A Las Vegas algorithm to solve the elliptic curve discrete logarithm problem

Ayan Mahalanobis* Vivek Mallick†

February 5, 2018

Abstract

In this paper, we describe a new Las Vegas algorithm to solve the elliptic curve discrete logarithm problem. The algorithm depends on a property of the group of rational points of an elliptic curve and is thus not a generic algorithm. The algorithm that we describe has some similarities with the most powerful index-calculus algorithm for the discrete logarithm problem over a finite field.

1 Introduction

Public-key cryptography is a backbone of this modern society. Many of the public-key cryptosystems depend on the *discrete logarithm problem* as their cryptographic primitive. Of all the groups used in a discrete logarithm based protocol, the group of *rational points of an elliptic curve* is the most popular. In this paper, we describe a **Las Vegas algorithm** to solve the elliptic curve discrete logarithm problem.

There are two kinds of attack on the discrete logarithm problem. One is generic. This kind of attack works in any group. Examples of such attacks are the baby-step giant-step attack [7, Proposition 2.22] and Pollard's rho [7, Section 4.5]. The other kind of attack depends on the group used. Example of such attack is the index-calculus attack [7, Section 3.8] on the multiplicative group of a finite field. An attack similar to index calculus for elliptic curves, known as xedni calculus, was developed by Silverman [8, 11]. However, it was found to be no better than exhaustive search. Another simailar work in the direction of ours is Semaev [10].

In this paper, we describe an attack which is particular to the elliptic curves. The attack is a Las Vegas algorithm. The attack uses a theorem for elliptic curve. The idea behind the attack is completely new and is of a completely different genre from the existing ones [1, 3–5]. In comparison to xedni calculus, our algorithm is fairly straightforward to understand, implement and is better than the exhaustive search.

*ayan.mahalanobis@gmail.com
†vmallick@iiserpune.ac.in

The main algorithm is divided into two algorithms. The first one reduces the elliptic curve discrete logarithm problem to a problem in linear algebra. We call the linear algebra problem, Problem L. This reduction is a Las Vegas algorithm with **probability of success** 0.6 and is **polynomial** in both time and space complexity. The second half of the algorithm is solving Problem L. This is the current bottle-neck of the whole algorithm and better algorithms to solve Problem L will produce better algorithms to solve elliptic curve discrete logarithm problem. The success of the main algorithm is $0.6 \times (\log p)^2/p$ where every pass is polynomial time in time and space complexity.

1.1 The central idea behind our attack

Let G be a cyclic group of prime order p. Let P be a non-identity element and $Q(= mP)$ belong to G. The *discrete logarithm problem* is to compute the m. One way to find m is to find integers n_i, for $i = 1, 2, \ldots, k$ for some positive integer k and $1 \leq n_i < p$ such that $\sum_{i=1}^{k} n_i = m \bmod p$. The last equality is hard to compute because we do not know m. However we can decide whether

$$\sum_{i=1}^{k} n_i P = Q \tag{1}$$

and based on that we can decide if $\sum_{i=1}^{k} n_i = m \bmod p$. Once the equality holds, we have found m and the discrete logarithm problem is solved.

The number of possible choices of n_i for a given k that can solve the discrete logarithm problem is the number of partitions of m into k parts modulo a prime p. The applicability of the above method depends on, how fast can one decide on the equality in the above equation and on the probability, how likely is it that a given set of positive integers n_i sums to $m \bmod p$?

An obvious question is raised, can one choose a set of n_i in such a way that the probability of an equality is higher than the random selection? In the next section, we find a way to check for equality in the case of elliptic curves, however our choice of n_i is uniformly random. Then the algorithm is somewhat straightforward, fix a k, choose n_i uniformly random and then check for equality. Once there is a set of n_i for which the equality is found, we have solved the discrete logarithm problem.

2 The elliptic curve discrete logarithm problem

The elliptic curve discrete logarithm problem (ECDLP) is the heart and soul of modern public-key cryptography. This paper is about a new probabilistic algorithm to solve this problem. Our algorithm is a fairly straightforward application of the Riemann-Roch theorem. We denote by $\mathcal{E}(\mathbb{F}_q)$ the group of rational points of the elliptic curve $\mathcal{E}$ over $\mathbb{F}_q$. It is well known that there is an isomorphism $\mathcal{E}(\mathbb{F}_q) \to \mathrm{Pic}^0(\mathcal{E})$ given by $P \mapsto [P] - [\mathcal{O}]$ [9, Proposition 4.10].

