The Discrete Logarithm Problem on Algebraic Curves

David Jao

University of Waterloo

Workshop on Computational challenges arising in algorithmic number theory and Cryptography
Fields Institute, Toronto

November 2, 2006

Outline

Outline

1. Discrete Logarithms
   - Definitions and notation
   - Relationship between different groups; DLOG reduction
2. Known facts about DLOG reduction
   - Reductions between elliptic curves
   - Reductions from elliptic curves to hyperelliptic Jacobians

Outline

1. Discrete Logarithms
   - Definitions and notation
   - Relationship between different groups; DLOG reduction
2. Known facts about DLOG reduction
   - Reductions between elliptic curves
   - Reductions from elliptic curves to hyperelliptic Jacobians
3. Open problems in DLOG reduction
   - Elliptic curves not admitting reductions
   - Reductions between hyperelliptic Jacobians
   - Reductions from elliptic curves to non-hyperelliptic Jacobians

Outline

The Discrete Logarithm Problem

- Let G be a cyclic group of order n, with generator g.
- The *discrete logarithm* of a group element $h \in G$, denoted $\mathrm{DLOG}_g(h)$, is the residue class $x \in \mathbb{Z}/n\mathbb{Z}$ satisfying

$$g^x = h.$$

The Discrete Logarithm Problem

- Let G be a cyclic group of order n, with generator g.
- The *discrete logarithm* of a group element $h \in G$, denoted $\mathrm{DLOG}_g(h)$, is the residue class $x \in \mathbb{Z}/n\mathbb{Z}$ satisfying

$$g^x = h.$$

- Many cryptographic protocols require a group for which computing $\mathrm{DLOG}_g(h)$ is hard.

The Discrete Logarithm Problem

- Let G be a cyclic group of order n, with generator g.
- The *discrete logarithm* of a group element $h \in G$, denoted $\mathrm{DLOG}_g(h)$, is the residue class $x \in \mathbb{Z}/n\mathbb{Z}$ satisfying

$$g^x = h.$$

- Many cryptographic protocols require a group for which computing $\mathrm{DLOG}_g(h)$ is hard.
- What determines the difficulty of computing discrete logarithms?

Things that do NOT matter for DLOG

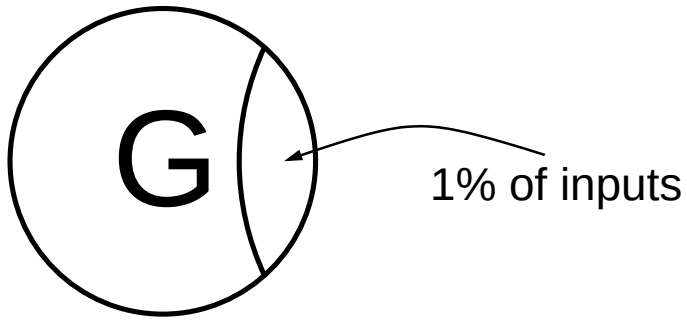
- Choice of h does not affect difficulty of computing $\mathrm{DLOG}_g(h)$
  - except for rare exceptions such as $\mathrm{DLOG}_g(g)$, $\mathrm{DLOG}_g(e)$, ...

Things that do NOT matter for DLOG

- Choice of h does not affect difficulty of computing $\mathrm{DLOG}_g(h)$
  - except for rare exceptions such as $\mathrm{DLOG}_g(g)$, $\mathrm{DLOG}_g(e)$, ...
- **Proof:** Suppose we have an algorithm $\mathcal{A}$ which computes $\mathrm{DLOG}_g(h)$ quickly on 1% of inputs $h \in G$.

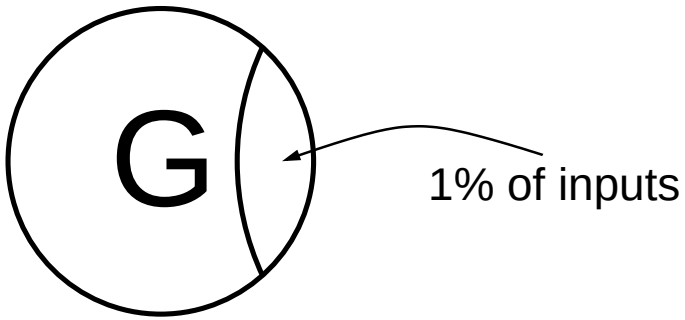
Things that do NOT matter for DLOG

- Choice of h does not affect difficulty of computing $\mathrm{DLOG}_g(h)$
  - except for rare exceptions such as $\mathrm{DLOG}_g(g)$, $\mathrm{DLOG}_g(e)$, ...
- **Proof:** Suppose we have an algorithm $\mathcal{A}$ which computes $\mathrm{DLOG}_g(h)$ quickly on 1% of inputs $h \in G$.



Things that do NOT matter for DLOG

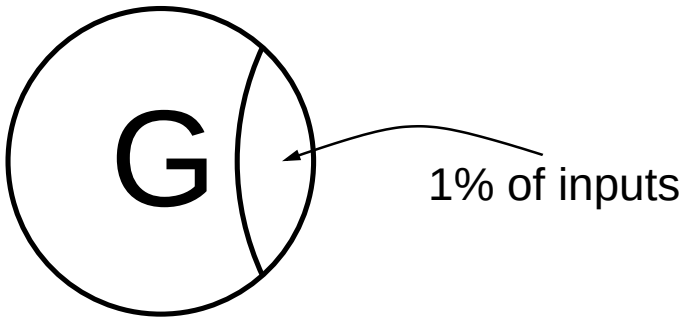
- Choice of h does not affect difficulty of computing $\mathrm{DLOG}_g(h)$
  - except for rare exceptions such as $\mathrm{DLOG}_g(g)$, $\mathrm{DLOG}_g(e)$, ...
- **Proof:** Suppose we have an algorithm $\mathcal{A}$ which computes $\mathrm{DLOG}_g(h)$ quickly on 1% of inputs $h \in G$.



- We want to find the discrete log of g^k.

