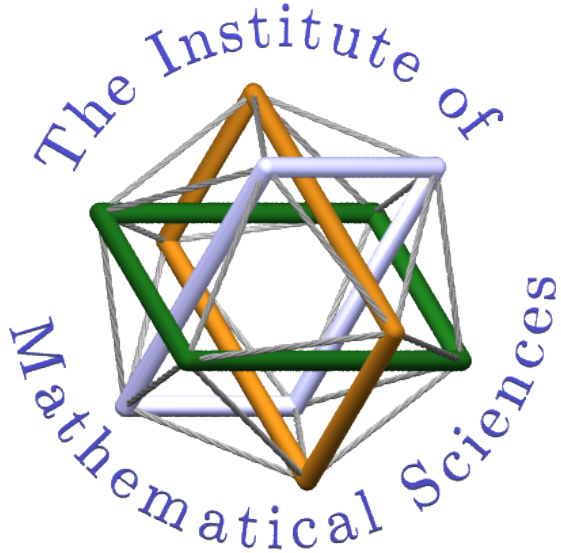
On Using Torsion Points in the Elliptic Curve Index Calculus

Guénaël Renault
Sorbonne Universités UPMC, INRIA, CNRS LIP6



General Context

Discrete Logarithm Problem (DLP)

Given a finite cyclic group $(\mathbb{G} = \langle g \rangle, +)$ and $h \in \mathbb{G}$, find k such that

$$h = [k]g = \underbrace{g + \cdots + g}_{k \text{ times}}$$

- **Generic algorithms** $O\left(\sqrt{\#\mathbb{G}}\right)$
  - Baby Step Giant Step, Pollard's rho, etc.
  - For any **black box group** $\mathbb{G}$, optimal complexity (Shoup)
- **Index Calculus** can be quasi-polynomial, sub-exponential
  - sieving + linear algebra
  - $\mathbb{G} = (\mathbb{F}_{2^k}^{\times}, \times)$
  - $\mathbb{G} = (\mathbb{F}_q^{\times}, \times)$, $\mathbb{G} = (J_C(\mathbb{F}_q), +)$ with genus $g > 2$

☞ $\mathbb{G} = E(\mathbb{F}_q)$ **no sub-exponential** index calculus algo. in general

Context

☞ Index calculus algo. adaptation for $E(\mathbb{F}_{q^n})$ (n small)

- Semaev/Gaudry/Diem ($\approx$ 2005) (Point Decomposition Problem)
- Semaev Summation Polynomial
- Polynomial System Solving

☞ Increasing the efficiency by using the symmetries

☞ Using Symmetries in the Index Calculus for ECDLP (J. Crypto. 2014)
(J.-C. Faugère, P. Gaudry, L. Huot, G. R.)

☞ Symmetrized Summation Polynomials (Eurocrypt'14)
(J.-C. Faugère, L. Huot, A. Joux, G. R., V. Vitse)

Outline

Outline

Index Calculus for ECDLP

Algorithm (Gaudry 2005)

Input: $P, Q \in E(\mathbb{F}_{q^n})$
Output: x such that $Q = [x]P$

1. Def. factor base: $\mathcal{F} = \{(x, y) \in E(\mathbb{F}_{q^n}) \mid x \in \mathbb{F}_q\}$
2. Sieving: $[a_j]P \oplus [b_j]Q = P_1 \oplus \cdots \oplus P_n,\ P_i \in \mathcal{F}$ until having $\#\mathcal{F} + 1$ such relations
3. Linear algebra $\sum_j [\lambda_j \cdot a_j]P \oplus [\lambda_j \cdot b_j]Q = 0_{E(\mathbb{F}_{q^n})}$

Point Decomposition Problem

Given

- $R \in E$
- $\mathcal{F}$ a factor base of points in E

find $P_1, \ldots, P_n \in \mathcal{F}$ such that $R = P_1 \oplus \ldots \oplus P_n$

Point Decomposition Problem

PDP$(n, R, \mathcal{F})$

Given

- $R \in E$
- $\mathcal{F}$ a factor base of points in E

$$\text{find } P_1, \ldots, P_n \in \mathcal{F} \text{ such that } R = P_1 \oplus \ldots \oplus P_n$$

☞ Modeling the problem as a polynomial system $\{g_1, \ldots, g_s\}$ and solve this system:

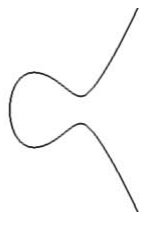
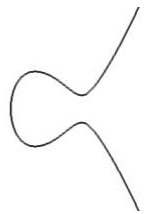
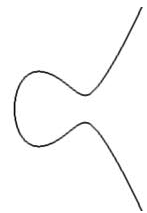
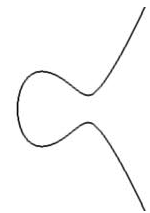
$$\begin{cases} (x_i, y_i) \in E \\ (x_1, y_1) \oplus (x_2, y_2) \oplus \cdots \oplus (x_n, y_n) = (R_x, R_y) \end{cases}$$

☞ The solution has to be found in $\mathcal{F}$

Algebraic modelling of PDP: Summation polynomials

Semaev, 2004, Gaudry, 2005

☞ Projection of the PDP$(n, R = 0, \mathcal{F} = \{(x, y) \in E(\mathbb{F}_{q^n}) \mid x \in \mathbb{F}_q\})$

PDP: $\mathbf{g}_1($  $,\ldots,$  $) = \cdots = \mathbf{g}_s($  $,\ldots,$  $) = 0$

Projection π^n

Summation: $\mathbf{f}_n($ ——— $,\ldots,$ ——— $) = 0$

Algebraic modelling of PDP: Summation polynomials

Semaev, 2004, Gaudry, 2005

☞ Projection of the PDP$(n, R = 0, \mathcal{F} = \{(x, y) \in E(\mathbb{F}_{q^n}) \mid x \in \mathbb{F}_q\})$

PDP: $\langle \mathbf{g}_1(x_1, \ldots, x_m, y_1, \ldots, y_m), \ldots, \mathbf{g}_s(x_1, \ldots, x_m, y_1, \ldots, y_m) \rangle$

$\pi : (x, y) \to x$ | Elimination (Resultant, Gröbner basis)

Summation: $\langle \mathbf{f}_n(x_1, \ldots, x_n) \rangle = \langle \mathbf{g}_1, \ldots, \mathbf{g}_s \rangle \cap \mathbb{F}_{q^n}[x_1, \ldots, x_n]$

$\deg_{x_i}(\mathbf{f}_n) \leqslant 2^{n-2}$

Characterization

$$\mathbf{f}_n(x_1, ..., x_n) = 0$$

$$\Updownarrow$$

$\exists (y_1, ..., y_n) \in \overline{\mathbb{F}}_{q^n}^n$ s.t. $\forall i, P_i = (x_i, y_i) \in E$ and $P_1 \oplus \cdots \oplus P_n = 0$

Algebraic modelling of PDP: Summation polynomials

Semaev, 2004, Gaudry, 2005

☞ Projection of the PDP$(n, R = 0, \mathcal{F} = \{(x, y) \in E(\mathbb{F}_{q^n}) \mid x \in \mathbb{F}_q\})$

PDP: $\langle \mathbf{g}_1(x_1, \ldots, x_m, y_1, \ldots, y_m), \ldots, \mathbf{g}_s(x_1, \ldots, x_m, y_1, \ldots, y_m) \rangle$

$\pi : (x, y) \to x$ | Elimination (Resultant, Gröbner basis)

Summation: $\langle \mathbf{f}_n(x_1, \ldots, x_n) \rangle = \langle \mathbf{g}_1, \ldots, \mathbf{g}_s \rangle \cap \mathbb{F}_{q^n}[x_1, \ldots, x_n]$

$\deg_{x_i}(\mathbf{f}_n) \leqslant 2^{n-2}$

Application in Index Calculus: (*Gaudry 2005*)

Solving PDP$(R, \mathcal{F})$ with factor base $\mathcal{F} = \{(x, y) \in E(\mathbb{F}_{q^n}) \mid x \in \mathbb{F}_q\}$.

