An Attack on a Trace-Zero Cryptosystem

Claus Diem and Jasper Scholten

Institut für Experimentelle Mathematik, Universität Duisburg-Essen, Germany
and
ESAT / COSIC, K.U. Leuven, Belgium

Abstract. It was recently proposed in the literature that the discrete logarithm problem (DLP) in trace-zero groups of genus 2 curves with respect to constant field extensions of degree 3 is a fast and secure alternative to the well established cryptographic primitive of the DLP in elliptic curves over prime fields.
We present a novel attack on this primitive. We show that the DLP in the trace-zero group can always be transferred into the DLP in the class group of a curve of genus at most 6 over the prime field. Asymptotically, the DLP can be solved faster by transferring it into the DLP in the class group of this curve and using index calculus methods than by attacking it directly via generic methods. The speed-up one obtains corresponds to a reduction of 1/6th of the bit length.
We discuss practical aspects of our attack and argue that for cryptographically relevant group sizes (even for "low security" applications of 128 bit length), our attack always leads to a considerable speed-up in the calculation of the DLP in relation to generic attacks.

1 Introduction

The discrete logarithm problem (DLP) in elliptic curves is a well established cryptographic primitive for public key cryptosystems. After the publication of influential articles by Cantor ([2]) and Koblitz ([15], [14]), the DLP in degree 0 class groups (Jacobian groups) of hyperelliptic curves (of genus ≥ 2) received attention as an alternative cryptographic primitive. This primitive seemed to be particularly interesting from the point of view of implementation as for comparable group size the ground field is smaller (the degree 0 class group of a curve of genus g over $\mathbb{F}_q$ has roughly q^g elements), and if one chooses the parameters appropriately, elements of the ground field can completely fit into registers of the processor.

It was however subsequently shown that under some constraints on the genera of the curves one can mount *index calculus attacks* against the DLP in degree 0 class groups of hyperelliptic curves. In particular, it was shown by Gaudry ([7]) that for hyperelliptic curves over $\mathbb{F}_q$ of a fixed genus g the DLP in these groups can be attacked in a time of $\tilde{O}(q^2)$ bit operations (where the $\tilde{O}$-notation means that we disregard logarithmic factors). If one fixes a genus $g \geq 5$ and restricts ones attention to the cryptographically important case of hyperelliptic curves

over $\mathbb{F}_q$ which have a degree 0 class group of *prime order*, this is a speed-up against generic attacks like e.g. the ρ-method which have a heuristic running time of $\Theta(q^{g/2})$ group operations. Because of this result and previous results by Adleman, DeMarrais and Huang ([1]), hyperelliptic curves of genus ≥ 5 were soon considered to be cryptographically weak.

The main feature of Gaudry's index calculus algorithm is that the factor base consists of all points over the ground field. The asymptotical complexity is dominated by the linear algebra part. At the end of [7] an idea of Harley is mentioned which can be used to attack curves of genus 4: One reduces the factor base. With this idea one can solve the DLP in class groups of hyperelliptic genus 4 curves in $\tilde{O}(q^{(2-\frac{1}{5})}) = \tilde{O}(q^{\frac{9}{5}})$ bit operations. This idea was subsequently analyzed by Thériault who combined it with another method: A large prime variation. With this approach one can asymptotically even solve the DLP in class groups of hyperelliptic genus 3 curves faster than with generic attacks: One obtains a speed-up corresponding to the reduction of the bit length by $1/21^{\text{th}}$ in comparison with generic attacks. (In the meantime, with a double large prime variation, Gaudry, Thériault, Thomé ([9]) and Nagao ([19])[1] have shown that this DLP can even be solved in $\tilde{O}(q^{4/3})$ bit operations, which is equivalent to a reduction of the bit length by $1/9^{\text{th}}$.)

Because of these results, it has been a challenging task to find new alternatives to elliptic curves for which – at least for cryptographically relevant group sizes – no attack which improves the well-known generic attacks is known. One of these alternatives seemed to be trace-zero groups of degree 0 class groups of genus 2 curves with respect to constant field extensions of degree 3 of prime fields $\mathbb{F}_p$. In [18], Lange argues that they are a fast alternative to elliptic curves over prime fields or degree 0 class groups of genus 2 curves over prime fields, especially for "low security" applications of just below 128 bit group size. (However, in [18] there is an example with 192 bit group size as well.)

Let p be a prime number and let $\mathcal{H}/\mathbb{F}_p$ be a genus 2 curve, explicitly given by a hyperelliptic equation $y^2 = f(x)$ with $\deg(f) = 5$. The cryptographic primitive discussed in [18] is the DLP in the *trace-zero group* $\mathcal{T}$ inside the degree 0 divisor class group $\mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3})$ (for definition of $\mathcal{T}$ see next section). We note that $\mathcal{T}$ has roughly p^4 elements.

In this work, we present an attack on this primitive. Our attack is based on a method which allows to transfer the DLP in $\mathcal{T}$ into the DLP in the degree 0 class group $\mathrm{Cl}^0(\mathcal{X}/\mathbb{F}_p)$ for a curve $\mathcal{X}/\mathbb{F}_p$ of genus at most 6. Given an explicit hyperelliptic equation of $\mathcal{H}/\mathbb{F}_p$, the algorithmic construction of $\mathcal{X}/\mathbb{F}_p$ can be performed in randomized polynomial time in $\log(p)$ and is very fast for cryptographically relevant size. This shows that the DLP in $\mathcal{T}$ cannot be stronger than the DLP in the resulting group $\mathrm{Cl}^0(\mathcal{X}/\mathbb{F}_p)$.

The reduced factor base index calculus algorithms (possibly with large prime variation) can easily be generalized from hyperelliptic to more general curves

[1] We were informed by Thériault that the algorithm in [19] is not correct as it is presented.

like the curves $\mathcal{X}/\mathbb{F}_p$ constructed by our method. With the double-large prime variation algorithm ([9], [19]), one obtains the following result (see Section 5).

Theoretical result *Let $a, b \in \mathcal{T}$ such that $b \in \langle a \rangle$. Then the DLP with respect to a and b can be solved in a randomized running time of*

$$\tilde{O}(p^{2(1-\frac{1}{6})}) = \tilde{O}(p^{\frac{5}{3}}).$$

This result should be compared with the running times of generic attacks on the DLP in $\mathcal{T}$: If one restricts ones attention to trace-zero groups $\mathcal{T}$ of prime group order, generic attacks (like e.g. the ρ-method) give a running time of $\Theta(\sqrt{\#\mathcal{T}}) = \Theta(p^2)$ group operations in $\mathcal{T}$. The asymptotic speed-up corresponding to a reduction of $1/6^{\text{th}}$ of the bit length in relatsion to generic attacks is larger than the asymptotic speed-up of the recent index calculus with reduced factor base and a double-large prime variation for genus 3 curves.

We are also interested in the question whether our approach leads to a speed-up under parameter sizes proposed by Lange. To simplify the analysis, here we restrict our attention to the reduced factor base algorithm without large prime variation. In Section 6 we argue that our approach leads to the following practical result.

Practical result *Assume that $\mathcal{T}$ has prime group order and a size at least 128 bit. Then with our method, one obtains a speed-up for the calculation of the DLP which is equivalent to a reduction of the bit length of* at least *3 %. This decrease becomes larger for growing group size and reaches 14 % ($1/7^{th}$) in the limit. The storage requirements are thereby bounded by $\kappa \cdot p$ field elements for some small constant κ.*

This result holds if one compares the running time of our attack with the running time of generic attacks on $\mathcal{T}$ as well as with generic attacks on the DLP in elliptic curves (with prime group order) over prime fields of comparable size.

2 A trace-zero cryptosystem

Let us describe the cryptographic primitive presented in [18] in more detail:

Let p be a prime, and let $\mathcal{H}/\mathbb{F}_p$ be a genus 2 curve, given by an explicit equation of the form

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

where $f(x) \in \mathbb{F}_p[x]$ has degree 5. Now consider the curve $\mathcal{H}$ over the degree 3 constant field extension of $\mathbb{F}_{p^3}$ of $\mathbb{F}_p$ and its degree 0 (divisor) class group $\mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3}) \simeq \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{p^3})$ (which is denoted by $\mathrm{Pic}^0_{\mathbb{F}_{p^3}}(\mathcal{H})$ in [20]). This group contains the degree 0 class group $\mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_p) \simeq \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_p)$ of $\mathcal{H}$ over $\mathbb{F}_p$.

