Étude des systèmes polynomiaux intervenant dans le calcul d'indice pour la résolution du problème du logarithme discret sur les courbes

Jean-Charles Faugère[1] Pierrick Gaudry[2]
Louise Huot[1] Guénaël Renault[1]

1 : équipe SALSA, CNRS/INRIA/LIP6/UPMC
2 : équipe CARAMEL, CNRS/INRIA/LORIA

Journées "Codage et Cryptographie" 2011
5 avril 2011

Adaptation of index calculus (Gaudry//Diem)

Algorithm

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

1. Factor base : $\mathcal{F} = \{(x, y) \in E(\mathbb{F}_{q^n}) \mid x \in \mathbb{F}_q\}$
2. Compute relations :

$$[a_j]P \oplus [b_j]Q = P_1 \oplus \cdots \oplus P_n, \ P_i \in \mathcal{F}$$

   until having $\#\mathcal{F} + 1$ such relations $\left(p = \frac{1}{n!}\right)$
3. Linear algebra $\sum_j [\lambda_j \cdot a_j]P \oplus [\lambda_j \cdot b_j]Q = 0_{E(\mathbb{F}_{q^n})}$

Complexity

For n fixed, $\widetilde{O}(q^{2-\frac{2}{n}})$ *(Gaudry, pprint 2004 and JSC 2009 / Diem, ANTS 2006)*

Adaptation of index calculus (Gaudry//Diem)

Algorithm

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

1. Factor base : $\mathcal{F} = \{(x, y) \in E(\mathbb{F}_{q^n}) \mid x \in \mathbb{F}_q\}$
2. Compute relations :

$$[a_j]P \oplus [b_j]Q = P_1 \oplus \cdots \oplus P_n, \ P_i \in \mathcal{F}$$

   until having $\#\mathcal{F} + 1$ such relations $\left(p = \frac{1}{n!}\right)$
3. Linear algebra $\sum_j [\lambda_j \cdot a_j]P \oplus [\lambda_j \cdot b_j]Q = 0_{E(\mathbb{F}_{q^n})}$

Complexity

For n fixed, $\widetilde{O}(q^{2-\frac{2}{n}})$ *(Gaudry, pprint 2004 and JSC 2009 / Diem, ANTS 2006)*

Problem : point decomposition

Given

- $R \in E(\mathbb{F}_{q^n})$
- $\mathcal{F} = \{(x, y) \in E(\mathbb{F}_{q^n}) \mid x \in \mathbb{F}_q\} \subset E(\mathbb{F}_{q^n})$

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

Algebraic method

Modelling the problem as a polynomial system $\{g_1, \ldots, g_s\}$ and solve this system.

Related work

Joux, Vitse : eprint.iacr.org/2010/157

Use of hybrid approach (specialization of one variable)

- decrease the cost of solving system
- add an exhaustive search on $\mathbb{F}_q$

$\Longrightarrow$ limits the size of $\mathbb{F}_q$, $q \sim 2^{30}$

This work

- Decrease the cost of solving system in comparison to Gaudry//Diem method.
- No exhaustive search, complexity linear w.r.t. $\log(q)$.

$\Longrightarrow$ for n fixed, no limit on q

Solving polynomial systems

Let $\mathcal{S} = \{p_1 = 0, \ldots, p_\ell = 0\}$ where $p_i \in \mathbb{K}[x_1, \ldots, x_n]$,

Solving $\mathcal{S} \iff$ compute $\mathcal{V}_{\mathbb{K}}(\langle p_1, \ldots, p_\ell \rangle)$

Problem : How to compute $\mathcal{V}_{\mathbb{K}}(\langle p_1, \ldots, p_\ell \rangle)$?

Gröbner basis

Property

If $|\mathcal{V}_{\overline{\mathbb{K}}}| < \infty$, $s \geq n$ and $\mathcal{G}$ is a Gröbner basis of $\langle p_1, \ldots, p_\ell \rangle$ w.r.t. lexicographical order with $x_1 > \ldots > x_n$ then $\mathcal{G}$ has a **triangular form**

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

Solving polynomial systems

Let $\mathcal{S} = \{p_1 = 0, \ldots, p_\ell = 0\}$ where $p_i \in \mathbb{K}[x_1, \ldots, x_n]$,

$$\text{Solving } \mathcal{S} \iff \text{compute } \mathcal{V}_{\mathbb{K}}(\langle p_1, \ldots, p_\ell \rangle)$$

Problem : How to compute $\mathcal{V}_{\mathbb{K}}(\langle p_1, \ldots, p_\ell \rangle)$?
Solution : Compute a Gröbner basis w.r.t. lexicographical order of $\langle p_1, \ldots, p_\ell \rangle$.

