Summation polynomials and symmetries for the ECDLP over extension fields

Vanessa VITSE
Joint work with Faugère, Huot, Joux and Renault

Université Joseph Fourier – Grenoble

Background

The Elliptic Curve Discrete Log Problem

E elliptic curve defined over finite field $\mathbb{F}_q$, and $P, Q \in E(\mathbb{F}_q)$.

$$\text{Goal (ECDLP) : compute } x \text{ s.t. } Q = [x]P$$

- If $\mathbb{F}_q$ **prime field**: no known non-generic algorithms in general.
- If $\mathbb{F}_q = \mathbb{F}_{p^n}$ **extension field**: decomposition index calculus (Gaudry/Diem).

Decomposition index calculus

Outline of the attack:

1. Choose a **factor base** $\mathcal{F} \subset E(\mathbb{F}_{q^n})$.
2. Relation search step: look for **decompositions** of the form

$$[a]P + [b]Q = P_1 + \cdots + P_n, \quad P_i \in \mathcal{F}$$

3. Linear algebra step: once $\approx |\mathcal{F}|$ relations are computed, use sparse matrix algorithms to extract discrete log of Q.

Decomposition index calculus

Outline of the attack:

1. Choose a **factor base** $\mathcal{F} \subset E(\mathbb{F}_{q^n})$.
2. Relation search step: look for **decompositions** of the form

$$[a]P + [b]Q = P_1 + \cdots + P_n, \quad P_i \in \mathcal{F}$$

3. Linear algebra step: once $\approx |\mathcal{F}|$ relations are computed, use sparse matrix algorithms to extract discrete log of Q.

Made possible by the **Weil restriction** structure:
define $\mathcal{F}$ as algebraic curve in E seen as a dim. n abelian variety over $\mathbb{F}_q$.

Gaudry/Diem's decomposition

- Standard choice is $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}$

Gaudry/Diem's decomposition

- Standard choice is $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}$
- Use Semaev polynomials:

Semaev summation polynomials

For all $k \geq 2$, there exists $S_k \in \mathbb{F}_{q^n}[X_1, \ldots, X_k]$ s.t.

$$S_k(x_1, \ldots, x_k) = 0 \iff \exists P_i \in E(\overline{\mathbb{F}_q}), x(P_i) = x_i \text{ and } \sum_i P_i = \mathcal{O}$$

Gaudry/Diem's decomposition

- Standard choice is $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}$
- Use Semaev polynomials:

Semaev summation polynomials

For all $k \geq 2$, there exists $S_k \in \mathbb{F}_{q^n}[X_1, \ldots, X_k]$ s.t.

$$S_k(x_1, \ldots, x_k) = 0 \iff \exists P_i \in E(\overline{\mathbb{F}_q}), x(P_i) = x_i \text{ and } \sum_i P_i = \mathcal{O}$$

degree 2^{k-2} in each var. $\rightarrow$ hard to compute for $k \geq 5$

Gaudry/Diem's decomposition

- Standard choice is $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}$
- Use Semaev polynomials:

Semaev summation polynomials

For all $k \geq 2$, there exists $S_k \in \mathbb{F}_{q^n}[X_1, \ldots, X_k]$ s.t.

$$S_k(x_1, \ldots, x_k) = 0 \Longleftrightarrow \exists P_i \in E(\overline{\mathbb{F}_q}), x(P_i) = x_i \text{ and } \sum_i P_i = \mathcal{O}$$

degree 2^{k-2} in each var. $\rightarrow$ hard to compute for $k \geq 5$

- Decomposition try for $R = [a]P + [b]Q$: solve $S_{n+1}(x_1, \ldots, x_n, x(R)) = 0$ with $x_i \in \mathbb{F}_q$

  Restriction of scalar $\rightsquigarrow$ resolution of multivariate polynomial system with n var./eqn., total degree $n\,2^{n-2}$.

Gaudry/Diem's decomposition

- Standard choice is $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}$
- Use Semaev polynomials:

Semaev summation polynomials

For all $k \geq 2$, there exists $S_k \in \mathbb{F}_{q^n}[X_1, \ldots, X_k]$ s.t.

$$S_k(x_1, \ldots, x_k) = 0 \iff \exists P_i \in E(\overline{\mathbb{F}_q}), x(P_i) = x_i \text{ and } \sum_i P_i = \mathcal{O}$$

degree 2^{k-2} in each var. $\rightarrow$ hard to compute for $k \geq 5$

- Decomposition try for $R = [a]P + [b]Q$: solve $S_{n+1}(x_1, \ldots, x_n, x(R)) = 0$ with $x_i \in \mathbb{F}_q$

  Restriction of scalar $\rightsquigarrow$ resolution of multivariate polynomial system with n var./eqn., total degree $n\,2^{n-2}$. **This is the hardest part.**

Natural improvements

- Factor base $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}$ is **invariant** by $-$:

$$P \in \mathcal{F} \Leftrightarrow -P \in \mathcal{F}$$

$\rightarrow$ possible to divide size of factor base by 2 by considering decompositions of the form $R = \pm P_1 \cdots \pm P_n$
$\rightarrow$ less relations needed and faster linear algebra