Let $\sigma \in \mathrm{Gal}(\mathbb{F}_{p^3}/\mathbb{F}_p)$ be the Frobenius automorphism. This automorphism induces an automorphism σ^* on $\mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3})$. This automorphism fixes the elements

of $\mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_p)$, and it induces a homomorphism $\mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3}) \longrightarrow \mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3})$, $P \mapsto P + \sigma^*(P) + (\sigma^2)^*(P)$. The trace-zero subgroup $\mathcal{T}$ of $\mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3})$ is by definition the kernel of this homomorphism.

For later use we remark that $\mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_p)$ consists exactly of the elements of $\mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3})$ which are fixed by σ^*. It follows that the image of the homomorphism $\mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3}) \longrightarrow \mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3})$ lies in $\mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_p)$. The induced homomorphism

$$\mathrm{N} : \mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3}) \longrightarrow \mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_p)$$

is called the *norm-homomorphism*, the trace-zero group $\mathcal{T}$ is the kernel of this homomorphism.[2]

The cryptographic primitive discussed in [18] is the DLP in the trace-zero group $\mathcal{T}$. It is argued that for "low-security" applications with just below 128 bit length on a 32-bit processor, this primitive is advantageous to the DLP in elliptic curves over prime fields. The main reasons for this are that one can use the Frobenius operation to speed up scalar multiplications and that under the condition on the bit length, field elements completely fit into registers of the processor.

3 The general idea

Before we come to the details of our attack, we give here some information on the ideas behind our construction. The basic idea is to try to find (smooth, projective) curves $\mathcal{C}/\mathbb{F}_p$ with covers (i.e. non-constant morphisms)

$$c : \mathcal{C}/\mathbb{F}_{p^3} \longrightarrow \mathcal{H}/\mathbb{F}_{p^3} \tag{1}$$

and then to consider the homomorphism

$$\mathcal{T} \hookrightarrow \mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3}) \xrightarrow{c^*} \mathrm{Cl}^0(\mathcal{C}/\mathbb{F}_{p^3}) \xrightarrow{\mathrm{N}} \mathrm{Cl}^0(\mathcal{C}/\mathbb{F}_p) \tag{2}$$

induced by this cover. (Here c^* is the pull-back homomorphism defined (e.g.) in [20, II, §3], and N is the norm-homomorphism which is defined analogously to the norm-homomorphism above.) The idea is that if the genus of $\mathcal{C}$ is not "too large" and the kernel of the "transfer homomorphism" (2) is small, it might be possible to transfer the DLP in $\mathcal{T}$ into the DLP in $\mathrm{Cl}^0(\mathcal{C}/\mathbb{F}_p)$ and to solve it there with index-calculus methods.

The main question is how to construct suitable curves $\mathcal{C}/\mathbb{F}_p$ and covers c. A first idea would be to consider a cover

$$c : \mathcal{C}/\mathbb{F}_p \longrightarrow \mathcal{H}/\mathbb{F}_p \tag{3}$$

[2] As we write the composition of two divisors in an additive way and as $\mathcal{T}$ is called the "trace-zero group", it would be reasonable to speak of the "trace-homomorphism" instead of the "norm-homomorphism". The terminology "norm-homomorphism" has historical reasons and comes from an ideal-theoretic setting.

and the corresponding transfer homomorphism

$$\mathcal{T} \hookrightarrow \mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3}) \xrightarrow{c^*} \mathrm{Cl}^0(\mathcal{C}/\mathbb{F}_{p^3}) \xrightarrow{\mathrm{N}} \mathrm{Cl}^0(\mathcal{C}/\mathbb{F}_p). \tag{4}$$

However, by the definition of c as a morphism defined over $\mathbb{F}_p$, we have a commutative diagram

$$\begin{array}{ccccc} \mathcal{T} & \longrightarrow & \mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3}) & \xrightarrow{c^*} & \mathrm{Cl}^0(\mathcal{C}/\mathbb{F}_{p^3}) \\ & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{N}} \\ & & \mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_p) & \xrightarrow{c^*} & \mathrm{Cl}^0(\mathcal{C}/\mathbb{F}_p), \end{array}$$

and by the definition of $\mathcal{T}$ as the kernel of $\mathrm{N} : \mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3}) \longrightarrow \mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_p)$, it follows that homomorphism (4) is trivial.

The basic idea of our approach is to construct covers $c : \mathcal{C}/\mathbb{F}_p \longrightarrow \mathcal{H}/\mathbb{F}_p$ such that additionally $\mathcal{C}/\mathbb{F}_p$ has an automorphism τ of order 3 such that $c \circ \tau \neq c$. Then we consider the twist $\mathcal{C}^\tau/\mathbb{F}_p$ of $\mathcal{C}/\mathbb{F}_p$ with respect to the constant field extension $\mathbb{F}_{p^3}/\mathbb{F}_p$ and τ described in [20, X §2]. By definition of $\mathcal{C}^\tau$, we have an isomorphism $\phi : \mathcal{C}^\tau/\mathbb{F}_{p^3} \xrightarrow{\sim} \mathcal{C}/\mathbb{F}_{p^3}$. Instead of the cover (3) we now consider the cover

$$c \circ \phi : \mathcal{C}^\tau/\mathbb{F}_{p^3} \longrightarrow \mathcal{H}/\mathbb{F}_{p^3}$$

and the corresponding transfer homomorphism

$$\mathcal{T} \hookrightarrow \mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3}) \xrightarrow{c^*} \mathrm{Cl}^0(\mathcal{C}/\mathbb{F}_{p^3}) \xrightarrow{\phi^*} \mathrm{Cl}^0(\mathcal{C}^\tau/\mathbb{F}_{p^3}) \xrightarrow{\mathrm{N}} \mathrm{Cl}^0(\mathcal{C}^\tau/\mathbb{F}_p). \tag{5}$$

In the next sections we show how one can use Galois theory and Riemann-Roch spaces to construct suitable covers such that the kernel of the transfer homomorphism (5) is always small.

Comparison with the GHS attack

The idea to try to attack the DLP in class groups of curves of low genus (in particular in the group of rational points of an elliptic curve) by using a cover as (1) is also used in the GHS attack (this aspect of the GHS attack was already present in the original work [8], and it was stressed in [4], [11], [12] and [13]). In this sense our attack is similar to the GHS attack. Our concrete construction is however different from the GHS attack.

4 Methods and results

Curves and function fields

In the rest of this work, we assume that the reader is familiar with the theory of curves as well as the theory of function fields (in one variable) and with Galois

theory. Concerning curves, our notation follows [20]. A good introduction to the theory of function fields is [21], and in Appendix A of the same book all results on Galois theory we need are stated.

Let us recall the equivalence of the theories of curves and function fields. Let K be a perfect field (e.g. a finite field).

To every curve $\mathcal{X}/K$ one can associate its function field $K(\mathcal{X})$ which consists of morphisms ("functions") $\mathcal{X}/K \longrightarrow \mathbb{P}^1/K$. (We regard $\mathbb{P}^1/K$ with a fixed coordinate system which identifies $\mathbb{P}^1(\overline{K})$ with $\mathbb{A}^1(\overline{K})\dot{\cup}\{\infty\} = \overline{K}\dot{\cup}\{\infty\}$, where $\overline{K}$ is an algebraic closure of K). The "field of constants" K is algebraically closed in $K(\mathcal{X})$ (one says that K is the *exact/full constant field* of $K(\mathcal{X})/K$ or that $K(\mathcal{X})/K$ is *regular* (cf. [17, VIII, §4])). Conversely, to every function field F/K with exact constant field K, one can associate in an essentially unique way a curve $\mathcal{X}$ with $K(\mathcal{X}) \simeq F$. Moreover, the points in $\mathcal{X}(K)$ correspond bijectively to places (equivalence classes of valuations) of degree 1 of F/K. We denote a point of a curve $\mathcal{X}/K$ and the corresponding place by the same letter.

If $c : \mathcal{X}/K \longrightarrow \mathcal{Y}/K$ is a cover, then we have an induced inclusion $K(\mathcal{Y}) \hookrightarrow K(\mathcal{X})$ which is given by $(a : \mathcal{Y}/K \longrightarrow \mathbb{P}^1/K) \mapsto (a \circ c : \mathcal{X}/K \longrightarrow \mathbb{P}^1/K)$. Conversely, every inclusion of function fields induces a cover of the corresponding curves.

Finally, we recall: If $\mathcal{X}/K$ is a curve, and D a divisor on $\mathcal{X}/K$, then the *Riemann-Roch space* associated to D is the space

$$\mathcal{L}(D) := \{\phi \in K(\mathcal{X}) |\ (\phi) \geq -D\} \cup \{0\}.$$

Similarly, one can define a Riemann-Roch space in $\overline{K}(\mathcal{X})$ which we denote by the same symbol. To distinguish the two, we write $\mathcal{L}(D) \subset K(\mathcal{X})$ or $\mathcal{L}(D) \subset \overline{K}(\mathcal{X})$. By the Riemann-Roch theorem ([21, I.5.15]), these are finite dimensional vector spaces.

