Cover and Decomposition Attack on Elliptic Curves

Vanessa VITSE – Antoine JOUX

Université de Versailles Saint-Quentin, Laboratoire PRISM

Arbeitsgemeinschaft in Codierungstheorie and Kryptographie
20 April 2011

Section 1

Known attacks of the ECDLP

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 $\#G = \prod_i p_i^{\alpha_i}$
2. $G \subset (\mathbb{F}_q^*, \times)$: index calculus method with complexity in $L_q(1/3)$ where $L_q(\alpha) = exp(c(\log q)^{\alpha}(\log\log q)^{1-\alpha})$.
3. $G \subset (J_{\mathcal{C}}(\mathbb{F}_q), +)$: index calculus method with sub-exponential complexity (depending of the genus $g > 2$)

Basic outline of index calculus methods
(additive notations)

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

$$a_i \cdot g + b_i \cdot h = \sum_{j=1}^{N} c_{i,j} \cdot g_j$$

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

Hardness of ECDLP

ECDLP

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

Hardness of ECDLP

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

Lift of the ECDLP via cover maps

$\pi : \mathcal{C} \to E$ cover map,
$\mathcal{C}$ curve defined over $\mathbb{F}_q$ of genus g, E elliptic curve defined over $\mathbb{F}_{q^n}$

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

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

Lift of the ECDLP via cover maps

$\pi : \mathcal{C} \to E$ cover map,
$\mathcal{C}$ curve defined over $\mathbb{F}_q$ of genus g, E elliptic curve defined over $\mathbb{F}_{q^n}$

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

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

$$\ker(Tr \circ \pi^*) \cap \langle P \rangle = \{O\}$$
$$\Rightarrow g \geq n$$

Lift of the ECDLP via cover maps

$\pi : \mathcal{C} \to E$ cover map,
$\mathcal{C}$ curve defined over $\mathbb{F}_q$ of genus g, E elliptic curve defined over $\mathbb{F}_{q^n}$

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

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

$$\ker(Tr \circ \pi^*) \cap \langle P \rangle = \{O\}$$
$$\Rightarrow g \geq n$$

2. use index calculus on $J_{\mathcal{C}}(\mathbb{F}_q)$:
$\to$ efficient if $\mathcal{C}$ is hyperelliptic with small genus g or has a small degree plane model

Lift of the ECDLP via cover maps

$\pi : \mathcal{C} \to E$ cover map,
$\mathcal{C}$ curve defined over $\mathbb{F}_q$ of genus g, E elliptic curve defined over $\mathbb{F}_{q^n}$

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

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

$$\ker(Tr \circ \pi^*) \cap \langle P \rangle = \{O\}$$
$$\Rightarrow g \geq n$$

2. use index calculus on $J_{\mathcal{C}}(\mathbb{F}_q)$:
   $\to$ efficient if $\mathcal{C}$ is hyperelliptic with small genus g or has a small degree plane model

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

The GHS construction

Gaudry-Heß-Smart (binary fields), Diem (odd characteristic)

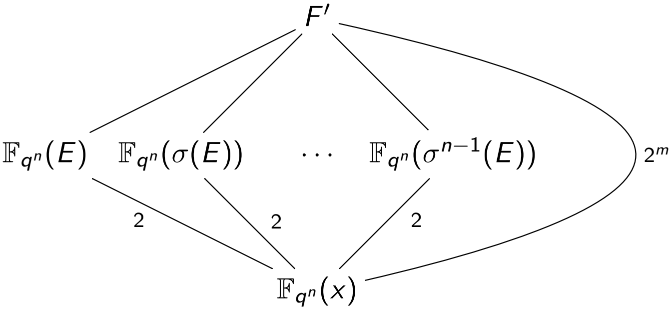
$\sigma_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ Frobenius automorphism

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

- F is the function field of the wanted curve
- the construction depends on $x \in \mathbb{F}_{q^n}(E)$ such that $\mathbb{F}_{q^n}(E)$ is a degree 2 extension of $\mathbb{F}_{q^n}(x)$

The GHS construction

Gaudry-Heß-Smart (binary fields), Diem (odd characteristic)



