# Le problème de décompositions de points dans les variétés Jacobiennes

Alexandre Wallet

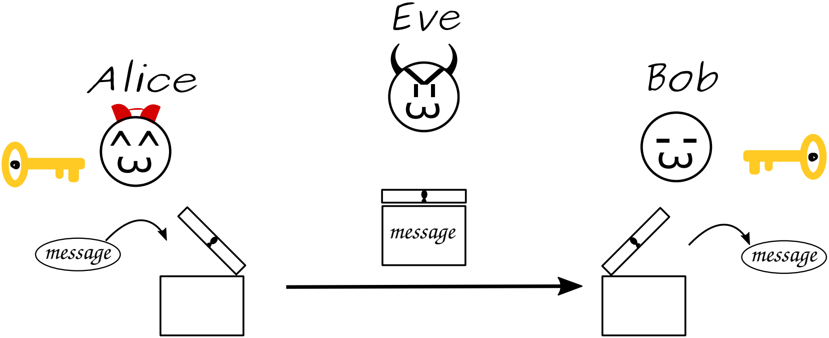
PhD Director: Jean-Charles Faugère
PhD Advisor: Vanessa Vitse

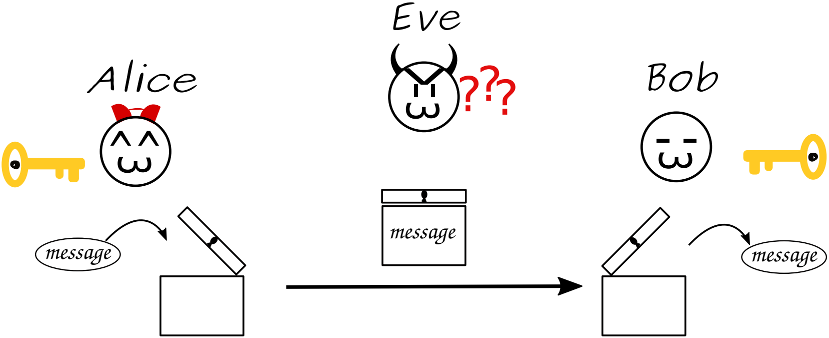
LIP6, Département CALSCI, équipe PolSys
4 Place Jussieu, UPMC

1. Context and background
    - Cryptography and Discrete Logarithms
    - Short(est) tour of Jacobian varieties
    - About Index-Calculus
2. Contribution : improving smooth relations harvesting
3. Decomposition attacks on curves: state of the art
4. Contribution: summation Ideals
5. Contribution: degree reduction in even characteristic
6. Conclusion & perspectives

# Basic cryptography

# Basic cryptography






**Question:** How can Alice and Bob share this common key ?

**Solution:** Use the Discrete Logarithm Problem !

# What is the Discrete Logarithm Problem

## Discrete Logarithm Problem (DLP)

$(G, +)$ abelian group. Given $g, h \in G$, find (if it exists) $x \in \mathbb{Z}$ s.t.:

$$[x] \cdot g = h.$$

**Is this a hard problem ?**

## Diffie-Hellman Key Exchange

$$\begin{array}{ccc}
\textit{Alice} & & \textit{Bob} \\
[a]g = A & & B = [b]g \\
& \xrightarrow{\quad A \quad} & \\
& \xleftarrow[\quad B \quad]{} & \\
key = [a]B & & key = [b]A \\
= [ab]g & & = [ab]g
\end{array}$$

## Groups used:

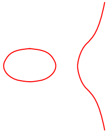
- $\mathbb{F}_q^\times$
- elliptic curves $E(\mathbb{F}_q)$
- **Jacobian of algebraic curves** $\mathcal{J}_{\mathbb{F}_q}(\mathcal{C})$

Several other protocols: El-Gamal, DSA/ECDSA, Pairings...

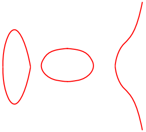
# Algebraic curves and Jacobian varieties

$\mathcal{C} : C(x,y) = 0$, for some polynomial $C$, algebraic curve of **genus** $g$.

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

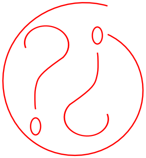


$g = 2$: hyperelliptic: $y^2 + h_1(x)y = x^5 + \dots$
$h_1 \in \mathbb{F}_q[x], \deg h_1 \leq 2$



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

Non-hyperelliptic (all the rest).



# Algebraic curves and Jacobian varieties

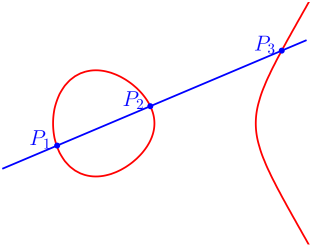
$\mathcal{C} : C(x, y) = 0$, for some polynomial $C$, algebraic curve of **genus** $g$.

- **Divisors:** formal sum $D = \sum n_i P_i,\ n_i \in \mathbb{Z}, P_i \in \mathcal{C}$
- **Degree:** $\deg D = \sum n_i$
- $\mathrm{Div}^0 = \{D \text{ s.t.} \deg D = 0\}$

- **Function on $\mathcal{C}$:** rational fraction $f(x, y)$
- **Principal divisor div $f$:** zeros $(n_i > 0)$ + poles $(n_i < 0)$
- $\{\text{ Principal divisors }\} = \mathrm{Prin}(\mathcal{C}) \leqslant \mathrm{Div}^0$

Example for $g = 1$ and line $f(x, y) = 0$:

$$P_1 + P_2 + P_3 - 3P_\infty = \text{div } f$$



# Algebraic curves and Jacobian varieties

$\mathcal{C} : C(x, y) = 0$, for some polynomial $C$, algebraic curve of **genus** $g$.

- Divisors: formal sum $D = \sum n_i P_i,\ \ n_i \in \mathbb{Z}, P_i \in \mathcal{C}$
- Degree: $\deg D = \sum n_i$
- $\mathrm{Div}^0 = \{D \text{ s.t.} \deg D = 0\}$

- Function on $\mathcal{C}$: rational fraction $f(x, y)$
- Principal divisor $\mathrm{div}\, f$: zeros $(n_i > 0)$ + poles $(n_i < 0)$
- $\{\,\text{Principal divisors}\,\} = \mathrm{Prin}(\mathcal{C}) \leqslant \mathrm{Div}^0$

**Jacobian Variety**

**as Class group:**

$$\mathbf{Jac}(\mathcal{C}) = \mathbf{Div}^0(\mathcal{C}) \,/\, \mathbf{Prin}(\mathcal{C})$$

**as Algebraic Variety:**

$$\mathbf{Jac}(\mathcal{C}) = \mathcal{C}^g / \mathcal{S}_g$$

Group law expressed by rational functions

# Jacobian elements and group law

$\mathcal{C} : C(x, y) = 0$ algebraic curve of genus $g$, $D \in \mathrm{Div}^0(\mathcal{C})$, $\mathcal{O} \in \mathcal{C}$.