Theorem 2.1. *Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_q$ and $P_1, P_2, \dots, P_k$ 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.*

Proof. Assume that $\sum_{i=1}^{k} P_i = \mathcal{O}$ in $\mathbb{F}_q$ and then it is such in the algebraic closure $\bar{\mathbb{F}}_q$. From the above isomorphism, $\sum_{i=1}^{k} P_i \mapsto \sum_{i=1}^{k}[P_i] - k[\mathcal{O}]$. Then $\sum_{i=1}^{k}[P_i] - k[\mathcal{O}]$ is zero in the Picard group $\mathrm{Pic}^0_{\bar{\mathbb{F}}_q}(\mathcal{E})$. Then there is a rational function $\dfrac{\phi}{z^{n'}}$ over $\bar{\mathbb{F}}_q$ such that

$$\sum_{i=1}^{k}[P_i] - k[\mathcal{O}] = \mathrm{div}\left(\frac{\phi}{z^{n'}}\right) \tag{2}$$

Bezout's theorem justifies that $\deg(\phi) = n'$, since ϕ is zero on $P_1, P_2, \dots, P_k$. We now claim, there is ψ over $\mathbb{F}_q$ which is also of degree n' and passes through $P_1, P_2, \dots, P_k$. First thing to note is that there is a finite extension of $\mathbb{F}_q$, $\mathbb{F}_{q^N}$(say) in which all the coefficients of ϕ lies and $\gcd(q, N) = 1$. Let G be the Galois group of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$ and define

$$\psi = \sum_{\sigma \in \mathcal{G}} \phi^{\sigma}. \tag{3}$$

Clearly $\deg(\psi) = n'$. Note that, since P_i for $i = 1, 2, \dots, k$ is in $\mathbb{F}_q$ is invariant under σ. Furthermore, σ being a field automorphism, P_i is a zero of ϕ^{σ} for all $\sigma \in G$. This proves that P_i are zeros of ψ and then Bezout's theorem shows that these are the all possible zeros of ψ on $\mathcal{E}$. The only thing left to show is that ψ is over $\mathbb{F}_q$. To see that, lets write $\phi = \sum_{i+j+k=n'} a_{ijk} x^i y^j z^k$. Then $\psi = \sum_{i+j+k=n'} \sum_{\sigma \in G} a^{\sigma}_{ijk} x^i y^j z^k$. However, it is well known that $\sum_{\sigma \in G} a^{\sigma} \in \mathbb{F}_q$ for all $a \in \mathbb{F}_{q^N}$.

Conversely, if we are given a curve $\mathcal{C}$ of degree n' that passes through $P_1, P_2, \dots, P_k$. Then consider the rational function $\mathcal{C}/z^{n'}$. Then this function has zeros on P_i, $i = 1, 2, \dots, k$ and poles of order k at $\mathcal{O}$. The above isomorphism says $\sum_{i=1}^{k} P_i = \mathcal{O}$. ■

2.1 How to use the above theorem in our algorithm

We choose k such that $k = 3n'$ for some positive integer n'. Then we choose random points $P_1, P_2, \dots, P_s$ and $Q_1, Q_2, \dots, Q_t$ such that $s + t = k$ from $\mathcal{E}$ and 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 by choosing a new set of points $P_1, P_2, \dots, P_s$ and $Q_1, Q_2, \dots, Q_t$. 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. This gives rise to distinct points P_i and Q_j on $\mathcal{E}$.

The only question remains, how do we say if there is a homogeneous curve of degree n' passing through these selected points? One can answer this question using linear algebra.

Let $C = \sum_{i+j+k=n'} a_{ijk} x^i y^j z^k$ be a *complete* homogeneous curve of degree n'. We assume that an ordering of i, j, k is fixed throughout this paper 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. In other words, $\overline{P}$ is a linear combination of a_{ijk} with the fixed ordering. 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 $\mathcal{M}^{\mathrm{T}}$, the transpose of $\mathcal{M}$.