$\Updownarrow$

Finding $(x_1, \ldots, x_n)$ with $x_i \in \mathbb{F}_q$ s.t. $\mathbf{f}_{n+1}(x_1, ..., x_n, (-R)_x) = 0$

☞ In Weierstrass model $R_x = (-R)_x$

From summation polynomials to PoSSo

Problem

We want to find $P_1, \ldots, P_n \in \mathcal{F} = \{(x, y) \in E \mid x \in \mathbb{F}_q\}$ such that

$$R = P_1 + \cdots + P_n \iff P_1 + \cdots + P_n - R = 0_E$$

$$\Updownarrow$$

Finding $(x_1, \ldots, x_n)$ with $x_i \in \mathbb{F}_q$ s.t. $\mathbf{f}_{n+1}(x_1, ..., x_n, R_x) = 0$

Solving process: Restriction of scalar on sum. polynomial

$\mathbb{F}_{q^n} \simeq \mathbb{F}_q(\omega)$: n dimensional $\mathbb{F}_q$-vector space

$$f_{n+1}(x_1, \ldots, x_n, R_x) = 0_E = \sum_{i=0}^{n-1} \varphi_i(x_1, \ldots, x_n) \cdot \omega^i$$

From summation polynomials to PoSSo

Solving process: Restriction of scalar on sum. polynomial

$\mathbb{F}_{q^n} \simeq \mathbb{F}_q(\omega)$: n dimensional $\mathbb{F}_q$-vector space

$$f_{n+1}(x_1, \ldots, x_n, R_x) = 0_E = \sum_{i=0}^{n-1} \varphi_i(x_1, \ldots, x_n) \cdot \omega^i$$

$$\Rightarrow \begin{cases} - & \mathcal{S} = \{\varphi_0, \ldots, \varphi_{n-1}\} \subset \mathbb{F}_q[x_1, \ldots, x_n] \\ - & n \text{ variables, } n \text{ equations} \\ - & \text{solutions in } \mathbb{F}_q \end{cases}$$

$\mathcal{H}_1$: The polynomial systems $\mathcal{S}$ are zero-dimensional

Outline

Solving 0-dim polynomial systems

Let $\mathcal{S} = \{f_1, \ldots, f_n\}$ where $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ and $\mathrm{Deg}(f_i) \leq 2^{n-1}$

Solving $\mathcal{S}$ means here to compute $\mathcal{V}_{\mathbb{K}}(\langle \mathcal{S} \rangle)$

Solving 0-dim polynomial systems

Let $\mathcal{S} = \{f_1, \ldots, f_n\}$ where $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ and $\mathrm{Deg}(f_i) \leq 2^{n-1}$

Solving $\mathcal{S}$ means here to compute $\mathcal{V}_{\mathbb{K}}(\langle \mathcal{S} \rangle)$

Gröbner basis

Since $|\mathcal{V}_{\overline{\mathbb{K}}}| < \infty$, the Gröbner basis $\mathcal{G}$ of $\langle \mathcal{S} \rangle$ w.r.t. lexicographical order with $x_1 > \ldots > x_n$ then $\mathcal{G}$ has a **triangular form**

$$\begin{cases} h_{1,1}(x_1, \ldots, x_n), \ldots, h_{1,k_1}(x_1, \ldots, x_n) \\ \vdots \\ h_{n-1,1}(x_{n-1}, x_n), \ldots, h_{n-1,k_{n-1}}(x_{n-1}, x_n) \\ h_n(x_n) \end{cases}$$

☞ Factoring univariate polynomials over a finite field.

Solving 0-dim polynomial systems

Let $\mathcal{S} = \{f_1, \ldots, f_n\}$ where $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ and $\mathrm{Deg}(f_i) \leq 2^{n-1}$

Solving $\mathcal{S}$ means here to compute $\mathcal{V}_{\mathbb{K}}(\langle \mathcal{S} \rangle)$

☞ Compute a GB of $\langle \mathcal{S} \rangle$ w.r.t. a lexicographical order.

Zero-dim solve

1. Compute GB DRL from $\mathcal{S}$ (F_4/F_5)
2. Compute GB LEX from GB DRL (FGLM)

Solving 0-dim polynomial systems

Let $\mathcal{S} = \{f_1, \ldots, f_n\}$ where $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ and $\mathrm{Deg}(f_i) \leq 2^{n-1}$

Compute GB DRL from $\mathcal{S}$

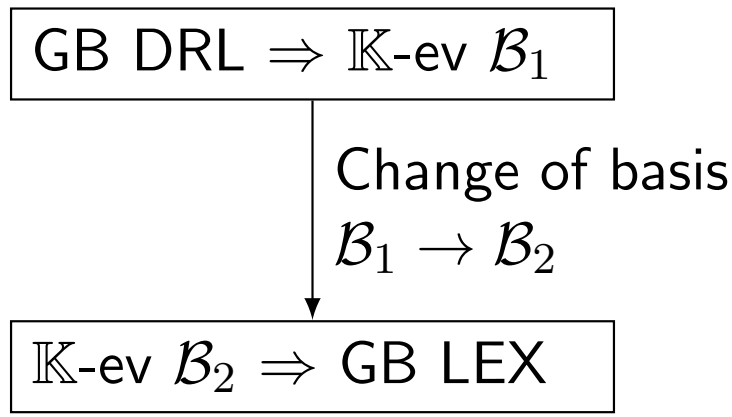
☞ Linear alg. on Macaulay mat.

$$\begin{array}{c} \\ \vdots \\ t_{i,j} f_i \end{array} \begin{array}{c} m_1 > m_2 > \ldots \\ \left(\begin{array}{ccc} c_{i,j}^1 & c_{i,j}^2 & \ldots \end{array} \right) \end{array}$$

Faugère F_4, F_5

Compute GB LEX from GB DRL

☞ See $\mathbb{K}[x_1, \ldots, x_n]/\langle \mathcal{S} \rangle$ as a $\mathbb{K}$-ev



Faugère, Gaudry, Huot, R. ISSAC'14

$$\rightsquigarrow O\left(ne^{n\omega}2^{(n-1)n\omega} + n \cdot \deg(\langle S \rangle)^{\omega}\right)$$

☞ $\deg(\langle S \rangle)$ = the number of solutions (with multiplicities)

☞ ω represents the linear algebra constant

On the complexity of computing GB DRL

☞ These results are usually obtain for homogeneous polynomial systems

☞ In order to avoid fall of degree issues, need to consider regular situation

Regular sequences

A sequence of homogeneous polynomials $(f_1, \ldots, f_n) \subset \mathbb{K}[x_1, \ldots, x_n]$ is said to be regular when

$$f_{i+1} \text{ is a regular element in } \mathbb{K}[x_1, \ldots, x_n]/\langle f_1, \ldots f_i \rangle$$

Affine regular sequences

A sequence of affine polynomials $(f_1, \ldots, f_n) \subset \mathbb{K}[x_1, \ldots, x_n]$ is said to be regular when the sequence $f_1^{(h)}, \ldots, f_n^{(h)}$ of corresponding homogeneous component of highest degree is regular.

