Summation polynomials and symmetries for the ECDLP over extension fields

Vanessa VITSE

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.

Step 2 **hopeless** if $\mathcal{F}$ arbitrary subset of $E(\mathbb{F}_{q^n})$.

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.

Step 2 **hopeless** if $\mathcal{F}$ arbitrary subset of $E(\mathbb{F}_{q^n})$.
Only method so far: define $\mathcal{F}$ algebraically, over subfield $\mathbb{F}_q$
$\rightarrow$ Weil restriction structure

Gaudry/Diem's decomposition

- Standard choice is $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}$
  $\rightarrow$ algebraic curve in the Weil restriction of E seen as a dim. n abelian variety over $\mathbb{F}_q$
  $\rightarrow \#\mathcal{F} \simeq q$
  $\rightarrow$ look for decomp. of $R = [a]P + [b]Q$ in sums of n points of $\mathcal{F}$.

Gaudry/Diem's decomposition

- Standard choice is $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}$
  $\rightarrow$ algebraic curve in the Weil restriction of E seen as a dim. n abelian variety over $\mathbb{F}_q$
  $\rightarrow \#\mathcal{F} \simeq q$
  $\rightarrow$ look for decomp. of $R = [a]P + [b]Q$ in sums of n points of $\mathcal{F}$.

- Still not obvious to find decompositions. Main tool: description of the addition law on E with Semaev polynomials.

Semaev polynomials

Semaev summation polynomials

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

$$S_k(a_1, \dots, a_k) = 0 \iff \exists P_i \in E(\overline{\mathbb{F}_q}),\ x(P_i) = a_i \text{ and } \sum_i P_i = \mathcal{O}$$

Semaev polynomials

Semaev summation polynomials

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

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

$$\begin{array}{ccc} (P_1, \ldots, P_k) & \in & E^k \\ \downarrow & & \downarrow x \\ (x(P_1), \ldots, x(P_k)) & \in & \mathbb{A}^k \end{array}$$

Semaev polynomials

Semaev summation polynomials

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

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

$$\begin{array}{ccccc} (P_1, \ldots, P_k) & \in & E^k & \hookleftarrow & \{(P_1, \ldots, P_k) : \sum_i P_i = \mathcal{O}\} \simeq E^{k-1} \\ \downarrow & & \downarrow x & & \\ (x(P_1), \ldots, x(P_k)) & \in & \mathbb{A}^k & & \end{array}$$

Semaev polynomials

Semaev summation polynomials

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

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

$$\begin{array}{ccccc}
(P_1, \ldots, P_k) & \in & E^k & \hookleftarrow & \{(P_1, \ldots, P_k) : \sum_i P_i = \mathcal{O}\} \simeq E^{k-1} \\
\downarrow & & \downarrow x & & \downarrow x \\
(x(P_1), \ldots, x(P_k)) & \in & \mathbb{A}^k & \hookleftarrow & V(S_k)
\end{array}$$

Semaev polynomials

Semaev summation polynomials

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

$$S_k(a_1, \dots, a_k) = 0 \iff \exists P_i \in E(\overline{\mathbb{F}_q}),\ x(P_i) = a_i \text{ and } \sum_i P_i = \mathcal{O}$$

$$\begin{array}{ccccc}
(P_1, \dots, P_k) & \in & E^k & \hookleftarrow & \{(P_1, \dots, P_k) : \sum_i P_i = \mathcal{O}\} \simeq E^{k-1} \\
\downarrow & & \downarrow x & & \downarrow x \\
(x(P_1), \dots, x(P_k)) & \in & \mathbb{A}^k & \hookleftarrow & V(S_k)
\end{array}$$

"Projection of the group law on x"

Semaev polynomials

Semaev summation polynomials

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

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

$$\begin{array}{ccccc}
(P_1, \ldots, P_k) & \in E^k & \hookleftarrow & \{(P_1, \ldots, P_k) : \sum_i P_i = \mathcal{O}\} \simeq E^{k-1} \\
\big\downarrow & \big\downarrow x & & \big\downarrow x \\
(x(P_1), \ldots, x(P_k)) & \in \mathbb{A}^k & \hookleftarrow & V(S_k)
\end{array}$$

