

Signature Calculus and the Discrete Logarithm Problem for Elliptic Curves (Preliminary Version)

Ming-Deh Huang and Wayne Raskind

Introduction

This is the third 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 [HR2], we used signature calculus to study the DLP for the group \mathbb{F}_p^* of invertible elements of the finite prime field, \mathbb{F}_p . In this paper, we use the method to study the DLP for the group $\tilde{E}(\mathbb{F}_p)$ of rational points of an elliptic curve \tilde{E} defined over \mathbb{F}_p . Recall that in this context, the DLP is formulated as follows: let $\#\tilde{E}(\mathbb{F}_p) = \ell$ be prime and Q a point in $\tilde{E}(\mathbb{F}_p)$ of order ℓ . Suppose we are given another element R . Then the DLP is to determine n so that $R = nQ$ in a computationally efficient way. The expected computational complexity of this problem is the basis of elliptic curve cryptography.

We approach the discrete logarithm problem for $\tilde{E}(\mathbb{F}_p)$ by lifting the two elements whose relation we seek to compute to $E(K)$ where E is an elliptic curve over an algebraic number field K , and use a suitable principal homogeneous space under E over K to “test” the lifting, and derive relations by using the reciprocity law. We then prove the random polynomial time equivalence of the elliptic curve discrete logarithm problem with the problem of computing the ratios of “signatures” of

certain principal homogeneous spaces.

The unifying approach based on global duality provides an ideal setting to investigate the feasibility of the index calculus method for discrete logarithm problems. In [HR1] we show that in this setting, index calculus method arises quite naturally for the discrete-log problem in the multiplicative case and the corresponding signature computation problem. We will show that, in contrast, a similar method cannot be fashioned for the elliptic curve case, and that the success in one case and the lack thereof in the other is due to the difference of nature in the pairings involved.

Although we show that the testing principal homogeneous spaces exist, it remains an interesting question how they can be explicitly constructed. A partial solution for the construction will be presented in the Appendix.

1. The Global Framework for ECDL

Let E be an elliptic curve over a number field 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 can write an affine equation for E in Weierstrass form

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

where a and b are in the ring of integers K with $4a^3 + 27b^2 \neq 0$. This last condition ensures that the polynomial $x^3 + ax + b$ has no double roots. If \mathfrak{p} is a prime ideal of the ring of integers of K with residue field \mathbb{F} of characteristic at least 5 and \mathfrak{p} does not divide $4a^3 + 27b^2$, then we get an elliptic curve \tilde{E} over \mathbb{F} . We call E a *lifting* of \tilde{E} to K . We denote by $\tilde{E}(\mathbb{F})$ the set of solutions of this equation with x and y in \mathbb{F} , together with a point “at infinity” and by $E(K)$ the set of rational points of E over K . Recall that a principal homogeneous space under E is a smooth curve F together with a simply transitive algebraic group action of E on F . The isomorphism classes of such principal homogeneous spaces are classified by the group $H^1(G, E(\bar{K}))$, where $G = \text{Gal}(\bar{K}/K)$. We also write $H^1(G, E(\bar{K}))$ as $H^1(K, E)$. 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 any principal homogeneous space becomes isomorphic to E over a finite extension of

K . Let $\alpha \in H^1(K, E)$ and $Q \in E(K)$. Let v a place of K , and K_v the completion of K at v . Then we consider the pairings $\langle \alpha, Q \rangle \in Br(K)$ and $\langle \alpha_v, Q_v \rangle_v \in Br(K_v) \cong \mathbb{Q}/\mathbb{Z}$ (see [HR1] for details). We will be interested in the situation where $\alpha \in H^1(K, E)[\ell]$, in which case we have the following commutative diagram:

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

In the case of the local field K_v , the pairing is perfect. For $\psi \in H^1(K_v, E)[\ell]$ and $\beta \in E(K_v)$, let $\langle \psi, \beta \rangle \in \mathbb{Z}/\ell\mathbb{Z}$ denote the result of the pairing on β and ψ , where we identify $Br(K_v)[\ell]$ with $\mathbb{Z}/\ell\mathbb{Z}$ by the invariant map.

For $\chi \in H^1(K, \mathbb{Z}/\ell\mathbb{Z})$ and $\alpha \in K^*$, let $\langle \chi, \alpha \rangle_v = \langle \chi_v, \alpha_v \rangle$.

