The Height Function and the Elliptic Curve Discrete Logarithm Problem

Ming-Deh Huang
University of Southern California

Discrete Logarithm Problem (DL)

A: a finite abelian group

$x \in A$, y in the subgroup generated by x

To compute a positive integer n so that $y = nx$.

In cryptographic applications, we often assume that x is an element of order ℓ where ℓ is a large prime number.

Primary examples of A: $\mathbb{F}_q^*$, $E(\mathbb{F}_q)$.

DL is the basis of many public-key cryptosystems including Digital Signature Algorithm (DSA) and Elliptic Curve Cryptography (ECC)

Index Calculus for $\mathbb{F}_p^*$

- Lifting from $\mathbb{F}_p^*$ to $\mathbb{Z}$ (or O_K of a global field K)

- Lifting is ”natural” and easy – $a \in \mathbb{F}_p^*$ to a as an integer

For ECDL, it may be natural to consider lifting from $\bar{E}(\mathbb{F}_p)$ to some $E(K)$ where E is defined over a number field (global field) K and E mod $\wp$ is $\bar{E}$ for a prime $\wp$. But lifting points is not as easy.

Given $a \in \mathbb{F}_p^* =< g >$, find e mod ℓ such that $a = g^e \pmod{p}$

Index Calculus:

- S: a set of primes up to a smoothness bound (subexp in $\log p$)
- Lift random g^r to $g^r \bmod p \in \mathbb{Z}_S^*/\mathbb{Z}_S^{*\ell}$ → d-log (mod ℓ) of all primes in S.
- Lift $ag^r \bmod p$ (for random r) to $\mathbb{Z}_S^*/\mathbb{Z}_S^{*\ell}$

$\mathbb{F}_\ell$-rank of $\mathbb{Z}_S^*/\mathbb{Z}_S^{*\ell} = \#S$. Need at least $\#S + 1$ many lifts so that (1) the d-log of a basis can be determined (2) an extra lift yields the d-log of a through linear dependency.

Similar strategy for to find m such that $T = mS$ in $\bar{E}(\mathbb{F}_P)$ (IC or Xedni)

- Lift random a_iS to $P_i \in E(K)$ and one random $T + bS$ to some $Q \in E(K)$ for some elliptic curve E/K.

- Suppose P_1 , ..., P_r generate $E(K)/\ell E(K)$, which is of rank r (over $\mathbb{F}_\ell$). Then $Q = \sum e_iP_i$ for some e_i. Reduction mod $\wp$ yields the d-log for T:

$$Q = \sum e_iP_i \Rightarrow bS + T = \sum e_i(a_iS) \Rightarrow T = (-b + \sum e_ia_i)S$$

For this kind of methods to work, we need to lift n random points from $\bar{E}(\mathbb{F}_p)$ to some $E(K)$ where the lifts are dependent; $n \geq r + 1$ if rank$(E(K)) = r$.

For an elliptic curve E defined over a number field K, we have a *canonical height*

$$\widehat{h} : E(\bar{K}) \to \mathbb{R}_{\geq 0}$$

Let $\bar{E}/\mathbb{F}_p$, and $\lambda = (\alpha_0, \ldots, \alpha_r)$ with $\alpha_i \in \bar{E}(\mathbb{F}_p)$.

Let E/K, $\Lambda = (P_0, \ldots, P_r)$ with $P_i \in \mathcal{E}(K)$.

We say that $(\bar{E}, \lambda)$ is lifted to (E, Λ) if $\bar{E} = E \bmod \wp$, $\alpha_i = P_i \bmod \wp$, for some prime $\wp$.

We say that λ is h-good for K if $(\bar{E}, \lambda)$ can be lifted to some (E, Λ) over K where the canonical heights of the lifted points in Λ are bounded by h, and the rank of $E(K)$ is at most r (the lifted points are dependent).

Let G be a cyclic subgroup of $\bar{E}(\mathbb{F}_p)$. The number of h-good $(r+1)$-tuples from G is not too small even if h is subexponential in $\log p$.