Natural improvements

- Factor base $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}$ is **invariant** by $-$:

  $$P \in \mathcal{F} \Leftrightarrow -P \in \mathcal{F}$$

  $\rightarrow$ possible to divide size of factor base by 2 by considering decompositions of the form $R = \pm P_1 \cdots \pm P_n$
  $\rightarrow$ less relations needed and faster linear algebra

- Semaev polynomials are **symmetric** (in the usual sense)

  $\rightarrow$ expression in terms of elementary symmetric polynomials $e_1 = X_1 + \cdots + X_n, \ldots, e_n = X_1 \ldots X_n$ speeds up computation of polynomials and resolution of systems

Natural improvements

- Factor base $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}$ is **invariant** by $-$:

$$P \in \mathcal{F} \Leftrightarrow -P \in \mathcal{F}$$

$\rightarrow$ possible to divide size of factor base by 2 by considering decompositions of the form $R = \pm P_1 \cdots \pm P_n$
$\rightarrow$ less relations needed and faster linear algebra

- Semaev polynomials are **symmetric** (in the usual sense)

$\rightarrow$ expression in terms of elementary symmetric polynomials $e_1 = X_1 + \cdots + X_n, \ldots, e_n = X_1 \ldots X_n$ speeds up computation of polynomials and resolution of systems

Computation of decompositions still slow if $n \leq 4$, intractable if $n \geq 5$

Our contribution

Main idea

Replace x by arbitrary rational map $\varphi : E \to \mathbb{F}_{q^n}$ in definition of factor base:

$$\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : \varphi(P) \in \mathbb{F}_q\}$$

Implies ability to define and compute associated summation polynomials.

Useful generalization?

Our contribution

Main idea

Replace x by arbitrary rational map $\varphi : E \to \mathbb{F}_{q^n}$ in definition of factor base:

$$\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : \varphi(P) \in \mathbb{F}_q\}$$

Implies ability to define and compute associated summation polynomials.

Useful generalization? **Yes!**

Our contribution

Main idea

Replace x by arbitrary rational map $\varphi : E \to \mathbb{F}_{q^n}$ in definition of factor base:

$$\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : \varphi(P) \in \mathbb{F}_q\}$$

Implies ability to define and compute associated summation polynomials.

Useful generalization? **Yes!**

If φ well-chosen:

- $\mathcal{F}$ can have more invariance properties $\to$ further reduction of its size
- associated summation polynomial have more symmetries $\to$ easier to compute and faster decompositions

Summation polynomials

Theorem

For any rational map $\varphi : E \to \mathbb{F}_{q^n}$ and $k \geq 3$, there exists a unique monic $P_{\varphi,k} \in \mathbb{F}_{q^n}[X_1, \ldots, X_k]$, irreducible, symmetric, s.t.

$$P_{\varphi,k}(a_1, \ldots, a_k) = 0 \iff \exists P_i \in E(\overline{\mathbb{F}_q}), \varphi(P_i) = a_i \text{ and } \sum_i P_i = \mathcal{O}$$

Summation polynomials

Theorem

For any rational map $\varphi : E \to \mathbb{F}_{q^n}$ *and* $k \geq 3$*, there exists a unique monic* $P_{\varphi,k} \in \mathbb{F}_{q^n}[X_1, \ldots, X_k]$*, irreducible, symmetric, s.t.*

$$P_{\varphi,k}(a_1, \ldots, a_k) = 0 \iff \exists P_i \in E(\overline{\mathbb{F}_q}), \varphi(P_i) = a_i \text{ and } \sum_i P_i = \mathcal{O}$$

$\deg_{X_i} P_{\varphi,k}$ proportional to $(\deg \varphi)^k$ in general, and also for all interesting cases so far

$\rightarrow$ computation tractable only if $\deg \varphi$ and k small.

Computation of summation polynomials

First method: Riemann-Roch

Observation

$P_1 + \cdots + P_k = \mathcal{O} \Leftrightarrow \exists f \in \bar{\mathbb{F}}_q(C)$ s.t. $\mathrm{div}(f) = (P_1) + \cdots + (P_k) - k(\mathcal{O})$

Function f in Riemann-Roch space $\mathcal{L}(k(\mathcal{O}))$.

Computation of summation polynomials

First method: Riemann-Roch

Observation

$P_1 + \cdots + P_k = \mathcal{O} \Leftrightarrow \exists f \in \bar{\mathbb{F}}_q(C)$ s.t. $\mathrm{div}(f) = (P_1) + \cdots + (P_k) - k(\mathcal{O})$
Function f in Riemann-Roch space $\mathcal{L}(k(\mathcal{O}))$.