From Riemann-Roch theorem: $\exists\ P_1, \dots, P_k \in \mathcal{C}$ , $\mathbf{k} \leq \mathbf{g}$ s.t.:

$$D \sim \sum_{i=1}^{k} (P_i), \text{ where } (P_i) = P_i - \mathcal{O}.$$

$\mathcal{C} : C(x, y) = 0$ algebraic curve of genus $g$, $D \in \mathrm{Div}^0(\mathcal{C})$, $\mathcal{O} \in \mathcal{C}$.

From Riemann-Roch theorem: $\exists\ P_1, \ldots, P_k \in \mathcal{C}$ , $\mathbf{k} \leq \mathbf{g}$ s.t.:

$$D \sim \sum_{i=1}^{k} (P_i), \text{ where } (P_i) = P_i - \mathcal{O}.$$

Example with $g = 1$ - elliptic curve $E : y^2 = x^3 + ax + b$

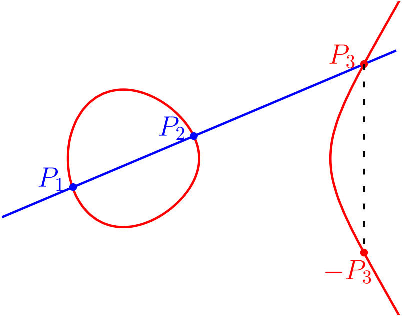
Line through $P_1, P_2 : f(x, y) = 0$.

$\Rightarrow$ div $f = (P_1) + (P_2) + (P_3)$.

$\Rightarrow$ in $\mathcal{J}(E)$ : $(P_1) + (P_2) + (P_3) = \mathcal{O}$.

Define:

$$(P_1) + (P_2) := -(P_3).$$



# Jacobian elements and group law

$\mathcal{C} : C(x,y) = 0$ algebraic curve of genus $g$, $D \in \mathrm{Div}^0(\mathcal{C})$, $\mathcal{O} \in \mathcal{C}$.

From Riemann-Roch theorem: $\exists\ P_1, \ldots, P_k \in \mathcal{C}$ , $\mathbf{k} \leq \mathbf{g}$ s.t.:

$$D \sim \sum_{i=1}^{k} (P_i), \text{ where } (P_i) = P_i - \mathcal{O}.$$

Example with $g = 2$ - hyperelliptic curve $\mathcal{H} : y^2 = x^5 + ax^3 + bx^2 + cx + d$

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

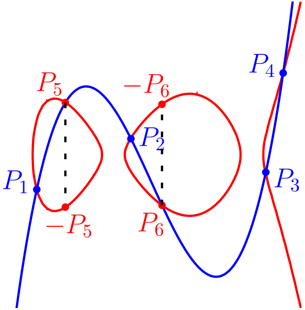
$\Rightarrow \operatorname{div} f = (P_1) + \cdots + (P_4) + (P_5) + (P_6)$

$\Rightarrow$ in $\mathcal{J}(\mathcal{H}) : (P_1) + \cdots + (P_6) = \mathcal{O}$

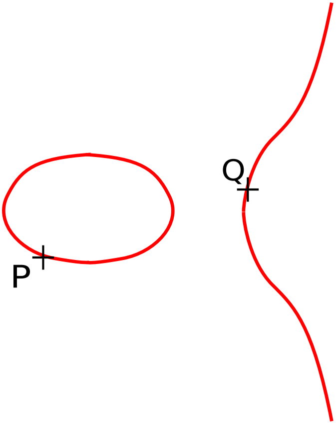
Define:

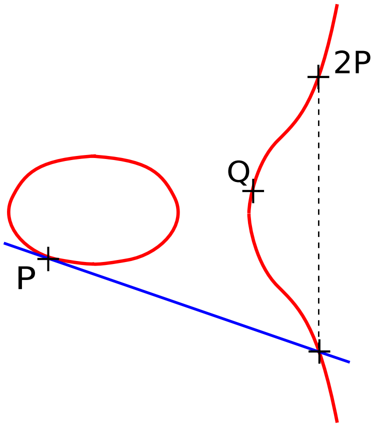
$$\underbrace{(P_1) + (P_2)}_{D_1} + \underbrace{(P_3) + (P_4)}_{D_2} = \underbrace{(-P_5) + (-P_6)}_{D_3}$$