Solving polynomial systems

Let $\mathcal{S} = \{p_1 = 0, \ldots, p_\ell = 0\}$ where $p_i \in \mathbb{K}[x_1, \ldots, x_n]$,

$$\text{Solving } \mathcal{S} \Longleftrightarrow \text{compute } \mathcal{V}_{\mathbb{K}}(\langle p_1, \ldots, p_\ell \rangle)$$

Problem : How to compute $\mathcal{V}_{\mathbb{K}}(\langle p_1, \ldots, p_\ell \rangle)$?
Solution : Compute a Gröbner basis w.r.t. lexicographical order of $\langle p_1, \ldots, p_\ell \rangle$.

Procedure

1. Compute GB DRL (F_4/F_5)
2. Compute GB LEX (FGLM + Issac 2011 J.C. Faugère/C. Mou)

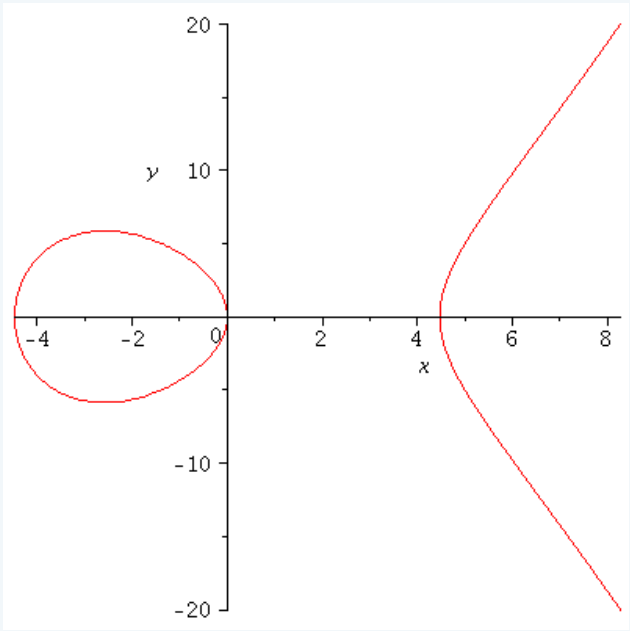
$$\rightsquigarrow O\left(n^{\omega \cdot d_{reg}} + n \cdot nbsol^{\omega}\right)$$

Curve representations

Weierstrass

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

$\forall P = (x, y) \in E, \ominus P = (x, -y)$.

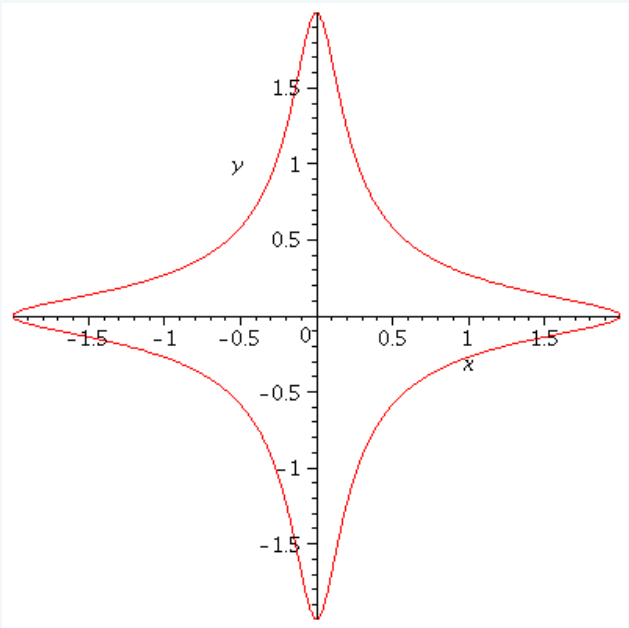


Edwards

(Edwards, Bulletin of the AMS 2007)

$$E_d : x^2 + y^2 = 1 + dx^2y^2$$

where $d \neq 0, 1$ and d nonsquare.
$\forall P = (x, y) \in E, \ominus P = (-x, y)$.



