The point decomposition problem in Jacobian varieties

Jean-Charles Faugère[2], **Alexandre Wallet**[1,2]

[1]ENS Lyon, Laboratoire LIP, Equipe AriC

[2]UPMC Univ Paris 96, CNRS, INRIA, LIP6, Equipe PolSys

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. Conclusion

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]

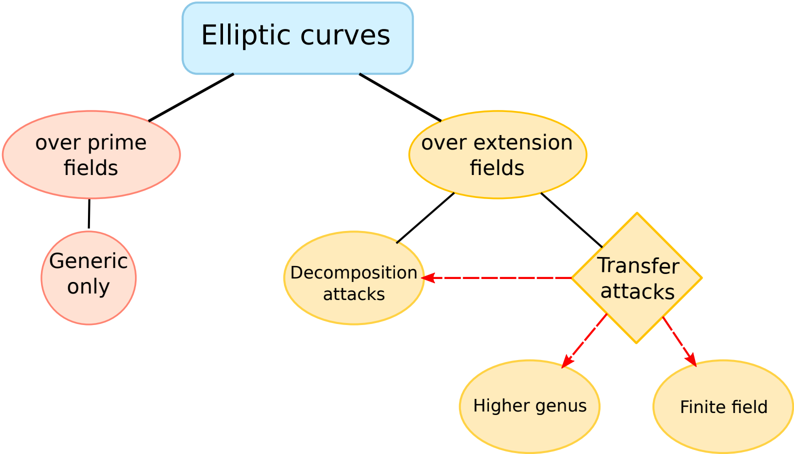
"Large degree"

$L_{q^g}(1/3)$

[EGTT'13]

poly. time

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:**

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

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

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. $\sim N$ x $\underbrace{\text{Find 1 relation}}$

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

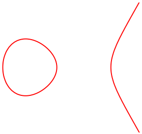
Compute discrete logs in abelian varieties.
How efficient can we be ?

Transfer attacks !

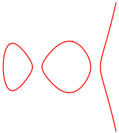
Algebraic curves, Jacobian varieties, group law

$\mathcal{C} : P(x, y) = 0$, 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

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

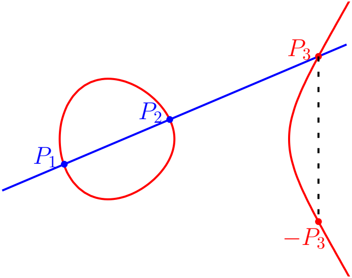
for some $P_1, \ldots, P_k \in \mathcal{C}$, $\mathbf{k} \leq \mathbf{g}$

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

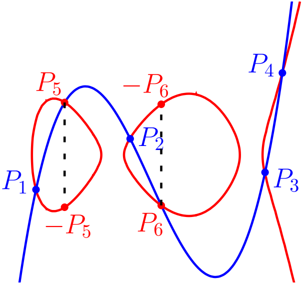
Ex: $g = 2$, $\mathcal{H}$ hyperelliptic, point at infinity $\mathcal{O}$

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

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



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.

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

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.:

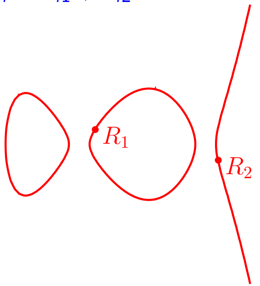
$$f(x_{R_i}, y_{R_i}) = f(x_{D_{ij}}, y_{D_{ij}}) = 0.$$

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



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, $D_1, \dots, D_m \in \mathcal{F}$ 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.:

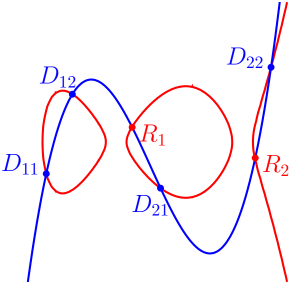
$$f(x_{R_i}, y_{R_i}) = f(x_{D_{ij}}, y_{D_{ij}}) = 0.$$

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

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

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

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

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

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

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:

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

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

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

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

Restriction of scalars

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

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

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

Decomposition Polynomial DP_R

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

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

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

Factor base:

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

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

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

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

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

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

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

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

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

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

Factor base:

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

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

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

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

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

$O(nD^{\omega})$

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]

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

Reminder: solving PDP_{ng} = solving $\{N_{ij}(\bar{\mathbf{a}}) = 0\}_{j>0, i \le ng}$ 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 $\{N_{ij}(\bar{\mathbf{a}}) = 0\}_{j>0, i \le ng}$.
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:
$$\begin{aligned} N_{m-1}(a_d) &= a_{d,0}^2 + a_{d,0} + \lambda_0 + \textstyle\sum_{\mathbf{j}\geq \mathbf{1}} a_{d,\mathbf{j}}^2 \mathbf{t}^{2j} + \textstyle\sum_{\mathbf{j}\geq \mathbf{1}} (a_{d,\mathbf{j}} + \lambda_j)\mathbf{t}^j \\ &= N_{m-1,0}(\bar{a_d}) + \textstyle\sum_{\mathbf{j}\geq \mathbf{1}} N_{m-1,j}(a_{d,\mathbf{1}}, \ldots, a_{d,n-1})\mathbf{t}^j. \end{aligned}$$

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:

- $\#\bar{\mathbf{a}} = n(n-1)g$
- $\#\text{eqs} = n(n-1)g$
- 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 $= 2$

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

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

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

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.

Conclusion

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 ?

Merci !