Correspondences on Hyperelliptic Curves and Applications to the Discrete Logarithm

Gerhard Frey[1] and Ernst Kani[**][2]

[1] Institute for Experimental Mathematics, University of Duisburg-Essen, 45219
Essen, Germany,
frey@iem.uni-due.de,
WWW home page: http:www.esaga.uni-due.de/gerhard.frey
[2] Department of Mathematics and Statistics, Queen's University
Kingston, Ontario, K7L 3N6, Canada
Kani@mast.queensu.ca,
WWW home page: http:www.mast.queensu.ca/ kani/

Abstract. The discrete logarithm is an important crypto primitive for public key cryptography. The main source for suitable groups are divisor class groups of carefully chosen curves over finite fields. Because of index-calculus algorithms one has to avoid curves of genus ≥ 4 and non-hyperelliptic curves of genus 3. An important observation of Smith [S] is that for "many" hyperelliptic curves of genus 3 there is an explicit isogeny of their Jacobian variety to the Jacobian of a non-hyperelliptic curve. Hence divisor class groups of these hyperelliptic curves are mapped in polynomial time to divisor class groups of non-hyperelliptic curves. Behind his construction are results of Donagi, Recillas and Livné using classical algebraic geometry. In this paper we only use the theory of curves to study Hurwitz spaces with monodromy group S_4 and to get correspondences for hyperelliptic curves. For hyperelliptic curves of genus 3 we find Smith's results now valid for ground fields with odd characteristic, and for fields with characteristic 2 one can apply the methods of this paper to get analogous results at least for curves with ordinary Jacobian.

Keywords: hyperelliptic curves, discrete logarithms, curves of genus 3.

1 Introduction

One fundamental need for many applications of public key cryptography is the construction of groups with hard discrete logarithm. Nowadays, the main source for such groups comes from arithmetic geometry and consists of divisor class groups of curves over finite fields $\mathbb{F}_q$ with q elements.

This development was a great stimulus for computational arithmetic geometry. A bit disappointing is that the same methods used for construction of candidates

[**] supported by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada (NSERC)

for cryptographically strong curves can be used for attacks (see Section 2). The outcome is that curves of genus larger than 3 do not provide strong groups. Even more surprising is Diem's result [D] that for genus 3 there is an index-calculus algorithm which makes the divisor class groups of generic curves weak but does not affect the (more special) hyperelliptic curves.

Assume now that the characteristic of the ground field from 2. It was Smith [S] who first realized that explicit isogenies for hyperelliptic curves of genus 3 can be used to transfer divisor classes of $\mathcal{O}(q^5)$ hyperelliptic curves to those of non-hyperelliptic curves of genus 3 and so make the discrete logarithm insecure again. In his work he used results from "classical" algebraic geometry due to Recillas, Donagi and Livné [DL].

The purpose of this paper is to give an elementary approach to Smith's results which uses only the theory of curves and elementary algebra and is otherwise self-contained. This is based on the observation that the so-called "trigonal construction" of Recillas, Donagi and Smith is a consequence of the study of certain curve covers of $\mathbb{P}^1$ whose monodromy (or Galois) group is the symmetric group S_4. As a result, we find for every g a Hurwitz space (cf. Section 4) which parameterizes a subspace of those hyperelliptic curves C of genus g which admit a non-trivial correspondence to a curve D of genus g that can be expected to be non-hyperelliptic.

Moreover, if the ground field is $\mathbb{F}_q$, then this correspondence is computable in polynomial time in $\log(q)$.

For $g = 3$ we find the results of Smith again (and are able to extend them to the case of characteristic 3 which he excludes.) To be more precise: By our methods we find a rapidly computable isogeny from the Jacobian variety J_C of C to the Jacobian variety J_D of D of small degree. A more detailed study of the correspondence shows that this isogeny has as kernel an isotropic subspace of the points of order 2 of J_C and is indeed the isogeny studied by Smith. (Details will be given in a forthcoming paper of the second author [Ka].) But we emphasize that for application to cryptography the results given in this paper are sufficient.

In addition we show that the space of hyperelliptic curves for which the correspondence exists is parameterized by the $(g+1)$-fold product of the generic elliptic curve with a point of order 3 which gives immediately and without any heuristic that $\mathcal{O}(q^{g+2})$ isomorphism classes of hyperelliptic curves over $\mathbb{F}_q$ are affected.

Another advantage of our approach is that it can be applied also in characteristic 2 (but at present only to curves with an ordinary Jacobian variety). In the last section we give a short sketch of this generalization; for details we again refer to [Ka].

1.1 Discrete Logarithms

Many protocols for public key crypto systems are based on discrete logarithms in groups G of prime order ℓ (see [F]).

Definition 1. The *computational Diffie-Hellman problem* (DHCP) for G is: For randomly given elements $a, b \in G$ compute $k \in \mathbb{Z}/(\mathrm{ord}(b))$ such that $b^k = a$. In this case we write: $k := \log_b(a)$.

There are families of algorithms using only the structure "group" (and called *generic*) that compute discrete logarithms (DL) with complexity $\mathcal{O}(\ell^{1/2})$, e.g. the baby-step-giant step algorithm of Shanks and Pollard's ρ-algorithm ([ACF]). By work of Maurer and Wolf [MW] we know that in *black box groups* we cannot do better. This motivates the search for families of "concrete" groups G for which DHCP cannot be solved with algorithms of complexity smaller than $\sim \sqrt{\ell}$, and we shall say that the discrete logarithm in G is "weak" if we find an algorithm that computes discrete logarithms faster, for instance with complexity $\mathcal{O}(\ell^d)$ with $d < 1/2$, or polynomial in $\log(\ell)$ or subexponential in $\log(\ell)$ ([ACF]).

1.2 Index-Calculus

All known algorithms that compute the DL in groups G' faster than the generic ones are built in the following way. One finds a transfer of the DL in G' to the DL in a group G that is computed in subexponential or even polynomial time and in G one can apply the pattern of index-calculus, which we want to describe now.

One destroys the "homogeneity" of groups and chooses a "factor base" consisting of relatively few elements. Then one computes G as $\mathbb{Z}$-module given by the free abelian group generated by the base elements modulo relations.

Next one has to prove that with high probability every element of G can be written (fast and explicitly) as a sum of elements in the factor base.

So one has to find a method to create sufficiently many relations in a short time. Usually this is done by a kind of "sieving". Crucial for the method is to balance the number of elements in the factor base to make the linear algebra over $\mathbb{Z}$ manageable and to guarantee "smoothness" of arbitrary elements with respect to this base.

The classical example for index-calculus is applied to the discrete logarithm in the multiplicative group of finite fields. The method was discovered by Kraitchik 1922 [Kr], re-invented several times and named as index-calculus by Odlyzko 1984 [O]. Theorems about the distribution of numbers with only small prime divisors and sieving (algebraic number field sieve and function field sieve) yield an algorithm of subexponential complexity with $\alpha = 1/3$.

1.3 Acknowledgment

The authors would like to thank very much the referee for encouragement, careful reading of the manuscript and for very helpful comments.

2 Discrete Logarithms in Divisor Class Groups

The success of the classical index-calculus method relies on the fact that points on the group scheme $\mathcal{G}_m$, the multiplicative group, can be easily lifted to points

defined over number fields. This picture changes radically if we replace the multiplicative group by abelian varieties of positive dimension, for instance by elliptic curves or more generally by Jacobian varieties of curves of genus ≥ 1 because of structural results like the Mordell-Weil theorem, which prevents the existence of "smooth" points over number fields.
To compute in J_C one presents its points by divisor classes of degree 0.