- m "magic number" such that the genus g of F' depends essentially of $[F' : \mathbb{F}_{q^n}(x)] = 2^m$
- For most elliptic curves E, $m \simeq n \rightarrow g$ is of order 2^n

Observations

1. For most elliptic curves, g is of the order of 2^n
   - Index calculus on $J_{\mathcal{C}}(\mathbb{F}_q)$ usually slower than generic methods on $E(\mathbb{F}_{q^n})$
   - Possibility of using isogenies from E to a vulnerable curve [Galbraith] $\rightarrow$ increase the number of vulnerable curves
2. Kernel of $Tr \circ \pi^*$ intersects $\langle P \rangle \subset E(\mathbb{F}_{q^n})$ trivially in most cryptographic settings
3. Complexity of the Weil descent usually negligible compared to the index calculus phase, unless isogeny walk used

Index calculus step of the Weil Descent

[Adleman, DeMarais, Huang, Gaudry, Diem, Enge, Thomé, Thériault...]

Index calculus on $J_H(\mathbb{F}_q)$, H hyperelliptic

1. factor base: $\mathcal{F} = \{D \sim (u,v) : \; u \in \mathbb{F}_q[x] \text{ irred}, \; \deg(u) \leq B\}$
2. relation search:
   $D = (u,v)$ decomposes in $\mathcal{F} \leftrightarrow u$ is B-smooth over $\mathbb{F}_q[x]$
3. sparse linear algebra in $\tilde{O}(\#\mathcal{F}^2)$

- g large: optimal choice of B in $log_q(L_{q^g}(1/2))$
  $\rightarrow$ complexity in $L_{q^g}(1/2)$
- g small: $B = 1$, $\#\mathcal{F} = O(q)$
  relation search in $\tilde{O}(g!q)$: faster than linear algebra step when q large
  $\rightarrow$ double large prime variation to rebalance the two steps [Thériault]

Double large prime variation

Idea: reduce the factor base to rebalance the 2 steps

- In the factor base $\mathcal{F} = \{D \sim (u, v) : \ u \in \mathbb{F}_q[x], \deg(u) = 1\}$, choose: $\mathcal{F}' \subset \mathcal{F}$ set of "small primes"; $\mathcal{F} \setminus \mathcal{F}'$ set of "large primes"
- Discard all relations involving more than 2 large primes
- After collecting about $\#\mathcal{F}$ relations 2LP, eliminate all the large primes to obtain $\simeq \#\mathcal{F}'$ relations involving only small primes
- Linear algebra in $\tilde{O}((\#\mathcal{F}')^2)$

Double large prime variation

Idea: reduce the factor base to rebalance the 2 steps

- In the factor base $\mathcal{F} = \{D \sim (u, v) : \ u \in \mathbb{F}_q[x], \deg(u) = 1\}$, choose: $\mathcal{F}' \subset \mathcal{F}$ set of "small primes"; $\mathcal{F} \setminus \mathcal{F}'$ set of "large primes"
- Discard all relations involving more than 2 large primes
- After collecting about $\#\mathcal{F}$ relations 2LP, eliminate all the large primes to obtain $\simeq \#\mathcal{F}'$ relations involving only small primes
- Linear algebra in $\tilde{O}((\#\mathcal{F}')^2)$

Asymptotic best choice when $q \to \infty$ (g fixed): $\#\mathcal{F}' = q^{1-1/g}$

$$\Rightarrow \text{complexity in } \tilde{O}(q^{2-2/g})$$

Double large prime variation

Idea: reduce the factor base to rebalance the 2 steps

- In the factor base $\mathcal{F} = \{D \sim (u, v) : \; u \in \mathbb{F}_q[x], \deg(u) = 1\}$, choose: $\mathcal{F}' \subset \mathcal{F}$ set of "small primes"; $\mathcal{F} \setminus \mathcal{F}'$ set of "large primes"
- Discard all relations involving more than 2 large primes
- After collecting about $\#\mathcal{F}$ relations 2LP, eliminate all the large primes to obtain $\simeq \#\mathcal{F}'$ relations involving only small primes
- Linear algebra in $\tilde{O}((\#\mathcal{F}')^2)$