Things that do NOT matter for DLOG

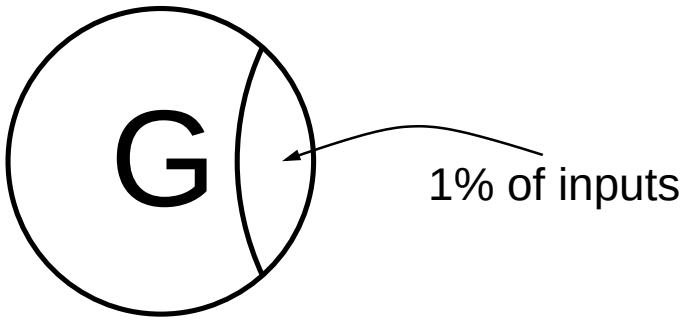
- Choice of h does not affect difficulty of computing $\mathrm{DLOG}_g(h)$
  - except for rare exceptions such as $\mathrm{DLOG}_g(g)$, $\mathrm{DLOG}_g(e)$, ...
- **Proof:** Suppose we have an algorithm $\mathcal{A}$ which computes $\mathrm{DLOG}_g(h)$ quickly on 1% of inputs $h \in G$.



- We want to find the discrete log of g^k.
- For random r, we expect $\mathcal{A}$ to work on $g^r g^k$ 1% of the time.

Things that do NOT matter for DLOG

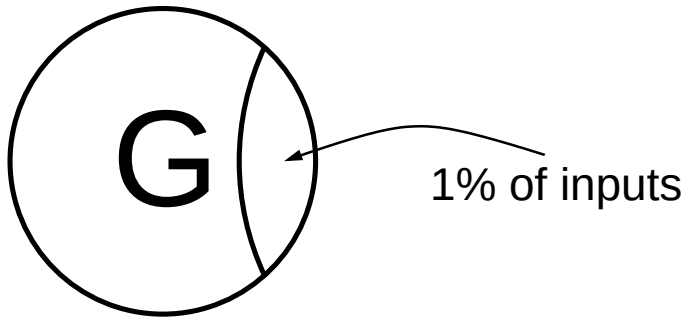
- Choice of h does not affect difficulty of computing $\mathrm{DLOG}_g(h)$
  - except for rare exceptions such as $\mathrm{DLOG}_g(g)$, $\mathrm{DLOG}_g(e)$, ...
- **Proof:** Suppose we have an algorithm $\mathcal{A}$ which computes $\mathrm{DLOG}_g(h)$ quickly on 1% of inputs $h \in G$.



- We want to find the discrete log of g^k.
- For random r, we expect $\mathcal{A}$ to work on $g^r g^k$ 1% of the time.
  - The probability of **not** succeeding after N steps is $(.99)^N$.

Things that do NOT matter for DLOG

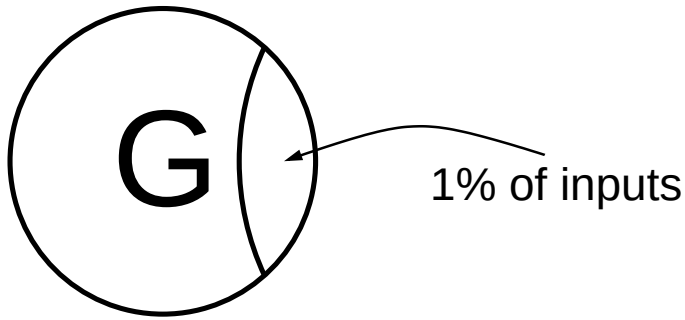
- Choice of h does not affect difficulty of computing $\mathrm{DLOG}_g(h)$
  - except for rare exceptions such as $\mathrm{DLOG}_g(g)$, $\mathrm{DLOG}_g(e)$, ...
- **Proof:** Suppose we have an algorithm $\mathcal{A}$ which computes $\mathrm{DLOG}_g(h)$ quickly on 1% of inputs $h \in G$.



- We want to find the discrete log of g^k.
- For random r, we expect $\mathcal{A}$ to work on $g^r g^k$ 1% of the time.
  - The probability of **not** succeeding after N steps is $(.99)^N$.
- Eventually $\mathcal{A}(g^r g^k)$ will return $(r+k)$. We can then find k since we know r and $(r+k)$.

Things that do NOT matter for DLOG

- Choice of h does not affect difficulty of computing $\mathrm{DLOG}_g(h)$
  - except for rare exceptions such as $\mathrm{DLOG}_g(g)$, $\mathrm{DLOG}_g(e)$, ...
- **Proof:** Suppose we have an algorithm $\mathcal{A}$ which computes $\mathrm{DLOG}_g(h)$ quickly on 1% of inputs $h \in G$.



- We want to find the discrete log of g^k.
- For random r, we expect $\mathcal{A}$ to work on $g^r g^k$ 1% of the time.
  - The probability of **not** succeeding after N steps is $(.99)^N$.
- Eventually $\mathcal{A}(g^r g^k)$ will return $(r+k)$. We can then find k since we know r and $(r+k)$.
- Therefore, **on average** the discrete log problem is equivalent for all $h \in G$.

Things that do NOT matter for DLOG (cont'd)

What affects the difficulty of computing $\mathrm{DLOG}_g(h)$?

Things that do NOT matter for DLOG (cont'd)

What affects the difficulty of computing $\mathrm{DLOG}_g(h)$?

- Is it the element h? No ...

Things that do NOT matter for DLOG (cont'd)

What affects the difficulty of computing $\mathrm{DLOG}_g(h)$?

- Is it the element h? No ...
- Is it the generator g?

Things that do NOT matter for DLOG (cont'd)

What affects the difficulty of computing $\mathrm{DLOG}_g(h)$?

- Is it the element h? No ...
- Is it the generator g? No ...

$$\mathrm{DLOG}_{g'}(h) = \frac{\mathrm{DLOG}_g(h)}{\mathrm{DLOG}_g(g')}.$$

Things that do NOT matter for DLOG (cont'd)

What affects the difficulty of computing $\mathrm{DLOG}_g(h)$?

- Is it the element h? No ...
- Is it the generator g? No ...

$$\mathrm{DLOG}_{g'}(h) = \frac{\mathrm{DLOG}_g(h)}{\mathrm{DLOG}_g(g')}.$$

- Is it the size of G?

