The point decomposition problem in Jacobian varieties

Alexandre Wallet

ENS Lyon, Laboratoire LIP, Equipe AriC

1 Generalities
- Discrete Logarithm Problem
- Short State-of-the-Art for curves
- About Index-Calculus

2 Harvesting and Decomposition attacks

3 Degree reduction and practical computations

4 Summation Ideals

5 A geometric recreation: harvesting by sieving

Discrete Logarithm Problem (DLP)

Let $g, h = [x] \cdot g \in (G, +)$, with $x \in \mathbb{Z}$. Compute x.

Is this a hard problem ?

Classic

- Generic group: **yes**
- For some groups: **no**
- Cryptography: **“yes”**

Quantum

“NO”

Security basis for Diffie-Hellman, El-Gamal, Digital Signatures,...

Today’s groups:

Elliptic curves $E(\mathbb{F}_q)$

Jacobian of algebraic curves $\mathcal{J}_{\mathbb{F}_q}(\mathcal{C})$

Computing Discrete Logs

exp. time

DLP ON CURVES
g: genus
q: #Field

Generic alg.

Index Calculus

lower bound: $\Omega(q^{\frac{g}{2}})$

Baby-steps Giant-steps ρ-Pollard $O(q^{\frac{g}{2}})$

"Small genus"

$g \geq 2$
$\sim O(q^{2-\frac{2}{g}})$
[G'00], [D'07]
[GTTD'07]

Decomposition $q = \mathbf{q}^n$
$O(\mathbf{q}^{2-\frac{2}{ng}})$
[G'09,D'11],[N'10]
[GTTD'07]

subexp. time

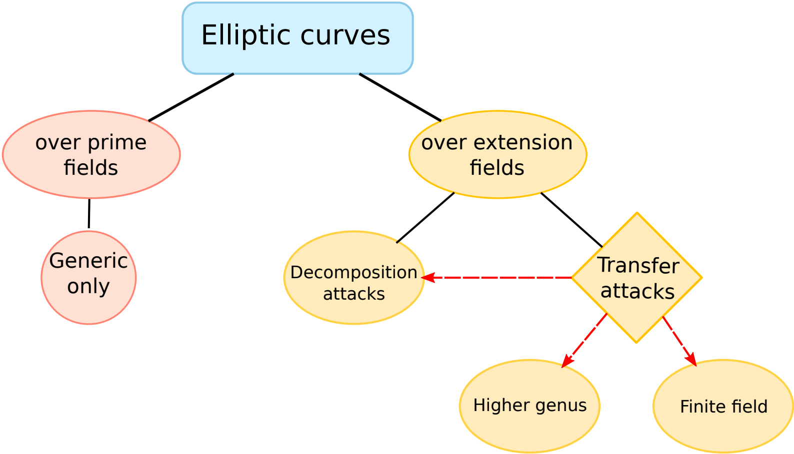
"Large genus"
$L_{q^g}(1/2)$
[ADH'99], [EGS'02]

"Large degree"
$L_{q^g}(1/3)$
[EGTT'13]

poly. time

Situation for elliptic curves

For cryptography: **mostly elliptic curves ($g = 1$)**



$\mathcal{C}$: algebraic curve $\quad G \in \mathcal{J}(\mathcal{C})$: Jacobian variety of $\mathcal{C}$

Inputs
$G,\ H = [x]G$

Harvesting

1) Select **Factor base**

$$\mathcal{F} = \{F_1, \dots, F_N\} \subset \mathcal{J}(\mathcal{C})$$

N too small: harvesting too hard — trade-off [GTTD'07] — N too big: linear algebra too long

+ easy to enumerate

+ elements should be "small"

2) Find N **relations:**

$$[a]G + [b]H = [c_{i1}]F_1 + \cdots + [c_{iN}]F_N$$

$$\left(c_{ij}\right)^T$$ sparse matrix

Several techniques

Today: $\mathcal{C}$ over $\mathbb{F}_{q^n}$

done by solving polynomial systems

(aka: Decomposition attacks)

Linear Algebra

1) Compute $v \neq 0$ s.t.

$$\left(c_{ij}\right) \left(v\right) = 0$$

2) Use v to retrieve $[x]$

Discrete Logarithm
$[x]$

Complexity

linalg $\sim O(N^2)$ well-known

harvest. $\sim N \times \underbrace{\text{Find 1 relation}}_{\text{What about this ?}}$

Today's target: harvesting in Index-Calculus for curves over $\mathbb{F}_{q^n}$.

Motivations:

Algorithmic Number Theory	Computational Algebraic Geometry	Cryptography

Compute discrete logs in abelian varieties.
How efficient can we be ?

Transfer attacks !

1 Generalities

2 Harvesting and Decomposition attacks
- What is a relation ?
- How to find a relation ?
- Complexity and Polynomial System Solving

3 Degree reduction and practical computations

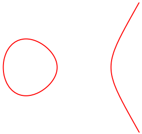
4 Summation Ideals

5 A geometric recreation: harvesting by sieving

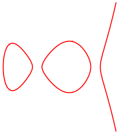
Algebraic curves, Jacobian varieties, group law

$\mathcal{C} : P(x, y) = 0$, for some $P \in \mathbb{F}_q[X, Y]$, algebraic curve of **genus** g.

$g = 1$: elliptic: $y^2 = x^3 + Ax + B, A, B \in \mathbb{F}_q$



$g = 2$: hyperelliptic: $y^2 + h_1(x)y = x^5 + \ldots$
$h_1 \in \mathbb{F}_q[x], \deg h_1 \leq 2$



$g \geq 3$: hyperelliptic: $y^2 + h_1(x)y = x^{2g+1} + \ldots$
$h_1 \in \mathbb{F}_q[x], \deg h_1 \leq g$

Non-hyperelliptic (all the rest).

Algebraic curves, Jacobian varieties, group law

$\mathcal{C} : P(x, y) = 0$, for some $P \in \mathbb{F}_q[X, Y]$, algebraic curve of **genus** g.

Fix a point $\mathcal{O}$. $\mathcal{J}(\mathcal{C})$: Jacobian variety

$\mathcal{J}(\mathcal{C})$ is a **quotient group.**

Its elements are **"reduced divisors".**

In practice, a reduced divisor is

$$D = \sum_{i=1}^{k} P_i - k\mathcal{O}.$$

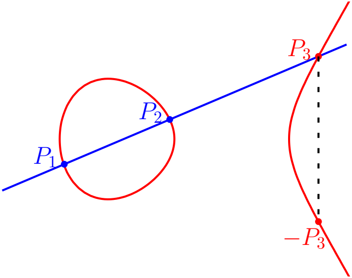
for some $P_1, \ldots, P_k \in \mathcal{C}$, $\mathbf{k} \leq \mathbf{g}$

Ex: $g = 1$, E elliptic, point at infinity $\mathcal{O}$

Line through P_1, P_2 : $f(x, y) = 0$.

In $\mathcal{J}(E)$: $P_1 + P_2 + P_3 - 3\mathcal{O} = 0$,

so that $(P_1 - \mathcal{O}) + (P_2 - \mathcal{O}) = ([-P_3] - \mathcal{O})$.



Algebraic curves, Jacobian varieties, group law

$\mathcal{C} : P(x, y) = 0$, for some $P \in \mathbb{F}_q[X, Y]$, algebraic curve of **genus** g.