Asymptotic best choice when $q \to \infty$ (g fixed): $\#\mathcal{F}' = q^{1-1/g}$

$$\Rightarrow \text{complexity in } \tilde{O}(q^{2-2/g})$$

Practical best choice depends on the actual cost of the two phases and the computing power available (easy to parallelize the relation search but not the linear algebra)

Index calculus step of the Weil Descent

Index calculus on $J_{\mathcal{C}}(\mathbb{F}_q)$, $\mathcal{C}$ small degree plane curve [Diem]

$\mathcal{C}$ plane curve of degree d, $P_0 \in \mathcal{C}(\mathbb{F}_q)$ base point, D_∞ divisor associated to the line at infinity

1. factor base: $\mathcal{F} = \{(P) - (P_0), P \in \mathcal{C}(\mathbb{F}_q)\} \cup \{D_\infty - d(P_0)\}$
   small primes: $\mathcal{F}' \subset \mathcal{F}$
2. relation search: for each $P_1, P_2 \in \mathcal{F}'$, consider f the equation of the line through P_1, P_2: $div(f) = (P_1) + (P_2) + D - D_\infty$
   $\rightarrow$ relation if D sum of $d-2$ points in $\mathcal{F}$, only 2 of which not in $\mathcal{F}'$
3. sparse linear algebra in $\tilde{O}(\#\mathcal{F}'^2)$

Index calculus step of the Weil Descent

Index calculus on $J_{\mathcal{C}}(\mathbb{F}_q)$, $\mathcal{C}$ small degree plane curve [Diem]

$\mathcal{C}$ plane curve of degree d, $P_0 \in \mathcal{C}(\mathbb{F}_q)$ base point, D_∞ divisor associated to the line at infinity

1. factor base: $\mathcal{F} = \{(P) - (P_0), P \in \mathcal{C}(\mathbb{F}_q)\} \cup \{D_\infty - d(P_0)\}$
   small primes: $\mathcal{F}' \subset \mathcal{F}$
2. relation search: for each $P_1, P_2 \in \mathcal{F}'$, consider f the equation of the line through P_1, P_2: $div(f) = (P_1) + (P_2) + D - D_\infty$
   $\rightarrow$ relation if D sum of $d-2$ points in $\mathcal{F}$, only 2 of which not in $\mathcal{F}'$
3. sparse linear algebra in $\tilde{O}(\#\mathcal{F}'^2)$

Asymptotic best choice when $q \to \infty$ (d fixed): $\#\mathcal{F}' = \tilde{O}(q^{1-1/(d-2)})$

$\Rightarrow$ complexity in $\tilde{O}(q^{2-2/(d-2)})$

Index calculus step of the Weil Descent

Index calculus on $J_{\mathcal{C}}(\mathbb{F}_q)$, $\mathcal{C}$ small degree plane curve [Diem]

$\mathcal{C}$ plane curve of degree d, $P_0 \in \mathcal{C}(\mathbb{F}_q)$ base point, D_∞ divisor associated to the line at infinity

1. factor base: $\mathcal{F} = \{(P) - (P_0), P \in \mathcal{C}(\mathbb{F}_q)\} \cup \{D_\infty - d(P_0)\}$
   small primes: $\mathcal{F}' \subset \mathcal{F}$
2. relation search: for each $P_1, P_2 \in \mathcal{F}'$, consider f the equation of the line through P_1, P_2: $div(f) = (P_1) + (P_2) + D - D_\infty$
   $\rightarrow$ relation if D sum of $d-2$ points in $\mathcal{F}$, only 2 of which not in $\mathcal{F}'$
3. sparse linear algebra in $\tilde{O}(\#\mathcal{F}'^2)$

Asymptotic best choice when $q \to \infty$ (d fixed): $\#\mathcal{F}' = \tilde{O}(q^{1-1/(d-2)})$

$$\Rightarrow \text{complexity in } \tilde{O}(q^{2-2/(d-2)})$$

$\rightarrow$ for $g = 3$, DLP easier on non-hyperelliptic curves

Decomposition attack

Idea from Gaudry and Diem: no transfer, but apply directly index calculus on $E(\mathbb{F}_{q^n})$ (or $J_H(\mathbb{F}_{q^n})$)

