# GLOBAL DUALITY, SIGNATURE CALCULUS AND THE DISCRETE LOGARITHM PROBLEM

MING-DEH HUANG AND WAYNE RASKIND

### Abstract

We develop a formalism for studying the discrete logarithm problem for the multiplicative group and for elliptic curves over finite fields by lifting the respective group to an algebraic number field and using global duality. One of our main tools is the *signature* of a Dirichlet character (in the multiplicative group case) or principal homogeneous space (in the elliptic curve case), which is a measure of its ramification at certain places. We then develop *signature calculus*, which generalizes and refines the index calculus method. Finally, using some heuristics, we show the random polynomial time equivalence for these two cases between the problem of computing signatures and the discrete logarithm problem. This relates the discrete logarithm problem to some very well-known problems in algebraic number theory and arithmetic geometry.

### Introduction

Let $A$ be a finite abelian group, which we write additively, and let $x$ be an element of $A$. Let $y$ be in the subgroup generated by $x$, so that $y = nx$ for some positive integer $n$. Recall that the *discrete logarithm problem* (DLP) is to determine $n$ in a computationally efficient way. The computational complexity of this problem when the bit size of the inputs is large is the basis of many public-key encryption schemes used today. Two of the most important examples of finite abelian groups that are used in public-key cryptography are the multiplicative group of a finite field and the group of points on an elliptic curve over a finite field (see [**19**] and [**23**] for the original papers and [**20**] for a survey of work as of 2000).

In what follows below, we will assume that $\ell$ is a large prime number dividing the order of $A$ and that $x$ is an element of order $\ell$. For $p$ a prime number and $q$ a power of $p$, we denote by $\mathbb{F}_q$ the finite field with $q$ elements and by $\mathbb{F}_q^*$ its multiplicative group of nonzero elements.

One of the best-known techniques to address the DLP is *index calculus*, which uses relations between elements of an abelian algebraic group to derive linear relations between their discrete logarithms. In the case of the multiplicative group of a finite prime field, $\mathbb{F}_p$, taking sufficiently many random liftings of elements of $\mathbb{F}_p^*$ to

https://doi.org/10.1112/S1461157000001509 Published online by Cambridge University Press

*LMS J. Comput. Math.* **12** (2009) 228–263

integers will ensure that some will only be divisible by small (compared to $p$) prime numbers. Then such relations can be derived because we know how to efficiently factor integers that are products of powers of small prime numbers. We will explain this more below and the reader can also consult e.g. [**22**], §5.1 or [**28**] for more details. Trying to imitate this method for an elliptic curve by lifting the curve to an algebraic number field has turned out to be less effective, because the behavior of the height function on the Mordell-Weil group of the lifted curve makes it far more difficult to derive relations like those just mentioned in the multiplicative group case (see [**15**] or [**17**] for more details). However an important aspect of index calculus has not been addressed in these studies, namely, the idea of leveraging small primes to tackle a computational problem that involves large primes, and it is not clear how this idea can be put to work in a setting that involves the Mordell-Weil groups of elliptic curves. In this paper we address this issue in both cases from the perspective of arithmetic duality and propose a unified method which we call *signature calculus*.

Our general strategy to address the DLP in an abelian algebraic group is to take a lifting of the group to an algebraic number field and use the reciprocity law of global class field theory. Others have taken this approach (see e.g. [**10**], [**11**], [**26**]), and we refine their methods and give a general exposition of the theory. We explain below in detail how this works for the multiplicative group of a finite field and for the group of points of an elliptic curve over a finite field. The idea is to construct a suitable "test" element, which is a Dirichlet character in the multiplicative group case and a principal homogeneous space in the elliptic curve case. This element pairs with the lifting of a point of the group and the reciprocity law gives an equation between the local terms of the pairing. The lifting from a finite field $\mathbb{F}_p$ to a global field preserves discrete logarithms at a place over $p$. This method thus allows us to distribute information on the discrete logarithms among a set of places which depends on the choice of test element and the manner of lifting. We define the *signature* of these test elements, which measures the ramification at primes above $p$ and $\ell$. Though the signatures are small, they uniquely identify the objects they represent (Dirichlet characters and principal homogeneous spaces). They are, in fact, succinct representations of those objects, and using some heuristics, we then show how the computation of the signature is equivalent to the respective DLP.

The original motivation for this work was to improve the known algorithms for the DLP for the multiplicative group and for elliptic curves over finite fields. While this paper synthesizes and generalizes known methods for addressing these problems, we have not come to any definite conclusion about whether the DLP should be more tractable than previously thought. Our approach shows that the difficulty of the DLP in this context is related to some well-known problems in computational number theory. For example, our methods indicate that the DLP for the multiplicative group of the finite prime field is closely related to the efficient construction of class fields of real quadratic fields, which is an active area of research (see [**8**], [**34**], §7.7, and [**35**]).

The unified approach based on global duality provides an ideal setting to compare and contrast index calculus methods in the multiplicative group and elliptic curve cases. The signature computation problem involves large primes, and the

question naturally arises as to whether small primes can be utilized to tackle the problem with greater computational efficiency, in a similar way as we mentioned for the multiplicative group. Following the equivalence results we show that in this setting, the index calculus method arises quite naturally for the discrete-log problem in the multiplicative group case and the corresponding signature computation problem. In contrast, our work here shows that a similar method cannot be fashioned in this way for the elliptic curve case. The success in one case and the lack thereof in the other is due to the difference in the nature of the pairings involved. In the multiplicative case, a Dirichlet character which is unramified at a finite place $v$ can nevertheless pair nontrivially with local non-units at $v$. This makes it possible for small primes to play a role in forming relations among values of local pairings. In the elliptic curve case, if $v$ is a good reduction place, there is a bijection between principal homogeneous spaces under a smooth proper model $\mathcal{E}_v$ of $E$ over the ring of local integers $R_v$ and the corresponding objects under the reduction of $\mathcal{E}_v$ mod $v$ (see e.g. [**24**], Chapter III, Remark 3.11(a)), and a theorem of Lang ([**21**], Theorem 2) implies that the latter objects are trivial. For small primes of bad reduction not dividing $\ell$, only the group of components of the special fibre of the Néron model of the elliptic curve over the ring of integers plays a role, and the order of this group is unlikely to be divisible by $\ell$ (see §5.1.2 below for more details). As a result, only primes of large norm can play a role in forming relations among values of local pairings in the elliptic curve case.

The computation of signatures is an intriguing problem, since an explicit description of the objects involved (Dirichlet characters and principal homogeneous spaces) and their associated field extensions would be huge (requiring a lot of computation), but the signatures sought are small. Although we show that the testing Dirichlet characters and principal homogeneous spaces exist, it remains an interesting question as to how they can be explicitly constructed. This is easier to handle in the multiplicative case, where we also derive a concrete number theoretic characterization of the character signature by working out the local pairings using norm residue symbols. For the elliptic curve case, we have a partial solution.

Similar ideas as used in this paper can be employed to study the discrete log problem in any connected abelian algebraic group $\mathcal{G}$ over a finite field. By a theorem of Chevalley (see [**4**] and [**7**] for a modern proof), such a group sits in an exact sequence:

$$0 \to L \to \mathcal{G} \to A \to 0,$$

where $L$ is an abelian linear algebraic group and $A$ is an abelian variety. The group $L$ is itself an extension of a unipotent group by a torus. Using these results and somewhat more complicated homological algebra than that used below, we can lift to an algebraic number field and produce cohomology classes against which to test a lifting of an element whose discrete log we seek to compute. We can then use an appropriate version of global duality in this situation (see [**2**]) to get an equation among the terms of the local pairings. We decided not to write this paper in that generality because it would serve to raise the technical level even higher than it is here, and we are not convinced of the utility of doing this in groups other than

abelian varieties and algebraic tori.

A survey of some this material appeared in [**16**], but the present paper is a more formal and detailed exposition which contains significant new material that is not in that paper. We have tried to be completely mathematically precise while retaining the cryptographic motivation and applications. In order to do this, in § 1 we recall some concepts from étale cohomology, global duality and index calculus. The reader who is familiar with these concepts may want to glance at this section to be familiar with our notation.

The idea of using global methods in this way was originally proposed by Frey [**10**], whom we thank for inspiration, helpful discussions, and for inviting us to present our work at the Elliptic Curve Cryptography (ECC) conference in Bochum in September 2004. Methods of this type have also been used by Frey and Rück [**11**], and by Nguyen [**26**]. Finally, we would like to express our deep gratitude to the referee for careful reading of the manuscript and many suggestions for improvement.

## 1. *Notation, Preliminaries and the Global Framework*

In this section we briefly call some basic methods and results from algebraic number theory, étale cohomology and the theory of abelian varieties. As all of this material can be found in the literature, our exposition here is rather terse, and we give references for more details. Readers who are comfortable with these concepts are invited to skim this section to get acquainted with the notation.

### 1.1. *Notation and Preliminaries*

If $A$ is an abelian group and $n$ is a positive integer, we denote by $A[n]$ the subgroup of elements $a$ of $A$ with $na = 0$. If $\ell$ is a prime number, we denote by $A\{\ell\}$ the $\ell$-primary part of $A$, which is the direct limit of the $A[\ell^m]$ for $m \geqslant 0$. If $A$ is a locally compact abelian group that is either profinite or torsion, we denote by $A^*$ the group $\text{Hom}_{cont}(A, \mathbb{Q}/\mathbb{Z})$ of continuous homomorphisms and refer to it as the *Pontryagin dual* of $A$. Here $A$ has its topology (profinite or discrete) and $\mathbb{Q}/\mathbb{Z}$ the discrete topology. Note that * is an exact functor since $\mathbb{Q}/\mathbb{Z}$ is a divisible abelian group.

Let $S$ be a base scheme and $X, Y$ schemes together with morphisms $f : X \to S$ and $g : Y \to S$. We shall sometimes refer to $X, Y$ as *schemes over $S$*. Recall that the fibre product $X \times_S Y$ of $X$ and $Y$ over $S$ is a scheme over $S$ together with morphisms to $X$ and $Y$ satisfying the universal property: for any scheme $Z$ over $S$ together with morphisms to $X$ and $Y$, there is a unique morphism from $Z$ to the fibre product that makes the obvious diagram commutative. For example, if $X = \text{Spec}(A), Y = \text{Spec}(B)$ and $S = \text{Spec}(C)$ are affine schemes, then the fibre product of $X$ and $Y$ over $S$ is $\text{Spec}(A \otimes_C B)$, and the general case may be done by gluing affine schemes (see e.g. [**13**], Chapter II, Theorem 3.3).

Let $R$ be a discrete valuation ring with fraction field $K$ and residue field $F$, and let $X$ be a smooth proper scheme over $Y = \text{Spec}(R)$. Recall that this means that the structure morphism:

$$f : X \to Y$$

is smooth and proper. The former condition means that the fibres over $K$ and $F$ are smooth, and the latter means that $f$ is separated and universally closed (i.e. that if we change base by a morphism $Z \to Y$, then the morphism:

$$X \times_Y Z \to Z$$

is closed). A projective morphism is proper. Recall that if $X \to Y$ is a proper morphism, then a point $P \in X(K)$ may be lifted to a point in $X(R)$. If the morphism is projective, this is accomplished by multiplying the homogeneous coordinates of the point by a suitable power of a uniformizing parameter of $R$ to clear the denominators. If $E$ is an elliptic curve over $K$, we may clear the denominators in defining defining equations to obtain a two dimensional scheme $\mathcal{E}$ over $R$ (not necessarily smooth over $R$) whose fibre over $K$ is $E$. Then $\mathcal{E}$ is proper over $R$, whereas the multiplicative group is affine and decidedly not proper over $R$. Note that $\mathcal{E}$ will not be a group-scheme in general unless $E$ has good reduction.

In the next few paragraphs, we give a very brief and terse review of étale cohomology, referring the reader to [**24**] for more details.

Let $f : Y \to X$ be a morphism of schemes. If $x \in X$ and $y \in Y$, let $\mathcal{O}_{X,x}$ be the local ring of $X$ at $x$ and $\mathcal{O}_{Y,y}$ be the local ring of $Y$ at $y$. Then we say that $f$ is *flat* if for each $y \in Y$ and $x \in X$ with $f(y) = x$, $\mathcal{O}_{Y,y}$ is a flat $\mathcal{O}_{X,x}$-module. Let $\mathfrak{m}_x$ and $\mathfrak{m}_y$ be the maximal ideals of the local rings $\mathcal{O}_{X,x}$ and $\mathcal{O}_{Y,y}$, respectively. Then $f$ is *unramified* at $y$ if $\mathfrak{m}_x$ generates $\mathfrak{m}_y$ and $\mathcal{O}_{Y,y}/\mathfrak{m}_y$ is a finite separable field extension of $\mathcal{O}_{X,x}/\mathfrak{m}_x$. When $X$ and $Y$ are the spectra of the rings of integers in algebraic number fields $K$ and $L$, this is the same as the usual definition of unramified in algebraic number theory. For example, consider the quadratic extension $\mathbb{Q}(i)/\mathbb{Q}$, let $Y = \mathrm{Spec}(\mathbb{Z}[i])$ and $X = \mathrm{Spec}(\mathbb{Z})$. If a rational prime $p$ splits in $L$, say $p = (x+iy)(x-iy)$, then $p$ generates the maximal ideal of the local ring, $\mathbb{Z}[i]_{(x+iy)}$, since $x - iy$ is invertible in this ring. But if we take the ideal $(2) = (1+i)^2$, 2 does not generate the ideal $(1+i)$ in $\mathbb{Z}[i]_{(1+i)}$, and therefore the morphism $f : Y \to X$ is ramified at $(1+i)$.

We say that $f$ is *étale* if it is flat and unramified. In the 1960's, Grothendieck suggested taking étale morphisms rather than inclusions of Zariski open sets to use as the "open sets" in a "finer topology" than the Zariski topology. This is called the étale topology and the machinery of homological algebra works in the very same way to give a cohomology theory called *étale cohomology*. Grothendieck's original motivation was to provide a good cohomology theory for varieties over finite fields to prove the Weil conjectures, but the theory has turned out to be very useful in many other contexts.

The étale cohomology of a field is essentially equivalent to its Galois cohomology. That is, if $K$ is a field, $\overline{K}$ is a separable closure of $K$, and $G = Gal(\overline{K}/K)$, any sheaf $\mathcal{F}$ for the étale topology gives rise to the $G$-module $M = \mathcal{F}_{\overline{K}}$, the stalk of $\mathcal{F}$

at the geometric point $\mathrm{Spec}(\overline{K})$ of $\mathrm{Spec}(K)$. Note that $M$ is a discrete $G$-module upon which $G$ acts continuously, in that the stabilizer of any element of $M$ is an open subgroup of $G$ with its Krull topology. Conversely, a discrete $G$-module $M$ upon which $G$ acts continuously gives rise to an étale sheaf by the correspondence $L \mapsto M^{Gal(\overline{K}/L)}$, where $L$ is a finite separable extension of $K$. Via this correspondence, we can compute the étale cohomology of such a sheaf $\mathcal{F}$ by computing the (profinite) group cohomology of $G$ with values in the module $M$ associated to it (see [24], pp. 52-53, especially Theorem 1.9 on p. 53 for more on this). But if $X$ is an open subset of the spectrum of the ring of algebraic integers in a number field, using group cohomology can be awkward when computing cohomology with values in sheaves that are not locally constant. For example, the ideal class group of $X$ can be expressed by the étale cohomology group $H^1(X, \mathbb{G}_{m,X})$, but it is more cumbersome to express this in terms of group cohomology. We also note that the fundamental group of an algebraic variety of dimension greater than 1 can be trivial while its étale cohomology may still be very interesting. In this paper, we will denote by $H^*(X, \mathcal{F})$ the étale cohomology of a scheme $X$ with values in an étale sheaf $\mathcal{F}$ on $X$. If $X$ is the spectrum of a field $K$ and $\mathcal{F}$ is associated to the Galois module $M$ as above, we will often write $H^*(K, M)$ instead of $H^*(X, \mathcal{F})$. We hope that the preceding remarks explain the utility of and need for using étale cohomology in this paper.