Our construction

As in the introduction, let $\mathcal{H}/\mathbb{F}_p$ be a genus 2 curve. We assume that $\mathcal{H}$ is given by an explicit hyperelliptic explicit equation $y^2 = f(x)$, where – a bit more general than in [18] – $f(x)$ has degree 5 or 6. We further assume that p is not 2 or 3.

Let $H := \mathbb{F}_p(\mathcal{H})$ be the function field of $\mathcal{H}$. We remark that for almost all points P in $\mathcal{H}(\overline{\mathbb{F}}_p)$ the space $\mathcal{L}(2P) \subset \overline{\mathbb{F}}_p H$ consists only of the constant functions. However for the 6 fixed points $P \in \mathcal{H}(\overline{\mathbb{F}}_p)$ of the hyperelliptic involution, one has $\dim(\mathcal{L}(2P)) = 2$. (Explicitly, these 6 points are the 5 or 6 points with x-coordinate 0 and additionally the unique point "at infinity" if $\deg(f) = 5$.) These 6 points are called the *Weierstraß Points* of $\mathcal{H}$. We also recall that by the Riemann-Roch theorem, for any point $P \in \mathcal{H}(\overline{\mathbb{F}}_p)$, $\mathcal{L}(3P) \subset \overline{\mathbb{F}}_p H$ is 2-dimensional.

The prerequisite for our construction is as follows:

Let P be a point in $\mathcal{H}(\mathbb{F}_p)$ which is not a Weierstraß point and which is not a fixed point of an automorphism of order 3. Let $\mathcal{L}(3P) \subset H$ be the Riemann-Roch space associated to $3P$, and let $w \in \mathcal{L}(3P)$ be a non-constant function.

As there are at most 6 Weierstraß points in $\mathcal{H}(\mathbb{F}_p)$ and only a bounded (in fact ≤ 16) number of fixed points of automorphisms of order 3 (usually $\mathcal{H}/\overline{\mathbb{F}}_p$ has no automorphisms of order 3), in cryptographic applications, essentially every point $P \in \mathcal{H}(\mathbb{F}_p)$ fulfills the prerequisites. How to find the function w is discussed in Section 5, as are all other algorithmic questions. In this section, we concentrate on the theoretical background of the construction.

Lemma 1. *The extensions $H/\mathbb{F}_p(w)$ and $\overline{\mathbb{F}}_pH/\overline{\mathbb{F}}_p(w)$ are of degree 3, separable and not Galois.*

Proof. Let $(w)_\infty$ be the pole-divisor of w. By definition of w as a non-constant element of $\mathcal{L}(3P)$, $(w)_\infty$ can only be $3P, 2P$ or P. We can rule out the cases $2P$ and P as by assumption $\mathcal{L}(2P)$ consists only of the constant functions. As $(w)_\infty$ has degree 3, so has the cover $w : \mathcal{H} \longrightarrow \mathbb{P}^1$. This implies that $[H : \mathbb{F}_p(w)] = [\overline{\mathbb{F}}_pH : \overline{\mathbb{F}}_p(w)] = 3$.

The extensions are separable as by assumption $p \neq 3$.

We only have to show that $\overline{\mathbb{F}}_pH/\overline{\mathbb{F}}_p(w)$ is not Galois. To prove this, note that by definition of w as an element of $\mathcal{L}(3P)$, the place P is totally ramified in the extension $\overline{\mathbb{F}}_pH/\overline{\mathbb{F}}_p(w)$. Now, if $\overline{\mathbb{F}}_pH/\overline{\mathbb{F}}_p(w)$ was Galois, it would be cyclic (of order 3), and the ramified places of $\overline{\mathbb{F}}_pH$ with respect to $\overline{\mathbb{F}}_pH/\mathbb{F}_p(w)$ would be exactly the the fixed points of a non-trivial automorphism of $\overline{\mathbb{F}}_pH/\overline{\mathbb{F}}_p(w)$. We have however assumed that that P is not such a fixed point. □

Let C be the Galois closure of the extension $H/\mathbb{F}_p(w)$. As $\overline{\mathbb{F}}_pH/\overline{\mathbb{F}}_p(w)$ is not Galois, we have that $\overline{\mathbb{F}}_pC/\overline{\mathbb{F}}_pH$ is non-trivial. As the Galois group of a degree 3 extension is either $\mathbb{Z}/3\mathbb{Z}$ or S_3, it follows that the Galois group of $\overline{\mathbb{F}}_pC/\overline{\mathbb{F}}_p(w)$ is S_3. This implies: $\mathbb{F}_p$ is the exact constant field of C and the Galois group of $C/\mathbb{F}_p(w)$ is also S_3. In particular, there exists an automorphism τ of $C/\mathbb{F}_p(w)$ of order 3.

By fixing H, the Frobenius automorphism $\sigma \in \mathrm{Gal}(\mathbb{F}_{p^3}/\mathbb{F}_p)$ extends to an automorphism of $\mathbb{F}_{p^3}H$ which we also denote by σ. We now consider the fixed field $(\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}$ of $\mathbb{F}_{p^3}C$ under $\sigma\tau$. As τ operates trivially on $\mathbb{F}_{p^3}$, one can easily see that $\mathbb{F}_p$ is the exact constant field of $C^{\langle\sigma\tau\rangle}$.

Just as the group $\mathrm{Cl}^0(C)$ consists of the elements of $\mathrm{Cl}^0(\mathbb{F}_{p^3}C)$ which are fixed under σ^*, $\mathrm{Cl}^0((\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle})$ consists of the elements of $\mathrm{Cl}^0(\mathbb{F}_{p^3}C)$ which are fixed under $(\sigma\tau)^*$.

It is the degree 0 class group of this field in which we want to transfer the original DLP. We do so with the following "transfer homomorphism".

$$\mathcal{T} \hookrightarrow \mathrm{Cl}^0(\mathbb{F}_{p^3}H) \xrightarrow{\mathrm{Con}} \mathrm{Cl}^0(\mathbb{F}_{p^3}C) \xrightarrow{\mathrm{N}} \mathrm{Cl}^0((\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}). \tag{6}$$

Here, $\mathrm{Con} : \mathrm{Cl}^0(\mathbb{F}_{p^3}H) \longrightarrow \mathrm{Cl}^0(\mathbb{F}_{p^3}C)$ is the conorm-homomorphism (cf. [21, Definition III. 1.8]) and $\mathrm{N} : \mathrm{Cl}^0(\mathbb{F}_{p^3}C) \longrightarrow \mathrm{Cl}^0((\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle})$ is the norm-homomorphism. The latter homomorphism is given by

$$\mathrm{Cl}^0(\mathbb{F}_{p^3}C) \longrightarrow \mathrm{Cl}^0(\mathbb{F}_{p^3}C),\ P \mapsto P + (\sigma\tau)^*(P) + ((\sigma\tau)^2)^*(P)$$

and identification of the image (which is $(\sigma\tau)^*$-invariant) with an element of $\mathrm{Cl}^0((\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle})$.

For comparison with Section 3, note that $(\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}$ is the function field of the twist $\mathcal{C}^\tau/\mathbb{F}_p$ of $\mathcal{C}/\mathbb{F}_p$ with respect to τ and the constant field extension $\mathbb{F}_{p^3}/\mathbb{F}_p$.

The main results concerning the resulting function field $(\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}$ and the transfer homomorphism (6) are formulated in the following proposition.

Proposition 1. *Let $\mathcal{H}/\mathbb{F}_p$, $w \in H$ and $(\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}$ be defined as above. Then*

a) every non-trivial element in the kernel of the transfer homomorphism (6) has order 3.
b) the resulting function field $(\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}$ has genus ≤ 6.

A *proof* of item a) is sketched in Appendix A, a proof of item b) is sketched in Appendix B.

Remark 1. The condition that the ground field $\mathbb{F}_p$ is a prime field is not necessary. All statements in this work can be generalized to hyperelliptic curves over finite fields of characteristic $\neq 2, 3$.

Remark 2. As mentioned in Appendix B, under a certain arithmetic condition, w can be chosen such that $(\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}$ has genus ≤ 5. This leads to a slightly better attack. For this reason, curves satisfying that condition were excluded from [18]. Furthermore, if one chooses the defining polynomial $f \in \mathbb{F}_p[x]$ of degree 5 or 6, the point $P \in \mathcal{H}(\mathbb{F}_p)$ and the function $w \in \mathcal{L}(3P) \subset H$ uniformly at random, the probability that $g((\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}) \leq 5$ is in $O(\frac{1}{p})$ and thus negligible for large p.

