Decomposition attacks over hyperelliptic curves

Alexandre WALLET[1,2,3] and Jean-Charles Faugère[2,3]

[1]Université de Lyon, ENSL, CNRS, INRIA, UCBL, UMR 5668, LIP, 69000, Lyon, France

[2]Sorbonne Universités, UPMC Univ Paris 06, CNRS, UMR 7606, LIP6, F-75005, Paris, France

[3] INRIA, équipe PolSys, centre Paris, F-75005, Paris, France

Motivations

- **Algorithmic Number Theory**
  - Computations of discrete logs in abelian varieties in general
  - Jacobian varieties of algebraic curves are abelian varieties
- **Cryptography: Diffie-Hellman $\leq$ DLP, signature algorithms**
  - Elliptic curves $=$ abelian varieties of dimension 1
  - Transfer attacks: elliptic curves $\longrightarrow$ hyperelliptic curves

How to compute discrete logs ?

✗ **Generic algorithms**
Exponential at best [1].

✓ **Index-Calculus algorithms**
How "better" are they ?

Decomposition attack

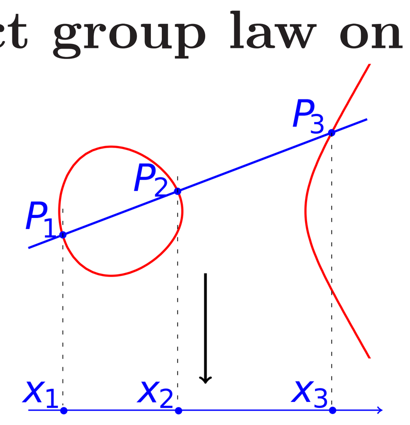
Example over an elliptic curve $E(\mathbb{F}_{q^n})$:
Given (many) $R \in E(\mathbb{F}_{q^n})$, find relations as $R = P_1 + \cdots + P_n$.

- **summation polynomials $\sim$ project group law on the x-line**

$P_1 + P_2 + P_3 = 0$

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

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



- **restriction of scalars gives polynomial systems**

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

$$\begin{cases} R = P_1 + \cdots + P_n \\ P_i \in \mathcal{F} \end{cases} \rightarrow \begin{cases} s_1(X_1, \ldots, X_n) = 0 \\ \vdots \\ s_n(X_1, \ldots, X_n) = 0 \end{cases}$$

Solve with Gröbner basis computation

$$\rightarrow \begin{cases} X_1 + Q_1(X_n) = 0 \\ \vdots \\ X_{n-1} + Q_{n-1}(X_n) = 0 \\ U(X_n) = X_n{}^D + \ldots = 0 \end{cases} \rightarrow$$

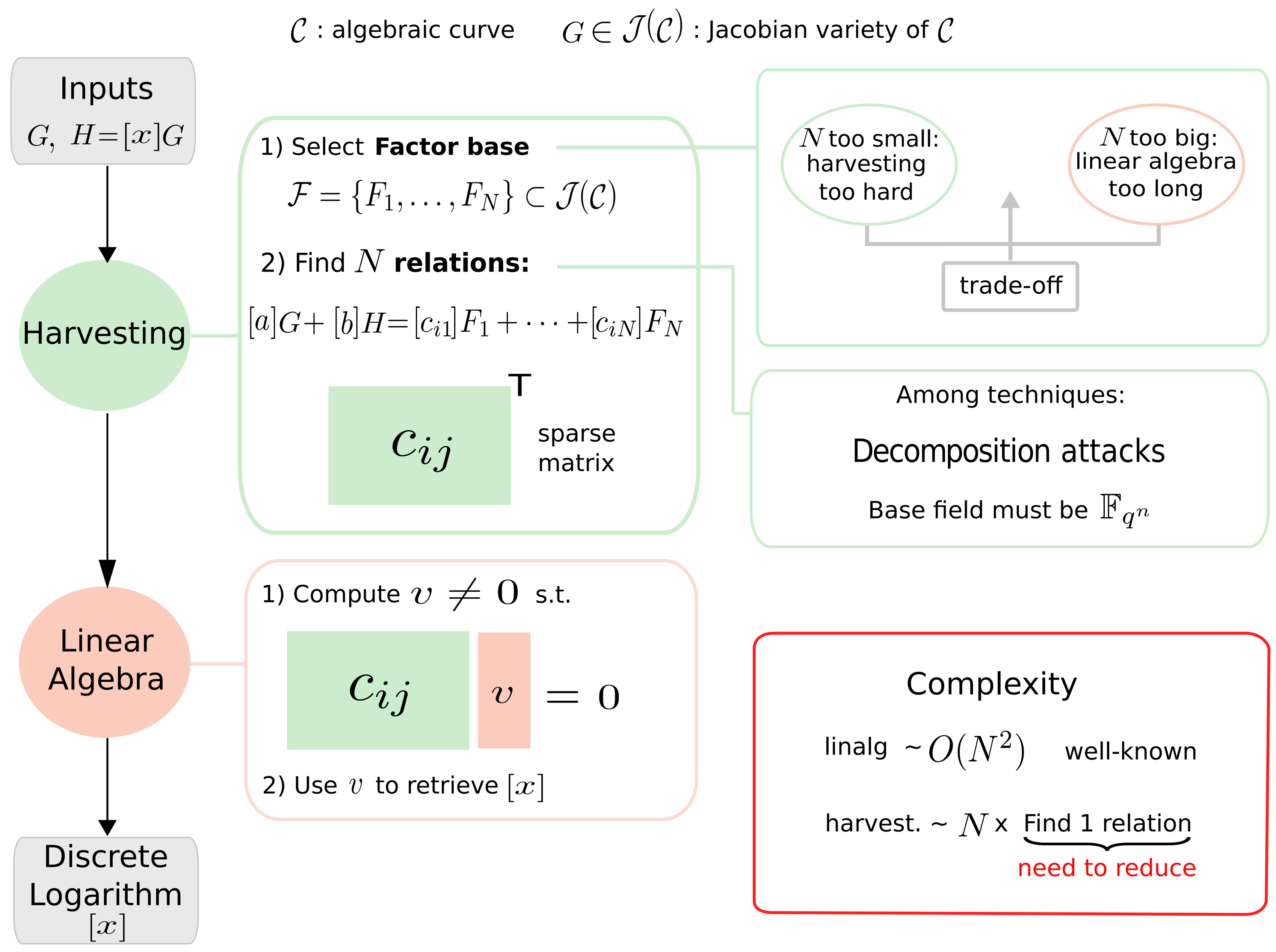
- Find roots of U over $\mathbb{F}_q$
- any root gives a relation
- Probability(root) $\sim \frac{1}{n!}$