"Projection of the group law on x"

Degree 2^{k-2} in each variable $\rightarrow$ hard to compute for $k \geqslant 5$

Back to Gaudry/Diem's decomposition

- Standard choice is $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}$
  $\rightarrow$ algebraic curve in the Weil restriction of E seen as a dim. n abelian variety over $\mathbb{F}_q$
  $\rightarrow \#\mathcal{F} \simeq q$
  $\rightarrow$ look for decomp. of $R = [a]P + [b]Q$ in sums of n points of $\mathcal{F}$.
- Still not obvious to find decompositions. Main tool: description of the addition law on E with Semaev polynomials.

Back to Gaudry/Diem's decomposition

- Standard choice is $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}$
  $\rightarrow$ algebraic curve in the Weil restriction of E seen as a dim. n abelian variety over $\mathbb{F}_q$
  $\rightarrow \#\mathcal{F} \simeq q$
  $\rightarrow$ look for decomp. of $R = [a]P + [b]Q$ in sums of n points of $\mathcal{F}$.
- Still not obvious to find decompositions. Main tool: description of the addition law on E with Semaev polynomials.
- Decomposition try for $R = [a]P + [b]Q$: solve

$$S_{n+1}(x_1, \ldots, x_n, x(R)) = 0 \text{ with } x_i \in \mathbb{F}_q$$

Restriction of scalar $\rightsquigarrow$ resolution of multivariate polynomial system defined over $\mathbb{F}_q$ with n variables/equations, total degree $n\,2^{n-2}$.

Back to Gaudry/Diem's decomposition

- Standard choice is $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}$
  $\rightarrow$ algebraic curve in the Weil restriction of E seen as a dim. n abelian variety over $\mathbb{F}_q$
  $\rightarrow \#\mathcal{F} \simeq q$
  $\rightarrow$ look for decomp. of $R = [a]P + [b]Q$ in sums of n points of $\mathcal{F}$.
- Still not obvious to find decompositions. Main tool: description of the addition law on E with Semaev polynomials.
- Decomposition try for $R = [a]P + [b]Q$: solve

$$S_{n+1}(x_1, \ldots, x_n, x(R)) = 0 \text{ with } x_i \in \mathbb{F}_q$$

Restriction of scalar $\rightsquigarrow$ resolution of multivariate polynomial system defined over $\mathbb{F}_q$ with n variables/equations, 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 $n \leqslant 4$, intractable if $n \geqslant 5$

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* $k \geqslant 3$*, there exists a unique (up to constant)* $P_{\varphi,k} \in \mathbb{F}_{q^n}[X_1, \ldots, X_k]$*, irreducible, symmetric, s.t.*

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

Summation polynomials

Theorem

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

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

"Projection of the group law on φ"

Summation polynomials

Theorem

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

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

"Projection of the group law on φ"

$\deg_{X_i} P_{\varphi,k}$ proportional to $(\deg \varphi)^k$ in general, and also for all interesting cases so far
→ computation tractable only if $\deg \varphi$ and k small.

Computation of summation polynomials

First method: Riemann-Roch

Observation

$P_1 + \cdots + P_k = \mathcal{O} \Leftrightarrow \exists f \in \bar{\mathbb{F}}_q(E)$ 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

$P_1 + \cdots + P_k = \mathcal{O} \Leftrightarrow \exists f \in \bar{\mathbb{F}}_q(E)$ 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

$P_1 + \cdots + P_k = \mathcal{O} \Leftrightarrow \exists f \in \bar{\mathbb{F}}_q(E)$ 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

$P_1 + \cdots + P_k = \mathcal{O} \Leftrightarrow \exists f \in \bar{\mathbb{F}}_q(E)$ 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

$P_1 + \cdots + P_k = \mathcal{O} \Leftrightarrow \exists f \in \bar{\mathbb{F}}_q(E)$ 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!