Contributions

Precise study of the Edwards (Jacobi intersections) representation

Use of symmetries

↓

Simplification of the algebraic modelling
of the point decomposition problem

↓

In practice : $\div 100$ solving time

$\rightsquigarrow$ action linked to the 2-torsion point

Summation polynomials in Weierstrass representation

Semaev, Technical report 2004

Projection of point decomposition problem

$$\langle f_m(x_1, \ldots, x_m) \rangle = \langle g_1, \ldots, g_s \rangle \cap \mathbb{F}_{q^n}[x_1, \ldots, x_m]$$

Let E be an elliptic curve defined over $\mathbb{K}$. For all $m \geq 2$ the m^{th} summation polynomial is defined by $\forall (x_1, \ldots, x_m) \in \overline{\mathbb{K}}^m$,

$$f_m(x_1, ..., x_m) = 0$$
$$\Leftrightarrow$$
$$\exists (y_1, ..., y_m) \in \overline{\mathbb{K}}^m \text{ s.t. } \forall i, P_i = (x_i, y_i) \in E \text{ and } P_1 \oplus \cdots \oplus P_m = 0_{E(\overline{\mathbb{K}})}$$

$\rightsquigarrow \forall m > 2, f_m$ is symmetric

Property

If E is defined by a Weierstrass equation then $\deg_{x_i}(f_m) = 2^{m-2}$.

Application of summation polynomials

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

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

where R is a fixed point in E.

Solution : Weil restriction on summation polynomial

$\mathbb{F}_{q^n}$: n dimensional $\mathbb{F}_q$-vectoriel space

$$(m = n+1) \quad f_{n+1}(x_1, \ldots, x_n, x_R) = 0_{\mathbb{F}_{q^n}} = \sum_{i=0}^{n-1} \varphi_i(x_1, \ldots, x_n) \cdot \omega^i$$

$$\Rightarrow \begin{cases} - & \mathcal{S} = \{\varphi_0, \ldots, \varphi_{n-1}\} \subset \mathbb{F}_q[x_1, \ldots, x_n] \\ - & n \text{ variables, } n \text{ equations of maximal degree } 2^{n(n-1)} \\ - & \text{solutions in } \mathbb{F}_q \end{cases}$$

System symmetrization

$f_{n+1}(x_1, \ldots, x_n, x_R)$ symmetric $\quad \Longrightarrow \quad \forall i = 0, .., n-1,\ \varphi_i$ symmetric

$\Longrightarrow \quad \mathcal{S} = \{\varphi_0, \ldots, \varphi_{n-1}\} \subset \mathbb{F}_q[x_1, \ldots, x_n]^{\mathfrak{S}_n}$

Theorem

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

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.

Corollary

$$\mathcal{S} = \langle \varphi_0, \ldots, \varphi_{n-1} \rangle \subset \mathbb{F}_q[x_1, \ldots, x_n]$$

$$\downarrow$$

change of variables $e_1, \ldots, e_n$

$$\downarrow$$

$$\mathcal{S}_{\mathfrak{S}_n} = \langle \psi_0, \ldots, \psi_{n-1} \rangle \subset \mathbb{F}_q[e_1, \ldots, e_n]$$

- $\mathcal{S}_{\mathfrak{S}_n} \subset \mathbb{F}_q[e_1, \ldots, e_n]$
- n variables
- n equations of maximal degree 2^{n-1}
- solutions in $\mathbb{F}_q$

Summation polynomials for Edwards curves

For all $P = (x, y) \in E_d$ we have $\ominus P = (-x, y)$.

$$\left| \begin{array}{l} P_1 \oplus \cdots \oplus P_m = 0_{E_d} \\ f_m(x_1, \ldots, x_m) = 0_{\mathbb{F}_{q^n}} \end{array} \right. \Longrightarrow \left| \begin{array}{l} (\ominus P_1) \oplus \cdots \oplus (\ominus P_m) = 0_{E_d} \\ f_m(-x_1, \ldots, -x_m) = 0_{\mathbb{F}_{q^n}} \end{array} \right.$$

Problem

$$\Rightarrow \deg_{x_i}(f_m) = (2^{m-2})^2$$

Solution : $x \leftrightarrow y$

Summation polynomials for Edwards curves : $f_{n+1}(y_1, \ldots, y_n, y_R)$.
Algorithm adaptation : $\mathcal{F} = \{(x, y) \in E_d(\mathbb{F}_{q^n}) \mid y \in \mathbb{F}_q\}$

Semaev modelling: Weierstrass vs. Edwards

Weierstrass

LEX Gröbner Basis of $\mathcal{S}_{\mathfrak{S}_n}$:

$$\begin{cases} e_1 + h_1(e_n) \\ e_2 + h_2(e_n) \\ \vdots \\ e_{n-2} + h_{n-2}(e_n) \\ e_{n-1} + h_{n-1}(e_n) \\ h_n(e_n) \end{cases}$$

