Cover and Decomposition Attacks on Elliptic Curves

Vanessa VITSE
Joint work with Antoine JOUX

Université de Versailles Saint-Quentin, Laboratoire PRiSM

Séminaire de Théorie des Nombres de Caen – LMNO

1. Background
   - Generalities on DLP and motivations
   - Weil descent
   - Index calculus for Jacobians of curves
   - Decomposition attack

2. Decomposition attack on hyperelliptic curves over extension fields
   - Generalities
   - New results

3. Cover and decomposition attacks

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)

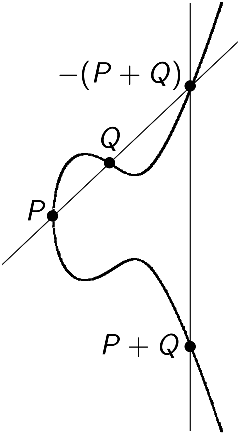
Given a group G and $g, h \in G$, find – when it exists – an integer x s.t.

$$h = g^x$$

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 $g > 2$

Good candidates for DLP-based cryptosystems

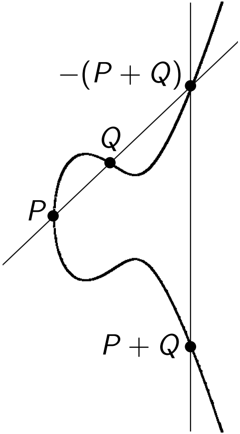


ECDLP: Given $P \in E(\mathbb{F}_q)$ and $Q \in \langle P \rangle$ find x such that $Q = [x]P$

In general, no known attack better than generic algorithms $\rightsquigarrow$ shorter keys

Security (bits)	Finite Field DLP	ECDLP
80	1 248	160
96	1 776	192
112	2 432	224
128	3 248	256

Good candidates for DLP-based cryptosystems

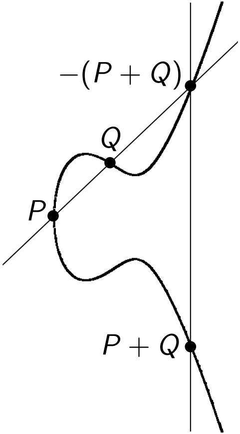


ECDLP: Given $P \in E(\mathbb{F}_q)$ and $Q \in \langle P \rangle$ find x such that $Q = [x]P$

Attacks on special curves:

- Curves defined over prime fields
  - small embedding degree (transfer via pairings)
  - anomalous curves (p-adic lifts)
- Curves defined over extension fields
  - Weil descent: transfer from $E(\mathbb{F}_{p^n})$ to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_p)$ where $\mathcal{C}$ is a genus $g \geq n$ curve
  - Decomposition index calculus on $E(\mathbb{F}_{p^n})$

Good candidates for DLP-based cryptosystems



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

Attacks on special curves:

- Curves defined over prime fields
  - small embedding degree (transfer via pairings)
  - anomalous curves (p-adic lifts)
- Curves defined over extension fields
  - Weil descent: transfer from $E(\mathbb{F}_{p^n})$ to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_p)$ where $\mathcal{C}$ is a genus $g \geq n$ curve
  - Decomposition index calculus on $E(\mathbb{F}_{p^n})$

Objective of this talk

Present a combined attack for curves over extension fields

1 Background
- Generalities on DLP and motivations
- Weil descent
- Index calculus for Jacobians of curves
- Decomposition attack

2 Decomposition attack on hyperelliptic curves over extension fields
- Generalities
- New results

3 Cover and decomposition attacks

Transfer of the ECDLP via cover maps (Weil descent)

Let $\mathcal{W} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ be the **Weil restriction** of $E_{|\mathbb{F}_{q^n}}$ elliptic curve.
Inclusion of a curve $\mathcal{C}_{|\mathbb{F}_q} \hookrightarrow \mathcal{W}$ induces a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

Transfer of the ECDLP via cover maps (Weil descent)

Let $\mathcal{W} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ be the **Weil restriction** of $E_{|\mathbb{F}_{q^n}}$ elliptic curve.
Inclusion of a curve $\mathcal{C}_{|\mathbb{F}_q} \hookrightarrow \mathcal{W}$ induces a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

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

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

Transfer of the ECDLP via cover maps (Weil descent)

Let $\mathcal{W} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ be the **Weil restriction** of $E_{|\mathbb{F}_{q^n}}$ elliptic curve.
Inclusion of a curve $\mathcal{C}_{|\mathbb{F}_q} \hookrightarrow \mathcal{W}$ induces a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

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

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

$\ker(Tr \circ \pi^*) \cap \langle P \rangle = \{\mathcal{O}_E\}$
$\Rightarrow g$ genus of $\mathcal{C}$ s.t. $g \geq n$

Transfer of the ECDLP via cover maps (Weil descent)

Let $\mathcal{W} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ be the **Weil restriction** of $E_{|\mathbb{F}_{q^n}}$ elliptic curve.
Inclusion of a curve $\mathcal{C}_{|\mathbb{F}_q} \hookrightarrow \mathcal{W}$ induces a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

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

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

$\ker(Tr \circ \pi^*) \cap \langle P \rangle = \{\mathcal{O}_E\}$
$\Rightarrow g$ genus of $\mathcal{C}$ s.t. $g \geq n$

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

Transfer of the ECDLP via cover maps (Weil descent)

Let $\mathcal{W} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ be the **Weil restriction** of $E_{|\mathbb{F}_{q^n}}$ elliptic curve.
Inclusion of a curve $\mathcal{C}_{|\mathbb{F}_q} \hookrightarrow \mathcal{W}$ induces a **cover map** $\pi : \mathcal{C}(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n})$.