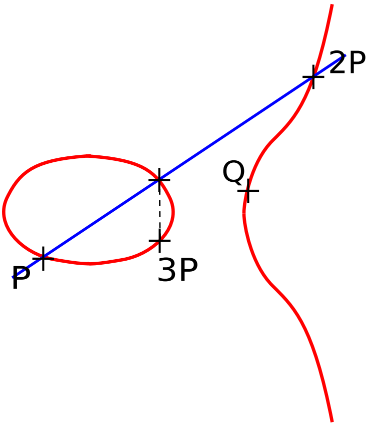
$$D_1 + D_2 := D_3$$

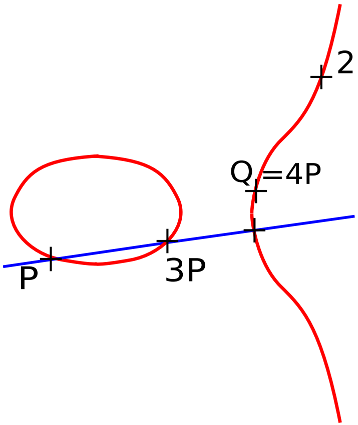


# A discrete logarithm on an elliptic curve



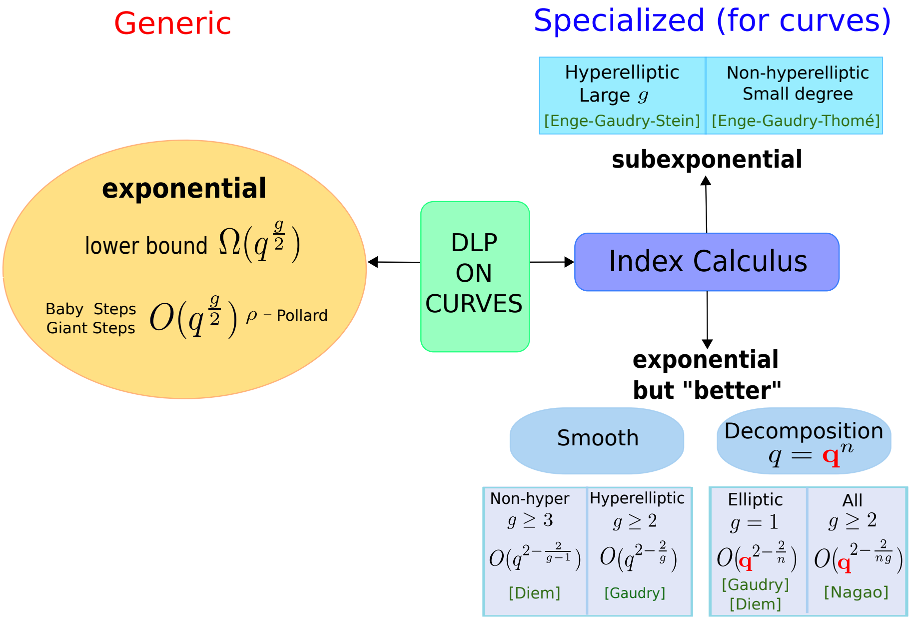

2P
Q
P


2P
Q
P
3P

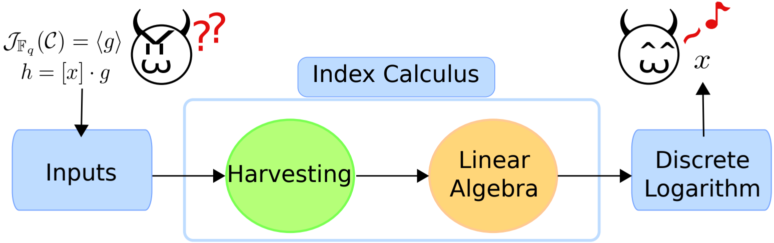



In crypto, the group is finite... **But what if Q**$\approx 2^{80}$**P ?**

# How to compute Discrete Logs in Jacobian varieties



# About Index-Calculus




What ?

1) Select **Factor base**

$$\mathcal{F} = \{F_1, \ldots, F_N\} \subset \mathcal{J}_{\mathbb{F}_q}(\mathcal{C})$$

2) Find $N$ **relations:** $a, b, c_{ij} \in \mathbb{Z}$

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

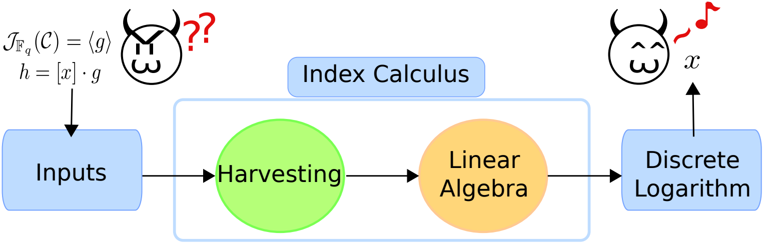
How ?

Smooth Test if some $u \in \mathbb{F}_q[x]$ is $\mathbb{F}_q$−split

Decomposition $\mathbb{F}_q = \mathbb{F}_{\tilde{q}^n}$

Solve polynomial systems over $\mathbb{F}_{\tilde{q}}$

3) Build (very sparse) matrix $(c_{ij})$




What ?

1) Select **Factor base**

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

2) Find $N$ **relations:** $a, b, c_{ij} \in \mathbb{Z}$

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

How ?

Smooth — Test if some $u \in \mathbb{F}_q[x]$ is $\mathbb{F}_q$−split

Decomposition — $\mathbb{F}_q = \mathbb{F}_{\tilde{q}^n}$

Solve polynomial systems over $\mathbb{F}_{\tilde{q}}$

3) Build (very sparse) matrix $(c_{ij})$

What ?

1) Compute $v \in \ker(c_{ij}) \setminus \{0\}$

How ?

Wiedemann

Filtering

2) Use $v$ to retrieve $[x]$

# About curves' security

How to increase security and keep a "reasonable" field ??

| | **Pros:** | **Cons:** | **Comments:** |
|---|---|---|---|
| Higher genus | $\#\mathcal{J}(\mathcal{H}) \approx q^g$ **more security** | **Expensive arithmetic** | $g = 2$ **competitive** with $g = 1$ † |
| Extension $\mathbb{F}_{q^n}$ | $\#\mathcal{J}(\mathcal{H}) \approx q^{ng}$ **better arithmetic same security** | **Decomposition attacks** †† | attack practical only for **very** small $g, n$. |

† [Gaudry'07, Gaudry-Lubicz'09, Renes&al.'16, ...]
†† [Gaudry'09, Nagao'10, Diem'11]

How to increase security and keep a "reasonable" field ??

| | **Pros:** | **Cons:** | **Comments:** |
|---|---|---|---|
| **Higher genus** | $\#\mathcal{J}(\mathcal{H}) \approx q^g$ more security | Expensive arithmetic | $g = 2$ competitive with $g = 1$†† |
| **Extension $\mathbb{F}_{q^n}$** | $\#\mathcal{J}(\mathcal{H}) \approx q^{ng}$ better arithmetic same security | **Decomposition attacks**† | **make attack practical for more $g, n$.** |

1 Context and background

2 Contribution : improving smooth relations harvesting
- Old-school smooth harvesting
- New approach: Harvesting by Sieving
- Timings

3 Decomposition attacks on curves: state of the art

4 Contribution: summation Ideals

5 Contribution: degree reduction in even characteristic

6 Conclusion & perspectives

# Old-school harvesting for smooth divisors

## non-hyperelliptic case

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

Factor base $\mathcal{F} = \{ P \in \mathcal{C}(\mathbb{F}_q) \}$ (rational points). **To find one relation:**

### Non-hyperelliptic case [Diem'08]

1. Select $P_1, P_2 \in \mathcal{F}$.
2. Compute $F \in \mathbb{F}_q[x]$ describing $\mathcal{C} \cap$ the line $(P_1 P_2)$.
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 $g \geq 3$. ([Diem] $\deg C = g + 1$)

Factor base $\mathcal{F} = \{ P \in \mathcal{C}(\mathbb{F}_q) \}$ (rational points). **To find one relation:**

### Non-hyperelliptic case [Diem'08]

1. Select $P_1, P_2 \in \mathcal{F}$.
2. Compute $F \in \mathbb{F}_q[x]$ describing $\mathcal{C} \cap$ the line $(P_1 P_2)$.
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

# 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:**
[JouxVitse'12]: small extensions $\longrightarrow$ different context
[SarkarSingh'14]: hyperelliptic only $\longrightarrow$ sort, backtracking, hyperelliptic only

**Cons:**
different context
sort, backtracking, hyperelliptic only

**Our contribution:**

- Clarify formulation of [SarkharSing'14]
- Skip computations, better memory efficiency, no sorting.
- Adapt to all curve types and to other Index-Calculus variants.

