

Weil Descent Attack for Artin-Schreier Curves

Nicolas Thériault, University of Toronto

Abstract

In this paper, we show how the method introduced by Gaudry, Hess and Smart can be extended to a family of algebraic curves using Artin-Schreier extensions. This family also extends the number of hyperelliptic curves in characteristic 2 vulnerable to the Weil descent attack obtained by Galbraith. We also show that the genus of the resulting curve will be one of two easily computable values.

1 Introduction

Given a curve C defined over a field K , the Weil descent attack consists in finding a curve \tilde{C} defined over a subfield k of K and a map Φ from $\text{Jac}(C)(K)$ to $\text{Jac}(\tilde{C})(k)$ with a relatively small kernel. If $|\ker(\Phi)|$ is small, then the discrete log problem on $\text{Jac}(C)(K)$ can only be as difficult as the discrete log on $\text{Jac}(\tilde{C})(k)$.

In this paper, we show how the attack first described by Gaudry, Hess and Smart ([11]) for elliptic curves in characteristic 2 (and implemented by Jacobson, Menezes and Stein in [13]), and its extension to hyperelliptic curves in characteristic 2 by Galbraith ([5]), can be extended to a family of Artin-Schreier curves. We also improve the bound on the genus of \tilde{C} obtained by Galbraith.

For a fixed characteristic, if the genus \tilde{g} of \tilde{C} is not too large, the discrete log problem on $\text{Jac}(\tilde{C})(k)$ will then run in $O\left(\tilde{g}^5 q^{2 - \frac{4}{2\tilde{g}+1} + \epsilon}\right)$ bit operations instead of the $O\left(g^5 q^{2n - \frac{4n}{2g+1} + \epsilon}\right)$ bit operations that would be needed to attack the discrete log directly on $\text{Jac}(C)(K)$ (or $O(g^2 q^{gn/2 + \epsilon})$ for genus 1 or 2) (see [10] and [21]). This has the effect of decreasing the security of some curves over the field K that may otherwise appear secure enough for cryptographic applications.

In this paper, we show that given a characteristic p Artin-Schreier curve of genus g defined over a field K by an equation of the form

$$Y^p - h(X)^{p-1}Y = f(X) + (\alpha X + \beta)h(X)^p$$

(and some extra conditions), we can find a curve \tilde{C} defined over the subfield k of K by an equation of the form

$$\tilde{y}^p - \tilde{h}(\tilde{c})^{p-1}\tilde{y} = \tilde{f}(\tilde{c})$$

(see Lemma 14 and Corollary 15 for a more detailed description of the equation of \tilde{C}) of genus

$$\tilde{g} = gp^{m-1} - (p-1) \quad \text{or} \quad gp^{m-1}$$

(Theorem 10), where

$$m = \dim_{\mathbb{F}_p} \left(\text{span}_{\mathbb{F}_p} \left\{ \begin{pmatrix} 1 \\ \sigma^0(\alpha) \end{pmatrix}, \begin{pmatrix} 1 \\ \sigma^1(\alpha) \end{pmatrix}, \dots, \begin{pmatrix} 1 \\ \sigma^{n-1}(\alpha) \end{pmatrix} \right\} \right)$$

(Corollary 7). We also have an easily computable map from the ideal class group of C to the ideal class group of \tilde{C} .

This paper is divided as follows. The curves considered here are described in detail in section 2. Section 3 gives some details on Artin-Schreier extensions. In section 4, we construct the function field F of a curve isomorphic to a subvariety of the Weil restriction of scalars of C over k and we compute its genus in section 5. Sections 6 and 7 deal with obtaining the curve C' defined over k . The algorithm is laid out in section 8. Finally, more details are given about characteristic 2 curves in section 9 and some examples are given in section 11.

2 Setup

Let p be a prime and $q = p^l$. Let $K = \mathbb{F}_{q^n}$ be a field of characteristic p with $n > 1$ and $k = \mathbb{F}_q$ be its subfield of order q . Let C be a curve of genus g defined over K by

$$Y^p - h(X)^{p-1}Y = f(X) + (\alpha X + \beta)h(X)^p$$

where $f(X), h(X) \in K[X]$ are defined over k and $f(X)$ is such that

$$\gcd(\deg(f), p) = 1 \quad \text{and} \quad C \text{ is nonsingular.} \quad (1)$$

We will also assume that $\beta \in K$, $\alpha \in K \setminus k$ and one of the following conditions holds:

$$\begin{cases} \text{Tr}_{K/\mathbb{F}_p}(\beta) = 0 \\ \gcd\left(\frac{\sigma^n - 1}{\min_{\alpha}(\sigma)}, \sigma - 1\right) = 1 \end{cases} \quad (2)$$

where $\min_{\alpha}(\sigma)$ is the polynomial in σ (the Frobenius of K over k) in $\mathbb{F}_p[\sigma]$ of minimal degree such that $\sigma - 1$ divides $\min_{\alpha}(\sigma)$ and $\min_{\alpha}(\sigma)$ applied to α gives 0. Although the second part of condition 2 may seem strange, it will hold in most cases. In particular, it holds for every $\alpha \in K \setminus k$ when n is coprime with p . The conditions in 2 enable us to make a key Galois-theoretic construction, namely the extension of the Frobenius to certain function fields.

Remarks:

1. The Weil descent attack was originally studied by Gaudry, Hess and Smart [11] in the case of elliptic curves in characteristic 2.
2. The case $\deg(h) \leq 1$ in characteristic 2 has been studied in the hyperelliptic curves case by Galbraith [5]. In that paper, Galbraith gives a weaker result than the one presented here, with only an upper bound for the genus of the algebraic restriction.
3. This method also works if the curve C is singular. However, curves considered for cryptography are assumed to be nonsingular to avoid weaknesses inherent to the Jacobian of singular curves.

4. We note that the curve C is isomorphic to a curve C' given by

$$Z^p - h(X)^{p-1}Z = f_1(X)h_1(X) + (\alpha X + \beta)h(X)^p$$

where $h_1(X)$ is the largest squarefree factor of $h(X)$ and $\gcd(f_1(X), h(X)) = 1$.

3 Artin-Schreier Extensions

We will use σ to denote the Frobenius automorphism of K/k . That is,

$$\sigma(\omega) = \omega^q = \omega^{p^l}$$

for every $\omega \in K$. We also set

$$\mathcal{P}(z) = z^p - z$$

for the Artin-Schreier operator. Also, for any $f(t) \in \mathbb{F}_p[t]$ ($f(t) = \sum_i d_i t^i$), where t is an operator on K , the operator

$$* : \mathbb{F}_p[t] \times K \rightarrow K$$

will act as

$$f(t) * \omega = \sum_i d_i t^i(\omega).$$

Lemma 1: *Let $\omega \in K$. Given any linear combination of the form*

$$\sum_{i=0}^{n-1} c_i \sigma^i(\omega) = \gamma \quad \text{over } \mathbb{F}_p \text{ with } \sum_{i=0}^{n-1} c_i = 0,$$

there exists $\nu \in \mathbb{F}_p(\omega) \subset K$ such that $\mathcal{P}(\nu) = \nu^p - \nu = \gamma$.

Proof: This is a generalization to characteristic p of the proof of lemma 5 in [11]. The following is an outline of the argument:

Let $f(t) \in \mathbb{F}_p[t]$ be defined as

$$f(t) = \sum_{i=0}^{n-1} c_i t^i.$$

then $\gamma = f(\sigma) * \omega$ and $f(\sigma) * 1 = 0$. If we set ρ to act on K as $\rho(\omega) = \omega^p$, then $f(\sigma) = f(\rho^l)$ and $f(\rho^l) * 1 = f(\sigma) * 1 = 0$, so $\rho - 1$ divides $f(\rho^l)$ (since 1 is fixed under ρ) and we can define $\nu \in \mathbb{F}_p(\omega)$ as

$$\nu = \left(\frac{f(\rho^l)}{\rho - 1} \right) * \omega.$$

Then

$$\begin{aligned} \nu^p - \nu &= (\rho - 1) * \nu \\ &= (\rho - 1) * \left(\left(\frac{f(\rho^l)}{\rho - 1} \right) * \omega \right) \\ &= f(\rho^l) * \omega \\ &= f(\sigma) * \omega \\ &= \gamma \end{aligned}$$

which gives the desired result. Q.E.D.

Proposition 2: *For every additive subgroup $\Delta \subseteq \mathbb{K}$ with $\mathcal{P}(\mathbb{K}) \subseteq \Delta \subseteq \mathbb{K}$, there is a field $\mathbb{L} = \mathbb{K}(\mathcal{P}^{-1}(\Delta))$ obtained by adjoining all roots of all polynomials $z^p - z - d$ for $d \in \Delta$. The map $\Delta \mapsto \mathbb{L} = \mathbb{K}(\mathcal{P}^{-1}(\Delta))$ defines a one-to-one correspondance between additive groups Δ and abelian extensions \mathbb{L}/\mathbb{K} of exponent p .*

Proof: This is Kummer theory, see [17] theorem 3.3, page 279 for more details.

3.1 Genus

Proposition 3: *Let \mathbb{L}/\mathbb{K} be a rational algebraic function field of characteristic $p > 0$. Suppose that $w \in \mathbb{L}$ is an element such that $w \notin \mathcal{P}(\mathbb{L})$ (i.e. $\mathcal{P}(z) \neq w$ for every $z \in \mathbb{L}$). Let $\mathbb{F} = \mathbb{L}(\theta)$ with $\theta^p - \theta = w$. For a place $P \in \mathbb{P}_{\mathbb{L}}$ we define the integer r_P by*

$$r_P = \begin{cases} r & \text{if there is an element } z \in \mathbb{L} \text{ such that } v_P(w - (z^p - z)) = -r < 0 \\ -1 & \text{if } v_P(w - (z^p - z)) \geq 0 \text{ for all } z \in \mathbb{L} \end{cases} .$$

If at least one place $Q \in \mathbb{P}_{\mathbb{L}}$ satisfies $r_Q > 0$, then \mathbb{K} is algebraically closed in \mathbb{F} and

$$g = \frac{p-1}{2} \left(-2 + \sum_{P \in \mathbb{P}_{\mathbb{L}}} (r_P + 1) \deg P \right)$$

where g is the genus of \mathbb{F}/\mathbb{K} .

