

# Weil descent attack for Kummer extensions

Nicolas Thériault, University of Toronto

## Abstract

In this paper, we show how the Weil descent attack of Gaudry, Hess and Smart can be adapted to work for some hyperelliptic curves defined over fields of odd characteristic. This attack applies to a family of hyperelliptic and superelliptic curves over quadratic field extensions, as well as two families of hyperelliptic curves defined over cubic extensions. We also show that those are the only families of nonsingular curves defining Kummer extensions for which this method will work.

## 1 Introduction

In [3], Claus Diem showed that some elliptic curves defined over fields of odd characteristic may be vulnerable to a Weil descent attack. However no description of a practical Weil descent attack for elliptic or hyperelliptic curves has yet been published.

In this paper, we give a GHS-like attack for some curves whose function fields are Kummer extensions over the field  $K(x)$ .

The attack works for the following families of curves:

1. Nonsingular superelliptic curves defined over  $\mathbb{F}_{q^n}$  ( $n$  divisible by 2) by an equation of the form

$$Y^r = (X - a)h(X)$$

with  $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$  and  $h(X)$  defined over  $\mathbb{F}_q$ . The resulting curve is superelliptic of genus  $rg + (r - 1)(r - 2)/2$  where  $g$  is the genus of the original curve.

2. Nonsingular hyperelliptic curves defined over  $\mathbb{F}_{q^n}$  ( $n$  divisible by 3) by an equation of the form

$$Y^2 = (X - a)h(X)$$

with  $a \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$  and  $h(X)$  defined over  $\mathbb{F}_q$ . The resulting curve is hyperelliptic of genus  $4g + 1$  where  $g$  is the genus of the original curve.

3. Nonsingular hyperelliptic curves defined over  $\mathbb{F}_{q^n}$  ( $n$  divisible by 3) by an equation of the form

$$Y^2 = (X - a)(x - a^q)h(X)$$

with  $a \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$  and  $h(X)$  defined over  $\mathbb{F}_q$ . The resulting curve is hyperelliptic of genus  $4g - 1$  where  $g$  is the genus of the original curve.

We also show that these are the only families of curves for which this method can work.

This paper is divided as follows: The curves considered here are described in section 2. We show how to construct the function field associated to the Weil restriction of scalars in section 3. In section 4, we give conditions under which the GHS-like attack can be possible. The attack for the first family of curves (for quadratic field extensions) is explained in 5. The attacks for the two other families of curves (for cubic field extensions) are described in 6. Finally, some examples are given in section 8.

## 2 Curves

Let  $k = \mathbb{F}_q$  be a field of characteristic  $p$  ( $q = p^l$ ,  $l \geq 1$ ) and  $K = \mathbb{F}_{q^n}$  its extension of degree  $n$  ( $n > 1$ ). Let  $\sigma$  be the Frobenius of  $K$  over  $k$ .

Let  $C$  be a nonsingular curve of genus  $g > 0$  over  $K$  defined by the equation

$$Y^r = f(X)$$

with

$$\gcd(r, \deg(f)) = 1 \quad \text{and} \quad r|(q-1) \tag{1}$$

(we require  $r|(q-1)$  to insure that  $k$  contains a primitive  $r$ -th root of unity, it also implies that  $\gcd(p, r) = 1$ ). Note that for  $C$  to be nonsingular,  $f(X)$  must be separable.

## 3 Weil Descent

Let  $\{\Psi_0, \Psi_1, \dots, \Psi_{n-1}\}$  be a basis for  $K$  over  $k$  with sum 1. Let

$$X = \sum_{i=0}^{n-1} u_i \Psi_i \quad \text{and} \quad Y = \sum_{i=0}^{n-1} v_i \Psi_i,$$

where  $u_i$  and  $v_i$  are variables over  $k$ , and for every constant  $a \in K$ , let

$$a = \sum_{i=0}^{n-1} a_i \Psi_i \quad a_i \in k.$$

Then the equation of  $C$  can be written in the form

$$\sum_{i=0}^{n-1} G_i(u_0, u_1, \dots, u_{n-1}, v_0, v_1, \dots, v_{n-1}) \Psi_i = 0.$$

We also extend  $\sigma$  to  $k[u_0, u_1, \dots, u_{n-1}, v_0, v_1, \dots, v_{n-1}]$  such that it applies trivially. We then get the variety  $\mathcal{A}$  over  $k$  given by:

$$\mathcal{A} : \begin{cases} G_0(u_0, u_1, \dots, u_{n-1}, v_0, v_1, \dots, v_{n-1}) = 0 & \sigma(u_0) = u_0 & \sigma(v_0) = v_0 \\ G_1(u_0, u_1, \dots, u_{n-1}, v_0, v_1, \dots, v_{n-1}) = 0 & \sigma(u_1) = u_1 & \sigma(v_1) = v_1 \\ \vdots & \vdots & \vdots \\ G_{n-1}(u_0, u_1, \dots, u_{n-1}, v_0, v_1, \dots, v_{n-1}) = 0 & \sigma(u_{n-1}) = u_{n-1} & \sigma(v_{n-1}) = v_{n-1}. \end{cases}$$

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

### 3.1 Varieties

**Lemma 1:** Variety  $\mathcal{A}$  (over  $k$ ) is birationally equivalent to variety  $\mathcal{B}$  over  $K$  defined by

$$\mathcal{B} : \begin{cases} y_0^r = \sigma^0(f)(x_0) & \sigma(x_0) = x_1 & \sigma(y_0) = y_1 \\ y_1^r = \sigma^1(f)(x_1) & \sigma(x_1) = x_2 & \sigma(y_1) = y_2 \\ \vdots & \vdots & \vdots \\ y_{n-2}^r = \sigma^{n-2}(f)(x_{n-2}) & \sigma(x_{n-2}) = x_{n-1} & \sigma(y_{n-2}) = y_{n-1} \\ y_{n-1}^r = \sigma^{n-1}(f)(x_{n-1}) & \sigma(x_{n-1}) = x_0 & \sigma(y_{n-1}) = y_0 \end{cases} .$$

Proof: 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  $u_0, u_1, \dots, u_{n-1}$  and  $v_0, v_1, \dots, v_{n-1}$ .

Let  $x_0 = X$  and  $y_0 = Y$ . Then

$$\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{bmatrix} = T \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix} = T \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_{n-1} \end{bmatrix}$$

since

$$x_i = \sigma^i(x_0) = \sigma^i(X) = u_0 \sigma^i(\Psi_0) + u_1 \sigma^i(\Psi_1) + \dots + u_{n-1} \sigma^i(\Psi_{n-1})$$

and

$$y_i = \sigma^i(y_0) = \sigma^i(Y) = v_0 \sigma^i(\Psi_0) + v_1 \sigma^i(\Psi_1) + \dots + v_{n-1} \sigma^i(\Psi_{n-1}).$$

For every  $i$ , we have

$$\sigma^i(Y^r - f(X)) = y_i^r - \sigma^i(f)(x_i)$$

and

$$Y^r - f(X) = \sum_{i=0}^{n-1} G_i(u_0, u_1, \dots, u_{n-1}, v_0, v_1, \dots, v_{n-1}) \Psi_i,$$

so

$$\begin{aligned} T \begin{bmatrix} G_0(u_0, \dots, u_{n-1}, v_0, \dots, v_{n-1}) \\ G_1(u_0, \dots, u_{n-1}, v_0, \dots, v_{n-1}) \\ \vdots \\ G_{n-1}(u_0, \dots, u_{n-1}, v_0, \dots, v_{n-1}) \end{bmatrix} &= \begin{bmatrix} \sum_{j=0}^{n-1} G_j(u_0, \dots, u_{n-1}, v_0, \dots, v_{n-1}) \sigma^0(\Psi_j) \\ \sum_{j=0}^{n-1} G_j(u_0, \dots, u_{n-1}, v_0, \dots, v_{n-1}) \sigma^1(\Psi_j) \\ \vdots \\ \sum_{j=0}^{n-1} G_j(u_0, \dots, u_{n-1}, v_0, \dots, v_{n-1}) \sigma^{n-1}(\Psi_j) \end{bmatrix} \\ &= \begin{bmatrix} \sigma^0 \left( \sum_{j=0}^{n-1} G_j(x_0, \dots, x_{n-1}, y_0, \dots, y_{n-1}) \Psi_j \right) \\ \sigma^1 \left( \sum_{j=0}^{n-1} G_j(x_0, \dots, x_{n-1}, y_0, \dots, y_{n-1}) \Psi_j \right) \\ \vdots \\ \sigma^{n-1} \left( \sum_{j=0}^{n-1} G_j(x_0, \dots, x_{n-1}, y_0, \dots, y_{n-1}) \Psi_j \right) \end{bmatrix} \end{aligned}$$

$$= \begin{bmatrix} y_0^r - \sigma^0(f)(x_0) \\ y_1^r - \sigma^1(f)(x_1) \\ \vdots \\ y_{n-1}^r - \sigma^{n-1}(f)(x_{n-1}) \end{bmatrix},$$

hence  $T$  applied to the equations of  $\mathcal{A}$  gives the equations of  $\mathcal{B}$ . Q.E.D.

We remove the conditions  $\sigma(x_i) = x_{i+1}$ ,  $\sigma(y_i) = y_{i+1}$  ( $i \in \{0, 1, \dots, n-2\}$ ),  $\sigma(x_{n-1}) = x_0$  and  $\sigma(y_{n-1}) = y_0$  in variety  $\mathcal{B}$  (i.e. we make the  $x_i$ 's independent from each other and the  $y_i$ 's also independent from each other) to get variety  $\mathcal{C}$  defined by

$$\mathcal{C} : \begin{cases} y_0^r = \sigma^0(f)(x_0) \\ y_1^r = \sigma^1(f)(x_1) \\ \vdots \\ y_{n-1}^r = \sigma^{n-1}(f)(x_{n-1}) \end{cases}.$$

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

$$\mathcal{D} : \begin{cases} y_0^r = \sigma^0(f)(x) \\ y_1^r = \sigma^1(f)(x) \\ \vdots \\ y_{n-1}^r = \sigma^{n-1}(f)(x) \end{cases},$$

which is a curve over  $K$ .

**Lemma 2:** For  $j = 0, 1, \dots, n-1$ , let  $\overline{y_j}$  be a root of the equation

$$y_j^r = \sigma^j(f)(x).$$

If  $F = K(x, \overline{y_0}, \overline{y_1}, \dots, \overline{y_{n-1}})$ , then  $[F : K(x)] = r^m$  for some  $m \in \mathbb{N}$ ,  $F = K(x, \overline{y_0}, \overline{y_1}, \dots, \overline{y_{m-1}})$  and  $\mathcal{D}$  has an irreducible component with function field isomorphic to  $F$ .