Free relations

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 $P + T \in \mathcal{F}$.

Action of small torsion points

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

Free relations

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 yields many more:

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

Relation amplification

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

Consequences

- Pro: size of factor base $\mathcal{F}$ can be effectively divided by ℓ

Relation amplification

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

Consequences

- Pro: size of factor base $\mathcal{F}$ can be effectively divided by ℓ
- Con: decreases the probability that a random R can be decomposed

Relation amplification

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

Consequences

- Pro: size of factor base $\mathcal{F}$ can be effectively divided by ℓ
- Con: decreases the probability that a random R can be decomposed
- **Main advantage:** big speed-up in computation of summation polynomials and point decomposition

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

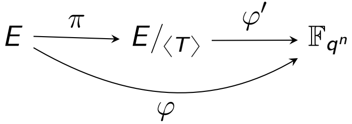
Goal: factor base $\mathcal{F} = \{P : \varphi(P) \in \mathbb{F}_q\}$ invariant by τ_T, $T \in E[\ell]$

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 $E \to E/_{\langle T \rangle}$:



Equivariant morphisms

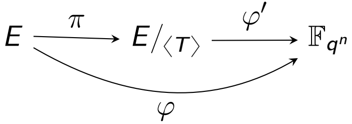
Goal: factor base $\mathcal{F} = \{P : \varphi(P) \in \mathbb{F}_q\}$ invariant by τ_T, $T \in E[\ell]$

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 $E \to E/_{\langle T \rangle}$:



Same summation polynomials: $P_{\varphi,n} = P_{\varphi',n}$

Equivariant morphisms

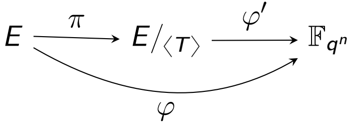
Goal: factor base $\mathcal{F} = \{P : \varphi(P) \in \mathbb{F}_q\}$ invariant by τ_T, $T \in E[\ell]$

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 $E \to E/_{\langle T \rangle}$:



Same summation polynomials: $P_{\varphi,n} = P_{\varphi',n}$
$\Rightarrow$ equivalent decompositions on E with φ and on $E_{/\langle T \rangle}$ with φ', but
no use of torsion on the latter!

Equivariant morphisms

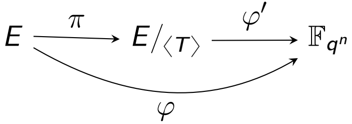
Goal: factor base $\mathcal{F} = \{P : \varphi(P) \in \mathbb{F}_q\}$ invariant by τ_T, $T \in E[\ell]$

~~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 $E \to E/_{\langle T \rangle}$:



Same summation polynomials: $P_{\varphi,n} = P_{\varphi',n}$
$\Rightarrow$ equivalent decompositions on E with φ and on $E_{/\langle T \rangle}$ with φ', but
no use of torsion on the latter!

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 $f^{(\ell)} = f \circ \cdots \circ f = Id$
- Invariance of $\mathcal{F}$ requires stability by f of $\mathbb{F}_q$, or rather $\mathbb{P}^1(\mathbb{F}_q)$

$$\Rightarrow f \text{ element of } \mathrm{PGL}_2(\mathbb{F}_q) \text{ of exact order } \ell$$

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 $f^{(\ell)} = f \circ \cdots \circ f = Id$
- Invariance of $\mathcal{F}$ requires stability by f of $\mathbb{F}_q$, or rather $\mathbb{P}^1(\mathbb{F}_q)$

$$\Rightarrow f \text{ element of } \mathrm{PGL}_2(\mathbb{F}_q) \text{ of exact order } \ell$$

