International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.6 Aug-Sept – 2022
DOI:10.46647/ijetms.2022.v06i05.019 ISSN: 2581-4621

Using Oblique Elimination to Solve Elliptic Curve Discrete Logarithm Problem

Abdullah Ansari
Department of Scientific Computing, modeling and simulation - Savitribai Phule Pune University, Pune, Maharashtra

ABSTRACT
The elliptic curve discrete logarithm problem is believed to be a secure cryptographic primitive for over three and a half decades. This problem was reduced to a problem in linear algebra problem by a Las Vegas algorithm. That algorithm was presented in IndoCrypt 2018. It was further shown that the linear algebra problem can be solved by zero minors. In this paper, we propose oblique elimination as a way to solve the elliptic curve discrete logarithm problem. This paper provides an improved version of the oblique elimination algorithm along with an example. This paper also provides an implementation of the oblique elimination algorithm.

Keywords – Public key cryptography, ECDLP, LasVegas, Gaussian Elimination, Oblique Elimination.

1. Introduction

The integer factorization problem, the discrete logarithm problem and the elliptic curve discrete logarithm problem (ECDLP) form the basis of modern public-key cryptography. Transport Layer Security (TLS) defines a set of rules known as a protocol that governs the security of communications over a computer network. TLS 1.3, published in 2018, uses ECDLP as a cryptographic primitive.

Let **E** be a non-singular elliptic curve over $\mathbb{F}_q$. In this paper all curves are projective plane curves and O is the point at infinity. This point O also serves as the identity of the group of rational points of **E**. With a slight abuse of notation, we will denote the group of rational points of **E** by **E** as well. We will further assume that **E** is of prime order p. Since any group of prime order is cyclic, in this paper we assume that **E** is generated by P. Let Q = mP where $1 \leq m < p$. The elliptic curve discrete logarithm problem is to find the integer m.

ECDLP was proposed to be used in public-key cryptography in 1985 by Koblitz [8] and Miller [10]. Since then, this problem has been under attack. Many algorithms or attacks have been proposed to solve this problem. One notable attack was developed by Semaev [11]. This attack has been studied extensively. For more on this attack see [6].

Mahalanobis et al. [9] proposed a new attack on ECDLP. This work was followed up by Ansari et al. [2]. In the first paper it was shown that one can solve ECDLP using Gaussian elimination. It was then noticed that this Gaussian elimination is actually the same as finding a 2 × 2 zero-minor in a non-singular matrix over $\mathbb{F}_q$. In the second paper, the idea of finding a non-zero minor was formally put down [2, Section 3]. Then a way to move from 2 × 2 minor to a minor of arbitrary size was adopted by using Schur complements. In this paper, we try to find a 2 × 2 zero minor using oblique elimination.

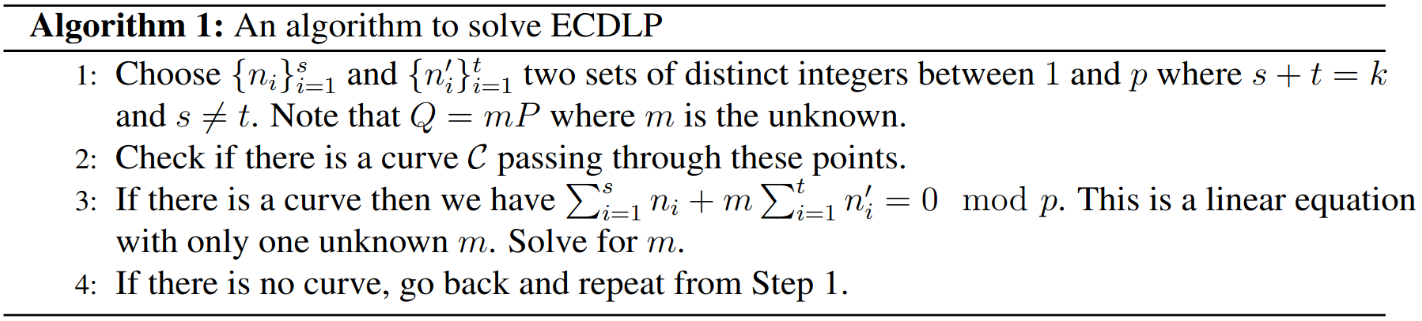
2. A LasVegas algorithm to solve the elliptic curve discrete logarithm problem