*Proof:* This is a generalization to Kummer extensions of the proof of lemma 3 in [13]. The following is an outline of the argument:

Every extension  $K(x, \overline{y_j})/K(x)$  has prime degree  $r$  and is Galois over  $K(x)$  since the irreducible factors of  $f(X)$  (and hence those of  $\sigma^j(f)(X)$ ) are present to the power 1. Then there exists a minimal subset  $\{\overline{y_{j_1}}, \overline{y_{j_2}}, \dots, \overline{y_{j_m}}\}$  of the  $\overline{y_j}$ 's such that  $F = K(x, \overline{y_{j_0}}, \overline{y_{j_1}}, \dots, \overline{y_{j_{m-1}}})$ . Let  $I$  be the kernel of the homomorphism

$$\varphi : K[x, y_0, y_1, \dots, y_{n-1}] \rightarrow K[x, \overline{y_0}, \overline{y_1}, \dots, \overline{y_{n-1}}].$$

Then  $I$  is a prime ideal of dimension one (since  $K[x]$  has transcendence degree one over  $K$ ) generated by  $\{x, \overline{y_0}, \overline{y_1}, \dots, \overline{y_{n-1}}\}$ .  $I$  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  $F$ . To obtain  $F = K(x, \overline{y_0}, \overline{y_1}, \dots, \overline{y_{m-1}})$ , suppose that  $\overline{y_j} \in K(x, \overline{y_0}, \overline{y_1}, \dots, \overline{y_{j-1}})$ , i.e.  $\overline{y_j}^r$  can be written in the form

$$\overline{y_j}^r = Q(x)^r \prod_{i=0}^{j-1} (\overline{y_i}^r)^{c_i}$$

with  $Q(x)$  a rational function in  $K(x)$ . By applying  $\sigma$  we get

$$\begin{aligned}
\overline{y_{j+1}}^r &= \sigma(\overline{y_j}^r) \\
&= \sigma\left(Q(x)^r \prod_{i=0}^{j-1} (\overline{y_i}^r)^{c_i}\right) \\
&= \left(\sigma(Q)(x)\right)^r \prod_{i=0}^{j-1} (\overline{y_{i+1}}^r)^{c_i} \\
&= \left(\left(\sigma(Q)(x)\right)^r \prod_{i=1}^{j-1} (\overline{y_i}^r)^{c_{i-1}}\right) \left(Q(x)^r \prod_{i=0}^{j-1} (\overline{y_i}^r)^{c_i}\right)^{c_{j-1}} \\
&= \left(\sigma(Q)(x)Q(x)^{c_{j-1}}\right)^r \prod_{i=0}^{j-1} (\overline{y_i}^r)^{d_i}
\end{aligned}$$

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.  $\overline{y_{j+1}} \in K(x, \overline{y_0}, \overline{y_1}, \dots, \overline{y_{j-1}})$  and by induction so are all remaining  $\overline{y_i}$ 's. Then  $F$  can be obtained by adjoining to  $K$  the roots of the first  $m$  equations in  $\mathcal{D}$ . Q.E.D.

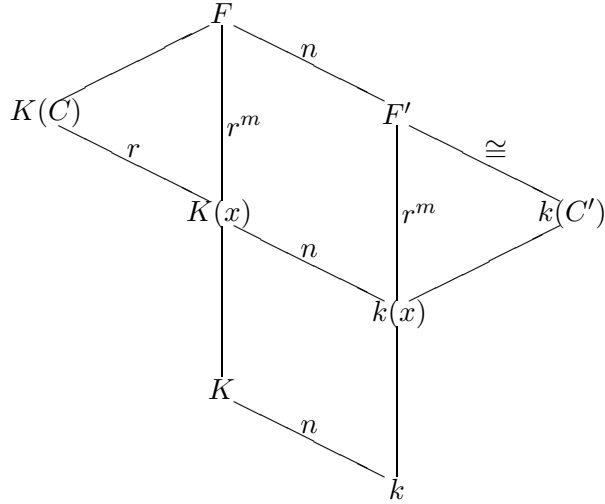
### 3.2 Fields

Let  $F$  be as in Lemma 2. Assume that  $\sigma$  can be extended from  $K$  to  $F$  with order  $n$ , via  $\sigma(\overline{y_i}) = \zeta_i \overline{y_{i+1}}$  ( $i \in \{0, 1, \dots, n-2\}$ ) and  $\sigma(\overline{y_{n-1}}) = \zeta_{n-1} \overline{y_0}$ , where the  $\zeta_i$ 's are  $r$ -th roots of unity (in  $k$  by condition 1) satisfying

$$\prod_{i=0}^{n-1} \zeta_i = 1.$$

In practice, we begin by setting  $\zeta_i = 1$  for  $i \in \{0, 1, \dots, m-1\}$  and compute  $\sigma^i(\overline{y_0})$  for  $i \in \{m, m+1, \dots, n\}$  (these are completely determined by the image under  $\sigma$  of  $\overline{y_0}, \overline{y_1}, \dots, \overline{y_{m-1}}$  by Lemma 2). If  $\sigma^n(\overline{y_0}) = \overline{y_0}$  (as will be the case for the curves considered in section 4),  $\sigma$  already has order  $n$  on  $F$ ; otherwise, we would have to look for a change of variable on the  $\overline{y_i}$ 's,  $i \in \{1, 2, \dots, m-1\}$  that would give  $\sigma^n(\overline{y_0}) = \overline{y_0}$ .

If  $\sigma$  commute with the Galois group of  $F$  over  $K(x)$ , let  $F'$  be the fixed field of  $F$  under  $\sigma$ . Then  $F'$  is an extension of degree  $r^m$  of  $k$  and we take it as the function field of  $C'$ . This gives us the following field diagram:



The following proposition will be useful to compute the genus of the various field extensions.

**Proposition 3:** *Suppose that  $\mathbb{F}'/\mathbb{F}$  is a finite separable extension of algebraic function fields having the same constant field  $\mathbb{K}$  such that  $\gcd([\mathbb{F}' : \mathbb{F}], \text{char}(\mathbb{K})) = 1$ . Let  $g$  (resp.  $g'$ ) denote the genus of  $\mathbb{F}/\mathbb{K}$  (resp.  $\mathbb{F}'/\mathbb{K}$ ). Then*

$$2g' - 2 = [\mathbb{F}' : \mathbb{F}](2g - 2) + \sum_{P \in \mathbb{P}_{\mathbb{F}}} \sum_{P' | P} (e(P'|P) - 1) \deg(P')$$

where  $e(P'|P)$  is the ramification index of  $P'$  and  $\mathbb{P}_{\mathbb{F}} = \{P | P \text{ is a place of } \mathbb{F}/\mathbb{K}\}$ .

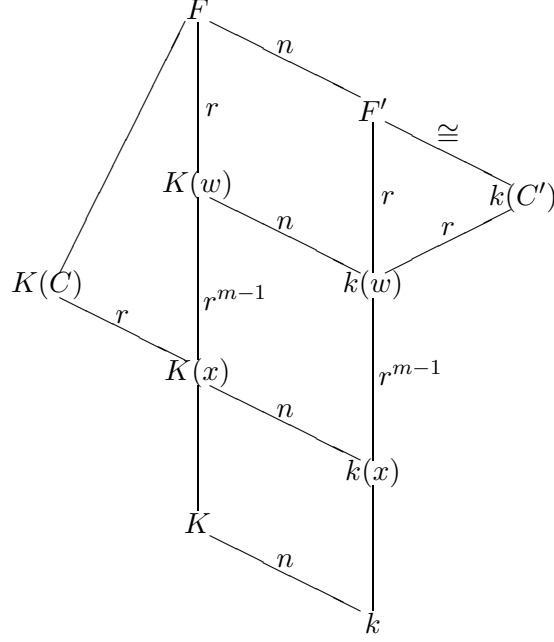
**Proof:** This is Hurwitz genus formula applied to the extensions considered in this paper. See [22] proposition III.5.6, page 95 for more details.

## 4 Rational function fields

The main idea used in the Gaudry, Hess and Smart attack (for elliptic curves over fields of characteristic 2) to obtain the equation of  $F'$  consisted in finding a subfield  $L$  of  $F$  such that  $[F : L] = 2$  and  $L$  is a rational function field of  $K$ , and then to restrict  $L$  to a rational function field  $L'$  over  $k$ . We follow the same idea for Kummer extensions.

First we will look at conditions under which there exists a rational function field  $L = K(w)$ ,  $K(x) \subset K(w) \subset F$ , with  $[F : K(w)] = r$ , such that  $K(w)$  is obtained from  $K(x)$  by adjoining combinations of the  $\overline{y}_i$ 's and  $F$  is obtained from  $K(w)$  by adjoining a single  $\overline{y}_i$  (by symmetry, we will assume that  $F = K(w, \overline{y}_0)$ ). Next, we will consider under which conditions the fixed field of  $K(w)$  under  $\sigma$  is a rational function field over  $k$ . Finally, we will show that if all the conditions obtained above are satisfied, then  $\sigma$  commutes with the galois group of  $F$  over  $K(w)$ , hence  $F = KF'$  (with  $F'$  the fixed field of  $F$  under  $\sigma$ ).

To do the second part, we will look at whether or not we can find a generator of  $K(w)$  over  $K$  which is fixed under  $\sigma$  (i.e. find  $w$  such that  $\sigma(w) = w$ ). When combined with the third part, it will give us the following field diagram:



**Theorem 4:** If  $L$  is a rational function field such that  $K(x) \subset L \subset F$  and  $F = L(\overline{y_0})$  where  $F$  is the function field obtained in Lemma 2, then either  $L$  is of the form

$$L = K(x, u) \quad \text{with} \quad u^r = \frac{x-b}{x-a}$$

with  $a, b \in K$  distinct (case  $m = 2$ ) or  $r = 2$  and  $L$  is of the form

$$L = K(x, u, v) \quad \text{with} \quad u^2 = \frac{x-b}{x-a} \quad \text{and} \quad v^2 = \frac{x-c}{x-a}$$

with  $a, b, c \in K$  distinct (case  $m = 3, r = 2$ ).

**Proof:** Let  $L$  be a subfield of  $F$  containing  $K(x)$  such that  $F = L(\overline{y_0})$  and assume that  $L$  is rational. Then  $L$  is obtained from  $K(x)$  by adjoining  $m-1$   $\overline{v_i}$ 's of the form

$$\overline{v_i} = \frac{\overline{y_0}}{\overline{y_{i_j}}} \quad \text{or} \quad \overline{v_i} = \frac{\overline{y_{i_j}}}{\overline{y_0}}.$$

Since curve  $C$  is nonsingular, so are the curves

$$y_i^r = \sigma^i(f)(x)$$

and the  $\overline{v_i}$ 's are roots of equations of the form  $v_i^r = h_i(x)$  where the  $h_i(x)$ 's are separable, and, by construction  $h_i(x) = \frac{p_1(x)}{p_2(x)}$  with  $p_1, p_2 \in K[x]$  and  $\deg(p_1) = \deg(p_2)$ . In order for  $L$  to be rational, then  $K(x, \overline{v_i})$  must have genus 0 for every  $i$ . The only places of  $K(x)$  which are ramified in  $K(x, \overline{v_i})$  are those over  $p_1(x)$  and  $p_2(x)$  and if  $P \in \mathbb{P}_{K(x)}$  is ramified, there is a unique  $P' \in \mathbb{P}_{K(x, \overline{v_i})}$  over  $P$  and  $e(P'|P) = r$ . Then Proposition 3 gives

$$0 = \text{genus}(K(x, \overline{v_i})/K) = 1 + r \cdot (0 - 1) + \frac{1}{2}(r-1)(\deg(p_1) + \deg(p_2))$$

which forces  $\deg(p_1) = \deg(p_2) = 1$  and  $h_i(x)$  is of the form

$$h_i(x) = \frac{x - a_{i,1}}{x - a_{i,2}}.$$

If there are 4 or more distinct  $a_j$ 's in the  $m - 1$   $h_i(x)$ 's, then  $L$  must contain  $K(x, v)$ , with

$$v^r = \frac{(x - b_1)(x - b_2)}{(x - b_3)(x - b_4)}$$

for some  $b_1, b_2, b_3$  and  $b_4$  among the  $a_j$ 's. However, the genus of  $K(x, v)$  would be then  $2(r - 1) > 0$  (using Proposition 3), which would contradict the hypothesis that  $L$  is rational. The only cases we need to consider are therefore isomorphic to  $L = K(x, u)$  ( $m = 2$ ) with

$$u^r = \frac{x - b}{x - a}$$

and  $L = K(x, u, v)$  ( $m = 3$ ) with

$$u^r = \frac{x - b}{x - a} \quad \text{and} \quad v^r = \frac{x - c}{x - a}$$

(obviously,  $a, b, c \in K$  are all distinct).

However, in the second case ( $L = K(x, u, v)$ ), the only places of  $K(x)$  which are ramified in  $L$  are  $(x - a)$ ,  $(x - b)$  and  $(x - c)$  and if  $P \in \mathbb{P}_{K(x)}$  is ramified, there are  $r$  distinct  $P' \in \mathbb{P}_L$  over  $P$  and  $e(P'|P) = r$ , hence

$$\text{genus}(L/K) = 1 + r^2 \cdot (0 - 1) + \frac{1}{2}(r - 1) \cdot 3r = (r - 1)(r - 2)/2$$

(using Proposition 3). Since we need the genus of  $L$  to be 0,  $r$  must be 2 in that case. Q.E.D.