☞ Complexity DRL(pol. sys. affine regular) $<$ DRL(its homogenization)

$\mathcal{H}_2$: The affine polynomial systems $\mathcal{S}$ are regular $(\mathcal{H}_2 \Rightarrow \mathcal{H}_1)$

Outline

Invariant Polynomial/System

Let be given a polynomial system

$$\mathcal{S}: \begin{cases} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_{n-1}(x_1, \ldots, x_n) \\ f_n(x_1, \ldots, x_n) \end{cases}$$

$\sigma \in \mathbb{G} \subset \mathsf{GL}(\mathbb{K}, n), \quad \sigma \cdot f_i = f_i(\sigma \cdot \underline{x})$

☞ Assume all f_i are invariant under the action of $\mathbb{G}$.
How this assumption can help in solving the polynomial system?

Invariant ring

Definition

Let $\mathbb{K}[x_1, \ldots, x_n]$ be a polynomial ring and $\mathbb{G} \subset \mathsf{GL}(\mathbb{K}, n)$.

$$\mathbb{K}[x_1, \ldots, x_n]^{\mathbb{G}} = \{p \in \mathbb{K}[x_1, \ldots, x_n] \mid \sigma \cdot p = p \text{ for all } \sigma \in \mathbb{G}\}$$

We want to efficiently solve

$$\mathcal{S} : \begin{cases} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_{n-1}(x_1, \ldots, x_n) \\ f_n(x_1, \ldots, x_n) \end{cases}$$

under the assumption $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]^{\mathbb{G}}$

Hironaka decomposition

Hilbert's finiteness theorem

Let $\mathbb{G} \subset \mathrm{GL}(\mathbb{K}, n)$. Its invariant ring $\mathbb{K}[x_1, \ldots, x_n]^{\mathbb{G}}$ is finitely generated.

$$\mathbb{K}[x_1, \ldots, x_n]^{\mathbb{G}} = \bigoplus_{i=1}^{t} \eta_i \mathbb{K}[\theta_1, \ldots, \theta_n] \,.$$

- *primary invariants* $\theta_1, \ldots, \theta_n \in \mathbb{K}[x_1, \ldots, x_n]^{\mathbb{G}}$
- *secondary invariants* $\eta_1, \ldots, \eta_t \in \mathbb{K}[x_1, \ldots, x_n]^{\mathbb{G}}$

☞ primary invariants are algebraically independent

Example of Hironaka decomposition

$$\mathbb{Q}[x_1, x_2, x_3]^{A_3} = \bigoplus_{i=1}^{2} \eta_i \mathbb{Q}[\theta_1, \theta_2, \theta_3]$$

where

- $\theta_1 = x_1 + x_2 + x_3$, $\theta_2 = x_1x_2 + x_2x_3 + x_1x_3$, $\theta_3 = x_1x_2x_3$
- $\eta_1 = 1$, $\eta_2 = x_1^2x_3 + x_1x_2^2 + x_2x_3^2$

$f = x_1^3x_2^4x_3 + x_1^4x_2^2x_3^2 + x_1^3x_2^3x_3^2 + x_1^2x_2^4x_3^2 + x_1^4x_2x_3^3 + x_1^3x_2^2x_3^3 + x_1^2x_2^3x_3^3 + x_1^2x_2^2x_3^4 + x_1x_2^3x_3^4 + x_1^3x_2 + 2x_1^2x_2^2 + x_1x_2^3 + x_1^3x_3 + 5x_1^2x_2x_3 + 5x_1x_2^2x_3 + x_2^3x_3 + 2x_1^2x_3^2 + 5x_1x_2x_3^2 + 2x_2^2x_3^2 + x_1x_3^3 + x_2x_3^3$

$$f \in \mathbb{Q}[x_1, x_2, x_3]^{A_3} \rightsquigarrow f = \theta_1^2\theta_2\eta_1 + \theta_2\theta_3\eta_2$$

Solving by using symmetries

$$\mathbb{K}[x_1,\ldots,x_n]^{\mathbb{G}} = \bigoplus_{i=1}^{t} \eta_i \cdot \mathbb{K}[\theta_1,\ldots,\theta_n]\,.$$

Change of variable: $f \in \mathbb{K}[x_1,\ldots,x_n]^{\mathbb{G}} \longrightarrow \tilde{f}(\theta_1,\ldots,\theta_n,\eta_1,\ldots,\eta_t)$

$$\mathcal{I} = \langle \mathcal{S} \rangle \in \mathbb{K}[x_1,\ldots,x_n] \longrightarrow \mathcal{J} = (\mathcal{I} \cup \mathcal{I}_\Omega) \cap \mathbb{K}[y_1,\ldots,y_{n+t}]$$

with $\mathcal{I}_\Omega = \langle \theta_1 - y_1, \ldots, \theta_n - y_n, \eta_1 - y_{n+1}, \ldots, \eta_t - y_{n+t} \rangle$

Computing $\mathcal{V}(\mathcal{I})/\mathbb{G}$

- Compute LEX Gröbner basis $\mathcal{G}_\Omega$ of $\mathcal{I} \cup \mathcal{I}_\Omega$
- $\mathcal{G} = \mathcal{G}_\Omega \cap \mathbb{K}[y_1,\ldots,y_{n+t}]$ is a Gröbner basis of $\mathcal{J} = I(\mathcal{V}(\mathcal{I})/\mathbb{G})$.

$$\mathcal{V}(\mathcal{I}) = \bigcup_{(v_1,\ldots,v_{n+t}) \in \mathcal{V}(\mathcal{I})/\mathbb{G}} \mathcal{V}\left(\mathcal{G}\left(y_1 = v_1, \ldots, y_{n+t} = v_{n+t}\right)\right)$$

Solving by using symmetries

$$\mathbb{K}[x_1,\ldots,x_n]^{\mathbb{G}} = \bigoplus_{i=1}^{t} \eta_i \cdot \mathbb{K}[\theta_1,\ldots,\theta_n]\,.$$

Change of variable: $f \in \mathbb{K}[x_1,\ldots,x_n]^{\mathbb{G}} \longrightarrow \tilde{f}(\theta_1,\ldots,\theta_n,\eta_1,\ldots,\eta_t)$

$$\mathcal{I} = \langle \mathcal{S} \rangle \in \mathbb{K}[x_1,\ldots,x_n] \longrightarrow \mathcal{J} = (\mathcal{I} \cup \mathcal{I}_\Omega) \cap \mathbb{K}[y_1,\ldots,y_{n+t}]$$

with $\mathcal{I}_\Omega = \langle \theta_1 - y_1, \ldots, \theta_n - y_n, \eta_1 - y_{n+1}, \ldots, \eta_t - y_{n+t} \rangle$

Computing $\mathcal{V}(\mathcal{I})/\mathbb{G}$

- Compute LEX Gröbner basis $\mathcal{G}_\Omega$ of $\mathcal{I} \cup \mathcal{I}_\Omega$
- $\mathcal{G} = \mathcal{G}_\Omega \cap \mathbb{K}[y_1,\ldots,y_{n+t}]$ is a Gröbner basis of $\mathcal{J} = I(\mathcal{V}(\mathcal{I})/\mathbb{G})$.