The fundamental sequence

$$0 \rightarrow Br(K) \rightarrow \bigoplus_v Br(K_v) \xrightarrow{\Sigma_v \text{inv}_v} \mathbb{Q}/\mathbb{Z} \rightarrow 0$$

and the commutative diagram above imply that for $\chi \in H^1(K, E)[\ell]$ and $\alpha \in E(K)$,

$$0 = \sum_v \langle \chi, \alpha \rangle_v.$$

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 ℓ . 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 ℓ . 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

From

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

we get by the snake lemma

$$\begin{aligned} 0 \rightarrow E_1(K_v)[\ell] \rightarrow E(K_v)[\ell] \rightarrow \tilde{E}(k)[\ell] \rightarrow E_1(K_v)/\ell E_1(K_v) \\ \rightarrow E(K_v)/\ell E(K_v) \rightarrow \tilde{E}(k)/\ell \tilde{E}(k) \rightarrow 0. \end{aligned}$$

Suppose ℓ 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 $E(K_v)/\ell E(K_v) \cong E_1(K_v)/\ell E_1(K_v)$.

Suppose $v \nmid \ell$. Then $E_1(K_v)/\ell E_1(K_v) = 0$, hence $E(K_v)/\ell E(K_v) \cong \tilde{E}(k)/\ell \tilde{E}(k)$.

Hence if ℓ does not divide the order of $\tilde{E}(k)$ and $v \nmid \ell$, then $E(K_v)/\ell E(K_v) = 0$, and by virtue of the local duality, $H^1(K_v, E)[\ell] = 0$.

Suppose $|\tilde{E}(k)|$ is divisible by ℓ but not ℓ^2 , then $\tilde{E}(k)/\ell \tilde{E}(k) \cong \mathbb{Z}/\ell\mathbb{Z}$. Suppose moreover that $v \nmid \ell$. Then $E(K_v)/\ell E(K_v) \cong \tilde{E}(k)/\ell \tilde{E}(k) \cong \mathbb{Z}/\ell\mathbb{Z}$, and by virtue of the local duality, $H^1(K_v, E)[\ell] = \mathbb{Z}/\ell\mathbb{Z}$.

Suppose $v|\ell$ and $K_v \cong \mathbb{Q}_\ell$, 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 ℓ , 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 virtue of local duality.

This completes the proof of the lemma.

2. Principal Homogeneous Spaces ramified over p and ℓ

Throughout this section, let p, ℓ be odd, rational primes. Let K/\mathbb{Q} be a real quadratic extension. Let $X = \text{Spec}(\mathcal{O}_K)$. Let Σ be the set of all places at which E has bad reduction, together with all the archimedean places. Let \mathcal{E} be a smooth proper model of E over the open subset $X - \Sigma$.

PROPOSITION 1. *Let S be a finite set of places of K containing all bad reduction places of E and the places above ℓ . Then if $\text{III}(E)\{\ell\} = 0$, we have the exact sequence:*

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

Proof: Consider the Cassels-Tate exact sequence

$$E(K)^{(\ell)} \rightarrow \prod_{v \in S} E(K_v)^{(\ell)} \rightarrow H^1(\mathcal{O}_S, \mathcal{E})\{\ell\}^* \rightarrow \text{III}(E)\{\ell\} \rightarrow 0.$$

LEMMA 2. *Let B be a torsion abelian group. Then we have*

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

and

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

Proof:

Consider the tautological exact sequence:

$$0 \rightarrow B[\ell] \rightarrow B \xrightarrow{\ell} B \rightarrow B/\ell B \rightarrow 0.$$

Since $*$ is an exact functor on the category of locally compact abelian groups, we get the exact sequence:

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

This completes the proof of the lemma.

The proposition follows from the lemma, the assumption that $\text{III}(E)\{\ell\} = 0$ and the Cassels-Tate sequence above.

For the remainder of this section we assume that p and ℓ split in K , and E has good reduction at p and ℓ , with $\#\tilde{E}(\mathbb{F}_p) = \ell$ and $\ell \neq \#\tilde{E}(\mathbb{F}_\ell)$. Moreover we assume that ℓ is sufficiently large so that $E(L)[\ell]$ is trivial for all quadratic extension L over \mathbb{Q} . Finally, we assume that the discriminant of E is small compared to ℓ , which implies that for a bad reduction place v not dividing ℓ , we have $E(K_v)/\ell = 0$. To see this we note that the discriminant being small implies that the places of bad reduction do not divide ℓ , and ℓ does not divide the order of $\tilde{E}(k)$, where k is the residue field of K_v , and it follows from the argument in Lemma 1 that $E_0(K_v)/\ell E_0(K_v) = 0$. Since the order of the j -invariant of E at v is not divisible by ℓ and ℓ is greater than 3, the cardinality of $E(K_v)/E_0(K_v)$ is not divisible by ℓ (see for example Cor 9.2, p. 362, of [Si]). Hence $E(K_v)/\ell = 0$.