- Better if φ also invariant or equivariant wrt. $[-1]$

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 $f^{(\ell)} = f \circ \cdots \circ f = Id$
- Invariance of $\mathcal{F}$ requires stability by f of $\mathbb{F}_q$, or rather $\mathbb{P}^1(\mathbb{F}_q)$

$$\Rightarrow f \text{ element of } \mathrm{PGL}_2(\mathbb{F}_q) \text{ of exact order } \ell$$

- Better if φ also invariant or equivariant wrt. $[-1]$

Fact

$$\varphi \text{ strictly equivariant wrt. translation by } T \in E[\ell] \ \Rightarrow \ \ell \mid \deg \varphi$$

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 [FHJRV, Eurocrypt 2014]

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 [FHJRV, Eurocrypt 2014]

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)

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

Two-torsion in char 2: results [FHJRV, Eurocrypt 2014]

Target: IPSEC Oakley curve, defined over $\mathbb{F}_{2^{31\times 5}}$.
Cardinality is 12 times a 151-bit prime → 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 [FHJRV, Eurocrypt 2014]

Target: IPSEC Oakley curve, defined over $\mathbb{F}_{2^{31\times 5}}$.
Cardinality is 12 times a 151-bit prime → 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 [FHJRV, Eurocrypt 2014]

Target: IPSEC Oakley curve, defined over $\mathbb{F}_{2^{31\times 5}}$.
Cardinality is 12 times a 151-bit prime → 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 [FHJRV, Eurocrypt 2014]

Target: IPSEC Oakley curve, defined over $\mathbb{F}_{2^{31\times 5}}$.
Cardinality is 12 times a 151-bit prime → 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 $\approx$ 37 years (but easy to distribute).

With additional symmetries: $\approx$ 5.5 hr 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. $\forall P \in E$,

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

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: 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. $\forall P \in E$,

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

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

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

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)

- $P_{\varphi,k}(X_1,\ldots,X_k) = P_{\varphi,k}(-X_1,-X_2,X_3,\ldots,X_k) = \ldots$
  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 ?

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*

$$Q_{\varphi,k}(X_1,\ldots,X_k) = \frac{P_{\varphi,k}(X_1,\ldots,X_k)}{(X_1\ldots X_k)^{2^{k-3}}}$$

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:

$\sigma_i =$ 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 $X_1^2 + X_1^{-2}, \ldots, X_k^2 + X_k^{-2}$

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

s_i = i-th elementary symmetric polynomial in $X_1^2, \ldots, X_k^2$ (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

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 [FGHR, JoC 2013]: $\approx$ 60 days 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 [FGHR, JoC 2013]: $\approx$ 60 days for one relation.

With full 2-torsion: $\approx$ 2.5 days for one relation.

Equivariance for higher order torsion

Let G be a subgroup of $E(\mathbb{F}_{q^n})$.
Can we find maps $E \to \mathbb{P}^1$ strictly equivariant wrt. to translation by any point of G?

Equivariance for higher order torsion

Let G be a subgroup of $E(\mathbb{F}_{q^n})$.
Can we find maps $E \to \mathbb{P}^1$ strictly equivariant wrt. to translation by any point of G? Yes, but not for any G

Equivariance for higher order torsion

Let G be a subgroup of $E(\mathbb{F}_{q^n})$.
Can we find maps $E \to \mathbb{P}^1$ strictly equivariant wrt. to translation by any point of G? Yes, but not for any G

Strict equivariance $\Rightarrow$ injective homomorphism $G \to \mathrm{PGL}_2(\mathbb{F}_q)$
with also $[-1] \Rightarrow$ homom. $G \rtimes \mathbb{Z}/2\mathbb{Z} \to \mathrm{PGL}_2(\mathbb{F}_q)$, injective on G.

Equivariance for higher order torsion

Let G be a subgroup of $E(\mathbb{F}_{q^n})$.
Can we find maps $E \to \mathbb{P}^1$ strictly equivariant wrt. to translation by any point of G? Yes, but not for any G

Strict equivariance $\Rightarrow$ injective homomorphism $G \to \mathrm{PGL}_2(\mathbb{F}_q)$
with also $[-1] \Rightarrow$ homom. $G \rtimes \mathbb{Z}/2\mathbb{Z} \to \mathrm{PGL}_2(\mathbb{F}_q)$, injective on G.