Let $X$ be a fixed base scheme and let $\mathcal{G}$ be an algebraic group over $X$. If $Y$ and $U$ are schemes over $X$, we will suppress $X$ in our notation and denote by $Y_U$ the fibre product of $Y$ and $U$ over $X$. Recall that a *torseur* over $X$ under $\mathcal{G}$ is a scheme $Y$ with an action of $\mathcal{G}$ that is locally isomorphic for the étale topology to $\mathcal{G}$ with its natural $\mathcal{G}$-action. That is, there is a covering of $X$ by étale morphisms $f_i : U_i \to X$ such that $Y_{U_i} \cong \mathcal{G}_{U_i}$ with its $\mathcal{G}_{U_i}$-action (see [24], Chapter III, §4, Proposition 4.1). For many $\mathcal{G}$, if we did this in the Zariski topology, we would not get very interesting objects, in general, and one of the original motivations for the étale topology was to be able to express well-known torseurs in such terms with a good topology. For example, if $K$ is a field and $\mathcal{G}$ is the constant group scheme $\mathbb{Z}/n\mathbb{Z}$, then a torseur $\mathcal{T}$ over $\mathrm{Spec}(K)$ under $\mathcal{G}$ may be described (up to isomorphism) by taking a finite separable field extension $L/K$ and a trivialization $\pi^*\mathcal{T} \cong \mathrm{Spec}(L) \times \mathbb{Z}/n\mathbb{Z}$, where $\pi^*$ denotes the pullback of $\mathcal{T}$ to $L$. To these data we can associate a Dirichlet character $\chi$ with $n\chi = 0$. Such characters are classified by the étale cohomology group $H^1(K, \mathbb{Z}/n\mathbb{Z})$. If we used the Zariski topology, we would have $H^1_{Zar}(K, \mathbb{Z}/n\mathbb{Z}) = 0$. More generally, the group $H^1(X, \mathcal{G})$ classifies $\mathcal{G}$-torseurs over $X$, up to isomorphism. If $X$ is the spectrum of a field $K$ and $\mathcal{G} = \mathbb{G}_{m,X}$, then Hilbert's theorem 90 (see e.g. [31], Chapter X, Proposition 2) implies that $H^1(X, \mathbb{G}_{m,X}) = 0$. If $A$ is an abelian variety the group $H^1(K, A)$ is very interesting, and its elements are referred to as *principal homogeneous spaces* under $A$ over $K$. These will play a big role in this paper.

Let $\tilde{E}$ be an elliptic curve over a finite field $\mathbb{F}$. Let $R$ be a discrete valuation ring with quotient field $K$ and residue field $\mathbb{F}$. Then a *lifting* $E$ of $\tilde{E}$ to $K$ is a smooth proper scheme $\mathcal{E}$ over $R$ whose generic fibre is $E$ and whose special fibre is $\tilde{E}$. We shall use rather simple liftings below, but let us point out that it is a theorem of

Deuring [**9**] that if $\tilde{E}$ is an elliptic curve over a finite field with an endomorphism $\varphi$, then the pair $(\tilde{E}, \varphi)$ can be lifted to a discrete valuation ring $R$ whose quotient field is an algebraic number field. If the curve is *ordinary*, as are the curves we consider in this paper, then one can lift the curve together with the whole endomorphism ring. A more systematic approach to liftings of ordinary elliptic curves is given by Serre-Tate theory (see e.g. [**32**], §5).

Let $K$ be a finite extension of the field of rational numbers $\mathbb{Q}$, which we call an *algebraic number field.* Fix an algebraic closure $\overline{K}$ of $K$ and let $G = Gal(\overline{K}/K)$. We consider normalized absolute values $v$ on $K$, which we call *places*. We will call places *nonarchimedean, real* or *complex* according to whether the completion $K_v$ is such a field. As most of our discussion will pertain to Dirichlet characters that are $\ell$-torsion, where $\ell$ is an odd prime number, we shall ignore the real and complex places for the most part. The nonarchimedean places of $K$ are in bijection with the prime ideals of height one in the ring of integers $\mathcal{O}_K$. We shall often implicitly use this bijection in our notation and terminology. For example, if we consider the prime spectrum of $\mathcal{O}_K$, we will sometimes refer to its closed points as "places."

If $M$ is a discrete $G$-module upon which $G$ acts continuously (where $G$ has the Krull topology in which open subgroups are those of finite index), we will denote by $H^i(K, M)$ the $i-th$ Galois cohomology group of $G$ with values in $M$, and similarly for $K_v$.

We shall mainly be using three types of fields, finite fields, denoted by $\mathbb{F}$, algebraic number fields, denoted by $K$, and the completion of an algebraic number field at a finite place $v$, denoted by $K_v$.

Let $n$ be a positive integer prime to the characteristic of $K$ and denote by $\mu_n$ the group of $n$-th roots of unity in $\overline{K}$. Then we have the *Kummer exact sequence*:

$$0 \to \mu_n \to \overline{K}^* \xrightarrow{n} \overline{K}^* \to 0.$$

If we take Galois cohomology of this sequence and use the fact that $H^1(G, \overline{K}^*) = 0$ (Hilbert's theorem 90), then we get the isomorphism:

$$K^*/K^{*n} \xrightarrow{\sim} H^1(G, \mu_n),$$

which we refer to as *Kummer theory*. More generally, for any scheme $X$, let $\mathbb{G}_{m,X}$ be the sheaf for the étale topology associated to the presheaf given by sending $U$ étale over $X$ to the group of invertible regular functions on $U$. Then for any positive integer $n$ that is prime to the characteristic of every residue field of $X$, we have the *Kummer exact sequence of sheaves for the étale topology*

$$0 \to \mu_n \to \mathbb{G}_{m,X} \xrightarrow{n} \mathbb{G}_{m,X} \to 0.$$

Taking étale cohomology of this sequence gives the short exact sequence:

$$0 \to H^0(X, \mathbb{G}_{m,X})/n \to H^1(X, \mu_n) \to H^1(X, \mathbb{G}_{m,X})[n] \to 0.$$

Let $S$ be a finite set of places of an algebraic number field $K$ and $\mathcal{O}_S$ the ring of $S$-integers of $K$. If $S$ contains all of the primes of $\mathcal{O}$ that divide $n$ and the ideal class group of $\mathcal{O}_S$ is of order prime to $n$, then from the preceding short exact sequence we get the isomorphism:

$$\mathcal{O}_S^* / \mathcal{O}_S^{*n} \xrightarrow{\sim} H^1(G_S, \mu_n),$$

where $G_S$ is the Galois group of a maximal extension of $K$ that is unramified outside $S$. This isomorphism will also be referred to as "Kummer theory." If $E$ is an elliptic curve over $K$ and $E[n]$ denotes the group of points over $\overline{K}$ that are killed by $n$, we have the similar sequence:

$$0 \to E[n] \to E(\overline{K}) \xrightarrow{n} E(\overline{K}) \to 0,$$

which gives the exact sequence:

$$0 \to E(K)/n \to H^1(G, E[n]) \to H^1(G, E(\overline{K}))[n] \to 0.$$

Again, we will refer to this as "Kummer theory".

Recall the Brauer group $Br(K)$ of similarity classes of finite dimensional central simple algebras over $K$, which can be described in terms of Galois cohomology by

$$Br(K) \cong H^2(K, \overline{K}^*).$$

If $K$ is an algebraic number field and $K_v$ is a completion of $K$, we have the invariant map:

$$inv_v : Br(K_v) \to \mathbb{Q}/\mathbb{Z},$$

which is an isomorphism if $v$ is nonarchimedean, injective with image isomorphic to $\mathbb{Z}/2\mathbb{Z}$ if $v$ is real, and the zero map if $v$ is complex.

One of the most important results in algebraic number theory is the Brauer-Hasse-Noether exact sequence:

$$(\dagger) \ 0 \to Br(K) \to \sum_v Br(K_v) \xrightarrow{\sum_v inv_v} \mathbb{Q}/\mathbb{Z} \to 0.$$

This is the beginning of the theory of *global duality*, which shows how to relate the arithmetic of $K$ with that of all of the $K_v$. The following subsections review this theory briefly in the context in which we shall use it.

1.2. *Reciprocity Law for the Multiplicative Group*

We review the reciprocity law in this context, mostly following the exposition of ([**31**], Chapter XIV). Let $K^*$ denote the set of nonzero elements of $K$, which is an abelian group under multiplication. We consider a Dirichlet character $\chi$ of $K$, which we view as an element of the Galois cohomology group $H^1(K, \mathbb{Q}/\mathbb{Z})$, where $G$ acts trivially on $\mathbb{Q}/\mathbb{Z}$. This group is nothing but $\text{Hom}_{cont}(G, \mathbb{Q}/\mathbb{Z})$. Note that the image of any such homomorphism is a finite cyclic group since $G$ is profinite

and $\mathbb{Q}/\mathbb{Z}$ is discrete with any finite subgroup being cyclic. Let $H$ be the kernel of this homomorphism and $L$ be the subfield of $\overline{K}$ fixed by $H$. Then we can view $\chi$ as being represented by $L/K$ together with a homomorphism:

$$Gal(L/K) \to \mathbb{Q}/\mathbb{Z}.$$

If the order of the image of this map is $n$, we can view $\chi$ as an element of $H^1(K, \mathbb{Z}/n\mathbb{Z})$.

Let $\partial(\chi)$ denote the image of $\chi$ under the boundary map

$$H^1(K, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\partial} H^2(K, \mathbb{Z})$$

in the long exact cohomology sequence associated to the short exact sequence of $G$-modules with trivial action:

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Then for $a \in K^*$ we consider

$$<\chi, a> := a \cup \partial(\chi) \in H^2(K, \overline{K}^*),$$

which is defined by taking cup-product under the pairing:

$$K^* = H^0(K, \overline{K}^*) \times H^2(K, \mathbb{Z}) \to H^2(K, \overline{K}^*) \cong Br(K).$$

If $L$ is the extension associated to $\chi$ (that is, $L = \overline{K}^{\ker \chi}$), then we have that $<\chi, a> = 0$ if and only if $a$ is a norm from $L^*$.

If $K$ is an algebraic number field, $\chi \in H^1(K, \mathbb{Q}/\mathbb{Z})$, $a \in K^*$ and $v$ is a place of $K$, then we can restrict $\chi$ to each $K_v$ and regard $a$ as an element of $K_v^*$. Note that we may have $\chi_v = 0$. We then denote the value of the local pairing by $<\chi_v, a_v>$. If $v$ is a nonarchimedean place then $Br(K_v) \cong \mathbb{Q}/\mathbb{Z}$ and we view $<\chi_v, a_v>$ as an element of $\mathbb{Q}/\mathbb{Z}$. Note also that if $v$ is a place where $\chi$ is unramified and $a$ is a unit at $v$, then $<\chi_v, a_v> = 0$ (see e.g. [**31**], Ch. V, Proposition 3b and Remark 1) at the bottom of p. 82). That is, every unit is a norm from an unramified extension of nonarchimedean local fields. Thus $<\chi_v, a_v> = 0$ for all but finitely many $v$. Since the local pairings are compatible with the global pairings, the exact sequence (†) above for the Brauer group of an algebraic number field shows that we have the *reciprocity law*

$$\sum_v <\chi_v, a_v> = 0 \in \mathbb{Q}/\mathbb{Z}.$$

If $L/K$ is a finite Galois extension, we can view this as a pairing:

$$\hat{H}^0(Gal(L/K), L^*) \times H^2(Gal(L/K), \mathbb{Z}) \to H^2(Gal(L/K), L^*) = Br(L/K),$$

where $\hat{H}$ denotes Tate cohomology and $Br(L/K)$ denotes the kernel of the restriction map $Br(K) \to Br(L)$. If $K$ is a nonarchimedean local field, then this pairing is nondegenerate (see [**31**], Corollary to Proposition 3 of Ch XIV, §1).

1.3. *Reciprocity Law for Elliptic Curves*

Let $E$ be an elliptic curve over $K$. Thus $E$ is a smooth, projective algebraic curve of genus 1 together with a distinguished rational point $O$, which serves as the identity element in an abelian group structure on $E$ that can be defined geometrically by a chord and tangent method. We denote by $E(K)$ the set of points of $E$ over $K$. Recall that a *principal homogeneous space* of $E$ over $K$ is a curve $F$ of genus 1 over $K$ together with a simply transitive group action of $E$ on $F$. In other words, a principal homogeneous space is a torseur under $E$ over $K$, as defined above. The isomorphism classes of such principal homogeneous spaces are classified by the group $H^1(K, E(\overline{K}))$, which we will often denote by $H^1(K, E)$. A principal homogeneous space is trivial if and only if it has a rational point over $K$, in which case it is isomorphic to $E$ over $K$. Thus, for any principal homogeneous space $F$, there is a finite extension $L/K$ such that $F_L$ becomes isomorphic to $E_L$. Let $Q \in E(K)$ and $\alpha \in H^1(K, E)$. We consider the pairings

$$< \alpha, Q > \in Br(K)$$

$$< \alpha_v, Q_v > \in Br(K_v) \cong \mathbb{Q}/\mathbb{Z}.$$

These are not as easy to describe explicitly as in the case of the multiplicative group, but we give here a quick if somewhat terse definition. Given an abelian variety $A$ over $K$, let $\hat{A}$ denote its dual, which is $Ext^1_K(A, \mathbb{G}_{m,X})$, where $\mathbb{G}_{m,X}$ is the multiplicative group scheme and the $Ext$ is taken in the category of algebraic groups over $K$ (see [**33**], VII, §3, Théorème 6). An elliptic curve is self-dual, so that we can identify $E(K)$ with $Ext^1_K(E, \mathbb{G}_{m,X})$. Given $Q \in E(K)$, represent it as a 1-extension of algebraic groups using this identification

$$0 \to \mathbb{G}_{m,X} \to X \to E \to 0,$$

and let

$$(\dagger\dagger)\ 0 \to \overline{K}^* \to X(\overline{K}) \to E(\overline{K}) \to 0$$

be the short exact sequence of $\overline{K}$-points of these groups. Then given an element $\alpha \in H^1(G, E(\overline{K}))$, let $< \alpha, Q >= \partial_Q(\alpha)$, the image of $\alpha$ under the boundary map:

$$H^1(G, E(\overline{K})) \overset{\partial_Q}{\to} H^2(G, \overline{K}^*)$$

in the long exact cohomology sequence obtained from the short exact sequence $(\dagger\dagger)$. For $\alpha \in H^1(G, E(\overline{K}))$ and $Q \in E(K)$ we denote by $\alpha_v$ the image of $\alpha$ in $H^1(G_v, E(\overline{K}_v))$ (which may be zero) and by $Q_v$ the image of $Q$ in $E(K_v)$. We can make a similar definition over the nonarchimedean fields $K_v$ for $\alpha_v \in H^1(G_v, E(\overline{K}_v))$ and $Q_v \in E(K_v)$ to get $< \alpha_v, Q_v > \in Br(K_v) \cong \mathbb{Q}/\mathbb{Z}$.

We will be interested in the situation where $\alpha \in H^1(K, E)[\ell]$, in which case we have the following commutative diagram:

$$
\begin{array}{ccccc}
E(K)/\ell & \times & H^1(K, E)[\ell] & \to & Br(K)[\ell] \\
\downarrow & & \downarrow & & \downarrow \\
E(K_v)/\ell & \times & H^1(K_v, E)[\ell] & \to & Br(K_v)[\ell]
\end{array}
$$

The bottom pairing is perfect (local duality for abelian varieties, see e.g. [**25**], Ch. I, §3, Corollary 3.4).