5 Algorithmic aspects

As above, let $f \in \mathbb{F}_p[x]$ be an explicitly given square-free polynomial of degree 5 or 6. We keep all notations from the previous section. Furthermore, we assume that $p \geq 53$. The reason is that under this assumption, by the "Serre bound" ([21, Theorem V.3.1]), one has $\#\mathcal{H}(\mathbb{F}_p) \geq 26 > 22 = 6 + 16$, thus there are points which are not Weierstraß points and not fixed points of an automorphism of order 3.

It follows an outline of an algorithm to calculate $(\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}$. After that we also discuss how to map elements from $\mathcal{T}$ to $\mathrm{Cl}^0((\mathbb{F}_{p^3}H)^{\langle\sigma\tau\rangle})$ via the transfer homomorphism (6).

Algorithm: Calculation of $(\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}$ (Outline)

Input. A prime $p \geq 53$ and a square-free polynomial $f \in \mathbb{F}_p[x]$ of degree 5 or 6, defining the hyperelliptic curve $\mathcal{H}/\mathbb{F}_p$ (or the hyperelliptic function field H).

Output. An explicit description of the field $(\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}$ as an extension of $\mathbb{F}_p(w)$ as well as two elements $\tilde{x}$ and $\tilde{y} \in \mathbb{F}_{p^3}(\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}$ that satisfy the equation $\tilde{y}^2 = f(\tilde{x})$ and define the inclusion $H \hookrightarrow \mathbb{F}_{p^3}(\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle} = \mathbb{F}_{p^3}C$.

1. Choose a random point $P \in \mathcal{H}(\mathbb{F}_p)$ which does not have x-coordinate 0 or ∞.
2. Calculate a basis of $\mathcal{L}(3P) \subset H$.
3. Choose a non-constant function $w \in \mathcal{L}(3P)$.
4. Find the minimal polynomial m_0 of x over $\mathbb{F}_p(w)$.
5. Let $\Delta \in \mathbb{F}_p(w)$ be the discriminant of m_0. If Δ is a square in $\mathbb{F}_p[\zeta_3](w)$, return to Step 1.
   (This (unlikely) case corresponds to $\overline{\mathbb{F}}_p H/\overline{\mathbb{F}}_p(w)$ being cyclic.)
6. *(Now C is $\mathbb{F}_p(w)[x,v]/(m_0, v^2 - \Delta)$.)*
   Let $b \leftarrow vx \in C = \mathbb{F}_p(w)[x,v]/(m_0, v^2 - \Delta)$.
   (Then b is a primitive element of $C/\mathbb{F}_p(w)$.
7. Calculate how the automorphism τ operates on C.
8. Choose some element $\zeta \in \mathbb{F}_{p^3} \setminus \mathbb{F}_p$, and let $c \leftarrow \zeta b + \sigma\tau(\zeta b) + (\sigma\tau)^2(\zeta b) \in C$.
   (Then we have $\mathbb{F}_{p^3}(\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle} = \mathbb{F}_p(w)[c]$.)
   Calculate the minimal polynomial m_1 of c over $\mathbb{F}_p(w)$.
9. Determine how to express the coordinate functions x and $y \in H$ as elements of $\tilde{x}, \tilde{y} \in \mathbb{F}_{p^3}(w)[c]$, i.e. as $\mathbb{F}_{p^3}(w)$-linear combinations of $1, c, c^2, c^3, c^4, c^5$.
10. (Output) The minimal polynomial m_1 together with the elements $\tilde{x}$ and $\tilde{y}$.

In Step 2, one needs an algorithm to calculate Riemann-Roch spaces. Such an algorithm is given in [10]. As this algorithm is also crucial for the later index calculus algorithm in the resulting class group $\mathrm{Cl}^0((\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle})$, in Appendix C, we give some background information on this algorithm.

We note that in Steps 5 and 6, we use the classical theory of cubic equations.

To perform Step 7, one can proceed as follows. The polynomial m_0 splits completely over C. One root is x, and for the other two roots, explicit expressions in x and v can be calculated. Suppose these roots are x_1 and x_2. The automorphism τ maps x to one of the x_i, say $\tau(x) = x_1$. Then $\tau(x_1) = x_2$, $\tau(x_2) = x$, $\tau(vx) = vx_1$, $\tau(vx_1) = vx_2$ and $\tau(vx_2) = vx$, and these 6 elements form a basis of the vector space C over $\mathbb{F}_p(w)$. This enables one to compute a matrix that describes τ with resect to this basis.

It can be shown that all the above steps can be performed in randomized polynomial time in $\log(p)$. Moreover, the outlined algorithm can be specified in such a way that the total degree of the resulting polynomial m_1 is a polynomial over $\mathbb{F}_p[w]$ and has a degree which is bounded by an absolute constant. This is an important remark for a theoretical analysis of the following index calculus step.

The arguments for a theoretical analysis of the algorithm are however quite lengthy, and we omit them. From a practical point of view, the above calculations are very fast. An implementation in the computer algebra system Magma does all these calculations in some seconds on a Personal Computer.

The output of the algorithm allows one to efficiently compute the transfer homomorphism (6). The following approach is particularly efficient from a practical point of view:

Let $\mathcal{O}^\infty := \mathbb{F}_p[x]$, and let $\mathcal{O}^\infty(\mathbb{F}_{p^3}H) \subset \mathbb{F}_{p^3}H$, $\mathcal{O}^\infty(\mathbb{F}_{p^3}C) \subset \mathbb{F}_{p^3}(C)$, $\mathcal{O}^\infty((\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}) = \mathcal{O}^\infty(\mathbb{F}_{p^3}C) \cap (\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle} \subset (\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}$ be its integral closures.

Almost every element $a \in \mathcal{T}$ is determined by an ideal $(x^2 + \alpha_1 x + \alpha_0, y - \beta_1 x - \beta_0)$ of $\mathcal{O}^\infty(\mathbb{F}_{p^3}H)$. The conorm is the $\mathcal{O}^\infty(\mathbb{F}_{p^3}C)$-ideal $I := (\tilde{x}^2 + \alpha_1\tilde{x} + \alpha_0, \tilde{y} - \beta_1\tilde{x} - \beta_0)$. The norm of this ideal to $\mathcal{O}^\infty((\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle})$ is $I \cdot (\sigma\tau)(I) \cdot (\sigma\tau)^2(I) \cap (\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}$. Generators can be calculated efficiently.

We are thus left with the task to solve the resulting DLP in $\mathrm{Cl}^0((\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle})$. Using Proposition 2 in Appendix C, we obtain the theoretical result stated in the introduction.

6 Practical aspects of index calculus in the resulting function fields

In this section, we are concerned with practical aspects of our attack. As stated above, from a practical point of view, calculating w, the necessary field equations and transferring the DLP in $\mathrm{Cl}^0(H)$ a DLP in $\mathrm{Cl}^0((\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle})$ does not constitute a problem in terms of the running time. We now consider the problem of calculating the resulting DLP with a generalization of the reduced factor base index calculus algorithm by Gaudry-Harley-Thériault ([22]) from hyperelliptic to general function fields / curves.

In Appendix C, we have compiled some background information on the generalization of this algorithm to general function fields / curves, and in Appendix D we analyze the algorithm from a practical point of view.

In order to apply this analysis to our case, we first remark that the automorphism τ of C induces an automorphism of order 3 on $(\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}$. (The reason is that τ commutes with $\sigma\tau$.) Using Remark 4, we apply the results in the appendix with $q = \frac{p}{3}$. We have to estimate the constants k_{add} and k_{fac} (see Appendix D for definitions). To do so, we implemented the resulting function field $(\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}$ in Magma and did computations using the divisor arithmetic. This arithmetic was mostly implemented by Hess and follows the description in [10].

As described in Appendix D, we give all timings relative to one multiplication in $\mathbb{Z}/\ell\mathbb{Z}$, where $\ell := \#\mathcal{T} \approx p^4$ is the size of the subgroup of $\mathrm{Cl}^0((\mathbb{F}_{p^3}C)^{\sigma\tau})$ in which we want to calculate the DLP. Using several off-the-shelf Personal Computers with 32 bit processors, we have determined the following approximate values for for reduction of an effective degree $7(= g(\mathbb{F}_{p^3}C)^{\sigma\tau}) + 1)$ divisor along a place of degree 1:

p	32 bit	48 bit
	$1.9 \cdot 10^5$	$2.2 \cdot 10^5$

(7)

To determine whether an effective divisor of degree $6(= g((\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}))$ splits can be done in negligible amount of time: As implemented in Magma, the $\mathcal{O}^\infty((\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle})$-ideal of a divisor in ideal representation is given by a $\mathbb{F}_p[w]$-basis which in particular contains a univariate polynomial in $\mathbb{F}_p[w]$. The roots of this polynomial gives the w-coordinates of the places in the divisor. If the polynomial P splits completely, so does the divisor (the converse also holds in practice). By testing whether P splits completely, one can determine just as fast as for hyperelliptic curves whether a divisor splits completely. This means that

the values in the above table are the values of k_{add}. (This also has been varified experimentally.)

