Comp.*, **68**, 807–822, 1999.
[14] J. Neukirch. *Algebraic Number Theory.* Springer-Verlag, 1999.
[15] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, **44**, 483–494, 1985.
[16] J. H. Silverman. *The Arithmetic of Elliptic Curves* GTM 106, Springer-Verlag, 1986.
[17] N.P. Smart. On the performance of hyperelliptic cryptosystems. *Advances in Cryptology, EUROCRYPT '99*, Springer-Verlag, LNCS 1592, 165–175, 1999.
[18] 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

Computer Science Department, Woodland Road, University of Bristol, BS8 1UB, UK
E-mail address: nigel@cs.bris.ac.uk