On Index Calculus Algorithms for Subfield Curves

Steven D. Galbraith[1] Robert Granger[2] **Simon-Philipp Merz**[3]
Christophe Petit[4,5]

[1]Mathematics Department, University of Auckland, New Zealand
[2]Department of Computer Science, University of Surrey, UK
[3]Royal Holloway, University of London, UK
[4]Département d'informatique, Université libre de Bruxelles, Belgium
[5]School of Computer Science, University of Birmingham, UK

October 2020

SAC2020 - WWW

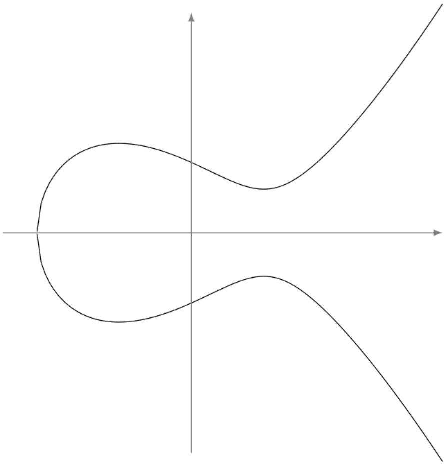
Introduction: Elliptic curves

- Elliptic curves are non-singular plane curves, $(x,y) \in F^2$, satisfying an equation

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

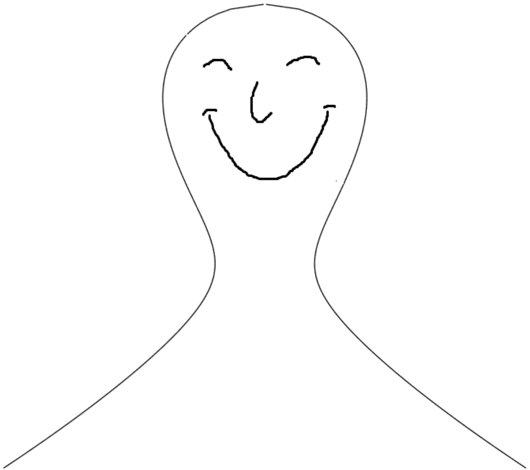
  for fixed a_i in some field F and the point $\mathcal{O}_E$ at infinity.

- Points (x,y) on a curve form an abelian group under the "chord and tangent" rule.



Introduction: Elliptic curves

- Security of elliptic curve cryptography depends on hardness of **ECDLP**: Given P and $[k]P$, compute k.
- Elliptic curves standardised for cryptographic use and widely used.



Koblitz curves and the Frobenius endomorphism

Definition

A Koblitz curve, or subfield curve, is an elliptic curve defined over a small finite field $\mathbb{F}_q$ which is considered over a large extension field $\mathbb{F}_{q^n}$.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad \text{with } x, y \in \mathbb{F}_{q^n} \text{ and } a_i \in \mathbb{F}_q$$

- Standardised by NIST (but now being deprecated).
- Allow for faster scalar multiplication of points.
- q-power Frobenius endomorphism well defined

$$\pi : E(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n}),\ (x, y) \mapsto (x^q, y^q).$$

Koblitz curves and the Frobenius endomorphism

Definition

A Koblitz curve, or subfield curve, is an elliptic curve defined over a small finite field $\mathbb{F}_q$ which is considered over a large extension field $\mathbb{F}_{q^n}$.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad \text{with } x, y \in \mathbb{F}_{q^n} \text{ and } a_i \in \mathbb{F}_q$$

- Standardised by NIST (but now being deprecated).
- Allow for faster scalar multiplication of points.
- q-power Frobenius endomorphism well defined

$$\pi : E(\mathbb{F}_{q^n}) \to E(\mathbb{F}_{q^n}), (x, y) \mapsto (x^q, y^q).$$

Motivation

Idea: Use Frobenius endomorphism on Koblitz curves for cryptanalysis of ECDLP.

Let $|\langle P\rangle| = r$, where P generates the subgroup containing the ECDLP instance.