## 5 Case $m = 2$

We let  $[F : L] = r$  and  $L = K(x, u)$  with  $u^r = \frac{x-b}{x-a}$ .

### 5.1 Curves and rational field $L$

By construction,  $\frac{\overline{y_0}}{\overline{y_1}} \in L = K(x, u)$ , and since  $\overline{y_0}^r = f(x)$ ,  $\overline{y_1}^r = \sigma(f)(x)$  with  $f(x)$  and  $\sigma(f)(x)$  separable ( $C$  is nonsingular), then, up to symmetry on the choice of  $a$  and  $b$ ,  $f(x)$  must be of the form

$$f(x) = h(x) \prod_{j=0}^i (x - \sigma^j(a))$$

where  $h(x)$  is fixed under  $\sigma$ ,  $a$  has order  $> i$  under  $\sigma$  and  $b = \sigma^{i+1}(a) \neq a$  (since  $\sigma(f)(x) = h(x) \prod_{j=1}^{i+1} (x - \sigma^j(a))$ ).

In order to get  $m = 2$ , it must be possible to write  $\sigma^2(f)(x)$  in terms of  $f(x)$ ,  $\sigma(f)(x)$  and factors to the power  $r$ . But  $\sigma^2(f)(x) = h(x) \prod_{j=2}^{i+2} (x - \sigma^j(a))$ , so  $\sigma^{i+1}(a) = a$  (otherwise  $(x - \sigma^{i+2}(a))$ , which has degree one in  $\sigma^2(f)(x)$ , would be absent from both  $f(x)$  and  $\sigma(f)(x)$ ).

If we assume that  $i \geq 1$ , then  $\sigma^2(f)(x)$  must be of the form  $f(x) \cdot \sigma(f)(x) \cdot Q(x)^r$  for some  $Q(x) \in K(x)$  since both  $(x - a)$  and  $(x - \sigma^{i+1}(a))$  are present with degree one in  $\sigma^2(f)(x)$ . Then

$Q(x)^r$  would have to contain all the irreducible factors of  $h(x)$  and/or  $(x - \sigma^2(a))$  (if  $i \geq 2$ ) to the power  $-1$ , which is impossible unless  $\deg(h) = 0$  and  $i = 1$ . But  $Q(x)^r$  must also contain  $(x - \sigma(a))$  to the power  $-2$ , which is impossible unless  $r = 2$ , forcing  $C$  to be of the form

$$Y^2 = h(X - a)(X - \sigma(a))$$

with  $h \in K$ , contradicting the assumption that  $C$  has genus greater than 0. Therefore  $i = 0$ ,  $a$  has order 2 under  $\sigma$  (so 2 divides  $n$ ) and  $f(x)$  is of the form

$$f(x) = (x - a)h(x)$$

with  $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$  and  $h(x) \in \mathbb{F}_q[x] = k[x]$ .

We can now set

$$u = \frac{y_1}{y_0},$$

which gives

$$\sigma(u) = \frac{y_0}{y_1} = \frac{1}{u} \quad \text{and} \quad \sigma^2(u) = u$$

hence  $\sigma$  extends to  $K(x, u)$  with order  $n$ . From

$$u^r = \frac{x - b}{x - a} = 1 - \frac{a - b}{x - a}$$

we get

$$x = a + \frac{a - b}{u^r - 1} = \frac{au^r - b}{u^r - 1}$$

hence  $K(x, u) = K(u)$ .

We summarize this in the following lemma:

**Lemma 5:** *The only curves for which  $[F : K(x)] = r^2$  and such that there exists a rational field  $L$  containing  $K(x)$  with  $[F : L] = r$  are of the form*

$$Y^r = (X - a)h(X).$$

*In this form,  $[K : k] = n$  with  $n$  divisible by 2,  $a \in K \setminus k$  is such that  $\sigma^2(a) = a$  and  $h(x) \in K[x]$  is defined over  $k$  and satisfies  $\gcd(h(x), x - a) = 1$ . In this case,*

$$L = K(u)$$

*with*

$$u^r = \frac{x - \sigma(a)}{x - a}$$

*and*

$$\sigma(u) = \frac{1}{u}.$$

## 5.2 Restriction and function fields

In order to compute the fixed field of  $K(u)$  under  $\sigma$ , we let

$$w = \frac{au + \sigma(a)}{u + 1}.$$

Then

$$\sigma(w) = \sigma\left(\frac{au + \sigma(a)}{u + 1}\right) = \frac{\sigma(a)\frac{1}{u} + a}{\frac{1}{u} + 1} = \frac{\sigma(a) + au}{1 + u} = w,$$

so  $w$  is fixed under  $\sigma$  and  $K(w) = K(u)$  since

$$u = \frac{\sigma(a) - w}{w - a}.$$

The fixed field of  $K(w)$  under  $\sigma$  is therefore  $k(w)$ , and, in terms of  $w$ ,  $x$  can be written as

$$x = \frac{a(\sigma(a) - w)^r - \sigma(a)(w - a)^r}{(\sigma(a) - w)^r - (w - a)^r}.$$

Since  $u = \frac{\bar{y}_1}{\bar{y}_0}$ , then  $\sigma(\bar{y}_0) = \bar{y}_1 = u\bar{y}_0$  and  $\sigma^2(\bar{y}_0) = \sigma(u\bar{y}_0) = \bar{y}_0$ , hence  $\sigma$  extends to  $F$  with order  $n$  (since 2 divides  $n$ ). If  $\tau$  is a generator of  $\text{Gal}(F/K(w))$ , then  $\tau(\bar{y}_0) = \zeta_r \bar{y}_0$  with  $\zeta_r$  a primitive  $r$ -th root of unity (which is in  $k$  by condition (1)) and

$$\sigma(\tau(\bar{y}_0)) = \sigma(\zeta_r \bar{y}_0) = \zeta_r \sigma(\bar{y}_0) = \zeta_r v \bar{y}_0 = v \tau(\bar{y}_0) = \tau(v \bar{y}_0) = \tau(\sigma(\bar{y}_0))$$

so  $\text{Gal}(F/K(w))$  commutes with  $\sigma$ .

**Theorem 6:** Let  $K = \mathbb{F}_{q^n}$ ,  $n$  even and  $C$  be a curve of genus  $g$  defined over  $K$  by

$$C : Y^r = (X - a)h(X)$$

where  $h(X) \in K[X]$  is defined over  $k$  and  $a \in K \setminus k$ ,  $\sigma^2(a) = a$ . Then the function field of  $C$  can be embedded in the function field of a curve  $C'$  of genus

$$g' = rg + \frac{(r-1)(r-2)}{2}$$

defined over  $k$  by the equation

$$\tilde{y}^r = (\eta + \sigma(\eta)u(w))^r (x(w) - a)h(x(w))$$

where  $\eta = \sum_{i=0}^{n/2-1} \sigma^{2i}(\mu)$  for some  $\mu \in K$  such that  $\text{Tr}_{K/k}(\mu) = 1$ .

Proof: Since  $\text{Gal}(F/K(w))$  commutes with  $\sigma$ , we have  $F = KF'$  (where  $F'$  is the fixed field of  $F$  under  $\sigma$ ), hence  $F'/k$  and  $F/K$  have the same genus  $g'$ .

We first consider  $g$ , the genus of  $K(C)/K$ . Since  $\gcd(\deg(h) + 1, r) = 1$ , the only places of  $K(x)$  which are ramified in  $K(C)$  are  $(x - a)$ , the place at infinity and the places over  $h(x)$ , and, if  $P \in \mathbb{P}_{K(x)}$  is ramified, there is a unique  $P' \in \mathbb{P}_{K(C)}$  over  $P$  and its ramification index is  $r$ . Then, using Proposition 3, we have

$$g' = 1 + r(0 - 1) + \frac{1}{2}(r-1)(\deg(h) + 2) = \frac{1}{2}(r-1)\deg(h),$$

so  $\deg(h) = 2g/(r-1)$ .

We can now compute  $g'$  in terms of  $g$ . The only places of  $K(x)$  which are ramified in  $F$  are  $(x-a)$ ,  $(x-\sigma(a))$ , the place at infinity and the places over  $h(x)$ , and, if  $P \in \mathbb{P}_{K(x)}$  is ramified, there are  $r$  distinct  $P' \in \mathbb{P}_{K(C)}$  over  $P$  and their ramification index is  $r$ . Then, from Proposition 3, the genus of  $F'/k$  (and  $F/K$ ) is

$$\begin{aligned} g' &= 1 + r^2(0-1) + \frac{1}{2}(r-1) \cdot r(\deg(h) + 3) \\ &= 1 - r^2 + \frac{1}{2}(r-1) \cdot r \left( \frac{2g}{r-1} + 3 \right) \\ &= rg + \frac{(r-1)(r-2)}{2} \end{aligned}$$

It remains to find an equation defining  $F'$  over  $L' = k(w)$ . Let  $\mu \in K$  such that  $Tr_{K/k} = 1$ , then  $F$  restrict to  $F'$  via the trace map. In particular,  $Tr_{F'/F'}(\mu w) = w$ , and  $Tr_{F'/F'}(\mu \epsilon) = \epsilon$  for every  $\epsilon \in k$ .

To simplify the notation, we let

$$\eta = \sum_{i=0}^{n/2-1} \sigma^{2i}(\mu),$$

so  $Tr_{K/k} = \eta + \sigma(\eta)$  and  $\sigma^2(\eta) = \eta$ . We now set

$$\begin{aligned} \tilde{y} &= Tr_{F'/F'}(\mu \bar{y}_0) \\ &= \sum_{i=0}^{n-1} \sigma^i(\mu \bar{y}_0) \\ &= \bar{y}_0 \sum_{i=0}^{n/2-1} \sigma^{2i}(\mu) + u \bar{y}_0 \sum_{i=0}^{n/2-1} \sigma^{2i+1}(\mu) \\ &= \eta \bar{y}_0 + \sigma(\eta) u \bar{y}_0 \\ &= (\eta + \sigma(\eta) u) \bar{y}_0 \end{aligned}$$

Then  $\tilde{y} \in F'$  and  $\tilde{y} \notin k(w)$  (since  $\bar{y}_0 \notin K(u) = K(w)$ ), hence  $F' = k(w, \tilde{y})$ . If we compute  $\tau(\tilde{y})$ , we have

$$\tau(\tilde{y}) = \tau((\eta + \sigma(\eta) u) \bar{y}_0) = (\eta + \sigma(\eta) u) \tau(\bar{y}_0) = \zeta_r (\eta + \sigma(\eta) u) \bar{y}_0 = \zeta_r \tilde{y}.$$

Then  $N_{F'/L'}(\tilde{y})$  is

$$\begin{aligned} N_{F'/L'}(\tilde{y}) &= \prod_{i=0}^{r-1} \tau^i(\tilde{y}) \\ &= \prod_{i=0}^{r-1} \zeta_r^i \tilde{y} \\ &= \zeta_r^{\frac{r(r-1)}{2}} \tilde{y}^r \\ &= \zeta_r^{\frac{r(r-1)}{2}} (\eta + \sigma(\eta) u)^r \bar{y}_0^r \\ &= \zeta_r^{\frac{r(r-1)}{2}} (\eta + \sigma(\eta) u)^r (x-a) h(x) \\ &= \zeta_r^{\frac{r(r-1)}{2}} (\eta + \sigma(\eta) u(w))^r (x(w) - a) h(x(w)) \end{aligned}$$

hence  $F'/k(w)$  is defined by the equation

$$\tilde{y}^r = (\eta + \sigma(\eta)u(w))^r (x(w) - a)h(x(w))$$

Q.E.D.

**Corollary 7:** *If curve  $C$  is nonsingular and defined over  $K$  by*

$$C : Y^r = (X - a)h(X) = (X - a) \sum_{i=0}^d h_i X^i$$

with  $h(X)$  defined over  $k(X)$  of degree  $d \equiv -2 \pmod{r}$  ( $C$  has genus  $g = (r-1)d/2$ ) and  $\sigma^2(a) = a$ , then  $F'$  is the function field of the nonsingular curve  $C''$  of genus  $g' = rg + (r-1)(r-2)/2 = (r-1)((d+1)r-2)/2$  defined over  $k$  by

$$Z^r = (a - \sigma(a))^{d+3} q(w) \sum_{i=0}^d h_i (a(w - \sigma(a))^r - \sigma(a)(w - a)^r)^i q(w)^{d-i}$$

where  $q(w) = (w - \sigma(a))^r - (w - a)^r$ .

