Introduction to elliptic curve cryptography Sub-exponential algorithms for the discrete logarithm problem

Sorina Ionica

Laboratoire MIS, Université de Picardie Jules Verne, France

May 16, 2018

Index calculus : general idea

Let $\mathbb{G}$ be a finite cylic group of order r.

- Choose a factor base $\mathcal{F} = \{P_1, \dots P_n\}$.
- Search for relations : Choose random $a_i \in \mathbb{Z}$ and try to decompose

$$a_i P = \sum_{i=1}^{n} c_{ij} P_j.$$

  until n relations are found.

- Linear algebra : Let $A = (a_i)_{i=\overline{1,n}}$ and $M = (c_{ij})_{i,j}$.
  - Find $v = (v_1, \dots, v_n)$ the unique solution to $XM = A \pmod{r}$

An example

Index calculus in a prime field $\mathbb{F}_p$

- the factor base: prime integers (mod p) smaller than a certain smoothness bound B.
- Relation search: take random combinations and factor them

Let $p = 83$. Set the factor base $\mathcal{F} = \{2, 3, 5, 7\}$.

$\underline{2^1 = 2}$
$2^9 = 14 = 2 \cdot 7$
$2^{12} = 29$
$2^{15} = 66 = 2 \cdot 3 \cdot 11$

$\underline{2^7 = 45 = 3^2 \cdot 5}$
$2^{10} = 28 = 2^2 \cdot 7$
$2^{13} = 58 = 2 \cdot 29$
$2^{16} = 49 = 7^2$

$\underline{2^8 = 7}$
$2^{11} = 56 = 2^3 \cdot 7$
$2^{14} = 33 = 3 \cdot 11$
$\underline{2^{17} = 3 \cdot 5}$.

An example

$$\begin{array}{c} \begin{matrix} 2 & 3 & 5 & 7 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \end{array} \cdot X = \begin{pmatrix} 1 \\ 7 \\ 8 \\ 17 \end{pmatrix}$$

Thus $\log_2(2) = 1, \log_2(3) = 72, \log_2(5) = 27, \log_2(7) = 8$.

Index calculus : general idea

Let $\mathbb{G}$ be a finite cylic group of order r.

- Choose a factor base $\mathcal{F} = \{P_1, \dots P_n\}$.
- Search for relations : Choose random $a_i \in \mathbb{Z}$ and try to decompose

$$a_i P = \sum_{j=1}^{n} c_{ij} P_j.$$

  until n relations are found.

- Linear algebra : Let $A = (a_i)_{i=\overline{1,n}}$ and $M = (c_{ij})_{i,j}$.
  - Find $v = (v_1, \dots, v_n)$ the unique solution to $XM = A \pmod r$
- Descent phase: find a relation involving Q :
  $aP + bQ = \sum_{i=1}^{n} c_i P_i$, where $\gcd(b, r) = 1$
  and compute the DLP of Q as $(\sum_{j=1}^{n} c_j v_j - a) b^{-1} \pmod r$

An example

$$\begin{array}{c} \begin{matrix} 2 & 3 & 5 & 7 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \end{array} \cdot X = \begin{pmatrix} 1 \\ 7 \\ 8 \\ 17 \end{pmatrix}$$

Thus $\log_2(2) = 1, \log_2(3) = 72, \log_2(5) = 27, \log_2(7) = 8.$

We have $31^2 = 48 = 2^4 \cdot 3 \Rightarrow 2\log_2(31) = 76 \Rightarrow \log_2(31) = 38.$

Complexity

- Relation search : specific to the group that is considered
  Intuitively, the larger $\mathcal{F}$ is, the higher the probability of decomposition
- Linear algebra : $O((\#\mathcal{F})^{\omega})$, with $\omega = 2.81$.
  $\Rightarrow$ the Lanczos and Wiedemann algorithms for sparse linear algebra $O((\#\mathcal{F})^2)$

Balance the costs of the two phases

Complexity

Given a prime number p, one can compute a discrete log in $\mathbb{F}_p$ in expected time

$$O(\exp(\sqrt{2} \cdot (\log p \log\log p)^{1/2})).$$

This is subexponential in $\log p$.

Index calculus in finite fields

- $\mathbb{G} \subset (\mathbb{F}_q^*, \times)$, $\mathrm{char}\ \mathbb{F}_q$ large : subexponential time $O(exp((\frac{96}{9})^{1/3}(\log q)^{1/3}(\log\log q)^{2/3})$ (Joux-Lercier 2006)
- $\mathbb{G} \subset (\mathbb{F}_q^*, \times)$, $\mathrm{char}\ \mathbb{F}_q$ small : subexponential time $O(exp((\frac{96}{9})^{1/3}(\log q)^{1/4}(\log\log q)^{3/4})$ (Joux 2013)
- $\mathbb{G} \subset (\mathbb{F}_q^*, \times)$, $\mathrm{char}\ \mathbb{F}_q$ large : subexponential time $O(exp((\frac{48}{9})^{1/3}(\log q)^{1/3}(\log\log q)^{2/3})$ (Kim-Barbulescu 2016), $q = p^n$, n composite

Index calculus in elliptic curve groups

Search for decompositions of the type $R = P_1 + P_2 + \dots P_n$.

Semaev's summation polynomials

There is a polynomial $f_{n+1} \in \mathbb{F}_p[X_1, \dots X_{n+1}]$ such that $R = P_1 + \dots P_n$ iff $f_{n+1}(x_R, x_{P_1}, \dots, x_{P_n}) = 0$.

- No known way to define the factor base for elliptic curves defined over $\mathbb{F}_p$.
- Gaudry's algorithm for the case where E is an elliptic curve defined over $\mathbb{F}_{p^n}$, using Semaev's ideas

Key lengths

Table : Complexity of generic attacks

method	Fastest known attack
RSA	Number Field Sieve $exp(\frac{1}{2}(logN)^{\frac{1}{3}}(log \log N)^{\frac{2}{3}})$
ECC	Pollard-rho $\sqrt{r} = exp(\frac{1}{2}\log r)$
Finite fields $\mathbb{F}_q$	NFS $exp((\frac{96}{9})^{1/3}(logq)^{\frac{1}{3}}(log \log q)^{\frac{2}{3}})$

A cryptographic scheme is said to offer a n bits security level if an attaquer has to perform 2^n operations to break the underlying mathematical problem.

Key lengths

Table : Complexity of generic attacks

method	Fastest known attack
RSA	Number Field Sieve $exp(\frac{1}{2}(logN)^{\frac{1}{3}}(log \log N)^{\frac{2}{3}})$
ECC	Pollard-rho $\sqrt{r} = exp(\frac{1}{2} \log r)$
Finite fields $\mathbb{F}_q$	NFS $exp((\frac{96}{9})^{1/3}(logq)^{\frac{1}{3}}(log \log q)^{\frac{2}{3}})$

Table : Key sizes

Security level	RSA	ECC	$\mathbb{F}_q$
80 bits	1024	160	1024
128 bits	3072	256	3072
256 bits	15360	512	15360

http://www.keylength.com