If not otherwise stated, a curve C defined over a perfect field K (i.e. all algebraic extensions of K are separable) is assumed to be projective, smooth and geometrically connected. Its genus is denoted by $g(C)$.
With K_s we denote the algebraic closure of K, and with C_s the curve obtained from C by constant field extension from K to K_s.
By G_K we denote the Galois group of K_s/K, i.e. the group of automorphisms of K_s that fix K elementwise.
A *divisor* on C_s is a formal sum $D = \sum_{P \in C(K_s)} z_P P$ with $z_P \in \mathbb{Z}$ and almost all $z_P = 0$. The degree of D is $\sum z_P$. Two divisors D_1, D_2 are equivalent iff there is a function f on C_s such that the divisor of zeros and poles of f is equal to $D_1 - D_2$. $\mathrm{Pic}^0(C_s)$ is the group of divisor classes of degree 0 of C_s. There is (after the choice of a "point at infinity" $P_\infty \in C(K_s)$) a canonical isomorphism between $J_C(K_s)$ and $\mathrm{Pic}^0(C_s)$.
We now assume that $P_\infty \in C(K)$. Since G_K acts on points, divisors, functions and hence on the divisor class group of C_s in a canonical way, we get that the divisor class group of degree 0 of C is $\mathrm{Pic}^0(C) = \mathrm{Pic}^0(C_s)^{G_K}$ and that this group is canonically isomorphic to $J_C(K)$.
The whole arithmetic in these divisor class groups is ruled by the theorem of Riemann-Roch. As one consequence we state that with fixed P_∞ we can represent (not necessarily uniquely) elements in $\mathrm{Pic}^0(C)$ by divisors $P_1 + \cdots + P_t - t \cdot P_\infty$ with $t \leq g(C)$ and $P_i \in C(K_s)$ such that the natural action of G_K leaves this sum invariant.
To use these groups for cryptographic purposes one chooses C over a finite field $\mathbb{F}_q$ and one has to solve deep problems in computational arithmetic geometry like point counting and addition formulas in divisor class groups. For the needs of cryptography, this has been solved at least partly in a satisfying way. We state in particular that the results of Heß [He] yield algorithms for group operations in divisor class groups that are of polynomial complexity both in $g(C)$ (with fixed q) and $\log(q)$ (with fixed $g(C)$).
As was said above, one of the main motivation for suggesting divisor class groups for DL-systems (by Miller [M] and Koblitz [Ko1],[Ko2] around 1985) was the difficulty to apply the "classical" index-calculus, and this is true till today. But there are various other ways to find "special" elements in $\mathrm{Pic}^0(C)$ if the genus of C is larger than 1: There are classes which are presented by less than $g(C)$ points, and it may happen that the points representing the given class are rational over K. Hence one can find factor bases, do index-calculus in a very refined way and gets the following result:

Theorem 1 (Diem, Gaudry, Thomé, Thériault[DGTT]). *There exists an algorithm which computes, up to* $\log(q)$*-factors, the DL in the divisor class group of curves of genus* $g(C)$ *in expected time of* $\mathcal{O}(q^{(2-2/g(C))})$.

As one consequence of the Hasse-Weil theorem (which is the analogue of the Riemann hypothesis for curves), we get that for $K = \mathbb{F}_q$ the order of $\mathrm{Pic}^0(C)$ is $\mathcal{O}(q^{g(C)})$. It follows that for genus $g(C) > 3$ the index-calculus algorithm is much faster than the generic algorithms, and hence these curves yield rather weak crypto systems and should be avoided.
But a closer look, done by Diem [D], shows that one can alter the factor base such that the *degree* of a plane model of C becomes the essential measure for the efficiency of the index-calculus algorithm.

Theorem 2 (Diem). *If* C *is given by a plane curve of degree* d *(singularities allowed) then the DL in the group of divisor classes of degree* 0 *is, up to* $\log(q)$*-factors, of complexity* $\mathcal{O}(q^{2-\frac{2}{d-2}})$.

One sees immediately that curves of genus 1 (elliptic curves) and of genus 2 are not affected by these results since for them the order of $\mathrm{Pic}^0(C)$ over $\mathbb{F}_q$ is $\mathcal{O}(q)$ respectively $\mathcal{O}(q^2)$.

3 Isogenies and Correspondences

Let C be a curve over K of genus $g(C) > 0$ with Jacobian variety J_C.
We exploit the fact that $\mathrm{Pic}^0(C)$ is canonically isomorphic to $J_C(K)$ and use the theory of abelian varieties.

Definition 2. Let A, A' be abelian varieties of dimension g over K and let $\eta : A \to A'$ be a K-rational homomorphism[3] whose kernel is a finite group scheme A_0. Then η is called an *isogeny* and A is *isogenous* to A'. The *degree* of η is the order of A_0. Moreover, an isogeny η is *separable* iff A_0 is an étale group scheme, and then the degree of η is $|A_0(K_s)|$.

Remark 1.

- The homomorphisms of abelian varieties are analogous to those of abelian groups. In particular, for any finite (K-) subgroup scheme A_0 of A there is a (K-rational) isogeny of A with $ker(\eta) = A_0$ and this isogeny is, up to isomorphisms, uniquely determined.
- On the other hand, abelian varieties are kind of rigid: If η is a morphism from A to A' mapping the neutral element 0_A of A to the neutral element $0_{A'}$ of A' then η is a homomorphism.
- As above, assume that A, A' are abelian varieties of the same dimension and that A or A' is simple, i.e. has no proper abelian variety as subvariety. Then a morphism $\eta : A \to A'$ mapping 0_A to $0_{A'}$ is an isogeny iff it is not constant.

[3] i.e. η is a morphism of varieties compatible with the addition morphisms on A and A'

Let $f : D \to C$ be a non-constant K-rational morphism from the curve D to the curve C. Then f induces an embedding f^* of the function field $F(C)$ of C into the function field $F(D)$ of D, and the degree $\deg(f) := [F(D) : f^*F(C)]$ of this field extension is called the *degree* of f.

As before, let C_s and D_s be the curves over K_s obtained by constant field extension from K to K_s. Then f induces a morphism $f_s : D_s \to C_s$ (which we usually denote by f again).

The morphism $f : D \to C$ induces two homomorphisms f^* and f_* on the associated divisor groups. To define the first, let $P \in C(K_s)$ be a point. Then $f^*(P)$ is by definition the divisor of D_s which is given by the formal sum of the points (with multiplicity in ramification points) lying in $f^{-1}(P)$. By linear extension f^* defines a homomorphism from the divisor group of C_s to the divisor group of D_s, called the *conorm map* (associated to f).

It is a basic fact of curve theory that divisors of degree n are mapped to divisors of degree $\deg(f) \cdot n$ and that principal divisors are mapped to principal divisors. We thus obtain an induced homomorphism from $\mathrm{Pic}^0(C_s)$ to $\mathrm{Pic}^0(D_s)$ which is again denoted by f^*. This map is Galois invariant, and so it maps $\mathrm{Pic}^0(C)$ to $\mathrm{Pic}^0(D)$.

The map f_* is by definition the linear extension of f to the group of divisors of D_s. Since f_* maps a principal divisor (t) to the principal divisor $(N(t))$ of its norm, we see that f_* induces a homomorphism, again denoted by f_*, from $\mathrm{Pic}^0(D_s)$ to $\mathrm{Pic}^0(C_s)$ that is Galois invariant. It is called the *norm map* (associated to f).

Using the functorial properties of Jacobians, one can show that f^* induces an (algebraic) homomorphism from J_C to J_D and that f_* induces an (algebraic) homomorphism from J_D to J_C.

Now assume that C_1, C_2, D are curves over K. Let $f_i : D \to C_i$ be non-constant K-rational morphisms. It follows that $T_{f_1,f_2} := (f_2)_* \circ f_1^*$ induces a homomorphism from J_{C_1} to J_{C_2} that we call *the correspondence attached to* (f_1, f_2).

We shall describe T_{f_1,f_2} explicitly in the special case that f_1 is fully ramified in a point $P_\infty \in C_1(K_s)$; i.e., that there is a unique point Q_∞ of D_s that is mapped to P_∞ by f_1.

We can represent a divisor class c of degree 0 of C_1 by $\sum_{i \leq g_1} P_i - g_1 P_\infty$, where $g_1 = g(C_1)$. Let $(Q_{i,j})_{1 \leq i \leq g_1, 1 \leq j \leq \deg(f_1)}$ be the set of points (listed with multiplicities) in $D(K_s)$ which are mapped to $P_1, \ldots, P_{g_1}$ by f_1. Then $T_{f_1,f_2}(c)$ is the divisor class of $\sum_{i,j} f_2(Q_{i,j}) - \deg(f_1) g_1 f_2(Q_\infty)$.

Lemma 1. *In the above situation, assume in addition that J_{C_1} is a simple abelian variety, and that there is no non-constant morphism of degree $\leq \deg(f_1)$ from C_2 to the projective line. Then T_{f_1,f_2} has a finite kernel, and if $g(C_1) = g(C_2)$, then T_{f_1,f_2} is an isogeny.*

Proof Since J_{C_1} is simple, it is enough to show that T_{f_1,f_2} is not the zero map. So take a point $Q_1 \in D(K_s) \setminus f_2^{-1}(f_2(Q_\infty))$ and let c be the class of $P - P_\infty$, where $P = f_1(Q_1)$. Then $T_{f_1,f_2}(c)$ is the class of the divisor $D_P :=$

$\sum_{Q\in f_1^{-1}(P)} f_2(Q) - \deg(f_1)\cdot f_2(Q_\infty)$. Note that $D_P \neq 0$ (as a divisor). If the class of D_P is trivial, then we find a non-constant function on C_2 with pole order $\leq \deg(f_1)$ and hence a non-constant map of C_2 to the projective line of degree $\leq \deg(f_1)$, contradiction.