# Illustration for non-hyperelliptic curves

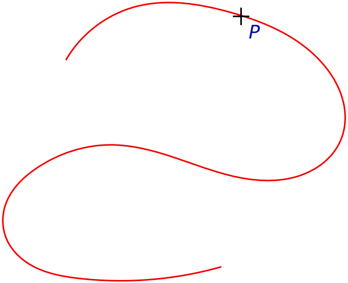
$\mathcal{C} : C(x, y) = 0$ **non-hyperelliptic** of genus $g \geq 3$. ([Diem] $\deg C = g + 1$)

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:

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



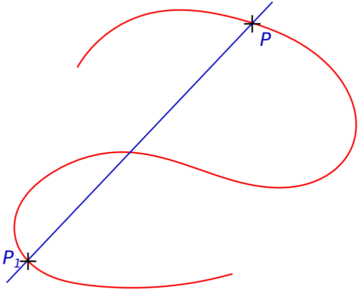
$\mathcal{C} : C(x, y) = 0$ **non-hyperelliptic** of genus $g \geq 3$. ([Diem] $\deg C = g + 1$)

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:

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



# Illustration for non-hyperelliptic curves

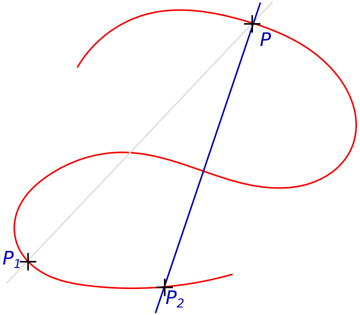
$\mathcal{C} : C(x, y) = 0$ **non-hyperelliptic** of genus $g \geq 3$. ([Diem] $\deg C = g + 1$)

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:

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



# Illustration for non-hyperelliptic curves

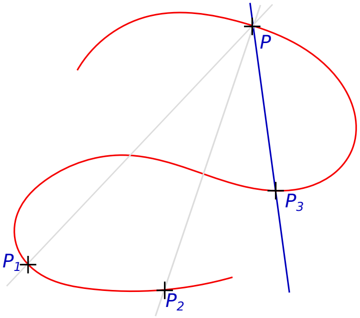
$\mathcal{C} : C(x, y) = 0$ **non-hyperelliptic** of genus $g \geq 3$. ([Diem] $\deg C = g + 1$)

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:

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



# Illustration for non-hyperelliptic curves

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

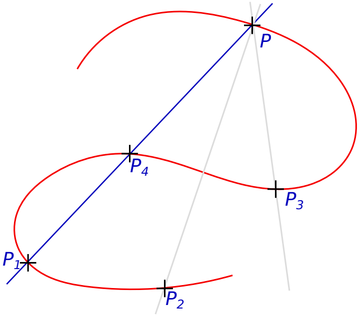
Factor base $\mathcal{F} = \{P, P_1, P_2, \ldots\}$. **First round of sieving:** fix $P = (x_P, y_P)$.

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

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

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

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



# Illustration for non-hyperelliptic curves

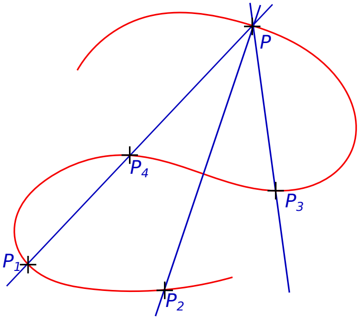
$\mathcal{C} : C(x,y) = 0$ **non-hyperelliptic** of genus $g \geq 3$. ([Diem] $\deg C = g+1$)

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 !**

## Analysis in the non-hyperelliptic case

For one loop:

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

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

Overall:

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

### Relations management

- Loop on $P$ uses all lines through $P$: **no duplicate relations.**
- How to handle the table ?
  1. Counter list: factorize only splitting polynomials
  2. Hash tables & more memory: no factorization at all

# 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.

1. Context and background
2. Contribution : improving smooth relations harvesting
3. Decomposition attacks on curves: state of the art
    - On elliptic curves [Diem], [Gaudry]
    - On hyperelliptic curves [Nagao]
4. Contribution: summation Ideals
5. Contribution: degree reduction in even characteristic
6. Conclusion & perspectives

# What are Decomposition attacks?

From now on, assume the base field is some $\mathbb{F}_{q^n}$, $n \geq 2$.

## Point $m$-Decomposition Problem ($\mathrm{PDP}_m$)

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. $R = D_1 + \cdots + D_m$.

**Decomposition harvesting = solving multiple $\mathrm{PDP}_m$ instance, for some $m$.**

How can this be done ? Let's see on elliptic curves.

# 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 (Semaev)

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:

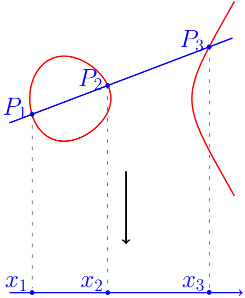
$$S_m(x_1, \ldots, x_m) = 0 \Leftrightarrow \ \exists\ y_1, \ldots, y_m \in \overline{\mathbb{F}} \text{ s.t. } P_i = (x_i, y_i) \in E \text{ and}$$
$$P_1 + \cdots + P_m = \mathcal{O}.$$

**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 $\mathrm{PDP}_m$ for elliptic curves [Diem], [Gaudry]

**Goal:** Find decomposition $P_1 + \cdots + P_m$ of $R \in E(\mathbb{F}_q)$

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

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

# Solving $\text{PDP}_m$ for elliptic curves [Diem], [Gaudry]

**New goal:** Solve $S_{m+1}(x_R, X_1, \ldots, X_m)$ Under-determined

# Solving $\mathrm{PDP}_m$ for elliptic curves [Diem], [Gaudry]

**New goal:** Solve $S_{n+1}(x_R, X_1, \ldots, X_n)$ Under-determined

1. Base field is $\mathbb{F}_{q^n} = \mathrm{Span}_{\mathbb{F}_q}(1, \mathbf{t}, \ldots, \mathbf{t^{n-1}})$. Let $\mathbf{m} = \mathbf{n}$, and $X_i = \sum_{i=1}^{n-1} X_{ij}\mathbf{t^j}$.

   Then $\exists\ s_i \in \mathbb{F}_q[X_{1,0}, \ldots, X_{n,n-1}]$ s.t.: $X_{ij} \in \mathbb{F}_q$

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

# Solving $\mathrm{PDP}_m$ for elliptic curves [Diem], [Gaudry]

**New goal:** Solve $S_{n+1}(x_R, X_1, \ldots, X_n)$ Under-determined

1. Base field is $\mathbb{F}_{q^n} = \mathrm{Span}_{\mathbb{F}_q}(1, \mathbf{t}, \ldots, \mathbf{t^{n-1}})$. Let $\mathbf{m} = \mathbf{n}$, and $X_i = \sum_{i=1}^{n-1} X_{ij}\mathbf{t^j}$.