We then have that $< \alpha_v, Q_v >= 0$ for almost all $v$. The fundamental sequence (†), the identification $Br(K_v)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$, and the commutative diagram above imply that for $\alpha \in H^1(K, E)[\ell]$ and $Q \in E(K)$,

$$
\sum_v < \alpha_v, Q_v >= 0 \in \mathbb{Q}/\mathbb{Z}.
$$

1.4. *Cohomological basis of the unified approach*

Our approach is based on duality theorems for Galois modules and for abelian varieties over number fields. Let $K$ be an algebraic number field and $\mathcal{O}_K$ the ring of integers in $K$. Let $X = \mathrm{Spec}(\mathcal{O}_K)$ and $U$ be a nonempty open subset of $X$ with complement $S$. Thus $U$ consists of all but finitely many places of $K$. Let $\ell$ be a prime number that is invertible on $U$ and let $\mu_\ell$ be the sheaf of $\ell$-th roots of unity. We are interested in the groups $H^i(U, \mu_\ell)$. To aid us in computing them and related cohomology groups, we have the *Poitou-Tate exact sequence* (see e.g. [**25**], Ch. I, §4, Theorem 4.10c):

$$
0 \to H^0(U, \mu_\ell) \to \bigoplus_{v \in S} H^0(K_v, \mu_\ell) \to H^2(U, \mathbb{Z}/\ell\mathbb{Z})^* \to
$$

$$
H^1(U, \mu_\ell) \to \bigoplus_{v \in S} H^1(K_v, \mu_\ell) \to H^1(U, \mathbb{Z}/\ell\mathbb{Z})^* \to
$$

$$
H^2(U, \mu_\ell) \to \bigoplus_{v \in S} H^2(K_v, \mu_\ell) \to H^0(U, \mathbb{Z}/\ell\mathbb{Z})^* \to 0.
$$

This sequence summarizes many of the basic results from class field theory. Let $K_S$ be a maximal extension of $K$ that is unramified outside $S$ and put $G_S = Gal(K_S/K)$. Then any locally constant sheaf $\mathcal{F}$ on $U$ whose stalks at geometric points are $\ell$-primary torsion gives rise to a $G_S$-module $M$, and we have $H^i(U, \mathcal{F}) \cong H^i(G_S, M)$ (see e.g. [**29**], Proposition 2.3; this is a nontrivial fact, which depends on all primes dividing $\ell$ being in $S$). We shall often use this latter notation for the multiplicative group case. We are mainly interested in the middle line of the Poitou-Tate sequence:

$$
(*)_{\mu_\ell} : \quad H^1(G_S, \mu_\ell) \to \bigoplus_{v \in S} H^1(K_v, \mu_\ell) \to H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})^*
$$

and the dual sequence obtained by taking the Pontryagin dual and using Tate local duality:

$$(*)_{\mathbb{Z}/\ell\mathbb{Z}} : H^1(G_S, \mathbb{Z}/\ell\mathbb{Z}) \to \bigoplus_{v\in S} H^1(K_v, \mathbb{Z}/\ell\mathbb{Z}) \to H^1(G_S, \mu_\ell)^*.$$

For an elliptic curve $E$ over $K$ that has a smooth proper model $\mathcal{E}$ over $U$ on which $\ell$ is invertible, we have the *Cassels-Tate exact sequence* (see [**25**], Ch. II, §5, Theorem 5.6b):

$$(**) \; E(K)^{(\ell)} \to \bigoplus_{v\in S} E(K_v)^{(\ell)} \to H^1(U, \mathcal{E})\{\ell\}^* \to \text{Ш}(E)\{\ell\} \to 0.$$

Here $(\ell)$ denotes completion with respect to subgroups of $\ell$-power index, $\{\ell\}$ denotes the $\ell$-primary part of a torsion abelian group, and $\text{Ш}(E)$ is the Shafarevich-Tate group of everywhere locally trivial principal homogeneous spaces under $E$, which we assume to be finite.

We give here a very terse explanation of the common origin of these two exact sequences, as it is the key to our unified approach in the multiplicative group and elliptic curve cases. Let $\mathcal{F}$ be a sheaf on $U$ and $j_!\mathcal{F}$ denote extension of $\mathcal{F}$ by zero from $U$ to $X$ (see [**24**], II, §3, p.76). We have $j^*j_!\mathcal{F} = \mathcal{F}$, so that $H^i(U, j^*j_!\mathcal{F}) \cong H^i(U, \mathcal{F})$. We will abuse notation somewhat by denoting the group $H^i(X, j_!\mathcal{F})$ by $H^i_c(U, \mathcal{F})$. This is meant to remind us of cohomology with compact support (see [**24**], Ch. III, §1, bottom of page 93), except for the fact that $X$ is not really complete, because of the infinite places. We have a long exact sequence of cohomology with support (see [**24**], Chapter III, §1, pp. 91-92):

$$\cdots H^i_S(X, j_!\mathcal{F}) \to H^i(X, j_!\mathcal{F}) \to H^i(U, j^*j_!\mathcal{F}) \to H^{i+1}_S(X, j_!\mathcal{F}) \to H^{i+1}(X, j_!\mathcal{F}).$$

For a place $v$ of $K$, which we identify with a closed point of $X$, let $A^h_v$ denote the henselization of the local ring of $X$ at $v$ (one can also take the completion). Then using the identifications:

$$H^i_S(X, j_!\mathcal{F}) \cong \bigoplus_{v\in S} H^i_v(X, j_!\mathcal{F})$$

$$H^i_v(X, j_!\mathcal{F}) = H^i_v(A^h_v, j_!\mathcal{F})$$

$$H^i(K_v, \mathcal{F}) \cong H^{i+1}_v(A^h_v, j_!\mathcal{F})$$

for $v \in S$ (see [**25**], Proposition 1.1, page 182 for the last isomorphism, which uses the fact that we have a sheaf of the form $j_!\mathcal{F}$), we get the exact sequence

$$\cdots H^i_c(U, \mathcal{F}) \to H^i(U, \mathcal{F}) \to \bigoplus_{v\in S} H^i(K_v, \mathcal{F}) \to H^{i+1}_c(U, \mathcal{F}) \cdots .$$

The Poitou-Tate and Cassels-Tate exact sequences are then derived from this one sequence by taking $\mathcal{F} = \mu_\ell$ (resp. $\mathcal{F} = \mathcal{E}$) and using the Artin-Verdier duality

theorem (see e.g. [**25**], Chapter II, §3, Corollary 3.2) (resp. the duality theorem for abelian varieties (see [**25**], Chapter II, §5, Theorem 5.2)). For the latter case, we could use $\mathcal{E}[\ell]$, which we can view as a locally constant étale sheaf on $U$, just as we did for $\mu_\ell$ in the multiplicative group case. We have the exact sequence (note that $\mathcal{E}(U) = E(K)$):

$$0 \to E(K)/\ell E(K) \to H^1(U, \mathcal{E}[\ell]) \to H^1(U, \mathcal{E})[\ell] \to 0.$$

However, we are really interested in the group on the right, so we prefer to deal with it directly.

## 2. *Overview*

Our approach to the discrete log problem uses the Poitou-Tate exact sequence in the case of the multiplicative group and the Cassels-Tate exact sequence in the case of elliptic curves. In each case, the method will be to find a suitable element of $H^1(U, \mathcal{F})$ of order $\ell$ against which to "test" a lifting to $K$ of an element over the finite field whose discrete log we seek to compute and then use the reciprocity laws that are encoded in the exact sequences to create linear relations involving the discrete logs.

In the case of multiplicative groups we will focus on the following part of the Poitou-Tate exact sequence (notation being the same as in § 1.4):

$$H^1(G_S, \mu_\ell) \to \bigoplus_{v \in S} H^1(K_v, \mu_\ell) \to H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})^*.$$

We fix a basis $B_v$ of $K_v^*/K_v^{*\ell}$ for each $v \in S$, and define for every Dirichlet character $\chi \in H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ the *local signature* of $\chi$ at $v$, denoted $\sigma(\chi_v)$, to be the tuple that enumerates the values of local pairings $< \chi_v, \beta_{v,i} >$ where $\beta_{v,i} \in B_v$. We define the *signature* of $\chi$ to be the tuple that enumerates $\sigma(\chi_v)$, where $v \in S$. By virtue of local duality, $\chi_v$ is uniquely determined by the local signature of $\chi$ at $v$. Hence the signature of $\chi$ uniquely determines the image of $\chi$ under the map $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z}) \to \bigoplus_{v \in S} H^1(K_v, \mathbb{Z}/\ell\mathbb{Z})$.

Suppose that the class number of the number field $K$ is not divisible by $\ell$. Then

$$\mathcal{O}_S^*/\mathcal{O}_S^{*\ell} \cong H^1(G_S, \mu_\ell)$$

and $H^1(K_v, \mu_\ell) \cong K_v^*/K_v^{*\ell}$ (Kummer theory). Thus the Poitou-Tate sequence becomes:

$$\mathcal{O}_S^*/\mathcal{O}_S^{*\ell} \to \bigoplus_{v \in S} K_v^*/K_v^{*\ell} \to H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})^*.$$

The reciprocity law encoded in the sequence can be expressed explicitly as follows: for $\chi \in H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ and $\alpha \in \mathcal{O}_S^*$,

$$\sum_{v \in S} < \chi_v, \alpha_v > = 0.$$

The basic idea in our approach is to lift elements from $\mathbb{G}_m(\mathbb{F}_p) = \mathbb{F}_p^*$ to $\mathbb{G}_m(\mathcal{O}_S) = \mathcal{O}_S^*$, then use the Poitou-Tate sequence to construct suitable testing Dirichlet characters, and use the reciprocity law encoded in the sequence to relate signature computation and discrete-log computation.

In the case of elliptic curves we will use the Cassels-Tate sequence (**) in § 1.4, where $U$ is an open subset of $\mathrm{Spec}(\mathcal{O}_K)$ on which $E$ has good reduction and $\ell$ is invertible, and $\mathcal{E}$ is a smooth proper model of $E$ over $U$. We will make the assumption that the Shafarevich-Tate group is finite of order not divisible by $\ell$ (this is analogous to the condition in the multiplicative group case that $\ell$ does not divide the class number), and derive the following version of the Cassels-Tate sequence for our application (see § 5.2 ):

$$E(K)/\ell \to \prod_{v \in S} E(K_v)/\ell \to (H^1(U_S, \mathcal{E})[\ell])^* \to 0.$$

The reciprocity law encoded in the sequence can be expressed explicitly as follows: for $\chi \in H^1(U_S, \mathcal{E})[\ell]$ and $\alpha \in E(K)$,

$$\sum_{v \in S} <\chi_v, \alpha_v> = 0.$$

We fix a basis $B_v$ of $E(K_v)/\ell E(K_v)$ for each $v \in S$, and define for $\chi \in H^1(U_S, \mathcal{E})[\ell]$ the *local signature* of $\chi$ at $v$, denoted $\sigma(\chi_v)$, to be the tuple that enumerates the values of the local pairings $<\chi_v, \beta_{v,i}>$ where $\beta_{v,i} \in B_v$. Note again by local duality, $\chi_v$ is uniquely determined by the local signature of $\chi$ at $v$. We define the *signature* of $\chi$ as the tuple that enumerates $\sigma(\chi_v)$, where $v \in S$.

Suppose $\tilde{E}$ is an elliptic curve over a finite field with a point of order $\ell$, and $E$ is a lifting of $\tilde{E}$. The basic idea in our approach in this situation is similar to the multiplicative case: lift elements from $\mathcal{E}(\mathbb{F}_p) = \tilde{E}(\mathbb{F}_p)$ to $\mathcal{E}(U_S) = E(K)$, use the Cassels-Tate sequence to construct a suitable testing principal homogeneous space, and then use the reciprocity law encoded in the sequence to relate the signature computation and the discrete-log computation.

The approach outlined above will be developed in detail in the next few sections. In the next section we demonstrate how the classical index calculus method emerges in the context of this approach as the result of one particular choice of testing Dirichlet characters and method of lifting.

A natural lifting to consider is from the group of units of $\mathbb{F}_p$ to the group of units of a real quadratic field $K$. This situation is studied in detail in § 4. A brief summary is as follows. Suppose $p$ and $\ell$ both split in $K$, and suppose there is a Dirichlet character $\chi$ ramified exactly at a place $u$ over $\ell$ and a place $v$ over $p$. Then from the reciprocity law it will follow that

$$<\chi_u, \alpha_u> + <\chi_v, \alpha_v> = 0.$$

The image of $\alpha_u$ in $K_u^*/K_u^{*\ell}$ is easy to compute in terms of the 1-unit $1 + \ell$. The image of $\alpha_v$ in $K_v^*/K_v^{*\ell}$ in terms of $g$ is determined by the discrete-log of $\alpha$ mod $v$ based $g$. More explicitly if $\alpha_u$ is equivalent to $(1 + \ell)^a$ modulo $K_u^{*\ell}$ and $\alpha \equiv g^t$

(mod $v$). Then

$$0 = < \chi_u, \alpha_u > + < \chi_v, \alpha_v >= a < \chi_u, 1 + \ell > + t < \chi_v, g >.$$

This consideration leads to a heuristic equivalence result between the signature computation and the discrete-log computation.

An analogous situation for an elliptic curve $\tilde{E}$ over $\mathbb{F}_p$ is studied in § 5, where we consider a lifting of $\tilde{E}$ to an elliptic curve $E$ that is heuristically often of rank 1 over a quadratic field $K/\mathbb{Q}$. Suppose $p$ and $\ell$ both split in $K$, and suppose there is a principal homogeneous space $\chi$ ramified exactly at a place $u$ over $\ell$ and a place $v$ over $p$. For a lifted point $Q \in E(K)$, we have from the reciprocity law,

$$< \chi_u, Q_u > + < \chi_v, Q_v >= 0.$$

The image of $Q_u$ in $E(K_u)/\ell E(K_u)$ is easy to compute and the image of $Q_v$ in $E(K_v)/\ell E(K_v)$ is determined by the discrete logarithm. And once again we are led to a heuristic equivalence result between the signature computation and the discrete-log computation.

The basic idea of the classical index calculus is to find enough linear relations on a set of discrete logarithms so that they can be solved using linear algebra. We consider a similar method for signature computation which we call *signature calculus*. The idea is to find enough linear relations on local signatures so as to solve for them using linear algebra. The classical index calculus also exemplifies the "smoothness trick" - the idea of utilizing small primes to tackle a problem that involves a much larger prime. The signature computation problems in the equivalence results involve large primes, and the question arises as to whether there is a signature calculus method using the smoothness trick. This is addressed in the next section as well as in § 6.

## 3. *Classical Index Calculus from the Perspective of Arithmetic Duality*

We briefly review the classical index calculus method. Let $p$ be an odd prime. Given positive integers $g$ and $t$ such that $g \bmod p$ generates the group $\mathbb{F}_p^*$, we would like to compute $n$ such that $t \equiv g^n \pmod{p}$. We will fix $g$ and denote the discrete-log of $t$ with respect to $g$ by $\theta(t)$ (also called the *index* of $t$ base $g$). The core of the classical index calculus method for solving the discrete-log problem in $\mathbb{F}_p^*$ is to compute $\theta(q)$ for primes $q$ up to a chosen bound $B$.

Let $F$ be the set of primes up to some bound $B$. The strategy of the index calculus is to form sufficiently many linear relations between these indices $\theta(q)$, $q \in F$, so that they can be solved using linear algebra. To this end we generate random $r$ so that $g^r \bmod p$ is $B$-smooth, that is

$$g^r \bmod p = \prod_{q \in F} q^{e_q(r)}$$

with $e_q(r) \in \mathbb{Z}_{\geqslant 0}$. Note that this equation gives a multiplicative relation between a random power of the generator $g$ and elements in the factor base $F$. From the equation we get the linear relation:

$$r \equiv \sum_{q \in F} e_q(r)\theta(q) \pmod{p-1}.$$

With sufficiently many relations found, we can solve for the unknown $\theta(q)$. Once this is done, we pick random $s$ until $tg^s$ is congruent modulo $p$ to a $B$-smooth number:

$$tg^s = \prod_{q \in F} q^{v(q)}.$$

Then we have

$$\theta(t) = \sum_{q \in F} v(q)\theta(q) - s.$$

If $r$ is chosen uniformly randomly in $\{1, ..., p-1\}$, the probability that the integer $g^r \bmod p$ is $B$-smooth grows with $B$, but the number of linear equations, hence the time, needed to solve for the unknowns also grows with $B$. It turns out that when $B$ is set to be subexponential in $\log p$ of the form $e^{c\sqrt{\log p \log \log p}}$ for some constant $c > 0$, the probability that $g^r \bmod p$ is $B$-smooth is at least $B^{-c'}$ for some constant $c'$, and the number of unknowns and linear equations is $O(B)$. That is how we end up with a subexponential algorithm for solving the discrete-log problem.