As to k_{fac}, using the Magma function Support, one obtains a running time which is about 3 times larger than k_{add}. As k_{add} has to be multiplied with $6! = 720$, this is also negligible.

As in [22] and Appendix D, we denote the number of elements in the factor base by p^r ($r < 1$). In the next table we compiled the optimal value of r for p a 32-bit and 48-bit prime based on our estimates and (22).

p	32 bit	48 bit
r	$1 - 1/7 \cdot (1 - 0.752) \approx 1 - 0.035$	$1 - 1/7 \cdot (1 - 0.497) \approx 1 - 0.072$

(8)

Following the analyis in Appendix D, the final running time is equivalent to

$$36 \cdot \left(\frac{p}{3}\right)^{2r} \approx 4 \cdot p^{2r} \tag{9}$$

multiplications in $\mathbb{Z}/\ell\mathbb{Z}$ (see (23)).

For comparison with the running time obtained by generic attacks, let us assume that $\#\mathcal{T}$ is prime. Then all generic attacks have a running time of $\Theta(\sqrt{\ell})$. We take the ρ-method for comparison. Its expected running time is

$$\sqrt{\frac{\pi}{2}} \cdot \sqrt{\frac{1}{6}} \cdot p^2 \approx 0.5 \cdot p^2 \tag{10}$$

group operations in $\mathcal{T}$. Here, the factor $\sqrt{\frac{1}{6}}$ comes from the fact that we take advantage of the hyperelliptic involution and the Frobenius operation.

We want to express the constant of the ρ-method in terms of multiplications in $\mathbb{Z}/\ell\mathbb{Z}$. As we are interested in a lower bound on the running time of the ρ-method, we make the assumption that the running time for multiplication is quadratic in the bit length. If it is lower, the time for the ρ-method expressed in multiplications in $\mathbb{Z}/\ell\mathbb{Z}$ increases.

According to ([18, Table in Section 5]), one needs roughly 160 multiplications in $\mathbb{F}_p$ to add elements of $\mathcal{T}$. This corresponds to 10 multiplications in $\mathbb{Z}/\ell\mathbb{Z}$, so that the constant of the ρ-method is 5. (One can also use the usual addition in $\mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_{p^3})$, but this alternative seems to be slightly slower.)

The same holds if one compares the constant of our attack with the constant of an attack via the ρ-method on elliptic curves over prime fields of size ℓ. The best known methods to add and double points need a rough time equivalent of 9-10 multiplications (cf. [18, table in Section 5]). In this case, one can also conclude that the two constants are roughly equal.

We conclude:

Let $\mathcal{T}$ have prime group order. Then based on our estimates our attack leads in combination with the reduced factor based index calculus algorithm to a speed-up in the calculation of the DLP which for 128 bit (resp. 192 bit) group size corresponds to a reduction of the bit length of at least 3% (resp. 7%).

For growing group size, this reduction becomes larger and converges against a theoretical limit of $1/7 \approx 14\%$. This result holds if one compares our attack with a generic attack on the DLP in $\mathcal{T}$ itself as well as if one compares our attack with an attack on the DLP in an elliptic curve over a prime field (with prime group order) of a size which is comparable to the group order of $\mathcal{T}$.

Discussion on our estimates

The above discussion relies heavily on the estimate of k_{add}. An important question is now how k_{add} would change if one did more thorough experiments with the resulting function fields, using a specific implementation in C (and comparing the reduction times to multiplication times in C). Given that the implementation in Magma is a general purpose implementation, it is very reasonable to assume that the value for k_{add} is an *upper bound* for the value which can be obtained with a specific implementation.

Additionally, one can use a large prime variation and a double large prime variation which lead to a further decrease in the running time, albeit an increase in the storage requirements.

7 Conclusion

We have shown that the DLP in trace-zero groups of genus 2 curves over finite fields of characteristic $\neq 2, 3$ with respect to field extensions of degree 3 can always be transferred into the DLP in a degree 0 class group of a curve / function field of genus at most 6 over the base field. The DLP in the resulting degree 0 class group can then be attacked with index calculus methods. Asymptotically this leads to a speed-up in the calculation of the DLP which corresponds to a reduction of the bit length by $1/6^{\text{th}}$.

A practical study has provided strong evidence that for groups of prime order and a size of at least 128 bit, our attack leads to a speed-up in the calculation of the DLP which for trace-zero groups with prime order corresponds to *at least* 3% reduction of the bit length in comparison to the ρ-method. It is however important to remark that as usual for index calculus algorithms, in contrast to the ρ-method, storage requirements are huge (e.g. $\kappa \cdot 2^{31}$ elements of size 32 bits for 128 bit group size for some small constant κ), and it is difficult (but not completely impossible) to parallelize the second (linear algebra) part of the index calculus algorithm.

Acknowledgment

We thank G. Frey, F. Hess and P. Gaudry for discussions.
Support by the IST Programme "Ecrypt" of the European Union is gratefully acknowledged.

References

[1] L. Adelman, J. DeMarrais, and M.-D. Huang. A Subexponential Algorithm for Discrete Logarithms over the Rational Subgroup of the Jacobian of Large Genus Hyperelliptic Curves over Finite Fields. In *Proceedings of the First International Symposium on Algorithmic Number Theory*, pages 28–40, 1984.

[2] D. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, 177(95-101), 1987.

[3] A. Chistov. The complexity of constructing the ring of integers of a global field. *Soviet Math. Docl.*, 39:597–600, 1989.

[4] C. Diem. The GHS Attack in odd Characteristic. *J. Ramanujan Math. Soc.*, 18:1–32, 2003.

[5] W. Eberly and E. Kaltofen. On randomized Lanczos algorithms. In W. Küchlin, editor, *Proceedings ISSAC 1997*, pages 176–183. ACM Press, 1997.

[6] A. Enge and P. Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta. Arith.*, 102:83–103, 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] P. Gaudry, N. Thériault, and E. Thomé. A double large prime variation for small genus hyperelliptic index calculus. forthcomming, a primininary version is available under http://eprint.iacr.org/2004/153.

[10] F. Heß. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Computation*, 11, 2001.

[11] F. Heß. The GHS Attack Revisited. In E. Biham, editor, *Advances in Cryptology — EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 374–387. Springer-Verlag, 2003.

[12] F. Heß. Generalising the GHS Attack on the Elliptic Curve Discrete Logarithm. *LMS J. Comput. Math.*, 7:167–192, 2004.

[13] F. Heß. Weil descent attacks. In G. Seroussi I. Blake and N. Smart, editors, *Advances in Elliptic Curve Cryptography*. Cambridge University Press, 2004.

[14] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1:130–150, 1989.

[15] N. Koblitz. A family of Jacobians suitable for discrete log cryptosystems. In *Advances in Cryptlogy — CRYPTO 1988*, LNCS, pages 94–99. Springer-Verlag, 1990.

[16] B. LaMacchia and A. Odlyzko. Solving large sparse linear systems over finite fields. In A. Menezes and S. Vanstone, editors, *Advances in Cryptology — Crypto 1990*, volume 537 of *LNCS*, pages 109–133, Berlin, 1990. Springer-Verlag.

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

[18] T. Lange. Trace-Zero Subvariety for Cryptosystems. *J. Ramanujan Math. Society*, 2004.

[19] K. Nagao. Improvement of Thériault Algorithm of Index Calculus of Jacobian of Hyperelliptic Curves of Small Genus. available under http://eprint.iacr.org/2004/161/.

[20] J. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.

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

[22] N. Thériault. Index calculus attack for hyperelliptic curves of small genus. In *Advances in Cryptology — ASIACRYPT 2003*, volume 2894 of *LNCS*, pages 75–92, Berlin, 2003. Springer-Verlag.

A On the kernel of the transfer homomorphism

The goal of this section is to prove a slightly weaker result than item a) of Proposition 1: We will show that the kernel is annihilated by 12 (see however Remark 3 below).