Things that do NOT matter for DLOG (cont'd)

What affects the difficulty of computing $\mathrm{DLOG}_g(h)$?

- Is it the element h? No ...
- Is it the generator g? No ...

$$\mathrm{DLOG}_{g'}(h) = \frac{\mathrm{DLOG}_g(h)}{\mathrm{DLOG}_g(g')}.$$

- Is it the size of G?
  Note that by size you mean isomorphism class, since G is cyclic.

Effect of $|G|$ on DLOG

Size of G does have some effect on DLOG:

- All else being equal, a larger group size makes DLOG harder
- Certain group sizes are insecure no matter what the group
  - e.g. if $|G|$ is smooth (that is, all prime divisors of $|G|$ are small) then DLOG on G is easy.

Effect of $|G|$ on DLOG

Size of G does have some effect on DLOG:

- All else being equal, a larger group size makes DLOG harder
- Certain group sizes are insecure no matter what the group
  - e.g. if $|G|$ is smooth (that is, all prime divisors of $|G|$ are small) then DLOG on G is easy.

On the other hand, size is not the only factor.

Effect of $|G|$ on DLOG

Size of G does have some effect on DLOG:

- All else being equal, a larger group size makes DLOG harder
- Certain group sizes are insecure no matter what the group
  - e.g. if $|G|$ is smooth (that is, all prime divisors of $|G|$ are small) then DLOG on G is easy.

On the other hand, size is not the only factor.
Groups of equal size can (conjecturally) have inequivalent discrete log problems.

Effect of $|G|$ on DLOG

Size of G does have some effect on DLOG:

- All else being equal, a larger group size makes DLOG harder
- Certain group sizes are insecure no matter what the group
  - e.g. if $|G|$ is smooth (that is, all prime divisors of $|G|$ are small) then DLOG on G is easy.

On the other hand, size is not the only factor.
Groups of equal size can (conjecturally) have inequivalent discrete log problems.

- DLOG in $(\mathbb{Z}/p\mathbb{Z})^*$ is conjectured to be hard.

Effect of $|G|$ on DLOG

Size of G does have some effect on DLOG:

- All else being equal, a larger group size makes DLOG harder
- Certain group sizes are insecure no matter what the group
  - e.g. if $|G|$ is smooth (that is, all prime divisors of $|G|$ are small) then DLOG on G is easy.

On the other hand, size is not the only factor.
Groups of equal size can (conjecturally) have inequivalent discrete log problems.

- DLOG in $(\mathbb{Z}/p\mathbb{Z})^*$ is conjectured to be hard.
- DLOG in $\mathbb{Z}/(p-1)\mathbb{Z}$ is easy.

Effect of $|G|$ on DLOG

Size of G does have some effect on DLOG:

- All else being equal, a larger group size makes DLOG harder
- Certain group sizes are insecure no matter what the group
  - e.g. if $|G|$ is smooth (that is, all prime divisors of $|G|$ are small) then DLOG on G is easy.

On the other hand, size is not the only factor.
Groups of equal size can (conjecturally) have inequivalent discrete log problems.

- DLOG in $(\mathbb{Z}/p\mathbb{Z})^*$ is conjectured to be hard.
- DLOG in $\mathbb{Z}/(p-1)\mathbb{Z}$ is easy.
  - $\mathbb{Z}/(p-1)\mathbb{Z}$ is an additive group.

Effect of $|G|$ on DLOG

Size of G does have some effect on DLOG:

- All else being equal, a larger group size makes DLOG harder
- Certain group sizes are insecure no matter what the group
  - e.g. if $|G|$ is smooth (that is, all prime divisors of $|G|$ are small) then DLOG on G is easy.

On the other hand, size is not the only factor.
Groups of equal size can (conjecturally) have inequivalent discrete log problems.

- DLOG in $(\mathbb{Z}/p\mathbb{Z})^*$ is conjectured to be hard.
- DLOG in $\mathbb{Z}/(p-1)\mathbb{Z}$ is easy.
  - $\mathbb{Z}/(p-1)\mathbb{Z}$ is an additive group.
  - Group multiplication is addition.

Effect of $|G|$ on DLOG

Size of G does have some effect on DLOG:

- All else being equal, a larger group size makes DLOG harder
- Certain group sizes are insecure no matter what the group
  - e.g. if $|G|$ is smooth (that is, all prime divisors of $|G|$ are small) then DLOG on G is easy.

On the other hand, size is not the only factor.
Groups of equal size can (conjecturally) have inequivalent discrete log problems.

- DLOG in $(\mathbb{Z}/p\mathbb{Z})^*$ is conjectured to be hard.
- DLOG in $\mathbb{Z}/(p-1)\mathbb{Z}$ is easy.
  - $\mathbb{Z}/(p-1)\mathbb{Z}$ is an additive group.
  - Group multiplication is addition.
  - Group exponentiation is multiplication.

Effect of $|G|$ on DLOG

Size of G does have some effect on DLOG:

- All else being equal, a larger group size makes DLOG harder
- Certain group sizes are insecure no matter what the group
  - e.g. if $|G|$ is smooth (that is, all prime divisors of $|G|$ are small) then DLOG on G is easy.

On the other hand, size is not the only factor.
Groups of equal size can (conjecturally) have inequivalent discrete log problems.

- DLOG in $(\mathbb{Z}/p\mathbb{Z})^*$ is conjectured to be hard.
- DLOG in $\mathbb{Z}/(p-1)\mathbb{Z}$ is easy.
  - $\mathbb{Z}/(p-1)\mathbb{Z}$ is an additive group.
  - Group multiplication is addition.
  - Group exponentiation is multiplication.
  - Logarithm is division.

Effect of $|G|$ on DLOG

Size of G does have some effect on DLOG:

- All else being equal, a larger group size makes DLOG harder
- Certain group sizes are insecure no matter what the group
  - e.g. if $|G|$ is smooth (that is, all prime divisors of $|G|$ are small) then DLOG on G is easy.

On the other hand, size is not the only factor.
Groups of equal size can (conjecturally) have inequivalent discrete log problems.

