Algebraic approaches for the Elliptic Curve Discrete Logarithm Problem over Prime Fields

Christophe Petit, Michiel Kosters, Ange Messeng

University of Oxford, University of California Irvine,
University of Passau

Elliptic Curve Discrete Logarithm Problem

- **Elliptic Curve Discrete Logarithm Problem** (ECDLP)
  Let K a finite field and let E be an elliptic curve over K.
  Let $P \in E(K)$ and let $Q \in G :=< P >$.
  Find $k \in \mathbb{Z}$ such that $Q = kP$.
- In practice K is a prime field, a binary field with prime degree extension, or $\mathbb{F}_{p^n}$ with n relatively small

Elliptic Curve Discrete Logarithm Problem

- **Elliptic Curve Discrete Logarithm Problem** (ECDLP)
  Let K a finite field and let E be an elliptic curve over K.
  Let $P \in E(K)$ and let $Q \in G :=< P >$.
  Find $k \in \mathbb{Z}$ such that $Q = kP$.
- In practice K is a prime field, a binary field with prime degree extension, or $\mathbb{F}_{p^n}$ with n relatively small
- **Elliptic Curve Cryptography secure** $\Rightarrow$ **ECDLP hard**

Is ECDLP hard ?

- Can apply generic attacks

Is ECDLP hard ?

- Can apply generic attacks
- For exceptional parameters, can reduce it to another discrete logarithm problem
  - Anomalous attack
  - Reduction to finite field DLP using pairings
  - Reduction to a hyperelliptic curve DLP

Is ECDLP hard ?

- Can apply generic attacks
- For exceptional parameters, can reduce it to another discrete logarithm problem
  - Anomalous attack
  - Reduction to finite field DLP using pairings
  - Reduction to a hyperelliptic curve DLP
- Index calculus approaches being developed since 2004, but mostly focused on extension fields

Is ECDLP hard ?

- Can apply generic attacks
- For exceptional parameters, can reduce it to another discrete logarithm problem
  - Anomalous attack
  - Reduction to finite field DLP using pairings
  - Reduction to a hyperelliptic curve DLP
- Index calculus approaches being developed since 2004, but mostly focused on extension fields
- Our goal : extend previous index calculus algorithms to ECDLP over prime fields

Outline

Previous index calculus algorithms for ECDLP

New variants for curves over prime fields

Outline

Previous index calculus algorithms for ECDLP

New variants for curves over prime fields

Index Calculus for Elliptic Curves

1. Fix $m \in \mathbb{Z}$, and fix $V \subset K$ with $|V|^m \approx K$
   Define a *factor basis*

$$\mathcal{F} = \{(x, y) \in E(K) \mid x \in V\}$$

Index Calculus for Elliptic Curves

1. Fix $m \in \mathbb{Z}$, and fix $V \subset K$ with $|V|^m \approx K$
   Define a *factor basis*

$$\mathcal{F} = \{(x, y) \in E(K) \mid x \in V\}$$

2. Compute about $|\mathcal{F}|$ *relations*

$$a_i P + b_i Q \;=\; P_{i,1} + P_{i,2} + \ldots + P_{i,m}$$

   with $P_{i,j} \in \mathcal{F}$

Index Calculus for Elliptic Curves

1. Fix $m \in \mathbb{Z}$, and fix $V \subset K$ with $|V|^m \approx K$
   Define a *factor basis*

$$\mathcal{F} = \{(x, y) \in E(K) \mid x \in V\}$$

2. Compute about $|\mathcal{F}|$ *relations*

$$a_i P + b_i Q \;=\; P_{i,1} + P_{i,2} + \ldots + P_{i,m}$$

   with $P_{i,j} \in \mathcal{F}$
3. Linear algebra on relations gives $aP + bQ = 0$

