Global methods for discrete logarithm problems

Ming-Deh Huang and Wayne Raskind
University of Southern California

Global methods: a unifying framework to study DL and ECDL.

- help explain the difference of success of index calculus in these two situations.

- lead to interesting problems in explicit class field theory.

The Discrete logarithm problem

Given a finite abelian group G, and $a, b \in G$, to find an integer n, if it exists, such that

$$b = a^n$$

$$b = na$$

if the additive group notation is preferred.

The multiplicative case: $G = \mathbb{F}_q^*$.

The elliptic curve discrete logarithm problem: $G = E(\mathbb{F}_q)$ E is an elliptic curve defined over a finite field $\mathbb{F}_q$.

Frey (2000):

"Hasse's results on Brauer groups make it possible, at least in theory, to lift the problem [of discrete logarithm] to global fields ... and it may well be that his celebrated sequence for global fields K and its completions K_l:

$$0 \to Br(K) \to \oplus_l Br(K_l) \stackrel{\sum \mathrm{inv}_l}{\to} \mathbb{Q}/\mathbb{Z} \to 0$$

can play an important role."

Nguyen (2001): Brauer group computation and Index calculus

Global methods reveal similarities and differences between DL and ECDL

1. Index calculus naturally arises as a special case of the global method for DL. In contrast the nature of local duality on elliptic curves inhibits the viability of index calculus on ECDL. To be explained more later...

2. Global methods are based on the construction of appropriate Galois cohomology classes.

   (a) DL - random polynomial time equivalent to *signature computation* for cyclic extensions with prescribed ramification over certain real quadratic fields

   (b) ECDL - random polynomial time reducible to signature computation of certain homogeneous spaces.

The global-local framework for the multiplicative case

K: a number field,

v: a prime of K,

K_v: the completion of K at v.

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

$$K^*/K^{*\ell} \xrightarrow{\delta} H^1(K,\mu_\ell)$$

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

For $\chi \in H^1(K,\mathbb{Z}/\ell\mathbb{Z})$ and $\alpha \in K^*$.

$$< \chi, \alpha >:= \delta\alpha \cup \chi$$

Tate local duality.

$<,>$: $K_v^*/K_v^{*\ell} \times H^1(K_v,\mathbb{Z}/\ell\mathbb{Z}) \to Br(K_v)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$ is a perfect pairing of finite groups.

For $\chi \in H^1(K,\mathbb{Z}/\ell\mathbb{Z})$ and $\alpha \in K^*$, let

$$< \chi, \alpha >_v = < \chi_v, \alpha_v > .$$

The framework in the multiplicative case

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

$$0 \to Br(K) \to \oplus_v Br(K_v) \stackrel{\Sigma_v \mathsf{inv}_v}{\to} \mathbb{Q}/\mathbb{Z} \to 0$$

For $\chi \in H^1(K,\mathbb{Z}/\ell\mathbb{Z})$ and $\alpha \in K^*$,

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

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

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

where the sum is over all v such that either χ is ramified, or $v(\alpha) \neq 0$.

If α is a unit of K,

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

where the sum is over all v such that χ is ramified.

Index Calculus method

Suppose $p \equiv 1 \pmod{\ell}$ and $p \not\equiv 1 \pmod{\ell^2}$.

Suppose $t = g^n$ in $\mathbb{F}_p^*[\ell]$ and n is to be computed, given g and t.

Lift $g \in \mathbb{F}_p$ to $g \in \mathbb{Z}$ (as an integer).

Lift $r = g^a t$ to a smooth integer β in $\mathbb{Z}$ (with a being random).

Suppose β is B-smooth: $\beta = \prod_q q^{e_q}$.

Then $(n + a) = \log_g \beta = \sum_q e_q \log_g q$.

$O(B)$ relations will allow us to solve for the unknown quantities, including n.

Index Calculus method revisited

$t = g^n$ in $\mathbb{F}_p^*[\ell]$

$r = g^a t$ lifted to $\beta = \prod_q q^{e_q}$.

Let $\chi \in H^1(\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z})$ be ramified only at p.

$< \chi, \beta >_p + \sum_q < \chi, \beta >_q = 0$

$< \chi, \beta >_p = (a + n) < \chi, g >_p$

$< \chi, \beta >_q = < \chi, q^{e_q} >_q = e_q < \chi, q >_q$

$\Rightarrow$

$(a + n) < \chi, g >_p = -\sum_q e_q < \chi, q >_q$

If β is B-smooth then we get a linear relation modulo ℓ of n and $< \chi, q >_q < \chi, g >_p^{-1}$, $q < B$.

