How special is the Elliptic Curve Discrete Logarithm Problem?

Ming-Deh Huang
University of Southern California

November 10, 2016

A word on quantum computation and discrete logarithms

A word on quantum computation and discrete logarithms

- All discrete logarithm problems are equal under the quantum computation model (assuming basic group operations are efficient to perform under Turing machine model)

A word on quantum computation and discrete logarithms

- All discrete logarithm problems are equal under the quantum computation model (assuming basic group operations are efficient to perform under Turing machine model)
- It is not clear if large scale quantum computation is achievable.

A word on quantum computation and discrete logarithms

- All discrete logarithm problems are equal under the quantum computation model (assuming basic group operations are efficient to perform under Turing machine model)
- It is not clear if large scale quantum computation is achievable.
- Complexity - under the classical Turing model - of the discrete logarithm problems is practically important in cryptography.

A word on quantum computation and discrete logarithms

- All discrete logarithm problems are equal under the quantum computation model (assuming basic group operations are efficient to perform under Turing machine model)
- It is not clear if large scale quantum computation is achievable.
- Complexity - under the classical Turing model - of the discrete logarithm problems is practically important in cryptography.
- Questions like
    - P=NP?
    - Discrete-log $\in$ P?

  remain important in complexity theory.

Historical background on ECDL

Historical background on ECDL

- Elliptic curve discrete logarithm problem (ECDLP) was brought into spot light along with the introduction of elliptic curve cryptography independently by Koblitz and Miller in 1985.

Historical background on ECDL

- Elliptic curve discrete logarithm problem (ECDLP) was brought into spot light along with the introduction of elliptic curve cryptography independently by Koblitz and Miller in 1985.
- ‘Elliptic curves have been objects of intense study in Number Theory for the last 90 years. To quote Lang "It is possible to write endlessly on Elliptic Curves (This is not a threat)." (Miller in Crypto 85)

Historical background on ECDL

- Elliptic curve discrete logarithm problem (ECDLP) was brought into spot light along with the introduction of elliptic curve cryptography independently by Koblitz and Miller in 1985.
- 'Elliptic curves have been objects of intense study in Number Theory for the last 90 years. To quote Lang "It is possible to write endlessly on Elliptic Curves (This is not a threat)." (Miller in Crypto 85)
- Lenstra's integer factoring using elliptic curves

Historical background on ECDL

- Elliptic curve discrete logarithm problem (ECDLP) was brought into spot light along with the introduction of elliptic curve cryptography independently by Koblitz and Miller in 1985.
- 'Elliptic curves have been objects of intense study in Number Theory for the last 90 years. To quote Lang "It is possible to write endlessly on Elliptic Curves (This is not a threat)." (Miller in Crypto 85)
- Lenstra's integer factoring using elliptic curves
- Coppersmith L[1/3] algorithm for discrete-log on $\mathbb{F}_{2^n}$

Historical background on ECDL

- Elliptic curve discrete logarithm problem (ECDLP) was brought into spot light along with the introduction of elliptic curve cryptography independently by Koblitz and Miller in 1985.
- 'Elliptic curves have been objects of intense study in Number Theory for the last 90 years. To quote Lang "It is possible to write endlessly on Elliptic Curves (This is not a threat)." (Miller in Crypto 85)
- Lenstra's integer factoring using elliptic curves
- Coppersmith L[1/3] algorithm for discrete-log on $\mathbb{F}_{2^n}$
- 'It is my intent to show that elliptic curves have a rich enough arithmetic structure so that they will provide a fertile ground for planting the seeds of cryptography.' (Miller Crypto 85)

Barrier of lifting and height

Barrier of lifting and height

- All subexponential algorithms for DLP over large prime fields use lifting to $\mathbb{Q}$ or number fields.

Barrier of lifting and height

- All subexponential algorithms for DLP over large prime fields use lifting to $\mathbb{Q}$ or number fields.
- For ECDLP on $E(\mathbb{F}_p)$, it is natural to try to lift to $E(\mathbb{Q})$ or $E(K)$ where K is a number field.

Main idea of the Index Calculus method

Barrier of lifting and height

- All subexponential algorithms for DLP over large prime fields use lifting to $\mathbb{Q}$ or number fields.
- For ECDLP on $E(\mathbb{F}_p)$, it is natural to try to lift to $E(\mathbb{Q})$ or $E(K)$ where K is a number field.