Pollard's ρ algorithm solves ECDLP in $\mathcal{O}(\sqrt{r})$

$\Downarrow$

Speed-up of $\sqrt{n}$ for Koblitz curves [WZ98]

Index Calculus for ECDLP

$\Downarrow$

Speed-up of n in relation collection and n^2 in linear algebra possible for Koblitz curves [This work]

For higher genus see [Gau00]

Motivation

Idea: Use Frobenius endomorphism on Koblitz curves for cryptanalysis of ECDLP.

Let $|\langle P \rangle| = r$, where P generates the subgroup containing the ECDLP instance.

Pollard's ρ algorithm solves ECDLP in $\mathcal{O}(\sqrt{r})$

$\Downarrow$

Speed-up of $\sqrt{n}$ for Koblitz curves [WZ98]

Index Calculus for ECDLP

$\Downarrow$

Speed-up of n in relation collection and n^2 in linear algebra possible for Koblitz curves [This work]

For higher genus see [Gau00]

Motivation

Idea: Use Frobenius endomorphism on Koblitz curves for cryptanalysis of ECDLP.

Let $|\langle P\rangle| = r$, where P generates the subgroup containing the ECDLP instance.

Pollard's ρ algorithm solves ECDLP in $\mathcal{O}(\sqrt{r})$

$\Downarrow$

Speed-up of $\sqrt{n}$ for Koblitz curves [WZ98]

Index Calculus for ECDLP

$\Downarrow$

Speed-up of n in relation collection and n^2 in linear algebra possible for Koblitz curves [This work]

For higher genus see [Gau00]

Motivation

Idea: Use Frobenius endomorphism on Koblitz curves for cryptanalysis of ECDLP.

Let $|\langle P \rangle| = r$, where P generates the subgroup containing the ECDLP instance.

Pollard's ρ algorithm solves ECDLP in $\mathcal{O}(\sqrt{r})$

$\Downarrow$

Speed-up of $\sqrt{n}$ for Koblitz curves [WZ98]

Index Calculus for ECDLP

$\Downarrow$

Speed-up of n in relation collection and n^2 in linear algebra possible for Koblitz curves [This work]

For higher genus see [Gau00]

Introduction: Index Calculus Method

Idea: Reduce the computation of discrete logarithms to linear algebra!

Framework of index calculus

1. **Factor base:** Define subset $\mathcal{F}$ of elliptic curve.
2. **Relation collection:** Decompose points $[a_j]P + [b_j]Q$ as sum of factor base elements, $\sum_{P_i \in |\mathcal{F}|} e_{ij} P_i$.
3. **Linear algebra:** After collecting $|\mathcal{F}|$ linearly independent relations, compute vector $(\lambda_1, \ldots, \lambda_{|\mathcal{F}|})^T$ in right kernel of matrix $(e_{ji})_{1 \leq i,j \leq |\mathcal{F}|}$.
4. **Compute:** $k = -\frac{\sum_{1 \leq j \leq |\mathcal{F}|} a_j \lambda_j}{\sum_{1 \leq j \leq |\mathcal{F}|} b_j \lambda_j}$

$$\begin{pmatrix} e_{11} & e_{12} & \cdots & e_{1s} \\ e_{21} & e_{22} & \cdots & e_{2s} \\ \vdots & & \ddots & \vdots \\ e_{s1} & e_{s2} & \cdots & e_{ss} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_s \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Introduction: Index Calculus Method

Idea: Reduce the computation of discrete logarithms to linear algebra!

Framework of index calculus

1. **Factor base:** Define subset $\mathcal{F}$ of elliptic curve.
2. **Relation collection:** Decompose points $[a_j]P + [b_j]Q$ as sum of factor base elements, $\sum_{P_i \in |\mathcal{F}|} e_{ij} P_i$.
3. **Linear algebra:** After collecting $|\mathcal{F}|$ linearly independent relations, compute vector $(\lambda_1, \ldots, \lambda_{|\mathcal{F}|})^T$ in right kernel of matrix $(e_{ji})_{1 \leq i,j \leq |\mathcal{F}|}$.
4. **Compute:** $k = -\frac{\sum_{1 \leq j \leq |\mathcal{F}|} a_j \lambda_j}{\sum_{1 \leq j \leq |\mathcal{F}|} b_j \lambda_j}$

$$\begin{pmatrix} e_{11} & e_{12} & \ldots & e_{1s} \\ e_{21} & e_{22} & \ldots & e_{2s} \\ \vdots & & \ddots & \vdots \\ e_{s1} & e_{s2} & \ldots & e_{ss} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_s \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Introduction: Index Calculus Method

Idea: Reduce the computation of discrete logarithms to linear algebra!

