Index calculus attacks on hyperelliptic curves with efficient endomorphisms

Sulamithe TSAKOU and Sorina Ionica

MIS, University of Picardie Jules Verne

22 Novembre 2022

Discrete logarithm problem (DLP)

The security of many existing cryptographic schemes relies on the difficulty of solving the discrete logarithm problem (DLP).

The discrete logarithm problem in $\mathbb{G}$

Given $g, h \in \mathbb{G}$ such that $\mathbb{G} =< g >$, find (if it exists) x such that

$$h = xg.$$

- The simplest attack: exhaustive search can find $x \in \{1, \cdots, \#\mathbb{G}\}$ in time $O(\#\mathbb{G})$.
- In a generic group, we can attack the DLP with the baby-step-giant-step algorithm, the Pollard-rho algorithm or the Pohlig-Hellman reduction .
- For certain groups that we know the structure, we can use the index calculus algorithm to solve the DLP.

Index calculus

- Define a factor base : $\mathcal{F} = \{g_1, g_2, \ldots, g_N\}$
- Relation search: $\forall a_i \in \mathbb{Z}$ random, decompose $a_i g = \sum_{j=1}^{N} c_{ij} g_j$ until N relations are found
- Linear algebra: take $A = (a_i)_{i=\overline{1,N}}$ and $M = (c_{ij})_{i,j=\overline{1,N}}$
  - Find $X = (x_1, x_2, \cdots, x_N)$ unique solution of $MX = A \pmod{r}$.
- Descent phase: take random $a, b \in \mathbb{Z}$ and decompose $ag + bh = \sum_{j=1}^{N} c_j g_j$, $(b, r) = 1$. Compute $x = log_g h = (\sum_{j=1}^{N} c_j x_j - a) b^{-1}$

Index calculus attacks on elliptic curves

Let E be an elliptic curve defined over $\mathbb{F}_{q^n}$.

- Factor base $\mathcal{F}_x = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}(Gaudry)$.
- Search for relations of the form $R = P_1 + P_2 + \cdots + P_n$; $P_i \in \mathcal{F}_x$, $i = 1, 2, \cdots, n$.

Semaev polynomials

There exists $S_{x,n+1} \in \mathbb{F}_{q^n}[X_1, X_2, \cdots, X_{n+1}]$ such that $R = P_1 + P_2 + \cdots + P_n$ if and only if

$$S_{x,n+1}(x(P_1), x(P_2), \cdots, x(P_n), x(R)) = 0. \qquad (1)$$

Perform Weil descent over $\mathbb{F}_q$ and get a system $\mathcal{S}$ of n equations and n variables which is then solved using Gröbner basis algorithms

Remark: $S_{x,n+1}$ is symmetric and has degree 2^{n-1} in each variable.

The complexity of the index calculus on elliptic curve

Let E be an elliptic curve defined over $\mathbb{F}_{q^n}$.

- The factor basis $\mathcal{F}_x$ has approximately q elements.
- The probability that a random point decomposes in n elements of $\mathcal{F}_x$ is
$$\frac{\#\mathcal{F}_x^n/S_n}{\#E(\mathbb{F}_{q^n})} = \frac{1}{n\,!}.$$

The complexity of the index calculus on elliptic curve

- The complexity of solving the polynomial system is in

$$\mathcal{O}\left(\begin{pmatrix} n+d \\ n \end{pmatrix}^{\omega}\right)$$

where d is the solving degree of the system. Assuming that $\mathcal{S}$ is regular, d is bounded by $n2^{n-1} - n + 1$.

- By using Stirling's formula, the complexity of the relation search step is in

$$\mathcal{O}\left(n!(2^{n(n-1)}e^n n^{-1/2})^{\omega} q\right).$$

- The linear algebra step has a complexity in $\mathcal{O}(cq^2)$.

The "$n-1$" variant (Joux-Vitse 2011)

Decomposition in $n-1$ points

- Compute the n-th summation polynomial instead of the $(n+1)$-th.
- Obtain a polynomial system $\mathcal{S}$ of n equations with $n-1$ variables of total degree 2^{n-2}.
- The probability to decompose a given point in the factor base is $\frac{1}{(n-1)!q}$

Complexity of the $n-1$ variant

The complexity of the variant $n-1$ is in

$$\mathcal{O}\left((n-1)!(2^{(n-1)(n-2)}e^n n^{-1/2})^{\omega} q^2\right).$$

The "$n-2$" variant (T.- Ionica 2022)

Compute the $(n-1)$-th summation polynomial instead of the n-th.