Principle

- Factor base:
  $\mathcal{F} = \{D_Q \in J_H(\mathbb{F}_{q^n}) \ : \ D_Q \sim (Q) - (\mathcal{O}_H), Q \in H(\mathbb{F}_{q^n}), x(Q) \in \mathbb{F}_q\}$
- Decomposition of an arbitrary divisor $D \in J_H(\mathbb{F}_{q^n})$ into ng divisors of the factor base $D \sim \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O}_H))$

Decomposition attack

Idea from Gaudry and Diem: no transfer, but apply directly index calculus on $E(\mathbb{F}_{q^n})$ (or $J_H(\mathbb{F}_{q^n})$)

Principle

- Factor base:
  $\mathcal{F} = \{D_Q \in J_H(\mathbb{F}_{q^n}) \ : \ D_Q \sim (Q) - (\mathcal{O}_H), Q \in H(\mathbb{F}_{q^n}), x(Q) \in \mathbb{F}_q\}$
- Decomposition of an arbitrary divisor $D \in J_H(\mathbb{F}_{q^n})$ into ng divisors of the factor base $D \sim \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O}_H))$

- interesting when g is small ($g \leq 3$)
- every curves are equally weak under this attack
- decomposition is harder (need to solve polynomial systems)

Nagao's approach for decompositions

How to check if $D = (u, v)$ can be decomposed ?

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

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

- Polynomial $F_{\lambda_1,\ldots,\lambda_\ell}(x)$ with roots $x(Q_1), \ldots, x(Q_{ng})$
- $F_{\lambda_1,\ldots,\lambda_\ell} \in \mathbb{F}_q[x] \Leftrightarrow$ components of the λ_i in a $(\mathbb{F}_{q^n}/\mathbb{F}_q)$-linear base satisfy a system of polynomial equations
- Decomposition of $D \leftrightarrow$ solve a quadratic polynomial system of $(n-1)ng$ equations and variables + test if $F_{\lambda_1,\ldots,\lambda_\ell}$ is split in $\mathbb{F}_q[x]$

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

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

- consider $\mathcal{L}(4(O_H) - D) = \langle u(x), y - v(x), x\,u(x) \rangle$
- starting from $f(x,y) = x\,u(x) + \lambda_1(y - v(x)) + \lambda_2 u(x)$
  compute $F_{\lambda_1,\lambda_2}(x) = f(x,y)f(x,-y)/u(x)$
  $\rightarrow$ monic deg. 4 poly. in x, with roots $x(Q_i)$, quadratic in λ_1, λ_2
- find $\lambda_1, \lambda_2 \in \mathbb{F}_{67^2}$ s.t. F_{λ_1,λ_2} is in $\mathbb{F}_{67}[x]$

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

- $F_{\lambda_1,\lambda_2}(x) = x^4 + (-\lambda_1^2+2\lambda_2+52t+3)\,x^3 + \ldots \in \mathbb{F}_{67}[x]$

  $\Rightarrow \lambda_1, \lambda_2$ s.t. $\begin{cases} -\lambda_1^2+2\lambda_2+52t+3 \in \mathbb{F}_{67} \\ \vdots \end{cases}$

- Weil restriction: solve a quadratic polynomial system with 4 var/eq and check if resulting F_{λ_1,λ_2} splits in linear factors

Nagao's decomposition

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

- $\lambda_1 = 7 + 40t,\ \lambda_2 = 8 + 53t$: $F_{\lambda_1,\lambda_2}(x) = x^4 + 53x^3 + 26x^2 + 44x + 12$
- $\lambda_1 = 55 + 37t,\ \lambda_2 = 52 - t$: $F_{\lambda_1,\lambda_2}(x) = (x-23)(x-34)(x-51)(x-54)$
  $\rightsquigarrow D = (Q_1) + (Q_2) + (Q_3) + (Q_4) - 4(O_H)$ where
  $Q_1 = \left| \begin{matrix} 23 \\ 23t+12 \end{matrix} \right., Q_2 = \left| \begin{matrix} 34 \\ 10t+43 \end{matrix} \right., Q_3 = \left| \begin{matrix} 51 \\ 17t+3 \end{matrix} \right., Q_4 = \left| \begin{matrix} 54 \\ 23t+15 \end{matrix} \right.$

Nagao's decomposition

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

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:

- $\lambda_1 = 7 + 40t,\ \lambda_2 = 8 + 53t$: $F_{\lambda_1,\lambda_2}(x) = x^4 + 53x^3 + 26x^2 + 44x + 12$
- $\lambda_1 = 55 + 37t,\ \lambda_2 = 52 - t$: $F_{\lambda_1,\lambda_2}(x) = (x-23)(x-34)(x-51)(x-54)$
  $\rightsquigarrow D = (Q_1) + (Q_2) + (Q_3) + (Q_4) - 4(O_H)$ where
  $Q_1 = \left| \begin{array}{c} 23 \\ 23t+12 \end{array} \right., Q_2 = \left| \begin{array}{c} 34 \\ 10t+43 \end{array} \right., Q_3 = \left| \begin{array}{c} 51 \\ 17t+3 \end{array} \right., Q_4 = \left| \begin{array}{c} 54 \\ 23t+15 \end{array} \right.$

Non-hyperelliptic case

- Use a resultant to compute $F_{\lambda_1,\ldots,\lambda_\ell}(x)$
- Decomposition of $D \to$ solve a polynomial system of $(n-1)ng$ equations and variables with degree > 2

Complexity of decomposition attacks

- Complexity of the relation search:
  system resolution at least polynomial in $2^{n(n-1)g}$
  $\rightarrow$ relevant only for n and g small enough
  $\rightarrow$ total complexity in $\tilde{O}(q)$
- Complexity of the linear algebra in $\tilde{O}(q^2)$

Complexity of decomposition attacks

- Complexity of the relation search:
  system resolution at least polynomial in $2^{n(n-1)g}$
  $\rightarrow$ relevant only for n and g small enough
  $\rightarrow$ total complexity in $\tilde{O}(q)$
- Complexity of the linear algebra in $\tilde{O}(q^2)$

Double large prime variation ?

- Overall asymptotic complexity in $q^{2-2/ng}$ as $q \rightarrow \infty$, n fixed
- In practice, huge cost of the decompositions $\rightarrow$ almost no rebalance needed

Complexity of decomposition attacks

- Complexity of the relation search:
  system resolution at least polynomial in $2^{n(n-1)g}$
  $\rightarrow$ relevant only for n and g small enough
  $\rightarrow$ total complexity in $\tilde{O}(q)$
- Complexity of the linear algebra in $\tilde{O}(q^2)$

Double large prime variation ?

- Overall asymptotic complexity in $q^{2-2/ng}$ as $q \rightarrow \infty$, n fixed
- In practice, huge cost of the decompositions $\rightarrow$ almost no rebalance needed

In the elliptic case: use Semaev's summation polynomials instead

Section 2

Results

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

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 $J_{\mathcal{C}}(\mathbb{F}_{q^d})$
2. use decomposition attack on $J_{\mathcal{C}}(\mathbb{F}_{q^d})$ with base field $\mathbb{F}_q$ to solve the DLP

A combined attack

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

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

Cover and decomposition attack

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 $J_{\mathcal{C}}(\mathbb{F}_{q^d})$
2. use decomposition attack on $J_{\mathcal{C}}(\mathbb{F}_{q^d})$ with base field $\mathbb{F}_q$ to solve the DLP

Typical case $\mathbb{F}_{p^6}$

1. cover map lifts DLP to genus 3 curve over $\mathbb{F}_{p^2}$
2. decomposition on genus 3 curve

Algorithm with precomputation

Precomputation on $J_{\mathcal{C}}(\mathbb{F}_{q^d})$

- Find enough relations between factor base elements with a modified relation search
- Do linear algebra to get logs of factor base elements

Individual logarithms on $E(\mathbb{F}_{q^n})$

- Use cover map to lift DLP from $E(\mathbb{F}_{q^n})$ to $J_{\mathcal{C}}(\mathbb{F}_{q^d})$
- Use a Nagao's style decomposition to obtain representation as sum of factor base elements
- Recover discrete logarithm

A modified relation search

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

Improvement

Compute relations between elements of $\mathcal{F}$: $\sum_{i=1}^{ng+2} ((Q_i) - (\mathcal{O}_H)) \sim 0$

- Finding such a relation $\rightsquigarrow$ working in $\mathcal{L}((ng+2)(\mathcal{O}_H))$
- Resolution of an underdetermined quadratic polynomial system of $n(n-1)g + 2n - 2$ equations in $n(n-1)g + 2n$ variables.
- After initial precomputation, each specialization of the last two variables yields an easy to solve system.