- *Pros*: $\deg(\mathcal{J}) = \deg(\mathcal{I})/\#\mathbb{G} \rightsquigarrow$ complx of FGLM step / by $(\#\mathbb{G})^\omega$.
- *Cons*: DRL GB of $\mathcal{J}$ may be more difficult to compute
  - $n + t$ variables
  - $\eta_1,\ldots,\eta_t$ are not independent $\rightsquigarrow$ add equations: $F(\eta_1,\ldots,\eta_t) = 0$.

Invariant ring as polynomial ring

Symmetric group: the well known example

$$\mathbb{K}[x_1, \ldots, x_n]^{\mathfrak{S}_n} = \mathbb{K}[e_1, \ldots, e_n]$$

where $e_k = \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}$ is the k^{th} elementary symmetric polynomial.

- Applying the change of variables

$$\begin{cases} y_1 = e_1(x_1, \ldots, x_n) \\ \vdots \\ y_n = e_n(x_1, \ldots, x_n) \end{cases}$$

$$\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n] \longrightarrow \mathcal{J} \subset \mathbb{K}[y_1, \ldots, y_n]$$

- The evolution of the degree

$$\deg(\mathcal{I}) = n! \cdot \deg(\mathcal{J})$$

Invariant ring as polynomial ring

Theorem (Shepard, Todd ; Chevalley)

If $\text{char}(\mathbb{K}) \nmid \#\mathbb{G}$ then

$$\mathbb{G} \text{ is a } \textbf{reflection group} \implies \mathbb{K}[x_1, \ldots, x_n]^{\mathbb{G}} = \mathbb{K}[\theta_1, \ldots, \theta_n]$$

where $\theta_1, \ldots, \theta_n \in \mathbb{K}[x_1, \ldots, x_n]$ are algebraically independent.

- Applying the change of variables

$$\begin{cases} y_1 = \theta_1(x_1, \ldots, x_n) \\ \vdots \\ y_n = \theta_n(x_1, \ldots, x_n) \end{cases}$$

$$\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n] \longrightarrow \mathcal{J} \subset \mathbb{K}[y_1, \ldots, y_n]$$

- The evolution of the degree

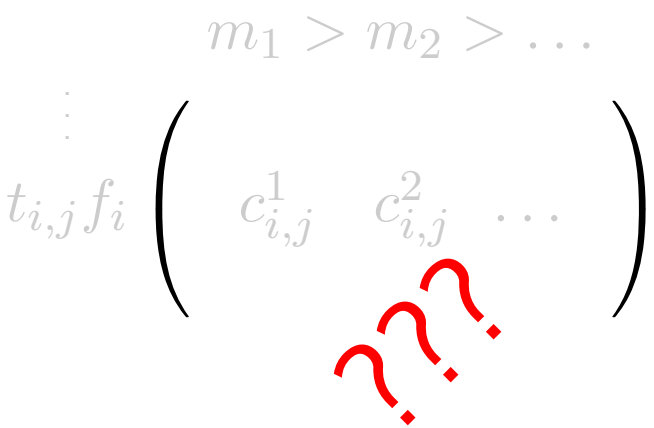
$$\deg(\mathcal{I}) = \#\mathbb{G} \cdot \deg(\mathcal{J})$$

Evolution on the total complexity for solving PoSSo

Let $\mathcal{S} = \{f_1, \ldots, f_n\}$ where $f_i \in \mathbb{K}[x_1, \ldots, x_n]^{\mathbb{G}}$ with $\mathbb{G}$ reflection grp

Compute GB DRL from $\mathcal{S}$

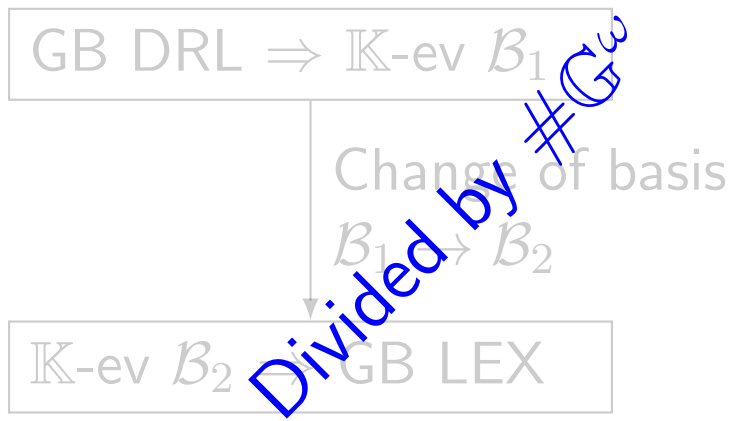
☞ Linear alg. on Macaulay mat.



Faugère F_4, F_5

Compute GB LEX from GB DRL

☞ See $\mathbb{K}[x_1, \ldots, x_n]/\langle \mathcal{S} \rangle$ as a $\mathbb{K}$-ev



Faugère, Gaudry, Huot, R. ISSAC'14

On the complexity of computing GB DRL and Symmetries

$\mathcal{S} = \{f_1, \ldots, f_n\} \subset \mathbb{K}[\theta_1, \ldots, \theta_n] \subset \mathbb{K}[x_1, \ldots, x_n]$, $\mathrm{Deg}(\theta_i) = w_i$

- $\mathcal{S}$ regular
- $\theta_i^{(h)}$ algebraically independent

DRL with weights $(w_1, \ldots, w_n)$ (*Faugère, Safey El Din, Verron, 2013*)

The complexity of GB DRL is divided by $(w_1 \cdots w_n)^\omega$

Regularity preservation (*Faugère, Gaudry, Huot, R.*)

The system obtained after the change of coordinates is still regular.

Corollary

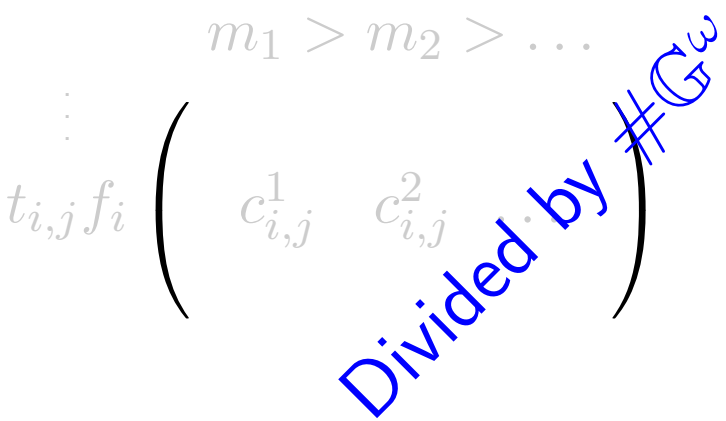
$\mathcal{S} = \{f_1, \ldots, f_n\} \subset \mathbb{K}[x_1, \ldots, x_n]^{\mathbb{G}}$, $\mathbb{G}$ reflection group. Using the symmetries divides the complexity for solving $\mathcal{S}$ by $\#G^\omega$ (no other hypothesis).