Main idea of the Index Calculus method

- Suppose g is a generator of $\mathbb{F}_p^*$ and θ is to be found so that $h = g^\theta \mod p$

Barrier of lifting and height

- All subexponential algorithms for DLP over large prime fields use lifting to $\mathbb{Q}$ or number fields.
- For ECDLP on $E(\mathbb{F}_p)$, it is natural to try to lift to $E(\mathbb{Q})$ or $E(K)$ where K is a number field.

Main idea of the Index Calculus method

- Suppose g is a generator of $\mathbb{F}_p^*$ and θ is to be found so that $h = g^\theta \mod p$
- Consider a factor S base consisting of primes 2, 3, ...,q_i,.. up to a bound B

Barrier of lifting and height

- All subexponential algorithms for DLP over large prime fields use lifting to $\mathbb{Q}$ or number fields.
- For ECDLP on $E(\mathbb{F}_p)$, it is natural to try to lift to $E(\mathbb{Q})$ or $E(K)$ where K is a number field.

Main idea of the Index Calculus method

- Suppose g is a generator of $\mathbb{F}_p^*$ and θ is to be found so that $h = g^\theta \mod p$
- Consider a factor S base consisting of primes 2, 3, ...,q_i,.. up to a bound B
- If $g^a h \mod p = \prod_i q_i^{e_i}$ (an S-unit) then we have a *relation*

$$a + \theta = \sum_i e_i \theta_i \mod (p-1)$$

where θ_i is the d-log of q_i: $g^{\theta_i} = q_i \mod p$.

Barrier of lifting and height

- All subexponential algorithms for DLP over large prime fields use lifting to $\mathbb{Q}$ or number fields.
- For ECDLP on $E(\mathbb{F}_p)$, it is natural to try to lift to $E(\mathbb{Q})$ or $E(K)$ where K is a number field.

Main idea of the Index Calculus method

- Suppose g is a generator of $\mathbb{F}_p^*$ and θ is to be found so that $h = g^\theta \mod p$
- Consider a factor S base consisting of primes 2, 3, ...,q_i,.. up to a bound B
- If $g^a h \mod p = \prod_i q_i^{e_i}$ (an S-unit) then we have a *relation*

$$a + \theta = \sum_i e_i \theta_i \mod (p-1)$$

  where θ_i is the d-log of q_i: $g^{\theta_i} = q_i \mod p$.
- If B is subexponential in $\log p$ then the density of S-units

Height and lifting

Height and lifting

- Suppose $E \mod p = \overline{E}$.

Height and lifting

- Suppose $E \mod p = \overline{E}$.
- $E(\mathbb{Q})$ has finite rank (Mordell-Weil Theorem), say r.

Height and lifting

- Suppose $E \mod p = \overline{E}$.
- $E(\mathbb{Q})$ has finite rank (Mordell-Weil Theorem), say r.
- If we can lift $r+1$ random points from $\overline{E}(\mathbb{F}_p)$ to $E(\mathbb{Q})$ we have a dependence

$$a_1 P_1 + \ldots + a_{r+1} P_{r+1} = 0$$

upon reduction mod p we get a relation

$$\sum_i a_i \theta_i = 0 \mod N$$

where $N = \overline{E}(\mathbb{F}_p)$ and $\overline{P}_i = \theta_i \alpha$ and $\langle \alpha \rangle = \overline{E}(\mathbb{F}_p)$.

- Lifting points from $\overline{E}(\mathbb{F}_p)$ to $E(\mathbb{Q})$ is difficult.

- Lifting points from $\overline{E}(\mathbb{F}_p)$ to $E(\mathbb{Q})$ is difficult.
- The number of $r+1$-tuple from $E(\mathbb{F}_p)$ liftable to points in $E(\mathbb{Q})$ of height bounded subexponential in $\log p$ is not big enough

- Lifting points from $\overline{E}(\mathbb{F}_p)$ to $E(\mathbb{Q})$ is difficult.
- The number of $r+1$-tuple from $E(\mathbb{F}_p)$ liftable to points in $E(\mathbb{Q})$ of height bounded subexponential in $\log p$ is not big enough
- $n(r,h) :=$ number of $(r+1)$-tuples λ from some cyclic subgroup of $E(\mathbb{F}_p)$ that can be lifted to some (E_λ, Λ) over $\mathbb{Q}$ where E_λ has rank bounded by r and the canonical heights of the points in Λ are bounded by h.