PROPOSITION 2. *Let S be a finite set of places of K containing all bad reduction places of E and the places above ℓ , but no other places away from ℓ and p . Suppose*

- (1) $\text{III}(E)\{\ell\} = 0$;
(2) the map $E(K)/\ell \rightarrow E(K_u)/\ell \oplus E(K_{u'})/\ell$ is an isomorphism, where u and u' are the two places of K over ℓ .

Then the \mathbb{F}_ℓ -dimension of $H^1(\mathcal{O}_S, \mathcal{E})[\ell]$ equals $n(S) - 2$ where $n(S)$ is the number of finite places in $S - \Sigma$.

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

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

by Proposition 1. 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 map

$$E(K)/\ell \rightarrow E(K_u)/\ell \oplus E(K_{u'})/\ell \cong \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$$

is an isomorphism, it follows that the image of the map

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

is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$. Hence the \mathbb{F}_ℓ -dimension of $H^1(\mathcal{O}_S, \mathcal{E})[\ell]$ equals $n(S) - 2$.

PROPOSITION 3. *Let S be the set consisting of all bad reduction places of E , together with the two places u and u' over ℓ , and one place v over p . Suppose*

- (1) $\text{III}(E)\{\ell\} = 0$;
(2) the map $E(K)/\ell \rightarrow E(K_u)/\ell \oplus E(K_{u'})/\ell$ is an isomorphism.

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

Proof Suppose u, u' are the places over ℓ , v, v' the places over p . Let $R = \Sigma \cup \{u, u'\}$ and $T = \Sigma \cup \{u, u', v\}$. Then from Proposition 2 we know that $H^1(\mathcal{O}_R, \mathcal{E})[\ell]$ has dimension zero and $H^1(\mathcal{O}_T, \mathcal{E})[\ell]$ has dimension one. So there exists $\chi \in H^1(\mathcal{O}_T, \mathcal{E})[\ell] - H^1(\mathcal{O}_R, \mathcal{E})[\ell]$ and χ must be ramified at v .

For $w = u, u', v$, let $R_w \in E(K_w) - \ell E(K_w)$, so that the class of R_w generates $E(K_w)/\ell$. Then Proposition 3 implies that $\langle \chi, R_v \rangle_v \neq 0$ for any nontrivial $\chi \in H^1(\mathcal{O}_S, \mathcal{E})[\ell]$. Moreover, $(\frac{\langle \chi, R_u \rangle_u}{\langle \chi, R_v \rangle_v}, \frac{\langle \chi, R_{u'} \rangle_{u'}}{\langle \chi, R_v \rangle_v})$ is the same for all such χ . We call this pair the *signature* of $H^1(\mathcal{O}_S, \mathcal{E})[\ell]$ with

respect to R_u , $R_{u'}$ and R_v .

We remark that in the proposition above the assumption that the map $E(K)/\ell \rightarrow E(K_u)/\ell \oplus E(K_{u'})/\ell$ is an isomorphism can be replaced by the assumption that the image of $E(K)/\ell$ in $E(K_u)/\ell \oplus E(K_{u'})/\ell$ and in $E(K_v)/\ell \oplus E(K_u)/\ell \oplus E(K_{u'})/\ell$ are both of \mathbb{F}_ℓ -dimension two.

Suppose in addition to the map $E(K)/\ell \rightarrow E(K_u)/\ell \oplus E(K_{u'})/\ell$ being an isomorphism, we assume that the map $E(K)/\ell \rightarrow E(K_v)/\ell$ is nontrivial. In this case we may form R_w 's as follows. Let $Q, R \in E(K)$ so that their classes generate $E(K)/\ell$. Suppose without loss of generality that the class of Q is nontrivial in $E(K_u)/\ell$ and the class of R is nontrivial in $E(K_{u'})/\ell$. As $E(K)/\ell \rightarrow E(K_v)/\ell$ is nontrivial, the class of either Q or R is nontrivial in $E(K_v)/\ell$. Suppose without loss of generality the class of Q is nontrivial in $E(K_v)/\ell$. Then we may take $R_v = Q$, $R_u = Q$ and $R_{u'} = R$.

3. ECDL and Signature Computation

In this section we show that the elliptic curve discrete logarithm problem is random polynomial time equivalent to computing the signature of homogeneous spaces with prescribed ramification as described in Proposition 3.

ECDL: Given an elliptic curve \tilde{E} defined over a prime finite field \mathbb{F}_p with $\#E(\mathbb{F}_p) = \ell$ being prime, and two non-zero points \tilde{Q} and \tilde{R} in $E(\mathbb{F}_p)$, to determine m so that $\tilde{R} = m\tilde{Q}$.