2.2 Why look at the left-kernel instead of the kernel

In this paper, we will use the left-kernel more often than the (right)kernel of $\mathcal{M}$. We denote the left-kernel by $\mathcal{K}$ and kernel by $\mathcal{K}'$. We first prove the following theorem:

Theorem 2.2. *The following are equivalent:*

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

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

Proof. The proof uses a simple counting argument. First recall the well-known fact that the number of monomials of degree d is $\binom{d+2}{2}$. Furthermore, notice two things – all multiples of $\mathcal{E}$ belongs to $\mathcal{K}'$ and the dimension of that vector-space (multiples of $\mathcal{E}$) is $\binom{n'-1}{2} = \dfrac{(n'-2)(n'-1)}{2}$, where n' is as defined earlier.

Now, $\mathcal{M}$ was as defined earlier, has $3n'$ rows and $\dfrac{(n'+1)(n'+2)}{2}$ columns. Then $\mathcal{K} = 0$ means that the row-rank of $\mathcal{M}$ is $3n'$. So the dimension of the $\mathcal{K}'$ is

$$\frac{(n'+1)(n'+2)}{2} - 3n' = \frac{(n'-2)(n'-1)}{2}.$$

This proves (a) implies (b).

Conversely, if $\mathcal{K}'$ contains all the curves that are a multiple of $\mathcal{E}$ then its dimension is at least $\dfrac{(n'-2)(n'-1)}{2}$, then the rank is $3n'$, making $\mathcal{K} = 0$. ■

It is easy to see, while working with the above theorem $\mathcal{M}$ cannot repeat any row. So from now onward we would assume that $\mathcal{M}$ has no repeating rows. For all practical purposes this means that we are working with distinct(unique) partitions.

A question that becomes significantly important later is, instead of choosing k points from the elliptic curve what happens if we choose $k + l$ points for some positive integer l. The answer to the question lies in the following theorem.

Theorem 2.3. *If $l \geq 1$, the dimension of the left kernel of $\mathcal{M}$ is l.*

Proof. First assume $l \geq 1$. In this case, any non-trivial element of $\mathcal{K}'$ will define a curve which passes through more than $3n'$ point of the elliptic curve. Since the elliptic curve is irreducible, it must be a component of the curve. Thus the equation defining the curve must be divisible by the equation defining the elliptic curve. Thus, the dimension of $\mathcal{K}'$ is the dimension of all degree n' homogeneous polynomials which are divisible by the elliptic curve. This is the same is the dimension of all degree $n' - 3$ homogeneous polynomials. Thus, we get

$$\dim(\mathcal{K}') = \frac{(n'-2)(n'-1)}{2}.$$

On the other hand, by rank-nullity theorem, it follows:

$$\begin{aligned} \dim(\mathcal{K}') + \dim(\text{image}(\mathcal{M})) &= \tfrac{(n'-2)(n'-1)}{2} \\ \dim(\mathcal{K}) + \dim(\text{image}(\mathcal{M}^{\mathrm{T}})) &= 3n' + l. \end{aligned}$$

Thus, since row rank and the column rank of a matrix are equal,

$$\dim(\mathcal{K}) = 3n' + l - \frac{(n'-2)(n'-1)}{2} + \dim(\mathcal{K}') = l.$$

■

Corollary 2.4. *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 $\mathcal{M}$.*

Proof. Assume that there is a non-trivial curve $\mathcal{C}$ intersecting $\mathcal{E}$ in $3n'$ points. Then construct the matrix $\mathcal{M}'$ whose rows are the points of intersection. Then from the earlier theorem we see that $\mathcal{K}$ for this matrix $\mathcal{M}'$ is non-zero. In all the vectors of $\mathcal{K}$ if we put zeros in the place where where we deleted rows then those are element of the left kernel of $\mathcal{M}$. It is clear that these vectors will have at least l zeros.

Conversely, if there is a vector with at least l zeros in $\mathcal{K}$, then by deleting l zeros from the vector and corresponding rows from $\mathcal{M}$ we have the required result from the theorem above. ■

2.3 Veronese embedding and our algorithm

There is an alternate way of looking at our algorithm through Veronese embedding [6, Page 21: Example 2.4]. We present that in this section.

