The GHS Attack in odd Characteristic

Claus Diem

March 24, 2003

Abstract

The GHS attack is originally an approach to attack the discrete-logarithm problem (DLP) in the group of rational points of an elliptic curve over a non-prime finite field of characteristic 2. It is a method to transform the original DLP into DLPs in class groups of specific curves of higher genera over smaller fields.

In this article we give a generalization of the attack to degree 0 class groups of (hyper-)elliptic curves over non-prime fields of arbitrary characteristic. We solve the problem under which conditions the kernel of the "transformation homomorphism" (GHS-conorm-norm homomorphism) is small. We then analyze the resulting curves for the case that the characteristic is odd.

2000 Mathematics Subject Classification Primary 94A60, 11T71. Secondary 11Y99, 14H30.

1 Introduction

The discrete-logarithm problem (DLP) in the group of rational points of an elliptic curve over a finite field and more generally in the degree 0 divisor class group of a (hyper-)elliptic curve over a finite field is a well-studied cryptographic primitive for public-key cryptosystems. The security of this primitive relies on the difficulty of solving the DLP.

In [8], a new approach to attack the DLP in the group of rational points of elliptic curves over non-prime finite fields of characteristic 2 was introduced. Following [16], we call this approach the *GHS attack*.

The GHS attack is a method to transform the DLP in the group of rational points of an elliptic curve over a non-prime field into DLPs in class groups of specific curves of higher genera over smaller fields. The hope is that if the genus of a resulting curve is not "too large" and one finds "nice" explicit equations, it might be possible to solve the DLP via index calculus methods.

The curves of higher genera over smaller fields were originally discovered as smooth, projective curves which are birational to components of intersections of Weil restrictions of an affine part of the elliptic curve with certain hyperplanes. Then function field theory was applied to study the resulting curves; see [8, 3.2-3.4], expecially [8, Theorem 12]. In this article, our starting point is a generalization of the function field theoretic approach developed in [8]. (The role of Weil restrictions in the GHS attack is discussed in an appendix. There one also finds a discussion how the GHS attack fits into Frey's "Weil descent" idea.)

Notations and terminology

The terminology follows [13] and [21]. By a *function field*, we mean a finitely generated field extension $F|k$ of transcendence degree 1. If k is a perfect field (e.g. a finite field), the function field $F|k$ is called *regular* if k is algebraically closed in F; cf. [13, VIII, 4].

We make the following convention: If $K|k$ is a finite extension of fields, we denote function fields/curves over K with a prime and those over k without a prime. This philosophy is not consistent with the notations in [8]. For example, the meaning of F and F' is interchanged.

Outline of the GHS attack for (hyper-)elliptic curves in arbitrary characteristic

We give a brief description of a generalization of the original GHS attack from elliptic curves to (hyper-)elliptic curves and from characteristic 2 to arbitrary characteristic in the function field-theoretic setting. We will refer to this generalization also as *GHS attack.*

Let p be a prime, q a power of p, $n > 1$ an odd natural number.[1] Let H' be a (hyper-)elliptic curve over $\mathbb{F}_{q^n}$. Let an explicit (hyper-)elliptic equation of an affine part of H' be fixed. The fixed equation of H' induces an explicit description of $\mathrm{Cl}^0(H')$, the degree 0 divisor class group of H' (see for example [17]), and with respect to this description, we consider the DLP in $\mathrm{Cl}^0(H')$.

Assume that – with the possible exception of vulnerability to the GHS attack which we will study – H' would be regarded as "cryptographically suitable". For the present article it is most important that $\#\mathrm{Cl}^0(H')$ should be prime up to a small cofactor, and the large prime factor of $\#\mathrm{Cl}^0(H')$ should be $\geq 2^{160}$. In order to guarantee that the known index calculus attacks are not more efficient than generic attacks, the genus of H' should

[1] In [8], it is shown that in characteristic 2 the GHS attack can also be applied to certain elliptic curves if n is even. In this article, we concentrate on the case that n is odd. The case that p is odd and $n = 2$ is discussed in [22].

be at most 3; cf. [2], [7]. [2]

Let $\mathbb{F}_{q^n}(H')$ be the function field of H'. Then $\mathrm{Cl}^0(\mathbb{F}_{q^n}(H')) = \mathrm{Cl}^0(H')$. Let the extension $F'|K(H')$ be defined as in (2), and let us assume for simplicity that $F'|K$ is regular; see also Lemma 1. Then there exists a regular function field $F|\mathbb{F}_q$ such that $\mathbb{F}_{q^n}F = F'$; see Proposition 3.

Consider the following homomorphism of groups.

$$\mathrm{N}_{F'|F} \circ \mathrm{Con}_{F'|\mathbb{F}_{q^n}(H')} : \mathrm{Cl}^0(\mathbb{F}_{q^n}(H')) \longrightarrow \mathrm{Cl}^0(F) \tag{1}$$

Here, $\mathrm{Con}_{F'|\mathbb{F}_{q^n}(H')}$ is the conorm homomorphism, and $\mathrm{N}_{F'|F}$ is the norm homomorphism. We call homomorphism (1) the *GHS-conorm-norm homomorphism.*

Via this homomorphism, one wishes to transform the DLP in $\mathrm{Cl}^0(\mathbb{F}_{q^n}(H'))$ into the DLP in $\mathrm{Cl}^0(F)$. In order that this is possible, it is necessary that the large subgroup of prime order is preserved, i.e. that the kernel of (1) and the large subgroup of prime order have trivial intersection. We will give a condition which is both necessary as well as sufficient in order that this is the case; see Proposition 5 and Theorem 1.

The goal of the attack is now to find a "nice" explicit (for example hyperelliptic) equation of F, represent $\mathrm{Cl}^0(F)$ with the help of this equation and then try to break instances of the DLP in $\mathrm{Cl}^0(K(H'))$ by transforming them with (1) into instances of the DLP in $\mathrm{Cl}^0(F)$ and then solving them with index calculus methods; cf. [2], [7].

Besides finding "nice" equations for F, it is of greatest importance that $\#\mathrm{Cl}^0(F) \approx q^{g(F)}$ is not too large ($g(F)$ = genus of F). For example, if $q^{g(F)} \geq 2^{1024}$, by the current state of the art of index calculus, it is impossible to solve the resulting DLP in $\mathrm{Cl}^0(F)$.

The attack was previously analyzed in detail for elliptic curves and $p = 2$; see [8], [16], [12], [14]. Similar results to the ones in [8] can be found in [5] for certain hyperelliptic curves – again for $p = 2$.

In this article, we prove in particular (see Section 6):

Let p be odd. Then:

- *If n is prime, $n \geq 11$, and $H' = E'$ is an elliptic curve such that $q^n \geq 2^{160}$, then $\#\mathrm{Cl}^0(F) \approx q^{g(F)} \geq 2^{5000}$.*
- *For $n = 5, 7$ there exist examples of elliptic curves E' for which the genus of F is 5 respectively 7. These examples are optimal in the sense*

[2] Furthermore, $\#\mathrm{Cl}^0(H')$ should not equal p (cf. [19], [20]), and the (multiplicative) order of p modulo the large prime factor of $\#\mathrm{Cl}^0(H')$ should be so large that the attacks via the Weil- and the Tate-pairing (cf. [15], [4]) are infeasible.

that the genus of F is smallest possible under the condition that the large subgroup prime order of $E'(K) \simeq \mathrm{Cl}^0(E')$ is preserved under (1).

In the first case, the size of $\mathrm{Cl}^0(F)$ is so large that the attack fails unless a substantial improvement on the solution of the DLP in class groups of high-genus curves / function fields is made or some very special properties of the function field F can be exploited. In the second case, the attack might be successful.

The rest of the article is organized as follows: In the next section, we prove the existence of the function field F, in Section 3, we prove under which conditions the kernel of the GHS-conorm-norm homomorphism is small. We then turn to the case that the characteristic is odd. After having given some background information on Kummer theory of function fields, we analyze the genera of the resulting function fields, first for general odd extension degree in Section 5, and then for prime extension degree in Section 6. In Section 7, we show how for certain important examples explicit defining equations for F can be derived. In the last section, we draw conclusions, and in an appendix we discuss the relation between the GHS attack and Frey's "Weil descent" idea.

2 The GHS attack in arbitrary characteristic

We begin by showing that the necessary constructions for the attack can be carried out independently of the characteristic provided that the extension degree n is odd.

We first fix some notation that we will use throughout the article.

Let $K|k$ be a non-trivial extension of finite fields of odd degree n. Let $\overline{K}$ denote a fixed algebraic closure of K. Let H' be a (hyper-)elliptic curve over K, i.e. a smooth geometrically irreducible curve of genus $g \geq 1$ over K such that there exists a non-constant morphism of degree 2 from the curve to the projective line.

Let $K(H')$ be the function field of H' and fix some embedding $K(x) \hookrightarrow K(H')$ such that the extension $K(H')|K(x)$ has degree 2 (for $g \geq 2$, $K(H')$ contains a unique rational subfield of index 2, and the embedding $K(x) \hookrightarrow K(H')$ is unique up to an automorphism of $K(x)$).

Fix a separable closure $K(x)^{\mathrm{sep}}$ of $K(x)$ (containing $K(H')$ and $\overline{K}(x)$). In the following, we will entirely work within this closure. If $\widetilde{K}|K$ is some algebraic extension (inside $\overline{K}$), we denote the composite $\widetilde{K}K(H')$ (inside $K(x)^{\mathrm{sep}}$) by $\widetilde{K}(H')$.

We denote the Frobenius automorphism of $K|k$ by $\sigma_{K|k}$. By setting $\sigma_{K|k}(x) := x$, $\sigma_{K|k}$ extends to an automorphism of $K(x)|k(x)$, also denoted by $\sigma_{K|k}$. We extend $\sigma_{K|k}$ to some automorphism $\widehat{\sigma_{K|k}}$ of $K(x)^{\mathrm{sep}}$ and let $\sigma_{K|k}^i(K(H'))$ be the image of $K(H')$ under $\widehat{\sigma_{K|k}}^{\,i}$. (As $K(H')|K(x)$ is Galois, this is independent of the chosen extension of $\sigma_{K|k}$.)

Let

$$F' := K(H')\,\sigma_{K|k}(K(H'))\cdots\sigma_{K|k}^{n-1}(K(H')). \tag{2}$$

This is the Galois closure of $K(H')$ over $k(x)$ (inside $k(x)^{\mathrm{sep}}$); cf. [21, A.11.]. Let $m, \overline{m} \in \mathbb{N}$ be defined by

$$[F' : K(x)] = 2^m\,, \quad [\overline{K}F' : \overline{K}(x)] = 2^{\overline{m}}. \tag{3}$$

Lemma 1 *Either $F'|K$ is regular or F' is regular over the unique quadratic extension of K.*

Proof Let $\widetilde{K}$ be the algebraic closure of K in F'. Then $\mathrm{Gal}(\widetilde{K}|K) \simeq \mathrm{Gal}(\widetilde{K}(x)|K(x))$. This group is on the one hand cyclic and on the other hand a quotient of $\mathrm{Gal}(F'|K(x))$. Now $\mathrm{Gal}(F'|K(x))$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$, and thus its only cyclic quotients are the trivial group and the cyclic group of order 2. □

Under our assumption that n is odd, we have the following lemma:

Lemma 2 *The Frobenius $\sigma_{K|k}$ on $K(x)$ extends to an automorphism of $F'|k(x)$ of order n, and two such extensions are conjugate to each other in $\mathrm{Gal}(F'|k(x))$.*

Proof By Galois theory, we have a short exact sequence

$$1 \longrightarrow \mathrm{Gal}(F'|K(x)) \longrightarrow \mathrm{Gal}(F'|k(x)) \longrightarrow \mathrm{Gal}(K(x)|k(x)) \longrightarrow 1,$$

where $\mathrm{Gal}(K(x)|k(x)) \simeq \mathrm{Gal}(K|k)$. The order of $\mathrm{Gal}(F'|K(x))$, 2^m, is prime to n, since by assumption n is odd. By two well-known group-theoretic theorems by Zassenhaus (which are rather elementary in the special case we are considering), the sequence splits and two sections are conjugate to each other; see [11, I, 18.1,18.2]. The statement of the lemma is a reformulation of this fact. □

Now let us fix an extension $\widetilde{\sigma_{K|k}}$ of $\sigma_{K|k}$ as in the lemma, and let $F := F'^{\langle\widetilde{\sigma_{K|k}}\rangle}$ be the fixed field under $\widetilde{\sigma_{K|k}}$. Then $[F' : F] = n, F' = KF$ and $F \cap K = k$.