Homogeneous Space Signature Computation: We are given an elliptic curve E defined over \mathbb{Q} , a real quadratic field K , primes ℓ and p , places u and u' over ℓ and a place v over p . We assume the conditions in Proposition 3 are satisfied, hence we are also given $Q, R \in E(K)$ such that $Q \not\equiv 0 \pmod{\ell E(K_w)}$ for $w = u, v$ and $R \not\equiv 0 \pmod{\ell E(K_{u'})}$. For the set S consisting of u, u', v and all places of bad reduction of E , we are to compute the signature of $H^1(\mathcal{O}_S, \mathcal{E})[\ell]$ with respect to R_w , $w = u, u', v$, where $R_w \in E(K)$ and R_w generates $E(K_w)/\ell E(K_w)$. (One convenient choice would be $R_v = Q$, $R_u = Q$ and $R_{u'} = R$.)

THEOREM 1. *The problems ECDL and Homogeneous Space Signature Computation are random polynomial time equivalent.*

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

Given \tilde{E}/\mathbb{F}_p where $\tilde{E}(\mathbb{F}_p)[\ell] = \langle \tilde{Q} \rangle$, and \tilde{R} , to compute m so that $\tilde{R} = m\tilde{Q}$.

1. Construct E/\mathbb{Q} with $Q \in E(\mathbb{Q})$ such that $\tilde{Q} = Q \pmod{p}$. This can be done as follows. Suppose \tilde{E} is specified by an affine equation $y^2 = x^3 + \bar{a}x + \bar{b}$ where $\bar{a} = a \pmod{p}$, $\bar{b} = b \pmod{p}$ with $0 \leq a, b < p$ and $\tilde{Q} = (u \pmod{p}, v \pmod{p})$ with $0 < u, v < p$. Choose a random integer r , $0 \leq r < p$, and let $Q = (u, v + rp)$. Let $b_r = (v + rp)^2 - (u^3 + au)$. Then $Q \in E_r(\mathbb{Q})$ where E_r is the elliptic curve with the affine equation $y^2 = x^3 + ax + b_r$. Set $E = E_r$. The point Q cannot be torsion for otherwise it would have to be in $E(\mathbb{Q})[\ell]$, which has no non-zero point since ℓ is big. The height of Q is far smaller than that of a point in $\ell E(\mathbb{Q})$, so Q is not in $\ell E(\mathbb{Q})$. 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 ℓ and that $|\tilde{E}(\mathbb{F}_\ell)|$ is not divisible by ℓ . 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 ℓ both split. This can be done as follows. Suppose E is defined by the affine equation $y^2 = x^3 + ax + c$. Suppose $\tilde{R} = (\mu \pmod{p}, \nu \pmod{p})$ with $0 < \mu, \nu < p$. Choose a random positive integer $r < p$. Set $\mu_r = \mu + rp$. Let β be a root of $y^2 = \mu_r^3 + a\mu_r + c$. Then (μ_r, β) 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 ℓ splits in K and that the images of R and Q in $E(K_u)/\ell \oplus E(K_{u'})/\ell$ are independent; otherwise repeat the above steps with a different r until a suitable K is found. Say the class of Q is nontrivial in $E(K_u)/\ell$ and the class of R is nontrivial in $E(K_{u'})/\ell$.

4. Compute the signature (α, β) of $H^1(\mathcal{O}_S, \mathcal{E})[\ell]$ with respect to $R_v = Q$, $R_u = Q$ and $R_{u'} = R$, where S is the set consisting of u, u', v and all places of bad reduction of E . Then for all nontrivial $\chi \in H^1(\mathcal{O}_S, \mathcal{E})[\ell]$,

$$\alpha = \frac{\langle \chi, Q \rangle_u}{\langle \chi, Q \rangle_v} \text{ and } \beta = \frac{\langle \chi, R \rangle_{u'}}{\langle \chi, Q \rangle_v}.$$

5. Identify K_u with \mathbb{Q}_ℓ and compute n so that $R \equiv nQ \pmod{\ell E(K_u)}$ as follows. Compute $d = |\tilde{E}(\mathbb{F}_\ell)|$. Observe that dQ and dR are both in $E_1(\mathbb{Q}_\ell)$. Compute n such that $n(dQ) \equiv (dR) \pmod{\ell}$ in $E_1(\mathbb{Q}_\ell)$. Then $d(nQ - R) = \ell Z$ for some $Z \in E_1(\mathbb{Q}_\ell)$. Since d is not divisible by ℓ , $d^{-1} \in \mathbb{Z}_\ell$, so $nQ - R = d^{-1}\ell Z = \ell(d^{-1}Z) \in \ell E(\mathbb{Q}_\ell)$.