Let the notations be as in Proposition 1. We want to prove that the kernel of the homomorphism

$$\begin{gathered}\mathcal{T} \hookrightarrow \mathrm{Cl}^0(\mathbb{F}_{p^3}H) \xrightarrow{\mathrm{Con}} \mathrm{Cl}^0(\mathbb{F}_{p^3}C) \xrightarrow{\mathrm{N}} \mathrm{Cl}^0((\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}) \hookrightarrow \\ \mathrm{Cl}^0(\mathbb{F}_{p^3}C) \xrightarrow{\mathrm{N}} \mathrm{Cl}^0(\mathbb{F}_{p^3}H) \xrightarrow{\mathrm{Con}} \mathrm{Cl}^0(\mathbb{F}_{p^3}C) \xrightarrow{\mathrm{N}} \mathrm{Cl}^0(\mathbb{F}_{p^3}H) \xrightarrow{[2]} \mathrm{Cl}^0(\mathbb{F}_{p^3}H)\end{gathered} \tag{11}$$

is annihilated by 12. (Here and in the following, for some integer z, $[z]$ denotes multiplication by z.) Clearly, this implies the claim.

Let $\iota_{\mathcal{T}} : \mathcal{T} \hookrightarrow \mathrm{Cl}^0(\mathbb{F}_{p^3}H)$ be the inclusion, and let us abbreviate $\mathrm{Con}_{\mathbb{F}_{p^3}C/\mathbb{F}_{p^3}H}$ by Con and $\mathrm{N}_{\mathbb{F}_{p^3}C/\mathbb{F}_{p^3}H}$ by N.

As C/H is a field extension of degree 2, there exists an automorphism α of C of order 2 such that $C^{\langle\alpha\rangle} = H$. Note that

$$\mathrm{N} \circ \mathrm{Con} = [2] \quad \text{and} \quad \mathrm{Con} \circ \mathrm{N} = \mathrm{id} + \alpha^*.$$

Because of these identities, the homomorphism in (11) can be rewritten as

$$[2] \circ \mathrm{N} \circ (\mathrm{id} + \alpha^*) \circ (\textstyle\sum_{i=0}^{2}((\sigma\tau)^i)^*) \circ \mathrm{Con} \circ \iota_T. \tag{12}$$

As σ^* commutes with α^* and τ^*, (12) is equal to

$$\begin{gathered}\textstyle\sum_{i=0}^{2} \left(\mathrm{N} \circ (\mathrm{id} + \alpha^*) \circ (\tau^i)^* \circ \mathrm{Con} \circ [2] \circ \iota_{\mathcal{T}} \circ (\sigma^i)^* \right) = \\ \textstyle\sum_{i=0}^{2} \left(\mathrm{N} \circ (\mathrm{id} + \alpha^*) \circ (\tau^i)^* \circ \mathrm{Con} \circ \mathrm{N} \circ \mathrm{Con} \circ \iota_{\mathcal{T}} \circ (\sigma^i)^* \right) = \\ \textstyle\sum_{i=0}^{2} \left(\mathrm{N} \circ (\mathrm{id} + \alpha^*) \circ (\tau^i)^* \circ (\mathrm{id} + \alpha^*) \circ \mathrm{Con} \circ \iota_{\mathcal{T}} \circ (\sigma^i)^* \right).\end{gathered} \tag{13}$$

As $\mathrm{Gal}(C/\mathbb{F}_p(w))$ is isomorphic to S_3, we have the relation $\alpha\tau\alpha = \tau^2$. This implies

$$(\mathrm{id} + \alpha^*) \circ (\tau^i)^* \circ (\mathrm{id} + \alpha^*) = (\tau^* + (\tau^2)^*) \circ (\mathrm{id} + \alpha^*). \tag{14}$$

for $i = 1, 2$. As $\mathrm{Cl}^0(\mathbb{F}_{p^3}(w)) = 0$, we have

$$\begin{gathered}(\mathrm{id} + \tau^* + (\tau^2)^*) \circ (\mathrm{id} + \alpha^*) = \textstyle\sum_{\beta \in \mathrm{Gal}(\mathbb{F}_{p^3}C/\mathbb{F}_{p^3}(w))} \beta^* = \\ \mathrm{Con}_{\mathbb{F}_{p^3}C/\mathbb{F}_{p^3}(w)} \circ \mathrm{N}_{\mathbb{F}_{p^3}C/\mathbb{F}_{p^3}(w)} = 0.\end{gathered}.$$

This implies

$$(\mathrm{id} + \alpha^*) \circ (\tau^i)^* \circ (\mathrm{id} + \alpha^*) = (\tau^* + (\tau^2)^*) \circ (\mathrm{id} + \alpha^*) = -\mathrm{id} - \alpha^* \tag{15}$$

Furthermore, we have

$$(\mathrm{id} + \alpha^*) \circ (\mathrm{id} + \alpha^*) = [2] \circ (\mathrm{id} + \alpha^*) \tag{16}$$

Inserting (15) and (16) into (13), we obtain

$$\mathrm{N} \circ (\mathrm{id} + \alpha^*) \circ \mathrm{Con} \circ \iota_{\mathcal{T}} \circ ([2] - \sigma - \sigma^2). \tag{17}$$

As by definition of $\mathcal{T}$ we have $(\mathrm{id} + \sigma + \sigma^2)|_{\mathcal{T}} = 0$, this is equal to

$$\begin{gathered} \mathrm{N} \circ (\mathrm{id} + \alpha^*) \circ \mathrm{Con} \circ \iota_{\mathcal{T}} \circ [3] = \\ \mathrm{N} \circ \mathrm{Con} \circ \mathrm{N} \circ \mathrm{Con} \circ \iota_{\mathcal{T}} \circ [3] = \\ [12] \circ \iota_{\mathcal{T}}. \end{gathered}$$

□

Remark 3. By using the theory of Jacobian varieties, one can show that

$$\mathrm{N} \circ \tau^i \circ \mathrm{Con} = [-1]$$

for $i = 1, 2$, and with this identity one can prove that the kernel of the transfer homomorphism (6) is annihilated by 3.

B Genus calculations

This section serves three purposes: First, we want to sketch a proof of item b) of Proposition 1. Second, we want to give some more background on our Galois theoretic construction. Third, we want to indicate that with a modification of our construction, one can under certain conditions achieve that the resulting function field has genus ≤ 5.

As in the previous sections, let $p \neq 2, 3$ be a prime number. As we are mostly interested in genus calculations and the genera of curves / function fields do not change if one extends the base field, we start off with any hyperelliptic curve $\mathcal{H}/\overline{\mathbb{F}}_p$. Let $\overline{H} := \overline{\mathbb{F}}_p(\mathcal{H})$ be the function field of $\mathcal{H}$. More generally than in the main body of the work we fix any function $w \in \overline{H}$ of degree 3 (i.e. such that $[\overline{H} : \overline{\mathbb{F}}_p(w)] = 3$) satisfying the only condition is that $\overline{H}/\overline{\mathbb{F}}_p(w)$ is not Galois (i.e. not cyclic).

Let $\overline{C}$ be the Galois closure of $\overline{H}/\overline{\mathbb{F}}_p(w)$. Then $\mathrm{Gal}(\overline{C}/\overline{\mathbb{F}}_p(w)) \approx S_3$, and we have a non-trivial automorphism τ on $\overline{C}$ of order 3. Let $\overline{D} := \overline{C}^{\langle \tau \rangle}$ (such that $[\overline{D} : \overline{\mathbb{F}}_p(w)] = 2$). Note that is the context of the main body of the work, we have $\overline{C} = \overline{\mathbb{F}}_p C$.

By the Hurwitz genus formula ([21, Theorem III.4.12]), there is a strong relationship between the *ramification pattern* of $\overline{H}/\overline{\mathbb{F}}_p(w)$ and the genera of the function fields $\overline{C}$ and $\overline{D}$.

Let P be a place of $\overline{\mathbb{F}}_p(w)/\overline{\mathbb{F}}_p$. As $[\overline{H} : \overline{\mathbb{F}}_p(w)] = 3$, there are the following three possibilities for the splitting behavior of P in $\overline{H}$.

1. $P = Q_1 + Q_3 + Q_3$ for three different places Q_i of $\overline{H}/\overline{\mathbb{F}}_p$. (In this case, P is called *unramified* in the extension $\overline{H}/\overline{\mathbb{F}}_p(w)$.)

2. $P = 2Q_1 + Q_2$ for two different places Q_i of $\overline{H}/\overline{\mathbb{F}}_p$.

3. $P = 3Q$ for one place Q of $\overline{H}/\overline{\mathbb{F}}_p$. (In this case, P is called *completely ramified* in the extension $\overline{H}/\overline{\mathbb{F}}_p(w)$.)

Let r_2 be the number of places of $\overline{\mathbb{F}}_p(w)$ of the 2^{nd} form, and let r_3 be the number of places of $\overline{\mathbb{F}}_p(w)$ which are completely ramified in $\overline{H}$. Then by the Hurwitz genus formula and the fact that $g(\overline{H}) = 2$, we have

$$r_2 + 2r_3 = 8. \tag{18}$$

(We remark that we assumed that $p \neq 2, 3$ such that all ramification is tame.)