If $F'|K$ is regular, it follows that $F|k$ is regular. If $F'|K(x)$ is not regular, let $\lambda|k$ be the unique quadratic extension. Then by Lemma 1, $F'|K\lambda$ is regular, and $F|\lambda$ is regular.

$$\begin{tikzcd}
F' \arrow[d, dash] \arrow[dr, dash] & & \\
F \arrow[ddrr, dash] & K(H') \arrow[dr, dash] & \\
& & K(x) \arrow[d, dash] \\
& & k(x)
\end{tikzcd}$$

Proposition 3 *Assume that $F'|K$ is regular. Then there exists a subextension $F|k(x)$ of $F'|k(x)$ such that $F|k$ is regular and $KF = F'$. Further, any two such extensions $F|k(x)$ are isomorphic.*

If $F'|K$ is not regular, let $\lambda|k$ be the unique quadratic extension. Then $F'|\lambda K$ is regular and there exists a subextension $F|\lambda(x)$ of $F'|\lambda(x)$ such that $F'|\lambda$ is regular and $\lambda K\,F = KF = F'$. Again, any two such extensions are isomorphic.

Proof We have to show that any extension $F_1|k(x)$ or $F_1|\lambda(x)$ as in the proposition is isomorphic to the extension $F|k(x)$ or $F|\lambda(x)$ constructed above. Assume that $F'|K$ is regular (the other case is proved analogously). Let $F_1|k(x)$ be a subextension of $F'|k(x)$ such that $F_1|k$ is regular and $KF_1 = F'$. The fact that $F_1|k$ is regular is equivalent to $F_1 \cap \overline{k}(x) = k(x)$. In particular we have $F_1 \cap K(x) = k(x)$. This means that the restriction homomorphism $\mathrm{Gal}(F'|F_1) \longrightarrow \mathrm{Gal}(K(x)|k(x))$ is an isomorphism; see [13, VI, Theorem 1.12]. Thus $F'|F$ and $F'|F_1$ are cyclic extensions of order n, and there exists a generating element in the Galois groups of $F'|F_1$ which restrict to $\sigma_{K|k} \in \mathrm{Gal}(K(x)|k(x))$. By Lemma 2, this generating element of $\mathrm{Gal}(F'|F_1)$ is conjugate to the above chosen extension $\widetilde{\sigma_{K|k}}$ of $\sigma_{K|k}$. This implies that $F|k(x)$ and $F_1|k(x)$ are isomorphic field extensions. $\square$

Remark If n is not odd but $n = m$, Lemma 2 and thus Proposition 3 still hold. This follows from the fact that in this case $F' \simeq K(H') \otimes_{K(x)} \sigma_{K|k}(K(x)) \otimes_{K(x)} \cdots \otimes_{K(H')} \sigma_{K|k}^{n-1}(K(H'))$.

3 The kernel of the GHS-conorm-norm homomorphism

We keep the notations of the last section. For instance, $K|k$ is an extension of finite fields of arbitrary characteristic of odd degree n. Again, we work entirely within a fixed separable closure of $K(x)$.

We first want to state a necessary condition in order that – in cryptographically relevant situations – the kernel of (1) does not contains the large subgroup of prime order.

The idea is as follows: Assume that $K(H')|k(x)$ is Galois. Then by construction, $F' = K(H')$, thus $KF = K(H')$. In cryptographically relevant situations, it follows that the large subgroup of prime order is contained in the kernel of (1).

Lemma 4 *Let μ be an intermediate field of $K|k$. The following statements are equivalent:*

1. $K(H') = \sigma_{K|\mu}(K(H'))$ *(where $\sigma_{K|\mu} = \sigma_{K|k}^{[\mu:k]}$ is the Frobenius of $K|\mu$)*
2. $K(H')|\mu(x)$ *is Galois*
3. *There exists an extension $M|\mu(x)$ of degree 2 such that $M|\mu$ is regular and $KM = K(H')$.*

Proof As the Galois closure of $K(H')|\mu(x)$ is $K(H')\sigma_{K|\mu}(K(H'))\cdots {\sigma_{K|\mu}}^{[K:\mu]-1}(K(H'))$, the equivalence of the first two points is obvious.

It is also obvious that the third condition implies the first two.

So let $K(H')|\mu(x)$ be Galois. By Proposition 3 applied to $K|\mu$ instead of $K|k$, we see that there exists an extension $M|\mu(x)$ such that $M|\mu$ is regular and $KM = K(H')$. By construction $M|\mu(x)$ has degree 2. $\square$

Remark If n is even, the first two points are also equivalent, and the third implies these two points.

Let μ be an intermediate field of $K|k$ such that $\mu \subsetneq K$, assume that the conditions of the lemma are satisfied, and let $M|\mu(x)$ be as in the lemma. We claim that (1) factors through the norm homomorphism from $\mathrm{Cl}^0(K(H'))$ to $\mathrm{Cl}^0(M)$.

Let F_0' be the Galois closure of $M|k(x)$. By the argumentation following Lemma 2 applied to $\mu|k$, $M|k(x)$ and F_0', there exists an extension $F_0|k(x)$ with $\mu F_0 = F_0'$ and $F_0 \cap \mu = k$. As in the last section, let λ be the unique extension of k of degree 2. Then depending on whether $F'|K$ is regular or $F'|\lambda K$ is regular, $F_0|k$ is regular or $F_0|\lambda$ is regular. Further $F' = KF_0' = KF_0$, and thus by Proposition 3 $F_0|k(x)$ is isomorphic to $F|k(x)$. (In particular, F is contained in the Galois extension $F_0'|k(x)$.) We thus obtain the following diagram.

$$\begin{tikzcd}
F' = KF_0 \arrow[d, dash] \arrow[dr, dash] & \\
F_0' = \mu F_0 \arrow[dd, equal] \arrow[dr, dash] & K(H') = KM \arrow[d, dash] \\
& M \\
F_0, F &
\end{tikzcd}$$

This induces the commutative diagram

$$\begin{tikzcd}
\mathrm{Cl}^0(F') \arrow[d] & \mathrm{Cl}^0(K(H')) \arrow[l] \arrow[d] \\
\mathrm{Cl}^0(\mu F_0) \arrow[d] & \mathrm{Cl}^0(M) \arrow[l] \\
\mathrm{Cl}^0(F). &
\end{tikzcd}$$

(Here the left-arrows are conorm homomorphisms and the down-arrows are norm homomorphisms.) It follows that (1) factors through $\mathrm{norm}_{K(H')|M} : \mathrm{Cl}^0(K(H')) \longrightarrow \mathrm{Cl}^0(M)$.

Proposition 5 *Let μ be an intermediate field of $K|k$ and assume that $K(H')|\mu(x)$ is Galois. Then there exists a regular function field $M|\mu$ with $KM = K(H')$ such that (1) factors through $\mathrm{N}_{K(H')|M} : \mathrm{Cl}^0(K(H')) \longrightarrow \mathrm{Cl}^0(M)$.*

Cryptological application Assume that the curve H' is cryptographically suitable – i.e. in particular the genus of H' is small (≤ 3) and the order of $\mathrm{Cl}^0(K(H'))$ is prime up to a small cofactor – and that a field $\mu \subsetneq K$ as in the proposition exists. Then the proposition implies that the kernel of (1) contains the large subgroup of prime order, and thus the GHS attack fails. This follows from the theorem of Hasse-Weil; cf. [21, V.2.1.].

The following theorem can be viewed as a converse to the last proposition.

Theorem 1 *Let $K|k$, H', F and F' be as in Proposition 3. Assume that for no intermediate field μ of $K|k$ such that $\mu \subsetneq K$, $K(H')|\mu(x)$ is Galois. Then the kernel of (1) contains only elements of order a 2-power.* [3]

[3] After having finished the preparation of the manuscript, we were informed that in the context of [8], F. Hess obtained a similar result.

Proof In fact, we will prove that the kernel of (1) is annihilated by multiplication with 2^{m-1}, i.e. that every element of the kernel has an order dividing 2^{m-1}.

We first fix a notation: If $\alpha : A_1 \hookrightarrow A_2$ is a homomorphism of function fields, we denote the conorm from $\mathrm{Cl}^0(A_1)$ to $\mathrm{Cl}^0(A_2)$ with respect to α by $\underline{\alpha}$.

Let $\iota : K(H') \hookrightarrow F'$ be the inclusion. As in Section 2, let $\widetilde{\sigma_{K|k}}$ be a fixed extension of $\sigma_{K|k}$ to $F'|k(x)$ and let $F = F'^{\langle \widetilde{\sigma_{K|k}} \rangle}$.

Then by definition, $\mathrm{Con}_{F'|K(H')} = \underline{\iota}$, and

$$\mathrm{Con}_{F'|F} \circ \mathrm{N}_{F'|F} \circ \mathrm{Con}_{F'|K(H')} = \sum_{i=0}^{n-1} \underline{\widetilde{\sigma_{K|k}}^{\,i}} \circ \underline{\iota} : \mathrm{Cl}^0(K(H')) \longrightarrow \mathrm{Cl}^0(F').$$

As the conorm homomorphism $\mathrm{Con}_{F'|F}$ is injective (see [21, III.6.3. (f)]), the kernel of $\mathrm{N}_{F'|F} \circ \mathrm{Con}_{F'|K(H')} : \mathrm{Cl}^0(K(H')) \longrightarrow \mathrm{Cl}^0(F)$, i.e. the kernel of (1), equals the kernel of

$$\sum_{i=0}^{n-1} \underline{\widetilde{\sigma_{K|k}}^{\,i}} \circ \underline{\iota} : \mathrm{Cl}^0(K(H')) \longrightarrow \mathrm{Cl}^0(F').$$

We want to study the kernel of this homomorphism.

Let $\overline{\sigma_{K|k}^{i}} : K(H') \longrightarrow \sigma_{K|k}^{i}(K(H'))$ be the restriction of $\widetilde{\sigma_{K|k}}^{\,i}$ to $K(H')$. Let $\iota_i : \sigma_{K|k}^{i}(K(H')) \hookrightarrow F'$ be the inclusions. Then $\sum_{i=0}^{n-1} \underline{\widetilde{\sigma_{K|k}}^{\,i}} \circ \underline{\iota} = \sum_{i=0}^{n-1} \underline{\iota_i} \circ \underline{\overline{\sigma_{K|k}^{i}}}$.