6. Now

$$\begin{aligned} 0 &= \sum_{w \in \{v, u, u'\}} \langle \chi, R \rangle_w \\ &= m \langle \chi, Q \rangle_v + n \langle \chi, Q \rangle_u + \langle \chi, R \rangle_{u'}. \end{aligned}$$

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

We make the heuristic assumption that it is likely for E and K to satisfy the conditions in Proposition 3. Note that by construction $E(Q)$ is of rank at least one. The points Q and R are likely to be integrally independent in $E(K)$ as they both have small height by construction. So $E(K)$ is likely to be of rank at least two and we make the heuristic assumption that with nontrivial probability its rank is exactly two. Moreover, since $Q \in E(\mathbb{Q})$ and $R \in E(K) - E(\mathbb{Q})$, the images of Q and R are likely to be independent in $E(K_u)/\ell \oplus E(K_{u'})/\ell$, heuristically speaking.

Next we give a random polynomial time reduction from Homogeneous Space Signature Computation to ECDL.

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

$$\begin{aligned} \langle \chi, Q \rangle_v + \langle \chi, Q \rangle_u + \langle \chi, Q \rangle_{u'} &= 0, \\ \langle \chi, R \rangle_v + \langle \chi, R \rangle_u + \langle \chi, R \rangle_{u'} &= 0. \end{aligned}$$

Suppose $Q = a_w R_w \pmod{\ell E(K_w)}$ and $R = b_w R_w \pmod{\ell E(K_w)}$ for $w = u, u', v$. Note that from Lemma 1, a_v and b_v can be computed by solving ECDL on the reduction of E modulo v . On the other hand a_w, b_w for $w = u, u'$, can be computed in a manner as described in Step 5 above.

Then we get

$$\begin{aligned} a_v \langle \chi, R_v \rangle_v + a_u \langle \chi, R_u \rangle_u + a_{u'} \langle \chi, R_{u'} \rangle_{u'} &= 0, \\ b_v \langle \chi, R_v \rangle_v + b_u \langle \chi, R_u \rangle_u + b_{u'} \langle \chi, R_{u'} \rangle_{u'} &= 0 \end{aligned}$$

Condition (2) of Proposition 2 implies that the two relations above are linearly independent. From these we can compute the signature of χ ; that is $(\frac{\langle \chi, R_u \rangle_u}{\langle \chi, R_v \rangle_v}, \frac{\langle \chi, R_{u'} \rangle_{u'}}{\langle \chi, R_v \rangle_v})$.

4. Feasibility of Index Calculus

In reducing the discrete-log problems to the signature computations, the basic idea is to lift elements from a finite field \mathbb{F}_p to a global field K where discrete logarithms are preserved at a place over p , then pair the elements with testing Dirichlet characters in the multiplicative case [HR1], or principal homogeneous spaces in the elliptic curve case. The reciprocity laws then allow us to distribute information of the discrete logarithms among a set of places. This set of places depend on the choice of a Dirichlet character (resp. homogeneous space) and the manner of lifting. In this context, the classical index calculus method emerges in this context as the result of one particular choice of Dirichlet character and method of lifting [HR1]. We note that one important reason why index calculus is viable in the multiplicative case is due to the fact that locally unramified Dirichlet characters are nontrivially paired with non-units. This makes it possible for small primes to play a role in forming relations among values of local pairings. For the elliptic curve case, pairing a principal homogeneous space χ and a global point α yields similarly a relation:

$$0 = \sum_v \langle \chi, \alpha \rangle_v .$$

In this case, a locally unramified principal homogeneous space at a good reduction place is simply trivial. 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 ℓ divides $\#\tilde{E}(\mathbb{F}_v)$. Since $\#\tilde{E}(\mathbb{F}_v)$ is of the 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 2 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 the index calculus method is lacking in the case of elliptic curve discrete logarithm problem.

References

- [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 duality and discrete logarithm problems: a general framework*, preprint 2006
- [HR2] M.-D. Huang and W. Raskind, *Global duality and the discrete logarithm problem for the multiplicative group*, preprint 2006
- [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, Univesität Essen, 2001
- [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.
- [S] J.-P. Serre, *Local Fields*, *Graduate Texts in Mathematics*, Volume 67, Springer Verlag 1979.
- [Si] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, *Graduate Texts in Mathematics*, Volume 151, Springer Verlag 1994.

Appendix: Concrete construction of the testing principal homogeneous spaces

In the following lemma, K can be any number field where our lifted elliptic curve E is defined, $G = G(\bar{K}/K)$, H is the subgroup of G corresponding to $K(E[l])/K$, so H is normal in G and $G(K(E[l])/K)$ is isomorphic to G/H .

