

# Global Methods for Discrete Logarithm Problems II: Signature Calculus in the Multiplicative Group Case

Ming-Deh Huang and Wayne Raskind

## Introduction

This is the second in a series of papers in which we develop a unified method for treating the discrete logarithm problem (DLP) in various contexts. In [HR1], we described a formalism using global duality for a unified approach to the DLP for the multiplicative group and for elliptic curves over finite fields. The main tool to be employed is what we call *signature calculus*. In this paper, we use signature calculus to study the DLP in detail for the group  $\mathbb{F}_p^*$  of invertible elements of the finite prime field,  $\mathbb{F}_p$ . Recall that in this context, the DLP is formulated as follows: let  $\ell$  be a prime number dividing  $p - 1$ , so that there is an element  $Q$  of  $\mathbb{F}_p^*$  of order  $\ell$ . Suppose we are given another element  $R$  that we know is in the subgroup generated by  $Q$ , so that  $R = Q^n$  for some positive integer  $n$  with  $0 \leq n \leq \ell - 1$ . Then the DLP is to determine  $n$  in a computationally efficient way. The expected computational complexity of this problem is the basis of many public-key cryptographic systems.

We approach the discrete logarithm problem for  $\mathbb{F}_p^*$  by lifting an element whose discrete log we seek to compute to an algebraic number field  $K$ , and use a suitable Dirichlet character of  $K$  of order  $\ell$  to “test” the lifting, and derive relations by using the reciprocity law of global class field theory. In this context the classical index calculus method arises as a special case of our global method in a way that is reminiscent of Nguyen’s work [N] on the index calculus method for Brauer group computations. We then prove the random polynomial time equivalence

of the discrete logarithm problem with the problem of computing the ratios of “signatures” of certain real quadratic Dirichlet characters - equivalently, of computing the “ramification signature” of certain cyclic extensions over real quadratic number fields.

### 1. The global framework

In [HRI], we outlined the general method and recalled basic concepts from algebraic number theory as they pertain to the subject at hand. Here we very briefly set notation. Let  $K$  be an algebraic number field,  $v$  a place of  $K$ , and  $K_v$  the completion of  $K$  at  $v$ . We consider Dirichlet characters of  $K$  of order  $\ell$ , which we regard as elements of the Galois cohomology group  $H^1(G, \mathbb{Z}/\ell\mathbb{Z})$ , where  $G = \text{Gal}(\bar{K}/K)$  is the absolute Galois group of  $K$ . If  $\chi$  is such a character and  $a \in K^*$ , we have for each place  $v$  of  $K$  the local norm residue symbols

$$\langle \chi_v, a_v \rangle_v \in \mathbb{Z}/\ell\mathbb{Z}.$$

Then  $\langle \chi_v, a_v \rangle_v = 0$  for almost all  $v$  and we have the reciprocity law:

$$\sum_v \langle \chi_v, a_v \rangle_v = 0 \in \mathbb{Z}/\ell\mathbb{Z}.$$

Let  $L_\chi$  be the extension of  $K$  corresponding to the kernel of  $\chi$ . For  $a \in K^*$ ,  $\langle \chi, a \rangle = 0$  iff  $a$  is a norm from the extension  $L_\chi$ . (see [S], Corollary 1 of §1 of Chapter XIV). Suppose  $v$  is a nonarchimedean place of  $K$  with completion  $K_v$ . If  $\chi$  is a ramified character of  $K_v$ , then  $\langle \chi, a \rangle \neq 0$  for some unit  $a \in K_v^*$ . On the other hand if  $\chi$  is unramified, every unit  $a$  of  $K_v$  is a norm from the extension  $L_\chi$ , so  $\langle \chi, a \rangle = 0$ . (see [S], Proposition 3a) of §2 of Chapter V.) Therefore in the case of a number field  $K$ , for  $\chi \in H^1(K, \mathbb{Z}/\ell\mathbb{Z})$ ,  $a \in K$ , and a place  $v$  of  $K$ ,  $\langle \chi, a \rangle_v = 0$  if  $\chi$  is unramified at  $v$  and  $a$  is a local unit at  $v$ . Hence

$$\sum_v \langle \chi_v, a_v \rangle_v = 0,$$

where the sum is over all  $v$  such that either  $\chi$  is ramified, or  $v(a) \not\equiv 0 \pmod{\ell}$ .