Evolution on the total complexity for solving PoSSo

Let $\mathcal{S} = \{f_1, \ldots, f_n\}$ where $f_i \in \mathbb{K}[x_1, \ldots, x_n]^{\mathbb{G}}$ with $\mathbb{G}$ reflection grp

Compute GB DRL from $\mathcal{S}$

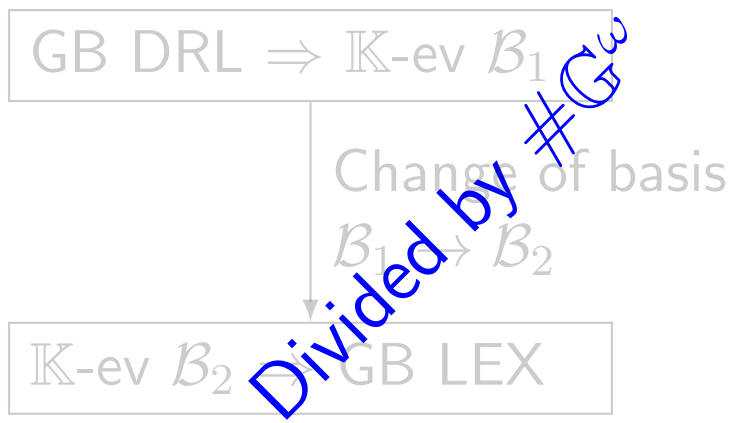
☞ Linear alg. on Macaulay mat.



Faugère F_4, F_5

Compute GB LEX from GB DRL

☞ See $\mathbb{K}[x_1, \ldots, x_n]/\langle \mathcal{S} \rangle$ as a $\mathbb{K}$-ev



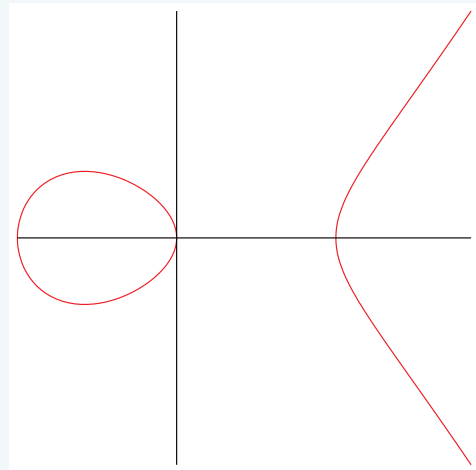
Faugère, Gaudry, Huot, R. ISSAC'14

Outline

Elliptic curve representations

Ordinary elliptic curves

Weierstrass equation, $E : y^2 = x^3 + ax + b$



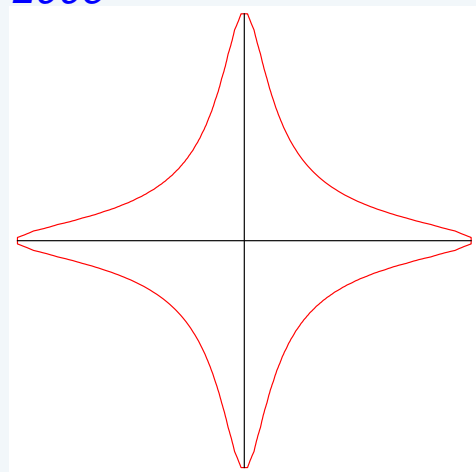
Arithmetic:

- Number of operations in $\mathbb{F}_{q^n}$:
  - (Doubling) 5 mult + 6 squares + 1 div
  - (Adding) 12 mult + 2 squares
- Group law not unified

Efficient arithmetic on Elliptic curves

Edwards, Bulletin of the AMS 2007 ; Bernstein et al., AFRICACRYPT 2008

Edwards representation, $E : ax^2 + y^2 = 1 + dx^2y^2$



Arithmetic:

- Number of operations in $\mathbb{F}_{q^n}$:
  - (Doubling) 3 mult + 4 squares
  - (Adding) 10 mult + 1 square + 1 div
- Group law unified $\rightsquigarrow$ resistant to side channel attacks.

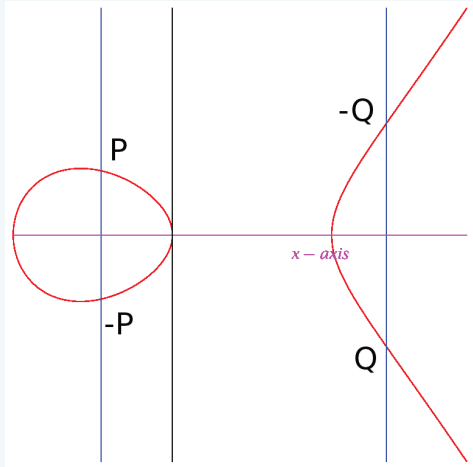
Elliptic curve representations

Ordinary elliptic curves

Weierstrass equation, $E : y^2 = x^3 + ax + b$

Symmetry:

- (negative of a point) $P = (x, y) \Rightarrow \ominus P = (x, -y)$.
  $\rightsquigarrow$ Reflection w.r.t. x-axis.



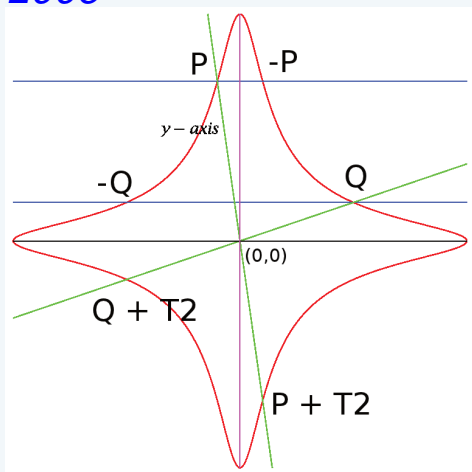
Efficient arithmetic on Elliptic curves

Edwards, Bulletin of the AMS 2007 ; Bernstein et al., AFRICACRYPT 2008

Edwards representation, $E : ax^2 + y^2 = 1 + dx^2y^2$

Symmetries:

- (negative of a point) $P = (x, y) \Rightarrow \ominus P = (-x, y)$.
  $\rightsquigarrow$ Reflection w.r.t. y-axis.
- (addition with T_2) $P = (x, y)$ and $T_2 = (0, -1)$
  $\Rightarrow P \oplus T_2 = (-x, -y)$.
  $\rightsquigarrow$ Point reflection w.r.t. $(0, 0)$.



Application of summation polynomials

PDP(R,$\mathcal{F}$)

We want to find $P_1, \ldots, P_n \in \mathcal{F} = \{(x, y) \in E \mid x \in \mathbb{F}_q\}$ such that

$$R = P_1 \oplus \cdots \oplus P_n \Longleftrightarrow P_1 \oplus \cdots \oplus P_n \ominus R = 0_E$$

where R is a fixed point in E.

