Problème du logarithme discret sur courbes elliptiques

Vanessa VITSE

Université de Versailles Saint-Quentin, Laboratoire PRISM

Groupe de travail équipe ARITH – LIRMM

Discrete logarithm problem

Discrete logarithm problem (DLP)

Given a group G and $g, h \in G$, find – when it exists – an integer x s.t.

$$h = g^x$$

Discrete logarithm problem

Discrete logarithm problem (DLP)

Given a group G and $g, h \in G$, find – when it exists – an integer x s.t.

$$h = g^x$$

Difficulty is related to the group:

1. Generic attack: complexity in $\Omega(\max(\alpha_i\sqrt{p_i}))$ if $\#G = \prod_i p_i^{\alpha_i}$

Discrete logarithm problem

Discrete logarithm problem (DLP)

Given a group G and $g, h \in G$, find – when it exists – an integer x s.t.

$$h = g^x$$

Difficulty is related to the group:

1. Generic attack: complexity in $\Omega(\max(\alpha_i \sqrt{p_i}))$ if $\#G = \prod_i p_i^{\alpha_i}$
2. $G \subset (\mathbb{Z}/n\mathbb{Z}, +)$: solving DLP has polynomial complexity with extended Euclid algorithm

Discrete logarithm problem

Discrete logarithm problem (DLP)

Given a group G and $g, h \in G$, find – when it exists – an integer x s.t.

$$h = g^x$$

Difficulty is related to the group:

1. Generic attack: complexity in $\Omega(\max(\alpha_i \sqrt{p_i}))$ if $\#G = \prod_i p_i^{\alpha_i}$
2. $G \subset (\mathbb{Z}/n\mathbb{Z}, +)$: solving DLP has polynomial complexity with extended Euclid algorithm
3. $G \subset (\mathbb{F}_q^*, \times)$: index calculus method with complexity in $L_q(1/3)$ where $L_q(\alpha) = \exp(c(\log q)^\alpha (\log \log q)^{1-\alpha})$.

Discrete logarithm problem

Discrete logarithm problem (DLP)

Given a group G and $g, h \in G$, find – when it exists – an integer x s.t.

$$h = g^x$$

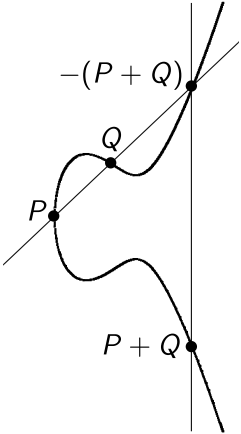
Difficulty is related to the group:

1. Generic attack: complexity in $\Omega(\max(\alpha_i\sqrt{p_i}))$ if $\#G = \prod_i p_i^{\alpha_i}$
2. $G \subset (\mathbb{Z}/n\mathbb{Z}, +)$: solving DLP has polynomial complexity with extended Euclid algorithm
3. $G \subset (\mathbb{F}_q^*, \times)$: index calculus method with complexity in $L_q(1/3)$ where $L_q(\alpha) = \exp(c(\log q)^\alpha(\log\log q)^{1-\alpha})$.
4. $G \subset (\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q), +)$: index calculus method asymptotically faster than generic attacks, depending of the genus $g > 2$

Elliptic curve DLP

Good candidates for DLP-based cryptosystems:

elliptic curves defined over finite fields



ECDLP: Given $P \in E(\mathbb{F}_q)$ and $Q \in \langle P \rangle$ find x such that $Q = [x]P$

- On $\mathbb{F}_p$ (p prime): in general, no known attack better than generic algorithms
  $\rightarrow$ good security
- On $\mathbb{F}_{p^n}$ (for faster hardware arithmetic): possible to apply *index calculus*
  $\rightarrow$ security reduction in some cases

Section 1

The index calculus method

Introduction to index calculus

Originally developed for the factorization of large integers, improving on the square congruence method of Fermat.

Index calculus based Number/Function Field Sieve hold records for both integer factorization and finite field DLP.

Idea

- Find group relations between a "small" number of generators (or *factor base* elements)
- With sufficiently many relations and linear algebra, deduce the group structure and the DL of elements

Basic outline

$(G, +) = \langle g \rangle$ finite abelian group of prime order r, $h \in G$

1. Choice of a factor base: $\mathcal{F} = \{g_1, \ldots, g_N\} \subset G$

Basic outline

$(G,+) = \langle g \rangle$ finite abelian group of prime order r, $h \in G$

1. Choice of a factor base: $\mathcal{F} = \{g_1, \ldots, g_N\} \subset G$
2. Relation search: decompose $[a_i]g + [b_i]h$ (a_i, b_i random) into $\mathcal{F}$

$$[a_i]g + [b_i]h = \sum_{j=1}^{N} [c_{ij}]g_j, \text{ where } c_{ij} \in \mathbb{Z}$$

Basic outline

$(G, +) = \langle g \rangle$ finite abelian group of prime order r, $h \in G$

1. Choice of a factor base: $\mathcal{F} = \{g_1, \ldots, g_N\} \subset G$
2. Relation search: decompose $[a_i]g + [b_i]h$ (a_i, b_i random) into $\mathcal{F}$

$$[a_i]g + [b_i]h = \sum_{j=1}^{N} [c_{ij}]g_j, \text{ where } c_{ij} \in \mathbb{Z}$$

3. Linear algebra: once k relations found ($k \geq N$)
   - construct the matrices $A = \begin{pmatrix} a_i & b_i \end{pmatrix}_{1 \leq i \leq k}$ and $M = (c_{ij})_{\substack{1 \leq i \leq k \\ 1 \leq j \leq N}}$
   - find $v = (v_1, \ldots, v_k) \in \ker({}^t M)$ such that $vA \neq \begin{pmatrix} 0 & 0 \end{pmatrix} \mod r$
   - compute the solution of DLP: $x = -\left(\sum_i a_i v_i\right) / \left(\sum_i b_i v_i\right) \mod r$

An example: the prime field case

- Choice of factor base: equivalence classes of prime integers smaller than a smoothness bound B (usually together with -1)
- Relation search: a combination $[a_i]g$ yields a relation if its representative in $\left[-\frac{p-1}{2}; \frac{p-1}{2}\right]$ is B-smooth

An example: the prime field case

- Choice of factor base: equivalence classes of prime integers smaller than a smoothness bound B (usually together with -1)
- Relation search: a combination $[a_i]g$ yields a relation if its representative in $\left[-\frac{p-1}{2}; \frac{p-1}{2}\right]$ is B-smooth

$p = 107$, $G = \mathbb{Z}/p\mathbb{Z}^*$, $g = 31$, $\mathcal{F} = \{-1; 2; 3; 5; 7\}$, find the DL of $h = 19$.