A sieving technique

Idea: combine the modified relation search with a sieving technique
$\rightarrow$ avoid the factorisation of $F_{\lambda_1,\ldots,\lambda_\ell}$ in $\mathbb{F}_q[X]$

A sieving technique

Idea: combine the modified relation search with a sieving technique
$\rightarrow$ avoid the factorisation of $F_{\lambda_1,\ldots,\lambda_\ell}$ in $\mathbb{F}_q[X]$

Sieving method

1. Specialisation of 1 variable $\lambda_{i,1}$ instead of $(\lambda_{i,1}, \lambda_{i,2})$
2. Express all remaining variables in terms of $\lambda_{i,2}$
   $\rightarrow$ F becomes a polynomial in $\mathbb{F}_q[X, \lambda_{i,2}]$, with a smaller degree in $\lambda_{i,2}$ (as low as 2 in our applications)
3. Enumeration in $X \in \mathbb{F}_q$ instead of $\lambda_{i,2}$
   $\rightarrow$ corresponding values of $\lambda_{i,2}$ are easier to compute
4. Possible to recover the values of $\lambda_{i,2}$ for which there were $\deg_X F$ associated values of X

A sieving technique

Idea: combine the modified relation search with a sieving technique
$\rightarrow$ avoid the factorisation of $F_{\lambda_1,\ldots,\lambda_\ell}$ in $\mathbb{F}_q[X]$

Sieving method

1. Specialisation of 1 variable $\lambda_{i,1}$ instead of $(\lambda_{i,1}, \lambda_{i,2})$
2. Express all remaining variables in terms of $\lambda_{i,2}$
   $\rightarrow$ F becomes a polynomial in $\mathbb{F}_q[X, \lambda_{i,2}]$, with a smaller degree in $\lambda_{i,2}$ (as low as 2 in our applications)
3. Enumeration in $X \in \mathbb{F}_q$ instead of $\lambda_{i,2}$
   $\rightarrow$ corresponding values of $\lambda_{i,2}$ are easier to compute
4. Possible to recover the values of $\lambda_{i,2}$ for which there were $\deg_X F$ associated values of X

Remark

This sieving works well with double large prime variation

Complexity with the modified relation search

On the asymptotic side...

Decomposition in $ng + 2$ instead of ng points seems worse:

- Double large prime variation less efficient:
  $\rightarrow$ complexity in $O(q^{2-2/(ng+2)})$ instead of $O(q^{2-2/ng})$
- With the sieving: complexity in $O(q^{2-2/(ng+1)})$

Complexity with the modified relation search

On the asymptotic side...

Decomposition in $ng + 2$ instead of ng points seems worse:

- Double large prime variation less efficient:
  $\rightarrow$ complexity in $O(q^{2-2/(ng+2)})$ instead of $O(q^{2-2/ng})$
- With the sieving: complexity in $O(q^{2-2/(ng+1)})$

But in practice...

- better actual complexity for all accessible values of q
- much faster to compute decompositions with our variant
  $\rightarrow$ about 750 times faster in our application to sextic extensions

Application to $E(\mathbb{F}_{q^6})$

Extension degree $n = 6$ recommended for some Optimal Extension Fields (fast arithmetic). Potential attacks on curves defined over $\mathbb{F}_{q^6}$:

- GHS: cover $\mathcal{C}_{|\mathbb{F}_q}$ with genus $g \geq 9$ (genus 9 very rare: less than q^3 curves)
  $\rightsquigarrow$ index calculus on $J_{\mathcal{C}}(\mathbb{F}_q)$ is usually slower than generic attacks
- direct decomposition attack fails to compute any relation

Combined attack on $\mathbb{F}_{q^6} — \mathbb{F}_{q^3} — \mathbb{F}_q$ or $\mathbb{F}_{q^6} — \mathbb{F}_{q^2} — \mathbb{F}_q$