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

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

$\ker(Tr \circ \pi^*) \cap \langle P \rangle = \{\mathcal{O}_E\}$
$\Rightarrow g$ genus of $\mathcal{C}$ s.t. $g \geq n$

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

Main difficulty: find a convenient curve $\mathcal{C}$ with a genus small enough

The GHS technique

Goal: find fields F and F' s.t.

$$
\begin{tikzcd}[arrows=dash]
 & & F' = \mathbb{F}_{q^n} \cdot F = \mathbb{F}_{q^n}(\mathcal{C}) \arrow[dl] \arrow[d] \\
 & \mathbb{F}_{q^n}(E) \arrow[dl] & F = \mathbb{F}_q(\mathcal{C}) \arrow[ddll] \\
\mathbb{F}_{q^n} \arrow[d] & & \\
\mathbb{F}_q & &
\end{tikzcd}
$$

The GHS technique

Goal: find fields F and F' s.t.

$$\begin{tikzcd}
& & F' = \mathbb{F}_{q^n} \cdot F = \mathbb{F}_{q^n}(\mathcal{C}) \arrow[d, dash] \arrow[loop above, "\sigma"] \\
& \mathbb{F}_{q^n}(E) \arrow[ur, dash] & F = F'^{\sigma} \\
\mathbb{F}_{q^n} \arrow[ur, dash] \arrow[d, dash] \arrow[loop above, "\sigma"] & & \\
\mathbb{F}_q \arrow[uurr, dash] & &
\end{tikzcd}$$

Lift of Frobenius σ must exist on F', with fixed subfield F

The GHS technique

Goal: find fields F and F' s.t.

$$\begin{tikzcd}
 & & & F' \arrow[loop above, "\sigma"] \arrow[d, dash] \\
 & & \mathbb{F}_{q^n}(E) \arrow[ur, dash] & F = F'^{\sigma} \\
 & \mathbb{F}_{q^n}(x) \arrow[loop above, "\sigma"] \arrow[ur, dash, "2"] & & \\
\mathbb{F}_{q^n} \arrow[loop above, "\sigma"] \arrow[ur, dash] & \mathbb{F}_q(x) \arrow[u, dash] \arrow[uurr, dash] & & \\
\mathbb{F}_q \arrow[u, dash] \arrow[ur, dash] & & &
\end{tikzcd}$$

No lift of Frobenius on $\mathbb{F}_{q^n}(E)$, but on index 2 subfield $\mathbb{F}_{q^n}(x)$

The GHS technique

Goal: find fields F and F' s.t.

$$
\begin{tikzcd}[arrows=dash]
 & & & F' = \prod_{i=0}^{n-1} \mathbb{F}_{q^n}(E^{\sigma^i}) \arrow[loop above, "\sigma"] \\
 & & \mathbb{F}_{q^n}(E) \arrow[ur] & F = F'^{\sigma} \arrow[u] \\
 & \mathbb{F}_{q^n}(x) \arrow[loop above, "\sigma"] \arrow[ur, "2"] & & \\
\mathbb{F}_{q^n} \arrow[loop above, "\sigma"] \arrow[ur] & \mathbb{F}_q(x) \arrow[u] \arrow[uurr] & & \\
\mathbb{F}_q \arrow[u] \arrow[ur] & & &
\end{tikzcd}
$$

Choose for F' compositum of function fields $\mathbb{F}_{q^n}(E^{\sigma^i})$.

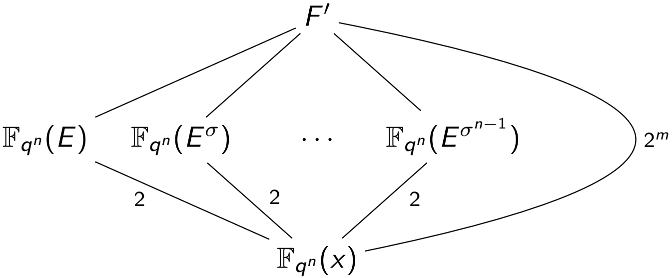
The GHS technique

Goal: find fields F and F' s.t.

$$\begin{tikzcd}
 & & & F' = \prod_{i=0}^{n-1} \mathbb{F}_{q^n}(E^{\sigma^i}) \arrow[loop above, "\sigma"] \arrow[dl, dash] \arrow[d, dash] \\
 & & \mathbb{F}_{q^n}(E) \arrow[dl, dash, "2"'] & F = F'^{\sigma} \arrow[ddll, dash] \\
 & \mathbb{F}_{q^n}(x) \arrow[loop above, "\sigma"] \arrow[dl, dash] \arrow[d, dash] & & \\
\mathbb{F}_{q^n} \arrow[loop above, "\sigma"] \arrow[d, dash] & \mathbb{F}_q(x) \arrow[dl, dash] & & \\
\mathbb{F}_q & & &
\end{tikzcd}$$

Choose for F' compositum of function fields $\mathbb{F}_{q^n}(E^{\sigma^i})$.
Construction depends of the choice of x, i.e. of the equation for E

Magic number



- m "magic number": the genus g of F' depends essentially of $[F' : \mathbb{F}_{q^n}(x)] = 2^m$
- For most elliptic curves E, $m \simeq n \rightarrow g(\mathcal{C})$ is of order 2^n
- For the few elliptic curves admitting a small genus cover $\mathcal{C}$, use index calculus methods on $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$