1. Write equation of E in terms of φ and a 2nd var. w (usually x or y)
2. Compute basis of $\mathcal{L}(k(\mathcal{O})) = \langle 1, f_2(\varphi, w), \ldots, f_k(\varphi, w)\rangle$ and consider $f = f_k(\varphi, w) + \lambda_{k-1} f_{k-1}(\varphi, w) + \cdots + \lambda_1$

Computation of summation polynomials

First method: Riemann-Roch

Observation

$P_1 + \cdots + P_k = \mathcal{O} \Leftrightarrow \exists f \in \bar{\mathbb{F}}_q(C)$ s.t. $\mathrm{div}(f) = (P_1) + \cdots + (P_k) - k(\mathcal{O})$

Function f in Riemann-Roch space $\mathcal{L}(k(\mathcal{O}))$.

1. Write equation of E in terms of φ and a 2nd var. w (usually x or y)
2. Compute basis of $\mathcal{L}(k(\mathcal{O})) = \langle 1, f_2(\varphi, w), \ldots, f_k(\varphi, w)\rangle$ and consider $f = f_k(\varphi, w) + \lambda_{k-1} f_{k-1}(\varphi, w) + \cdots + \lambda_1$
3. Resultant of f with equation of E wrt. w gives degree k polynomial F in $\mathbb{F}_{q^n}[\lambda_1, \ldots, \lambda_{k-1}][\varphi]$

Computation of summation polynomials

First method: Riemann-Roch

Observation

$P_1 + \cdots + P_k = \mathcal{O} \Leftrightarrow \exists f \in \bar{\mathbb{F}}_q(C)$ s.t. $\mathrm{div}(f) = (P_1) + \cdots + (P_k) - k(\mathcal{O})$
Function f in Riemann-Roch space $\mathcal{L}(k(\mathcal{O}))$.

1. Write equation of E in terms of φ and a 2nd var. w (usually x or y)
2. Compute basis of $\mathcal{L}(k(\mathcal{O})) = \langle 1, f_2(\varphi, w), \ldots, f_k(\varphi, w) \rangle$ and consider $f = f_k(\varphi, w) + \lambda_{k-1} f_{k-1}(\varphi, w) + \cdots + \lambda_1$
3. Resultant of f with equation of E wrt. w gives degree k polynomial F in $\mathbb{F}_{q^n}[\lambda_1, \ldots, \lambda_{k-1}][\varphi]$

Steps 2-3 similar to Nagao's method for higher genus decomposition attacks

Computation of summation polynomials

First method: Riemann-Roch

Observation

$P_1 + \cdots + P_k = \mathcal{O} \Leftrightarrow \exists f \in \bar{\mathbb{F}}_q(C)$ s.t. $\mathrm{div}(f) = (P_1) + \cdots + (P_k) - k(\mathcal{O})$
Function f in Riemann-Roch space $\mathcal{L}(k(\mathcal{O}))$.

1. Write equation of E in terms of φ and a 2nd var. w (usually x or y)
2. Compute basis of $\mathcal{L}(k(\mathcal{O})) = \langle 1, f_2(\varphi, w), \ldots, f_k(\varphi, w)\rangle$ and consider $f = f_k(\varphi, w) + \lambda_{k-1} f_{k-1}(\varphi, w) + \cdots + \lambda_1$
3. Resultant of f with equation of E wrt. w gives degree k polynomial F in $\mathbb{F}_{q^n}[\lambda_1, \ldots, \lambda_{k-1}][\varphi]$
4. Equate coeff. of F with elementary sym. polynomials $e_1, \ldots, e_k$ and compute Gröbner basis of these k equations wrt. elimination order.
5. The Gröbner basis contains $P_{\varphi,k}$ symmetrized, i.e. expressed in terms of $e_1, \ldots, e_k$

Computation of summation polynomials

Second method: induction and resultants

Observation

$$P_1 + \cdots + P_k = \mathcal{O} \Leftrightarrow \exists Q \in E \text{ s.t. } \begin{cases} P_1 + \cdots + P_j + Q = \mathcal{O} \\ P_{j+1} + \cdots + P_k - Q = \mathcal{O} \end{cases}$$

Computation of summation polynomials

Second method: induction and resultants

Observation

$$P_1 + \cdots + P_k = \mathcal{O} \Leftrightarrow \exists Q \in E \text{ s.t. } \begin{cases} P_1 + \cdots + P_j + Q = \mathcal{O} \\ P_{j+1} + \cdots + P_k - Q = \mathcal{O} \end{cases}$$

Assume for simplicity $\varphi(P) = \varphi(-P)\ \forall P \in E$. Then

$$P_1 + \cdots + P_k = \mathcal{O}$$

$$\Updownarrow$$

$$P_{\varphi,j+1}(\varphi(P_1), \ldots, \varphi(P_j), X) \text{ and } P_{\varphi,k-j+1}(\varphi(P_{j+1}), \ldots, \varphi(P_k), X)$$

have a common root

Computation of summation polynomials

Second method: induction and resultants

Observation

$$P_1 + \cdots + P_k = \mathcal{O} \Leftrightarrow \exists Q \in E \text{ s.t. } \begin{cases} P_1 + \cdots + P_j + Q = \mathcal{O} \\ P_{j+1} + \cdots + P_k - Q = \mathcal{O} \end{cases}$$

Assume for simplicity $\varphi(P) = \varphi(-P)\ \forall P \in E$. Then

$$P_1 + \cdots + P_k = \mathcal{O}$$
$$\Updownarrow$$
$$P_{\varphi,j+1}(\varphi(P_1), \ldots, \varphi(P_j), X) \text{ and } P_{\varphi,k-j+1}(\varphi(P_{j+1}), \ldots, \varphi(P_k), X)$$
have a common root

$$P_{\varphi,k}(X_1, \ldots, X_k) = \mathrm{Res}(P_{\varphi,j+1}(X_1, \ldots, X_j, X), P_{\varphi,k-j+1}(X_{j+1}, \ldots, X_k, X))$$

Computation by induction still requires to know $P_{\varphi,3}$.

