A Las Vegas algorithm to solve Elliptic Curve Discrete Logarithm Problem

Ayan Mahalanobis Vivek Mohan Mallick Ansari Abdullah

Indocrypt 2018
December 11, 2018

Overview of the talk

We propose a new attack on the ECDLP.

Overview of the talk

We propose a new attack on the ECDLP.

The attack reduces ECDLP to a problem in linear algebra. We call that Problem L.

Overview of the talk

We propose a new attack on the ECDLP.

The attack reduces ECDLP to a problem in linear algebra. We call that Problem L.

The reduction algorithm is a Las Vegas algorithm with high probability of success.

Overview of the talk

We propose a new attack on the ECDLP.

The attack reduces ECDLP to a problem in linear algebra. We call that Problem L.

The reduction algorithm is a Las Vegas algorithm with high probability of success.

We made some progress in solving Problem L, we report on that.

Overview of the talk

We propose a new attack on the ECDLP.

The attack reduces ECDLP to a problem in linear algebra. We call that Problem L.

The reduction algorithm is a Las Vegas algorithm with high probability of success.

We made some progress in solving Problem L, we report on that.

We implemented our algorithm using NTL, we report on some experimental data.

The discrete logarithm problem

We assume that $\mathcal{E}(\mathbb{F}_q)$ be a group of prime order p. Let P and Q be two non-identity points, such that, $Q = mP$ for $1 \leq m < p$. The discrete logarithm problem is to find the m.

The discrete logarithm problem

We assume that $\mathcal{E}(\mathbb{F}_q)$ be a group of prime order p. Let P and Q be two non-identity points, such that, $Q = mP$ for $1 \leq m < p$. The discrete logarithm problem is to find the m.

Attacks on DLP

There are two kinds of attack on DLP.

- One is generic attack.
- Other kind of attacks are the index-calculus kind of attacks on DLP.

The discrete logarithm problem

We assume that $\mathcal{E}(\mathbb{F}_q)$ be a group of prime order p. Let P and Q be two non-identity points, such that, $Q = mP$ for $1 \leq m < p$. The discrete logarithm problem is to find the m.

Attacks on DLP

There are two kinds of attack on DLP.

- One is generic attack.
- Other kind of attacks are the index-calculus kind of attacks on DLP.

Non-generic attack

Our attack is of the second kind.

A theorem

Definition

An elliptic curve $\mathcal{E}$ over a field $\mathbb{F}_q$ is a non-singular plane curve of degree 3 together with a point $\mathcal{O}$.

Theorem

Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_q$ and $P_1, P_2, \ldots, P_k$ be points on that curve, where $k = 3n'$ for some positive integer n'. Then $\sum_{i=1}^{k} P_i = \mathcal{O}$ if and only if there is a curve $\mathcal{C}$ of degree n' that passes through these points. Multiplicities are intersection multiplicities.

How to use the theorem

- Choose k such that $k = 3n'$ for some positive integer n'.
- Choose random non-identity points $P_1, P_2, \ldots, P_s$ and $Q_1, Q_2, \ldots, Q_t$ such that $s + t = k$.
- Check if there is a homogeneous curve of degree n' that passes through these points; where $P_i = n_i P$ and $Q_j = -n'_j Q$ for some integers n_i and n'_j.
- If there is a curve, the discrete logarithm problem is solved.
- Otherwise repeat the process.
- To choose these points P_i and Q_j, we choose a random point n_i, n'_j and compute $n_i P$ and $-n'_j Q$.
- We would choose n_i and n'_j to be distinct from the ones chosen before to give rise to distinct points P_i and Q_j on $\mathcal{E}$.

How do we know if there is a curve

Let $C = \sum_{i+j+k=n'} a_{ijk} x^i y^j z^k$ be a complete homogeneous curve of degree n'. An ordering of i, j, k is fixed and C is presented according to that ordering. By complete we mean that the curve has all the possible monomials of degree n'. We need to check if P_i, $i = 1, 2, \ldots, s$ and Q_j for $j = 1, 2, \ldots, t$ satisfy the curve C. Note that, there is no need to compute the values of a_{ijk}, just mere existence will solve the discrete logarithm problem.