In fact, let $n(r, h)$ be the number of $r+1$-tuples from G that are h-good. Then $\frac{n(r,h)}{N^{r+1}}$ is bounded by $\frac{2^{O(r^3)}(h/\log|\Delta|)^{O(r^2)}}{N}$

In order for the ratio to be at least $\frac{1}{\mathrm{subexp}(\log p)}$, r has to be $\Omega(\log^{1/4} p)$, even if h is $\mathrm{subexp}(\log p)$.

Reason:

For $E(K)$ of rank r, the number of points in $E(K)$ with canonical height bounded by h is $2^{O(r^2)}(h/\log\Delta_E)^{r/2}$ (where the constant is independent of E).

Any $r+1$ points of $E(K)$ of height bounded by h have a $\mathbb{Z}$-linear relation with coefficients bounded by $2^{O(r^2)}(h/\log\Delta_E)^{r/2}$.

Lifting to a given $E(K)$ seems difficult.

Lifting to *some* $E(\mathbb{Q})$ is easy:

$y^2 = x^3 + ax + b \pmod{p} \Rightarrow y^2 = x^3 + ax + b'$ where $b' \equiv b \pmod{p}$

Given K, lifting to dependent points on *some* E/K is difficult, if rank of $E(K)$ is bounded by a constant.

Question: What if we allow the degree of K to grow?

Global method: originally proposed by Frey (1999). Method of this type have also been used by Nguyen (2001) on Index Calculus for Brauer group computations.

Basic idea of the global method: to address the DLP in an abelian algebraic group, we use a lifting of the group over a number field and use the reciprocity law of global class field theory.

The global method circumvents the difficulty of lifting (to dependent points), using global duality to transform the problem into *signature computation* problem.

Reciprocity Law for the Multiplicative Group

A Dirichlet character χ of K is a homomorphism of $G = Gal(\overline{K}/K)$ into $\mathbb{Q}/\mathbb{Z}$, an element of the Galois cohomology group $H^1(G, \mathbb{Q}/\mathbb{Z})$.

Reciprocity law: for any Dirichlet character χ of K and any $a \in K^*$,

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

A finite sum: $< \chi_v, a_v >_v$=0 for all but finitely many v.

Reciprocity Law for Elliptic Curves

A *principal homogeneous space* of an elliptic curve E over K is a curve F of genus 1 over K together with a group action of E on F. The isomorphism classes of such principal homogeneous spaces are classified by the group $H^1(G, E(\overline{K}))$, where $G = Gal(\overline{K}/K)$.

For $\chi \in H^1(G, E)$ and $Q \in E(K)$, we have the pairings $< \chi, Q > \in Br(K)$ and $< \chi_v, Q_v >_v \in Br(K_v) \cong \mathbb{Q}/\mathbb{Z}$.

The *reciprocity law*:

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

To address the DLP in $\mathbb{F}_p^*$ or $E(\mathbb{F}_p)$:

Construct a suitable “test” element (Dirichlet character, or a principal homogeneous space)

This element pairs with a point of the group to give an equation between the local terms of this pairing.

Need testing elements to have ramification at a place over p and we need to control ramification at other places.

Exact sequences from duality

S: a finite set of places of K containing all places over ℓ.

G_S: the Galois group of a maximal extension of K that is unramified outside S.

μ_ℓ: the Galois module of ℓ-th roots of unity.

For an abelian group A, A^* denotes Hom$(A, \mathbb{Q}/\mathbb{Z})$.

Subsequence from the *Poitou-Tate exact sequence*

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

If the order of the class group of K is not divisible by ℓ, then $H^1(G_S,\mu_\ell) \cong O_S^*/O_S^{*\ell}$ and the last map in this sequence is surjective.

(Index calculus essentially computes the image of the first map where S consists of a factor base together with p and ℓ.)

Cassels-Tate exact sequence

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

Here (ℓ) denotes completion with respect to subgroups of ℓ-power index and $\{\ell\}$ denotes the ℓ-primary part.