An example: the prime field case

- Choice of factor base: equivalence classes of prime integers smaller than a smoothness bound B (usually together with -1)
- Relation search: a combination $[a_i]g$ yields a relation if its representative in $\left[-\frac{p-1}{2}; \frac{p-1}{2}\right]$ is B-smooth

$p = 107$, $G = \mathbb{Z}/p\mathbb{Z}^*$, $g = 31$, $\mathcal{F} = \{-1; 2; 3; 5; 7\}$, find the DL of $h = 19$.

$$
\begin{aligned}
g^1 &= 31, \text{ not smooth} \\
g^2 &= -2 = -1 \times 2 \\
g^3 &= 45 = 3^2 \times 5 \\
g^4 &= 4 = 2^2 \\
g^5 &= 17, \text{ not smooth}
\end{aligned}
$$

An example: the prime field case

- Choice of factor base: equivalence classes of prime integers smaller than a smoothness bound B (usually together with -1)
- Relation search: a combination $[a_i]g$ yields a relation if its representative in $\left[-\frac{p-1}{2}; \frac{p-1}{2}\right]$ is B-smooth

$p = 107$, $G = \mathbb{Z}/p\mathbb{Z}^*$, $g = 31$, $\mathcal{F} = \{-1; 2; 3; 5; 7\}$, find the DL of $h = 19$.

$$\begin{aligned}
g^1 &= 31, \text{ not smooth} \\
g^2 &= -2 = -1 \times 2 \\
g^3 &= 45 = 3^2 \times 5 \\
g^4 &= 4 = 2^2 \\
g^5 &= 17, \text{ not smooth} \\
&\ldots
\end{aligned}$$

$$\begin{aligned}
&\ldots \\
g^{13} &= -49 = -1 \times 7^2 \\
g^{14} &= -21 = -1 \times 3 \times 7 \\
g^{15} &= -9 = -1 \times 3^2 \\
g^{16} &= 42 = 2 \times 3 \times 7 \\
g^{21} &= -35 = -1 \times 5 \times 7
\end{aligned}$$

An example: the prime field case

- Choice of factor base: equivalence classes of prime integers smaller than a smoothness bound B (usually together with -1)
- Relation search: a combination $[a_i]g$ yields a relation if its representative in $\left[-\frac{p-1}{2}; \frac{p-1}{2}\right]$ is B-smooth

$p = 107$, $G = \mathbb{Z}/p\mathbb{Z}^*$, $g = 31$, $\mathcal{F} = \{-1; 2; 3; 5; 7\}$, find the DL of $h = 19$.

$$\begin{pmatrix} 2 \\ 3 \\ 4 \\ 13 \\ 14 \\ 15 \\ 16 \\ 21 \end{pmatrix} = \begin{array}{c} \begin{array}{ccccc} -1 & 2 & 3 & 5 & 7 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array} X \mod 106 \quad \Rightarrow \quad X = \begin{pmatrix} 53 \\ 55 \\ 34 \\ 41 \\ 33 \end{pmatrix}$$

An example: the prime field case

- Choice of factor base: equivalence classes of prime integers smaller than a smoothness bound B (usually together with -1)
- Relation search: a combination $[a_i]g$ yields a relation if its representative in $\left[-\frac{p-1}{2}; \frac{p-1}{2}\right]$ is B-smooth

$p = 107$, $G = \mathbb{Z}/p\mathbb{Z}^*$, $g = 31$, $\mathcal{F} = \{-1; 2; 3; 5; 7\}$, find the DL of $h = 19$.

$$\log(-1) = 53 \quad \log(2) = 55 \quad \log(3) = 34 \quad \log(5) = 41 \quad \log(7) = 33$$

$$gh = 54 = 2 \times 3^3 = (g^{55})(g^{34})^3 = g^{51} \Rightarrow h = g^{50}$$

General remarks

1. Relation search very specific to the group and can be the main obstacle

2. On the other hand, linear algebra almost the same for all groups

3. Balance to find between the two phases:
   - if $\#\mathcal{F}$ small, few relations needed and fast linear algebra but small probability of decomposition $\rightsquigarrow$ many trials before finding a relation

   - if $\#\mathcal{F}$ large, easy to find relations but many of them needed and slow linear algebra

The linear algebra step

The matrix of relations

- very large for real-world applications: typical size is several millions rows/columns.
- extremely **sparse**: only a few non-zero coefficients per row

$\Rightarrow$ use sparse linear algebra techniques instead of standard resolution tools

The linear algebra step

The matrix of relations

- very large for real-world applications: typical size is several millions rows/columns.
- extremely **sparse**: only a few non-zero coefficients per row

$\Rightarrow$ use sparse linear algebra techniques instead of standard resolution tools

Main ideas:

- Keep the matrix sparse (~~Gauss~~)
- Use matrix-vector products: cost only proportional to the number of non-zero entries

Two principal algorithms: Lanczos and Wiedemann

Complexity in $O(n^2c)$ if n relations with c non-zero entries per relation

Improving the linear algebra step

Remark

- Relation search always straightforward to distribute
- Not so true for the linear algebra

Often advantageous to compute many more relations than needed and use extra information to simplify the relation matrix

Two methods:

1. **Structured Gaussian elimination:**
   Particularly well-suited when elements of the factor base have different frequencies (e.g on finite fields)
2. **Large prime variations**

Structured Gaussian elimination [LaMacchia-Odlyzko]

Goal: reduce the size of the matrix while keeping it sparse.
Distinction between the matrix columns (i.e. the factor base elements):

- dense columns correspond to “small primes”
- other columns correspond to “large primes”

Structured Gaussian elimination [LaMacchia-Odlyzko]

Goal: reduce the size of the matrix while keeping it sparse.
Distinction between the matrix columns (i.e. the factor base elements):

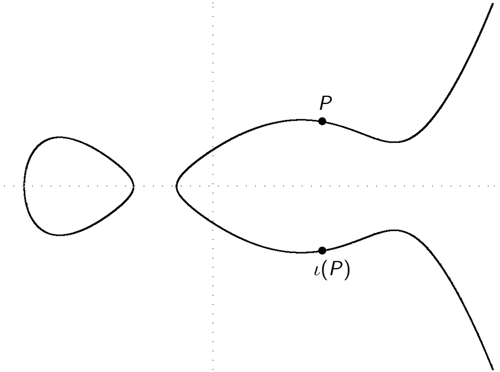
- dense columns correspond to "small primes"
- other columns correspond to "large primes"

1. If a column contains only one non-zero entry, remove it and the corresponding row.
   Also, remove columns/rows containing only zeroes.
2. Mark some new columns as dense
3. Find rows with only one ± 1 coefficient in the non-dense part
   - Use this coefficient as a pivot to clear its column
   - Remove corresponding row and column
4. Remove rows that have become too dense and go back to step 1