Framework of index calculus

1. **Factor base:** Define subset $\mathcal{F}$ of elliptic curve.
2. **Relation collection:** Decompose points $[a_j]P + [b_j]Q$ as sum of factor base elements, $\sum_{P_i \in |\mathcal{F}|} e_{ij} P_i$.
3. **Linear algebra:** After collecting $|\mathcal{F}|$ linearly independent relations, compute vector $(\lambda_1, \ldots, \lambda_{|\mathcal{F}|})^T$ in right kernel of matrix $(e_{ji})_{1 \le i,j \le |\mathcal{F}|}$.
4. **Compute:** $k = -\frac{\sum_{1 \le j \le |\mathcal{F}|} a_j \lambda_j}{\sum_{1 \le j \le |\mathcal{F}|} b_j \lambda_j}$

$$\begin{pmatrix} e_{11} & e_{12} & \ldots & e_{1s} \\ e_{21} & e_{22} & \ldots & e_{2s} \\ \vdots & \ddots & & \vdots \\ e_{s1} & e_{s2} & \ldots & e_{ss} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_s \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Introduction: Index Calculus Method

Idea: Reduce the computation of discrete logarithms to linear algebra!

Framework of index calculus

1. **Factor base:** Define subset $\mathcal{F}$ of elliptic curve.
2. **Relation collection:** Decompose points $[a_j]P + [b_j]Q$ as sum of factor base elements, $\sum_{P_i \in |\mathcal{F}|} e_{ij} P_i$.
3. **Linear algebra:** After collecting $|\mathcal{F}|$ linearly independent relations, compute vector $(\lambda_1, \ldots, \lambda_{|\mathcal{F}|})^T$ in right kernel of matrix $(e_{ji})_{1 \le i,j \le |\mathcal{F}|}$.
4. **Compute:** $k = -\frac{\sum_{1 \le j \le |\mathcal{F}|} a_j \lambda_j}{\sum_{1 \le j \le |\mathcal{F}|} b_j \lambda_j}$

$$\begin{pmatrix} e_{11} & e_{12} & \ldots & e_{1s} \\ e_{21} & e_{22} & \ldots & e_{2s} \\ \vdots & & \ddots & \vdots \\ e_{s1} & e_{s2} & \ldots & e_{ss} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_s \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Idea: Reduce the computation of discrete logarithms to linear algebra!

Framework of index calculus

1. **Factor base:** Define subset $\mathcal{F}$ of elliptic curve.
2. **Relation collection:** Decompose points $[a_j]P + [b_j]Q$ as sum of factor base elements, $\sum_{P_i \in |\mathcal{F}|} e_{ij} P_i$.
3. **Linear algebra:** After collecting $|\mathcal{F}|$ linearly independent relations, compute vector $(\lambda_1, \ldots, \lambda_{|\mathcal{F}|})^T$ in right kernel of matrix $(e_{ji})_{1 \le i,j \le |\mathcal{F}|}$.
4. **Compute:** $k = -\frac{\sum_{1 \le j \le |\mathcal{F}|} a_j \lambda_j}{\sum_{1 \le j \le |\mathcal{F}|} b_j \lambda_j}$

$$\begin{pmatrix} e_{11} & e_{12} & \ldots & e_{1s} \\ e_{21} & e_{22} & \ldots & e_{2s} \\ \vdots & \ddots & & \vdots \\ e_{s1} & e_{s2} & \ldots & e_{ss} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_s \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Introduction: Index Calculus Method

Idea: Reduce the computation of discrete logarithms to linear algebra!