- DLOG in $(\mathbb{Z}/p\mathbb{Z})^*$ is conjectured to be hard.
- DLOG in $\mathbb{Z}/(p-1)\mathbb{Z}$ is easy.
  - $\mathbb{Z}/(p-1)\mathbb{Z}$ is an additive group.
  - Group multiplication is addition.
  - Group exponentiation is multiplication.
  - Logarithm is division.
  - Divison is easy by Euclid's algorithm.

What determines the difficulty of DLOG?

- Choice of h does not matter on average.

What determines the difficulty of DLOG?

- Choice of h does not matter on average.
- Choice of g does not matter at all.

What determines the difficulty of DLOG?

- Choice of h does not matter on average.
- Choice of g does not matter at all.
- Choice of size of the group is *necessary* but not *sufficient* to ensure DLOG is hard.

What determines the difficulty of DLOG?

- Choice of h does not matter on average.
- Choice of g does not matter at all.
- Choice of size of the group is *necessary* but not *sufficient* to ensure DLOG is hard.
  - Group size must be relatively large
  - Group size must not be smooth

What determines the difficulty of DLOG?

- Choice of h does not matter on average.
- Choice of g does not matter at all.
- Choice of size of the group is *necessary* but not *sufficient* to ensure DLOG is hard.
  - Group size must be relatively large
  - Group size must not be smooth
- The choice of bit representation that one uses to represent elements of G is important.

What determines the difficulty of DLOG?

- Choice of h does not matter on average.
- Choice of g does not matter at all.
- Choice of size of the group is *necessary* but not *sufficient* to ensure DLOG is hard.
  - Group size must be relatively large
  - Group size must not be smooth
- The choice of bit representation that one uses to represent elements of G is important.
- After correcting for the above issues, it is widely believed that DLOG difficulty is a function of group size (within a single family of groups, bit representations, smoothness constraints, etc.)

Current status of DLOG in various groups

Any group of order n:

- $O(\sqrt{p})$ where p is the largest prime divisor of n [Pollard]

Current status of DLOG in various groups

Any group of order n:

- $O(\sqrt{p})$ where p is the largest prime divisor of n [Pollard]

Multiplicative group of a finite field $\mathbb{F}_q$:

- $O(L_q(\frac{1}{3}, c))$ where $L_q(\frac{1}{3}, c) \stackrel{\text{def}}{=} \exp(c(\log q)^{\frac{1}{3}}(\log\log q)^{1-\frac{1}{3}})$

Current status of DLOG in various groups

Any group of order n:

- $O(\sqrt{p})$ where p is the largest prime divisor of n [Pollard]

Multiplicative group of a finite field $\mathbb{F}_q$:

- $O(L_q(\frac{1}{3}, c))$ where $L_q(\frac{1}{3}, c) \stackrel{\text{def}}{=} \exp(c(\log q)^{\frac{1}{3}}(\log\log q)^{1-\frac{1}{3}})$

Ideal class group of an imaginary quadratic field:

- $L_n(\frac{1}{2}, c)$ [Hafner, McCurley; Düllmann]

Current status of DLOG in various groups

Any group of order n:

- $O(\sqrt{p})$ where p is the largest prime divisor of n [Pollard]

Multiplicative group of a finite field $\mathbb{F}_q$:

- $O(L_q(\frac{1}{3}, c))$ where $L_q(\frac{1}{3}, c) \stackrel{\text{def}}{=} \exp(c(\log q)^{\frac{1}{3}}(\log\log q)^{1-\frac{1}{3}})$

Ideal class group of an imaginary quadratic field:

- $L_n(\frac{1}{2}, c)$ [Hafner, McCurley; Düllmann]

Elliptic curves (with some exceptions):

- $O(\sqrt{p})$ where p is the largest prime divisor of n.

Current status of DLOG in various groups

Any group of order n:

- $O(\sqrt{p})$ where p is the largest prime divisor of n [Pollard]

Multiplicative group of a finite field $\mathbb{F}_q$:

- $O(L_q(\frac{1}{3}, c))$ where $L_q(\frac{1}{3}, c) \stackrel{\text{def}}{=} \exp(c(\log q)^{\frac{1}{3}}(\log\log q)^{1-\frac{1}{3}})$

Ideal class group of an imaginary quadratic field:

- $L_n(\frac{1}{2}, c)$ [Hafner, McCurley; Düllmann]

Elliptic curves (with some exceptions):

- $O(\sqrt{p})$ where p is the largest prime divisor of n.

Jacobians of hyperelliptic curves of genus g over a finite field $\mathbb{F}_q$:

- $g = 2$: $O(n^{1/2})$
- $g = 3$: $O(n^{4/9})$ [Gaudry, Thomé, Thériault, Diem]
- $g = 4$: $O(n^{3/8})$ ["]
- $g \geq \log q$: $O(L_n(\frac{1}{2}, c))$ [Adelman, DeMarrais, Huang; Enge, Gaudry]

Current status of DLOG in various groups

Any group of order n:

- $O(\sqrt{p})$ where p is the largest prime divisor of n [Pollard]

Multiplicative group of a finite field $\mathbb{F}_q$:

- $O(L_q(\frac{1}{3}, c))$ where $L_q(\frac{1}{3}, c) \stackrel{\text{def}}{=} \exp(c(\log q)^{\frac{1}{3}}(\log\log q)^{1-\frac{1}{3}})$

Ideal class group of an imaginary quadratic field:

- $L_n(\frac{1}{2}, c)$ [Hafner, McCurley; Düllmann]

Elliptic curves (with some exceptions):

- $O(\sqrt{p})$ where p is the largest prime divisor of n.

Jacobians of hyperelliptic curves of genus g over a finite field $\mathbb{F}_q$:

- $g = 2$: $O(n^{1/2})$
- $g = 3$: $O(n^{4/9})$ [Gaudry, Thomé, Thériault, Diem]
- $g = 4$: $O(n^{3/8})$ ["]
- $g \geq \log q$: $O(L_n(\frac{1}{2}, c))$ [Adelman, DeMarrais, Huang; Enge, Gaudry]

In all cases, DLOG difficulty is a function of group size.