4 Hurwitz Spaces Attached to Hyperelliptic Curves in Odd Characteristic

4.1 The Case of Algebraically Closed Ground Field

In this subsection we *assume that $K = K_s$ is algebraically closed.*
For the first statements of this section K is allowed to have arbitrary characteristic but for the major part it is necessary to assume that the characteristic of K is odd. This hypothesis will be done in due time.

We first review the following concepts and terminology.

Let $f : D \to C$ be a non-constant separable morphism of curves. We call f (or D, if the context is clear) a *cover* of C. Let $\tilde{F}$ be the splitting field (or Galois closure) of the associated extension $F(D)/f^*F(C)$ of function fields. Since K is algebraically closed, it follows that $\tilde{F} = F(\tilde{D})$ is the function field of a curve $\tilde{D}/K$. Moreover, the inclusion $F(D) \subset \tilde{F}$ induces an (essentially unique) cover $f' : \tilde{D} \to D$. We call the composition $\tilde{f} = f \circ f' : \tilde{D} \to C$ the *Galois closure* of the cover $f : D \to C$.
The *monodromy group* of $f : D \to C$ is the group $G_f := \mathrm{Aut}(\tilde{f}) = \{\alpha \in \mathrm{Aut}(\tilde{D}) : \tilde{f}\circ\alpha = \tilde{f}\}$ of automorphisms of its Galois closure $\tilde{f}$. Thus, G_f is (isomorphic to) the Galois group of the Galois field extension $\tilde{F}/f^*F(C)$, i.e., $G_f \simeq \mathrm{Gal}(\tilde{F}/f^*F(C))$.
If $P \in \tilde{D}(K)$, let $G_P = G_P(\tilde{f}) = \{\alpha \in G_f : \alpha(P) = P\}$ be the ramification group (or decomposition group) at P. Thus $|G_P| = e_P(\tilde{f})$ is the ramification index of P. The set $\mathrm{Ram}(\tilde{f})$ of ramified points Q of $\tilde{f}$ on C is the set of points in $C(K)$ for which one (and hence each) point in $\tilde{f}^{-1}(Q)$ has ramification index > 1.
We recall that a cover $f : D \to C$ is *tamely ramified* if it is separable and if all ramification indices are prime to the characteristic of the ground field. In this case all ramification groups G_P are cyclic, the contribution of the point $P \in D(K)$ to the discriminant divisor of f is $|G_P| - 1$ and the *Riemann–Hurwitz genus formula* (used many times in the following) is very easy to handle. Moreover the compositum of tamely ramified covers is tamely ramified, and the so-called Lemma of Abhyankar holds. For all these facts we refer to [St].
The cover $\tilde{f}$ (respectively f) is *unramified* if $\mathrm{Ram}(\tilde{f}) = \emptyset$.
We observe:

Lemma 2. *If $C = \mathbb{P}^1$, then $G_f = \langle G_P\rangle_{P\in\tilde{D}(K)}$.*

For $U := \langle G_P\rangle_{P\in\tilde{D}(K)}$ has as its fixed field the function field of an unramified cover of $\mathbb{P}^1$, so $U = G_f$ because $\mathbb{P}^1$ has no non-trivial unramified covers.

The collection $(\{G_P\}_{P\in\tilde{f}^{-1}(Q)} : Q \in \mathrm{Ram}(\tilde{f}))$ of the conjugacy classes of the ramification subgroups of G_f (indexed by the set $\mathrm{Ram}(\tilde{f})$) is called the *ramification type* $\mathbf{C}$ of the cover $\tilde{f}$ (or of the cover f).

A *Hurwitz space* is a moduli space which parameterizes (isomorphism classes) of covers $h : C \to \mathbb{P}^1$ of the projective line of given degree n and given ramification type. Hence Hurwitz spaces are moduli spaces for covers with given ramification type and monodromy group.

We now turn to the construction of certain covers (and associated Hurwitz spaces) whose monodromy group is S_4, the symmetric group of degree 4. For this, *we shall assume for the rest of this subsection that* $\mathrm{char}(K) \neq 2$.

Lemma 3. *Assume that $f : C \to \mathbb{P}^1$ is a tamely ramified cover of degree n and that for every ramified point $Q \in \mathbb{P}^1(K)$ the number of points in $f^{-1}(Q)$ with even ramification order is even. Then $G_f \subset A_n$, the alternating group of degree n.*

Proof Let $\{P_1, \dots, P_t\}$ be the ramified points over Q. Let e_i be the ramification index of P_i. Since e_i is prime to the characteristic of K by hypothesis, the multiplicity of the discriminant divisor of f at Q is $\sum_{i=1}^{t}(e_i - 1)$ and hence is even. So the field discriminant $\mathrm{disc}(F(C)/f^*F(\mathbb{P}^1))$ is a square in $f^*F(\mathbb{P}^1) \simeq K(x)$, and hence by field theory, $G_f \leq A_n$.

Theorem 3. *Let $f_2 : C_1 \to \mathbb{P}^1$ be a cover of degree 3 such that every point on $\mathbb{P}^1$ has at least one unramified extension.*
Let $f_1 : C \to C_1$ be a ramified cover of degree 2 with ramification points $P_1, \dots, P_{2t}$ on C_1 such that exactly one point in ${f_2}^{-1}(f_2(P_j))$ is unramified with respect to f_1 and such that all ramification points of f_2 are unramified under f_1.
Define $f : C \to \mathbb{P}^1$ by $f = f_2 \circ f_1$. Denote by $\tilde{C}_1$ the Galois closure of the cover given by f_2, by $\tilde{C}$ the Galois closure of the cover $f : C \to \mathbb{P}^1$ and by C_Δ the cover over $\mathbb{P}^1$ obtained by adjoining the square root of the discriminant of f_2 to the function field of $\mathbb{P}^1$.

1. *The monodromy group of f_2 is isomorphic to S_3, the symmetric group of degree 3.*
2. *The cover $\tilde{C}_1/C_\Delta$ is unramified and is cyclic of degree 3.*
3. *The monodromy group G_f of f is isomorphic to S_4.*

Proof 1. The assumption on the ramification behavior of f_2 forces that f_2 cannot be Galois. Since $\deg(f_2) = 3$, it thus follows that its Galois closure has Galois group S_3.
2. From part 1. (or otherwise), we see that that the discriminant divisor $\mathrm{disc}(f_2)$ of f_2 cannot be a square, and hence C_Δ is the unique quadratic cover of $\mathbb{P}^1$ over which $\tilde{f}_2$ factors. By Galois theory, $\tilde{C}_1/C_\Delta$ is a Galois extension with cyclic Galois group of order 3. Since all ramification indices of f_2 (and hence of $\tilde{f}_2$) are ≤ 2, we see that $\tilde{C}_1/C_\Delta$ is unramified.

3. Let $F = F(\mathbb{P}^1)$, $F_1 = F(C_1)$ and $F_2 = F(C)$ be the function fields of the curves $\mathbb{P}^1$, C_1 and C. Then f_1 and f_2 induce inclusions $F \subset F_1 \subset F_2$. Since the assumptions of Lemma 3 are satisfied for f, we see from the proof of the lemma that $\mathrm{disc}(F_2/F)$ is a square in F, and so the hypotheses of the following Proposition 1 are satisfied. It thus follows from that proposition that $G_f \simeq S_4$, as claimed.

Proposition 1. *Let $F \subset F_1 \subset F_2$ be a tower of separable field extensions, and let $\tilde{F}_2/F$ be the Galois closure (or splitting field) of F_2/F. Assume that F_i/F is not normal for $i = 1, 2$ and that $[F_2 : F_1] = 2$ and $[F_1 : F] = 3$. If the discriminant* $\mathrm{disc}(F_2/F)$ *is a square in F and if* $\mathrm{char}(F) \neq 2$, *then* $\mathrm{Gal}(\tilde{F}_2/F) \simeq S_4$.