Framework of index calculus

1. **Factor base:** Define subset $\mathcal{F}$ of elliptic curve.
2. **Relation collection:** Decompose points $[a_j]P + [b_j]Q$ as sum of factor base elements, $\sum_{P_i \in |\mathcal{F}|} e_{ij} P_i$.
3. **Linear algebra:** After collecting $|\mathcal{F}|$ linearly independent relations, compute vector $(\lambda_1, \ldots, \lambda_{|\mathcal{F}|})^T$ in right kernel of matrix $(e_{ji})_{1 \le i,j \le |\mathcal{F}|}$.
4. **Compute:** $k = -\frac{\sum_{1 \le j \le |\mathcal{F}|} a_j \lambda_j}{\sum_{1 \le j \le |\mathcal{F}|} b_j \lambda_j}$

$$\begin{pmatrix} e_{11} & e_{12} & \dots & e_{1s} \\ e_{21} & e_{22} & \dots & e_{2s} \\ \vdots & \ddots & & \vdots \\ e_{s1} & e_{s2} & \dots & e_{ss} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_s \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Semaev's summation polynomials $\{S_m \in \mathbb{F}_{q^n}[x_1, \ldots, x_m]\}_{m \in \mathbb{N}}$:
$S_m(X_1, \ldots, X_m) = 0$, if and only if there exist $(Y_1, \ldots, Y_m) \in \overline{\mathbb{F}}_{q^n}^m$ such that $(X_i, Y_i) \in E(\overline{\mathbb{F}}_{q^n})$ for all $1 \leq i \leq m$ and $\sum_{i=1}^m (X_i, Y_i) = \mathcal{O}_E$ on the curve.

Weil descent:
Rewrite polynomials over $\mathbb{F}_{q^n}$ as n equations over $\mathbb{F}_q$.

Framework for elliptic curves due to [Sem04], [Die11] and [Gau09]:

1. **Factor base:** Define $\mathbb{F}_q$-vector subspace V of $\mathbb{F}_{q^n}$ and let

$$\mathcal{F} := \{P \in E(\mathbb{F}_{q^n}) : x(P) \in V\}.$$

2. **Relation collection:**
   - Compute $R = aP + bQ$.
   - Try to find root for $S_{m+1}(x_1, \ldots, x_m, x(R)) \in \mathbb{F}_{q^n}[x_1, \ldots, x_{m+1}]$ with $x_i \in V$.
   - Apply Weil descent and solve polynomial system using Gröbner basis techniques.

Previous work: Faster resolution of the polynomial systems.

This work: Reduce number of required solutions to solve ECDLP on Koblitz curves.

Framework for elliptic curves due to [Sem04], [Die11] and [Gau09]:

1. **Factor base:** Define $\mathbb{F}_q$-vector subspace V of $\mathbb{F}_{q^n}$ and let

$$\mathcal{F} := \{P \in E(\mathbb{F}_{q^n}) : x(P) \in V\}.$$

2. **Relation collection:**
   - Compute $R = aP + bQ$.
   - Try to find root for $S_{m+1}(x_1, \ldots, x_m, x(R)) \in \mathbb{F}_{q^n}[x_1, \ldots, x_{m+1}]$ with $x_i \in V$.
   - Apply Weil descent and solve polynomial system using Gröbner basis techniques.

Previous work: Faster resolution of the polynomial systems.

This work: Reduce number of required solutions to solve
ECDLP on Koblitz curves.

Introduction: Index Calculus Method for elliptic curves

Framework for elliptic curves due to [Sem04], [Die11] and [Gau09]:

1. **Factor base:** Define $\mathbb{F}_q$-vector subspace V of $\mathbb{F}_{q^n}$ and let

$$\mathcal{F} := \{P \in E(\mathbb{F}_{q^n}) : x(P) \in V\}.$$

2. **Relation collection:**
   - Compute $R = aP + bQ$.
   - Try to find root for $S_{m+1}(x_1, \ldots, x_m, x(R)) \in \mathbb{F}_{q^n}[x_1, \ldots, x_{m+1}]$ with $x_i \in V$.
   - Apply Weil descent and solve polynomial system using Gröbner basis techniques.

Previous work: Faster resolution of the polynomial systems.

This work: Reduce number of required solutions to solve ECDLP on Koblitz curves.

Symmetry breaking

Elliptic curves are abelian $\Rightarrow$ can permute m points in solution for the relation search

$$R = P_1 + P_2 + \cdots + P_m.$$

"Breaking symmetry" refers to removing this redundancy.