The hyperelliptic curve case

$\mathcal{H}: \; y^2 + h_0(x)y = h_1(x), \quad h_0, h_1 \in \mathbb{F}_q[x], \; \deg h_0 \leq g, \; \deg h_1 = 2g+1$
hyperelliptic curve of genus g with (unique) point at infinity $\mathcal{O}_{\mathcal{H}}$

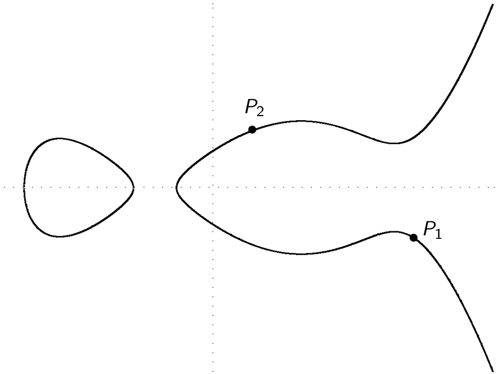
- hyperelliptic involution $\iota : (x_P, y_P) \mapsto (x_P, -y_P - h_0(x_P))$
- $\#\mathcal{H}(\mathbb{F}_q) \simeq q$



The Jacobian variety of $\mathcal{H}$

Divisor class group

Elements of $\mathrm{Jac}_{\mathcal{H}}$ are (equivalence class of) formal sums of points of $\mathcal{H}$



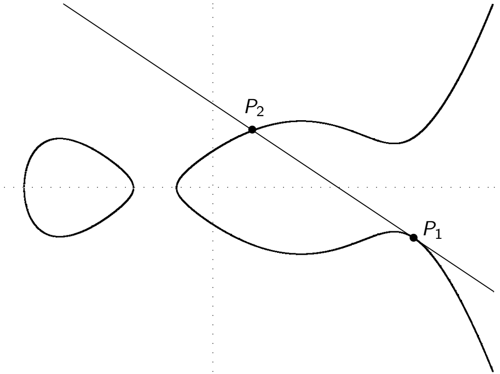
$$D=(P_1)+(P_2)-2(\mathcal{O}_{\mathcal{H}})$$

The Jacobian variety of $\mathcal{H}$

Divisor class group

Elements of $\mathrm{Jac}_{\mathcal{H}}$ are (equivalence class of) formal sums of points of $\mathcal{H}$

$\mathcal{C} : f(x, y) = 0$ intersects $\mathcal{H}$ in $P_1, \ldots, P_m \rightsquigarrow (P_1) + \cdots + (P_m) - m(\mathcal{O}_{\mathcal{H}}) \sim 0$



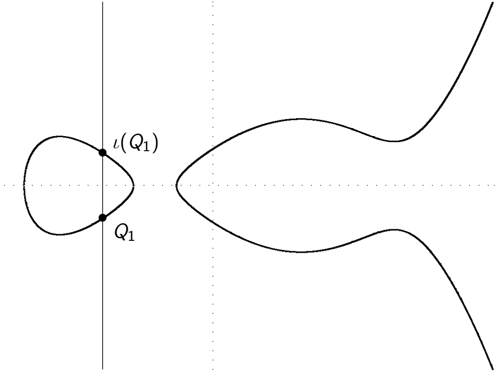
$2(P_1) + (P_2) + (P_3) + (P_4) - 5(\mathcal{O}_{\mathcal{H}}) \sim 0$

The Jacobian variety of $\mathcal{H}$

Divisor class group

Elements of $\mathrm{Jac}_{\mathcal{H}}$ are (equivalence class of) formal sums of points of $\mathcal{H}$

$\mathcal{C} : f(x,y) = 0$ intersects $\mathcal{H}$ in $P_1, \dots, P_m \rightsquigarrow (P_1) + \cdots + (P_m) - m(\mathcal{O}_{\mathcal{H}}) \sim 0$



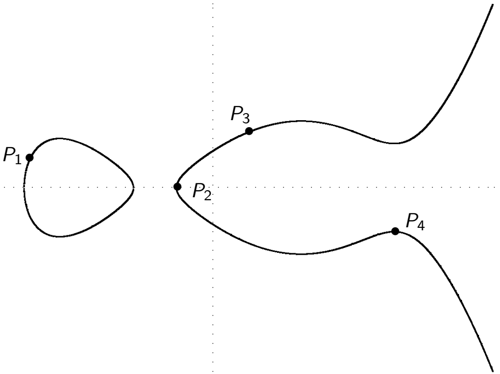
$$-\Big((Q_1) - (\mathcal{O}_{\mathcal{H}})\Big) \sim (\iota(Q_1)) - (\mathcal{O}_{\mathcal{H}})$$

The Jacobian variety of $\mathcal{H}$

Divisor class group

Elements of $\mathrm{Jac}_{\mathcal{H}}$ are (equivalence class of) formal sums of points of $\mathcal{H}$

$\mathcal{C} : f(x, y) = 0$ intersects $\mathcal{H}$ in $P_1, \ldots, P_m \rightsquigarrow (P_1) + \cdots + (P_m) - m(\mathcal{O}_{\mathcal{H}}) \sim 0$



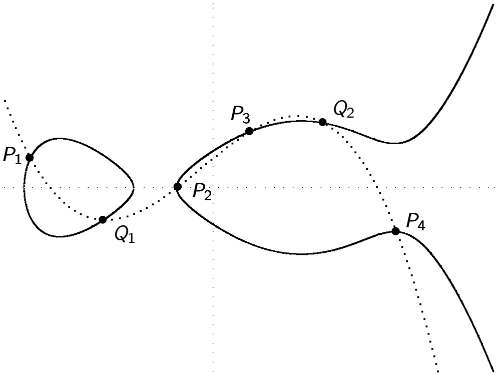
Addition law ?

The Jacobian variety of $\mathcal{H}$

Divisor class group

Elements of $\mathrm{Jac}_{\mathcal{H}}$ are (equivalence class of) formal sums of points of $\mathcal{H}$

$\mathcal{C} : f(x,y) = 0$ intersects $\mathcal{H}$ in $P_1, \ldots, P_m \rightsquigarrow (P_1)+\cdots+(P_m)-m(\mathcal{O}_{\mathcal{H}}) \sim 0$



Reduction:

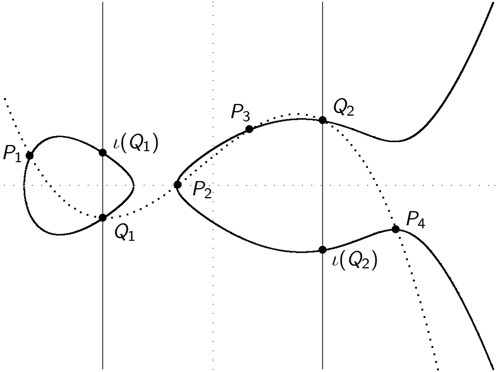
$$
\begin{aligned}
& (P_1)+(P_2)+(P_3)+(P_4)-4(\mathcal{O}_{\mathcal{H}}) \\
\sim\quad & -(Q_1)-(Q_2)+2(\mathcal{O}_{\mathcal{H}})
\end{aligned}
$$