Next we relate index calculus to signature calculus.

Let $\ell$ be an odd prime such that $p \equiv 1 \pmod{\ell}$. Let $K = \mathbb{Q}$, $X = \mathrm{Spec}(\mathbb{Z})$, and $U = X - S$, where $S$ is a finite set of primes containing $p$ and $\ell$. The extension $\mathbb{Q}(\mu_p)/\mathbb{Q}$ is cyclic of degree $p - 1$. Since $p \equiv 1 \pmod{\ell}$, there is a unique sub-extension $L/\mathbb{Q}$ of degree $\ell$. We fix an isomorphism $Gal(L/\mathbb{Q}) \cong \mathbb{Z}/\ell\mathbb{Z}$ and denote by $\chi$ the corresponding Dirichlet character, which is ramified only at $p$. Then $\chi$ can be regarded as an element of $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$. The extension $\mathbb{Q}(\mu_{\ell^2})/\mathbb{Q}$ is cyclic of degree $\ell(\ell - 1)$, and has a unique sub-extension $L'/\mathbb{Q}$ of degree $\ell$ ramified only at $\ell$. Hence there is similarly a Dirichlet character $\psi \in H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ ramified only at $\ell$ that corresponds to an isomorphism $Gal(L'/\mathbb{Q}) \cong \mathbb{Z}/\ell\mathbb{Z}$.

Now let $F$ be the set of primes up to some bound $B$ as before where $B < \ell$. Let $S = F \cup \{p, \ell\}$ and let $T = F \cup \{p\}$. We easily compute that the $\mathbb{F}_\ell$ dimension of $H^1(G_S, \mu_\ell)$ is $\#S = \#F + 2$ and the $\mathbb{F}_\ell$ dimension of $\bigoplus_{v \in S} H^1(\mathbb{Q}_v, \mathbb{Z}/\ell\mathbb{Z})$ is $\#F + 4$.

Let $\mathbb{Z}_S$ (resp. $\mathbb{Z}_F$) denote the ring of $S$-integers (resp. $F$-integers) in $\mathbb{Q}$. By the Poitou-Tate sequence and the fact that the class group of $\mathbb{Z}_S$ is trivial, we then get that $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ has $\mathbb{F}_\ell$ dimension two. Since $\chi \in H^1(G_T, \mathbb{Z}/\ell\mathbb{Z}) \subset H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$, and $\psi \in H^1(G_S, \mathbb{Z}/\ell\mathbb{Z}) - H^1(G_T, \mathbb{Z}/\ell\mathbb{Z})$, it follows that $H^1(G_T, \mathbb{Z}/\ell\mathbb{Z})$ has $\mathbb{F}_\ell$ dimension one and is generated by $\chi$.

We fix $p$ and $g$ as the basis of $\mathbb{Q}_p^* / \mathbb{Q}_p^{*\ell}$. For $q \in F$, $\mathbb{Q}_q^* / \mathbb{Q}_q^{*\ell}$ is of $\mathbb{F}_\ell$-dimension 1 generated by $q$, and by local duality the local signature $< \chi_q, q >$ uniquely determines $\chi_q$. Since $\sum_v < \chi_v, p_v >=< \chi_p, p >= 0$, the local signature at of

$\chi$ at $p$ is determined by $< \chi_p, g >$. As we will see below, the classical index calculus method amounts to determining in a computationally efficient manner $(< \chi_p, g >)^{-1} < \chi_q, q >$, $q \in F$. These are the local signatures of $\chi$ at $q \in F$ normalized by $(< \chi_p, g >)^{-1}$. Since $< \chi_p, g >$ determines the local signature of $\chi$ at $p$ and since $H^1(G_T, \mathbb{Z}/\ell\mathbb{Z})$ has $\mathbb{F}_\ell$ dimension one generated by $\chi$, these normalized local signatures determine the image of $H^1(G_T, \mathbb{Z}/\ell\mathbb{Z})$ in $\bigoplus_{v \in T} H^1(\mathbb{Q}_v, \mathbb{Z}/\ell\mathbb{Z})$.

Consider again the Poitou-Tate sequence in this situation. We have that $\mathbb{Z}_S^* / \mathbb{Z}_S^{*\ell} \cong H^1(G_S, \mu_\ell)$, and from $(*)_{\mathbb{Z}/\ell\mathbb{Z}}$ we have that for all $\alpha \in \mathbb{Z}_S^*$,

$$\sum_{v \in S} < \chi_v, \alpha_v >= 0 \in \mathbb{Z}/\ell\mathbb{Z},$$

and this yields a (homogeneous) linear equation of the local signatures if we have the image of an $\alpha \in \mathbb{Z}_S^*$ expressed in terms of the local basis of $\mathbb{Q}_v^* / \mathbb{Q}_v^{*\ell}$ for all $v \in S$. The only place where the local image may be hard to compute is $p$, for what we need there is none other than the discrete-log of $\alpha \bmod p$ based $g$. To avoid having to compute this, we may try to lift a random power $g^r \bmod$ to $\mathbb{Z}_S^*$, so that the discrete-log at $p$ is already predetermined. Note that the set of $B$-smooth integers is contained in $\mathbb{Z}_S^*$. Hence we pick random $r$ until $g^r \bmod$ is $B$-smooth. Then we have

$$\alpha_r = g^r \bmod p = \prod_{q \in F} q^{e_q(r)}$$

with $e_q(r) \in \mathbb{Z}_{\geqslant 0}$. Observe that the exponents $r$ and $e_q(r)$'s in the equation tells us what the image of $\alpha_r$ is in $\mathbb{Q}_v^* / \mathbb{Q}_v^{*\ell}$ for $v = p$ and $v \in F$. Since $\alpha_r \in \mathbb{Z}_S^*$, we have

$$0 = \sum_{v \in S} < \chi_v, (\alpha_r)_v >= r < \chi_p, g > + \sum_{q \in F} e_q(r) < \chi_q, q > .$$

With sufficiently many $\alpha_r$ that generate $\mathbb{Z}_F^* / \mathbb{Z}_F^{*\ell}$, we can solve for the unknown

$$(< \chi_p, g >)^{-1} < \chi_q, q > .$$

We observe that the normalized local signatures $(< \chi_p, g >)^{-1} < \chi_q, q >$ are closely related to $\theta(q) \bmod \ell$. Indeed for $q \in F$, since $q \in \mathbb{Z}_S^*$ and $q$ is a local unit at $v \neq q$ in $S$,

$$0 = \sum_{v \in S} < \chi_v, q >= < \chi_p, q > + < \chi_q, q >= \theta(q) < \chi_p, q > + < \chi_q, q > .$$

Hence,

$$\theta(q) \bmod \ell = -(< \chi_p, g >)^{-1} < \chi_q, q > .$$

Therefore, we have in essence derived the classical index calculus method as a signature calculus method. The reason why we normalize the signature is to make it independent of the particular $\chi$ we choose in the one-dimensional subspace, for if we multiply $\chi$ by $a \in (\mathbb{Z}/\ell\mathbb{Z})^*$, we don't change $(< \chi_p, g >)^{-1} < \chi_q, q >$.

This way of approaching the DLP helps to point out a crucial difference between the multiplicative group and elliptic curve cases. Namely, in the multiplicative group

case, when we take a bigger factor base $F$, we enlarge the rank of the group of units $\mathbb{Z}_F^*$. In the elliptic curve case, it does us no good to take points with values in $S$-integers, since these are the same as the integral points, because an elliptic curve is *proper*, whereas the multiplicative group is *affine*. Thus the only way to get the relations we need in this way is to find a lifted curve of high Mordell-Weil rank, which is not easy to do.

In the preceding discussion, we were able to explicitly construct a desired Dirichlet character of $\mathbb{Q}$ because we know enough about abelian extensions of $\mathbb{Q}$ to explicitly compute everything we need. In the discussion below, we will be working with real quadratic fields instead of $\mathbb{Q}$, and there we know much less about how to explicitly construct abelian extensions. However, using the exact sequence $(*)_{\mu_\ell}$ and making some assumptions which are heuristically satisfied, we will demonstrate the existence of a suitable Dirichlet character by explicitly computing the $\mathbb{F}_\ell$-dimensions of the first and second terms, and showing that the former is less than the latter. More generally, we use the following basic strategy to find a suitable testing element. In the multiplicative group case, look for an algebraic number field $K$ such that the $\mathbb{F}_\ell$-dimension of the first term of the middle row of $(*)_{\mu_\ell}$ is smaller than that of the second. This will then guarantee the existence of an element of order $\ell$ in $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})^*$. Lifting to units of a real quadratic field instead of to smooth integers in $\mathbb{Z}$ provides us with some technical advantages, and allows us to more easily compare and contrast the discrete log problems for the multiplicative group and for elliptic curves over finite fields.

In the elliptic curve case, we look for a quadratic extension $K/\mathbb{Q}$ in which both $p$ and $\ell$ split together with an elliptic curve $E/K$ that lifts $\tilde{E}$, such that $E(K)$ is of rank 1. We also assume that a generator of the torsion-free quotient of $E(K)$ is not divisible by $\ell$ in $E(K_u)$ for all $u \in T$, where $T$ consists of one place above $p$ and both above $\ell$. Thus we treat the multiplicative group and elliptic curve cases in close parallel.

## 4. *Signature Computation for the Multiplicative Group*

### 4.1. *Characters with Prescribed Ramification*

Throughout this section, let $p, \ell$ be rational primes with $p \equiv 1 \pmod{\ell}$ and $\ell > 2$. Let $K/\mathbb{Q}$ be a real quadratic extension where $p$ and $\ell$ split. Let $\Sigma$ be the set of all places over $\ell$ and $p$, together with all the archimedean places. For any place $u$ of $K$ let $P_u$ denote the prime ideal corresponding to $u$. For any finite set $S$ of places of $K$, let $G_S$ denote the Galois group of a maximal extension of $K$ that is unramified outside of $S$.

PROPOSITION 1. *Let $S$ be a subset of $\Sigma$ that contains both places over $\ell$ and both archimedean places, but no non-archimedian places that do not divide $\ell$ and $p$. Suppose*

1. *$\ell \nmid h_K$ where $h_K$ is the class number of $K$;*
2. *$K$ has a unit $\alpha$ that satisfies $\alpha^{l-1} \not\equiv 1 \pmod{P_w^2}$ for some $w \in S$ over $\ell$ (that is, locally $\alpha$ is not an $\ell$-th power at some place over $\ell$).*

*Then the $\mathbb{F}_\ell$-dimension of $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ equals $n(S) - 1$ where $n(S)$ is the number of finite places in $S$.*

**Proof**: First, note that if $w$ is a place of $K$ dividing $\ell$, then $\alpha^{\ell-1} \equiv 1 \pmod{P_w}$. If $U^{(r)}$ denotes the group of units that are congruent to 1 modulo $P_w^r$, then we have an isomorphism $U^{(1)}/U^{(2)} \cong U^{(1)}/U^{(1)\,\ell}$. Thus, for a prime $w$ dividing $\ell$, it is equivalent to say that $\alpha^{l-1} \not\equiv 1 \pmod{P_w^2}$ and that $\alpha$ is not an $\ell$-th power in $K_w$. Consider the sequence:

$$(*)_{\mu_\ell} : H^1(G_S, \mu_\ell) \xrightarrow{f} \bigoplus_{v \in S} H^1(K_v, \mu_\ell) \xrightarrow{\rho} H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})^* \to$$
$$H^2(G_S, \mu_\ell) \xrightarrow{g} \bigoplus_{v \in S} H^2(K_v, \mu_\ell) \to \cdots .$$

We claim that under the hypotheses of the proposition, $\rho$ is surjective. To see this, the hypothesis that $\ell$ does not divide the class number of $K$ implies that it does not divide the class number of $\mathcal{O}_S$. By Kummer theory, we then have that:

$$H^2(G_S, \mu_\ell) \cong Br(\mathcal{O}_S)[\ell].$$

But then the map $g$ is injective, so $\rho$ is surjective. Now consider the map

$$f : H^1(G_S, \mu_\ell) \xrightarrow{f} \bigoplus_{v \in S} H^1(K_v, \mu_\ell).$$

Again using the hypothesis that $\ell$ does not divide the class number of $K$, we have that:

$$\mathcal{O}_S^*/\mathcal{O}_S^{*\ell} \cong H^1(G_S, \mu_\ell).$$

Consider the exact sequence:

$$0 \to \mathcal{O}^* \to \mathcal{O}_S^* \to \mathbb{Z}S \to Cl(\mathcal{O}) \to Cl(\mathcal{O}_S) \to 0.$$

Going modulo $\ell$ and using the hypotheses of the theorem, we see that the sequence:

$$0 \to \mathcal{O}^*/\mathcal{O}^{*\ell} \to \mathcal{O}_S^*/\mathcal{O}_S^{*\ell} \to \mathbb{Z}S/\ell\mathbb{Z}S \to 0$$

is exact. This shows that the $\mathbb{F}_\ell$-dimension of the group in the middle is $n(S)+1$. The hypotheses about the units show that $f$ is injective. The target has dimension $2n(S)$ because $H^1(K_v, \mu_\ell)$ is isomorphic to $\mathbb{Q}_v^*/\mathbb{Q}_v^{*\ell}$. If $v \mid p$, then this group is of dimension 2 over $\mathbb{F}_\ell$ because $\ell \mid p - 1$. If $v \mid \ell$, then this group is also of dimension 2, spanned by a prime element of $\mathbb{Q}_\ell$ and by a 1-unit. Thus the cokernel of $f$ is of dimension $n(S) - 1$. This completes the proof of the proposition.

PROPOSITION 2. *Let $S$ be the set consisting of one place $u$ over $\ell$, one place $v$ over $p$, and both archimedean places. Suppose*

*1. $\ell \nmid h_K$ where $h_K$ is the class number of $K$;*

2. *$K$ has a unit $\alpha$ that satisfies $\alpha^{l-1} \not\equiv 1 \pmod{P_w^2}$ for all places $w \mid \ell$ and $\alpha^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{P_v}$ (that is, locally $\alpha$ is not an $\ell$-th power at $v$ and the two places over $\ell$).*

*Then the $\mathbb{F}_\ell$-dimension of $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ is one. If $\chi$ is any nonzero element of this group, then $\chi$ is ramified at $u$ and $v$.*

**Proof** Suppose $u, u'$ are the places over $\ell$. Let $R$ be the set consisting of $u, u'$ and both archimedean places. Let $T$ be the set consisting of $u, u', v$ and both archimedean places. Then from Proposition 1 it follows that $H^1(G_R, \mathbb{Z}/\ell\mathbb{Z})$ has dimension one and $H^1(G_T, \mathbb{Z}/\ell\mathbb{Z})$ has dimension two. Hence there exists a nontrivial $\psi \in H^1(G_R, \mathbb{Z}/\ell\mathbb{Z})$, and some $\chi \in H^1(G_T, \mathbb{Z}/\ell\mathbb{Z}) - H^1(G_R, \mathbb{Z}/\ell\mathbb{Z})$. By construction $\chi$ is ramified at $v$, and by the condition on $\alpha$ at $v$ we get $< \chi_v, \alpha_v > \neq 0$. As for $\psi$, by the reciprocity law we have $< \psi_u, \alpha_u > + < \psi_{u'}, \alpha_{u'} > = 0$, so either $< \psi_u, \alpha_u >$ and $< \psi_{u'}, \alpha_{u'} >$ are both zero or both non-zero. But if both are zero then by the condition on $\alpha$ at $u$ and $u'$ it would follow that $\psi$ is unramified at both places, violating the condition that $\ell$ does not divide the class number of $K$. Hence $< \psi_u, \alpha_u >$ and $< \psi_{u'}, \alpha_{u'} >$ are both non-zero. Since $< \psi_{u'}, \alpha_{u'} > \neq 0$, there exists $c \in \mathbb{Z}/\ell\mathbb{Z}$ such that $< \chi_{u'}, \alpha_{u'} > = c < \psi_{u'}, \alpha_{u'} >$, and letting $\phi = \chi - c\psi$, we have $< \phi_{u'}, \alpha_{u'} > = 0$. Now $\phi \in H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ since $< \phi_{u'}, \alpha_{u'} > = 0$, and $\phi$ is nontrivial since $< \phi_v, \alpha_v > = < \chi_v, \alpha_v > \neq 0$. Hence $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ is of dimension at least one. Since $\psi$ is ramified at $u'$, it follows that $\psi \notin H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$, and since $\psi \in H^1(G_R, \mathbb{Z}/\ell\mathbb{Z}) \subset H^1(G_T, \mathbb{Z}/\ell\mathbb{Z})$, it follows that $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ is a proper subset of $H^1(G_T, \mathbb{Z}/\ell\mathbb{Z})$, hence it can be of dimension at most one. We conclude that its dimension must be one, and the proposition follows.