Outline

The concept of DLOG reduction

- Goal: To establish relationships between discrete logarithms on group A and group B.
- The basic tool for this reduction is group homomorphisms.
- Let $\phi\colon G \to G'$ be a group homomorphism. To simplify, we assume that G has prime order.

The concept of DLOG reduction

- Goal: To establish relationships between discrete logarithms on group A and group B.
- The basic tool for this reduction is group homomorphisms.
- Let $\phi\colon G \to G'$ be a group homomorphism. To simplify, we assume that G has prime order.
- Let $g, h \in G$. To compute $\mathrm{DLOG}_g(h)$ in G:

The concept of DLOG reduction

- Goal: To establish relationships between discrete logarithms on group A and group B.
- The basic tool for this reduction is group homomorphisms.
- Let $\phi\colon G \to G'$ be a group homomorphism. To simplify, we assume that G has prime order.
- Let $g, h \in G$. To compute $\mathrm{DLOG}_g(h)$ in G:
  1. Compute $\phi(g)$ and $\phi(h)$

The concept of DLOG reduction

- Goal: To establish relationships between discrete logarithms on group A and group B.
- The basic tool for this reduction is group homomorphisms.
- Let $\phi\colon G \to G'$ be a group homomorphism. To simplify, we assume that G has prime order.
- Let $g, h \in G$. To compute $\mathrm{DLOG}_g(h)$ in G:
  1. Compute $\phi(g)$ and $\phi(h)$
  2. Compute $x = \mathrm{DLOG}_{\phi(g)}(\phi(h))$

The concept of DLOG reduction

- Goal: To establish relationships between discrete logarithms on group A and group B.
- The basic tool for this reduction is group homomorphisms.
- Let $\phi\colon G \to G'$ be a group homomorphism. To simplify, we assume that G has prime order.
- Let $g, h \in G$. To compute $\mathrm{DLOG}_g(h)$ in G:
  1. Compute $\phi(g)$ and $\phi(h)$
  2. Compute $x = \mathrm{DLOG}_{\phi(g)}(\phi(h))$
  3. Then $x = \mathrm{DLOG}_g(h)$, because $g^x = h$ if and only if $\phi(g)^x = \phi(h)$.

The concept of DLOG reduction

- Goal: To establish relationships between discrete logarithms on group A and group B.
- The basic tool for this reduction is group homomorphisms.
- Let $\phi\colon G \to G'$ be a group homomorphism. To simplify, we assume that G has prime order.
- Let $g, h \in G$. To compute $\mathrm{DLOG}_g(h)$ in G:
  1. Compute $\phi(g)$ and $\phi(h)$
  2. Compute $x = \mathrm{DLOG}_{\phi(g)}(\phi(h))$
  3. Then $x = \mathrm{DLOG}_g(h)$, because $g^x = h$ if and only if $\phi(g)^x = \phi(h)$.
- In other words, if you can easily compute DLOG in G' (Step 2), then you can easily compute DLOG in G.

The concept of DLOG reduction

- Goal: To establish relationships between discrete logarithms on group A and group B.
- The basic tool for this reduction is group homomorphisms.
- Let $\phi\colon G \to G'$ be a group homomorphism. To simplify, we assume that G has prime order.
- Let $g, h \in G$. To compute $\mathrm{DLOG}_g(h)$ in G:
  1. Compute $\phi(g)$ and $\phi(h)$
  2. Compute $x = \mathrm{DLOG}_{\phi(g)}(\phi(h))$
  3. Then $x = \mathrm{DLOG}_g(h)$, because $g^x = h$ if and only if $\phi(g)^x = \phi(h)$.
- In other words, if you can easily compute DLOG in G' (Step 2), then you can easily compute DLOG in G.
- However, you also need to be able to easily compute the homomorphism ϕ (Step 1).

Elliptic curves

- A group homomorphism between elliptic curves is called an *isogeny*.
- An isogeny is a rational function — it is given by a quotient of polynomials.
- The *degree* of an isogeny is the degree of the polynomial.
- **Theorem (Tate, 1966):** Two elliptic curves over a finite field have the same size if and only if they are *isogenous* (i.e. there exists an isogeny between them).
- Isogenous is an equivalence relation. We will call the equivalence classes *isogeny classes*.

Example of an isogeny

- $p = 7925599076663155737601$
- $E_1 : y^2 = x^3 + 12046162683058694734 * x + 7901506751297038348133$ in GF(p)
- $E_2 : y^2 = x^3 + (3021319262486407622796 * u + 4101162511412606196442) * x + (7040333493178698383420 * u + 174577275676632103431)$ in GF(p^2)
- ϕ: $E_1 \longrightarrow E_2$ given by $\phi(x, y) = ((x^7 + (2646061772402770501474 * u + 28775605307889315926 5) * x^6 + (13293530722861505653 8 * u + 3530390499615039152484) * x^5 + (463794718376492302 73 * u + 1073811655050424931224) * x^4 + (2474785317056152334847 * u + 1839199255709390890698) * x^3 + (4285381276738035289332 * u + 2268033696082534919907) * x^2 + (1160928171089162069604 * u + 447867418402154326079 3) * x + (3220829138361157238167 * u + 4664892256879213165649))/(x^6 + (2646061772402770501474 * u + 28775605307889315926 5) * x^5 + (1945985508507744496834 * u + 648093055215868995 31) * x^4 + (4591727489633569666202 * u + 1570102870983786495532) * x^3 + (1500460390828721967700 * u + 692170444361451309763 5) * x^2 + (1297386801518789580736 * u + 285069874090833393640 0) * x + (3945372319876153578002 * u + 361974201101530900968)), (x^9 * y + (396909265860415575221 1 * u + 439443361794991760769 8) * x^8 * y + (653503558986201519334 8 * u + 779053291492004982110 9) * x^7 * y + (142198737502751098509 1 * u + 47681237267235708636) * x^6 * y + (230396899509609634966 1 * u + 3345680927799022267788) * x^5 * y + (243327773580243744178 9 * u + 335179462792558750055 3) * x^4 * y + (151602679570769848004 6 * u + 818260455738162732467) * x^3 * y + (102705817773763612561 4 * u + 3693613550368489401398) * x^2 * y + (450864584106502597890 9 * u + 491859307018303225658 5) * x * y + (8333818603777677580 * u + 6166744817175250513803) * y)/(x^9 + (396909265860415575221 1 * u + 439443361794991760769 8) * x^8 + (472198538858288575305 2 * u + 333051503235034633646 1) * x^7 + (355977212666782882640 97 * u + 615342200698874578176 5) * x^6 + (190294095199030591345 2 * u + 832145497772529583998) * x^5 + (255389155365196737883 3 * u + 549429624397957274232) * x^4 + (582104136352814424328 1 * u + 489551452715872062891 8) * x^3 + (746557228296674389403 4 * u + 123645603788466192332) * x^2 + (475221656789097062097 8 * u + 497829871306819801522) * x + (6192295778031003334018 * u + 4253951270570522301 94)))