- LEMMA 3. (1) *Every 1-cocycle of G with values in $E[l]$ representing an element of $H^1(K, E[l])$ induces a G -homomorphism from H to $E[l]$.*
- (2) *Every G -homomorphism from H to $E[l]$ determines a Kummer extension over $K(E[l])$ of degree 0 or l or l^2 which is Galois over K . Moreover it gives rise to some (non-unique) element of $H^1(K, E[l])$, if $G(K(E[l])/K)$ is of order prime to l .*

Proof (1) Let F be a 1-cocycle of $H^1(K, E[l])$. Then for all $\sigma, \tau \in G$, $F(\sigma\tau) = \sigma F(\tau) + F(\sigma)$. Suppose $\sigma, \tau \in H$. Then $\sigma F(\tau) = F(\tau)$ since $F(\tau) \in E[l]$. Hence F is a group homomorphism when restricted to H . For $\sigma \in H$ and $\tau \in G$, let $\sigma^\tau = \tau\sigma\tau^{-1}$, then $\sigma^\tau\tau = \tau\sigma$, so $F(\sigma^\tau\tau) = F(\tau\sigma)$. Now,

$$\begin{aligned} F(\sigma^\tau\tau) &= \sigma^\tau F(\tau) + F(\sigma^\tau) = F(\tau) + F(\sigma^\tau) \\ F(\tau\sigma) &= \tau F(\sigma) + F(\tau). \end{aligned}$$

Hence $F(\sigma^\tau) = \tau F(\sigma)$, and it follows that F is a G -homomorphism when restricted to H .

(2) Let $H \rightarrow E[l]$ be a G -homomorphism. Let H_0 be the kernel of f . Then H_0 is G -invariant, hence the fixed field L of H_0 is Galois over K . Moreover as $G(L/K(E[l])) = H/H_0$ injects into $E[l]$ and $K(E[l])$ contains all l -roots of unity, the extension $L/K(E[l])$ must be Kummer of degree 0 or l or l^2 .

Let $\bar{G} = G(L/K) = G/H_0$ and $\bar{H} = G(L/K(E[l])) = H/H_0$. We can regard f as an \bar{G} -homomorphism from \bar{H} to $E[l]$. Since \bar{G} is an extension of \bar{H} by \bar{G}/\bar{H} , and the orders of \bar{H} and \bar{G}/\bar{H} are relatively prime, it follows from Schur-Zassenhaus Lemma that \bar{G} is a semi-direct product of \bar{H} and \bar{G}/\bar{H} . Hence there is a subgroup A of \bar{G} isomorphic to \bar{G}/\bar{H} , such that $A \cap \bar{H} = \{1\}$ and $\bar{G} = \bar{H}A$. We extend f to \bar{G} by setting

$f(\tau) = 0$ for all $\tau \in A$ and then for all $g = \sigma\tau \in G$ with $\sigma \in \bar{H}$ and $\tau \in A$, setting $f(\sigma\tau) = f(\sigma)$. Note that $f(g)$ is well-defined since σ and τ are uniquely determined by g . To check that the 1-cocycle condition is satisfied, suppose $\sigma_i \in \bar{H}$ and $\tau_i \in A$ for $i = 1, 2$. Then since

$$(\sigma_1\tau_1)(\sigma_2\tau_2) = \sigma_1\sigma_2^{\tau_1}\tau_1\tau_2,$$

$$f((\sigma_1\tau_1)(\sigma_2\tau_2)) = f(\sigma_1\sigma_2^{\tau_1}\tau_1\tau_2) = f(\sigma_1\sigma_2^{\tau_1}).$$

Since f restricts to a \bar{G} -homomorphism on \bar{H} ,

$$f(\sigma_1\sigma_2^{\tau_1}) = f(\sigma_1) + f(\sigma_2^{\tau_1}) = f(\sigma_1) + \tau_1 f(\sigma_2).$$

On the other hand, $\sigma_1\tau_1 f(\sigma_2\tau_2) = \tau_1 f(\sigma_2)$ and $f(\sigma_1\tau_1) = f(\sigma_1)$, so

$$\sigma_1\tau_1 f(\sigma_2\tau_2) + f(\sigma_1\tau_1) = f(\sigma_1) + \tau_1 f(\sigma_2).$$

Therefore

$$f((\sigma_1\tau_1)(\sigma_2\tau_2)) = \sigma_1\tau_1 f(\sigma_2\tau_2) + f(\sigma_1\tau_1).$$

That is f is a 1-cocycle for $H^1(\bar{G}, E[l])$. Finally, f yields an element of $H^1(K, E[l])$ by the inflation map.