We will refer to the conclusion of the last proposition as "backtracking," since it allows us in some cases to go from a set of places that includes all places above $\ell$ to one that does not.

*Remarks*
(i) We explain why we made the assumptions of Proposition 2, their necessity and sufficiency for the conclusion, and how they affect the signature computations later in the paper:

Condition (1) is made to ensure that the Dirichlet characters of degree $\ell$ that we get will not be everywhere unramified, as such characters would be of no use to us for the signature computation. Cohen-Lenstra heuristics predict that the probability that $\ell$ will not divide the class number of a given real quadratic field is about $1 - \frac{1}{\ell}$ (see [**5**, **6**]).

Conditions (2) and (3) are meant to ensure that there do not exist characters of $K$ of degree $\ell$ that are ramified only at $u$ or only at $v$. Such characters would not help our signature computation. For example, suppose the character $\chi$ is ramified at $v$ and unramified everywhere else. Then if we pair $\chi$ with a global unit $a$ of our real quadratic field, we would get that $< \chi_u, a_u > = 0$ since $\chi$ is unramified at $u$ and $a$ is a unit. The reciprocity law would then give us that $< \chi_v, a_v > = - < \chi_u, a_u > = 0$, and this would not help us in the signature computation. If *neither* condition (2)

nor (3) holds, then there are Dirichlet characters $\chi'$ and $\chi''$, one ramified only at $u$ and the other ramified only at $v$. Thus, while the character $\chi = \chi' + \chi''$ is ramified at both $u$ and $v$, this would not help for our signature computation, since for a global unit $a$, we would have:

$$< \chi_u, a_u > = < \chi'_u, a_u > + < \chi''_u, a_u > = 0,$$

since $\chi'$ is ramified only at $u$ and $\chi''$ is unramified at $u$. Similarly for $v$.

(ii) One can give an alternative (and perhaps simpler) proof of Proposition 2 using the ideal theoretic formulation of class field theory. Briefly, using the hypotheses of the proposition, one easily calculates the $\ell$-rank of the Galois group of the ray class field modulo $I = \mathfrak{p}\mathfrak{l}^2$, where $\mathfrak{p}$ is an ideal of $K$ lying over $p$ and $\mathfrak{l}$ is an ideal lying over $\ell$. This is the maximal abelian extension of $K$ with conductor bounded by $I$, and its Galois group is isomorphic to a generalized class group by class field theory. Using basic exact sequences and the hypotheses of the proposition, we can explicitly calculate this class group. The reason why we did not write the proof this way is that we want to stress the analogy with elliptic curves, where the Poitou-Tate exact sequence has an analogue (the Cassels-Tate exact sequence), but the analogue of the ideal theoretic formulation of class field theory is less developed.

Assuming the conditions in Proposition 2, then $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$. Every nontrivial character in it is ramified at $u$ and $v$ and unramified at all other finite places; moreover, $< \chi_u, \alpha_u > \neq 0$ and $< \chi_v, \alpha_v > \neq 0$, and $< \chi_u, \alpha_u > + < \chi_v, \alpha_v > = 0$. This group of characters corresponds to a unique cyclic extension $K_S$ of degree $\ell$ over $K$ which is ramified at $u$ and $v$ and unramified at all other finite places.

At $u$, we take the class of $1 + \ell$ as a generator of the group $\mathcal{O}^*_{K_u}/\mathcal{O}^{*\ell}_{K_u} \cong \mathbb{Z}^*_\ell/\mathbb{Z}^{*\ell}_\ell \cong \mathbb{Z}/\ell\mathbb{Z}$. It is easy to see that this element does generate because it is not congruent to 1 modulo any higher power of $\ell$ and it is very simple to calculate with. For $0 \neq \chi \in H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$, let $\sigma_u(\chi) = < \chi_u, 1 + \ell_u >$. Let $g \in \mathbb{Z}$ so that $g \bmod p$ generates the multiplicative group of $\mathbb{F}_p$. Then the class of $g$ generates $\mathcal{O}^*_{K_v}/\mathcal{O}^{*\ell}_{K_v} \cong \mathbb{Z}^*_p/\mathbb{Z}^{*\ell}_p \cong \mathbb{Z}/\ell\mathbb{Z}$. For $\chi \in H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$, let $\sigma_v(\chi) = < \chi_v, g_v > \neq 0$. If we take $\chi'$ satisfying the conditions we have put, then $\chi' = a\chi$ for some $a \in (\mathbb{Z}/\ell\mathbb{Z})^*$, and hence we don't change $\sigma_u(\chi)\sigma_v(\chi)^{-1} \in \mathbb{Z}/\ell\mathbb{Z}$. This last quantity only depends on $K_S$ and we call it the *ramification signature* of $K_S$ with respect to $1 + \ell$ and $g$; it is nonzero.

## 4.2. *DL and Signature Computation*

In this section we argue that the discrete logarithm problem in the multiplicative case is random polynomial time equivalent to computing the signature of cyclic extensions with prescribed ramification as described in Proposition 2.

**DL Problem**: Suppose we are given $p$, $\ell$, $\tilde{g}$ and $a$, where $p$ and $\ell$ are prime with $p \equiv 1 \pmod{\ell}$, $\tilde{g}$ is a generator for the group $\mathbb{F}^*_p[\ell]$ of elements killed by $\ell$, and $a \in \mathbb{F}^*_p[\ell]$. Then compute $m \bmod \ell$ such that $a = \tilde{g}^m$ in $\mathbb{F}_p$.

**Signature Computation Problem**: Suppose we are given $K$, $p$, $\ell$, $u$, $u'$, $v$, $\alpha$ and $g$, where $K = \mathbb{Q}(\sqrt{D})$ is a real quadratic field, $\ell$, $p$ are primes that split in $K$, $u$ and $u'$ are the two places of $K$ over $\ell$, $v$ is a place of $K$ over $p$, $\alpha$ is a unit of $K$, and $g$ is a positive integer less than $p$ where $g \bmod p$ is a generator for $\mathbb{F}_p^*$, such that: (1) the class number of $K$ is not divisible by $\ell$, (2) $\alpha^{l-1} \not\equiv 1 \pmod{P_u^2}$, $\alpha^{l-1} \not\equiv 1 \pmod{P_{u'}^2}$, and (3) $\alpha^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{P_v}$. Then compute the ramification signature, with respect to $1 + \ell$ and $g$, of the cyclic extension of degree $\ell$ over $K$ which is ramified at $u, v$ and unramified elsewhere.

In the following we argue that the problems DL and Signature Computation are random polynomial time equivalent. We first give a random polynomial time reduction from DL to Signature Computation. This part of the argument depends on some heuristic assumptions that will be made clear below. We then give a random polynomial time reduction from Signature Computation to DL. This part of the argument does not depend on any heuristic assumption.

Let $a = \tilde{g}^m$ in $\mathbb{F}_p$ where $m$ is to be computed. If $a^{\frac{p-1}{\ell}} = 1$, then $m \equiv 0 \pmod{\ell}$. So suppose $a^{\frac{p-1}{\ell}} \neq 1$. We lift $a$ to some unit $\alpha$ of a real quadratic field $K$ such that $\alpha \equiv a \pmod{v}$ for some place $v$ of $K$ over $p$. This can be done as follows.

1. Compute $b \in \mathbb{F}_p$ such that $ab = 1$ in $\mathbb{F}_p$.
2. $c \leftarrow 2^{-1}(a + b)$; $d \leftarrow 2^{-1}(a - b)$. Note that $c^2 - d^2 = 1$, and $a = c + d$. We may assume $d \neq 0$ otherwise $a^2 = 1$ and $m = (p-1)/2$ or $p - 1$.
3. Lift $d$ to an integer. Let $\gamma \in \bar{\mathbb{Q}}$ be such that $\gamma^2 = 1 + d^2$.
4. Check if $1 + d^2$ is a quadratic residue modulo $\ell$. Otherwise substitute $d + rp$ for $d$ for random $r$ until the condition is met. This is to make sure that $\ell$ splits in $K$.
5. $\gamma^2 = 1 + d^2 \equiv c^2 \pmod{p}$ implies $\gamma \equiv c \pmod{v}$, and $\gamma \equiv -c \pmod{v'}$ where $v$ and $v'$ are the two places of $K$ over $p$.
6. Let $\alpha = \gamma + d$. Then $\alpha \equiv c + d \equiv a \pmod{v}$. Note that the norm of $\alpha$ is $d^2 - \gamma^2 = -1$, so $\alpha$ is a unit of $K$.

We make the heuristic assumption that it is likely for $K$ to satisfy the conditions in Proposition 2. (Note that condition (3) is satisfied since $\alpha \equiv a \pmod{v}$ and $a^{\frac{p-1}{\ell}} \neq 1$.) We argue below that computing the discrete logarithm $m$ where $a = \tilde{g}^m$ is reduced to solving the Signature Computation problem on input $K$, $p$, $\ell$, $u$, $v$, $\alpha$ and $g$, where $K = \mathbb{Q}(\gamma)$ with $\gamma^2 = 1 + d^2$, $\alpha = \gamma + d$, $u$ and $v$ are as constructed above, and $g$ is the positive integer less than $p$ such that $g \bmod p$ maps to $\tilde{g}$ under the natural isomorphism between $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{F}_p$. A simple analysis shows that the expected time complexity in constructing these objects is $O(\log^3 p)$.

For $\chi \in H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ that is ramified at $u$ and $v$, and unramified elsewhere, we have

$$0 = <\chi_u, \alpha_u> + <\chi_v, \alpha_v>.$$

Moreover since $\alpha^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{v}$, $\alpha$ generates $\mathcal{O}_{K_v}^* / \mathcal{O}_{K_v}^{*\ell}$, so $<\chi_v, \alpha_v> \neq 0$, and it follows that $<\chi_u, \alpha_u> \neq 0$.

In general, for a field $k$ and $a, b \in k^*$, we write $a \sim^l b$ if $a/b \in k^{*\ell}$.

We have $\alpha \sim^l g^m$ in $K_v$ since $\alpha \equiv a \equiv g^m \pmod{v}$. Hence

$$< \chi_v, \alpha_v > = < \chi_v, g_v^m > = m < \chi_v, g_v > .$$

Write $\alpha = \xi(1 + y\ell) \pmod{\ell^2}$ with $\xi^{\ell-1} = 1$ after identifying $\alpha$ with its isomorphic image in $\mathbb{Q}_\ell$. Since $1 + \ell\mathbb{Z}_\ell/1 + \ell^2\mathbb{Z}_\ell \cong \mathbb{Z}_\ell^*/\mathbb{Z}_\ell^{*\ell}$, we have $\alpha \sim^\ell (1 + \ell)^y$, and

$$0 = < \chi_u, \alpha_u > = < \chi_u, (1 + \ell)_u^y > = y < \chi_u, 1 + \ell_u > .$$

Hence we have

$$< \chi_u, \alpha_u > + < \chi_v, \alpha_v > = y < \chi_u, 1 + \ell_u > + m < \chi_v, g_v > .$$

So $y\sigma_u(\chi) + m\sigma_v(\chi) = 0$. From this we see that if the ramification signature $\sigma_u(\chi)(\sigma_v(\chi))^{-1}$ is determined then $m$ is determined. The expected time in this reduction is $O(\log^3 p)$.

Next we give a polynomial time reduction from Signature Computation on input $K, p, \ell, u, v, \alpha$ and $g$, to DL on input $p, \ell, g \bmod p$ and $a$ where $\alpha \equiv a \pmod{v}$.

Call the oracle to DL on input $p$, $\ell$, $g \bmod p$ and $a$ to compute $m$ such that $g^m = a \pmod{p}$. Then $\alpha \equiv g^m \pmod{v}$.

Write $\alpha = \xi(1 + y\ell) \pmod{\ell^2}$ with $\xi^{\ell-1} = 1$ after identifying $\alpha$ with its isomorphic image in $\mathbb{Q}_\ell$. Then $\alpha \sim^\ell (1 + \ell)^y$. Again, $\xi \bmod \ell^2$ and hence $y$ can be computed efficiently in time $O(||\alpha|| \log \ell + \log^3 \ell) = O(||\alpha|| \log p + \log^3 p)$, where $||\alpha||$ is the bit length of $\alpha$.

For $\chi \in H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ that is ramified at $u$ and $v$, and unramified elsewhere, we have as before $< \chi_v, \alpha_v > = < \chi_v, g_v^m > = m < \chi_v, g_v >$, and $< \chi_u, \alpha_u > = < \chi_u, (1 + \ell)_u^y > = y < \chi_u, 1 + \ell_u > .$ Hence

$$0 = < \chi_u, \alpha_u > + < \chi_v, \alpha_v > = y < \chi_u, 1 + \ell_u > + m < \chi_v, g_v >$$

from this we can determine the ramification signature $\sigma_u(\chi)(\sigma_v(\chi))^{-1}$. The running time in this reduction is $O(||\alpha|| \log p + \log^3 p)$.

## 5. *Signature Calculus for ECDL*

### 5.1. *Preliminaries*

In this section we will demonstrate the existence of principal homogeneous spaces of order $\ell$ under elliptic curves over number fields with prescribed ramification. We begin by describing $H^1(K_v, E)[\ell]$ in general terms when $E$ has good reduction at $v$.

LEMMA 1. *Let $K_v$ be a local field with finite residue field $k$. Let $E$ be an elliptic curve defined over $K_v$ with good reduction.*

1. *Suppose the characteristic of $k$ is $\ell$. Then $H^1(K_v, E)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$ if $K_v \cong \mathbb{Q}_\ell$ and $\ell \nmid \#\tilde{E}(k)$.*
2. *Suppose the characteristic of $k$ is not $\ell$. Then*
   - *(a) $H^1(K_v, E)[\ell] = 0$ if $\ell \nmid \#\tilde{E}(k)$;*
   - *(b) $H^1(K_v, E)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$ if $\ell \mid \#\tilde{E}(k)$ but $\ell^2 \nmid \#\tilde{E}(k)$.*

**Proof**

Let $E_1(K_v)$ be the kernel of the reduction map from $E(K_v)$ to $\tilde{E}(k)$. From the commutative diagram

$$
\begin{array}{ccccccccc}
0 & \to & E_1(K_v) & \to & E(K_v) & \to & \tilde{E}(k) & \to & 0 \\
& & \downarrow \ell & & \downarrow \ell & & \downarrow \ell & & \\
0 & \to & E_1(K_v) & \to & E(K_v) & \to & \tilde{E}(k) & \to & 0
\end{array}
$$

and the snake lemma, we get the exact sequence

$$
0 \to E_1(K_v)[\ell] \to E(K_v)[\ell] \to \tilde{E}(k)[\ell] \to E_1(K_v)/\ell E_1(K_v)
$$
$$
\to E(K_v)/\ell E(K_v) \to \tilde{E}(k)/\ell\tilde{E}(k) \to 0.
$$

If $\ell$ does not divide the order of $\tilde{E}(k)$, then $\tilde{E}(k)[\ell]$ and $\tilde{E}(k)/\ell\tilde{E}(k)$ are both 0. Hence $E(K_v)/\ell E(K_v) \cong E_1(K_v)/\ell E_1(K_v)$.