Fix a point $\mathcal{O}$. $\mathcal{J}(\mathcal{C})$: Jacobian variety

$\mathcal{J}(\mathcal{C})$ is a **quotient group.**

Its elements are **"reduced divisors".**

In practice, a reduced divisor is

$$D = \sum_{i=1}^{k} P_i - k\mathcal{O}.$$

for some $P_1, \ldots, P_k \in \mathcal{C}$, $\mathbf{k} \leq \mathbf{g}$

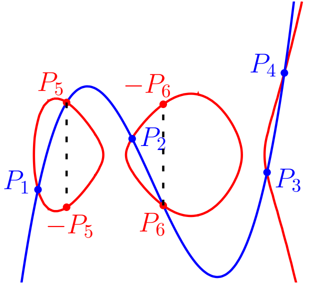
Ex: $g = 2$, $\mathcal{H}$ hyperelliptic, point at infinity $\mathcal{O}$

Cubic through $P_1, \ldots, P_4$: $f(x, y) = 0$

In $\mathcal{J}(\mathcal{H})$: $P_1 + \cdots + P_6 - 6\mathcal{O} = 0$

so that: $\underbrace{(P_1 + P_2 - 2\mathcal{O})}_{D_1} + \underbrace{(P_3 + P_4 - 2\mathcal{O})}_{D_2}$

$$= \underbrace{[-P_5] + [-P_6] - 2\mathcal{O}}_{D_3}$$



Point m-Decomposition Problem (PDP_m)

Let $\mathcal{H}$ be a curve of genus g, $R \in \mathcal{J}(\mathcal{H})$ and $\mathcal{F} \subset \mathcal{J}(\mathcal{H})$.

Find, if possible, $D_1, \ldots, D_m \in \mathcal{F}$ s.t. $R = D_1 + \cdots + D_m$.

Harvesting = solving multiple PDP_m instances, for some fixed m.

Geometry of relations

Point m-Decomposition Problem (PDP_m)

Let $\mathcal{H}$ be a curve of genus g, $R \in \mathcal{J}(\mathcal{H})$ and $\mathcal{F} \subset \mathcal{J}(\mathcal{H})$.

Find, if possible, $D_1, \ldots, D_m \in \mathcal{F}$ s.t. $R = D_1 + \cdots + D_m$.

Harvesting = solving multiple PDP_m instances, for some fixed m.

Let $R = \sum_i (x_{R_i}, y_{R_i}) - g\mathcal{O} \in \mathcal{J}(\mathcal{H})$.

$R = \sum_{i,j} (x_{D_{ij}}, y_{D_{ij}}) - mg\mathcal{O} \Leftrightarrow \exists\, f(x, y)$ s.t.:

$$f(x_{R_i}, y_{R_i}) = f(x_{D_{ij}}, y_{D_{ij}}) = 0.$$

Such f's form a **linear space of finite dim:**

$$f \in \mathrm{Span}(f_1, \ldots, f_d) \Rightarrow f = \sum_{i=1}^{d} a_i f_i$$

Goal: find $(a_i)_{i \leq d}$.

Geometry of relations

Point m-Decomposition Problem (PDP_m)

Let $\mathcal{H}$ be a curve of genus g, $R \in \mathcal{J}(\mathcal{H})$ and $\mathcal{F} \subset \mathcal{J}(\mathcal{H})$.

Find, if possible, $D_1, \ldots, D_m \in \mathcal{F}$ s.t. $R = D_1 + \cdots + D_m$.

Harvesting = solving multiple PDP_m instances, for some fixed m.

Let $R = \sum_i (x_{R_i}, y_{R_i}) - g\mathcal{O} \in \mathcal{J}(\mathcal{H})$.

$R = \sum_{i,j} (x_{D_{ij}}, y_{D_{ij}}) - mg\mathcal{O} \Leftrightarrow \exists\, f(x,y)$ s.t.:

$$f(x_{R_i}, y_{R_i}) = f(x_{D_{ij}}, y_{D_{ij}}) = 0.$$

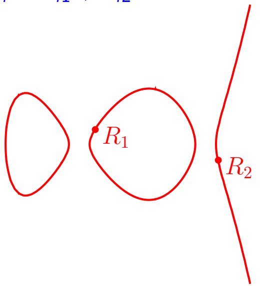
Such f's form a **linear space of finite dim:**

$$f \in \mathrm{Span}(f_1, \ldots, f_d) \Rightarrow f = \sum_{i=1}^{d} a_i f_i$$

Goal: find $(a_i)_{i \le d}$.

Ex: $g = 2$ and $m = 2$

$D_i = D_{i1} + D_{i2} - 2\mathcal{O}$.



Point m-Decomposition Problem (PDP_m)

Let $\mathcal{H}$ be a curve of genus g, $R \in \mathcal{J}(\mathcal{H})$ and $\mathcal{F} \subset \mathcal{J}(\mathcal{H})$.

Find, if possible, $D_1, \ldots, D_m \in \mathcal{F}$ s.t. $R = D_1 + \cdots + D_m$.

Harvesting = solving multiple PDP_m instances, for some fixed m.

Let $R = \sum_i (x_{R_i}, y_{R_i}) - g\mathcal{O} \in \mathcal{J}(\mathcal{H})$.

$R = \sum_{i,j} (x_{D_{ij}}, y_{D_{ij}}) - mg\mathcal{O} \Leftrightarrow \exists\, f(x,y)$ s.t.:

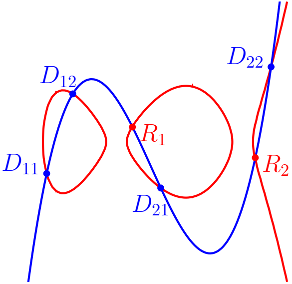
$$f(x_{R_i}, y_{R_i}) = f(x_{D_{ij}}, y_{D_{ij}}) = 0.$$

Such f's form a **linear space of finite dim:**

$$f \in \mathrm{Span}(f_1, \ldots, f_d) \Rightarrow f = \sum_{i=1}^{d} a_i f_i$$

Goal: find $(a_i)_{i \le d}$.

Ex: $g = 2$ and $m = 2$
$D_i = D_{i1} + D_{i2} - 2\mathcal{O}$.



Solving PDP$_m$ [G'09], [N'10], [D'11]

Goal: Find $(a_i)_{i \leq d}$ "in a smart way"

Assume base field is $\mathbb{F}_{q^n} = \mathrm{Span}_{\mathbb{F}_q}(1, \mathbf{t}, \ldots, \mathbf{t}^{\mathbf{n-1}})$

Solving PDP$_m$ [G'09], [N'10], [D'11]

Goal: Find $(a_i)_{i \leq d}$ "in a smart way"

Assume base field is $\mathbb{F}_{q^n} = \text{Span}_{\mathbb{F}_q}(1, \mathbf{t}, \ldots, \mathbf{t}^{\mathbf{n-1}})$

Restriction of scalars

Write $x = \sum_j x_j \mathbf{t}^j$, $x_j \in \mathbb{F}_q$, $\bar{x} = (x_1, \ldots, x_n)$:

$$(x, y) \in \mathcal{H} \Leftrightarrow (\bar{x}, \bar{y}) \in \mathcal{W}$$

where $\mathcal{W}$: Weil Restriction of $\mathcal{H}$ over $\mathbb{F}_q$

Factor base:

$$\begin{aligned} \mathcal{F} &= \{P - \mathcal{O} \ : \ P \in \mathcal{H}, x(P) \in \mathbb{F}_q\} \\ &= \mathcal{W} \cap \{x_j = 0\}_{j>0} \end{aligned}$$