Recall that a subgroup of the group of rational points of a projective elliptic curve **E** over a finite field $\mathbb{F}_q$ of order p a prime is considered for the elliptic curve discrete logarithm problem. Let O be the point at infinity and the additive identity of **E**. We are only dealing with plane projective curves in this paper. The algorithm that we summarize in this section was already presented by Mahalanobis et. al. [9]. So, this exposition will be less formal but more intuitive. Recall that in the discrete logarithm problem there are two points P and Q (= mP) in **E**. The problem is to compute the integer m. For sake of simplicity, we assume that $0 < m < p$. Our standard reference for elliptic curve discrete logarithm problem is Hoffstein et. al. [7, Chapter 5]. We state Theorem 5.36 (b) from that book.

Theorem 1.*Let D =* $\sum_{P\in E}$ P *be a divisor on* ***E****. Then D is the divisor of a rational function on* ***E*** *if and only if deg(D) = 0 and sum(D) = O.*

Let n' be a positive integer and $k = 3n'$. Now notice that the polynomial z^n intersects the elliptic curve **E** at the point of infinity $3n'$ times counting multiplicity. Thus, for any rational function $\frac{f}{z^{n'}}$where$f$is a homogeneous projective plane curve of degree n' intersects **E** at $3n'$ points. Those points become points of a divisor on **E**. If those set of points are P_i , $1 < i < k$, from the above theorem, we see that $\sum_{i=1}^{k} P_i = O$.

The whole algorithm is based on this simple idea. Before we state it, let us define C to be a plane projective curve $\sum_{i+j+k=n'} a_{i,j,k}x^i y^j z^k$ where $i, j, k \geq 0$. In the algorithm, we are looking for the existence of such C for some chosen distinct points $\{P_i;\ i = 1, 2, \ldots, k\}$ on **E**. The algorithm can be simply stated as follows:



```
Algorithm 1: An algorithm to solve ECDLP
1: Choose $\{n_i\}_{i=1}^{s}$ and $\{n'_i\}_{i=1}^{t}$ two sets of distinct integers between 1 and $p$ where $s + t = k$
   and $s \neq t$. Note that $Q = mP$ where $m$ is the unknown.
2: Check if there is a curve $\mathcal{C}$ passing through these points.
3: If there is a curve then we have $\sum_{i=1}^{s} n_i + m \sum_{i=1}^{t} n'_i = 0 \mod p$. This is a linear equation
   with only one unknown $m$. Solve for $m$.
4: If there is no curve, go back and repeat from Step 1.
```

The only problem above is how to check if there is a curve, i.e., *Step 2*. Solving this makes solving the elliptic curve discrete logarithm problem by the above algorithm so rewarding. The above ideas that we explained can be put together in the form of a theorem.

Theorem 2. *Let* ***E*** *be an elliptic curve over* $\mathbb{F}_q$ *and* $P_1, P_2, P_3, \ldots, P_k$ *be points on it, where*$k = 3n'$ *for some positive integer* n' *. Then* $\sum_{i=1}^{k} P_i$ *if and only if there is a curve C over* $\mathbb{F}_q$ *of degree* n' *that passes through these points.*

One way we try to solve *Step 2*, is to construct a matrix M. The rows of that matrix is the polynomial C evaluated at P_i and $Q_i$where$P_i = n_i P$ and $Q_i = n' Q_i$. These are points on the elliptic curve. Then the kernel K′ of M contain the plane projective homogeneous curves that passes through these points $\{P_i\}$ and $\{Q_i\}$ of the elliptic curve.