The recipe First we list the basic ingredients for constructing an element in $H^1(K, E[l])$.

(1) Some $P \in E[l]$ and $\pi \in K(P)$ so that P reduces modulo a p to some point in $E(\mathbb{F}_p)$ and there is a 1-1 correspondence between the conjugates of π and the conjugates of P . That is,

$$\begin{aligned} \{\sigma\pi | \sigma \in G\} &= \{\pi_1, \dots, \pi_m\} \\ \{\sigma P | \sigma \in G\} &= \{P_1, \dots, P_m\} \end{aligned}$$

with $\pi = \pi_1$ and $P = P_1$, and for $\sigma \in G = G(\bar{K}/K)$,

$$\sigma\pi_i = \pi_j \Leftrightarrow \sigma P_i = P_j.$$

(2) A basis S and T for $E[l]$ with respect to which $E[l]$ is identified with \mathbb{F}_l^2 and every $\tau \in G(K(E[l])/K)$ is represented by an element in $GL_2(\mathbb{F}_l)$.

A map

$$\begin{array}{ccc} \mathbb{F}_l^2 & \xrightarrow{\varphi} & \mathbb{F}_l^2 & \text{s.t.} \\ \lambda & \rightarrow & \varphi(\lambda) & \\ \downarrow \tau & & \uparrow \tau^t & \\ \mu & \rightarrow & \varphi(\mu) & \end{array}$$

Construction Suppose with respect to the chosen basis, $\varphi(P_i)$ is represented by $(e_i, f_i) \in \mathbb{F}_l^2$. Set

$$\begin{aligned} A_1 &= \prod_{i=1}^m \pi_i^{e_i} \\ A_2 &= \prod_{i=1}^m \pi_i^{f_i} \end{aligned}$$

Let α_1, α_2 and L be such that

$$\begin{aligned} \alpha_1^l &= A_1 \\ \alpha_2^l &= A_2 \\ L &= K(E[l])(\alpha_1, \alpha_2) \end{aligned}$$

Fix some $\zeta \in \mu_l$. For all $\sigma \in H = G(L/K(E[l]))$, if

$$\begin{aligned} \sigma(\alpha_1) &= \alpha_1 \zeta^i \\ \sigma(\alpha_2) &= \alpha_2 \zeta^j \end{aligned}$$

then set $f(\sigma) = jS - iT$.

Claim L/K is Galois and f is a G -homomorphism from H to $E[l]$ where $G = G(L/K)$. Consequently, f gives rise to an element of $H^1(K, E[l])$ in the manner discussed in the previous lemma.

The Claim is justified below. First we show that L/K is Galois. Let $\tau \in G = G(\bar{K}/K)$. When restricted to $K(E[l])$, τ is represented by some matrix $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ with respect to the chosen basis S and T for $E[l]$. We will denote this matrix also by τ and hence its transpose $\tau^t = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

$$\begin{aligned} \tau A_1 &= \prod_{i=1}^m (\tau \pi_i)^{e_i} \\ \tau A_2 &= \prod_{i=1}^m (\tau \pi_i)^{f_i} \end{aligned}$$

Suppose $\tau P_i = P_j$. Then from (2) (of Recipe),

$$\tau^t \begin{pmatrix} e_j \\ f_j \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e_j \\ f_j \end{pmatrix} = \begin{pmatrix} e_i \\ f_i \end{pmatrix} \pmod{l}.$$

So

$$\begin{aligned} (\tau \pi_i)^{e_i} &= \pi_j^{e_i} = \pi_j^{ae_j + bf_j + lx}, \text{ for some } x, \\ (\tau \pi_i)^{f_i} &= \pi_j^{f_i} = \pi_j^{ce_j + df_j + ly}, \text{ for some } y \end{aligned}$$

It follows that

$$\begin{aligned} \tau A_1 &= A_1^a A_2^b u^l \\ \tau A_2 &= A_1^c A_2^d v^l \end{aligned}$$

for some $u, v \in K(E[l])$, and that

$$\tau(\alpha_1^l) = (\alpha_1^a \alpha_2^b u)^l,$$

therefore,

$$\tau \alpha_1 = \alpha_1^a \alpha_2^b u \zeta_1,$$

for some $\zeta_1 \in \mu_l$. Similarly,

$$\tau \alpha_2 = \alpha_1^c \alpha_2^d v \zeta_2,$$

for some $\zeta_2 \in \mu_l$. Hence $\tau \alpha_1, \tau \alpha_2 \in L$, so L/K is Galois.