How do we know if there is a curve

Let $C = \sum_{i+j+k=n'} a_{ijk} x^i y^j z^k$ be a complete homogeneous curve of degree n'. An ordering of i, j, k is fixed and C is presented according to that ordering. By complete we mean that the curve has all the possible monomials of degree n'. We need to check if P_i, $i = 1, 2, \ldots, s$ and Q_j for $j = 1, 2, \ldots, t$ satisfy the curve C. Note that, there is no need to compute the values of a_{ijk}, just mere existence will solve the discrete logarithm problem.

Let P be a point on $\mathcal{E}$. We denote by $\overline{P}$ the value of C when the values of x, y, z in P is substituted in C. Similarly for Qs. We now form a matrix $\mathcal{M}$ where the rows of $\mathcal{M}$ are $\overline{P_i}$ for $i = 1, 2, \ldots, s$ and $\overline{Q_j}$ for $j = 1, 2, \ldots, t$. If this matrix has a non-zero left-kernel, we have solved the discrete logarithm problem. By *left-kernel* we mean the kernel of $\mathcal{M}^{\mathsf{T}}$, the transpose of $\mathcal{M}$.

Why look at left-kernel

We use $\mathcal{K}$ for the left-kernel of $\mathcal{M}$ and $\mathcal{K}'$ as the (right) kernel.

Why look at left-kernel

We use $\mathcal{K}$ for the left-kernel of $\mathcal{M}$ and $\mathcal{K}'$ as the (right) kernel.

Theorem

The following are equivalent:

(A) $\mathcal{K} = 0$.

(B) $\mathcal{K}'$ *only contain curves that are a multiple of* $\mathcal{E}$.

Why look at left-kernel

We use $\mathcal{K}$ for the left-kernel of $\mathcal{M}$ and $\mathcal{K}'$ as the (right) kernel.

Theorem

The following are equivalent:

(A) $\mathcal{K} = 0$.

(B) $\mathcal{K}'$ *only contain curves that are a multiple of* $\mathcal{E}$.

Take the number of points $k = 3n' + l$, then

Theorem

If $l \geq 1$, *the dimension of the left kernel of* $\mathcal{M}$ *is* l.

What really works

Corollary

Assume that $\mathcal{M}$ has $3n' + l$ rows, computed from the same number of points of the elliptic curve $\mathcal{E}$. If there is a curve $\mathcal{C}$ intersecting $\mathcal{E}$ non-trivially in $3n'$ points among $3n' + l$ points, then there is a vector v in $\mathcal{K}$ with at least l zeros. Conversely, if there is a vector v in $\mathcal{K}$ with at least l zeros, then there is a curve $\mathcal{C}$ passing through those $3n'$ points that correspond to the non-zero entries of v in $\mathcal{M}$.

What is the advantage

In the exhaustive search we would have picked a random set of $3n'$ points and then checked to see if the sum of those points is Q. In the above algorithm we are taking a set of $3n' + l$ points and then checking all possible $3n'$ subsets of this set simultaneously. There are $\binom{3n'+l}{l}$ such subsets. This is one of the main advantage of our algorithm.

The algorithm

A sketch of the algorithm

Choose $k = 3n' + l$.

- Choose points from the elliptic curve.
- Construct the matrix $\mathcal{M}$.
- Compute the left-kernel $\mathcal{K}$ of $\mathcal{M}$.
- If the left kernel contains a vector with l zeros we are done.
- If not, repeat.

Problem L

Problem

Let W be a l-dimensional subspace of a n-dimensional vector space V. The vectors in the vectors space are presented as linear sum of some fixed basis of V. The problem is to determine, if W contains a vector with l zeros. If there is one such vector, find that vector.

Theorem

When p tends to infinity, the probability of success of the above algorithm is approximately $1 - \frac{1}{e} \approx 0.6321$. The number of rows of the matrix $\mathcal{M}$ required to reach this probability is $O(\log p)$. This makes our algorithm polynomial in both time and space complexity.