We know that the sum of $3n'$ points $P_1, P_2, \ldots, P_{3n'}$ on an elliptic curve $\mathcal{E}$, embedded in $\mathbb{P}^2$, is zero if and only if there exists a curve C of degree n' in $\mathbb{P}^2$ such that the algebraic-geometric intersection $C \cap \mathcal{E}$ is the set $\{P_1, \ldots, P_{3n'}\}$, counting multiplicity. Given a collection of points $\mathcal{P} = \{P_1, P_2, \ldots, P_{3n'+l}\}$ on the elliptic curve, we need to find some subset that has sum zero. To find this subset, we try to find a curve of degree n'

which passes through $3n'$ points of $\mathcal{P}$. This can be thought of in the following way in terms of the Veronese embedding.

Recall that the Veronese embedding $\nu_{n'} : \mathbb{P}^2 \to \mathbb{P}^D$ where $D = \frac{(n'+1)(n'+2)}{2}$, is given by $\nu_{n'}(x_0 : x_1 : x_2) = (z_1 : z_2 : \cdots : z_D)$, where $z_i = x_1^{a_1^i} x_2^{a_2^i} x_3^{a_3^i}$ for some bijection

$$\begin{aligned} \Phi : \{k \in \mathbb{Z} \,|\, 1 \le k \le D\} &\to \left\{(n_1, n_2, n_3) \in \mathbb{N}^3 \,\middle|\, n_1 + n_2 + n_3 = n'\right\}. \\ i &\mapsto (a_1^i, a_2^i, a_3^i) \end{aligned}$$

We claim that a curve passes through $3n'$ points $\{P_{m_i},\ 1 \le i \le 3n'\}$ if and only if $\nu_{n'}(P_{m_i})$ lie in a hyperplane H of $\mathbb{P}^D$. First, suppose that the curve of degree n', given by the equation $\sum_{i,j,k:i+j+k=n'} c_{ijk} x_1^i x_2^j x_3^k = 0$. Consider, the hyperplane H given by the equation

$$H(z_1, \ldots, z_D) = \sum_{i=1}^{D} c_{\Phi(i)} z^D.$$

It is clear that $\nu_{n'}(P_{m_i}) \in H$. On the other hand, if $\nu_{n'}(P_{m_i}) \in H = \sum_{i=1}^D h_i z_i$, they lie on the curve $\sum_{i=1}^D h_i x_1^{a_1^i} x_2^{a_2^i} x_3^{a_3^i}$ where $(a_1^i, a_2^i, a_3^i) = \Phi(i)$ as above.

To put it in an algebraic-geometric context, let v be the composition

$$\begin{tikzcd} \mathcal{E} \arrow[r, tail] \arrow[rr, bend right, "v"'] & \mathbb{P}^2 \arrow[r, "\nu_{n'}"] & \mathbb{P}^D. \end{tikzcd}$$

The intersection of $\mathcal{E}$ with a curve of degree n' corresponds to the zeroes of a section of a degree n' line bundle. Any such line bundle is the pull-back of a degree 1 line bundle on $\mathbb{P}^D$ via the Veronese map $\nu_{n'}$. The H, as defined above, defines the degree 1 divisor corresponding to this line bundle on $\mathbb{P}^D$. Thus, the problem of finding which $3n'$ points among a collection of points $\mathcal{P}$ on an elliptic curve lie on a degree n' curve reduces to finding which $3n'$ points in the image $\nu_{n'}(\mathcal{P})$ lie on a hyperplane. The latter is the linear algebra problem that we are interested in.

3 The main algorithm – reducing ECDLP to a linear algebra problem (Problem L)

The algorithm that we present in this paper has two parts. One reduces it to a problem in linear algebra and the other solves that linear algebra problem which we call Problem L. The first algorithm, Algorithm 1, is Las Vegas in nature with high success probability. Furthermore, the algorithm is polynomial time in both time and space complexity.