Proof Let $\tilde{F}_1$ be the Galois closure of F_1/F. Since $[F_2 : F_1] = 2$, we see that $\tilde{F}_2/\tilde{F}_1$ is a compositum of quadratic extensions which are all conjugate to $F_2\tilde{F}_1$, and so $N := \mathrm{Gal}(\tilde{F}_2/\tilde{F}_1)$ is an elementary abelian 2-group.
Since $\mathrm{disc}(F_2/F)$ is a square, we know that $G := \mathrm{Gal}(F_2/F)$ is a subgroup of the alternating group A_6. Thus also $N \leq A_6$. But every non-cyclic elementary abelian 2-group of A_6 is of the form $\{g_ig_j\}$, where $g_1, g_2, g_3 \in S_6$ are 3 disjoint transpositions, and hence $|N| \leq 4$. Now $N \neq 1$ because otherwise $F_2 = \tilde{F}_1$, so F_2/F would be normal, contradiction. Moreover, $|N| \neq 2$ because otherwise $N = \langle g \rangle \trianglelefteq G$, where $g \in A_6$ is a $(2,2)$-cycle. Since $3 = [F_1 : F] \mid |G|$, $\exists \sigma \in G$ of order 3 which therefore centralizes g. But no such pair (g, σ) exists in A_6, contradiction. Thus $|N| = 4$, and hence $|G| = [\tilde{F}_2 : \tilde{F}_1][\tilde{F}_1 : F] = |N| \cdot 6 = 24$.
Let $P_3 = \langle \sigma \rangle$ be a 3-Sylow subgroup of G. If $P_3 \trianglelefteq G$, then the "Normalizator/Centralizator theorem" [Hu] yields that $G/C_G(P_3)$ with $C_G(P_3)$ the centralizer of P_3 would be a subgroup of Aut P_3 and hence $C_G(P_3)$ would have index dividing 2. So it would contain N. This is a contradiction because as was mentioned above, the elements of N do not centralize σ. Thus, by Sylow, G has 4 distinct 3-Sylow subgroups $P_{3,i}$ and so the conjugation action on the set $\{P_{3,i}\}_{i=1}^4$ defines a homomorphism $\varphi : G \to S_4$ whose kernel is $N_1 := \cap_{i=1}^4 N_G(P_{3,i})$. Clearly, $3 \nmid |N_1|$, so $|N_1| \mid 2$ (because $|N_G(P_{3,i})| = 6$). If $|N_1| = 2$, then $N_1 \not\leq N$ because N has no subgroup of order 2 which is normal in G. But then N_1N is an elementary abelian subgroup of order 8 in A_6, contradiction. Thus $N_1 = 1$, so φ is injective and hence yields an isomorphism $G \simeq S_4$.

Remark 2. In the situation of Theorem 3, assume that s points $Q_1, \ldots, Q_s$ of $\mathbb{P}^1$ ramify in the cover f_2. Then the Riemann-Hurwitz formula [St] shows that $g(C_1) = s/2 - 2$ and $g(C_\Delta) = s/2 - 1$. In particular, $s \geq 4$ because $g(C_1) \geq 0$.
Moreover, if (as in Theorem 3) $2t$ points of C_1 ramify in the cover f_1, then $g(C) = 2g(C_1) - 1 + t = s + t - 5$.
We thus see that $s + t$ points of $\mathbb{P}^1$ ramify in the S_4-cover $\tilde{f} : \tilde{C} \to \mathbb{P}^1$. Since all have ramification index 2, we see by the Riemann-Hurwitz formula that $g(\tilde{C}) = 6(s + t - 4) + 1$.
The ramification structure of $\tilde{f}$ is a follows. If $Q' \in \tilde{C}(K)$ lies above some Q_i, then Q' is unramified over $\tilde{C}_2$ so $G_{Q'}$ is generated by a transposition (because $\mathrm{Gal}(\tilde{C}/\tilde{C}_2) = N$ contains all $(2,2)$-cycles of S_4). On the other hand, if $P' \in \tilde{C}(K)$

lies above some $f_2(P_i)$, then P' is ramified over $\tilde{C}_2$, so $G_{P'}$ is generated by a $(2,2)$-cycle. Thus, the ramification type $\mathbf{C}$ of $\tilde{f}$ consists of s conjugacy classes of transpositions and t conjugacy classes of $(2,2)$-cycles of S_4.

The covers considered in Theorem 3 naturally give rise to Hurwitz spaces $\tilde{\mathcal{H}}_{s,t}$ and $\mathcal{H}_{s,t}$ as follows. For a given $s \geq 4$ and t, let $\tilde{\mathcal{H}}_{s,t}(K)$ denote the set of isomorphism classes of covers $f = f_2 \circ f_1 : C \to \mathbb{P}^1$ of the type defined in Theorem 3. (As usual, two covers $f : C \to \mathbb{P}^1$ and $f' : C' \to \mathbb{P}^1$ are called isomorphic if there is an isomorphism $\alpha : C \to C'$ such that $f' \circ \alpha = f$.) Moreover, since the group $\mathrm{Aut}(\mathbb{P}^1)$ acts on $\tilde{\mathcal{H}}_{s,t}(K)$ (via $(\alpha, f) \mapsto \alpha \circ f$), we can also consider the orbit space $\mathcal{H}_{s,t}(K) := \mathrm{Aut}(\mathbb{P}^1)\backslash\tilde{\mathcal{H}}_{s,t}(K)$. Then we have

Theorem 4. *The moduli problem $\tilde{\mathcal{H}}_{s,t}$ is finely represented by a Hurwitz space $\tilde{\mathbb{H}}_{s,t}/K$ of dimension $s+t$ and the moduli problem $\mathcal{H}_{s,t}$ is coarsely represented by the quotient space $\mathbb{H}_{s,t} = \mathrm{Aut}(\mathbb{P}^1)\backslash\tilde{\mathbb{H}}_{s,t}$ of dimension $s+t-3$.*

Proof By Theorem 3 and Remark 2 we see that we can identify $\tilde{\mathcal{H}}_{s,t}(K)$ with the set $\mathcal{H}^{in}(S_4, \mathbf{C})$ of S_4-covers with ramification type $\mathbf{C}$ as in Remark 2. Since this extension is tamely ramified, the assertions follow from the work of Fried/Völklein and Wewers, as was discussed in [FK], p. 37.

4.2 Rationality

We now investigate to what extent the constructions of the previous subsection can be done over an arbitrary perfect ground field K (with $\mathrm{char}(K) \neq 2$). Here a basic difficulty is that the technique of Galois closure does not lead in general to curve covers.

To explain this in more detail, let $f : D \to C$ be a K-cover of curves, i.e. f is a separable, non-constant K-morphism of curves over K. As before, f gives rise to a separable extension $F(D)/f^*F(C)$ of the associated function fields, and so we can consider the splitting field (or Galois closure) $\tilde{F}$ of the extension $F(D)/f^*F(C)$.

However, $\tilde{F}$ need not in general be the function field of a (geometrically connected) curve $\tilde{D}/K$. For this it is sufficient and necessary that K is algebraically closed in $\tilde{F}$. In this case we say that f *admits a Galois closure*, for we have as before two induced Galois covers $f' : \tilde{D} \to D$ and $\tilde{f} = f \circ f' : \tilde{D} \to C$. It is immediate that if $\tilde{f}$ exists, then this construction commutes with base-change, and so $G_f := \mathrm{Aut}(\tilde{f}) \simeq G_{f_s}$ is the (geometric) monodromy group of the K_s-cover $f_s : D_s \to C_s$

Theorem 5. *Let $f_2 : C_1 \to \mathbb{P}^1_K$ and $f_1 : C \to C_1$ be two K-covers of curves such that their base-changes with K_s satisfy the hypotheses of* Theorem 3.
Then $f = f_2 \circ f_1 : C \to \mathbb{P}^1_K$ admits a Galois closure if and only if the field discriminant $\delta := \mathrm{disc}(F(C)/f^*F(\mathbb{P}^1_K))$ is a square in $f^*F(\mathbb{P}^1_K) \simeq K(x)$. If this is the case, then the Galois closure of f is an S_4-cover $\tilde{f} : \tilde{C} \to \mathbb{P}^1_K$.

Proof Let $F := f^*F(\mathbb{P}^1_K) \subset F(C) =: F_2$, and let $\tilde{F}$ be the splitting field of the extension F_2/F.
Suppose first that f admits a Galois closure, i.e. that K is algebraically closed in $\tilde{F}$. Then $\tilde{F}$ and K_s are linearly disjoint over K, so $\tilde{F}K_s$ is the splitting field of the extension F_2K_s/FK_s, and $\mathrm{Gal}(\tilde{F}/F) = \mathrm{Gal}(\tilde{F}K_s/FK_s)$. By the proof of Theorem 3 we know that $\mathrm{Gal}(\tilde{F}K_s/FK_s) \leq A_6$, and so also $\mathrm{Gal}(\tilde{F}/F) \leq A_6$. By field theory, this means that $\delta \in (F^\times)^2$.
Conversely, assume that δ is a square in F. Then the tower $F \subset F_1 := f_1^*F(C_1) \subset F_2$ of field extensions satisfies the hypotheses of Proposition 1, and so $\mathrm{Gal}(\tilde{F}/F) \simeq S_4$. Since also $\mathrm{Gal}(\tilde{F}K_s/FK_s) \simeq S_4$ by Theorem 3, it follows that $\tilde{F}$ and K_s are linearly disjoint over K, so K is algebraically closed in $\tilde{F}$ and hence f admits a Galois closure.