   Then $\exists\ s_i \in \mathbb{F}_q[X_{1,0}, \ldots, X_{n,n-1}]$ s.t.: $X_{ij} \in \mathbb{F}_q$

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

2. Add constraints: look for $P_i$ s.t. $x_i \in \mathbb{F}_q \Leftrightarrow X_{1,j} = \cdots = X_{n,j} = 0,\ j > 0$

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

0-dimensional

# Solving 0-dimensional systems with Gröbner Bases tools

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

$\Delta$: degree of regularity

$D$: #solutions

$n$ variables

$s$ equations

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

$O(nD^{\omega})$

$\omega$: 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

$\Delta$: degree of regularity

$D$: #solutions

$n$ variables
$s$ equations

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

$O(nD^{\omega})$

computational bottleneck

**Goal:** reduce $D$

## About degrees of ideals

Let $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathcal{I} \subset \mathbb{F}[\mathbf{x}]$. HS : Hilbert Series

$$\begin{aligned} \deg \mathcal{I} &= \#\text{points “when cut by } \dim \mathcal{I} \text{ hyperplanes”} \\ &= \mathrm{HS}_{\mathbb{F}[\mathbf{x}]/\mathcal{I}}(1) \\ &= \dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/\mathcal{I} \text{ when } \dim \mathcal{I} = 0. \end{aligned}$$

With weights $\mathbf{w} = (w_1, \ldots, w_n)$:

$$\begin{aligned} \deg_{\mathbf{w}} \mathcal{I} &= \frac{\mathrm{HS}_{\mathbb{F}[\mathbf{x}]/\mathcal{I}}(1)}{\prod_{i=1}^{n} w_i} \\ &= \dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/\mathcal{I} \text{ when } \dim \mathcal{I} = 0. \end{aligned}$$

# About degrees of ideals

Let $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathcal{I} \subset \mathbb{F}[\mathbf{x}]$. HS : Hilbert Series

$$\begin{aligned}\deg \mathcal{I} &= \#\text{points "when cut by } \dim \mathcal{I} \text{ hyperplanes"}\\ &= \mathrm{HS}_{\mathbb{F}[\mathbf{x}]/\mathcal{I}}(1)\\ &= \dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/\mathcal{I} \text{ when } \dim \mathcal{I} = 0.\end{aligned}$$

With weights $\mathbf{w} = (w_1, \ldots, w_n)$:

$$\begin{aligned}\deg_{\mathbf{w}} \mathcal{I} &= \frac{\mathrm{HS}_{\mathbb{F}[\mathbf{x}]/\mathcal{I}}(1)}{\prod_{i=1}^n w_i}\\ &= \dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/\mathcal{I} \text{ when } \dim \mathcal{I} = 0.\end{aligned}$$

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

**Corollary:** If $\dim \mathcal{I} = 0$, #solutions is divided by $\prod_{i=1}^n w_i$.

# Degree of systems in $\mathrm{PDP}_m$ solving on elliptic curves

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

$$\deg W = n!\, 2^{n(n-1)}$$

FGLM runs in $O(\deg W^{\omega})$ + Probability for a relation: $1/n!$

Known reduction: $\deg W = 2^{n(n-1)} \; > \; 2^{(n-1)^2 \dagger} \; > \; 2^{(n-1)(n-2)\dagger\dagger}$

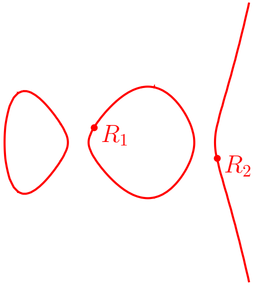
$\mathrm{PDP}_m$ solving for **higher genus?**

†: [Faugère-Gaudry-Huot-Renault]
††: [Faugère-Huot-Joux-Renault-Vitse]

$\mathcal{H} : y^2 + h_1(x)y = h_0(x)$,
$R = \{R_1, \dots, R_g\} \in \mathcal{J}(\mathcal{H})$, $R_i = (x_{R_i}, y_{R_i})$.

**Goal:** $R = P_1 + \cdots + P_m$

Example if $g = 2$ and $m = 4$:



$\mathcal{H} : y^2 + h_1(x)y = h_0(x)$,
$R = \{R_1, \ldots, R_g\} \in \mathcal{J}(\mathcal{H})$, $R_i = (x_{R_i}, y_{R_i})$.

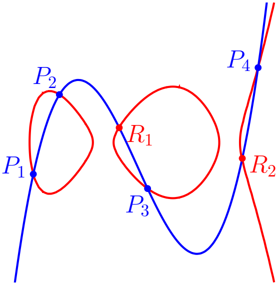
**Goal:** $R = P_1 + \cdots + P_m$

[Nagao] Find $f(x, y)$ of lowest degree s.t.:
$f(x_{R_i}, y_{R_i}) = f(x_i, y_i) = 0$.

Space of such $f$'s: $\mathrm{Span}(f_1, \ldots, f_d)$

$$f = \sum_{i=1}^{d} a_i f_i, \ \mathbf{a} = (a_1, \ldots, a_d).$$

Example if $g = 2$ and $m = 4$:



# Geometric view of Decompositions

$\mathcal{H} : y^2 + h_1(x)y = h_0(x)$,
$R = \{R_1, \ldots, R_g\} \in \mathcal{J}(\mathcal{H})$, $R_i = (x_{R_i}, y_{R_i})$.

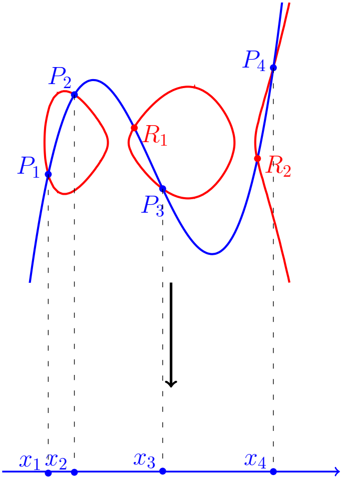
**Goal:** $R = P_1 + \cdots + P_m$

[Nagao] Find $f(x, y)$ of lowest degree s.t.:
$f(x_{R_i}, y_{R_i}) = f(x_i, y_i) = 0$.

Space of such $f$'s: $\mathrm{Span}(f_1, \ldots, f_d)$

$$f = \sum_{i=1}^{d} a_i f_i, \ \mathbf{a} = (a_1, \ldots, a_d).$$

Example if $g = 2$ and $m = 4$:




## Decomposition Polynomial $DP_R$

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

If $f$ describes a decomposition:

$$DP_R(x_i) = 0, \ 1 \le i \le m$$

## Solving $\mathrm{PDP}_m$ for hyperelliptic curves [Nagao]

$\mathcal{H}$ of genus $g$, defined over $\mathbb{F}_{q^n}$, $R \in \mathcal{J}(\mathcal{H})$.