- Lifting points from $\overline{E}(\mathbb{F}_p)$ to $E(\mathbb{Q})$ is difficult.
- The number of $r+1$-tuple from $E(\mathbb{F}_p)$ liftable to points in $E(\mathbb{Q})$ of height bounded subexponential in $\log p$ is not big enough
- $n(r,h) :=$ number of $(r+1)$-tuples λ from some cyclic subgroup of $E(\mathbb{F}_p)$ that can be lifted to some (E_λ, Λ) over $\mathbb{Q}$ where E_λ has rank bounded by r and the canonical heights of the points in Λ are bounded by h.
- Then $n(r,h)$ is bounded by $2^{O(r^3)} h^{O(r^2)} N^r$ where $N = |E(\mathbb{F}_p)|$ (Huang, Kueh and Tan, ANTS 2000).

- Points of height bounded by h on $E(\mathbb{Q})$, if dependent, have small dependence relation: $\sum_i c_i P_i = 0$ with $|c_i| \leq 2^{cr^2} h^r$.

- Points of height bounded by h on $E(\mathbb{Q})$, if dependent, have small dependence relation: $\sum_i c_i P_i = 0$ with $|c_i| \leq 2^{cr^2} h^r$.
- Reduction mod p gives $\sum_i c_i \overline{P}_i = 0$.

- Points of height bounded by h on $E(\mathbb{Q})$, if dependent, have small dependence relation: $\sum_i c_i P_i = 0$ with $|c_i| \leq 2^{cr^2} h^r$.
- Reduction mod p gives $\sum_i c_i \overline{P}_i = 0$.
- Such relation could have been found by exhaustive search, without lifting!

- Points of height bounded by h on $E(\mathbb{Q})$, if dependent, have small dependence relation: $\sum_i c_i P_i = 0$ with $|c_i| \leq 2^{cr^2} h^r$.
- Reduction mod p gives $\sum_i c_i \overline{P}_i = 0$.
- Such relation could have been found by exhaustive search, without lifting!
- If $E(\mathbb{Q})$ has rank r we don't expect to be able to lift more than r points unless their relation is already known.

Reduction to the multiplicative case via Pairing

Reduction to the multiplicative case via Pairing

- Menezes, Okamoto and Vanstone (STOC 91) reduces ECDL to DL over finite fields using Weil pairing

Reduction to the multiplicative case via Pairing

- Menezes, Okamoto and Vanstone (STOC 91) reduces ECDL to DL over finite fields using Weil pairing
- At the cost of computing in the field $\mathbb{F}_q(E[\ell])$, the extension where the ℓ-torsion are defined.

Reduction to the multiplicative case via Pairing

- Menezes, Okamoto and Vanstone (STOC 91) reduces ECDL to DL over finite fields using Weil pairing
- At the cost of computing in the field $\mathbb{F}_q(E[\ell])$, the extension where the ℓ-torsion are defined.
- Frey and Rück: Tate pairing computable in $\mathbb{F}_q(\mu_\ell)$, efficiently if $\mu_\ell \subset \mathbb{F}_q$.

Reduction via pairing

Discrete logarithm problem on $E(\mathbb{F}_q)$

- $\#E(\mathbb{F}_q) = \ell$, ℓ prime not dividing q.
- Given $\alpha, \beta \in E(\mathbb{F}_q)$, to find m such that $m\alpha = \beta$

Reduction via pairing

Discrete logarithm problem on $E(\mathbb{F}_q)$

- $\#E(\mathbb{F}_q) = \ell$, ℓ prime not dividing q.
- Given $\alpha, \beta \in E(\mathbb{F}_q)$, to find m such that $m\alpha = \beta$

Tate-Lichtenbaum pairing

- Suppose $\mu_\ell \subset \mathbb{F}^*$
- $$\langle , \rangle : E(\mathbb{F})[\ell] \times E[\mathbb{F}]/\ell E[\mathbb{F}] \to \mathbb{F}^*/\mathbb{F}^{*\ell}$$