Solving PDP$_m$ [G'09], [N'10], [D'11]

Goal: Find $(a_i)_{i\leq d}$ "in a smart way"

Assume base field is $\mathbb{F}_{q^n} = \text{Span}_{\mathbb{F}_q}(1, \mathbf{t}, \ldots, \mathbf{t^{n-1}})$

Restriction of scalars

Write $x = \sum_j x_j \mathbf{t}^j$, $x_j \in \mathbb{F}_q$, $\bar{x} = (x_1, \ldots, x_n)$:

$$(x, y) \in \mathcal{H} \Leftrightarrow (\bar{x}, \bar{y}) \in \mathcal{W}$$

where $\mathcal{W}$: Weil Restriction of $\mathcal{H}$ over $\mathbb{F}_q$

Decomposition Polynomial DP_R

$$DP_R(x) = \frac{\text{Res}_y(\mathcal{H}, f)}{\prod(x - x_{R_i})} = x^m + \sum_{i=0}^{m-1} N_i((a_i))x^i$$

If f describes $R = \sum_{i,j} (x_{ij}, y_{ij}) - m\mathcal{O}$:

$$DP_R(x_{ij}) = 0, \ \forall\, i \leq m, \forall\, j \leq n-1$$

Factor base:

$$\mathcal{F} = \{P - \mathcal{O} \ : \ P \in \mathcal{H}, x(P) \in \mathbb{F}_q\}$$
$$= \mathcal{W} \cap \{x_j = 0\}_{j>0}$$

Write $N_i((a_i)) = \sum_{j\geq 0} N_{ij}((\bar{a}_i))\mathbf{t}^j$:

$$D_1, \ldots, D_m \in \mathcal{F} \Rightarrow DP_R(x) \in \mathbb{F}_q[x]$$
$$\Leftrightarrow N_{ij}((\bar{a}_i)) = 0, \forall\, i, \forall\, j > 0$$

Solving PDP_m [G'09], [N'10], [D'11]

Goal: Find $(a_i)_{i \leq d}$ "in a smart way"

Assume base field is $\mathbb{F}_{q^n} = \mathrm{Span}_{\mathbb{F}_q}(1, \mathbf{t}, \ldots, \mathbf{t}^{\mathbf{n-1}})$

Restriction of scalars

Write $x = \sum_j x_j \mathbf{t}^j$, $x_j \in \mathbb{F}_q$, $\bar{x} = (x_1, \ldots, x_n)$:

$$(x, y) \in \mathcal{H} \Leftrightarrow (\bar{x}, \bar{y}) \in \mathcal{W}$$

where $\mathcal{W}$: Weil Restriction of $\mathcal{H}$ over $\mathbb{F}_q$

Factor base:

$$\mathcal{F} = \{P - \mathcal{O} \ : \ P \in \mathcal{H},\ x(P) \in \mathbb{F}_q\}$$
$$= \mathcal{W} \cap \{x_j = 0\}_{j>0}$$

Decomposition Polynomial DP_R

$$DP_R(x) = \frac{\mathrm{Res}_y(\mathcal{H}, f)}{\prod(x - x_{R_i})} = x^m + \sum_{i=0}^{m-1} N_i((a_i))x^i$$

If f describes $R = \sum_{i,j} (x_{ij}, y_{ij}) - m\mathcal{O}$:

$$DP_R(x_{ij}) = 0, \ \forall\, i \leq m, \forall\, j \leq n-1$$

Write $N_i((a_i)) = \sum_{j \geq 0} N_{ij}((\bar{a}_i))\mathbf{t}^j$:

$$D_1, \ldots, D_m \in \mathcal{F} \Rightarrow DP_R(x) \in \mathbb{F}_q[x]$$
$$\Leftrightarrow N_{ij}((\bar{a}_i)) = 0, \forall\, i, \forall\, j > 0$$

Finding relations $\sim$ solving Polynomial systems.

For $\mathbf{m} = \mathbf{ng}$, $\{N_{ij}(\bar{a}_i) = 0\}_{i \leq m, j > 0}$ is generally 0-dimensional.

Solving 0-dimensional systems with Gröbner Bases tools

Original System	$\longrightarrow$	DRL Basis F4, F5	$\longrightarrow$	Change order FGLM	$\longrightarrow$	Univariate Solving

Δ: degree of regularity

D: #solutions

n variables

s equations

$$O\left(s\binom{n+\Delta}{\Delta}^{\omega}\right)$$

$$O(nD^{\omega})$$

ω: lin. alg. exponent

Solving 0-dimensional systems with Gröbner Bases tools

Original System $\longrightarrow$ DRL Basis F4, F5 $\longrightarrow$ Change order FGLM $\longrightarrow$ Univariate Solving

Δ: degree of regularity

D: #solutions

n variables

s equations

$O(s\binom{n+\Delta}{\Delta}^{\omega})$

$O(nD^{\omega})$

In PDP$_{ng}$ setting $\mathbb{F}_{q^n}$, genus g

$\Delta = \tilde{O}(D^{1/n})$

$D = 2^{n(n-1)g}$

1 relation costs $O((ng)!D^{\omega})$

$+$ Proba that all roots of DP_R in $\mathbb{F}_q \sim 1/(ng)!$

D is the main complexity parameter.
Can we reduce it ?

Situation

Known reductions:
[FGHR'14], [FHJRV'14], [GG'14]
Uses Summation polynomials and symmetries (invariant theory)

only for $g = 1$ (elliptic curves).

Higher genus:
No reduction known before

Ex: $g = 2, n = 3, \log q = 15$
Find 1 relation $\sim$ 12 days.

Contributions[1]:

- Reduction of D for **hyperelliptic** curves of all genus, **if** $\mathbf{q = 2^n}$.
- Practical harvesting on a meaningul curve ($\#\mathcal{J}(\mathcal{H}) \sim 184$ bits prime).

[1] J-C. Faugère, A.W., *The Point Decomposition Problem in Hyperelliptic Curves*. Designs, Codes and Cryptography [In revision]

1 Generalities

2 Harvesting and Decomposition attacks

3 Degree reduction and practical computations
- Structure of DP_R
- Degree reduction
- Impact, comparisons

4 Summation Ideals

5 A geometric recreation: harvesting by sieving

Structure of DP_R in even characteristic, part 1

$\mathcal{H} : y^2 + h_1(x)y = h_0(x)$ hyperelliptic of genus g over $\mathbb{F}_{2^{kn}}$, fix $R \in \mathcal{J}(\mathcal{H})$.

$$DP_R(x) = x^m + \sum_{i=0}^{m-1} N_i(\mathbf{a})x^i \quad \& \quad \forall\, i, \deg N_i(\mathbf{a}) = 2.$$

With $\mathbb{F}_{2^{kn}} = \mathrm{Span}_{\mathbb{F}_{2^k}}(\mathbf{t}^j)_{j \leq n-1}$, $N_i(\mathbf{a}) = \sum_j N_{ij}(\bar{\mathbf{a}})\mathbf{t}^j$.

Reminder: solving PDP_{ng} = solving $\{N_{ij}(\bar{\mathbf{a}}) = 0\}_{j>0, i \leq ng}$ over $\mathbb{F}_{2^k}$.