A first symmetry

☞ The problem has intrinsic symmetries: $R = P_1 \oplus P_2 \Leftrightarrow R = P_2 \oplus P_1$

Does not imply that summation polynomials are symmetric in general.
Fortunately it is the case!

☞ How to use more symmetries?

System symmetrization - Weierstrass model

$$f_{n+1}(x_1, \ldots, x_n, x_R) \in \mathbb{F}_{q^n}[x_1, \ldots, x_n]^{\mathfrak{S}_n}$$

Corollary (*Gaudry 2005*)

$$f_{n+1}(x_1, \ldots, x_n, x_R) \in \mathbb{F}_{q^n}[x_1, \ldots, x_n]^{\mathfrak{S}_n}$$

$$\downarrow$$

change of variables $e_1, \ldots, e_n$

$$\downarrow$$

$$\widetilde{f}_{n+1}(e_1, \ldots, e_n, x_R) \in \mathbb{F}_{q^n}[e_1, \ldots, e_n]$$

$$\downarrow$$

Weil restriction

$$\downarrow$$

$$\mathcal{S}_{\mathfrak{S}_n} = \{\varphi_1, \ldots, \varphi_n\} \subset \mathbb{F}_q[e_1, \ldots, e_n]$$

☞ $\mathrm{Deg}(\varphi_i) \leq 2^{n-1}$

$\mathcal{H}_2$: The affine polynomial systems $\mathcal{S}_{\mathfrak{S}_n}$ are regular

Edwards curves: Action of 2-torsion point

☞ Reflection w.r.t. y-axis, projection on the y_i's for summation polynomial

Definition

$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ has a 2-torsion point $T_2 = (0, -1)$

Property

$\forall P = (x, y) \in E_{a,d}(\mathbb{F}_{q^n})$,
$P \oplus T_2 = (-x, -y)$.

Action on the points (geometry)

For any combination of an even number of additions by T_2:

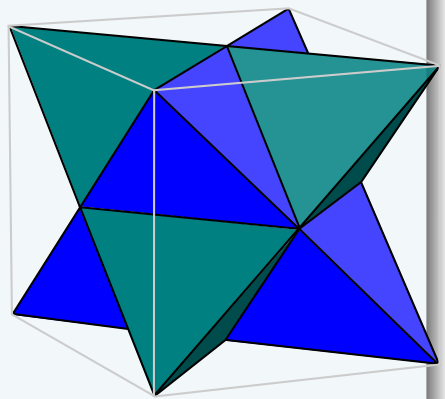
$$P_1 \oplus \cdots \oplus P_n = R \iff (P_1 \oplus T_2) \oplus (P_2 \oplus T_2) \oplus P_3 \oplus \cdots \oplus P_n = R$$
$$(y_1, \ldots, y_n) \in V_R \iff (-y_1, -y_2, y_3, \ldots, y_n) \in V_R$$

What is the name of the group $\mathbb{G}$ acting on the variety?

The Coxeter group $D_n \supset \mathfrak{S}_n$

Definition

D_n is the symmetry group of the n-demihypercube.



$$D_n = (\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_n \Longrightarrow \#D_n = n! \cdot 2^{n-1}$$

$(\mathbb{Z}/2\mathbb{Z})^{n-1}$: even sign changes on $\{y_1, \ldots, y_n\}$.

D_n properties

- Reflection group
- $\mathbb{F}_q[y_1, \ldots, y_n]^{D_n} = \mathbb{F}_q[s_1, \ldots, s_{n-1}, e_n]$
  - $s_i = \sum_{1 \le j_1 < \ldots < j_i \le n} \prod_{k=1}^{i} y_{j_k}^2$ elem. symmetric polynomial in $y_1^2, \ldots, y_n^2$.
  - $e_n = \prod_{k=1}^{n} y_k$ the n^{th} elem. symmetric polynomial.

From geometry to algebra

Let $\mathbb{G}$ be a linear group.

Problem

$$\mathbb{G} \cdot \mathcal{S} = \mathcal{S} \not\Longleftarrow \mathbb{G} \cdot \langle \mathcal{S} \rangle = \langle \mathcal{S} \rangle \Longleftrightarrow \mathbb{G} \cdot \mathcal{V}(\langle \mathcal{S} \rangle) = \mathcal{V}(\langle \mathcal{S} \rangle)$$

Invariance of summation polynomials under D_n (*Faugère, Gaudry, Huot, R.*)

$$f_{n+1}(y_1, \ldots, y_n, y_R) \in \mathbb{F}_{q^n}[y_1, \ldots, y_n]^{D_n}$$

☞ We are in the conditions of Shepard, Todd Thm (large charac.)

New change of variables

Corollary

$$f_{n+1}(y_1,\dots,y_n,y_R) \in \mathbb{F}_{q^n}[y_1,\dots,y_n]^{D_n}$$

$$\downarrow$$

change of variables $s_1,\dots,s_{n-1},e_n$

$$\downarrow$$

$$\widetilde{f}_{n+1}(s_1,\dots,s_{n-1},e_n,x_R) \in \mathbb{F}_{q^n}[s_1,\dots,s_{n-1},e_n]$$

$$\downarrow$$

Weil restriction

$$\downarrow$$

$$\mathcal{S}_{D_n} = \{\varphi_1,\dots,\varphi_n\} \subset \mathbb{F}_q[s_1,\dots,s_{n-1},e_n]$$

Each $s_i = \theta_i(e_1,\dots,e_n)$ with $\mathrm{Deg}(\theta_i) = 2 \rightarrow$ weights $(2,\dots,2,1)$

Theorem (*Faugère, Gaudry, Huot, R.*)

Under the same hypothesis $\mathcal{H}_2$ on $\mathcal{S}_{\mathfrak{S}_n}$, by using the action of T_2 the complexity for solving PDP is divided by $2^{\omega(n-1)}$

Some practical results

Magma or fgb

- $\#\mathbb{F}_q$: 16 bits

n		Step 1 Time (s)	Step 2 Time (s)	Total time (s)	# ops
4	W. sym	6	460	466	2^{29}
	E/J D_n	0	3	3	2^{23}
5 fgb	W. sym	> 2 days			
	E/J D_n	567	2165	2732	2^{45}

- $n = 4$

$\#\mathbb{F}_q$ (bits)		32	64	128	160
Total time (s)	W. sym	6922	4717	5837	6898
	E/J D_n	43	40	53	73

Outline

Action of the 2-torsion in charac. 2 (*Faugère, Huot, Joux, R., Vitse*)

Elliptic curve E defined over $\mathbb{F}_{2^{kn}}$ with $j(E) \neq 0$:

$$y^2 + xy = x^3 + ax^2 + b$$

Assume $b = \gamma^4$.

T_2 the 2-torsion point of E

- $T_2 = (0, \gamma^2)$
- $P \oplus T_2 = \frac{\gamma^2}{x(P)}$

☞ No chance to use such a point as in large characteristic!

Characteristic 2: change of coordinates for a better action

Elliptic curve E defined over $\mathbb{F}_{2^{kn}}$ with $j(E) \neq 0$:

$$y^2 + xy = x^3 + ax^2 + b$$

Assume $b = \gamma^4$.