Theorem

The only possible subgroups are:

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

Case $\ell | q - 1$

If φ equivariant for $\langle T_\ell \rangle \subset E[\ell]$, we can always assume that

$$\varphi(P + T_\ell) = \zeta\varphi(P), \quad \zeta \in \mu_\ell^*(\mathbb{F}_q).$$

So $\varphi(P + T)/\varphi(P)$ independent of P if $T \in \langle T_\ell \rangle$

Case $\ell | q - 1$

If φ equivariant for $\langle T_\ell \rangle \subset E[\ell]$, we can always assume that

$$\varphi(P + T_\ell) = \zeta\varphi(P), \quad \zeta \in \mu_\ell^*(\mathbb{F}_q).$$

So $\varphi(P + T)/\varphi(P)$ independent of P if $T \in \langle T_\ell \rangle$

$\Rightarrow$ **Homomorphism** ("linear map") from $\langle T_\ell \rangle$ to $\mu_\ell(\mathbb{F}_q)$,

$$T \mapsto \frac{\varphi(P + T)}{\varphi(P)}.$$

Case $\ell | q-1$

If φ equivariant for $\langle T_\ell \rangle \subset E[\ell]$, we can always assume that

$$\varphi(P+T_\ell) = \zeta\varphi(P), \quad \zeta \in \mu_\ell^*(\mathbb{F}_q).$$

So $\varphi(P+T)/\varphi(P)$ independent of P if $T \in \langle T_\ell \rangle$

$\Rightarrow$ **Homomorphism** ("linear map") from $\langle T_\ell \rangle$ to $\mu_\ell(\mathbb{F}_q)$,

$$T \mapsto \frac{\varphi(P+T)}{\varphi(P)}.$$

Sounds familiar?

Case $\ell | q-1$

If φ equivariant for $\langle T_\ell \rangle \subset E[\ell]$, we can always assume that

$$\varphi(P + T_\ell) = \zeta\varphi(P), \quad \zeta \in \mu_\ell^*(\mathbb{F}_q).$$

So $\varphi(P + T)/\varphi(P)$ independent of P if $T \in \langle T_\ell \rangle$

$\Rightarrow$ **Homomorphism** ("linear map") from $\langle T_\ell \rangle$ to $\mu_\ell(\mathbb{F}_q)$,

$$T \mapsto \frac{\varphi(P+T)}{\varphi(P)}.$$

Sounds familiar? **Pairings** are not far away...

Cartier pairing

Let ψ be the ℓ-isogeny $E \to E/_{\langle T_\ell \rangle}$. Then there exists a pairing on $\ker \psi \times \ker \hat{\psi} \simeq \langle T_\ell \rangle \times E[\ell]/_{\langle T_\ell \rangle}$.

Cartier pairing

Let ψ be the ℓ-isogeny $E \to E/_{\langle T_\ell \rangle}$. Then there exists a pairing on $\ker\psi \times \ker\hat{\psi} \simeq \langle T_\ell \rangle \times E[\ell]/_{\langle T_\ell \rangle}$.

Cartier pairing

Let $T \in \langle T_\ell \rangle$ and $\overline{T'} \in E[\ell]/_{\langle T_\ell \rangle}$. Let $g_{T'}$ the function with divisor

$$\psi^*((\psi(T')) - (\mathcal{O})) = \sum_{i=1}^{\ell}(T' + [i]T_\ell) - \sum_{i=1}^{\ell}([i]T_\ell).$$

Then $e_\psi(T, \overline{T'}) = g_{T'}(P + T)/g_{T'}(P)$ is independent of $P \in E$.

$e_\psi : \langle T_\ell \rangle \times E[\ell]/_{\langle T_\ell \rangle} \to \mu_\ell$ well-defined, non-degenerate bilinear map.