Structure of DP_R in even characteristic, part 1

$\mathcal{H} : y^2 + h_1(x)y = h_0(x)$ hyperelliptic of genus g over $\mathbb{F}_{2^{kn}}$, fix $R \in \mathcal{J}(\mathcal{H})$.

$$DP_R(x) = x^m + \sum_{i=0}^{m-1} N_i(\mathbf{a})x^i \quad \& \quad \forall\, i, \deg N_i(\mathbf{a}) = 2.$$

With $\mathbb{F}_{2^{kn}} = \mathrm{Span}_{\mathbb{F}_{2^k}}(\mathbf{t}^j)_{j \leq n-1}$, $N_i(\mathbf{a}) = \sum_j N_{ij}(\bar{\mathbf{a}})\mathbf{t}^j$.

Reminder: solving PDP_{ng} = solving $\{N_{ij}(\bar{\mathbf{a}}) = 0\}_{j>0, i \leq ng}$ over $\mathbb{F}_{2^k}$.

$N_i(\mathbf{a})$ square $\Rightarrow$ $\forall\, j, N_{ij}(\bar{\mathbf{a}})$ squares $\Rightarrow$ **replace quadratic eqs by linear eqs**

Proposition: Number of squares

Let $h_1(x) = \sum_{i=\mathbf{t}}^{\mathbf{s}} \alpha_i x^i$, and let $\mathbf{L} = \mathbf{s} - \mathbf{t} + \mathbf{1}$ be the **length** of $h_1(x)$.
There are exactly $\mathbf{g} - \mathbf{L} - \mathbf{1}$ squares among the $N_i(\mathbf{a})$.

Consequence: $(\mathbf{n} - \mathbf{1})(\mathbf{g} - \mathbf{L} - \mathbf{1})$ replacements in $\{N_{ij}(\bar{\mathbf{a}}) = 0\}_{j>0, i \leq ng}$.
Find $\mathbf{n} - \mathbf{1}$ more if $\alpha_s \in \mathbb{F}_{2^k}$.

Structure of DP_R in even characteristic, part 2

In $\mathcal{H} : y^2 + h_1(x)y = h_0(x)$, we usually have $h_1(x)$ monic.

Proposition: N_{m-1} is univariate

Let $\mathbf{a} = (a_1, \ldots, a_d)$. Then $N_{m-1}(a_d) = {a_d}^2 + a_d + \lambda$ for some $\lambda \in \mathbb{F}_{2^{kn}}$.

Rewrite:
$$\begin{aligned} N_{m-1}(a_d) &= a_{d,0}^2 + a_{d,0} + \lambda_0 + \textstyle\sum_{\mathbf{j}\geq\mathbf{1}} a_{d,\mathbf{j}}^2 \mathbf{t}^{2j} + \sum_{\mathbf{j}\geq\mathbf{1}} (a_{d,\mathbf{j}} + \lambda_j)\mathbf{t}^j \\ &= N_{m-1,0}(\bar{a}_d) + \textstyle\sum_{\mathbf{j}\geq\mathbf{1}} N_{m-1,j}(a_{d,\mathbf{1}}, \ldots, a_{d,n-1})\mathbf{t}^j. \end{aligned}$$

Proposition: "presolving"

$\{N_{m-1,j}(a_{d,\mathbf{1}}, \ldots, a_{d,n-1})\}_{j\geq 1}$ is 0-dimensional and has a solution in $\mathbb{F}_{2^k}$ whp.

Consequence: determines $\mathbf{n-1}$ vars in the full system, removes $\mathbf{n-1}$ eqs.

Analysis of degree reduction

Base field $\mathbb{F}_{2^{kn}}$, $m = ng$. Implies $d = (n-1)g$. Let $\mathbf{L}$ be the length of h_1.

Genericity assumption:
PDP_{ng} systems behave like regular systems of dimension 0.

Before reduction:

- $\#\bar{\mathbf{a}} = n(n-1)g$
- $\#\mathrm{eqs} = n(n-1)g$
- Eqs have deg $= 2$

$\Rightarrow d_{old} = 2^{n(n-1)g}$

After reduction:

- $n-1$ determined vars
- $(n-1)(g-\mathbf{L}-1)$ linear eqs
- remaining have deg $= 2$

$\Rightarrow d_{new} = 2^{(n-1)((n-1)g+\mathbf{L}-2)}$

$$2^{(n-1)((n-1)g-1)} \quad \leq \quad d_{new} \quad \leq \quad 2^{(n-1)(ng-1)}$$

$$\textbf{factor} \qquad \mathbf{2^{(n-1)(g+1)}} \qquad \frac{d_{old}}{d_{new}} \qquad \mathbf{2^{n-1}}$$

Impact of the reduction

For $g = 2,\ n = 3,\ d_{old} = 2^{12} = 4096,\ d_{new} = 2^6 = 64.$

- Toy-example for one PDP_6 instance:

fields	tool	time for d_{old}	time for d_{new}	**ratio**
$\mathbb{F}_{2^{45}} \mid \mathbb{F}_{2^{15}}$	Magma 2.19	~ 1500s	~ 0.029s	**75000**

- $\mathcal{H}$ with $L_{h_1} = 1$, over $\mathbb{F}_{2^{93}} = \mathbb{F}_{2^{31 \cdot 3}}$ and $\#\mathcal{J}(\mathcal{H}) = 2 \times 3 \times p$, with $\log p = 184$.

#cores	tool	old	this work
8000	C (optimized[2])	$\sim$ 30 **years** unfeasible	$\sim$ **7 days** practical

- comparison with recent DL over 768 bits finite field:

	#rels	harvesting time	matrix size*	matrix density*	$\log p$	#linalg.
[KDL+'17]	$\sim 2^{33}$	6 months	2^{24}	184	768	$\sim 2^{56}$
our work	$\sim 2^{31}$	7 days	2^{28}	87	184	$\sim 2^{63}$

[2] F5 with code gen., Sparse-FGLM [FM'11], NTL lib.

Situation

Target: harvesting in Index-Calculus for hyperelliptic curves over $\mathbb{F}_{q^n}$.

Results:

- degree reduction if $q = 2^k$ for hyperelliptics
- practical, meaningful computations in genus 2

Questions:

- What about q odd ?
- What about non-hyperelliptics ?
- Reduction of $\mathcal{F}$'s size ?

Situation

Target: harvesting in Index-Calculus for hyperelliptic curves over $\mathbb{F}_{q^n}$.

Results:

- degree reduction if $q = 2^k$ for hyperelliptics
- practical, meaningful computations in genus 2

Questions:

- What about q odd ?
- What about non-hyperelliptics ?
- Reduction of $\mathcal{F}$'s size ?

- For elliptic curves, reduction achieved using **Summation polynomials**.
- Works for even and odd characteristic.
- Enables factor basis reduction $\Rightarrow$ faster linear algebra

Let's see how it is done.

1 Generalities

2 Harvesting and Decomposition attacks

3 Degree reduction and practical computations

4 Summation Ideals
- Summation polynomials ?
- Generalization, Analysis for Index Calculus
- Degree Reduction in even characteristic

5 A geometric recreation: harvesting by sieving

Summation polynomials for elliptic curves

Let E be an elliptic curve over $\mathbb{F}$ with point at infinity $\mathcal{O}$, and $m \geq 3$.