Variants:

- Rewrite Semaev's summation polynomial in terms of elementary symmetric polynomials [FGHR14].
- Use m disjoint factor bases $\mathcal{F}_i$ and force $P_i \in \mathcal{F}_i$
  $\Rightarrow$ gain factor $(m-1)!$ [Matsuo].

Improved symmetry breaking for Koblitz curves - save m!

Lemma

Let $\langle P\rangle$ be large subgroup of prime order of Koblitz curve that contains the ECDLP instance. Then there exists $\lambda \in \mathbb{Z}$ such that

$$\pi(Q) = [\lambda]Q \text{ for all } Q \in \langle P\rangle.$$

Choose factor bases with $\mathcal{F}_1 = \mathcal{F}$, $\mathcal{F}_2 = \pi(\mathcal{F})$, …, $\mathcal{F}_m = \pi^{m-1}(\mathcal{F})$.

1. Decompose points as sums of the form

$$R = P_1 + \cdots + P_m, \quad \text{where} \quad P_i \in \mathcal{F}_i.$$

2. Rewrite relation as

$$R = P_1' + [\lambda]P_2' + \cdots + [\lambda^{m-1}]P_m' \quad \text{where all } P_i' \in \mathcal{F}_1 = \mathcal{F}.$$

Improved symmetry breaking for Koblitz curves - save $m!$

Lemma

Let $\langle P \rangle$ be large subgroup of prime order of Koblitz curve that contains the ECDLP instance. Then there exists $\lambda \in \mathbb{Z}$ such that

$$\pi(Q) = [\lambda]Q \text{ for all } Q \in \langle P \rangle.$$

Choose factor bases with $\mathcal{F}_1 = \mathcal{F}$, $\mathcal{F}_2 = \pi(\mathcal{F})$, ..., $\mathcal{F}_m = \pi^{m-1}(\mathcal{F})$.

1. Decompose points as sums of the form

$$R = P_1 + \cdots + P_m, \quad \text{where} \quad P_i \in \mathcal{F}_i.$$

2. Rewrite relation as

$$R = P_1' + [\lambda]P_2' + \cdots + [\lambda^{m-1}]P_m' \quad \text{where all } P_i' \in \mathcal{F}_1 = \mathcal{F}.$$

Improved symmetry breaking for Koblitz curves - save $m!$

Lemma

Let $\langle P\rangle$ be large subgroup of prime order of Koblitz curve that contains the ECDLP instance. Then there exists $\lambda \in \mathbb{Z}$ such that

$$\pi(Q) = [\lambda]Q \text{ for all } Q \in \langle P\rangle.$$

Choose factor bases with $\mathcal{F}_1 = \mathcal{F}$, $\mathcal{F}_2 = \pi(\mathcal{F})$, $\ldots$, $\mathcal{F}_m = \pi^{m-1}(\mathcal{F})$.

1. Decompose points as sums of the form

$$R = P_1 + \cdots + P_m, \quad \text{where} \quad P_i \in \mathcal{F}_i.$$

2. Rewrite relation as

$$R = P_1' + [\lambda]P_2' + \cdots + [\lambda^{m-1}]P_m' \quad \text{where all } P_i' \in \mathcal{F}_1 = \mathcal{F}.$$

Frobenius invariant factor bases

Use q-power Frobenius invariant factor bases, i.e. $\pi(\mathcal{F}) = \mathcal{F}$.

$$R = P_1 + P_2 + \cdots + P_m$$

$$\pi(R) = \pi(P_1) + \pi(P_2) + \cdots + \pi(P_m)$$

$$\pi^2(R) = \pi^2(P_1) + \pi^2(P_2) + \cdots + \pi^2(P_m)$$

$$\vdots$$

$$\pi^{n-1}(R) = \pi^{n-1}(P_1) + \pi^{n-1}(P_2) + \cdots + \pi^{n-1}(P_m)$$

Problem:

- Relations might not be linearly independent
  $\Rightarrow$ need more than a single Frobenius invariant factor base for n independent relations

Frobenius invariant factor bases

Use q-power Frobenius invariant factor bases, i.e. $\pi(\mathcal{F}) = \mathcal{F}$.