Proof: This is the Hurwitz genus formula applied to curves in Artin-Schreier form. See [20] proposition III.7.8, page 115 for more details.

Note that the curve C is isomorphic to the curve

$$C_0 : Z^p - Z = \alpha X + \beta + \frac{f(X)}{h(X)^p}$$

(setting $Z = Yh(X)$ and dividing the resulting equation by $h(X)^p$). Since C_0 is in Artin-Schreier form, we can apply Proposition 3. The first part of (1) insures that

$$v_{\infty} \left(\alpha X + \beta + \frac{f(X)}{h(X)^p} - (z^p - z) \right) = -\max\{\deg(f) - p \deg(h), 1\}$$

for every $z \in K(X)$. The second part of (1) insures that for any place P over $h(X)$,

$$v_P \left(\alpha X + \beta + \frac{f(X)}{h(X)^p} - (z^p - z) \right) < 0.$$

4 Varieties

Let $\{\Psi_0, \dots, \Psi_{n-1}\}$ be a basis of K over k with $\sum_{i=0}^{n-1} \Psi_i = 1$. Let

$$X = \sum_{i=0}^{n-1} x_i \Psi_i \quad , \quad Y = \sum_{i=0}^{n-1} y_i \Psi_i \quad , \quad \alpha = \sum_{i=0}^{n-1} a_i \Psi_i \quad \text{and} \quad \beta = \sum_{i=0}^{n-1} b_i \Psi_i$$

where $a_i, b_i \in k$ and x_i, y_i are variables over k . Substituting X, Y, α and β in the equation of C , we get

$$\sum_{i=0}^{n-1} G_i(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1}) \Psi_i = 0$$

where the G_i 's are polynomials in $k[x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1}]$. We also extend σ to the ring $k[x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1}]$ such that it applies trivially. We define \mathcal{A} to be the variety over k obtained from the curve C by

$$\mathcal{A} : \begin{cases} G_0(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1}) = 0 & \sigma(x_0) = x_0 & \sigma(y_0) = y_0 \\ G_1(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1}) = 0 & \sigma(x_1) = x_1 & \sigma(y_1) = y_1 \\ \vdots & \vdots & \vdots \\ G_{n-1}(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1}) = 0 & \sigma(x_{n-1}) = x_{n-1} & \sigma(y_{n-1}) = y_{n-1}. \end{cases}$$

\mathcal{A} is the Weil restriction of scalars of C to k .

Lemma 4: Variety \mathcal{A} (over k) is birationally equivalent to variety \mathcal{B} over K defined by

$$\mathcal{B} : \begin{cases} v_0^p - v_0 = \alpha_0 u_0 + \beta_0 + \frac{f(u_0)}{h(u_0)^p} & \sigma(u_0) = u_1 & \sigma(v_0) = v_1 \\ v_1^p - v_1 = \alpha_1 u_1 + \beta_1 + \frac{f(u_1)}{h(u_1)^p} & \sigma(u_1) = u_2 & \sigma(v_1) = v_2 \\ \vdots & \vdots & \vdots \\ v_{n-2}^p - v_{n-2} = \alpha_{n-2} u_{n-2} + \beta_{n-2} + \frac{f(u_{n-2})}{h(u_{n-2})^p} & \sigma(u_{n-2}) = u_{n-1} & \sigma(v_{n-2}) = v_{n-1} \\ v_{n-1}^p - v_{n-1} = \alpha_{n-1} u_{n-1} + \beta_{n-1} + \frac{f(u_{n-1})}{h(u_{n-1})^p} & \sigma(u_{n-1}) = u_0 & \sigma(v_{n-1}) = v_0 \end{cases}$$

with $\alpha_i = \sigma^i(\alpha)$ and $\beta_i = \sigma^i(\beta)$.

Proof: First note that \mathcal{B} is birationally equivalent to the variety \mathcal{B}' given by

$$\mathcal{B}' : \begin{cases} w_0^p - h(u_0)^{p-1} w_0 = f(u_0) + (\alpha_0 u_0 + \beta_0) h(u_0)^p \\ w_1^p - h(u_1)^{p-1} w_1 = f(u_1) + (\alpha_1 u_1 + \beta_1) h(u_1)^p \\ \vdots \\ w_{n-1}^p - h(u_{n-1})^{p-1} w_{n-1} = f(u_{n-1}) + (\alpha_{n-1} u_{n-1} + \beta_{n-1}) h(u_{n-1})^p \\ \sigma(u_0) = u_1 & \sigma(w_0) = w_1 \\ \sigma(u_1) = u_2 & \sigma(w_1) = w_2 \\ \vdots & \vdots \\ \sigma(u_{n-2}) = u_{n-1} & \sigma(w_{n-2}) = w_{n-1} \\ \sigma(u_{n-1}) = u_0 & \sigma(w_{n-1}) = w_0 \end{cases}$$

where $w_i = h(u_i)v_i$ (since $\sigma(w_i) = \sigma(h(u_i)v_i) = h(\sigma(u_i))\sigma(v_i)$).

Let T be the linear transformation

$$T : k^n \rightarrow V$$

(where V is a subspace of K^n isomorphic to K) given by the matrix

$$T = (\sigma^i(\Psi_j))_{0 \leq i, j \leq n-1}.$$

This is invertible since $\{\Psi_0, \Psi_1, \dots, \Psi_{n-1}\}$ is a basis of K/k . We extend T to act trivially on x_0, x_1, \dots, x_{n-1} and y_0, y_1, \dots, y_{n-1} .

Let $u_0 = X$ and $w_0 = Y$. Then

$$T \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{bmatrix} = \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \end{bmatrix} \quad \text{and} \quad T \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix} = \begin{bmatrix} w_0 \\ w_1 \\ \vdots \\ w_{n-1} \end{bmatrix}$$

since

$$u_i = \sigma^i(u_0) = \sigma^i(X) = x_0\sigma^i(\Psi_0) + x_1\sigma^i(\Psi_1) + \dots + x_{n-1}\sigma^i(\Psi_{n-1})$$

and

$$w_i = \sigma^i(w_0) = \sigma^i(Y) = y_0\sigma^i(\Psi_0) + y_1\sigma^i(\Psi_1) + \dots + y_{n-1}\sigma^i(\Psi_{n-1}).$$

Since T is invertible, it will suffice to show that T applied to the equations of \mathcal{A} gives the equations of \mathcal{B}' . We have

$$\sigma^i(Y^p - h(X)^{p-1}Y - f(X) - (\alpha X + \beta)h(X)^p) = w_i^p - h(u_i)^{p-1}w_i - f(u_i) - (\alpha_i u_i + \beta_i)h(u_i)^p$$

and

$$Y^p - h(X)^{p-1}Y - f(X) - (\alpha X + \beta)h(X)^p = \sum_{i=0}^{n-1} G_i(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1})\Psi_i$$

hence

$$\begin{aligned} T \begin{bmatrix} G_0(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1}) \\ G_1(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1}) \\ \vdots \\ G_{n-1}(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1}) \end{bmatrix} \\ &= \begin{bmatrix} \sum_{j=0}^{n-1} G_j(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1})\sigma^0(\Psi_j) \\ \sum_{j=0}^{n-1} G_j(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1})\sigma^1(\Psi_j) \\ \vdots \\ \sum_{j=0}^{n-1} G_j(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1})\sigma^{n-1}(\Psi_j) \end{bmatrix} \\ &= \begin{bmatrix} \sigma^0 \left(\sum_{j=0}^{n-1} G_j(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1})\Psi_j \right) \\ \sigma^1 \left(\sum_{j=0}^{n-1} G_j(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1})\Psi_j \right) \\ \vdots \\ \sigma^{n-1} \left(\sum_{j=0}^{n-1} G_j(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1})\Psi_j \right) \end{bmatrix} \\ &= \begin{bmatrix} w_0^p - h(u_0)^{p-1}w_0 - f(u_0) - (\alpha_0 u_0 + \beta_0)h(u_0)^p \\ w_1^p - h(u_1)^{p-1}w_1 - f(u_1) - (\alpha_1 u_1 + \beta_1)h(u_1)^p \\ \vdots \\ w_{n-1}^p - h(u_{n-1})^{p-1}w_{n-1} - f(u_{n-1}) - (\alpha_{n-1} u_{n-1} + \beta_{n-1})h(u_{n-1})^p \end{bmatrix}. \end{aligned}$$

Q.E.D.