However, the situation is hopeless from an algorithmic point of view, because most of the curves that one finds from this kernel K' contain the elliptic curve **E**. But when one looks at the following theorem it is not so hopeless when dealing with the *left-kernel* of M. Recall the left-kernel is the kernel of the transpose M^T.

Theorem 3. *The following are equivalent:*
(a) The left-kernel K of M is the zero subspace.

(b) The kernel(right) K' only contains curves that are a multiple of E.

Now the algorithm is clear. Pick $k$distinct points. If the matrix M does not have a non-zero left-kernel, a new set of k points are chosen and the algorithm restarts. This approach generates k points and checks if there is a curve passing through them which is the same as trying to partition the unknown integer m into some parts. This algorithm has complexity the same as the exhaustive search. Thus, this algorithm is useless.
The situation improves significantly and becomes interesting when instead of $k$points we choose $k + l$ points. Then the algorithm tests if there is a curve that passes through any $k$points out of these $k + l$ points. This approach checks if any of the k points of $k + l$points satisfy the curve C. Thus, we get to check $l$points simultaneously. It was shown that the complexity is the best when have $k = l$. Henceforth, we assume that the *left-kernel* K of M is of size $l \times 2l$. The following theorem is from [9]

Theorem 4. *If $l \geq 1$then the dimension of the left kernel of M is l.*

The following corollary from [2] supports the previous statement.

Theorem 5. *Assume that M has $3n' + l$ rows, computed from the same number of points of the elliptic curve E. If there is a curve C intersecting E non-trivially in $3n'$ points, among $3n' + l$ points, then there is a vector v in K with at least l zeros. Conversely, if there is a vector v in K with at least l zeros, then there is a curve C passing through those $3n'$ points that correspond to the non-zero entries of v in M.*

From the above theorem we see that we are looking for a vector with $l$zeros in the left-kernel K. It is hard to imagine how to go about looking for that. In the next section we move into a more precise way of finding such a vector by changing the problem to a problem of finding a zero-minor in a non-singular matrix.

3. Using minors to solve ECDLP

Recall that the matrix K is $2l \times l$ matrix over $\mathbb{F}_q$. It is straight-forward to see that that matrix K can be written in this form:

$$\mathcal{K} = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \dots & a_{1,l} & 0 & 0 & \dots & 0 & 1 \\ a_{2,1} & a_{2,2} & a_{2,3} & \dots & a_{2,l} & 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{l,1} & a_{l,2} & a_{l,3} & \dots & a_{l,l} & 1 & 0 & \dots & 0 & 0 \end{pmatrix}$$

One can arrive to the above matrix from the original K by row-reduction. The right-hand side is the transpose of a $l \times l$ identity matrix over $\mathbb{F}_q$. We will be mostly interested in the non-identity left-sided $l \times l$ part of the above matrix. We will call it A. It is safe to assume that it is a non-singular $l \times l$ matrix over $\mathbb{F}_q$. Furthermore, it is safe to assume that A has no zero entries, or else the discrete logarithm problem is solved. Thus, it is clear that every row of K has precisely $l - 1$zeros.
Let α and β be non-empty subsets of {1, 2, 3, . . ., l} of same size with the same ordering as {1, 2, 3, . . ., l}. Let A[α|β] is the square sub-matrices of A whose elements are the intersection of rows from α and columns from β. The minor A[α|β] is the determinant of the sub-matrix.