The Jacobian variety of $\mathcal{H}$

Divisor class group

Elements of $\mathrm{Jac}_{\mathcal{H}}$ are (equivalence class of) formal sums of points of $\mathcal{H}$

$\mathcal{C} : f(x,y) = 0$ intersects $\mathcal{H}$ in $P_1, \ldots, P_m \rightsquigarrow (P_1)+\cdots+(P_m)-m(\mathcal{O}_{\mathcal{H}}) \sim 0$



Reduction:

$$\begin{aligned} & (P_1)+(P_2)+(P_3)+(P_4)-4(\mathcal{O}_{\mathcal{H}}) \\ \sim\ & -(Q_1)-(Q_2)+2(\mathcal{O}_{\mathcal{H}}) \\ \sim\ & (\iota(Q_1))+(\iota(Q_2))-2(\mathcal{O}_{\mathcal{H}}) \end{aligned}$$

Representations of elements of $\mathrm{Jac}_{\mathcal{H}}$

Reduced representation

An element $[D] \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$ has a unique reduced representation

$$D \sim (P_1) + \cdots + (P_r) - r(\mathcal{O}_{\mathcal{H}}), \quad r \leq g,\ P_i \neq \iota(P_j) \text{ for } i \neq j$$

Mumford representation

One-to-one correspondence between elements of $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$ and couples of polynomials $(u, v) \in \mathbb{F}_q[x]^2$ s.t.

- u monic, $\deg u \leq g$
- $\deg v < \deg u$
- u divides $v^2 + vh_0 - h_1$

- Cantor's algorithm for addition law
- $\#\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q) \simeq q^g$

Adleman-DeMarrais-Huang's index calculus

Analog of the integer factorization for elements of the Jacobian variety:

Proposition

Let $D = (u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$. If u factorizes as $\prod_j u_j$ over $\mathbb{F}_q$, then

- $D_j = (u_j, v_j)$ is in $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$, where $v_j = v \bmod u_j$
- $D = \sum_j D_j$

Adleman-DeMarrais-Huang's index calculus

Analog of the integer factorization for elements of the Jacobian variety:

Proposition

Let $D = (u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$. If u factorizes as $\prod_j u_j$ over $\mathbb{F}_q$, then

- $D_j = (u_j, v_j)$ is in $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$, where $v_j = v \bmod u_j$
- $D = \sum_j D_j$

Allows to apply index calculus [Enge-Gaudry]

- Factor base: $\mathcal{F} = \{(u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q) : u \text{ irreducible, } \deg u \leq B\}$ ("small prime divisors")
- Element $[a_i]D_0 + [b_i]D_1$ yields a relation if corresponding u polynomial is B-smooth

Adleman-DeMarrais-Huang's index calculus

Analog of the integer factorization for elements of the Jacobian variety:

Proposition

Let $D = (u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$. If u factorizes as $\prod_j u_j$ over $\mathbb{F}_q$, then

- $D_j = (u_j, v_j)$ is in $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$, where $v_j = v \bmod u_j$
- $D = \sum_j D_j$

Allows to apply index calculus [Enge-Gaudry]

- Factor base: $\mathcal{F} = \{(u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q) : u \text{ irreducible}, \ \deg u \leq B\}$ ("small prime divisors")
- Element $[a_i]D_0 + [b_i]D_1$ yields a relation if corresponding u polynomial is B-smooth

Subexponential complexity in $L_{q^g}(1/2)$ when $q \to \infty$ and $g = \Omega(\log q)$

The small genus case

Gaudry's algorithm for small genus curves

- Factor base: $\mathcal{F} = \{(u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q) \ : \ \deg u = 1\}$ of size $\simeq q$
- $D = (u, v)$ decomposable $\Leftrightarrow$ u splits over $\mathbb{F}_q$
- Probability of decomposition $\simeq 1/g!$

$\Rightarrow O(g!q)$ tests (relation search) $+$ $O(gq^2)$ field operations (linear alg.)

Total cost: $O((g^2 \log^3 q)g!q + (g^2 \log q)q^2)$

The small genus case

Gaudry's algorithm for small genus curves

- Factor base: $\mathcal{F} = \{(u,v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q) \ : \ \deg u = 1\}$ of size $\simeq q$
- $D = (u,v)$ decomposable $\Leftrightarrow$ u splits over $\mathbb{F}_q$
- Probability of decomposition $\simeq 1/g!$

$\Rightarrow$ $O(g!q)$ tests (relation search) + $O(gq^2)$ field operations (linear alg.)

Total cost: $O((g^2 \log^3 q)g!q + (g^2 \log q)q^2)$

For fixed genus g, relation search in $\tilde{O}(q)$ **vs** linear algebra in $\tilde{O}(q^2)$

- resolution of the DLP in $\tilde{O}(q^2)$

  $\Rightarrow$ better than generic attacks as soon as $g > 4$
- possible improvement by rebalancing the two phases

Double large prime variation

Gaudry - Thomé - Thériault - Diem

- Define new factor base $\mathcal{F}' \subset \mathcal{F}$ with $\#\mathcal{F}' = q^\alpha$
  $\mathcal{F}'$: "small primes" $\mathcal{F} \setminus \mathcal{F}'$: "large primes"
  $\rightsquigarrow$ linear algebra in $\tilde{O}(q^{2\alpha})$
- Keep relations involving at most two large primes, discard others
- After collecting $\simeq \#\mathcal{F}$ relations 2LP, possible to eliminate the large primes and obtain $\simeq \#\mathcal{F}'$ relations involving only small primes

- Asymptotically optimal choice $\alpha = 1 - 1/g$
  $\rightsquigarrow$ total complexity in $\tilde{O}(q^{2-2/g})$
  $\rightsquigarrow$ better than generic attacks as soon as $g \geq 3$

- Practical best choice depends on actual cost of the 2 phases and computing power available

Index calculus on small degree plane curves [Diem '06]

Diem's algorithm

- applies to Jacobians of curves admitting a small degree plane model
- uses divisors of simple functions to find relations between factor base elements
- relies strongly on the double large prime variation

Index calculus on small degree plane curves [Diem '06]

Diem's algorithm

- applies to Jacobians of curves admitting a small degree plane model
- uses divisors of simple functions to find relations between factor base elements
- relies strongly on the double large prime variation

For $\mathcal{C}_{|\mathbb{F}_q}$ of fixed degree d, complexity in $\tilde{O}(q^{2-2/(d-2)})$

- most genus g curves admit a plane model of degree $g+1$
  $\rightsquigarrow$ complexity in $\tilde{O}(q^{2-2/(g-1)})$
- not true for hyperelliptic curves

Index calculus on small degree plane curves [Diem '06]