Relation search : Semaev polynomials

- **Semaev polynomials** relate the x-coordinates of points that sum up to 0 :
  $S_r(x_1, \ldots, x_r) = 0$
  $\Leftrightarrow\ \exists (x_i, y_i) \in E(\bar{K})$ s.t. $(x_1, y_1) + \cdots + (x_r, y_r) = 0$

- **Relation search**
  - Compute $(X, Y) := aP + bQ$ for random a, b
  - Search for $x_i \in V$ with $S_{m+1}(x_1, \ldots, x_m, X) = 0$
  - For any such solution, find corresponding y_i values

Existing Variants

- Semaev
  - $K = \mathbb{F}_p$ and V contains all "small" elements
  - No algorithm to solve S_{m+1}

Existing Variants

- Semaev
  - $K = \mathbb{F}_p$ and V contains all "small" elements
  - No algorithm to solve S_{m+1}
- Gaudry-Diem
  - $K = \mathbb{F}_{q^n}$ and $V = \mathbb{F}_q$
  - Reduction to polynomial system over $\mathbb{F}_q$
  - Generic bounds give $L_{q^n}(2/3)$ complexity if $q = L_{q^n}(2/3)$

Existing Variants

- Semaev
  - $K = \mathbb{F}_p$ and V contains all "small" elements
  - No algorithm to solve S_{m+1}
- Gaudry-Diem
  - $K = \mathbb{F}_{q^n}$ and $V = \mathbb{F}_q$
  - Reduction to polynomial system over $\mathbb{F}_q$
  - Generic bounds give $L_{q^n}(2/3)$ complexity if $q = L_{q^n}(2/3)$
- Diem, FPPR, P-Quisquater
  - $K = \mathbb{F}_{2^n}$ and V a vector space of K over $\mathbb{F}_2$
  - Reduction to polynomial system over $\mathbb{F}_2$
  - Experiments suggest system "somewhat easy"

Relation search : Weil Descent

- For each relation solve a *generalized root-finding problem*

  Given $f \in \mathbb{F}_{q^n}[x_1, \ldots, x_m]$ *and vector space* $V \subset \mathbb{F}_{q^n}$*,*
  find $x_i \in V$ *such that* $f(x_1, \ldots, x_m) = 0$

Relation search : Weil Descent

- For each relation solve a *generalized root-finding problem*

  Given $f \in \mathbb{F}_{q^n}[x_1, \ldots, x_m]$ *and vector space* $V \subset \mathbb{F}_{q^n}$*,*
  find $x_i \in V$ *such that* $f(x_1, \ldots, x_m) = 0$

- Solved by Weil Descent : reduction to polynomial system
  - Fix a basis for V over $\mathbb{F}_q$
  - Introduce variables $x_{ij} \in \mathbb{F}_q$ with $x_i = \sum_j x_{ij} v_j$
  - See single equation $f\left(\sum_j x_{1j} v_j, \ldots, \sum_j x_{mj} v_j\right) = 0$
    over $\mathbb{F}_{q^n}$ as a system of n equations over $\mathbb{F}_q$

Limits of previous works

- Fields with $q = L_{q^n}(2/3)$ are not used in practice

Limits of previous works

- Fields with $q = L_{q^n}(2/3)$ are not used in practice
- In binary case asymptotic complexity is not clear, and practical complexity is poor

Limits of previous works

- Fields with $q = L_{q^n}(2/3)$ are not used in practice
- In binary case asymptotic complexity is not clear, and practical complexity is poor
- Not clear how to extend to prime fields : no subspace available and we a priori want small degree equations

Outline

Previous index calculus algorithms for ECDLP

New variants for curves over prime fields

Main idea

- Find low degree rational maps L_j such that

$$\#\{x \in \mathbb{F}_p \mid L(x) = L_{n'} \circ \ldots \circ L_1(x) = 0\} \approx \prod \deg L_j \approx p^{1/m}$$

- Define $V = \{x \in \mathbb{F}_p \mid L(x) = 0\}$
- Define $\mathcal{F} = \{(x, y) \in E(K) \mid x \in V\}$

