Cover and Decomposition Attack on Elliptic Curves

Vanessa VITSE – Antoine Joux

Université de Versailles Saint-Quentin, Laboratoire PRISM

Journées Codes et Cryptographie 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 attacks: 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: $\mathcal{F} = \{g_1, \dots, g_N\} \subset G$
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 $v = (v_1, \dots, v_k) \in \ker({}^t M)$ such that $vA \neq 0 \mod \#G$
   - compute the solution of DLP: $x = -\left(\sum_i a_i v_i\right) / \left(\sum_i b_i v_i\right) \mod \#G$

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 $Q = [x]P$

Specific attacks on few families of curves:

1. Curves defined over prime fields
   - lift to characteristic zero fields: anomalous curves
   - transfer to $\mathbb{F}_{p^k}^*$ via pairings: curves with small embedding degree
   - otherwise only generic attacks (Pollard's Rho)

Hardness of ECDLP

ECDLP

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

Specific attacks on few families of curves:

1. Curves defined over prime fields
   - lift to characteristic zero fields: anomalous curves
   - transfer to $\mathbb{F}_{p^k}^*$ via pairings: curves with small embedding degree
   - otherwise only generic attacks (Pollard's Rho)

2. Curves defined over extension fields
   - Weil descent: transfer from $E(\mathbb{F}_{p^n})$ to $J_{\mathcal{C}}(\mathbb{F}_p)$ where $\mathcal{C}$ has genus $g \geq n$
   - direct index calculus methods on $E(\mathbb{F}_{p^n})$

Lift of the ECDLP via cover maps

$\pi : \mathcal{C} \to E$ cover map where $\mathcal{C}$ curve defined over $\mathbb{F}_q$ and E elliptic curve defined over $\mathbb{F}_{q^n}$

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

$$\begin{array}{ccc} J_{\mathcal{C}}(\mathbb{F}_{q^n}) & \xrightarrow{Tr} & J_{\mathcal{C}}(\mathbb{F}_q) \\ \uparrow \pi^* & \nearrow & \\ E(\mathbb{F}_{q^n}) \simeq J_E(\mathbb{F}_{q^n}) & & \end{array}$$

Lift of the ECDLP via cover maps

$\pi : \mathcal{C} \to E$ cover map where $\mathcal{C}$ curve defined over $\mathbb{F}_q$ and E elliptic curve defined over $\mathbb{F}_{q^n}$

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

$$\begin{array}{ccc} J_{\mathcal{C}}(\mathbb{F}_{q^n}) & \xrightarrow{Tr} & J_{\mathcal{C}}(\mathbb{F}_q) \\ \uparrow \pi^* & \nearrow & \\ E(\mathbb{F}_{q^n}) \simeq J_E(\mathbb{F}_{q^n}) & & \end{array}$$

2. use index calculus on $J_{\mathcal{C}}(\mathbb{F}_q)$: if $\mathcal{C}$ is hyperelliptic with small genus g
   - factor base: $\mathcal{F} = \{D \sim (u, v) : \deg(u) = 1\}$ (Mumford representation)
   - decomposition: $D = (u, v)$ decomposes in $\mathcal{F} \Rightarrow u$ is split over $\mathbb{F}_q$
   - complexity in $q^{2-2/g}$ as $q \to \infty$, g fixed

Lift of the ECDLP via cover maps

$\pi : \mathcal{C} \to E$ cover map where $\mathcal{C}$ curve defined over $\mathbb{F}_q$ and E elliptic curve defined over $\mathbb{F}_{q^n}$

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

$$\begin{array}{ccc} J_{\mathcal{C}}(\mathbb{F}_{q^n}) & \xrightarrow{Tr} & J_{\mathcal{C}}(\mathbb{F}_q) \\ \uparrow \pi^* & \nearrow & \\ E(\mathbb{F}_{q^n}) \simeq J_E(\mathbb{F}_{q^n}) & & \end{array}$$

2. use index calculus on $J_{\mathcal{C}}(\mathbb{F}_q)$: if $\mathcal{C}$ is hyperelliptic with small genus g
   - factor base: $\mathcal{F} = \{D \sim (u, v) : \deg(u) = 1\}$ (Mumford representation)
   - decomposition: $D = (u, v)$ decomposes in $\mathcal{F} \Rightarrow u$ is split over $\mathbb{F}_q$
   - complexity in $q^{2-2/g}$ as $q \to \infty$, g fixed

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

The GHS construction

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

Given an elliptic curve $E_{|\mathbb{F}_{q^n}}$ and a degree 2 map $E \to \mathbb{P}^1$,
construct a curve $\mathcal{C}_{|\mathbb{F}_q}$ and a cover map $\pi : \mathcal{C} \to E$.

The GHS construction

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

Given an elliptic curve $E_{|\mathbb{F}_{q^n}}$ and a degree 2 map $E \to \mathbb{P}^1$, construct a curve $\mathcal{C}_{|\mathbb{F}_q}$ and a cover map $\pi : \mathcal{C} \to E$.

Problem: 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] $\to$ increase the number of vulnerable 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 $D \sim \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O}_H))$
- complexity in $q^{2-2/ng}$ as $q \to \infty$

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 $D \sim \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O}_H))$
- complexity in $q^{2-2/ng}$ as $q \to \infty$

- 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 over $\mathbb{F}_q$ of $(n-1)ng$ equations and variables + test if $F_{\lambda_1,\ldots,\lambda_\ell}$ is split in $\mathbb{F}_q[X]$

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 over $\mathbb{F}_q$ of $(n-1)ng$ equations and variables + test if $F_{\lambda_1,\ldots,\lambda_\ell}$ is split in $\mathbb{F}_q[X]$

- complexity of the polynomial system resolution
  $\rightarrow$ relevant approach only for n and g small enough
- in the elliptic case: use Semaev's summation polynomials instead

Section 2

A new index calculus method

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

- 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.
- Can be combined with a sieving technique to avoid factorizing the resulting polynomial $F_{\lambda_1,\ldots,\lambda_\ell}$.

Still need a few Nagao's style decompositions to actually solve the DLP (descent phase).

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

Genus 3 cover

Most favorable case for this combined attack:

- extension degree $n = 6$ (occurs for OEF), and
- $E_{|\mathbb{F}_{q^6}}$ has a genus 3 cover by $H_{|\mathbb{F}_{q^2}}$
  $\rightarrow$ occurs for $\Theta(q^4)$ curves directly [Thériault, Momose-Chao]
  $\rightarrow$ for most curves after an isogeny walk

On curves defined over such extension fields:

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

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

$E: \; y^2 = (x-c)(x-\alpha)(x-\sigma(\alpha))$ defined over $\mathbb{F}_{p^6}$ where $p = 2^{22}+15$, such that $\#E = 4 \cdot 13611586746147123344665259856820622016 01$.

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

1. Relation search:
   - lex GB of a system of 10 eq. and 8 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

$E: \ y^2 = (x-c)(x-\alpha)(x-\sigma(\alpha))$ defined over $\mathbb{F}_{p^6}$ where $p = 2^{22}+15$, such that $\#E = 4 \cdot 136115867461471233446652598568206220160 1$.

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

1. Relation search:
   - lex GB of a system of 10 eq. and 8 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
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

A 130-bit example

$E: \; y^2 = (x - c)(x - \alpha)(x - \sigma(\alpha))$ defined over $\mathbb{F}_{p^6}$ where $p = 2^{22} + 15$, such that $\#E = 4 \cdot 13611586746147123344665259856820622016 01$.

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

1. Relation search:
   - lex GB of a system of 10 eq. and 8 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
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 on a single core

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 ≤ 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?