Action of small torsion points

Fact: many elliptic curves only have *near-prime* cardinality
$\rightarrow$ admit small order points. Use them to speed DLP!

Action of small torsion points

Fact: many elliptic curves only have *near-prime* cardinality
$\rightarrow$ admit small order points. Use them to speed DLP!

Let $T \in E(\mathbb{F}_{q^n})$ point of small order ℓ, $\tau_T : E \rightarrow E$ translation-by-T map.
Suppose $\mathcal{F}$ invariant by τ_T, i.e. $P \in \mathcal{F}$ iff $P + T \in \mathcal{F}$. Then:

Action of small torsion points

Fact: many elliptic curves only have *near-prime* cardinality
$\rightarrow$ admit small order points. Use them to speed DLP!

Let $T \in E(\mathbb{F}_{q^n})$ point of small order ℓ, $\tau_T : E \rightarrow E$ translation-by-T map.
Suppose $\mathcal{F}$ invariant by τ_T, i.e. $P \in \mathcal{F}$ iff $P + T \in \mathcal{F}$. Then:

- Each decomposition $R = P_1 + \cdots + P_n$ yields many more:

$$\begin{aligned} R &= (P_1 + T) + (P_2 + [\ell - 1]T) + \cdots + P_n \\ &= (P_1 + T) + (P_2 + T) + (P_3 + [\ell - 2]T) + \cdots + P_n \\ &= \ldots \end{aligned}$$

Action of small torsion points

Fact: many elliptic curves only have *near-prime* cardinality
$\rightarrow$ admit small order points. Use them to speed DLP!

Let $T \in E(\mathbb{F}_{q^n})$ point of small order ℓ, $\tau_T : E \rightarrow E$ translation-by-T map.
Suppose $\mathcal{F}$ invariant by τ_T, i.e. $P \in \mathcal{F}$ iff $P + T \in \mathcal{F}$. Then:

- Each decomposition $R = P_1 + \cdots + P_n$ yields many more:

$$\begin{aligned} R &= (P_1 + T) + (P_2 + [\ell - 1]T) + \cdots + P_n \\ &= (P_1 + T) + (P_2 + T) + (P_3 + [\ell - 2]T) + \cdots + P_n \\ &= \ldots \end{aligned}$$

- Size of $\mathcal{F}$ can be effectively divided by ℓ

Equivariant morphisms

Goal: factor base $\mathcal{F} = \{P : \varphi(P) \in \mathbb{F}_q\}$ invariant by τ_T, $T \in E[\ell]$

First idea

Look for *invariant* $\varphi : E \to \mathbb{F}_{q^n}$, i.e.

$$\varphi(P + T) = \varphi(P)\ \forall P \in E.$$

Equivariant morphisms

Goal: factor base $\mathcal{F} = \{P : \varphi(P) \in \mathbb{F}_q\}$ invariant by τ_T, $T \in E[\ell]$

First idea

Look for *invariant* $\varphi : E \to \mathbb{F}_{q^n}$, i.e.

$$\varphi(P + T) = \varphi(P)\ \forall P \in E.$$

But then φ factorizes through quotient isogeny $E \to E/_{\langle T \rangle}$:

$$E \xrightarrow{\ \pi\ } E/_{\langle T \rangle} \xrightarrow{\ \varphi'\ } \mathbb{F}_{q^n}, \qquad \varphi = \varphi' \circ \pi : E \to \mathbb{F}_{q^n}$$

Equivalent decompositions on E with φ and on $E_{/\langle T \rangle}$ with φ'!

Equivariant morphisms

Goal: factor base $\mathcal{F} = \{P : \varphi(P) \in \mathbb{F}_q\}$ invariant by τ_T, $T \in E[\ell]$

~~First idea~~ BAD IDEA

Look for *invariant* $\varphi : E \to \mathbb{F}_{q^n}$, i.e.

$$\varphi(P + T) = \varphi(P) \; \forall P \in E.$$

But then φ factorizes through quotient isogeny $E \to E/_{\langle T \rangle}$:

$$E \xrightarrow{\pi} E/_{\langle T \rangle} \xrightarrow{\varphi'} \mathbb{F}_{q^n}, \qquad \varphi = \varphi' \circ \pi : E \to \mathbb{F}_{q^n}$$

Equivalent decompositions on E with φ and on $E_{/\langle T \rangle}$ with φ'!