$O(B)$ relations will allow us to solve for the unknown quantities, including n.

$$(n+a) = \log_g \beta = \sum_q e_q \log_g q.$$

$$(a+n) < \chi, g >_p = < \chi, \beta >_p = -\sum_q e_q < \chi, q >_q .$$

The choice of $\chi \in H^1(K, \mathbb{Z}/l\mathbb{Z})$ introduces an extra degree of freedom.

The construction of an appropriate χ with prescribed ramification is closely related to global and local class field theory.

Cyclic extensions and characters of order ℓ with prescribed ramification

We fix the following notation.

p, ℓ: rational odd primes with $\ell || p-1$

$K/\mathbb{Q}$: real quadratic where p and ℓ split.

α: fundamental unit of K

u, v: places of K with $u|\ell$ and $v|p$

P_u, P_v: prime ideals for u and v

Suppose

1. $\ell \not| h_K$ where h_K is the class number of K, and

2. $\alpha^{l-1} \not\equiv 1 \pmod{P_u^2}$, or

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

Then there is a $\chi \in H^1(K, \mathbb{Z}/\ell\mathbb{Z})$ ramified at u and v and unramified at all other finite places.

χ corresponds to a unique cyclic extension of degree ℓ over K which is ramified at u and v and unramified at all other finite places.

$< \chi, \alpha >_u \neq 0$ and $< \chi, \alpha >_v \neq 0$, and $< \chi, \alpha >_u + < \chi, \alpha >_v = 0$.

Signature of ramification

K, ℓ, p, u, v, $u|\ell$, $v|p$, and $\ell||p-1$ as before.

Let $g \in \mathbb{Z}$ so that $g \bmod p$ generates the multiplicative group of $\mathbb{F}_p$.

The class of g generates $O_v^*/\ell \cong \mathbb{Z}/\ell\mathbb{Z}$.

The class of $1+\ell$ generates $O_u^*/\ell \cong \mathbb{Z}/\ell\mathbb{Z}$.

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

$(< \chi, 1+l >_u, < \chi, g >_v)$ is called the *signature* of χ.

$< \chi, 1+l >_u (< \chi, g >_v)^{-1}$ is called the *ramification signature* of M, the unique cyclic extension M of degree ℓ over K which is ramified at u and v and unramified elsewhere.

$\psi_w : K_w^*/\ell \to \mathbb{Z}/\ell\mathbb{Z}$ where

$\psi_w(\alpha) = \chi_w(\theta_w(\alpha))$

$\theta_w : K_w^* \to G_w^{\mathsf{ab}}$ the Artin map

Then

$\psi_v(g) =< \chi, g >_v$; $\psi_u(1+\ell) =< \chi, 1+\ell >_u$.

M: the cyclic extension corresponding to χ.

$M(\mu_\ell) = K(\mu_\ell)(A^{\frac{1}{\ell}})$ with $A \in K(\mu_\ell)$.

$m :=< \chi, g >_v$, $n :=< \chi, 1+\ell >_u$.

$\mathbb{Q}_p^{ur}(A^{\frac{1}{\ell}}) = \mathbb{Q}_p^{ur}(p^{\frac{m}{\ell}})$, $\mathbb{Q}_\ell(\mu_\ell)^{ur}(A^{\frac{1}{\ell}}) = \mathbb{Q}_\ell(\mu_\ell)^{ur}(\zeta^{\frac{n}{\ell}})$.

DL and Signature Computation

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 ℓ, p, places u, v satisfying the conditions above (ℓ not dividing h_K, fundamental unit not a local ℓ-th power), to compute the ramification signature of the cyclic extension of degree ℓ over K which is ramified at u, v and unramified elsewhere.

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

Reduction from DL to Signature Computation

Lift a to some unit α of a real quadratic field K such that $\alpha \equiv a \pmod{v}$.

Suppose K satisfies the conditions in **Signature Computation**.

Then $\alpha \sim^{\ell} (1+\ell)^y$ and y can be computed efficiently.

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

$$\begin{aligned} 0 &= <\chi, \alpha>_u + <\chi, \alpha>_v \\ &= <\chi, (1+\ell)^y>_u + <\chi, g^m>_v \\ &= y<\chi, 1+\ell>_u + m<\chi, g>_v \end{aligned}$$

$m = -y<\chi, 1+\ell>_u (<\chi, g>_v)^{-1}$.