$\mathcal{E}$: a smooth proper model of E over an open subset U of the ring of integers of K on which ℓ is invertible and put $S = X - U$.

S: a finite set of places of K containing all bad reduction places of E and the places above ℓ.

If $Ш(E)\{\ell\} = 0$, then from Cassels-Tate we derive:

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

Strategy to find a suitable testing element with prescribed ramification: look for an algebraic number field K such that the $\mathbb{F}_\ell$-dimension of the first term of (*) is smaller than that of the second. This will guarantee the existence of an element of order ℓ in $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$(resp. $H^1(\mathcal{O}_S, \mathcal{E})[\ell]$).

$$(*)\; H^1(G_S, \mu_\ell) \to \bigoplus_{v \in S} H^1(K_v, \mu_\ell) \to H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})^* \to 0$$

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

Proposition 1. *Let K be real quadratic field in which ℓ and p split. Let S be the set consisting of one place u over ℓ, one place v over p, and both archimedean places. Suppose*

1. *$\ell \not| h_K$ 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.

Proposition 2. *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. $Ш(E)\{\ell\} = 0$;

2. *the map* $E(K)/\ell \to E(K_u)/\ell \oplus E(K_{u'})/\ell$ *is an isomorphism.*

Then the $\mathbb{F}_\ell$*-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.

$$H^1(G_S,\mu_\ell) \to \bigoplus_{v\in S} H^1(K_v,\mu_\ell) \to H^1(G_S,\mathbb{Z}/\ell\mathbb{Z})^* \to 0$$

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

Dual sequences:

$$0 \to H^1(G_S,\mathbb{Z}/\ell\mathbb{Z}) \to \bigoplus_{v\in S} H^1(K_v,\mathbb{Z}/\ell\mathbb{Z}) \to (O_S^*/O_S^{*\ell})^*$$

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

$$0 \to H^1(G_S, \mathbb{Z}/\ell\mathbb{Z}) \to \bigoplus_{v \in S} H^1(K_v, \mathbb{Z}/\ell\mathbb{Z}) \to (O_S^*/O_S^{*\ell})^*$$

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

Signature calculus is the problem of computing the image of the map $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z}) \to \bigoplus_{v \in S} H^1(K_v, \mathbb{Z}/\ell\mathbb{Z})$ (resp. $H^1(\mathcal{O}_S, \mathcal{E})[\ell] \to \prod_{v \in S} H^1(K_v, E)[\ell]$).

The element for which we want to solve d-log is lifted to the right-hand group O_S^* (resp. $E(K)$). The exact sequence translates the d-log problem to the signature calculus problem.

Let $K = \mathbb{Q}$, $S = F \cup \{p\}$, and F: the set of primes up to some bound B.

$$0 \to H^1(G_S, \mathbb{Z}/\ell\mathbb{Z}) \to \bigoplus_{v \in S} H^1(\mathbb{Q}_v, \mathbb{Z}/\ell\mathbb{Z}) \to (\mathbb{Z}_S^*/\mathbb{Z}_S^{*\ell})^*$$

Index calculus computes the image of $\mathbb{Z}_S^*/\mathbb{Z}_S^{*\ell} \to \bigoplus_{v \in S} \mathbb{Q}_v^*/\mathbb{Q}_v^{*\ell}$.

Sufficiently many smooth $g^a \bmod p$ determine the image.

From this the image of $H^1(G_S, \mathbb{Z}/\ell\mathbb{Z}) \to \bigoplus_{v \in S} H^1(\mathbb{Q}_v, \mathbb{Z}/\ell\mathbb{Z})$ can also be determined using linear algebra.

$H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$, generated by a Dirichlet character χ ramified only at p.