Let  $\chi \in H^1(K, \mathbb{Z}/\ell\mathbb{Z})$  and  $a$  a unit of  $\mathcal{O}_K$ . Then

$$\sum_v \langle \chi_v, a_v \rangle_v = 0,$$

where the sum is over all  $v$  such that  $\chi$  is ramified.

The main idea of our approach is to lift elements of a finite field  $\mathbb{F}_p$  to a global field  $K$  where discrete logarithms are preserved at a place over  $p$ . The above identity then allows us to distribute information of a discrete logarithm among a set of places depending on the choice of  $\chi$  and the manner of lifting. As we saw in ([HRI], §2), the classical index calculus emerges in this context as the result of one particular choice of  $\chi$  and method of lifting. Section 4 presents a different construction of  $\chi$  which, together with a different method of lifting, leads to random polynomial time equivalence between the discrete logarithm problem and what is called the *signature computation* problem. In Section 6 we discuss how the construction of an appropriate  $\chi$  with prescribed ramification is closely related to class field theory.

## 2. 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  $\alpha$  be a fundamental unit of  $K$ . 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. Suppose*

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

*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:** The Poitou-Tate global duality theorem gives an exact sequence:

$$\dots \bigoplus_{v \in S} H^0(K_v, \mathbb{Z}/\ell\mathbb{Z}) \xrightarrow{g} H^2(G_S, \mu_\ell)^* \rightarrow H^1(G_S, \mathbb{Z}/\ell\mathbb{Z}) \xrightarrow{\rho} \bigoplus_{v \in S} H^1(K_v, \mathbb{Z}/\ell\mathbb{Z}) \xrightarrow{h} H^1(G_S, \mu_\ell)^* \rightarrow \dots$$

First, we claim that under the hypotheses of the theorem,  $\rho$  is injective. 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:

$$H^2(G_S, \mu_\ell) \xrightarrow{g^*} \bigoplus_{v \in S} H^2(K_v, \mu_\ell)$$

is injective, so the map  $g$  is surjective. This gives the injectivity of  $\rho$ . Now consider the dual map to  $h$ :

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

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:

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

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

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

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  $h^*$  is injective and we claim that the target has dimension  $2n(S)$ . This can be seen easily because  $H^1(K_v, \mu_\ell)$  is isomorphic to  $\mathbb{Q}_v^*/\ell$ . If  $v \mid p$ , then this group is of dimension 2 over  $\mathbb{F}_\ell$  because  $\ell \mid p - 1$ . If  $v \nmid \ell$ , 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  $h^*$  is of dimension  $n(S) - 1$  and is dual to the kernel of  $h$ , so this is of dimension  $n(S) - 1$ , too. 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)  $\alpha^{l-1} \not\equiv 1 \pmod{P_u^2}$ ;

$$(3) \alpha^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{P_v}.$$

Then the  $\mathbb{F}_\ell$ -dimension of  $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$  is one.

**Proof** Suppose  $u, u'$  are the places over  $\ell$ ,  $v, v'$  the places over  $p$ . 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 we know 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 2. So there exists  $\chi \in H^1(G_T, \mathbb{Z}/\ell\mathbb{Z}) - H^1(G_R, \mathbb{Z}/\ell\mathbb{Z})$ . Such  $\chi$  must be ramified at  $v$ , and by the condition on  $\alpha$  at  $v$  we get  $\langle \chi, \alpha \rangle_v \neq 0$ . Let  $\psi$  be a nontrivial element of  $H^1(G_R, \mathbb{Z}/\ell\mathbb{Z})$ . Then by the condition of  $\alpha$  at  $u$  we have  $\langle \psi, \alpha \rangle_u \neq 0$ . Since  $\langle \psi, \alpha \rangle_u + \langle \psi, \alpha \rangle_{u'} = 0$ , it follows that  $\langle \psi, \alpha \rangle_{u'} \neq 0$ , so there exists  $c \in \mathbb{Z}/\ell\mathbb{Z}$  such that  $\langle \chi, \alpha \rangle_{u'} + c \langle \psi, \alpha \rangle_{u'} = 0$ . Let  $\phi = \chi + c\psi$ . Then  $\phi \in H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$  since  $\langle \phi, \alpha \rangle_{u'} = 0$ , and  $\phi$  is a nontrivial since  $\langle \phi, \alpha \rangle_v = \langle \chi, \alpha \rangle_v \neq 0$ . Since  $\psi \notin H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ , 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 can be of dimension at most one. Since it has a nontrivial element  $\phi$ , we conclude that its dimension must be one, and the proposition follows.