Diem's algorithm

- applies to Jacobians of curves admitting a small degree plane model
- uses divisors of simple functions to find relations between factor base elements
- relies strongly on the double large prime variation

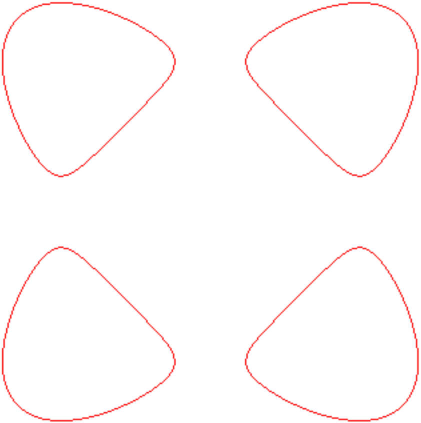
For $\mathcal{C}_{|\mathbb{F}_q}$ of fixed degree d, complexity in $\tilde{O}(q^{2-2/(d-2)})$

- most genus g curves admit a plane model of degree $g+1$
  $\rightsquigarrow$ complexity in $\tilde{O}(q^{2-2/(g-1)})$
- not true for hyperelliptic curves

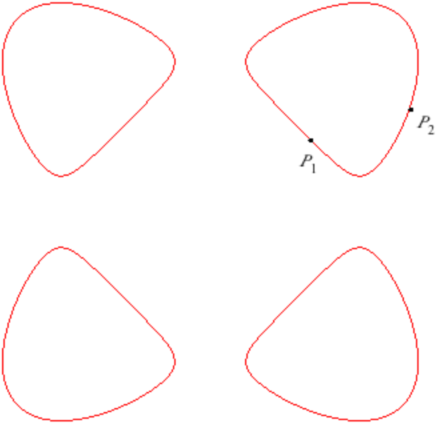
Consequence

Jacobians of non-hyperelliptic curves usually weaker than those of hyperelliptic curves (especially true for $g = 3$).

Idea of index calculus on small degree plane curves

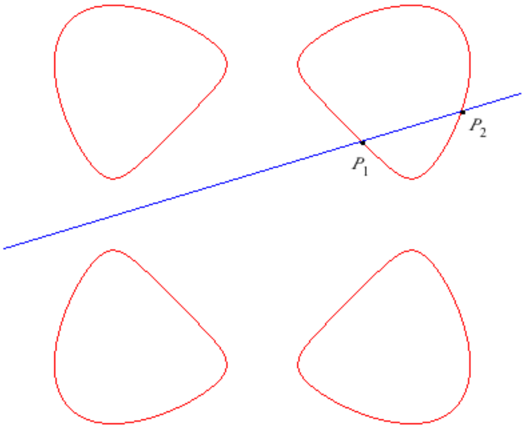


Idea of index calculus on small degree plane curves



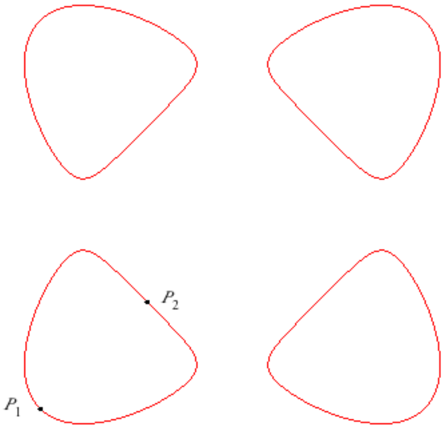
- Take P_1, P_2 small primes

Idea of index calculus on small degree plane curves



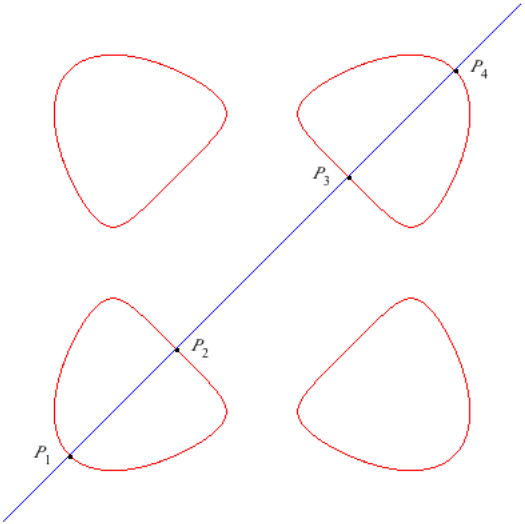
- Take P_1, P_2 small primes
- L line through P_1 and P_2
  if $L \cap \mathcal{C}(\mathbb{F}_q) = \{P_1, \ldots, P_d\}$,
  then relation:
  $(P_1) + \cdots + (P_d) - D_\infty \sim 0$

Idea of index calculus on small degree plane curves



- Take P_1, P_2 small primes
- L line through P_1 and P_2
  if $L \cap \mathcal{C}(\mathbb{F}_q) = \{P_1, \ldots, P_d\}$,
  then relation:
  $(P_1) + \cdots + (P_d) - D_\infty \sim 0$

Idea of index calculus on small degree plane curves



- Take P_1, P_2 small primes
- L line through P_1 and P_2
  if $L \cap \mathcal{C}(\mathbb{F}_q) = \{P_1, \ldots, P_d\}$,
  then relation:
  $(P_1) + \cdots + (P_d) - D_\infty \sim 0$

Summary

Asymptotic comparison on $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$

Genus	2	3	4	5
Generic methods	q	$q^{3/2}$	q^2	$q^{5/2}$
Classical index calculus	q^2	q^2	q^2	q^2
2LP, hyperelliptic case	q	$q^{4/3}$	$q^{3/2}$	$q^{8/5}$
2LP, small degree case (non hyperelliptic)	–	q	$q^{4/3}$	$q^{3/2}$

Summary

Asymptotic comparison on $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$

Genus	2	3	4	5
Generic methods	q	$q^{1.5}$	q^2	$q^{2.5}$
Classical index calculus	q^2	q^2	q^2	q^2
2LP, hyperelliptic case	q	$q^{1.33}$	$q^{1.5}$	$q^{1.6}$
2LP, small degree case (non hyperelliptic)	–	q	$q^{1.33}$	$q^{1.5}$

Section 2

Decomposition index calculus

Application to elliptic curves

No canonical choice of factor base nor natural way of finding decompositions

Application to elliptic curves

No canonical choice of factor base nor natural way of finding decompositions

What kind of "decomposition" over $E(K)$?