Favorable cases for this attack: $E_{|\mathbb{F}_{q^6}}$ admits either a

1. (hyperelliptic) genus 2 cover $H'_{|\mathbb{F}_{q^3}}$
2. non-hyperelliptic genus 3 cover $\mathcal{C}_{|\mathbb{F}_{q^2}}$
3. hyperelliptic genus 3 cover $H_{|\mathbb{F}_{q^2}}$

Covers of $E(\mathbb{F}_{q^6})$

1. Genus 2 cover by $H'_{|\mathbb{F}_{q^3}}$:

E is in Scholten form

$$y^2 = \alpha x^3 + \beta x^2 + \sigma(\beta)x + \sigma(\alpha), \quad (\alpha, \beta \in \mathbb{F}_{q^6}, \sigma_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}})$$

- $\Theta(q^6)$ elliptic curves can be expressed in Scholten form

Covers of $E(\mathbb{F}_{q^6})$

1. Genus 2 cover by $H'_{|\mathbb{F}_{q^3}}$:

E is in Scholten form

$$y^2 = \alpha x^3 + \beta x^2 + \sigma(\beta)x + \sigma(\alpha), \quad (\alpha, \beta \in \mathbb{F}_{q^6}, \sigma_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}})$$

- $\Theta(q^6)$ elliptic curves can be expressed in Scholten form
- natural genus 2 curve defined over $\mathbb{F}_{q^6}$:

$$y^2 = \alpha x^6 + \beta x^4 + \sigma(\beta)x^2 + \sigma(\alpha)$$

Covers of $E(\mathbb{F}_{q^6})$

1. Genus 2 cover by $H'_{|\mathbb{F}_{q^3}}$:

E is in Scholten form

$$y^2 = \alpha x^3 + \beta x^2 + \sigma(\beta)x + \sigma(\alpha), \quad (\alpha, \beta \in \mathbb{F}_{q^6}, \sigma_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}})$$

- $\Theta(q^6)$ elliptic curves can be expressed in Scholten form
- natural genus 2 curve defined over $\mathbb{F}_{q^6}$:

$$y^2 = \alpha x^6 + \beta x^4 + \sigma(\beta)x^2 + \sigma(\alpha)$$

- after the change of coordinates $(x, y) = \left(\frac{X-c}{X-\sigma(c)}, \frac{Y}{(X-\sigma(c))^3}\right)$, genus 2 cover defined over $\mathbb{F}_{q^3}$

$$Y^2 = \alpha(X-c)^6 + \beta(X-c)^4(X-\sigma(c))^2 + \sigma(\beta)(X-c)^2(X-\sigma(c))^4 + \sigma(\alpha)(X-\sigma(c))^6$$

Covers of $E(\mathbb{F}_{q^6})$

2. Non-hyperelliptic genus 3 cover by $\mathcal{C}_{|\mathbb{F}_{q^2}}$ [Momose-Chao]
   - E is of the form $y^2 = (x-\alpha)(x-\alpha^{q^2})(x-\beta)(x-\beta^{q^2})$, where $\alpha, \beta \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$ or $\alpha \in \mathbb{F}_{q^{12}} \setminus (\mathbb{F}_{q^4} \cup \mathbb{F}_{q^6})$ and $\beta = \alpha^{q^6}$
   - occurs for $\Theta(q^6)$ curves

Covers of $E(\mathbb{F}_{q^6})$

2. Non-hyperelliptic genus 3 cover by $\mathcal{C}_{|\mathbb{F}_{q^2}}$ [Momose-Chao]
   - E is of the form $y^2 = (x-\alpha)(x-\alpha^{q^2})(x-\beta)(x-\beta^{q^2})$, where $\alpha, \beta \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$ or $\alpha \in \mathbb{F}_{q^{12}} \setminus (\mathbb{F}_{q^4} \cup \mathbb{F}_{q^6})$ and $\beta = \alpha^{q^6}$
   - occurs for $\Theta(q^6)$ curves

3. Hyperelliptic genus 3 cover by $H_{|\mathbb{F}_{q^2}}$ [Thériault, Momose-Chao]
   - E is of the form $y^2 = h(x)(x-\alpha)(x-\alpha^{q^2})$,
     where $\alpha \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$, $h \in \mathbb{F}_{q^2}[x]$
   - occurs for $\Theta(q^4)$ curves directly
   - occurs for most curves with cardinality divisible by 4, after an isogeny walk of length $O(q^2)$