Contributions

Improvements for decomposition attacks on hyperelliptic curves

- **Generalization of summation polynomials:**
  - Computational definition:
    1. Description of $\mathcal{V}_{n,R} = \{(P_1, \ldots, P_n) \ : \ \sum P_i = R\}$
    2. Summation polynomials $=$ Gröbner basis of an elimination ideal
  - Analysis of geometric and algebraic structure
    - Codim $\mathcal{V}_{n,R} =$ genus
    - deg $\mathcal{V}_{n,R} = 2^{n-\text{genus}}$
  - Exploited in a new decomposition attack over hyperelliptic curves
- **In characteristic 2:**
  - Reduction of D using Frobenius action
    - Reduction factor: at least 2^{n-1}, up to $2^{(n-1)(\text{genus}+1)}$
  - Decomposition attacks now practical for more parameters
    - Harvesting over a meaningful curve

Index Calculus for Jacobian varieties



PoSSo with Gröbner bases

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

	DRL basis F4, F5	Change order FGLM
	Δ: degree of regularity	D: #solutions in alg. closure
n variables, s equations	$O\left(s\binom{n+\Delta}{\Delta}^\omega\right)$	$O(nD^\omega)$
In Decomposition attacks	$\Delta = \tilde{O}(D^{1/n})$	$D = 2^{n(n-1)\text{genus}}$

Find 1 relation $= O((n \cdot \text{genus})! \times D)$

Reduction: for elliptic curves: [2, 3]; for hyperelliptic curves: this work

Impact of the reduction

For genus $= 2$, $n = 3$, $D = 2^{12} = 4096$, reduced degree $D = 2^6 = 64$.

- Toy-example for one try:

Fields	Tool	Time for D	Time for D	Ratio
$\mathbb{F}_{2^{45}} \mid \mathbb{F}_{2^{15}}$	Magma 2.19	1500s	0.029s	**75000**

- Meaningful harvesting: #target group $\sim 2^{184}$, using 8000 cores:

Field	Tool	old	this work
$\mathbb{F}_{2^{93}} \mid \mathbb{F}_{2^{31}}$	C (optimized)	$\sim$ 30 years unfeasible	$\sim$ **7** days practical

Linalg: $\sim 2^{56}$ operations: whole algorithm is practical.

References

[1] V. Shoup, *Lower bounds for Discrete Logarithms and Related Problem*, EUROCRYPT'97.

[2] J.C. Faugère, P. Gaudry, L. Huot, G. Renault, *Using symmetries in the Index Calculus for Elliptic Curves Discrete Logarithm*, J. of Cryptology, 2014

[3] J.C. Faugère, L. Huot, A. Joux, G. Renault, V. Vitse, *Symmetrized Summation Polynomials: using small order torsion point to speed up Elliptic Curve Index Calculus*, EUROCRYPT'14.

[4] J.C. Faugère, A. W., *The Point Decomposition Problem in Hyperelliptic Curves: toward efficient computations of Discrete Logarithms in even characteristic*, in revision.

[5] A.W., *The point decomposition problem in Jacobian varieties*, PhD. thesis.