Efficient computation of isogenies

- **Theorem (Tate, 1966):** Two elliptic curves over a finite field have the same size if and only if they are isogenous.
- If this isogeny could be **obtained** and **evaluated** efficiently, then we could state that elliptic curves of equal size have equivalent discrete logarithms.

Efficient computation of isogenies

- **Theorem (Tate, 1966):** Two elliptic curves over a finite field have the same size if and only if they are isogenous.
- If this isogeny could be **obtained** and **evaluated** efficiently, then we could state that elliptic curves of equal size have equivalent discrete logarithms.
- Unfortunately, the only known examples of isogenies that can be efficiently evaluated are:

Efficient computation of isogenies

- **Theorem (Tate, 1966):** Two elliptic curves over a finite field have the same size if and only if they are isogenous.
- If this isogeny could be **obtained** and **evaluated** efficiently, then we could state that elliptic curves of equal size have equivalent discrete logarithms.
- Unfortunately, the only known examples of isogenies that can be efficiently evaluated are:
  1. Isogenies of low degree

Efficient computation of isogenies

- **Theorem (Tate, 1966):** Two elliptic curves over a finite field have the same size if and only if they are isogenous.
- If this isogeny could be **obtained** and **evaluated** efficiently, then we could state that elliptic curves of equal size have equivalent discrete logarithms.
- Unfortunately, the only known examples of isogenies that can be efficiently evaluated are:
  1. Isogenies of low degree
  2. (sometimes) Endomorphisms (that is, isogenies from a curve to itself)

Efficient computation of isogenies

- **Theorem (Tate, 1966):** Two elliptic curves over a finite field have the same size if and only if they are isogenous.
- If this isogeny could be **obtained** and **evaluated** efficiently, then we could state that elliptic curves of equal size have equivalent discrete logarithms.
- Unfortunately, the only known examples of isogenies that can be efficiently evaluated are:
  1. Isogenies of low degree
  2. (sometimes) Endomorphisms (that is, isogenies from a curve to itself)
  3. Short compositions of isogenies of the above type

Efficient computation of isogenies

- **Theorem (Tate, 1966):** Two elliptic curves over a finite field have the same size if and only if they are isogenous.
- If this isogeny could be **obtained** and **evaluated** efficiently, then we could state that elliptic curves of equal size have equivalent discrete logarithms.
- Unfortunately, the only known examples of isogenies that can be efficiently evaluated are:
  1. Isogenies of low degree
  2. (sometimes) Endomorphisms (that is, isogenies from a curve to itself)
  3. Short compositions of isogenies of the above type
- Endomorphisms are not useful for reductions between **different** curves, so for reduction we must use isogenies of low degree.

Outline

Using isogenies to relate DLOG on elliptic curves

- Form a graph whose vertices are elliptic curves E and whose edges are low degree isogenies $\phi\colon E_1 \to E_2$.
- Galbraith (1999) observed that random walks on this graph produce efficiently computable isogenies which can be used for DLOG reduction.

Using isogenies to relate DLOG on elliptic curves

- Form a graph whose vertices are elliptic curves E and whose edges are low degree isogenies $\phi\colon E_1 \to E_2$.
- Galbraith (1999) observed that random walks on this graph produce efficiently computable isogenies which can be used for DLOG reduction.

1. These efficiently computable isogenies exist only when E_1 and E_2 are **endomorphous** or **near-endomorphous**.
   - Definition: Two elliptic curves over a finite field are *endomorphous* (resp., *near-endomorphous*) if their endomorphism rings are equal (resp., nearly equal).
   - Endomorphous is an equivalence relation. We will call the equivalence classes *endomorphism classes*.
   - All endomorphous and near endomorphous curves are isogenous.
   - For most isogeny classes, the converse holds: isogenous curves are near-endomorphous. However, there are exceptions.

Using isogenies to relate DLOG on elliptic curves

- Form a graph whose vertices are elliptic curves E and whose edges are low degree isogenies $\phi\colon E_1 \to E_2$.
- Galbraith (1999) observed that random walks on this graph produce efficiently computable isogenies which can be used for DLOG reduction.

1. These efficiently computable isogenies exist only when E_1 and E_2 are **endomorphous** or **near-endomorphous**.
   - Definition: Two elliptic curves over a finite field are *endomorphous* (resp., *near-endomorphous*) if their endomorphism rings are equal (resp., nearly equal).
   - Endomorphous is an equivalence relation. We will call the equivalence classes *endomorphism classes*.
   - All endomorphous and near endomorphous curves are isogenous.
   - For most isogeny classes, the converse holds: isogenous curves are near-endomorphous. However, there are exceptions.
2. Requires the heuristic assumption that *short* random walks have *roughly* uniform probability of reaching every vertex.

Using isogenies to relate DLOG on elliptic curves (cont'd)

- **Theorem:** (Jao, Miller, Venkatesan) Assuming the generalized Riemann hypothesis, there exists an absolute constant c such that random walks of length $(\log n)^c$ deviate from uniform probability by no more than a factor of 2, for isogenies of degree less than $c(\log n)^2$.