☞ Change of coordinates: $x \mapsto \frac{\gamma}{x+\gamma} + \lambda$

T_2 the 2-torsion point of E becomes

- $T_2 = (1 + \lambda, \gamma^2)$
- $P \oplus T_2 = x(P) + 1$

Characteristic 2: change of coordinates for a better action

Elliptic curve E defined over $\mathbb{F}_{2^{kn}}$ with $j(E) \neq 0$:

$$y^2 + xy = x^3 + ax^2 + b$$

Assume $b = \gamma^4$.

☞ Change of coordinates: $x \mapsto \frac{\gamma}{x+\gamma} + \lambda$

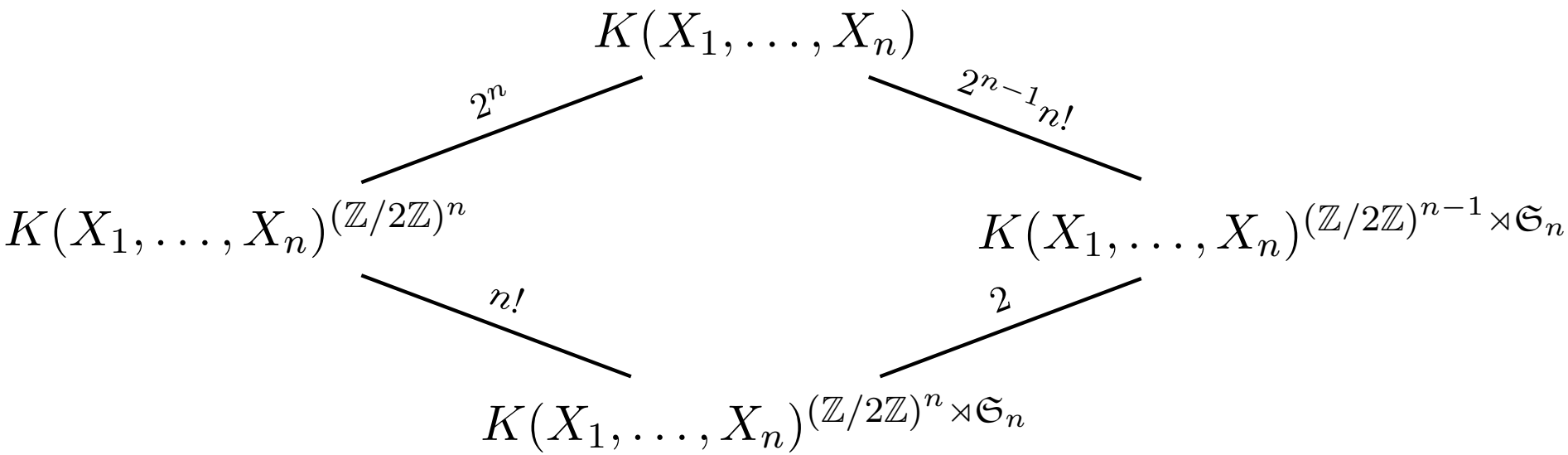
T_2 the 2-torsion point of E becomes

- $T_2 = (1 + \lambda, \gamma^2)$
- $P \oplus T_2 = x(P) + 1$

☞ Better action but no more linear, anyway we are in the modular case!

Some Galois theory with the action $X_i \mapsto X_i + 1$

$K = \mathbb{F}_{2^{kn}}$



- $K(X_1, \ldots, X_n)^{(\mathbb{Z}/2\mathbb{Z})^n} = K(X_1^2 + X_1, \ldots, X_n^2 + X_n)$
- $K(X_1, \ldots, X_n)^{(\mathbb{Z}/2\mathbb{Z})^n \rtimes \mathfrak{S}_n} = K(s_1, \ldots, s_n)$, $s_i = e_i(X_1^2 + X_1, \ldots, X_n^2 + X_n)$
- $K(X_1, \ldots, X_n)^{(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_n} = K(e_1, s_2, \ldots, s_n)$, $e_1 = X_1 + \cdots + X_n$

$$K[X_1, \ldots, X_n]^{(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_n} = K[e_1, s_2, \ldots, s_n]$$

Characteristic 2: conclusion (*Faugère, Huot, Joux, R., Vitse*)

Summation polynomial in characteristic 2 ($\lambda = 0, 1$)

- $f_{n+1}(x_1, \ldots, x_n, x_R) \in \mathbb{F}_{2^{kn}}[x_1, \ldots, x_n]^{D_n} = \mathbb{F}_{2^{kn}}[e_1, s_2 \ldots, s_n]$
- $f_{n+1}(x_1, \ldots, x_n, x_R) \in \mathbb{F}_{2^{kn}}[e_1^2, s_2^2 \ldots, s_{n-1}^2, s_n]$

Theorem

Under the same hypothesis $\mathcal{H}_2$ on $\mathcal{S}_{\mathfrak{S}_n}$, by using the action of T_2 the complexity for solving PDP is divided by $2^{\omega 2(n-1)}$

Practical results (Oakley 'Well-Known Groups' 3 over $\mathbb{F}_{2^{31\times 5}}$)

To obtain one relation

- Joux-Vitse $n-1$-method: ≈ 37 years
- This work: ≈ 5.5 hours

Outline

Iterative Construction

$$S_n(x_1, \ldots, x_n) = \mathrm{Res}_X(S_{n-k+1}(x_1, \ldots, x_{n-k}, X), S_{k+1}(x_{n-k+1}, \ldots, x_n, X))$$

$$k \in \{2, \ldots, n-2\}$$

$$\rightsquigarrow O(2^{n^2})$$

☞ In characteristic 2, rewrite it with smaller degrees!

Iterative Construction

$$S_n(x_1, \ldots, x_n) \in \mathbb{F}_{2^{kn}}[e_1^2, s_2^2 \ldots, s_{n-1}^2, s_n]$$

$s_i = e_i(X_1^2 + X_1, \ldots, X_n^2 + X_n)$

$$\mathrm{Res}_X\Big(\quad S^p_{n-k+1}\left(e^2_{1,n-k}, s^2_{2,n-k}, \ldots, s^2_{n-k-1,n-k}, s_{n-k,n-k}, X\right), \\ S^p_{k+1}\left(e^2_{1,k}, s^2_{2,k}, \ldots, s^2_{k-1,k}, s_{k,k}, X\right)\Big) \ .$$

$k \in \{2, \ldots, n-2\}$

$$\Omega : \begin{cases} e_1^2 &= e_{1,n-k}^2 + e_{1,k}^2 \\ s_2^2 &= s_{2,n-k}^2 + s_{2,k}^2 + \alpha_1\alpha_2 \\ s_3^2 &= s_{3,n-k}^2 + s_{3,k}^2 + \alpha_1 s_{2,k}^2 + \alpha_2 s_{2,n-k}^2 \\ s_4^2 &= s_{4,n-k}^2 + s_{4,k}^2 + \alpha_1 s_{3,k}^2 + \alpha_2 s_{3,n-k}^2 + s_{2,n-k}^2 s_{2,k}^2 \\ & \vdots \\ s_{n-2}^2 &= s_{n-k,n-k}^2 s_{k-2,k}^s + s_{n-k-1,n-k}^2 s_{k-1,k}^2 + s_{n-k-2,n-k}^2 s_{k,k}^2 \\ s_{n-1}^2 &= s_{n-k,n-k}^2 s_{k-1,k}^2 + s_{n-k-1,n-k}^2 s_{k,k}^2 \\ s_n &= s_{n-k,n-k} s_{k,k} \end{cases}$$

$\alpha_1 = e_{1,n-k}^2 + e_{1,n-k}$ and $\alpha_2 = e_{1,k}^2 + e_{1,k}$.