Remark 3. In the situation of Theorem 5, suppose that δ is not a square in $F \simeq K(x)$. Since δ is a square in $FK_s = K_s(x)$ (cf. Theorem 3), we see that $F' := F(\sqrt{\delta})$ is a quadratic constant extension of F, i.e., $F' = FK'$, where $K' = K(\sqrt{c})$, for some $c \in K$. Thus, it follows that the cover $f_{K'} : C_{K'} \to \mathbb{P}^1_{K'}$ (which is obtained from f by base-change with K') does admit a Galois closure. Moreover, by replacing the quadratic cover $f_1 : C \to C_1$ by its quadratic twist $f_1^\chi : C^\chi \to C_1$ (associated to the extension K'/K), we see that the twisted cover $f^\chi = f_2 \circ f_1' : C' \to \mathbb{P}^1_K$ satisfies the hypotheses of Theorem 5 and hence admits a Galois closure $\tilde{f}^\chi : \tilde{C}' \to \mathbb{P}^1_K$ with group S_4.
So we get: Either $f : C \to \mathbb{P}^1$ or its twist $f^\chi : C' \to \mathbb{P}^1$ admits a Galois closure, which is a S_4-cover.

4.3 The Hyperelliptic Case

For the rest of this section and for the whole following section we take $s = 4$. This is equivalent to the hypothesis that $g(C_1) = 0$ or to the hypothesis that C is a hyperelliptic curve of genus $t-1$ with hyperelliptic cover f_1. The curve C_Δ is an elliptic curve E, and we can choose as the origin of E for instance the unique point over Q_1. Then the cover $E/\mathbb{P}^1$ is given by computing modulo $-id_E$, i.e., by mapping a point on E to its $x-$coordinate, if E is given by a Weierstraß equation.
The moduli space of hyperelliptic curves $\mathcal{M}_{H,t-1}$ of genus $t-1$ has dimension $2t-3$.
For $t = 3$ Theorem 4 shows that the dimension of $\mathbb{H}_t := \mathbb{H}_{4,t}$ is 4 and hence larger than the dimension of the moduli space $\mathcal{M}_{H,2}$ of curves of genus 2. (Recall that all curves of genus 2 are hyperelliptic.). We can interpret this by the fact that there are infinitely many covers f_2 which give rise to the same isomorphism class of curves of genus 2. In fact for a given set of 6 points on $\mathbb{P}^1$ there are infinitely many maps of degree 3 such that pairs of these points have the same image.
For $t > 4$ the dimension of $\mathbb{H}_t$ is smaller than the dimension of $\mathcal{M}_{H,t-1}$, and so we will get only very special hyperelliptic curves attached to points on $\mathbb{H}_t$.
But the interesting case is $t = 4$. We get hyperelliptic curves of genus 3, and the

moduli space of such curves is irreducible and has dimension 5.
By elementary linear algebra we shall see in Subsection 5.1 that every hyperelliptic curve of genus 3 covers $\mathbb{P}^1$ by a map f such that f corresponds to a point in $\mathbb{H}_t$, and that, generically, to given hyperelliptic curve C there are exactly 2 such covers up to equivalence. Hence we get a 2-fold cover map from $\mathbb{H}_t$ to the moduli space of hyperelliptic curves of genus 3.

Construction of Points on $\mathbb{H}_t$ Take $f = f_2 \circ f_1 : C \to \mathbb{P}^1$ as above. It follows that both C_Δ and $\tilde{C}_1$ are elliptic curves E and E', respectively, which come equipped with an isogeny $\rho : E' \to E$ of degree 3.
We have a bit more: The monodromy group of f_2 is S_3. We embed it into the group of automorphisms $\mathrm{Aut}_K(E')$. Let φ be such an automorphism. Then φ is of the form $\pm id_{E'} + t_V$ where t_V is the translation on E' by a point V.
Let $\sigma \in S_3$ be an element of order 2 and $\tau \in S_3$ be an element of order 3. Since $\langle \sigma, \tau \rangle = S_3$, we have $\sigma = -id_{E'} + t_R$ with $R \in E'(\mathbb{F}_q)$ and $\tau = t_{V_3}$, where V_3 is a point of order 3 of E'. By an appropriate choice of the neutral elements of E and E' (we use that $K = K_s$) we can assume that $V = 0$ and that f_2 is an isogeny.
Let $R_1, R'_1, R_2, R'_2, \ldots, R_{2t}, R'_{2t}$ be the set of points on E' which ramify in $C \times_{C_1} E'/E'$. Then we find $\epsilon_j \in \{-1, 1\}; 1 \leq j \leq t$ such that after a suitable ordering we get $R_k = -R'_k$ for $k = 1, \ldots, 2t$ and $R_j = R_{t+j} + \epsilon_j \cdot V_3$ for $j = 1, \ldots, t$.
Conversely, begin with an elliptic curve E with $Q'_1, \ldots, Q'_4 \in E(K)[2]$, the group of points of order 2 of E. We normalize and assume that Q'_1 is the neutral element of E and denote by π_E the map from E to $E/\langle -id_E \rangle = \mathbb{P}^1$. Define $Q_j := \pi_E(Q'_j)$. Take E' with point V_3 of order 3 such that $\rho : E' \to E$ is an isogeny of degree 3 with kernel $\langle V_3 \rangle$.
Since $\rho(0_{E'}) = 0_E$, the curve $E'/\langle -id_{E'} \rangle$ is a projective line covering $E/\langle -id_E \rangle$ by a map f_ρ of degree 3 that is ramified exactly in $Q_1, \ldots, Q_4$ in the following way: In the inverse image of Q_i under f_ρ there is one point with ramification index 2 and one unramified point. Hence the discriminant divisor of f_ρ is $Q_1 + \cdots + Q_4$.
Define $\varGamma_\rho$ as the subset of E'^t consisting of all the t-tuples $(R_1, \ldots, R_t)$ for which $\{\pm R_j, \pm(R_j + \epsilon_j \cdot V_3));\ 1 \leq j \leq t\}$ (the signs ± taken independently) has strictly less than $4t$ elements.
Next choose t points $R_1, \ldots, R_t \in E'(K) \setminus \varGamma_\rho$.
Take $P_1, \ldots, P_{2t}$ as the images under $\pi_{E'}$ of $\{R_j, R_j + \epsilon_j \cdot V_3, j = 1, \ldots, t\}$. By assumption, these points are distinct and we have $f_\rho(P_j) = f_\rho(P_{j+t})$ for $j = 1, \ldots, t$.
It follows that $f_\rho, P_1, \cdots, P_{2t}$ give rise to a point in $\mathbb{H}_t$.
From the above considerations we know that we get all points of $\mathbb{H}_t$ by this construction.
Before we summarize we make one remark. We have to look at covers f modulo the equivalence relation induced by automorphisms of $\mathbb{P}^1$. But applying such an automorphism does not change the isomorphism class of the elliptic curve E.

Moreover elliptic curves with points of order 3 are parameterized by the modular curve $X_1(3)$ (which has genus 0).

Theorem 6. *We get a surjective map from the set of points of* $\{(E', V_3) \in X_1(3)(K), (R_1, \dots, R_t) \in E'(K)^t \setminus \varGamma_\rho\}$ *to* $\mathbb{H}_t(K)$ *with finite fibres.*
Hence there is a rational dominant morphism from $(\mathcal{E}_3)^t_{X_1(3)}$ *(the* t*-fold fibre product over* $X_1(3)$ *of the universal elliptic curve* $\mathcal{E}_3$ *over* $X_1(3)$*) to* $\mathbb{H}_t(K)$ *with finite fibres.*

4.4 The Trigonal Construction

The basic task of the classical "trigonal construction" of Recillas, Donagi and Livné (cf. [DL]) is the following. Given a curve C/K equipped with cover $f = f_2 \circ f_1 : C \to \mathbb{P}^1$ with degree $f_1 = 2$ and $f_1 = 3$ (for short this is called usually a (2,3)-cover), construct another curve D/K equipped with cover $g : D \to \mathbb{P}^1$ that has degree 4 and a surjective homomorphism $h : J_C \to J_D$ (of a specific type). In the cases studied by these authors, $g(D) = 3$, but this hypothesis is not necessary. Here we shall see that the construction of the S_4-cover via Galois closure (cf. Subsection 4.1) naturally solves this task.