**Goal:** Find $\mathbf{a}$ s.t. $DP_R(x) = x^m + \sum_{i=0}^{m-1} N_i(\mathbf{a}) x^i$ has root $x_1, \ldots, x_m$

# Solving PDP$_m$ for hyperelliptic curves [Nagao]

$\mathcal{H}$ of genus $g$, defined over $\mathbb{F}_{q^n}$, $R \in \mathcal{J}(\mathcal{H})$.

**Goal:** Find $\mathbf{a}$ s.t. $DP_R(x) = x^m + \sum_{i=0}^{m-1} N_i(\mathbf{a})x^i$ has root $x_1, \ldots, x_m \in \mathbb{F}_q$

1. Add constraints: Look for $P_i$ with $x_i \in \mathbb{F}_q$

$$\text{All } x_i \in \mathbb{F}_q \Rightarrow \text{ All } N_i(\mathbf{a}) \in \mathbb{F}_q$$

# Solving $\text{PDP}_m$ for hyperelliptic curves [Nagao]

$\mathcal{H}$ of genus $g$, defined over $\mathbb{F}_{q^n}$, $R \in \mathcal{J}(\mathcal{H})$.

**Goal:** Find $\mathbf{a}$ s.t. $DP_R(x) = x^{ng} + \sum_{i=0}^{ng-1} N_i(\mathbf{a})x^i$ has root $x_1, \ldots, x_{ng}$

1. Add constraints: Look for $P_i$ with $x_i \in \mathbb{F}_q$

$$\text{All } x_i \in \mathbb{F}_q \Rightarrow \text{ All } N_i(\mathbf{a}) \in \mathbb{F}_q$$

2. With $\mathbb{F}_{q^n} = \text{Span}_{\mathbb{F}_q}(1, \mathbf{t}, \ldots, \mathbf{t^{n-1}})$, write $a_i = \sum a_{ij}\mathbf{t^j}$.

   Then $\exists\ N_{ij} \in \mathbb{F}_q[a_{1,0}, \ldots, a_{d,n-1}]$ s.t.:

$$N_i(\mathbf{a}) = \sum_{j=0}^{n-1} N_{ij}(a_{1,0}, \ldots, a_{d,n-1})\mathbf{t^j}$$

3. $N_i(\mathbf{a}) \in \mathbb{F}_q \Leftrightarrow W = \{N_{ij}(a_{1,0}, \ldots, a_{d,n-1}) = 0 \text{ for } j > 0\}$.

   Set $\mathbf{m} = \mathbf{ng}$, so that $\dim W = 0$ and **solve** $W$.

# Degree of systems

$$W = \{N_{ij}(a_{1,0}, \ldots, a_{d,n-1}) = 0 \text{ for } j > 0\}$$

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

FGLM runs in $O(\deg W^{\omega})$ + Probability for a relation: $1/(ng)$!

- $+$ No degree reduction known.
- $+$ Huge degree, lot of variables.
- $+$ Very low probability of decomposition.

ex: $g = 2$, $n = 3$
$\deg = 4096, \#\text{vars} = 12$
proba$= 1/720$

$\Rightarrow$ very few practical cases (essentially $n(n-1)g \leq 12$).

# Situation

**Before this thesis:**

$\swarrow$ $\searrow$

Nagao: works for all genus.
**But:** quickly untractable.

ex: $g = 2, n = 3, k = \mathbb{F}_{2^{15}}$
Solving **one** $\mathrm{PDP}_6$ instance $\approx$ 1500sec.

Finding **one relation** $\approx$ 12.5 days!

$g = 1$: Summation more efficient.
**But:** only for $g = 1$!

**Contribution:**

- Introduce and analyze a Summation modelling for higher genus.
- Reduce systems' degree in even characteristic.

1 Context and background

2 Contribution : improving smooth relations harvesting

3 Decomposition attacks on curves: state of the art

4 Contribution: summation Ideals

5 Contribution: degree reduction in even characteristic

6 Conclusion & perspectives

# 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"*

# 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"*

From [Nagao]:
$$DP_R(x) = x^m + \sum_{i=0}^{m-1} N_i(\mathbf{a}) x^i \tag{1}$$

$R = (P_1) + \cdots + (P_m)$ iff $DP_R(x_i) = 0$ for all $i$. With $e_i = Sym_i(x_1, \ldots, x_m)$:

$$DP_R(x) = x^m + \sum_{i=0}^{m-1} (-1)^{m-i} e_{m-i} x^i \tag{2}$$

Equations (1) and (2) give:

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

**Theorem**

*Let $\mathcal{I}_{m,R} \subset \mathbb{F}[\mathbf{x}, \mathbf{a}]$ be the ideal defined previously. Then $\mathcal{V}_{m,R} = V(\mathcal{I}_{m,R})$.*

Conditions in $\mathbf{x}$ : **eliminate** $\mathbf{a}$

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

**$m^{th}$ Summation Ideals**

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

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

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

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

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

[Diem]: proven for $g = 1$

# New $\mathrm{PDP}_m$ solving for hyperelliptic curve

Input: $\mathcal{H}$ def. over $\mathbb{F}_{q^n}$, $R \in \mathcal{J}(\mathcal{H})$, $\mathcal{F} = \{(P) \in \mathcal{J}(\mathcal{H}) : x(P) \in \mathbb{F}_q\}$.

**Goal:** Find decomposition $R = (P_1) + \cdots + (P_{ng})$, $P_i \in \mathcal{F}$.

1. Compute $ng^{th}$ Summation Set $\mathbb{S}_{ng,R}$.

$$R = P_1 + \cdots + P_{ng} \Leftrightarrow \mathbb{S}_{ng,R}(x_1, \ldots, x_{ng}) = 0.$$

# New $\text{PDP}_m$ solving for hyperelliptic curve

Input: $\mathcal{H}$ def. over $\mathbb{F}_{q^n}$, $R \in \mathcal{J}(\mathcal{H})$, $\mathcal{F} = \{(P) \in \mathcal{J}(\mathcal{H}) : x(P) \in \mathbb{F}_q\}$.

**Goal:** Find decomposition $R = (P_1) + \cdots + (P_{ng})$, $P_i \in \mathcal{F}$.

1. Compute $ng^{th}$ Summation Set $\mathbb{S}_{ng,R}$.

$$R = P_1 + \cdots + P_{ng} \Leftrightarrow \mathbb{S}_{ng,R}(x_1, \ldots, x_{ng}) = 0.$$

2. $\mathbb{S}_{ng,R} = \{S_1, \ldots, S_r\}$ and $\mathbb{F}_{q^n} = \text{Span}_{\mathbb{F}_q}(1, \mathbf{t}, \ldots, \mathbf{t}^{\mathbf{n-1}})$.