Iterative Construction

$$S_n(x_1, \ldots, x_n) \in \mathbb{F}_{2^{kn}}[e_1^2, s_2^2 \ldots, s_{n-1}^2, s_n]$$

$s_i = e_i(X_1^2 + X_1, \ldots, X_n^2 + X_n)$

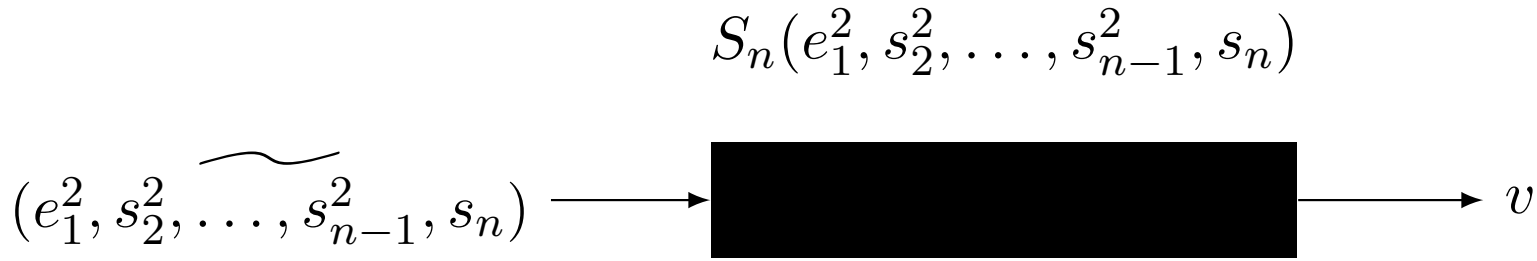
$$\mathrm{Res}_X\Big(\quad S^p_{n-k+1}\left(e^2_{1,n-k}, s^2_{2,n-k}, \ldots, s^2_{n-k-1,n-k}, s_{n-k,n-k}, X\right), \\ S^p_{k+1}\left(e^2_{1,k}, s^2_{2,k}, \ldots, s^2_{k-1,k}, s_{k,k}, X\right)\Big) \ .$$

$k \in \{2, \ldots, n-2\}$

- The change of var. Ω can be applied with a Grobner basis comp.
- On can obtain S_6 with this method
- We obtain S_7 by using some shortcuts (essentially by hand)

☞ The 8th Summation polynomial still intractable!

Sparse multivariate polynomial interpolation



Zippel's probabilistic algorithm

- Interpolation of dense univariate polynomials
- Iterative on the variables
- The evaluation step has to be very efficient ($O(nt2^{n-3})$ evaluations)

Sparse multivariate polynomial interpolation

$$S_n(e_1^2, s_2^2, \ldots, s_{n-1}^2, s_n)$$

$$(e_1^2, \widetilde{s_2^2, \ldots, s_{n-1}^2}, s_n) \longrightarrow \boxed{\mathrm{Res}_X\left(S_{n-k+1}^p, S_{k+1}^p\right)} \longrightarrow v$$

Zippel's probabilistic algorithm

- The evaluation step has to be very efficient ($O(nt2^{n-3})$ evaluations)

$$\Omega : \begin{cases} e_1^2 = e_{1,n-k}^2 + e_{1,k}^2 \\ s_2^2 = s_{2,n-k}^2 + s_{2,k}^2 + \alpha_1\alpha_2 \\ s_3^2 = s_{3,n-k}^2 + s_{3,k}^2 + \alpha_1 s_{2,k}^2 + \alpha_2 s_{2,n-k}^2 \\ s_4^2 = s_{4,n-k}^2 + s_{4,k}^2 + \alpha_1 s_{3,k}^2 + \alpha_2 s_{3,n-k}^2 + s_{2,n-k}^2 s_{2,k}^2 \\ \vdots \\ s_{n-2}^2 = s_{n-k,n-k}^2 s_{k-2,k}^s + s_{n-k-1,n-k}^2 s_{k-1,k}^2 + s_{n-k-2,n-k}^2 s_{k,k}^2 \\ s_{n-1}^2 = s_{n-k,n-k}^2 s_{k-1,k}^2 + s_{n-k-1,n-k}^2 s_{k,k}^2 \\ s_n = s_{n-k,n-k} s_{k,k} \end{cases}$$

$\alpha_1 = e_{1,n-k}^2 + e_{1,n-k}$ and $\alpha_2 = e_{1,k}^2 + e_{1,k}$.

Grobner basis comp. not enough efficient: 1.4sec. $\rightsquigarrow$ 5 years for S_8

Sparse multivariate polynomial interpol. using symmetry

$$S_n(e_1^2, s_2^2, \ldots, s_{n-1}^2, s_n)$$

$$(e_1^2, \widetilde{s_2^2, \ldots, s_{n-1}^2}, s_n) \longrightarrow \boxed{\mathrm{Res}_X\left(S^p_{n-k+1}, S^p_{k+1}\right)} \longrightarrow v$$

☞ $(\widetilde{s_1^2, \ldots, s_n^2})$ can be deduced from $(e_1^2, \widetilde{s_2^2, \ldots, s_{n-1}^2}, s_n)$

☞ The s_i^2 come from elem. symm. pol: $s_i^2 = e_i(x_1^4 + x_1^2, \ldots, x_n^4 + x_n^2)$

$$f_n(X) = X^n + \widetilde{s}_1^2 X^{n-1} + \cdots + \widetilde{s}_{n-1}^2 X + \widetilde{s}_n^2 = \prod_{i=1}^{n} \left(X + \left(\widetilde{x}_i^4 + \widetilde{x}_i^2\right)\right) .$$

$$f_n(X) = f_k(X) f_{n-k}(X)$$

☞ Evaluation points of S^p_{n-k+1}, S^p_{k+1} deduced from $f_k(x), f_{n-k}(X)$.

Sparse multivariate polynomial interpol. using symmetry

$$S_n(e_1^2, s_2^2, \ldots, s_{n-1}^2, s_n)$$

$$(e_1^2, \widetilde{s_2^2, \ldots, s_{n-1}^2}, s_n) \longrightarrow \mathrm{Res}_X\left(S^p_{n-k+1}, S^p_{k+1}\right) \longrightarrow v$$

Final computation with fast evaluation

Grobner basis comp. $\rightarrow$ factorization, 3 degree 2 pol. to solve (over $\mathbb{F}_{2^k}$)

✌ Using this fast evaluation we computed S_8 in ≈ 40.5h

Outline

Conclusion

☞ Here some introductory results are presented, more are given in our EC'14 paper:

Torsion points of small order

Faugère, Huot, Joux, R., Vitse EC'14

- Study more general projection (Diem's view point)
- Characterize the possible interesting torsion points
- Show how to use full 2-torsion in large char. (w/ experimental results)