Proof: Let  $\tilde{y}$  and  $\eta$  be as in Theorem 6. If we set

$$Q(w) = \frac{q(w)^{(d+2)/r} (a - \sigma(a))^{(d+2)/r}}{(\eta + \sigma(\eta)u(w))(w - a)} = \frac{((w - \sigma(a))^r - (w - a)^r)^{(d+2)/r} (a - \sigma(a))^{(d+2)/r}}{(\eta - \sigma(\eta))w - (\eta a - \sigma(\eta a))},$$

then

$$\begin{aligned} \sigma(Q(w)) &= \sigma \left( \frac{((w - \sigma(a))^r - (w - a)^r)^{(d+2)/r} (a - \sigma(a))^{(d+2)/r}}{(\eta - \sigma(\eta))w - (\eta a - \sigma(\eta a))} \right) \\ &= \frac{((w - a)^r - (w - \sigma(a))^r)^{(d+2)/r} (\sigma(a) - a)^{(d+2)/r}}{(\sigma(\eta) - \eta)w - (\sigma(\eta a) - \eta a)} \\ &= (-1)^{2((d+2)/r-1)} \frac{((w - \sigma(a))^r - (w - a)^r)^{(d+2)/r} (a - \sigma(a))^{(d+2)/r}}{(\eta - \sigma(\eta))w - (\eta a - \sigma(\eta a))} \\ &= Q(w), \end{aligned}$$

hence  $Q(w) \in k(w)$  and if we let  $Z = Q(w)\tilde{y}$ , then  $F' = k(w, \tilde{y}) = k(w, Z)$ . Since  $x(w) = (a(w - \sigma(a))^r - \sigma(a)(w - a)^r)/q(w)$ , we have

$$\begin{aligned} h(x(w)) &= \sum_{i=0}^d h_i x(w)^i = q(w)^{-d} \sum_{i=0}^d h_i x(w)^i q(w)^d \\ &= q(w)^{-d} \sum_{i=0}^d h_i (a(w - \sigma(a))^r - \sigma(a)(w - a)^r)^i q(w)^{d-i} \end{aligned}$$

and

$$(x(w) - a) = (a - \sigma(a))(w - a)^r / q(w),$$

hence

$$\begin{aligned}
Z^r &= Q(w)^r \tilde{y}^r \\
&= \frac{q(w)^{d+2} (a - \sigma(a))^{d+2}}{(\eta + \sigma(\eta)u(w))^r (w - a)^r} \tilde{y}^r \\
&= \frac{q(w)^{d+2} (a - \sigma(a))^{d+2}}{(\eta + \sigma(\eta)u(w))^r (w - a)^r} \cdot (\eta + \sigma(\eta)u(w))^r (x(w) - a) h(x(w)) \\
&= \frac{q(w)^{d+2} (a - \sigma(a))^{d+2}}{(w - a)^r} \cdot (x(w) - a) h(x(w)) \\
&= q(w)^{d+1} (a - \sigma(a))^{d+3} \cdot h(x(w)) \\
&= (a - \sigma(a))^{d+3} q(w) \cdot \sum_{i=0}^d h_i (a(w - \sigma(a))^r - \sigma(a)(w - a)^r)^i q(w)^{d-i}.
\end{aligned}$$

To show that  $C''$  is nonsingular, we first note that  $q(w) = r(a - \sigma(a))w^{r-1} + O(w^{r-2})$ , so  $Z^r$  is of the form

$$Z^r = h_d r (a - \sigma(a))^{d+1} w^{(d+1)r-1} + O(w^{(d+1)r-2}),$$

which has degree in  $w$  coprime to  $r$ , and by Proposition 3, the function field of the curve  $C''$  ( $k(w, Z)$ ) is

$$g' \leq (r - 1)((d + 1)r - 2)/2$$

with equality if and only if the curve is nonsingular. But, by Theorem 6,  $F' = k(w, Z)$  has genus  $rg + (r - 1)(r - 2)/2 = (r - 1)((d + 1)r - 2)/2$  over  $k$ , hence  $C''$  must be nonsingular. Q.E.D.

## 6 Case $m = 3$ , $r = 2$

If  $[F : L] = 2$  and  $L = K(x, u, v)$  with  $u^2 = \frac{x-b}{x-a}$  and  $v^2 = \frac{x-c}{x-a}$ , we will show that  $L'$  (the fixed field of  $K(w)$  under  $\sigma$ ) is not a rational function field over  $k(x)$ .

### 6.1 Curves

By construction,  $\frac{\bar{y}_0}{\bar{y}_1} \in L = K(x, u, v)$ , and since  $\bar{y}_0^r = f(x)$ ,  $\bar{y}_1^r = \sigma(f)(x)$  with  $f(x)$  and  $\sigma(f)(x)$  separable ( $C$  is nonsingular), then, up to symmetry on the choice of  $a$ ,  $b$  and  $c$ ,  $f(x)$  must be of the form

$$f(x) = h(x) \prod_{j=0}^i (x - \sigma^j(a))$$

where  $h(x)$  is fixed under  $\sigma$ ,  $a$  has order  $> i + 1$  under  $\sigma$  and  $\sigma^{i+1}(a)$  is equal to either  $b$  or  $c$ . Then

$$\begin{aligned}
\sigma(f)(x) &= h(x) \prod_{j=1}^{i+1} (x - \sigma^j(a)), \\
\sigma^2(f)(x) &= h(x) \prod_{j=2}^{i+2} (x - \sigma^j(a))
\end{aligned}$$

and

$$\sigma^3(f)(x) = h(x) \prod_{j=3}^{i+3} (x - \sigma^j(a))$$

We have two cases to consider depending on whether or not  $\sigma^{i+2}(a)$  is equal to  $a$ .

case 1:  $\sigma^{i+2}(a) \neq a$ . By construction,  $\frac{y_1}{y_2}$  must also be in  $L = K(x, u, v)$ , and since  $\overline{y_2}^r = \sigma^2(f)(x)$ , we have

$$\frac{\overline{y_1}^r}{\overline{y_2}^r} = \frac{\sigma(f)(x)}{\sigma^2(f)(x)} = \frac{(x - \sigma(a))}{(x - \sigma^{i+2}(a))}.$$

Then both  $\sigma(a)$  and  $\sigma^{i+2}(a)$  must be in  $\{a, b, c\}$ , but so are  $a$  and  $\sigma^{i+1}(a)$ . Since  $a$  has order  $> i + 2$  under  $\sigma$ , this is impossible unless  $\sigma(a) = \sigma^{i+1}(a)$ , i.e. if  $i = 0$ . Then  $f(x)$  is of the form

$$f(x) = (x - a)h(x)$$

and, up to symmetry on the choice of  $b$  and  $c$ , we have  $b = \sigma(a)$  and  $c = \sigma^2(a)$ . We can then set

$$u = \frac{y_1}{y_0} \quad \text{and} \quad v = \frac{y_2}{y_0}$$

hence

$$\sigma(u) = \frac{y_2}{y_1} = \frac{v}{u} \quad \text{and} \quad \sigma(v) = \frac{y_0}{y_1} = \frac{1}{u}$$

In order to get  $m = 3$ , it must be possible to write  $\sigma^3(f)(x)$  in terms of  $f(x)$ ,  $\sigma(f)(x)$ ,  $\sigma^2(f)(x)$  and factors to the power 2. Since  $\sigma^3(f)(x) = (x - \sigma^3(a))h(x)$ ,  $\sigma^3(a)$  must be in  $\{a, b, c\} = \{a, \sigma(a), \sigma^2(a)\}$ . But  $\sigma^3(a)$  can be neither  $\sigma(a)$  nor  $\sigma^2(a)$  since  $a$  has order  $> i + 2 = 2$  under  $\sigma$ , hence  $\sigma^3(a) = a$ .

case 2:  $\sigma^{i+2}(a) = a$ . If  $i$  was equal to 0, we would have  $m = 2$  (see section 5), hence  $i$  must be at least 1. In order to get  $m = 3$ , it must be possible to write  $\sigma^3(f)(x)$  in terms of  $f(x)$ ,  $\sigma(f)(x)$ ,  $\sigma^2(f)(x)$  and factors to the power 2. Note that in this case,  $(x - \sigma^{i+2}(a)) = (x - a)$  and  $(x - \sigma^{i+3}(a)) = (x - \sigma(a))$ .

Since  $(x - a)$  has power 1 in  $f(x)$ ,  $\sigma^2(f)(x)$  and  $\sigma^3(f)(x)$  and power 0 in  $\sigma(f)(x)$ , then only one of  $f(x)$  and  $\sigma^2(f)(x)$  can be used in constructing  $\sigma^3(f)(x)$ . Similarly,  $(x - \sigma(a))$  has power 1 in  $f(x)$ ,  $\sigma(f)(x)$  and  $\sigma^3(f)(x)$  and power 0 in  $\sigma^2(f)(x)$ , so only one of  $f(x)$  and  $\sigma(f)(x)$  can be used in constructing  $\sigma^3(f)(x)$ . The only possible options are then  $\sigma^3(f)(x) = \sigma(f)(x) \cdot \sigma^2(f)(x) \cdot Q(x)^2$  or  $\sigma^3(f)(x) = f(x) \cdot Q(x)^2$ , with  $Q(x) \in K(x)$ .

If  $\sigma^3(f)(x) = \sigma(f)(x) \cdot \sigma^2(f)(x) \cdot Q(x)^2$ , then  $\sigma^3(f)(x)$  would have to be equal to  $(x - a)(x - \sigma(a))$  (since  $\sigma^3(f)(x)$  is separable and any other factor would be to a power divisible by 2). This would force  $\sigma^3(f)(x) = f(x)$  (since they are both polynomials of the same degree in  $K[x]$  and  $f(x)$  also has  $(x - a)$  and  $(x - \sigma(a))$  as factors). But the curve  $Y^2 = f(X)$  would then have genus 0, which contradicts the assumption that  $C$  has genus  $\geq 1$ .

The only possibility is therefore  $\sigma^3(f)(x) = f(x) \cdot Q(x)^2$  for some  $Q(x) \in K(x)$ . If  $i$  is greater than 1, we get

$$Q(x)^2 = \frac{f(x)}{\sigma^3(f)(x)} = \frac{h(x) \prod_{j=0}^i (x - \sigma^j(a))}{h(x) \prod_{j=3}^{i+3} (x - \sigma^j(a))} = \frac{(x - \sigma^2(a))}{(x - \sigma^{i+1}(a))}$$

which is impossible since  $\frac{(x-\sigma^2(a))}{(x-\sigma^{i+1}(a))}$  is not a square in  $K(x)$  for  $i > 1$ , hence  $i$  must be equal to 1,  $\sigma^3(a) = a$  and  $f(x)$  is of the form

$$f(x) = (x - a)(x - \sigma(a))h(x).$$

Up to symmetry on the choice of  $b$  and  $c$ , we have  $b = \sigma(a)$  and  $c = \sigma^2(a)$ . We can then set

$$u = \frac{y_1}{y_2} \quad \text{and} \quad v = \frac{y_1}{y_0},$$

hence

$$\sigma(u) = \frac{y_2}{y_0} = \frac{v}{u} \quad \text{and} \quad \sigma(v) = \frac{y_2}{y_1} = \frac{1}{u}.$$

We summarize these arguments in the following lemma:

**Lemma 8:** *The only curves for which  $[F : K(x)] = 2^3$  and such that there exists a field  $L$  of genus 0 containing  $K(x)$  with  $[F : L] = 2$  are of the form*

$$Y^2 = (X - a)h(X)$$

or of the form

$$Y^2 = (X - a)(X - \sigma(a))h(X)$$

For both forms,  $[K : k] = n$  with  $n$  divisible by 3,  $a \in K \setminus k$  is such that  $\sigma^3(a) = a$  and  $h(x) \in K[x]$  is defined over  $k$  and satisfies  $\gcd(h(x), x - a) = 1$ . In both cases,

$$L = K(u, v)$$

with

$$u^2 = \frac{x - \sigma(a)}{x - a} \quad \text{and} \quad v^2 = \frac{x - \sigma^2(a)}{x - a}$$

and

$$\sigma(u) = \frac{v}{u} \quad \text{and} \quad \sigma(v) = \frac{1}{u}.$$

## 6.2 Rational field $L$

From  $u^2 = \frac{x-b}{x-a}$ , we have  $x = a + \frac{a-b}{u^2-1}$ , hence  $K(x, u, v) = K(u, v)$ . Also, using  $v^2 = \frac{x-c}{x-a}$ , we have  $x = a + \frac{a-c}{v^2-1}$ , so

$$\begin{aligned} \frac{a-c}{v^2-1} = \frac{a-b}{u^2-1} &\Rightarrow v^2-1 = \frac{a-c}{a-b}(u^2-1) \\ &\Rightarrow v^2 = \frac{a-c}{a-b} \left( u^2 - 1 + \frac{a-b}{a-c} \right) \\ &\Rightarrow v^2 = \frac{a-c}{a-b} \left( u^2 + \frac{c-b}{a-c} \right) \end{aligned}$$

Using  $b = \sigma(a) \neq a$ ,  $c = \sigma^2(a)$  and  $\sigma^3(a) = a$ , we get

$$\begin{aligned}
v^2 &= \frac{a-c}{a-b} \left( u^2 + \frac{c-b}{a-c} \right) \\
&= \frac{\sigma^2(b) - \sigma^2(a)}{a-b} \left( u^2 + \frac{\sigma(b) - \sigma(a)}{\sigma^2(b) - \sigma^2(a)} \right) \\
&= -\frac{\sigma^2(a-b)}{a-b} \left( u^2 + \frac{\sigma(a-b)}{\sigma^2(a-b)} \right) \\
&= -\frac{(a-b)^{q^2}}{a-b} \left( u^2 + \frac{(a-b)^q}{(a-b)^{q^2}} \right)
\end{aligned}$$

Since  $\gcd(r, p) = \gcd(2, p) = 1$ ,  $q = p^l$  is odd and we can set

$$\gamma = \frac{1}{(a-b)^{(q^2-q)/2}}, \quad \delta = \sigma(\gamma) \quad \text{and} \quad \rho = \sigma^2(\gamma)$$

which gives us

$$v^2 = -\delta^2(u^2 + \gamma^2)$$

Note that by construction of  $\gamma$ ,  $\delta$  and  $\rho$  we have

$$\gamma^2 \delta^2 \rho^2 = \frac{(a-b)^q}{(a-b)^{q^2}} \cdot \frac{(a-b)^{q^2}}{(a-b)} \cdot \frac{(a-b)}{(a-b)^q} = 1$$

hence the product  $\gamma\delta\rho$  is in  $k$  and is either 1 or  $-1$ .

We use two methods to find a generator  $z$  of  $K(u, v)$  over  $K$ . If  $K$  has a primitive fourth root of unity  $\zeta$  (if  $q^n \equiv 1 \pmod{4}$ ), then  $v^2 = -\delta^2(u - \zeta\gamma)(u + \zeta\gamma)$  and we can look at

$$z^2 = \left( \frac{v}{\delta(u - \zeta\gamma)} \right)^2 = -(u + \zeta\gamma)$$

On the other hand, if we can find two nonzero elements  $\beta$  and  $\eta$  in  $K$  such that  $\eta^2 + \beta^2 + 1 = 0$ , then  $(u_0, v_0) = (\gamma\beta, \gamma\delta\eta)$  is a point on  $v^2 = -\delta^2(u^2 + \gamma^2)$  and we look at the projection from  $(u_0, v_0)$  of  $(u, v)$  on the line  $\left( z, -\frac{\delta\beta}{\eta}z \right)$  (a parallel of the tangent to  $v^2 + \delta^2u^2 + \delta^2\gamma^2 = 0$  at  $(u_0, v_0)$ ). the following lemma show that these two method are sufficient to deal with every finite field of odd characteristic (since if  $p \equiv 1 \pmod{4}$ ,  $\mathbb{F}_p$  has a primitive fourth root of unity).

**Lemma 9:** *If  $p \equiv 3 \pmod{4}$ , then there exists at least one pair  $\beta, \eta \in \mathbb{F}_p \setminus \{0\}$  such that  $\eta^2 + \beta^2 + 1 = 0$ .*  
**Proof:** To find a pair  $\beta, \eta \in \mathbb{F}_p$  such that  $\eta^2 + \beta^2 + 1 = 0$ , we look for  $\alpha \in \mathbb{F}_p$  such that  $\alpha$  is a quadratic residue modulo  $p$  and  $\alpha + 1$  is a quadratic nonresidue (such an  $\alpha$  must exist since 1 is a quadratic residue and  $p - 1$  is quadratic nonresidue). Then, by quadratic reciprocity,  $-(\alpha + 1)$  must be a quadratic residue (since  $-1$  is a quadratic nonresidue) and we can therefore choose  $\beta$  to be a square root of  $\alpha$  in  $\mathbb{F}_p$  and  $\eta$  to be a square root of  $-(\alpha + 1)$  in  $\mathbb{F}_p$ , giving us  $\eta^2 = -(\beta^2 + 1)$ . Q.E.D.

In order to simplify the computation of  $\sigma(z)$ , we will require that  $\zeta$ ,  $\beta$  and  $\eta$  (if they are used) be in the field  $k$ , i.e. such that  $\sigma(\zeta) = \zeta$ ,  $\sigma(\beta) = \beta$  and  $\sigma(\eta) = \eta$ . The construction of  $z$  is divided into the following 3 cases:

1. If  $q \equiv 1$  or  $7 \pmod{12}$  (i.e.  $q \equiv 1 \pmod{6}$ ): We let  $\beta$  be a root of  $T^2 + (\gamma\delta\rho)T + 1$ , i.e.  $\beta$  is a primitive cube root of unity if  $\gamma\delta\rho = 1$  and a primitive sixth root of unity if  $\gamma\delta\rho = -1$  (these exist in  $k$  since  $q - 1$  is divisible by 6). We use the second method to construct  $z$  (projection) with  $\eta = \beta^2$ . We can then set

$$z = \frac{\beta^3\gamma(v - \beta\delta u)}{\beta^2v + \beta\delta u + \gamma\delta}$$

which gives

$$u = \beta\gamma + \frac{2\beta^4\gamma^2(z - \beta\gamma)}{z^2 + \beta^4\gamma^2} \quad \text{and} \quad v = \beta^2\gamma\delta - \frac{2\beta^3\gamma^2\delta(z + \beta^3\gamma)}{z^2 + \beta^4\gamma^2}$$

2. If  $q \equiv 5 \pmod{12}$ : We let  $\zeta$  be a primitive fourth root of unity (exists in  $k$  since  $q - 1$  is divisible by 4), and we can set

$$z = \frac{v}{\delta(u - \zeta\gamma)}$$

which gives

$$u = \zeta\gamma - \frac{2\zeta\gamma}{z^2 + 1} \quad \text{and} \quad v = -\frac{2\zeta\gamma\delta z}{z^2 + 1}$$

3. If  $q \equiv 11 \pmod{12}$  (in particular,  $p \equiv 11 \pmod{12}$ ): Using Lemma 9, we can find  $\beta$  and  $\eta$  in  $k$  such that  $\eta^2 + \beta^2 + 1 = 0$ , we can then set

$$z = \frac{\eta\gamma(\beta v - \eta\delta u)}{\eta v + \beta\delta u + \gamma\delta}$$

which gives

$$u = \beta\gamma + \frac{2\eta^2\gamma^2(z - \beta\gamma)}{z^2 + \eta^2\gamma^2} \quad \text{and} \quad v = \eta\gamma\delta - \frac{2\eta\gamma^2\delta(\beta z + \eta^2\gamma)}{z^2 + \eta^2\gamma^2}$$

Note: although  $p \equiv 1 \pmod{12}$  could also be handled in case 2, we use case 1 since finding a generator of  $K(z)$  over  $K$  fixed under  $\sigma$  will be more straightforward in that case.

Since  $\sigma^3(u) = \sigma^2(v/u) = \sigma(1/v) = u$  and  $\sigma^3(v) = v$ , then  $\sigma$  extends with order  $n$  in  $K(u, v)$  ( $3$  divides  $n$ ), hence  $\sigma$  extends with order  $n$  in  $K(z)$  for all three cases.

### 6.3 Restrictions

To prove that the fixed field under  $\sigma$  of  $L = K(z)$  is rational over  $k$ , we first prove the three following lemmas:

**Lemma 10:** *The polynomial  $T^{q+1} + T + 1 \in \mathbb{F}_q[T]$  splits over  $\mathbb{F}_{q^3}$  and if  $\epsilon_0$  is one of its roots, then  $\epsilon_0$  satisfies  $\epsilon_0\sigma(\epsilon_0)\sigma^2(\epsilon_0) = 1$ . If  $q \equiv 5 \pmod{6}$ , then  $\epsilon_0 \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ .*

**Proof:** Let  $\epsilon_0$  be a root of  $T^{q+1} + T + 1 = 0$  in  $\overline{\mathbb{F}_q}$ . Then  $\epsilon_0 \neq 0$  and  $\sigma(\epsilon_0) = -1 - \frac{1}{\epsilon_0} = -\frac{1+\epsilon_0}{\epsilon_0}$  (since  $\epsilon_0^{q+1} = \sigma(\epsilon_0) \cdot \epsilon_0$ ). We also have  $\sigma^2(\epsilon_0) = -1 - \frac{1}{\sigma(\epsilon_0)} = -\frac{1}{1+\epsilon_0}$ , which gives

$$\epsilon_0\sigma(\epsilon_0)\sigma^2(\epsilon_0) = \epsilon_0 \cdot \frac{-(1+\epsilon_0)}{\epsilon_0} \cdot \frac{-1}{1+\epsilon_0} = 1$$

and

$$\sigma^3(\epsilon_0) = \sigma\left(\frac{-1}{1+\epsilon_0}\right) = \frac{-1}{1-\frac{1+\epsilon_0}{\epsilon_0}} = \epsilon_0,$$

hence  $\epsilon_0 \in \mathbb{F}_{q^3}$ . If  $\epsilon_0$  is in  $\mathbb{F}_q$ , it must satisfy  $\epsilon_0^2 + \epsilon_0 + 1 = 0$ , so  $\epsilon_0$  must be a primitive cube root of unity, which is impossible if  $q \equiv 5 \pmod{6}$ . Q.E.D.

**Lemma 11:** *Let  $L = K(z)$  with  $\sigma(z) = \frac{a_1z+b_1}{a_2z+b_2} \notin K$  and  $a_2 \neq 0$  and suppose that the polynomial  $a_2T^{q+1} - b_2T^q + a_1T - b_1$  has at least one root  $\epsilon \in K$ . Then  $L = K(\hat{z})$  with  $\hat{z} = \frac{1}{z+\epsilon}$  satisfying  $\sigma(\hat{z}) = \hat{A}\hat{z} + \hat{B}$  with  $\hat{A} = \frac{b_2-a_2\epsilon}{a_2\sigma(\epsilon)+a_1} \neq 0$  and  $\hat{B} = \frac{a_2}{a_2\sigma(\epsilon)+a_1}$ .*

**Proof:** Let  $\epsilon \in K$  be a root of  $a_2T^{q+1} - b_2T^q + a_1T - b_1$ , then  $(a_2\sigma(\epsilon) + a_1)\epsilon - (b_2\sigma(\epsilon) + b_1) = 0$ , so  $a_2\sigma(\epsilon) + a_1 \neq 0$  (otherwise we would have  $\sigma(z) \in K$ ) and we have

$$\frac{b_2\sigma(\epsilon) + b_1}{a_2\sigma(\epsilon) + a_1} = \epsilon$$

Also,  $(b_2 - a_2\epsilon)\sigma(\epsilon) + (b_1 - a_1\epsilon) = 0$ , so  $b_2 - a_2\epsilon \neq 0$  (otherwise we would have  $\sigma(z) \in K$ ). We let  $\hat{z} = \frac{1}{z+\epsilon}$ , then we have:

$$\begin{aligned} \sigma(\hat{z}) &= \sigma\left(\frac{1}{z+\epsilon}\right) \\ &= \frac{1}{\frac{a_1z+b_1}{a_2z+b_2} + \sigma(\epsilon)} \\ &= \frac{a_2z + b_2}{(a_1z + b_1) + \sigma(\epsilon)(a_2z + b_2)} \\ &= \frac{a_2z + b_2}{(a_2\sigma(\epsilon) + a_1)z + (b_2\sigma(\epsilon) + b_1)} \\ &= \frac{1}{a_2\sigma(\epsilon) + a_1} \left( \frac{a_2z + b_2}{z + (b_2\sigma(\epsilon) + b_1)/(a_2\sigma(\epsilon) + a_1)} \right) \\ &= \frac{1}{a_2\sigma(\epsilon) + a_1} \left( \frac{a_2z + b_2}{z + \epsilon} \right) \\ &= \frac{b_2 - a_2\epsilon}{a_2\sigma(\epsilon) + a_1} \left( \frac{1}{z + \epsilon} \right) + \frac{a_2}{a_2\sigma(\epsilon) + a_1} \\ &= \hat{A}\hat{z} + \hat{B} \end{aligned}$$

where  $\hat{A} \neq 0$ , i.e.  $\sigma(\hat{z})$  is linear in  $\hat{z}$ . Q.E.D.