Reduction via pairing

Discrete logarithm problem on $E(\mathbb{F}_q)$

- $\#E(\mathbb{F}_q) = \ell$, ℓ prime not dividing q.
- Given $\alpha, \beta \in E(\mathbb{F}_q)$, to find m such that $m\alpha = \beta$

Tate-Lichtenbaum pairing

- Suppose $\mu_\ell \subset \mathbb{F}^*$
- $$\langle , \rangle : E(\mathbb{F})[\ell] \times E[\mathbb{F}]/\ell E[\mathbb{F}] \to \mathbb{F}^*/\mathbb{F}^{*\ell}$$

Reduction

- $\mathbb{F} := \mathbb{F}_q(\mu_\ell)$
- If $\beta = m\alpha$, then $\langle \alpha, \beta \rangle = \langle \alpha, \alpha \rangle^m$.
- So we are reduced to DL/$\mathbb{F}$: to find m such that

  $$b = a^m$$

  where $a = \langle \alpha, \alpha \rangle$ and $b = \langle \alpha, \beta \rangle$.

Tate pairing

Tate-Lichtenbaum pairing: suppose $\mu_\ell \subset \mathbb{F}$.

$$E(\mathbb{F})[\ell] \times E(\mathbb{F})/\ell E(\mathbb{F}) \to \mathbb{F}^*/\mathbb{F}^{*\ell}$$

For $S \in E(\mathbb{F})[\ell]$ and $D \in E(\mathbb{F})/\ell E(\mathbb{F})$,

$$(S, D) \to F_S(D)$$

where F_S is a function in $k(E)$ such that $(F_S) = \ell S$ (without loss of generality assume $D \neq S$).

- ℓ divides $|E(\mathbb{F})|$ but ℓ does not divide $|\mathbb{F}^*|$ $\to$ computational barrier $\mathbb{F}(\mu_\ell)$

- ℓ divides $|E(\mathbb{F})|$ but ℓ does not divide $|\mathbb{F}^*|$ $\to$ computational barrier $\mathbb{F}(\mu_\ell)$
- Pairing not taking values in μ_ℓ?

- ℓ divides $|E(\mathbb{F})|$ but ℓ does not divide $|\mathbb{F}^*|$ $\rightarrow$ computational barrier $\mathbb{F}(\mu_\ell)$
- Pairing not taking values in μ_ℓ?
- Local duality

Multilinear generalization of Tate pairing

Multilinear generalization of Tate pairing

- Let A be a principally polarized abelian variety of dimension g over a finite field $\mathbb{F}$.

Multilinear generalization of Tate pairing

- Let A be a principally polarized abelian variety of dimension g over a finite field $\mathbb{F}$.
- $V := A[\ell]$ the set of points P of A defined over $\overline{\mathbb{F}}$ such that $\ell P = 0$.

Multilinear generalization of Tate pairing

- Let A be a principally polarized abelian variety of dimension g over a finite field $\mathbb{F}$.
- $V := A[\ell]$ the set of points P of A defined over $\overline{\mathbb{F}}$ such that $\ell P = 0$.
- Set $d = 2g - 1$, let φ be the geometric Frobenius and put $N = 1 - \varphi$.

Multilinear generalization of Tate pairing

- Let A be a principally polarized abelian variety of dimension g over a finite field $\mathbb{F}$.
- $V := A[\ell]$ the set of points P of A defined over $\overline{\mathbb{F}}$ such that $\ell P = 0$.
- Set $d = 2g - 1$, let φ be the geometric Frobenius and put $N = 1 - \varphi$.
- Suppose N acts on $A[\ell]$ in a maximally nilpotent way. That is, $N^{d+1} = 0$, but $N^d \neq 0$.

Multilinear generalization of Tate pairing

- Let A be a principally polarized abelian variety of dimension g over a finite field $\mathbb{F}$.
- $V := A[\ell]$ the set of points P of A defined over $\overline{\mathbb{F}}$ such that $\ell P = 0$.
- Set $d = 2g - 1$, let φ be the geometric Frobenius and put $N = 1 - \varphi$.
- Suppose N acts on $A[\ell]$ in a maximally nilpotent way. That is, $N^{d+1} = 0$, but $N^d \neq 0$.
- Let $V_{2i-d} = \ker N^{i+1}$ and $Gr_{2i-d} = \ker N^{i+1} / \ker N^i$, for $i = 0, \ldots, d = 2g - 1$.