The conorm homomorphisms

$$\underline{\iota_i} : \mathrm{Cl}^0(\sigma_{K|k}^{i}(K(H'))) \longrightarrow \mathrm{Cl}^0(F')$$

induce a homomorphism

$$\oplus_i \underline{\iota_i} : \bigoplus_{i=0}^{n-1} \mathrm{Cl}^0(\sigma_{K|k}^{i}(K(H'))) \longrightarrow \mathrm{Cl}^0(F'),$$

and the conorm homomorphisms

$$\underline{\overline{\sigma_{K|k}^{i}}} : \mathrm{Cl}^0(K(H')) \longrightarrow \mathrm{Cl}^0(\sigma_{K|k}^{i}(K(H')))$$

induce a homomorphism

$$(\underline{\overline{\sigma_{K|k}^{i}}})_i : \mathrm{Cl}^0(K(H')) \longrightarrow \prod_{i=0}^{n-1} \mathrm{Cl}^0(\sigma_{K|k}^{i}(K(H'))) = \bigoplus_{i=0}^{n-1} \mathrm{Cl}^0(\sigma_{K|k}^{i}(K(H'))).$$

Combining these two homomorphisms, we obtain:

$$\sum_{i=0}^{n-1} \underline{\widetilde{\sigma_{K|k}}^{\,i}} \circ \underline{\iota} = \sum_{i=0}^{n-1} \underline{\iota_i} \circ \underline{\overline{\sigma^i_{K|k}}} = (\oplus_i\, \underline{\iota_i}) \circ (\underline{\overline{\sigma^i_{K|k}}})_i : \mathrm{Cl}^0(K(H')) \longrightarrow \mathrm{Cl}^0(F')$$

The homomorphism $(\underline{\overline{\sigma^i_{K|k}}})_i$ is obviously injective, and we will prove now that the exponent of the kernel of $\oplus_i\, \underline{\iota_i}$ divides 2^{m-1}.

The norm homomorphisms

$$\mathrm{N}_i := \mathrm{N}_{F'|\sigma^i_{K|k}(K(H'))} : \mathrm{Cl}^0(F') \longrightarrow \mathrm{Cl}^0(\sigma^i_{K|k}(K(H')))$$

induce a homomorphism

$$(\mathrm{N}_i)_i : \mathrm{Cl}^0(F') \longrightarrow \prod_{i=0}^{n-1} \mathrm{Cl}^0(\sigma^i_{K|k}(K(H'))) = \bigoplus_{i=0}^{n-1} \mathrm{Cl}^0(\sigma^i_{K|k}(K(H')))$$

We claim that $(\mathrm{N}_i)_i \circ (\oplus_i\, \underline{\iota_i}) = 2^{m-1}$. This implies in particular that the exponent of the kernel of $\oplus_i\, \underline{\iota_i}$ divides 2^{m-1}.

The claim follows from the following two claims:

- For $i = 0, \ldots, n-1$, $\mathrm{N}_{F'|\sigma^i_{K|k}(K(H'))} \circ \mathrm{Con}_{F'|\sigma^i_{K|k}(K(H'))}$: $\mathrm{Cl}^0(\sigma^i_{K|k}(K(H'))) \longrightarrow \mathrm{Cl}^0(\sigma^i_{K|k}(K(H')))$ is multiplication by 2^{m-1}.
- For $i, j = 0, \ldots, n-1$, $i \neq j$, $\mathrm{N}_{F'|\sigma^j_{K|k}(K(H'))} \circ \mathrm{Con}_{F'|\sigma^i_{K|k}(K(H'))}$: $\mathrm{Cl}^0(\sigma^i_{K|k}(K(H'))) \longrightarrow \mathrm{Cl}^0(\sigma^j_{K|k}(K(H')))$ is trivial.

The first claim is standard, we prove the second.

By assumption and Lemma 4, for no $i = 1, \ldots, n-1$, $K(H') = \sigma^i_{K|k}(K(H'))$. This means that for no $i, j = 0, \ldots, n-1$ with $i \neq j$, $\sigma^i_{K|k}(K(H')) = \sigma^j_{K|k}(K(H'))$.

Let $i \neq j \in \{0, \ldots, n-1\}$, let $L' := \sigma^i_{K|k}(K(H'))\, \sigma^j_{K|k}(K(H'))$. Then $L'|K(x)$ is an extension of degree 4, and $F'|L'$ is an extension of degree 2^{m-2}.

$$\begin{tikzcd}[column sep=small]
& F' \arrow[d, dash] & \\
& L' \arrow[dl, dash] \arrow[dr, dash] & \\
\sigma^i_{K|k}(K(H')) \arrow[dr, dash] & & \sigma^j_{K|k}(K(H')) \arrow[dl, dash] \\
& K(x) &
\end{tikzcd}$$

We have

$$\begin{gathered}\mathrm{N}_{F'|\sigma^j_{K|k}(K(H'))} \circ \mathrm{Con}_{F'|\sigma^i_{K|k}(K(H'))} = \\ \mathrm{N}_{L'|\sigma^j_{K|k}(K(H'))} \circ \mathrm{N}_{F'|L'} \circ \mathrm{Con}_{F'|L'} \circ \mathrm{Con}_{L'|\sigma^i_{K|k}(K(H'))} = \\ \mathrm{N}_{L'|\sigma^j_{K|k}(K(H'))} \circ [2^{m-2}] \circ \mathrm{Con}_{L'|\sigma^i_{K|k}(K(H'))},\end{gathered}$$

where $[2^{m-2}]$ denotes multiplication by 2^{m-2}. It thus suffices to prove that $\mathrm{N}_{L'|\sigma^j_{K|k}(K(H'))} \circ \mathrm{Con}_{L'|\sigma^i_{K|k}(K(H'))} = 0$. By the following lemma, $\mathrm{N}_{L'|\sigma^j_{K|k}(K(H'))} \circ \mathrm{Con}_{L'|\sigma^i_{K|k}(K(H'))} = \mathrm{Con}_{\sigma^j_{K|k}(K(H'))|K(x)} \circ \mathrm{N}_{\sigma^i_{K|k}(K(H'))|K(x)}$, and this is equal to 0 as $\mathrm{Cl}^0(K(x)) = 0$. □

Lemma 6 *Let A be a function field over a field K, let $B|A$ and $C|A$ be finite Galois extensions, let BC be a composite of B and C over A such that inside BC, $B \cap C = A$. Then*

$$\mathrm{N}_{BC|C} \circ \mathrm{Con}_{BC|B} = \mathrm{Con}_{C|A} \circ \mathrm{N}_{B|A} : \ \mathrm{Cl}^0(B|K) \longrightarrow \mathrm{Cl}^0(C|K).$$

Proof The statement follows from the corresponding statement on the level of divisors:

$$\mathrm{N}_{BC|C} \circ \mathrm{Con}_{BC|B} = \mathrm{Con}_{C|A} \circ \mathrm{N}_{B|A} : \ \mathrm{Div}(B|K) \longrightarrow \mathrm{Div}(C|K)$$

This statement can be proven as follows:

On the level of divisors, the conorm homomorphism is injective. It thus suffices to check that $\mathrm{Con}_{BC|C} \circ \mathrm{N}_{BC|C} \circ \mathrm{Con}_{BC|B} = \mathrm{Con}_{BC|C} \circ \mathrm{Con}_{C|A} \circ \mathrm{N}_{B|A} : \mathrm{Div}(B|K) \longrightarrow \mathrm{Div}(C|K)$.

We denote the conorm on the level of divisors with respect to a homomorphism of function fields $\alpha : A_1 \longrightarrow A_2$ also by α. If $\tau \in \mathrm{Gal}(BC|C)$, we denote its restriction to B by $\overline{\tau}$, and we denote the inclusion $B \hookrightarrow BC$ by ι. By assumption on the composite $BC|A$, $\mathrm{Gal}(BC|C) \longrightarrow \mathrm{Gal}(B|A), \tau \mapsto \overline{\tau}$ is an isomorphism (see [13, VI, Theorem 1.12]) and $\tau\iota = \iota\overline{\tau} : B \longrightarrow BC$.

Now, for $D \in \mathrm{Div}(B|K)$, $\mathrm{Con}_{BC|C} \circ \mathrm{N}_{BC|C} \circ \mathrm{Con}_{BC|B}(D) = \sum_{\tau \in \mathrm{Gal}(BC|C)} \tau(\iota(D)) = \iota(\sum_{\overline{\tau} \in \mathrm{Gal}(B|A)} \overline{\tau}(D)) = \mathrm{Con}_{BC|B} \circ \mathrm{Con}_{B|A} \circ \mathrm{N}_{B|A}(D) = \mathrm{Con}_{BC|A} \circ \mathrm{N}_{B|A}(D) = \mathrm{Con}_{BC|C} \circ \mathrm{Con}_{C|A} \circ \mathrm{N}_{B|A}(D)$. □

Remark The theorem is also valid for $n = [K : k]$ even, provided that the field F as in Proposition 3 exists.

Corollary 7 *Let n be prime and assume that $K(H') \subsetneq F'$. Then the kernel of (1) contains only elements of order a 2-power.*

4 Composites of (hyper-)elliptic function fields

For the rest of the article, we restrict ourselves to the case that the characteristic is odd.

The main goal is now to calculate the genus of $F' = K(H')\,\sigma_{K|k}(K(H')) \cdots \sigma_{K|k}^{n-1}(K(H'))$ or – what is the same – the genus of $\overline{K}F'|\overline{K}$ and furthermore to check whether $F'|K$ is regular.

In [8], Artin-Schreier Theory was used to study the extension $F'|K(x)$. Since we work in odd characteristic, we wish to substitute this by Kummer Theory.

We first give an exposition to the results we need and come back to the GHS attack in the following section.

Let Λ be a field with $\mathrm{char}(\Lambda) \neq 2$, let Λ^{sep} be a fixed separable closure, and let $\mu_2 \subseteq \Lambda^*$ be the subgroup consisting of 1 and -1.

We have a pairing

$$\begin{gathered}\mathrm{Gal}(\Lambda^{\mathrm{sep}}|\Lambda) \times \Lambda^* \longrightarrow \mu_2 \\ (\sigma, u) \mapsto \tfrac{\sigma(\nu)}{\nu} \text{ where } \nu^2 = u,\ \nu \in \Lambda^{\mathrm{sep}}.\end{gathered}$$

Let U be a finite subgroup of Λ^*/Λ^{*2}. Let $\Lambda[\sqrt[2]{U}]$ be the subfield of $\sqrt[2]{\Lambda}$ generated over Λ by the square roots of the preimages of the elements of U in Λ^*.

Then the above pairing induces a non-degenerate pairing

$$\langle\cdot,\cdot\rangle :\ \mathrm{Gal}(\Lambda[\sqrt[2]{U}]|\Lambda) \times U \longrightarrow \mu_2 \tag{4}$$

of finite abelian groups of exponent 2.

We can regard U as an $\mathbb{F}_2$-vector space. Since the pairing is non-degenerate,

$$[\Lambda[\sqrt[2]{U}] : \Lambda] = 2^{\dim_{\mathbb{F}_2}(U)}. \tag{5}$$

The non-degeneracy of the pairing also implies:

Lemma 8 *The assignment $V \mapsto \Lambda[\sqrt[2]{V}]$ gives bijection between the subvector spaces of U and the subextensions of $\Lambda[\sqrt[2]{U}]|\Lambda$.*

Now let K be a perfect field with $\mathrm{char}(K) \neq 2$. Fix an algebraic closure $\overline{K}$ and a separable closure $K(x)^{\mathrm{sep}}$ containing $\overline{K}(x)$. All the following extensions of $K(x)$ should be regarded inside $K(x)^{\mathrm{sep}}$. We now apply the above statements to the case that $\Lambda = K(x)$.

We fix the following notation: If $h \in K(x)^*$, its image in $K(x)^*/K(x)^{*2}$ is denoted by $\underline{h}$.

Let $f_1, \ldots, f_n \in K(x)^*$, let $L_i|k(x)$ be the extension given by $y_i^2 = f_i(x)$ inside $K(x)^{\mathrm{sep}}$. Let L be the composite of the L_i inside $K(x)^{\mathrm{sep}}$.

Let U be the $\mathbb{F}_2$-vector space generated by the $\underline{f_i} \in K(x)^*/K(x)^{*2}$. Let $\overline{U}$ be the image of U inside $\overline{K}(x)^*/\overline{K}(x)^{*2}$. Then $L = K(x)[\sqrt[2]{U}]$, $\overline{K}L = \overline{K}(x)[\sqrt[2]{\overline{U}}]$.