Definition

The m^{th} **summation polynomial** for E is $S_m \in \mathbb{F}[X_1, \ldots, X_m]$ generating the projection of the "group law ideal" over a set of coordinates:

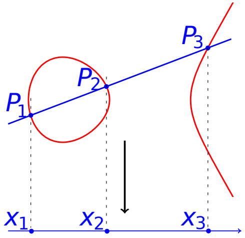
$$S_m(x_1, \ldots, x_m) = 0 \Leftrightarrow \exists\ y_1, \ldots, y_m \in \overline{\mathbb{F}} \text{ s.t. } P_i = (x_i, y_i) \in E \text{ and}$$
$$P_1 + \cdots + P_m = \mathcal{O}.$$

Projection of the group law on the x-line

$$P_1 + P_2 + P_3 = \mathcal{O}$$

algebra $\downarrow$ $\quad\uparrow$ geometry

$$S_3(x_1, x_2, x_3) = 0$$



Solving PDP$_m$ for elliptic curves, [G'09], [D'11]

Goal: Find decomposition $P_1 + \cdots + P_m$ of $R \in E(\mathbb{F}_{q^n})$

$$\underset{\text{geometry}}{R = P_1 + \cdots + P_m} \quad \Leftrightarrow \quad \underset{\text{algebra}}{S_{m+1}(x_R, x_1, \ldots, x_m) = 0}$$

New goal: Find $x_1, \ldots, x_m$ i.e. solve $S_{m+1}(x_R, X_1, \ldots, X_m)$

Solving PDP$_m$ for elliptic curves, [G'09], [D'11]

Goal: Find decomposition $P_1 + \cdots + P_m$ of $R \in E(\mathbb{F}_{q^n})$

$$\begin{array}{ccc} \text{geometry} & & \text{algebra} \\ R = P_1 + \cdots + P_m & \Leftrightarrow & S_{m+1}(x_R, x_1, \ldots, x_m) = 0 \end{array}$$

New goal: Find $x_1, \ldots, x_m$ i.e. solve $S_{m+1}(x_R, X_1, \ldots, X_m)$

Restriction of scalar:
$x_i = \sum_j x_{ij}\mathbf{t}^j$, $x_{ij} \in \mathbb{F}_q$.

Set factor base:
$\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) \ : \ x(P) \in \mathbb{F}_q\}$.

Then we can write: $S_{n+1}(x_R, X_1, \ldots, X_n) \ = \ \sum_{i=0}^{n-1} s_i(X_{1,0}, \ldots, X_{n,n-1})\mathbf{t}^\mathbf{j}$

We want $P_i \in \mathcal{F}$:

$$S_{n+1}(x_R, X_1, \ldots, X_n) = 0 \quad \Leftrightarrow \quad W = \begin{cases} s_1(X_1, \ldots, X_n) = 0 \\ \vdots \\ s_n(X_1, \ldots, X_n) = 0 \end{cases}$$

Known results

Heuristic: W is 0-dimensional. In practice: never failed.

	D	treshold for m	
As presented	$n! \cdot 2^{n(n-1)}$	$=4$	
	$\downarrow$		
S_m is symmetric	$2^{n(n-1)}$	< 6	immediate

Known results

Heuristic: W is 0-dimensional. In practice: never failed.

	D	treshold for m	
As presented	$n! \cdot 2^{n(n-1)}$	$=4$	
	$\downarrow$		
S_m is symmetric	$2^{n(n-1)}$	< 6	immediate
	$\downarrow$		
1 rational 2-torsion point	$2^{(n-1)^2}$	< 8	[FGHR'14]†, some models
	$\downarrow$		
all 2-torsion is rational	$2^{(n-1)(n-2)}$	"$= 8$"	[FHJRV'14]$^{\dagger *}$, any model

Now what about other curves ?

†: size of factor base is also reduced.

$*$: close to threaten Brainpool Curve! (over $\mathbb{F}_{31 \cdot 5}$).

Summation Variety

J-C. Faugère, A. Wallet, *The Point Decomposition Problem on Hyperelliptic curves*, DCC Journal [In revision]

$\mathcal{H}$ hyperelliptic curve over $\mathbb{F}$. $R \in \mathcal{J}(\mathcal{H})$.

Goal: Describe $\mathcal{V}_{m,R} = \{ (P_1, \dots, P_m) : \sum_{i=1}^{m} (P_i) = R \}$ *"Summation Variety"*

Summation Variety

J-C. Faugère, A. Wallet, *The Point Decomposition Problem on Hyperelliptic curves*, DCC Journal [In revision]

$\mathcal{H}$ hyperelliptic curve over $\mathbb{F}$. $R \in \mathcal{J}(\mathcal{H})$.

Goal: Describe $\mathcal{V}_{m,R} = \{\,(P_1,\ldots,P_m) : \sum_{i=1}^{m}(P_i) = R\}$ *"Summation Variety"*

Definition of Decomposition polynomial:

$$R = (P_1) + \cdots + (P_m) \Leftrightarrow \forall\, i, DP_R(x_i) = 0$$

With $e_i = Sym_i(x_1,\ldots,x_m)$:

$$DP_R(x) = x^m + \sum_{i=0}^{m-1} N_i(\mathbf{a})x^i = x^m + \sum_{i=0}^{m-1}(-1)^{m-i}e_{m-i}x^i$$

Summation Variety

J-C. Faugère, A. Wallet, *The Point Decomposition Problem on Hyperelliptic curves*, DCC Journal [In revision]

$\mathcal{H}$ hyperelliptic curve over $\mathbb{F}$. $R \in \mathcal{J}(\mathcal{H})$.

Goal: Describe $\mathcal{V}_{m,R} = \{ (P_1, \ldots, P_m) : \sum_{i=1}^{m} (P_i) = R \}$ *"Summation Variety"*

Definition of Decomposition polynomial:

$$R = (P_1) + \cdots + (P_m) \Leftrightarrow \forall\, i, DP_R(x_i) = 0$$

With $e_i = Sym_i(x_1, \ldots, x_m)$:

$$DP_R(x) = x^m + \sum_{i=0}^{m-1} N_i(\mathbf{a}) x^i = x^m + \sum_{i=0}^{m-1} (-1)^{m-i} e_{m-i} x^i$$

This gives a polynomial ideal:

$$\mathcal{I}_{m,R} = \begin{cases} N_{m-1}(\mathbf{a}) = e_1, \\ \vdots \\ N_0(\mathbf{a}) = (-1)^{m+1} e_m. \end{cases}$$

Theorem

The ideal $\mathcal{I}_{m,R} \subset \mathbb{F}[\mathbf{a}, \mathbf{e}]$ is a polynomial parametrization of ${\mathcal{V}_{m,R}}^{\mathfrak{S}_m}$.

Conditions in $\mathbf{e} = \mathrm{Sym}(x_i)$: **eliminate** $\mathbf{a}$

Geometry	Algebra
projection onto $\mathbf{e}$	Gröbner basis of $\mathcal{I}_{m,R} \cap \mathbb{F}[\mathbf{e}]$.

m^{th} Summation Ideals

For $m \geq g + 1$, the $\mathbf{m^{th}}$ **summation ideal** for $\mathcal{H}$ is $\mathcal{I}_{m,R} \cap \mathbb{F}[\mathbf{e}]$.

If $\langle \mathbb{S}_{m,R} \rangle = \mathcal{I}_{m,R} \cap \mathbb{F}[\mathbf{e}]$, then $\mathbb{S}_{m,R}$ is called **a set of m-summation polynomials**, or **a** $\mathbf{m^{th}}$ **summation set**.

Properties of Summation Ideals

$\mathbb{S}_{m,R}(\mathbf{x})$: evaluation of all $S \in \mathbb{S}_{m,R}$ at $\mathbf{x}$. $\mathcal{H}$ hyperelliptic curve over $\mathbb{F}$.

