Cover and Decomposition Index Calculus on Elliptic Curves made practical

Application to a previously unreachable curve over $\mathbb{F}_{p^6}$

Vanessa VITSE – Antoine JOUX

Université de Versailles Saint-Quentin, Laboratoire PRISM

Eurocrypt 2012

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:

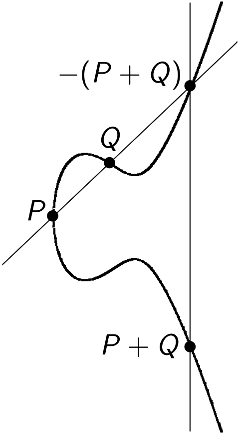
1. Generic attacks: complexity in $\Omega(\max(\alpha_i\sqrt{p_i}))$ if $\#G = \prod_i p_i^{\alpha_i}$
2. $G \subset (\mathbb{F}_q^*, \times)$: index calculus method with complexity in $L_q(1/3)$ where $L_q(\alpha) = \exp(c(\log q)^\alpha(\log\log q)^{1-\alpha})$.
3. $G \subset (\mathrm{Jac}_\mathcal{C}(\mathbb{F}_q), +)$: index calculus method better than generic attacks (if $g > 2$)

The discrete logarithm problem on elliptic curves

Use the group of points of an elliptic curve defined over a finite field

(EC)DLP: given $P, Q \in G$, find (if it exists) x st $Q = [x]P$

The group law is a good compromise between simplicity and intricacy

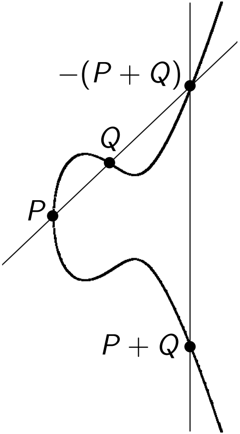


The discrete logarithm problem on elliptic curves

Use the group of points of an elliptic curve defined over a finite field

(EC)DLP: given $P, Q \in G$, find (if it exists) x st $Q = [x]P$

The group law is a good compromise between simplicity and intricacy



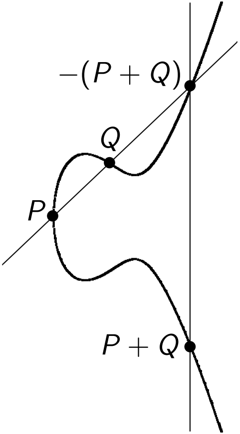
Choice of the field:

- Prime field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$: good security but modular arithmetic difficult to implement in hardware
- Extension field $\mathbb{F}_{p^n}$: interesting when $p = 2$ or p fits into a computer word

The discrete logarithm problem on elliptic curves

Use the group of points of an elliptic curve defined over a finite field

(EC)DLP: given $P, Q \in G$, find (if it exists) x st $Q = [x]P$
The group law is a good compromise between simplicity and intricacy



Choice of the field:

- Prime field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$: good security but modular arithmetic difficult to implement in hardware
- Extension field $\mathbb{F}_{p^n}$: interesting when $p = 2$ or p fits into a computer word
Potentially vulnerable to index calculus

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

Index calculus

Two difficulties :

1. **From a practical point of view :** linear algebra often the most delicate phase
   - matrices are huge (several millions of unknowns) but very sparse (only a few non-zero coeff. per row)
   - difficult to distribute dedicated algorithms

Index calculus

Two difficulties :

1. **From a practical point of view :** linear algebra often the most delicate phase
   - matrices are huge (several millions of unknowns) but very sparse (only a few non-zero coeff. per row)
   - difficult to distribute dedicated algorithms
2. **From a theoretical point of view :** how to find relations?
   - on $E(\mathbb{F}_p)$, no known method
   - on $E(\mathbb{F}_{p^n})$, two existing methods:
     - transfer to $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_p)$ via Weil descent
     - direct decompositions (Gaudry/Diem)

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

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

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

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

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

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

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

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

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

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

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

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

Principle

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

Principle

- Factor base:
  $\mathcal{F} = \{D_Q \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n}) \ : \ D_Q \sim (Q) - (\mathcal{O}_{\mathcal{H}}), Q \in \mathcal{H}(\mathbb{F}_{q^n}), x(Q) \in \mathbb{F}_q\}$
- Decomposition of an arbitrary divisor $D \in \mathrm{Jac}_{\mathcal{H}}(\mathbb{F}_{q^n})$ into ng divisors of the factor base $D \sim \sum_{i=1}^{ng} ((Q_i) - (\mathcal{O}_{\mathcal{H}}))$
- Asymptotic complexity in $q^{2-2/ng}$ as $q \to \infty$

- all curves are equally weak under this attack
- decomposition is hard: need to **solve polynomial systems**

Nagao's approach for decompositions

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

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

where f is in the Riemann-Roch space $\mathcal{L}\left(ng(\mathcal{O}_{\mathcal{H}}) - D\right)$

Decomposition of D: resolution of a quadratic polynomial system over $\mathbb{F}_q$

- $n(n-1)g$ variables
  from scalar restriction of coord. of f in projectivized Riemann-Roch space
- $(n-1)\,ng$ equations
  expressing that elementary symmetric polynomials of the $x(Q_i)$ lie in $\mathbb{F}_q$.