Main idea

- Find low degree rational maps L_j such that

$$\#\{x \in \mathbb{F}_p \mid L(x) = L_{n'} \circ \ldots \circ L_1(x) = 0\} \approx \prod \deg L_j \approx p^{1/m}$$

- Define $V = \{x \in \mathbb{F}_p \mid L(x) = 0\}$
- Define $\mathcal{F} = \{(x, y) \in E(K) \mid x \in V\}$

- Relation search : solve the polynomial system

$$\begin{cases} S_{m+1}(x_{11}, \ldots, x_{m1}, X) = 0 & \\ x_{i,j+1} = L_j(x_{i,j}) & i = 1, \ldots, m; j = 1, \ldots, n' - 1 \\ 0 = L_{n'}(x_{i,n'}) & i = 1, \ldots, m. \end{cases}$$

Remarks

- One can write similar systems in binary cases, and show they are equivalent to Weil descent systems
- *Precomputation* of the maps L_j can a priori be used for any DLP defined over any curve over the same field

Remarks

- One can write similar systems in binary cases, and show they are equivalent to Weil descent systems
- *Precomputation* of the maps L_j can a priori be used for any DLP defined over any curve over the same field
- Remaining of the talk :
  - How to compute the maps L_j ?
  - How to solve the system ?

Finding good maps : $p-1$ "smooth"

- Suppose $\mathbf{p-1} = S \cdot N'$ with $S \approx p^{1/m}$ **smooth**
- We want low degree rational maps L_j such that

$$\#\{x \in \mathbb{F}_p \mid L(x) = L_{n'} \circ \ldots \circ L_1(x) = 0\} \approx \prod \deg L_j \approx p^{1/m}$$

Finding good maps : $p-1$ "smooth"

- Suppose $\mathbf{p-1} = S \cdot N'$ with $S \approx p^{1/m}$ **smooth**
- We want low degree rational maps L_j such that

$$\#\{x \in \mathbb{F}_p \mid L(x) = L_{n'} \circ \ldots \circ L_1(x) = 0\} \approx \prod \deg L_j \approx p^{1/m}$$

- Take $L(X) = X^S - 1$ and V subgroup of order S in $\mathbb{F}_p^*$
- If $S = \prod_{j=1}^{n'} q_j$ take $L_j(X) = X^{q_j}$ and $L_{n'}(X) = X^{q_{n'}} - 1$

Finding good maps : $p-1$ "smooth"

- Suppose $\mathbf{p}-\mathbf{1}=S\cdot N'$ with $S\approx p^{1/m}$ **smooth**
- We want low degree rational maps L_j such that

$$\#\{x\in\mathbb{F}_p\mid L(x)=L_{n'}\circ\ldots\circ L_1(x)=0\}\approx\prod\deg L_j\approx p^{1/m}$$

- Take $L(X)=X^S-1$ and V subgroup of order S in $\mathbb{F}_p^*$
- If $S=\prod_{j=1}^{n'}q_j$ take $L_j(X)=X^{q_j}$ and $L_{n'}(X)=X^{q_{n'}}-1$
- Remark : NIST P-224 curve satisfies

$$p-1=2^{96}\cdot N'$$

Finding good maps : isogeny Kernels

- Find an **auxiliary curve** E' with $\#E'(\mathbb{F}_p) = S \cdot N'$ and $S = \prod_{j=1}^{n'} q_j \approx p^{1/m}$ smooth
- Let G be a subgroup of $E'(\mathbb{F}_p)$ with order S

Finding good maps : isogeny Kernels

- Find an **auxiliary curve** E' with $\#E'(\mathbb{F}_p) = S \cdot N'$ and $S = \prod_{j=1}^{n'} q_j \approx p^{1/m}$ smooth
- Let G be a subgroup of $E'(\mathbb{F}_p)$ with order S
- Compute isogenies φ_j such that $\varphi = \varphi_{n'} \circ \ldots \circ \varphi_1$ has kernel G