   $\exists\ s_{ij} \in \mathbb{F}_q[X_1, \ldots, X_{ng}]$ s.t.:

$$\forall\ 1 \leq i \leq r,\ S_i(x_1, \ldots, x_{ng}) \ = \ \sum_{i=0}^{n-1} s_{ij}(x_1, \ldots, x_{ng})\mathbf{t}^{\mathbf{j}}.$$

3. $$\mathbb{S}_{ng,R}(x_1, \ldots, x_{ng}) = 0 \quad \Leftrightarrow \quad W = \begin{cases} s_{11}(x_1, \ldots, x_{ng}) = 0 \\ \vdots \\ s_{rn}(x_1, \ldots, x_{ng}) = 0 \end{cases}$$

# Analysis, comparison with Nagao

$$\mathbb{S}_{ng,R}(x_1,\ldots,x_{ng}) = 0 \quad \Leftrightarrow \quad W = \begin{cases} s_{11}(x_1,\ldots,x_{ng}) = 0 \\ \vdots \\ s_{rn}(x_1,\ldots,x_{ng}) = 0 \end{cases}$$

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

- $r \geq g = \mathrm{Codim}\mathbf{V} \Rightarrow \dim W = 0$.
- $m = ng \Rightarrow \deg \mathbf{V} = 2^{(n-1)g}$.
- $W \subset \mathcal{W}_n(\mathbf{V})$ - **Weil Restriction** of $\mathbf{V}$ over $\mathbb{F}_q$: $\deg \mathcal{W}_n(\mathbf{V}) = (\deg \mathbf{V})^n$.

# Analysis, comparison with Nagao

$$\mathbb{S}_{ng,R}(x_1,\ldots,x_{ng}) = 0 \quad \Leftrightarrow \quad W = \begin{cases} s_{11}(x_1,\ldots,x_{ng}) = 0 \\ \vdots \\ s_{rn}(x_1,\ldots,x_{ng}) = 0 \end{cases}$$

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

- $r \geq g = \mathrm{Codim}\mathbf{V} \Rightarrow \dim W = 0$.
- $m = ng \Rightarrow \deg \mathbf{V} = 2^{(n-1)g}$.
- $W \subset \mathcal{W}_n(\mathbf{V})$ - **Weil Restriction** of $\mathbf{V}$ over $\mathbb{F}_q$: $\deg \mathcal{W}_n(\mathbf{V}) = (\deg \mathbf{V})^n$.

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

- Same degree as Nago $\Rightarrow$ Same practical cases...
- Less variables but need to compute an elimination basis.

**The two modellings are "equivalent".**

1 Context and background

2 Contribution : improving smooth relations harvesting

3 Decomposition attacks on curves: state of the art

4 Contribution: summation Ideals

5 Contribution: degree reduction in even characteristic
- Square coefficients of $DP_R$
- Degree reduction for Nagao's approach
- Degree reduction for summation approach
- Simulation of a realistic DL computation

6 Conclusion & perspectives

# Structure of $DP_R$ in even characteristic

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

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

Fix $R \in \mathcal{J}(\mathcal{H})$ and $DP_R(x) = x^m + \sum_{i=0}^{m-1} N_i(\mathbf{a})x^i$.

## Square coefficients

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

In Summation approach:
Induces **weight system** on variables.
**Weighted degree is smaller.**

# Degree reduction for Nagao's approach over $\mathbb{F}_{2^{kn}}$

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

With additional reductions:

**Theorem**

*Let $h_1(x) = \sum_{i=\mathbf{t}}^{\mathbf{d}} \alpha_i x^i$, and let $\mathbf{L} = \mathbf{d} - \mathbf{t}$. Solving a $PDP_{ng}$ instance on $\mathcal{H}$ can be done by solving a system of degree:*

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

From $\mathbf{d}_{\text{old}} = \mathbf{2^{(n-1)ng}}$, we obtain:

| | | | | | |
|---|---|---|---|---|---|
| (tight bounds) | $2^{(n-1)((n-1)g-1)}$ | $\leq$ | $d_{\text{new}}$ | $\leq$ | $2^{(n-1)(ng-1)}$ |
| factor | $2^{(n-1)(g+1)}$ | | $\dfrac{d_{old}}{d_{new}}$ | | $2^{n-1}$ |

## Degree reduction for Nagao's approach over $\mathbb{F}_{2^{kn}}$

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

With additional reductions:

**Theorem**

*Let $h_1(x) = \sum_{i=\mathbf{t}}^{\mathbf{d}} \alpha_i x^i$, and let $\mathbf{L} = \mathbf{d} - \mathbf{t}$. Solving a $PDP_{ng}$ instance on $\mathcal{H}$ can be done by solving a system of degree:*

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

From $\mathbf{d}_{\text{old}} = \mathbf{2}^{(\mathbf{n-1})\mathbf{ng}}$, we obtain:

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

Example: $g = 2, n = 3$. Type II curve $y^2 + xy = x^5 + ax^3 + bx^2 + c$ over $\mathbb{F}_{2^{45}}$

Solving over $\mathbb{F}_{2^{15}}$ with Magma 2.19:

- $d_{\text{old}} = 2^{12} = 4096$. Time: $\approx 1500$s.
- $d_{\text{new}} = 2^6 = 64$. Time: $\approx 0.029$s

**Ratio: $\approx$ 75000**

# Square equations and weights: degree reduction

Let $k = \#\text{squared } N_i(\mathbf{a})$. Renumber s.t.:

$$DP_R(x) = x^m + \sum_{i=m-k}^{m-1} \tilde{N}^2_{m-i}(\mathbf{a})x^i + \sum_{i=0}^{m-k-1} N_{m-i}(\mathbf{a})x^i.$$

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

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

# Square equations and weights: degree reduction

Let $k = \#$squared $N_i(\mathbf{a})$. Renumber s.t.:

$$DP_R(x) = x^m + \sum_{i=m-k}^{m-1} \tilde{N}_{m-i}^2(\mathbf{a})x^i + \sum_{i=0}^{m-k-1} N_{m-i}(\mathbf{a})x^i.$$

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

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

## 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 $\mathbb{F}_{2^{kn}}$, step 1

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

**Theorem**

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

With $\mathbb{F}_{2^{kn}} = \mathrm{Span}_{\mathbb{F}_{\mathbf{2}^k}}(1, \mathbf{t}, \ldots, \mathbf{t}^{\mathbf{n-1}})$, write $e_i = \sum_{i=0}^{n-1} e_{ij}\mathbf{t}^{\mathbf{j}}$.

weight $e_i = 2 \Rightarrow$ weight $e_{ij} = 2 \Rightarrow \deg \mathcal{W}_n(\mathbf{V}_*) \cap V(e_{ij}) = 2 \deg \mathcal{W}_n(\mathbf{V}_*)$

# Degree reduction in summation approach over $\mathbb{F}_{2^{kn}}$, step 1

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

**Theorem**

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

With $\mathbb{F}_{2^{kn}} = \mathrm{Span}_{\mathbb{F}_{2^k}}(1, \mathbf{t}, \ldots, \mathbf{t^{n-1}})$, write $e_i = \sum_{i=0}^{n-1} e_{ij}\mathbf{t^j}$.