Equivariant morphisms

Goal: factor base $\mathcal{F} = \{P : \varphi(P) \in \mathbb{F}_q\}$ invariant by τ_T, $T \in E[\ell]$

Better idea

Look for *equivariant* $\varphi : E \to \mathbb{F}_{q^n}$, i.e. $\exists$ rational map $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ s.t.

$$\varphi(P + T) = f(\varphi(P)) \; \forall P \in E.$$

Equivariant morphisms

Goal: factor base $\mathcal{F} = \{P : \varphi(P) \in \mathbb{F}_q\}$ invariant by τ_T, $T \in E[\ell]$

Better idea

Look for *equivariant* $\varphi : E \to \mathbb{F}_{q^n}$, i.e. $\exists$ rational map $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ s.t.

$$\varphi(P+T) = f(\varphi(P)) \; \forall P \in E.$$

- So $f^{(\ell)} = f \circ \cdots \circ f = Id$
- Also invariance of $\mathcal{F}$ requires $\mathbb{F}_q$ stable by f

$\Rightarrow$ f element of $PGL(2, \mathbb{F}_q)$ of exact order ℓ

Existence

Theorem

The torsion subgroups wrt. which a rational map $\varphi : E \to \mathbb{F}_{q^n}$ can be equivariant but not invariant are:

- $E[2]$
- $\langle T \rangle \subset E[\ell]$, *with either*
  - $\ell = char(\mathbb{F}_q)$
  - $\ell | q - 1$
  - $\ell | q + 1$

In all cases $\deg(\varphi)$ *is a multiple of* ℓ.

Also possible equivariance (or invariance for $\ell = 2$) wrt. $[-1]$ map $P \mapsto -P$

Two-torsion in char 2: morphism

$E : y^2 + xy = x^3 + ax^2 + b$ ordinary elliptic curve over binary field $\mathbb{F}_{q^n}$.
Non-trivial 2-torsion point is $T_2 = (0, b^{1/2})$.

Two-torsion in char 2: morphism

$E : y^2 + xy = x^3 + ax^2 + b$ ordinary elliptic curve over binary field $\mathbb{F}_{q^n}$.
Non-trivial 2-torsion point is $T_2 = (0, b^{1/2})$.

Proposition

Let $\varphi : E \to \mathbb{F}_{q^n},\ (x, y) \mapsto \dfrac{b^{1/4}}{x + b^{1/4}}$. *Then* $\forall P \in E$,

- $\varphi(P + T_2) = \varphi(P) + 1$
- $\varphi(-P) = \varphi(P)$

Two-torsion in char 2: morphism

$E : y^2 + xy = x^3 + ax^2 + b$ ordinary elliptic curve over binary field $\mathbb{F}_{q^n}$.
Non-trivial 2-torsion point is $T_2 = (0, b^{1/2})$.

Proposition

Let $\varphi : E \to \mathbb{F}_{q^n},\ (x, y) \mapsto \dfrac{b^{1/4}}{x + b^{1/4}}$. *Then* $\forall P \in E$,

- $\varphi(P + T_2) = \varphi(P) + 1$
- $\varphi(-P) = \varphi(P)$

Factor base can be effectively divided by 4 $\to \#\mathcal{F} \approx q/4$

Two-torsion in char 2: summation polynomials

Since $P_1 + \cdots + P_k = (P_1 + T_2) + (P_2 + T_2) + P_3 + \cdots + P_k = \ldots,$
we have $P_{\varphi,k}(X_1, \ldots, X_k) = P_{\varphi,k}(X_1 + 1, X_2 + 1, X_3, \ldots, X_k) = \ldots$

$\rightarrow$ invariant if even number of $+1$ added.

Two-torsion in char 2: summation polynomials

Since $P_1 + \cdots + P_k = (P_1 + T_2) + (P_2 + T_2) + P_3 + \cdots + P_k = \ldots$,
we have $P_{\varphi,k}(X_1, \ldots, X_k) = P_{\varphi,k}(X_1 + 1, X_2 + 1, X_3, \ldots, X_k) = \ldots$

$\rightarrow$ invariant if even number of $+1$ added.

Proposition

- *$P_{\varphi,k}$ invariant under affine action of the group $G_2 = (\mathbb{Z}/2\mathbb{Z})^{k-1} \rtimes \mathfrak{S}_k$.*
- *Invariant ring $\mathbb{F}_{q^n}[X_1, \ldots, X_k]^{G_2}$ free algebra, generated by*

$$\begin{aligned} e_1 &= X_1 + \cdots + X_k \\ s_2 &= Y_1 Y_2 + \cdots + Y_{k-1} Y_k \\ &\vdots \\ s_k &= Y_1 \ldots Y_k \end{aligned}$$

where $Y_i = X_i^2 + X_i$.