Using isogenies to relate DLOG on elliptic curves (cont'd)

- **Theorem:** (Jao, Miller, Venkatesan) Assuming the generalized Riemann hypothesis, there exists an absolute constant c such that random walks of length $(\log n)^c$ deviate from uniform probability by no more than a factor of 2, for isogenies of degree less than $c(\log n)^2$.
- Proof relies on the correspondence between curves in an endomorphism class and ideal classes in an imaginary quadratic order (or in a quaternion algebra).

Using isogenies to relate DLOG on elliptic curves (cont'd)

- **Theorem:** (Jao, Miller, Venkatesan) Assuming the generalized Riemann hypothesis, there exists an absolute constant c such that random walks of length $(\log n)^c$ deviate from uniform probability by no more than a factor of 2, for isogenies of degree less than $c(\log n)^2$.
- Proof relies on the correspondence between curves in an endomorphism class and ideal classes in an imaginary quadratic order (or in a quaternion algebra).
- Curves are still required to be endomorphous or near-endomorphous.

Using isogenies to relate DLOG on elliptic curves (cont'd)

- **Theorem:** (Jao, Miller, Venkatesan) Assuming the generalized Riemann hypothesis, there exists an absolute constant c such that random walks of length $(\log n)^c$ deviate from uniform probability by no more than a factor of 2, for isogenies of degree less than $c(\log n)^2$.
- Proof relies on the correspondence between curves in an endomorphism class and ideal classes in an imaginary quadratic order (or in a quaternion algebra).
- Curves are still required to be endomorphous or near-endomorphous.
- **Corollary:** All near-endomorphous elliptic curves over the same field have equivalent discrete logarithm problems **on average**.

Outline

Weil Descent

- Discovered by [Gaudry, Hess, Smart]
- Let E be an elliptic curve over $\mathbb{F}_{q^k}$. There exists a computable group homomorphism from E to a hyperelliptic Jacobian over $\mathbb{F}_q$.

Weil Descent

- Discovered by [Gaudry, Hess, Smart]
- Let E be an elliptic curve over $\mathbb{F}_{q^k}$. There exists a computable group homomorphism from E to a hyperelliptic Jacobian over $\mathbb{F}_q$.
- For some values of E and q^k, the genus of the hyperelliptic curve is large enough to make this attack practical.

Weil Descent

- Discovered by [Gaudry, Hess, Smart]
- Let E be an elliptic curve over $\mathbb{F}_{q^k}$. There exists a computable group homomorphism from E to a hyperelliptic Jacobian over $\mathbb{F}_q$.
- For some values of E and q^k, the genus of the hyperelliptic curve is large enough to make this attack practical.
- If E' is isogenous to a curve E which is vulnerable to Weil descent, then E' can be attacked too [Galbraith, Hess, Smart]
  - Construction relies on random walks of isogenies
  - Requires uniform mixing of random walks

Reductions from elliptic curves to hyperelliptic Jacobians

- Informally: If you can improve the current state of the art for subexponential hyperelliptic curve discrete logarithms, then elliptic curve discrete logarithms are also affected [Bauer, Hamdy]

Reductions from elliptic curves to hyperelliptic Jacobians

- Informally: If you can improve the current state of the art for subexponential hyperelliptic curve discrete logarithms, then elliptic curve discrete logarithms are also affected [Bauer, Hamdy]
- Current DLOG algorithms for hyperelliptic curves are $O(L_n(\frac{1}{2}, c))$ for genus $g \geq \log q$.

Reductions from elliptic curves to hyperelliptic Jacobians

- Informally: If you can improve the current state of the art for subexponential hyperelliptic curve discrete logarithms, then elliptic curve discrete logarithms are also affected [Bauer, Hamdy]
- Current DLOG algorithms for hyperelliptic curves are $O(L_n(\frac{1}{2}, c))$ for genus $g \geq \log q$.
- $O(L_n(\alpha, c))$ for $\alpha < \frac{1}{2}$ implies elliptic curve DLOG is subexponential.

Reductions from elliptic curves to hyperelliptic Jacobians

- Informally: If you can improve the current state of the art for subexponential hyperelliptic curve discrete logarithms, then elliptic curve discrete logarithms are also affected [Bauer, Hamdy]
- Current DLOG algorithms for hyperelliptic curves are $O(L_n(\frac{1}{2}, c))$ for genus $g \geq \log q$.
- $O(L_n(\alpha, c))$ for $\alpha < \frac{1}{2}$ implies elliptic curve DLOG is subexponential.
- $O(L_n(\frac{1}{2}, c))$ for $g \ll \log q$ implies elliptic curve DLOG is subexponential.

Reductions from elliptic curves to hyperelliptic Jacobians

- Informally: If you can improve the current state of the art for subexponential hyperelliptic curve discrete logarithms, then elliptic curve discrete logarithms are also affected [Bauer, Hamdy]
- Current DLOG algorithms for hyperelliptic curves are $O(L_n(\frac{1}{2}, c))$ for genus $g \geq \log q$.
- $O(L_n(\alpha, c))$ for $\alpha < \frac{1}{2}$ implies elliptic curve DLOG is subexponential.
- $O(L_n(\frac{1}{2}, c))$ for $g \ll \log q$ implies elliptic curve DLOG is subexponential.
- Subexponential for $g = 2[, 4, 5, 7, 8, 10, \ldots]$ implies elliptic curve DLOG is subexponential.

Outline

1. Discrete Logarithms
   - Definitions and notation
   - Relationship between different groups; DLOG reduction
2. Known facts about DLOG reduction
   - Reductions between elliptic curves
   - Reductions from elliptic curves to hyperelliptic Jacobians
3. Open problems in DLOG reduction
   - Elliptic curves not admitting reductions
   - Reductions between hyperelliptic Jacobians
   - Reductions from elliptic curves to non-hyperelliptic Jacobians

Elliptic curves which are not near-endomorphous

- There exist elliptic curves E_1, E_2 over the same finite field which are isogenous but neither endomorphous nor near-endomorphous.

Elliptic curves which are not near-endomorphous

- There exist elliptic curves E_1, E_2 over the same finite field which are isogenous but neither endomorphous nor near-endomorphous.
- There is no known algorithm for efficiently constructing such pairs of elliptic curves.