We remove the conditions $\sigma(u_i) = u_{i+1}$, $\sigma(v_i) = v_{i+1}$ ($i \in \{0, 1, \dots, n-2\}$), $\sigma(u_{n-1}) = u_0$ and $\sigma(v_{n-1}) = v_0$ in variety \mathcal{B} (i.e. we make the u_i 's independent from each other and the v_i 's also

independent from each other) to get variety \mathcal{C} defined by

$$\mathcal{C} : \begin{cases} v_0^p - v_0 = \alpha_0 u_0 + \beta_0 + \frac{f(u_0)}{h(u_0)^p} \\ v_1^p - v_1 = \alpha_1 u_1 + \beta_1 + \frac{f(u_1)}{h(u_1)^p} \\ \vdots \\ v_{n-1}^p - v_{n-1} = \alpha_{n-1} u_{n-1} + \beta_{n-1} + \frac{f(u_{n-1})}{h(u_{n-1})^p} \end{cases}$$

We then intersect \mathcal{C} with the n hyperplanes $u_i = x$ to get the variety \mathcal{D} given by

$$\mathcal{D} : \begin{cases} v_0^p - v_0 = \alpha_0 x + \beta_0 + \frac{f(x)}{h(x)^p} \\ v_1^p - v_1 = \alpha_1 x + \beta_1 + \frac{f(x)}{h(x)^p} \\ \vdots \\ v_{n-1}^p - v_{n-1} = \alpha_{n-1} x + \beta_{n-1} + \frac{f(x)}{h(x)^p} \end{cases}$$

which is a curve over K

Lemma 5: *Let F_i be the splitting field over $K(x)$ of the equation*

$$v_i^p - v_i = \alpha_i x + \beta_i + \frac{f(x)}{h(x)^p}$$

for $i = 0, 1, \dots, n-1$ i.e. $F_i = K(x)(\overline{v}_i)$ with \overline{v}_i a root of the equation above. If $F = F_0 F_1 \cdots F_{n-1}$ is their compositum, then $[F : K(x)] = p^m$ for some $m \in \mathbb{N}$ and \mathcal{D} has function field isomorphic to F .

Proof: This is a generalization to characteristic p of the proof of lemma 3 in [11]. The following is an outline of the argument:

There is no ambiguity in forming F since every extension $F_i/K(x)$ has prime degree p , hence F is Galois over $K(x)$. Then there exists a minimal subset $\{\overline{v}_{i_1}, \overline{v}_{i_2}, \dots, \overline{v}_{i_m}\}$ of the \overline{v}_i 's such that $F = F_{i_1} F_{i_2} \cdots F_{i_m}$. Let I be the kernel of the homomorphism

$$\varphi : K[x, v_0, v_1, \dots, v_{n-1}] \rightarrow K[x, \overline{v}_0, \overline{v}_1, \dots, \overline{v}_{n-1}] = F.$$

Then I is a prime ideal of dimension one (since F has transcendence degree one over K) generated by $\{x, \overline{v}_0, \overline{v}_1, \dots, \overline{v}_{n-1}\}$. I contains the left hand sides of the equations defining \mathcal{D} by construction of F . Then I defines an irreducible component of \mathcal{D} having function field isomorphic to F . Q.E.D.

Lemma 6: *Let m be as in Lemma 5. Then $m = \dim_{\mathbb{F}_p} \left(\Delta_0 / (\Delta_0 \cap \mathcal{P}(K(x))) \right)$ with*

$$\Delta_0 = \text{span}_{\mathbb{F}_p} \left\{ \overline{v}_0^p - \overline{v}_0, \overline{v}_1^p - \overline{v}_1, \dots, \overline{v}_{n-1}^p - \overline{v}_{n-1} \right\}$$

and $F = F_0 F_1 \cdots F_{m-1}$ with F_i as in Lemma 5.

Proof: Let $\Delta = \Delta_0 + \mathcal{P}(K(x))$. Then $\Delta/\mathcal{P}(K(x)) \cong \Delta_0/(\Delta_0 \cap \mathcal{P}(K(x)))$. From Proposition 2, we have $F = K(x)(\mathcal{P}^{-1}(\Delta)) = K(x)(\mathcal{P}^{-1}(\Delta_0))$ and $m = \dim_{\mathbb{F}_p} \left(\Delta/\mathcal{P}(K(x)) \right)$ which gives us the

result for m . To obtain $F = F_0 F_1 \cdots F_{m-1}$, suppose that $\overline{v_j^p} - \overline{v_j}$ is a linear combination over \mathbb{F}_p of the previous $j - 1$ terms, i.e.

$$\overline{v_j^p} - \overline{v_j} = \sum_{i=0}^{j-1} c_i (\overline{v_i^p} - \overline{v_i})$$

with the c_i 's in \mathbb{F}_p . By applying σ we get

$$\begin{aligned} \overline{v_{j+1}^p} - \overline{v_{j+1}} &= \sigma(\overline{v_j^p} - \overline{v_j}) \\ &= \sigma\left(\sum_{i=0}^{j-1} c_i (\overline{v_i^p} - \overline{v_i})\right) \\ &= \sum_{i=0}^{j-1} c_i (\overline{v_{i+1}^p} + \overline{v_{i+1}}) \\ &= \sum_{i=1}^{j-1} c_{i-1} (\overline{v_i^p} - \overline{v_i}) + c_{j-1} \sum_{i=0}^{j-1} c_i (\overline{v_i^p} - \overline{v_i}) \\ &= \sum_{i=1}^{j-1} d_i (\overline{v_i^p} - \overline{v_i}) \end{aligned}$$

with $d_0 = c_{j-1}c_0$ and $d_i = c_{i-1} + c_{j-1}c_i$ for $i \in \{1, 2, \dots, j-1\}$, i.e. the $j + 1^{\text{th}}$ term is a linear combination of the first j terms and by induction so are all remaining terms. Then F is obtained by adjoining to K the roots of m consecutive equations in \mathcal{D} . Q.E.D.

Remark: Up to this point, all results hold even if the coefficients of $f(X)$ and $h(X)$ are not in k . From now on, the results require that $f(X)$ and $h(X)$ have their coefficients in k .

Corollary 7: For m as in Lemma 5, we have

$$m = m_\alpha = \dim_{\mathbb{F}_p} \left(\text{span}_{\mathbb{F}_p} \left\{ \begin{pmatrix} 1 \\ \alpha_0 \end{pmatrix}, \begin{pmatrix} 1 \\ \alpha_1 \end{pmatrix}, \dots, \begin{pmatrix} 1 \\ \alpha_{n-1} \end{pmatrix} \right\} \right)$$

and K is the exact constant field of F .

Proof: From Lemma 6, $\Delta_0 \subseteq K(x)$ is

$$\begin{aligned} \Delta_0 &= \text{span}_{\mathbb{F}_p} \left\{ \overline{v_0^p} - \overline{v_0}, \overline{v_1^p} - \overline{v_1}, \dots, \overline{v_{n-1}^p} - \overline{v_{n-1}} \right\} \\ &= \text{span}_{\mathbb{F}_p} \left\{ \alpha_0 x + \beta_0 + \frac{f(x)}{h(x)^p}, \alpha_1 x + \beta_1 + \frac{f(x)}{h(x)^p}, \dots, \alpha_{n-1} x + \beta_{n-1} + \frac{f(x)}{h(x)^p} \right\}. \end{aligned}$$

To each function

$$\alpha_i x + \beta_i + \frac{f(x)}{h(x)^p} \in K(x)$$

we associate the vector

$$\begin{pmatrix} \alpha_i \\ \beta_i \\ 1 \end{pmatrix} \in K^3.$$

It is then clear that

$$\Delta_0 \cong \text{span}_{\mathbb{F}_p} \left\{ \begin{pmatrix} \alpha_0 \\ \beta_0 \\ 1 \end{pmatrix}, \begin{pmatrix} \alpha_1 \\ \beta_1 \\ 1 \end{pmatrix}, \dots, \begin{pmatrix} \alpha_{n-1} \\ \beta_{n-1} \\ 1 \end{pmatrix} \right\}.$$

Since applying \mathcal{P} to any non-constant function in $K(x)$ with x^r as highest power of x would give terms in x^p , in particular in x^{rp} , we have $\Delta_0 \cap \mathcal{P}(K(x)) = \Delta_0 \cap \mathcal{P}(K)$ ($r \geq 1$ and $\gcd(r, p) = 1$ from condition 1). Let $u \in \Delta_0 \cap K$, then

$$u = \sum_{i=0}^{j-1} c_i \left(\alpha_i x + \beta_i + \frac{f(x)}{h(x)^p} \right) \quad \text{with} \quad x \sum_{i=0}^{j-1} c_i \alpha_i = 0 \quad \text{and} \quad \frac{f(x)}{h(x)^p} \sum_{i=0}^{j-1} c_i = 0$$

(since $u \in K$), which gives

$$u = \sum_{i=0}^{j-1} c_i \beta_i \quad \text{with} \quad \sum_{i=0}^{j-1} c_i = 0$$

and by Lemma 1, $u \in \mathcal{P}(K)$. Then $\Delta_0 \cap K = \Delta_0 \cap \mathcal{P}(K)$ and we get

$$\begin{aligned} \Delta_0 / (\Delta_0 \cap \mathcal{P}(K(x))) &= \Delta_0 / (\Delta_0 \cap K) \\ &\cong \text{span}_{\mathbb{F}_p} \left\{ \begin{pmatrix} \alpha_0 \\ 1 \end{pmatrix}, \begin{pmatrix} \alpha_1 \\ 1 \end{pmatrix}, \dots, \begin{pmatrix} \alpha_{n-1} \\ 1 \end{pmatrix} \right\}. \end{aligned}$$

Proposition 2 gives us that $F = K(x)(\mathcal{P}^{-1}(\Delta))$, so to get that K is the exact constant field of F , we must show that $\Delta \cap K \subseteq \mathcal{P}(K)$. But we have already shown that $\Delta_0 \cap K = \Delta_0 \cap \mathcal{P}(K)$, so

$$\Delta \cap K = (\Delta_0 + \mathcal{P}(K)) \cap K = (\Delta_0 \cap K) + (\mathcal{P}(K) \cap K) = (\Delta_0 \cap \mathcal{P}(K)) + \mathcal{P}(K) = \mathcal{P}(K)$$

hence K is algebraically closed in F . Q.E.D.

If we define the monic polynomial $\min_\alpha(\sigma)$ by

$$\min_\alpha(\sigma) = \sum_{i=0}^m c_i \sigma^i = \sigma^m + \sum_{i=0}^{m-1} c_i \sigma^i \quad (3)$$

then $\min_\alpha(\sigma)$ is the monic polynomial in σ of minimal degree which is divisible by $\sigma - 1$ (since $\min_\alpha(\sigma) * 1 = 0$) and such that $\min_\alpha(\sigma) * \alpha = 0$.