Summation property

$$\mathbb{S}_{m,R}(\mathbf{x}) = 0 \Leftrightarrow \exists\ y_1, \ldots, y_m \in \overline{\mathbb{F}} \text{ s.t. } P_i = (x_i, y_i) \in \mathcal{H} \text{ and } (P_1) + \cdots + (P_m) = R.$$

Invariance by permutations

$\langle \mathbb{S}_{m,R} \rangle^{\mathfrak{S}_m} = \langle \mathbb{S}_{m,R} \rangle$, and the modelling computes a symmetrized summation set.

Let $\mathbf{V} = V(\mathcal{I}_{m,R} \cap \mathbb{F}[\mathbf{e}])$:

$\operatorname{Codim} \mathbf{V} = g \quad \Rightarrow \quad \#\mathbb{S}_{m,R} \geq g$

in practice, $\#\mathbb{S}_{m,R} \gg g$

Heuristic: $\deg \mathbf{V} = 2^{m-g}$

[D'11]: proven for $g = 1$

New PDP$_m$ solving for hyperelliptic curve

Let $\mathcal{H}$ defined over $\mathbb{F}_{q^n} = \mathrm{Span}_{\mathbb{F}_q}(1, \mathbf{t}, \ldots, \mathbf{t}^{n-1})$, fix $R \in \mathcal{J}(\mathcal{H})$

0) **Factor base:** $\mathcal{F} = \{(P) \in \mathcal{J}(\mathcal{H}) : x(P) \in \mathbb{F}_q\}$.

1) Compute ng^{th} Summation Set $\mathbb{S}_{ng,R} = \{S_1, \ldots, S_r\}$.

2) Restriction of scalars $\mathbb{F}_{q^n} \to \mathbb{F}_q$ on each $S_i = \sum_j s_{ij}(e_1, \ldots, e_{ng})\mathbf{t}^j$

3) Solve the system $W = \begin{cases} s_{11}(e_1, \ldots, e_{ng}) = 0 \\ \vdots \\ s_{rn}(e_1, \ldots, e_{ng}) = 0 \end{cases}$

New PDP$_m$ solving for hyperelliptic curve

Let $\mathcal{H}$ defined over $\mathbb{F}_{q^n} = \text{Span}_{\mathbb{F}_q}(1, \mathbf{t}, \ldots, \mathbf{t}^{n-1})$, fix $R \in \mathcal{J}(\mathcal{H})$

0) **Factor base:** $\mathcal{F} = \{(P) \in \mathcal{J}(\mathcal{H}) : x(P) \in \mathbb{F}_q\}$.

1) Compute ng^{th} Summation Set $\mathbb{S}_{ng,R} = \{S_1, \ldots, S_r\}$.

2) Restriction of scalars $\mathbb{F}_{q^n} \to \mathbb{F}_q$ on each $S_i = \sum_j s_{ij}(e_1, \ldots, e_{ng})\mathbf{t}^j$

3) Solve the system $W = \begin{cases} s_{11}(e_1, \ldots, e_{ng}) = 0 \\ \vdots \\ s_{rn}(e_1, \ldots, e_{ng}) = 0 \end{cases}$

$r \geq g = \text{Codim}\mathbf{V}$

$\deg \mathbf{V} = 2^{(n-1)g}$ $\quad\Rightarrow\quad$ $\deg W = (\deg \mathbf{V})^n = \mathbf{2^{n(n-1)g}}$

$W \subset \mathcal{W}_n(\mathbf{V})$

Same degree as Nagao's approach

Structure of DP_R in even characteristic, the return

$\mathcal{H} : y^2 + h_1(x)y = h_0(x)$ hyperelliptic of genus g over $\mathbb{F}_{2^{kn}}$, $R \in \mathcal{J}(\mathcal{H})$.

$$DP_R(x) = x^m + \sum_{i=0}^{m-1} N_i(\mathbf{a})x^i = x^m + \sum_{i=0}^{m-1} (-1)^{m-i} e_{m-i} x^i$$

Recall: there are squares among the $N_i(\mathbf{a})$!

In Nagao's approach:
$N_i(\mathbf{a})$ square $\Rightarrow \sqrt{N_{ij}(\bar{\mathbf{a}})} = 0$
Replaced by linear equations

First part of the talk

In Summation approach:
Induces **weight system** on the e_i's.
"Weighted degree is smaller."

What does this mean ?

Square equations and weighted structure

Let $\tilde{N}_i$ be the squares among the $N_i(\mathbf{a})$'s.

$$\mathcal{I}_{m,R}: \begin{cases} \tilde{N}_i^2(\mathbf{a}) = e_i \\ N_i(\mathbf{a}) = e_i \end{cases} \qquad \mathcal{J}_{m,R}: \begin{cases} \tilde{N}_i(\mathbf{a}) = e_i \\ N_i(\mathbf{a}) = e_i \end{cases}$$

$$\mathcal{I}_e = \mathcal{I}_{m,R} \cap \mathbb{F}[\mathbf{e}] \qquad \mathcal{J}_e = \mathcal{J}_{m,R} \cap \mathbb{F}[\mathbf{e}]$$

Square equations and weighted structure

Let $\tilde{N}_i$ be the squares among the $N_i(\mathbf{a})$'s.

$$\mathcal{I}_{m,R}: \begin{cases} \tilde{N}_i^2(\mathbf{a}) = e_i \\ N_i(\mathbf{a}) = e_i \end{cases} \qquad\qquad \mathcal{J}_{m,R}: \begin{cases} \tilde{N}_i(\mathbf{a}) = e_i \\ N_i(\mathbf{a}) = e_i \end{cases}$$

$$\mathcal{I}_e = \mathcal{I}_{m,R} \cap \mathbb{F}[\mathbf{e}] \quad \xleftarrow[w_i=2,\, w_i=1]{\varphi(e_i)=e_i^{w_i}} \quad \boxed{\mathcal{J}_e = \mathcal{J}_{m,R} \cap \mathbb{F}[\mathbf{e}]}$$

Theorem

With $\varphi(e_i) = e_i^{w_i}$, $\mathcal{I}_e$ is the radical of $\varphi(\mathcal{J}_e)$.

Applications: Find points in $V(\mathcal{J}_e)$ instead of $V(\mathcal{I}_e)$.
"Weighted degree of $\mathcal{J}_e$ is smaller than $\deg \mathcal{I}_e$"

Degree reduction in summation approach over $\mathbb{F}_{2^{kn}}$

Proposition: With $\varphi(e_i) = e_i^{w_i}$, $\deg_{\mathbf{w}} \mathcal{J}_e = \dfrac{\deg \varphi(\mathcal{J}_e)}{\prod_{i=1}^{n} w_i}$.

Let $\mathbf{V}_J = V(\mathcal{J}_e)$, $\mathbf{V}_I = V(\mathcal{I}_e)$.

Corollary

There is a constant C depending on h_1 s.t. $\deg_{\mathbf{w}}(\mathbf{V}_J) = C \cdot \dfrac{\deg \mathbf{V}_I}{2^{m-g+L-1}}$.

Degree reduction in summation approach over $\mathbb{F}_{2^{kn}}$

Proposition: With $\varphi(e_i) = e_i^{w_i}$, $\deg_{\mathbf{w}} \mathcal{J}_e = \dfrac{\deg \varphi(\mathcal{J}_e)}{\prod_{i=1}^{n} w_i}$.