Lemma 9 *$L|K$ is regular iff $U \longrightarrow \overline{U}$ is an isomorphism.*

Proof $L|K$ is regular iff $[L : K(x)] = [\overline{K}L : \overline{K}(x)]$. By (5) this is equivalent to $U \xrightarrow{\sim} \overline{U}$. □

Especially:

Lemma 10 *Let all f_i be monic, i.e. the leading coefficient is 1. Then $L|K$ is regular.*

Proof Under this condition, all elements of U are images of monic rational functions. Now, if a monic rational function of K is a square in $\overline{K}(x)$, it is also a square in $K(x)$. (As $\overline{K}|K$ is separable.) □

We want to study the ramification of $L|K(x)$ in terms of the ramification of $L_i|K(x)$.

Lemma 11 *$L|K(x)$ is ramified at a place $\mathfrak{p}$ of $K(x)|K$ iff there exists an i such that $L_i|K(x)$ is ramified. If this is the case, the ramification index of $\mathfrak{p}$ in $L|K(x)$ is 2.*

Proof This is a special case of Abhyankar's Lemma; see [18, Lemma (2.14)] or [21, Proposition III.8.9]. [4] □

Let κ be the algebraic closure of K in L. We now want to calculate the genus of the function field $L|\kappa$. Since the genus is invariant under extension of the constant field, we can instead calculate the genus of $\overline{K}L|\overline{K}$.

Let r be the number of places of $\overline{K}(x)|\overline{K}$ which ramify in at least one of the $\overline{K}L_i|\overline{K}(x)$. By the above lemma this is equal to the number of ramified places of $\overline{K}L|\overline{K}(x)$. Let

$$\overline{m} := \dim_{\mathbb{F}_2}(\overline{U}). \tag{6}$$

Then by (5) $[\overline{K}L : \overline{K}(x)] = 2^{\overline{m}}$, and by the Hurwitz genus formula (see [21, III.5.6])

$$\begin{aligned} g(L|\kappa) = g(\overline{K}L|\overline{K}) &= 2^{\overline{m}}(0-1) + \tfrac{1}{2}r(2-1)\tfrac{2^{\overline{m}}}{2} + 1 \\ &= -2^{\overline{m}} + r2^{\overline{m}-2} + 1 = 2^{\overline{m}-2}(r-4) + 1. \end{aligned} \tag{7}$$

If $\overline{m} \geq 3$, $g(L|\kappa) = g(\overline{K}L|\overline{K})$ is odd. In particular:

[4] We would like to stress that the lemma is only valid because we assumed that $\mathrm{char}(K) \neq 2$. In particular, it cannot be applied to study the GHS attack in characteristic 2.

Lemma 12 *If $\overline{m} \geq 3$, $L|\kappa$ is not a rational function field.*

Applying this result to subextensions of $\overline{K}L|\overline{K}(x)$ – which by Lemma 8 all have the form $\overline{K}(x)[\sqrt[2]{\overline{V}}]$ for some vector subspace $\overline{V}$ of $\overline{U}$ –, we obtain: If $\overline{m} \geq 4$, $\overline{K}L|\overline{K}(x)$ does not contain a rational subfield of index 2. This implies:

Lemma 13 *If $\overline{m} \geq 4$, $L|K(x)$ does not contain a rational subfield of index 2.*

Proof Let $M|K(x)$ be a subfield of index 2. Then either $\overline{K}L|\overline{K}M$ is an extension of degree 2 or it is trivial. In both cases, $g(\overline{K}M|\overline{K}) \geq 1$. □

We will need the following explicit description of $K(x)^*/K^{*2}$.

Let P be the set of monic irreducible polynomials over K. Unique factorization in the ring $K[x]$ induces an isomorphism

$$\begin{aligned} K^* \oplus \textstyle\bigoplus_{p\in P} \mathbb{Z} &\xrightarrow{\sim} K(x)^*, \\ (c, (f_p)_{p\in P}) &\mapsto c \textstyle\prod_{p\in P} p^{f_p}. \end{aligned}$$

Thus

$$K^*/K^{*2} \oplus \textstyle\bigoplus_{p\in P} \mathbb{F}_2 \xrightarrow{\sim} K(x)^*/K(x)^{*2}\,. \tag{8}$$

Note that if K is finite (and as always $\mathrm{char}(K)$ is odd), $K^*/K^{*2} \simeq \mathbb{F}_2$.

5 Analysis of the GHS attack in odd characteristic

We now apply the above results to the special case of the GHS attack in odd characteristic with respect to an odd extension degree n.

Let k be a finite field of odd characteristic, $K|k$ an extension of odd degree n. Let H' be a (hyper-)elliptic curve of genus g, and let $K(H')|K(x)$ be an extension of degree 2.

As in Section 2, let F' be the Galois closure of $K(H')|k(x)$ inside $K(x)^{\mathrm{sep}}$. In order for the attack to be successful we assume (see Proposition 5):

For no intermediate field μ of $K|k$ with $\mu \subsetneq K$, $K(H')|\mu(x)$ is Galois.

The extension $K(H')|K(x)$ is given by a Weierstraß-equation of the form

$$y^2 = c\, f(x),$$

where f is a monic square-free polynomial of degree $2g+1$ or $2g+2$ and $c \in K^*$. By Kummer Theory we can change c by multiplication with an element of K^{*2}. Since $K^*/K^{*2} \simeq \mathbb{F}_2 \simeq k^*/k^{*2}$, we can choose $c \in k^*$ and we do so.

Now F' is generated over $K(x)$ by $y_0, \ldots, y_{n-1}$ where y_i satisfies

$$y_i^2 = c\,\sigma_{K|k}^{\,i}(f)(x).$$

Thus $F' = K(x)[\sqrt[2]{U}]$ where $U \subseteq K(x)^*/K(x)^{*2}$ is the vector subspace generated by the images $\underline{\sigma_{K|k}^{\,i}(f)}$ of $\sigma_{K|k}^{\,i}(f)$ in $K(x)^*/K(x)^{*2}$. Let $\overline{U}$ be the image of U in $\overline{K}(x)^*/\overline{K}(x)^{*2}$. Then by (5), the numbers m and $\overline{m}$ defined in (3) can be expressed as follows:

$$m = \dim_{\mathbb{F}_2}(U)\,, \quad \overline{m} = \dim_{\mathbb{F}_2}(\overline{U}). \tag{9}$$

Lemma 10 and Proposition 3 imply:

Proposition 14 *If $c = 1$, $F'|K$ is regular, and so is $F|k$.*

We fix the following notations: Let $\sigma_k \in \mathrm{Gal}(\overline{K}|k) \simeq \mathrm{Gal}(\overline{K}(x)|k(x))$ be the Frobenius automorphism relative to k. Analogously to $\sigma_{K|k}^{\,i}(K(H'))$ we define $\sigma_k^{\,i}(\overline{K}(H'))$. Then $\sigma_k^{\,i}(\overline{K}(H'))$ equals the composite $\overline{K}\,\sigma_{K|k}^{\,i}(K(H'))$. Moreover, $\overline{K}F' = \overline{K}(H')\,\sigma_k(\overline{K}(H')) \cdots \sigma_k^{\,n-1}(\overline{K}(H'))$.

We ask at which places $\overline{K}F'|\overline{K}(x)$ is ramified, i.e. by Lemma 11 which places of $\overline{K}(x)|\overline{K}$ ramify in at least one of the extensions $\sigma_k^{\,i}(\overline{K}(H'))|\overline{K}(x)$.

We identify the places of $\overline{K}(x)|\overline{K}$ with $\overline{P} \cup \{\infty\}$, where $\overline{P}$ is the set of monic linear polynomials over $\overline{K}$. The Frobenius σ_k operates on the places, and this operation corresponds to the operation on $\overline{P} \cup \{\infty\}$ induced by the operation on $\overline{K}(x)$ (where $\sigma_k(\infty) = \infty$).

The extension $\overline{K}(H')|\overline{K}(x)$ is ramified at some place $p \in P$ iff p divides f. (Note our assumption that f be square free.) It is ramified at ∞ iff the $\deg(f) = 2g + 1$. Let R be the set of ramified places of $\overline{K}(H')|\overline{K}(x)$, i.e. $\#R = 2g + 2$. Then $\sigma_k^{\,i}(\overline{K}(H'))|\overline{K}(x)$ is ramified exactly at $\sigma_k^{\,i}(R)$, and $\overline{K}F'|\overline{K}(x)$ is ramified exactly at $\bigcup_{i=0}^{n-1} \sigma_k^{\,i}(R)$. Let $r := \#\bigcup_{i=0}^{n-1} \sigma_k^{\,i}(R)$ be the number of ramified places of $\overline{K}F'|\overline{K}(x)$.

By (7) we obtain

$$g(F) = g(F') = 2^{\overline{m}-2}(r - 4) + 1. \tag{10}$$

The number $\overline{m}$ is obviously bounded from above by n. Further, $r \leq n \cdot \#R = n(2g + 2)$. Thus

$$g(F) \leq 2^{n-2}((2g + 2)n - 4) + 1 = 2^{n-1}((g + 1)n - 2) + 1. \tag{11}$$

We are searching for a lower bound for $g(F)$.

As in the last section, if $h \in K(x)^*$, we denote its image in $K(x)^*/K(x)^{*2}$ by $\underline{h}$. If $h \in \overline{K}(x)^*$, we denote its image in $\overline{K}(x)^*/\overline{K}(x)^{*2}$ by $\overline{\underline{h}}$.

Since $\overline{U}$ is $\overline{m}$-dimensional, there exist i_l, $l = 1, \ldots, \overline{m}$ such that $\overline{\sigma_{K|k}^{i_l}(f)}$ form a basis for $\overline{U}$. This means in particular that $\bigcup_{i=0}^{n-1} \sigma_k^i(R) = \bigcup_{l=1}^{\overline{m}} \sigma_k^{i_l}(R)$, and we have $r = \# \bigcup_{l=1}^{\overline{m}} \sigma_k^{i_l}(R) \leq \overline{m} \cdot \# R = \overline{m}(2g+2)$. This implies

$$\overline{m} \geq \lceil \frac{r}{2g+2} \rceil. \tag{12}$$

Here, for $x \in \mathbb{Q}$, $\lceil x \rceil$ denotes the smallest integer greater or equal x.

We now want to bound r from below by a function depending only on n. We use the fact that *by assumption* for no intermediate field μ of $K|k$ with $\mu \subsetneq K$, $\mathrm{Gal}(K(H'))|\mu(x))$ is Galois.

The group $\mathrm{Gal}(\overline{K}|k)$ operates on $\bigcup_{i=0}^{n-1} \sigma_k^i(R)$. Let $\mathrm{Gal}(\overline{K}|\Delta)$ be the kernel of the homomorphism $\mathrm{Gal}(\overline{K}|k) \longrightarrow \mathrm{Aut}(\bigcup_{i=0}^{n-1} \sigma_k^i(R))$.

Lemma 15 $K \subseteq \Delta$.

Proof We show $K = K \cap \Delta$. We have $\mathrm{Gal}(\overline{K}|K \cap \Delta) = \langle \mathrm{Gal}(\overline{K}|K) \cup \mathrm{Gal}(\overline{K}|\Delta) \rangle$. The polynomial $c\,f$ is fixed by both of these groups, thus it is fixed by $\mathrm{Gal}(\overline{K}|K \cap \Delta)$. It follows that $c\,f \in K \cap \Delta$, and this implies that $K(H')|K \cap \Delta(x)$ is Galois. It follows from the assumption that $K = K \cap \Delta$. □

By definition of Δ, we have an injective homomorphism

$$\mathrm{Gal}(\Delta|k) \hookrightarrow \mathrm{Aut}(\bigcup_{i=0}^{n-1} \sigma_k^i(R)). \tag{13}$$

Let $\delta := [\Delta : k]$, let $\delta = \prod_{p \text{ prime}} p^{\delta_p}$ be the prime decomposition of δ. By (13) we know that the cyclic group of order δ can be embedded in the symmetric group on r elements. This implies

$$r \geq \sum_{p, \delta_p \neq 0} p^{\delta_p}. \tag{14}$$

Let $n = \prod_{p \text{ prime}} p^{n_p}$ be the prime decomposition of n. By the above lemma, $n|\delta$, thus for all primes p, $n_p \leq \delta_p$. With (14), we obtain

$$r \geq \sum_{p, n_p \neq 0} p^{n_p}. \tag{15}$$

Inserting (12) and (15) into the right-hand side of (10), we obtain

$$g(F) \geq 2^{\lceil \frac{\sum_{p, n_p \neq 0} p^{n_p}}{2g+2} \rceil - 2} (\sum_{p, n_p \neq 0} p^{n_p} - 4) + 1 \tag{16}$$

Combining everything we obtain the following theorem.