5 Genus of F

For every $i \in \{1, \dots, m-1\}$, let $t_i = v_i - v_0$, $\gamma_i = \alpha_i - \alpha_0 \in K$ and $\delta_i = \beta_i - \beta_0 \in K$.

Since we are working over Artin-Schreier extensions, F is the splitting field of

$$\left\{ \begin{array}{l} v_0^p - v_0 = \alpha_0 x + \beta_0 + \frac{f(x)}{h(x)^p} \\ t_1^p - t_1 = \gamma_1 x + \delta_1 \\ t_2^p - t_2 = \gamma_2 x + \delta_2 \\ \vdots \\ t_{m-1}^p - t_{m-1} = \gamma_{m-1} x + \delta_{m-1} \end{array} \right. .$$

Lemma 8: Let L be the splitting field of $t_i^p - t_i = \gamma_i x + \delta_i$ for every i in $\{1, \dots, m-1\}$. Then L is an extension of degree p^{m-1} of $K(x)$. It is also a rational function field having generator c (i.e. $L = K(c)$) such that

$$x = \lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i c^{p^i} \quad (4)$$

with $\lambda_i \in K$ and $\lambda_0, \lambda_{m-1} \neq 0$.

Proof: By construction $F = L(\bar{v}_0)$, so $[F : L] = p$. By Lemma 5, we have $[F : K(x)] = p^m$, hence $[L : K(x)] = p^{m-1}$. Using a change of variable, we will transform the system

$$\left\{ \begin{array}{l} t_1^p - t_1 = \gamma_1 x + \delta_1 \\ t_2^p - t_2 = \gamma_2 x + \delta_2 \\ \vdots \\ t_{m-1}^p - t_{m-1} = \gamma_{m-1} x + \delta_{m-1} \end{array} \right. \quad \text{into} \quad \left\{ \begin{array}{l} s_0 = x \\ s_1^p - s_1 = \epsilon_1 s_0 + \rho_1 \\ s_2^p - s_2 = \epsilon_2 s_1 + \rho_2 \\ \vdots \\ s_{m-1}^p - s_{m-1} = \epsilon_{m-1} s_{m-2} + \rho_{m-1} \end{array} \right. .$$

To do this, we proceed by induction on s_i as follows: We first set $s_0 = x$. Suppose that at some point we have $s_i^p - s_i = \epsilon_i s_{i-1} + \rho_i$ for $i \in \{0, 1, \dots, j\}$ (with $\epsilon_i \neq 0$) and $t_i^p - t_i = \gamma_i' s_{j-1} + \delta_i'$ for $i \in \{j+1, j+2, \dots, m-1\}$. For $i \in \{j+1, j+2, \dots, m-1\}$ we set

$$t_i'' = t_i' - \left(\frac{\gamma_i'}{\epsilon_j} \right)^{\frac{1}{p}} s_j$$

(the choice of t_i'' is well defined since, for fields of characteristic p , the p^{th} root is well defined and unique. We then get

$$\begin{aligned} 0 &= t_i'^p - t_i' - \gamma_i' s_{j-1} - \delta_i' \\ &= \left(t_i'' + \left(\frac{\gamma_i'}{\epsilon_j} \right)^{\frac{1}{p}} s_j \right)^p - \left(t_i'' + \left(\frac{\gamma_i'}{\epsilon_j} \right)^{\frac{1}{p}} s_j \right) - \gamma_i' s_{j-1} - \delta_i' \\ &= t_i''^p + \frac{\gamma_i'}{\epsilon_j} s_j^p - t_i'' - \left(\frac{\gamma_i'}{\epsilon_j} \right)^{\frac{1}{p}} s_j - \gamma_i' s_{j-1} - \delta_i' \\ &= t_i''^p + \frac{\gamma_i'}{\epsilon_j} (s_j + \epsilon_j s_{j-1} + \rho_j) - t_i'' - \left(\frac{\gamma_i'}{\epsilon_j} \right)^{\frac{1}{p}} s_j - \gamma_i' s_{j-1} - \delta_i' \\ &= t_i''^p + \frac{\gamma_i'}{\epsilon_j} s_j + \frac{\gamma_i' \rho_j}{\epsilon_j} - t_i'' - \left(\frac{\gamma_i'}{\epsilon_j} \right)^{\frac{1}{p}} s_j - \delta_i' \\ &= t_i''^p - t_i'' - \left(\left(\frac{\gamma_i'}{\epsilon_j} \right)^{\frac{1}{p}} - \frac{\gamma_i'}{\epsilon_j} \right) s_j - \left(\delta_i' - \frac{\gamma_i' \rho_j}{\epsilon_j} \right), \end{aligned}$$

i.e. $t_i''^p - t_i'' = \gamma_i'' s_j + \delta_i''$ for $i \geq j+1$ and $t_{j+1}'' = s_{j+1}$.

It remains to show that at all time in this process, $\epsilon_j \neq 0$ for $0 \leq j < m$. Suppose that $\epsilon_j = 0$ for some j , so $s_j^p - s_j - \rho_j = 0$. By definition of m , and since s_j is a linear combination of $\{t_1, t_2, \dots, t_j\}$ over K , $s_j^p - s_j - \rho_j = s_j^p - s_j - \epsilon_j s_{j-1} - \rho_j$ must be irreducible. But from Corollary 7, K is the exact constant field of F , which would force $s_j^p - s_j = \rho_j$ to be in $\mathcal{P}(K)$, contradicting the irreducibility of $s_j^p - s_j - \rho_j$.

Setting $s_{m-1} = c$ and substituting back into the system, we get $x(c)$ as in (4) with $\lambda_0 = \prod_{i=1}^{m-1} \frac{-1}{\epsilon_i}$ and $\lambda_{m-1} = \prod_{i=1}^{m-1} \left(\frac{1}{\epsilon_i}\right)^{p^{i-1}}$ hence $\lambda_0, \lambda_{m-1} \neq 0$. Q.E.D.

Corollary 9: $x(c)$ in Lemma 8 is a separable polynomial in $K(c)$.

Proof: Let $x'(c)$ be the derivative of $x(c)$, then $x'(c) = \lambda_0 \in K \setminus \{0\}$ (K has characteristic p) so $\gcd(x(c), x'(c)) = 1$ and $x(c)$ must be separable. Q.E.D.

Since F/L is given by the equation

$$v_0^p - v_0 = \alpha_0 x + \beta_0 + \frac{f(x)}{h(x)^p}$$

and since $L = K(c)$, F/K is given by

$$v_0^p - v_0 = \alpha_0 x(c) + \beta_0 + \frac{f(x(c))}{h(x(c))^p}.$$

We now write $\alpha_0 x + \beta_0 + \frac{f(x)}{h(x)^p}$ in the form $f_0(x) + \frac{f_1(x)}{h(x)^p}$ with $\deg(f_1) < p \cdot \deg(h)$. Then F/K is defined by

$$v_0^p - v_0 = f_0(x(c)) + \frac{f_1(x(c))}{h(x(c))^p}.$$

Furthermore, the map $x \rightarrow x(c)$ gives an embedding of the function field of C to F (the function field of \mathcal{D}).

Theorem 10: F/K is a function field of genus \tilde{g} over the exact constant field K with

$$\tilde{g} = \begin{cases} gp^{m-1} - (p-1) & \text{if } \deg(f) \leq p \deg(h) + 1 \text{ and } \sum_{i=0}^{m-1} (-1)^i (a\lambda_i)^{p^{-i}} = 0 \\ gp^{m-1} & \text{otherwise} \end{cases}$$

where a is the coefficient of x in $\alpha_0 x + \beta_0 + \frac{f(x)}{h(x)^p}$.

Proof: In Proposition 3, we have that $r_P \neq 0$ if and only if P is over $h(x)$ or $P = \infty$ and $r_\infty = \min\{\deg(f) - p \cdot \deg(h), 1\}$, so we can write:

$$\frac{2g}{p-1} - r_\infty + 1 = \frac{2g}{p-1} - \min\{\deg(f) - p \cdot \deg(h), 1\} + 1 = \sum_{P|h(x)} (r_P + 1) \deg(P).$$

By Corollary 9, any place Q over $h(x(c))$ is also over P for some P over $h(x)$, and $r_Q = r_P$.

Furthermore, $\sum_{Q|P} \deg(Q) = p^{m-1} \deg(P)$, so

$$\begin{aligned} \sum_{Q|h(x(c))} (r_Q + 1) \deg(Q) &= \sum_{P|h(x)} \sum_{Q|P} (r_Q + 1) \deg(Q) \\ &= \sum_{P|h(x)} \sum_{Q|P} (r_P + 1) \deg(Q) \end{aligned}$$

$$\begin{aligned}
&= \sum_{P|h(x)} (r_P + 1) \sum_{Q|P} \deg(Q) \\
&= \sum_{P|h(x)} (r_P + 1) p^{m-1} \deg(P) \\
&= p^{m-1} \sum_{P|h(x)} (r_P + 1) \deg(P) \\
&= p^{m-1} \left(\frac{2g}{p-1} - \min\{\deg(f) - p \cdot \deg(h), 1\} + 1 \right)
\end{aligned}$$

and, by Proposition 3, this is equal to $\frac{2\tilde{g}}{p-1} - r_\infty + 1$. We must therefore compute r_∞ , to get

$$\tilde{g} = \frac{p-1}{2} \left(p^{m-1} \left(\frac{2g}{p-1} - r + 1 \right) + r_\infty - 1 \right)$$

with $r = \deg(f_0(x)) = \min\{\deg(f) - p \cdot \deg(h), 1\}$. Since r_∞ depends only on $f_0(x(c))$, we must deal with two cases: $r > 1$ and $r = 1$.