1. Background
   - Generalities on DLP and motivations
   - Weil descent
   - **Index calculus for Jacobians of curves**
   - Decomposition attack

2. Decomposition attack on hyperelliptic curves over extension fields
   - Generalities
   - New results

3. Cover and decomposition attacks

Basic outline of index calculus

$(G, +) = \langle g \rangle$ 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 of index calculus

$(G,+) = \langle g \rangle$ 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 of index calculus

$(G,+) = \langle g\rangle$ 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 $v = (v_1, \ldots, v_k) \in \ker({}^tM)$ such that $vA \neq \begin{pmatrix} 0 & 0 \end{pmatrix} \mod r$
   - compute the solution of DLP: $x = -\left(\sum_i a_i v_i\right) / \left(\sum_i b_i v_i\right) \mod r$

Adleman-DeMarrais-Huang's index calculus

"Factorization" on the Jacobian variety of a hyperelliptic curve $\mathcal{H}$

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

"Factorization" on the Jacobian variety of a hyperelliptic curve $\mathcal{H}$

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

Adleman-DeMarrais-Huang's index calculus

"Factorization" on the Jacobian variety of a hyperelliptic curve $\mathcal{H}$

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

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 hyperelliptic 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 hyperelliptic 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 $g > 4$

The small genus case

Gaudry's algorithm for small genus hyperelliptic 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 $\tilde{O}(q^2)$
- possible improvement by rebalancing the two phases with double large prime variation: resolution in $\tilde{O}(q^{2-2/g})$

  $\Rightarrow$ better than generic attacks as soon as $g \geq 3$

Index calculus on small dimension abelian varieties

Decomposition attack on DLP over $\mathcal{A}_{|\mathbb{F}_q}$, n-dimensional abelian variety

Gaudry's method

1. Choose $U \subset \mathcal{A}$ dense affine subset and coord. $(x_1, \ldots, x_n, y_1, \ldots, y_m)$ on U s.t. $\mathbb{F}_q(\mathcal{A})$ algebraic extension of $\mathbb{F}_q(x_1, \ldots, x_n)$
2. Define factor base $\mathcal{F} = \{P \in U : x_2(P) = \ldots = x_n(P) = 0\}$
3. Decompose enough points of $\mathcal{A}$ as sum of n points of $\mathcal{F}$ using group law over $\mathcal{A} \leftrightarrow$ solve a multivariate polynomial system (and check rationality of solutions)
4. Extract the logarithms with sparse linear algebra

Index calculus on small dimension abelian varieties

Decomposition attack on DLP over $\mathcal{A}_{|\mathbb{F}_q}$, n-dimensional abelian variety

Gaudry's method

1. Choose $U \subset \mathcal{A}$ dense affine subset and coord. $(x_1, \ldots, x_n, y_1, \ldots, y_m)$ on U s.t. $\mathbb{F}_q(\mathcal{A})$ algebraic extension of $\mathbb{F}_q(x_1, \ldots, x_n)$
2. Define factor base $\mathcal{F} = \{P \in U : x_2(P) = \ldots = x_n(P) = 0\}$
3. Decompose enough points of $\mathcal{A}$ as sum of n points of $\mathcal{F}$ using group law over $\mathcal{A}$ $\leftrightarrow$ solve a multivariate polynomial system (and check rationality of solutions)
4. Extract the logarithms with sparse linear algebra

$\mathcal{F}$ should have $\simeq q$ points

$\rightarrow$ need $O(q)$ relations

$\rightarrow$ linear algebra in $\tilde{O}(nq^2)$

Index calculus on small dimension abelian varieties

Decomposition attack on DLP over $\mathcal{A}_{|\mathbb{F}_q}$, n-dimensional abelian variety

Gaudry's method

1. Choose $U \subset \mathcal{A}$ dense affine subset and coord. $(x_1, \ldots, x_n, y_1, \ldots, y_m)$ on U s.t. $\mathbb{F}_q(\mathcal{A})$ algebraic extension of $\mathbb{F}_q(x_1, \ldots, x_n)$
2. Define factor base $\mathcal{F} = \{P \in U : x_2(P) = \ldots = x_n(P) = 0\}$
3. Decompose enough points of $\mathcal{A}$ as sum of n points of $\mathcal{F}$ using group law over $\mathcal{A} \leftrightarrow$ solve a multivariate polynomial system (and check rationality of solutions)
4. Extract the logarithms with sparse linear algebra

For fixed n, one relation costs $\tilde{O}(1)$
$\Rightarrow$ relation search in $\tilde{O}(q)$ vs linear algebra in $\tilde{O}(q^2)$

Index calculus on small dimension abelian varieties

Decomposition attack on DLP over $\mathcal{A}_{|\mathbb{F}_q}$, n-dimensional abelian variety

Gaudry's method

1. Choose $U \subset \mathcal{A}$ dense affine subset and coord. $(x_1, \ldots, x_n, y_1, \ldots, y_m)$ on U s.t. $\mathbb{F}_q(\mathcal{A})$ algebraic extension of $\mathbb{F}_q(x_1, \ldots, x_n)$
2. Define factor base $\mathcal{F} = \{P \in U : x_2(P) = \ldots = x_n(P) = 0\}$
3. Decompose enough points of $\mathcal{A}$ as sum of n points of $\mathcal{F}$ using group law over $\mathcal{A}$ $\leftrightarrow$ solve a multivariate polynomial system (and check rationality of solutions)
4. Extract the logarithms with sparse linear algebra