To prove (1) suppose the characteristic of $k$ is $\ell$. If $K_v \cong \mathbb{Q}_\ell$, then $E_1(K_v)/\ell E_1(K_v) \cong \mathbb{Z}/\ell\mathbb{Z}$. If moreover $|\tilde{E}(k)|$ is not divisible by $\ell$, then $E(K_v)/\ell E(K_v) \cong E_1(K_v)/\ell E_1(K_v) \cong \mathbb{Z}/\ell\mathbb{Z}$, hence $H^1(K_v, E)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$ by local duality.

To prove (2), suppose the characteristic of $k$ is not $\ell$. Then $E_1(K_v)/\ell E_1(K_v) = 0$, and it follows from the long exact sequence that $E(K_v)/\ell E(K_v) \cong \tilde{E}(k)/\ell\tilde{E}(k)$. If $\ell$ does not divide the order of $\tilde{E}(k)$, then $E(K_v)/\ell E(K_v) \cong \tilde{E}(k)/\ell\tilde{E}(k) = 0$, and by local duality, $H^1(K_v, E)[\ell] = 0$. This proves 2(a). If $|\tilde{E}(k)|$ is divisible by $\ell$ but not $\ell^2$, then $\tilde{E}(k)/\ell\tilde{E}(k) \cong \mathbb{Z}/\ell\mathbb{Z}$. Hence $E(K_v)/\ell E(K_v) \cong \tilde{E}(k)/\ell\tilde{E}(k) \cong \mathbb{Z}/\ell\mathbb{Z}$, and by local duality, $H^1(K_v, E)[\ell] = \mathbb{Z}/\ell\mathbb{Z}$. Thus 2(b) is proved.

### 5.1.1.  Ranks of Quadratic Twists of Elliptic Curves over $\mathbb{Q}$

Let $E$ be an elliptic curve over $\mathbb{Q}$ and fix a Weierstrass equation for $E$:

$$
y^2 = x^3 + ax + b.
$$

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic extension of $\mathbb{Q}$ and let $E_d$ be the quadratic twist of $E$ given by the equation

$$
dy^2 = x^3 + ax + b.
$$

Let $G$ be the Galois group of $K$ over $\mathbb{Q}$ and $\sigma$ a generator of $G$. Denote by $V$ the group $E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$, by $V^+$ the fixed space by $\sigma$, and by $V^-$ the subspace of $V$ where $\sigma$ acts by $-1$. Now

$$V = V^+ \oplus V^-,$$

$V^+ = E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$, and we see easily that $V^- = E_d(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$, via the isomorphism sending a point $(x, y)$ in $E_d(\mathbb{Q})$ to $(x, \sqrt{d}y)$ in $V^-$.

In the algorithm in § 5.3 below, it will help to have a lifting $E/\mathbb{Q}$ of our original elliptic curve $\tilde{E}/\mathbb{F}_p$ such that $E(\mathbb{Q})$ has rank one and $E_d(\mathbb{Q})$ has rank zero. Standard conjectures about the behavior of the rank of the Mordell-Weil group of an elliptic curve predict that it should be quite possible to find such a situation. For example, a conjecture of Goldfeld [12] says that the rank of a quadratic twist $E_d$ of an elliptic curve $E$ over $\mathbb{Q}$ should be on average as small as the sign of the functional equation of its $L$-function would allow, i.e. either 0 or 1, depending on whether this sign is $+1$ or -1. In fact, assuming the Riemann hypothesis for all of the curves $E_d$, Heath-Brown [14] has proved that at least $1/4$ of all the $E_d$ with the sign in the functional equation of the L-function being $+1$ will have rank 0 and at least $3/4$ of all the $E_d$ with the sign being -1 will have rank 1 (see [14], Theorem 4). In the algorithm, we will first lift $\tilde{E}/\mathbb{F}_p$ to $E/\mathbb{Q}$ that has rank at least one by construction, and we will make the heuristic assumption that $E(\mathbb{Q})$ is of rank exactly one and therefore the sign of the functional equation is -1 (see [1], §3 for why this is considered to be reasonable). Using ([27], Theorem 7.2), Heath-Brown's result just mentioned, and taking sufficiently many random $d$, we can heuristically arrange for the sign of the functional equation of $E_d$ to be equal to $+1$ and for $E_d(\mathbb{Q})$ to have rank 0. When we make the heuristic assumption in § 5.3 below that the rank of $E(K)$ is exactly one, we shall mean this.

5.1.2. The Group $E(K_v)/\ell$ at Bad Reduction Primes $v$ of $E$

Let $\tilde{E}$ be an elliptic curve over $\mathbb{F}_p$, $p \geqslant 5$, given in Weierstrass form by an affine equation

$$y^2 = x^3 + \tilde{a}x + \tilde{b}.$$

In the algorithm below, we will want to lift $\tilde{E}$ to an elliptic curve $E$ over $\mathbb{Q}$ with Weierstrass equation

$$y^2 = x^3 + ax + b,$$

having good reduction at $\ell$ and such that at any prime $v$ of bad reduction, $E(K_v)/\ell = 0$. We give a heuristic here about why this should be possible. In our lifting in the algorithm presented in § 5.3, $|a|$ is at most $p^2$ and $|b|$ is at most $p^4$, so the discriminant $\Delta$ of a minimal Weierstrass equation for $E$ is of order at most $p^8$. At a prime $v$ of split multiplicative reduction prime, the group of connected components of the Néron model of $E$ over the ring of integers of $\mathbb{Q}_v$ will be of order the power of $v$ in the discriminant. Since $\ell$ is of the same order as $p$, this power is very unlikely to be divisible by $\ell$. At other primes of bad reduction, the group of connected components is of order at most 4 (see [36], Ch. VII, Theorem 6.1). Thus the order of the group of components is very unlikely to be divisible by $\ell$. This implies that it is very likely

that for small primes $v$ of bad reduction for $E$, $E(K_v)/\ell = 0$. To see this, recall (see e.g. [**36**], Theorem 15.1 of Appendix C) that $E(K_v)$ has a filtration:

$$E(K_v) \supseteq E_0(K_v) \supseteq E_1(K_v),$$

where $E_0(K_v)$ is the group of points specializing to points of the smooth locus $\tilde{E}'^0$ of the special fibre $\tilde{E}'$ of the minimal regular proper model $\mathcal{E}$ of $E$ over the ring of integers $R$ of $K_v$ and $E_1(K_v)$ is the kernel of the reduction map

$$E_0(K_v) \to \tilde{E}'^0(\mathbb{F}).$$

Now $E(K_v)/E_0(K_v)$ is the group of connected components of the special fibre of the Néron model of $E$ over $R$, and $E_1(K)$ is a pro-$v$-group, where $v$ is the residue characteristic of $K_v$. $E_0(K_v)/E_1(K_v)$ is the group of points on the connected component of identity of the special fibre of the Néron model. This last group is isomorphic to either the additive group or the multiplicative group of the residue field, $\mathbb{F}_v$. Thus, unless $v$ is large (at least the size of $\ell$), the order of this group will not be divisible by $\ell$. We cannot have $v = \ell$, since $E$ is assumed to have good reduction at $\ell$. If $v$ is larger than $\ell$, it is possible but still unlikely that $\ell$ will divide $v - 1$. In summary, it is very likely that $E(K_v)/\ell = 0$ for small primes (less than $\ell$) $v$ of bad reduction and this is likely to hold even if $v$ is not small. We shall use this heuristic in the algorithm in § 5.3 below.

5.2.  *Principal Homogeneous Spaces Ramified over $p$ and $\ell$*

    Throughout this section, let $p, \ell$ be odd, rational primes. Let $K/\mathbb{Q}$ be a quadratic extension, $X = \mathrm{Spec}(\mathcal{O}_K)$ and $\Sigma$ be the set of all places at which $E$ has bad reduction. Since we shall be dealing with the group of points on an elliptic curve modulo $\ell$, where $\ell$ is an odd prime, we shall ignore the archimedean places. Let $\mathcal{E}$ be a smooth proper model of $E$ over the open subset $U = X - \Sigma$. If $S$ is any set of places of $K$ containing $\Sigma$, denote by $U_S$ the open set $X - S$. We denote by $\mathrm{III}(E)$ the Shafarevich-Tate group of everywhere locally trivial principal homogeneous spaces under $E$ over $K$.

PROPOSITION 3. *Let $S$ be a finite set of places of $K$ containing all bad reduction places of $E$ and the places above $\ell$. Then if $\mathrm{III}(E)\{\ell\} = 0$, we have the exact sequence:*

$$E(K)/\ell \to \prod_{v \in S} E(K_v)/\ell \to (H^1(U_S, \mathcal{E})[\ell])^* \to 0.$$

Proof: Consider the Cassels-Tate exact sequence

$$(**) \; E(K)^{(\ell)} \to \prod_{v \in S} E(K_v)^{(\ell)} \to H^1(U_S, \mathcal{E})\{\ell\}^* \to \mathrm{III}(E)\{\ell\} \to 0.$$

LEMMA 2. *Let $B$ be a torsion abelian group such that $B[\ell^n]$ and $B/\ell^n B$ are finite groups. Then we have*

$$B[\ell]^* \cong B^*/\ell B^*$$

*and*

$$B\{\ell\}^* \cong B^{*(\ell)}$$

Proof: Let $n$ be a positive integer and consider the tautological exact sequence:

$$0 \to B[\ell^n] \to B \xrightarrow{\ell^n} B \to B/\ell^n B \to 0.$$

Since the functor * (see §1 for notation) is exact on the category of locally compact abelian groups, we get the exact sequence:

$$0 \to (B/\ell^n B)^* \to B^* \xrightarrow{\ell^n} B^* \to B[\ell^n]^* \to 0.$$

We then get the first conclusion of the lemma by taking $n = 1$ and the second by passing to the inverse limit over $n$ and noting that

$$\varprojlim_n \operatorname{Hom}(B[\ell^n], \mathbb{Q}/\mathbb{Z}) \cong \operatorname{Hom}(\varinjlim_n B[\ell^n], \mathbb{Q}/\mathbb{Z}).$$

This completes the proof of the lemma.

The proposition then follows from the lemma, the assumption that $\text{Ш}(E)\{\ell\} = 0$, and the Cassels-Tate sequence above by reducing the terms mod $\ell$.

For the remainder of this section we assume that $p$ and $\ell$ split in $K$, and that $E$ has good reduction at $p$ and $\ell$, with $\#\tilde{E}(\mathbb{F}_p) = \ell$ and $\ell \neq \#\tilde{E}(\mathbb{F}_\ell)$. By Lemma 1 and Tate local duality, $E(K_w)/\ell$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ for all $w$ dividing either $p$ or $\ell$. Moreover, because we assume that $\ell$ is sufficiently large, a theorem of Kamienny [**18**] ensures that $E(L)[\ell]$ is trivial for all quadratic extensions $L$ over $\mathbb{Q}$. Finally, we assume that $E(K_v)/\ell = 0$ for all bad reduction places $v$ of $E$ (see § 5.1.2 for why this is reasonable, heuristically).

PROPOSITION 4. *Let $S$ be a finite set of places of $K$ containing all bad reduction places of $E$ and the two places $u$ and $u'$ above $\ell$. $S$ may or may not contain places above $p$, but assume that it contains no good reduction places that do not divide $\ell$ or $p$. Suppose*

1. *$\text{Ш}(E)\{\ell\} = 0$;*

2. *the image of the map $E(K)/\ell \to \prod_{v \in S} E(K_v)/\ell E(K_v)$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$. Then the $\mathbb{F}_\ell$-dimension of $H^1(U_S, \mathcal{E})[\ell]$ equals $n(S) - 1$ where $n(S)$ is the number of finite places in $S - \Sigma$.*

Proof: Since $\text{Ш}(E)\{\ell\} = 0$, we have the exact sequence

$$E(K)/\ell \to \prod_{v \in S} E(K_v)/\ell \to (H^1(U_S, \mathcal{E})[\ell])^* \to 0$$

by Proposition 3. The middle group in the sequence $\prod_{v \in S} E(K_v)/\ell$ is isomorphic to the direct sum of $n(S)$ copies of $\mathbb{Z}/\ell\mathbb{Z}$ by Lemma 1. Since the image of the map

$$E(K)/\ell \to \prod_{v \in S} E(K_v)/\ell$$

is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$, it follows that the $\mathbb{F}_\ell$-dimension of $H^1(U_S, \mathcal{E})[\ell]$ equals $n(S) - 1$.

**PROPOSITION 5.** *Let $S$ be the set consisting of all bad reduction places of $E$, together with one place $u$ over $\ell$ and one place $v$ over $p$. Suppose*

1. *$\text{III}(E)\{\ell\} = 0$;*
2. *the map $E(K)/\ell E(K) \to E(K_w)/\ell E(K_w)$ is an isomorphism for $w = v$ and $w \mid \ell$.*

*Then the $\mathbb{F}_\ell$-dimension of $H^1(U_S, \mathcal{E})[\ell]$ is one. Moreover, every nontrivial element of $H^1(U_S, \mathcal{E})[\ell]$ is ramified at $v$.*

**Proof** The proof is very similar to that of Proposition 2. Suppose $u, u'$ are the places over $\ell$, $v, v'$ the places over $p$. Let $R = \Sigma \cup \{u, u'\}$ and $T = \Sigma \cup \{u, u', v\}$. Let $\alpha \in E(K) - \ell E(K)$. Since $E(K_w)/\ell E(K_w)$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ for $w = v$ and all $w|\ell$, $E(K)/\ell E(K) \cong E(K_w)/\ell E(K_w)$ implies that $\alpha_w \in E(K_w) - \ell E(K_w)$. From Proposition 4 we know that $H^1(U_R, \mathcal{E})[\ell]$ has dimension one and $H^1(U_T, \mathcal{E})[\ell]$ has dimension two. Hence there exists a nontrivial $\psi \in H^1(U_R, \mathcal{E})$, and some $\chi \in H^1(U_T, \mathcal{E}) - H^1(U_R, \mathcal{E})$. By construction $\chi$ is ramified at $v$, and by the condition on $\alpha$ at $v$ we get $< \chi_v, \alpha_v > \neq 0$. As for $\psi$, by the reciprocity law we have $< \psi_u, \alpha_u > + < \psi_{u'}, \alpha_{u'} >= 0$, so either $< \psi_u, \alpha_u >$ and $< \psi_{u'}, \alpha_{u'} >$ are both zero or both non-zero. But if both are zero then by the condition on $\alpha$ at $u$ and $u'$ it would follow that $\psi$ is unramified at both places, violating the condition that $\psi$ is nontrivial. Hence $< \psi_u, \alpha_u >$ and $< \psi_{u'}, \alpha_{u'} >$ are both non-zero. Since $< \psi_{u'}, \alpha_{u'} > \neq 0$, there exists $c \in \mathbb{Z}/\ell\mathbb{Z}$ such that $< \chi_{u'}, \alpha_{u'} >= c < \psi_{u'}, \alpha_{u'} >$, and letting $\phi = \chi - c\psi$, we have $< \phi_{u'}, \alpha_{u'} >= 0$. Now $\phi \in H^1(U_S, \mathcal{E})$ since $< \phi_{u'}, \alpha_{u'} >= 0$, and $\phi$ is a nontrivial since $< \phi_v, \alpha_v >=< \chi_v, \alpha_v > \neq 0$. Hence $H^1(U_S, \mathcal{E})$ is of dimension at least one. Since $\psi$ is ramified at $u'$, it follows that $\psi \notin H^1(U_S, \mathcal{E})$, and since $\psi \in H^1(U_R, \mathcal{E}) \subset H^1(U_T, \mathcal{E})$, it follows that $H^1(U_S, \mathcal{E})$ is a proper subset of $H^1(U_T, \mathcal{E})$, hence it can be of dimension at most one. We conclude that its dimension must be one, and the proposition follows.