$r > 1$: Let $f_0(x) = \sum_{i=0}^r a_i x^i$, then

$$f_0(x(c)) = \sum_{i=0}^r a_i \left(\lambda_{-1} + \sum_{j=0}^{m-1} \lambda_j c^{p^j} \right)^i.$$

The term in c^j , the highest power of c with $\gcd(j, p) = 1$, is $r a_r \lambda_{m-1}^{r-1} \lambda_0 c^{(r-1)p^{m-1}+1}$ and all other terms either have degree less than $(r-1)p^{m-1} + 1$ or have degree sp with $s < (r-1)p^{m-1} + 1$, hence $r_\infty = (r-1)p^{m-1} + 1$ which gives:

$$\tilde{g} = \frac{p-1}{2} \left(p^{m-1} \left(\frac{2g}{p-1} - r + 1 \right) + (r-1)p^{m-1} \right) = p^{m-1}g.$$

$r = 1$: Let $f_0(x) = ax + b$, then $f_0(x(c)) = (a\lambda_{-1} + b) + \sum_{i=0}^{m-1} a\lambda_i c^{p^i}$ and

$$r_\infty = \begin{cases} -v_\infty(f_0(x(c)) - (z^p - z)) & \text{if } v_\infty < 0 \text{ for some } z \in L \\ -1 & \text{else} \end{cases}$$

It is easy to show that $f_0(x(c))$ can be written as $z^p - z + b'$ for some $f \in K[c]$ (so $r_\infty = -1$) if $\sum_{i=0}^{m-1} (-1)^i (a\lambda_i)^{p^{-i}} = 0$ and $z^p - z + a'x + b'$ with $a' \neq 0$ (so $r_\infty = 1$) otherwise. This gives us:

$$\begin{aligned}
\tilde{g} &= \frac{p-1}{2} \left(p^{m-1} \frac{2g}{p-1} + r_\infty - 1 \right) \\
&= p^{m-1}g + \frac{p-1}{2}(r_\infty - 1) \\
&= \begin{cases} gp^{m-1} - (p-1) & \text{if } \sum_{i=0}^{m-1} (-1)^i (a\lambda_i)^{p^{-i}} = 0 \\ gp^{m-1} & \text{otherwise} \end{cases}.
\end{aligned}$$

Q.E.D.

6 Extending the Frobenius

Lemma 11: *If one of the conditions from (2) is satisfied, i.e. if $\gcd\left(\frac{\sigma^n - 1}{\min_\alpha(\sigma)}, \sigma - 1\right) = 1$ or $\text{Tr}_{K/\mathbb{F}_p}(\beta) = 0$, then, the Frobenius σ of K over k can be extended to a k -automorphism on F with order exactly n . In this case, we have*

$$\begin{aligned}\sigma(c) &= \frac{\lambda_0}{\sigma(\lambda_0)}c + \nu_\beta \\ \sigma(\overline{v_0}) &= \overline{v_0} + s_1(c)\end{aligned}$$

with $\nu_\beta^p - \nu_\beta = \min_\alpha(\sigma) * \beta$.

Proof: Since $L = K(c)$ is rational, we must have $\sigma(c) = \lambda c + \lambda'$ for some $\lambda \in K \setminus \{0\}$ and $\lambda' \in K$. Since $\sigma(x) = x$, we have

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

Equating the coefficients of c , we get that $\lambda_0 = \sigma(\lambda_0)\lambda$ and since $\lambda_0 \neq 0$, $\lambda = \frac{\lambda_0}{\sigma(\lambda_0)}$. To compute λ' , we use polynomial (3) obtained in section 4, which satisfies $\min_\alpha(\sigma) * \alpha = 0$ and $\min_\alpha(\sigma) * 1 = 0$.

We first need to extend σ to F . By definition of $\overline{v_i}$, we can set $\sigma(\overline{v_i}) = \overline{v_{i+1}}$ for every i in $\{0, 1, \dots, m-2\}$. We have to define $\sigma(\overline{v_{m-1}}) = \sigma^m(\overline{v_0})$ in terms of $\overline{v_0}, \overline{v_1}, \dots, \overline{v_{m-1}}$ in such a way that $\sigma^n(\overline{v_0}) = \overline{v_0}$. If we apply $\min_\alpha(\sigma)$ to $\overline{v_0}^p - \overline{v_0}$, we have (using Lemma 1):

$$\begin{aligned}\min_\alpha(\sigma) * (\overline{v_0}^p - \overline{v_0}) &= \min_\alpha(\sigma) * \left(\alpha_0 x + \beta_0 + \frac{f(x)}{h(x)^p}\right) \\ &= (\min_\alpha(\sigma) * \alpha) x + \min_\alpha(\sigma) * \beta + (\min_\alpha(\sigma) * 1) \frac{f(x)}{h(x)^p} \\ &= \min_\alpha(\sigma) * \beta \\ &= \nu^p - \nu\end{aligned}$$

for some $\nu \in K$ given by $\left(\frac{\min_\alpha(\rho^l)}{\rho-1}\right) * \beta$ where $\rho * \beta = \beta^p$. We also have

$$\begin{aligned}\min_\alpha(\sigma) * (\overline{v_0}^p - \overline{v_0}) &= (\min_\alpha(\sigma) * \overline{v_0})^p - \min_\alpha(\sigma) * \overline{v_0} \\ &= \left(\sigma(\overline{v_{m-1}}) + \sum_{i=0}^{m-1} c_i \overline{v_i}\right)^p - \left(\sigma(\overline{v_{m-1}}) + \sum_{i=0}^{m-1} c_i \overline{v_i}\right).\end{aligned}$$

Then

$$\mathcal{P} \left(\sigma(\overline{v_{m-1}}) + \sum_{i=0}^{m-1} c_i \overline{v_i} - \nu \right) = 0,$$

and since $\mathcal{P}(\omega) = 0$ if and only if $\omega \in \mathbb{F}_p$, we get

$$\sigma^m(\overline{v_0}) = \sigma(\overline{v_{m-1}}) = \nu + r - \sum_{i=0}^{m-1} c_i \overline{v_i}$$

for some $r \in \mathbb{F}_p$ and $\min_\alpha(\sigma) * \overline{v_0} = \nu + r$. Let $q(\sigma) = \frac{\sigma^n - 1}{\min_\alpha(\sigma)}$, then

$$\begin{aligned} (q(\sigma)\min_\alpha(\sigma)) * \overline{v_0} &= (\sigma^n - 1) * \overline{v_0} \\ &= \sigma^n(\overline{v_0}) - \overline{v_0} \end{aligned}$$

and

$$\begin{aligned} (q(\sigma)\min_\alpha(\sigma)) * \overline{v_0} &= q(\sigma) * (\min_\alpha(\sigma) * \overline{v_0}) \\ &= q(\sigma) * (\nu + r) \\ &= q(\rho^l) * \left(\left(\frac{\min_\alpha(\rho^l)}{\rho - 1} \right) * \beta \right) + q(\sigma) * r \\ &= \left(\frac{\rho^{ln} - 1}{\rho - 1} \right) * \beta + q(\sigma) * r \\ &= \text{Tr}_{F/\mathbb{F}_p}(\beta) + q(\sigma) * r. \end{aligned}$$

In order to have $\sigma^n(\overline{v_0}) = \overline{v_0}$, we need $\text{Tr}_{F/\mathbb{F}_p}(\beta) + q(\sigma) * r = 0$ with $r \in \mathbb{F}_p$. But r is fixed under σ , so $q(\sigma) * r = r(q(\sigma) * 1)$. If $\text{Tr}_{F/\mathbb{F}_p}(\beta) = 0$, we can take $r = 0$. If $\text{Tr}_{F/\mathbb{F}_p}(\beta) \neq 0$, we need a solution to $r(q(\sigma) * 1) = -\text{Tr}_{F/\mathbb{F}_p}(\beta)$. This will be possible if and only if $q(\sigma) * 1 \neq 0$, i.e. if $\sigma - 1$ does not divide $q(\sigma) = \frac{\sigma^n - 1}{\min_\alpha(\sigma)}$. We will therefore be able to extend σ with order n on F if and only if at least one of conditions 2 is satisfied. If one of these conditions is satisfied, we solve for r and set $\nu_\beta = \nu + r$. This also gives us

$$\sigma^m(v_0) = \sigma(v_{m-1}) = \nu_\beta - \sum_{i=0}^{m-1} c_i v_i.$$

We now consider the effect of σ on t_{m-1} . For $i \in \{1, 2, \dots, m-2\}$, we have $\sigma(t_i) = \sigma(v_i - v_0) = v_{i+1} - v_1 = t_{i-1} - t_1$, but for $i = m-1$ we get

$$\begin{aligned} \sigma(t_{m-1}) &= \sigma(v_{m-1} - v_0) \\ &= \sigma(v_{m-1}) - v_1 \\ &= \left(\nu_\beta - \sum_{i=0}^{m-1} c_i v_i \right) - (t_1 + v_0) \\ &= \nu_\beta - t_1 - \left(\sum_{i=1}^{m-1} c_i (v_i - v_0) + \sum_{i=0}^{m-1} c_i v_0 \right) - v_0 \\ &= \nu_\beta - t_1 - \sum_{i=1}^{m-1} c_i t_i - \left(1 + \sum_{i=0}^{m-1} c_i \right) v_0 \\ &= \nu_\beta - t_1 - \sum_{i=1}^{m-1} c_i t_i - (\min_\alpha(\sigma) * 1) v_0 \\ &= \nu_\beta - t_1 - \sum_{i=1}^{m-1} c_i t_i. \end{aligned}$$