Thus, let $f = f_2 \circ f_1 : C \to \mathbb{P}^1$ be a $(2,3)$-cover as in Theorem 3, and let $\tilde{f} = f \circ f' : \tilde{C} \to \mathbb{P}^1$ be its Galois closure. Thus $G_f = \mathrm{Aut}(\tilde{f}) \simeq S_4$. The Galois group $H := \mathrm{Aut}(f')$ of $\tilde{C}/C$ has order 4 and contains two transpositions; let σ be one of these. Then σ is contained in precisely two of the stabilizers $T_1, \dots, T_4$ of the elements $\{1, 2, 3, 4\}$ on which S_4 acts. If $T = T_i$ is one of these, then we have $T \cap H = \langle \sigma \rangle$.
Let $\pi_T : \tilde{C} \to D := \tilde{C}/T$ be the quotient map. Then $\tilde{f}$ factors over π_T as $\tilde{f} = g \circ \pi_T$, where $g : D \to \mathbb{P}^1$ has $\deg(g) = 4$. Note that g is primitive (does not factor over a quadratic subcover).
We can use the Hurwitz genus formula to compute the genus of D. (Assume $s = 4$.) Since the Galois closure of $g : D \to \mathbb{P}^1$ is $\tilde{f} : \tilde{C} \to \mathbb{P}^1$, we see that exactly the points on $\mathbb{P}^1$ ramified in $\tilde{C}$ are ramified in D. Since the fixed field of the subgroup A_4 is $C_\Delta = E$, the discriminant divisor of g equals the discriminant divisor of $C_\Delta/\mathbb{P}^1$ plus 2 times another divisor. This is enough to conclude that the points $Q_1, \dots, Q_4$ have one ramified extension of order 2 and the t points in $\{f_2(P_1), \dots, f_2(P_{2t})\}$ (recall that the image under f_2 of $\{P_1, \dots, P_{2t}\}$ consists of exactly t points) have 2 ramified extensions. It follows that the genus of D is equal to $t - 1$, and hence is equal to the genus of C.
Finally, we construct a correspondence from J_C to J_D. For this, let $\pi_\sigma : \tilde{C} \to D' := \tilde{C}/\langle \sigma \rangle$ be the quotient map. Then f' factors over π_σ as $f' = \varphi_1 \circ \pi_\sigma$ and similarly π_S factors as $\pi_S = \varphi_2 \circ \pi_\sigma$.
We remark that φ_1 cannot be unramified. For otherwise the compositum of the function fields $F(D')$ and $F(\tilde{C}_1)$ would be unramified over $F(C) \cdot F(\tilde{C}_1)$. But the discussion in the proof of Theorem 3 shows that this is not true. We choose one of these ramification points as P_∞ on C and so the assumptions of Lemma

1 are satisfied for $\varphi_1 : D' \to C$.

Definition 3. The correspondence $T_C(f) := T_{\varphi_1,\varphi_2}$ is the homomorphism from $\mathrm{Pic}^0(C)$ to $\mathrm{Pic}^0(D)$ induced by $\varphi_{2*} \circ \varphi_1^*$.

Using Lemma 1, we obtain:

Theorem 7. *Assume that the Jacobian J_C is a simple abelian variety and that D is not hyperelliptic. Then $T_C(f)$ is an isogeny.*[4]

4.5 Rationality Questions over Finite Fields

Let K be the finite field $\mathbb{F}_q$ with q elements (q odd), and let K_s be its separable closure. Let C be a hyperelliptic curve of genus $g(C) > 1$ defined over $\mathbb{F}_q$ with cover $f : C_s \to \mathbb{P}^1$ defined over K_s as above. We want to give conditions for the rationality of the isogeny of J_{C_s} induced by the correspondence $T_C(f)$.
Given C, there is a uniquely determined $\mathbb{F}_q$-rational 2-cover f_1 of C to the projective line, denoted by C_1, with $2t = 2g(C)+2$ ramification points $P_1, \ldots, P_{2t} \in C_1(K_s)$. The discriminant divisor $\mathrm{disc}(f_1) = P_1 + \ldots + P_{2t}$ is K-rational, so in particular the set $\{P_1, \ldots, P_{2t}\}$ is invariant under G_K.
Conversely, to a given Galois invariant set $\{P_1, \ldots, P_{2t}\}$ of points on $C_1 = \mathbb{P}^1$ we find (in general) two hyperelliptic covers $C/\mathbb{P}^1$ and $C'/\mathbb{P}^1$ whose branch loci are $\{P_1, \ldots, P_{2t}\}$. These two curves are twists of each other and become isomorphic over K_s.
We now assume that the set $\{P_1, \ldots, P_{2t}\}$ is given and that we have a 3-cover $f_2 : \mathbb{P}^1 \to \mathbb{P}^1$ defined over $\mathbb{F}_q$ which maps $\{P_1, \ldots, P_{2t}\}$ pairwise to t points on $\mathbb{P}^1$. Then we know from Remark 3 that there is exactly one $\mathbb{F}_q$-rational quadratic cover f_1 of $\mathbb{P}^1$ such that $f := f_2 \circ f_1$ admits a Galois closure with Galois group S_4 and so there is a uniquely determined hyperelliptic curve cover $C/\mathbb{P}^1$ defined over $\mathbb{F}_q$ with branch points $\{P_1, \ldots, P_{2t}\}$. By the discussion of the "trigonal construction" in Subsection 4.4, it is clear that the constructed curve D and the correspondence $T_C(f)$ from J_C to J_D are both defined over $\mathbb{F}_q$. Hence the question about rationality of curves C with rational $T_C(f)$ boils down to the question of finding f_2.
This motivates the study of covers $h = f_2 : C_1 = \mathbb{P}^1 \to \mathbb{P}^1$ with h of degree 3 defined over $\mathbb{F}_q$ with discriminant divisor $Q_1 + \cdots + Q_4$, $Q_i \neq Q_j \in \mathbb{P}^1(K_s)$ for $i \neq j$. First we see that $\{Q_1, \ldots, Q_4\}$ is Galois invariant. Let $Q'_1, \ldots, Q'_4$ be the *unramified* extensions of $Q_1, \ldots, Q_4$ under h. These 4 points are exactly the ramification points of $\tilde{C}_1/C_1$ where as usual $\tilde{C}_1$ is the Galois closure of $h : C_1 = \mathbb{P}^1 \to \mathbb{P}^1$. Hence $\tilde{C}_1$ is an absolutely irreducible curve over $\mathbb{F}_q$ of genus 1. Moreover, since our ground field is $\mathbb{F}_q$, the curve $\tilde{C}_1$ is an elliptic curve E' defined over $\mathbb{F}_q$. The monodromy group of h is S_3. As was seen in the discussion before Theorem 6, this implies that E' has an $\mathbb{F}_q$-rational point V_3 of order 3.

[4] A closer study ([Ka]) of the situation shows that the theorem is true without the extra assumptions, and that the kernel of T_C is a maximally isotropic subgroup of $J_C[2]$. In addition it is shown that $T_C(f)$ induces the isogeny constructed in [DL].

Lemma 4. *Let $h : \mathbb{P}^1 = C_1 \to \mathbb{P}^1$ be as above. Then $\tilde{C}_1$ is characterized as the elliptic curve E' which is uniquely determined by an affine equation $Y^2 = g'_4(X)$ with zeroes $Q_1, \dots, Q_4$ and which has an $\mathbb{F}_q$-rational point V_3 of order 3.*
Let $E = E'/\langle V_3 \rangle$. Then h induces an isogeny of degree 3 from E' to E and E has an $\mathbb{F}_q$-rational point of order 3. This determines uniquely the twist class of E.

Conversely: Let E' be an elliptic curve with a K-rational point V_3 of order 3 and let $\rho : E' \to E$ be the isogeny with kernel $\langle V_3 \rangle$. Let $\sigma' = -id_{E'} + t_R$ with some point $R \in E'(\mathbb{F}_q)$ be an automorphism of E' of order 2 and $C_1 := E'/\langle \sigma' \rangle$. Take $\sigma = -id_E + t_{\rho(R)}$ and $\mathbb{P}^1 = E/\langle \sigma \rangle$. Then ρ induces a map $h' : C_1 \to \mathbb{P}^1$ with $\tilde{C}_1 = E'$ and the required properties.