It is clear from the construction that f is a group homomorphism from $G(L/K(E[l]))$ to $E[l]$. Now we verify that for $\sigma \in G(L/K(E[l]))$ and $\tau \in G(K(E[l])/K)$, $f(\sigma^\tau) = \tau f(\sigma)$.

Let the inverse of the matrix for τ be

$$\begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} = \delta^{-1} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

where δ is the determinant of the matrix for τ .

Then by the argument above,

$$\tau^{-1} \alpha_1 = \alpha_1^{a'} \alpha_2^{b'} u' \zeta_3$$

for some $u' \in K(E[l])$ and $\zeta_3 \in \mu_l$.

Suppose $\sigma \alpha_1 = \alpha_1^i$ and $\sigma \alpha_2 = \alpha_2^j$. Then

$$\tau \sigma \tau^{-1}(\alpha_1) = \tau \sigma(\alpha_1^{a'} \alpha_2^{b'} u' \zeta_3) = \tau(\alpha_1^{a'} \alpha_2^{b'} u' \zeta_3 \zeta^{ia' + jb'}) = \alpha_1 \tau(\zeta^{ia' + jb'}).$$

Note that

$$\tau(e_l(S, T)) = e_l(\tau S, \tau T) = e_l(aS + bT, cS + dT) = e_l(S, T)^\delta.$$

Hence $\tau\zeta = \zeta^\delta$, and so

$$\sigma^\tau(\alpha_1) = \alpha_1 \zeta^{\delta(ia' + jb')}.$$

Similarly,

$$\sigma^\tau(\alpha_2) = \alpha_1 \zeta^{\delta(ic' + jd')}.$$

Hence

$$\begin{aligned} F(\sigma^\tau) &= \delta(ic' + jd')S - \delta(ia' + jb')T \\ &= (-ic + ja)S + (-id + jb)T \end{aligned}$$

On the other hand, $\tau f(\sigma) = \tau(jS - iT)$, and since

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} j \\ -i \end{pmatrix} = \begin{pmatrix} -ic + ja \\ -id + jb \end{pmatrix},$$

it follows that $f(\sigma^\tau) = \tau f(\sigma)$.

Ramification Let w be a place over p in K and v be a place of $K(P)$ over w . Choose π so that ℓ does not divide $v(\pi)$ and v is the only place of $K(P)$ where π has nontrivial valuation. Then the extension $K(E[\ell])(\alpha_1, \alpha_2)$ over K is unramified away from w and places over ℓ . By construction the cocycle f , when restricted to the extension above $K(E[\ell])$, is determined from a homomorphism from the Galois group of $K(E[\ell])(\alpha_1, \alpha_2)$ over $K(E[\ell])$ to $E[\ell]$ (which as a group is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$). So f is unramified away from w and places over ℓ . To ensure that f is ramified at a place of K over p is more complicated. Here we consider the case where $K(P)/K$ is Galois. Since w splits completely in $K(P)$, the conjugates of v are in one-to-one correspondence with the conjugates of P and π . In particular, $v(\pi_i) = 0$ for $i \neq 1$. Suppose without loss of generality that e_1 is nonzero. Then $v(\alpha_1) = e_1 v(\pi)$, which is not divisible by ℓ . So the extension $K(E[\ell])(\alpha_1, \alpha_2)$ over $K(E[\ell])$ is ramified over v , consequently f is ramified at w .

Two cases The φ map in (2) above may not always exist. Below we describe two important cases where such a map does exist.

Case I Suppose $\Gamma = G(K(E[\ell])/K)$ is isomorphic to a subgroup of $\mathbb{Z}/(l-1)\mathbb{Z} \oplus \mathbb{Z}/(l-1)\mathbb{Z}$. Then with respect to a suitable basis of $E[\ell]$, Γ can be identified with $\left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \mid \lambda, \mu \in \mathbb{F}_l^* \right\}$. The following map φ

meets the requirement in the recipe: $\varphi(x_1, x_2) = (y_1, y_2)$ where $y_i = x_i^{-1}$ if $x_i \neq 0$ and $y_i = x_i = 0$ otherwise.

Case II Suppose $\Gamma = G(K(E[l])/K)$ is isomorphic to a subgroup of $SL_2(\mathbb{F}_\ell)$. Choose a basis S and T for $E[l]$ with respect to which $E[l]$ is identified with \mathbb{F}_ℓ^2 and every $\tau \in G(K(E[l])/K)$ is represented by an element in $SL_2(\mathbb{F}_\ell)$. It is straightforward to check that the following map φ meets the requirement in the recipe: $\varphi(x_1, x_2) = (x_2, -x_1)$.

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`