By the construction in section 5, $s_{m-1} = t_{m-1} - \sum_{i=1}^{m-2} d_i t_i$ and $t_j = \sum_{i=1}^{m-1} \hat{d}_{i,j} s_i$ for some d_i 's and some $\hat{d}_{i,j}$'s in K , so

$$\begin{aligned}
\sigma(c) &= \sigma(s_{m-1}) \\
&= \sigma(t_{m-1}) - \sum_{i=1}^{m-2} \sigma(d_i) \sigma(t_i) \\
&= \left(\nu_\beta - t_1 - \sum_{i=1}^{m-1} c_i t_i \right) - \sum_{i=1}^{m-2} \sigma(d_i) (t_{i+1} - t_1) \\
&= \nu_\beta + \sum_{i=1}^{m-1} \mu_i s_i
\end{aligned}$$

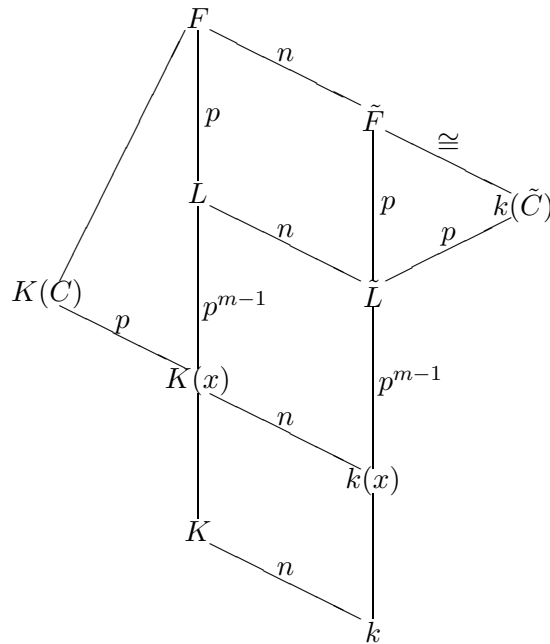
for some μ_i 's in K . But since $\deg_c(s_i) = p^{m-i}$ and $\sigma(c) = \lambda c + \lambda'$, we must have $\mu_i = 0$ for $i < m-1$. Since $s_{m-1} = c$, we get $\sigma(c) = \lambda c + \nu_\beta$ (and we have $\mu_{m-1} = \lambda$). Finally, to get $\sigma(\bar{v}_0)$, we use that $\bar{v}_1 - \bar{v}_0$ is a solution to $t_1^p - t_1 = \gamma_1 x(c) + \delta_1$, so $\bar{v}_1 - \bar{v}_0 = s_1(c)$ (since $s_1 = t_1 = v_1 - v_0$). Q.E.D.

Note: if we have either $\gcd(n, p) = 1$ or $m_\alpha = n$, then $\gcd\left(\frac{\sigma^n - 1}{\min_\alpha(\sigma)}, \sigma - 1\right) = 1$ and condition 2 is always satisfied.

7 Restriction

Theorem 12: *Let σ be an extension of the Frobenius automorphism of K over k to F of order n . Let \tilde{F} be the fixed field of F under σ . Then \tilde{F} is a function field of genus \tilde{g} over the exact constant field k , where \tilde{g} is the genus of F over K .*

Proof: This is a generalization to characteristic p of the proof of theorem 12 in [11]. Let $L = K(c)$ and \tilde{L} its restriction under σ . We have the following field diagram (where \tilde{C} is the curve we are looking for):



Lemma 13: $\text{Gal}(F/L) = \langle \tau \rangle$ with $\tau(\bar{v}_i) = \bar{v}_i + 1$ for every i and $\sigma(\tau(\omega)) = \tau(\sigma(\omega))$ for every $\omega \in F$.

Proof: Remember that $\bar{v}_j - \bar{v}_0$ is a root of $t_j^p - t_j - \gamma_j x - \delta_j = 0$, hence $\bar{v}_j - \bar{v}_0 \in L$. Let $\varsigma \in \text{Gal}(F/L)$, then ς fixes L , in particular $\varsigma(\bar{v}_j - \bar{v}_0) = \bar{v}_j - \bar{v}_0$ for every j . Then $\varsigma(\bar{v}_j) - \bar{v}_j = \varsigma(\bar{v}_0) - \bar{v}_0$ for every j . But $\varsigma \in \text{Gal}(F/L) \subset \text{Gal}(F/K)$, so ς is completely determined by its action on the \bar{v}_j 's and for every j , $\varsigma(\bar{v}_j) = \bar{v}_j + r_j$ with $r_j \in \{0, 1, \dots, p-1\}$. Then $r_j = r_0$ for every j and ς is completely determined by its action on \bar{v}_0 , with $\varsigma(\bar{v}_j) = \bar{v}_j + r$ for some $r \in \{0, 1, \dots, p-1\}$, so $\varsigma = \tau^r$ and $\text{Gal}(F/L) = \langle \tau \rangle$. But for every $i \in \{0, 1, \dots, n-1\}$ and $j \in \{0, 1, \dots, p-1\}$, we have

$$\sigma^i(\tau^j(\bar{v}_0)) = \sigma^i(\bar{v}_0 + j) = \sigma^i(\bar{v}_0) + j = \bar{v}_i + j = \tau^j(\bar{v}_i) = \tau^j(\sigma^i(\bar{v}_0))$$

hence σ and τ commute. Q.E.D.

Lemma 14: Let $\mu \in K$ be such that $\text{Tr}_{K/k}(\mu) = 1$ and set $\tilde{c} = \text{Tr}_{L/\tilde{L}}(\mu\lambda_0 c)$ and $\tilde{v} = \text{Tr}_{F/\tilde{F}}(\mu\bar{v}_0)$. Then we have $\tilde{L} = k(\tilde{c})$ and $\tilde{F} = k(\tilde{c}, \tilde{v})$. Furthermore, $\tilde{c} = \lambda_0 c + \tilde{\lambda}$ and the Artin-Schreier equation defining \tilde{F} over \tilde{L} is

$$\tilde{v}^p - \tilde{v} = \text{Tr}_{K/k}(\mu^p \alpha)x + \text{Tr}_{K/k}(\mu^p \beta) + \frac{f(x)}{h(x)^p} + \text{Tr}_{F/\tilde{F}}(\mu^p \bar{v}_0) - \text{Tr}_{F/\tilde{F}}(\mu \bar{v}_0).$$

Proof: From Lemma 11, we have $\sigma(\lambda_0 c) = \sigma(\lambda_0)\sigma(c) = \lambda_0 c + \sigma(\lambda_0)\nu_\beta$ hence

$$\begin{aligned} \tilde{c} &= \mu\lambda_0 c + \sum_{i=1}^{n-1} \sigma^i(\mu) \left(\lambda_0 c + \sum_{j=0}^{i-1} \sigma^{j+1}(\lambda_0)\sigma^j(\nu_\beta) \right) \\ &= \lambda_0 c \sum_{i=0}^{n-1} \sigma^i(\mu) + \sum_{i=1}^{n-1} \sigma^i(\mu) \sum_{j=0}^{i-1} \sigma^{j+1}(\lambda_0)\sigma^j(\nu_\beta) \\ &= \lambda_0 c + \tilde{\lambda} \end{aligned}$$

with $\tilde{\lambda} \in K$ and $\tilde{c} \in \tilde{L}$ by definition, so $\tilde{L} = k(\tilde{c})$. From Lemma 13, τ restricts to \tilde{F}/\tilde{L} , with $\tau(\tilde{v}) = \tilde{v} + 1$. then

$$\text{Tr}_{\tilde{F}/\tilde{L}}(\tilde{v}) = \sum_{i=0}^{p-1} \tau^i(\tilde{v}) = \sum_{i=0}^{p-1} \tilde{v} + i = \begin{cases} 1 & \text{if } p = 2 \\ 0 & \text{else} \end{cases}$$

and

$$\begin{aligned} \tilde{v}^p &= \text{Tr}_{F/\tilde{F}}(\mu^p \bar{v}_0^p) \\ &= \text{Tr}_{F/\tilde{F}} \left(\mu^p \left(\bar{v}_0 + \alpha_0 x + \beta_0 + \frac{f(x)}{h(x)^p} \right) \right) \\ &= \text{Tr}_{F/\tilde{F}}(\mu^p \bar{v}_0) + \text{Tr}_{F/\tilde{F}}(\mu^p \alpha_0)x + \text{Tr}_{F/\tilde{F}}(\mu^p \beta_0) + \text{Tr}_{F/\tilde{F}}(\mu^p) \frac{f(x)}{h(x)^p} \\ &= \text{Tr}_{K/k}(\mu^p \alpha_0)x + \text{Tr}_{K/k}(\mu^p \beta_0) + \frac{f(x)}{h(x)^p} + \text{Tr}_{F/\tilde{F}}(\mu^p \bar{v}_0), \end{aligned}$$

which gives us the norm

$$\begin{aligned} N_{\tilde{F}/\tilde{L}}(\tilde{v}) &= \prod_{i=0}^{p-1} \tau^i(\tilde{v}) = \prod_{i=0}^{p-1} (\tilde{v} + i) = \tilde{v}^p - \tilde{v} \\ &= \text{Tr}_{K/k}(\mu^p \alpha)x + \text{Tr}_{K/k}(\mu^p \beta) + \frac{f(x)}{h(x)^p} + \text{Tr}_{F/\tilde{F}}(\mu^p \bar{v}_0) - \text{Tr}_{F/\tilde{F}}(\mu \bar{v}_0). \end{aligned}$$

Q.E.D.

To map the ideal class group of $K(C)$ to the ideal class group of $k(\tilde{C})$, we first use the map $x \rightarrow x(\tilde{c})$ to map into $F = K(c, \bar{v}_0) = K(\tilde{c}, \bar{v}_0)$ (since $\tilde{c} = \lambda_0 c + \tilde{\lambda}$), and then use the norm $N_{F/\tilde{F}}$ to map into \tilde{F} .