Theorem 8. *Let $\{P_1, \dots, P_t\}$ be a $G(K_s/\mathbb{F}_q)$-invariant set of t points in $\mathbb{P}^1(K_s)$. Let $g_4(X)$ be a polynomial of degree 4 over $\mathbb{F}_q$ with distinct roots such that the elliptic curve $E' : Y^2 = g_4(X)$ has an $\mathbb{F}_q$-rational point Q of order 3. Let $\tilde{P}_1, \dots, \tilde{P}_t$ be points on E' with X-coordinates $P_1, \dots, P_t$. Choose $\epsilon_1, \dots, \epsilon_t \in \{1, -1\}$ and define P_{t+j} as the X-coordinate of $\tilde{P}_j + \epsilon_j Q$. Assume that the cardinality of $\{P_1, \dots, P_t, P_{t+1}, \dots, P_{2t}\}$ is $2t$ (this is generically true).*
Then there is an (up to $\mathbb{F}_q$-isomorphism) unique hyperelliptic curve cover $C/\mathbb{P}^1$ with branch points $\{P_1, \dots, P_t, P_{t+1}, \dots, P_{2t}\}$ that has an $\mathbb{F}_q$-rational correspondence of the form $T_C(f)$.

Remark 4. From the point of view of Hurwitz spaces Theorem 8 is a satisfying result. But it does not solve the problem: For given C decide whether E' exists and compute the equation for E'.
We shall see an explicit result for $g(C) = 3$ in the next section.

4.6 Computational Aspects

We continue to take $K = \mathbb{F}_q$ and we assume that the conditions of Theorem 8 are satisfied for the curve C.

Precomputation
1) We know equations for E'/C_1 and we can compute the isogeny ρ.
2) Next compute an equation for $H := C \times_{C_1} E'$ (i.e. compute the compositum $F(C)F(E')$ of the function fields of C and E' over the rational function field $\mathbb{F}_q(T)$ embedded by the cover maps $C \to C_1$ and $E' \to C_1$).
3) Knowing ρ, we can compute an equation for a conjugate H^τ of H with respect to the automorphism τ of order 3 of E' and hence for the Galois closure $\tilde{H} = \tilde{C}$ of f.
4) Determine a subcover $D' = \tilde{C}/\langle \sigma \rangle$ of degree 2 of $\tilde{C}$ which covers C but not E' and compute an equation of the cover $\varphi_1 : D' \to C$.
5) Choose a point $P_\infty \in C(\mathbb{F}_q)$ (this exists in all interesting cases) and compute $\varphi_1^*(P_\infty) = R^1_\infty + R^2_\infty$.
6) Determine a subcover D of degree 3 over D' and compute an equation for D

and for the cover $\varphi_2 : D' \to D$.
7.) Compute $S^j_\infty = \varphi(R^j_\infty)$.

All these computations can be performed (cf.[He]) in time and space polynomial in $\log(q)$.

Transfer of DL: Let c be a divisor class group of C. Present c by

$$\sum_{j=1,\dots,g(C)} P_j \ - g(C) \cdot P_\infty.$$

Lift the points P_j to points $R_{i,j}$ on D' by using the equation of the curve cover $\varphi_1 : D' \to C$ (or of the extension $F(D')/F(C)$).
Determine the images $S_{i,j}$ of $R_{i,j}$ on the curve to D by using the equation of the curve cover $\varphi_2 : D' \to D$.
Then $T(f)(c)$ is the class of $\sum_{j=1,\dots,g(C),i=1,2} S_{i,j} \ - g(C)(S^1_\infty + S^2_\infty)$.
By methods of [He] one finds a representative of $T(f)(c)$ as difference of divisors of degree bounded by $g(D)$ in polynomial time in $\log(q)$.

Result: For a known map $f : C \to \mathbb{P}^1$ one can compute $T_C(f)$ in polynomial time in $\log(q)$.

5 Curves of Genus 3

5.1 The Construction of Trigonal Subcovers

We recall that to every $\mathbb{F}_q$-rational point on $\mathbb{H}_4$ we have an attached hyperelliptic curve C of genus 3 and a map $f : C \to \mathbb{P}^1$ of degree 6 such that $T_C(f)$ is $\mathbb{F}_q$-rational. C is determined up to $\mathbb{F}_q$-isomorphisms, and $T_C(f)$ is computable in time and space polynomial in $\log(q)$.
Let us look at the situation over K_s. Since the dimension of $\mathbb{H}_4$ is 5 we get a dominant map from $\mathbb{H}_4$ to the moduli space of hyperelliptic curves of genus 3. In other words: For given Weierstraß points $Q_1, \dots, Q_8$ of a "generic" hyperelliptic curves C we find a cover $f_2 : \mathbb{P}^1 \to \mathbb{P}^1$ *over* K_s that maps these points pairwise to 4 different points. In fact, there will be generically 2 such covers ([DL]). We give a proof for this fact by elementary linear algebra.

Theorem 9. *Over K_s there is a rational dominant map of degree 2 from $\mathbb{H}_4$ to $\mathcal{M}_{H,3}$, the moduli space of hyperelliptic curves of genus 3.*

Proof We fix 8 different points on $\mathbb{P}^1(K_s)$ lying in an affine part with affine coordinates $u_1, \dots, u_8$.
We look for a rational function $h(U) = \frac{U^3+x_1U^2+x_2U+x_3}{x_4U^3+x_5U^2+x_6U+x_7}$ with $x_i \in K_s$ such that (without loss of generality) $h(u_1) = h(u_2) = 0; h(u_3) = h(u_4) = \infty, h(u_5) = h(u_6) = 1$ and $h(u_7) = h(u_8) = t$ where t is an appropriately chosen element in

K_s.
Hence $(x_1, \ldots, x_7)$ has to be a solution of the system of linear equations

$$\begin{pmatrix} u_1^2 & u_1 & 1 & 0 & 0 & 0 & 0 \\ u_2^2 & u_2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & u_3^3 & u_3^2 & u_3 & 1 \\ 0 & 0 & 0 & u_4^3 & u_4^2 & u_4 & 1 \\ u_5^2 & u_5 & 1 & -u_5^3 & -u_5^2 & -u_5 & -1 \\ u_6^2 & u_6 & 1 & -u_6^3 & -u_6^2 & -u_6 & -1 \\ u_7^2 & u_7 & 1 & -t \cdot u_7^3 & -t \cdot u_7^2 & -t \cdot u_7 & -t \\ u_8^2 & u_8 & 1 & -t \cdot u_8^3 & -t \cdot u_8^2 & -t \cdot u_8 & -t \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = \begin{pmatrix} -u_1^3 \\ -u_2^3 \\ 0 \\ 0 \\ -u_5^3 \\ -u_6^3 \\ -u_7^3 \\ -u_8^3 \end{pmatrix}$$

The parameter t occurs linearly exactly in two rows of the system and hence the determinant of the extended matrix of the system is a polynomial of degree 2 in t over K_s. The condition of solvability of the system, namely that the rank of the extended matrix is ≤ 7, is satisfied if t is a zero of this polynomial, and so generically two values are possible for t.

Now take a hyperelliptic curve C over $\mathbb{F}_q$ given by an equation $Y^2 = f_8(X)$ and let $\{u_1, \ldots, u_8\}$ be the set of roots of f_8. On this set we have an action of the absolute Galois group of $\mathbb{F}_q$. We know that these values come in pairs u_j, u_{4+j} $(j = 1, \ldots, 4)$ with members behaving in the same way under the Galois action, and we look for a $\mathbb{F}_q$-rational map h with $h(u_j) = h(u_{4+j}) = t_j$.
A first condition is that the set $\{t_1, \ldots, t_4\}$ is Galois invariant, too.
In addition, one knows that the absolute Galois group of $\mathbb{F}_q$ is generated by the Frobenius automorphism ϕ_q, and so the cycles induced by this action on $\{t_1, \ldots, t_4\}$ induce cycles of quadratic polynomials defined over $\mathbb{F}_q(t_1, \ldots, t_4)$ with zeros $u_j, \ldots, u_{4+j}$. This is enough to list necessary and sufficient conditions for the rationality of h (over a possibly quadratic extension of $\mathbb{F}_q$) in terms of the decomposition of $f_8(X)$ in irreducible factors over $\mathbb{F}_q$.
For a detailed discussion we refer to [S].

Algorithmic Aspects For a given $f_1 : C \to \mathbb{P}^1$, we first check whether the Weierstraß points satisfy the Galois condition from above. If so, we solve the linear system found in the proof of Theorem 9 if possible, and hence we obtain the rational map h ($= f_2$ in our notation above). These computations are done in an extension field of $\mathbb{F}_q$ of degree at most 8. Next we compute the discriminant of h and so we find the elliptic curves E and E'. To determine the twist class of C, we compute the class of the discriminant of $h \circ f_1$ modulo squares (alternatively, one can check whether there is a point on $\mathbb{P}^1(\mathbb{F}_q)$ that is completely split under $h \circ f_1$). Now we can proceed as in subsection 4.6.