Two-torsion in char 2: results (1)

Writing down $P_{\varphi,k}$ in terms of invariant generators $e_1, s_2, \ldots, s_k$ makes a **huge** difference:

k		3	4	5	6	7	8
Semaev polynomials	nb of monomials	3	6	39	638	–	–
	timings	0 s	0 s	26 s	725 s	×	×
$P_{\varphi,k}$	nb of monomials	2	3	9	50	2 247	470 369
	timings	0 s	0 s	0 s	1 s	383 s	40.5 h

Computations for $k = 4$ to 7 in two steps:

1. take resultant of partially symmetrized summation polynomials
2. express resultant in terms of invariant generators using elimination (Gröbner basis)

Two-torsion in char 2: results (1)

Writing down $P_{\varphi,k}$ in terms of invariant generators $e_1, s_2, \ldots, s_k$ makes a **huge** difference:

k		3	4	5	6	7	8
Semaev polynomials	nb of monomials	3	6	39	638	–	–
	timings	0 s	0 s	26 s	725 s	$\times$	$\times$
$P_{\varphi,k}$	nb of monomials	2	3	9	50	2 247	470 369
	timings	0 s	0 s	0 s	1 s	383 s	40.5 h

Computations for $k = 4$ to 7 in two steps:

1. take resultant of partially symmetrized summation polynomials
2. express resultant in terms of invariant generators using elimination (Gröbner basis)

Resultant too large for $k = 8$ case $\rightarrow$ dedicated interpolation technique

Two-torsion in char 2: results (2)

Target: IPSEC Oakley curve, defined over $\mathbb{F}_{2^{31\times 5}}$.
Cardinality is 12 times a 151-bit prime $\rightarrow$ can use 2-torsion point.

Difficulty of point decomposition $R = P_1 + \cdots + P_5$, $P_i \in \mathcal{F}$?

Two-torsion in char 2: results (2)

Target: IPSEC Oakley curve, defined over $\mathbb{F}_{2^{31\times 5}}$.
Cardinality is 12 times a 151-bit prime $\rightarrow$ can use 2-torsion point.

Difficulty of point decomposition $R = P_1 + \cdots + P_5$, $P_i \in \mathcal{F}$?

Gaudry-Diem's approach: intractable. Resolution of corresponding polynomial system does not succeed on a personal computer

Two-torsion in char 2: results (2)

Target: IPSEC Oakley curve, defined over $\mathbb{F}_{2^{31\times 5}}$.
Cardinality is 12 times a 151-bit prime $\rightarrow$ can use 2-torsion point.

Difficulty of point decomposition $R = P_1 + \cdots + P_5$, $P_i \in \mathcal{F}$?

Gaudry-Diem's approach: intractable. Resolution of corresponding polynomial system does not succeed on a personal computer

"$n-1$" approach: only known approach before this work. Estimated timing for one relation is ≈ 37 years (but easy to distribute).

Two-torsion in char 2: results (2)

Target: IPSEC Oakley curve, defined over $\mathbb{F}_{2^{31\times 5}}$.
Cardinality is 12 times a 151-bit prime $\rightarrow$ can use 2-torsion point.

Difficulty of point decomposition $R = P_1 + \cdots + P_5$, $P_i \in \mathcal{F}$?

Gaudry-Diem's approach: intractable. Resolution of corresponding polynomial system does not succeed on a personal computer

"$n-1$" approach: only known approach before this work. Estimated timing for one relation is ≈ 37 years (but easy to distribute).

With additional symmetries: ≈ 20 min for one relation.

Still too slow for ECDLP resolution, but threatens non-standard problems e.g. oracle-assisted static Diffie-Hellman.

Two-torsion in odd char: morphism

$E : y^2 = c\,x(x-1)(x-\lambda)$ elliptic curve over $\mathbb{F}_{q^n}$ in twisted Legendre form.
Three non-trivial 2-torsion points $T_0 = (0,0)$, $T_1 = (1,0)$, $T_2 = (\lambda, 0)$.

Two-torsion in odd char: morphism

$E : y^2 = c\,x(x-1)(x-\lambda)$ elliptic curve over $\mathbb{F}_{q^n}$ in twisted Legendre form.
Three non-trivial 2-torsion points $T_0 = (0,0)$, $T_1 = (1,0)$, $T_2 = (\lambda, 0)$.

Proposition

If λ and $1-\lambda$ squares, then $\exists\,\varphi : E \to \mathbb{F}_{q^n}$ degree 2 map s.t. $\forall P \in E$,

- $\varphi(P+T_0) = -\varphi(P)$, $\quad \varphi(P+T_1) = \dfrac{1}{\varphi(P)}$, $\quad \varphi(P+T_2) = -\dfrac{1}{\varphi(P)}$
- $\varphi(-P) = \varphi(P)$

Factor base can be effectively divided by 8 $\to \#\mathcal{F} \approx q/8$

Two-torsion in odd char: morphism

$E : y^2 = c\,x(x-1)(x-\lambda)$ elliptic curve over $\mathbb{F}_{q^n}$ in twisted Legendre form.
Three non-trivial 2-torsion points $T_0 = (0,0)$, $T_1 = (1,0)$, $T_2 = (\lambda, 0)$.