In [2] it was shown that if det(K[α|β]) = 0 then there exists a vector with $l$zeros in K. A formal proof is given in Ansari et al. [2]. We will not repeat the proof, but the idea is easy to see through. If we have a zero minor in A, look at the corresponding rows of the submatrix. By row-operations we can reduce the last row of that sub-matrix to a zero row. Now think of the same row operations in K. It will provide zeros the size of the minor in the A-part of the matrix. Keeping in mind the sparse nature of the other part of K, this same row operations will create non-zero entries in the row, which has given the zero row in the submatrix with zero minor. The number of non-zero entries thus created is on the right-hand side of the matrix K. Because of the 1 present in that row, the number of non-zero entries thus created by the row-operations in K is one less than the number of zero entries created on the left-hand side of K i.e., A. The statement of the theorem follows:

Theorem 6. *If det(K[α|β]) = 0 for some non-empty subset α, β ⊆{1, 2, 3, ..., k}, there exists a vector with k zero in the linear span of the rows of the left-kernel K. Furthermore, the position of zeros are positions β and {k + i : i ∉α}.*

The following example illustrates the above theorem.

$$\mathcal{K}_0 = \begin{bmatrix} 70 & 18 & 1 & 17 & 10 & 0 & 0 & 0 & 0 & 1 \\ 10 & 13 & 54 & 43 & 48 & 0 & 0 & 0 & 1 & 0 \\ 23 & 43 & 8 & 24 & 57 & 0 & 0 & 1 & 0 & 0 \\ 29 & 29 & 56 & 61 & 48 & 0 & 1 & 0 & 0 & 0 \\ 49 & 38 & 21 & 46 & 27 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$\mathcal{A}_0$ has a 2×2 zero minor,

$$M^{\alpha}_{\beta} = det \begin{vmatrix} 70 & 18 \\ 10 & 13 \end{vmatrix} = 0$$

$$\alpha = \{1, 2\} \; and \; \beta = \{1, 2\}$$

Row one from $\mathcal{K}_0$ can be reduced by the operation $R_1 - (7 \times R_2)$.

$$\mathcal{A}_1 = \begin{bmatrix} 0 & 0 & 61 & 8 & 39 & 0 & 0 & 0 & 66 & 1 \\ 10 & 13 & 54 & 43 & 48 & 0 & 0 & 0 & 1 & 0 \\ 23 & 43 & 8 & 24 & 57 & 0 & 0 & 1 & 0 & 0 \\ 29 & 29 & 56 & 61 & 48 & 0 & 1 & 0 & 0 & 0 \\ 49 & 38 & 21 & 46 & 27 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The matrix A_1 has now five zeros in the first row. This solves the elliptic curve discrete logarithm problem. Thus, if there exists a zero minor in A the elliptic curve discrete logarithm problem is solved. Thus, we now see that the new problem that mutated from the elliptic curve discrete logarithm problem is to find a zero minor in a non-singular matrix.

4. The Oblique Elimination method

The oblique elimination method was first proposed by Tchuente [13] and was further improved by Gader [5]. The improved version was called minimal variables oblique elimination by Gader [5]. In this paper, oblique elimination means minimal variable oblique elimination. In this paper, we study oblique elimination in a slightly different way from that given in Gader [5]. In this section, we develop our modified version of oblique elimination. The modified oblique elimination is similar to the classical Gaussian elimination as both the methods reduce the columns to zero using row operations. However, Gaussian elimination works top-down in a straight-line fashion. But oblique elimination works diagonally. Before we go any further, we need to define an oblique for a matrix.

Definition 6.1 *(Oblique). Let A be a* $l \times l$ *matrix. Then the* i^{th} *oblique of A is defined as* {$a_{l-i+1,1}$, $a_{l-i+2,2}$, $a_{l-i+3,3}$, . . ., $a_{l,i}$} *where i ∈[1, l].*

Just like Gaussian elimination, oblique elimination reduces a matrix to an upper triangular matrix. The oblique elimination that we implemented repeatedly reduces obliques one after the other to zero. It starts from the bottom left and then coming down the oblique by using row operations.