Complexity and comparison with other attacks

Estimations for E elliptic curve defined over $\mathbb{F}_{p^6}$ with $|p| \simeq 27$ bits and $\#E(\mathbb{F}_{p^6}) = 4\ell$ with ℓ a 160-bit prime

Attack	Asymptotic complexity	162-bit example cost	Ratio of vulnerable curves (without isogeny walk)
Pollard	p^3	2^{99}	1
Ind. calc. on $H_{\vert\mathbb{F}_{p^2}}$, $g(H)=3$	$p^{8/3}$	2^{90}	$1/p^2$
Ind. calc. on $H_{\vert\mathbb{F}_{p}}$, $g(H)=9$	$p^{16/9}$	2^{68}	$\leq 1/p^3$
Decomp. on $E_{\vert\mathbb{F}_{(p^2)^3}}$	$p^{8/3}$	2^{97}	1
Decomp. on $E_{\vert\mathbb{F}_{p^6}}$	$p^{5/3}$	2^{135}	1
Decomp. on $H_{\vert\mathbb{F}_{p^2}}$, $g(H)=3$	$p^{5/3}$	2^{65}	$1/p^2$
Decomp. on $H_{\vert\mathbb{F}_{p^3}}$, $g(H)=2$	$p^{5/3}$	2^{112}	1

A 130-bit example

A seemingly secure curve

$E: \ y^2 = (x-c)(x-\alpha)(x-\sigma(\alpha))$ defined over $\mathbb{F}_{p^6}$ where $p = 2^{22}+15$, such that $\#E = 4 \cdot 1361158674614712334466525985682062201601$.

GHS $\rightsquigarrow$ $\mathbb{F}_p$-defined cover of genus 33, too large for efficient index calculus

Decomposition on the genus 3 hyperelliptic cover $H_{|\mathbb{F}_{p^2}}$:
using structured Gaussian elimination instead of the 2LP variation

1. Relation search
   - lex GB of a system of 8 eq. and 10 var. in 1 min (Magma on a 2.6 GHz Intel Core 2 Duo proc)
   - sieving phase: $\simeq 25 \cdot p$ relations in about 1 h with 200 cores (2.93 GHz quadri-core Intel Xeon 5550 proc)

     $\rightsquigarrow$ 750 times faster than Nagao's

A 130-bit example (2)

Decomposition on the genus 3 hyperelliptic cover $H_{|\mathbb{F}_{p^2}}$:

2. Linear algebra on the very sparse matrix of relations:
   - Structured Gaussian elimination: 1 357 sec on a single core
     $\rightsquigarrow$ reduces by a factor 3 the number of unknowns
   - Lanczos algorithm: 27 h16 min on 128 cores (MPI communications)
   - Logarithms of all remaining elements in the factor base obtained in 10 min on a single core

3. Descent phase: $\simeq$ 10 sec for one point

A 130-bit example (2)

Decomposition on the genus 3 hyperelliptic cover $H_{|\mathbb{F}_{p^2}}$:

2. Linear algebra on the very sparse matrix of relations:
   - Structured Gaussian elimination: 1 357 sec on a single core $\rightsquigarrow$ reduces by a factor 3 the number of unknowns
   - Lanczos algorithm: 27 h16 min on 128 cores (MPI communications)
   - Logarithms of all remaining elements in the factor base obtained in 10 min on a single core

3. Descent phase: $\simeq$ 10 sec for one point

- Complete resolution in 3700 CPU hours
- Linear algebra by far the slowest phase (parallelization issue: 42.5 MB of data broadcast at each round)
- No further balance possible due to relation exhaustion

Conclusion

- New index calculus algorithm to compute DL on elliptic curves defined over extension fields of composite degree
- Efficient attack on elliptic curves defined over sextic extension field $\rightarrow$ practical resolution of DLP on a 130-bit elliptic curve in 3700 CPU hours or 30 h real time with $\leq$ 200 cores
- Also available on every elliptic curves defined over a degree 4 extension field, but advantage over generic methods less significant
- How to target more curves?