REMARK 1. *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:*

(i) *is made to ensure that the Dirichlet characters of degree  $\ell$  that we get will not be everywhere unramified, as this will be of no use to us for the signature computation.*

*If one of the conditions (ii) and (iii) are satisfied, but not both, then we may get a Dirichlet character of degree  $\ell$  that is ramified at only one of the two places. This can be seen from the ideal theoretic formulation of global class field theory, as follows (see e.g. [R], §6.3 for more details). Let  $I$  be an ideal of  $\mathcal{O}_K$  and let  $K_I$  be the maximal abelian extension of  $K$  with conductor dividing  $I$ . This is a finite extension which is unramified outside of the places of  $K$  corresponding to prime ideals dividing  $I$ . The Galois group  $\text{Gal}(K_I/K)$  is isomorphic to a generalized ideal class group that we'll denote by  $Cl_I(\mathcal{O}_K)$ . For example,  $Cl_{(1)}(\mathcal{O}_K) = Cl(\mathcal{O}_K)$ . Then we have an exact sequence (modulo 2-torsion, due to the fact that we are ignoring real places):*

$$\cdots \mathcal{O}_K^* \rightarrow (\mathcal{O}_K/I)^* \rightarrow Cl_I(\mathcal{O}_K) \rightarrow Cl(\mathcal{O}_K).$$

If we take for example  $I = \mathfrak{p}$ , where  $\mathfrak{p}$  is an ideal of  $\mathcal{O}_K$  lying over  $p$ , then we get assuming (i) that

$$\text{Coker}[\mathcal{O}_K^* \rightarrow (\mathcal{O}_K/\mathfrak{p})^*]\{\ell\} \cong Cl_{\mathfrak{p}}(\mathcal{O}_K)\{\ell\}.$$

If condition (ii) is not satisfied, then the image of

$$\mathcal{O}_K^* \rightarrow (\mathcal{O}_K/\mathfrak{p})^*$$

is 2-torsion, and hence there is an extension of  $K$  of degree  $\ell$  which is ramified precisely at  $\mathfrak{p}$ . The same holds if we take  $I = \mathfrak{l}^r$ , where  $\mathfrak{l}$  is an ideal of  $\mathcal{O}_K$  lying above  $\ell$  and  $r \geq 2$ . Thus conditions (ii) and (iii) are meant to ensure that there do not exist characters of  $K$  of degree  $\ell$  that are ramified only at  $\mathfrak{p}$  or only at  $\mathfrak{l}$ . 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  $\langle \chi_u, a_u \rangle_u = 0$  since  $\chi$  is unramified at  $u$  and  $a$  is a unit. The reciprocity law would then give us that  $\langle \chi_v, a_v \rangle_v = -\langle \chi_u, a_u \rangle_u = 0$ , and this would not help us in the signature computation. If neither condition (ii) nor (iii) 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:

$$\langle \chi_u, a_u \rangle_u = \langle \chi'_u, a_u \rangle_u + \langle \chi''_u, a_u \rangle_u = 0,$$

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

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,  $\langle \chi, \alpha \rangle_u \neq 0$  and  $\langle \chi, \alpha \rangle_v \neq 0$ , and  $\langle \chi, \alpha \rangle_u + \langle \chi, \alpha \rangle_v = 0$ . 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 the generator of the group  $\mathcal{O}_u^*/\ell \cong \mathbb{Z}_\ell^*/\ell \cong \mathbb{Z}/\ell\mathbb{Z}$ . For  $\chi \in H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ , we call  $\sigma_u(\chi) = \langle \chi, 1 + \ell \rangle_u$  the  $u$ -signature of  $\chi$ .

Let  $g \in \mathbb{Z}$  so that  $g \bmod p$  generates the multiplicative group of  $\mathbb{F}_p$ . Then the class of  $g$  generates  $O_v^*/\ell \cong \mathbb{Z}_p^*/\ell \cong \mathbb{Z}/\ell\mathbb{Z}$ . For  $\chi \in H^1(K, \mathbb{Z}/\ell\mathbb{Z})$ , we call  $\sigma_v(\chi) = \langle \chi, g \rangle_v \neq 0$  the  $v$ -signature of  $\chi$ .

We call the pair  $(\sigma_u(\chi), \sigma_v(\chi))$  the *signature* of  $\chi$ . Since  $\sigma_u(\chi)\sigma_v(\chi)^{-1} \in \mathbb{Z}/\ell\mathbb{Z}$  is the same for  $\chi \in H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ , it depends on  $K_S$  alone and we call it the *ramification signature* of  $K_S$ .