A better complexity of the Grobner basis computation

$$\mathcal{O}\left((2^{(n-2)(n-3)}e^n n^{-1/2})^\omega\right).$$

On a curve defined over $\mathbb{F}_{q^6}$ where q is a 20 bits prime number, we have found a relation in about 9 days.

Reducing the factor base (FGHR 2012)

Take $T_2 \in E[2]$. Given

$$R = P_1 + P_2 + \cdots + P_n \tag{2}$$

with $P_i \in \mathcal{F}_x$ then

$$R = (P_1 + k_1 T_2) + (P_2 + k_2 T_2) + \ldots + (P_n + k_n T_2), \tag{3}$$

with $\sum k_i = 0 \pmod 2$ if and only if $P_i + k_i T_2 \in \mathcal{F}_x$.

Theorem (FHJRV 2014)

Let $T_2 \in E(\mathbb{F}_{q^n})[2]$ + extra conditions. There exists $\mu : E \to \mathbb{P}_1$ of degree 2 such that

$$\mathcal{F}_\mu = \{P \in E(\mathbb{F}_{q^n}) : \mu(P) \in \mathbb{P}_1(\mathbb{F}_q)\}$$

is invariant under the action of T_2.

Reducing the factor base

Semaev polynomials with respect to μ

There exists a unique monic $S_{\mu,m} \in \mathbb{F}_{q^n}[X_1, \ldots, X_m]$ such that for all $P_i \in E(\mathbb{F}_{q^n})$:

$$\mu(P_i) = \mu_i \text{ and } \sum_{i=1}^{m} P_i = \mathcal{O} \text{ iff } S_{\mu,m}(\mu_1, \ldots, \mu_m) = 0. \tag{1}$$

Further improvements

- Reduce factor base size by a factor 2 for certain elliptic curves.
- $S_{\mu,m}$ has more symmetries than $S_{x,m}$ $\rightarrow$ faster decompositions by a factor $2^{\omega(m-2)}$.

Our idea

- Let E be an ordinary elliptic curve defined over $\mathbb{F}_{q^n}$ such that $\#E(\mathbb{F}_{q^n}) = hr$, h small, r large prime. Let $G =< P >$ the subgroup of order r.

- Consider $\phi : E \to E$ then $\phi(P) = \lambda P$, where λ is known. Morever we assume that $\phi^k = \pm 1 \pmod{r}$.

- Suppose that for $Q \in \mathcal{F}_\mu$ then $\phi(Q) \in \mathcal{F}_\mu$.
- Then we can perform index calculus on $\mathcal{F}_\mu / \sim$, where $Q \sim \lambda^i Q$, $i \in \{1, \ldots, k-1\}$.

Our idea

- The size of the factor base is reduced by a factor of k.
- The probability that a point decomposes in $\mathcal{F}_\mu/\sim$ and the complexity of the solving the polynomial systems is inchanged.
- Then, we improve the complexity of the relation search step by a factor of k.
- We improve the complexity of the linear algebra step by a factor of k^2.

Remark: $Q \sim -Q$ was already used in the initial proposal for $\mathcal{F}_x$.

The Frobenius was used on binary elliptic curves by Galbraith *et al* (2020) and J.-J. Chi-Domínguez, F. Rodríguez-Henríquez, and B. Smith (2021).

Curves defined over an extension field of composite degree

- Let E be a crypto friendly elliptic curve defined over $\mathbb{F}_{q^n}$ with $q \geq 2$, $n = m_1 m_2$, $m_1 \in \{2, 3, 4\}$ and m_2 a large prime.
- Assume that E admits a model over $\mathbb{F}_{q^{m_1}}$. The curve E admits $\pi_{m_1} : P = (x, y) \mapsto (x^{q^{m_1}}, y^{q^{m_1}})$.
- Define the factor basis by $\mathcal{F}_{E,x} = \{P \in E(\mathbb{F}_{q^n}) \mid x(P) \in \mathbb{F}_{q^{m_2}}\}$. For $Q \in \mathcal{F}_{E,x}$ then $\pi_{m_1}(Q) \in \mathcal{F}_{E,x}$.
- We can perform the index calculus algorithm on $\mathcal{F}_{E,x}/\sim$ where $P \sim \pi^i_{m_1}(P)$, $i \in \{1, \cdots, m_2 - 1\}$.