Corollary 15: *If $\gcd(n, p) = 1$, then \tilde{F} is defined over k by*

$$\tilde{v}^p - \tilde{v} = \text{Tr}_{K/k}(\alpha)x(\tilde{c}) + \text{Tr}_{K/k}(\beta) + \frac{f(x(\tilde{c}))}{h(x(\tilde{c}))^p}$$

where

$$x(\tilde{c}) = \lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i \left(\frac{1}{\lambda_0} \tilde{c} - \frac{\tilde{\lambda}}{\lambda_0} \right)^{p^i}$$

which is isomorphic to the curve

$$\tilde{C} : \tilde{y}^p - h(x(\tilde{c}))^{p-1} \tilde{y} = f(x(\tilde{c})) + (\text{Tr}_{K/k}(\alpha)x(\tilde{c}) + \text{Tr}_{K/k}(\beta))h(x(\tilde{c}))^p.$$

Proof: We apply Lemma 14 with $\mu \equiv n^{-1} \pmod{p}$ (μ exists since $\gcd(n, p) = 1$). Then $\mu^p = \mu$ and $\sigma(\mu) = \mu$, so we have:

$$\begin{aligned} \text{Tr}_{K/k}(\mu) &= n\mu = 1 & , & & \text{Tr}_{K/k}(\mu^p \alpha) &= \text{Tr}_{K/k}(\alpha) & , \\ \text{Tr}_{K/k}(\mu^p \beta) &= \text{Tr}_{K/k}(\beta) & \text{and} & & \text{Tr}_{F/F'}(\mu^p \bar{v}_0) &= \text{Tr}_{F/F'}(\mu \bar{v}_0) & . \end{aligned}$$

To get the equation of \tilde{C} , we simply set $\tilde{v} = \frac{\tilde{y}}{h(x(\tilde{c}))}$ and multiply the resulting equation by $h(x(\tilde{c}))^p$. Q.E.D.

8 Algorithm

Assuming that curve C satisfies condition 2 and is defined over the field $K = \mathbb{F}_p(\omega)$, then the algorithm can be written as follows:

1. For i from 0 up to n , write $\sigma^i(\alpha)$ as vectors over \mathbb{F}_p .
2. Compute $\min_\alpha(\sigma)$ such that $\min_\alpha(\sigma) * \alpha = 0$ and $\min_\alpha(\sigma) * 1 = 0$.
3. $m = \deg_\sigma(\min_\alpha(\sigma))$.
4. Compute $\nu = \left(\frac{\min_\alpha(\rho^l)}{\rho^{-1}} \right) * \beta$ where $\rho(\omega) = \omega^p$.
5. Compute $\text{Tr}_{K/\mathbb{F}_p}(\beta)$ and $q(\sigma) = \frac{\sigma^n - 1}{\min_\alpha(\sigma)}$.
6. If $\text{Tr}_{K/\mathbb{F}_p}(\beta) = 0$ set $\nu_\beta = \nu$, otherwise set $\nu_\beta = \nu - \frac{\text{Tr}_{K/\mathbb{F}_p}(\beta)}{q(\sigma) * 1}$.
7. Find an i between 0 and $n - 1$ such that $\text{Tr}_{K/k}(\omega^i) \neq 0$ and set $\mu = \frac{\omega^i}{\text{Tr}_{K/k}(\omega^i)}$.
8. For i from 1 up to $m - 1$, compute $\gamma_i = \sigma^i(\alpha) - \alpha$ and $\delta_i = \sigma^i(\beta) - \beta$.
9. Starting form $\gamma'_i = \gamma_i$ and $\delta'_i = \delta_i$, compute ϵ_i and ρ_i as follows:
For i from 1 up to $m - 1$:

- set $\epsilon_i = \gamma'_i$ and $\rho_i = \delta'_i$;
 - for j from $i + 1$ up to $m - 1$ replace γ'_j by $\left(\frac{\gamma'_j}{\epsilon_i}\right)^{1/p} - \left(\frac{\gamma'_j}{\epsilon_i}\right)$ and δ'_j by $\delta'_j - \frac{\rho_i \gamma'_j}{\epsilon_i}$.
10. Set $s_{m-1} = c$. For i from $m - 2$ down to 0 , set $s_i = \frac{1}{\epsilon_{i+1}}(s_{i+1}^p - s_{i+1} - \rho_{i+1})$.
 11. Compute $\tilde{\lambda} = \sum_{i=1}^{n-1} \sigma^i(\mu) \sum_{j=0}^{i-1} \sigma^j(\sigma(\lambda_0)\nu_\beta)$ where λ_0 is the coefficient of c^1 in s_0 and set $c = \frac{1}{\lambda_0}(\tilde{c} - \tilde{\lambda})$.
 12. Compute $x(\tilde{c}) = s_0(\tilde{c})$ and $s_1(\tilde{c})$.
 13. Compute $\tilde{h}(\tilde{c}) = h(x(\tilde{c}))$.
 14. Compute $Tr_{F/\tilde{F}}((\mu^p - \mu)\overline{v_0}) = \sum_{i=0}^{n-1} \sigma^i(\mu^p - \mu) \sum_{j=0}^i \sigma^j(s_1(\tilde{c}))$.
 15. Compute $\tilde{f}(\tilde{c}) = f(x(\tilde{c})) + (Tr_{K/k}(\mu^p \alpha)x(\tilde{c}) + Tr_{K/k}(\mu^p \beta) + Tr_{F/\tilde{F}}((\mu^p - \mu)\overline{v_0}))\tilde{h}(\tilde{c})^p$.

The curve \tilde{C} is then given by the equation

$$\tilde{C} : \tilde{y}^p - \tilde{h}(\tilde{c})^{p-1}\tilde{y} = \tilde{f}(\tilde{c}).$$

We use the map $x \rightarrow x(\tilde{c})$ to embed $K(C)$ into $F = K(\tilde{c}, \overline{v_0})$, then the norm $N_{F/\tilde{F}}$ to restrict to $\tilde{F} = k(\tilde{C})$.

9 Characteristic 2

For this section, we will assume that K has characteristic 2, i.e. $p = 2$. The equation of the curve is then

$$Y^2 + h(X)Y = f(X) + (\alpha X + \beta)h(X)^2.$$

Then condition (1) is equivalent to

$$\begin{cases} \gcd(\deg(f), 2) = 1 \\ C \text{ nonsingular} \end{cases}$$

and the genus of the curve is $g = \deg(h) + \frac{1}{2} \max\{\deg(f) - 1, 0\}$. For elliptic curves, we have the following lemma:

Lemma 16: *Any curve of the form $Y^2 + XY = X^3 + \alpha X^2 + \beta$ is isomorphic to a curve of the form $Z^2 + h(W)Z = f(W) + (\bar{\alpha}W + \bar{\beta})h(W)^2$.*

Proof: Let C be the curve given by $Y^2 + XY = X^3 + \alpha X^2 + \beta$. We apply the following change of variable:

$$W = \frac{X}{\sqrt{\beta}} \quad \text{and} \quad Z = \frac{Y}{\sqrt{\beta}} + 1 \quad \text{i.e.} \quad X = \sqrt{\beta}W \quad \text{and} \quad Y = \sqrt{\beta}Z + \sqrt{\beta}.$$

Then we have:

$$\begin{aligned} 0 &= Y^2 + XY + X^3 + \alpha X^2 + \beta \\ &= (\sqrt{\beta}Z + \sqrt{\beta})^2 + (\sqrt{\beta}W)(\sqrt{\beta}Z + \sqrt{\beta}) + (\sqrt{\beta}W)^3 + \alpha(\sqrt{\beta}W)^2 + \beta \\ &= \beta(Z^2 + WZ + \sqrt{\beta}W^3 + \alpha W^2 + W) \\ &= \beta(Z^2 + h(W)Z + f(W) + (\bar{\alpha}W + \bar{\beta})h(W)^2) \end{aligned}$$

with $h(W) = W$, $f(W) = W$, $\bar{\alpha} = \sqrt{\beta}$ and $\bar{\beta} = \alpha$ Then the curve C is isomorphic to the curve $C' : Z^2 + h(W)Z = f(W) + (\bar{\alpha}W + \bar{\beta})h(W)^2$. Q.E.D.

9.1 Fields

To get conditions on n in order for m to have the possibility of taking a given value, we note that $\min_{\alpha}(\sigma)$ must divide $\sigma^n + 1$. If we find the minimal value of i such that $\min_{\alpha}(\sigma)$ divides $\sigma^i + 1$, then i must divide n . Note that $\min_{\alpha}(\sigma) = \sigma^m + 1 + \sum_{j=1}^{m-1} d_j \sigma^j$ and each $d_j \in \{0, 1\}$, hence we can list all the possible $\min_{\alpha}(\sigma)$.

For m between 2 and 20, we can build a table of necessary prime divisors of n (Table 1). However, it may not be sufficient that n be divisible by one of the primes in the list for m to insure that K contains elements with that given m . In many cases, n must be divisible by the product of two or more of the primes in the list, possibly to a power greater than 1.

We could also build a list of the sufficient divisors of n for the field K to have elements with a given value of m , however this table would be much longer. For example, the list of sufficient divisors for n to admit $m = 9$ is

$$9, 10, 12, 15, 16, 17, 21, 28, 124, 186, 210, 217, 252, 254, 255$$

and the list for $m = 20$ contains 190 integers.

Another way to look at Table 1 goes as follows: if n is divisible by an element of the right hand side, then there exists an element of the field K such that m is less or equal to the value on the left hand side.