Proposition

If λ and $1-\lambda$ squares, then $\exists\, \varphi : E \to \mathbb{F}_{q^n}$ degree 2 map s.t. $\forall P \in E$,

- $\varphi(P+T_0) = -\varphi(P), \quad \varphi(P+T_1) = \dfrac{1}{\varphi(P)}, \quad \varphi(P+T_2) = -\dfrac{1}{\varphi(P)}$
- $\varphi(-P) = \varphi(P)$

Factor base can be effectively divided by 8 $\to \#\mathcal{F} \approx q/8$

Note: $z \mapsto -z$, $z \mapsto 1/z$ and $z \mapsto -1/z$ "simplest" choice of homographies. Only one can be affine.

Two-torsion in odd char: summation polynomials (1)

- $P_{\varphi,k}(X_1,\ldots,X_k) = P_{\varphi,k}(-X_1,-X_2,X_3,\ldots,X_k) = \ldots$
  Invariance by any even number of sign changes.

Two-torsion in odd char: summation polynomials (1)

- $P_{\varphi,k}(X_1,\dots,X_k) = P_{\varphi,k}(-X_1,-X_2,X_3,\dots,X_k) = \dots$
  Invariance by any even number of sign changes.
- However $P_{\varphi,k}(X_1,\dots,X_k) \neq P_{\varphi,k}(1/X_1,1/X_2,X_3,\dots,X_k)$. So ?

Two-torsion in odd char: summation polynomials (1)

- $P_{\varphi,k}(X_1,\ldots,X_k) = P_{\varphi,k}(-X_1,-X_2,X_3,\ldots,X_k) = \ldots$
  Invariance by any even number of sign changes.
- However $P_{\varphi,k}(X_1,\ldots,X_k) \neq P_{\varphi,k}(1/X_1,1/X_2,X_3,\ldots,X_k)$. So ?
  - Either only use first invariance (from $\varphi(P+T_0) = -\varphi(P)$).
    Then $P_{\varphi,k}$ belongs to explicit invariant ring $\rightarrow$ results as in char. 2 case.

Two-torsion in odd char: summation polynomials (1)

- $P_{\varphi,k}(X_1,\ldots,X_k) = P_{\varphi,k}(-X_1,-X_2,X_3,\ldots,X_k) = \ldots$
  Invariance by any even number of sign changes.
- However $P_{\varphi,k}(X_1,\ldots,X_k) \neq P_{\varphi,k}(1/X_1,1/X_2,X_3,\ldots,X_k)$. So ?

  - Either only use first invariance (from $\varphi(P+T_0) = -\varphi(P)$).
    Then $P_{\varphi,k}$ belongs to explicit invariant ring $\rightarrow$ results as in char. 2 case.
  - Or consider invariant *rational fraction*

$$Q_{\varphi,k}(X_1,\ldots,X_k) = \frac{P_{\varphi,k}(X_1,\ldots,X_k)}{X_1\ldots X_k}$$

and work with invariant fields instead.

Two-torsion in odd char: summation polynomials (2)

Proposition

- *$Q_{\varphi,k}$ is invariant under action of the group $G_4 = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^{k-1} \rtimes \mathfrak{S}_k$.*
- *Invariant field $\mathbb{F}_{q^n}(X_1, \ldots, X_k)^{G_4}$ has explicit generators $w_0, w_1, \sigma_1, \ldots, \sigma_{k-2}$.*

Two-torsion in odd char: summation polynomials (2)

Proposition

- *$Q_{\varphi,k}$ is invariant under action of the group* $G_4 = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^{k-1} \rtimes \mathfrak{S}_k$.
- *Invariant field $\mathbb{F}_{q^n}(X_1, \ldots, X_k)^{G_4}$ has explicit generators* $w_0, w_1, \sigma_1, \ldots, \sigma_{k-2}$.

FYI:

σ_i = i-th elementary symmetric polynomial in $X_1^2 + X_1^{-2}, \ldots, X_k^2 + X_k^{-2}$

Two-torsion in odd char: summation polynomials (2)

Proposition

- *$Q_{\varphi,k}$ is invariant under action of the group $G_4 = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^{k-1} \rtimes \mathfrak{S}_k$.*
- *Invariant field $\mathbb{F}_{q^n}(X_1, \ldots, X_k)^{G_4}$ has explicit generators $w_0, w_1, \sigma_1, \ldots, \sigma_{k-2}$.*

FYI:

σ_i = i-th elementary symmetric polynomial in $X_1^2 + X_1^{-2}, \ldots, X_k^2 + X_k^{-2}$

$w_0 = \sum_{i=0}^{\lfloor n/2 \rfloor} s_{2i}/(X_1 \cdots X_n)$, $\quad w_1 = \sum_{i=1}^{\lfloor (n-1)/2 \rfloor} s_{2i+1}/(X_1 \cdots X_n)$, where

s_i = i-th elementary symmetric polynomial in $X_1^2, \ldots, X_n^2$ (and $s_0 = 1$).

Symmetrization

How to express an invariant rational fraction in terms of generators of the invariant field?

Symmetrization

How to express an invariant rational fraction in terms of generators of the invariant field?

- For polynomials in invariant ring: **elimination theory**.