Oblique elimination uses the element above the elements of an oblique and uses row-operation to reduce the oblique to zero. Note that in our case, if we have a zero above any oblique then we have the extra zero in a row and ECDLP is solved. The element $a_{i,j}$ of an oblique is reduced by multiplying the $i-1$ row of the matrix with $\frac{-a_{i,j}}{a_{i-1,j}}$. Thus, i^{th} row is reduced using row operation $R_i + \left(-a_{i,j}/a_{i-1,j}\right)R_{i-1}$.Notice that we are going down diagonally down from left to right in the matrix. This is necessary to see that the zero that we made is not corrupted by other row-operations. After reducing an element in the oblique, we check for the new row for *l-zeros*. If such a row exists, the ECDLP is solved.

The following illustrate the oblique elimination process.

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} \\ a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} \end{bmatrix}$$

We start with the first iteration reducing element $a_{5,1}$ using the element $a_{4,1}$. The second iteration reduces $a_{4,1}$, $a_{5,2}$ using $a_{3,1}$and $a_{4,2}$ respectively. Similarly, the third iteration reduces the third oblique having elements $a_{3,1}$, $a_{4,2}$, $a_{5,3}$ using elements, $a_{2,1}$, $a_{3,2}$, $a_{4,3}$ respectively.

This approach of oblique elimination is more efficient than the algorithm proposed by Gader [5] where there are numerous matrix multiplications in place of row-operations. Algorithm 2 provides a high-level description of the modified oblique elimination. We used the modified oblique elimination in our experiment. Algorithm 2 was implemented in C++ using NTL [12] and is available online [1].

Algorithm 2: Modified Oblique Elimination

```
Input: Matrix $M$ & oblique to be reduced
Output: When a row with $l$-zeros is found
row = number of rows in M
col = 0
for $i$ : row to 1 do
    ele = $-\frac{M[i][col]}{M[i-1][col]}$
    M[i] = M[i] + (ele * M[i-1])
    if $M$ contains $l$-zeros then
        DLP is solved - STOP
```

5. Example of Oblique Elimination

The following example demonstrates oblique elimination, as described in algorithm 2. Let A be a 5×5 matrix over $\mathbb{F}_{43}$.

$$A = A_0 = \begin{bmatrix} 26 & 30 & 25 & 10 & 29 \\ 9 & 22 & 6 & 3 & 19 \\ 12 & 32 & 34 & 27 & 6 \\ 17 & 2 & 25 & 21 & 38 \\ 29 & 22 & 23 & 26 & 42 \end{bmatrix}$$

The first oblique has element {29}. We reduce the first oblique using the row operation $R_5 + \left(-\frac{29}{17}\right) R_4$ simplifying this expression results in $R_5 + 16R_4$to get

$$A_1 = \begin{bmatrix} 26 & 30 & 25 & 10 & 29 \\ 9 & 22 & 6 & 3 & 19 \\ 12 & 32 & 34 & 27 & 6 \\ 17 & 2 & 25 & 21 & 38 \\ 0 & 11 & 36 & 18 & 15 \end{bmatrix}$$

Now, we check if the row has *l-zeros*. If we find *l-zeros* we stop, else we continue.
The second iteration reduces the second oblique. Second oblique of A_1 has elements {17, 11}. The first element in this oblique is 17 and is reduced using the element above it. The following row operation is performed $R_4 + \left(-\frac{17}{12}\right) R_3$ simplifying this expression; we get $R_4 + 38R_3$ after this row operation we get,

$$A_2 = \begin{bmatrix} 26 & 30 & 25 & 10 & 29 \\ 9 & 22 & 6 & 3 & 19 \\ 12 & 32 & 34 & 27 & 6 \\ 0 & 14 & 27 & 15 & 8 \\ 0 & 11 & 36 & 18 & 15 \end{bmatrix}$$

Now, we search for *l-zeros* in the fourth row. If it has *l-zeros* we stop, otherwise we continue. The second oblique element is 11 and is reduced using the row-operation $R_5 + 33R_4$ to get, the following and we check for *l-zeros* in the fifth row.