Table 1:

m	prime divisors of n
2	2
3	2, 3
4	2, 3, 7
5	2, 3, 5, 7
6	2, 3, 5, 7, 31
7	2, 3, 5, 7, 31
8	2, 3, 5, 7, 31, 127
9	2, 3, 5, 7, 17, 31, 127
10	2, 3, 5, 7, 17, 31, 73, 127
11	2, 3, 5, 7, 11, 17, 31, 73, 127
12	2, 3, 5, 7, 11, 17, 23, 31, 73, 89, 127
13	2, 3, 5, 7, 11, 13, 17, 23, 31, 73, 89, 127
14	2, 3, 5, 7, 11, 13, 17, 23, 31, 73, 89, 127, 8191
15	2, 3, 5, 7, 11, 13, 17, 23, 31, 43, 73, 89, 127, 8191
16	2, 3, 5, 7, 11, 13, 17, 23, 31, 43, 73, 89, 127, 151, 8191
17	2, 3, 5, 7, 11, 13, 17, 23, 31, 43, 73, 89, 127, 151, 257, 8191
18	2, 3, 5, 7, 11, 13, 17, 23, 31, 43, 73, 89, 127, 151, 257, 8191, 131071
19	2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 43, 73, 89, 127, 151, 257, 8191, 131071
20	2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 43, 73, 89, 127, 151, 257, 8191, 131071, 524287

10 Conclusion

We have shown how the GHS Weil descent attack can be adapted to Artin-Schreier curves (over the field K of characteristic p) of the form

$$Y^p - h(X)^{p-1}Y = f(X) + (\alpha X + \beta)h(X)^p,$$

with $f(X)$ and $h(X)$ defined over the subfield k and some extra conditions (conditions (1) and (2)).

In particular, for these curves to be used in cryptography, $|\text{Jac}(C)(K)|$ should be almost prime (i.e. a prime multiplied by a small factor). If $|\text{Jac}(C)(K)|$ divides $|\text{Jac}(\tilde{C})(k)|$ (or a small multiple of $|\text{Jac}(\tilde{C})(k)|$), experimental results seem to indicate that $|\ker(\Phi)|$ is likely to be small.

The main reason the Weil descent attack can be an effective way of solving the discrete log problem for a curve C is due to the index calculus attack for curves of genus greater than 2. For curves of genus 1 or 2, the best known attacks for the discrete log problem (Shank's Baby Step-Giant Step algorithm, Pollard's ρ method) require $O(g^2 q^{g/2+\epsilon})$ bit operations. But for hyperelliptic curves of genus 3 or higher, if the genus g is not too large, we can use the index calculus attack (see [10] and [21] for $g! < q$, see also [1], [3], [9] and [16] for $g! > q$) which gives a running time of $O\left(g^4 q^{2-\frac{4}{2g+1}+\epsilon}\right)$ (for $(g-1)! < q$). Since Jacobian arithmetic for Artin-Schreier curves over the field \mathbb{F}_q can be done in $O(p^7 g^2 (\log(q))^2)$ bit operations (compared to $O(g^2 (\log(q))^2)$ in characteristic 2), the index calculus attack can be adapted to Artin-Schreier curves in a given characteristic with the same asymptotic running times.

11 Examples

Example 1:

Let $K = \mathbb{F}_{2^{78}}$ and $k = \mathbb{F}_{2^{26}}$ (i.e. $q = 2^{26}$ and $n = 3$. Given any $\alpha \in K \setminus k$ (i.e. such that $\text{min}_\alpha(\sigma) = \sigma^3 + 1$) and any $\beta \in K$ (condition 2 is satisfied). Then, for a curve C of genus $g = 2$ given by an equation of the form

$$C : Y^2 - h(X)Y = f(X) + (\alpha X + \beta)h(X)^2$$

with $h(X)$ and $f(X)$ defined over k , we can construct a curve \tilde{C} of genus 7 or 8 defined over k (since $m = 3$, $\tilde{g} = g2^{m-1} - 1$ or $g2^{m-1}$). The order of $\text{Jac}(\tilde{C})(k)$ is greater than the order of $\text{Jac}(C)(K)$ ($q^7 + O(q^{13/2})$ or $q^8 + O(q^{15/2})$ instead of $q^6 + O(q^{9/2})$), so the kernel of the map from $\text{Jac}(C)(K)$ to $\text{Jac}(\tilde{C})(k)$ need not be trivial even if $|\text{Jac}(C)(K)|$ is almost prime. Although the discrete log problem should be very difficult to solve directly on C (equivalent to solving the discrete log for an elliptic curve over a field of 156 bits), it should be somewhat easier on \tilde{C} (equivalent to solving the discrete log for an elliptic curve over a field of close to 120 bits).

Example 2:

Let $K = \mathbb{F}_{3^{162}}$ and $k = \mathbb{F}_{3^{27}}$ (i.e. $q = 3^{27}$ and $n = 6$. Given $\alpha \in K \setminus k$ and $\beta \in K$ in one of the following cases:

- α is a root of $a^{q^3} + a^{q^2} + 2a^q + 2a = 0$ and $\text{Tr}_{K/\mathbb{F}_3}(\beta) = 0$ (true for a third of the elements of K);

- α is a root of $a^{q^3} + 2a^{q^2} + 2a^q + a = 0$ and $\text{Tr}_{K/\mathbb{F}_3}(\beta) = 0$ (true for a third of the elements of K);
- α is a root of $a^{q^3} + 2a = 0$ and β is any element in K ;

(i.e. such that $m = 3$ and condition 2 is satisfied), then for a curve C of genus $g = 1$ given by an equation of the form

$$C : Y^3 - Y = X^2 + \alpha X + \beta$$

(note that in this case, C is elliptic) we can construct a curve \tilde{C} of genus 7 or 9 defined over k (since $m = 3$, $\tilde{g} = g3^{m-1} - 2$ or $g3^{m-1}$). The order of $\text{Jac}(\tilde{C})(k)$ is greater than the order of $\text{Jac}(C)(K)$ ($q^7 + O(q^{13/2})$ or $q^9 + O(q^{17/2})$ instead of $q^6 + O(q^3)$), so the kernel of the map from $\text{Jac}(C)(K)$ to $\text{Jac}(\tilde{C})(k)$ need not be trivial even if $|\text{Jac}(C)(K)|$ is almost prime. Although the discrete log problem is intractable directly on C (we have an elliptic curve over a field of just over 256 bits), it should be much easier (although still difficult) on \tilde{C} (equivalent to solving the discrete log for an elliptic curve over a field of close to 128 bits).

References

- [1] L. M. Adleman, J. DeMarrais, M.-D. Huang, A subexponential algorithm for discrete logarithms over hyperelliptic curves of large genus over $\text{GF}(q)$, *Theoret. Comput. Sci.*, **226**, no. 1-2, pp. 7-18, 1999.
- [2] C. Diem, The GHS attack in odd characteristic, *J. Ramanujan Math. Soc.*, **18** no. 1, 2003.
- [3] A. Enge, Computing discrete logarithms in high-genus hyperelliptic jacobians in provably subexponential time, *Math. Comp.*, **71**, no. 238, pp. 729-742, 2002.
- [4] G. Frey, Applications of arithmetical geometry to cryptographic constructions, *Finite fields and applications (Augsburg, 1999)*, Springer-Verlag, 128-161, 2001.
- [5] S.D. Galbraith, Weil descent of Jacobians, *proceedings WCC 2001*, Discrete Applied Mathematics Journal 6, 2001.
- [6] S.D. Galbraith, Limitations of constructive Weil descent, *Public-Key Cryptography and Computational Number Theory, September 11-15, 2000, Warsaw, Poland*, Walter de Gruyter, 59-70, 2001.
- [7] S. D. Galbraith, F. Hess, N. P. Smart, Extending the GHS Weil descent attack, *Advances in Cryptology - EUROCRYPT 2002*, Springer-Verlag, LNCS 2332, 29-44, 2002.
- [8] S. D. Galbraith, N. P. Smart, A cryptographic application of Weil descent, *Cryptography and coding (Cirencester, 1999)*, Springer-Verlag, LNCS 1746, 191-200, 1999.
- [9] T. Garefalakis, D. Panario, The index calculus method using non-smooth polynomials, *Math. Comp.*, **70**, no 235, pp. 1253-1264, 2001.
- [10] P. Gaudry, An algorithm for solving the discrete log problem on hyperelliptic curves, *Advances in cryptology - EUROCRYPT 2000*, Springer-Verlag, LNCS 1807, pp. 19-34, 2000.

- [11] P. Gaudry, F. Hess and N. P. Smart, Constructive and destructive facets of Weil descent on elliptic curves, *J. Cryptology*, **15**, 19-46, 2002.
- [12] F. Hess, G. Seroussi, N.P. Smart, Two topics in hyperelliptic cryptography, *SAC 2001*, 2001.
- [13] M. Jacobson, A. Menezes, A. Stein, Solving elliptic curve discrete logarithm problems using Weil descent, *J. Ramanujan Math. Soc.*, **16** no. 3, 231–260, 2001.
- [14] M. Maurer, A. Menezes, E. Teske, Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree, *Indocrypt 2001*, Springer-Verlag, LNCS 2247, 195-213, 2001.
- [15] A. Menezes, M. Qu, Analysis of the Weil Descent Attack of Gaudry, Hess and Smart, *Topics in Cryptology – CT-RSA 2001*, Springer-Verlag, LNCS 2020, 308-318, 2001.
- [16] V. Müller, A. Stein, C. Thiel, Computing discrete logarithms in real quadratic congruence function fields of large genus, *Math. Comp.*, **68**, no. 226, pp. 807-822, 1999.
- [17] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, 1999
- [18] A. Seigo, Weil descent of elliptic curves over finite fields of characteristic three. *Advances in cryptology—ASIACRYPT 2000 (Kyoto)*, Springer-Verlag, LNCS 1976, 248-258, 2000
- [19] N.P. Smart, How secure are elliptic curves over composite extension fields?, *Proceedings EUROCRYPT 2001*, Springer-Verlag, LNCS 2045, 30-39, 2001.
- [20] H. Stichtenoth, *Algebraic function fields and Codes*, Springer-Verlag, 1993.
- [21] N. Thériault, Index calculus attack for hyperelliptic curves of small genus, preprint, 2003.
- [22] N. Thériault, Weil descent attack for Kummer extensions, preprint, 2003.