  If new generators are $Y_i = f_i(X_1, \ldots, X_k)$, compute Gröbner basis of $\{Y_1 - f_1, \ldots, Y_m - f_m\} \subset K[X_1, \ldots, X_k, Y_1, \ldots, Y_m]$ wrt. an elimination order, then compute normal form of invariant polynomial.

Symmetrization

How to express an invariant rational fraction in terms of generators of the invariant field?

- For polynomials in invariant ring: **elimination theory**.

  If new generators are $Y_i = f_i(X_1, \ldots, X_k)$, compute Gröbner basis of $\{Y_1 - f_1, \ldots, Y_m - f_m\} \subset K[X_1, \ldots, X_k, Y_1, \ldots, Y_m]$ wrt. an elimination order, then compute normal form of invariant polynomial.

- For rational fractions in invariant field: ??

Symmetrization

How to express an invariant rational fraction in terms of generators of the invariant field?

- For polynomials in invariant ring: **elimination theory**.

  If new generators are $Y_i = f_i(X_1, \ldots, X_k)$, compute Gröbner basis of $\{Y_1 - f_1, \ldots, Y_m - f_m\} \subset K[X_1, \ldots, X_k, Y_1, \ldots, Y_m]$ wrt. an elimination order, then compute normal form of invariant polynomial.

- For rational fractions in invariant field: ??

  However in our case $Q_{\varphi,k}$ is **polynomial** in our choice of invariant generators
  $\rightarrow$ inductive computation with partially symmetrized resultants OK.

Two-torsion in odd char: results (1)

k	3	4	5	6
Semaev polynomials	5	36	940	–
$P_{\varphi,k}(s_1,\ldots,s_{k-1},e_k)$	5	13	182	4125
$Q_{\varphi,k}(\sigma_1,\ldots,\sigma_{k-2},w_0,w_1)$	3	6	32	396

Comparison of number of monomials for:

- Semaev polynomials, symmetrized wrt. the action of $\mathfrak{S}_k$
- $P_{\varphi,k}$ symmetrized wrt. the action of only one 2-torsion point
- $Q_{\varphi,k}$ symmetrized wrt. the action of the full 2-torsion

Two-torsion in odd char: results (1)

k	3	4	5	6
Semaev polynomials	5	36	940	–
$P_{\varphi,k}(s_1,\ldots,s_{k-1},e_k)$	5	13	182	4125
$Q_{\varphi,k}(\sigma_1,\ldots,\sigma_{k-2},w_0,w_1)$	3	6	32	396

Comparison of number of monomials for:

- Semaev polynomials, symmetrized wrt. the action of $\mathfrak{S}_k$
- $P_{\varphi,k}$ symmetrized wrt. the action of only one 2-torsion point
- $Q_{\varphi,k}$ symmetrized wrt. the action of the full 2-torsion

Note: less sparse than in char. 2

Two-torsion in odd char: results (2)

Target: random curve over OEF $\mathbb{F}_{(2^{31}+413)^5}$, with full 2-torsion and near-prime cardinality.

Difficulty of point decomposition $R = P_1 + \cdots + P_5$, $P_i \in \mathcal{F}$?

Two-torsion in odd char: results (2)

Target: random curve over OEF $\mathbb{F}_{(2^{31}+413)^5}$, with full 2-torsion and near-prime cardinality.

Difficulty of point decomposition $R = P_1 + \cdots + P_5$, $P_i \in \mathcal{F}$?

Gaudry-Diem's approach: intractable.

Two-torsion in odd char: results (2)

Target: random curve over OEF $\mathbb{F}_{(2^{31}+413)^5}$, with full 2-torsion and near-prime cardinality.

Difficulty of point decomposition $R = P_1 + \cdots + P_5$, $P_i \in \mathcal{F}$?

Gaudry-Diem's approach: intractable.

With one 2-torsion point: ≈ 90 h for one relation.

Two-torsion in odd char: results (2)

Target: random curve over OEF $\mathbb{F}_{(2^{31}+413)^5}$, with full 2-torsion and near-prime cardinality.

Difficulty of point decomposition $R = P_1 + \cdots + P_5$, $P_i \in \mathcal{F}$?

Gaudry-Diem's approach: intractable.

With one 2-torsion point: $\approx$ 90 h for one relation.

With full 2-torsion: $\approx$ 15 min for one relation.

Further developments

- Higher order torsion points:
  Computations for small values of $\ell > 2$ are possible.

  Pro: smaller factor base $\rightarrow$ less relations and faster linear algebra

  Con: larger degree for summation polynomials $\rightarrow$ harder decompositions

Further developments

- Higher order torsion points:
  Computations for small values of $\ell > 2$ are possible.

  Pro: smaller factor base $\rightarrow$ less relations and faster linear algebra

  Con: larger degree for summation polynomials $\rightarrow$ harder decompositions

- More automorphisms ($j = 0$ or 1728):
  Equivariance of φ wrt. automorphisms besides $[-1]$ would lead to more symmetries.

Summation polynomials and symmetries for the ECDLP over extension fields

Vanessa VITSE
Joint work with Faugère, Huot, Joux and Renault

Université Joseph Fourier – Grenoble