Theorem (T.- Ionica 2021)

The complexity of the relation collection step in the index calculus algorithm in the group $E(\mathbb{F}_{q^n})$ with $n = m_1 m_2$ is

$$\mathcal{O}(\frac{q^{m_2}}{m_2}\left(2^{m_1(m_1-1)} e^{m_1} m_1^{-1/2}\right)^{\omega} m_1! + q^{m_2} m_1)$$

GLV curves

Introduced by Gallant, Lambert and Vanstone.

- Let $q \equiv 1 \pmod 4$ be a prime, $E_1 : y^2 = x^3 + ax$, $a \in \mathbb{F}_{q^n}$ and $\alpha \in \mathbb{F}_{q^n}$ of order 4
- $\phi : E_1 \to E_1$ defined by $P = (x, y) \mapsto (-x, \alpha y)$.
- $\mathcal{F}_{E_1,x} = \{P \in E_1(\mathbb{F}_{q^n}) \mid x(P) \in \mathbb{F}_q\}$ is closed under ϕ.

- Let $q \equiv 1 \pmod 3$ be a prime, $E_2 : y^2 = x^3 + b$, $b \in \mathbb{F}_{q^n}$ and $\beta \in \mathbb{F}_{q^n}$ the cubic root of 1 in $\mathbb{F}_q$
- $\psi : E_2 \to E_2$ defined by $P = (x, y) \mapsto (\beta x, y)$.
- The factor base $\mathcal{F}_{E_2,x}$ is closed with respect to ψ.

Choosing the factor base

Assume that $\mu : E \to \mathbb{P}_1$ such that $\mu(P) = \mu(-P)$ for $P \in E(\mathbb{F}_{q^n})$ and index calculus performs on $\mathcal{F}_\mu$. Recall $\phi^k = \pm 1$.

Trace and norm with respect to ϕ

$$\begin{aligned} \mathrm{Tr}_\phi(\mu) : E &\to \mathbb{P}_1 \\ Q &\mapsto (\mu(Q) + \mu(\phi(Q)) + \cdots + \mu(\phi^{k-1}(Q)), 1) \\ N_\phi(\mu) : E &\to \mathbb{P}_1 \\ Q &\mapsto (\mu(Q) \bullet \mu(\phi(Q)) \bullet \cdots \bullet \mu(\phi^{k-1}(Q)), 1). \end{aligned}$$

Redefine the factor base for $\mu' = \mathrm{Tr}_\phi(\mu)$. Then the factor base $\mathcal{F}_{\mu'}$ is invariant under ϕ.

Index calculus on GLS curves

Galbraith, Lynn and Scott 2008

Let E defined over $\mathbb{F}_q$, E' a quadratic twist such that $E'(\mathbb{F}_{q^n})$ is crypto friendly. Take $\phi : E \to E'$ the twist and define

$$\psi = \phi \pi \phi^{-1}$$

Then $\psi^n(Q) + Q = 0$ for all points in $Q \in E'(\mathbb{F}_{q^n})$.

Define the factor base using $\mu' = \mathrm{Tr}_\psi(x)$. We get

$$\begin{aligned} \mu' : E' &\to \mathbb{P}^1 \\ Q &\mapsto x(Q) + u^k x(Q)^q + u^{k(1+q)} x(Q)^{q^2} + \cdots + u^{k(1+q+\cdots+q^{n-2})} x(Q)^{q^{n-1}} \end{aligned}$$

has degree q^{n-1}.

Index calculus on GLS curves

Relation collection on $\mathcal{F}_{\mu'}/\sim$ where $Q \sim \psi(Q)$.