Main idea [Semaev '04]:

- consider decompositions in a fixed number of points of $\mathcal{F}$

$$R = [a]P + [b]Q = P_1 + \cdots + P_m$$

- convert this algebraically by using the $(m+1)$-*th summation polynomial*:

$$f_{m+1}(x_R, x_{P_1}, \ldots, x_{P_m}) = 0$$
$$\Leftrightarrow \exists \epsilon_1, \ldots, \epsilon_m \in \{1, -1\}, R = \epsilon_1 P_1 + \cdots + \epsilon_m P_m$$

Gaudry and Diem (2004)

"Decomposition attack": index calculus on $E(\mathbb{F}_{q^n})$

- Natural factor base: $\mathcal{F} = \{(x,y) \in E(\mathbb{F}_{q^n}) : x \in \mathbb{F}_q\}$, $\#\mathcal{F} \simeq q$
- Relations involve n points: $R = P_1 + \cdots + P_n$
- Restriction of scalars: decompose along a $\mathbb{F}_q$-linear basis of $\mathbb{F}_{q^n}$

$$f_{n+1}(x_R, x_{P_1}, \ldots, x_{P_n}) = 0 \Leftrightarrow \begin{cases} \varphi_1(x_{P_1}, \ldots, x_{P_n}) = 0 \\ \vdots \\ \varphi_n(x_{P_1}, \ldots, x_{P_n}) = 0 \end{cases} \qquad (\mathcal{S}_R)$$

One decomposition trial $\leftrightarrow$ resolution of $\mathcal{S}_R$ over $\mathbb{F}_q$

Gaudry and Diem (2004)

"Decomposition attack": index calculus on $E(\mathbb{F}_{q^n})$

- Natural factor base: $\mathcal{F} = \{(x,y) \in E(\mathbb{F}_{q^n}) : x \in \mathbb{F}_q\}$, $\#\mathcal{F} \simeq q$
- Relations involve n points: $R = P_1 + \cdots + P_n$
- Restriction of scalars: decompose along a $\mathbb{F}_q$-linear basis of $\mathbb{F}_{q^n}$

$$f_{n+1}(x_R, x_{P_1}, \ldots, x_{P_n}) = 0 \Leftrightarrow \begin{cases} \varphi_1(x_{P_1}, \ldots, x_{P_n}) = 0 \\ \vdots \\ \varphi_n(x_{P_1}, \ldots, x_{P_n}) = 0 \end{cases} \qquad (\mathcal{S}_R)$$

One decomposition trial $\leftrightarrow$ resolution of $\mathcal{S}_R$ over $\mathbb{F}_q$

- With "double large prime" variation, overall complexity in $\tilde{O}\left(n! 2^{3n(n-1)} q^{2-2/n}\right)$
- Bottleneck: $\deg I(\mathcal{S}_R) = 2^{n(n-1)}$. But most solutions not in $\mathbb{F}_q$

Variant "$n-1$" [Joux-V. '10]

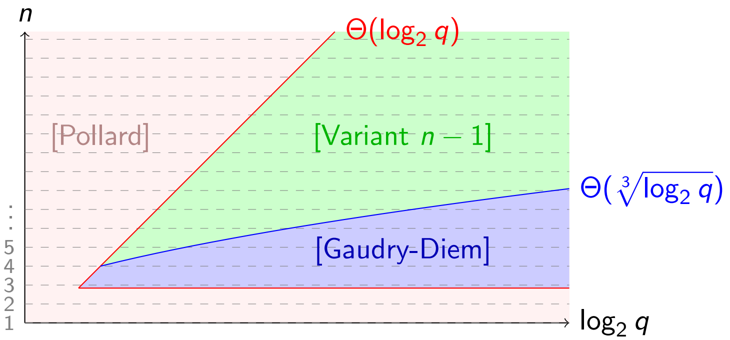
Decompositions into $m = n-1$ points

- compute the n-th summation polynomial (instead of $n+1$-th) with partially symmetrized resultant
- solve $\mathcal{S}_R$ with $n-1$ var, n eq and total degree 2^{n-2}
- $(n-1)!q$ expected numbers of trials to get one relation

Computation speed-up

1. $\mathcal{S}_R$ is overdetermined and $I(\mathcal{S}_R)$ has very low degree (0 or 1 excep.)
   - resolution with a *grevlex* Gröbner basis
   - no need to change order (FGLM)
2. Speed up computations with F4Remake

Comparaison of the three attacks of ECDLP over $\mathbb{F}_{q^n}$



Under some heuristic assumptions, complexity of variant $n-1$ in

$$\tilde{O}\left((n-1)!\left(2^{(n-1)(n-2)}e^n n^{-1/2}\right)^{\omega} q^2\right)$$

Example of application to $E(\mathbb{F}_{p^5})$

Standard 'Well Known Group' 3 Oakley curve

E elliptic curve defined over $\mathbb{F}_{2^{155}}$,
$\#E(\mathbb{F}_{2^{155}}) = 12 \cdot 3805993847215893016155463826195386266397436443$

- $\mathcal{F} = \{P \in E(\mathbb{F}_{2^{155}}) : x(P) \in \mathbb{F}_{2^{31}}\}$
- Decomposition test with variant $n-1$ takes 22.95 ms using F4Remake (on 2.93 GHz Intel Xeon)

Example of application to $E(\mathbb{F}_{p^5})$

Standard 'Well Known Group' 3 Oakley curve

E elliptic curve defined over $\mathbb{F}_{2^{155}}$,
$\#E(\mathbb{F}_{2^{155}}) = 12 \cdot 3805993847215893016155463826195386266397436443$

- $\mathcal{F} = \{P \in E(\mathbb{F}_{2^{155}}) : x(P) \in \mathbb{F}_{2^{31}}\}$
- Decomposition test with variant $n-1$ takes 22.95 ms using F4Remake (on 2.93 GHz Intel Xeon)

- too slow for complete DLP resolution
- but efficient threat for Oracle-assisted Static Diffie-Hellman Problem (only one relation needed)

Decompositions on $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$

$\mathcal{H}|_{\mathbb{F}_{q^n}}$ hyperelliptic curve of genus g with a unique point $\mathcal{O}$ at infinity

Gaudry's framework

- Factor base containing about q elements
  $\mathcal{F} = \{D_Q \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n}) \ : \ D_Q \sim (Q) - (\mathcal{O}), Q \in \mathcal{H}(\mathbb{F}_{q^n}), x(Q) \in \mathbb{F}_q\}$
- Decomposition search: try to write arbitrary divisor $D \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$ as sum of ng divisors of $\mathcal{F}$

Asymptotic complexity for n, g fixed in $\tilde{O}(q^{2-2/ng})$

Decompositions on $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$

$\mathcal{H}|_{\mathbb{F}_{q^n}}$ hyperelliptic curve of genus g with a unique point $\mathcal{O}$ at infinity

Gaudry's framework

- Factor base containing about q elements
  $\mathcal{F} = \{D_Q \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n}) \;:\; D_Q \sim (Q) - (\mathcal{O}), Q \in \mathcal{H}(\mathbb{F}_{q^n}), x(Q) \in \mathbb{F}_q\}$
- Decomposition search: try to write arbitrary divisor $D \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$ as sum of ng divisors of $\mathcal{F}$

Asymptotic complexity for n, g fixed in $\tilde{O}(q^{2-2/ng})$

How to check if D can be decomposed?