Algorithm 1: Reducing ECDLP to a linear algebra problem (Problem L)

```
Data: Two points $P$ and $Q$, such that $mP = Q$
Result: $m$
Select a positive integers, $n'$ and $l = 3n'$. Initialize a matrix with $3n' + l$ rows
  and $\binom{n'+2}{2}$ columns. Initialize a vector $\mathcal{I}$ of length $3n' - 1$ and another vector $\mathcal{J}$
  of length $l + 1$. Initialize integers $A, B = 0$.
repeat
    for $i = 1$ to $3n' - 1$ do
        repeat
            choose a random integer $r$ in the range $[1, p)$
        until $r$ is not in $\mathcal{I}$
        $\mathcal{I}[i] \leftarrow r$
        compute $rP$
        compute $\overline{rP}$
        insert $\overline{rP}$ as the $i^{\text{th}}$ row of the matrix $\mathcal{M}$
    end
    for $i = 1$ to $l + 1$ do
        repeat
            choose a random integer $r$ in the range $[1, p)$
        until $r$ is not in $\mathcal{J}$
        $\mathcal{J}[i] \leftarrow r$
        compute $-rQ$
        compute $\overline{-rQ}$
        insert $\overline{-rQ}$ as the $(3n' + i - 1)^{\text{th}}$ row of the matrix $\mathcal{M}$
    end
    compute $\mathcal{K}$ as the left-kernel of $\mathcal{M}$
until $\mathcal{K}$ has a vector $v$ with $l$ zeros (Problem L)
for $i = 1$ to $3n' - 1$ do
    if $v[i] \neq 0$ then
        $A = A + \mathcal{I}[i]$
    end

end
for $i = 3n'$ to $3n' + l$ do
    if $v[i] \neq 0$ then
        $B = B + \mathcal{J}[i - 3n' + 1]$
    end

end
return $A \times B^{-1} \bmod p$
```

3.0.1 Why is this algorithm better than exhaustive search

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.

3.0.2 Probability of success of the above algorithm

To compute the probability, we need to understand the number of unique partitions of an integer m modulo a prime p. For our definition of partition, order of the parts does not matter. The number of partitions is proved in the following theorem:

Theorem 3.1. *Let k be an integer greater than 2. The number of k unique partitions of m modulo a odd prime p is* $\dfrac{(p-1)(p-2)\ldots(p-k+2)(p-k)}{k!}$.

Proof. The argument is a straight forward counting argument. We think of k parts as k boxes. Then the first box can be filled with $p-1$ choices, second with $p-2$ choices as so on. The last but one, $k-1$ box can be filled with $p-k+1$ choices. When all $k-1$ boxes are filled then there is only one choice for the last box, it is m minus the sum of the other boxes. So it seems that the count is $(p-1)(p-2)\ldots(p-k+1)$ choices.

However there is a problem, the choice in the last box might not be different from the first $k-1$ choices. To remove that possibility we remove a choice from the last but one box. That choice is m minus the sum of the first $k-2$ boxes divided by 2.

Since order does not matter, we divide by $k!$. ■

Consider the event, m is fixed, we pick k integers less than p. What is the probability that those numbers form a partition of m. From the above theorem, number of favorable events is $\dfrac{(p-1)(p-2)\ldots(p-k+2)(p-k)}{k!}$ and the total number of events is $\binom{p}{k}$. Since for all practical purposes k is much smaller than p, we approximate the probability to be $\frac{1}{p}$.

Now we look at the probability of success of our algorithm. In our algorithm we choose $3n'$ points from $3n' + l$ points. This can be done in $\binom{3n'+l}{l}$ ways. Then the probability of success of the algorithm is $1 - \left(1 - \frac{1}{p}\right)^{\binom{3n'+l}{l}}$.

Let us first look at the $\left(1 - \frac{1}{p}\right)^{p}$. It is well known that $\left(1 - \frac{1}{p}\right)^{p}$ tends to $\frac{1}{e}$ when p tends to infinity. So if we can make $\binom{3n'+l}{l}$ close to p, then we can claim the asymptotic probability of our algorithm is $1 - \frac{1}{e}$ which is greater than $\frac{1}{2}$.

Since we are dealing with matrices, it is probably the best that we try to keep the size of it as small as possible. Note that the binomial coefficient is the biggest when it is of the form $\binom{2n}{n}$ for some positive integer n. Furthermore, from Stirling's approximation it follows that for large enough n, $\binom{2n}{n} \approx \frac{4^n}{\sqrt{\pi n}}$.

So, when we take $3n' = l$ and such that $\binom{3n'+l}{l} = p$ then l is the solution to the equation $l = O(1) + \log l + \log p$.