### 3. DL and Signature Computation

In this section we show 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:** Given  $\mathbb{F}_p$  with  $p \equiv 1 \pmod{\ell}$  and  $p \not\equiv 1 \pmod{\ell^2}$ , a generator for its multiplicative group  $g$ , and an element  $a$  to compute  $m \bmod \ell$  where  $a = g^m$  in  $\mathbb{F}_p$ .

**Signature Computation Problem:** Given a real quadratic field  $K$ , primes  $\ell, p$ , places  $u, v$  satisfying the conditions in Proposition 2, to compute the ramification signature of the cyclic extension of degree  $\ell$  over  $K$  which is ramified at  $u, v$  and unramified elsewhere.

**THEOREM 1.** *The problems DL and Signature Computation are random polynomial time equivalent.*

For the proof of the theorem, we first give a random polynomial time reduction from DL to Signature Computation. This part of the proof depends on some heuristic assumption which will be made clear below.

Let  $a = g^m$  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)  $c \leftarrow \frac{a+b}{2}$ ;  $d \leftarrow \frac{a-b}{2}$ . 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) Treat  $d$  as 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 for  $v$  and a place  $u$  of  $K$  over  $\ell$ . (Note that the second condition is satisfied since  $\alpha \equiv a \pmod{v}$  and  $a^{\frac{p-1}{\ell}} \neq 1$ .) Then for  $\chi \in H^1(K, \mathbb{Z}/\ell\mathbb{Z})$  that is ramified at  $u$  and  $v$ , and unramified elsewhere, we have

$$0 = \langle \chi, \alpha \rangle_u + \langle \chi, \alpha \rangle_v .$$

Moreover since  $\alpha^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{v}$ ,  $\alpha$  generates  $O_v^*/\ell$ , so  $\langle \chi, \alpha \rangle_v \neq 0$ , and it follows that  $\langle \chi, \alpha \rangle_u \neq 0$ .

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

$$\langle \chi, \alpha \rangle_v = \langle \chi, g^m \rangle_v = m \langle \chi, g \rangle_v .$$

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  $\alpha \sim^\ell (1 + \ell)^y$ . Note that  $\xi \pmod{\ell^2}$  and hence  $y$  can be computed efficiently, and we have

$$0 = \langle \chi, \alpha \rangle_u = \langle \chi, (1 + \ell)^y \rangle_u = y \langle \chi, 1 + \ell \rangle_u .$$

Hence we have

$$\langle \chi, \alpha \rangle_u + \langle \chi, \alpha \rangle_v = y \langle \chi, 1 + \ell \rangle_u + m \langle \chi, g \rangle_v$$

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.

Next we give a random polynomial time reduction from Signature Computation to DL.

Find  $\alpha$  an unit of  $K$  which is not an  $\ell$ -th power. Then  $0 = \langle \chi, \alpha \rangle_u + \langle \chi, \alpha \rangle_v$  with  $\langle \chi, \alpha \rangle_v$  and  $\langle \chi, \alpha \rangle_u$  both nontrivial.

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,  $\xi \pmod{\ell^2}$  and hence  $y$  can be computed efficiently.

Determine  $a$  such that  $\alpha \equiv a \pmod{v}$  and solve for  $m \pmod{\ell}$  where  $g^m = a \pmod{p}$ . Then  $\alpha \equiv g^m \pmod{v}$ .

For  $\chi \in H^1(K, \mathbb{Z}/\ell\mathbb{Z})$  that is ramified at  $u$  and  $v$ , and unramified elsewhere, we have as before  $\langle \chi, \alpha \rangle_v = \langle \chi, g^m \rangle_v = m \langle \chi, g \rangle_v$ , and  $\langle \chi, \alpha \rangle_u = \langle \chi, (1 + \ell)^y \rangle_u = y \langle \chi, 1 + \ell \rangle_u$ . Hence

$$0 = \langle \chi, \alpha \rangle_u + \langle \chi, \alpha \rangle_v = y \langle \chi, 1 + \ell \rangle_u + m \langle \chi, g \rangle_v$$

from this we can determine the signature  $\sigma_u(\chi)(\sigma_v(\chi))^{-1}$ .

#### 4. Characterization of ramification signature

The computational complexity of signature calculus is an intriguing question, since the class field that is involved can be big and expensive to construct but the signature that is sought is comparatively small. The goal of this section is to provide further characterization of ramification signature.