Cartier pairing

Let ψ be the ℓ-isogeny $E \to E/_{\langle T_\ell \rangle}$. Then there exists a pairing on $\ker \psi \times \ker \hat{\psi} \simeq \langle T_\ell \rangle \times E[\ell]/_{\langle T_\ell \rangle}$.

Cartier pairing

Let $T \in \langle T_\ell \rangle$ and $\overline{T'} \in E[\ell]/_{\langle T_\ell \rangle}$. Let $g_{T'}$ the function with divisor

$$\psi^*((\psi(T')) - (\mathcal{O})) = \sum_{i=1}^{\ell} (T' + [i]T_\ell) - \sum_{i=1}^{\ell} ([i]T_\ell).$$

Then $e_\psi(T, \overline{T'}) = g_{T'}(P + T)/g_{T'}(P)$ is independent of $P \in E$.

$e_\psi : \langle T_\ell \rangle \times E[\ell]/_{\langle T_\ell \rangle} \to \mu_\ell$ well-defined, non-degenerate bilinear map.

Because $T_\ell \in E(\mathbb{F}_{q^n})$ and $\ell | q-1$, function $g_{T'}$ is defined over $\mathbb{F}_{q^n}$.

Equivariant morphism for $\ell | q-1$

If T_ℓ, T' generate $E[\ell]$ then $g_{T'} : E \to \mathbb{P}^1$ is a strictly equivariant morphism.

To get equivariance wrt. $[-1]$, set $\varphi(P) = \dfrac{g_{T'}(P)}{g_{T'}(-P)}$ (at least if ℓ odd), so $\varphi(-P) = 1/\varphi(P)$.

Equivariant morphism for $\ell | q - 1$

If T_ℓ, T' generate $E[\ell]$ then $g_{T'} : E \to \mathbb{P}^1$ is a strictly equivariant morphism.

To get equivariance wrt. $[-1]$, set $\varphi(P) = \dfrac{g_{T'}(P)}{g_{T'}(-P)}$ (at least if ℓ odd), so $\varphi(-P) = 1/\varphi(P)$.

Proposition

This construction essentially yields all morphisms $E \to \mathbb{P}^1$ equivariant wrt. to translation by a ℓ-torsion point.

Case $\ell | q + 1$ is very similar, except that the action on $\mathbb{P}^1$ is less nice than $z \mapsto \zeta z$.

Summation polynomial and invariant ring

Assume $\varphi(P + T_\ell) = \zeta\varphi(P)$ and $\varphi(-P) = 1/\varphi(P)$.
As in the 2-torsion case, we have:

Proposition

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

$$s_1 = Y_1 + \ldots + Y_k,\ \ldots\ ,\ s_{k-1} = Y_1 \ldots Y_{k-1} + \ldots + Y_2 \ldots Y_k,\ e_k = X_1 \ldots X_k$$

where $Y_i = X_i^\ell$.

Summation polynomial and invariant ring

Assume $\varphi(P + T_\ell) = \zeta\varphi(P)$ and $\varphi(-P) = 1/\varphi(P)$.
As in the 2-torsion case, we have:

Proposition

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

$$s_1 = Y_1 + ... + Y_k,\ \ ...\ ,\ s_{k-1} = Y_1...Y_{k-1} + ... + Y_2...Y_k,\ e_k = X_1...X_k$$

where $Y_i = X_i^\ell$.

Equivariance wrt. $[-1]$ more difficult to take into account: replacing polynomials by rational fractions gives no simplification.

Still allows to reduce size of factor base by 2.

Example

For $\ell = 3$ $(\ell | q-1)$, and $E : y^2 = x^3 + (x+a)^2$, the point $T = (0, a)$ has order 3.