Rebalance with double large prime variation:
(heuristic) asymptotic complexity in $\tilde{O}(q^{2-2/n})$ as $q \to \infty$, n fixed

Index calculus on small dimension abelian varieties

- Generalizes the classical index calculus on $\mathcal{A} = \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$ where $\mathcal{H}$ is hyperelliptic with small genus g
- Main application so far: $\mathcal{A} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ where E elliptic curve defined over $\mathbb{F}_{q^n}$ [Gaudry-Diem]

Index calculus on small dimension abelian varieties

- Generalizes the classical index calculus on $\mathcal{A} = \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_q)$ where $\mathcal{H}$ is hyperelliptic with small genus g
- Main application so far: $\mathcal{A} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ where E elliptic curve defined over $\mathbb{F}_{q^n}$ [Gaudry-Diem]

Practical difficulty

In general, polynomial systems arising from decompositions are huge $\rightsquigarrow$ find nice representations of $\mathcal{A}$ and clever reformulation of the decompositions

- For elliptic curves, use Semaev's summation polynomials
- For $\mathcal{A} = W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n}))$: no equivalent of Semaev's polynomials, use reformulation by Nagao instead

The Riemann-Roch based approach of Nagao

$\mathcal{C}$ curve defined over $\mathbb{F}_{q^n}$ of genus g with a unique point $\mathcal{O}$ at infinity.

Factor base

$\mathcal{F} = \{D_Q \in \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \ : \ D_Q \sim (Q) - (\mathcal{O}), Q \in \mathcal{C}(\mathbb{F}_{q^n}), x(Q) \in \mathbb{F}_q\}$

How to check if D can be decomposed ?

$$D + \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O})) \sim 0 \Leftrightarrow D + \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O})) = div(f)$$

where $f \in \mathcal{L}_D = \mathcal{L}\left(ng(\mathcal{O}) - D\right)$, $\mathbb{F}_{q^n}$-vector space of dim. $(n-1)g + 1$

The Riemann-Roch based approach of Nagao

$\mathcal{C}$ curve defined over $\mathbb{F}_{q^n}$ of genus g with a unique point $\mathcal{O}$ at infinity.

Factor base

$\mathcal{F} = \{D_Q \in \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \ : \ D_Q \sim (Q) - (\mathcal{O}), Q \in \mathcal{C}(\mathbb{F}_{q^n}), x(Q) \in \mathbb{F}_q\}$

How to check if D can be decomposed ?

$$D + \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O})) \sim 0 \Leftrightarrow D + \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O})) = div(f)$$

where $f \in \mathcal{L}_D = \mathcal{L}\left(ng(\mathcal{O}) - D\right)$, $\mathbb{F}_{q^n}$-vector space of dim. $(n-1)g+1$

- Set of decomp. of D parametrized by $\mathbb{P}(\mathcal{L}_D) \simeq \mathbb{P}^\ell$, $\ell = (n-1)g$
- $(\lambda_1, \ldots, \lambda_\ell)$ affine chart of $\mathbb{P}(\mathcal{L}_D)$ s.t. $Q_i \neq \mathcal{O}$ for all $i = 1, \ldots, ng$

The Riemann-Roch based approach of Nagao

$\mathcal{C}$ curve defined over $\mathbb{F}_{q^n}$ of genus g with a unique point $\mathcal{O}$ at infinity.

Factor base

$\mathcal{F} = \{D_Q \in \mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n}) \;:\; D_Q \sim (Q) - (\mathcal{O}), Q \in \mathcal{C}(\mathbb{F}_{q^n}), x(Q) \in \mathbb{F}_q\}$

How to check if D can be decomposed ?

$$D + \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O})) \sim 0 \Leftrightarrow D + \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O})) = div(f)$$

where $f \in \mathcal{L}_D = \mathcal{L}\,(ng(\mathcal{O}) - D)$, $\mathbb{F}_{q^n}$-vector space of dim. $(n-1)g + 1$

- Set of decomp. of D parametrized by $\mathbb{P}(\mathcal{L}_D) \simeq \mathbb{P}^\ell$, $\ell = (n-1)g$
- $(\lambda_1, \ldots, \lambda_\ell)$ affine chart of $\mathbb{P}(\mathcal{L}_D)$ s.t. $Q_i \neq \mathcal{O}$ for all $i = 1, \ldots, ng$

Goal: determine $\lambda_1, \ldots, \lambda_\ell$ such that $x(Q_i) \in \mathbb{F}_q$

Nagao's approach for hyperelliptic curves

Given the Mumford representation of $D = (u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$

- $\mathcal{L}\left(ng(\mathcal{O}_{\mathcal{H}}) - D\right) = \langle u, xu, \ldots, x^{m_1}u, y - v, x(y - v), \ldots, x^{m_2}(y - v)\rangle$

$$f_{\lambda_1,\ldots,\lambda_{\ell+1}}(x, y) = u \sum_{i=0}^{m_1} \lambda_{2i+1}x^i + (y - v) \sum_{i=0}^{m_2} \lambda_{2i+2}x^i$$

Affine chart of $\mathbb{P}(\mathcal{L}_D) \leftrightarrow \lambda_{\ell+1} = 1$

Nagao's approach for hyperelliptic curves

Given the Mumford representation of $D = (u, v) \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$