- $\deg(h_n) = 2^{n(n-1)}$
- $|\mathcal{V}_{\overline{\mathbb{K}}}| = 2^{n(n-1)}$

Semaev modelling: Weierstrass vs. Edwards

Weierstrass

LEX Gröbner Basis of $\mathcal{S}_{\mathfrak{S}_n}$:

$$\begin{cases} e_1 + h_1(e_n) \\ e_2 + h_2(e_n) \\ \vdots \\ e_{n-2} + h_{n-2}(e_n) \\ e_{n-1} + h_{n-1}(e_n) \\ h_n(e_n) \end{cases}$$

- $\deg(h_n) = 2^{n(n-1)}$
- $|\mathcal{V}_{\overline{\mathbb{K}}}| = 2^{n(n-1)}$

Edwards

LEX Gröbner Basis of $\mathcal{S}_{\mathfrak{S}_n}$:

$$\begin{cases} e_1 + h_1(e_{n-1}, e_n) \\ e_2 + h_2(e_{n-1}, e_n) \\ \vdots \\ e_{n-2} + h_{n-2}(e_{n-1}, e_n) \\ h_{n-1}(e_{n-1}, e_n) \\ h_n(e_n) \end{cases}$$

- $\deg(h_n) = 2^{(n-1)^2}$
- $\deg_{e_{n-1}}(h_{n-1}) = 2^{n-1}$
- $|\mathcal{V}_{\overline{\mathbb{K}}}| = 2^{n(n-1)}$

Group action

Definition

- $\phi : G \times V \longrightarrow V$
- $\forall v \in V,\ \phi(\mathsf{Id}(G), v) = v$
- $\forall g, g' \in G,\ \forall v \in V,\ \phi(g, \phi(g', v)) = \phi(gg', v)$

Action on the points (geometry)

Group action

Definition

- $\phi : G \times V \longrightarrow V$
- $\forall v \in V,\ \phi(\mathsf{Id}(G), v) = v$
- $\forall g, g' \in G,\ \forall v \in V,\ \phi(g, \phi(g', v)) = \phi(gg', v)$

Action on the points (geometry)

$$P_1 \oplus \cdots \oplus P_n = R \iff P_2 \oplus P_1 \oplus P_3 \oplus \cdots \oplus P_n = R$$

Group action

Definition

- $\phi : G \times V \longrightarrow V$
- $\forall v \in V,\ \phi(\mathsf{Id}(G), v) = v$
- $\forall g, g' \in G,\ \forall v \in V,\ \phi(g, \phi(g', v)) = \phi(gg', v)$

Action on the points (geometry)

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

Group action

Definition

$E_d : x^2 + y^2 = 1 + dx^2y^2$ has a 2-torsion point $T_2 = (0, -1)$ i.e. $[2]T_2 = 0_{E_d}$.

Property

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

Action on the points (geometry)

Group action

Definition

$E_d : x^2 + y^2 = 1 + dx^2y^2$ has a 2-torsion point $T_2 = (0, -1)$ i.e. $[2]T_2 = 0_{E_d}$.

Property

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

Action on the points (geometry)

$$P_1 \oplus \cdots \oplus P_n = R \iff (P_1 \oplus T_2) \oplus (P_2 \oplus T_2) \oplus P_3 \oplus \cdots \oplus P_n = R$$

For any combination of an even number of T_2.

$$\rightsquigarrow \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} = 2^{n-1} \text{ solutions}$$

Group action

Definition

$E_d : x^2 + y^2 = 1 + dx^2y^2$ has a 2-torsion point $T_2 = (0, -1)$ i.e. $[2]T_2 = 0_{E_d}$.

Property

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

Action on the points (geometry)

$$P_1 \oplus \cdots \oplus P_n = R \iff (P_1 \oplus T_2) \oplus (P_2 \oplus T_2) \oplus P_3 \oplus \cdots \oplus P_n = R$$

$$(y_1, \ldots, y_n) \in V_R \iff (-y_1, -y_2, y_3, \ldots, y_n) \in V_R$$

For any combination of an even number of T_2.

$$\rightsquigarrow \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} = 2^{n-1} \text{ solutions}$$

The Coxeter group D_n

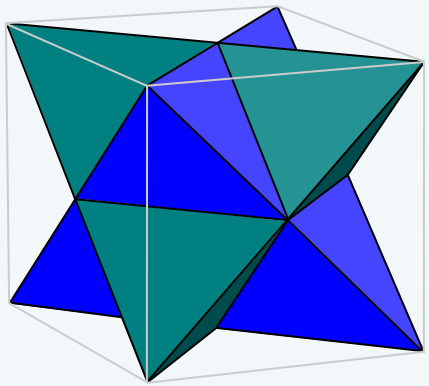
Definition

D_n is the symmetry group of the n-demihypercube.