Let $\mathbf{V}_J = V(\mathcal{J}_e)$, $\mathbf{V}_I = V(\mathcal{I}_e)$.

Corollary

There is a constant C depending on h_1 s.t. $\deg_{\mathbf{w}}(\mathbf{V}_J) = C \cdot \dfrac{\deg \mathbf{V}_I}{2^{m-g+L-1}}$.

Let $W = \mathcal{W}_n(\mathbf{V}_J) \cap \bigcap_{i,j\geq 1} V(e_{ij})$. Experimentally, $C = 2^{L-1}$.

Corollary: In PDP_{ng} instances $(m = ng)$, with L =length of h_1:

$$\deg W = C^n \cdot \frac{d_{old}}{2^{(n-1)(g-L+1)+n(L-1)}} = \frac{d_{old}}{2^{(n-1)(g-L+1)}}.$$

Comparison of approaches after reduction

With additional reductions, same reduction as in the first part of the talk.

	Best reduction	Implementation	Best running time†
Nagao	immediate when $\mathbf{L} = 0$	Easy	≈ 0.029s.
Summation	needs $\mathbf{L} = 0$ and additional work	Tricky	≈ 0.34s.

In practice: better use approach of the first part.

†: on toy examples ($\sim \mathbb{F}_{2^{45}}$)

Perspectives

Limits: if $g \geq 2$, **can't reduce degree in odd char.**

Why?
- Degree of equations too small to exploit **Frobeniuses**
- Summation Variety not invariant under **Jacobian** 2-**torsion**

$\swarrow \qquad \searrow$

"Summation" framework for Abelian varieties

Generalization with **Kummer varieties**

Arithmetic in $g = 2$ well-understood **(theta functions)**

Explicit "Jacobian" summation polynomials

$\searrow \qquad \swarrow$

Exploitation of more symmetries for decomposition attacks

ex: set of 2-torsion points is larger in $g = 2$, action expresses linearly
Factor base invariant under 2-torsion can be built.

1 Generalities

2 Harvesting and Decomposition attacks

3 Degree reduction and practical computations

4 Summation Ideals

5 A geometric recreation: harvesting by sieving
- Old-school smooth harvesting
- New approach: harvesting by sieving
- Timings

$\mathcal{C} : C(x, y) = 0$ **non-hyperelliptic** of genus $g \geq 3$. ([D'08] $\deg C \leq g + 1$)

Factor base $\mathcal{F} = \{ P \in \mathcal{C}(\mathbb{F}_q) \}$ (rational points).

To find one relation:

Non-hyperelliptic case [D'08]

1. Select $P_1, P_2 \in \mathcal{F}$.
2. Compute $F \in \mathbb{F}_q[x]$ describing
   $\mathcal{C} \cap$ the line $(P_1 P_2)$, with P_1, P_2 removed.
3. If F splits over $\mathbb{F}_q$ ("div$(P_1 P_2)$ is smooth")
   Then relation.
   Else Try new P_1, P_2.

   $\deg F = g - 1$ so probability : $\dfrac{1}{(g-1)!}$

Old-school harvesting for smooth divisors

non-hyperelliptic case

$\mathcal{C} : C(x, y) = 0$ **non-hyperelliptic** of genus $g \geq 3$. ([D'08] $\deg C \leq g + 1$)

Factor base $\mathcal{F} = \{ P \in \mathcal{C}(\mathbb{F}_q) \}$ (rational points).

To find one relation:

Non-hyperelliptic case [D'08]

1. Select $P_1, P_2 \in \mathcal{F}$.
2. Compute $F \in \mathbb{F}_q[x]$ describing $\mathcal{C} \cap$ the line $(P_1 P_2)$, with P_1, P_2 removed.
3. If F splits over $\mathbb{F}_q$ ("$\mathrm{div}(P_1 P_2)$ is smooth")
   Then relation.
   Else Try new P_1, P_2.

   $\deg F = g - 1$ **so probability :** $\dfrac{\mathbf{1}}{(\mathbf{g-1})!}$

1. "Free"
2. Cheap
3. Costs $\approx g^2 \log q$

95% **of time: checking if smooth or not**

and duplicate relations

$\#\mathcal{F} \approx q \times (g-1)!$ tries for a relation $\Rightarrow$ harvesting in $\approx (g-1)!q(g^2 \log q)$

New approach: Harvesting by Sieving

V.Vitse, A.Wallet, *Improved Sieving on Algebraic curves*, LatinCrypt 2015

Sieving = time-memory trade-off.

Theory: Add **one degree of freedom** in decompositions.

Practice: **Store results of cheap computations.** ~~Smoothness checks~~

Existing:
[SS'14]: hyperelliptic only

$\longrightarrow$

Cons:
sort, backtracking, hyperelliptic only

Our contribution:

- Adapt sieve to **all curve types**
- Suitable for other Index-calculus variants
- Compared to [SS'14]: skip computations, better memory efficiency, no sorting.

$\mathcal{C} : C(x, y) = 0$ **non-hyperelliptic** of genus $g \geq 3$. ([D'08] $\deg C \leq g + 1$)

Factor base $\mathcal{F} = \{P, P_1, P_2, \ldots\}$. **First round of sieving:** fix $P = (x_P, y_P)$.

$$\text{Slope of a line through } P\text{: } \lambda_P(P_i) = \frac{y_i - y_P}{x_i - x_P} \text{ (cheap!)}$$

Loop over $\mathcal{F}$, compute $\lambda_P(P_i)$'s:

$$\begin{array}{cccccc} & \lambda_P(P_1) & \lambda_P(P_2) & \lambda_P(P_3) & \ldots & \\ T = [& 0 & 0 & 0 & \ldots &] \end{array}$$

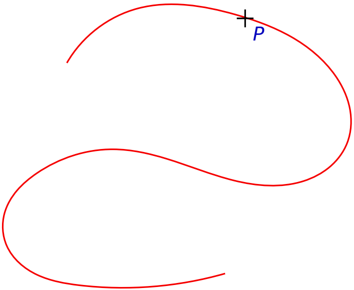


Illustration for non-hyperelliptic curves

$\mathcal{C} : C(x, y) = 0$ **non-hyperelliptic** of genus $g \geq 3$. ([D'08] $\deg C \leq g + 1$)

Factor base $\mathcal{F} = \{P, P_1, P_2, \dots\}$. **First round of sieving:** fix $P = (x_P, y_P)$.

$$\text{Slope of a line through } P\text{: } \lambda_P(P_i) = \frac{y_i - y_P}{x_i - x_P} \text{ (cheap!)}$$

Loop over $\mathcal{F}$, compute $\lambda_P(P_i)$'s:

$$\begin{array}{cccccc} & \lambda_P(P_1) & \lambda_P(P_2) & \lambda_P(P_3) & \dots & \\ T = [& 1 & 0 & 0 & \dots &] \end{array}$$

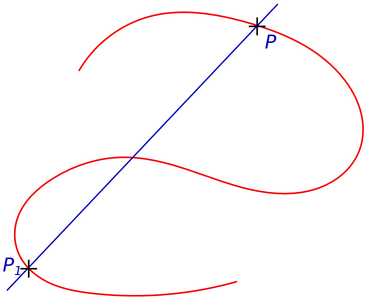


Illustration for non-hyperelliptic curves

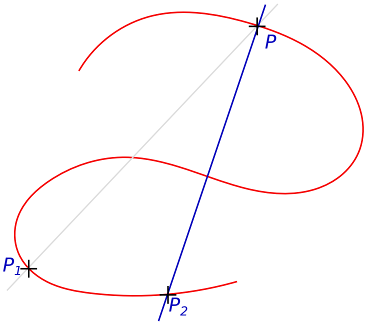
$\mathcal{C} : C(x,y) = 0$ **non-hyperelliptic** of genus $g \geq 3$. ([D'08] $\deg C \leq g+1$)