- $\mathcal{L}\left(ng(\mathcal{O}_{\mathcal{H}}) - D\right) = \langle u, xu, \ldots, x^{m_1}u, y - v, x(y - v), \ldots, x^{m_2}(y - v)\rangle$

$$f_{\lambda_1,\ldots,\lambda_{\ell+1}}(x, y) = u\sum_{i=0}^{m_1} \lambda_{2i+1}x^i + (y - v)\sum_{i=0}^{m_2} \lambda_{2i+2}x^i$$

  Affine chart of $\mathbb{P}(\mathcal{L}_D) \leftrightarrow \lambda_{\ell+1} = 1$

- Using equation of $\mathcal{H}$, compute $f_{\lambda_1,\ldots,\lambda_\ell,1}(x, y) \cdot f_{\lambda_1,\ldots,\lambda_\ell,1}(x, -y)/u$ to get a new polynomial with roots $x(Q_1), \ldots, x(Q_{ng})$:

$$F_{\lambda_1,\ldots,\lambda_\ell}(x) = x^{ng} + \sum_{i=0}^{ng-1} c_i(\lambda_1, \ldots, \lambda_\ell)x^i$$

  $\rightarrow$ coefficient c_i of x^i is quadratic in the $\lambda_i \in \mathbb{F}_{q^n}$

Nagao's approach for hyperelliptic curves

$F_{\lambda_1,\ldots,\lambda_\ell}(x) = x^{ng} + \sum_{i=0}^{ng-1} c_i(\lambda_1,\ldots,\lambda_\ell)x^i$ with roots $x(Q_1),\ldots,x(Q_{ng})$

$\rightarrow$ Weil restriction of scalars: let $\mathbb{F}_{q^n} = \mathbb{F}_q(t)$ and write

$$\begin{cases} \lambda_i = \lambda_{i,0} + \lambda_{i,1}t + \cdots + \lambda_{i,n-1}t^{n-1} \\ c_i(\lambda_1,\ldots,\lambda_\ell) = \sum_{j=0}^{n-1} c_{i,j}(\lambda_{1,0},\ldots,\lambda_{\ell,n-1})t^j \end{cases}$$

Nagao's approach for hyperelliptic curves

$F_{\lambda_1,\ldots,\lambda_\ell}(x) = x^{ng} + \sum_{i=0}^{ng-1} c_i(\lambda_1,\ldots,\lambda_\ell)x^i$ with roots $x(Q_1),\ldots,x(Q_{ng})$

$\rightarrow$ Weil restriction of scalars: let $\mathbb{F}_{q^n} = \mathbb{F}_q(t)$ and write

$$\begin{cases} \lambda_i = \lambda_{i,0} + \lambda_{i,1}t + \cdots + \lambda_{i,n-1}t^{n-1} \\ c_i(\lambda_1,\ldots,\lambda_\ell) = \sum_{j=0}^{n-1} c_{i,j}(\lambda_{1,0},\ldots,\lambda_{\ell,n-1})t^j \end{cases}$$

Then

$F_{\lambda_1,\ldots,\lambda_\ell} \in \mathbb{F}_q[x] \Leftrightarrow \forall i \in \{0,\ldots,ng-1\}, \forall j \in \{1,\ldots,n-1\},\ c_{i,j} = 0$

Nagao's approach for hyperelliptic curves

$F_{\lambda_1,\ldots,\lambda_\ell}(x) = x^{ng} + \sum_{i=0}^{ng-1} c_i(\lambda_1,\ldots,\lambda_\ell)x^i$ with roots $x(Q_1),\ldots,x(Q_{ng})$

$\rightarrow$ Weil restriction of scalars: let $\mathbb{F}_{q^n} = \mathbb{F}_q(t)$ and write

$$\begin{cases} \lambda_i = \lambda_{i,0} + \lambda_{i,1}t + \cdots + \lambda_{i,n-1}t^{n-1} \\ c_i(\lambda_1,\ldots,\lambda_\ell) = \sum_{j=0}^{n-1} c_{i,j}(\lambda_{1,0},\ldots,\lambda_{\ell,n-1})t^j \end{cases}$$

Then

$F_{\lambda_1,\ldots,\lambda_\ell} \in \mathbb{F}_q[x] \Leftrightarrow \forall i \in \{0,\ldots,ng-1\}, \forall j \in \{1,\ldots,n-1\},\ c_{i,j} = 0$

Decomposition of D

- solve a quadratic polynomial system of $(n-1)ng$ eq./var.
- test if $F_{\lambda_1,\ldots,\lambda_\ell}$ is split in $\mathbb{F}_q[x]$
- recover decomposition from roots of $F_{\lambda_1,\ldots,\lambda_\ell}$

Example for a genus 2 curve over $\mathbb{F}_{67^2} = \mathbb{F}_{67}[t]/(t^2 - 2)$

$\mathcal{H} : y^2 = x^5 + (50t + 66)x^4 + (40t + 22)x^3 + (65t + 23)x^2 + (61t + 3)x + 43t + 6$

Decomposition of

$D = [x^2 + (52t + 3)x + 21t + 2,\ (22t + 41)x + 25t + 42] \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{67^2})$

Example for a genus 2 curve over $\mathbb{F}_{67^2} = \mathbb{F}_{67}[t]/(t^2-2)$

$\mathcal{H} : y^2 = x^5 + (50t+66)x^4 + (40t+22)x^3 + (65t+23)x^2 + (61t+3)x + 43t + 6$
Decomposition of
$D = [x^2 + (52t+3)x + 21t + 2,\ (22t+41)x + 25t + 42] \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{67^2})$