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

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

Example : $n = 3$



D_3 is the symmetry group of the 3-demicube.

The invariant subring of D_n

Property

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

$$\Longrightarrow \varphi_i(y_1, \ldots, y_n) \in \mathbb{F}_q[y_1, \ldots, y_n]^{D_n} \text{ for all } i = 0, \ldots, n-1$$

Theorem

$$\mathbb{F}_q[y_1, \ldots, y_n]^{D_n} = \mathbb{F}_q[p_2, \ldots, p_{2(n-1)}, e_n]$$

- $p_i = \sum_{k=1}^{n} y_k^i$ the i^{th} power sum
- $e_n = \prod_{k=1}^{n} y_k$ the n^{th} elementary symmetric polynomial.

The invariant subring

Corollary

$$\mathcal{S} = \langle \varphi_0, \ldots, \varphi_{n-1} \rangle \subset \mathbb{F}_q[y_1, \ldots, y_n]$$
$$\downarrow$$
change of variables $p_2, \ldots, p_{2(n-1)}, e_n$
$$\downarrow$$
$$\mathcal{S}_{D_n} = \langle \mu_0, \ldots, \mu_{n-1} \rangle \subset \mathbb{F}_q[p_2, \ldots, p_{2(n-1)}, e_n]$$

where $\sum_{i=0}^{n-1} \varphi_i(y_1, \ldots, y_n) \cdot \omega^i = f_{n+1}(y_1, \ldots, y_n, y_R)$

$\mathcal{S}_{D_n}$: new system such that $\#\mathcal{V}(\mathcal{S}_{D_n}) = \#V_R/\#D_n = \#\mathcal{V}(\mathcal{S}_{\mathfrak{S}_n})/2^{n-1}$.

Complexity of **FGLM** $\div 2^{\omega(n-1)}$ with action of T_2.

Semaev modelling: Weierstrass vs. Edwards

Weierstrass

LEX Gröbner Basis of $\mathcal{S}_{\mathfrak{S}_n}$:

$$\begin{cases} e_1 + h_1(e_n) \\ e_2 + h_2(e_n) \\ \vdots \\ e_{n-1} + h_{n-1}(e_n) \\ h_n(e_n) \end{cases}$$

- $\deg(h_n) = 2^{n(n-1)}$
- $|\mathcal{V}_{\overline{\mathbb{K}}}| = 2^{n(n-1)}$

Edwards

LEX Gröbner Basis of $\mathcal{S}_{D_n}$:

$$\begin{cases} p_2 + h_1(e_n) \\ p_4 + h_2(e_n) \\ \vdots \\ p_{2(n-1)} + h_{n-1}(e_n) \\ h_n(e_n) \end{cases}$$

- $\deg(h_n) = 2^{(n-1)^2}$
- $|\mathcal{V}_{\overline{\mathbb{K}}}| = 2^{(n-1)^2}$

Some practical results

Magma (2.16–10) implementation (Intel Xeon 2.93 GHz with 120GB RAM)

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

n		System	DRL	LEX		Total
		Deg	Time (s)	Deg	Time (s)	time (s)
4	W. sym	8	6	4096	460	466
	E. Sym	8	0	518	188	188
	E. D_n	12	0	512	3	3
5 fgb	W. sym	16	∞			
	E. Sym	16	∞			
	E. D_n	32	10^5	65536	10^5	$2 \cdot 10^5$

- $n = 4$

$\#\mathbb{F}_q$ (bits)		32	64	128	160
Total time (s)	W. sym	7049	6490	7446	6559
	E. sym	1499	1511	1657	1534
	E. D_n	52	57	65	81

Conclusion

Summary

- Edwards + Jacobi Intersections : **action of 2-torsion point**
- New change of variables $\longleftarrow$ symmetric group + 2-torsion point
- Practical improvements
  - ▷ solving time $\div 100$
  - ▷ $n = 5$ solved
  - ▷ complexity of point decomposition problem linear w.r.t. $\log(q)$

Perspectives

- 4-torsion point of Jacobi Intersections curves
- Genus > 1