- Semaev's summation polynomials are no longer available
- use Riemann-Roch based reformulation of Nagao instead

Decompositions on $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$

Main difficulty in Nagao's decompositions

Solve a 0-dim quadratic polynomial system of $(n-1)ng$ eq./var. for each divisor $D(= [a_i]D_0 + [b_i]D_1) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$.

- complexity at least polynomial in $d = 2^{(n-1)ng}$
- relevant only for n and g small enough

Decompositions on $\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$

Main difficulty in Nagao's decompositions

Solve a 0-dim quadratic polynomial system of $(n-1)ng$ eq./var. for each divisor $D(=[a_i]D_0+[b_i]D_1) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$.

- complexity at least polynomial in $d = 2^{(n-1)ng}$
- relevant only for n and g small enough

In practice:

- Decompositions as $D \sim \sum_{i=1}^{ng}((Q_i)-(\mathcal{O}_{\mathcal{H}}))$ are too slow to compute
- Faster alternative [Joux-V.]: compute relations involving only elements of $\mathcal{F}$

$$\sum_{i=1}^{ng+2}((Q_i)-(\mathcal{O}_{\mathcal{H}})) \sim 0$$

The modified relation search

$\mathcal{H}$ hyperelliptic curve of genus g defined over $\mathbb{F}_{q^n}$, $n \geq 2$

- find relations of the form $\sum_{i=1}^{ng+2} ((Q_i) - (\mathcal{O}_{\mathcal{H}})) \sim 0$
- linear algebra: deduce DL of factor base elements up to a constant
- descent phase: compute two Nagao-style decompositions to complete the DLP resolution

The modified relation search

$\mathcal{H}$ hyperelliptic curve of genus g defined over $\mathbb{F}_{q^n}$, $n \geq 2$

- find relations of the form $\sum_{i=1}^{ng+2} ((Q_i) - (\mathcal{O}_{\mathcal{H}})) \sim 0$
- linear algebra: deduce DL of factor base elements up to a constant
- descent phase: compute two Nagao-style decompositions to complete the DLP resolution

- With Nagao: about $(ng)!\, q$ quadratic polynomial systems of $n(n-1)g$ eq./var. to solve
- With variant: only 1 under-determined quadratic system of $n(n-1)g + 2n - 2$ eq. and $n(n-1)g + 2n$ var.

The modified relation search

$\mathcal{H}$ hyperelliptic curve of genus g defined over $\mathbb{F}_{q^n}$, $n \geq 2$

- find relations of the form $\sum_{i=1}^{ng+2} ((Q_i) - (\mathcal{O}_{\mathcal{H}})) \sim 0$
- linear algebra: deduce DL of factor base elements up to a constant
- descent phase: compute two Nagao-style decompositions to complete the DLP resolution

- With Nagao: about $(ng)!\, q$ quadratic polynomial systems of $n(n-1)g$ eq./var. to solve
- With variant: only 1 under-determined quadratic system of $n(n-1)g + 2n - 2$ eq. and $n(n-1)g + 2n$ var.

Speed-up

Much faster to compute decompositions with our variant
$\rightarrow$ about 960 times faster for $(n, g) = (2, 3)$ on a 150-bit curve

Section 3

Cover and decomposition attacks

Transfer of the ECDLP via cover maps

Let E be an elliptic curve defined over $\mathbb{F}_{q^n}$ and $\mathcal{C}$ a curve defined over $\mathbb{F}_q$, such that there exists a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

Transfer of the ECDLP via cover maps

Let E be an elliptic curve defined over $\mathbb{F}_{q^n}$ and $\mathcal{C}$ a curve defined over $\mathbb{F}_q$, such that there exists a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

1. transfer the DLP from $E(\mathbb{F}_{q^n})$ to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$

$$\begin{tikzcd} \mathcal{C}(\mathbb{F}_{q^n}) \arrow[d, "\pi"] \\ E(\mathbb{F}_{q^n}) \end{tikzcd} \qquad \begin{tikzcd} \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \arrow[rr, "Tr"] & & \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q) \\ \mathrm{Jac}_E(\mathbb{F}_{q^n}) \simeq E(\mathbb{F}_{q^n}) \arrow[u, "\pi^*"] \arrow[urr, dotted] & & \end{tikzcd}$$

g genus of $\mathcal{C}$
s.t. $g \geq n$

$$\pi^*((P)) = \sum_{Q \in \pi^{-1}(\{P\})} (Q), \quad Tr(D) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)} D^\sigma$$

Transfer of the ECDLP via cover maps

Let E be an elliptic curve defined over $\mathbb{F}_{q^n}$ and $\mathcal{C}$ a curve defined over $\mathbb{F}_q$, such that there exists a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

1. transfer the DLP from $E(\mathbb{F}_{q^n})$ to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$

$$\begin{tikzcd} \mathcal{C}(\mathbb{F}_{q^n}) \arrow[d, "\pi"] \\ E(\mathbb{F}_{q^n}) \end{tikzcd} \qquad \begin{tikzcd} & \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \arrow[r, "Tr"] & \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q) \\ \mathrm{Jac}_E(\mathbb{F}_{q^n}) \simeq & E(\mathbb{F}_{q^n}) \arrow[u, "\pi^*"] \arrow[ur, dotted] & \end{tikzcd}$$

g genus of $\mathcal{C}$
s.t. $g \geq n$

2. use index calculus on $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$, complexity in
   - $\tilde{O}(q^{2-2/g})$ if $\mathcal{C}$ is hyperelliptic with small genus g [Gaudry '00]
   - $\tilde{O}(q^{2-2/(d-2)})$ if $\mathcal{C}$ has a small degree d plane model [Diem '06]

Transfer of the ECDLP via cover maps

Let E be an elliptic curve defined over $\mathbb{F}_{q^n}$ and $\mathcal{C}$ a curve defined over $\mathbb{F}_q$, such that there exists a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

1. transfer the DLP from $E(\mathbb{F}_{q^n})$ to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$

$$\begin{tikzcd} \mathcal{C}(\mathbb{F}_{q^n}) \arrow[d, "\pi"] & \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \arrow[r, "Tr"] & \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q) \\ E(\mathbb{F}_{q^n}) & \mathrm{Jac}_E(\mathbb{F}_{q^n}) \simeq E(\mathbb{F}_{q^n}) \arrow[u, "\pi^*"] \arrow[ur, dotted] & \end{tikzcd}$$

g genus of $\mathcal{C}$
s.t. $g \geq n$

2. use index calculus on $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$, complexity in
   - $\tilde{O}(q^{2-2/g})$ if $\mathcal{C}$ is hyperelliptic with small genus g [Gaudry '00]
   - $\tilde{O}(q^{2-2/(d-2)})$ if $\mathcal{C}$ has a small degree d plane model [Diem '06]