**Lemma 12:** *If  $\sigma(\hat{z}) = \hat{A}\hat{z} + \hat{B}$  with  $\hat{A}\sigma(\hat{A})\sigma^2(\hat{A}) = 1$ , then there exists  $A, B \in K$  such that  $\sigma(A\hat{z}) = A\hat{z} + B$ .*

**Proof:** In order to have  $\sigma(A\hat{z}) = A\hat{z} + B$ , we must have  $\sigma(A)\hat{A} = A$  (since  $\sigma(A\hat{z}) = \sigma(A)\hat{A}\hat{z} + \sigma(A)\hat{B}$ ), i.e.  $A$  is a root of the polynomial  $\hat{A}T^q - T$ . Let  $\alpha$  be any root of  $\hat{A}T^q - T$  over  $\overline{\mathbb{F}_q}$ , then  $\alpha = \sigma(\alpha)\hat{A}$ . This also gives us  $\sigma(\alpha) = \sigma^2(\alpha)\sigma(\hat{A})$  and  $\sigma^2(\alpha) = \sigma^3(\alpha)\sigma^2(\hat{A})$ , hence  $\alpha = \hat{A}\sigma(\hat{A})\sigma^2(\hat{A})\sigma^3(\alpha)$ . But  $\hat{A}\sigma(\hat{A})\sigma^2(\hat{A}) = 1$  by hypothesis, hence  $\sigma^3(\alpha) = \alpha$ , i.e.  $\alpha \in \mathbb{F}_{q^3} \subset K$ . Q.E.D.

We can now prove the following theorem:

**Theorem 13:**  *$L'$ , the fixed field of  $L = K(z)$  under  $\sigma$ , is rational over  $k$  and  $L = K(w)$ ,  $L' = k(w)$  for some  $w$  fixed under  $\sigma$ .*

**Proof:** To do this, we first find a generator  $\hat{z}$  of  $L$  over  $K$  such that  $\sigma(\hat{z}) = \hat{A}\hat{z} + \hat{B}$  (i.e.  $\hat{z}$  is linear in  $\hat{z}$ ), then find a constant  $A$  such that  $\sigma(A\hat{z}) = A\hat{z} + B$  for some  $B \in K$ . If  $\mu \in K$  is such that  $Tr_{K/k}(\mu) = 1$ , we can then find a generator  $w$  of  $L$  over  $K$  by computing

$$w = \sum_{i=0}^{n-1} \sigma^i(\mu A \hat{z})$$

To obtain  $\hat{z}$  and  $A$ , we have the three following cases (depending on the construction of  $z$ ):

1. If  $q \equiv 1$  or  $7 \pmod{12}$ : Using  $\sigma(\beta) = \beta$ ,  $\beta^2 + \gamma\delta\rho\beta + 1 = 0$  and  $\gamma^2\delta^2\rho^2 = 1$  to simplify when convenient, we get

$$\begin{aligned} \sigma(z) &= \sigma\left(\frac{\beta^3\gamma(v - \beta\delta u)}{\beta^2v + \beta\delta u + \gamma\delta}\right) \\ &= \frac{\beta^3\delta\left(\frac{1}{u} - \beta\rho\frac{v}{u}\right)}{\beta^2\frac{1}{u} + \beta\rho\frac{v}{u} + \delta\rho} \\ &= \frac{\beta^3\delta - \beta^4\delta\rho v}{\beta^2 + \beta\rho v + \delta\rho u} \\ &= \frac{\beta^3\delta - \beta^4\delta\rho\left(\beta^2\gamma\delta - \frac{2\beta^3\gamma^2\delta(z + \beta^3\gamma)}{z^2 + \beta^4\gamma^2}\right)}{\beta^2 + \beta\rho\left(\beta^2\gamma\delta - \frac{2\beta^3\gamma^2\delta(z + \beta^3\gamma)}{z^2 + \beta^4\gamma^2}\right) + \delta\rho\left(\beta\gamma + \frac{2\beta^4\gamma^2(z - \beta\gamma)}{z^2 + \beta^4\gamma^2}\right)} \\ &= \beta\delta^2\rho z + \delta\rho \end{aligned}$$

and we can set  $\hat{z} = z$  and  $\hat{A} = \beta\delta^2\rho$ . Since

$$\hat{A}\sigma(\hat{A})\sigma^2(\hat{A}) = (\beta\delta^2\rho)(\beta\gamma\rho^2)(\beta\gamma^2\delta) = \beta^3\gamma\delta\rho = 1,$$

there exists  $A, B \in K$  such that  $\sigma(A\hat{z}) = A\hat{z} + B$  (Lemma 12).

2. If  $q \equiv 5 \pmod{12}$ : Using  $\sigma(\zeta) = \zeta$ ,  $\zeta^2 = -1$  and  $\gamma^2\delta^2\rho^2 = 1$  to simplify when convenient, we get

$$\begin{aligned} \sigma(z) &= \sigma\left(\frac{v}{\delta(u - \zeta\gamma)}\right) \\ &= \frac{\frac{1}{u}}{\rho\left(\frac{v}{u} - \zeta\delta\right)} \\ &= \frac{1}{\rho(v - \zeta\delta u)} \\ &= \frac{1}{\rho\left(\left(-\frac{2\zeta\gamma\delta z}{z^2+1}\right) - \zeta\delta\left(\zeta\gamma - \frac{2\zeta\gamma}{z^2+1}\right)\right)} \\ &= -\frac{z^2 + 1}{\zeta\gamma\delta\rho(\zeta z^2 + 2z - \zeta)} \end{aligned}$$

and since the gcd of the numerator and the denominator is  $(z - \zeta)$ , we get

$$\sigma(z) = \frac{z + \zeta}{-\zeta^2\gamma\delta\rho z + \zeta^3\gamma\delta\rho}$$

In order to use Lemma 11, we need to find a root of  $P(t) = (-\zeta^2\gamma\delta\rho)t^{q+1} - (\zeta^3\gamma\delta\rho)t^q + t - \zeta$  in  $K$ . If we substitute  $t$  by  $(\gamma\delta\rho - \zeta)t_0 - \zeta$  in  $P(t)$ , this is equivalent to finding a root of  $t_0^{q+1} + t_0 + 1$  in  $K$ . Then, using Lemma 10, all the roots  $\epsilon$  of  $P(t)$  are of the form  $(\gamma\delta\rho - \zeta)\epsilon_0 - \zeta$  with  $\epsilon_0 \in K$  a root of  $t_0^{q+1} + t_0 + 1$ . Then, from Lemma 11,  $\hat{A} = \frac{-\epsilon_0}{\sigma(\epsilon_0)+1} = \epsilon_0^2$ . Since  $\hat{A}\sigma(\hat{A})\sigma^2(\hat{A}) = (\epsilon_0\sigma(\epsilon_0)\sigma^2(\epsilon_0))^2 = 1$  (by Lemma 10), Lemma 12 shows that there exists  $A, B \in K$  such that  $\sigma(A\hat{z}) = A\hat{z} + B$ .

3. If  $q \equiv 11 \pmod{12}$ : We first note that (after simplification)

$$(\beta\eta + \eta\gamma\delta\rho + \beta)(\beta\eta - \eta\gamma\delta\rho + \beta) = -(\eta^2 + \eta + 1)^2$$

hence  $\beta\eta + \eta\gamma\delta\rho + \beta \neq 0$  since  $\eta$  cannot be a primitive cube root of unity. Using  $\sigma(\beta) = \beta$ ,  $\sigma(\eta) = \eta$ ,  $\eta^2 + \eta + 1 = 0$  and  $\gamma^2\delta^2\rho^2 = 1$  to simplify when convenient, we get

$$\begin{aligned} \sigma(z) &= \sigma\left(\frac{\eta\gamma(\beta v - \eta\delta u)}{\eta v + \beta\delta u + \gamma\delta}\right) \\ &= \frac{\eta\delta\left(\beta\frac{1}{u} - \eta\rho\frac{v}{u}\right)}{\eta\frac{1}{u} + \beta\rho\frac{v}{u} + \delta\rho} \\ &= \frac{\eta\beta\delta - \eta^2\delta\rho v}{\eta + \beta\rho v + \delta\rho u} \\ &= \frac{\eta\beta\delta - \eta^2\delta\rho\left(\eta\gamma\delta - \frac{2\eta\gamma^2\delta(\beta z + \eta^2\gamma)}{z^2 + \eta^2\gamma^2}\right)}{\eta + \beta\rho\left(\eta\gamma\delta - \frac{2\eta\gamma^2\delta(\beta z + \eta^2\gamma)}{z^2 + \eta^2\gamma^2}\right) + \delta\rho\left(\beta\gamma + \frac{2\eta^2\gamma^2(z - \beta\gamma)}{z^2 + \eta^2\gamma^2}\right)} \\ &= \frac{\eta\delta(\eta^2 - \beta\gamma\delta\rho)z^2 - 2\beta\eta^3\gamma\delta z - \eta^3\gamma^2\delta(\eta^2 + \gamma\delta\rho\beta)}{-(\beta\eta + \eta\gamma\delta\rho + \beta)z^2 + 2\eta\gamma(\beta^2 - \eta)z + \gamma^2\eta^2(\beta\eta - \gamma\delta\rho\eta + \beta)} \end{aligned}$$

Since the gcd of the numerator and denominator is

$$(\beta\eta + \eta\gamma\delta\rho + \beta)z + \eta\gamma(\eta - \beta^2)$$

with the coefficient of  $z$  nonzero, we have

$$\sigma(z) = \frac{\eta\delta T_1 z + \eta^2\gamma\delta T_2}{T_3 z + \eta\gamma T_4}$$

with

$$\begin{aligned} T_1 &= \gamma\delta\rho(-2\beta^2\eta - \eta - \beta^2) + (-\beta - 2\beta\eta - \beta^3 - \beta^3\eta) \\ T_2 &= \gamma\delta\rho(\beta\eta + \beta^3 + 2\beta) + (\beta^2 + \beta^4 - \beta^2\eta + \eta) \\ T_3 &= \gamma\delta\rho(2\beta^3 - 2\beta\eta + 2\beta) + (\beta^4 - 2\beta^2\eta + \beta^2 + 1) \\ T_4 &= \gamma\delta\rho(\beta^2\eta + 1 + \beta^2) + (2\beta^3 + \beta - \beta\eta + \beta^3\eta) \end{aligned}$$

Note that (after simplification), both  $T_1T_4 - T_2T_3$  and  $(T_1 + T_4)^2$  are equal to

$$\gamma\delta\rho(-2\beta^3\eta - 6\beta\eta - 2\beta^5\eta - 6\beta - 6\beta^5 - 10\beta^3) + (-2\beta^2\eta - 6\beta^4\eta - 2\eta - 12\beta^4 - 12\beta^2)$$

and  $(T_1 + T_4) \neq 0$  (otherwise this would force  $(\eta\delta T_1)(\eta\gamma T_4) - (\eta^2\gamma\delta T_2)T_3 = \eta^2\gamma\delta(T_1T_4 - T_2T_3) = 0$  and  $\sigma(z)$  would be in  $K$ ). In order to use Lemma 11, we need to find a root of  $P(t) = T_3t^{q+1} - \eta\gamma T_4t^q + \eta\delta T_1t - \eta^2\gamma\delta T_2$  in  $K$ . If we substitute  $t$  by  $\eta\gamma\left(\frac{T_1+T_4}{T_3}t_0 + \frac{T_4}{T_3}\right)$  in

$P(t)$ , this is equivalent to finding a root of  $t_0^{q+1} + t_0 + 1$  in  $K$ . Then, using Lemma 10, all the roots  $\epsilon$  of  $P(t)$  are of the form  $\eta\gamma \left( \frac{T_1+T_4}{T_3}\epsilon_0 + \frac{T_4}{T_3} \right)$  with  $\epsilon_0 \in K$  a root of  $t_0^{q+1} + t_0 + 1$ . Then, from Lemma 11,  $\hat{A} = \frac{\eta\gamma}{\eta\delta} \frac{-\epsilon_0}{\sigma(\epsilon_0)+1} = \frac{\gamma}{\delta}\epsilon_0^2$ . Since

$$\hat{A}\sigma(\hat{A})\sigma^2(\hat{A}) = \frac{\gamma\delta\rho}{\delta\rho\gamma} (\epsilon_0\sigma(\epsilon_0)\sigma^2(\epsilon_0))^2 = 1$$

(by Lemma 10), Lemma 12 shows that there exists  $A, B \in K$  such that  $\sigma(A\hat{z}) = A\hat{z} + B$ .