We can conclude that (r_1, r_2) has to be $(8, 0), (6, 1), (4, 2), (2, 3), (0, 4)$. We will see below that the case $(0, 4)$ is not possible.

One can now use the ramification theory for Galois extensions of function fields as presented in [21, Theorem III.8.2] to study the ramification behavior of P in $\overline{C}/\overline{\mathbb{F}}_p(w)$ and in $\overline{D}/\overline{\mathbb{F}}_p(w)$. From the information one obtains in this way, one can then again with the Hurwitz genus formula calculate the genera of $\overline{D}$ and $\overline{D}$.

We omit the details of the arguments and just state that one can obtain the following formulae.

$$g(\overline{C}) = 3 + \frac{r_2}{2} = 7 - r_3 \tag{19}$$

and

$$g(\overline{D}) = -1 + \frac{r_2}{2} = 3 - r_3. \tag{20}$$

As remarked above, we can rule out that $r_2 = 0$. Indeed, this would be equivalent to $g(\overline{D}) = -1$. (In fact, if one starts with an arbitrary function $w \in \overline{H}$ such that $[\overline{H} : \overline{\mathbb{F}}_p(w)] = 3$, then the case $r_2 = 0, r_3 = 4$ can occur, and it corresponds exactly to the cyclic extensions $\overline{H}/\overline{\mathbb{F}}_p(w)$ which we have ruled out.)

After one has derived (19), a *proof of Proposition 1* is not difficult: At the beginning of Section 4, we have chosen w in such a way that $r_3 \geq 1$. By (19), it follows that $g((\mathbb{F}_{p^3}C)^{\langle\sigma\tau\rangle}) = g(\overline{C}) \leq 6$. □

We want to conclude with some additional remarks which we state without proof.

- If one chooses a polynomial $f \in \mathbb{F}_p[x]$ of degree 6 and a function $w \in H$ of degree 3 uniformly at random, the probability that $g(\mathcal{C} \leq 6$ is in $O(\frac{1}{p})$.
- There always exists a function $w \in \overline{H}$ with $r_3 \geq 2$, i.e. $g(\overline{C}) \leq 5$.
- Let $\mathcal{H}/\mathbb{F}_p$ be a hyperelliptic curve of genus 2 with function field H, and let $\mathcal{H}^\iota$ denote the quadratic twist of $\mathcal{H}/\mathbb{F}_p$ with respect to ι. Let us assume that $\mathcal{H}/\mathbb{F}_{p^3}$ does not have automorphisms of order 3, and that there is an element in $\mathrm{Cl}^0(\mathcal{H}/\mathbb{F}_3)$ of order 3 which is defined by a divisor of the form

$D - \infty_1 - \infty_2$, where D splits as $D = P_1 + P_2$ with $P_i \in \mathcal{H}(\mathbb{F}_p)$, or that there is an element in $\mathrm{Cl}^0(\mathcal{H}^\iota/\mathbb{F}_3)$ which is defined by a divisor of the form $D - \infty_1 - \infty_2$, where D is irreducible over $\mathbb{F}_p$. Then there exists a function $w \in H$ with $g(\overline{C}) \leq 5$. If the conditions are satisfied such a function can be found in randomized polynomial time in $\log(p)$, and one can mount a similar (but slightly more efficient) attack as the one presented in this work on the DLP in $\mathcal{T}$.

- The curves $\mathcal{H}/\overline{\mathbb{F}}_p$ for which there exists an $w \in \overline{\mathbb{F}}_p(\mathcal{H})$ with $r_3 = 3$ (i.e. $g(\overline{C}) = 4$) form a 2-dimensional algebraic family (inside the 3-dimensional algebraic family of all genus 2 curves).
- For growing p, the probability that a uniformly randomly chosen polynomial $f \in \mathbb{F}_p[x]$ of degree 6 defines a curve $\mathcal{H}/\mathbb{F}_p$ which has such a $w \in H$ with $g(\overline{C}) = 4$ is in $O(\frac{1}{p})$.

C On the arithmetic in class groups of general curves

The goal of the attack presented in this work is to solve the original DLP in $\mathcal{T}$ by transferring it into $\mathrm{Cl}^0(\mathcal{X}/\mathbb{F}_p)$, where $\mathcal{X}/\mathbb{F}_p$ is a curve of genus at most 6 and solving it there with index calculus methods. In order to apply an index calculus algorithm to the DLP in $\mathrm{Cl}^0(\mathcal{X}/\mathbb{F}_p)$, we need an efficient arithmetic in this group as well as a method to factorize elements over the factor base. In this section, recalling some results from [10], we comment on both of these problems from a general perspective. As in the rest of the paper, we work in the function field theoretic setting.

Let q be a prime power, and let F be a function field over the exact constant field $\mathbb{F}_q$. As in [10], we assume that F is given as an explicit separable extension $F/\mathbb{F}_q(x)[y]$ where y satisfies an equation of the form $f(x, y) = 0$ with $f(x, y) = y^n + a_1 y^{n-1} + \cdots + a_n \in \mathbb{F}_q[x, y]$. (Every function field (as always in one variable) over $\mathbb{F}_q$ can be given in this way ([21, III.9.2])). Let $f^h(x, y, z)$ be the homogenization of $f(x, y)$.

Let $\mathcal{O}_\infty$ be the local ring of the place "infinity" of $\mathbb{F}_q(x)$, and let $\mathcal{O}^\infty := \mathbb{F}_p[x]$. Let $\mathcal{O}_\infty(F) \subset F$ be the integral closure of $\mathcal{O}_\infty$ and $\mathcal{O}^\infty(F)$ the integral closure of $\mathbb{F}_q[x]$. We remark for later use that bases of $\mathcal{O}^\infty(F)$ over $\mathbb{F}_q[x]$ and of $\mathcal{O}_\infty(F)$ over $\mathcal{O}_\infty$ can be calculated in polynomial time in $\log(q)$ and the total degree of f ([3]).

For computational applications, we first of all need a representation of the places of F. They can for example be represented as points on the plane curve given by $f^h(x, y, z) = 0$ over extension fields of $\mathbb{F}_q$ plus some extra information in the case that the divisor involves singular points. By the very definition of $\mathrm{Div}(F)$, every element of this group is a formal sum of places of F. If one stores an element of F as such a formal sum, one speaks of a *free representation*. (When storing such a formal sum one should use a "sparse representation" which only involves the places which actually occur in the sum.) In the *ideal representation* of an element of $\mathrm{Div}(F)$ one first calculates bases of $\mathcal{O}^\infty(F)$ over $\mathbb{F}_q[x]$ and $\mathcal{O}_\infty(F)$ over $\mathcal{O}_\infty$ respectively. Then one represents each element of $\mathrm{Div}(F)$ by a

pair of ideals (I, J), where I is an $\mathcal{O}_\infty$-ideal and J is an $\mathcal{O}^\infty$-ideal. These ideals I, J are represented as free $\mathcal{O}_\infty$ (resp. $\mathcal{O}^\infty$-modules) over $\mathcal{O}_\infty(F)$ (resp. $\mathcal{O}_\infty(F)$) (see [10] for details).

For the derivation of a suitable representing system of $\mathrm{Cl}(F)$ by elements of $\mathrm{Div}(F)$, the following lemma, which is implicitly used in [10, Proposition 8.2], is crucial.

Lemma 2. *Let $D, A \in \mathrm{Div}(F)$, where A has degree 1. Assume that $\mathcal{L}(D) \neq 0$ but $\mathcal{L}(D-A) = 0$. Then $\dim(\mathcal{L}(D)) = 1$. Furthermore, one has $\deg(D) \leq g(F)$.*

Proof. By the Riemann-Roch theorem and the assumption one has $\dim(\mathcal{L}(D)) - \dim(\mathcal{L}(K-D)) = \deg(D)+1-g(F)$ and $-\dim(\mathcal{L}(K-D+A)) = \deg(D)-g(F)$, where K is a canonical divisor. This implies that $\dim(\mathcal{L}(D)) = 1 + \dim(\mathcal{L}(K-D)) - \dim(\mathcal{L}(K-D+A)) \leq 1$. The last statement follows immediately from the Riemann-Roch theorem. □

Apart from the representation of the elements of $\mathrm{Div}(F)$ themselves, the representation of elements of $\mathrm{Cl}(F)$ is now identical in both cases: First, one fixes a divisor A of degree 1 on F (for example a place of degree 1). Then the elements of $\mathrm{Cl}(F)$ are uniquely represented as divisors of the form $D - rA$, where $\deg(D) = r$ and $\deg(D)$ is minimal under all divisors with this property. (Such a divisor D is called *maximally reduced divisors along A*.) We call such this representation of an element in $\mathrm{Cl}(F)$ a *reduced ideal / free representation* with respect to A.