Theorem 2 *Let $K|k$ be an extension of finite fields of odd characteristic and odd degree $n = \prod_{p \text{ prime}} p^{n_p}$. Let H' be a (hyper-)elliptic curve over K of genus g. Choose some extension $K(H')|K(x)$ of degree 2, given by an equation of the form $y^2 = c\,f(x)$ where f is monic and $c \in K^*$.*

Then via the GHS attack one obtains a function field F, regular over k or its unique quadratic extension, an extension $KF|K(H')$ of degree 2^m for some $m \leq n$, and a homomorphism from $\mathrm{Cl}^0(K(H'))$ to $\mathrm{Cl}^0(F)$ with the following properties:

- *If $c = 1$, $F|k$ is regular.*
- *$g(F) \leq 2^{n-1}((g+1)n - 2) + 1$.*
- *If there exists some field μ with $k \subseteq \mu \subsetneq K$ such that $K(H')|\mu(x)$ is Galois, there exists a regular function field $M|\mu$ with $KM = K(H')$ such that the homomorphism factors through $\mathrm{N}_{K(H')|M} : \mathrm{Cl}^0(K(H')) \longrightarrow \mathrm{Cl}^0(M)$.* [5]
- *If there does not exist such a μ, the kernel of the homomorphism contains only elements of order a 2-power and*

$$g(F) \geq 2^{\lceil \frac{\sum_{p, n_p \neq 0} p^{n_p}}{2g+2} \rceil - 2} (\sum_{p, n_p \neq 0} p^{n_p} - 4) + 1.$$

Proof The existence of F and the homomorphism was already shown in Section 2. The first point is Proposition 14, the second is (11), the third is Proposition 5, the fourth is (16). □

Further, by Lemma 13:

Proposition 16 *Let $\overline{m}$ be defined as in (9). If $\overline{m} \geq 4$, $F'|K(x)$ does not contain a rational subfield of index 2.*

Note that this is a major difference between the GHS attack in odd characteristic and in characteristic 2. Indeed, according to [8], if H' is an elliptic curve and K has characteristic 2, one can always choose an extension $K(H')|K(x)$ such that $F'|K(x)$ has a rational subfield of index 2.

6 Analysis for prime extension degree

Now let n be an odd prime. We will analyze the attack in more detail in this case and outline some possible applications as well as limitations of the attack.

[5] In cryptological applications, this means that the large subgroup of prime order of $\mathrm{Cl}^0(K(H'))$ is *not* preserved under the homomorphism.

Let the notations be as above and let n be prime. We still assume that $K(H')|k(x)$ *is not Galois*, i.e. that $K(H') \subsetneq F'$, for otherwise the attack fails.

Note that by (16),

$$g(F) \geq 2^{\lceil \frac{n}{2g+2} \rceil - 2}(n-4) + 1. \tag{17}$$

We want to give a new bound for $g(F)$ from below.

The operation of $\mathrm{Gal}(K|k) \simeq \mathrm{Gal}(K(x)|k(x))$ on $K(x)^*$ restricts to an operation on the subgroup $\langle K^* \cup K(x)^{*2} \rangle$, and we obtain an operation on $K(x)^*/\langle K \cup K(x)^{*2} \rangle$. This group is included in $\overline{K}(x)^*/\overline{K}(x)^{*2}$, and $\overline{U}$ is a subgroup of $K(x)^*/\langle K \cup K(x)^{*2} \rangle$. The operation of $\mathrm{Gal}(K|k)$ induces a non-trivial operation of $\mathrm{Gal}(K|k)$ on $\overline{U}$ which gives rise to a non-trivial operation of the group ring $\mathbb{F}_2[\mathrm{Gal}(K|k)]$ on $\overline{U}$. By construction, $\overline{U}$ is the image of $\overline{f} \in \overline{K}(x)^*/\overline{K}(x)^{*2}$ under the operation of $\mathbb{F}_2[\mathrm{Gal}(K|k)]$. As $\mathbb{F}_2[\mathrm{Gal}(K|k)] \simeq \mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]$, $\overline{U}$ is a cyclic $\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]$-module with a non-trivial operation by $\mathbb{Z}/n\mathbb{Z}$.

Definition For some natural number n, let $\varphi_2(n)$ be the multiplicative order of 2 modulo n, i.e. $\varphi_2(n) = [\mathbb{F}_2[\zeta_n] : \mathbb{F}_2]$.

Lemma 17 *Let n be an odd prime number. Let V be a cyclic $\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]$-module. Then*

$$\dim_{\mathbb{F}_2}(V) = \kappa\, \varphi_2(n) \text{ or } \dim_{\mathbb{F}_2}(V) = 1 + \kappa\, \varphi_2(n)$$

for some $\kappa = 0, \ldots, \frac{n-1}{\varphi_2(n)}$. If the operation by $\mathbb{Z}/n\mathbb{Z}$ is non-trivial, then $\kappa \geq 1$.

Proof Let $V = \mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]\, v$ for some $v \in V$, and let $\mathrm{Ann}(v) \lhd \mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]$ be the annihilator of v. Then as $\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]$-module, V is isomorphic to $\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]/\mathrm{Ann}(v)$.

On the other hand, we have canonical isomorphisms $\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}] \simeq \mathbb{F}_2[x]/(x^n - 1) \simeq \mathbb{F}_2 \oplus \mathbb{F}_2[x]/(x^{n-1} + \cdots + x + 1)$ of rings, and the ring $\mathbb{F}_2[x]/(x^{n-1} + \cdots + x + 1)$ is (non-canonically) isomorphic to $\mathbb{F}_2[\zeta_n]^{\frac{n-1}{\varphi_2(n)}}$. This implies the result on the dimension of V. □

We obtain:

$$\overline{m} = \kappa\, \varphi_2(n) \text{ or } \overline{m} = 1 + \kappa\, \varphi_2(n) \tag{18}$$

for some $\kappa = 1, \ldots, \frac{n-1}{\varphi_2(n)}$.

Remark Note the similarity of this result with the one obtained in [16] (our $\overline{m}$ corresponds to m in [16]). However, there is an important difference.

In odd characteristic we have the additional bound $\overline{m} \geq \lceil \frac{n}{2g+2} \rceil$ (see (12) and note that $r \geq n$ as n is prime).

Equations (10) and (18) imply (as $r \geq n$):

Proposition 18 *Let n be prime. Then additionally to the bound (17), we have the following bound for the genus of F.*

$$g(F) \geq 2^{\varphi_2(n)-2}(n-4)+1$$

We now want to outline explicit examples of applications of the attack for $n = 5, 7$ and elliptic curves $H' = E'$. Then we will show that for cryptographically suitable elliptic curves and prime extension degree $n \geq 11$, $\log_2((\#k)^{g(F)}) \geq 5000$.

In order to be able to describe the vector space $\overline{U}$ explicitly we make the following definition.

Let S be the set of monic linear polynomials of $\overline{K}$ which divide at least one of the $\sigma^i_{K|k}(f)$. If we identify the places of $\overline{K}(x)|\overline{K}$ with $\overline{P} \cup \{\infty\}$ where $\overline{P}$ is the set of monic linear polynomials of $\overline{K}$, $S = \bigcup_{i=0}^{n-1} \sigma^i_k(R) \backslash \{\infty\}$ where – as in the last section – R is the set of ramified places of $\overline{K}(H')|\overline{K}(x)$.

By (8), $\overline{U}$ is included in $\mathbb{F}_2^S$. Here, if $(e_s)_{s \in S}$ denotes the standard basis of $\mathbb{F}_2^S$, e_s corresponds to $\underline{\overline{s}} \in \overline{U}$.

6.1 $\mathbf{n = 5}$ [6]

If $H' = E'$ is an elliptic curve, by (17), the genus of F is bounded from below by 2, and by Proposition 18, it is bounded from below by 5. We will now give examples of elliptic curves for which $F|k$ is regular and the genus of F is indeed 5.

Let p be a prime and q a power of p. Let $k = \mathbb{F}_q, K = \mathbb{F}_{q^5}$. Let $a \in K \backslash k$, let

$$f(x) = (x-a)(x-a^q)(x-a^{q^2})(x-a^{q^3}) \in K(x).$$

Let E' be the elliptic curve over K given by $y^2 = f(x)$. Let $K(E')|K(x)$ be the extension given by this equation.

Since f is monic, $F|k$ is regular; see Theorem 2. We want to calculate $\overline{m}$ and then $g(F)$.

We have $S = \{x-a, x-a^q, x-a^{q^2}, x-a^{q^2}, x-a^{q^3}, x-a^{q^4}\}$, $r = 5$.

We regard the image of $\overline{U}$ under the inclusion into $\mathbb{F}_2^S$. We enumerate the elements of S by $x-a \leftrightarrow 1, \ldots, x-a^{q^4} \leftrightarrow 5$ and identify $\mathbb{F}_2^S$ with $\mathbb{F}_2^5$. Then $\underline{\overline{f}}$

[6]Results similar to the ones for $n = 5$ or $n = 7$ can be obtained for $n = 3$. In this case, there exist elliptic curves E' over K such that $g(F) = 3$ and $F|k$ is regular and even hyperelliptic. Since there is little hope that in the foreseeable future the DLP in class groups of genus 3 hyperelliptic curves can be more efficiently attacked via index calculus methods than with generic attacks, we omit the details.

corresponds to the vector $\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$, and $\overline{\sigma_{K|k}(f)}, \overline{\sigma_{K|k}{}^2(f)}, \overline{\sigma_{K|k}{}^3(f)}, \overline{\sigma_{K|k}{}^4(f)}$ correspond to the vectors $\begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$. Thus $\overline{m} = \dim_{\mathbb{F}_2}(\overline{U})$ equals the rank of the matrix

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

which is 4. With (10) we conclude: $F|k$ is regular and $g(F) = 2^{4-2}(5-4) + 1 = 5$.

Note that this means that up to small subgroups $E'(\mathbb{F}_q)$ and $\mathrm{Cl}^0(F)$ are isomorphic.

6.2 n = 7

We want to give elliptic curves for which F is regular and $g(F) = 7$.

Let q be as above, $k = \mathbb{F}_q, K = \mathbb{F}_{q^7}$. Let $a \in K \backslash k$, let

$$f(x) = (x-a)(x-a^q)(x-a^{q^2})(x-a^{q^4}) \in K(x).$$

Let E' be the elliptic curve over K given by $y^2 = f(x)$. Let $K(E')|K(x)$ be the extension given by this equation. Again $F|k$ is regular.

Then $S = \{x-a, x-a^q, \ldots, x-a^{q^6}\}$, $r = 7$. As above we identify $\mathbb{F}_2^S$ with $\mathbb{F}_2^7$.

Now $\underline{\overline{f}}$ corresponds to the vector $\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, $\overline{m}$ equals the rank of the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

The first three columns are linearly independent, and the sum of the first, the second and the fourth equals zero. This relation is preserved under shifting. Thus the fourth up to the seventh vectors are linearly dependent on the first three. So the rank of the matrix is 3.

We conclude again with (10): $F|k$ is regular and $g(F) = 2^{3-2}(7-4)+1 = 7$. Again up to small subgroups, $E'(K)$ and $\mathrm{Cl}^0(F)$ are isomorphic.