- consider $\mathcal{L}(4(\mathcal{O}_{\mathcal{H}}) - D) = \langle u(x), y - v(x), x\,u(x)\rangle$
- from $f_{\lambda_1,\lambda_2,1}(x,y) = x\,u(x) + \lambda_1(y - v(x)) + \lambda_2 u(x)$ and $h(x)$ $\rightarrow F_{\lambda_1,\lambda_2}(x) = x^4 \ + \ (-\lambda_1^2 + 2\lambda_2 + 52t + 3)\,x^3 \ + \ \ldots \in \mathbb{F}_{67}[x]$ with roots $x(Q_i)$
- find $\lambda_1, \lambda_2 \in \mathbb{F}_{67^2}$ s.t. F_{λ_1,λ_2} is in $\mathbb{F}_{67}[x]$
  $\Rightarrow \lambda_1, \lambda_2$ such that $\begin{cases} -\lambda_1^2 + 2\lambda_2 + 52t + 3 \in \mathbb{F}_{67} \\ \vdots \end{cases}$

Example for a genus 2 curve over $\mathbb{F}_{67^2} = \mathbb{F}_{67}[t]/(t^2 - 2)$

Weil restriction: let $\lambda_1 = \lambda_{1,0} + t\lambda_{1,1}$ and $\lambda_2 = \lambda_{2,0} + t\lambda_{2,1}$

$$F_{\lambda_1,\lambda_2}(x) \in \mathbb{F}_{67}[x] \Rightarrow \begin{cases} -2\lambda_{1,0}\lambda_{1,1} + 2\lambda_{2,1} + 52 = 0 \\ \vdots \end{cases}$$ with 2 solutions:

- $\lambda_1 = 7 + 40t,\ \lambda_2 = 8 + 53t$: $F_{\lambda_1,\lambda_2}(x) = x^4 + 53x^3 + 26x^2 + 44x + 12$
- $\lambda_1 = 55 + 37t,\ \lambda_2 = 52 - t$: $F_{\lambda_1,\lambda_2}(x) = (x - 23)(x - 34)(x - 51)(x - 54)$

From $f_{\lambda_1,\lambda_2,1}(x, y) = x\,u(x) + \lambda_1(y - v(x)) + \lambda_2 u(x) = 0$ recover $y(Q_i)$

$\rightsquigarrow D = (Q_1) + (Q_2) + (Q_3) + (Q_4) - 4(O_{\mathcal{H}})$ where

$$Q_1 = \left| \begin{matrix} 23 \\ 23t+12 \end{matrix} \right., Q_2 = \left| \begin{matrix} 34 \\ 10t+43 \end{matrix} \right., Q_3 = \left| \begin{matrix} 51 \\ 17t+3 \end{matrix} \right., Q_4 = \left| \begin{matrix} 54 \\ 23t+15 \end{matrix} \right.$$

Complexity on hyperelliptic curves

Double large prime variation

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

What about hidden constants?

1 decomp. test $\leftrightarrow$ solve a quadratic system of $(n-1)ng$ eq/var

- Zero-dimensional ideal of degree $d = 2^{(n-1)ng}$
- Resolution with a lexicographic Gröbner basis computation
  Tools: grevlex basis with **F4Remake** + ordering change with **FGLM**
- Complexity: at least in $d^3 = 2^{3(n-1)ng}$
  $\to$ relevant only for n and g small enough

Huge cost of decompositions $\to$ need for rebalance not so clear in practice

1. Background
   - Generalities on DLP and motivations
   - Weil descent
   - Index calculus for Jacobians of curves
   - Decomposition attack

2. Decomposition attack on hyperelliptic curves over extension fields
   - Generalities
   - New results

3. Cover and decomposition attacks

Modification of the relation search [Joux-V.]

$\mathcal{H}$ hyperelliptic curve of genus g with a unique point $\mathcal{O}_\mathcal{H}$ at infinity

In practice, decompositions as $D \sim \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O}_\mathcal{H}))$ are too slow to compute

Another type of relations

Compute relations involving only elements of $\mathcal{F}$:

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

Heuristically, expected number of such relations is $\simeq q^{m-ng}/m!$
$\rightarrow$ as $\simeq q$ relations are needed, consider $m = ng + 2$

Modification of the relation search [Joux-V.]

$\mathcal{H}$ hyperelliptic curve of genus g defined over $\mathbb{F}_{q^n}$, $n \geq 2$
Find relations of the form $\sum_{i=1}^{ng+2} ((Q_i) - (\mathcal{O}_\mathcal{H})) \sim 0$

- Riemann-Roch based approach: work in $\mathcal{L}((ng+2)(\mathcal{O}_\mathcal{H})) = \langle 1, x, x^2, \ldots, x^{m_1}, y, yx, \ldots, yx^{m_2} \rangle$ of dimension $\ell + 1 = (n-1)g + 3$
- Derive $F_{\lambda_1,\ldots,\lambda_\ell}(x)$ whose roots are $x(Q_1), \ldots, x(Q_{ng+2})$
- $F_{\lambda_1,\ldots,\lambda_\ell}(x) \in \mathbb{F}_q[x] \Rightarrow$ under-determined quadratic polynomial system of $n(n-1)g + 2n - 2$ equations in $n(n-1)g + 2n$ variables.
- After initial lex Gröbner basis precomputation, each specialization of the last two variables yields an easy to solve system.