Elliptic curves which are not near-endomorphous

- There exist elliptic curves E_1, E_2 over the same finite field which are isogenous but neither endomorphous nor near-endomorphous.
- There is no known algorithm for efficiently constructing such pairs of elliptic curves.
- There is no known example of such a pair of elliptic curves.

Removing the "on average" clause

- Given arbitrary (not random) curves E_1 and E_2, can we show that their DLOG problems are equivalent?

Removing the "on average" clause

- Given arbitrary (not random) curves E_1 and E_2, can we show that their DLOG problems are equivalent?
- Let $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be ideal classes corresponding to E_1 and E_2.

Removing the "on average" clause

- Given arbitrary (not random) curves E_1 and E_2, can we show that their DLOG problems are equivalent?
- Let $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be ideal classes corresponding to E_1 and E_2.
- Finding an efficiently computable isogeny $\phi\colon E_1 \to E_2$ is equivalent to factoring the ideal class $\mathfrak{a}_1\mathfrak{a}_2^{-1}$ into a product of small primes.

Removing the "on average" clause

- Given arbitrary (not random) curves E_1 and E_2, can we show that their DLOG problems are equivalent?
- Let $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be ideal classes corresponding to E_1 and E_2.
- Finding an efficiently computable isogeny $\phi\colon E_1 \to E_2$ is equivalent to factoring the ideal class $\mathfrak{a}_1\mathfrak{a}_2^{-1}$ into a product of small primes.
- If you can do that efficiently, then you can solve DLOG on the ideal class group efficiently, using index calculus.

Removing the "on average" clause

- Given arbitrary (not random) curves E_1 and E_2, can we show that their DLOG problems are equivalent?
- Let $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be ideal classes corresponding to E_1 and E_2.
- Finding an efficiently computable isogeny $\phi\colon E_1 \to E_2$ is equivalent to factoring the ideal class $\mathfrak{a}_1\mathfrak{a}_2^{-1}$ into a product of small primes.
- If you can do that efficiently, then you can solve DLOG on the ideal class group efficiently, using index calculus.
  - This scenario seems unlikely, because an $O(L_n(\frac{1}{3}, c))$ algorithm for solving DLOG on ideal class groups leads to a subexponential solution of DLOG on elliptic curves [Bauer, Hamdy].

Removing the "on average" clause

- Given arbitrary (not random) curves E_1 and E_2, can we show that their DLOG problems are equivalent?
- Let $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be ideal classes corresponding to E_1 and E_2.
- Finding an efficiently computable isogeny $\phi\colon E_1 \to E_2$ is equivalent to factoring the ideal class $\mathfrak{a}_1\mathfrak{a}_2^{-1}$ into a product of small primes.
- If you can do that efficiently, then you can solve DLOG on the ideal class group efficiently, using index calculus.
  - This scenario seems unlikely, because an $O(L_n(\frac{1}{3}, c))$ algorithm for solving DLOG on ideal class groups leads to a subexponential solution of DLOG on elliptic curves [Bauer, Hamdy].
- However, note that representing ideal classes using elliptic curves is not the same as representing ideal classes using quadratic forms.

Removing the "on average" clause

- Given arbitrary (not random) curves E_1 and E_2, can we show that their DLOG problems are equivalent?
- Let $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be ideal classes corresponding to E_1 and E_2.
- Finding an efficiently computable isogeny $\phi\colon E_1 \to E_2$ is equivalent to factoring the ideal class $\mathfrak{a}_1\mathfrak{a}_2^{-1}$ into a product of small primes.
- If you can do that efficiently, then you can solve DLOG on the ideal class group efficiently, using index calculus.
  - This scenario seems unlikely, because an $O(L_n(\frac{1}{3}, c))$ algorithm for solving DLOG on ideal class groups leads to a subexponential solution of DLOG on elliptic curves [Bauer, Hamdy].
- However, note that representing ideal classes using elliptic curves is not the same as representing ideal classes using quadratic forms.
  - Remember, bit representation matters for DLOG!

Elliptic curves over different fields

- So far, all elliptic curves have been defined over a common finite field.
- What can we say about curves over different fields?

Elliptic curves over different fields

- So far, all elliptic curves have been defined over a common finite field.
- What can we say about curves over different fields?
- It is known that elliptic curves over $\mathbb{F}_{2^{210}}$ have weaker DLOG than curves of the same size over other fields [Menezes, Teske, Weng]

Elliptic curves over different fields

- So far, all elliptic curves have been defined over a common finite field.
- What can we say about curves over different fields?
- It is known that elliptic curves over $\mathbb{F}_{2^{210}}$ have weaker DLOG than curves of the same size over other fields [Menezes, Teske, Weng]
  - Proof of this fact also uses random walks on isogenies

Elliptic curves over different fields

- So far, all elliptic curves have been defined over a common finite field.
- What can we say about curves over different fields?
- It is known that elliptic curves over $\mathbb{F}_{2^{210}}$ have weaker DLOG than curves of the same size over other fields [Menezes, Teske, Weng]
  - Proof of this fact also uses random walks on isogenies
- Can we prove equivalence results for other fields?

Other reductions

1. Reductions between hyperelliptic Jacobians
   - What is the structure of isogenies between hyperelliptic Jacobians?
   - What does the graph of isogenies look like?

Other reductions

1. Reductions between hyperelliptic Jacobians
   - What is the structure of isogenies between hyperelliptic Jacobians?
   - What does the graph of isogenies look like?
2. Reductions from elliptic curves to non-hyperelliptic Jacobians
   - $O(L_n(\frac{1}{3}, c))$ solutions to DLOG have been found on Jacobians of certain non-hyperelliptic curves [Enge, Gaudry; Diem]
   - What are the implications for elliptic curve DLOG?

Other reductions

1. Reductions between hyperelliptic Jacobians
   - What is the structure of isogenies between hyperelliptic Jacobians?
   - What does the graph of isogenies look like?
2. Reductions from elliptic curves to non-hyperelliptic Jacobians
   - $O(L_n(\frac{1}{3}, c))$ solutions to DLOG have been found on Jacobians of certain non-hyperelliptic curves [Enge, Gaudry; Diem]
   - What are the implications for elliptic curve DLOG?
   - Stay tuned ...