Remark The example was constructed in the following way: $x^7 - 1$ splits over $\mathbb{F}_2$ into $(x+1)(x^3+x^2+1)(x^3+x+1)$. Let s be the cyclic shifting in $\mathbb{F}_2^7$. Then application of $(s+1)(s^3+s^2+1) = (s^4+s^2+s+1)$ to the first vector of the standard basis yields the vector corresponding to $\underline{\overline{f}}$. It follows that s^3+s+1 applied to this vector is trivial and $\overline{U}$ is 3-dimensional.

6.3 $\mathbf{n \geq 11}$

Let $n \geq 11$ be a prime. We want to give explicit lower bounds on $q^{g(F)} \approx \#\mathrm{Cl}^0(F)$ for elliptic curves $H' = E'$.

Let q be a power of a prime, $k = \mathbb{F}_q$, $K = \mathbb{F}_{q^n}$. Let $H' = E'$ be an elliptic curve over K. Let $c := \log_2(q^n)$, thus $\log_2(q) = \frac{c}{n}$.

Since $n \geq 11 > 8$, (17) implies

$$g(F) > 2^{\lceil \frac{n}{4} \rceil - 2}(n-4) > 2^{\lceil \frac{n}{4} \rceil - 2}\frac{1}{2}n = 2^{\lceil \frac{n}{4} \rceil - 3}\, n.$$

Together with the definition of c, we obtain

$$\log_2(q^{g(F)}) = \frac{g(F)\, c}{n} > 2^{\lceil \frac{n}{4} \rceil - 3}\, c.$$

It follows that if $n \geq 29$, then

$$\log_2(q^{g(F)}) > 32.$$

We now use Proposition 18 to obtain lower bounds on $\log_2(q^{g(F)}) = \frac{g(F)\,c}{n}$ for $n = 11, 13, 17, 19, 23$.

n	$\varphi_2(n)$	$g(F)$	$\log_2(q^{g(F)})$
11	10	$\geq 2^{10-2}(11-4)+1 = 1793$	$\geq 163\,c$
13	12	$\geq 2^{12-2}(13-4)+1 = 9217$	$\geq 709\,c$
17	8	$\geq 2^{8-2}(17-4)+1 = 833$	$\geq 49\,c$
19	18	$\geq 2^{18-2}(19-4)+1 = 983041$	$\geq 51739\,c$
23	11	$\geq 2^{11-2}(23-4)+1 = 9729$	$\geq 423\,c$

We thus obtain the following result:

Proposition 19 *Let $K|k$ be an extension of finite fields of prime degree $n \geq 11$, let $H' = E'$ be an elliptic curve. Then $\log_2((\#k)^{g(F)}) \geq 32\log_2(\#K)$. In particular, if $E'(K)$ has cryptographically relevant size, i.e. $\log_2(\#K) \geq 160$, then $\log_2((\#k)^{g(F)}) > 5000$.*

7 Explicit equations

In this section, we continue the discussion of the examples of the last section for $n = 5$ and $n = 7$. We show how one can derive explicit equations of the resulting fields F.

We keep the notations of the previous sections. We start off more generally with n some odd integer.

7.1 Four lemmata

The following four lemmata will be used to calculate explicit equations of the fields F. The proofs of the first two of them are also valid in characteristic 2.

Lemma 20 *The inclusions $\sigma_{K|k}^i(K(H')) \longrightarrow F'$ induce an isomorphism*

$$F' \simeq K(H') \otimes_{K(x)} \sigma_{K|k}(K(H')) \otimes_{K(x)} \cdots \otimes_{K(x)} \sigma_{K|k}^{m-1}(K(H')).$$

Proof If $m = n$, the statement is obvious, so we assume that $m < n$.

Let i_0 be the largest integer such that $[K(H') \cdots \sigma_{K|k}^{i_0-1}(K(H')) : K(x)] = 2^{i_0}$. We claim that $K(H') \cdots \sigma_{K|k}^{i_0-1}(K(H')) = F'$. This implies that $i_0 = m$, and the statement of the lemma follows.

By definition of i_0, $\sigma_{K|k}^{i_0}(K(H')) \subseteq K(H') \cdots \sigma_{K|k}^{i_0-1}(K(H'))$. It follows that $K(H')\,\sigma_{K|k}(K(H')) \cdots \sigma_{K|k}^{i_0}(K(H')) = K(H')\,\sigma_{K|k}(K(H')) \cdots \sigma_{K|k}^{i_0-1}(K(H'))$. Now we proceed by induction: Assume that for some j with $i_0 \leq j < n-1$, $\sigma_{K|k}^{j} \subseteq K(H')\,\sigma_{K|k}(K(H')) \cdots \sigma_{K|k}^{i_0-1}(K(H'))$. Then $\sigma_{K|k}^{j+1}(K(H')) \subseteq \sigma_{K|k}(K(H')) \cdots \sigma_{K|k}^{i_0}(K(H')) \subseteq K(H') \cdots \sigma_{K|k}^{i_0}(K(H')) = K(H')\,\sigma_{K|k}(K(H')) \cdots \sigma_{K|k}^{i_0-1}(K(H'))$.

It follows that $K(H') \cdots \sigma_{K|k}^{i_0-1}(K(H')) = F'$. □

Let $g(x,y) \in K(x)[y]$ be a defining polynomial for $K(H')$ over $K(x)$. For $i = 0, \ldots, m$, choose a root y_i of $\sigma_{K|k}^{i}(g)(x,y)$ in $\sigma_{K|k}^{i}(K(H'))$.

Recall that $\mathrm{Gal}(K|k)$ operates by taking preimages and conjugation on $\mathrm{Gal}(F'|K(x))$.

Lemma 21 *If all elements of* $\mathrm{Gal}(F'|K(x))$ *have norm 1 under the operation of* $\mathrm{Gal}(K|k)$*, there exists an extension* $\widetilde{\sigma_{K|k}}$ *of* $\sigma_{K|k}$ *to* $F'|k(x)$ *of order* n *which operates in the following way:*

$$\widetilde{\sigma_{K|k}} : \; y_0 \mapsto y_1,\, y_1 \mapsto y_2, \ldots, y_{m-1} \mapsto y_m.$$

Proof Let $\widetilde{\sigma_{K|k}}$ be an extension of $\sigma_{K|k}$ to $F'|k(x)$ of order n.

Applying Lemma 20 to $\sigma_{K|k}(K(H'))$ instead of $K(H')$, we see that $F' \simeq \sigma_K(K(H')) \otimes_{K(x)} \cdots \otimes_{K(x)} \sigma_{K|k}^{m}(K(H'))$. This implies that there exists an $\alpha \in \mathrm{Gal}(F'|K(x))$ such that $\alpha \circ \widetilde{\sigma_{K|k}}$ operates as described in the statement of the lemma. Now $\alpha \circ \widetilde{\sigma_{K|k}}$ has order n as α has – by assumption – norm 1. Thus $\alpha\,\widetilde{\sigma_{K|k}}$ is an extension of $\sigma_{K|k}$ of order n which operates on the y_i as stated in the lemma. □

Lemma 22 *Assume that* $\overline{m} = m = \varphi_2(n)$*. Then there is no proper subfield of* $F|k(x)$*.*

Proof Lemma 17 implies that there is no proper subspace of U which is invariant under the operation of $\mathrm{Gal}(K|k)$. This implies that there is no proper subextension of $F'|K(x)$ which is invariant under the operation by $\mathrm{Gal}(K|k)$, and it follows that there is no proper subfield of $F|k(x)$. □

The condition of the Lemma is in particular fulfilled in the examples for $n = 5$ and $n = 7$ in the last section. When searching for "nice" equations for F, we have to cope with this unpleasant fact.

The Galois group $\mathrm{Gal}(K|k)$ operates on $\mathrm{Gal}(F'|K(x))$ as well as on U. Moreover, via the non-degenerate pairing (4) $\mathrm{Gal}(F'|K(x))$ is naturally isomorphic to the dual space of U. The following lemma shows that under this isomorphism the induced operation of $\mathrm{Gal}(K|k)$ on the dual space of U is the same as the operation on $\mathrm{Gal}(F'|K(x))$.

Lemma 23 *Under the pairing (4) we have:*
For $\alpha \in \mathrm{Gal}(F'|K(x))$, $u \in U$ *and* $\sigma \in \mathrm{Gal}(K|k)$, $\langle \sigma(\alpha), u\rangle = \langle \alpha, \sigma^{-1}(u)\rangle$.

Proof Let $\alpha \in \mathrm{Gal}(F'|K(x))$, $u \in U$, $\sigma \in \mathrm{Gal}(K|k)$, and let $\nu \in F'$ such that $\nu^2 = u$. Then $\langle \sigma(\alpha), u\rangle = \frac{\sigma\alpha\sigma^{-1}(\nu)}{\nu} = \sigma(\frac{\alpha(\sigma^{-1}(\nu))}{\sigma^{-1}(\nu)}) = \frac{\alpha(\sigma^{-1}(\nu))}{\sigma^{-1}(\nu)} = \langle \alpha, \sigma^{-1}(u)\rangle$. □

Let us assume – as is the case in the examples for $n = 5$ and $n = 7$ in the last section – that the constant c in the defining equation $y^2 = cf$ of $K(H')|K(x)$ is equal to 1. Then $U \simeq \overline{U}$, $m = \overline{m}$, and $F|k$ is regular; cf. Proposition 14. From the preceding lemma it follows in particular:

Let n be prime and assume that $m = \kappa\varphi_2(n)$ for some $\kappa = 1, \ldots \frac{n-1}{\varphi_2(n)}$ (instead of $m = 1 + \kappa\varphi_2(n)$); cf. (18). Then all elements $u \in U$ satisfy $u + \sigma_{K|k}(u) + \cdots + \sigma_{K|k}^{n-1}(u) = 0$, and thus all elements $\alpha \in \mathrm{Gal}(F'|K(x))$ satisfy $\alpha\,\sigma_{K|k}(\alpha)\cdots\sigma_{K|k}^{n-1}(\alpha) = \mathrm{id}$, i.e. they have norm 1.

The assumption $m = \kappa\varphi_2(n)$ holds in particular for the examples for $n = 5$ and $n = 7$. We can thus use Lemma 21 to extend $\sigma_{K|k}$ to $F'|k(x)$.

7.2 n = 5

We continue with the example in Subsection 6.1.

For $i = 0, 1, 2, 3$, let y_i be a root of the equation $y^2 = \sigma_{K|k}^i(f)$ in F'. Let

$$y_4 := y_0\, y_1\, y_2\, y_3 / [(x-a)(x-a^q)(x-a^{q^2})(x-a^{q^3})^2].$$

Then y_4 is a root of the equation $y^2 = \sigma_{K|k}^4(f)$. Let

$$z := y_0 + y_1 + y_2 + y_3 + y_4.$$

As $m = 4 = \varphi_2(5)$, all elements of $\mathrm{Gal}(F'|K(x))$ have norm 1, and thus there exists an extension $\widetilde{\sigma_{K|k}}$ of $\sigma_{K|K}$ to $F'|k(x)$ which operates by

$$y_0 \mapsto y_1,\; y_1 \mapsto y_2,\; y_2 \mapsto y_3,\; y_3 \mapsto y_4.$$

We fix this extension and obtain a subfield F of F' as in Proposition 3. It follows that z is invariant under $\mathrm{Gal}(F'|F) \simeq \mathrm{Gal}(K|k)$, thus z lies in F. We claim that it is a primitive element of $F|k(x)$.

By Lemma 22, we only have to show that z does not lie in $k(x)$. Assume that $z \in k(x)$. Then in particular, it is fixed by the automorphism α of $F'|K(x)$ given by $y_0 \mapsto -y_0$, $y_1 \mapsto y_1$, $y_2 \mapsto y_2, y_3 \mapsto y_3$. We obtain that $z = \alpha(z) = -y_0 + y_1 + y_2 + y_3 - y_4$. It follows that $y_0 + y_4 = 0$, a contradiction.