$$\text{weight } e_i = 2 \Rightarrow \text{weight } e_{ij} = 2 \Rightarrow \deg \mathcal{W}_n(\mathbf{V}_*) \cap V(e_{ij}) = 2 \deg \mathcal{W}_n(\mathbf{V}_*)$$

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

**Corollary:** In $\mathrm{PDP}_{ng}$ instances $(m = ng)$, with $L =$length of $h_1$:

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

# Degree reduction in summation approach, step 2

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

With additional reductions:

**Theorem**

*Let $h_1(x) = \sum_{i=\mathbf{t}}^{\mathbf{d}} \alpha_i x^i$, and let $\mathbf{L} = \mathbf{d} - \mathbf{t}$. Solving a $PDP_{ng}$ instance on $\mathcal{H}$ can be done by solving a system of degree*

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

From $\mathbf{d_{old}} = \mathbf{2^{(n-1)ng}}$:

| | | | | | |
|---|---|---|---|---|---|
| (tight bounds) | $2^{(n-1)((n-1)g-1)}$ | $\leq$ | $d_{\text{new}}$ | $\leq$ | $2^{(n-1)(ng-1)}$ |
| factor | $2^{(n-1)(g+1)}$ | | $\dfrac{d_{old}}{d_{new}}$ | | $2^{n-1}$ |

# Degree reduction in summation approach, step 2

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

With additional reductions:

**Theorem**

*Let $h_1(x) = \sum_{i=\mathbf{t}}^{\mathbf{d}} \alpha_i x^i$, and let $\mathbf{L} = \mathbf{d} - \mathbf{t}$. Solving a $PDP_{ng}$ instance on $\mathcal{H}$ can be done by solving a system of degree*

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

From $\mathbf{d_{old} = 2^{(n-1)ng}}$:

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

**What is hidden:**

- Best reduction achieved for less types of curves.
- Need to find curves isomorphisms to obtain same reductions as in Nagao's.

# Comparison of approaches after reduction

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

**Winner for a realistic computation: Nagao's approach.**

†: for binary genus 2 curves over $\mathbb{F}_{2^{45}}$

# Simulation of a realistic DL computation

Parameters:

- $\mathcal{H} : y^2 + xy = x^5 + f_3x^3 + x^2x + f_0$, $g = 2$.
- Field $K = \mathbb{F}_{2^{93}}$, $n = 3$.
- $\#\mathcal{J}(\mathcal{H}) = 2 \times 3 \times p$, $\log p = 184$, $p$ prime.

$\Rightarrow$ **Generic bound $\approx 2^{92}$**.

Modelling for $\text{PDP}_6$ instances:

- Nagao with Degree reduction.
- Ideals have degree 64, field: $\mathbb{F}_{2^{31}}$.

Dedicated implementation:

- DRL Basis: code generating techniques and F5 alg.
- Change-ordering: Sparse FGLM [Faugère-Mou].

# Simulation of a realistic DL computation

Parameters:

- $\mathcal{H} : y^2 + xy = x^5 + f_3x^3 + x^2x + f_0$, $g = 2$.
- Field $K = \mathbb{F}_{2^{93}}$, $n = 3$.
- $\#\mathcal{J}(\mathcal{H}) = 2 \times 3 \times p$, $\log p = 184$, $p$ prime.

$\Rightarrow$ **Generic bound $\approx 2^{92}$**.

Modelling for $\mathrm{PDP}_6$ instances:

- Nagao with Degree reduction.
- Ideals have degree 64, field: $\mathbb{F}_{2^{31}}$.

Dedicated implementation:

- DRL Basis: code generating techniques and F5 alg.
- Change-ordering: Sparse FGLM [Faugère-Mou].

Solving one $\mathrm{PDP}_6$ instance:

$$
\begin{array}{rl}
 & \text{DRL Basis: } 3.87 \cdot 10^{-4}\text{sec.} \\
+ & \text{Sparse-FGLM: } 5.93 \cdot 10^{-4}\text{sec.} \\
+ & \text{Univariate Solving: } 2.22 \cdot 10^{-3}\text{sec.} \\
\hline
 & \approx 3.2 \cdot 10^{-3}\text{sec.}
\end{array}
$$

Finding **one** relation:

$\times$ $(ng)! = 720$ in avg.

**Avg. total time $\approx$ 2.3 sec.**

Parallel Harvesting:

$\approx 2^{31}$ relations with **8000** cores:
$\approx$ **7 days**.

(Before: estimation in years...)

1 Context and background

2 Contribution : improving smooth relations harvesting

3 Decomposition attacks on curves: state of the art

4 Contribution: summation Ideals

5 Contribution: degree reduction in even characteristic

6 Conclusion & perspectives

# About my work

**General Topic:** Index-Calculus over curves with genus $g \geq 2$

**Objectives:**

- Focus on the harvesting phase -> Improve existing methods
  Design new ones
- Sharpen complexity bounds -> Restrict set of practical parameters
  Highlight potential weaknesses

**Methods:**

- Analyze algebraic properties
- Exploit field's structure
  (characteristic, subfields, ...)

**Tools:**

- Computer Algebra (Magma, Maple)
- Efficient Gröbner Bases libraries
  (Maple/FGb)

# Conclusion

**Results:**

- > Improved harvesting phase in "Smooth" search
- > Introduced/analyzed Summation ideals for higher genus

  **Not presented:** – **Less efficient definition**
  – **Obstruction to incremental computations**
- > Reduced degree of $\mathrm{PDP}_m$ systems in even characteristic

  **Not presented:** – **Frobenius action over parametrizations in general**
  – **Reductions not linked to squares & technicalities.**
- > Made practical harvesting on a meaningful genus 2 curve

**Side results:**

- \+ Nagao > Summation in characteristic 2.
- \+ Experimentally, Nagao > Summation in characteristic $p$.

**Limits:**

- \- No reduction in characteristic $p > 2$
- \- Symmetries of Summation variety unclear
- \- Can't exploit Jacobian automorphisms (2-torsion,...).

**Generalization using Kummer Varieties**

> Give theoretical framework of "Summation Polynomials" for Abelian Varieties.

**If $\mathbf{g} = \mathbf{2}$:** group law well-understood with **theta functions**.
[Gaudry'07], [Gaudry-Lubicz'09], [Lubicz-Robert'15], [Costello & al.'16], ...

> Explicit "Jacobian" Summation Polynomials using theta arithmetic.

> Design new Decomposition Attack.

**Exploiting Symmetries:** if $g = 1$, degree reduction achieved with 2-torsion.

? Can we exploit automorphisms in the Kummer variety ?

**Thank you for your attention !**