The equivariant morphism is given by

$$\varphi(x,y) = \frac{\sqrt{3}y + i(x+3a)}{-\sqrt{3}y + i(x+3a)}.$$

Then the corresponding third summation polynomial is

$$\begin{aligned}P_{\varphi,3}(s_1,s_2,e_3) = & -27e_3^6+27s_1e_3^4+27s_2e_3^4-81e_3^5-9s_2^2e_3^2+54s_1e_3^3+54s_2e_3^3 \\ & -81e_3^4+s_1^3+3s_1^2s_2+3s_1s_2^2+s_2^3-9s_1^2e_3+27s_1e_3^2+27s_2e_3^2-27e_3^3 \\ & +\delta(12s_1^2e_3^3-(27a-16)(s_1^2e_3^2+s_2^2e_3)-(54a+16)(s_1s_2e_3^2+s_1s_2e_3)+12s_2^2),\end{aligned}$$

$\delta = 9/(27a-4)$.

Case $\ell = p$

If φ equivariant for $\langle T_p \rangle = E[p]$, we can always assume that

$$\varphi(P + T_p) = \varphi(P) + 1$$

So $\varphi(P + T) - \varphi(P)$ independent of P if $T \in E[p]$

Case $\ell = p$

If φ equivariant for $\langle T_p \rangle = E[p]$, we can always assume that

$$\varphi(P + T_p) = \varphi(P) + 1$$

So $\varphi(P + T) - \varphi(P)$ independent of P if $T \in E[p]$

$\Rightarrow$ **Homomorphism** ("linear map") from $E[p]$ to $(\mathbb{F}_q, +)$,

$$T \mapsto \varphi(P + T) - \varphi(P).$$

Case $\ell = p$

If φ equivariant for $\langle T_p \rangle = E[p]$, we can always assume that

$$\varphi(P + T_p) = \varphi(P) + 1$$

So $\varphi(P + T) - \varphi(P)$ independent of P if $T \in E[p]$

$\Rightarrow$ **Homomorphism** ("linear map") from $E[p]$ to $(\mathbb{F}_q, +)$,

$$T \mapsto \varphi(P + T) - \varphi(P).$$

Sounds familiar?

Case $\ell = p$

If φ equivariant for $\langle T_p \rangle = E[p]$, we can always assume that

$$\varphi(P + T_p) = \varphi(P) + 1$$

So $\varphi(P + T) - \varphi(P)$ independent of P if $T \in E[p]$

$\Rightarrow$ **Homomorphism** ("linear map") from $E[p]$ to $(\mathbb{F}_q, +)$,

$$T \mapsto \varphi(P + T) - \varphi(P).$$

Sounds familiar? Easy DLP in order p subgroup

Case $\ell = p$

If φ equivariant for $\langle T_p \rangle = E[p]$, we can always assume that

$$\varphi(P + T_p) = \varphi(P) + 1$$

So $\varphi(P + T) - \varphi(P)$ independent of P if $T \in E[p]$

$\Rightarrow$ **Homomorphism** ("linear map") from $E[p]$ to $(\mathbb{F}_q, +)$,

$$T \mapsto \varphi(P + T) - \varphi(P).$$

Sounds familiar? Easy DLP in order p subgroup $\rightarrow$ **anomalous attack.**

Equivariant morphism for $\ell = p$

Let $T_p \in E[p]$ and $g(x) = \prod_{i=1}^{(p-1)/2} (x - x([i]T_p))$

($g \leftrightsquigarrow p$-th root of p-th division polynomial).

Proposition

There exists $\lambda \in \mathbb{F}_{q^n}$ such that the map $\varphi(x, y) = \frac{yg'(x)}{g(x)}$ satisfies the equivariance properties

$$\varphi(P + T_p) = \varphi(P) + 1, \qquad \varphi(-P) = -\varphi(P).$$

Only such function, up to translation by a rational 2-torsion point.

Equivariant morphism for $\ell = p$

Let $T_p \in E[p]$ and $g(x) = \prod_{i=1}^{(p-1)/2} (x - x([i]T_p))$

($g \leftrightsquigarrow$ p-th root of p-th division polynomial).