For $j = (j_0, j_1, j_2, j_3) \in \mathbb{F}_2^{\{0,1,2,3\}}$, let

$$z_j := (-1)^{j_0} y_0 + (-1)^{j_1} y_1 + (-1)^{j_2} y_2 + (-1)^{j_3} y_3 + (-1)^{j_0+j_1+j_2+j_3} y_4.$$

Then $z_{(0,0,0,0)} = z$, and the z_j are the Galois conjugates of z under the operation of $\mathrm{Gal}(F'|K(x))$.

The z_i are the images of z under all inclusions of F into F' fixing $K(x)$. It follows that the minimal polynomial of z in $F|k(x)$ is

$$h := \prod_{j \in \mathbb{F}_2^{\{0,1,2,3\}}} (T - z_j) \in k(x)[T].$$

All y_i are contained in the Galois closure of $K[x]$ in F', and so is z. It follows that h is contained in $K[x,T]$, thus it is contained in $k[x,T]$.

The polynomial h is a defining polynomial for $F|k(x)$. It has degree 16 in T, and its degree in x is bounded by 32.

Note that we have chosen a particular extension of $\sigma_{K|k}$ to $F'|k(x)$, thus by construction h is the defining polynomial for a particular extension $F|k(x)$ such that $F|k$ is regular and $KF = F'$. However, by Proposition 3 these extensions are all isomorphic, thus h defines all these extensions.

7.3 n = 7

Let us now continue the example in Subsection 6.2.

For $i = 0, 1, 2$, let y_i be a root of the equation $y^2 = \sigma_{K|k}^{i}(f)$ in F'. Let

$$\begin{aligned}
y_3 &:= y_0\, y_1/[(x - a^q)(x - a^{q^2})] \\
y_4 &:= y_1\, y_2/[(x - a^{q^2})(x - a^{q^3})] \\
y_5 &:= y_2\, y_3/[(x - a^{q^3})(x - a^{q^4})] \\
y_6 &:= y_3\, y_4/[(x - a^{q^4})(x - a^{q^5})].
\end{aligned}$$

Then for all $i = 1, \ldots, 6$, y_i is a root of the equation $y^2 = \sigma_{K|k}^{i}(f)$. Let

$$z := y_0 + y_1 + y_2 + y_3 + y_4 + y_5 + y_6.$$

As $m = 3 = \varphi_2(7)$, all elements of $\mathrm{Gal}(F'|K(x))$ have norm 1, and thus there exists an extension $\widetilde{\sigma_{K|k}}$ of $\sigma_{K|k}$ to $F'|k(x)$ which operates by

$$y_0 \mapsto y_1,\ y_1 \mapsto y_2,\ y_2 \mapsto y_3.$$

We fix this extension and obtain a subfield F of F' as in Proposition 3. By construction, z is invariant under the operation of $\widetilde{\sigma_{K|k}}$, thus it lies in F. We claim that it is a primitive element of $F|k(x)$, and again by Lemma 22 we only have to show that it does not lie in $k(x)$.

Assume that $z \in k(x)$. Then in particular, it is fixed by the automorphism α of $F'|K(x)$ given by $y_0 \mapsto -y_0$, $y_1 \mapsto -y_1$, $y_2 \mapsto -y_2$. We have $z = \alpha(z) = -y_0 - y_1 - y_2 + y_3 + y_4 - y_5 + y_6$. It follows that $y_0 + y_1 + y_2 + y_5 = 0$. Applying the automorphism of $F'|K(x)$ given by $y_0 \mapsto -y_0$, $y_1 \mapsto y_1$, $y_2 \mapsto y_2$

to this equation, we obtain $-y_0+y_1+y_2-y_5=0$. It follows that $y_1+y_2=0$, a contradiction.

For $j=(j_0,j_1,j_2)\in\mathbb{F}_2^{\{0,1,2\}}$, let

$$\begin{aligned} j_3 &:= j_0+j_1\\ j_4 &:= j_1+j_2\\ j_5 &:= j_2+j_3 = j_0+j_1+j_2\\ j_6 &:= j_3+j_4 = j_0+j_1+j_1+j_2 = j_0+j_2 \end{aligned}$$

Let

$$z_j := \sum_{i=0}^{6}(-1)^{j_i} y_i.$$

Then $z_{(0,0,0)}=z$, and the z_j are the Galois conjugates of z under the operation of $\mathrm{Gal}(F'|K(x))$.

Analogous to the previous case, the minimal polynomial of z in $F|k(x)$ is

$$h := \prod_{j\in\mathbb{F}_2^{\{0,1,2\}}}(T-z_j)\in k(x)[T].$$

Again this is contained in $k[x,T]$. The polynomial h is a defining polynomial for $F|k(x)$ as well as the other extensions $F_1|k(x)$ such that $F_1|k$ is regular and $KF_1=F'$. It is a polynomial of degree 8 in T, and its degree in x is bounded by 16.

We finish with an explicit calculation based on these results. [7]

Let $p:=10000019$, this is a prime such that p^7 has 163 bit, let $a\in\mathbb{F}_{p^7}$ be a root of the following irreducible polynomial in the polynomial ring $\mathbb{F}_p[A]$.

$$A^7+5581056A^6+1071250A^5+7891954A^4+3686323A^3+1634662A^2+5314472A+6311551$$

Let E' be the elliptic curve over $\mathbb{F}_{p^7}$ given by

$$y^2=(x-a)(x-a^p)(x-a^{p^2})(x-a^{p^4}).$$

The order of $E'(\mathbb{F}_{p^7})$ is $4\cdot l$ where l is prime and

$$l=2500033250189525600163640252013683579685963948773.$$

One checks that $[\mathbb{F}_p[\zeta_l]:\mathbb{F}_p]$, i.e. the multiplicative order of p modulo l, is $\geq 10\,000$, thus the DLP in $E'(\mathbb{F}_{p^7})$ is resistant against the attacks based on the Weil- and the Tate-Pairing; cf. [15], [4]. This means that up to now the elliptic curve E' would have been regarded as cryptographically suitable.

[7]The following explicit example was calculated using the MAGMA computer algebra package.

Via the approach presented above one finds the following defining polynomial for F.

$$T^8 + (9999991x^4 + 703275x^3 + 1430019x^2 + 1502111x + 6267729)\,T^6+$$
$$(9999907x^6 + 4219650x^5 + 4300171x^4 + 4915913x^3+$$
$$3056838x^2 + 7690930x + 4968619)\,T^5+$$
$$(9999809x^8 + 549106x^7 + 50570x^6 + 6963813x^5 + 631870x^4+$$
$$2499584x^3 + 7550175x^2 + 7984600x + 8893034)\,T^4+$$
$$(9999795x^{10} + 4065481x^9 + 5800988x^8 + 8738342x^7 + 5465058x^6 + 1967241x^5+$$
$$2095794x^4 + 4444654x^3 + 8381656x^2 + 2592793x + 8848697)\,T^3+$$
$$(9999879x^{12} + 549106x^{11} + 8650912x^{10} + 1059594x^9 + 9156513x^8+$$
$$9340731x^7 + 7885968x^6 + 6953996x^5 + 5734556x^4+$$
$$4113592x^3 + 2896371x^2 + 9062942x + 3377385)\,T^2+$$
$$(9999971x^{14} + 4219650x^{13} + 7180437x^{12} + 8192553x^{11} + 6767478x^{10}+$$
$$4323463x^9 + 3837644x^8 + 4788445x^7 + 3851x^6 + 4376874x^5+$$
$$1282375x^4 + 5472015x^3 + 6147853x^2 + 4182920x + 4970743)\,T+$$
$$10000012x^{16} + 703275x^{15} + 7150095x^{14} + 2321271x^{13} + 9233281x^{12}$$
$$+2141319x^{11} + 5465933x^{10} + 1278572x^9 + 3721128x^8 + 1041848x^7+$$
$$191179x^6 + 8523379x^5 + 9649232x^4 + 2099202x^3 + 5892994x^2+$$
$$9327110x + 3852461$$

One can check that F has genus 7 and that l divides the order of $\mathrm{Cl}^0(F)$.

Moreover, F has at least two Weierstrass places of degree 1. One of these places is given by the simultaneous vanishing of $x+7735061$ and $T+3901461$, the other by the simultaneous vanishing of $x + 8799748$ and $T + 1933887$. The first pole number is 7 in both cases.

The reader should be warned however that in a similar manner one can also give examples such that F does not have any Weierstrass place of degree 1.

8 Conclusions

We showed that in principle the GHS attack can be generalized from elliptic curves over finite non-prime fields of characteristic 2 to (hyper-)elliptic curves over finite non-prime fields of arbitrary characteristic – provided that the extension degree in consideration is odd. We then analyzed the genera of the resulting curves for the case that the characteristic is odd.

For elliptic curves and applications of the GHS attack with respect to prime extension degree n we showed: For $n \geq 11$, the size of $\mathrm{Cl}^0(F)$ is so large that the attack fails unless there is a breakthrough in the solution of the DLP in class groups of high genus curves.

However for $n = 5$ and $n = 7$, there exist elliptic curves such that the genus of F is 5 respectively 7. For these examples, explicit equations of the resulting fields F can be derived. These results are optimal in the sense that the degree 0 class group of F is then up to small subgroups isomorphic to the group of rational points on the elliptic curve. It would now be an interesting task to try to break the DLP in the class groups of the resulting fields F using index calculus methods. However, before one can do so, the known index calculus attacks first have to generalized from hyperelliptic to more general curves to cope with the fact that the explicit equations we derived are not hyperelliptic.

Finally, we would like to stress that it might be possible to apply other methods than the GHS attack to transform the original DLP into potentially easier DLPs in class-groups of curves of higher genera over smaller fields. In particular for elliptic curves E', just as in even characteristic, it might be possible to use the "extended GHS attack"; see [6]. Here, one first applies an isogeny and then uses the GHS attack for the isogenous curve.

A The GHS attack and the Weil restriction [8]

The GHS attack can be viewed as a special case of Frey's "Weil descent" idea; cf. [3]. This idea is based on the idea of finding "nice" smooth, projective, irreducible k-curves X which are (over k) birational to curves on the "Weil restriction" W/k of H' with respect to $K|k$ and then trying to transform the DLP from $\mathrm{Cl}^0(H')$ into a DLP in $\mathrm{Cl}^0(X)$. More concretely, if $E' = H'$ is an elliptic curve, the original idea was to transform the DLP in $E'(K)$ into the DLP in $W(k)$ (by the definition of W, $E'(K) \simeq W(k)$), and from there to $\mathrm{Jac}(X)(k) \simeq \mathrm{Cl}^0(X)$ by pull-back.

Originally, the consideration of the function field F (in characteristic 2) was motivated by the fact that it is the function field of a curve on the Weil restriction W/k. In this appendix, we make the relation between Frey's "Weil descent" idea and the GHS attack a little bit more explicit (and thereby try to point out a common inaccuracy concerning the GHS attack).

Let us first recall the definition of the Weil restriction.

Let $S' \longrightarrow S$ be a finite, flat morphism of locally noetherian schemes, let Y' be a (quasi)-projective S'-scheme.

It is well known that there exists a (quasi)-projective S-scheme $W = \mathrm{Res}_S^{S'}(Y')$, called the *Weil restriction* of Y' with respect to $S' \longrightarrow S$, with the following *universal property* (for a proof see [1, 7.6]):

There is a S'-morphism $w : W \times_S S' \longrightarrow Y'$ such that: For all S-schemes X and all K-morphisms $c : X \times_S S' \longrightarrow Y'$, there exists a unique S-morphism $b : X \longrightarrow W$ such that $c = w \circ (b \times_S \mathrm{id}_{S'})$. (Conversely, any $b : X \longrightarrow W$ defines in a unique way a $c : X \times_S S' \longrightarrow Y'$. In fact, set $c := w \circ (b \times_S \mathrm{id}_{S'})$.)

[8] In this appendix, we use the theory of arithmetic algebraic geometry as in [10].