In all three cases,  $\sigma^n \hat{z} = \hat{z}$  since  $\hat{z}$  is in  $K(z)$ , and  $\sigma^n(A) = A$  since  $A \in K$ , hence

$$w = \sum_{i=0}^{n-1} \sigma^i(\mu A \hat{z})$$

is fixed under  $\sigma$  and  $w = \tilde{A}\hat{z} + \tilde{B}$  for  $\tilde{A} = \text{Tr}_{K/k}(\mu A)$  and some  $\tilde{B} \in K$ . Q.E.D.

From now on  $w$  is assumed to be the generator of  $L$  over  $K$  computed in the proof of Theorem 13.

## 6.4 Function fields

If  $u = \frac{\bar{y}_1}{\bar{y}_0}$  (if  $C$  has equation  $Y^2 = (X-a)h(X)$ ), then  $\sigma(\bar{y}_0) = \bar{y}_1 = u\bar{y}_0$ ,  $\sigma^2(\bar{y}_0) = v\bar{y}_0$  and  $\sigma^3(\bar{y}_0) = \bar{y}_0$ , hence  $\sigma$  extends to  $F$  with order  $n$  (since 3 divides  $n$ ). If  $\tau$  is a generator of  $\text{Gal}(F/K(w))$ , then  $\tau(\bar{y}_0) = -\bar{y}_0$  and

$$\sigma(\tau(\bar{y}_0)) = \sigma(-\bar{y}_0) = -\sigma(\bar{y}_0) = -v\bar{y}_0 = v\tau(\bar{y}_0) = \tau(v\bar{y}_0) = \tau(\sigma(\bar{y}_0))$$

so  $\text{Gal}(F/K(w))$  commutes with  $\sigma$ .

**Theorem 14:** *Let  $K = \mathbb{F}_{q^n}$ ,  $n$  even and  $C$  be a curve of genus  $g$  defined over  $K$  by*

$$C : Y^2 = (X-a)h(X)$$

where  $h(X) \in K[X]$  is defined over  $k$  and  $a \in K \setminus k$ ,  $\sigma^3(a) = a$ . Then the function field of  $C$  can be embedded in the function field of a curve  $C'$  of genus

$$g' = 4g + 1$$

defined over  $k$  by the equation

$$\tilde{y}^2 = (\eta + \sigma(\eta)u(w) + \sigma^2(\eta)v(w))^2(x(w) - a)h(x(w))$$

where  $\eta = \sum_{i=0}^{n/3-1} \sigma^{3i}(\mu)$  for some  $\mu \in K$  such that  $\text{Tr}_{K/k}(\mu) = 1$ .

**Proof:** Since  $\text{Gal}(F/K(w))$  commutes with  $\sigma$ , we have  $F = KF'$  (where  $F'$  is the fixed field of  $F$  under  $\sigma$ ), hence  $F'/k$  and  $F/K$  have the same genus  $g'$ .

We first consider  $g$ , the genus of  $K(C)/K$ . Since  $\gcd(\deg(h) + 1, 2) = 1$ , the only places of  $K(x)$  which are ramified in  $K(C)$  are  $(x-a)$ , the place at infinity and the places over  $h(x)$ , and, if

$P \in \mathbb{P}_{K(x)}$  is ramified, there is a unique  $P' \in \mathbb{P}_{K(C)}$  over  $P$  and its ramification index is 2. Then, using Proposition 3, we have

$$g = 1 + 2(0 - 1) + \frac{1}{2}(2 - 1)(\deg(h) + 2) = \frac{1}{2} \deg(h),$$

so  $\deg(h) = 2g$ .

We can now compute  $g'$  in terms of  $g$ . The only places of  $K(x)$  which are ramified in  $F$  are  $(x - a)$ ,  $(x - \sigma(a))$ ,  $(x - \sigma^2(a))$ , the place at infinity and the places over  $h(x)$ , and, if  $P \in \mathbb{P}_{K(x)}$  is ramified, there are  $2^2$  distinct  $P' \in \mathbb{P}_{K(C)}$  over  $P$  and their ramification index is 2. Then, from Proposition 3, the genus of  $F'/k$  (and  $F/K$ ) is

$$\begin{aligned} g' &= 1 + 2^3(0 - 1) + \frac{1}{2}(2 - 1) \cdot 2^2(\deg(h) + 4) \\ &= 1 - 8 + 2(2g + 4) \\ &= 4g + 1 \end{aligned}$$

It remains to find an equation defining  $F'$  over  $L' = k(w)$ . Let  $\mu \in K$  such that  $Tr_{K/k} = 1$ , then  $F$  restrict to  $F'$  via the trace map. In particular,  $Tr_{F/F'}(\mu w) = w$ , and  $Tr_{F/F'}(\mu \epsilon) = \epsilon$  for every  $\epsilon \in k$ .

To simplify the notation, we let

$$\eta = \sum_{i=0}^{n/3-1} \sigma^{3i}(\mu),$$

so  $Tr_{K/k} = \eta + \sigma(\eta) + \sigma^2(\eta)$  and  $\sigma^3(\eta) = \eta$ . We now set

$$\begin{aligned} \tilde{y} &= Tr_{F/F'}(\mu \bar{y}_0) \\ &= \sum_{i=0}^{n-1} \sigma^i(\mu \bar{y}_0) \\ &= \bar{y}_0 \sum_{i=0}^{n/3-1} \sigma^{3i}(\mu) + u \bar{y}_0 \sum_{i=0}^{n/3-1} \sigma^{3i+1}(\mu) + v \bar{y}_0 \sum_{i=0}^{n/3-1} \sigma^{3i+2}(\mu) \\ &= \eta \bar{y}_0 + \sigma(\eta) u \bar{y}_0 + \sigma^2(\eta) v \bar{y}_0 \\ &= (\eta + \sigma(\eta)u + \sigma^2(\eta)v) \bar{y}_0 \end{aligned}$$

Then  $\tilde{y} \in F'$  and  $\tilde{y} \notin k(w)$  (since  $\bar{y}_0 \notin K(u) = K(w)$ ), hence  $F' = k(w, \tilde{y})$ . If we compute  $\tau(\tilde{y})$ , we have

$$\tau(\tilde{y}) = \tau((\eta + \sigma(\eta)u + \sigma^2(\eta)v) \bar{y}_0) = (\eta + \sigma(\eta)u + \sigma^2(\eta)v) \tau(\bar{y}_0) = -(\eta + \sigma(\eta)u + \sigma^2(\eta)v) \bar{y}_0 = -\tilde{y}.$$

Then  $N_{F'/L'}(\tilde{y})$  is

$$\begin{aligned} N_{F'/L'}(\tilde{y}) &= \prod_{i=0}^1 \tau^i(\tilde{y}) \\ &= \prod_{i=0}^1 (-1)^i \tilde{y} \end{aligned}$$

$$\begin{aligned}
&= (-1)^{n/2} \tilde{y}^2 \\
&= (-1)^{n/2} (\eta + \sigma(\eta)u + \sigma^2(\eta)v)^2 \overline{y_0}^2 \\
&= (-1)^{n/2} (\eta + \sigma(\eta)u + \sigma^2(\eta)v)^2 (x-a)h(x) \\
&= (-1)^{n/2} (\eta + \sigma(\eta)u(w) + \sigma^2(\eta)v(w))^2 (x(w)-a)h(x(w))
\end{aligned}$$

hence  $F'/k(w)$  is defined by the equation

$$\tilde{y}^2 = (\eta + \sigma(\eta)u(w) + \sigma^2(\eta)v(w))^2 (x(w)-a)h(x(w))$$

Q.E.D.

If  $v = \frac{\overline{y_1}}{\overline{y_0}}$  (if  $C$  has equation  $Y^2 = (X-a)(X-\sigma(a))h(X)$ ), then  $\sigma(\overline{y_0}) = \overline{y_1} = v\overline{y_0}$ ,  $\sigma(\overline{y_1}) = \frac{v}{u}\overline{y_0}$  and  $\sigma^3(\overline{y_0}) = \overline{y_0}$ , hence  $\sigma$  extends to  $F$  with order  $n$  (since 3 divides  $n$ ). If  $\tau$  is a generator of  $\text{Gal}(F/K(w))$ , then  $\tau(\overline{y_0}) = -\overline{y_0}$  and

$$\sigma(\tau(\overline{y_0})) = \sigma(-\overline{y_0}) = -\sigma(\overline{y_0}) = -v\overline{y_0} = v\tau(\overline{y_0}) = \tau(v\overline{y_0}) = \tau(\sigma(\overline{y_0}))$$

so  $\text{Gal}(F/K(w))$  commutes with  $\sigma$ .

**Theorem 15:** Let  $K = \mathbb{F}_{q^n}$ ,  $n$  even and  $C$  be a curve of genus  $g$  defined over  $K$  by

$$C : Y^2 = (X-a)(X-\sigma(a))h(X)$$

where  $h(X) \in K[X]$  is defined over  $k$  and  $a \in K \setminus k$ ,  $\sigma^3(a) = a$ . Then the function field of  $C$  can be embedded in the function field of a curve  $C'$  of genus

$$g' = 4g - 1$$

defined over  $k$  by the equation

$$\tilde{y}^2 = \left( \eta + \sigma(\eta)v(w) + \sigma^2(\eta)\frac{v(w)}{u(w)} \right)^2 (x(w)-a)(x(w)-\sigma(a))h(x(w))$$

where  $\eta = \sum_{i=0}^{n/3-1} \sigma^{3i}(\mu)$  for some  $\mu \in K$  such that  $\text{Tr}_{K/k}(\mu) = 1$ .

**Proof:** Since  $\text{Gal}(F/K(w))$  commutes with  $\sigma$ , we have  $F = KF'$  (where  $F'$  is the fixed field of  $F$  under  $\sigma$ ), hence  $F'/k$  and  $F/K$  have the same genus  $g'$ .

We first consider  $g$ , the genus of  $K(C)/K$ . Since  $\gcd(\deg(h)+1, 2) = 1$ , the only places of  $K(x)$  which are ramified in  $K(C)$  are  $(x-a)$ ,  $(x-\sigma(a))$ , the place at infinity and the places over  $h(x)$ , and, if  $P \in \mathbb{P}_{K(x)}$  is ramified, there is a unique  $P' \in \mathbb{P}_{K(C)}$  over  $P$  and its ramification index is 2. Then, using Proposition 3, we have

$$g = 1 + 2(0-1) + \frac{1}{2}(2-1)(\deg(h)+3) = \frac{1}{2}(\deg(h)+1),$$

so  $\deg(h) = 2g - 1$ .