Proposition

There exists $\lambda \in \mathbb{F}_{q^n}$ such that the map $\varphi(x,y) = \frac{yg'(x)}{g(x)}$ satisfies the equivariance properties

$$\varphi(P + T_p) = \varphi(P) + 1, \qquad \varphi(-P) = -\varphi(P).$$

Only such function, up to translation by a rational 2-torsion point.

If φ can be computed efficiently for p large, gives a q-adic independent version of the anomalous attack.

Summation polynomial and invariant ring

Assume $\varphi(P + T_p) = \varphi(P) + 1$ and $\varphi(-P) = -\varphi(P)$.
As in the 2-torsion case, we have:

Proposition

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

$$e_1 = X_1 + ... + X_k,\ s_2 = Y_1 Y_2 + ... + Y_{k-1} Y_k, ...,\ s_k = Y_1 ... Y_k$$

where $Y_i = X_i^p - X_i$.

Summation polynomial and invariant ring

Assume $\varphi(P + T_p) = \varphi(P) + 1$ and $\varphi(-P) = -\varphi(P)$.
As in the 2-torsion case, we have:

Proposition

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

$$e_1 = X_1 + \ldots + X_k,\ s_2 = Y_1 Y_2 + \ldots + Y_{k-1} Y_k, \ldots,\ s_k = Y_1 \ldots Y_k$$

where $Y_i = X_i^p - X_i$.

Equivariance wrt. $[-1]$ more difficult to take into account: invariant ring is no longer a free algebra.

Still allows to reduce size of factor base by 2.

Example

For $p = 3$, and $E : y^2 = x^3 + (x + a)^2$, the point $T = (0, a)$ has order 3.

The equivariant morphism is simply given by

$$\varphi(x, y) = \frac{y}{x}.$$

Then the corresponding third summation polynomial is

$$P_{\varphi,3}(e_1, s_2, s_3) = 2ae_1^6 + e_1^2 s_2^2 + e_1^3 s_3 + 2s_2^3.$$

Much sparser than in the case $\ell | (q - 1)$.

Example

For $p = 3$, and $E : y^2 = x^3 + (x + a)^2$, the point $T = (0, a)$ has order 3.

The equivariant morphism is simply given by

$$\varphi(x, y) = \frac{y}{x}.$$

Then the corresponding third summation polynomial is

$$P_{\varphi,3}(e_1, s_2, s_3) = 2ae_1^6 + e_1^2 s_2^2 + e_1^3 s_3 + 2s_2^3.$$

Much sparser than in the case $\ell | (q - 1)$.

Fourth summation polynomial is

$$P_{\varphi,4}(e_1, s_2, s_3, s_4) = s_3^9 + e_1^3 s_3^8 + 120 \text{ other terms}.$$

Conclusion

- Use of 2-torsion points: huge speed-up for computations of decompositions

Conclusion

- Use of 2-torsion points: huge speed-up for computations of decompositions
- Higher order torsion points:
  Computations possible only for small values of $\ell > 2$ and n.

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

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

  ↳ currently no gain over classical decomposition method except possibly for 3-torsion in char. 3.

Conclusion

- Use of 2-torsion points: huge speed-up for computations of decompositions
- Higher order torsion points:
  Computations possible only for small values of $\ell > 2$ and n.

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

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

  ↳ currently no gain over classical decomposition method except possibly for 3-torsion in char. 3.

  ↳ new point of view on the anomalous attack

Conclusion

- Use of 2-torsion points: huge speed-up for computations of decompositions

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

  Pro: smaller factor base → less relations and faster linear algebra

  Con: larger degree for summation polynomials → harder decompositions

  ↳ currently no gain over classical decomposition method except possibly for 3-torsion in char. 3.
  ↳ new point of view on the anomalous attack

- Further developments: more automorphisms ($j = 0$ or 1728), hyperelliptic curves.

Summation polynomials and symmetries for the ECDLP over extension fields

Vanessa VITSE

Université Joseph Fourier – Grenoble