Multilinear generalization of Tate pairing

- Let A be a principally polarized abelian variety of dimension g over a finite field $\mathbb{F}$.
- $V := A[\ell]$ the set of points P of A defined over $\overline{\mathbb{F}}$ such that $\ell P = 0$.
- Set $d = 2g - 1$, let φ be the geometric Frobenius and put $N = 1 - \varphi$.
- Suppose N acts on $A[\ell]$ in a maximally nilpotent way. That is, $N^{d+1} = 0$, but $N^d \neq 0$.
- Let $V_{2i-d} = \ker N^{i+1}$ and $Gr_{2i-d} = \ker N^{i+1} / \ker N^i$, for $i = 0, \ldots, d = 2g - 1$.
- There is a unique filtration V.

$$V = V_d \supset V_{d-2} \supset \ldots \supset V_{-d}$$

such that $N(V_i) \subseteq V_{i-2}$ and N^i induces an isomorphism:

$$Gr_i V \to Gr_{-i} V.$$

- A non-trivial $2g$-linear alternating pairing on V taking values in $\mu_\ell^{\otimes g}$ induces a non-trivial multilinear pairing:

$$Gr_d V \times Gr_{d-2} V \times \ldots \times Gr_{-d} V \to \mu_\ell^{\otimes g}.$$

- A non-trivial $2g$-linear alternating pairing on V taking values in $\mu_\ell^{\otimes g}$ induces a non-trivial multilinear pairing:

$$Gr_d V \times Gr_{d-2} V \times \ldots \times Gr_{-d} V \to \mu_\ell^{\otimes g}.$$

- There is a $2g$-multilinear, alternating, nondegenerate form:

$$A[\ell] \times \cdots \times A[\ell] \to \mu_\ell^{\otimes g}. \tag{1}$$

This is a well-known generalization of the Weil pairing on elliptic curves. The nondegenerate alternating pairing induces a nontrivial $(2g)$-multilinear pairing on $Gr_i V$.

- A non-trivial $2g$-linear alternating pairing on V taking values in $\mu_\ell^{\otimes g}$ induces a non-trivial multilinear pairing:

$$Gr_d V \times Gr_{d-2} V \times \ldots \times Gr_{-d} V \to \mu_\ell^{\otimes g}.$$

- There is a $2g$-multilinear, alternating, nondegenerate form:

$$A[\ell] \times \cdots \times A[\ell] \to \mu_\ell^{\otimes g}. \tag{1}$$

  This is a well-known generalization of the Weil pairing on elliptic curves. The nondegenerate alternating pairing induces a nontrivial $(2g)$-multilinear pairing on $Gr_i V$.

- The map N induces an isomorphism between $Gr_i V$ and $Gr_{i-2} V$. These groups can all be identified with $Gr_d(V) = A(\mathbb{F})[\ell]$. In this way, we get a multilinear self-pairing on $A(\mathbb{F})[\ell]$

In the case where $V = E[\ell]$ where E is an elliptic curve over $\mathbb{F}$, $g = d = 1$, and the condition on N amounts to Frobenius trace being 2 modulo ℓ. The filtration is simply $V_1 \supset V_{-1}$. The Weil pairing induces on $Gr_1 V = V/V_{-1} \cong E(\mathbb{F})/\ell E(\mathbb{F})$ and $Gr_{-1} V = V_{-1} = E(\mathbb{F})[\ell]$ the Tate pairing.

Tate local duality

k: local field ($k = \mathbb{Q}_p$)
E/k: an elliptic curve

$$\langle , \rangle : H^1(k, E)[\ell] \times E(k)/\ell E(k) \to \mathrm{Br}(k)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$$

Multiplicative case

$$[,] : H^1(k, \mathbb{Z}/\ell\mathbb{Z}) \times k^*/k^{*\ell} \to \mathrm{Br}(k)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$$

$$
\begin{array}{cccc}
\langle , \rangle : H^1(k,E)[\ell] \times & E(k)/\ell E(k) & \to \mathbb{Z}/\ell\mathbb{Z} \\
& \uparrow & \\
& \bar{E}(\mathbb{F})/\ell\bar{E}(\mathbb{F}) &
\end{array}
$$