$$R = P_1 + P_2 + \cdots + P_m$$
$$\pi(R) = \pi(P_1) + \pi(P_2) + \cdots + \pi(P_m)$$
$$\pi^2(R) = \pi^2(P_1) + \pi^2(P_2) + \cdots + \pi^2(P_m)$$
$$\vdots$$
$$\pi^{n-1}(R) = \pi^{n-1}(P_1) + \pi^{n-1}(P_2) + \cdots + \pi^{n-1}(P_m)$$

Problem:

- Relations might not be linearly independent $\Rightarrow$ need more than a single Frobenius invariant factor base for n independent relations

Use q-power Frobenius invariant factor bases, i.e. $\pi(\mathcal{F}) = \mathcal{F}$.

$$R = P_1 + P_2 + \cdots + P_m$$

$$\pi(R) = \pi(P_1) + \pi(P_2) + \cdots + \pi(P_m)$$

$$\pi^2(R) = \pi^2(P_1) + \pi^2(P_2) + \cdots + \pi^2(P_m)$$

$$\vdots$$

$$\pi^{n-1}(R) = \pi^{n-1}(P_1) + \pi^{n-1}(P_2) + \cdots + \pi^{n-1}(P_m)$$

Problem:

- Relations might not be linearly independent $\Rightarrow$ need more than a single Frobenius invariant factor base for n independent relations

Frobenius invariant factor bases

Use q-power Frobenius invariant factor bases, i.e. $\pi(\mathcal{F}) = \mathcal{F}$.

$$R = P_1 + P_2 + \cdots + P_m$$
$$\pi(R) = \pi(P_1) + \pi(P_2) + \cdots + \pi(P_m)$$
$$\pi^2(R) = \pi^2(P_1) + \pi^2(P_2) + \cdots + \pi^2(P_m)$$
$$\vdots$$
$$\pi^{n-1}(R) = \pi^{n-1}(P_1) + \pi^{n-1}(P_2) + \cdots + \pi^{n-1}(P_m)$$

Problem:

- Relations might not be linearly independent
  $\Rightarrow$ need more than a single Frobenius invariant factor base for n independent relations

Frobenius invariant factor bases

Use q-power Frobenius invariant factor bases, i.e. $\pi(\mathcal{F}) = \mathcal{F}$.

$$
\begin{aligned}
R &= P_1 + P_2 + \cdots + P_m \\
\pi(R) &= \pi(P_1) + \pi(P_2) + \cdots + \pi(P_m) \\
\pi^2(R) &= \pi^2(P_1) + \pi^2(P_2) + \cdots + \pi^2(P_m) \\
&\vdots \\
\pi^{n-1}(R) &= \pi^{n-1}(P_1) + \pi^{n-1}(P_2) + \cdots + \pi^{n-1}(P_m)
\end{aligned}
$$

Problem:

- Relations might not be linearly independent $\Rightarrow$ need more than a single Frobenius invariant factor base for n independent relations

Frobenius invariant factor bases

An even better deal: Reduce the Frobenius invariant factor base(s) $\mathcal{F}$ to a smaller factor base(s) $\mathcal{F}'$ containing single representatives for each orbit.

- Rewrite relations in the form

$$R = [\lambda^{i_1}]P_1 + [\lambda^{i_2}]P_2 + \cdots + [\lambda^{i_m}]P_m \text{ where } P_i \in \mathcal{F}'.$$

- Need n times fewer relations.
- Reduce (sparse) linear algebra cost by $\approx n^2$.

Frobenius invariant factor bases

An even better deal: Reduce the Frobenius invariant factor base(s) $\mathcal{F}$ to a smaller factor base(s) $\mathcal{F}'$ containing single representatives for each orbit.

- Rewrite relations in the form

$$R = [\lambda^{i_1}]P_1 + [\lambda^{i_2}]P_2 + \cdots + [\lambda^{i_m}]P_m \text{ where } P_i \in \mathcal{F}'.$$

- Need n times fewer relations.
- Reduce (sparse) linear algebra cost by $\approx n^2$.