Analysis of Nagao's approach

- Solve a 0-dim quadratic polynomial system of $(n-1)ng$ eq./var. for each decomposition test
  $\to$ complexity at least polynomial in $d = 2^{(n-1)ng}$
  $\to$ in practice, resolution only possible for n and $g \leq 3$
  or $g = 1$ and $n \leq 5$ (using Semaev's summation polynomials)

- Proba. of decomposition is $\simeq 1/(ng)!$ and the factor base has $\simeq q$ elements
  $\to$ about $(ng)!q$ decomposition tests needed, even more for large prime variations

Relation search too slow for practical DLP resolution

Section 2

A new index calculus method

First ingredient: improved relation search for Jacobians

Using Nagao's approach to obtain enough decompositions is **too slow**

Another type of relations

Instead of decompositions, 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 $m = ng + 2$

First ingredient: improved relation search for Jacobians

Using Nagao's approach to obtain enough decompositions is **too slow**

Another type of relations

Instead of decompositions, 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 $m = ng + 2$

Similar type of relations considered in NFS, FFS and Diem's index calculus for small degree plane curves

Modified index calculus

$\mathcal{H}$ 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

Modified index calculus

$\mathcal{H}$ 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.

Modified index calculus

$\mathcal{H}$ 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.

Fast resolution

Goal: find a new set of generators of the ideal s.t. each specialization of two variables yields an easy to solve system → lex Gröbner basis

A special case: quadratic extensions in odd characteristic

Key point: define $\mathbb{F}_{q^2}$ as $\mathbb{F}_q(t)/(t^2 - \omega)$

Additional structure on the equations: polynomials obtained after restriction of scalars are multi-homogeneous of bidegree $(1, 1)$

$\rightarrow$ variables of the first homogeneous block belong to a 1-dim. variety

A special case: quadratic extensions in odd characteristic

Key point: define $\mathbb{F}_{q^2}$ as $\mathbb{F}_q(t)/(t^2-\omega)$

Additional structure on the equations: polynomials obtained after restriction of scalars are multi-homogeneous of bidegree $(1,1)$
$\rightarrow$ variables of the first homogeneous block belong to a 1-dim. variety

Decomposition method:

1. "specialization": choose a value for the first variables
2. remaining variables lie in a one-dimensional vector space $\rightsquigarrow$ easy to solve system

Further improvement possible by using a sieving technique

A special case: quadratic extensions in odd characteristic

Key point: define $\mathbb{F}_{q^2}$ as $\mathbb{F}_q(t)/(t^2 - \omega)$

Additional structure on the equations: polynomials obtained after restriction of scalars are multi-homogeneous of bidegree $(1,1)$
$\rightarrow$ variables of the first homogeneous block belong to a 1-dim. variety

Decomposition method:

1. "specialization": choose a value for the first variables
2. remaining variables lie in a one-dimensional vector space $\rightsquigarrow$ easy to solve system

Further improvement possible by using a sieving technique

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

The sieving technique

Fact: solutions of the polynomial system only give the polynomial
$F(x) = \prod_i (x - x(Q_i)) \in \mathbb{F}_q[x]$ $\quad\rightarrow$ remains to test if it is split.

The sieving technique

Fact: solutions of the polynomial system only give the polynomial $F(x) = \prod_i (x - x(Q_i)) \in \mathbb{F}_q[x]$ $\rightarrow$ remains to test if it is split.

Sieving method: avoid the factorization of F

1. Specialize first block of variables and express all remaining variables linearly in terms of one last unknown λ
   $\rightarrow$ F becomes a polynomial in $\mathbb{F}_q[x, \lambda]$ of deg. 2 in λ and $2g + 2$ in x
2. Enumeration in $x \in \mathbb{F}_q$ instead of λ
   $\rightarrow$ corresponding values of λ are easier to compute
3. Possible to recover the values of λ for which there were $\deg_x F$ associated values of x

Time-memory trade-off:

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

The sieving technique

Fact: solutions of the polynomial system only give the polynomial $F(x) = \prod_i (x - x(Q_i)) \in \mathbb{F}_q[x]$ $\rightarrow$ remains to test if it is split.

Sieving method: avoid the factorization of F

1. Specialize first block of variables and express all remaining variables linearly in terms of one last unknown λ
   $\rightarrow$ F becomes a polynomial in $\mathbb{F}_q[x, \lambda]$ of deg. 2 in λ and $2g + 2$ in x
2. Enumeration in $x \in \mathbb{F}_q$ instead of λ
   $\rightarrow$ corresponding values of λ are easier to compute
3. Possible to recover the values of λ for which there were $\deg_x F$ associated values of x

Time-memory trade-off:

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

Adapted to large prime variations by sieving only on "small primes"

Second ingredient: the 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

Second ingredient: the 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

Second ingredient: the 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

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

The sextic extension case

Extension degree $n = 6$ occurs for OEF; ideal target for this combined attack.

Most favorable case

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

Otherwise, for curves defined over such extension fields:

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

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 the hyperelliptic genus 3 cover defined over $\mathbb{F}_{p^2}$
   - 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

Scaling data for our implementation

Size of p	$\log_2 p \approx 23$	$\log_2 p \approx 24$	$\log_2 p \approx 25$
Group size	136 bits	142 bits	148 bits
Sieving (CPU.hours)	3 600	15 400	63 500
Sieving (real time)	3.5 hours	15 hours	62 hours
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

Cover and Decomposition Index Calculus on Elliptic Curves made practical

Application to a previously unreachable curve over $\mathbb{F}_{p^6}$

Vanessa VITSE – Antoine JOUX

Université de Versailles Saint-Quentin, Laboratoire PRISM

Eurocrypt 2012