A special case: quadratic extensions

$\mathcal{H}$ hyperelliptic curve of genus g defined over $\mathbb{F}_{q^2} = \mathbb{F}_q(t)/(P(t))$ with imaginary model $y^2 = h(x)$ where $\deg h = 2g+1$.

- Riemann-Roch: $f(x,y) = (x^{g+1} + \lambda_g x^g + \ldots + \lambda_0) + \mu y$

$$\Rightarrow F_{\lambda_0,\ldots,\lambda_g,\mu}(x) = (x^{g+1} + \lambda_g x^g + \ldots + \lambda_0)^2 - \mu^2 h(x)$$

A special case: quadratic extensions

$\mathcal{H}$ hyperelliptic curve of genus g defined over $\mathbb{F}_{q^2} = \mathbb{F}_q(t)/(P(t))$ with imaginary model $y^2 = h(x)$ where $\deg h = 2g+1$.

- Riemann-Roch: $f(x,y) = (x^{g+1} + \lambda_g x^g + \ldots + \lambda_0) + \mu y$

$$\Rightarrow F_{\lambda_0,\ldots,\lambda_g,\mu}(x) = (x^{g+1} + \lambda_g x^g + \ldots + \lambda_0)^2 - \mu^2 h(x)$$

- $\mu = 0 \rightsquigarrow$ trivial relation of the form $(P_1) + (\iota(P_1)) + \ldots + (P_{g+1}) + (\iota(P_{g+1})) - (2g+2)\mathcal{O}_{\mathcal{H}} \sim 0$

A special case: quadratic extensions

$\mathcal{H}$ hyperelliptic curve of genus g defined over $\mathbb{F}_{q^2} = \mathbb{F}_q(t)/(P(t))$ with imaginary model $y^2 = h(x)$ where $\deg h = 2g+1$.

- Riemann-Roch: $f(x,y) = (x^{g+1} + \lambda_g x^g + \ldots + \lambda_0) + \mu y$

$$\Rightarrow F_{\lambda_0,\ldots,\lambda_g,\mu}(x) = (x^{g+1} + \lambda_g x^g + \ldots + \lambda_0)^2 - \mu^2 h(x)$$

- $\mu = 0 \rightsquigarrow$ trivial relation of the form $(P_1) + (\iota(P_1)) + \ldots + (P_{g+1}) + (\iota(P_{g+1})) - (2g+2)\mathcal{O}_{\mathcal{H}} \sim 0$
- Weil restriction: $\lambda_i = \lambda_{i,0} + t\lambda_{i,1}$ and $\mu^2 = \mu_0 + t\mu_1$

$$F_{\lambda_0,\ldots,\lambda_g,\mu}(x) \in \mathbb{F}_q[x] \text{ and } \mu \neq 0$$
$$\Leftrightarrow (\lambda_{0,0},\ldots,\lambda_{g,0},\lambda_{0,1},\ldots,\lambda_{g,1},\mu_0,\mu_1) \in \mathbb{V}_{\mathbb{F}_q}(\mathrm{I} : (\mu_0,\mu_1)^\infty)$$

where I is the ideal corresponding to the quadratic polynomial system of $2g+2$ equations in $2g+4$ variables.

A special case: quadratic extensions

Key point

Define $\mathbb{F}_{q^2}$ as $\mathbb{F}_q(t)/(t^2-\omega)$ $\rightsquigarrow$ additional structure on the equations

$$F_{\lambda_0,\ldots,\lambda_g,\mu}(x) = (1\cdot x^{g+1} + \lambda_g x^g + \ldots + \lambda_0)^2 - \mu^2 h(x) \in \mathbb{F}_q[x] \Leftrightarrow$$
$$2(1\cdot x^{g+1} + \lambda_{g,0}x^g + \cdots + \lambda_{0,0})(\lambda_{g,1}x^g + \cdots + \lambda_{0,1}) - \mu_0 h_1(x) - \mu_1 h_0(x) = 0$$

A special case: quadratic extensions

Key point

Define $\mathbb{F}_{q^2}$ as $\mathbb{F}_q(t)/(t^2-\omega) \rightsquigarrow$ additional structure on the equations

$$F_{\lambda_0,\ldots,\lambda_g,\mu}(x) = (1\cdot x^{g+1} + \lambda_g x^g + \ldots + \lambda_0)^2 - \mu^2 h(x) \in \mathbb{F}_q[x] \Leftrightarrow$$
$$2(1\cdot x^{g+1} + \lambda_{g,0}x^g + \cdots + \lambda_{0,0})(\lambda_{g,1}x^g + \cdots + \lambda_{0,1}) - \mu_0 h_1(x) - \mu_1 h_0(x) = 0$$

The polynomials generating I are multi-homogeneous of deg $(1,1)$ in $(1,\lambda_{0,0},\ldots,\lambda_{g,0}),(\lambda_{0,1},\ldots,\lambda_{g,1},\mu_0,\mu_1)$

$\rightarrow$ speeds up the computation of the lex Gröbner basis:

genus	2	3	4
nb eq./var.	6/8	8/10	10/12
approx. timing	<1 sec	2 sec	1 h

$(g\log_2 q \simeq 70)$

A special case: quadratic extensions

The polynomials generating I are multi-homogeneous of deg $(1,1)$ in $(1,\lambda_{0,0},\dots,\lambda_{g,0}),(\lambda_{0,1},\dots,\lambda_{g,1},\mu_0,\mu_1)$