The global-local framework for ECDL

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

$<,>$: $E(K_v)/\ell \times H^1(K_v,E)[\ell] \to Br(K_v)[\ell] \to \mathbb{Z}/\ell\mathbb{Z}$ is perfect.

$$0 \to Br(K) \to \oplus_v Br(K_v) \stackrel{\Sigma_v \mathsf{inv}_v}{\to} \mathbb{Q}/\mathbb{Z} \to 0$$

$\chi \in H^1(K,E)[\ell]$ and $\alpha \in E(K)$,

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

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 and $K_v \cong \mathbb{Q}_\ell$. Then $H^1(K_v, E)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$ if $\ell \not| \#\bar{E}(k)$.

2. Suppose the characteristic of k is not ℓ. Then

   (a) $H^1(K_v, E)[\ell] = 0$ if $\ell \not| \#\bar{E}(k)$;

   (b) $H^1(K_v, E)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$ if $\ell \mid \#\bar{E}(k)$ but $\ell^2 \not| \#\bar{E}(k)$.

Why index calculus method seems to be lacking in the case of elliptic curve discrete logarithm problem.

In

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

we have nontrivial contribution from a place $v \not| \ell$ only if ℓ divides $\#\bar{E}(\mathbb{F}_v)$.

$\#\bar{E}(\mathbb{F}_v) = O(\#\mathbb{F}_v)$, the norm of v

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

Homogeneous spaces with prescribed ramification

$K/\mathbb{Q}$: a quadratic extension in which p and ℓ both split.

$E/\mathbb{Q}$: of Mordell-Weil rank ≤ 2.

$\ell \| \#\bar{E}(\mathbb{F}_p)$, $\ell \not| \#\bar{E}(\mathbb{F}_\ell)$

The ℓ-primary component of the Shafarevich-Tate group of E is finite

Then there exists $\chi \in H^1(K, E)[\ell]$ so that χ is ramified at $v|p$ and unramified away from v and the two places u, u' over ℓ.

Signature of χ:

$$(< \chi, S >_v : < \chi, R >_u : < \chi, R >_{u'}),$$

where $R \in E(\mathbb{Q}_\ell)$ such that $R \notin \ell E(\mathbb{Q}_\ell)$, and $S \in E(\mathbb{Q})$ is a generator for $E(\mathbb{Q})/\ell$ such that $S \notin \ell E(Q_p)$

ECDL to Signature

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

1. Construct $E/\mathbb{Q}$ with $S \in E(\mathbb{Q})$ such that $\bar{S} = S \bmod p$ and that S is not a torsion point.

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

3. Find and fix some $R \in E(\mathbb{Q}_\ell)$ such that $R \not\equiv 0 \pmod{\ell E(\mathbb{Q}_\ell)}$.

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

$$\begin{array}{ccc} E & \stackrel{\pi}{\to} & \bar{E} \\ S & \to & \bar{S} \\ T & \to & \bar{T} \end{array}$$

The class of S generates $E(K_v)/\ell \cong E(\mathbb{Q}_p)/\ell \cong \bar{E}(\mathbb{F}_p)/\ell \cong \mathbb{Z}/\ell\mathbb{Z}$

$T \equiv mS \bmod \ell E(K_v)$

5. Suppose $\chi \in H^1(K, E)[\ell]$ so that χ is ramified at a place $v|p$ and unramified away from v and the two places u, u' over ℓ. Then

$$0 = \sum_{w \in \{v,u,u'\}} < \chi, T >_w .$$

$< \chi, T >_v = < \chi, mS >_v = m < \chi, S >_v$ and m is to what we want to compute in the end.

6. Compute n so that $T \equiv nR \pmod{\ell E(K_u)}$.

7. Compute n' so that $T \equiv n'R \pmod{\ell E(K_{u'})}$, in a similar fashion.

8. Then

$$\begin{aligned} 0 &= \sum_{w \in \{v,u,u'\}} < \chi, T >_w \\ &= m < \chi, S >_v + n < \chi, R >_u + n' < \chi, R >_{u'} . \end{aligned}$$

So if we can compute

$$(< \chi, S >_v : < \chi, R >_u : < \chi, R >_{u'})$$

then since $< \chi, S >_v \neq 0$, we can determine m.