Factor base $\mathcal{F} = \{P, P_1, P_2, \dots\}$. **First round of sieving:** fix $P = (x_P, y_P)$.

$$\text{Slope of a line through } P\text{: } \lambda_P(P_i) = \frac{y_i - y_P}{x_i - x_P} \text{ (cheap!)}$$

Loop over $\mathcal{F}$, compute $\lambda_P(P_i)$'s:

$$\begin{array}{cccccc} & \lambda_P(P_1) & \lambda_P(P_2) & \lambda_P(P_3) & \dots & \\ T = [& 1 & 1 & 0 & \dots &] \end{array}$$



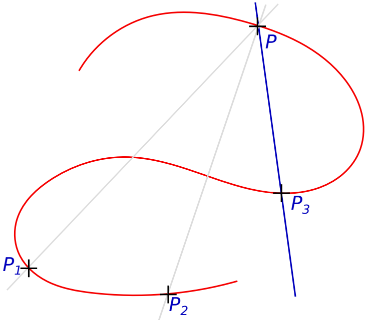
$\mathcal{C} : C(x, y) = 0$ **non-hyperelliptic** of genus $g \geq 3$. ([D'08] $\deg C \leq g + 1$)

Factor base $\mathcal{F} = \{P, P_1, P_2, \dots\}$. **First round of sieving:** fix $P = (x_P, y_P)$.

Slope of a line through P: $\lambda_P(P_i) = \dfrac{y_i - y_P}{x_i - x_P}$ (cheap!)

Loop over $\mathcal{F}$, compute $\lambda_P(P_i)$'s:

$$\begin{array}{cccccc} & \lambda_P(P_1) & \lambda_P(P_2) & \lambda_P(P_3) & \dots \\ T = & [\ 1 & 1 & 1 & \dots\ ] \end{array}$$



$\mathcal{C} : C(x, y) = 0$ **non-hyperelliptic** of genus $g \geq 3$. ([D'08] $\deg C \leq g + 1$)

Factor base $\mathcal{F} = \{P, P_1, P_2, \ldots\}$. **First round of sieving:** fix $P = (x_P, y_P)$.

Slope of a line through P: $\lambda_P(P_i) = \dfrac{y_i - y_P}{x_i - x_P}$ (cheap!)

Loop over $\mathcal{F}$, compute $\lambda_P(P_i)$'s:

$$\begin{array}{cccccc} & \lambda_P(P_1) & \lambda_P(P_2) & \lambda_P(P_3) & \ldots & \\ T = [& \mathbf{2} & 1 & 1 & \ldots &] \end{array}$$

$\lambda_P(P_i) = \lambda_P(P_j) \Leftrightarrow P, P_i, P_j$ lined up.

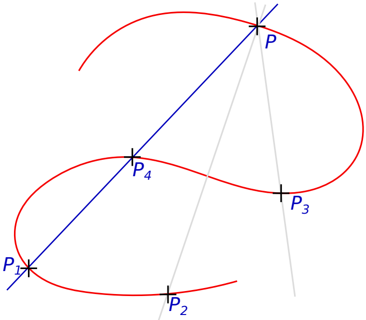


Illustration for non-hyperelliptic curves

$\mathcal{C} : C(x,y) = 0$ **non-hyperelliptic** of genus $g \geq 3$. ([D'08] deg $C \leq g+1$)

Factor base $\mathcal{F} = \{P, P_1, P_2, \dots\}$. **First round of sieving:** fix $P = (x_P, y_P)$.

$$\text{Slope of a line through } P\text{: } \lambda_P(P_i) = \frac{y_i - y_P}{x_i - x_P} \text{ (cheap!)}$$

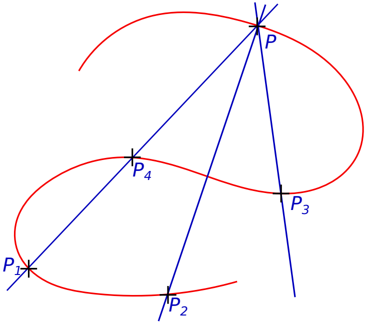
Loop over $\mathcal{F}$, compute $\lambda_P(P_i)$'s:

$$\begin{array}{cccccc} & \lambda_P(P_1) & \lambda_P(P_2) & \lambda_P(P_3) & \dots & \\ T = [& \mathbf{2} & 1 & 1 & \dots &] \end{array}$$

$\lambda_P(P_i) = \lambda_P(P_j) \Leftrightarrow P, P_i, P_j$ lined up.

When $\mathbf{T}[\lambda_\mathbf{i}] = \mathbf{g} \Rightarrow$ **Relation !**

Next round: remove P from $\mathcal{F}$, start again with P_1.



Analysis in the non-hyperelliptic case

For one loop:

- $\mathbf{O}(\mathbf{q})$ multiplications + $\mathbf{O}(\mathbf{q})$ storage.
- Expect $\approx \frac{\mathbf{q}}{\mathbf{g}!}$ relations.

$\Rightarrow$ Harvesting in $\approx \mathbf{g}!\mathbf{q}$.

Overall:
Old-school: $\approx (g-1)!q(g^2 \log q)$ $\Rightarrow$ Speed-up $\approx g \log q$.

Relations management:

Loop on P uses all lines through P: **no duplicate relations.**

Timings

q		78137	177167	823547	1594331
Genus 3, degree 4	Diem	11.5	27.5	135.1	266.1
	Sieving	3.6	9.3	46.9	94.6
	Ratio	**3.1**	**2.9**	**2.8**	**2.8**
Genus 4, degree 5	Diem	51.8	122.4	595.8	1174
	Sieving	15.5	40.1	195.1	387.6
	Ratio	**3.3**	**3.1**	**3.1**	**3**
Genus 5, degree 6	Diem	229.4	535.8	2581	5062
	Sieving	75.6	199	969.3	1909
	Ratio	**3**	**2.6**	**2.6**	**2.6**
Genus 7, degree 7	Diem	1382	3173	14990	29280
	Sieving	458.5	1199	5859	11510
	Ratio	**3**	**2.6**	**2.5**	**2.5**

Implementation in Magma; CPU Intel© Core i5@2.00Ghz processor.
Time to collect 10000 relations, expressed in seconds.

Timings

[Diem-Kochinke]:
> fix a **singular point** to start the sieving
$\Rightarrow$ degree of polynomial $\searrow$ by multiplicity
> no more singular points? **"jump to another model"**

	q	78137	177167	823547	1594331
Genus 5, degree 6	Diem & Kochinke	1.58	1.60	1.69	1.76
	Sieving	0.43	0.45	0.52	0.61
	Ratio	**3.67**	**3.60**	**3.23**	**2.90**
Genus 7, degree 7	Diem & Kochinke	8.59	8.68	8.97	9.20
	Sieving	1.21	1.25	1.56	1.93
	Ratio	**7.13**	**6.96**	**5.74**	**4.77**

Implementation in Magma; CPU Intel© Core i5@2.00Ghz processor.
Time to collect 10000 relations, expressed in seconds.