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,  $\theta_\nu : K_\nu^* \rightarrow G_\nu^{ab}$ , 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  $K(\mu_\ell)$ ,  $\alpha^{\theta_\nu(b)} = (a, b)_\nu \alpha$  where  $\alpha^\ell = a$ , and  $(a, b)_\nu$  denotes the local norm residue symbol (see p. 351 of [CF]).

Now let  $K, \ell, p, u, v, S$  be as in Proposition 2.

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  $g^{\frac{p-1}{\ell}} \equiv 1 \pmod{w}$ .

Let  $M = K_S$  be the cyclic extension corresponding to  $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ . Then  $M(\mu_\ell) = K(\mu_\ell)(A^{\frac{1}{\ell}})$  for some  $A \in K(\mu_\ell)^*$ . Let  $\chi \in H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$  be nontrivial. Then  $\chi$  corresponds to some  $A \in K(\mu_\ell)$  through  $H^1(K(\mu_\ell), \mathbb{Z}/\ell\mathbb{Z}) \cong H^1(K(\mu_\ell), \mu_\ell) \cong K(\mu_\ell)^*/\ell$ , so that for all  $\sigma$  in the absolute Galois group of  $K$ ,  $\chi(\sigma) = i$  iff  $\sigma(A^{\frac{1}{\ell}})/A^{\frac{1}{\ell}} = \zeta^i$ .

LEMMA 1.  $\sigma_u(\chi) = \langle \chi, 1 + \ell \rangle_u = \chi_u(\theta_u(1 + \ell))$  and  $\sigma_v(\chi) = \langle \chi, g \rangle_v = \chi_v(\theta_v(g))$

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

PROPOSITION 3. *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  $m = \sigma_v(\chi) = \langle \chi, g \rangle_v$ , and  $A \sim^\ell \zeta^n$  in  $\mathbb{Q}_\ell(\mu_\ell)^{ur}$  where  $n = \sigma_u(\chi) = \langle \chi, 1 + \ell \rangle_u$ .*

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

$$d = \langle \chi, b \rangle_v = \langle \chi, b \rangle_{v'} = (A, b)_{v'}$$

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

(I) At  $p$ :  $\mathbb{Q}_p^*/\ell = \mu_\ell \times \langle p \rangle / \ell$ . 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  $\mathbb{Q}_p^{ur}$ .

Let  $\chi \in H^1(K, \mathbb{Z}/\ell\mathbb{Z})$

$$\langle \chi, g \rangle_w = (A, g)_w = -(g, A)_w$$

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

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

Therefore,  $(g, A)_w = w(A)$ . Consequently,

$$\langle \chi, g \rangle_v = \langle \chi, g \rangle_w = -(g, A)_w = -w(A).$$

(II) At  $\ell$ : Denote by  $u'$  the place of  $K(\mu_\ell)$  over  $u$ . We have

$$(\ell - 1) \langle \chi, 1 + \ell \rangle_u = \langle \chi, 1 + \ell \rangle_{u'} = (A, 1 + \ell)_{u'}.$$

We verify below that  $(A, 1 + \ell)_{u'} = n$ . Then we can conclude that

$$\sigma_u(\chi) = \langle \chi, 1 + \ell \rangle_u = -n.$$

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 in  $H^1(\mathbb{Q}_\ell(\zeta), \mathbb{Z}/\ell\mathbb{Z})$  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-Schrier 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  $a, b \in \mathbb{Z}/\ell\mathbb{Z}$ . The restriction of  $a\psi + b\varphi$  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  $M'(\zeta) = \mathbb{Q}_\ell(\zeta)(\rho^{\frac{1}{\ell}})$ . Note

that  $\rho \sim^\ell \zeta^i$  in  $\mathbb{Q}_\ell(\zeta)^{ur}$  as  $\beta^{\frac{1}{i}} \in \mathbb{Q}_\ell(\zeta)^{ur}$ .

Since  $\varphi$  is unramified and  $1 + \ell$  is a unit,

$$\langle \varphi, 1 + \ell \rangle = 0.$$

So

$$\langle a\psi + b\varphi, 1 + \ell \rangle = a \langle \psi, 1 + \ell \rangle = a(\zeta, 1 + \ell).$$

Since  $1 + \ell = \eta_{\ell-1}\xi$  with  $\xi \equiv 1 \pmod{\lambda^\ell}$ ,

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

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

([CF] p.354 Our symbol is written additively.)