In order to formulate addition-/doubling algorithms in $\mathrm{Cl}(F)$, one has to have a *divisor reduction algorithm* of elements of $\mathrm{Div}(F)$. That is, one has to have an algorithm which given an element $D_{\mathrm{in}} \in \mathrm{Div}(F)$ calculates a divisor D_{out} such that D_{in} is linearly equivalent to $D_{\mathrm{out}} - dA$, where $d = \deg(D_{\mathrm{out}})$, and D_{out} is maximally reduced along A.

One way to find such an algorithm is to find a general algorithm to calculate Riemann-Roch spaces. Using the ideal-theoretic representation, such an algorithm is [10, Algorithm 6.1].

Given D_{in} in ideal representation, one can now proceed as follows: One calculates bases of the spaces $\mathcal{L}(D_{\mathrm{in}} + dA)$ for $d = g(F), g(F_{\mathrm{in}}) - 1 \ldots$ until the space is 1-dimensional. If then $f \in \mathcal{L}(D_{\mathrm{in}} + dA)$, the divisor $D_{\mathrm{out}} = (f) + D_{\mathrm{in}} + dA$ is maximally reduced along A and $D_{\mathrm{out}} - dA$ is linearly equivalent to D_{in}. (We remark that the algorithm in [10, Section 8] which uses the free representation is not appropriate for our purposes.)

Index Calculus in general curves of fixed genus

The algorithms of [7], [22] and [9] in principle also apply to more general than hyperelliptic curves. Let us describe briefly how the fact that the curves are more general enters the algorithms.

First, as above one fixes a place A of degree 1 of F. This place substitutes the place ∞ of the algorithm for hyperelliptic curves / function fields.

Let us assume that we want to calculate the discrete logarithm of $b \in \mathrm{Cl}^0(F)$ with respect to base $a \in \mathrm{Cl}^0(F)$. To find relations, as in the hyperelliptic case, one

chooses numbers $\alpha, \beta \in [1, \ldots, \#\,\mathrm{Cl}^0(F) - 1]$ uniformly at random and calculates the unique reduced representation $D - d \cdot A$ (with $d = \deg(D)$) of $\alpha a + \beta b$. Then one tries to factor D over the factor base which is a subset of the set of all places of degree 1 of F.

In order to perform these calculations, one can for example use the ideal arithmetic described above: One first calculates the divisor D in ideal representation, then one checks whether it splits completely, and if this is the case, one calculates a free representation.

Using the results of [10] one can show that for bounded total degree of f, all calculations necessary for index calculus as formulated in [7], [22] and [9] can be performed in polynomial time in $\log(q)$. With the above notations one obtains:[3]

Proposition 2. *Let g and δ be two natural numbers. Then there exists a randomized algorithm with the following input, output and running time.*

The input consists of a polynomial $f \in \mathbb{F}_q[x, y]$ of total degree $\leq \delta$ defining a function field F with the exact constant field $\mathbb{F}_q$ and two elements $a, b \in \mathrm{Cl}^0(F)$ given in free or ideal representation such that $a \in \langle b \rangle$. The output is an an $x \in \mathbb{N}$ with $x \cdot a = b$, and the running time is $\tilde{O}(q^{2-\frac{2}{g}})$.

D Practical aspects of the reduced factor base index calculus algorithm

In this section, we are interested in practical aspects of solving DLPs in $\mathrm{Cl}^0(F)$, where F is a general function field of (small) genus g with exact constant field $\mathbb{F}_q$, by means of the reduced factor base index calculus algorithm as in Section 3 of [22]. Our goal is to determine the optimal size of the factor base under realistic conditions.

We assume that the linear algebra part is done with Lanczos' algorithm as described in [5]. We thereby ignore the time needed to access the memory. This means essentially that a prerequisite for our analysis is that the matrix is stored in the RAM on an equally fast accessible device. Let ℓ be the order of the subgroup of $\mathrm{Cl}^0(F)$ in which we want to calculate the DLP.

A practical improvement

Before we go on, we describe a *practical* improvement of the index calculus algorithm which applies to all groups and is well-known to implementers of these algorithms: As stated above, in theoretical descriptions on index calculus algorithms, it is stated that one should try to factor $\alpha a + \beta b$ over the factor base. If α, β are random elements of $\mathbb{Z}/\ell\mathbb{Z}$, one needs roughly $\log_2(\ell)$ group operations for this. However, from a practical point of view, one can just always add a or b

[3] The arguments in [9] are sometimes not absolutely rigorous, and it seems that one should employ certain techniques from [6] in order to obtain a rigorous result. We would however like to stress that our generalization from hyperelliptic curves to more general curves does not cause any additional difficulties in the proof.

to a previous calculation and try to factor the resulting element over the factor base. Like this, one just needs one group operation in each iteration.

In fact, one can even do better: Assume one has found a relation of the form $\alpha a + \beta b = \sum_{i=1}^{g} p_i$, where the p_i are elements of the factor base (regarded as elements in $\mathrm{Cl}^0(F)$. If now p is any element of the factor base, one can try to factor $\sum_{i=1}^{g} p_i + p$ over the factor base. Assume one has found a relation $\sum_{i=1}^{g} p_i + p = \sum_{i=1}^{g} \tilde{p}_i$. Then one has the relation $\alpha a + \beta b = \sum_{i=1}^{g} \tilde{p}_i - p$.

If one proceeds like this, most of the time, one only has to reduce a degree $g+1$ divisor and not a degree $2g$ divisor which makes the calculations slightly faster. On the other hand, most rows of the matrix have $g+1$ instead of g entries which makes the linear algebra part slightly slower. In the analysis below, we assume that this approach is taken.

The unit of measurement

Let us fix a *unit of measurement*: The multiplication of two elements in the residue class ring $\mathbb{Z}/\ell\mathbb{Z}$ is said to have *time 1.* All other times will be given with respect to this one.

Let us assume that the arithmetic in $\mathrm{Cl}^0(F)$ is done with the ideal representation as in [10]. Let k_{add} be the time needed for the reduction of a divisor in ideal representation of degree $g+1$ along a degree one divisor A (i.e. the time for addition of two elements in $\mathrm{Cl}^0(F)$ given in "reduced ideal representation") plus the time needed to test whether a degree g divisor in ideal representation splits into a sum of places of degree 1. Let k_{fac} be the time to compute the free representation of totally split divisor of degree g in ideal representation. (These constants can be defined in analogous way if the arithmetic is done in another form of representation.)

The optimal size of the factor base

Just as in [22], let us denote the number of elements in the factor base by p^r ($r < 1$). Then the probability that a reduced divisor splits over the factor base is roughly

$$\frac{1}{g!}\left(\frac{q^r}{q}\right)^g.$$

The time to collect the relations is roughly

$$(k_{\mathrm{add}} g! + k_{\mathrm{fac}}) \cdot q^{g-(g-1)r}.$$

As stated above, we assume that the linear algebra is done with Lanczos' algorithm ([5]). According to the fact that the matrix will have about $g+1$ non-trivial entries in each row and the description in [5], one can expect a time of roughly

$$(2(g+1)+4)q^{2r} = (2g+6)q^{2r}$$

for this part of the algorithm (see also [16, (3.13)]). This leads to a total running time of

$$(g!k_{\text{add}} + k_{\text{fac}}) \cdot q^{g-(g-1)r} + (2g+6)q^{2r}. \tag{21}$$

(We remark that sometimes one also has to perform reductions of a degree $2g$ divisor instead of a $g+1$ divisor, but the number of these operations is negligible, and the times of these two different reductions are usually quite close.) As usual, to determine the optimal value of r, we determine the value of r such that both sides are equal. This amounts to

$$\frac{k_{\text{add}}g! + k_{\text{fac}}}{2g+6} = q^{(g+1)r-g}$$

or

$$r = 1 - \frac{1}{g+1}\left(1 - \frac{\log\left(\frac{k_{\text{add}}g!+k_{\text{fac}}}{2g+6}\right)}{\log(q)}\right). \tag{22}$$

The total running time is then

$$(4g+12) \cdot q^{2r}. \tag{23}$$

We have written the equation for r as a sum in the above form for the reason that this way one can easily see the different contributions: Without the reduction of the factor base, one would have $r = 1$ and a running time of roughly q^2, with the reduction one has asymptotically a decrease of $1/(g+1)$, but that reduction is lowered if $g!$, k_{add} or k_{fac} is large.

Remark 4. If F has an automorphism of order n, one can – as described in [7, Section 4.2] – decrease the factor base by a factor of n. In this case, just the same formulae as above hold if one substitutes $\frac{q}{n}$ for q.

The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT.
The information in this document reflects only the authors' views, is provided as is, and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.