Weil descent

- Take a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, i.e. $\{\omega, \ldots, \omega^{q^{n-1}}\}$.
- In $S_{x,n+1}(X_1, \ldots, X_n, x_R) = 0$ substitute $X_i,\ 1 \leq i \leq n$ by

$$X_{i1}\omega + X_{i2}\omega^q + \ldots + X_{in}\omega^{q^{n-1}}.$$

- Look for $(X_{ij})_{1 \leq i,j \leq n}$ such that
$\mu'_i = X_i + u^k X_i^q + u^{k(1+q)} X_i^{q^2} + \cdots + u^{k(1+q+\cdots+q^{n-2})} X_i^{q^{n-1}} \in \mathbb{F}_q$

Reduce the complexity of the relation search step to that of solving a system of n equations and n variables of degree 2^{n-1}.

Theorem (T.- Ionica 2021)

The relation collection on E' with the factor basis $\mathcal{F}_{\mu'}$ has complexity

$$\mathcal{O}((n-1)\,!(2^{n(n-2)}e^n n^{-1/2})^{\omega} q)$$

Curves admitting a 2-torsion point

- Let $E : y^2 = x^3 + ax$ defined over $\mathbb{F}_{q^n}$, such that $q \equiv 1 \pmod 4$ with $a \in \mathbb{F}_q$.
- This curve admit a 2-torsion point $T_2 = (0,0)$ and for $P = (x,y)$, $x(P + T_2) = \frac{x^3+ax}{x^2} - x \in \mathbb{F}_q$ whenever $x \in \mathbb{F}_q$.
- Define the factor basis by

$$\mathcal{F}_{E,x} = \{P \in E_1(\mathbb{F}_{q^n}) \mid x(P) \in \mathbb{F}_q\}.$$

  For a given point Q, the points $Q, Q + T_2 \in \mathcal{F}_{E,x}$.
- We can reduce the factor basis by a factor 2 with respect to the equivalence class $\{Q, Q + T_2\}$.

Curves admitting an efficient endomorphism and a 2-torsion point

Let E be an elliptic curve defined over the finite field $\mathbb{F}_{q^n}$.

Theorem (FHJRV 2014)

Let $T_2 \in E(\mathbb{F}_{q^n})[2]$ + extra conditions. There exists $\mu : E \to \mathbb{P}_1$ of degree 2 such that

$$\mathcal{F}_\mu = \{P \in E(\mathbb{F}_{q^n}) : \mu(P) \in \mathbb{P}_1(\mathbb{F}_q)\}$$

is invariant under the action of T_2.

Curves admitting an efficient endomorphism and a 2-torsion point

- E admits an endomorphism ψ such that $\psi^k(Q) = \pm Q$ for all $Q \in E$ and $T_2 \notin \mathrm{Ker}\ \psi$.
- Let $\mu' = \mathrm{Tr}_\psi(\mu)$ and redefine the factor basis

$$\mathcal{F}_{E,\mu'} = \{P \in E(\mathbb{F}_{q^n}) : \mu'(P) \in \mathbb{F}_q\}.$$

Theorem (T.- Ionica 2021)

The factor basis $\mathcal{F}_{E,\mu'}$ is invariant under T_2 and ψ. Morever, the summation polynomial $S_{n,\mu'}$ is invariant under the action of the group $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes S_n$.

Experiments on GLV-GLS curve defined over $\mathbb{F}_{q^2}$

Longa and Sica 2012 the GLS endomorphism + the CM endomorphism

For instance take ϕ with $\phi^2 + \phi + 1 = 0$ and ψ with $\psi^2 + 1 = 0$. Then $\mathcal{F}_{\mu'}$ is invariant under ϕ and ψ.

q	Time reduced basis	Time full basis	Reduction ratio
739	1.412 sec.	5.722 sec.	4.052
1051	3.475 sec.	14.909 sec.	4.290
2731	9.001 sec.	42.628 sec.	4.730
3163	11.037 sec.	58.304 sec.	5.280

Magma implementation 2.40GHz Intel Xeon E5-2680

Experiments for curves over composite extension field

In this case, we use the Frobenius endomorphism to reduce the size of the factor basis.

q	m_1	m_2	Time reduced base	Time full base	ratio
2	2	7	0.229 sec.	1.63 sec.	7.1
2	3	11	1039.4 sec.	11442.4 sec.	11
2	2	17	154755.566 sec.	2727802.448 sec.	17.6