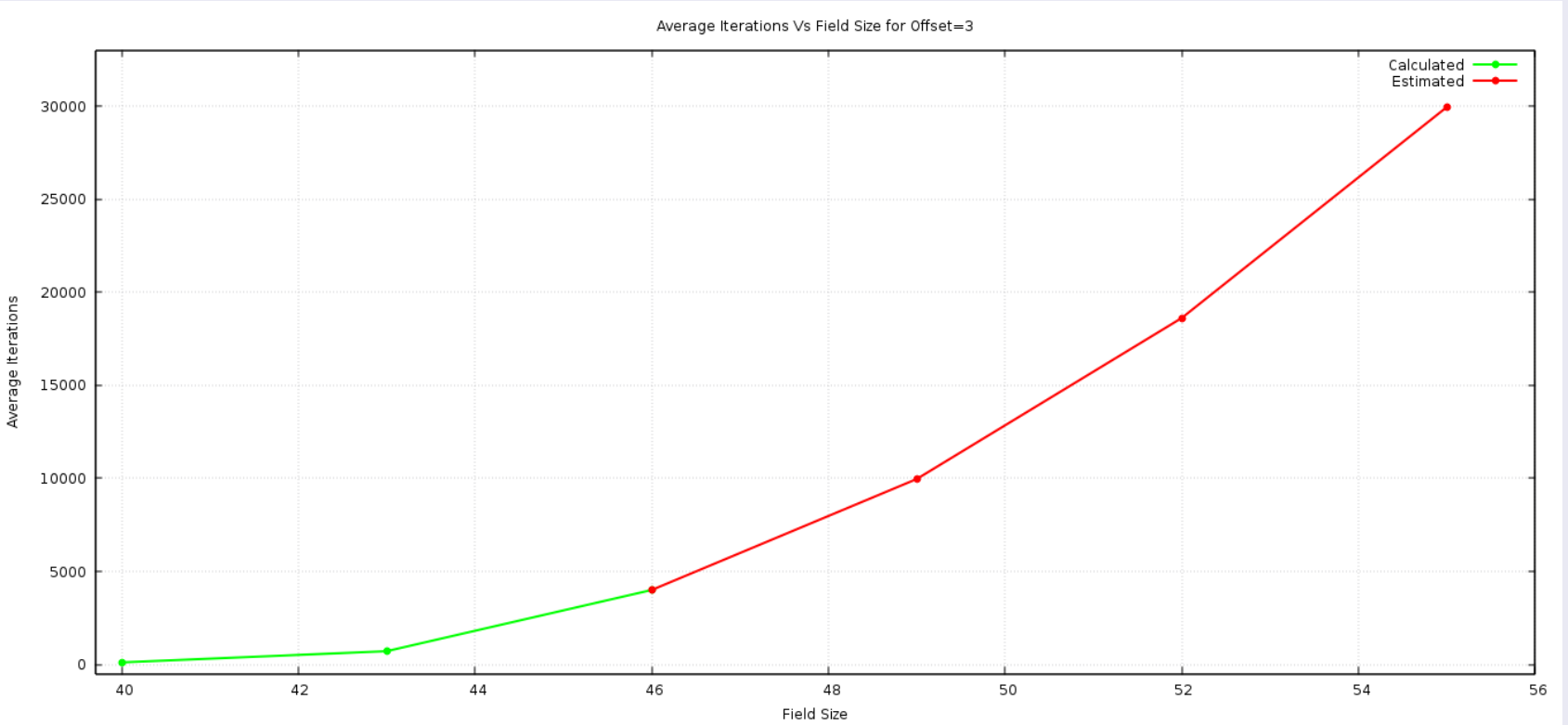
Solving Problem L

Take $3n' = l$. Then $\mathcal{K}$ is two $l \times l$ matrix stacked sideways.

$$\mathcal{K} = \left[\begin{array}{cccc|cccc} * & * & \dots & \cdots & 0 & \cdots & 0 & 1 \\ * & * & \dots & \cdots & 0 & \cdots & 1 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ * & * & \dots & \cdots & 1 & 0 & \cdots & 0 \end{array}\right]$$

- The matrix $\mathcal{K}$ Is the basis for the left-kernel $\mathcal{K}$. The size of the matrix is $l \times 2l$. We look for a square sub-matrix with determinant zero from the left part.
- In particular, for the purpose of this talk we look at the 2×2 submatrix.

Some experimental results



- Number of iterations 40. The average number of kernels computed is the y-axis. The x-axis is the size of the field.
- Number of cores used 66.