$$A_3 = \begin{bmatrix} 26 & 30 & 25 & 10 & 29 \\ 9 & 22 & 6 & 3 & 19 \\ 12 & 32 & 34 & 27 & 6 \\ 0 & 14 & 27 & 15 & 8 \\ 0 & 0 & 24 & 40 & 11 \end{bmatrix}$$

Similarly, the third iteration reduces the third oblique {12, 14, 24} from A_3 using the row operations$R_3 + 13R_2$, $R_4 + 17R_3$ and $R_5 + 6R_4$for the third, fourth and the fifth row respectively. Now, we get

$$A_4 = \begin{bmatrix} 26 & 30 & 25 & 10 & 29 \\ 9 & 22 & 6 & 3 & 19 \\ 0 & 17 & 26 & 23 & 39 \\ 0 & 0 & 14 & 34 & 10 \\ 0 & 0 & 0 & 18 & 35 \end{bmatrix}$$

We check if a row with *l-zeros* exists in A_4 , if such a row exists, we stop, otherwise we continue. The last oblique can be reduced in a similar manner.

6. Conclusion

This work presents oblique elimination as an alternative to Gaussian elimination to solve ECDLP. Gaussian, oblique elimination both reduce an input matrix to an upper triangular matrix. Even though both these algorithms stop when we have an upper triangular matrix, both of the algorithms have different approaches. Gaussian elimination works top down whereas oblique elimination works bottom up. This difference enables us to have an alternative approach to understand and solve ECDLP. In this paper we have developed an efficient algorithm for oblique elimination. The proposed algorithm avoids the matrix multiplication step which was employed in original oblique elimination method.

References

1. Ansari Abdullah. Las vegas ecdlp. https://bitbucket.org/abdullah0096/lasvegas-ecdlp.git, 2022.
2. Ansari Abdullah, Ayan Mahalanobis, and Vivek M Mallick. A new method for solving the elliptic curve discrete logarithm problem. Journal of Groups, complexity, cryptology, 12, 2021.
3. Tsuyoshi Ando. Totally positive matrices. Linear algebra and its applications, 90:165–219, 1987.
4. Richard A Brualdi and Hans Schneider. Determinantal identities: Gauss, Schur, Cauchy, Sylvester, Kronecker, Jacobi, Binet, Laplace, Muir, and Cayley. Linear Algebra and its applications, 52:769–791, 1983.
5. Paul D Gader. Tridiagonal factorizations of Fourier matrices and applications to parallel computations of discrete fourier transforms. Linear Algebra and its Applications, 102:169–209, 1988.
6. Steven D. Galbraith, Robert Granger, Simon-Philipp Merz, and Christophe Petit. On index calculus algorithms for subfield curves. In Orr Dunkelman, Michael J. Jacobson, Jr., and Colin O'Flynn, editors, Selected Areas in Cryptography, pages 115–138, Cham, 2021. Springer International Publishing.
7. Jeffrey Hoffstein, Jill Pipher, Joseph H Silverman, and Joseph H Silverman. An introduction to mathematical cryptography, volume 1. Springer, 2008.
8. Neal Koblitz. Elliptic curve cryptosystems. Mathematics of computation, 48(177):203–209, 1987.
9. Ayan Mahalanobis, Vivek Mohan Mallick, and Ansari Abdullah. A las vegas algorithm to solve the elliptic curve discrete logarithm problem. In International Conference on Cryptology in India, pages 215–227. Springer, 2018.
10. Victor S Miller. Use of elliptic curves in cryptography. In Conference on the theory and application of cryptographic techniques, pages 417–426. Springer, 1985.
11. Igor Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. Cryptology ePrint Archive, 2004.
12. Victor Shoup. NTL - a library for doing number theory. https://libntl.org/, 2022.
13. Maurice Tchuente. Parallel calculation of a linear mapping on a computer network. Linear Algebra and its Applications, 28:223–247, 1979.