The Gaudry-Heß-Smart technique

Construct $\mathcal{C}_{|\mathbb{F}_q}$ and $\pi : \mathcal{C} \to E$ from $E_{|\mathbb{F}_{q^n}}$ and a degree 2 map $E \to \mathbb{P}^1$

Transfer of the ECDLP via cover maps

Let E be an elliptic curve defined over $\mathbb{F}_{q^n}$ and $\mathcal{C}$ a curve defined over $\mathbb{F}_q$, such that there exists a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

1. transfer the DLP from $E(\mathbb{F}_{q^n})$ to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$

$$\begin{array}{ccc} \mathcal{C}(\mathbb{F}_{q^n}) & \quad & \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \xrightarrow{Tr} \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q) \\ \downarrow \pi & & \uparrow \pi^* \\ E(\mathbb{F}_{q^n}) & & \mathrm{Jac}_E(\mathbb{F}_{q^n}) \simeq E(\mathbb{F}_{q^n}) \end{array}$$

g genus of $\mathcal{C}$
s.t. $g \geq n$

2. use index calculus on $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$, complexity in
   - $\tilde{O}(q^{2-2/g})$ if $\mathcal{C}$ is hyperelliptic with small genus g [Gaudry '00]
   - $\tilde{O}(q^{2-2/(d-2)})$ if $\mathcal{C}$ has a small degree d plane model [Diem '06]

The Gaudry-Heß-Smart technique

Problem: for most elliptic curves, $g(\mathcal{C})$ is of the order of 2^n

A combined attack

Let $E(\mathbb{F}_{q^n})$ elliptic curve such that

- n is too large for a practical decomposition attack
- GHS provides covering curves $\mathcal{C}$ with too large genus

A combined attack

Let $E(\mathbb{F}_{q^n})$ elliptic curve such that

- n is too large for a practical decomposition attack
- GHS provides covering curves $\mathcal{C}$ with too large genus

Cover and decomposition attack [Joux-V.]

If n composite, combine both approaches:

1. use GHS on the subextension $\mathbb{F}_{q^n}/\mathbb{F}_{q^d}$ to transfer the DL to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^d})$
2. then use decomposition attack on $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^d})$ with base field $\mathbb{F}_q$ to solve the DLP

A combined attack

Let $E(\mathbb{F}_{q^n})$ elliptic curve such that

- n is too large for a practical decomposition attack
- GHS provides covering curves $\mathcal{C}$ with too large genus

Cover and decomposition attack [Joux-V.]

If n composite, combine both approaches:

1. use GHS on the subextension $\mathbb{F}_{q^n}/\mathbb{F}_{q^d}$ to transfer the DL to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^d})$
2. then use decomposition attack on $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^d})$ with base field $\mathbb{F}_q$ to solve the DLP

$\longrightarrow$ well adapted for curves defined over some Optimal Extension Fields

The sextic extension case

Comparisons and complexity estimates for 160 bits based on Magma

p 27-bit prime, $E(\mathbb{F}_{p^6})$ elliptic curve with 160-bit prime order subgroup

The sextic extension case

Comparisons and complexity estimates for 160 bits based on Magma

p 27-bit prime, $E(\mathbb{F}_{p^6})$ elliptic curve with 160-bit prime order subgroup

1. Generic attacks: $\tilde{O}(p^3)$ cost, $\approx 5 \times 10^{13}$ years

The sextic extension case

Comparisons and complexity estimates for 160 bits based on Magma

p 27-bit prime, $E(\mathbb{F}_{p^6})$ elliptic curve with 160-bit prime order subgroup

1. Generic attacks: $\tilde{O}(p^3)$ cost, $\approx 5 \times 10^{13}$ years
2. Former index calculus methods:

	Decomposition	GHS
$\mathbb{F}_{p^6}/\mathbb{F}_{p^2}$	$\tilde{O}(p^2)$ memory bottleneck	
$\mathbb{F}_{p^6}/\mathbb{F}_{p}$	intractable	efficient for $\leq 1/p^3$ curves $g = 9$: $\tilde{O}(p^{7/4})$, $\approx 1\,500$ years

The sextic extension case

Comparisons and complexity estimates for 160 bits based on Magma

p 27-bit prime, $E(\mathbb{F}_{p^6})$ elliptic curve with 160-bit prime order subgroup

1. Generic attacks: $\tilde{O}(p^3)$ cost, $\approx 5 \times 10^{13}$ years

2. Former index calculus methods:

	Decomposition	GHS
$\mathbb{F}_{p^6}/\mathbb{F}_{p^2}$	$\tilde{O}(p^2)$ memory bottleneck	
$\mathbb{F}_{p^6}/\mathbb{F}_p$	intractable	efficient for $\leq 1/p^3$ curves $g = 9$: $\tilde{O}(p^{7/4})$, $\approx 1\,500$ years

3. Cover and decomposition:
   $\tilde{O}(p^{5/3})$ cost using a hyperelliptic genus 3 cover defined over $\mathbb{F}_{p^2}$
   $\rightarrow$ occurs directly for $1/p^2$ curves and most curves after isogeny walk
   - Nagao-style decomposition: ≈ 750 years
   - Modified relation search: ≈ 300 years

A concrete attack on a 150-bit curve

$E: \ y^2 = x(x-\alpha)(x-\sigma(\alpha))$ defined over $\mathbb{F}_{p^6}$ where $p = 2^{25}+35$, such that $\#E = 4 \cdot 356814156285346166966901450449051336101786213$

- Previously unreachable curve: GHS gives cover over $\mathbb{F}_p$ of genus 33...

A concrete attack on a 150-bit curve

$E: \; y^2 = x(x-\alpha)(x-\sigma(\alpha))$ defined over $\mathbb{F}_{p^6}$ where $p = 2^{25}+35$, such that $\#E = 4 \cdot 356814156285346166966901450449051336101786213$

- Previously unreachable curve: GHS gives cover over $\mathbb{F}_p$ of genus 33...
- Complete resolution of DLP in about 1 month
  with cover and decomposition, using genus 3 hyperelliptic cover $\mathcal{H}_{|\mathbb{F}_{p^2}}$

Relation search

- lex GB: 2.7 sec with one core(1)
- sieving: $p^2/(2\cdot 8!) \simeq 1.4 \times 10^{10}$ relations in 62 h on 1 024 cores(2)
  $\rightarrow$ 960$\times$ faster than Nagao

Linear algebra

- SGE: 25.5 h on 32 cores(2)
  $\rightarrow$ fivefold reduction
- Lanczos: 28.5 days on 64 cores(2)
  (200 MB of data broadcast/round)

(Descent phase done in $\sim$ 14 s for one point)

(1) Magma on 2.6 GHz Intel Core 2 Duo

(2) 2.93 GHz quadri-core Intel Xeon 5550