Therefore,  $\langle a\psi + b\varphi, 1 + \ell \rangle = a$ .

The restriction of  $\chi_u$  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  $H^1(\mathbb{Q}_\ell, \mathbb{Z}/\ell\mathbb{Z})$ . From the discussion above,  $A \sim^\ell \zeta^a \beta^b$  under the identification of  $K(\mu_\ell)_{u'}$  with  $\mathbb{Q}_\ell(\mu_\ell)$ , and  $A \sim^\ell \zeta^a$  in  $\mathbb{Q}_\ell(\mu_\ell)^{ur}$ .

We have

$$(\ell - 1) \langle \chi, 1 + \ell \rangle_u = \langle \chi, 1 + \ell \rangle_{u'} = \langle a\psi + b\varphi, 1 + \ell \rangle = a.$$

So

$$n = \sigma_u(\chi) = \langle \chi, 1 + \ell \rangle_u = -a$$

where  $A \sim^\ell \zeta^a$  in  $\mathbb{Q}_\ell(\mu_\ell)^{ur}$ .

## References

- [CF] J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press 1967
- [F] G. Frey, *Applications of arithmetical geometry to cryptographic constructions*, In Proceedings of the Fifth International Conference on Finite Fields and Applications. Springer Verlag, page 128-161, 1999; Preprint also available at <http://www.exp-math.uni-essen.de/zahlentheorie/preprints/Index.html>.

- [FR] 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):865–874, 1994.
- [HKT] M.-D. Huang, K. L. Kueh, and K.-S. Tan *Lifting elliptic curves and solving the elliptic curve discrete logarithm problem* In ANTS, Lecture Notes in Computer Science, Volume 1838 Springer-Verlag, 2000.
- [HR1] M.-D. Huang and W. Raskind, *Global methods for the discrete logarithm problem II: the multiplicative group case*, preprint 2004
- [HR2] M.-D. Huang and W. Raskind, *Global methods for the discrete logarithm problem III: the elliptic curve case*, in preparation
- [JKSST] M.J. Jacobson, N. Koblitz, J.H. Silverman, A. Stein, and E. Teske. Analysis of the Xedni calculus attack. Design, Codes and Cryptography, 20 41-64, 2000
- [K] N. Koblitz *Elliptic curve cryptosystems* Mathematics of Computation, 48 203-209, 1987.
- [KMV] N. Koblitz, A. Menezes and S. Vanstone *The state of elliptic curve cryptography*, Design, Codes and Cryptography, 19, 173-193 (2000)
- [Ma] B. Mazur, *Notes on the étale cohomology of number fields*, Ann. Sci. École Normale Supérieure 6 (1973) 521-556
- [Mc] K. McCurley, *The discrete logarithm problem*, in Cryptology and Computational Number Theory, C. Pomerance, editor, Proceedings of Symposia in Applied Mathematics, Volume 42, 49-74, 1990
- [Mill] V. Miller *Uses of elliptic curves in cryptography*, In Advances in Cryptology: Proceedings of Crypto 85, Lecture Notes in Computer Science, volume 218, 417-426. Springer-Verlag, 1985.
- [MET] J.S. Milne, *Étale Cohomology*, Princeton Mathematical Series, Volume 33, Princeton University Press 1980
- [MAD] J.S. Milne, *Arithmetic Duality Theorems*, Perspectives in Mathematics, Volume 1., Academic Press 1986
- [N] K. Nguyen, Thesis, Universität Essen, 2001
- [R] W. Raskind, Abelian class field theory of arithmetic schemes, in *K-Theory and Algebraic Geometry: Connections with Quadratic Forms and Division Algebras*, B. Jacob and A. Rosenberg editors, Proceedings of Symposia in Pure Mathematics, Volume 58, American Mathematical Society 1995

- [SWD] O. Schirokauer, D. Weber, and T. Denny *Discrete logarithms: The effectiveness of the index calculus method* In ANTS II, volume 1122 of Lecture Notes in Computer Science. Springer-Verlag, 1996.
- [Se] J.-P. Serre, *Corps Locaux*, Paris Hermann 1962; English translation: *Local Fields*, Graduate Texts in Mathematics, Volume 67, Springer Verlag, Heidelberg-New York, 1979

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF SOUTHERN CALIFORNIA,  
LOS ANGELES, CA 90089-0781, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF  
SOUTHERN CALIFORNIA, LOS ANGELES, CA 90089-2532, USA  
*E-mail address:* `huang@pollux.usc.edu`, `raskind@math.usc.edu`