**REMARK 1.** *When we use these results below, we will assume that the rank of $E(K)$ is 1, so that the second condition in the last two propositions will likely be satisfied.*

Given such a $\chi$ as in the last proposition, we can then form its ramification signature just as we did in the multiplicative group case. Namely, we take generators $R_v$ of $E(K_v)/\ell = E(\mathbb{F})/\ell$ and $R_u$ of $E(K_u)/\ell$ and consider the number

$$(\langle \chi_v, R_v \rangle)^{-1} \langle \chi_u, R_u \rangle \in (\mathbb{Z}/\ell\mathbb{Z})^*,$$

which is defined and independent of the choice of $\chi$. We call it the *ramification signature* of $\chi$ with respect to the generators $R_u, R_v$.

Since the pairing between $H^1(K_v, E)[\ell]$ and $E(K_v)/\ell E(K_v)$ is perfect, both being isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$, there is a unique $\psi_v \in H^1(K_v, E)[\ell]$ such that $< \psi_v, R_v >= 1$. Similarly, there is a unique $\psi_u \in H^1(K_u, E)[\ell]$ such that $< \psi_u, R_u >= 1$. Let $\chi \in H^1(U_S, \mathcal{E})[\ell]$. Suppose $\chi_v = a_v \psi_v$ and $\chi_u = a_u \psi_u$. Then $< \chi_v, R_v >= a_v$

and $< \chi_u, R_u > = a_u$. So $a_u$ and $a_v$ constitute the signature for $\chi$ with respect to $R_u$ and $R_v$. Thus the signature $(a_u, a_v)$ succinctly represents the localization of $\chi$ at the ramified places. These localizations in turn determine $\chi$ uniquely, since the Shafarevich-Tate group is assumed to have trivial $\ell$-part. Therefore, the signature of $\chi$ can be regarded as a succinct representation of $\chi$ (by determining its localization at $u$ and $v$ as $\chi_u = a_u \psi_u$ and $\chi_v = a_v \psi_v$). We note that this representation requires only $O(\log \ell)$ bits whereas an explicit description of $\chi$ may require $\Omega(\ell)$ bits.

### 5.3. *ECDL and Signature Computation*

In this section we compare the elliptic curve discrete logarithm problem to computing the signature of homogeneous spaces with prescribed ramification as described in Proposition 5. First, we state both problems in a precise way:

**ECDL**: Given $p$, $\ell$, $\tilde{E}$, $\tilde{Q}$ and $\tilde{R}$, where $p$ and $\ell$ are prime, $\tilde{E}$ is an elliptic curve defined over $\mathbb{F}_p$ with $\#\tilde{E}(\mathbb{F}_p) = \ell$, and non-zero points $\tilde{Q}, \tilde{R} \in \tilde{E}(\mathbb{F}_p)$, to determine $m$ so that $\tilde{R} = m\tilde{Q}$.

**Homogeneous Space Signature Computation**: Suppose we are given $p$, $\ell$, $K$, $E$, $u$, $v$, $R$, $\rho_u$ and $\rho_v$, where $p$ and $\ell$ are prime, $K$ is a quadratic field where $p$ and $\ell$ both split, $u$ is a place of $K$ over $\ell$, $v$ is a place of $K$ over $p$, $E$ is an elliptic curve defined over $K$ that satisfies the conditions in Proposition 5, $R \in E(K) - \ell E(K)$, and $\rho_w$ that generates $E(K_w)/\ell E(K_w)$ for $w = u, v$. Then compute the signature of $H^1(U_S, \mathcal{E})[\ell]$ with respect to $\rho_u$ and $\rho_v$, where $S$ is the set consisting of $u, v$ and all places of bad reduction of $E$.

In the following we argue that the problems ECDL and Homogeneous Space Signature Computation are random polynomial time equivalent. We first give a random polynomial time reduction from ECDL to Homogeneous Space Signature Computation. This part of the proof depends on some heuristic assumptions that will be made clear below. We then give a random polynomial time reduction from Homogeneous Space Signature Computation to ECDL. That part of the proof does not depend on any heuristic assumption.

Given $\tilde{E}/\mathbb{F}_p$ where $\tilde{E}(\mathbb{F}_p)[\ell] = < \tilde{Q} >$, and $\tilde{R}$, we are to compute $m$ so that $\tilde{R} = m\tilde{Q}$. Without loss of generality we may assume that $\tilde{R} \neq 0$. Steps 1-4 of the reduction construct an instance $p$, $\ell$, $K$, $E$, $u$, $v$, $R$, $\rho_u$ and $\rho_v$, of the Homogeneous Space Signature Computation problem.

1. Suppose $\tilde{E}$ is specified by an affine equation $y^2 = x^3 + \bar{a}x + \bar{b}$ where $\bar{a} = a \bmod p$, $\bar{b} = b \bmod p$ with $0 \leqslant a, b < p$. Choose a random integer $r$, $0 \leqslant r < p$, and let $b_r = b + rp$. Let $E$ be the elliptic curve with the affine equation $y^2 = x^3 + ax + b_r$. Let $Q \in E(\mathbb{Q}_p)$ so that $\tilde{Q} = Q \bmod p$. Since $\tilde{E}(\mathbb{F}_p)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$, $E(\mathbb{Q}_p)/\ell \cong \tilde{E}(\mathbb{F}_p)/\ell \cong \mathbb{Z}/\ell\mathbb{Z}$ and the class of $Q$ generates $E(\mathbb{Q}_p)/\ell$.

2. Check that $E$ has good reduction at $\ell$ and that $|\tilde{E}(\mathbb{F}_\ell)|$ is not divisible by $\ell$. Otherwise, go back to 1. to find a different $E$.

3. Lift $\tilde{R}$ to $R \in E(K)$ where $K/\mathbb{Q}$ is a quadratic extension in which $p$ and $\ell$ both split. This can be done as follows. Suppose $E$ is defined by the affine equation $y^2 = x^3 + ax + c$. Suppose $\tilde{R} = (\mu \bmod p, \nu \bmod p)$ with $0 < \mu, \nu < p$. Choose a random positive integer $r < p$. Set $\mu_r = \mu + rp$. Let $\beta$ be a root of $y^2 = \mu_r^3 + a\mu_r + c$. Then $(\mu_r, \beta)$ is a lift of $\tilde{R}$ in $E(K)$ where $K = \mathbb{Q}(\beta)$. By construction, $p$ splits in $K$,

$$E(K_v)/\ell \cong E(\mathbb{Q}_p)/\ell \cong \tilde{E}(\mathbb{F}_p)/\ell \cong \mathbb{Z}/\ell\mathbb{Z}$$

and $R - mQ \in \ell E(K_v)$. Check that $\ell$ splits in $K$; otherwise repeat the above steps with a different $r$ until a suitable $K$ is found.

4. Set $\rho_v$ to be the class of $Q$ in $E(K_v)/\ell$. (For computational purposes $\tilde{Q}$ is sufficient to represent the class of $Q$.) Set $\rho_u$ to be $R_u$. (Here we note that by reciprocity laws we have $< \chi_u, R_u > + < \chi_v, R_v > = 0$. By construction, we have $< \chi_v, R_v > \neq 0$. It follows that $< \chi_u, R_u > \neq 0$, so the class of $R_u$ generates $E(K_u)/\ell$.)

5. Call the oracle for the Homogeneous Space Signature Computation on input $p$, $\ell$, $K$, $E$, $u$, $v$, $R$, $\rho_u$ and $\rho_v$, to compute the ramification signature $\alpha$ of $H^1(U_S, \mathcal{E})[\ell]$ with respect to $\rho_u$ and $\rho_v$ (where $S$ is the set consisting of $u, v$ and all places of bad reduction of $E$). Then for all nontrivial $\chi \in H^1(U_S, \mathcal{E})[\ell]$, $\alpha = < \chi_u, \rho_u > (< \chi_v, \rho_v >)^{-1}$.

6. Now

$$0 = \sum_{w \in \{v, u\}} < \chi_w, R_w >$$
$$= m < \chi_v, Q_v > + < \chi_u, R_u > .$$

From this we get $m + \alpha \equiv 0 \pmod{\ell}$. Hence $m$ can be determined.

We make the heuristic assumption that it is likely for $E$ and $K$ to satisfy the conditions in Proposition 5, and that with nonzero probability, $E(K)$ is of rank exactly one. The expected running time of this reduction is dominated by Step 2 where the number of rational points on the reduction of $E$ mod $\ell$ is counted. The running time of that step is $O(\log^8 \ell)$ [30], hence it is $O(\log^8 p)$.

Next we give a polynomial time reduction from Homogeneous Space Signature Computation with input $p$, $\ell$, $K$, $E$, $u$, $v$, $Q$, $\rho_u$ and $\rho_v$, to ECDL with input $p$, $\ell$, $\tilde{E}$, $\tilde{Q}$, $\tilde{R}$, where $\tilde{E}$ is the reduction of $E$ mod $v$, $\tilde{Q}$ (resp. $\tilde{R}$) is the reduction of $Q$ (resp. $\rho_v$) mod $v$.

For any nontrivial $\chi \in H^1(K, E)[\ell]$ that is unramified away from $u$ and $v$, we have

$$< \chi_v, Q_v > + < \chi_u, Q_u > = 0.$$

Suppose $Q = a_w \rho_w \pmod{\ell E(K_w)}$ for $w = u, v$. Note that from Lemma 1, $a_v$

can be computed by solving ECDL on the reduction of $E$ modulo $v$.

On the other hand $a_u$ can be computed in a manner as follows. Identify $K_u$ with $\mathbb{Q}_\ell$. Compute $d = |\tilde{E}(\mathbb{F}_\ell)|$. Observe that $dQ$ and $d\rho_u$ are both in $E_1(\mathbb{Q}_\ell)$. Compute $n$ such that $n(d\rho_u) \equiv (dQ) \pmod{\ell}$ in $E_1(\mathbb{Q}_\ell)$. Then $d(n\rho_u - Q) = \ell Z$ for some $Z \in E_1(\mathbb{Q}_\ell)$. Since $d$ is not divisible by $\ell$, $d^{-1} \in \mathbb{Z}_\ell$, so $n\rho_u - Q = d^{-1}\ell Z = \ell(d^{-1}Z) \in \ell E(\mathbb{Q}_\ell)$, so $n \equiv a_u \pmod{\ell}$.

Then we get

$$a_v < \chi_v, \rho_v > + a_u < \chi_u, \rho_u > = 0$$

From the above we can compute the the ramification signature; that is $< \chi_u, \rho_u > (< \chi_v, \rho_v >)^{-1}$. The running time of this reduction can be shown to be $O(\log^4 p) + O(M \log p)$ where $M$ is the maximum of the lengths of $Q$ and the coefficients in the affine model of $E$.

## 6. *Feasibility of Signature Calculus*

For the multiplicative group and elliptic curves over finite prime fields, we have provided heuristic arguments for the equivalence between the discrete-log problem and a signature computation problem that involves two large primes. A natural question to ask at this point is whether a signature calculus method that leverages small primes like the method described in § 3 can be fashioned for each case. We will describe such a method for Dirichlet characters and then discuss why a similar method is unlikely to work for principal homogeneous spaces.

### 6.1. *Signature Calculus for Dirichlet Characters*

Suppose we are given a real quadratic field $K$, primes $\ell$, $p$, places $u, v$ satisfying the conditions in Proposition 2. Let $K = \mathbb{Q}(\alpha)$ with $\alpha^2 \in \mathbb{Z}_{>0}$. To compute the signature of $\chi \in H^1(K, \mathbb{Z}/\ell\mathbb{Z})$ that is ramified precisely at $u$ and $v$, we generate random algebraic integers $\beta = r\alpha + s$ with $r, s \in \mathbb{Z}$ so that $\beta \equiv g \pmod{v}$. Write $\beta = \xi(1+a\ell) \pmod{\ell^2}$ with $\xi^{\ell-1} = 1$ after identifying $\beta$ with its isomorphic image in $\mathbb{Q}_\ell$. Then $\beta \sim^\ell (1+\ell)^a$. Now suppose the norm of $\beta$ is $B$-smooth for some integer $B$. Then

$$0 = \sum_w < \chi_w, \beta_w > = < \chi_v, g_v > + a < \chi_u, 1 + \ell_u > + \sum_w e_w < \chi_w, \pi_w >,$$

where $w$ in the last sum ranges over all places of $K$ of norm less than $B$, $\pi_w$ is a local parameter at $w$, and $e_w$ is the valuation of $\beta$ under $w$. Hence we have obtained a $\mathbb{Z}/\ell\mathbb{Z}$-linear relation on $(< \chi_v, g_v >)^{-1} < \chi_u, 1 + \ell_u >$, and $(< \chi_v, g_v >)^{-1} < \chi_w, \pi_w >$. With $O(B)$ relations we can solve for all these unknowns, in particular the signature

$$(< \chi_v, g_v >)^{-1} < \chi_u, 1 + \ell_u >$$

.

### 6.2. *The Elliptic Curve Case*

We see that one important reason why signature calculus is viable in the multiplicative case is due to the fact that locally unramified Dirichlet characters can be

paired nontrivially with non-units. For the elliptic curve case, pairing a principal homogeneous space $\chi$ and a global point $\alpha$ yields similarly a relation:

$$0 = \sum_v <\chi_v, \alpha_v>.$$

However from Lemma 1 we see that in the sum above we have nontrivial contribution from a place $v \nmid \ell$ (and where $E$ has good reduction) only if $\ell$ divides $\#\tilde{E}(\mathbb{F}_v)$. Since $\#\tilde{E}(\mathbb{F}_v)$ is of order $\#\mathbb{F}_v$, which is the norm of $v$, we see that the finite places of good reduction that are involved in the sum are all of large norm. As for the bad reduction places, the heuristic assumption that we discussed just before Proposition 4 implies that these will not play any role in this sum, since it will be likely that $E(K_v)/\ell = 0$ for such places $v$, because $v$ is of small norm. This explains why a signature calculus method is lacking in the case of elliptic curves.

## 7. *Characterization of ramification signature*

Let $K, \ell, p, u, v, S$ be as in Proposition 2 and denote by $K(\mu_n)$ the field obtained by adjoining the $n$-th roots of unity to $K$. The group, $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$, of Dirichlet characters determines a unique cyclic extension $K_S$ of degree $\ell$ ramified precisely at $u$ and $v$. As we shall see below, the signature of any character in $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ is closely related to the construction of the cyclotomic extension $K_S(\mu_\ell)$ as a Kummer extension of $K(\mu_\ell)$.

Let $g \in \mathbb{Z}$ so that $g \bmod p$ generates the multiplicative group of $\mathbb{F}_p$. Let $w$ be the place of $K(\mu_\ell)$ over $v$ such that $g^{\frac{p-1}{\ell}} \equiv \zeta \pmod w$.

Let $M = K_S$. Suppose $\chi \in H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ is nontrivial. Then $\chi$ determines some $A \in K(\mu_\ell)$ through $H^1(K(\mu_\ell), \mathbb{Z}/\ell\mathbb{Z}) \cong H^1(K(\mu_\ell), \mu_\ell) \cong K(\mu_\ell)^*/K(\mu_\ell)^{*\ell}$, such that $M(\mu_\ell) = K(\mu_\ell)(A^{\frac{1}{\ell}})$, and for all $\sigma$ in the absolute Galois group of $K$, $\chi(\sigma) = i$ iff $\sigma(A^{\frac{1}{\ell}})/A^{\frac{1}{\ell}} = \zeta^i$.

The following proposition provides a concrete characterization of the signature of $\chi$.