To understand the time complexity of this algorithm (without the linear algebra problem), the major work done is finding the kernel of a matrix. Using Gaussian elimination, there is an algorithm to compute the kernel which is cubic in time complexity. Thus we have proved the following theorem:

Theorem 3.2. *When p tends to infinity, the probability of success of the above algorithm is approximately $1 - \frac{1}{e} \approx 0.6321$. The size of the matrix required to reach this probability is $O(\log p)$. This makes our algorithm polynomial in both time and space complexity.*

3.1 Few comments

3.1.1 Accidentally solving the discrete logarithm problem

It might happen, that while computing rP and rQ in our algorithm, it turns out that for some r_1 and r_2, $r_1P = r_2Q$. In that case, we have solved the discrete logarithm problem. We should check for such accidents. However, in a real life situation, the possibility of an accident is virtually zero, so we ignored that in our algorithm completely.

3.1.2 On the number of Ps and Qs in our algorithm

The algorithm will take as input P and Q and produce different Ps and Qs and the produce a vector v with l many zeros. If all of these l zeros fall either in the place of Ps or Qs exclusively, then we have not solved the discrete logarithm problem. To avoid this, we have chosen Ps and Qs of roughly same size, with one more P than Q. This way the vector v will have atleast one non-zero in the place of both P and Q.

3.1.3 Allowing, detecting and using multiple intersection points in our algorithm

One obvious idea to make our algorithm slightly faster: allow multiplicities of intersection between the curve C and the elliptic curve $\mathcal{E}$. This will increase the computational complexity. Since the elliptic curve is smooth at the points one is interested in, one observes that with high probability the multiplicity of intersection will coincide with the multiplicity of the point in C. This reduces to checking if various partial derivatives are zero. This can easily be done by introducing extra rows in the matrix $\mathcal{M}$. Then the algorithm reduces to finding vectors with zeroes in a particular pattern. This is same as asking for special type of solutions in Problem L. However, this has to be implemented efficiently as probability of such an event occurring is around $1/p$ for large primes p.

4 Dealing with the linear algebra problem

This paper provides an efficient algorithm to reduce the elliptic curve discrete logarithm problem to a problem in linear algebra. We call it the Problem L.

At this stage we draw the attention of the reader to some similarities that emerge between the most powerful attack on the discrete logarithm problem over finite fields, the index-calculus algorithm, and our algorithm. In an index-calculus algorithm, the discrete logarithm problem is reduced to a linear algebra problem. Similar is the case with our algorithm. However, in our case, the linear algebra problem is of a different genre and not much is known about this problem. In this paper, we have not been able to solve the linear algebra problem completely. However, we made some progress and we report on that in this section.

Problem L. *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.*

This problem is connected with the earlier algorithm in a very straightforward way. We need to determine if the left-kernel of the matrix $\mathcal{M}$ contains a vector with l zeros and that is where Problem L must be solved efficiently for the overall algorithm to run efficiently. As is customary, we would assume that the kernel $\mathcal{K}$ is presented as a matrix of size $l \times (3n' + l)$, where each row is an element of the basis of $\mathcal{K}$.

A algorithm that we developed, uses Gaussian elimination algorithm multiple times to solve Problem L. In particular we use the row operations from the Gaussian elimination algorithm. Abusing our notations slightly, we denote the basis matrix of $\mathcal{K}$ by $\mathcal{K}$ as well. Now we can think of $\mathcal{K}$ to be made up of two blocks of $l \times l$ matrix. Our idea is to do Gaussian elimination to reduce each of these blocks to a diagonal matrix one after the other. The reason that we do that is, when the first block has been reduced to diagonal, every row of the matrix has at least $l - 1$ zeros. So we are looking for another zero in some row. The row reduction that produced the diagonal matrix in the first block might also have produced that extra zero and we are done. However, if this is not the case, we go on to diagonalize the second block and check for that extra zero like we did for the first block.