Let

- $\bar{E}$ be an elliptic curve defined over $\mathbb{F}$.
- E be defined over k with good reduction isomorphic to $\bar{E}$.
- Suppose $\bar{E}(\mathbb{F})[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$. Then $\bar{E}(\mathbb{F})[\ell]$ is isomorphic to $\bar{E}(\mathbb{F})/\ell\bar{E}(\mathbb{F})$, and isomorphic to $E(k)/\ell E(k)$ through the reduction map.
- If $\bar{\beta} = m\bar{\alpha}$ then
$$\langle \chi, \beta \rangle = m\langle \chi, \alpha \rangle$$

π: a generator for the unique prime ideal of k (uniformizing element)

Suppose $\mu_\ell \subset k$. Then

$$H^1(k, E)[\ell] \cong \mathrm{Hom}(\mathrm{Gal}(k(\pi^{1/\ell})/k), E(k)[\ell]).$$

π: a generator for the unique prime ideal of k (uniformizing element)

Suppose $\mu_\ell \subset k$. Then

$$H^1(k, E)[\ell] \cong \mathrm{Hom}(\mathrm{Gal}(k(\pi^{1/\ell})/k), E(k)[\ell]).$$

Fix a generator τ for $\mathrm{Gal}(k(\pi^{1/\ell})/k)$.
A cocycle α in $H^1(k, E)[\ell]$ is represented by $S = \alpha(\tau) \in E(k)[\ell]$.

π: a generator for the unique prime ideal of k (uniformizing element)

Suppose $\mu_\ell \subset k$. Then

$$H^1(k, E)[\ell] \cong \mathrm{Hom}(\mathrm{Gal}(k(\pi^{1/\ell})/k), E(k)[\ell]).$$

Fix a generator τ for $\mathrm{Gal}(k(\pi^{1/\ell})/k)$.
A cocycle α in $H^1(k, E)[\ell]$ is represented by $S = \alpha(\tau) \in E(k)[\ell]$.

Let $\chi \in H^1(k, \mathbb{Z}/\ell\mathbb{Z})$ be such that $\chi(\tau) = 1$.

π: a generator for the unique prime ideal of k (uniformizing element)

Suppose $\mu_\ell \subset k$. Then

$$H^1(k, E)[\ell] \cong \mathrm{Hom}(\mathrm{Gal}(k(\pi^{1/\ell})/k), E(k)[\ell]).$$

Fix a generator τ for $\mathrm{Gal}(k(\pi^{1/\ell})/k)$.
A cocycle α in $H^1(k, E)[\ell]$ is represented by $S = \alpha(\tau) \in E(k)[\ell]$.

Let $\chi \in H^1(k, \mathbb{Z}/\ell\mathbb{Z})$ be such that $\chi(\tau) = 1$.

Let $D \in E(k)/\ell E(k)$.
Then

$$\langle \alpha, D \rangle = [\chi, F_S(D)]$$

Reduction from elliptic curve to multiplicative local duality computation

If $\mu_\ell \subset k$, then

Reduction from elliptic curve to multiplicative local duality computation

If $\mu_\ell \subset k$, then

- Multiplicative local duality is polynomial time reduced to norm residue symbol computation and discrete logarithm in k.

Reduction from elliptic curve to multiplicative local duality computation

If $\mu_\ell \subset k$, then

- Multiplicative local duality is polynomial time reduced to norm residue symbol computation and discrete logarithm in k.
- Elliptic curve local duality computation is polynomial time reduced to Tate-Lichtenbaum pairing and multiplicative local duality computation.

Reduction from elliptic curve to multiplicative local duality computation

If $\mu_\ell \subset k$, then

- Multiplicative local duality is polynomial time reduced to norm residue symbol computation and discrete logarithm in k.
- Elliptic curve local duality computation is polynomial time reduced to Tate-Lichtenbaum pairing and multiplicative local duality computation.

Local duality computation without μ_ℓ?

Reduction from elliptic curve to multiplicative local duality computation

If $\mu_\ell \subset k$, then

- Multiplicative local duality is polynomial time reduced to norm residue symbol computation and discrete logarithm in k.
- Elliptic curve local duality computation is polynomial time reduced to Tate-Lichtenbaum pairing and multiplicative local duality computation.

Local duality computation without μ_ℓ?
Local and global duality?