As usual, W and w are unique up to a unique isomorphism. (The Weil restriction is usually defined as a representing object of the contravariant functor $\mathrm{Hom}_{S'}(-\otimes_S S', Y')$ from the category of S-schemes to the category of sets; cf. [1, 7.6]. The above mentioned universal property is an easy reformulation of this definition.)

Additionally, if $S' \longrightarrow S$ corresponds to an extension of fields $K|k$ and Y' is a K-variety, the Weil restriction W is a k-variety. Moreover, if Y' is geometrically reduced or geometrically irreducible or smooth, so is W, and if Y' is a abelian K-variety, (e.g. an elliptic curve), W is an abelian k-variety.

If S' and S are connected and $S' \longrightarrow S$ is Galois (in the sense of [9, V]), then $W \times_S S'$ is naturally isomorphic to $\prod_{\sigma \in \mathrm{Aut}(S' \longrightarrow S)} \sigma(Y')$, and under this isomorphism, $b \times_S \mathrm{id}_{S'} : X \times_S S' \longrightarrow Y'$ is given by $(\sigma(c))_{\sigma \in \mathrm{Aut}(S' \longrightarrow S)}$. Here, $\sigma(Y')$ is Y' regarded as a S' scheme via the structure morphism $Y' \longrightarrow S' \xrightarrow{\sigma} S'$.

We keep the notations of the article. We do not make an assumption on the characteristic of k, and we do not assume that $n = [K : k]$ is odd. However, we assume that as in Proposition 3, a function field $F|k$ which is linearly disjoint from $K|k$ and satisfies $K \otimes_k F \simeq KF = F'$ exists. [9]

Let $W := \mathrm{Res}_k^K(H')$ be the Weil restriction of H' with respect to $K|k$.

Under the bijection between isomorphism classes of function fields and isomorphism classes of normal, complete (projective), irreducible curves the field F corresponds to a normal (smooth, non-singular), projective, irreducible k-curve X.

As $K \otimes_k F \simeq KF$, the extension $KF|K(H')$ induces a covering (i.e. a finite morphism) $c : X_K = X \otimes_k K \longrightarrow H'$, and by the universal property of W this covering corresponds to a non-constant k-morphism from X to W.

We now describe this morphism more concretely. The extension $K(H')|K(x)$ corresponds to a covering $H' \longrightarrow \mathbb{P}^1_K$. Let $\mathrm{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(H')$ be the Weil restriction of H' with respect to $\mathbb{P}^1_K \longrightarrow \mathbb{P}^1_k$. This is a K-curve which is (in general) reducible. [10] By the universal property of $W = \mathrm{Res}_k^K(H')$, the universal morphism $\mathrm{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(H') \otimes_k K \simeq \mathrm{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(H') \times_{\mathbb{P}^1_k} \mathbb{P}^1_K \longrightarrow H'$ corresponds to a morphism $\mathrm{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(H') \longrightarrow \mathrm{Res}_k^K(H')$.

By the universal property of $\mathrm{Res}_k^K(\mathbb{P}^1_K)$, the identity $\mathrm{id} : \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K$ cor-

[9] For linear disjointness see [13, VIII, §3]. Note that if A is a field, $B|A$ is an algebraic extension of fields and $C|A$ is any extensions of fields, then the question whether $B|A$ and $C|A$ are linearly disjoint (in some common overfield) is equivalent to whether $B \otimes_A C$ is a field. In particular it is independent of the chosen common overfield of B and C.

[10] Let H' be an elliptic K-curve as in [8] (denoted there by E). Then in the situation of [8], the affine curve curve $\mathcal{C}$ studied in [8] is an affine open part of $\mathrm{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(H')$.

responds to a morphism $\mathbb{P}^1_k \longrightarrow \mathrm{Res}^K_k(\mathbb{P}^1_K)$ which is a closed immersion (see [1, 7.6, p. 197]), and $\mathrm{Res}^{\mathbb{P}^1_K}_{\mathbb{P}^1_k}(H')$ is naturally isomorphic to $\mathrm{Res}^K_k(H') \times_{\mathrm{Res}^K_k(\mathbb{P}^1_K)} \mathbb{P}^1_k$. The above morphism $\mathrm{Res}^{\mathbb{P}^1_K}_{\mathbb{P}^1_k}(H') \longrightarrow \mathrm{Res}^K_k(H')$ is induced by the morphism $\mathbb{P}^1_k \longrightarrow \mathrm{Res}^K_k(\mathbb{P}^1_K)$ via base-change, and as "closed immersion" is stable under base-change, it it is also a closed immersion.

Now, the covering $c : X_K \longrightarrow H'$ induces a morphism $X \longrightarrow \mathrm{Res}^{\mathbb{P}^1_K}_{\mathbb{P}^1_k}(H')$, and the morphism $X \longrightarrow \mathrm{Res}^K_k(H')$ factors through this morphism. [11]

The following argument shows that X is birational to its image in $\mathrm{Res}^{\mathbb{P}^1_K}_{\mathbb{P}^1_k}(H')$.

We only have to check this after base change. After base change $K|k$, the morphism $X \longrightarrow \mathrm{Res}^{\mathbb{P}^1_K}_{\mathbb{P}^1_k}(H')$ is given by

$$(\sigma^i_{K|k}(c))_{i=0}^{n-1} : \; X_K \longrightarrow H' \times_{\mathbb{P}^1_K} \sigma_{K|k}(H') \times_{\mathbb{P}^1_K} \cdots \times_{\mathbb{P}^1_K} \sigma^{n-1}_{K|k}(H').$$

(Where $\sigma_{K|k} : \mathrm{Spec}(K) \longrightarrow \mathrm{Spec}(K)$ is the automorphism corresponding to $\sigma_{K|k} : K \longrightarrow K$.)

On the total quotient rings, this morphism induces a homomorphism

$$K(H') \otimes_{K(x)} K(\sigma_{K|k}(H')) \otimes_{K(x)} \cdots \otimes_{K(x)} K(\sigma^{n-1}_{K|k}(H')) \longrightarrow F'.$$

By the very definition of F', this homomorphism is surjective, and it follows that X_K is birational to its image, i.e. it is the normalization of its image.

It follows also that X is the normalization of its image on W. Furthermore, one can show that – in the case that H' is an elliptic curve – the GHS-conorm-norm homomorphism is the same homomorphism as the one suggested by Frey (see above).

Not only the field F corresponds to a curve on the Weil restriction – whenever one is given a function field $A|k$, linearly disjoint to $K|k$, and a finite extension $K \otimes_k A \simeq KA|K(H')$, one obtains a smooth, projective, irreducible k-curve X with a covering $X_K \longrightarrow H'$. This induces a non-constant k-morphism $X \longrightarrow W$.

On the other hand, let X be a smooth, projective, irreducible k-curve with a k-morphism onto a k-curve on W and assume that X_K is also irreducible. Then the morphism $X \longrightarrow W$ induces a covering $X_K \longrightarrow H'$,

[11] Although it is stated correctly in [8] that the curve $\mathrm{Res}^{\mathbb{P}^1_K}_{\mathbb{P}^1_k}(H')$ is (in general) reducible, some authors seem to confuse $\mathrm{Res}^{\mathbb{P}^1_K}_{\mathbb{P}^1_k}(H')$ and its components. See for example the introductions to [6], [12], [16].

In particular, the proof of the existence of the function field F (our notation) given in [5, 4.2 and 4.5] is not correct as the author confuses (in [5, 4.2]) the curve $\mathrm{Res}^{\mathbb{P}^1_K}_{\mathbb{P}^1_k}(H')$ (our notation) with its components.

and this induces an extension $K(X_K)|K(H')$ of function fields. If we set $A := k(X)$, we obtain a function field $A|k$, linearly disjoint to $K|k$, and an extension $K \otimes_k A \simeq KA|K(H')$.

Moreover, one can show that if H' is an elliptic curve, just like in the GHS attack, the homomorphism $\mathrm{N}_{K(X_K)|k(X)} \circ \mathrm{Con}_{K(X_K)|K(H')} : H'(K) \simeq \mathrm{Cl}^0(K(H')) \longrightarrow \mathrm{Cl}^0(k(X))$ is the same homomorphism as the one suggested by Frey.

We thus obtain a possible reinterpretation of Frey's "Weil descent" idea in terms of covering theory of curves.

It is an interesting task to find other methods than the GHS attack for constructing suitable regular function fields $A|k$ with extensions $KA|K(H')$, or – what amounts to the same – to find suitable geometrically irreducible k-curves on the Weil restriction of H' with respect to $K|k$. But this is beyond the scope of this article.

Acknowledgments

It is a pleasure for me to thank G. Frey for introducing me to the subject and for fruitful discussions. I thank F. Hess for a discussion concerning Lemma 2.

The results in this article are based on results of my doctoral thesis. The thesis was supported by the Friedrich-Naumann-Stiftung, the Deutsche Forschungsgemeinschaft DFG and the Volkswagen Stiftung.

References

[1] S. Bosch, W. Lütkebohmert, and W. Raynaud. *Néron Models*. Springer-Verlag, Berlin, 1980.

[2] A. Enge and P. Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta. Arith.*, 102:83–103, 2002.

[3] G. Frey. How to disguise an elliptic curve (Weil descent). Talk at the 2nd Elliptic Curve Cryptography Workshop (ECC), 1998.

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

[5] S. Galbraith. Weil Descent Of Jacobians. In D. Augot and C. Carlet, editors, *Electronic Notes in Discrete Mathematics*, volume 6. Elsevier Science Publishers, 2001.

[6] S. Galbraith, F. Hess, and N. Smart. Extending the GHS Weil-Descent Attack. In *Eurocrypt 2002*, LNCS 2332, pages 29–44. Springer-Verlag, New York and Berlin, 2002.

[7] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in Cryptology, Eurocrypt 2000*, LNCS 1807, pages 19–34, New York and Berlin, 2000. Springer-Verlag.

[8] P. Gaudry, F. Hess, and N. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. Cryptology*, 15, 2002.

[9] A. Grothendieck. *Séminaire de Geometrie Algebrique 1960-61: Revêtements Etales et Groupe Fondamentale (SGA I).* Institut des Hautes Etudes Scientifiques, 1961.

[10] R. Hartshorne. *Algebraic Geometry.* Springer-Verlag, New York, 1977.

[11] B. Huppert. *Endliche Gruppen.* Springer-Verlag, Berlin, 1967.

[12] M. Jacobson, A. Menezes, and A. Stein. Solving Elliptic Curve Discrete Logarithm Problems Using Weil Descent. *J. Ramanujan Math. Soc.*, 16, 2001.

[13] S. Lang. *Algebra (Third Edition).* Addison-Wesley Publishing Company, 1993.

[14] M. Maurer, A. Menezes, and E. Teske. Analysis of the GHS Attack on the ECDLP over Characteristic Two Finite Fields of Composite Degree. *LMS Journal of Computation and Mathematics*, 5:127–174, 2002.

[15] A. Menezes, T. Okomoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in finite fields. *IEEE Transactions on Information Theory*, 39:1639–1646, 1993.

[16] A. Menezes and M. Qu. Analysis of the Weil Descent Attack of Gaudry, Hess and Smart. In *Topics in Cryptology - CT-RSA 2001*, LNCS 2020, pages 308–318. Springer-Verlag, 2001.

[17] S. Paulus and H.-G. Rück. Real and Imaginary Quadratic Representations of Hyperelliptic Function Fields. *Math. Comp.*, 227:1233–1241, 1999.

[18] H. Popp. *Fundamentalgruppen algebraischer Mannigfaltigkeiten.* Springer-Verlag, Berlin, 1970.

[19] H.-G. Rück. On the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 68:805–806, 1999.

[20] I. Semaev. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Math. Comp.*, 67:353–356, 1998.

[21] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, Berlin, 1993.

[22] Thériault. Weil-Descent Attack for Kummer Extensions. forthcomming.