Finding good maps : isogeny Kernels

- Find an **auxiliary curve** E' with $\#E'(\mathbb{F}_p) = S \cdot N'$ and $S = \prod_{j=1}^{n'} q_j \approx p^{1/m}$ smooth
- Let G be a subgroup of $E'(\mathbb{F}_p)$ with order S
- Compute isogenies φ_j such that $\varphi = \varphi_{n'} \circ \ldots \circ \varphi_1$ has kernel G
- Take L_j the x-coordinate part of φ_j, except for $L_{n'}$ taken in a slightly different way

Finding a smooth order curve

- Method 1 : pick random curves
- Method 2 : use complex multiplication

Finding a smooth order curve

- Method 1 : pick random curves
- Method 2 : use complex multiplication

- Method 1 needs at most $\approx |\mathcal{F}|$ trials on average
- Method 2 more efficient when you can chose p yourself (kind of trapdoor)

Solving the system

- Relation search : solve the polynomial system

$$\begin{cases} S_{m+1}(x_{11}, \ldots, x_{m1}, X) = 0 & \\ x_{i,j+1} = L_j(x_{i,j}) & i = 1, \ldots, m; j = 1, \ldots, n' - 1 \\ 0 = L_{n'}(x_{i,n'}) & i = 1, \ldots, m. \end{cases}$$

Solving the system

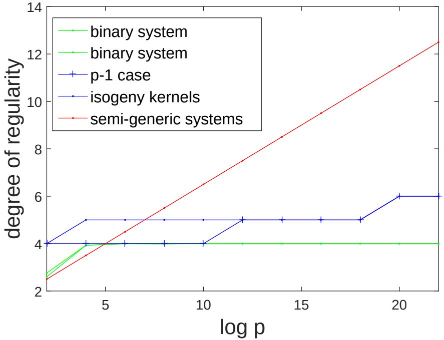
- Relation search : solve the polynomial system

$$\begin{cases} S_{m+1}(x_{11}, \ldots, x_{m1}, X) = 0 & \\ x_{i,j+1} = L_j(x_{i,j}) & i = 1, \ldots, m; j = 1, \ldots, n' - 1 \\ 0 = L_{n'}(x_{i,n'}) & i = 1, \ldots, m. \end{cases}$$

- Low degree equations, block triangular structure
- mn' variables and $mn' + 1$ equations
- Seems reasonable to expect dedicated algorithms, but here we start with Groebner basis algorithms

Groebner Basis Experiments

- Studied comparable size systems in binary and prime cases
- Measured average values of degree of regularity
- Compared with semi-generic systems



Solving the system : complexity ?

- Algorithm only practical for small parameters
- Generic bounds for solving polynomial systems suggest exponential-time ECDLP algorithm

Solving the system : complexity ?

- Algorithm only practical for small parameters
- Generic bounds for solving polynomial systems suggest exponential-time ECDLP algorithm
- Experiments using Groebner basis suggest systems easier than random systems of same size
- Sparse, block-triangular structure, and resemblance to the (polynomial time solvable) root-finding problem suggest to build dedicated algorithms to solve the systems

Solving the system : complexity ?

- Algorithm only practical for small parameters
- Generic bounds for solving polynomial systems suggest exponential-time ECDLP algorithm
- Experiments using Groebner basis suggest systems easier than random systems of same size
- Sparse, block-triangular structure, and resemblance to the (polynomial time solvable) root-finding problem suggest to build dedicated algorithms to solve the systems
- Open problem !

Conclusion

- Suggested an approach to generalize previous ECDLP algorithms to elliptic curves over prime fields
- Like previous ones, algorithm only practical for very small parameters (Pollard's rho definitely better for crypto sizes)
- Open problems : asymptotic complexity, dedicated polynomial system solving methods