Multiplicative local duality computation

$$\mu_\ell \to \mathbb{Z}/\ell\mathbb{Z} \text{ so that } \zeta \to 1$$

$$\begin{array}{ccccc}
H^1(k,\mathbb{Z}/\ell\mathbb{Z}) & \times & k^*/k^{*\ell} & \to & \mathbb{Z}/\ell\mathbb{Z} \\
\uparrow & & & & \\
H^(k,\mu_\ell) & & & & \\
\uparrow & & & & \\
k^*/k^{*\ell} & \times & k*/k^{*\ell} & \to & \mu_\ell
\end{array}$$

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

$$\pi \to \chi$$

$$\chi(\sigma) = \sigma(\pi^{\frac{1}{\ell}})/\pi^{\frac{1}{\ell}} \text{ for all } \sigma \in G_k.$$

$$[\chi, a] = i \Leftrightarrow (\pi, a) = \zeta^i$$

Global duality approach

- Frey's observation (2000): "Hesse's results on Brauer groups make it possible, at least in theory, to lift the problem to global fields ... and it may well be that the celebrated sequence for global fields K and their completions K_i:

$$0 \to Br(K) \to \oplus_i Br(K_i) \stackrel{\oplus \mathrm{inv}_i}{\to} \mathbb{Q}/\mathbb{Z} \to 0$$

  can play an important role."
- Nguyen (2001): Brauer group computation and index calculus
- Huang and Raskind (2004): Global methods for DL and ECDL and *signature calculus*
- Rubin and Silverberg: ECDL using Euler and Kolyvagin systems (ongoing)

Brauer group sequence

$Br(K)$: is an abelian group that classifies the equivalence classes of central simple algebras over K, where two such algebras A and B are equivalent if there are matrix algebras $M_n(K), M_m(K)$ such that

$$A \otimes_K M_n(K) \cong B \otimes_K M_m(K).$$

$Br(K_v) \cong \mathbb{Q}/\mathbb{Z}$ if v is nonarchimedean
$Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ and $Br(\mathbb{C}) = 0$.

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

The exact sequence

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

is the beginning of the theory of *global duality*.

$$\begin{array}{ccccc} & & & & 0 \\ & & & & \downarrow \\ H^1(K,E)[\ell] & \times & E(K)/\ell & \to & Br(K)[\ell] \\ \downarrow & & \downarrow & & \downarrow \\ \prod_v H^1(K_v,E)[\ell] & \times & \prod_v E(K_v)/\ell & \to & \Sigma_v Br(K_v)[\ell] \\ & & & & \downarrow \\ & & & & \mathbb{Q}/\mathbb{Z} \\ & & & & \downarrow \\ & & & & 0 \end{array}$$

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

D-log preserved at places over p.

We are given $\bar{E}/\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = \ell$ prime, $\ell \neq p$.
Given $\bar{\alpha}, \bar{\beta} \in E(\mathbb{F}_p)$ we would like to compute m such that $m\bar{\alpha} = \bar{\beta}$.

We are given $\bar{E}/\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = \ell$ prime, $\ell \neq p$.
Given $\bar{\alpha}, \bar{\beta} \in E(\mathbb{F}_p)$ we would like to compute m such that $m\bar{\alpha} = \bar{\beta}$.
Lift $\bar{E}$ to some $E/\mathbb{Q}$ together with α, β in $E(\mathbb{Q})$ (or $E(K)$) that reduce to $\bar{\alpha}$ and $\bar{\beta}$ respectively.
$E(\mathbb{Q}_p)/\ell E(\mathbb{Q}_p) \cong \bar{E}(\mathbb{F}_p)$

We are given $\bar{E}/\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = \ell$ prime, $\ell \neq p$.
Given $\bar{\alpha}, \bar{\beta} \in E(\mathbb{F}_p)$ we would like to compute m such that $m\bar{\alpha} = \bar{\beta}$.
Lift $\bar{E}$ to some $E/\mathbb{Q}$ together with α, β in $E(\mathbb{Q})$ (or $E(K)$) that reduce to $\bar{\alpha}$ and $\bar{\beta}$ respectively.
$E(\mathbb{Q}_p)/\ell E(\mathbb{Q}_p) \cong \bar{E}(\mathbb{F}_p)$
Suppose we have some $\chi \in H^1(\mathbb{Q}, E)[\ell]$ ramified only at p, and r and s. Then

$$\langle \chi, \alpha \rangle_p + \langle \chi, \alpha \rangle_r + \langle \chi, \alpha \rangle_s = 0$$

$$\langle \chi, \beta \rangle_p + \langle \chi, \beta \rangle_r + \langle \chi, \beta \rangle_s = 0$$