5.2 Application to Discrete Logarithms

We now apply our results to hyperelliptic curves C of genus 3 with the additional assumption that the Jacobian J_C is a simple abelian variety. (This is the interesting case for cryptography and is true generically.) First assume that $K = K_s$. We shall use two facts about curves of genus 3.

- The moduli space of curves of genus 3 is connected and has dimension 6. Generic curves of genus 3 can be given by plane curves of degree 4 (without singularities).
- The moduli space $\mathcal{M}_{H,3}$ of hyperelliptic curves of genus 3 is connected and has dimension 5 and the generic hyperelliptic curve has no primitive cover to $\mathbb{P}^1$ of degree 4.[5]

Thus, if C is a generic hyperelliptic curve of genus 3, then the curve D constructed by the above trigonal construction cannot be hyperelliptic because D is a primitive cover of $\mathbb{P}^1$ of degree 4.

Consequence
There is a 5-dimensional subvariety U of $\mathcal{M}_{H,3}$ such that for $C \in U$ the curve D is not hyperelliptic.

Now take $K = \mathbb{F}_q$ and q large. Then the number of isomorphism classes of hyperelliptic curves C of genus 3 defined over $\mathbb{F}_q$ and satisfying

1. J_C is a simple abelian variety
2. $C \in U$
3. $T_f(C)$ is rational over $\mathbb{F}_q$

is of order $\mathcal{O}(q^5)$.[6]
By Theorem 7 $T_C(f)$ is an isogeny over K_s and hence over $\mathbb{F}_q$ if $C \in U$. Even a very coarse and elementary estimate of the degree of this isogeny shows that for cryptographically interesting primes ℓ we get a transfer of the DL in $\mathrm{Pic}^0(C)[\ell]$ to the DL in $\mathrm{Pic}^0(D)[\ell]$ in polynomial time and Theorem 2 yields that the complexity of the discrete logarithm in $\mathrm{Pic}^0(C)[\ell]$ is, up to logarithmic factors, $\mathcal{O}(q)$.

Theorem 10 (Smith). *There are $\mathcal{O}(q^5)$ isomorphism classes of hyperelliptic curves of genus 3 defined over $\mathbb{F}_q$ for which the discrete logarithm in the divisor class group of degree 0 has complexity $\mathcal{O}(q)$, up to log-factors.*
Since $|\mathrm{Pic}^0(C)| = \mathcal{O}(q^3)$, the DL system of these hyperelliptic curves of genus 3 is weak.

6 The Case of Characteristic 2

The above method extends to the case of $\mathrm{char}(K) = 2$ with some minor modifications, provided that C is an *ordinary* hyperelliptic curve of genus 3. Two

[5] The authors would like to thank Lange ([L]) for pointing out this result

[6] For a sharper estimate see [S]

of the main differences here are that (i) the S_4-extension is now wildly ramified and that (ii) we cannot use the arguments involving the square roots of field discriminants. But both these problems can be circumvented in the ordinary case. We briefly outline the main ideas involved.

Let $K = \mathbb{F}_q$, where $q = 2^n$, and let C/K be a hyperelliptic curve of genus 3 with hyperelliptic cover $f_1 : C \to C_1 = \mathbb{P}^1$. Then C is *ordinary* (i.e. its Hasse-Witt invariant σ_C (or the 2-rank of J_C) equals 3) if and only if the discriminant divisor of f_1 is of the form $\mathrm{disc}(f_1) = 2(P_1+\ldots+P_4)$, where $P_1, \ldots, P_4 \in C_1(K_s)$ are 4 distinct points.
By the linear algebra method of Subsection 5.1 it is easy to construct (many!) degree 3 subcovers $f_2 : C_1 \to \mathbb{P}^1$ such that $f_{2*}(\mathrm{disc}(f_1)) = 4(\bar{P}_1 + \bar{P}_2)$, with $\bar{P}_1 \neq \bar{P}_2 \in \mathbb{P}^1(K_s)$.

As before, put $f = f_2 \circ f_1 : C \to \mathbb{P}^1_K$, and let $f_s : C_s \to \mathbb{P}^1$ be the cover induced by base-change. Then one can show that the monodromy group of f_s is again S_4. To see this, note that the hypothesis of "ordinary" implies that all non-trivial ramification groups G_P are still cyclic of order 2, and that each is generated by a $(2,2)$-cycle in S_6. Thus, by Lemma 2, it follows that $G_{f_s} \leq A_6$, and so the proof of Proposition 1 can be modified to show that $G_{f_s} \simeq S_4$.

By Galois theory (and group theory), the splitting field $\tilde{F}$ of $F(C)/f^*F(\mathbb{P}^1_K)$ is a Galois extension of $F := f^*F(\mathbb{P}^1_K)$ of order dividing 48. Since we know by the above that $\mathrm{Gal}(\tilde{F}K_s/FK_s) \simeq S_4$, we see that either $\mathrm{Gal}(\tilde{F}/F) \simeq S_4$, and that hence f has a Galois closure with group S_4, or that there is a quadratic twist f_1^χ of $f_1 : C \to C_1$ such that $f^\chi := f_2 \circ f_1^\chi$ has a Galois closure $\tilde{f}^\chi$ with group S_4.

Thus, up to a quadratic twist, $f : C \to \mathbb{P}^1_K$ has a Galois closure $\tilde{f} : \tilde{C} \to \mathbb{P}^1_K$ with monodromy group S_4. By the method of the trigonal construction of Subsection 4.4, we thus obtain a K-rational curve D equipped with a primitive cover $g : D \to \mathbb{P}^1_K$ of degree 4 and a correspondence $T_C(f) : J_C \to J_D$ which turns out to be an isogeny. This latter fact requires the arguments mentioned in the footnote to Theorem 7. It is to be hoped that D turns out to be non-hyperelliptic, but at present the authors do not know if the analogue of the second "known" fact of Subsection 5.2 is true in characteristic 2.

References

[ACF] H.Cohen, G. Frey, (eds.), Handbook of Elliptic and Hyperelliptic Curve Cryptography. CRC, 2005.

[DGTT] C. Diem, P. Gaudry, E. Thom, N. Thériault, A double large prime variation for small genus hyperelliptic index calculus. *Math. Comp.* **76** (2007), 475–492.

[D] C. Diem, An Index Calculus Algorithm for Plane Curves of Small Degree. In: F.Heß, S. Pauli, M.Pohst (eds.), Proc. ANTS VII, Springer LNCS 4076 (2006), 543-557.

[DL] R. Donagi, R.Livné, The arithmetic-geometric mean and isogenies for curves of higher genus. *Ann. Scuola Norm. Sup. Pisa Cl. Sci(4)* **28(2)** (1999), 323–339.

[F] G. Frey, Relations between Arithmetic Geometry and Public Key Cryptography. *Advances in Mathematics of Communications (AMC)* **4(2)** (2010), 281 - 305.

[FK] G. Frey, E. Kani, Curves of genus 2 with elliptic differentials and associated Hurwitz spaces. *Contemp. Math.* **487** (2009), 33–81.

[He] F. Hess, Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comp.* **33(4)** (2002), 425–445.

[Hu] B. Huppert, Endliche Gruppen I. Springer (1967).

[Ka] E. Kani, On the trigonal construction. In preparation.

[Ko1] N. Koblitz, Elliptic curve cryptosystems. Mathematics of Computation, **48** (1987), 203–209.

[Ko2] N. Koblitz, Hyperelliptic cryptosystems. Journal of Cryptology **1** (1989), 139–150.

[Kr] M. Kraitchik, Théorie des nombres,vol.1. Gauthier-Villars (1922).

[L] H. Lange, e-mail to G. Frey, 24. 3. 2009.

[MW] U.M. Maurer,S. Wolf, Lower bounds on generic algorithms in groups. LNCS **1403** (1998), 72–84.

[M] V. Miller, Short programs for functions on curves (1986), http://crypto.stanford.edu//miller/

[O] A.M. Odllyzko, Discrete logarithms in finite fields and their cryptographic significance, LNCS **209** (1985),224–314.

[S] B. Smith, Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves. In: Advances in Cryptology: EUROCRYPT 2008, Istanbul, LNCS **4965** (2008), pp. 163-180. Revised version in: *J. Cryptology* **22** (2009), 505–529.

[St] H. Stichtenoth, Algebraic function fields and codes, Springer-Verlag Berlin (1993).