Feasibility of index calculus

For the multiplicative case, once we fix a field K, lifting from $\mathbb{G}_m(\mathbb{F}_p) = \mathbb{F}_p^*$ to $\mathbb{G}_m(O_K) = O_K^*$ can be difficult. But lifting to S-units $\mathbb{G}_m(O_S) = O_S^*$ is relatively easy when S contains enough small primes. Once we have enough lifting that can generate the whole group, we can determine the signature and solve the d-log problem.

The analogous strategy for elliptic curve would be lifting from $\mathcal{E}(\mathbb{F}_p) = \bar{E}(\mathbb{F}_p)$ to $\mathcal{E}(O_S) = E(K)$. The set S of places does not make a difference - not until we consider duality.

For the elliptic curve case, pairing a principal homogeneous space χ and a global point α yields similarly a relation:

$$0 = \sum_v < \chi, \alpha >_v .$$

The finite places of good reduction that may be nontrivially involved in the sum are all of large norm.

Reason: At v where E has good reduction and $v \nmid \ell$, the pairing between $H^1(K_v, E)[\ell]$ and $E(K_v)/\ell$ is perfect. But $E(K_v)/\ell$ is isomorphic to $\bar{E}(\mathbb{F}_v)/\ell$, hence is nontrivial only if $\ell | \bar{E}(\mathbb{F}_v)$. Hence in the sum above we have nontrivial contribution from v only if ℓ divides $\#\tilde{E}(\mathbb{F}_v)$.

Random polynomail time equivalence

Theorem: DL is random polynomial time equivalent to Dirichlet character signature computation for real quadratic fields satisfying some mild conditions. ($K = \mathbb{Q}(\sqrt{D})$ with $D > 0$ and S consisting of a place $u|\ell$ and a place $v|p$ such that both p and ℓ split, $\ell \nmid \#cl(K)$, and a unit which is not an ℓ-th power at u and v; so that $H^1(G, \mathbb{Z}/\ell\mathbb{Z})$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$)

Theorem: ECDL is random polynomial time equivalent to principal homogeneous space signature computation for quadratic fields satisfying some mild conditions. ($K = \mathbb{Q}(\sqrt{D})$ and S consisting of a place $u|p$ and two places $v, v'|\ell$ such that both p and ℓ split, Shafarevich-Tate group has trivial ℓ-part, and the image of $E(K)/\ell$ in $\bigoplus_v E(K_v)/\ell$ has dimension 2.)

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

Determining the image of $E(K)/\ell \to \prod_{v \in S} E(K_v)/\ell$ boils down to d-log problem in $\bar{E}(\mathbb{F}_p)$.

Determining the image of $H^1(\mathcal{O}_S, \mathcal{E})[\ell] \to \prod_{v \in S} H^1(K_v, E)[\ell]$ is the signature calculus problem.

These two problems are equivalent by virtue of the exact sequence.

The image of

$$H^1(\mathcal{O}_S, \mathcal{E})[\ell] \to \prod_{v \in S} H^1(K_v, E)[\ell]$$

precisely annihilates the image of

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

under

$$\sum_{v \in S} <,>_v \colon \prod_{v \in S} H^1(K_v, E)[\ell] \times \prod_{v \in S} E(K_v)/\ell \to \mathbb{Z}/\ell\mathbb{Z}$$

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

Construct $E/\mathbb{Q}$ with $Q \in E(\mathbb{Q})$ such that $\tilde{Q} = Q \bmod p$.

Lift $\tilde{R}$ to $R \in E(K)$ where $K/\mathbb{Q}$ is a quadratic extension in which p and ℓ both split.

Now

$$\begin{aligned} 0 &= \sum_{w \in \{v,u,u'\}} < \chi, R >_w \\ &= m < \chi, Q >_v + n < \chi, R_u >_u + n' < \chi, R_{u'} >_{u'} . \end{aligned}$$

From this m can be determined.

Challenges

- Explicit construction of test elements - principal homogeneous spaces with prescribed ramification of large prime order ℓ
- Efficient methods to work with the testing characters and principal homogeneous spaces without having to explicitly construct these objects.
- Special cases where the signature problem becomes tractable.