We are given $\bar{E}/\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = \ell$ prime, $\ell \neq p$.
Given $\bar{\alpha}, \bar{\beta} \in E(\mathbb{F}_p)$ we would like to compute m such that $m\bar{\alpha} = \bar{\beta}$.
Lift $\bar{E}$ to some $E/\mathbb{Q}$ together with α, β in $E(\mathbb{Q})$ (or $E(K)$) that reduce to $\bar{\alpha}$ and $\bar{\beta}$ respectively.
$E(\mathbb{Q}_p)/\ell E(\mathbb{Q}_p) \cong \bar{E}(\mathbb{F}_p)$
Suppose we have some $\chi \in H^1(\mathbb{Q}, E)[\ell]$ ramified only at p, and r and s. Then

$$\langle \chi, \alpha \rangle_p + \langle \chi, \alpha \rangle_r + \langle \chi, \alpha \rangle_s = 0$$
$$\langle \chi, \beta \rangle_p + \langle \chi, \beta \rangle_r + \langle \chi, \beta \rangle_s = 0$$

If D-log and $\langle , \rangle$ can be efficiently computed at r and s. Then we can determine m such that $m\alpha = \beta$ in $E(\mathbb{Q}_p)/\ell E(\mathbb{Q}_p)$.

- From $\chi \in H^1(K, E)[\ell]$ ramified only at p, and r and s to get explicitly χ_r and χ_s

- From $\chi \in H^1(K, E)[\ell]$ ramified only at p, and r and s to get explicitly χ_r and χ_s
- Fix some $u_v \in E(K_v)/\ell E(K_v)$, $v = p, r, s$. To compute

$$(\langle \chi_p, u_p \rangle : \langle \chi_r, u_r \rangle_r : \langle \chi_s, u_s \rangle_s)$$

(signature)

- From $\chi \in H^1(K, E)[\ell]$ ramified only at p, and r and s to get explicitly χ_r and χ_s
- Fix some $u_v \in E(K_v)/\ell E(K_v)$, $v = p, r, s$. To compute

  $$(\langle \chi_p, u_p \rangle : \langle \chi_r, u_r \rangle_r : \langle \chi_s, u_s \rangle_s)$$

  (signature)
- D-log polynomial time equivalent to signature computation (under mild assumptions)

- From $\chi \in H^1(K, E)[\ell]$ ramified only at p, and r and s to get explicitly χ_r and χ_s
- Fix some $u_v \in E(K_v)/\ell E(K_v)$, $v = p, r, s$. To compute

  $$(\langle \chi_p, u_p \rangle : \langle \chi_r, u_r \rangle_r : \langle \chi_s, u_s \rangle_s)$$

  (signature)
- D-log polynomial time equivalent to signature computation (under mild assumptions)
- Such $\chi \in H^1(K, E)[\ell]$ with prescribed ramification can be explicitly constructed through Euler and Kolyvagin systems. Efficient identification of its localization χ_v at $v \neq p$ for local duality computation seems to be a challenging problem.

Barriers

Barriers

- Lifting

Barriers

- Lifting
- Height

Barriers

- Lifting
- Height
- μ_ℓ

Barriers

- Lifting
- Height
- μ_ℓ

'It is my intent to show that elliptic curves have a rich enough arithmetic structure so that they will provide a fertile ground for planting the seeds of cryptography.' (Miller Crypto 85)

Barriers

- Lifting
- Height
- μ_ℓ

'It is my intent to show that elliptic curves have a rich enough arithmetic structure so that they will provide a fertile ground for planting the seeds of cryptography.' (Miller Crypto 85)

- Arithmetic structure makes it very hard to solve the ECDLP?

Barriers

- Lifting
- Height
- μ_ℓ

'It is my intent to show that elliptic curves have a rich enough arithmetic structure so that they will provide a fertile ground for planting the seeds of cryptography.' (Miller Crypto 85)

- Arithmetic structure makes it very hard to solve the ECDLP?
- Arithmetic structure makes it possible to solve the ECDLP?
- How special is the ECDLP?