Examples of Frobenius invariant factor bases

Factor bases from **linearised polynomials**:

- $x^n - 1$ factors in $\mathbb{F}_2[x]$ as $(x-1)f_1 f_2 \dots f_s$, where the f_i are distinct irreducible polynomials of degree $\ell :=$ order of $2 \bmod n$.
- Let $f_j = \sum_k f_{j,k} x^k$ of degree ℓ and consider linearised polynomial

$$F_j(X) = \sum_k f_{j,k} X^{2^k}.$$

- $\mathcal{F} := \{P \in E(\mathbb{F}_{2^n}) : F_j(x(P)) = 0\}$ is a Frobenius invariant factor base of size $\approx 2^\ell$.

Further Frobenius invariant factor bases can be constructed using isogenies between algebraic tori and elliptic curves respectively [CL08].

Examples of Frobenius invariant factor bases

Factor bases from **linearised polynomials**:

- $x^n - 1$ factors in $\mathbb{F}_2[x]$ as $(x-1)f_1 f_2 \dots f_s$, where the f_i are distinct irreducible polynomials of degree $\ell :=$ order of $2 \bmod n$.
- Let $f_j = \sum_k f_{j,k} x^k$ of degree ℓ and consider linearised polynomial

$$F_j(X) = \sum_k f_{j,k} X^{2^k}.$$

- $\mathcal{F} := \{P \in E(\mathbb{F}_{2^n}) : F_j(x(P)) = 0\}$ is a Frobenius invariant factor base of size $\approx 2^\ell$.

Further Frobenius invariant factor bases can be constructed using isogenies between algebraic tori and elliptic curves respectively [CL08].

Examples of Frobenius invariant factor bases

Factor bases from **linearised polynomials**:

- $x^n - 1$ factors in $\mathbb{F}_2[x]$ as $(x-1)f_1 f_2 \ldots f_s$, where the f_i are distinct irreducible polynomials of degree $\ell :=$ order of $2 \bmod n$.
- Let $f_j = \sum_k f_{j,k} x^k$ of degree ℓ and consider linearised polynomial

$$F_j(X) = \sum_k f_{j,k} X^{2^k}.$$

- $\mathcal{F} := \{P \in E(\mathbb{F}_{2^n}) : F_j(x(P)) = 0\}$ is a Frobenius invariant factor base of size $\approx 2^\ell$.

Further Frobenius invariant factor bases can be constructed using isogenies between algebraic tori and elliptic curves respectively [CL08].

Motivation: Are the polynomial systems during index calculus with Frobenius invariant factor bases equally hard to solve as for standard choices? It depends!

- Factor base from linearised polynomials: $\approx$ Yes.
- Other constructions: Our experiments look less promising.

Further work is needed.

Experimental results

Motivation: Are the polynomial systems during index calculus with Frobenius invariant factor bases equally hard to solve as for standard choices? It depends!

- Factor base from linearised polynomials: $\approx$ Yes.
- Other constructions: Our experiments look less promising.

Further work is needed.

Experimental results

Motivation: Are the polynomial systems during index calculus with Frobenius invariant factor bases equally hard to solve as for standard choices? It depends!

- Factor base from linearised polynomials: $\approx$ Yes.
- Other constructions: Our experiments look less promising.

Further work is needed.

Perspectives and open problems

- How to exploit the blocks and homogeneous structure of polynomial systems arising from Frobenius invariant factor bases using the constructions of Couveignes-Lercier [CL08].
- Study practical impact asymptotically and for different characteristics.
- Give precise complexity estimates of index calculus methods for elliptic curves.

Conclusion

- Index calculus speed-up by factor $\approx n$ for relation collection step and $\approx n^2$ for linear algebra step for Koblitz curves.
- Construction of Frobenius invariant factor bases for some parameters.
- Larger speed-up of index calculus than speed-up of Pollard ρ for Koblitz curves, but index calculus still worse for curves used in practice.
- Security of Koblitz curves remains strong

Conclusion

- Index calculus speed-up by factor $\approx n$ for relation collection step and $\approx n^2$ for linear algebra step for Koblitz curves.
- Construction of Frobenius invariant factor bases for some parameters.
- Larger speed-up of index calculus than speed-up of Pollard ρ for Koblitz curves, but index calculus still worse for curves used in practice.
- Security of Koblitz curves remains strong