$\rightarrow \pi_1(\mathbb{V}(\mathrm{I}:(\mu_0,\mu_1)^\infty)) = \pi_1(\mathbb{V}(\mathrm{I}:(\lambda_{0,1},\dots,\lambda_{g,1},\mu_0,\mu_1)^\infty))$ has dim. 1
where $\pi_1 : (\lambda_{0,0},...,\lambda_{g,0},\lambda_{0,1},...,\lambda_{g,1},\mu_0,\mu_1) \mapsto (\lambda_{0,0},...,\lambda_{g,0})$

A special case: quadratic extensions

The polynomials generating I are multi-homogeneous of deg $(1,1)$ in $(1, \lambda_{0,0}, \ldots, \lambda_{g,0}), (\lambda_{0,1}, \ldots, \lambda_{g,1}, \mu_0, \mu_1)$

$\rightarrow \pi_1(\mathbb{V}(\mathrm{I}:(\mu_0,\mu_1)^\infty)) = \pi_1(\mathbb{V}(\mathrm{I}:(\lambda_{0,1},\ldots,\lambda_{g,1},\mu_0,\mu_1)^\infty))$ has dim. 1
where $\pi_1 : (\lambda_{0,0}, \ldots, \lambda_{g,0}, \lambda_{0,1}, \ldots, \lambda_{g,1}, \mu_0, \mu_1) \mapsto (\lambda_{0,0}, \ldots, \lambda_{g,0})$

Decomposition method

1. Outer loop:
   - "specialization": instead of evaluating e.g. $\lambda_{0,0}$, choose of a point $(\lambda_{0,0}, \ldots, \lambda_{g,0}) \in \pi_1(\mathbb{V}(\mathrm{I}:(\mu_0,\mu_1)^\infty))$
   - remaining variables lie in a one-dimensional vector space
2. Inner loop:
   - specialization of a second variable $\lambda_{0,1} \rightsquigarrow$ easy to solve system
   - factorization of $F_{\lambda_0,\ldots,\lambda_g,\mu}(x) \in \mathbb{F}_q[x] \rightsquigarrow$ potential relation

A second improvement: sieving

Idea: combine the modified relation search with a sieving technique
→ avoid the factorization of $F_{\lambda_0,\ldots,\lambda_g,\mu}$ in $\mathbb{F}_q[x]$

A second improvement: sieving

Idea: combine the modified relation search with a sieving technique
$\rightarrow$ avoid the factorization of $F_{\lambda_0,\ldots,\lambda_g,\mu}$ in $\mathbb{F}_q[x]$

Sieving method

1. Specialize $\lambda_{0,0},\ldots,\lambda_{g,0}$ and express all remaining var. in terms of $\lambda_{0,1}$
$\rightarrow$ F becomes a polynomial in $\mathbb{F}_q[x,\lambda_{0,1}]$ of degree 2 in $\lambda_{0,1}$
2. Enumeration in $x \in \mathbb{F}_q$ instead of $\lambda_{0,1}$
$\rightarrow$ corresponding values of $\lambda_{0,1}$ are easier to compute
3. Possible to recover the values of $\lambda_{0,1}$ for which there were $\deg_x F$ associated values of x

Time-memory trade-off:

$\lambda_{0,1}$	0	1	2	$\cdots$	i	$\cdots$	$p-1$
$\#x$	x_0	x_1	x_2	$\cdots$	x_i	$\cdots$	x_{p-1}

A second improvement: sieving

Idea: combine the modified relation search with a sieving technique
$\rightarrow$ avoid the factorization of $F_{\lambda_0,\dots,\lambda_g,\mu}$ in $\mathbb{F}_q[x]$

Sieving method

1. Specialize $\lambda_{0,0},\dots,\lambda_{g,0}$ and express all remaining var. in terms of $\lambda_{0,1}$
$\rightarrow$ F becomes a polynomial in $\mathbb{F}_q[x,\lambda_{0,1}]$ of degree 2 in $\lambda_{0,1}$
2. Enumeration in $x \in \mathbb{F}_q$ instead of $\lambda_{0,1}$
$\rightarrow$ corresponding values of $\lambda_{0,1}$ are easier to compute
3. Possible to recover the values of $\lambda_{0,1}$ for which there were $\deg_x F$ associated values of x

Time-memory trade-off:

$\lambda_{0,1}$	0	1	2	$\cdots$	i	$\cdots$	$p-1$
$\#x$	x_0	x_1	x_2	$\cdots$	x_i	$\cdots$	x_{p-1}

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

A combined attack

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

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

A combined attack

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

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

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

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 $\mathbb{F}_{p^2}$
   $\to$ 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

Cover and Decomposition Attacks on Elliptic Curves

Vanessa VITSE
Joint work with Antoine JOUX

Université de Versailles Saint-Quentin, Laboratoire PRiSM

Séminaire de Théorie des Nombres de Caen – LMNO

Scaling data for our implementation

Size of p	$\log_2 p \approx 23$	$\log_2 p \approx 24$	$\log_2 p \approx 25$
Sieving (CPU.hours)	3 600	15 400	63 500
Sieving (real time)	3.5 hours	15 hours	62 hours
Group size	136 bits	142 bits	148 bits
Matrix column nb (SGE reduction)	990 193 (4.2)	1 736 712 (4.8)	3 092 914 (5.4)
Lanczos (CPU.hours)	4 900	16 000	43 800
Lanczos (real time)	77 hours	250 hours	28.5 days

$\rightarrow$ approximately 200 CPU.years to break DLP over a 160-bit curve group