Algorithm 2: Multiple Gaussian elimination algorithm

```
Data: The basis matrix $\mathcal{K}$
Result: Determine if Problem L is solved. If yes, output the vector that solves
        Problem L
for $i$=1 to 2 do
    row reduce block $i$ to a lower triangular block
    check all rows of the new matrix to check if any one has $l$ zeros
    if there is a row with $l$ zeros then
        STOP and return the row
    end
    row reduce the lower-triangular block to a diagonal block
    check all rows of the new matrix to check if any one has $l$ zeros
end
STOP (Problem L not solved)
```

5 Complexity, implementation and conclusion

5.1 Complexity

We describe the complexity of the whole algorithm in this section. First note that the whole algorithm is the composition of two algorithms, one is Algorithm 1, which has success probability 0.6 and the other is the linear algebra problem. It is easy to see from conditional probability that the probability of success of the whole algorithm is the product of the probability of success of Algorithm 1 and Algorithm 2.

Let us now calculate the probability of Algorithm 2 under the condition that Algorithm 1 is successful. In other words, we know that Algorithm 1 has found a $\mathcal{K}$ whose span contains a vector with l zeros. What is the probability that Algorithm 2 will find it?

Notice that Algorithm 2 can only find zero if they are in certain positions and the number of such positions is l^2. Total number of ways that there can be l zeros in a vector of size $3n' + l$ is $\binom{3n'+l}{l}$. In our setting we have already assumed that $\binom{3n'+l}{l} \approx p$. Then the probability of success of the whole algorithm is

$$0.6 \times \frac{(\log p)^2}{p}.$$

Which is a significant improvement over exhaustive search!

One thing to notice, the probability of success is $1 - \left(1 - \frac{1}{p}\right)^{\binom{3n'+l}{l}}$ and in the probability estimate we have $\binom{3n'+l}{l}$ in the denominator. Furthermore, one observes that in this paper we have taken $\binom{3n'+l}{l}$ to approximately equal the prime p. One can now question our choice and argue, if we took $\binom{3n'+l}{l}$ to be much smaller than p, we might get a better algorithm. Alas, this is not the case, $1 - \left(1 - \frac{1}{p}\right)^{p^{\frac{1}{n}}}$ tends to 0 as p tends to infinity for $n \geq 2$.

5.2 Implementation

We have implemented the algorithm in sage [2]. Since the complexity of the algorithm is only little better than exhaustive search there is no point in providing details of implementation. However, we would like to mention that the algorithm works flawlessly with elliptic curves on fields of all characteristics.

5.3 Conclusion

We conclude this paper by saying that we have found a new genre of attack against the elliptic curve discrete logarithm problem. This attack has some similarities with the well-known index-calculus algorithm. In an index-calculus algorithm, the discrete logarithm problem is reduced to a problem in linear algebra and then the linear algebra problem is solved. However, the similarities are only skin deep as our linear algebra problem in completely new.

References

[1] D. Bernstein and T. Lange. Non-uniform cracks in the concerete: the power of free precomputation. In *Advances in Cryptology – ASIACRYPT 2013*, volume 8270 of *LNCS*, pages 321–340, 2013.

[2] The Sage Developers. *SageMath, the Sage Mathematics Software System*, 2016. `http://www.sagemath.org`.

[3] S. Galbraith and P. Gaudry. Recent progress on the elliptic curve discrete logarithm problem. *Designs, Codes and Cryptography*, 78:51–78, 2016.

[4] S. Galbraith and S. Gebregiyorgis. Summation polynomial algorithms for elliptic curves in characteristic two. In *Progress in Cryptology – INDOCRYPT 2014*, volume 8885 of *LNCS*, pages 409–427, 2014.

[5] Pierrick Gaudry. Index calculus for abeian varieties of small dimension and the elliptic curve discrete logarithm problem. *Journal of Symbolic computation*, 44:1690–1702, 2009.

[6] Joe Harris. *Algebraic Geometry.* Springer, 1992.

[7] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An introduction to mathematical cryptography.* Springer, 2008.

[8] Michael J. Jacobson, Neal Koblitz, Joseph H. Silverman, Andreas Stein, and Edlyn Teske. Analysis of the xedni calculus attack. *Designs, Codes and Cryptography*, 20(1), 41-64 2000.

[9] J. S. Milne. *Elliptic Curves.* BookSurge Publishers, 2006.

[10] Igor Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. https://eprint.iacr.org/2004/031, 2004.

[11] Joseph H. Silverman. The xedni calculus and the elliptic curve discrete logarithm problem. *Designs, Codes and Cryptography*, 20(1):5–20, 2000.

IISER Pune, Pashan, Pune, INDIA