We can now compute  $g'$  in terms of  $g$ . The only places of  $K(x)$  which are ramified in  $F$  are  $(x-a)$ ,  $(x-\sigma(a))$ ,  $(x-\sigma^2(a))$ , the place at infinity and the places over  $h(x)$ , and, if  $P \in \mathbb{P}_{K(x)}$

is ramified, there are  $2^2$  distinct  $P' \in \mathbb{P}_{K(C)}$  over  $P$  and their ramification index is 2. Then, from Proposition 3, the genus of  $F'/k$  (and  $F/K$ ) is

$$\begin{aligned} g' &= 1 + 2^3(0 - 1) + \frac{1}{2}(2 - 1) \cdot 2^2(\deg(h) + 4) \\ &= 1 - 8 + 2(2g + 3) \\ &= 4g - 1 \end{aligned}$$

It remains to find an equation defining  $F'$  over  $L' = k(w)$ . Let  $\mu \in K$  such that  $Tr_{K/k} = 1$ , then  $F$  restrict to  $F'$  via the trace map. In particular,  $Tr_{F'/F'}(\mu w) = w$ , and  $Tr_{F'/F'}(\mu \epsilon) = \epsilon$  for every  $\epsilon \in k$ .

To simplify the notation, we let

$$\eta = \sum_{i=0}^{n/3-1} \sigma^{3i}(\mu),$$

so  $Tr_{K/k} = \eta + \sigma(\eta) + \sigma^2(\eta)$  and  $\sigma^3(\eta) = \eta$ . We now set

$$\begin{aligned} \tilde{y} &= Tr_{F'/F'}(\mu \bar{y}_0) \\ &= \sum_{i=0}^{n-1} \sigma^i(\mu \bar{y}_0) \\ &= \bar{y}_0 \sum_{i=0}^{n/3-1} \sigma^{3i}(\mu) + v \bar{y}_0 \sum_{i=0}^{n/3-1} \sigma^{3i+1}(\mu) + \frac{v}{u} \bar{y}_0 \sum_{i=0}^{n/3-1} \sigma^{3i+2}(\mu) \\ &= \eta \bar{y}_0 + \sigma(\eta) v \bar{y}_0 + \sigma^2(\eta) \frac{v}{u} \bar{y}_0 \\ &= \left( \eta + \sigma(\eta) v + \sigma^2(\eta) \frac{v}{u} \right) \bar{y}_0 \end{aligned}$$

Then  $\tilde{y} \in F'$  and  $\tilde{y} \notin k(w)$  (since  $\bar{y}_0 \notin K(u) = K(w)$ ), hence  $F' = k(w, \tilde{y})$ . If we compute  $\tau(\tilde{y})$ , we have

$$\begin{aligned} \tau(\tilde{y}) &= \tau \left( \left( \eta + \sigma(\eta) v + \sigma^2(\eta) \frac{v}{u} \right) \bar{y}_0 \right) \\ &= \left( \eta + \sigma(\eta) v + \sigma^2(\eta) \frac{v}{u} \right) \tau(\bar{y}_0) \\ &= - \left( \eta + \sigma(\eta) v + \sigma^2(\eta) \frac{v}{u} \right) \bar{y}_0 \\ &= -\tilde{y}. \end{aligned}$$

Then  $N_{F'/L'}(\tilde{y})$  is

$$\begin{aligned} N_{F'/L'}(\tilde{y}) &= \prod_{i=0}^1 \tau^i(\tilde{y}) \\ &= \prod_{i=0}^1 (-1)^i \tilde{y} \\ &= (-1)^{n/2} \tilde{y}^2 \\ &= (-1)^{n/2} \left( \eta + \sigma(\eta) v + \sigma^2(\eta) \frac{v}{u} \right)^2 \bar{y}_0^2 \end{aligned}$$

$$\begin{aligned}
&= (-1)^{n/2} \left( \eta + \sigma(\eta)v + \sigma^2(\eta)\frac{v}{u} \right)^2 (x-a)(x-\sigma(a))h(x) \\
&= (-1)^{n/2} \left( \eta + \sigma(\eta)v(w) + \sigma^2(\eta)\frac{v(w)}{u(w)} \right)^2 (x(w)-a)(x(w)-\sigma(a))h(x(w))
\end{aligned}$$

hence  $F'/k(w)$  is defined by the equation

$$\tilde{y}^2 = \left( \eta + \sigma(\eta)v(w) + \sigma^2(\eta)\frac{v(w)}{u(w)} \right)^2 (x(w)-a)(x(w)-\sigma(a))h(x(w))$$

Q.E.D.

## 7 Conclusion

We have shown how a GHS-like Weil descent attack can be used to solve the discrete logarithm problem for hyperelliptic and superelliptic curves of the form

$$Y^r = (X-a)h(X)$$

over the field  $\mathbb{F}_{q^n}$  of characteristic  $p$ , with  $n$  divisible by 2,  $\gcd(p, r) = 1$ ,  $h(X)$  defined over  $\mathbb{F}_q$  and  $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ .

We have also shown a similar attack to solve the discrete log problem on families of nonsingular hyperelliptic curves in odd characteristic of the forms

$$Y^2 = (X-a)h(X)$$

and

$$Y^2 = (X-a)(X-\sigma(a))h(X)$$

over  $\mathbb{F}_{q^n}$  with  $n$  divisible by 3,  $h(X)$  defined over  $\mathbb{F}_q$  and  $a \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ .

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  $|\text{Jac}(\tilde{C})(k)|$ ), then experimental results seem to indicate that the kernel of the map from  $\text{Jac}(C)(K)$  to  $\text{Jac}(\tilde{C})(k)$  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  $\rho$  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 [12] and [23] for  $g! < q$ , see also [1], [4], [11] and [18] 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 superelliptic curves over the field  $\mathbb{F}_q$  can be done in  $O(r^7 g^2 (\log(q))^2)$  bit operations (see [9]), so for a fixed  $r$ , the index calculus attack for superelliptic curves of the form  $Y^r = f(X)$  takes an asymptotic running time of  $O\left(g^4 q^{2-\frac{4}{2g+1}+\epsilon}\right)$ .

## 8 Examples

### Example 1:

Let  $K = \mathbb{F}_{p^2}$  and  $k = \mathbb{F}_p$  with  $p$  an 80 bit prime. Given an hyperelliptic curve  $C$  of genus 2 of the form

$$C : Y^2 = (X - a)h(X)$$

with  $a \in K \setminus k$  and  $h(X)$  a polynomial of degree 4 defined over  $k$ , the curve  $C'$  obtained using the Weil descent attack will be hyperelliptic of genus 4 over  $k$ . Although the security of  $Jac(C)(\mathbb{F}_{p^2})$  would appear to be equivalent to the security of an elliptic curve over a field of 160 bits, using the index calculus attack on  $Jac(C')(\mathbb{F}_p)$  decreases its security to the level of an elliptic curve over a field of approximatively 125 bits.

### Example 2:

Let  $K = \mathbb{F}_{p^3}$  and  $k = \mathbb{F}_p$  with  $p$  an 30 bit prime. Given an hyperelliptic curve  $C$  of genus 3 given by an equation of the form

$$Y^2 = (X - a)h(X) \quad \text{or} \quad Y^2 = (X - a)(X - \sigma(a))h(X)$$

with  $a \in K \setminus k$  and  $h(X)$  a polynomial defined over  $k$ , the curve  $C'$  obtained using the Weil descent attack will be hyperelliptic of genus 11 (first equation) or 13 (second equation) over  $k$ . Although the security of  $Jac(C)(\mathbb{F}_{p^3})$  would appear to be equivalent to the security of an elliptic curve over a field of approximatively 256 bits, attacking from  $Jac(C')(\mathbb{F}_p)$  decreases its security to the level of an elliptic curve over a field of approximatively 110 bits (both security estimate assume the use of index calculus).

### Example 3:

Let  $K = \mathbb{F}_{p^3}$  and  $k = \mathbb{F}_p$  with  $p = 2^{61} - 1$ . Given an elliptic curve  $E$  of the form

$$E : Y^2 = (X - a)(X - \sigma(a))(X - d)$$

with  $a \in K \setminus k$  and  $d \in k$ , the curve  $C'$  obtained using the Weil descent attack will be hyperelliptic of genus 3 over  $k$ . Although elliptic curves over this field of 183 bits (proposed for cryptography in [2]) are secure enough for most cryptographic applications, using the index calculus attack on  $Jac(C')(\mathbb{F}_p)$  decreases their security to the level of elliptic curves over a field of approximatively 174 bits (which is less than expected, although it is still very secure in practice).

## 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] D. Bailey, C. Paar, Optimal extension fields for fast arithmetic in public-key algorithms, *Advances in Cryptology - CRYPTO'98*, Springer-Verlag, LNCS 1462, pp. 472-485, 1998.
- [3] C. Diem, The GHS attack in odd characteristic, *J. Ramanujan Math. Soc.*, **18** no. 1, pp. 1-32, 2003.

- [4] A. Enge, Computing discrete logarithms in high-genus hyperelliptic jacobians in provably subexponential time, *Math. Comp.*, **71**, no. 238, pp. 729-742, 2002.
- [5] G. Frey, Applications of arithmetical geometry to cryptographic constructions, *Finite fields and applications (Augsburg, 1999)*, Springer-Verlag, pp. 128-161, 2001.
- [6] S.D. Galbraith, Weil descent of Jacobians, *Discrete Applied Mathematics*, **128**, no. 1, pp. 165-180, 2003.
- [7] S.D. Galbraith, Limitations of constructive Weil descent, *Public-Key Cryptography and Computational Number Theory, September 11-15, 2000, Warsaw, Poland*, Walter de Gruyter, pp. 59-70, 2001.
- [8] S. D. Galbraith, F. Hess, N. P. Smart, Extending the GHS Weil descent attack, *Advances in Cryptology – EUROCRYPT 2002*, Springer-Verlag, LNCS 2332, pp. 29-44, 2002.
- [9] S. D. Galbraith, S. M. Paulus, N. P. Smart, Arithmetic on superelliptic curves, *Math. Comp.*, **71**, no. 237, pp. 393-405, 2002.
- [10] S. D. Galbraith, N. P. Smart, A cryptographic application of Weil descent, *Cryptography and coding (Cirencester, 1999)*, Springer-Verlag, LNCS 1746, pp. 191-200, 1999.
- [11] T. Garefalakis, D. Panario, The index calculus method using non-smooth polynomials, *Math. Comp.*, **70**, no 235, pp. 1253-1264, 2001.
- [12] 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.
- [13] P. Gaudry, F. Hess and N. P. Smart, Constructive and destructive facets of Weil descent on elliptic curves, *J. Cryptology*, **15**, pp. 19-46, 2002.
- [14] F. Hess, G. Seroussi, N.P. Smart, Two topics in hyperelliptic cryptography, *SAC 2001*, LNCS 2259, pp. 181-189, 2001.
- [15] M. Jacobson, A. Menezes, A. Stein, Solving elliptic curve discrete logarithm problems using Weil descent, *J. Ramanujan Math. Soc.*, **16** no. 3, pp. 231-260, 2001.
- [16] 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, pp. 195-213, 2001.
- [17] 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, pp. 308-318, 2001.
- [18] 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.
- [19] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, 1999.
- [20] A. Seigo, Weil descent of elliptic curves over finite fields of characteristic three. *Advances in cryptology—ASIACRYPT 2000 (Kyoto)*, Springer-Verlag, LNCS 1976, pp. 248-258, 2000.
- [21] N.P. Smart, How secure are elliptic curves over composite extension fields?, *Proceedings EUROCRYPT 2001*, Springer-Verlag, LNCS 2045, pp. 30-39, 2001.

- [22] H. Stichtenoth, *Algebraic function fields and Codes*, Springer-Verlag, 1993.
- [23] N. Thériault, Index calculus attack for hyperelliptic curves of small genus, preprint, 2003.
- [24] N. Thériault, Weil descent attack for Artin-Schreier curves, preprint, 2003.