PROPOSITION 6. *If we identify $K(\mu_\ell)_w$ with $\mathbb{Q}_p$ and $K_u$ with $\mathbb{Q}_\ell$, then $A \sim^\ell p^m$ in $\mathbb{Q}_p^{ur}$ where $-m = \sigma_v(\chi) =<\chi_v, g_v>$, and $A \sim^\ell \zeta^n$ in $\mathbb{Q}_\ell(\mu_\ell)^{ur}$ where $-n = \sigma_u(\chi) =<\chi_u, 1 + \ell_u>$.*

From the proposition it follows that if we identify $K(\mu_\ell)_w$ with $\mathbb{Q}_p$ and $K_u$ with $\mathbb{Q}_\ell$, then $A \sim^\ell p^m$ in $\mathbb{Q}_p^{ur}$ and $A \sim^\ell \zeta^n$ in $\mathbb{Q}_\ell(\mu_\ell)^{ur}$, and $m^{-1}n$ is the ramification signature of $K_S$ (that is, the normalized signature of all Dirichlet characters in $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$).

The rest of this section is devoted to the proof of this proposition. We set some notation first. For any local field $L$, let $L^{ur}$ denote the maximal unramified extension over $L$. For any place $\nu$ of a number field $K$, let $\theta_\nu$ denote the local Artin map,

$$\theta_\nu : K_\nu^* \to G_\nu^{ab},$$

where $G_\nu^{ab}$ denotes the Galois group of the maximal abelian extension of $K_\nu$. For $a, b \in K(\mu_\ell)$ and $\nu$ a prime of $K(\mu_\ell)$, we have

$$\alpha^{\theta_\nu(b)} = (a, b)_\nu \alpha$$

where $\alpha^l = a$, and $(a, b)_\nu$ denotes the local norm residue symbol (see p. 351 of [**3**]).

LEMMA 3. $\sigma_u(\chi) = < \chi_u, 1 + \ell_u > = \chi_u(\theta_u(1 + \ell))$ *and* $\sigma_v(\chi) = < \chi_v, g_v > = \chi_v(\theta_v(g))$

**Proof** This follows directly from [**31**], Chapter XIV, Proposition 3.

**Proof of Proposition 6** Suppose $v'$ is a place of $K(\mu_\ell)$ such that $v'|v$. Then $d < \chi_v, b_v > = < \chi_{v'}, b_{v'} >$ where $d = [K(\mu_\ell)_{v'} : K_v]$ (see [**31**], Proposition 7 of Ch. XIII). Moreover $< \chi_{v'}, b_{v'} > = \chi_{v'}(\theta_{v'}(b)) = i$ iff $(A, b)_{v'} = \zeta^i$. Identifying $i$ with $\zeta^i$, we may write

$$d < \chi_v, b_v > = < \chi_{v'}, b_{v'} > = (A, b)_{v'}$$

We analyze the situation at $p$ and $\ell$ separately.

(I) At $p$: $\mathbb{Q}_p^*/\ell = \mu_\ell \times < p > /\ell$. So under the identification of $K(\mu_\ell)_w$ with $\mathbb{Q}_p$, $A = up^{w(A)}$ where $u^\ell = 1$, and $e < \ell$. Since $\mathbb{Q}_p(u^{\frac{1}{\ell}})/\mathbb{Q}_p$ is unramified, $A \sim^\ell p^{w(A)}$ in $\mathbb{Q}_p^{ur}$, so $m = w(A)$.

Since

$$\left(\frac{g}{w}\right) \equiv g^{\frac{Nw-1}{\ell}} \equiv g^{\frac{p-1}{\ell}} \equiv \zeta \pmod{P_w},$$

and

$$(g, A)_w = i \text{ iff } \zeta^i = \left(\frac{g}{w}\right)^{w(A)},$$

it follows that $(g, A)_w = w(A)$. Therefore

$$< \chi_v, g_v > = < \chi_w, g_w > = (A, g)_w = -(g, A)_w = -w(A) = -m.$$

(II) At $\ell$: Denote by $u'$ the place of $K(\mu_\ell)$ over $u$. There is a ramified extension of degree $\ell$ over $\mathbb{Q}_\ell$, namely, the subextension $M_1$ of $\mathbb{Q}_\ell(\zeta_{\ell^2})$ of degree $\ell$ over $\mathbb{Q}_\ell$. Let $\psi$ be the ramified character in $H^1(\mathbb{Q}_\ell, \mathbb{Z}/\ell\mathbb{Z})$ whose restriction to $H^1(\mathbb{Q}_\ell(\zeta), \mathbb{Z}/\ell\mathbb{Z})$ corresponds to the class of $\zeta$ under the isomorphism $H^1(\mathbb{Q}_\ell(\zeta), \mathbb{Z}/\ell\mathbb{Z}) \cong H^1(\mathbb{Q}_\ell(\zeta), \mu_\ell) \cong \mathbb{Q}_\ell(\zeta)^*/\ell$. Then the kernel of $\psi$ corresponds to $M_1$.

There is an unramified extension $N$ of degree $\ell$ over $\mathbb{Q}_\ell$ (an Artin-Schreier extension). Let $N(\zeta) = \mathbb{Q}_\ell(\zeta)(\beta^{\frac{1}{\ell}})$ with $\beta \in \mathbb{Q}_\ell(\zeta)^*$. Let $\varphi$ be the unramified character in $H^1(\mathbb{Q}_\ell, \mathbb{Z}/\ell\mathbb{Z})$ whose restriction in $H^1(\mathbb{Q}_\ell(\zeta), \mathbb{Z}/\ell\mathbb{Z})$ corresponds to the class of $\beta$ under the isomorphism $H^1(\mathbb{Q}_\ell(\zeta), \mathbb{Z}/\ell\mathbb{Z}) \cong H^1(\mathbb{Q}_\ell(\zeta), \mu_\ell) \cong \mathbb{Q}_\ell(\zeta)^*/\ell$. Note that

since $N$ is unramified, $\beta^{\frac{1}{\ell}} \in \mathbb{Q}_\ell(\zeta)^{ur}$.

From Tate local duality we see that $H^1(\mathbb{Q}_\ell, \mathbb{Z}/\ell\mathbb{Z})$ has the same dimension as $\mathbb{Q}_\ell^*/\ell$. The latter is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$. So the dimension of $H^1(\mathbb{Q}_\ell, \mathbb{Z}/\ell\mathbb{Z})$ is two. Since the two characters $\psi$ and $\varphi$ are independent, one being ramified and the other not, they form a basis of $H^1(\mathbb{Q}_\ell, \mathbb{Z}/\ell\mathbb{Z})$ over $\mathbb{Z}/\ell\mathbb{Z}$. It follows that every character in $H^1(\mathbb{Q}_\ell, \mathbb{Z}/\ell\mathbb{Z})$ is of the form $a\psi + b\varphi$ with $a, b \in \mathbb{Z}/\ell\mathbb{Z}$. Suppose $\chi_u$ corresponds to $a\psi + b\varphi$, with $a, b \in \mathbb{Z}/\ell\mathbb{Z}$, under the isomorphism between $H^1(K_u, \mathbb{Z}/\ell\mathbb{Z})$ and $H^1(\mathbb{Q}_\ell, \mathbb{Z}/\ell\mathbb{Z})$. Then the restriction of $\chi_u$ in $H^1(\mathbb{Q}_\ell(\zeta), \mathbb{Z}/\ell\mathbb{Z})$ corresponds to the class of $\rho = \zeta^a\beta^b$, and gives rise to a cyclic extension $M'$ of degree $\ell$ over $\mathbb{Q}_\ell$ with $M'(\zeta) = \mathbb{Q}_\ell(\zeta)(\rho^{\frac{1}{\ell}})$. Therefore, $A \sim^\ell \zeta^a\beta^b$ under the identification of $K(\mu_\ell)_{u'}$ with $\mathbb{Q}_\ell(\mu_\ell)$, and $A \sim^\ell \zeta^a$ in $\mathbb{Q}_\ell(\mu_\ell)^{ur}$ as $\beta^{\frac{1}{\ell}} \in \mathbb{Q}_\ell(\zeta)^{ur}$. So $a = n$.

Since $\varphi$ is unramified and $1 + \ell$ is a unit, $<\varphi, 1+\ell> = 0$.

To calculate $<\psi, 1+\ell> = (\zeta, 1+\ell)$, let $\lambda = 1 - \zeta$ and $\eta_i = 1 - \lambda^i$ for $i = 1, 2,...$ Then $\zeta = \eta_1$ and $1 + \ell = \eta_{\ell-1}\xi$ with $\xi \equiv 1 \pmod{\lambda^\ell}$. Using the formulas for norm residue symbols involving $\eta_i$ and $\lambda$ (see [**3**] p.354; our symbol is written additively), we get

$$(\zeta, 1+\ell) = (\eta_1, 1+\ell) = (\eta_1, \eta_{\ell-1}\xi) = (\eta_1, \eta_{\ell-1}) = (\eta_1, \eta_\ell) + (\eta_\ell, \eta_1) - (\ell-1)(\eta_\ell, \lambda) = 1.$$

We have

$$(\ell-1) <\chi_u, 1+\ell_u> = <\chi_{u'}, 1+\ell_{u'}> = <a\psi+b\varphi, 1+\ell> = a<\psi, 1+\ell> = a(\zeta, 1+\ell) = a.$$

So

$$\sigma_u(\chi) = <\chi_u, 1+\ell_u> = -a = -n.$$

### References

1.  B. BEKTERMIROV, B. MAZUR, W. STEIN and M. WATKINS, 'Average ranks of elliptic curves: tension between data and conjectures', *Bull. American Math. Society* 44 (2007) 233-254 252

2.  V. BERKOVICH, 'Duality theorems in Galois cohomology of commutative algebraic groups', Selected translations. *Selecta Math. Soviet* 6 (1987), no. 3, 201–296 230

3.  J.W.S. CASSELS and A. FRÖHLICH, *Algebraic Number Theory* (Academic Press 1967). 260, 261

4.  C. CHEVALLEY, 'Une démonstration d'un théorème sur les groupes algébriques', *J. Mathématiques Pures et Appliquées* 39 (1960) 307-317 230

5.  H. COHEN and H.W. LENSTRA, JR., 'Heuristics on class groups of number fields', *Number theory, Noordwijkerhout 1983*, 33–62, Lecture Notes in Math., 1068 (Springer, Berlin, 1984). 247

6.  H. COHEN and H.W. LENSTRA, JR., 'Heuristics on class groups', Number theory (New York, 1982), *Lecture Notes in Math.*, 1052 (Springer, Berlin, 1984) 26–36.

7.  B. CONRAD, *A modern proof of Chevalley's theorem on algebraic groups*, J. Ramanujan Math. Soc. 17 (2002), no. 1, 1–18. 247

8.  H. DARMON, 'Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications', *Ann. of Math.* (2) 154 (2001), no. 3, 589–639. 230

9. M. DEURING, 'Die Typen der Multiplikatorenringe elliptischer Funktionenkörper', *Abh. Math. Sem. Hansischen Univ.* 14 (1941) 197-272. 229

10. G. FREY, 'Applications of arithmetical geometry to cryptographic constructions', *Proceedings of the Fifth International Conference on Finite Fields and Applications* (Springer Verlag, 1999) 128-161. 234
    229, 231

11. G. FREY and H.-G. RÜCK, 'A remark concerning $m$-divisibility and the discrete logarithm in the divisor class group of curves', *Mathematics of Computation*, 62(206) (1994) 865–874. 229, 231

12. D. GOLDFELD, 'Conjectures on elliptic curves over quadratic fields', in *Number Theory (Carbondale, Ill., 1979)*, Lecture Notes in Math. 751 (Springer, Berlin, 1979) 108–118. 252

13. R. HARTSHORNE, *Algebraic Geometry*, Graduate Texts in Mathematics, Volume 52 (Springer-Verlag, New York, Heidelberg, Berlin 1977). 231

14. D.R. HEATH-BROWN, 'The average analytic rank of elliptic curves', *Duke Math. J.* 122 (2004), no. 3, 591–623. 252

15. M.-D. HUANG, K. L. KUEH, and K.-S. TAN 'Lifting elliptic curves and solving the elliptic curve discrete logarithm problem', *ANTS IV, Lecture Notes in Computer Science*, 1838 (Springer-Verlag, 2000). 229

16. M.-D. HUANG and W. RASKIND, 'Signature calculus and discrete logarithm problems', *Proceedings of the 7th Algorithmic Number Theory Symposium (ANTS 2006)*, LNCS 4076 (Springer-Verlag, 2006) 558-572. 231

17. M.J. JACOBSON, N. KOBLITZ, J.H. SILVERMAN, A. STEIN, and E. TESKE, 'Analysis of the Xedni calculus attack', *Design, Codes and Cryptography* 20 (2000) 41-64. 229

18. S. KAMIENNY, 'Torsion points on elliptic curves and $q$-coefficients of modular forms', *Invent. Math.* 109 (1992), no. 2, 221–229. 254

19. N. KOBLITZ, 'Elliptic curve cryptosystems', *Mathematics of Computation* 48 (1987) 203-209. 228

20. N. KOBLITZ, A. MENEZES and S. VANSTONE, 'The state of elliptic curve cryptography', *Design, Codes and Cryptography* 19 (2000) 173-193. 228

21. S. LANG, 'Algebraic groups over finite fields', *Amer. J. Math.* 78 (1956) 555–563. 230

22. K. MCCURLEY, 'The discrete logarithm problem', *Cryptology and Computational Number Theory*, ed. C. Pomerance, Proceedings of Symposia in Applied Mathematics, 42 (1990) 49-74. 229

23. V. MILLER, 'Uses of elliptic curves in cryptography', *Advances in Cryptology: Proceedings of Crypto 85, Lecture Notes in Computer Science*, 218 (Springer-Verlag, 1985) 417-426. 228

24. J.S. MILNE, *Étale Cohomology* (Princeton Mathematical Series, Volume 33, Princeton University Press, 1980). 230, 232, 233, 239

25. J.S. MILNE, *Arithmetic Duality Theorems* (Perspectives in Mathematics, Volume 1., Academic Press, 1986). 238, 239, 240

26. K. NGUYEN, Thesis, Universität Essen, 2001. 229, 231

27. K. RUBIN and A. SILVERBERG, 'Ranks of elliptic curves', *Bull. Amer. Math. Soc. (N.S.)* 39 (2002), no. 4, 455–474. 252

**28.** O. Schirokauer, D. Weber, and T. Denny, 'Discrete logarithms: The effectiveness of the index calculus method', *ANTS II, volume 1122 of Lecture Notes in Computer Science*, ed. H. Cohen (Springer-Verlag, 1996) 337-362. 229

**29.** A. Schmidt, 'Rings of integers of type $K(\pi, 1)$', *Documenta Mathematica* 12 (2007) 441-471. 238

**30.** R. Schoof, 'Counting points on elliptic curves over finite fields', *Journal de Théorie des Nombres de Bordeaux* 7 (1995) 219-254. 257

**31.** J.-P. Serre, *Corps Locaux* Paris Hermann 1962; English translation: Local Fields, Graduate Texts in Mathematics, Volume 67, Springer Verlag, Heidelberg-New York, 1979. 233, 235, 236, 237, 260

**32.** J.-P. Serre, *Groupes p-divisibles (d'après J. Tate)* (Séminaire Bourbaki 1966/67, Exposé 318, reprinted by the Société Mathématique de France, 1995). 234

**33.** J.-P. Serre, *Groupes Algébriques et Corps de Classes* Hermann, Paris, 1975. English Translation *Algebraic Groups and Class Fields*, Graduate Texts in Mathematics 117, Springer Verlag, 1988. 237

**34.** G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions* (Princeton University Press, 1994). 229

**35.** G. Shimura, 'Class fields over real quadratic fields and Hecke operators', *Ann. Math.* 95 (1972) 130-190. 229

**36.** J.H. Silverman, *The Arithmetic of Elliptic Curves* (Graduate Texts in Mathematics, Volume 106, Springer Verlag, 1986). 252, 253

Ming-Deh Huang    huang@pollux.usc.edu

Department of Computer Science
University of Southern California
Los Angeles
CA 90089-0781
USA


Wayne Raskind    wraskind@asu.edu

Department of Mathematics
University of Southern California
Los Angeles
CA 90089-2532
USA
Current Address: School of Mathematical and Statistical Sciences
Arizona State University
PO Box 871804
Tempe, AZ 85287-1804
USA